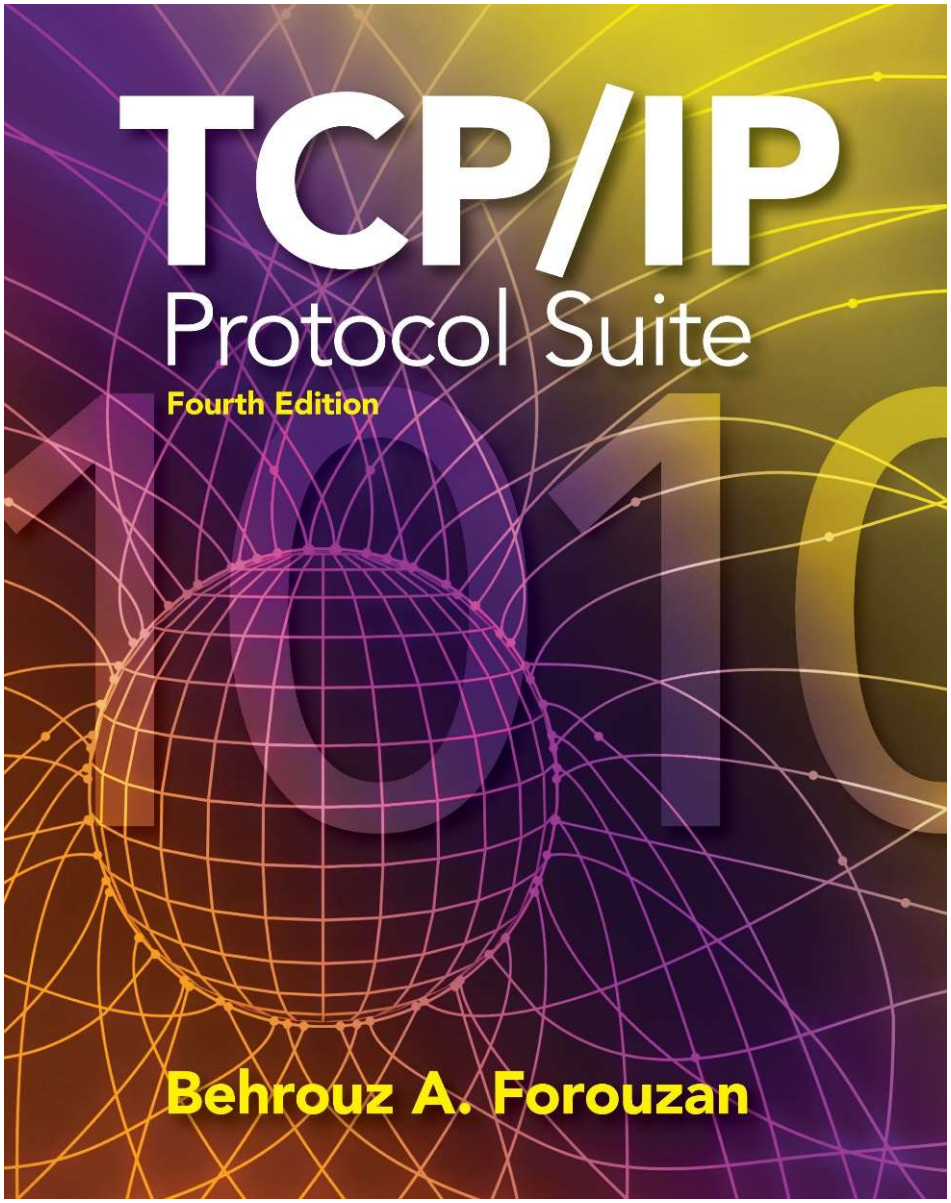
Chapter 3

Underlying Technology

Wired LANs



IEEE LAN STANDARDS

WIRED LOCAL AREA NETWORKS

A local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus.

LANs today are also linked to a wide area network (WAN) or the Internet.

The LAN market has seen several technologies such as Ethernet(802.3), token ring (802.5), token bus(802.4), FDDI, and ATM LAN, but Ethernet(802.3) is by far the dominant technology.

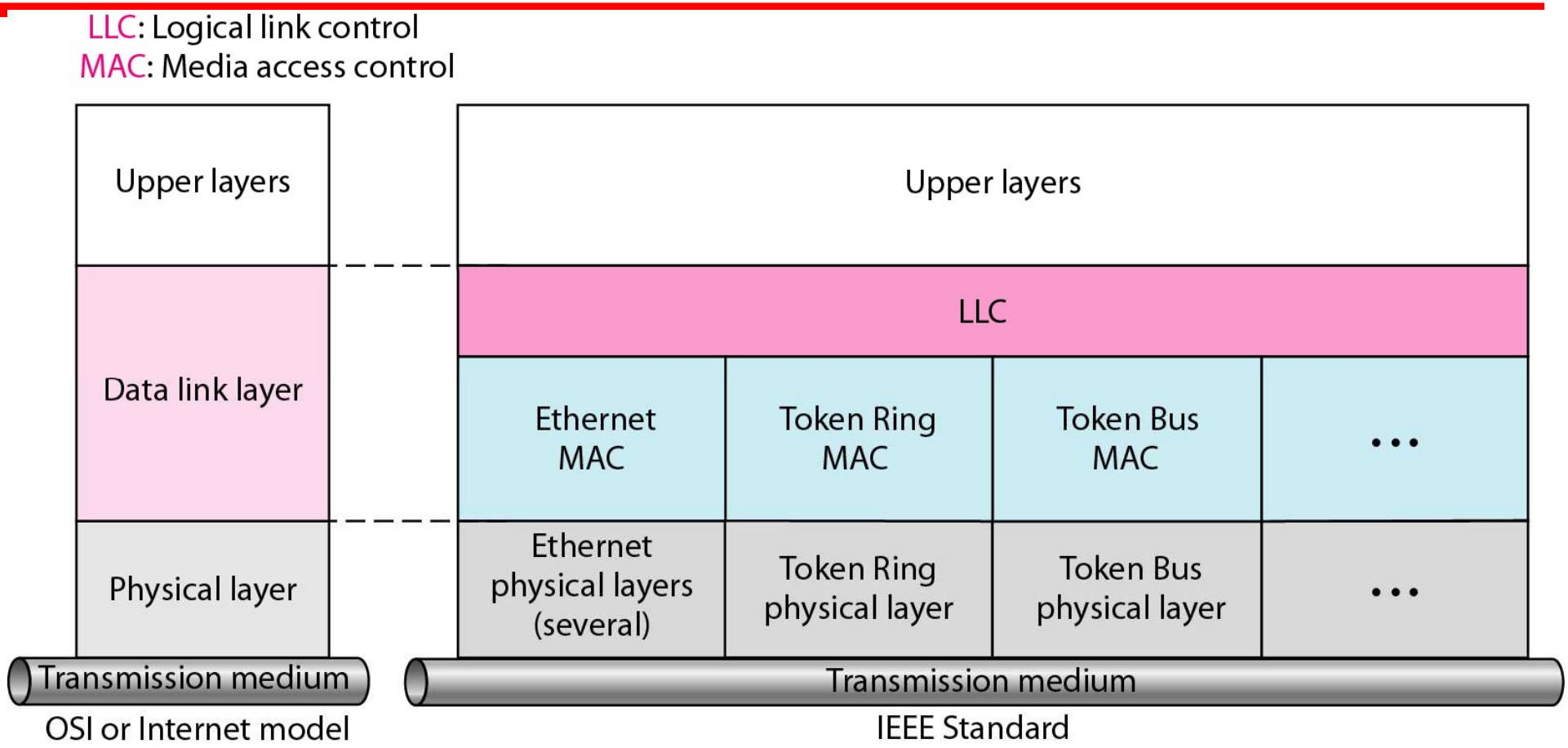
IEEE STANDARDS

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

Topics discussed in this section(Underlying Technology):

Data Link Layer- LLC, MAC
Physical Layer

IEEE standard for LANs



LLC is responsible for handling multiple Layer3 protocols (multiplexing/de-multiplexing) and link services like reliability and flow control.

MAC is responsible for framing and media access control for broadcast media.

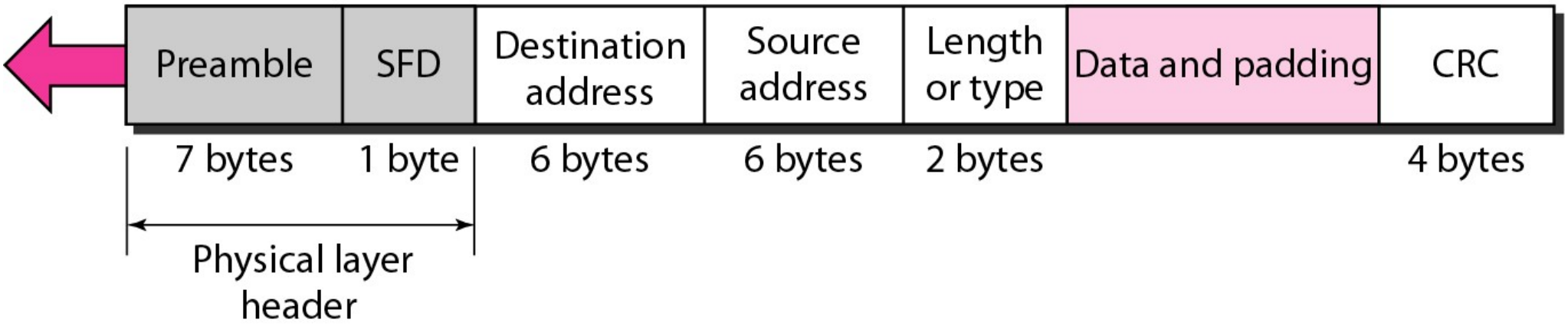
STANDARD ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations. We briefly discuss the Standard (or traditional) Ethernet in this section.

802.3 MAC frame

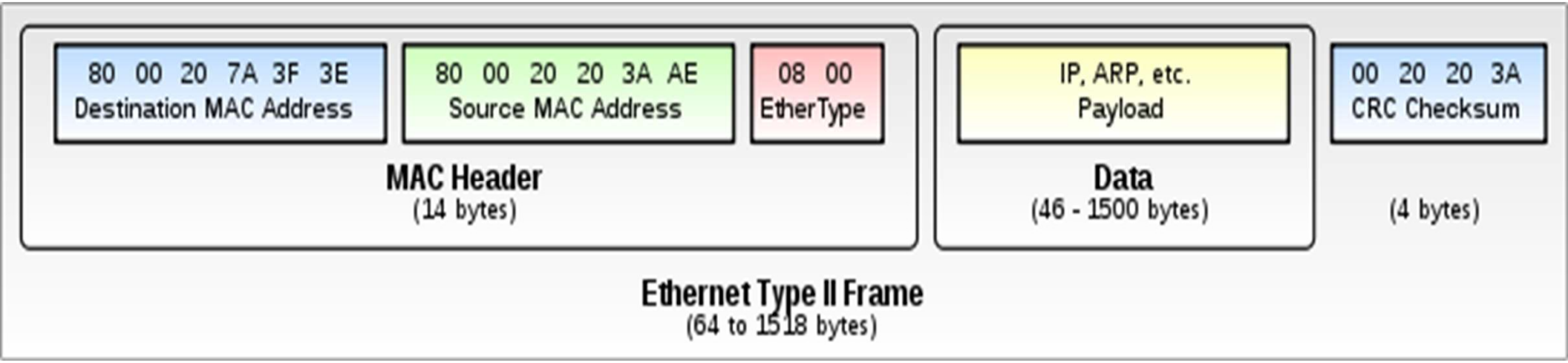
Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)

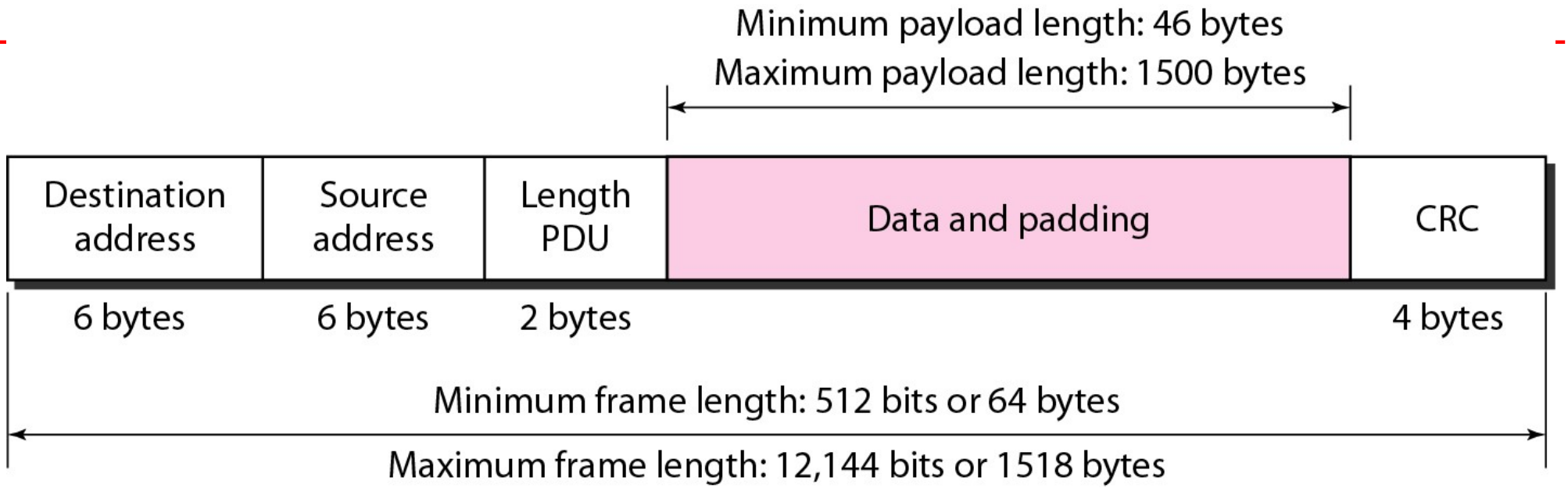


- **Preamble (7 bytes)**: used to synchronize receiver, sender clock rates.
- **SFD (1 byte): Start Frame Delimiter, flag (10101011):** Signals the beginning of the frame. Last two bits **11** alert the receiver that the next field is the destination address.
- **Destination and source address**: MAC address of source and destination.
- **Type/Length (2 Bytes):** Length: Up to 1500 (max length) Type: Identify higher-layer data(**0x0800** –IPv4 , **0x0806**-ARP)
- **CRC(Cyclic Redundancy Check 4 Bytes):** checked at receiver, if error is detected, the frame is simply dropped
- **Data:** 46 to 1500 Bytes (if shorter: add pad)Why? (explained after **CSMA/CD**)

Example: IEEE802.3 frame



Minimum and maximum lengths



Min Frame Length

46 byte min Data payload + **18**bytes Header &CRC =**64 bytes**.

Max Frame Length

1500 byte max Data payload + **18**bytes Header &CRC=**1518 bytes**

Note

Frame length:

Minimum: 64 bytes (512 bits)

Maximum: 1518 bytes (12,144 bits)

Problem

- An Ethernet MAC sublayer receives 1510 bytes of data from the upper layer. Can the data be encapsulated in one frame? If not, how many frames need to be sent? What is the size of the data in each frame?

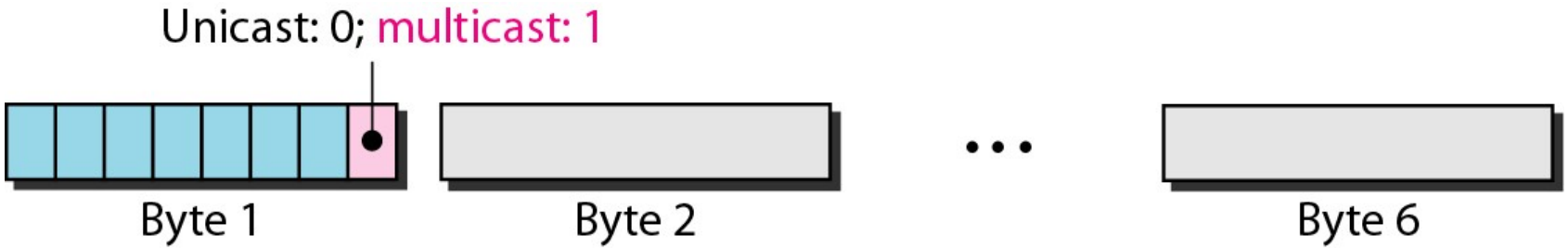
- **Solution**
- The maximum data size in the Standard Ethernet is **1500** bytes. The data of **1510** bytes, therefore, must be split between two frames.
- The standard dictates that the first frame must carry the maximum possible number of bytes (**1500**);

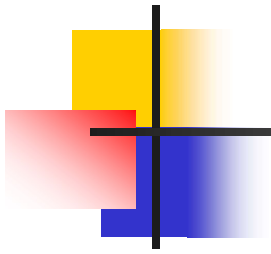
  the second frame then needs to carry only **10** bytes of data (it requires padding). The following shows the breakdown:
- Data size for the first frame: **1500 bytes**
- Data size for the second frame: **46 bytes** (10 Payload+18 header & CRC +with 18 padding)

Example of an Ethernet address in hexadecimal notation

- **48** bits (6 bytes) in length
- Uniquely assigned to each Ethernet network interface card (NIC)
- Usually written in hexadecimal notation

Unicast and multicast addresses





Note

The least significant bit of the first byte

defines the type of address.

If the bit is 0, the address is unicast;

otherwise, it is multicast.

A multicast address can be a destination address, but not a source address

Note

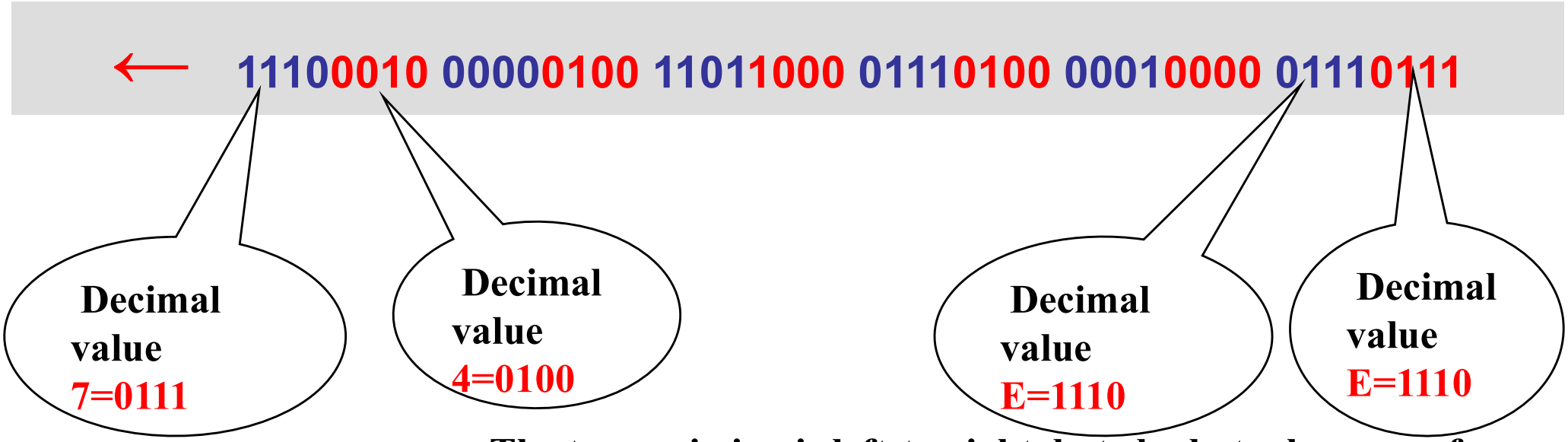
The broadcast destination address is a special case of the multicast address in which all bits are 1s.

Example 3.2

Show how the address 47:20:1B:2E:08:EE is sent out on line.

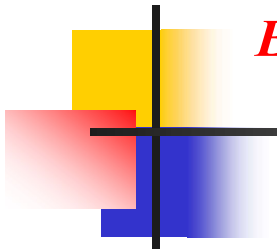
Solution

The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-left, bit by bit, as shown below:



47 is 0100 0111
The right-to-left order is 1110 0010 – LSB is 1 Multicast

The transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last. This means that the bit that defines an address as unicast or multicast arrives first at the receiver.



Example

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A b. 47:20:1B:2E:08:EE

c. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010.

b. This is a multicast address because 7 in binary is 0111.

c. This is a broadcast address because all digits are F's.

Meaning of some Terms

- **Propagation Delay(T_p):** Amount of time it takes for the first bit of signal to travel from the sender to the receiver.
  - **T_P = d/c** where **d** is the distance between the sender and the receiver and **c** is the speed of light (3 * 10^8 m/s).

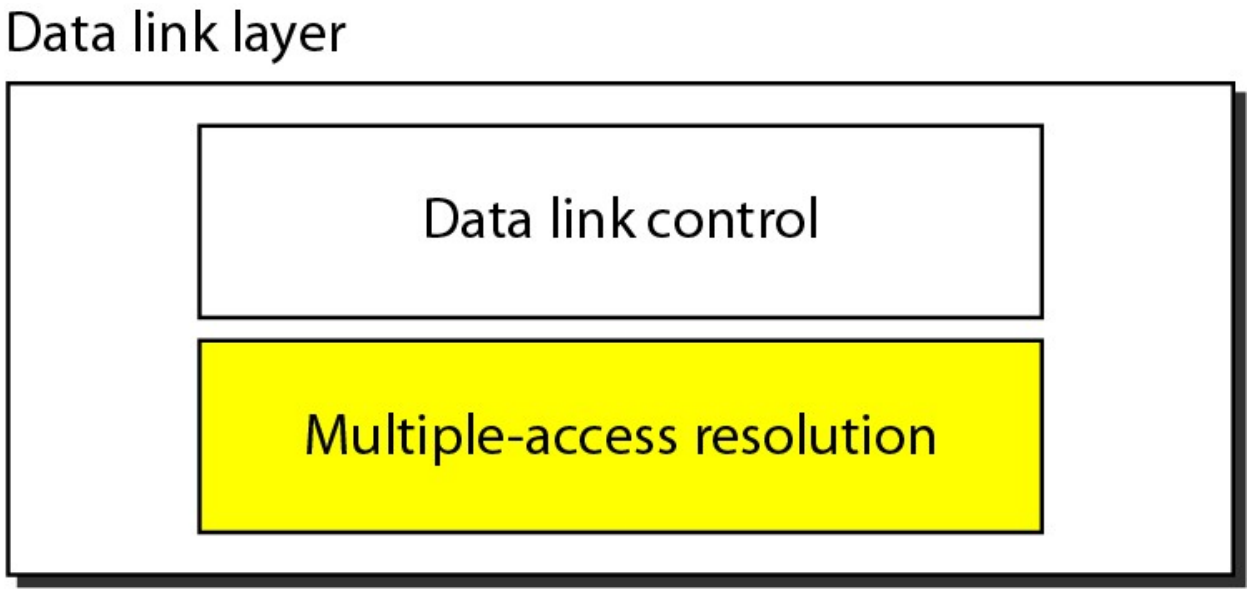
- **Transmission Delay(T_d):** It is the amount of time required to push all of the packet's bits into the wire. In other words, this is the delay caused by the data-rate of the link.

  - Transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits. It is given by the following formula:
  - **T_d = N/R** where *N* is the number of bits, and ***R*** is the rate of transmission (say in bits per second)

Solution

- The stations on a wireless network are a maximum of 300 km apart. If the network transmits 400-bit frames on a shared channel of 200 kbps. Find the propagation and Transmission Delay
- **Solution**
- Propagation Delay : = $\mathbf{T_P = d/c}$
  - =300 X 1000 / 3 X 10^8 =0.001 sec= 1ms
- Transmission delay = $\mathbf{T_d = N/R}$
  - 400/(200 X 10^3) = =0.002 sec=2ms

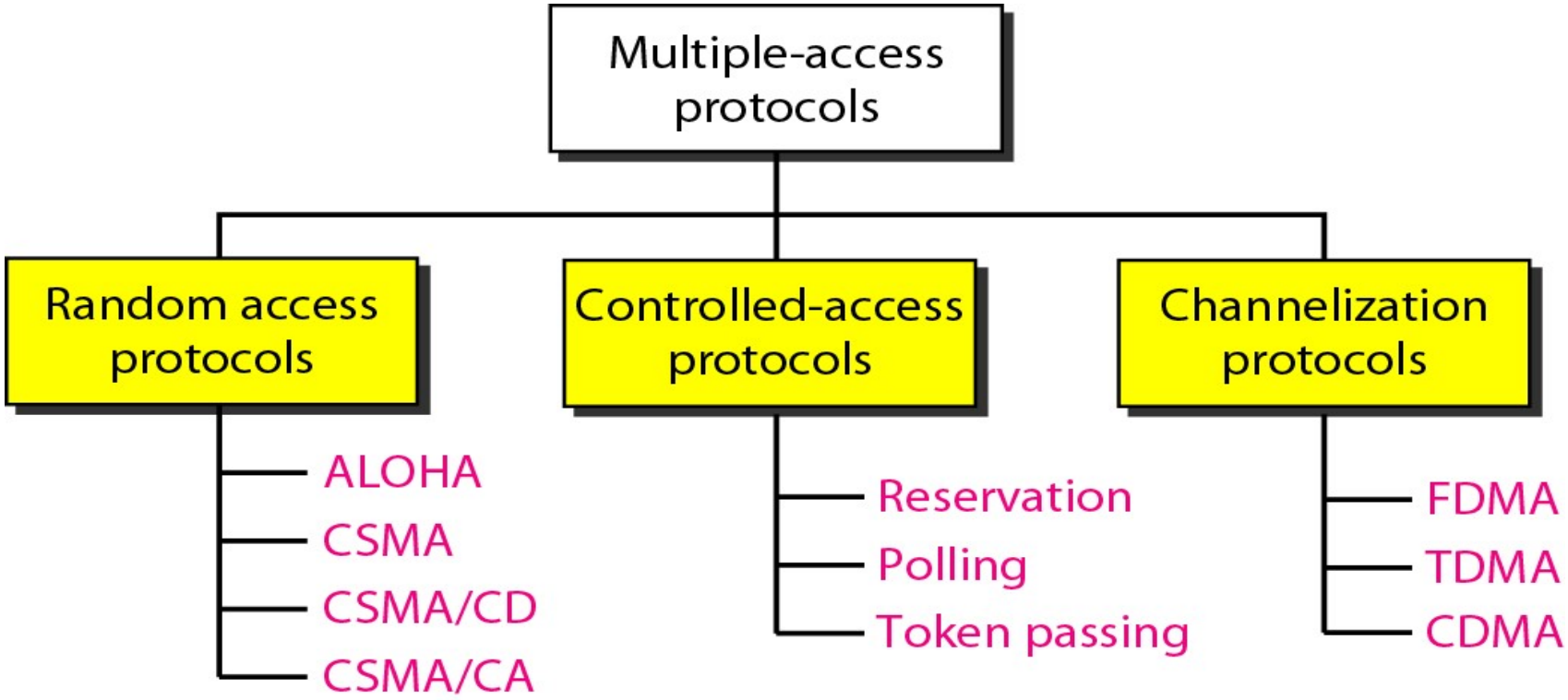
Data link layer divided into two functionality-oriented sublayers



The upper sublayer that is responsible for flow and error control is called the logical link control (LLC) layer;

The lower sublayer that is mostly responsible for Media Access Control

Taxonomy of multiple-access protocols discussed in this chapter



RANDOM ACCESS

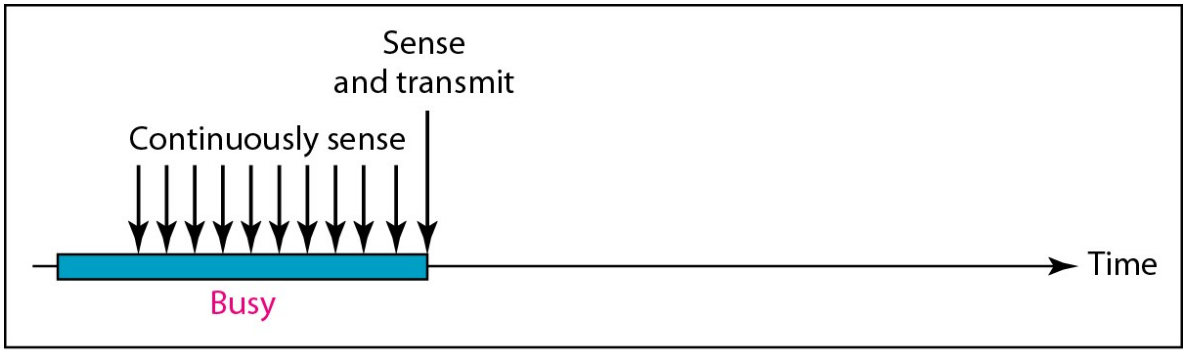
- **In random access or contention methods, no station is superior to another station and none is assigned the control over another.**
- **No station permits, or does not permit another station to send.**
- **At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.**

Two features give this method its name.

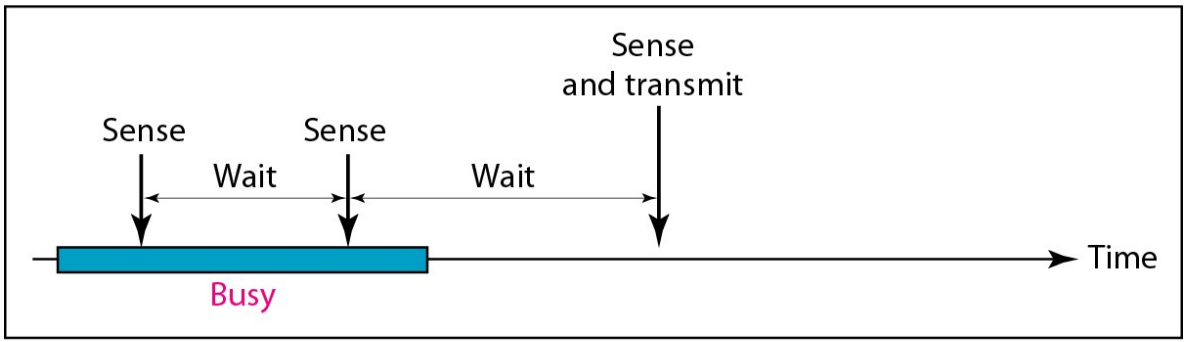
- First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called ***random access***.
- Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called ***contention*** methods.
- In a random access method, each station has the right to the medium without being controlled by any other station. However, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified

- **To avoid access conflict** or to resolve it when it happens, each station follows a procedure that answers the following questions:
  - **When** can the station **access** the medium?
  - **What** can the station **do if** the medium is **busy**?
  - How can the station determine the **success or failure of the transmission**?
  - **What** can the station **do** if there is an **access conflict**?

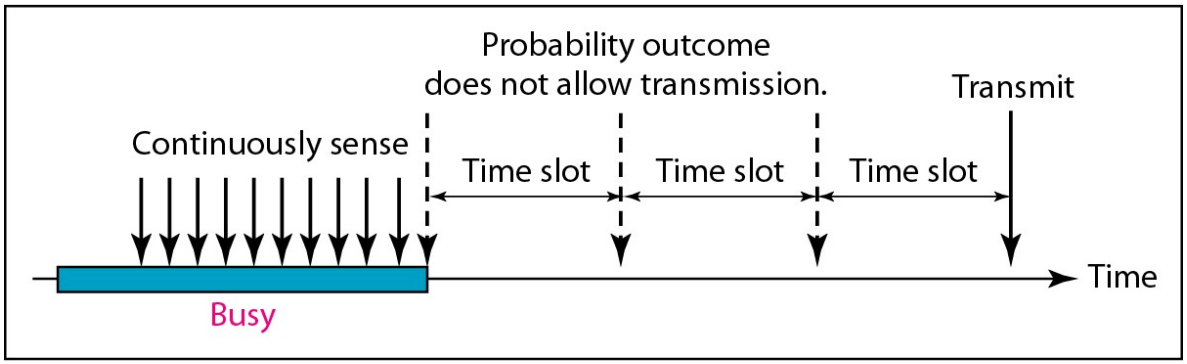
Behavior of three persistence methods



a. 1-persistent



b. Nonpersistent



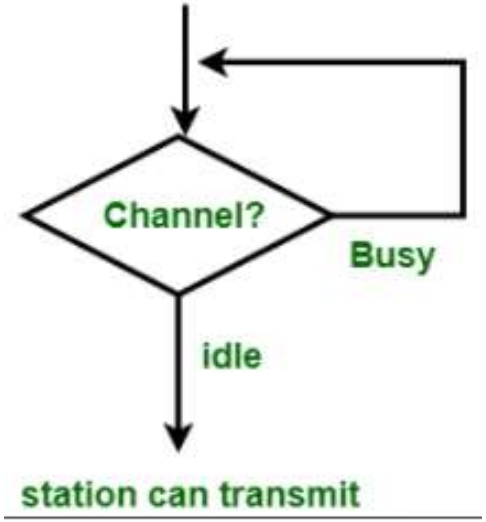
c. p-persistent

Persistent Methods –tells what to if media sensed is busy or if idle?

1-persistent CSMA

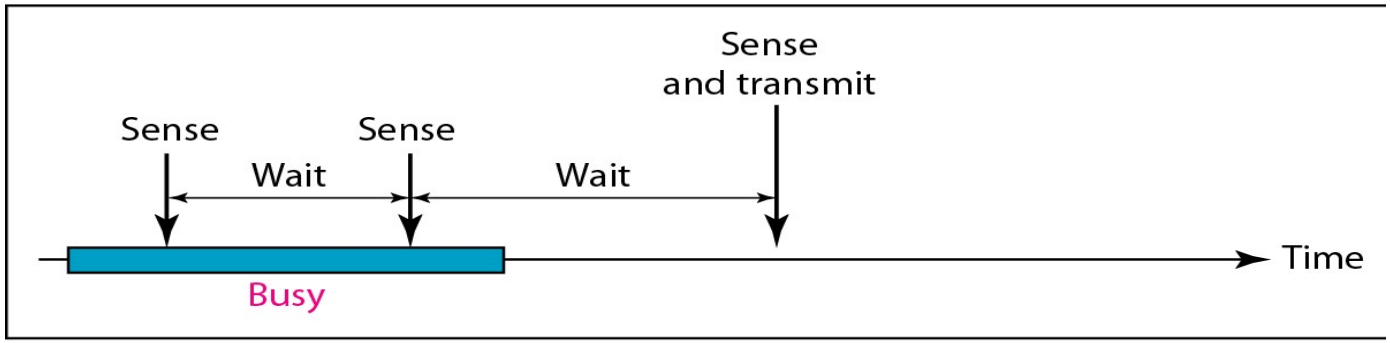
- 1-persistent CSMA (Carrier Sense Multiple Access): To send data, a station first listens to the channel to see if anyone else is transmitting.
- If so, the station waits (keeps sensing it) until the channel becomes idle. Otherwise, it transmits a frame.
- If a collision occurs, the station waits a random amount of time and starts all over again.

a. 1-persistent

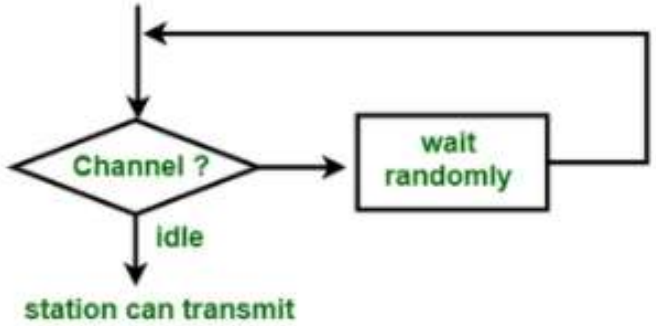


Non-persistent CSMA

- To send data, a station first listens to the channel to see if anyone else is transmitting.
- If so, the station waits a random period of time (instead of keeping sensing until the end of the transmission) and repeats the algorithm. Otherwise, it transmits a frame.
- If a collision occurs, the station waits a random amount of time and starts all over again.



b. Nonpersistent



P-Persistent CSMA

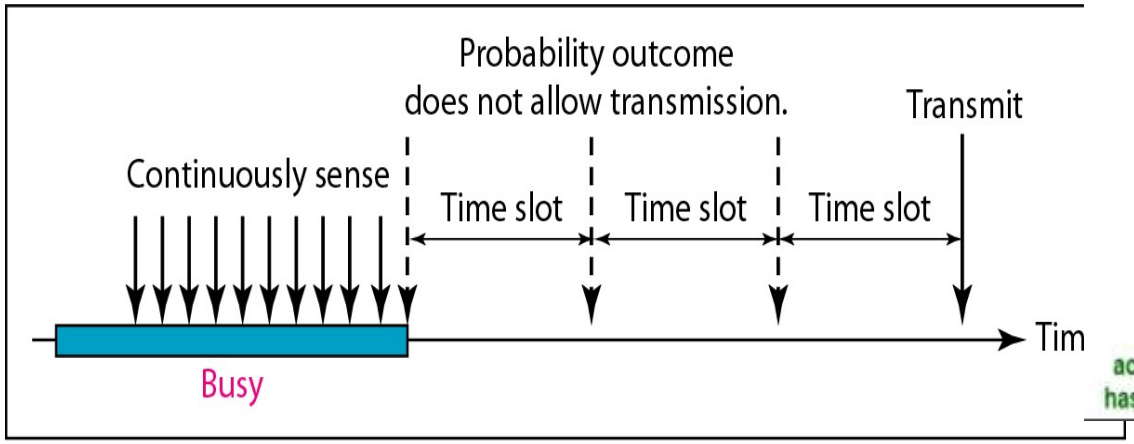
- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- In this method, after the station finds the line idle it follows these steps:

1. With probability *p,* the station sends its frame.

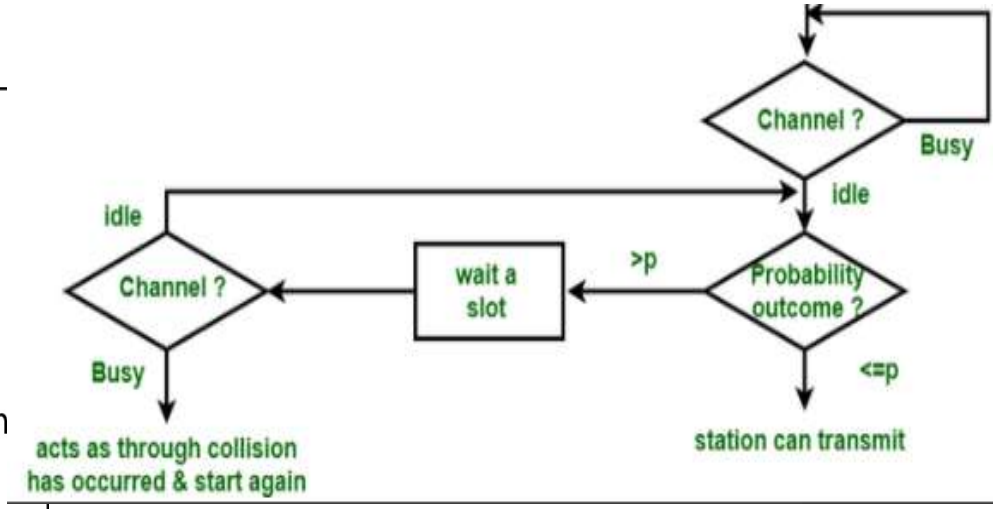
2. With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.

   a. If the line is idle, it goes to step 1.

   b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.



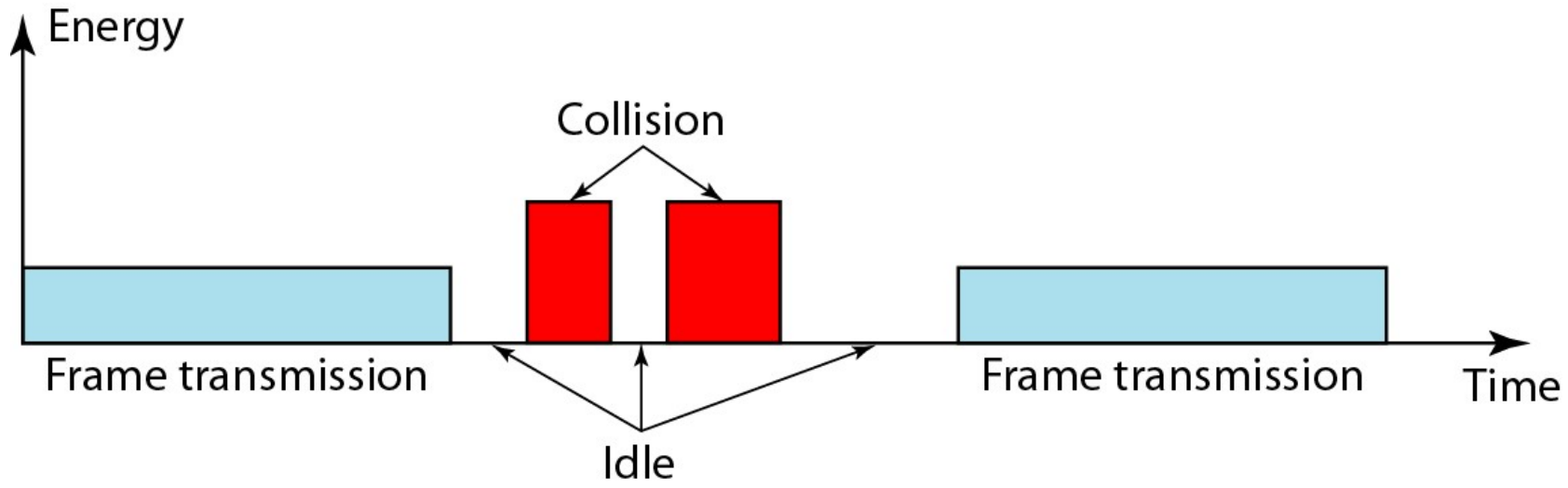
c. p-persistent



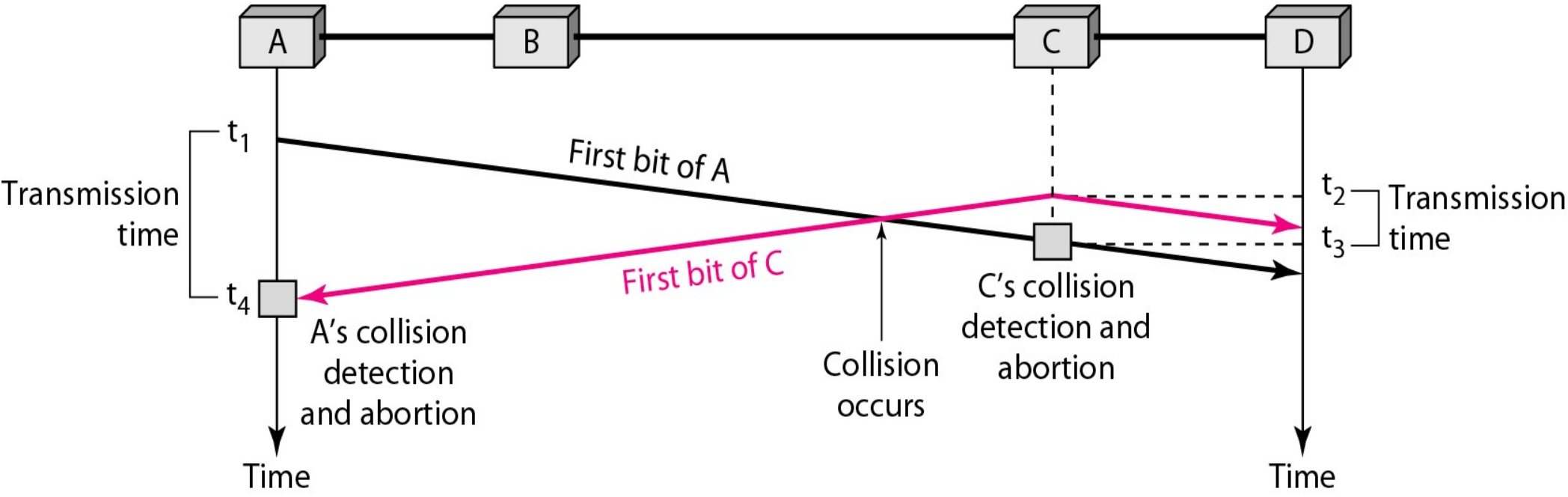
CSMA/CD

- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If a collision is detected the station aborts the transmission.
- No Acknowledgment

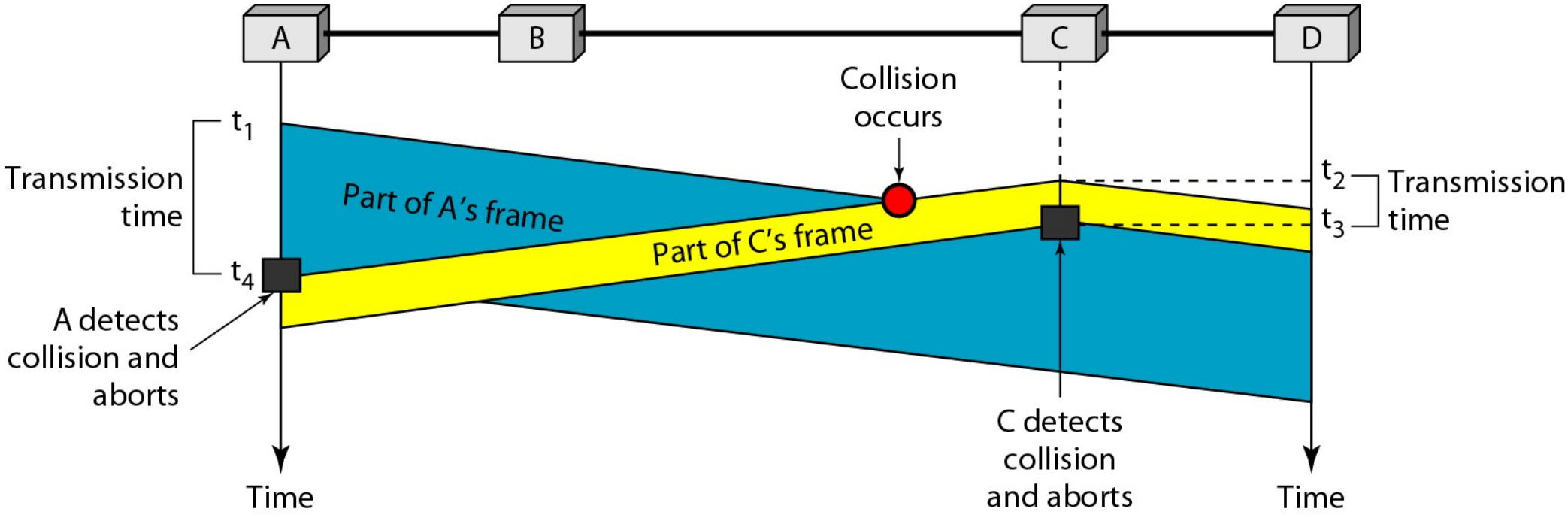
Energy level during transmission, idleness, or collision



Collision of the first bit in CSMA/CD

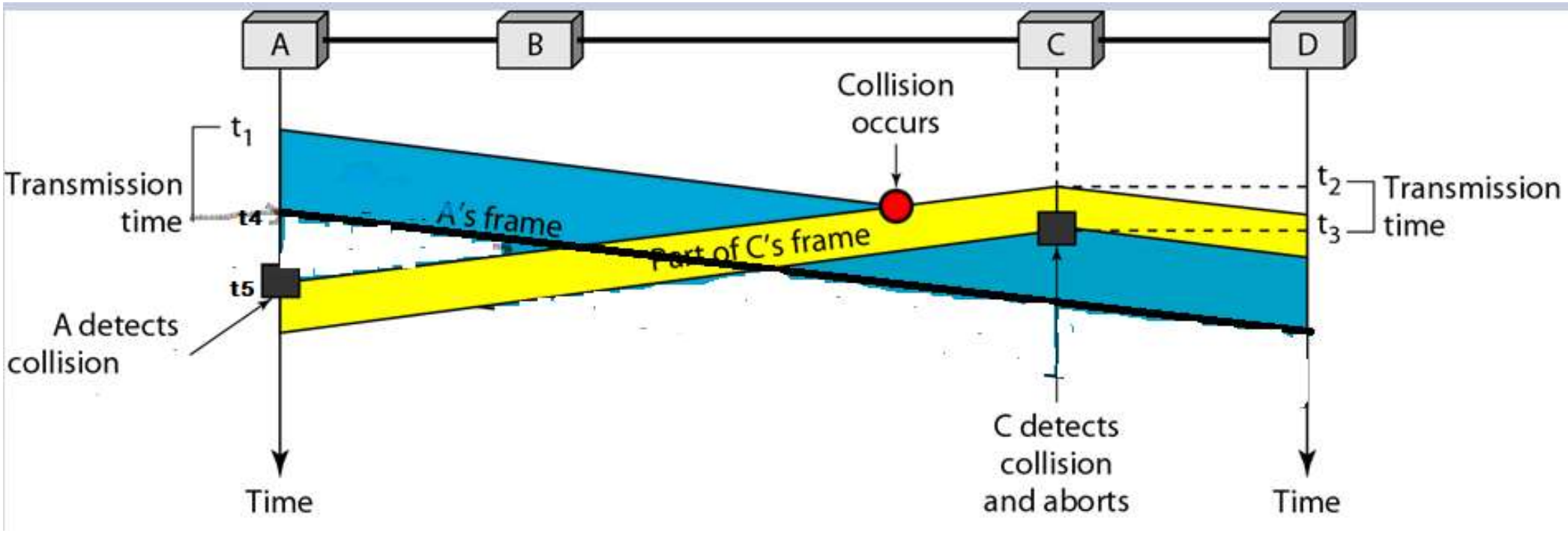


Collision and abortion in CSMA/CD



(t_4-t_1)*data rate –amount of data transmitted by A before detecting collision.

What if Frame size is smaller?



Station 'A' never understands that- collision happened with it's own Signal

Minimum Frame Size

- For ***CSMA/CD*** to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
- This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the link for collision detection.
- In the worst-case scenario, If the two stations involved in a collision are the **maximum distance apart**, the signal from the first takes time T_p to reach the second, and the effect of the collision takes another time T_p to reach the first
- Therefore, the frame transmission delay T_{fr}**(also called as** T_d **in** slide 19)must be at least two times the maximum propagation time T_p

$T_{fr} >= 2 * T_p$

Sender must have enough bits so that Transmission delay (T_d or T_{fr} Time for transmitting all bits of frame)

$$T_{fr} >= 2 * T_p \quad \text{and} \quad T_d = N/R$$

N- length of frame in bits

R- Data rate

$$N/R >= 2 * T_p$$

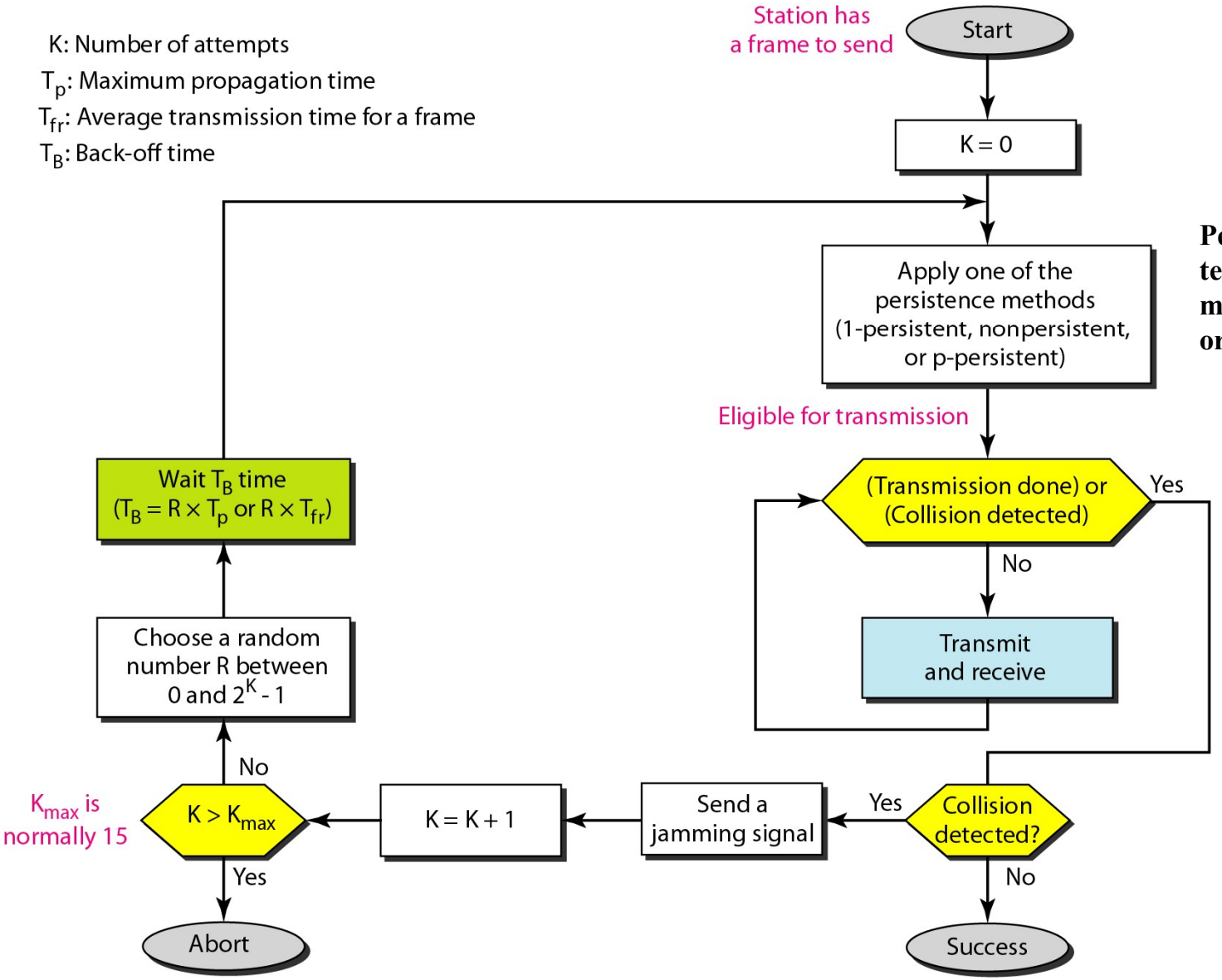
$$N >= 2 * T_p * R$$

$$\text{Frame Size} >= (2 * T_p) * R$$

$$\text{Frame Size} >= (2 * d/c) * R$$

because $T_p = d/c$

Flow diagram for the CSMA/CD



Persistent Methods – tells what to do if media sensed is busy or if idle?

Example

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

Solution

The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet.

Problem

- In a *CSMA/CD* network with a data rate of 10 Mbps, the minimum frame size is found to be 512 bits for the correct operation of the collision detection process.

What should be the minimum frame size if we increase the data rate to **100 Mbps**? To **1 Gbps**? To **10 Gbps**?

Solution

- Let us find the relationship between the minimum frame size and the data rate. We know that-

Frame Size >= (2 * Tp)* R

Frame Size >= (2 * d/c)* R

or

(frame size) = **[2 × (distance) / (propagation speed)]** × (data rate)]

or

frame size = K × (data rate)

This means that minimum frame size is proportional to the data rate (K is a constant).

- When the data rate is increased, the frame size must be increased in a network with a fixed length to continue the proper operation of the CSMA/CD.
- We calculate the minimum frame size based on the above proportionality relationship
- Data rate = 10 Mbps → minimum frame size = **512 bits**
- Data rate = 100 Mbps → minimum frame size = **5120 bits**
- Data rate = 1 Gbps → minimum frame size = **51,200 bits**
- Data rate = 10 Gbps → minimum frame size = **512,000 bits**

Fast Ethernet

- Fast Ethernet operates at 100Mbps. For the most part, the scheme/protocol remains the same as the 10Mbps case, except now the maximum length of the network is shortened.

- Minimum frame size is still kept at 64 bytes (for backward compatibility), which now arrive 10 times faster than they do in 10Mbps Ethernet.

- Hence the maximum length of the network must be 10 times smaller or about around 250 meters.

IEEE 802.3 (Ethernet) Cabling

Name	Cable	MAX Segment	Nodes/seg.
10Base5	Thick coaxial	500 meters	100
10Base2	Thin coaxial	200 meters	30
10Base-T	Twisted pair	100 meters	1024

- **10Base5 cabling:** This type of cabling is popularly referred to as **thicknet**. It was one of the earliest types of cables used for LAN's. The notation 10Base5 suggests that the LAN operates at 10 Mbps, uses baseband signaling and can support segments of up to 500 meters.

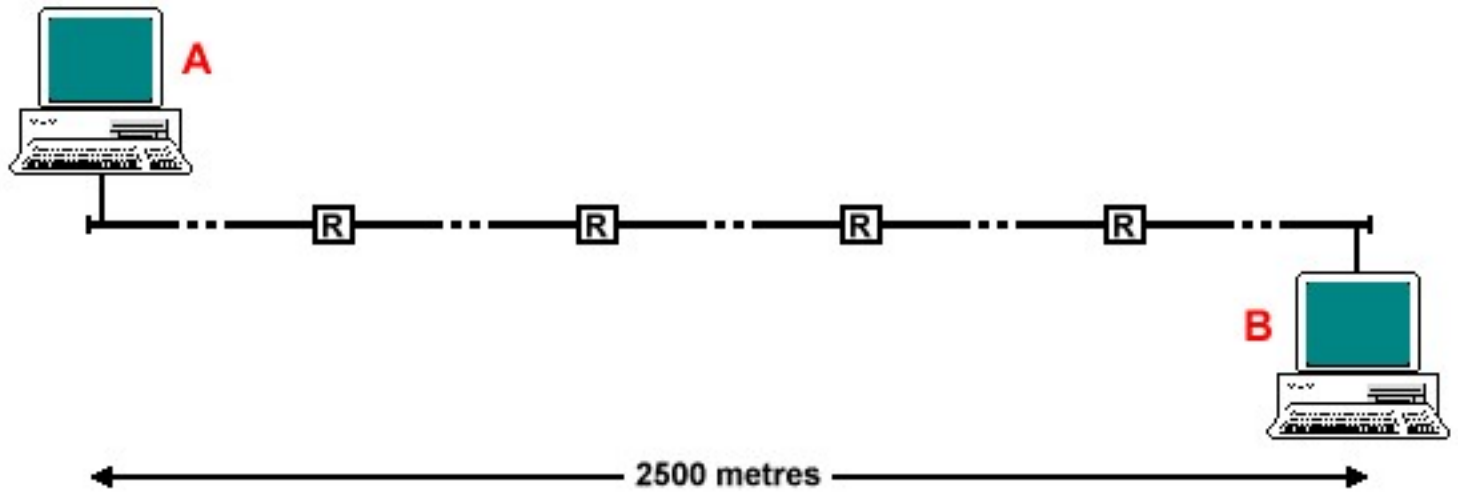
- **10Base2 cabling:** 10Base2 or **thinnet,** which in contrast to thicknet, bends easily. 10Base2 cables are easier to install and are relatively inexpensive. The only drawback of using the 10Base2 cable is that it can run for only 200 meters and can handle only 30 stations per cable segment.

- **10Base-T cabling**: there is no single, main cable because each station has a cable running to a central **hub** (a big repeater). Adding or removing stations is simpler in this configuration and cable breaks can be detected easily. The disadvantage of 10Base-T is that the maximum cable run from the hub is only 100 meters, sometimes 150 meters (if high quality twisted pairs are used). 10Base-T is most popular due to the ease of maintenance.

IEEE 802.3 (Ethernet)

- IEEE 802.3 has a certain maximum cable length/segment. To allow larger networks, multiple cables are connected by repeaters which amplifies and retransmits signals in both directions.

- Maximum distance between any 2 stations is 2500 m (with 5 segments each of 500 m) and no more than 4 repeaters can separate any 2 stations.



Why must the IEEE 802.3 (Ethernet) frame be at least 64 bytes long?

Calculations:

- Data rate =10Mbps
- LAN Length (L) = 500 m (per segment) x 5 segments = 2500 meters
- Velocity of propagation on the cable (V) = $2 * 10^8$ meters/sec
- Delay added by repeater (D) = ~3**µ**Sec x 2 (Bi-Direction) x 4 Repeaters = **24µSec**
- **Round Trip Delay (RTD) i.e. $2*T_P$**= (Total Distance/V) + Repeater Delays (D)

  Total Distance/V = $(2*2500/2 * 10^8) = 25 * 10^{-6}$ sec or **25µsec**

  Hence RTD i.e. **$2*T_p = 25 + 24 = 49$ µsec**
- Frame length(Num of bits) required to transmit for 49 **µsec**
- Frame Length= $49*10^{-6}$ sec* $10*10^6$ bits =490 bits nearest power of 2 is 512bits
- Hence the minimum frame size for the IEEE 802.3 (Ethernet) is 512 bits or **64 bytes.**

The maximum length (1518 bytes) restriction has two historical reasons:

- First, memory was very expensive when Ethernet was designed: A maximum length restriction helped to reduce the size of the buffer.

- Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Connecting Devices

Introduction

There are several ways of interconnecting Networks

When two or more networks are interconnected at the **physical layer** the type of device is called as a **repeater**.

When two or more devices are interconnected at the **MAC layer or data link layer**, the type of the device is called as a **bridge**

When two or more devices are interconnected at the **network layer**, the type of the device is called as a **router**

The device that interconnects at **higher level** is called as **gateway**, which generally performs some protocol conversion and security functions.

Repeaters

If Range extension is the problem – use repeaters.

A **repeater** is a device that operates only in the physical layer.

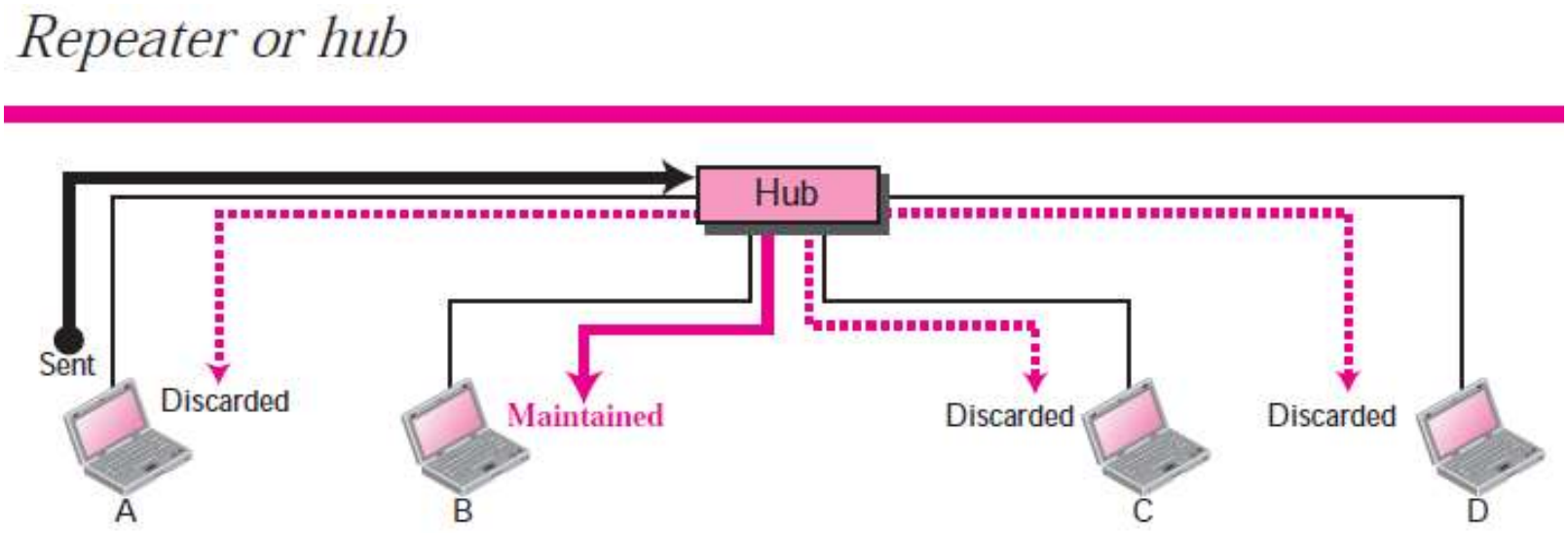
Signals that carry information within a network can travel a fixed distance after that distance signal fade outs(loose the integrity of data carried)

A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern and retransmits the refreshed signal.

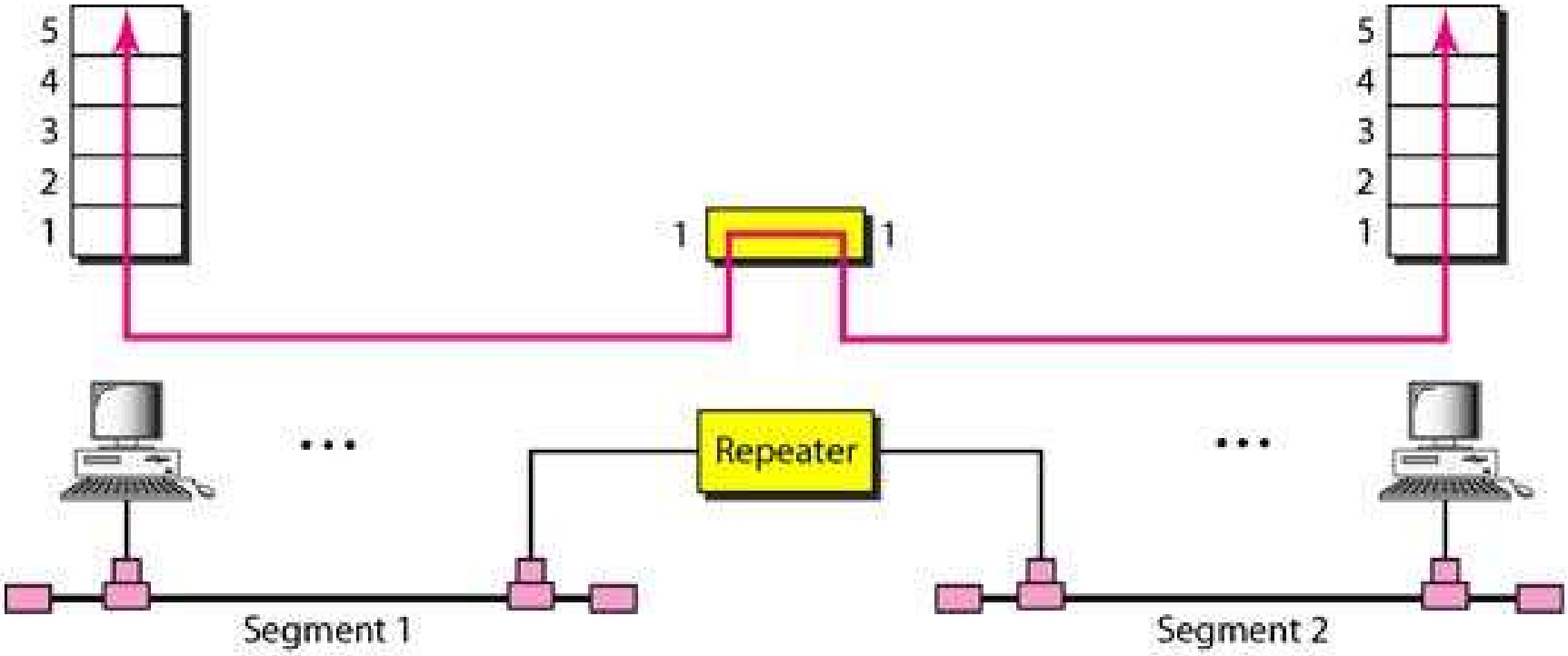
Ethernet LANs were using bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable.

In a star topology, a repeater is a multiport device, often called a **hub**, that can be used to serve as the connecting point and at the same time function as a repeater.

Repeater forwards every bit; it has no filtering capability.



A hub or a repeater is a physical-layer device. They do not have any data-link address and they do not check the data-link address of the received frame.


5
4
3
2
1
1
1
5
4
3
2
1
Repeater
Segment 1
Segment 2

Bridges

Why Bridges ?

There may be requirement in the organization that- they need to interconnect the departmental LANs in order to share the resources.

- Thus Bridges are used for **connecting multiple LANs** as shown in the figure.
- Bridged LAN or Extended LAN

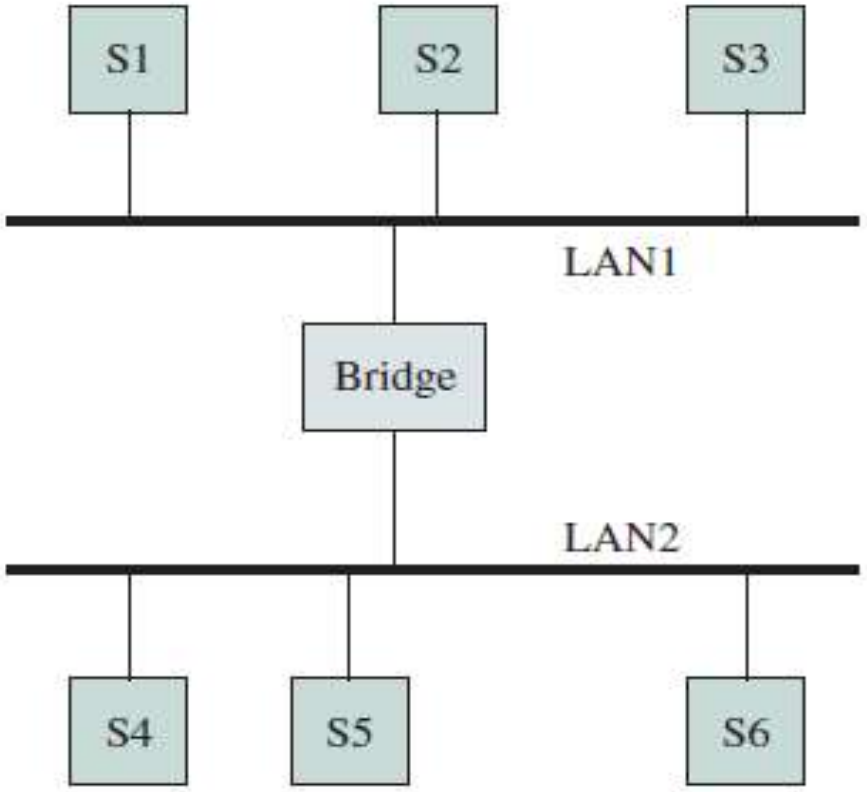


FIGURE 6.79 A bridged LAN

Bridges

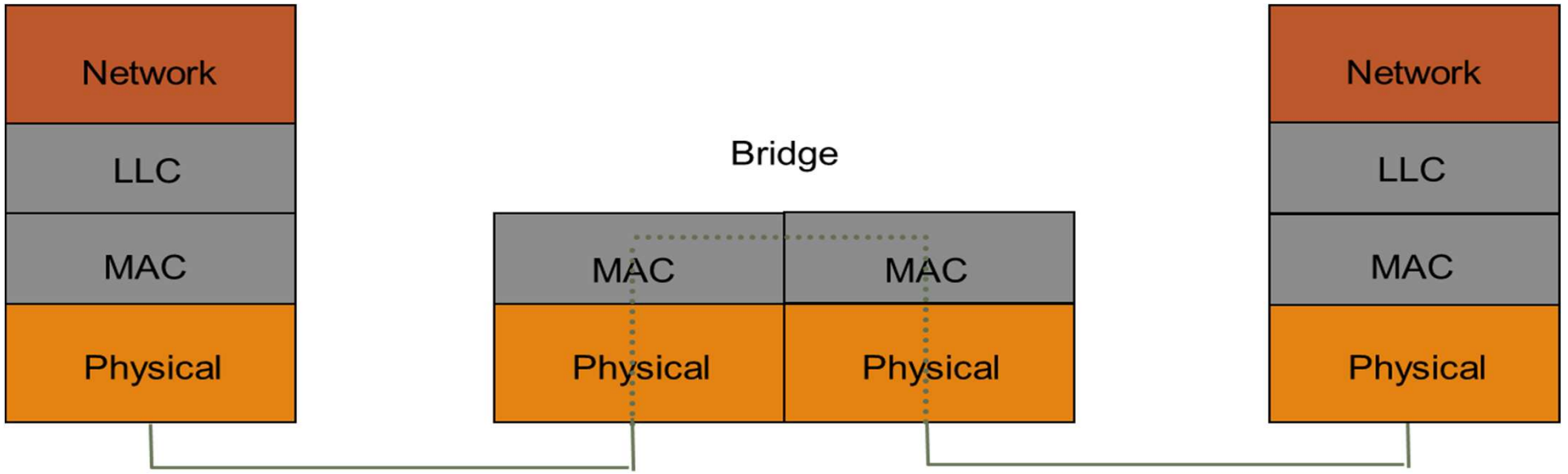
A bridge operates in both the physical and the data link layers.

As a physical-layer device-

it regenerates the signal it receives.

As a data link layer device,-

it can check the MAC addresses (source and destination) contained in the frame.



Types of Bridges

There are two types of bridges which are widely used:

- **Transparent Bridges**: These bridges are widely used in Ethernet LANs
- **Source Routing Bridges**: These bridges are widely used in Token Ring LANs and FDDI networks

Transparent Bridges

- These bridges were defined by the 802.1d committee.
- The term transparent refers to the fact that the **stations are completely unaware of the presence of the bridges** in the network
- Thus introducing a bridge **doesn't require the stations to be configured.**
- Following are the **functions** of the transparent bridges:
  1. **Forward** Frames from one LAN to another
  2. **Learn** which stations are attached to a given LAN
  3. **Avoid Loops** in the topology

Bridge Learning

When frame arrives on one of the ports of the bridge, the bridge has to decide whether it has to forward the frame.

To do so it needs to maintain a table called as the **forwarding table** or forwarding database

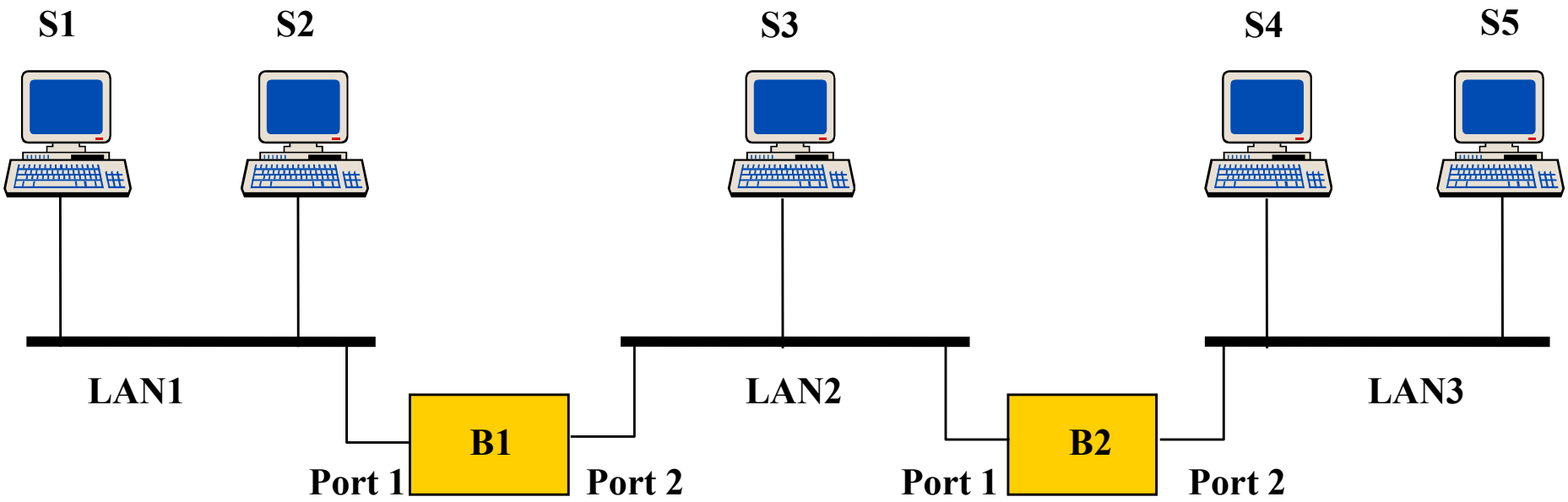
Use table lookup, and

- **discard** frame, if source & destination **in same LAN**
- **forward** frame, if source & destination **in different LAN**
- use **flooding**, if destination unknown

Use **backward learning** to build table

- observe **source address of arriving** LANs
- **handle topology changes** by removing old entries

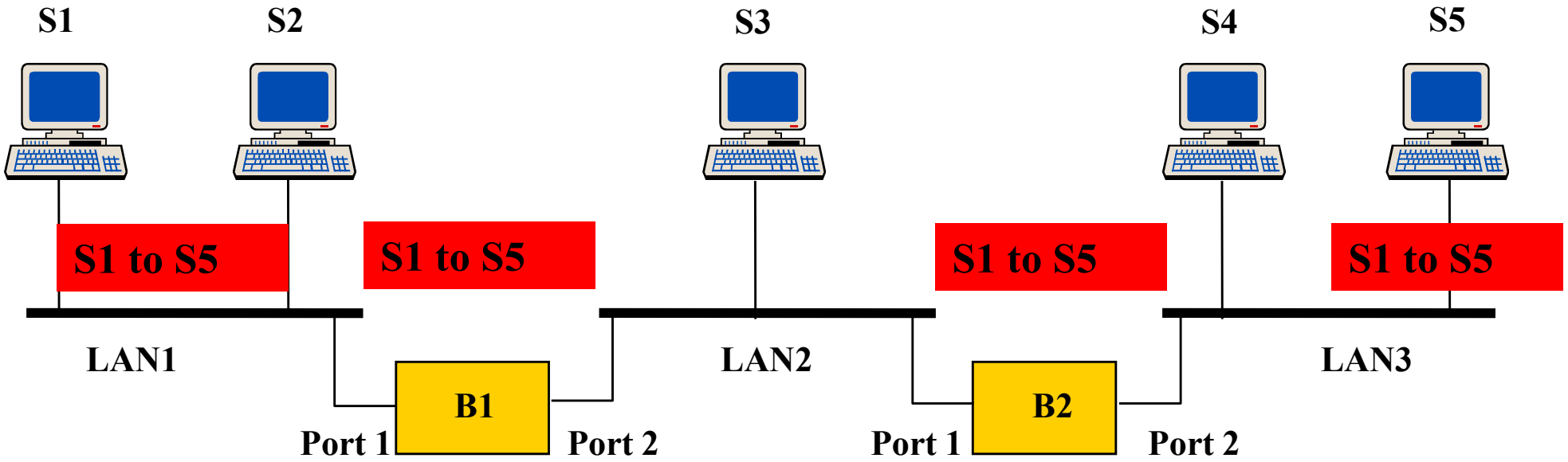
Example: How Table is built ?



Address	Port

Address	Port

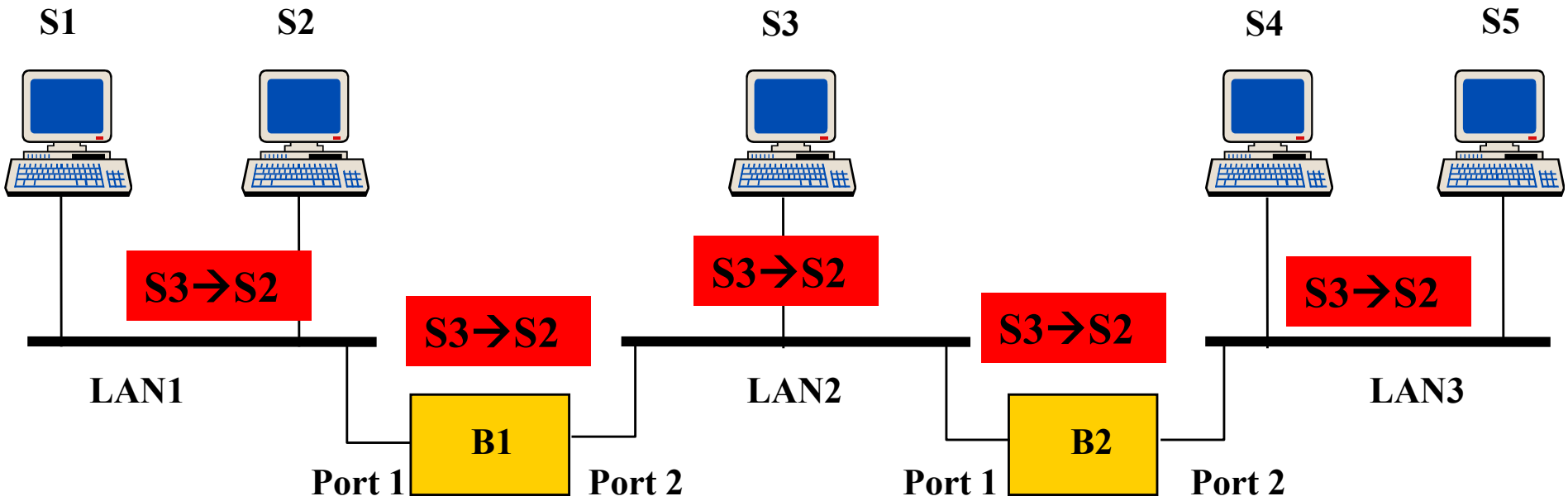
S1→S5



Address	Port
S1	1

Address	Port
S1	1

S3→S2

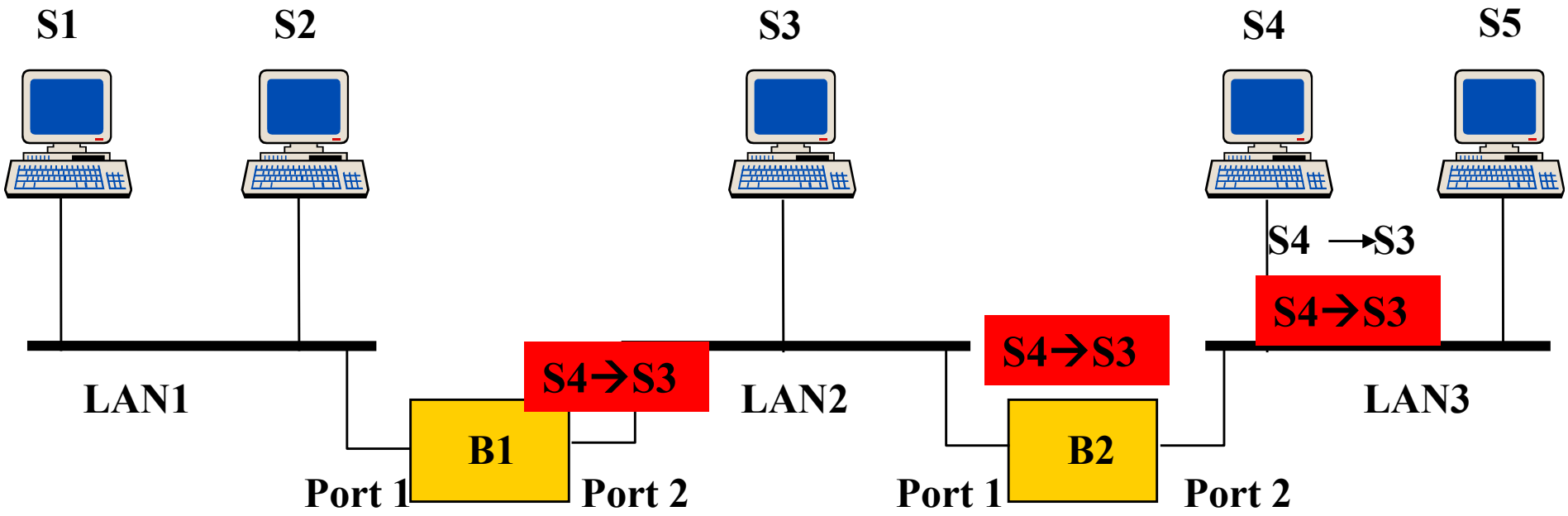


Address	Port
S1	1
S3	2

Address	Port
S1	1
S3	1

S4→S3

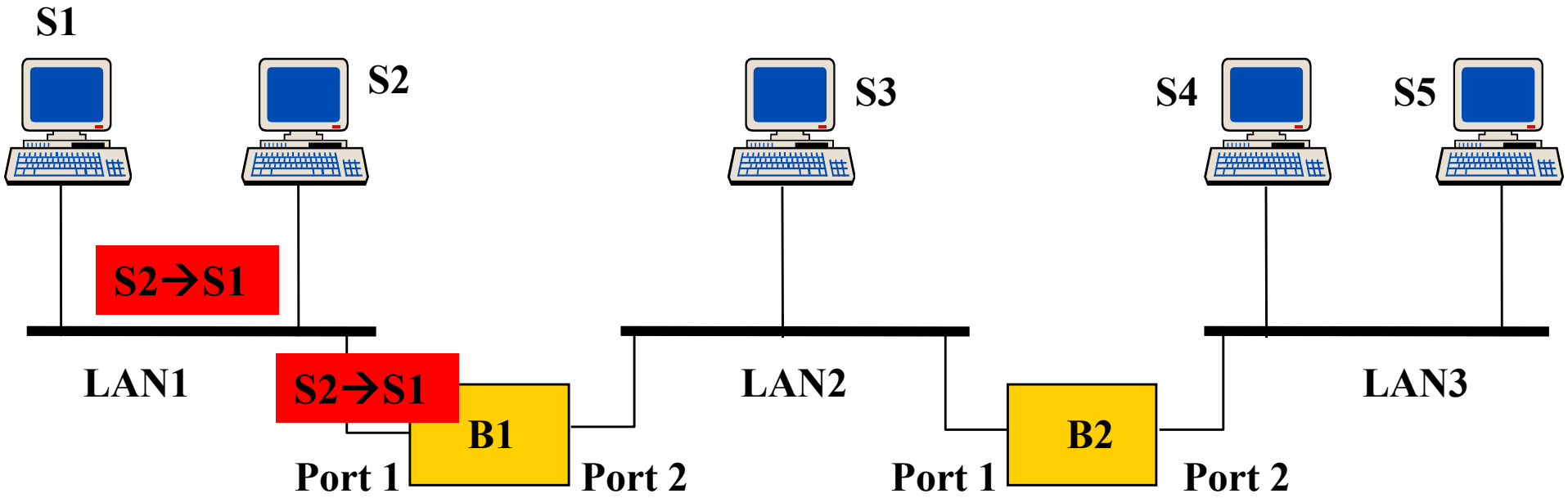
Details of S4 will be recorded in both B1 and B2 because S3 and B1 are connected in bus topology, therefore if a packet is forwarded it is received by all the nodes connected to the LAN



Address	Port
S1	1
S3	2
S4	2

Address	Port
S1	1
S3	1
S4	2

S2→S1



Address	Port
S1	1
S3	2
S4	2
S2	1

Address	Port
S1	1
S3	1
S4	2

S2->S1 Traffic is completely isolated now,
Note that bridges change collision domains.
What happens if S4->S2 now.

Example-*Learning bridge*

Gradual building of Table

Address	Port

a. Original

Address	Port
71:2B:13:45:61:41	1

b. After A sends a frame to D

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

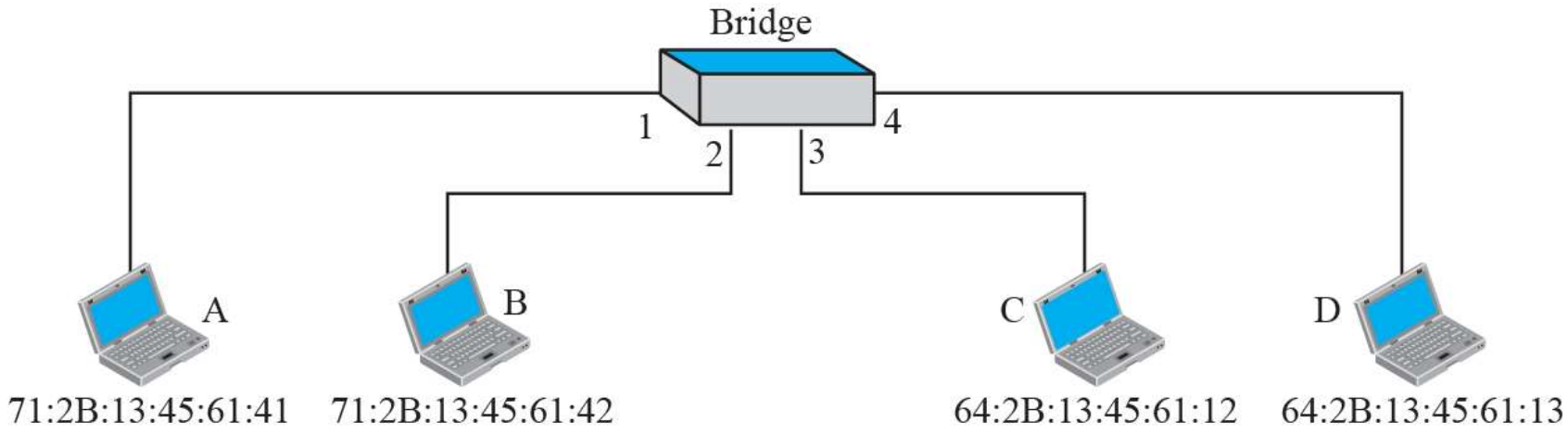
c. After D sends a frame to B

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

d. After B sends a frame to A

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

e. After C sends a frame to D



Adaptive Learning

Bridges can adopt to Dynamics of the Network

In a static network, tables eventually store all addresses & learning stops

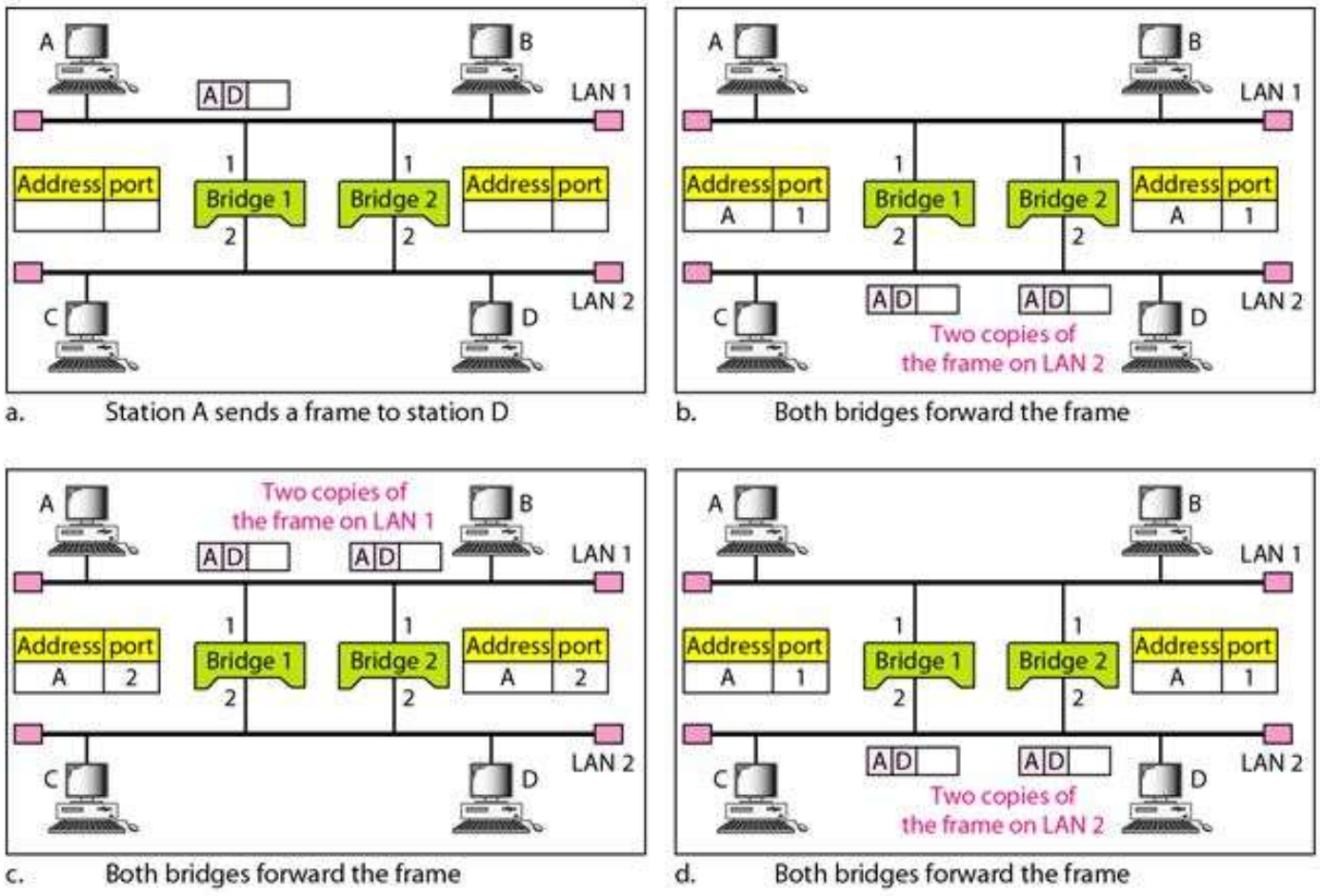
In practice, stations are added & moved all the time

- Introduce timer (minutes) to age each entry & force it to be relearned periodically
- If frame arrives on port that differs from frame address & port in table, update immediately

Two-Layer Switch

A two-layer switch performs at the physical and data link layer; it is a sophisticated bridge with faster forwarding capability.

Problem: Loops in the topology



a. Station A sends a frame to station D

b. Both bridges forward the frame

c. Both bridges forward the frame

d. Both bridges forward the frame

Even though redundant Bridge make the network more reliable, but can create loops in the system, which is very undesirable.

The **spanning tree algorithm** is used to create a loop less topology

Routers

A **router** is a three-layer device; it operates in the physical, data link, and network layers.

- **physical** layer device, it regenerates the signal it receives.
- **data link** layer device, the router checks the physical addresses (source and destination).
- **network layer** device, a router checks the network layer addresses(addresses in the IP layer)

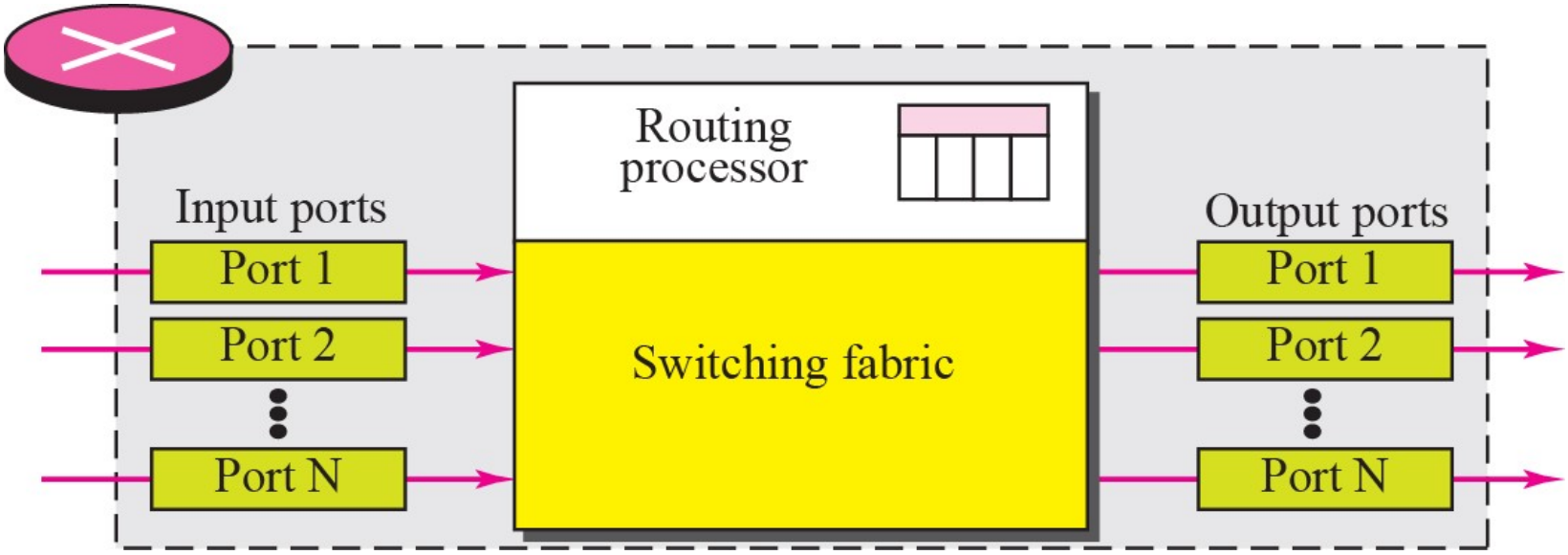
A router can connect LANs/WANs/LAN and WAN together. So Router is a an internetworking device; it connects independent networks together to form an internetwork.

A router is a three-layer (physical, data link, and network) device.

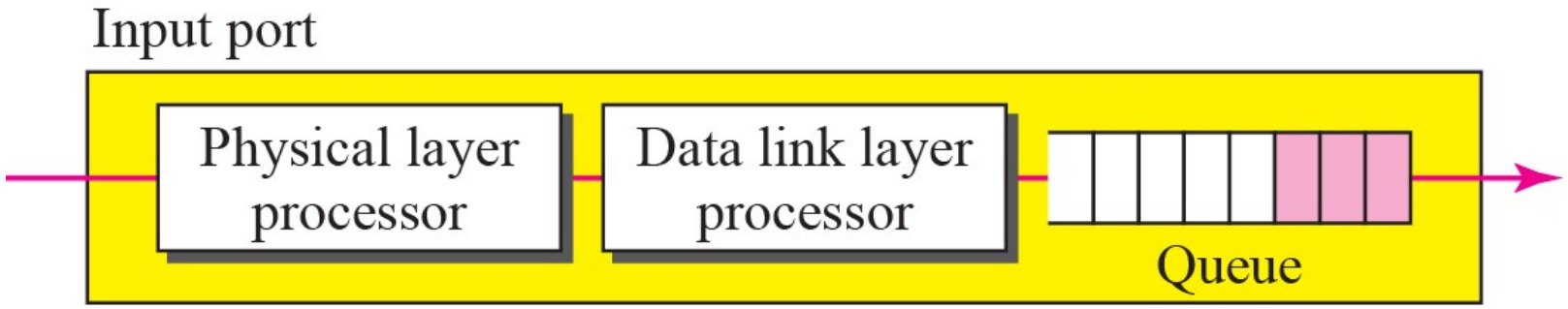
Structure of Router

Components :

Input ports, **Output ports**, the **Routing processor**, and the **Switching fabric**



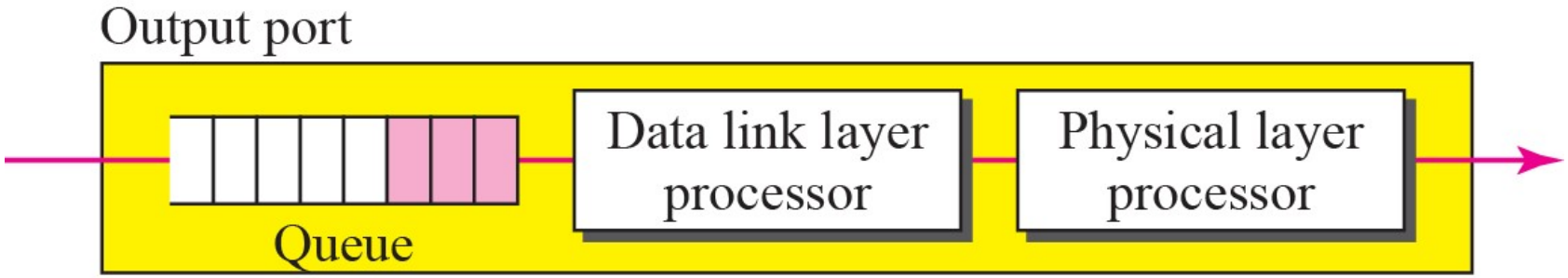
Input port



An input port performs the physical and data link layer functions of the router.

- **The bits are constructed from the received signal.**
- **Decapsulated from the frame. Errors are detected and corrected**
- **Packet is stored into input port buffer queue for further forwarding job.**

Output port



An output port performs the same functions as the input port, but in the reverse order.

Once packet is forwarded from input port buffer to output port buffer.

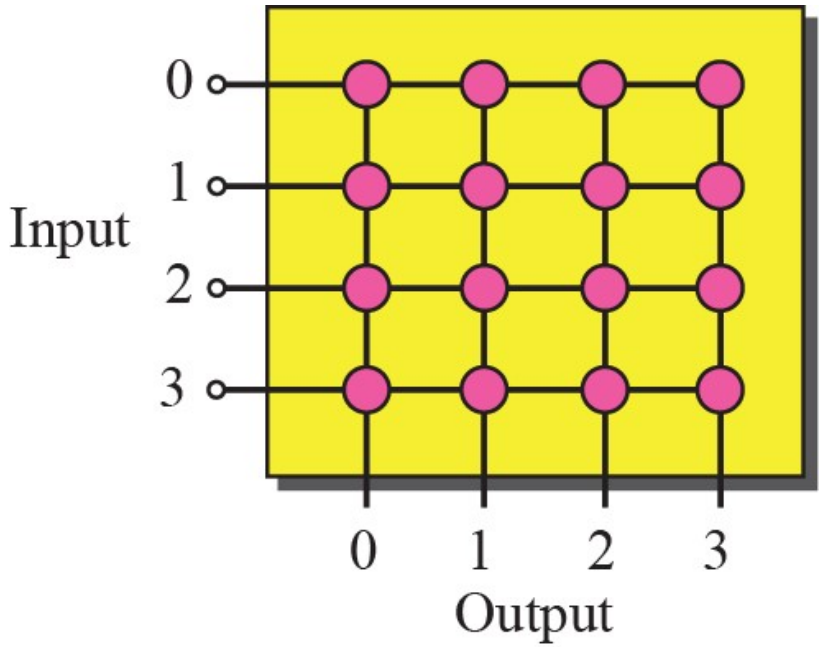
- **Outgoing packets are queued into output port buffer.**
- **The packet is encapsulated in a frame.**
- **Finally the physical layer functions are applied to the frame to create the signal to be sent**

Routing Processor

The routing processor performs the functions of the network layer.

The destination address is used to find the address of the next hop and, at the same time, the output port number from which the packet is sent out. This activity is sometimes referred to as ***table lookup*** because the routing processor searches the routing table.

Crossbar switch



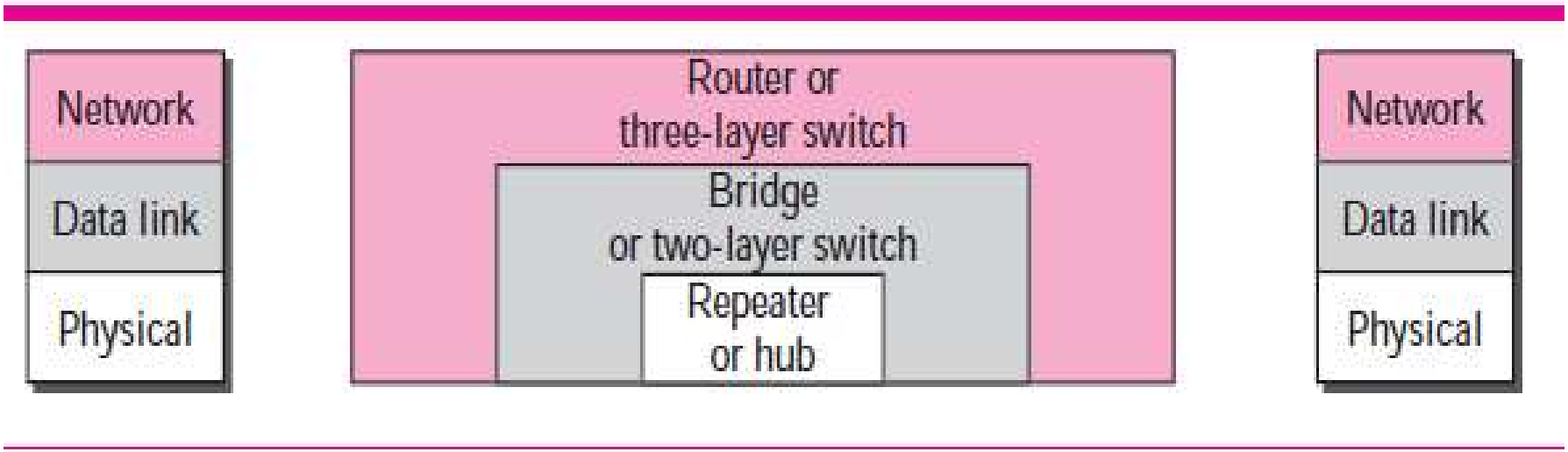
Switching fabric is responsible for moving the packet from the input queue to the output queue.

The simplest type of switching fabric is the crossbar switch.

A **crossbar switch** connects *n* inputs to *n* outputs in a **grid**, using electronic microswitches at each **Crosspoint.**

Similarly other kind of switches- **Banyan Switch, Batcher-Banyan Switch**

Connecting Devices and Layers



END OF CHAPTER