The Data Link Layer

Chapter 3

Data Link Layer Design Issues

- Network layer services
- Framing
- Error control
- Flow control

Data Link Layer Design Issues

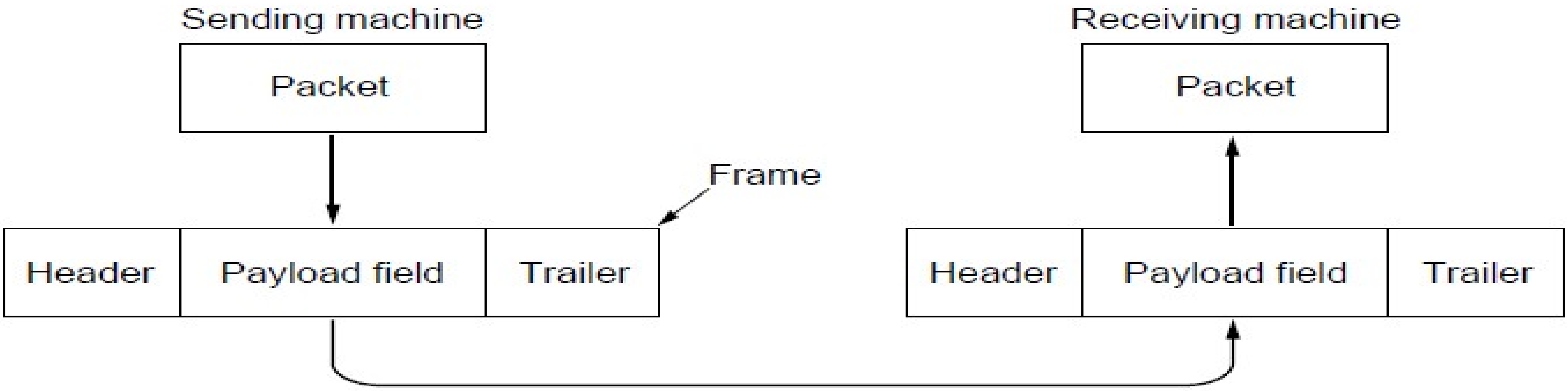
- Physical layer delivers bits of information to and from data link layer. The functions of Data Link Layer are:
  1. Providing a well-defined service interface to the network layer.
  2. Dealing with transmission errors.
  3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

- Data Link layer
  - Takes the packets from Network layer, and
  - Encapsulates them into **frames**

Data Link Layer Design Issues

- Each frame has a
  - Frame header
  - Payload field: a field for holding the packet, and
  - Frame trailer.
- Frame Management is what Data Link Layer does.

Packets and Frames

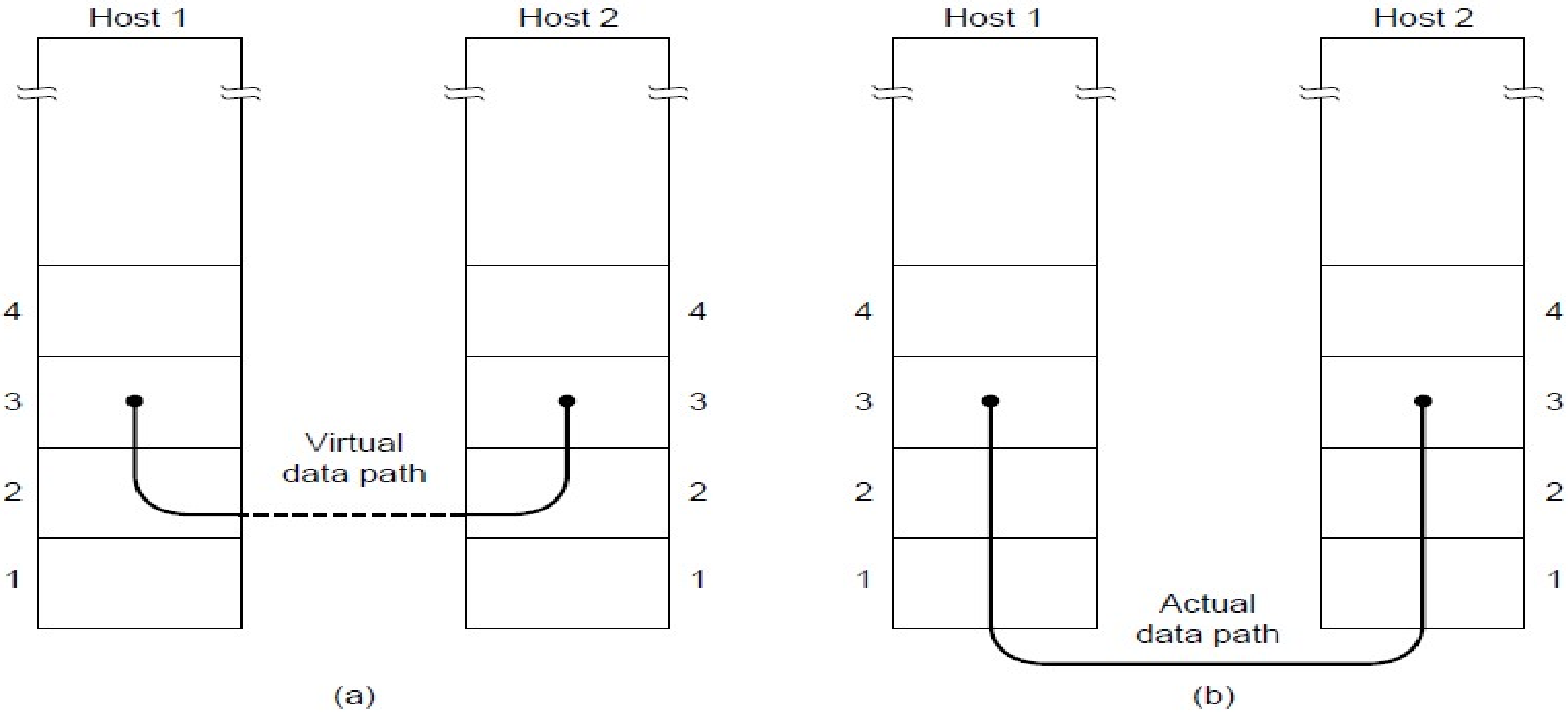


Relationship between packets and frames.

Services Provided to the Network Layer

- Principal Service Function of the data link layer is to transfer the data from the network layer on the source machine to the network layer on the destination machine.

Network Layer Services



(a) Virtual communication. (b) Actual communication.

Possible Services Offered

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service.

Unacknowledged Connectionless Service

- It consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

Acknowledged Connectionless Service

- Each frame send by the Data Link layer is acknowledged and the sender knows if a specific frame has been received or lost.
- Typically the protocol uses a specific time period that if has passed without getting acknowledgment it will re-send the frame.

Acknowledged Connection Oriented Service

- Source and Destination establish a connection first.
- Each frame sent is numbered
  - Data link layer guarantees that each frame sent is indeed received.
  - It guarantees that each frame is received only once and that all frames are received in the correct order.
- Examples:
  - Satellite channel communication,
  - Long-distance telephone communication, etc.

Acknowledged Connection Oriented Service

- Three distinct phases:
  1. Connection is established by having both side initialize variables and counters needed to keep track of which frames have been received and which ones have not.
  2. One or more frames are transmitted.
  3. Finally, the connection is released – freeing up the variables, buffers, and other resources used to maintain the connection.

Framing

- To provide service to the network layer the data link layer must use the service provided to it by physical layer.
- Stream of data bits provided to data link layer is not guaranteed to be without errors.
- Errors could be:
  - Number of received bits does not match number of transmitted bits (deletion o insertion)
  - Bit Value
- It is up to data link layer to correct the errors if necessary.

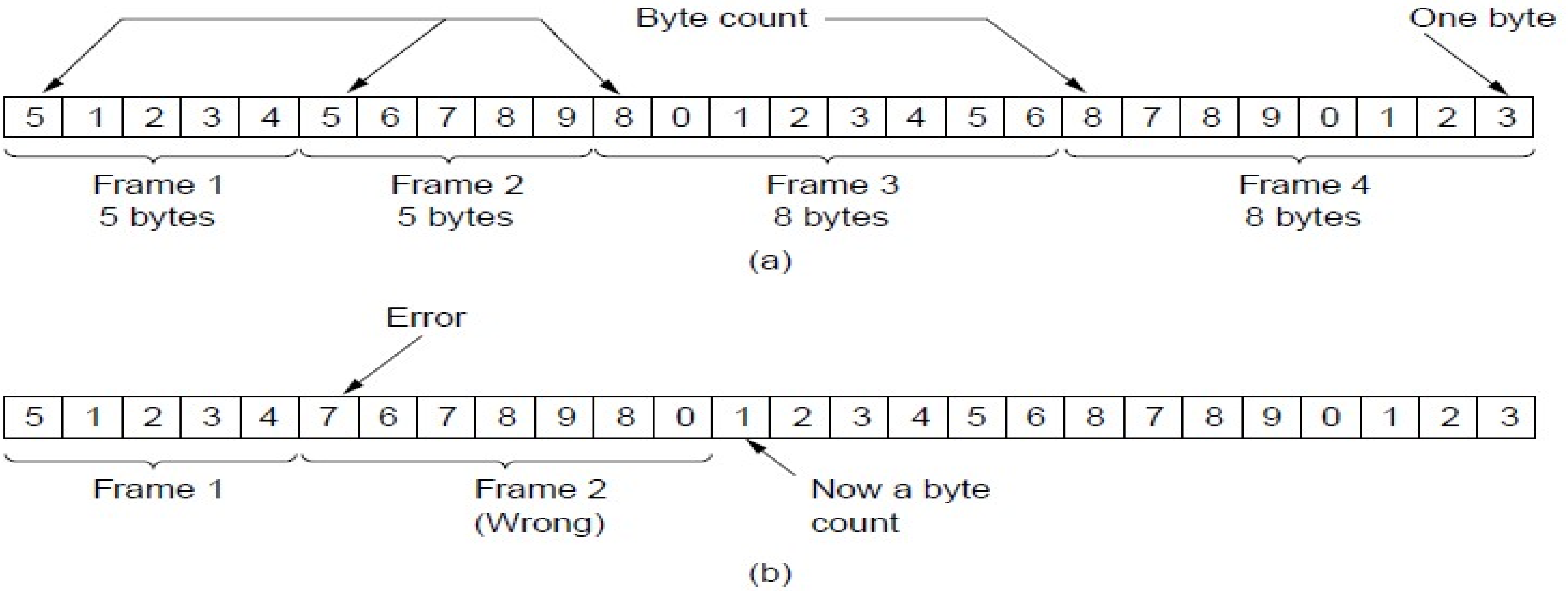
Framing

- Transmission of the data link layer starts with breaking up the bit stream
  - into discrete frames
  - Computation of a checksum for each frame, and
  - Include the checksum into the frame before it is transmitted.
- Receiver computes its checksum error for a receiving frame and if it is different from the checksum that is being transmitted will have to deal with the error.

Framing Methods

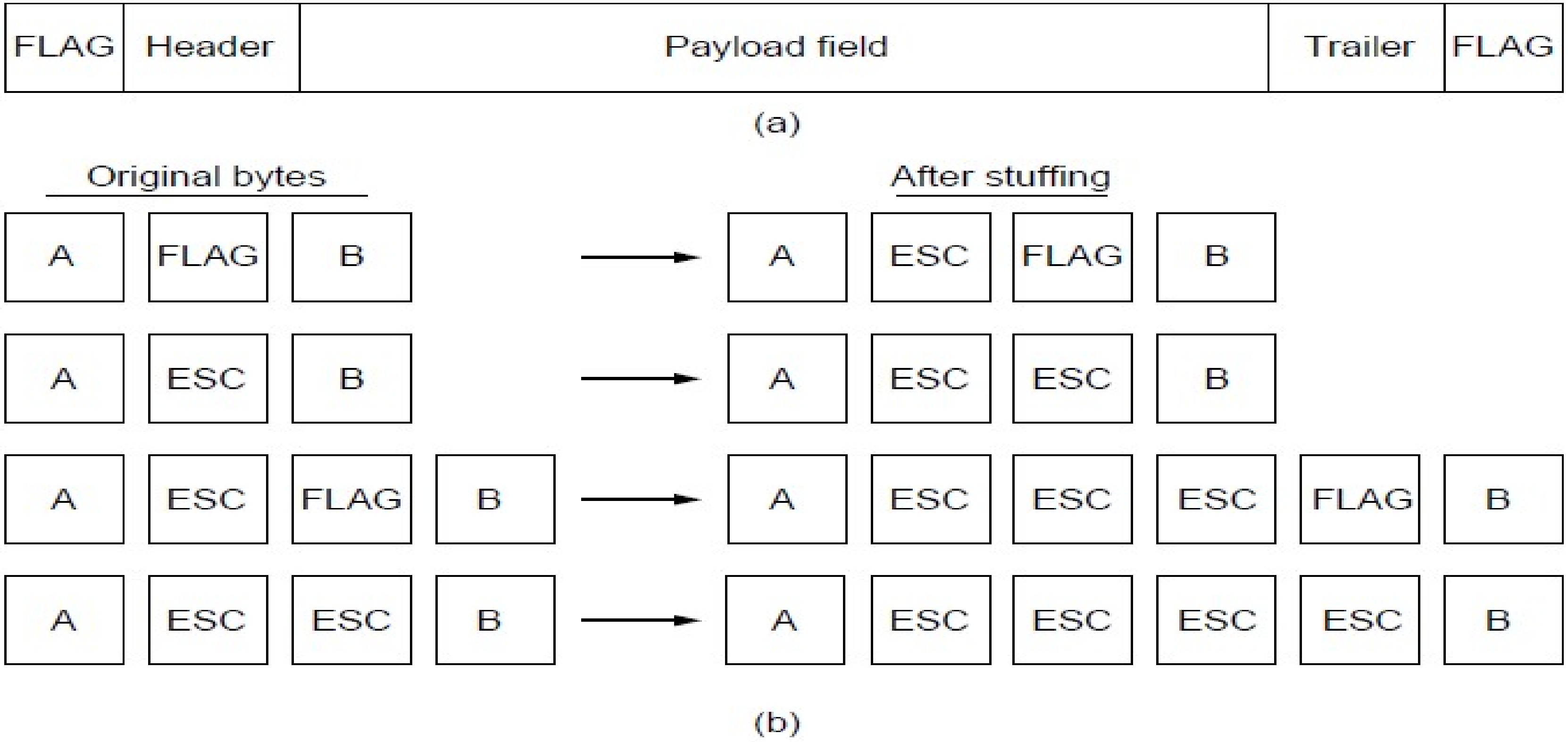
1. Byte count.
2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.
4. Physical layer coding violations.

Byte count Framing



A byte stream. (a) Without errors. (b) With one error.

Flag bytes with byte stuffing



FLAG | Header | Payload field | Trailer | FLAG

(a)

Original bytes → After stuffing

A FLAG B → A ESC FLAG B

A ESC B → A ESC ESC B

A ESC FLAG B → A ESC ESC ESC FLAG B

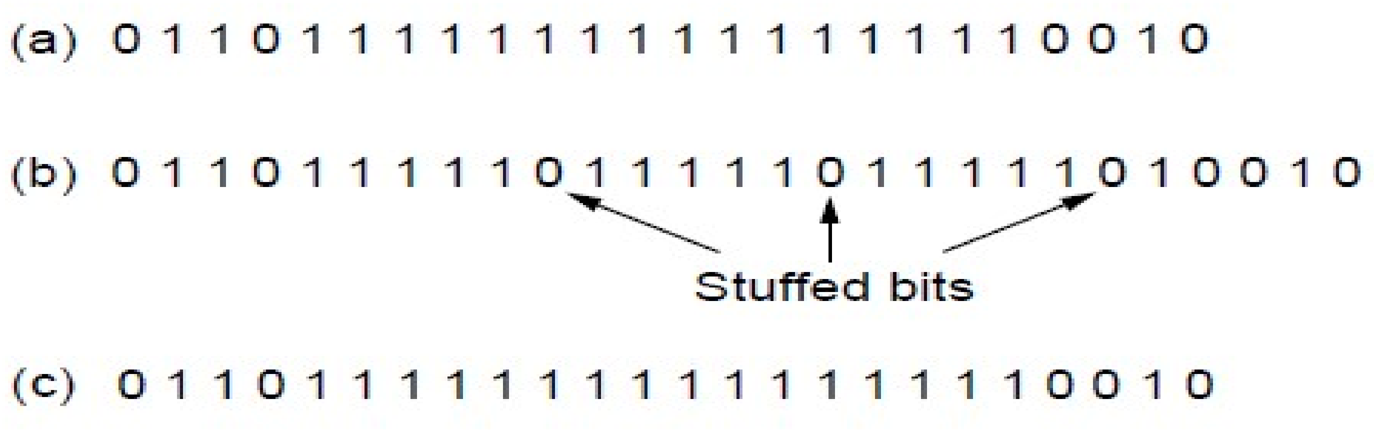
A ESC ESC B → A ESC ESC ESC ESC B

(b)

a) A frame delimited by flag bytes.

b) Four examples of byte sequences before and after byte stuffing.

Flag Bits with Bit Stuffing Framing Method


(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

Stuffed bits

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver’s memory after destuffing.

Error & Flow Control

- Error Control
  - Positive or Negative Acknowledgements

- Flow Control
  - Synchronization between Sender & Receiver

Error Detection and Correction

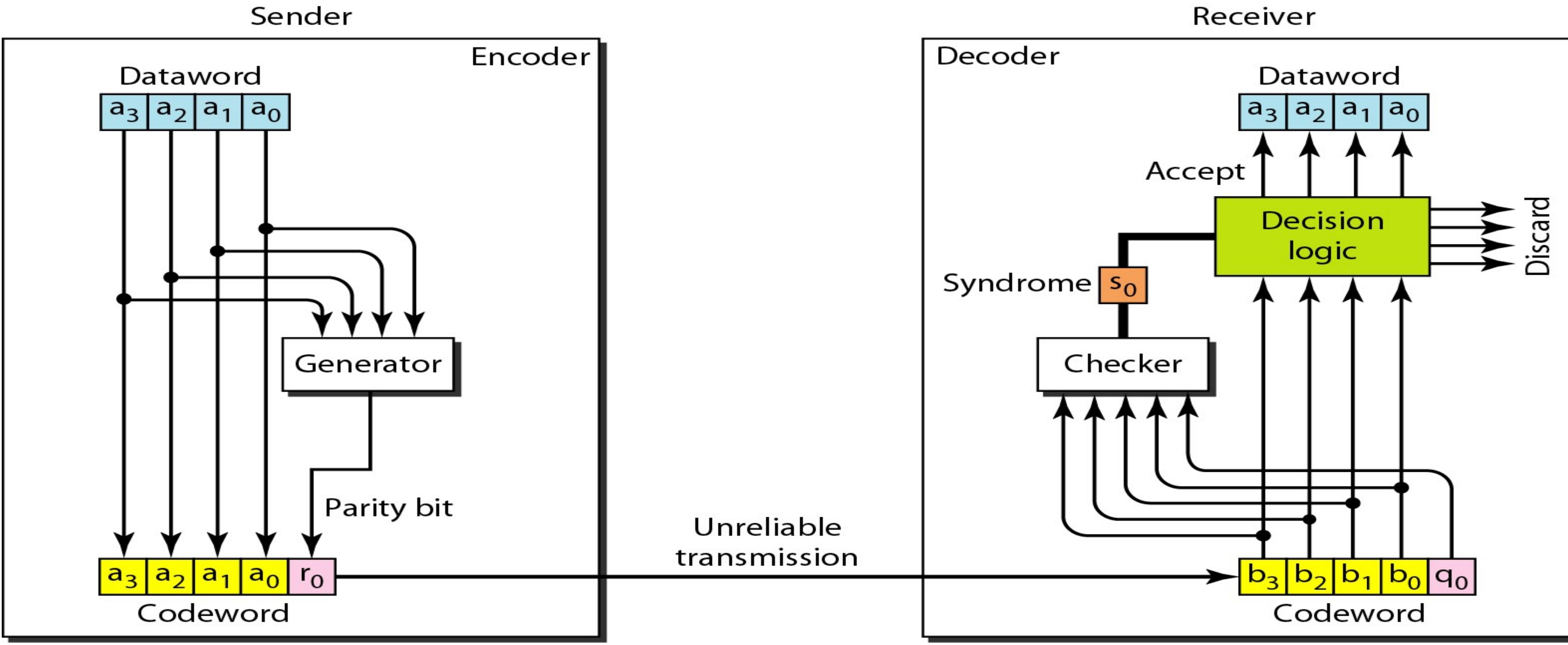
- During transmission, many factors like noise electromagnetic interference can change some part of data causing error in the data.
- A reliable systems must have a mechanism for detecting and correcting such errors.
- Data link layer or transport layer of the OSI model, supports the error detection and error correction mechanism.

- **Redundancy:** Error detection uses the concepts of redundancy. Redundancy means adding extra bits for detecting errors at destination.
- Parity: the simplest form of error detection is to append a single bit called a **parity bit** to a string of data.
- Two parity check methods
- **1. simple parity check**
- **2. two dimensional parity check**

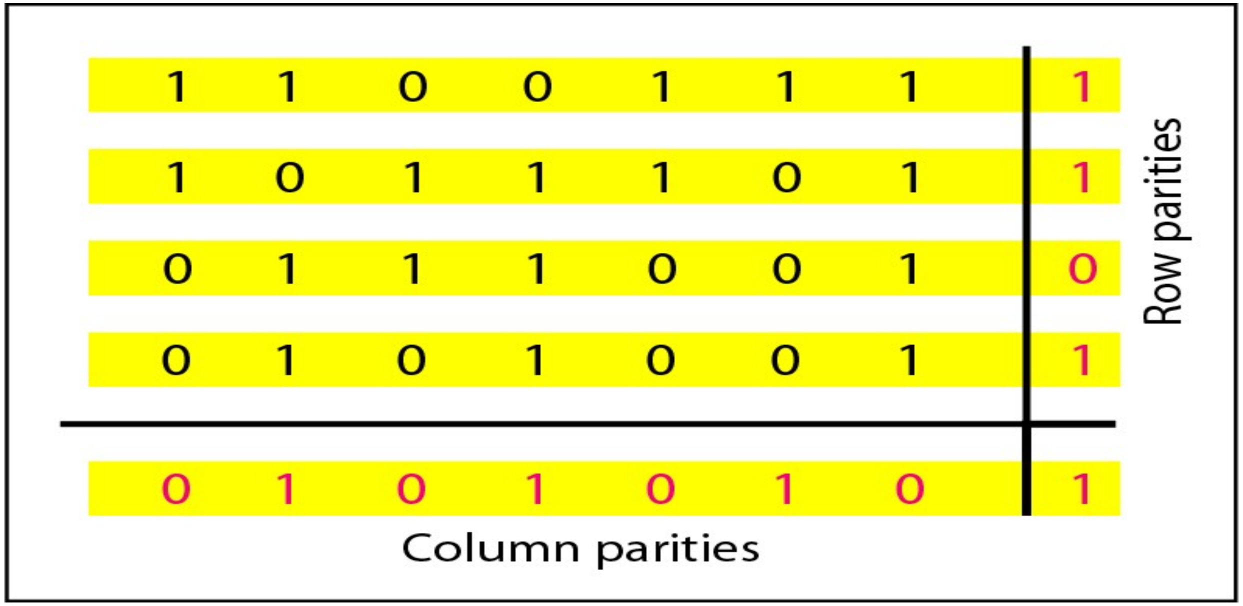
Simple parity-check code C(5, 4)

Datawords	Codewords	Datawords	Codewords
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

Figure 10.10 *Encoder and decoder for simple parity-check code*



Two-dimensional parity-check code



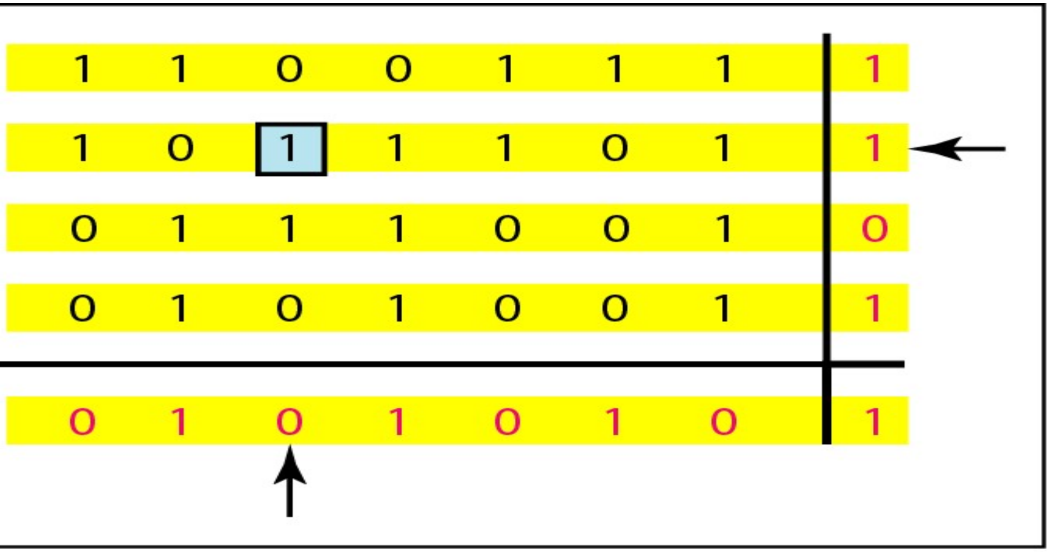
1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	1

Row parities

Column parities

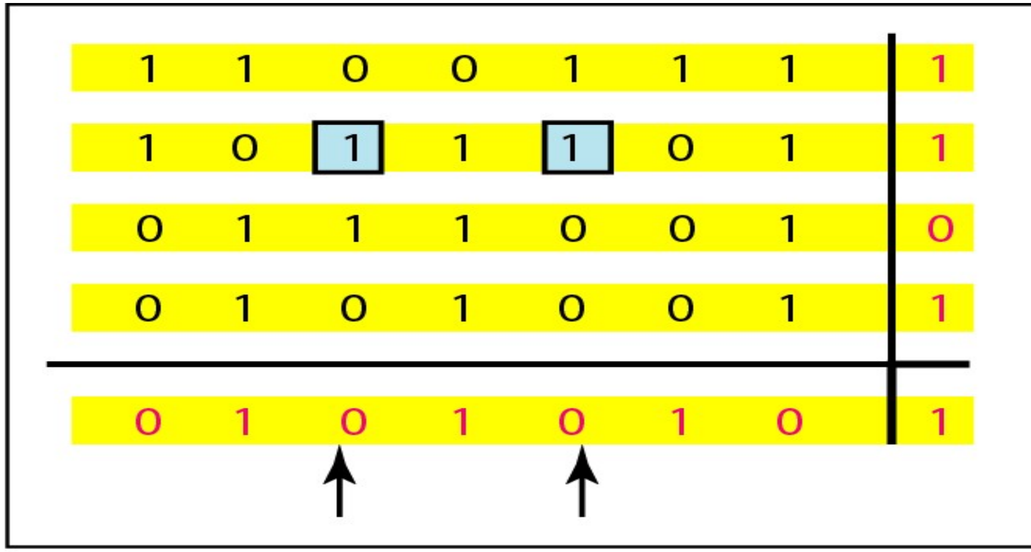
a. Design of row and column parities

Two-dimensional parity-check code



1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	1

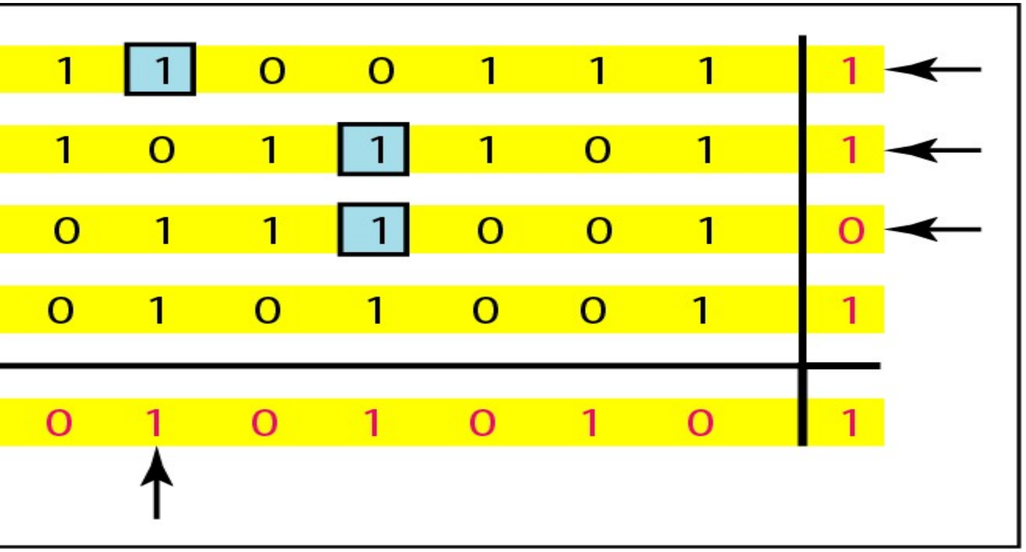
One error affects two parities



1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	1

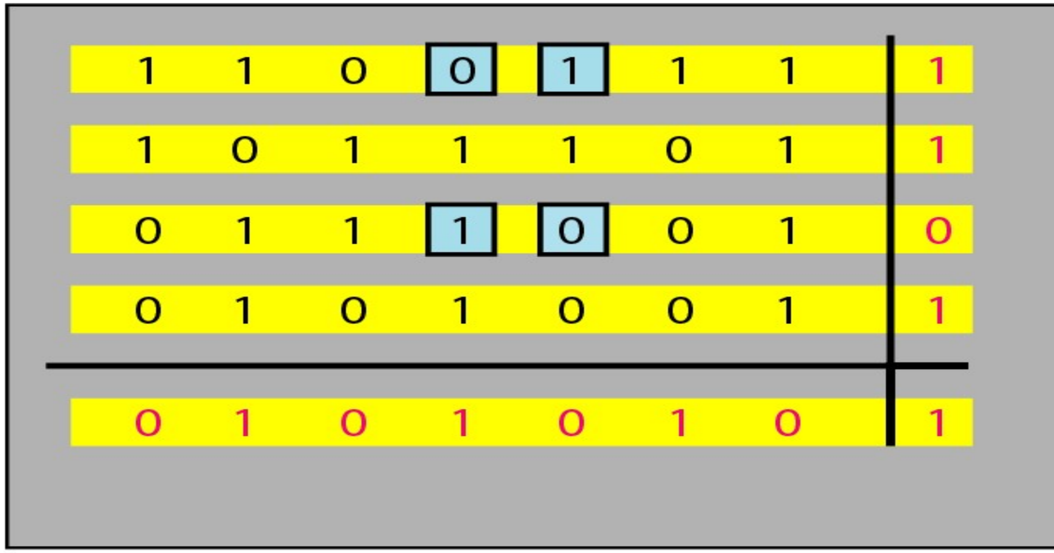
c. Two errors affect two parities

Two-dimensional parity-check code



1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	1

ree errors affect four parities



1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	1

e. Four errors cannot be detected

Hamming codes

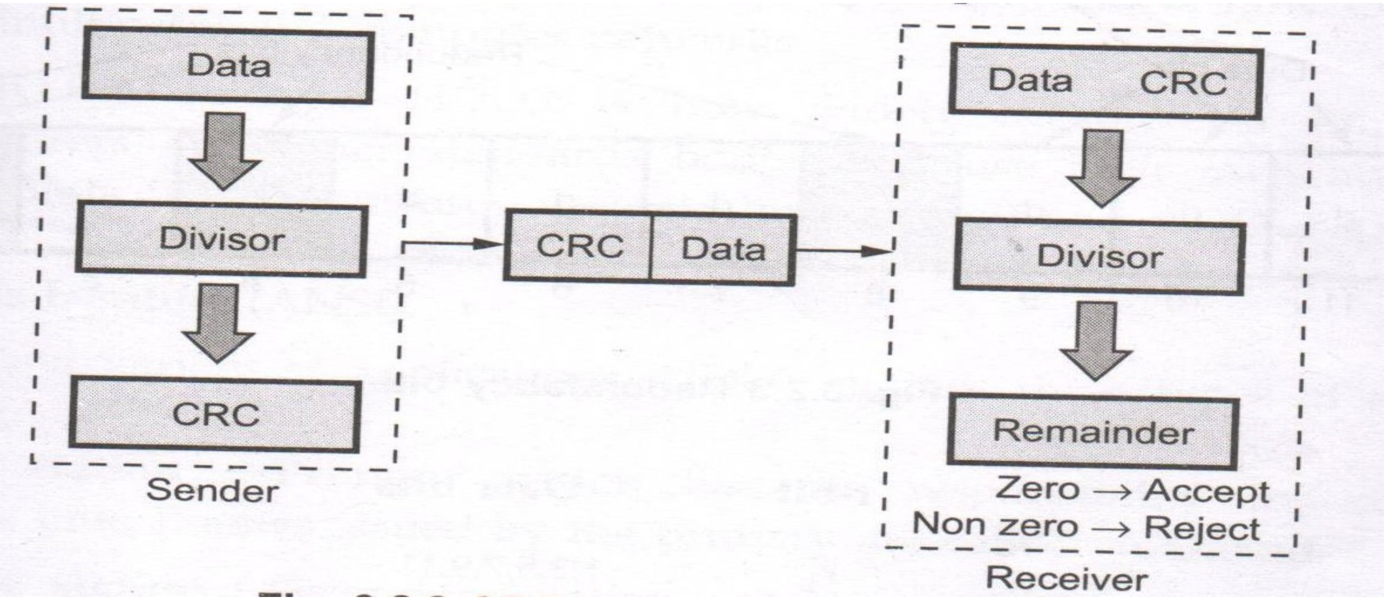
- Hamming code can perform error correction also along with detecting an error. Hamming code uses definite relationship between number of data bits and number of redundancy bits.

No of Data Bits m	No. of Redundancy Bits r	Total Bits n=m+r
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

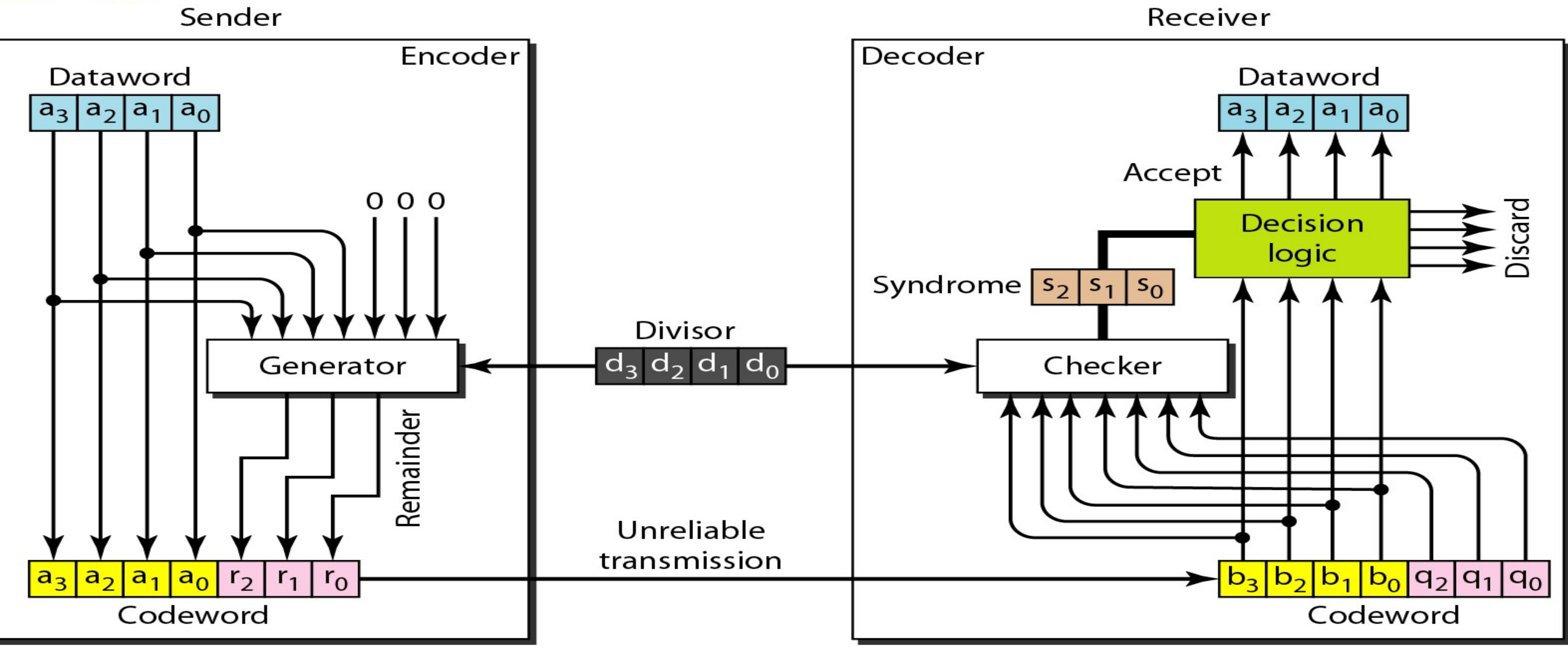
For m-data bits, parity bits are ‘r’ and total bits are m+r;
Parity can be placed in 2^n places
Parity can be calculated as $(m+r+1)\leq 2^r$

Cyclic Redundancy Check (CRC)

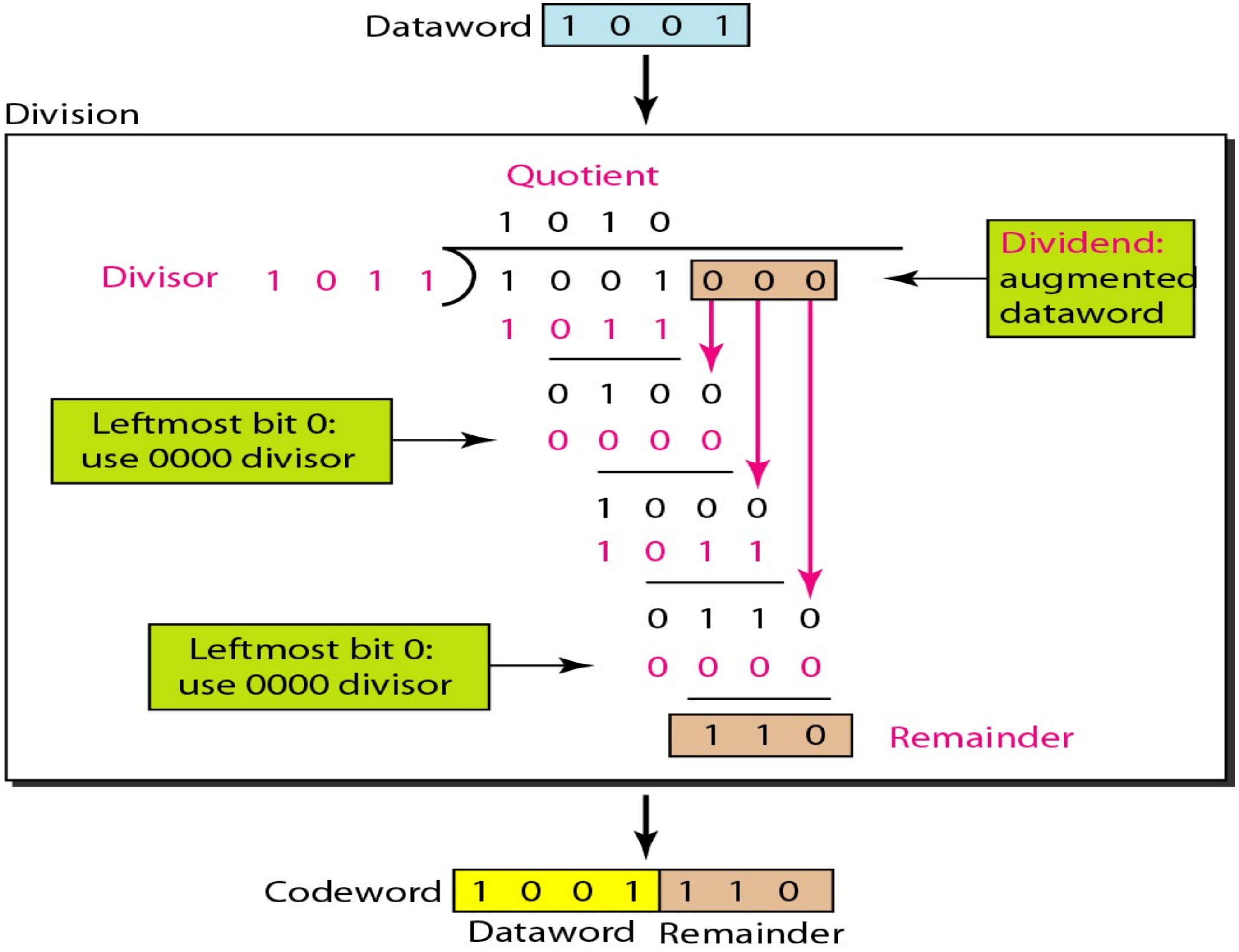
RC is based on binary division instead of addition bits as in parity check. In CR sequence of redundant bits (CRC remainder) is appended to the data unit, so th is exactly divisible by a second number. At the destination the received data ivided by same number. If any remainder is generated it indicates error in t ata and is rejected.



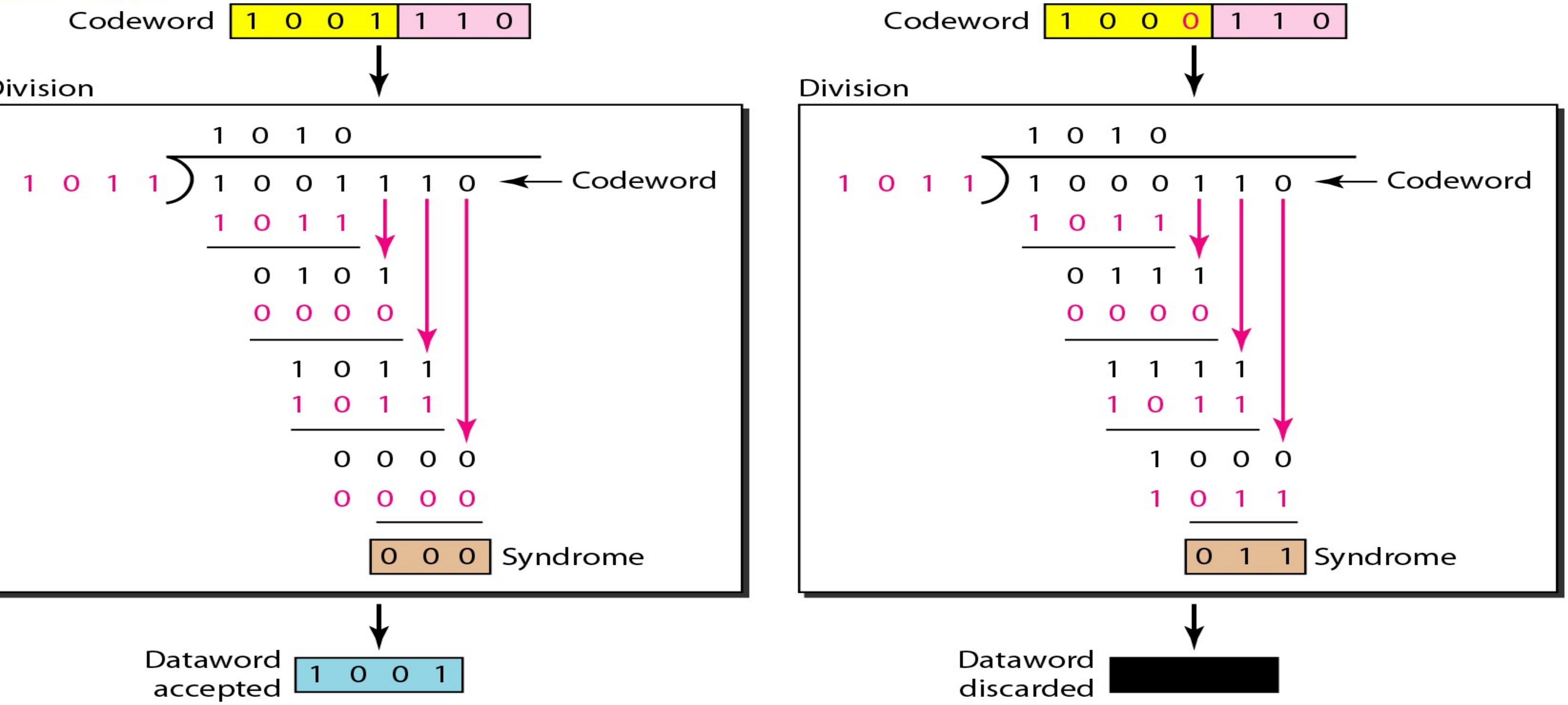
CRC encoder and decoder



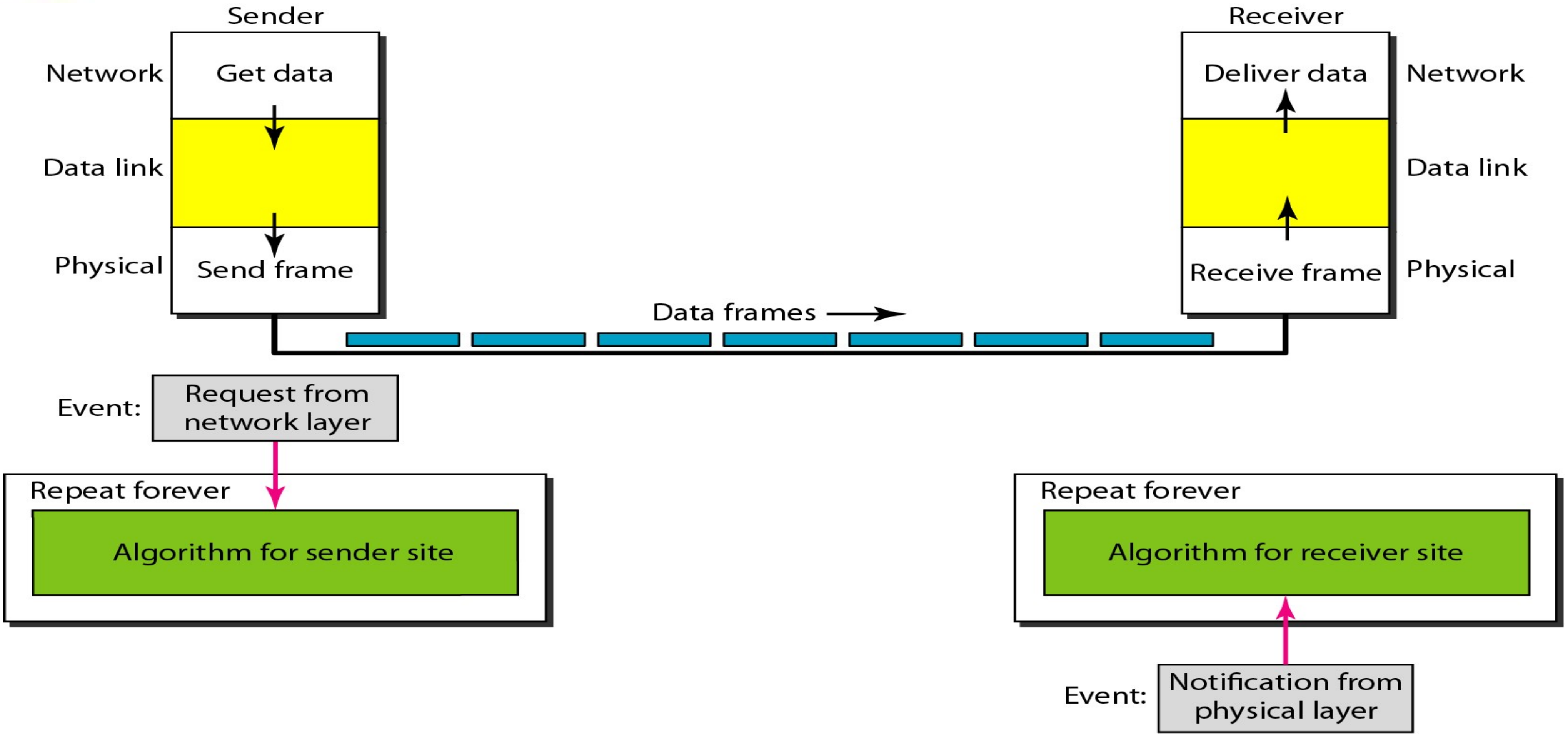
vision in CRC encoder



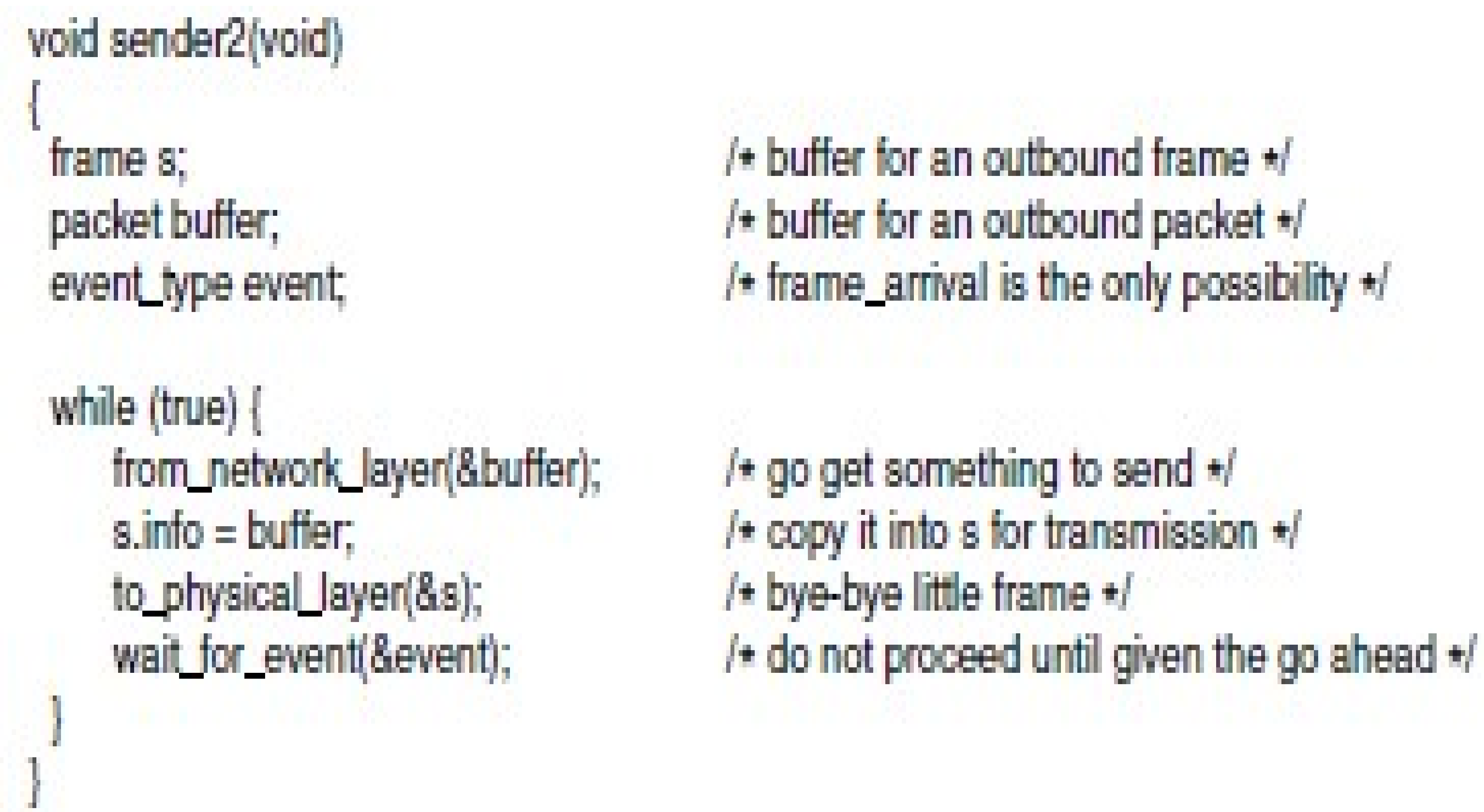
vision in the CRC decoder for two cases



e design of the simplest protocol with no flow or error cont



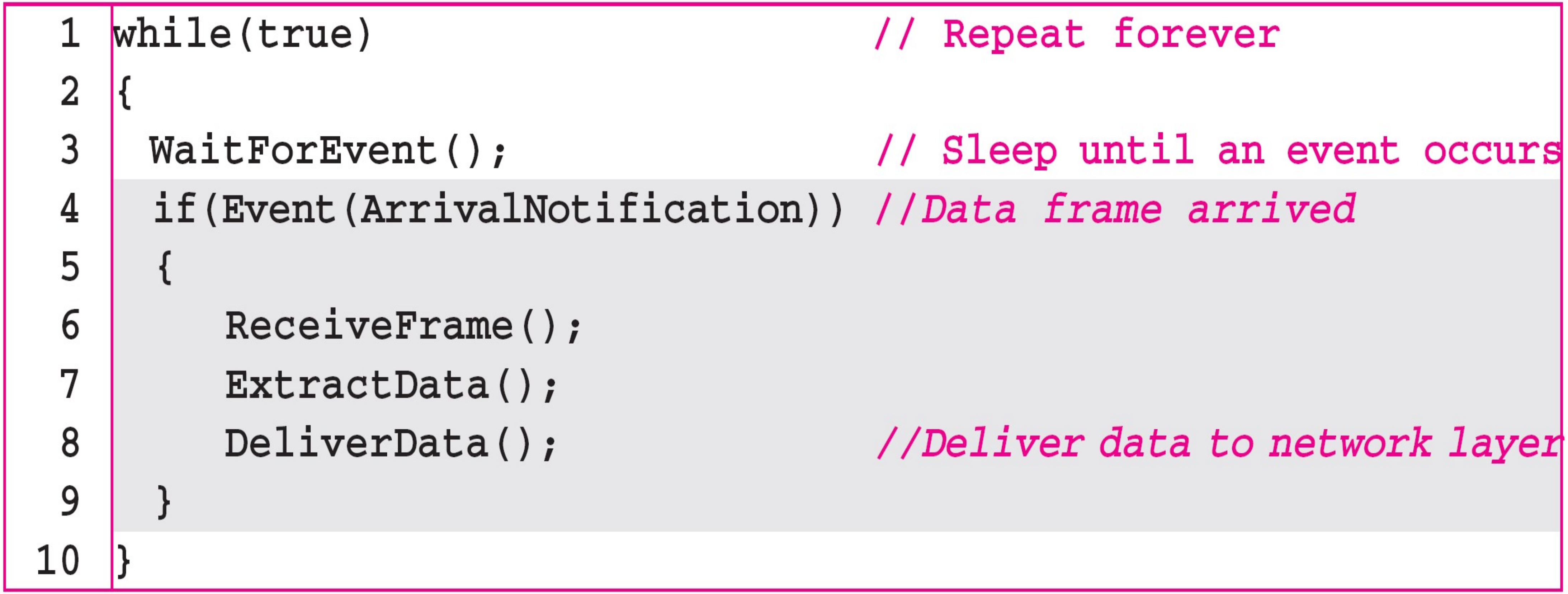
Sender-site algorithm for the simplest protocol



```
void sender2(void)
{
  frame s;                                    /* buffer for an outbound frame */
  packet buffer;                              /* buffer for an outbound packet */
  event_type event;                           /* frame_arrival is the only possibility */

  while (true) {
        from_network_layer(&buffer);          /* go get something to send */
        s.info = buffer;                      /* copy it into s for transmission */
        to_physical_layer(&s);                /* bye-bye little frame */
        wait_for_event(&event);               /* do not proceed until given the go ahead */
  }
}
```

Receiver-site algorithm for the simplest protocol



```
while(true)                      // Repeat forever
{
  WaitForEvent();                // Sleep until an event occurs
  if(Event(ArrivalNotification)) //Data frame arrived
  {
     ReceiveFrame();
     ExtractData();
     DeliverData();              //Deliver data to network layer
  }
}
```

eps in ARQ

RQ protocol is characterized by four functional steps.

ransmission of frames

rror checking at the receiver end.

cknowledgement

a) Negative if error is detected (NAK)

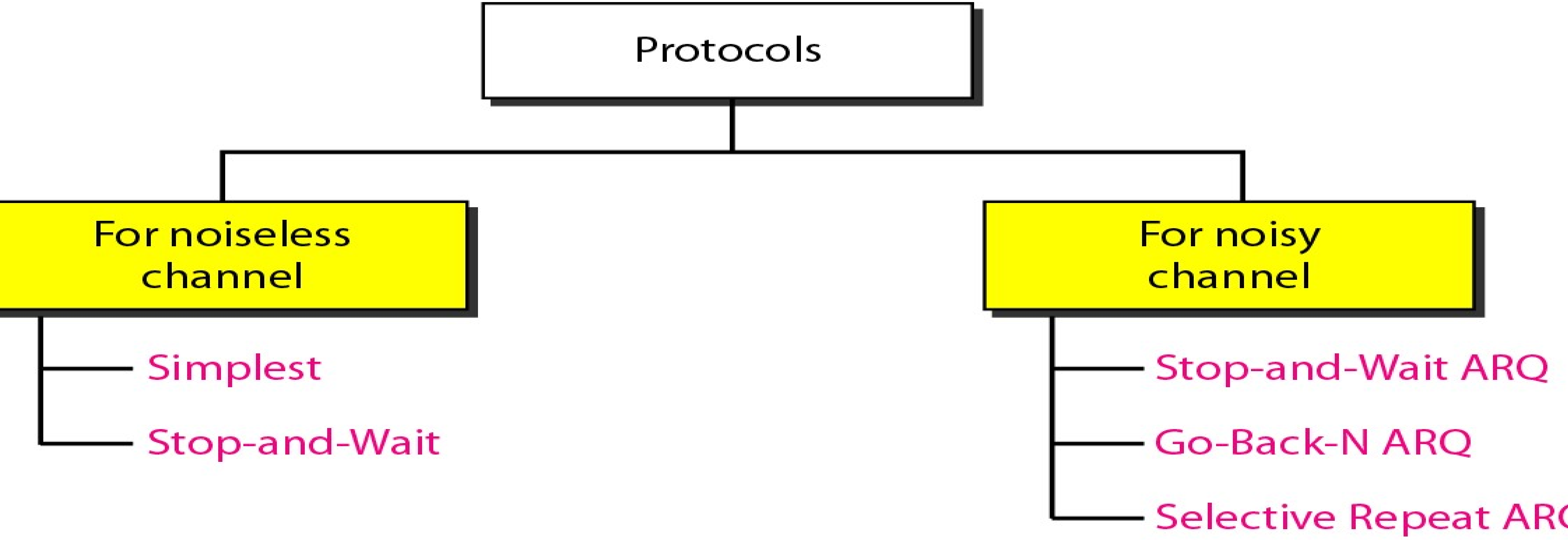
b) Positive if no error is detected (ACK)

etransmission if acknowledgement is negative (NAK) or if no acknowledgeme eceived within a stipulated time.

ay be noted that ARQ protocol require two way communication even if the informa ransfer is simplex i.e. one way only.

ormation is exchanged in the form of frames, the beginning and the end of w re identified by means of flags or special characters.

PROTOCOLS

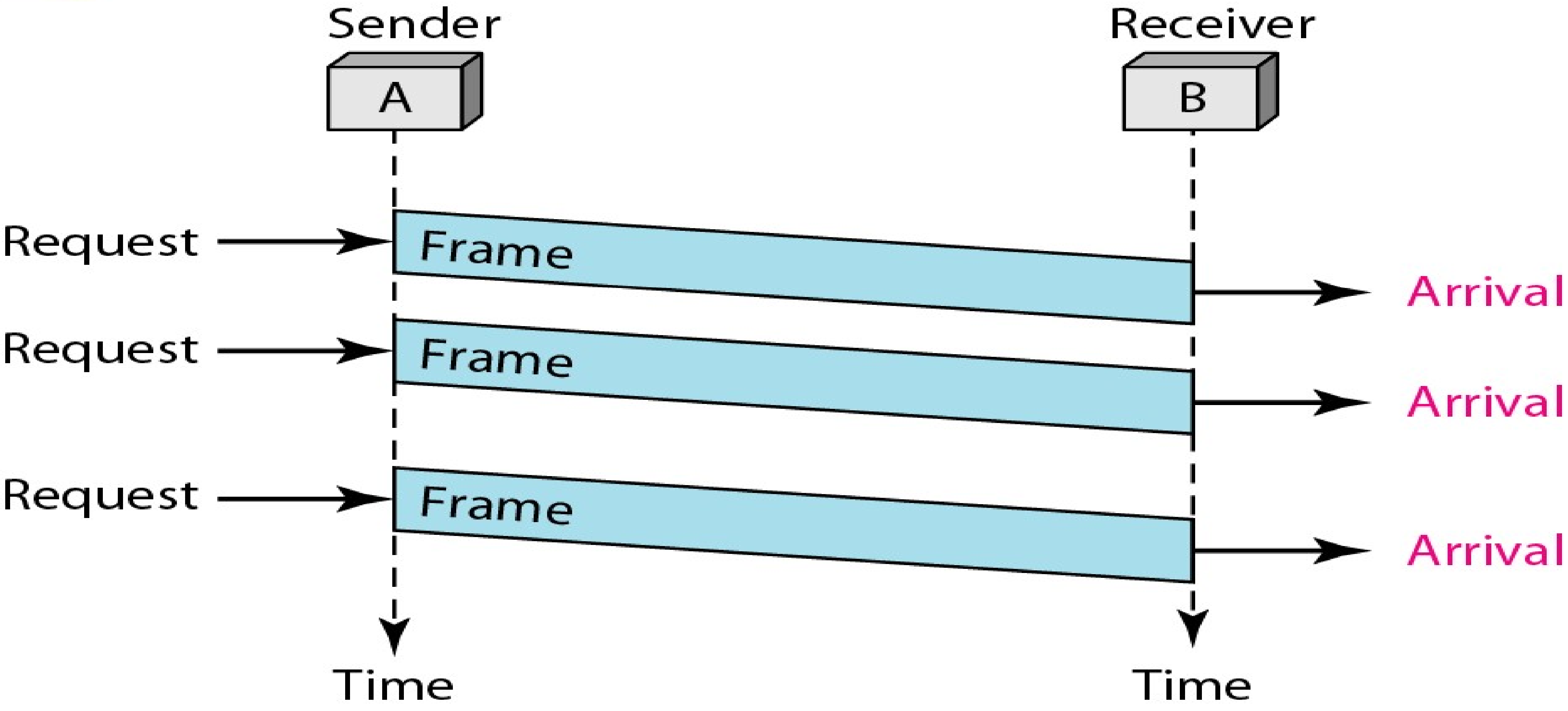

Protocols
For noiseless channel
Simplest
Stop-and-Wait
For noisy channel
Stop-and-Wait ARQ
Go-Back-N ARQ
Selective Repeat ARQ

NOISELESS CHANNELS

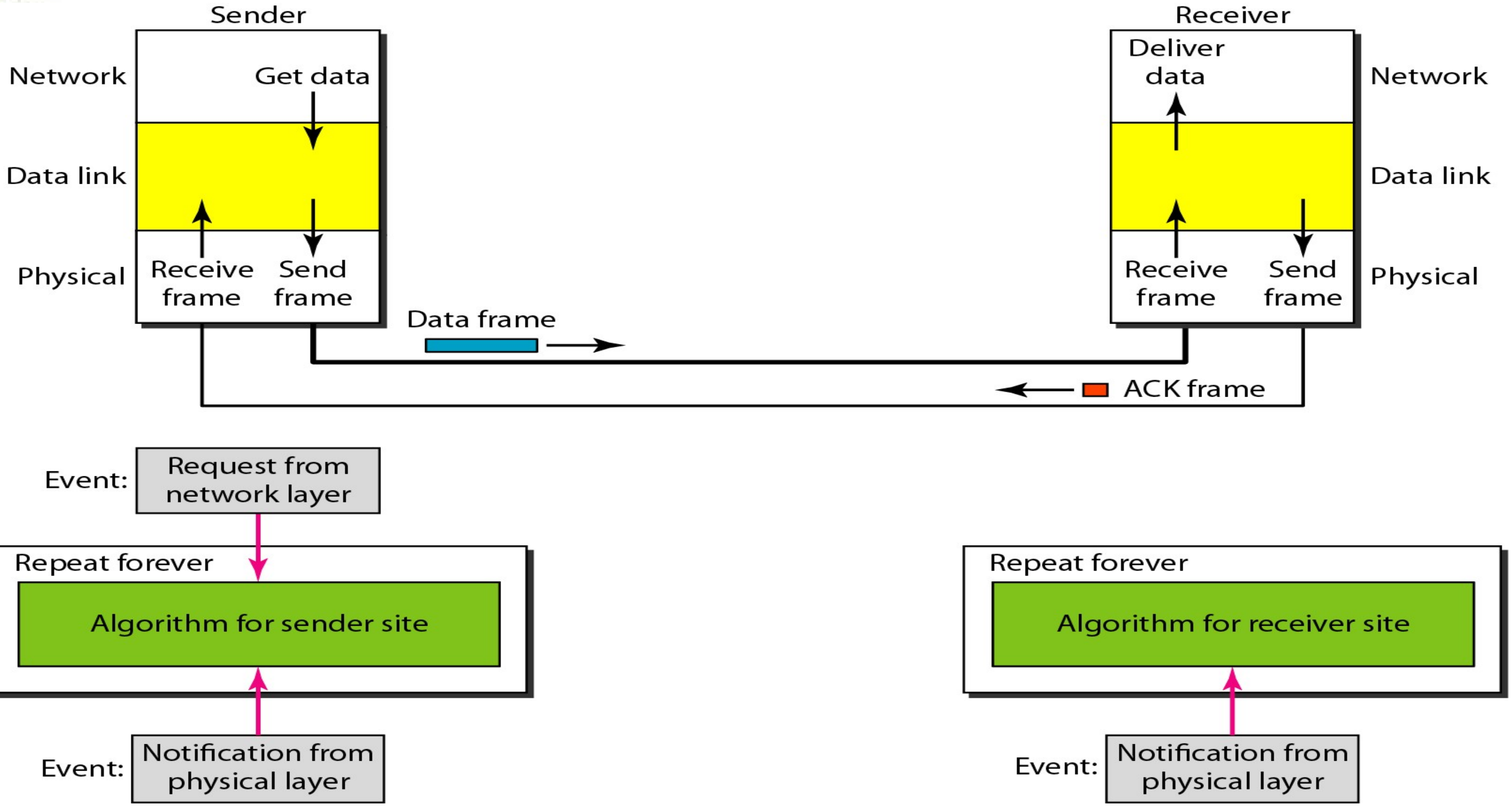
a) *Let us first assume we have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel.*

b) Simplex Protocol
Stop-and-Wait Protocol

Flow diagram for simplest protocol



Stop-and-Wait Protocol



Stop-and-wait protocol

Stop and wait ARQ is the simplest mechanism for error control and flow control.

ation

The sender transmits the frame, when frame arrives at receiver it checks for damage acknowledges to the sender accordingly. While transmitting a frame there can be situations.

rmal operation

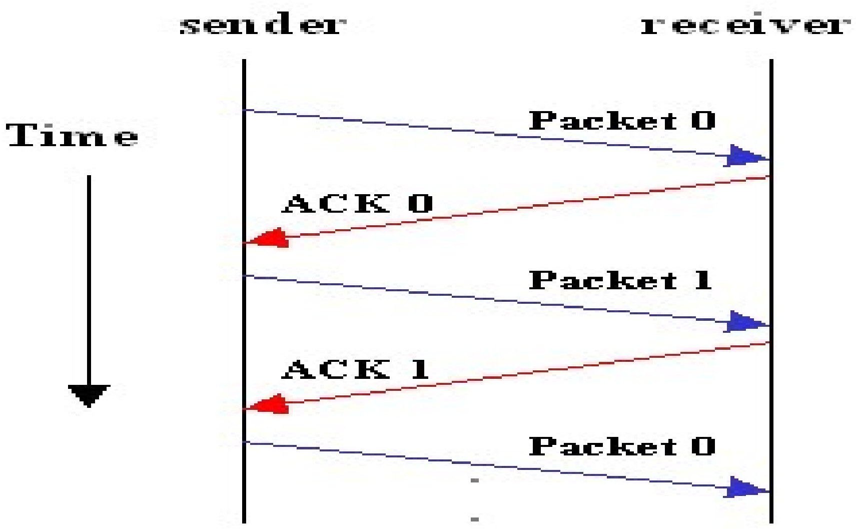
e frame is lost

e acknowledgement is lost

e acknowledgement is delayed

Normal Operation

After transmitting one packet, the sender waits for an ***acknowledgment (ACK)*** in normal operation

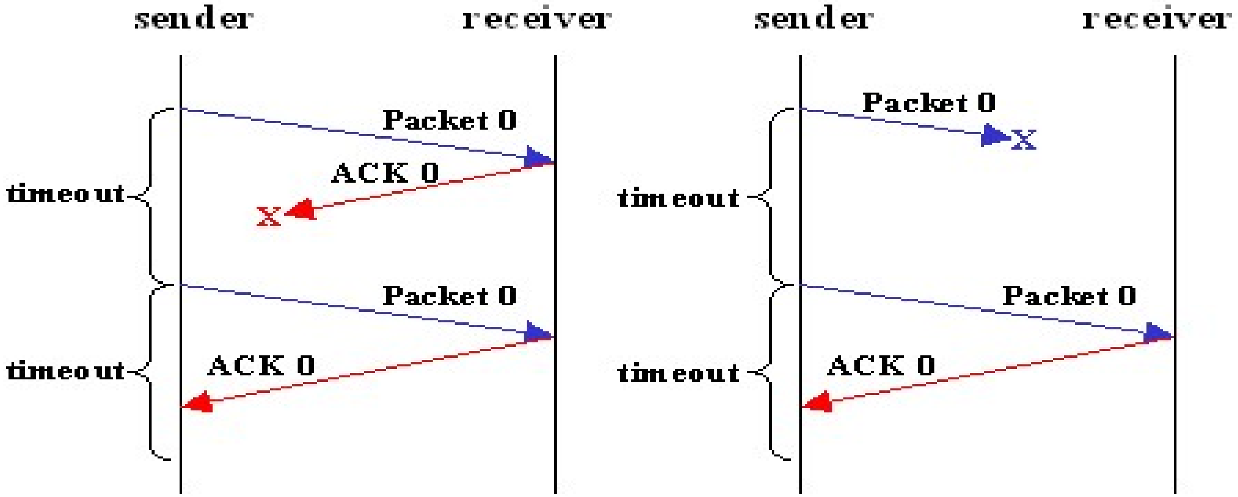


n this operation the sender sends frame 0 and waits for acknowledgement ACK0. after eceiving ACK0, sender sends next frame 1 and waits for its acknowledgement ACK1. this operation is repeated

Usually a timer is set by sender after each frame is transmitted, its acknowledgement must be received before timer expires

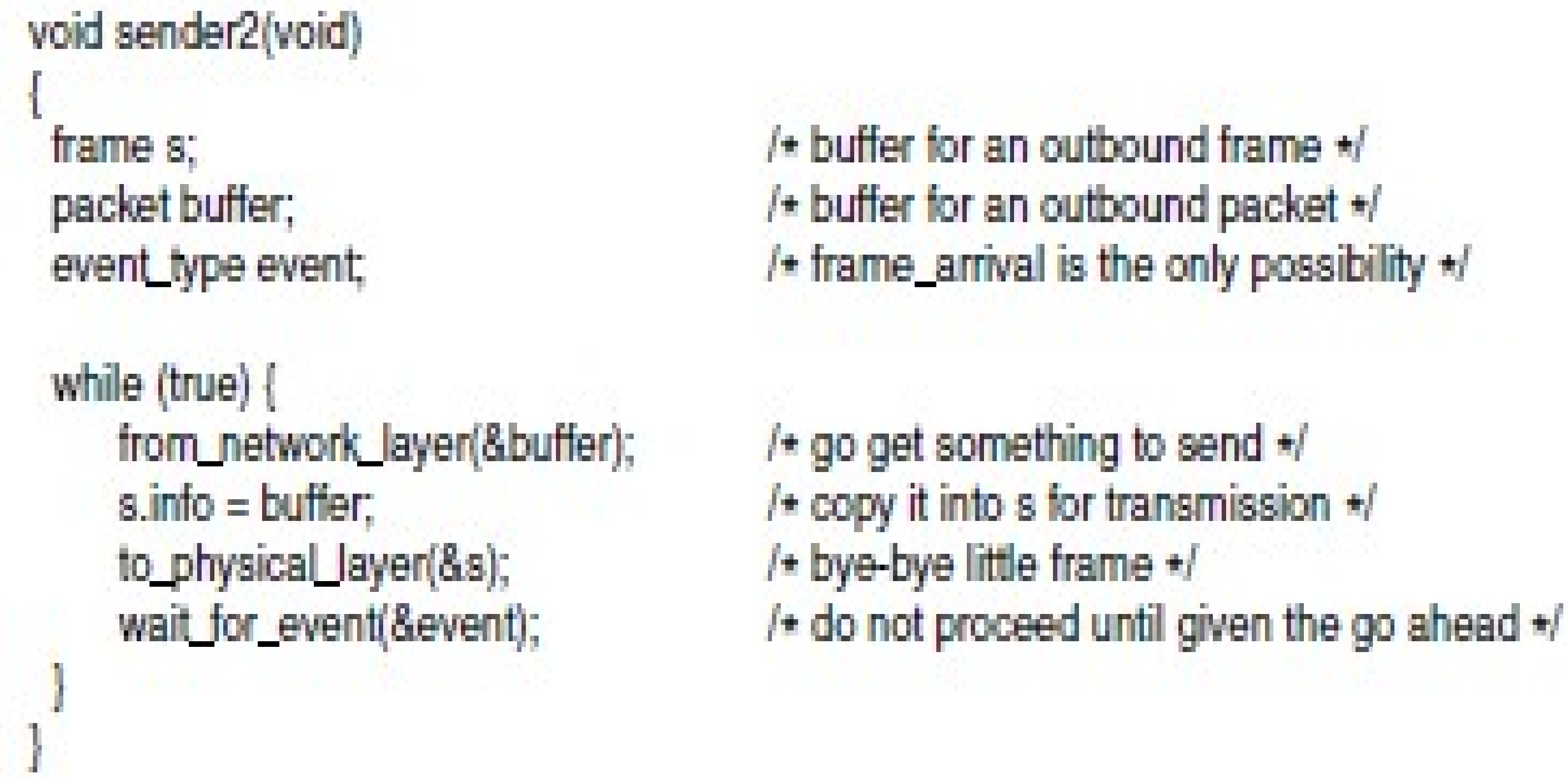
ost or Damaged Frame

If the sender doesn't receive ACK for previous sent packet after a certain period of time, t nder times out and retransmits



Vhen a receiver receives the frame and found it damaged or lost, it is discarded b etains its number. When sender does not receive its acknowledgement it retransmits tl ame frame.

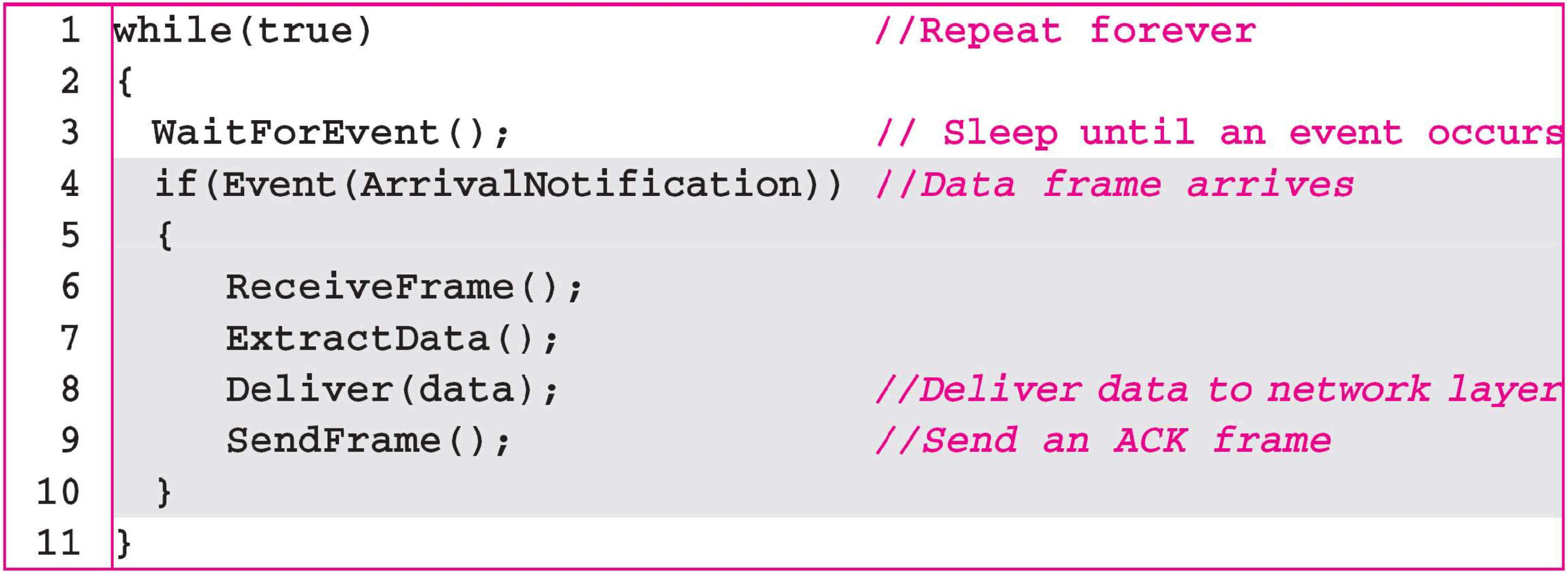
Sender-site algorithm for Stop-and-Wait Protocol



```
void sender2(void)
{
  frame s;                              /* buffer for an outbound frame */
  packet buffer;                        /* buffer for an outbound packet */
  event_type event;                     /* frame_arrival is the only possibility */

  while (true) {
        from_network_layer(&buffer);    /* go get something to send */
        s.info = buffer;                /* copy it into s for transmission */
        to_physical_layer(&s);          /* bye-bye little frame */
        wait_for_event(&event);         /* do not proceed until given the go ahead */
  }
}
```

Receiver-site algorithm for Stop-and-Wait Protocol



```
while(true)                               //Repeat forever
{
  WaitForEvent();                         // Sleep until an event occurs
  if(Event(ArrivalNotification))          //Data frame arrives
  {
     ReceiveFrame();
     ExtractData();
     Deliver(data);                       //Deliver data to network layer
     SendFrame();                         //Send an ACK frame
  }
}
```

NOISY CHANNELS

Although the Stop-and-Wait Protocol gives us an idea of how to add flow control predecessor, noiseless channels are nonexistent.

p-and-Wait Automatic Repeat Request
Go-Back-N Automatic Repeat Request
Selective Repeat Automatic Repeat Request

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sen frame and retransmitting of the frame when the timer expires.

In Stop-and-Wait ARQ, we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic.

In Stop-and-Wait ARQ, the acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.

top and Wait

Source transmits single frame

Wait for ACK

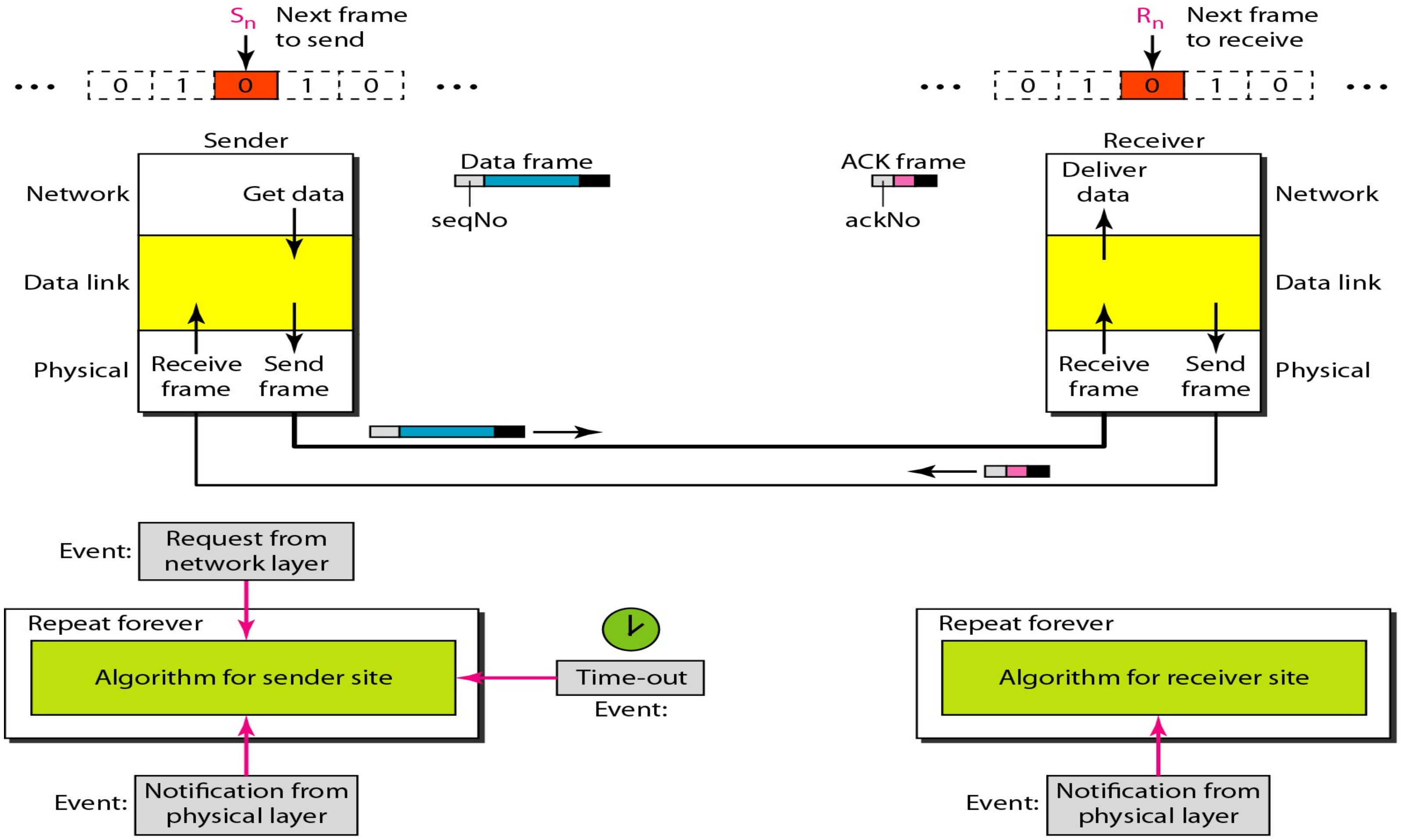
f received frame damaged, discard it

- Transmitter has timeout
- If no ACK within timeout, retransmit

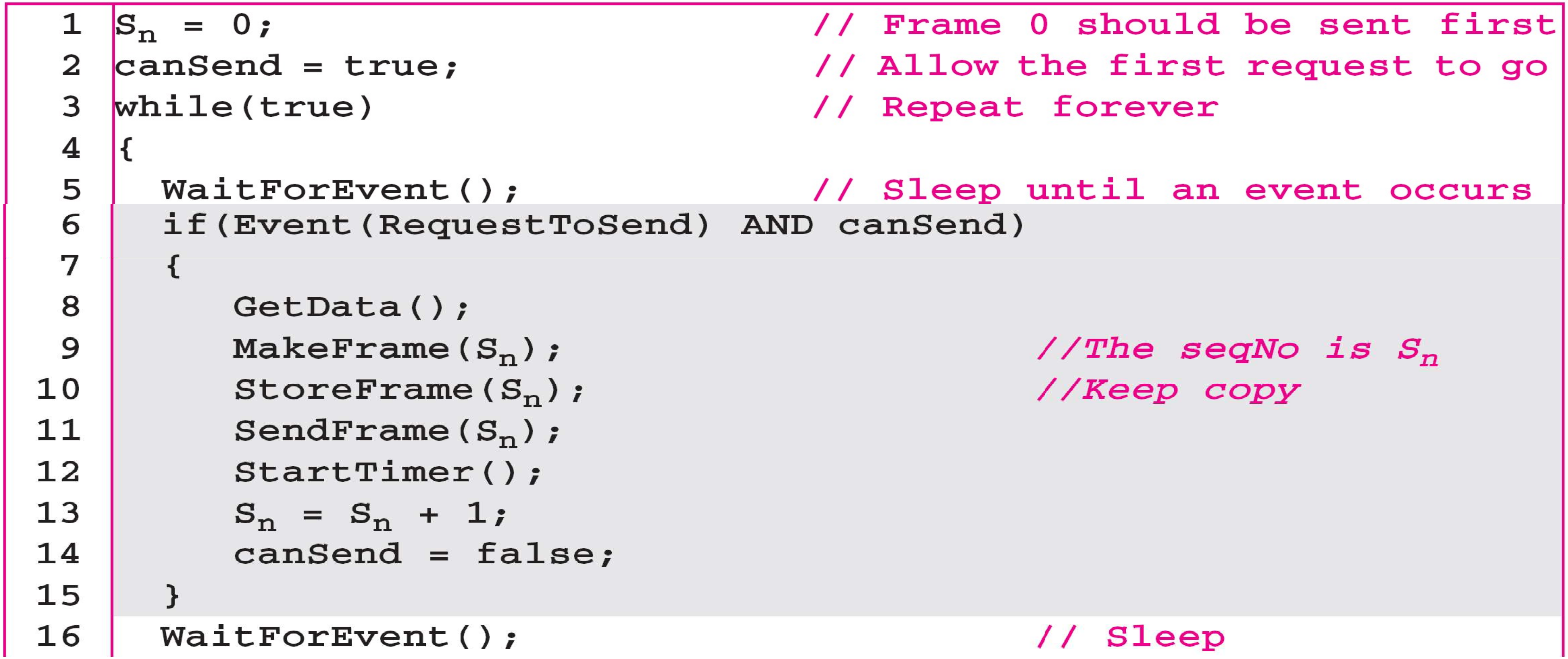
f ACK damaged, transmitter will not recognize it

- Transmitter will retransmit
- Receive gets two copies of frame
- Use ACK0 and ACK1

Design of the Stop-and-Wait ARQ Protocol

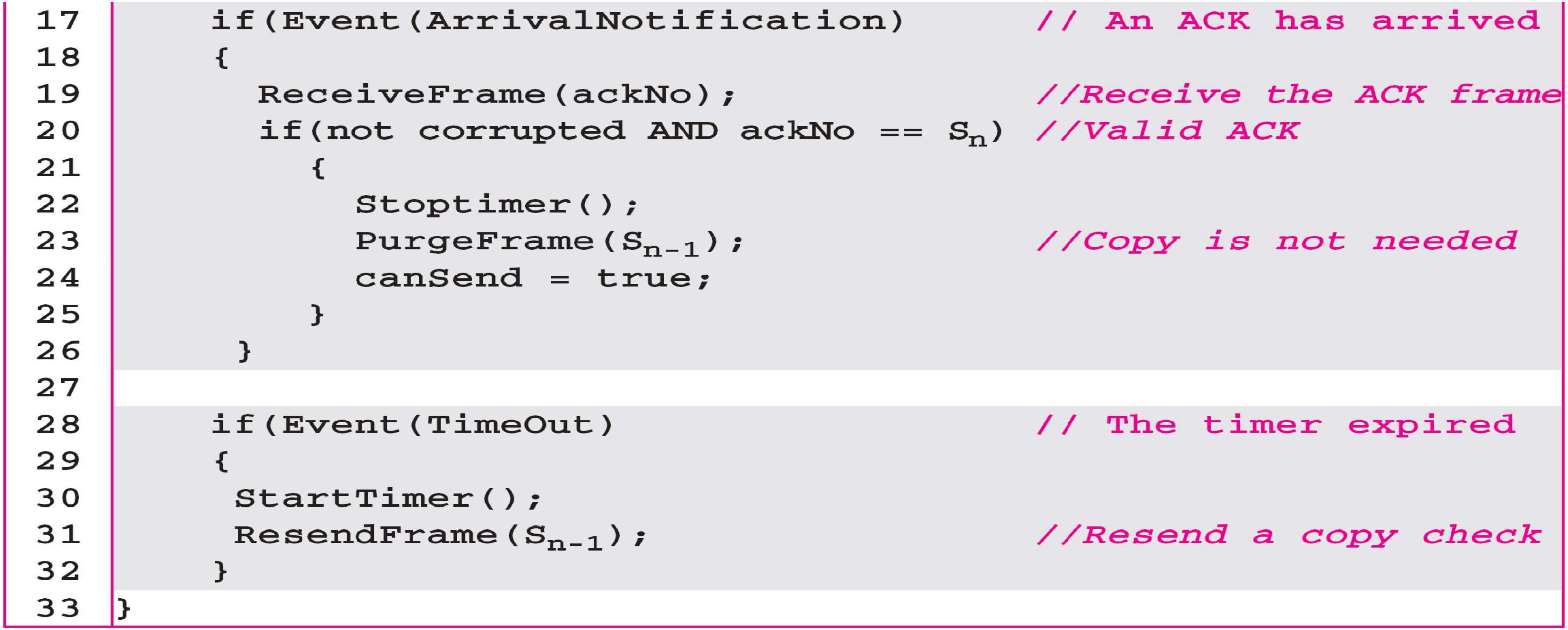


Sender-site algorithm for Stop-and-Wait ARQ



```
$S_n$ = 0;                            // Frame 0 should be sent first
canSend = true;                       // Allow the first request to go
while(true)                           // Repeat forever
{
  WaitForEvent();                     // Sleep until an event occurs
  if(Event(RequestToSend) AND canSend)
  {
     GetData();
     MakeFrame($S_n$);                          //The seqNo is $S_n$
     StoreFrame($S_n$);                         //Keep copy
     SendFrame($S_n$);
     StartTimer();
     $S_n$ = $S_n$ + 1;
     canSend = false;
  }
  WaitForEvent();                               // Sleep
```

Sender-site algorithm for Stop-and-Wait ARQ(continued)



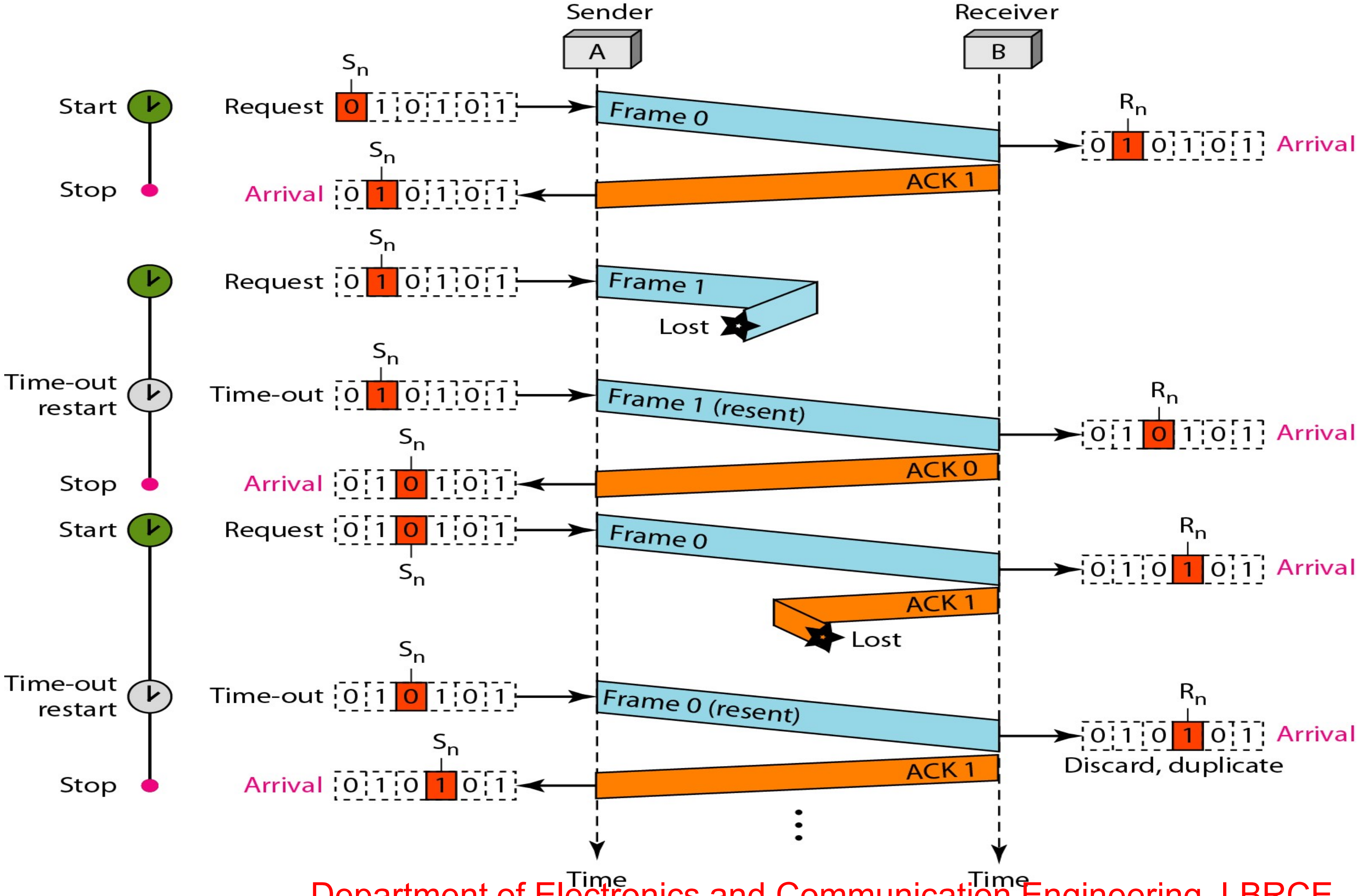
```
    if(Event(ArrivalNotification)       // An ACK has arrived
    {
      ReceiveFrame(ackNo);              //Receive the ACK frame
      if(not corrupted AND ackNo == $S_n$) //Valid ACK
        {
          Stoptimer();
          PurgeFrame($S_{n-1}$);        //Copy is not needed
          canSend = true;
        }
     }

    if(Event(TimeOut)                   // The timer expired
    {
     StartTimer();
     ResendFrame($S_{n-1}$);            //Resend a copy check
    }
}
```

Receiver-site algorithm for Stop-and-Wait ARQ Protocol

```
$R_n$ = 0;                          // Frame 0 expected to arrive first
while(true)
{
  WaitForEvent();                   // Sleep until an event occurs
  if(Event(ArrivalNotification))    //Data frame arrives
  {
     ReceiveFrame();
     if(corrupted(frame));
        sleep();
     if(seqNo == $R_n$)             //Valid data frame
     {
      ExtractData();
       DeliverData();               //Deliver data
       $R_n$ = $R_n$ + 1;
     }
      SendFrame($R_n$);             //Send an ACK
  }
}
```

Flow diagram for Stop-and-Wait ARQ Protocol



Sliding Window Protocols

a) Piggy Backing

b) Sending Window

c) Receiving Window

Sliding Window Protocols (2)

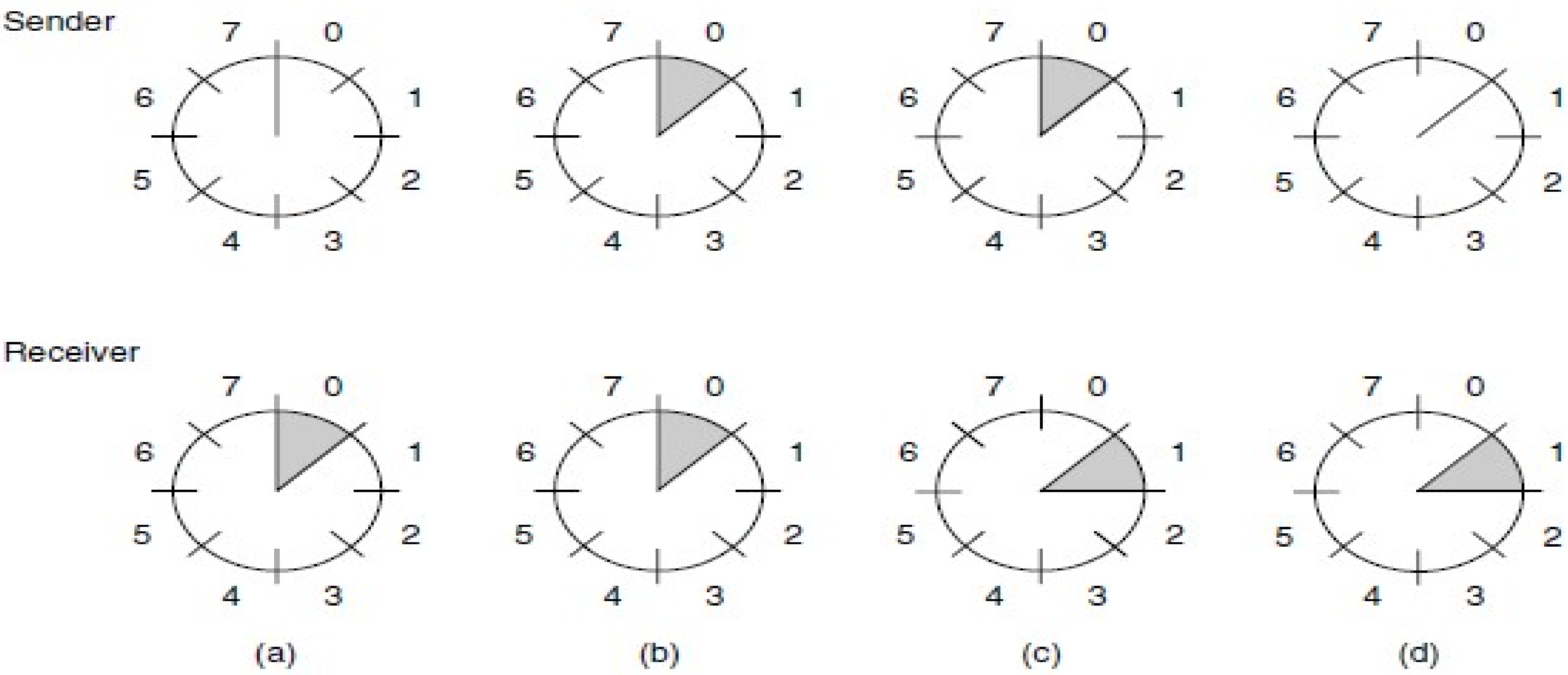
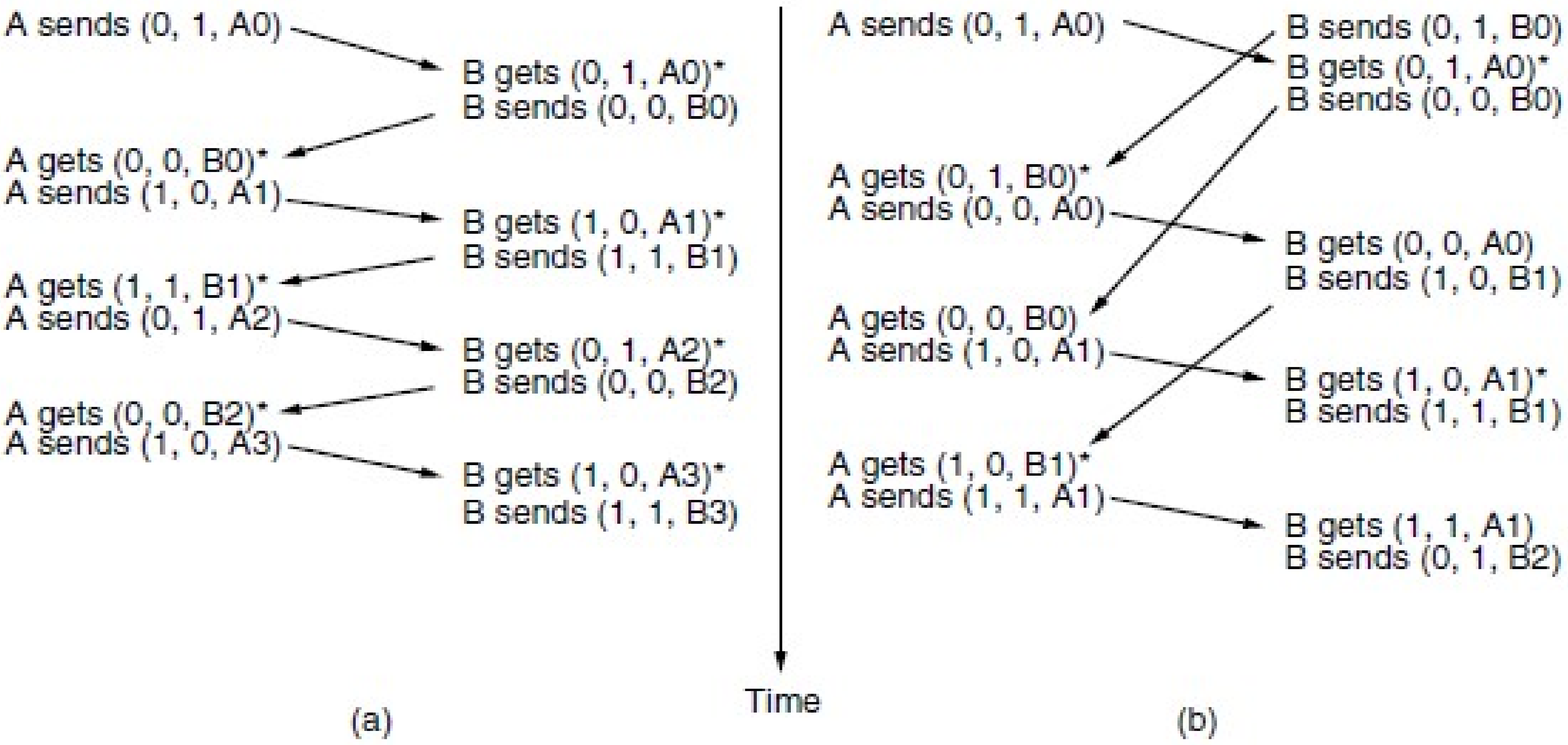
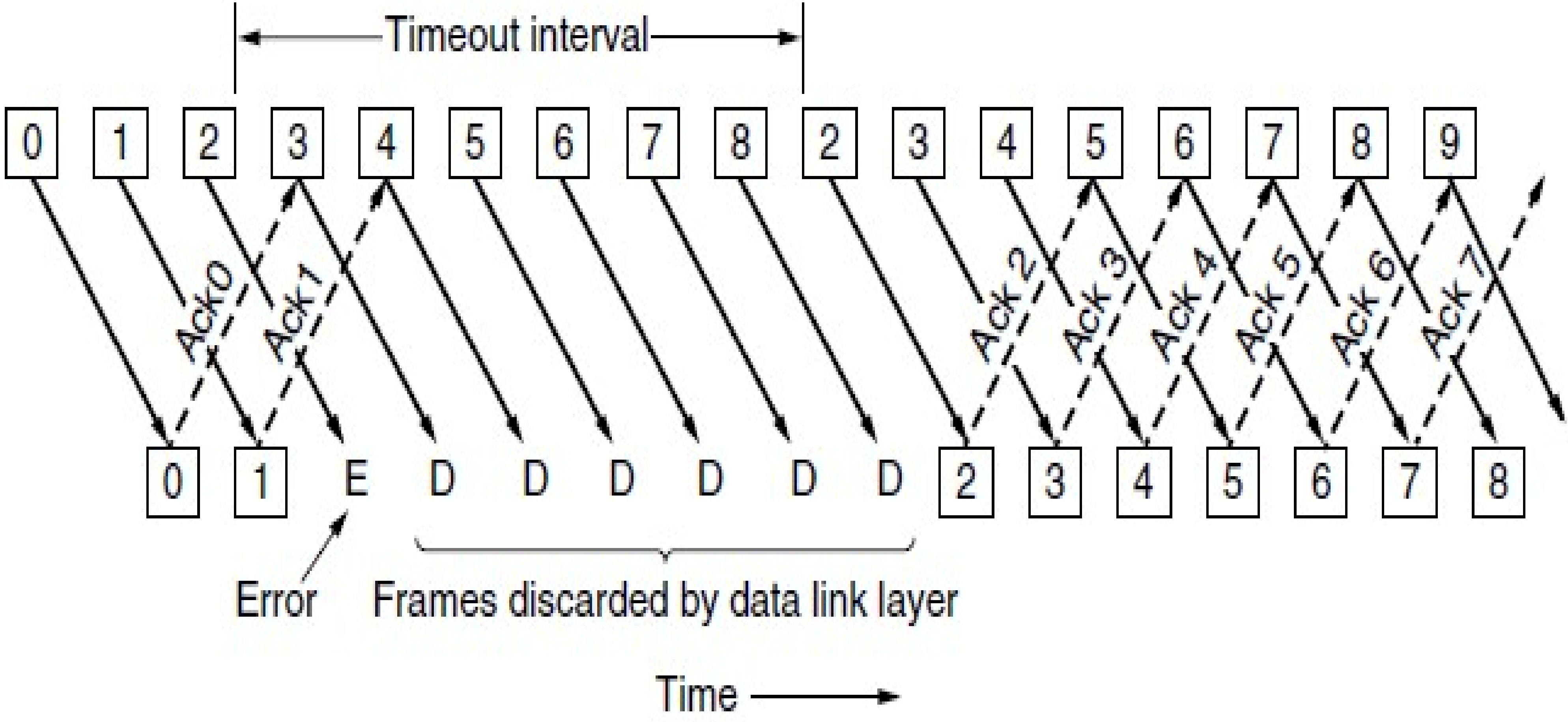


Figure 3-15. A sliding window of size 1, with a 3-bit sequence number. (a) Initially. (b) After the first frame has been sent. (c) After the first frame has been received. (d) After the first acknowledgement has been received.

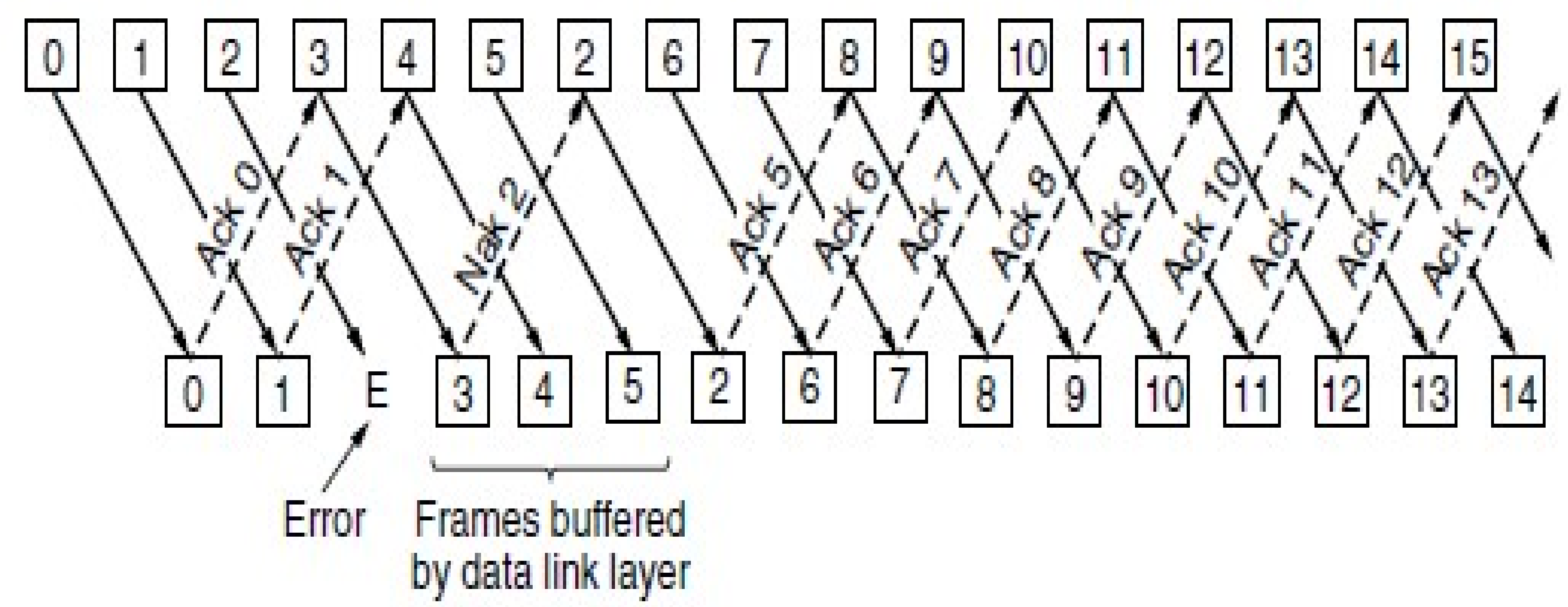
One-Bit Sliding Window Protocol



Go Back N Protocol



Selective Repeat



The Medium Access Control Sublayer

Chapter 4

The Medium Access Control Sublayer

a) The Channel Allocation Problem

b) Multiple Access Protocols

c) Ethernet

d) Data Link Layer Switching

Channel Allocation Problem

- Static channel allocation
- Assumptions for dynamic allocation.

Static Channel Allocation

a) Traditionally capacity of the channel is split among multiple competing use (e.g., TDM or FDM).

b) Example: FM radio stations.

c) However, when the number of senders is large and varying or the traffic is bursty FDM presents some problems.

Static Channel Allocation

a) If the spectrum is cut up into N regions and

- Fewer than N users are currently interested in communicating, a large piece o valuable spectrum will be wasted.
- More than N users want to communicate some of them will be denie permission for lack of bandwidth.

b) Dividing the channel into constant number of users of static sub channels is inherently inefficient.

Static Channel Allocation

$$T = \frac{1}{\mu C - \lambda}$$

C = 100 Mbps,

$1/\mu = 10{,}000$ bits

$\lambda = 5000$ frames/sec

T = 200 μsec

This result holds only when there is no contention in the channel.

Static Channel Allocation

a) Divide a single channel into N independent channels:

- C/N = 100/N Mbps,
- $1/\mu = 10{,}000$ bits
- □ $\lambda/N = 5000$ frames/sec
- T_N = Nx200 μsec
- For N=10 => T_N = 2 msec.

$$T_N = \frac{1}{\mu\left(\frac{C}{N}\right) - \left(\frac{\lambda}{N}\right)}$$

$$= \frac{N}{\mu C - \lambda} = \mathrm{NT}$$

Dynamic Channel Allocation

a) Dynamic channel allocation method is incorporated in all LANs and WANs.

b) Can handle all types of traffic conditions. Discipline is built up among the stations of the LAN so that fair opportunity is given to each station to transmit its data frames.

Assumptions for Dynamic Channel Allocation

1. Independent traffic
2. Single channel
3. Observable Collisions
4. Continuous or slotted time
5. Carrier sense or no carrier sense

Assumptions for Dynamic Channel Allocation

a) Single Channel:

- The single channel is available for all communication.
- All stations can transmit on it and all can receive from it.
- The stations are assumed to be equally capable in hardware though protocols may assign then different roles (i.e., priorities)

Assumptions for Dynamic Channel Allocation

a) Observable Collisions:

- If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled.
- This event is know as **collision**.
- All stations can detect that a collision has occurred. A collided frame must be retransmitted.
- No errors other than those generated by collision occur.

Assumptions for Dynamic Channel Allocation

a) Continuous or Slotted Time:

- Time may be assumed continuous. In which case frame transmission can begin at any instant.
- Alternatively, time may be slotted or divided into discrete intervals (called slots)
- Frame transmission must then begin at the start of a slot.
- A slot may contain 0, 1 or more frames, corresponding to an idle slot, a succeful transmission, or collision, respectively.

Assumptions for Dynamic Channel Allocation

a) Carrier Sense or No Carrier Sense:

- With the carrier sense assumption, stations can tell if the channel is in use before trying got use it.
- No station will attempt to use the channel while it is sensed as busy.
- If there is no carrier sense, stations cannot sense the channel before trying to use it.
- They will transmit then. One later they can determine whether the transmission was successful.

Multiple Access Protocols

- ALOHA
- Carrier Sense Multiple Access
- Collision-free protocols
- Limited-contention protocols
- Wireless LAN protocols

ALOHA

- 1970 Hawaii
- Norman Abramson and colleagues have enabled wireless communication between users in a remote island to the central computer in Honolulu.
- Two versions of the protocol now called ALOHA:
  - Pure ALOHA and
  - Slotted ALOHA

Pure ALOHA

a) Each user is free to transmit whenever they have data to be sent.

- There will be collisions
- Senders need some way to find out if this is the case.

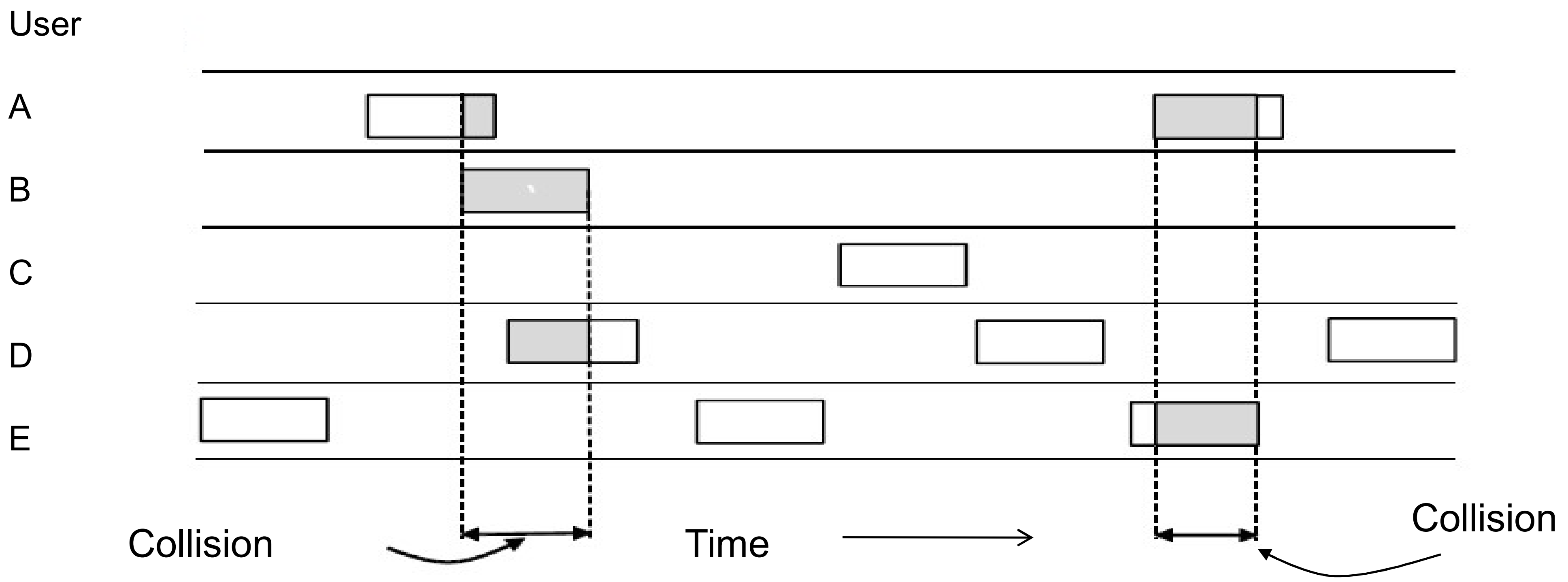
b) In ALOHA after the station transmits its message to the centra computer, the computer rebroadcast's the frame to all of the stations

- Original sending station can listen for the broadcast from the hub to see if its frame has gone through.

Pure ALOHA

  - In other wired systems the sender might be able to listen for collisions while transmitting.
- If the frame is destroyed, the sender just waits a random amount of time and sends it again.
  - Waiting time must be random or the sending frames will collide over and over.
  - **Contention** systems: multiple users that use the same channel in the way that might lead to conflicts.

PURE ALOHA (1)



In pure ALOHA, frames are transmitted at completely arbitrary times

Pure ALOHA

a) What is the efficiency of an ALOHA channel?

- Infinite collection of users typing at their terminals (stations).
- User states: WAITING or TYPING.
- When a line is finished, the user stops typing waiting for response.
- The station then transmits a frame containing the line over the shared channel to the central computer and checks the channel to see if it was successful.
- If so the users sees the reply and goes back to typing
- If not, the user continuously to wait while the station retransmits the frame over and over until it has been successfully send.

Pure ALOHA

a) Frame Time – denotes the amount of time needed to transmit the standard, fixed-length frame.

b) Each new frame is assumed to be generated by Poisson distribution with a mean of N frames per frame time.

   - If N>1 the user community is generating frames at a higher rate than the channel can handle, and nearly every frame will suffer a collision.
   - For reasonable throughput we expect 0 < N < 1.

Pure ALOHA

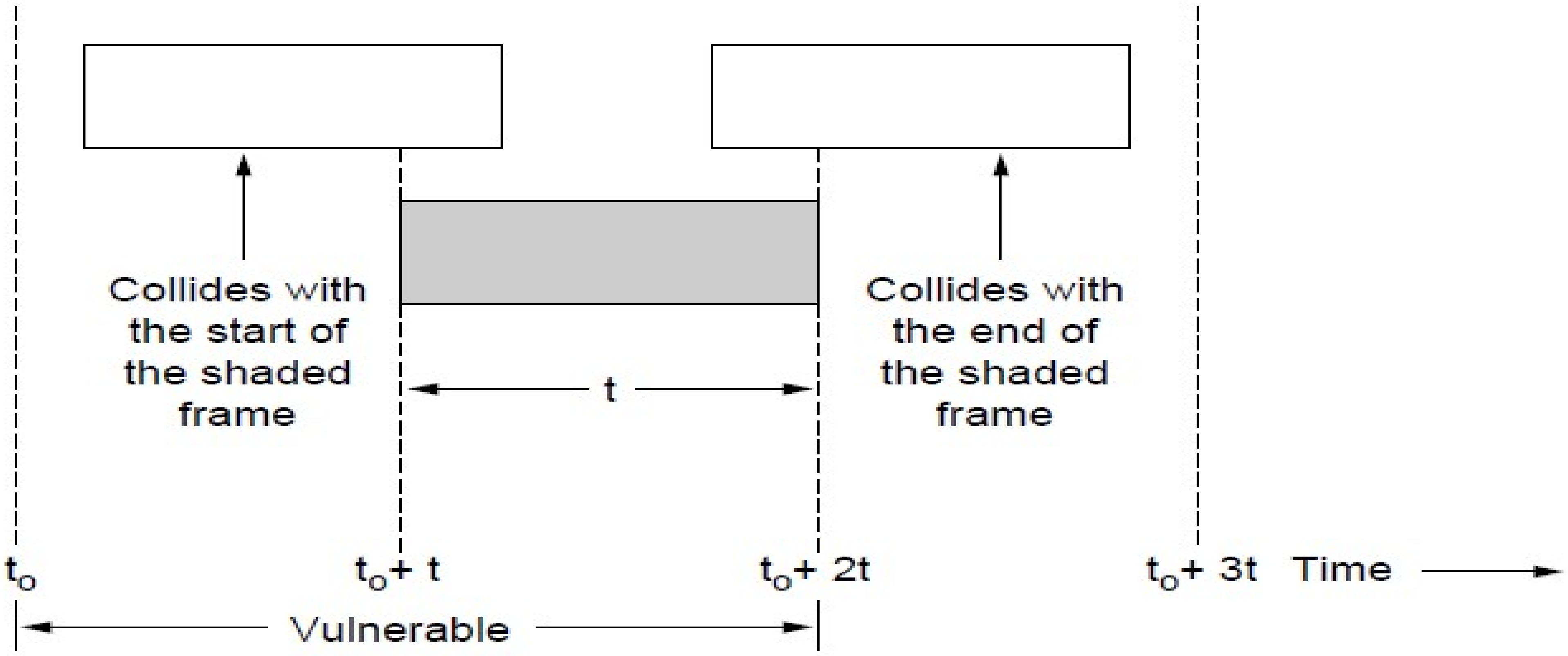
- In addition to the new frames, the stations also generate retransmissions of frames that previously suffered collisions.
- Assume that the new and the old frames combined are well modeled by a Poisson distribution with mean G frames per frame time. $G \geq N$.
  - Low load: $N \approx 0$ there will be few collisions, hence few retransmissions, $G \approx N$
  - High load: there will be many collisions, $G > N$.

Pure ALOHA

Under all loads the throughput S is just the offered load, G, times the probability P_0 of a transmission succeeding:

$$S = GP_0$$

ALOHA (2)


Collides with the start of the shaded frame
Collides with the end of the shaded frame
t
t_o
t_o+ t
t_o+ 2t
t_o+ 3t
Time
Vulnerable

Vulnerable period for the shaded frame.

Pure ALOHA

a) The probability that k frames are generated during a given frame time, in which G frames are expected, is given by the Poison distribution:

$$\Pr[k] = \frac{G^k e^{-G}}{k!}$$

- Probability of zero frames: e^{-G}
- In an interval two frame times long, the mean number of frames generated is 2G.
- Probability of no frames being initiated during the entire vulnerable period is given by $P_0 = e^{-2G}$.

Using *S = GP0, we get*

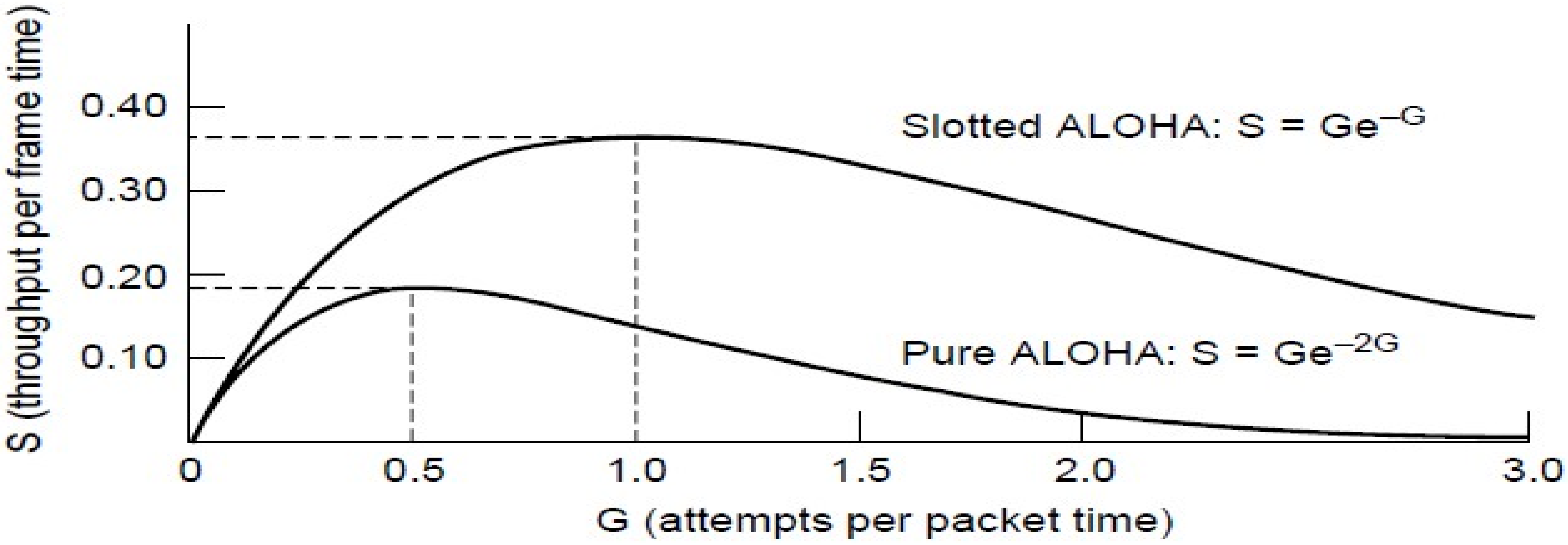
Pure ALOHA

a)

$$S = Ge^{-2G}.$$

- The relation between the offered traffic and the throughput is given in the next slide.
- The maximum throughput occurs at G=0.5 with S=1/2e which is about 0.184.
  - The maximum utilization of the channel thus is 18%.

ALOHA (3)



Throughput versus offered traffic for ALOHA systems.

Sloted ALOHA

a) Roberts in 1972 doubled the capacity of an ALOHA system.
   - Divide time into discrete intervals called **slots**.
   - Each interval corresponds to one frame.
   - Users will have to agree on slot boundaries.

b) Synchronization is required:
   - One special station emit a pip at the start of each interval, like clock.

Slotted ALOHA

- Slotted ALOHA
  - peaks at the G = 1
  - Throughput S = 1/e = 0.367 or 37%.
- The best case scenario:
  - 37% of slots are empty
  - 37% of successes, and
  - 26% collisions.

Carrier Sense Multiple Access (CSMA)

a) In CSMA a station senses the carrier on the channel before starting its own transmission. When the channel is sensed to be idle, a station can take one of three different approaches to transmit a packet on the channel.

b) When a station starts transmission of a frame, the other stations have to wait.

c) However, collisions may occur when two or more stations start their transmissions before hearing each other's signal.

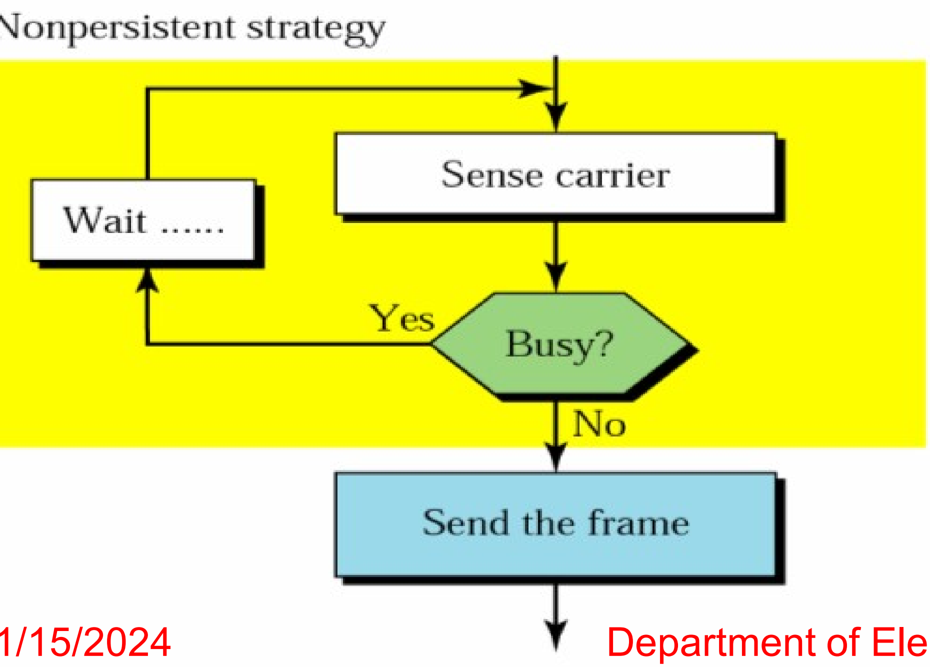
d) There are three approaches to CSMA:

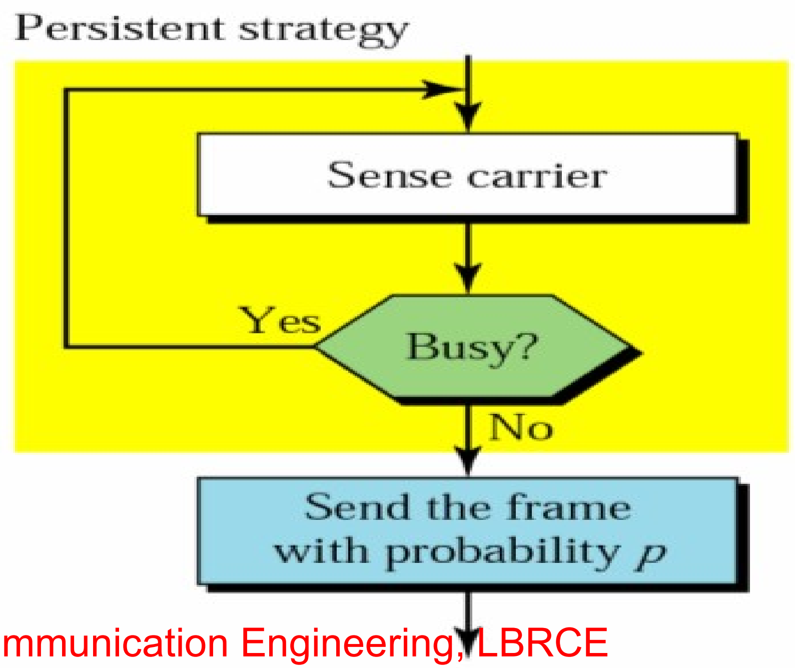
  - I-persistent CSMA
  - Non-persistent CSMA
  - P-persistent CSMA

- In Non-persistent CSMA the station checks whether the medium is free or not. If it is not it waits fo random amount of time and again checks and if it is available, station transmits the frame.

a) In I-persistent CSMA scheme, the station keeps monitoring the medium and transmit a frame wher is found available. The problem in this scheme is that two or more stations may sense the channel be idle and then all of them begin their transmissions immediately which causes collisions.

- In P-persistent CSMA the stations do not transmit as soon as they detect the medium to be free. It wa for a random amount of time. With introduction of this delay element the frame is transmitted and t probability of collision reduces.



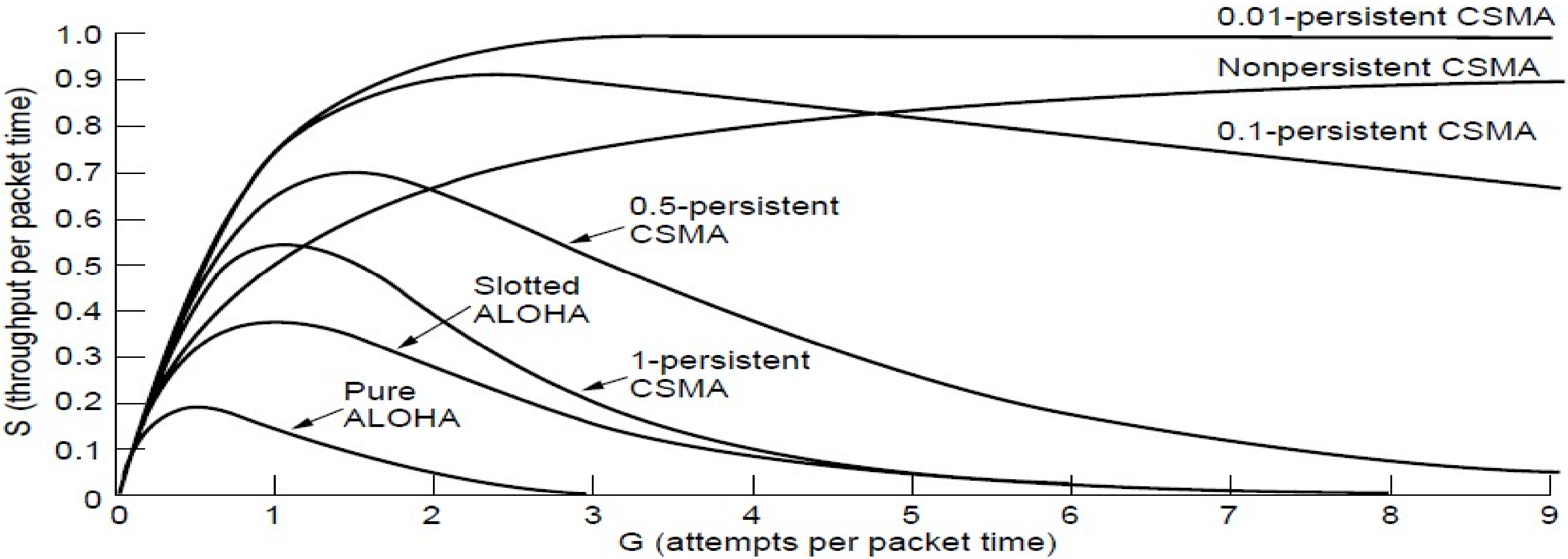


Carrier Sense Multiple Access Protocols

- Protocols in which stations listen for a carrier (i.e., transmission) and act accordingly are called **carrier sense** protocols.
- Several Versions of those protocols will be discussed.

1. Persistent and Nonpersistent CSMA
2. CSMA with Collision Detections

Persistent and Nonpersistent CSMA



Comparison of the channel utilization versus load for various random access protocols.

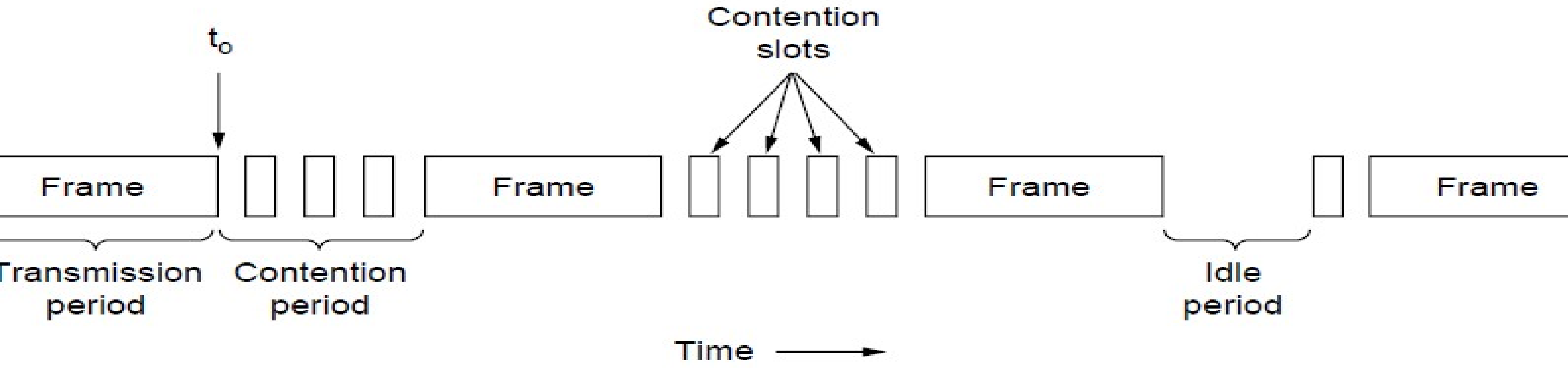
CSMA with Collision Detection

a) Protocols that sense Collisions are know as **CSMA with Collision Detection** (CSMA/CD)

b) This protocol is a basis of classical Ethernet LAN.

- The transmitting station is reading the data that it is transmitting.
- If it is garbled up then it will know that collision has occurred.

CSMA with Collision Detection



CSMA/CD can be in one of three states: contention, transmission, or idle.

CSMA with Collision Detection

- In CSMA/CD collisions do not occur once the station has unambiguousl captured the channel, but they still occur during the contention period.
- These collisions adversely affect the system performance (e.g., bandwidth delay product is large – long cable that has a large propagation delay τ anc frames are short).

Collision-Free Protocols

a) Collisions in any system adversely affect the overall system performance.

b) When the distance between station is large and packet length is short.

c) To resolve collision and contention two protocols are designed

1. Bit-map protocol 2. Binary count down

Basic Bit-Map Protocol

a) Each contention period consists of exactly N slots.

b) If station 0 has a frame to send, it transmits a 1 bit during the slot 0.

c) No other station is allowed transmit during this slot.

d) Regardless what station 0 does, station 1 gets to opportunity to transmit a 1 bit during slot 1, but only if it has a frame queued.

e) In general, station j may announce that it has a frame to send by inserting a 1 bit into slot j.

f) After all N slots have passed by, each station has complete knowledge of which stations wish to transmit. At which point they begin transmitting frames in numerical order.

Bit-Map Protocol

a) Protocols that broadcast their intention before that actually transmit are called **reservation protocols**.

b) Low-load conditions:

- Average wait conditions for low-numbered stations:
  - N/2 slots for current scan to finish, and
  - N slots for the following scan to run to completion before it may begin transmitting
  - 1.5N slots wait time.
- Average wait conditions for high-numbered stations:
  - 0.5N slots wait time.
- Mean of all stations is N times.

Bit-Map Protocol

- Efficiency:
  - Overhead bits N
  - Data bits d

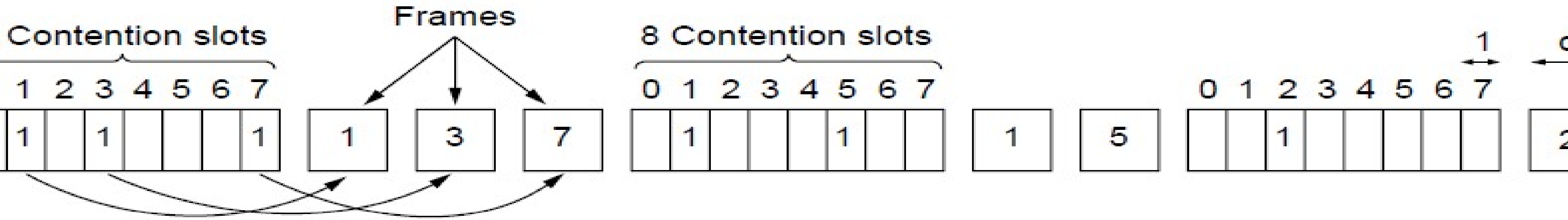
$$\frac{d}{(d + N)}$$

- High-load
  - N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame:
- Efficiency:

$$\frac{d}{(d + 1)}$$

- Mean delay:
  - Sum of the time it queues in the station +
  - ***(N(d+1)/2 once it gets to the head of its internal queue***

Collision-Free Protocols (1)



The basic bit-map protocol.

Binary Countdown

- A problem with the basic bit-map protocol is the overhead of 1 bit per station.
  - Large overhead for the network with large number of stations.
- A better solution is to use binary station addresses with a channel that combines transmissions.
- A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high-order bit. The addresses are assumed to be the same length.
- The bits in each address position from different stations are BOOLEAN.
  - They OR-ed together by the channel when they are send at the same time.
  - **Binary Countdown** protocol

Binary Countdown

a) Arbitration rule: As soon as a station sees that a high-ordered bit position that is 0 in its address has been overwritten with 1 it gives up.

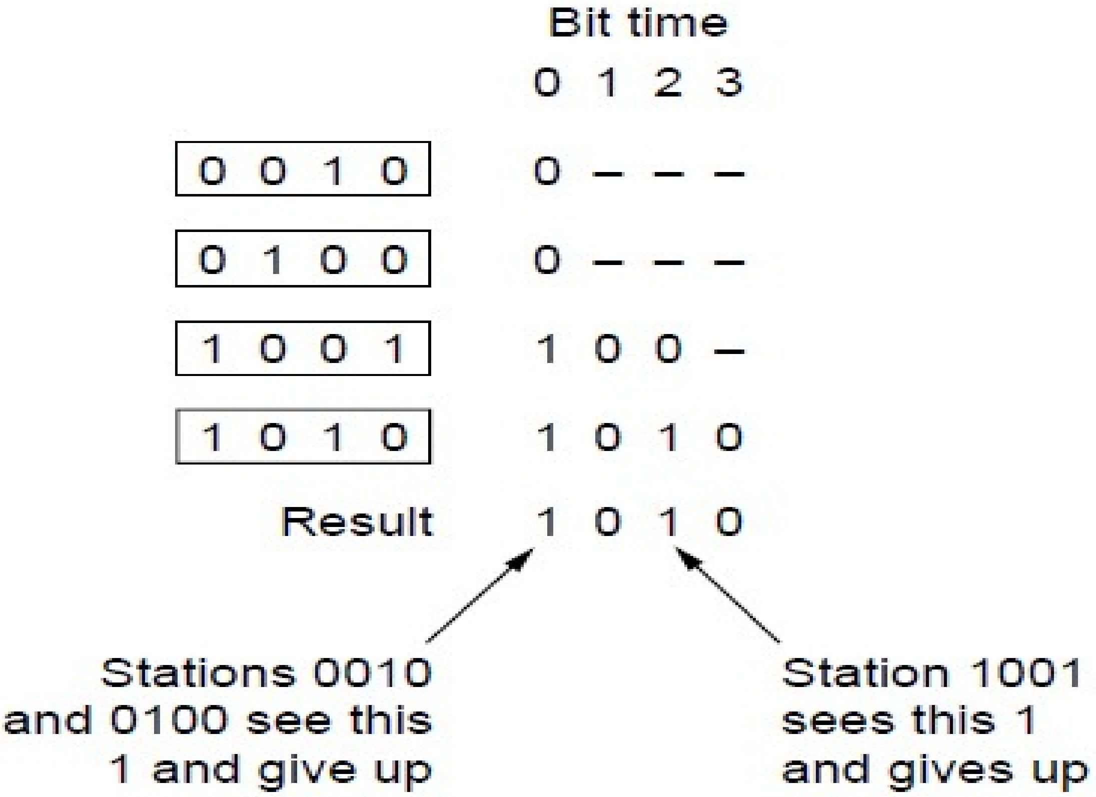
b) Example:

- If stations 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first bit time the stations transmit 0, 0, 1, and 1, respectively.
- They are OR-ed together to get 1.
- Stations 0010 and 0100 see the 1 and know that higher-numbered stations is competing for the channel and they give up for the current round.
- Stations 1001 and 1010 continue.

Binary Countdown

- The next bit is 0 so both stations continue.
- The next bit is 1 so the station 1001 gives up and station 1010 wins the bidding.
- This gives it a right to transmit the frame, after which a new cycle starts.

Binary Countdown



	Bit time			
	0	1	2	3
0 0 1 0	0	–	–	–
0 1 0 0	0	–	–	–
1 0 0 1	1	0	0	–
1 0 1 0	1	0	1	0
Result	1	0	1	0

Stations 0010 and 0100 see this 1 and give up

Station 1001 sees this 1 and gives up

The binary countdown protocol. A dash indicates silence.

Token Passing

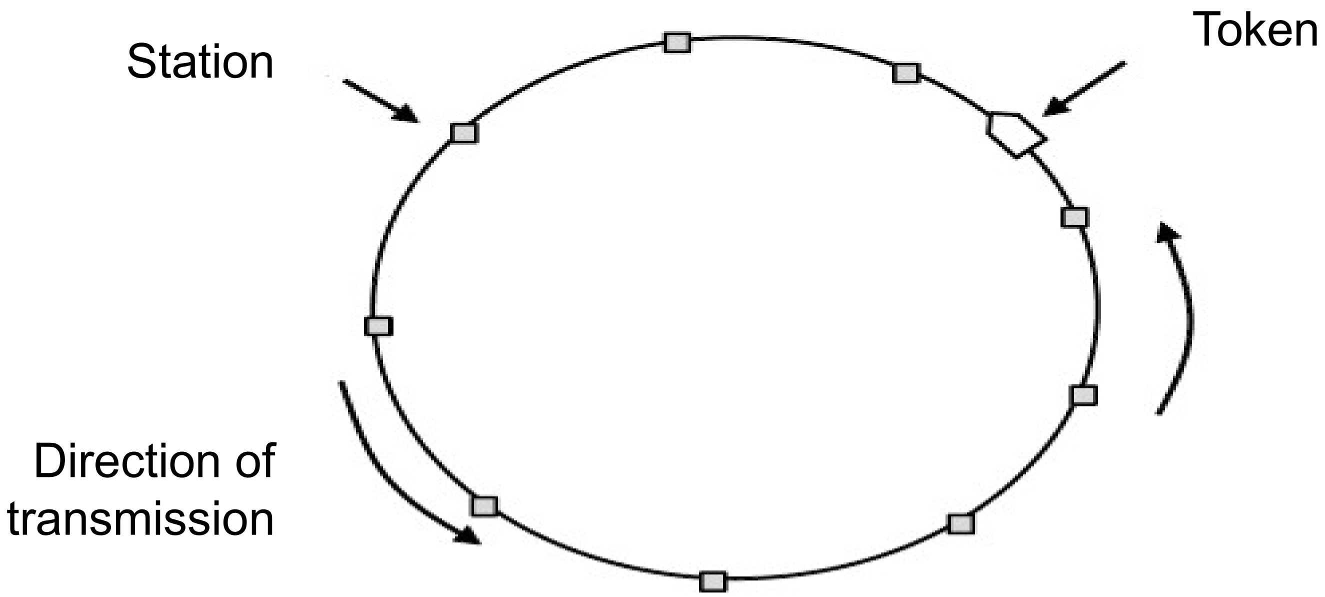
a) Message is passed called **token** form station to the next in the same predefined order.

b) Token Ring or Token Bus protocols work the same way.

c) One has to pay attention to the ring because if it is not removed from circulation it will end up being there forever.

d) Typically it will be removed by the receiving station and/or sending station.

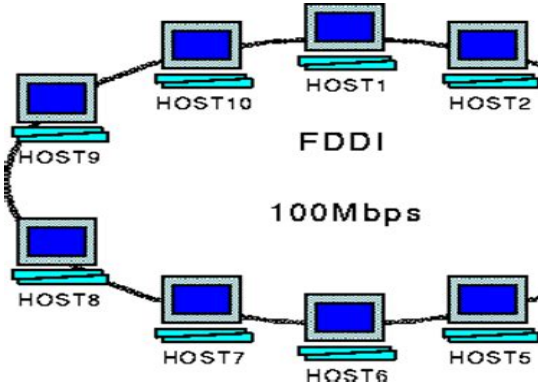
Collision-Free Protocols (2)

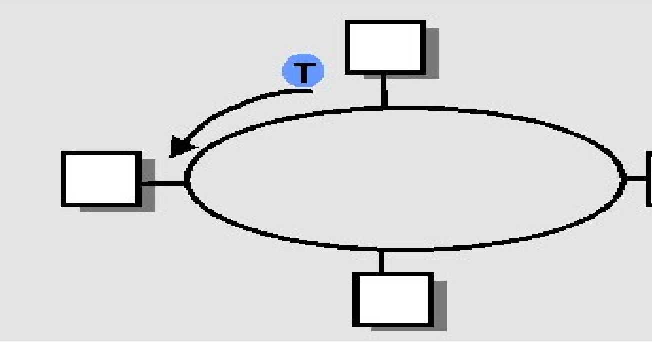


Token ring.

Token Passing Protocols

- Station that holds token transmits into ring
- token circulates among stations
- media:
  - token ring connection: IEEE802.5, FDDI
  - token bus, IEEE802.4
- to transmit
  - station must seize token
  - transmit packet while holding token
  - release (send out) token





Ethernet

- Ethernet Cabling
- MAC sublayer protocol
- Ethernet performance
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet

Ethernet Cabling

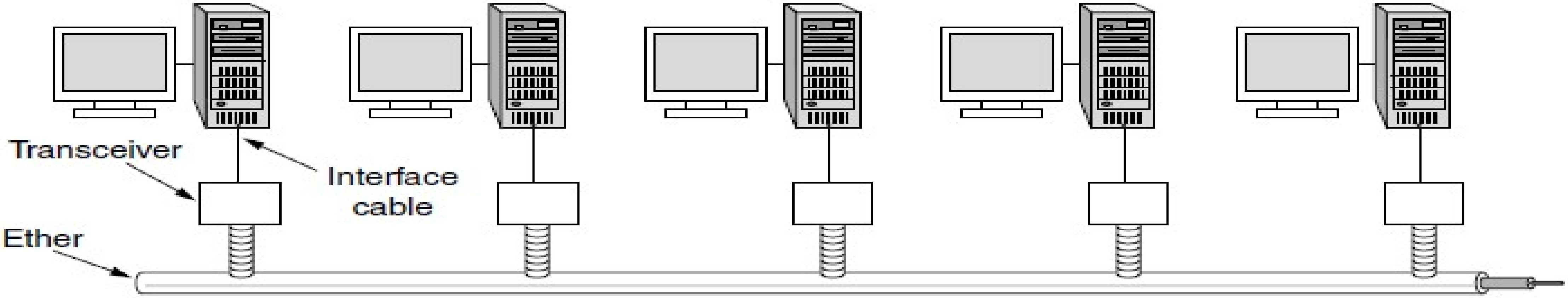
a) Thick Ethernet – a thick cable. Segment could be as long as 500 m Could be used to connect up to 100 computers.

b) Thin Ethernet – BNC connectors. Segment could be no longer thar 185 m. Could be used to connect up to 30 computers.

c) For a large length connectivity the cables could be connected by repeaters.

d) Repeater is a physical layer device that receives, amplifies, anc retransmits signals in both directions.

Classic Ethernet Physical Layer

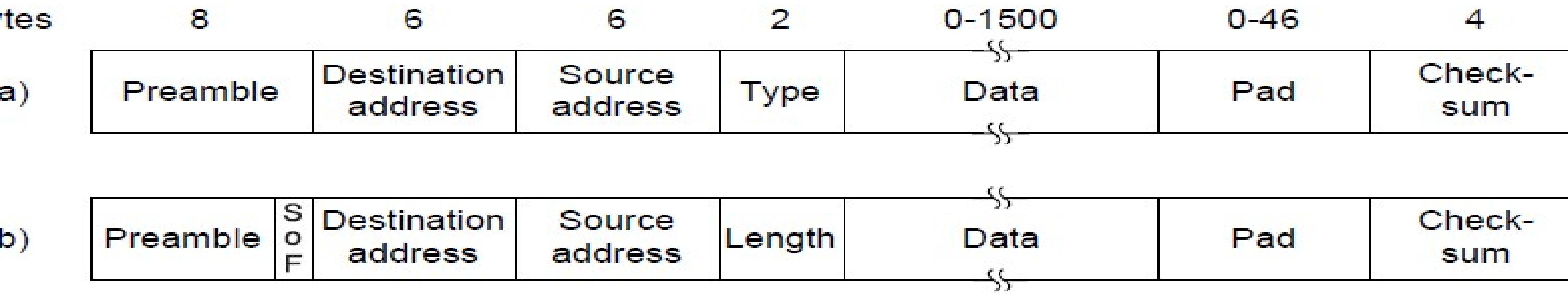


Architecture of classic Ethernet

Classical Ethernet

- Over each of those cables the signal was coded using Manchester encoding.
- Other restriction was that no two transceivers could be more than 2.5 km apart and no path between any two transceivers could traverse more than four repeaters.
- This limitation was impose due to the MAC protocol used.

MAC Sublayer Protocol (1)



tes	8	6	6	2	0-1500	0-46	4
a)	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum
b)	Preamble SoF	Destination address	Source address	Length	Data	Pad	Check-sum

Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

Classic Ethernet MAC Sublayer Protocol

- Format to send frames is shown in the figure in the previous slide.

1. Preamble – 8 bytes
   - 7x 10101010 and 10101011 <- Start of Frame Delimiter (802.3).
   - The Manchester encoding of this pattern produces 10-MHz wave for 6.4 μsec – used for synchronization.
   - The last two bits indicate the start of the frame.

Classic Ethernet MAC Sublayer Protocol

2. Two addresses each 6 bytes – destination + source
   - First bit of the destination address is 0 for ordinary addresses and 1 for group addresses.
   - Group address allow multiple destinations to listen to a single address – **Multicasting**.
   - Special address consisting of all 1 is reserved for **broadcasting**.
   - Uniqueness of the addresses:
     - First 3 bytes are used for (**Organizationally Unique Identifier**)
     - Blocks of 2^{24} addresses are assigned to a manufacturer.
     - Manufacturer assigns the last 3 bytes of the address and programs the complete address into the NIC.

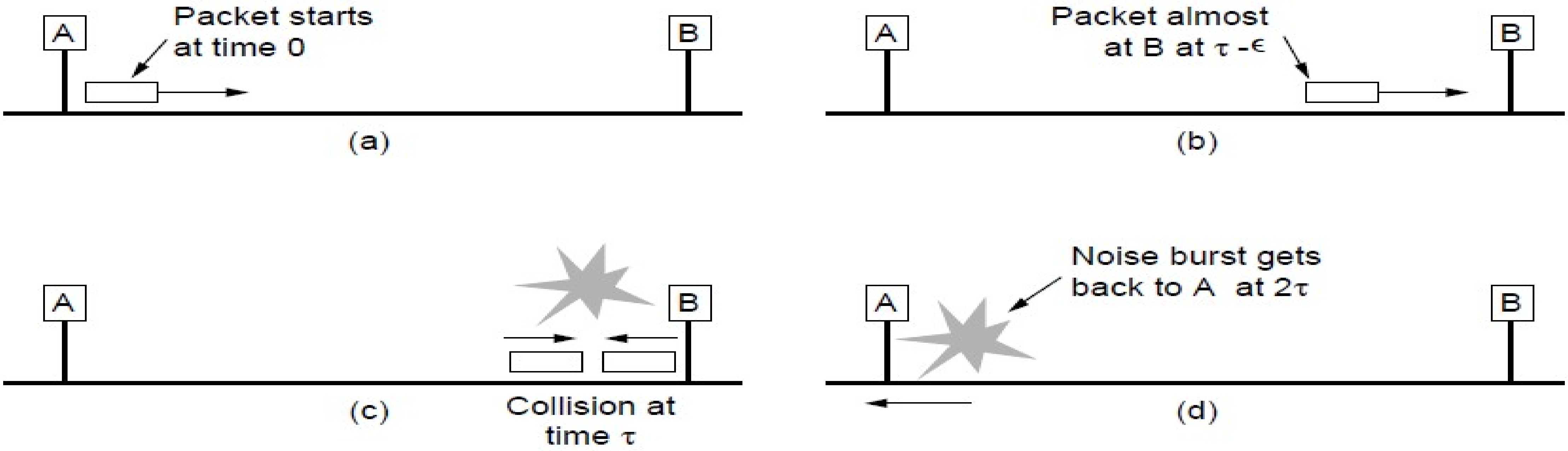
MAC Sublayer Protocol

3. Type or Length field.
   - Depending whether the frame is Ethernet or IEEE 802.3
   - Ethernet uses a Type field to tell the receiver what to do with the frame.
   - Multiple network-layer protocols may be in use at the same time on the same machine. So when Ethernet frame arrives, the operating system has to know which one to hand the frame to. The Type field specifies which process to give the frame to. E.g. 0x0800 indicates the frame contains IPv4 packet.

MAC Sublayer Protocol

4. Data Field
   - Up to 1500 bytes.
   - Minimum frame length – valid frames must be at least 64 bytes long – from destination address to checksum.
   - If data portion is less than 46 bytes the Pad field is used to fill out the frame to the minimum size.
   - Minimum filed length is also serves one very important role – prevents the sender to complete transmission before the first bit arrives at the destination.

MAC Sublayer Protocol (2)



Collision detection can take as long as 2τ.

MAC Sublayer Protocol

a) 10 Mbps LAN with a maximum length of 2500 m and four repeaters the round-trip time has been determined to be nearly 50 μsec in the worst case.

b) Shortest allowed frame must take at least this long to transmit.

- At 10 Mbps a bit takes 100 nsec
- 500 bits (numbit = 10 Mbps X 100 nsec) rounded up to 512 bits = 64 bytes.

MAC Sublayer Protocol

4. Checksum
   - It is a 32-bit CRC of the kind that we have covered earlier.
   - Defined as a generator polynomial described in the textbook.

Ethernet Performance

a) Here we see where the maximum cable distance between any two stations enters into the performance figures.

b) The longer the cable the longer the contention interval; This is why the Ethernet standard specifies the maximum cable length.

c) It would be instructive to reformulate the equation in the previous slide in terms of the frame length F, network bandwidth B and the cable length L, speed of signal propagation c, for the optimal case e contention slots per frame.

Ethernet Performance

- P = F/B the equation becomes:

$$E = \frac{1}{1 + 2BLe/cF}$$

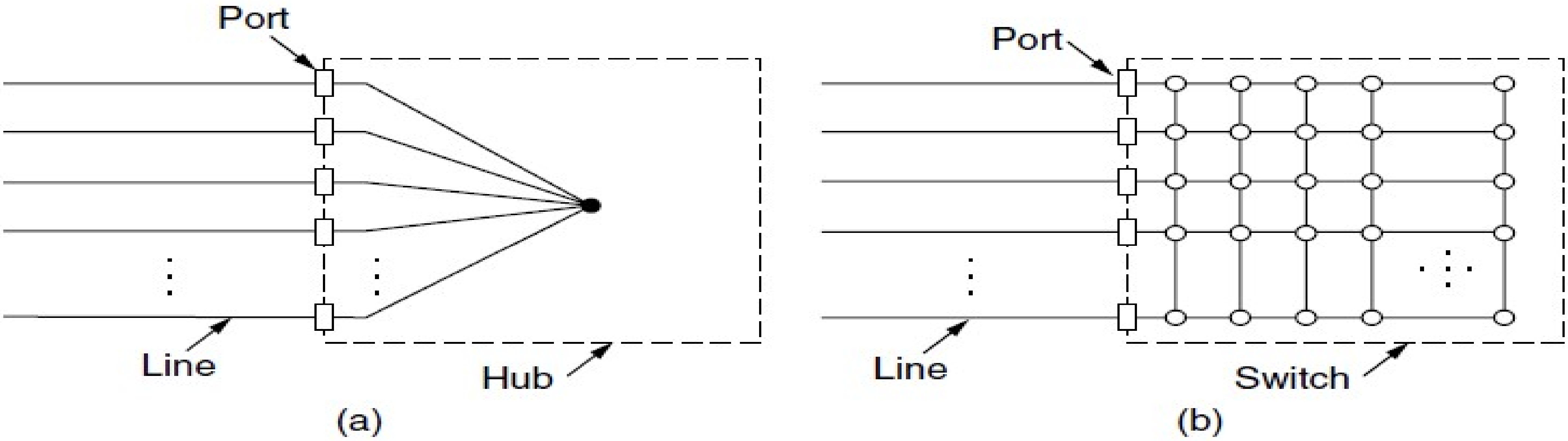
- When the term $2BLe/cF$ >> 0 the network efficiency becomes very low.
  - Increasing BL; Bandwidth and/or Length of the cable reduces the efficiency.
  - This is contrary to the design criteria to have largest possible bandwidth and longest connections.
  - Classical Ethernet will not be able to provide this.

Switched Ethernet

a) Wiring was changed from a long cable architecture to a more complex architecture:

- Each station has a dedicated cable running to a central **hub**. (Fig (a) in the next slide).
- Adding and removing a station become much easier.
- Cable length was reduced to 100 m for telephone twisted pair wires and to 200 hundred if Category 5 cable was used.
- Hubs do not increase capacity – they are equivalent to the single long cable of classic Ethernet.
  - As more stations were added the performance of each station degraded.

Switched Ethernet (1)



(a) Hub. (b) Switch.

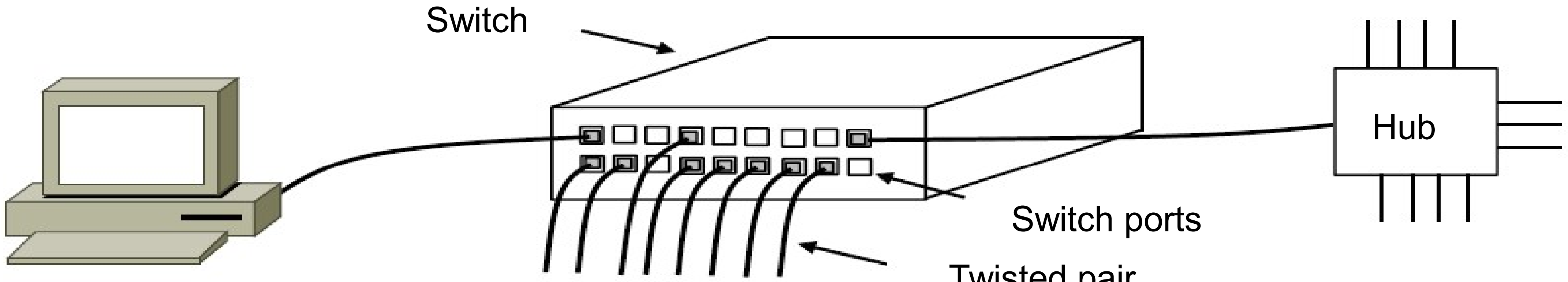
Switched Ethernet

- One could solve this problem by increasing the speed of the basic Ethernet from 1 Mbps to 10 Mbps, 100 Mbps or even 1 Gbps.
- However, multimedia applications requires even higher bandwidths.

a) **Switch** is the solution.

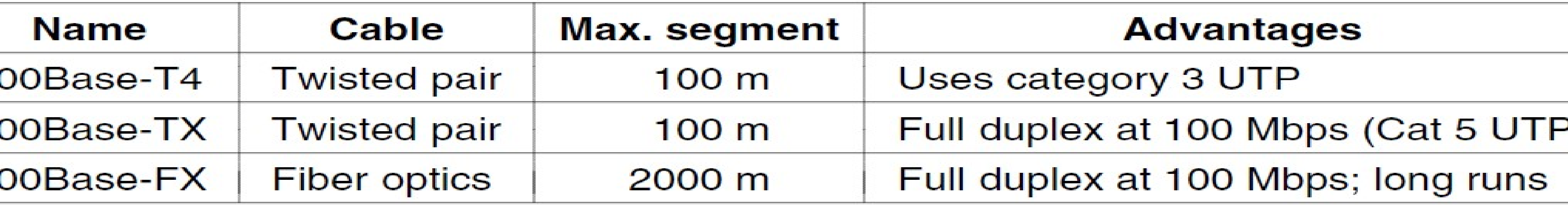
- Switch must be able to determine which frame goes to what station.
- Security benefits
- No collision can occur.

Switched Ethernet (2)



An Ethernet switch.

Fast Ethernet



Name	Cable	Max. segment	Advantages
00Base-T4	Twisted pair	100 m	Uses category 3 UTP
00Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP
00Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

The original fast Ethernet cabling.

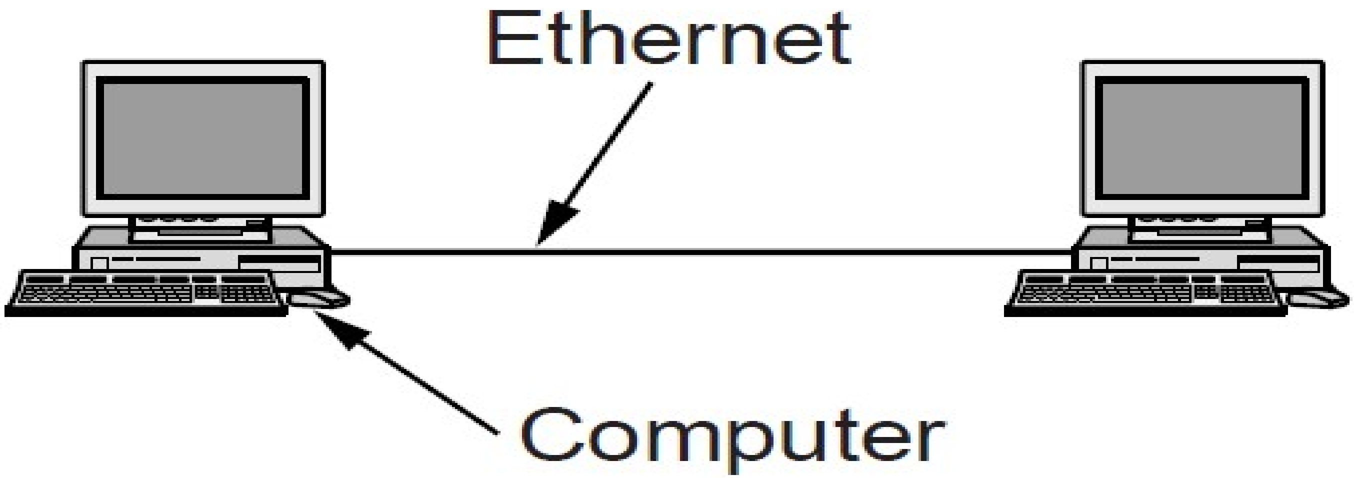
GigaBit Ethernet

a) After the standard for Fast Ethernet was adopted the work for yet even faster standard started: GigaBit Ethernet

b) Goals:

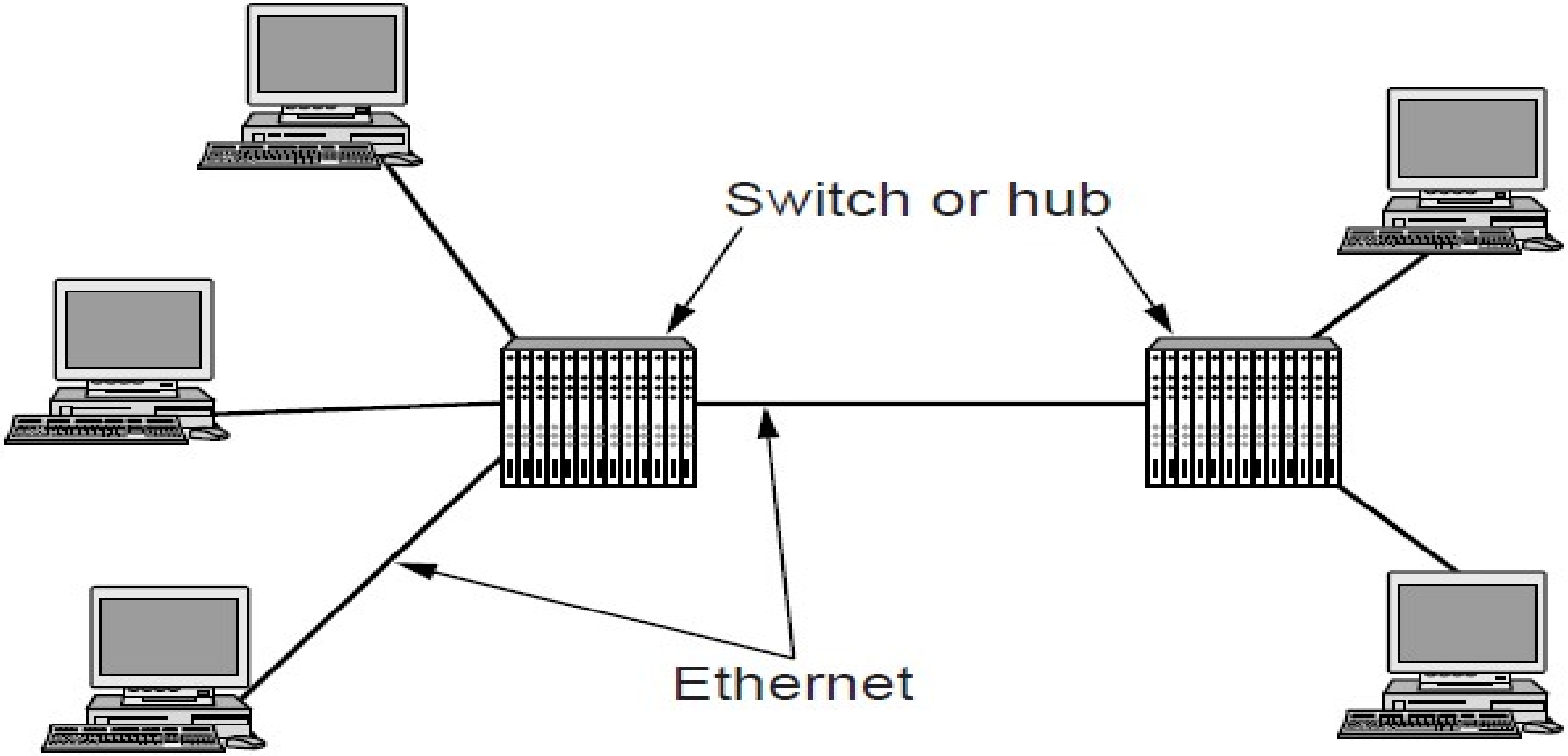
- Increase performance ten fold over Fast Ethernet.
- Maintain compatibility with both Classical and Fast Ethernet.
- Unacknowledged datagram service with both unicast and broadcast.
- Use the same 48-bit addressing scheme already in use,
- Maintain the same frame format including minimum and maximum sizes.

Gigabit Ethernet (1)



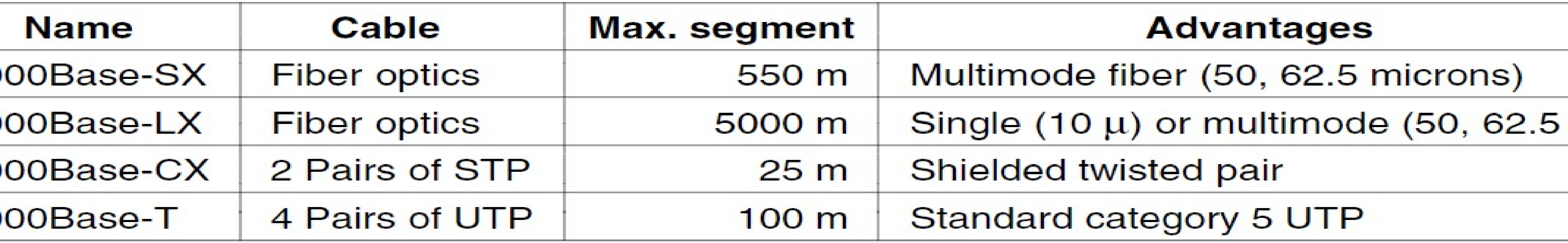
A two-station Ethernet

Gigabit Ethernet (2)



A two-station Ethernet

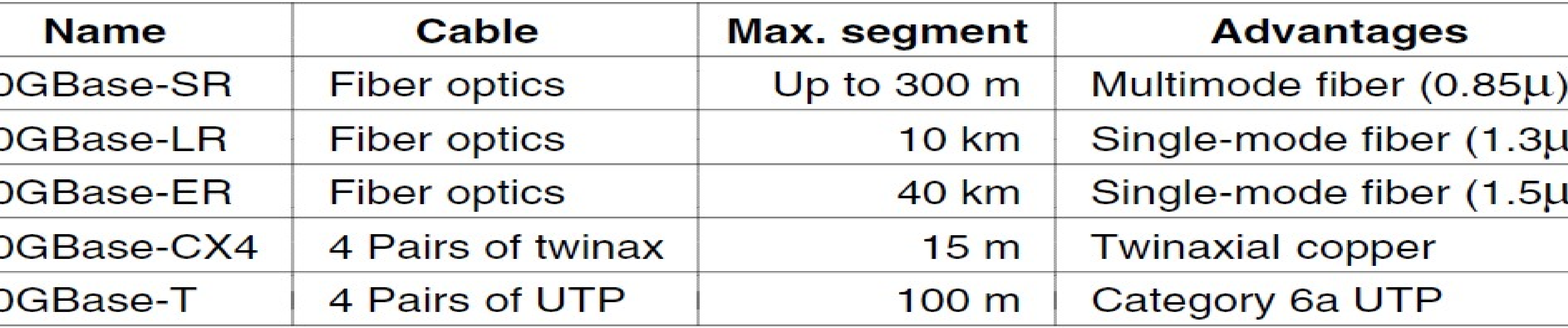
Gigabit Ethernet (3)



Name	Cable	Max. segment	Advantages
00Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
00Base-LX	Fiber optics	5000 m	Single (10 µ) or multimode (50, 62.5
00Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
00Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Gigabit Ethernet cabling.

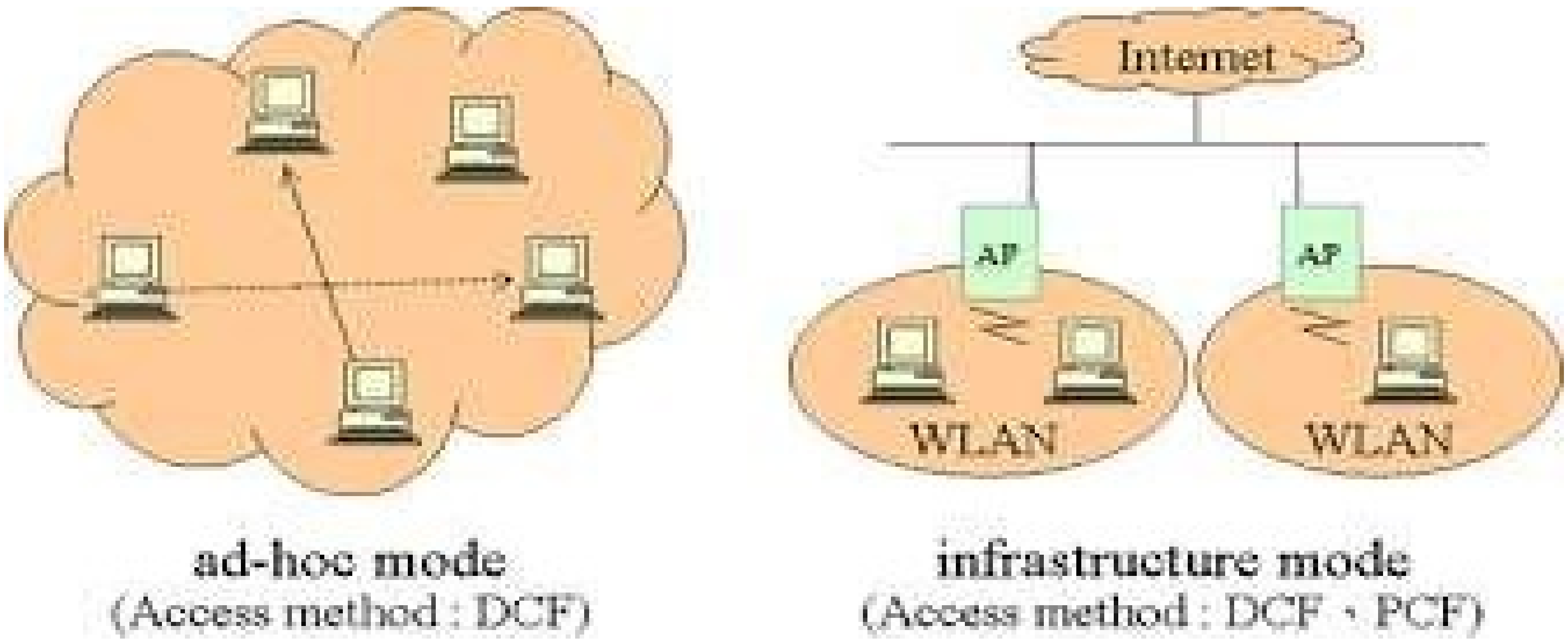
10 Gigabit Ethernet



Name	Cable	Max. segment	Advantages
0GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85μ)
0GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3μ
0GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5μ
0GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
0GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

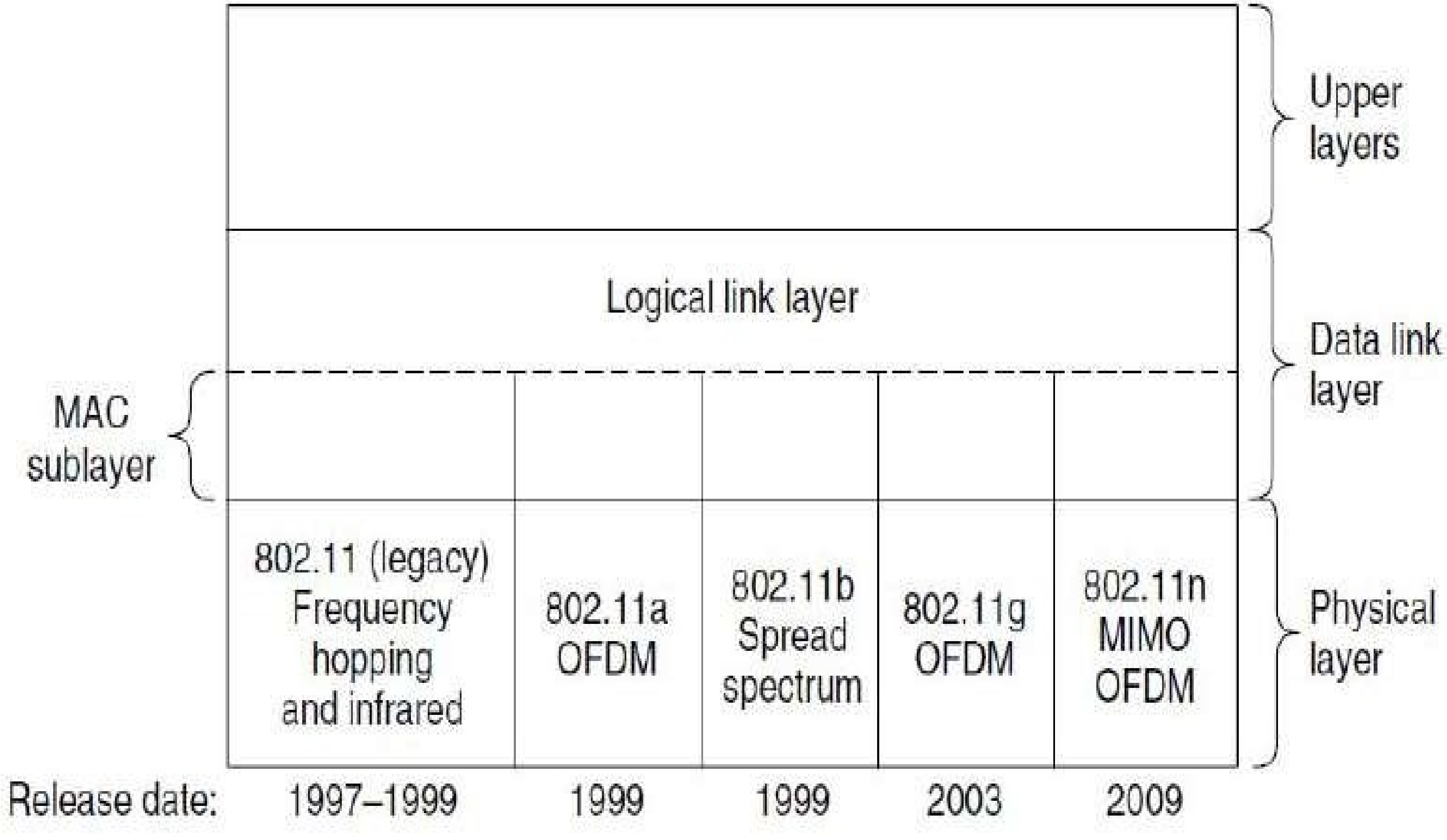
Gigabit Ethernet cabling

802.11 Wireless LAN Infrastructure

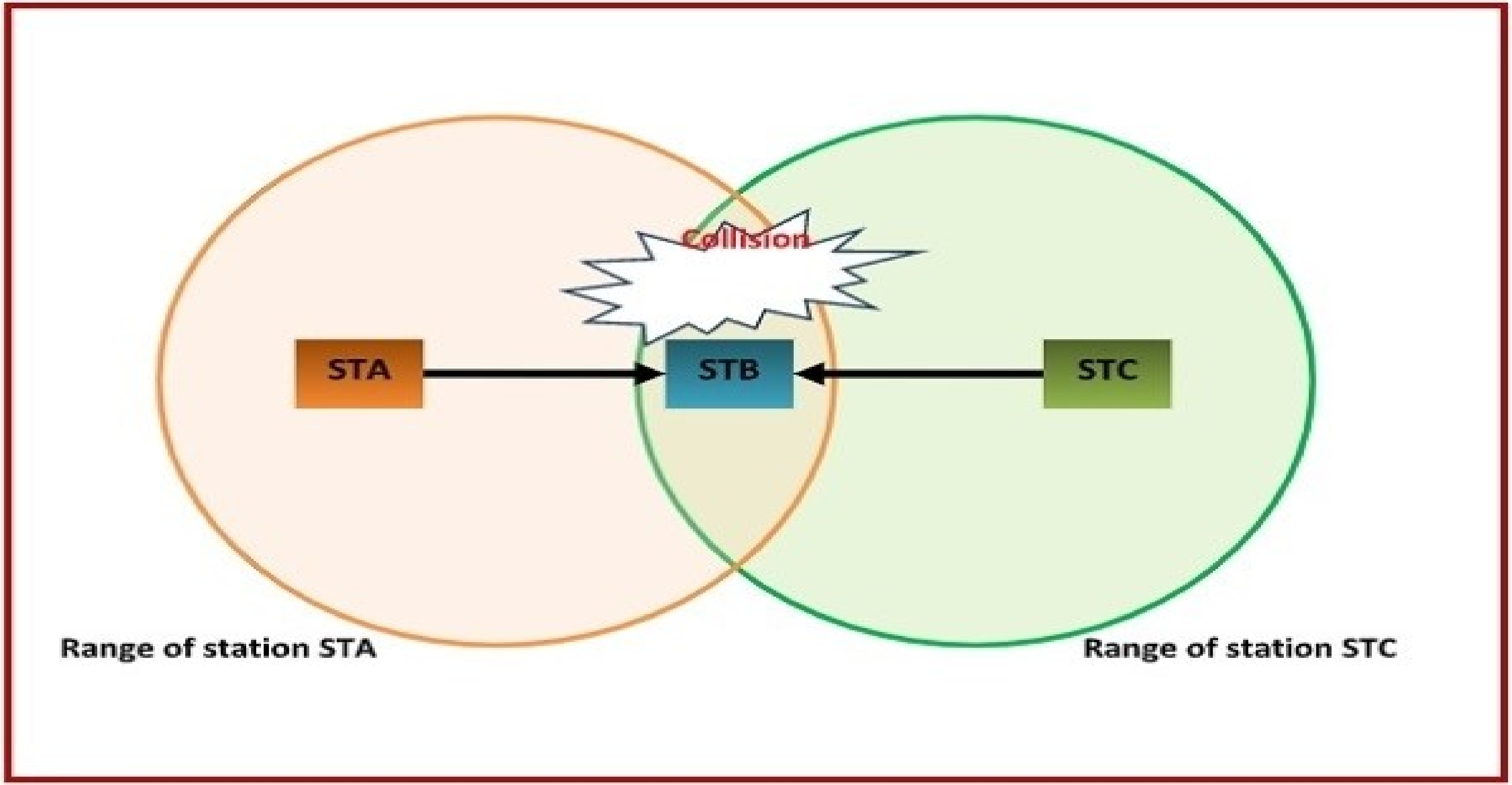


- 802.11 networks can be used in two modes: Infrastructure and Ad hoc Mode.
- **Infrastructure mode** requires a central access point that all devices connect to.
- **Ad-hoc mode** is also known as “peer-to-peer” **mode**. **Ad-hoc** networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other.

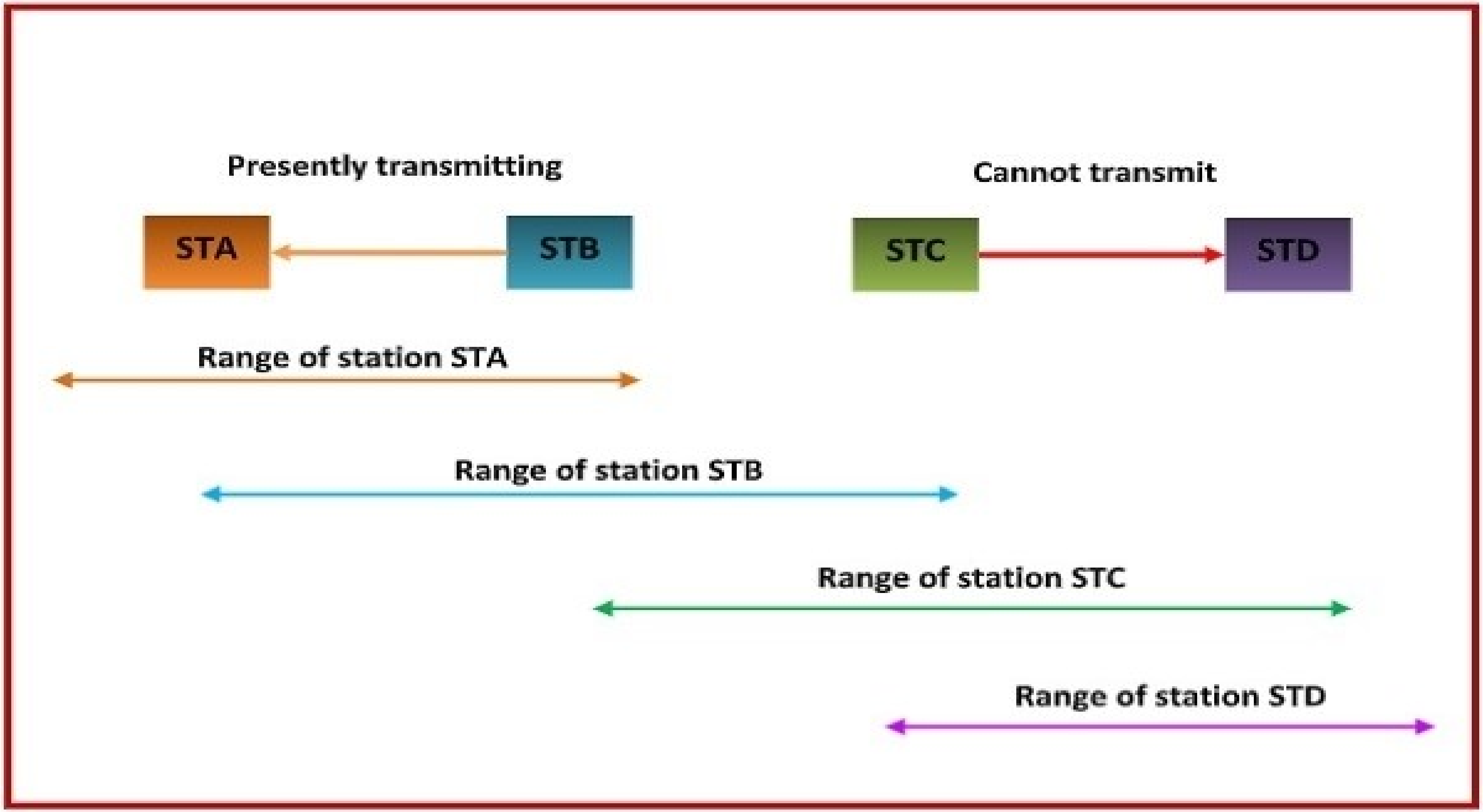
802.11 Protocol Stack



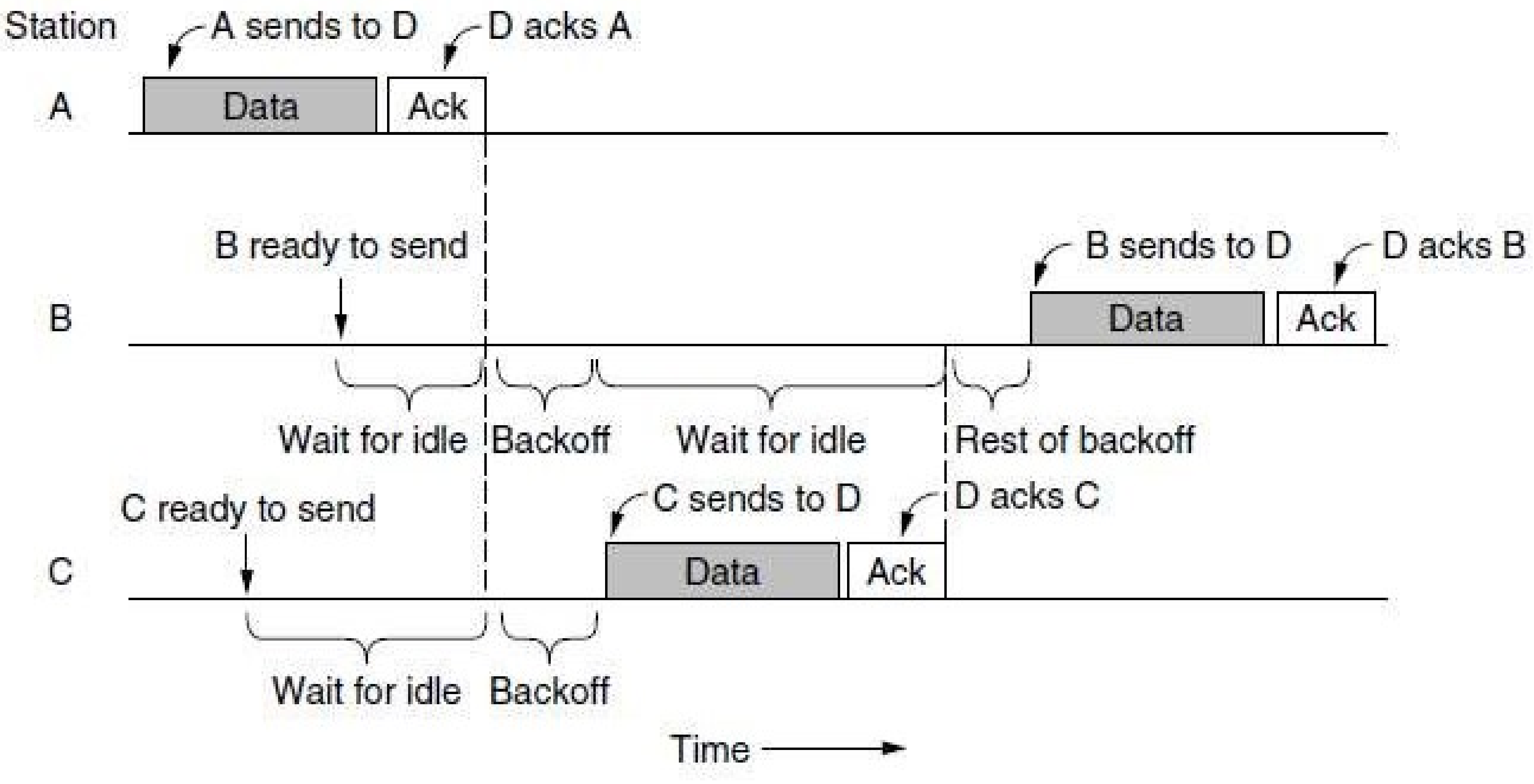
Hidden Problem



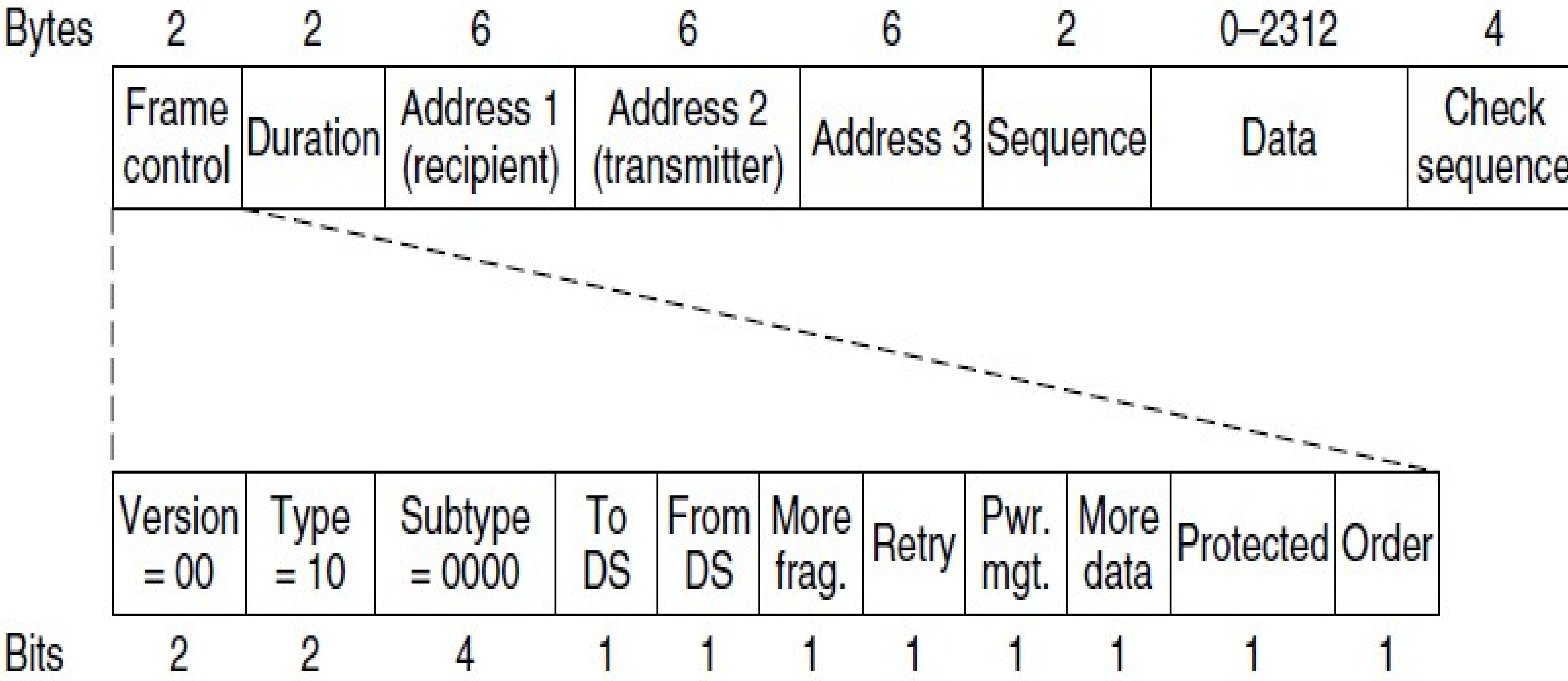
Exposed problem



Simple CSMA in action



802.11 Frame Format



	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence
Bytes	2	2	6	6	6	2	0–2312	4

	Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More frag.	Retry	Pwr. mgt.	More data	Protected	Order
Bits	2	2	4	1	1	1	1	1	1	1	1

802.11 Frame Format

- **Protocol Version:** zero for 802.11 standard
- **Type**= frame type: data, management, control
- **Subtype** = frame sub-type:

  To DS: When bit is set indicate that destination frame is for DS

  From DS: When bit is set indicate frame coming from DS

Retry: Set in case of retransmission frame

More fragments: Set when frame is followed by other fragment

Power Management: bit set when station go Power Save mode(PS)

More Data: this bit indicates that the sender has additional frames for the receiver.

Protected Frame: this bit indicates that the frame body has been encrypted for security.

Order: this "bit tells the receiver that the higher layer expects the sequence of frames to arrive strictly in order".

802.11 Services

- Association
- Reassociation
- Disassociation

802.11 Services

- **Association**

Establishes initial association between station and AP

- **Re-association**

Enables transfer of association from one AP to another, allowing station to move from one BSS to another

- **Disassociation**

Association termination notice from station or AP. A station should use this service before shutting down or leaving the network. The AP may use it before going down for maintenance

802.15 Bluetooth

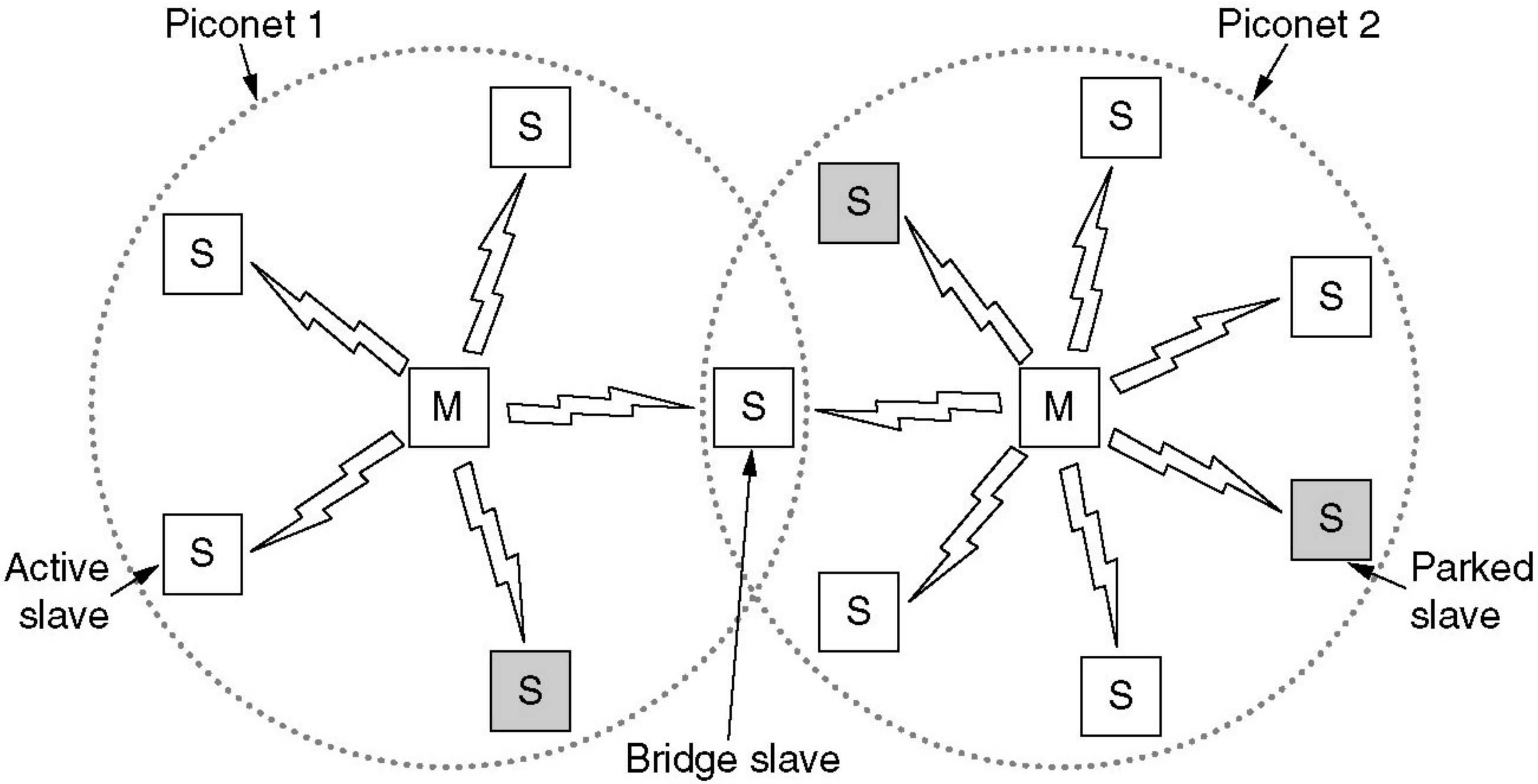
- Bluetooth Architecture
- The Bluetooth Protocol Stack
- The Bluetooth Frame Structure

802.15 Bluetooth

Bluetooth is a network technology that connects mobile devices wirelessly over a short range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, instead of RS-232 data cables of wired PANs.

There are two types of Bluetooth networks −
Piconets
Scatternets

Bluetooth Architecture



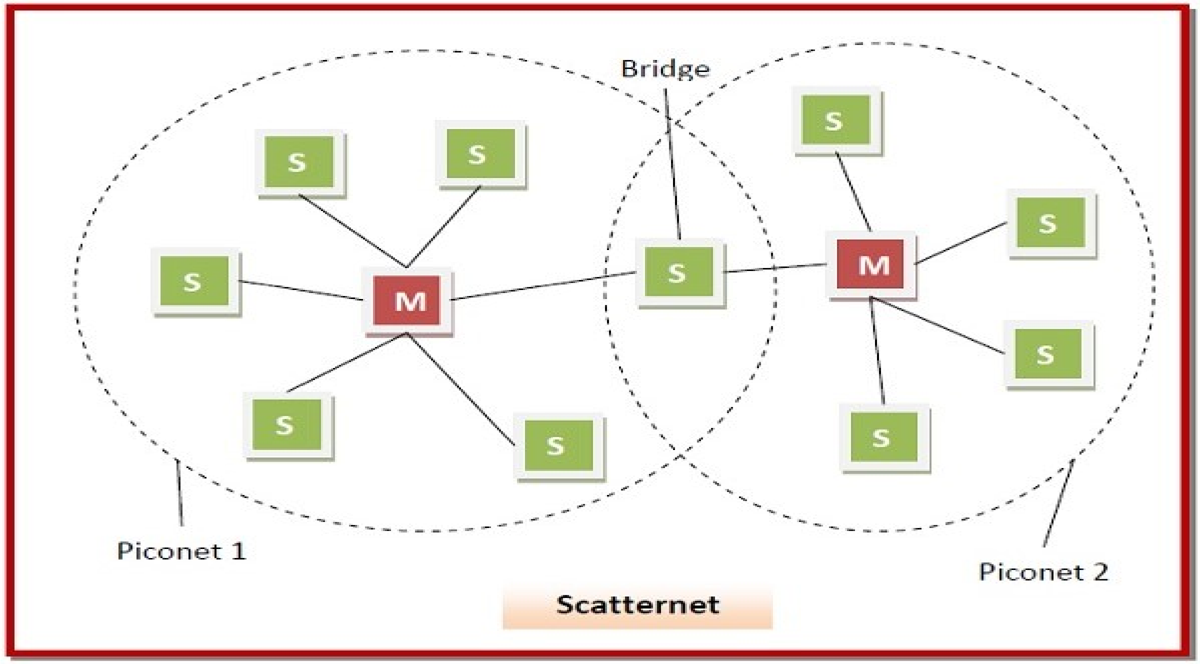
Piconets

Piconets are small Bluetooth networks, formed by at most 8 stations, one of which is the master node and the rest slave nodes (maximum of 7 slaves). Master node is the primary station that manages the small network. The slave stations are secondary stations that are synchronized with the primary station.

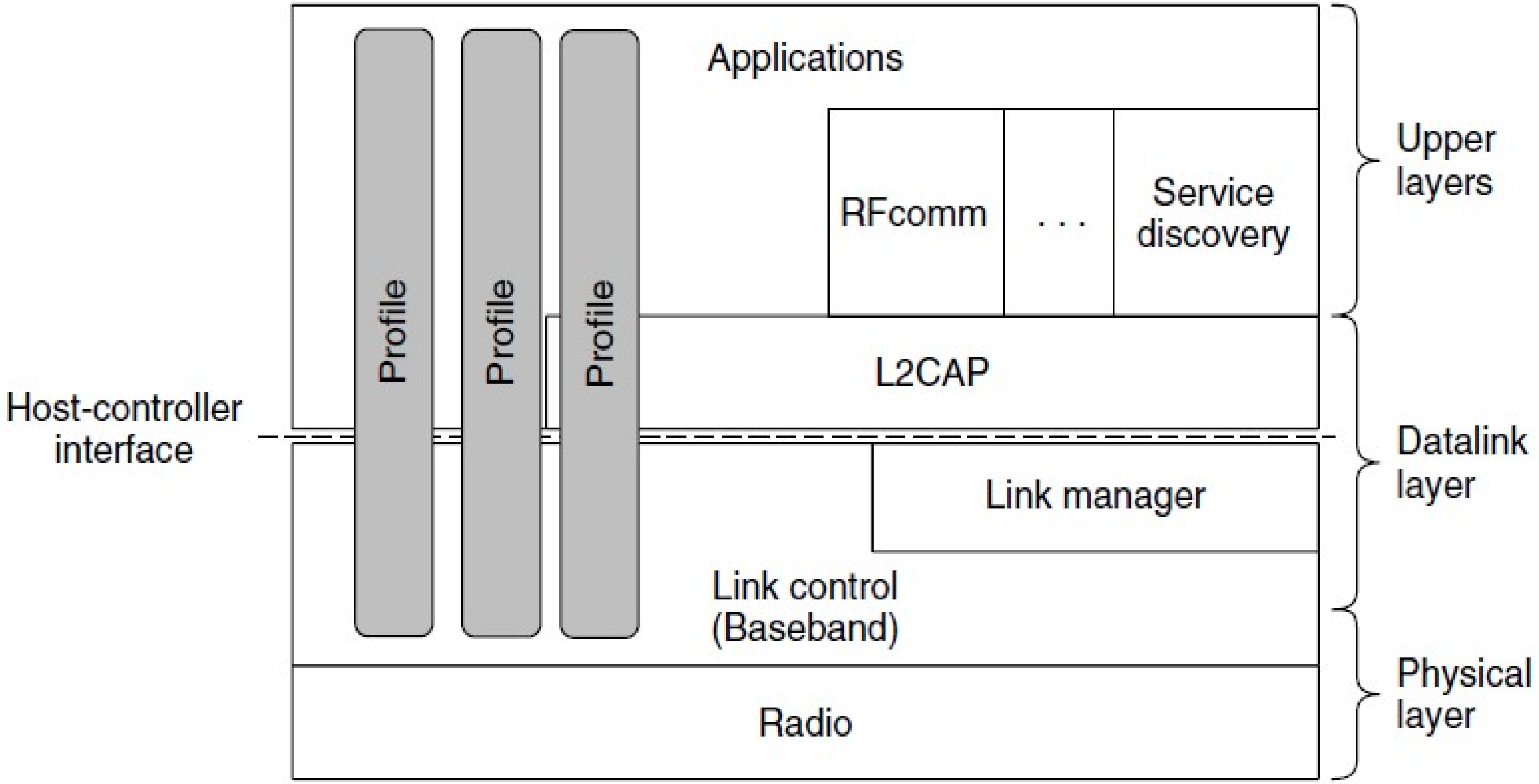
Communication can take place between a master node and a slave node in either one-to-one or one-to-many manner. However, no direct communication takes place between slaves. Each station, whether master or slave, is associated with a 48-bit fixed device address.

Scatternets

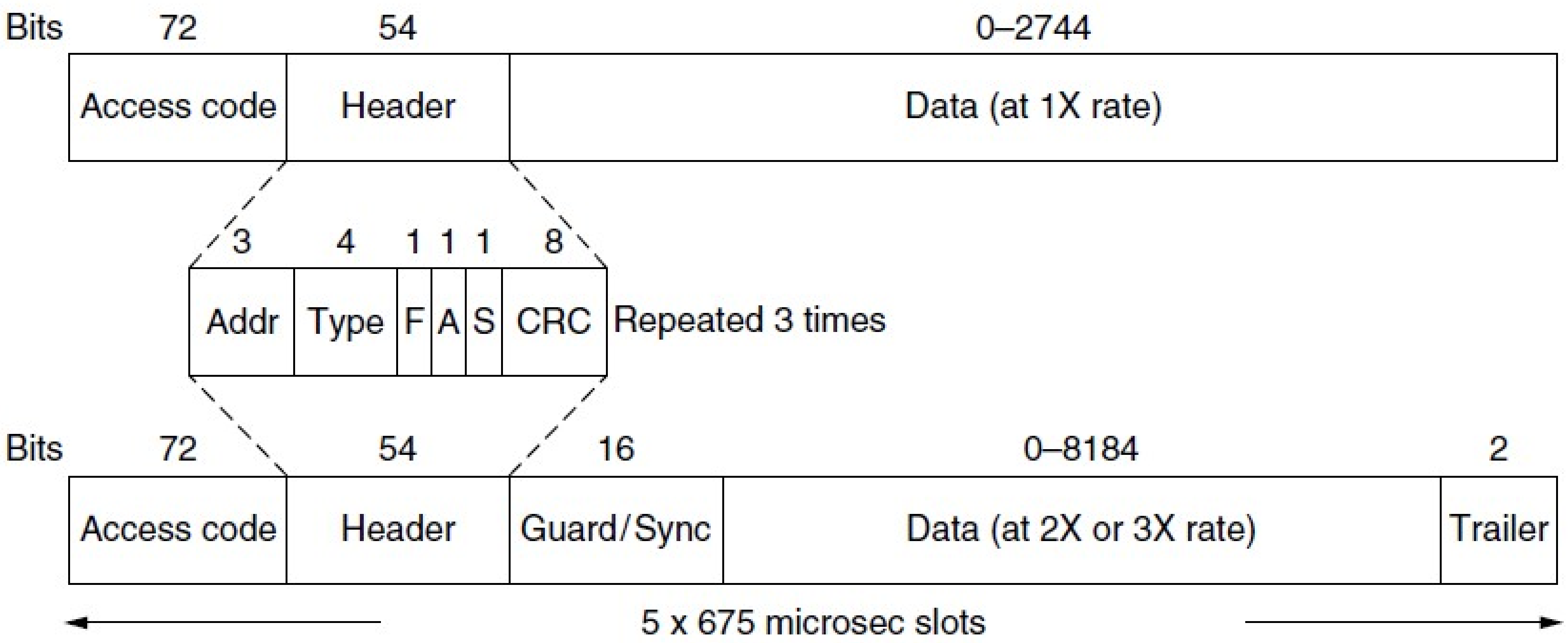
A scatternet is an interconnected collection of two or more piconets. Th are formed when a node in a piconet, whether a master or a slave, acts a slave in another piconet. This node is called the bridge between the t piconets, which connects the individual piconets to form the scatternet.



Bluetooth Protocol Stack



Bluetooth Frame Structure



Bits	72	54	0–2744
	Access code	Header	Data (at 1X rate)

3	4	1	1	1	8	
Addr	Type	F	A	S	CRC	Repeated 3 times

Bits	72	54	16	0–8184	2
	Access code	Header	Guard/Sync	Data (at 2X or 3X rate)	Trailer

5 x 675 microsec slots

(a) Basic rate data frame, top (b) Enhanced rate data frame, bottom