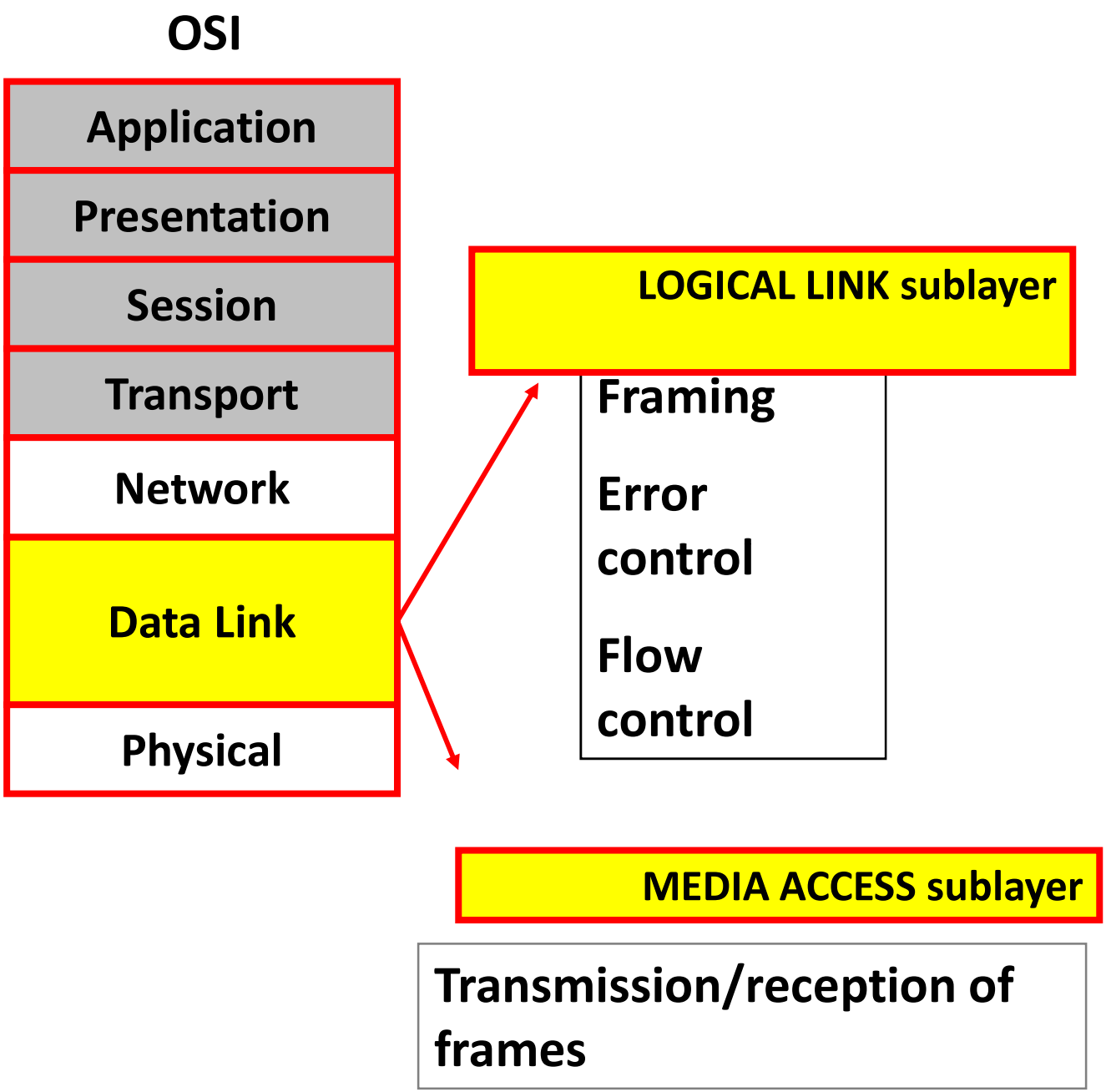
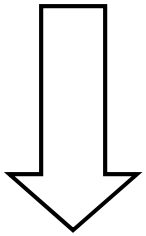
UNIT III

- **Medium Access sub layer:** Channel allocation problem, MAC Protocols: ALOHA, CSMA, CSMA/CD, MAC addresses, IEEE 802.X, Standard Ethernet, Wireless LANS. Bridges, Types of Bridges.


OSI
Application
Presentation
Session
Transport
Network
Data Link
Physical
LOGICAL LINK sublayer
Framing
Error control
Flow control
MEDIA ACCESS sublayer
Transmission/reception of frames

The Medium Access Sub layer



deals with

BROADCAST NETWORKS AND THEIR PROTOCOLS

Broadcast channels are sometimes referred to as ***multi-access channels*** *or* ***random access channels.***

Medium/Multiple Access

- **Problem**: When two or more nodes transmit at the same time, their frames will collide and the link bandwidth is **wasted** during collision
  - How to coordinate the access of multiple sending/receiving nodes to the shared link**???**
- **Solution**: We need a **protocol** to coordinate the transmission of the active nodes
- These protocols are called **Medium or Multiple Access Control (MAC) Protocols** belong to a **sublayer** of the data link layer called **MAC** (Medium Access Control)
- What is expected from Multiple Access Protocols:
  - Main task is to **minimize collisions** in order to **utilize the bandwidth** by:
    - Determining **when** a station can use the link (medium)
    - **what** a station should do when the link is **busy**
    - **what** the station should do when it is involved in **collision**

Channel Allocation Problem

- **Channel allocation** is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.
- Channel allocation problem can be solved by two schemes:
  - Static Channel Allocation in LANs and MANs
  - Dynamic Channel Allocation in LANs and MANs

Static Channel Allocation in LANs and MANs:

- It is the classical or traditional approach of allocating a single channel among multiple competing users. it uses Frequency Division Multiplexing (FDM).
- If there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion. since each user has a private frequency band, there is no interference between users.
- If the number of users are small and have heavy load, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

- Problem is When the number of senders are large and traffic becomes bursty.
  - If the spectrum is cut up into N regions and fewer than N users communicate. Then large piece of valuable spectrum is wasted.
  - If more than N users want to communicate, some will be denied permission for lack of bandwidth.
  - However even if number of users are held constant at N, dividing the single available channel into static channel is inefficient. This is because if some uses are quiescent, their bandwidth is simply lost.

Dynamic Channel Allocation in LANs and MANs

Five key assumptions:

1. **Station Model:** The model consists of **N** independent stations, each with a program or user that generates frames for transmission. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

2. **Single Channel Assumption**: A single channel is available for all communication. All stations can transmit on it and all can receive from it. As far as the hardware is concerned, all stations are equivalent, although some protocol software may assign priorities to them.

3.Collision Assumption: If two frames are transmitted simultaneously, they overlap in time and the resulting signal is distorted. This event is called a **collision**.

All stations can detect collisions. A collided frame must be transmitted again later. There are no errors other than those generated by collisions.

4a.Continuous Time: Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.

4b.Slotted Time: Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

- **5a.Carrier Sense: (LAN)** Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.
- **5b. No Carrier Sense:(Satellite)** Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether or not the transmission was successful.

Multiple Access Protocols

- ALOHA
- Carrier Sense Multiple Access Protocols(CSMA)
- Collision-Free Protocols
- Limited-Contention Protocols
- Wavelength Division Multiple Access Protocols
- Wireless LAN Protocols

ALOHA

- In 1970 Norman Abramson and his colleagues at university of Hawaii devised a new and elegant method to solve the channel allocation problem.
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- The main problem in shared media is collision when more than one station want to transmit simultaneously

ALOHA

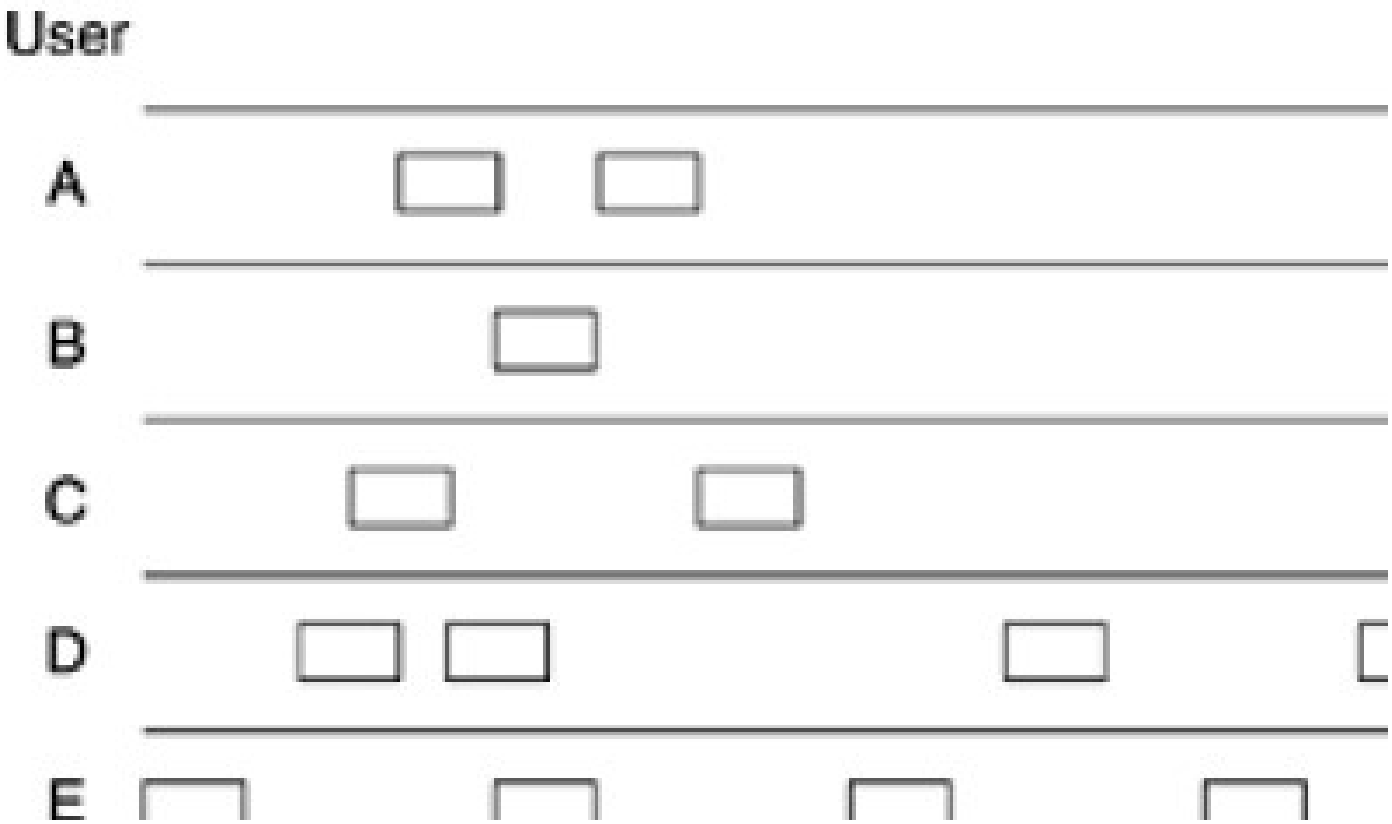
- Versions
  - Pure ALOHA (Mr. Norman Abramson in 1970s)
  - Slotted ALOHA (Mr. Roberts in 1972)

  The basic difference between the two is with respect to timing
  - Pure ALOHA does not require global time for synchronization
  - Slotted ALOHA does

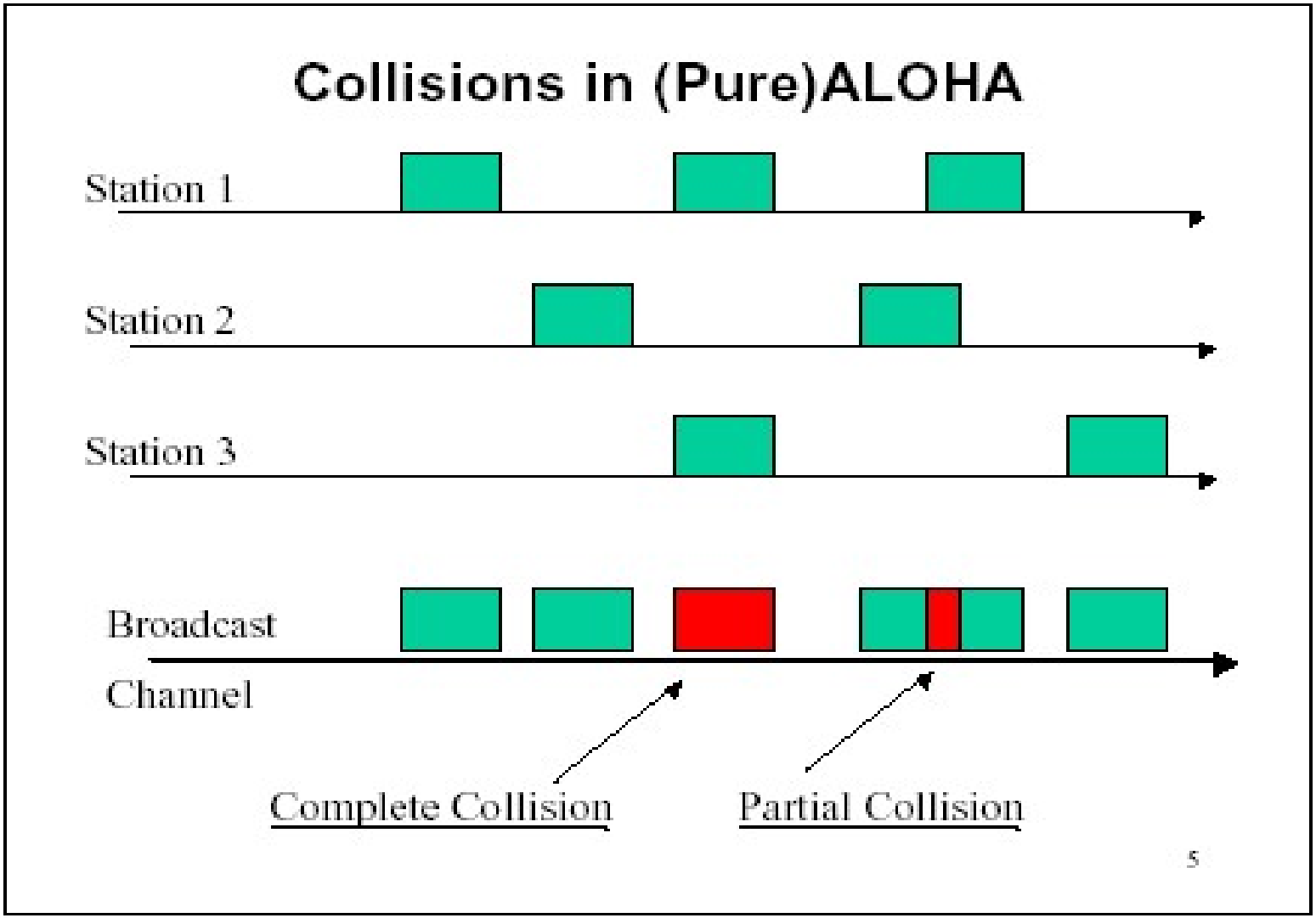
Pure ALOHA

- All frames from any station are of fixed length (L bits)
- A station that has data can transmit at any time
- There will be collisions and if collision detected the corresponding frames are destroyed.
- After transmitting a frame, the sender waits for an acknowledgment for an amount of time
- If no ACK was received, sender assumes that the frame or ACK has been destroyed and resends that frame after it waits for a *random* amount of time
- If station fails to receive an ACK after repeated transmissions, it gives up
- Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contention system.

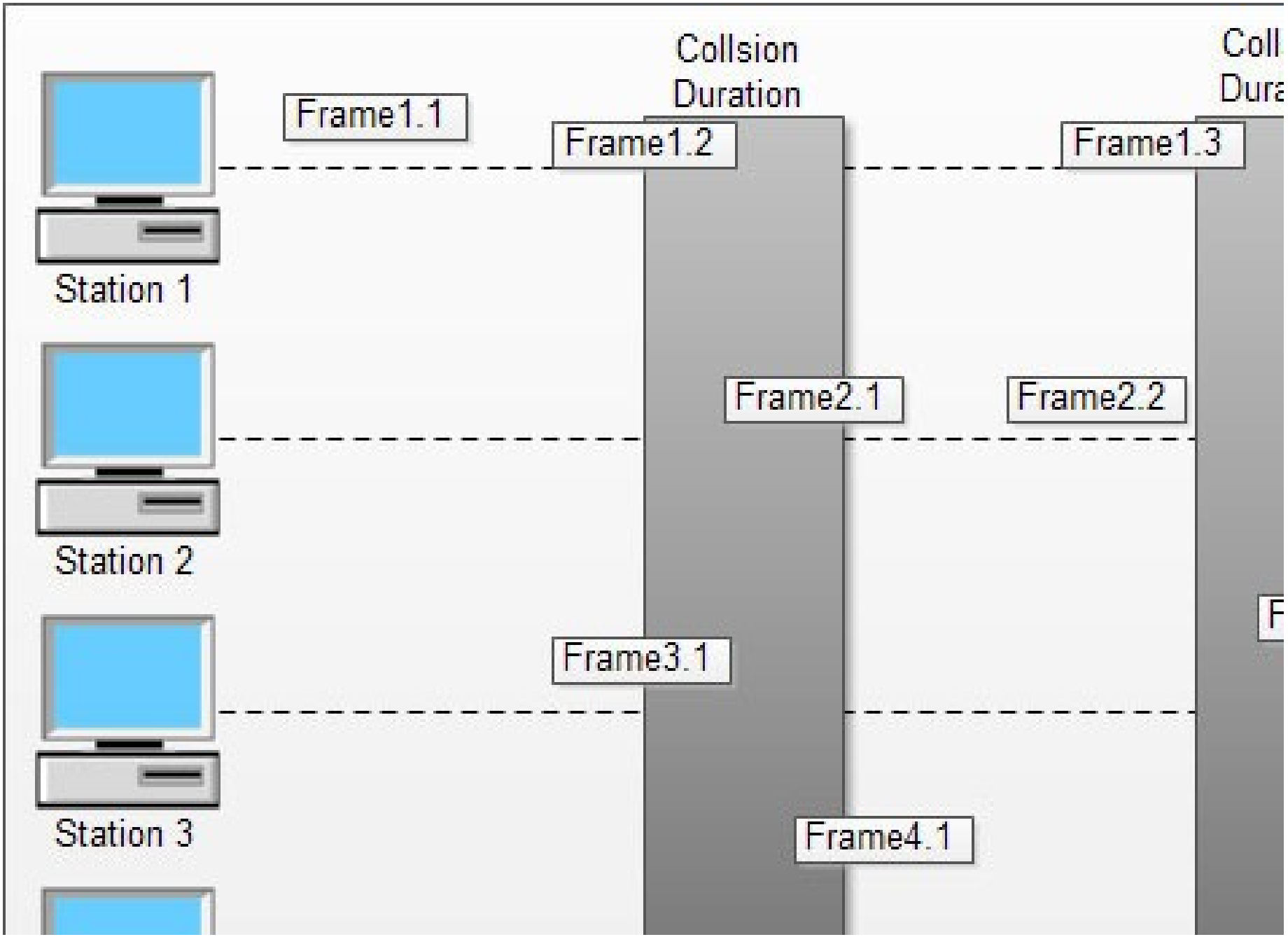
In pure ALOHA, frames are transmitted at completely arbitrary times.



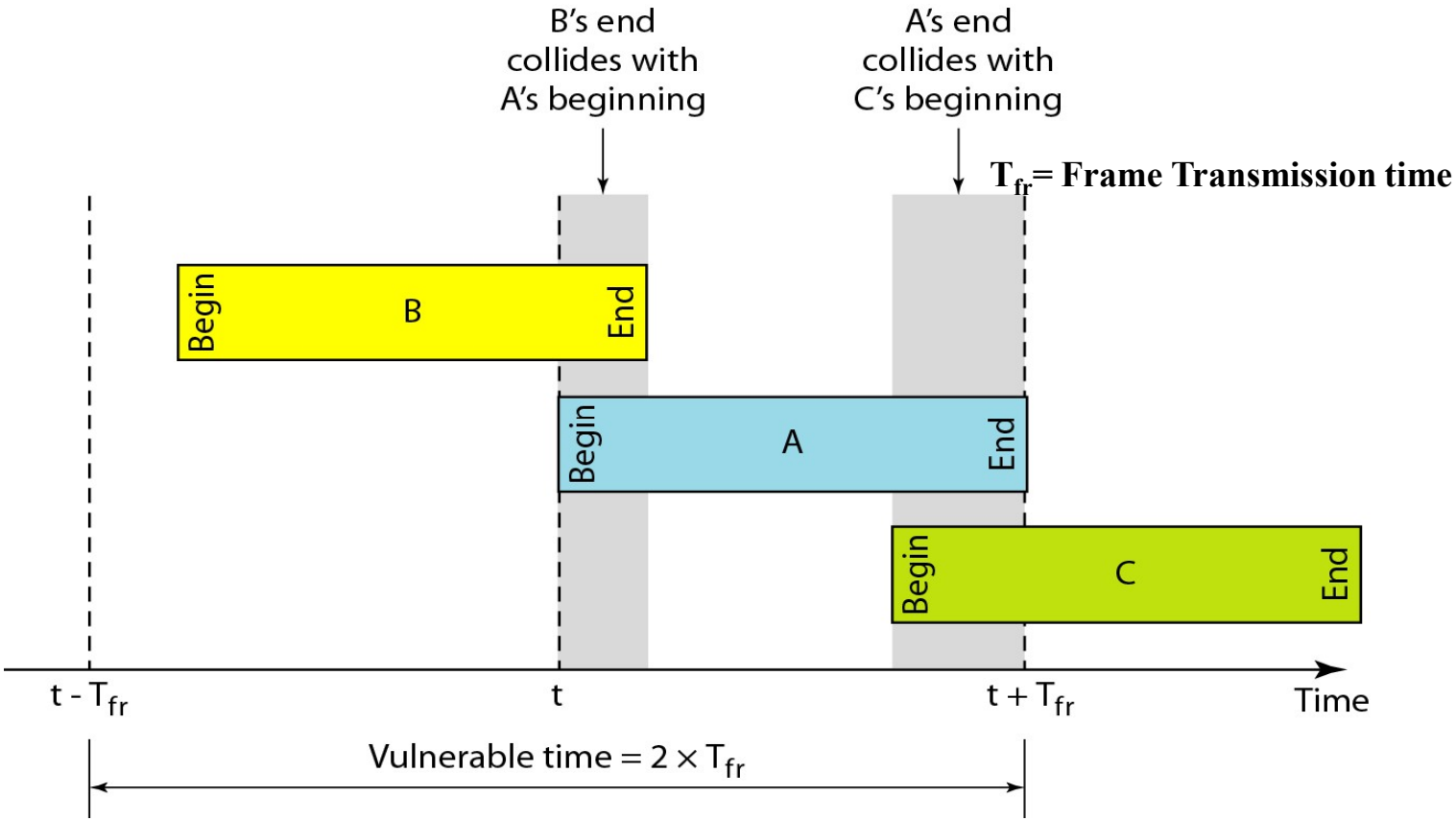
Pure ALOHA



In pure ALOHA, frames are transmitted at completely arbitrary times.


Collsion
Duration
Frame1.1
Frame1.2
Frame1.3
Station 1
Frame2.1
Frame2.2
Station 2
Frame3.1
Station 3
Frame4.1

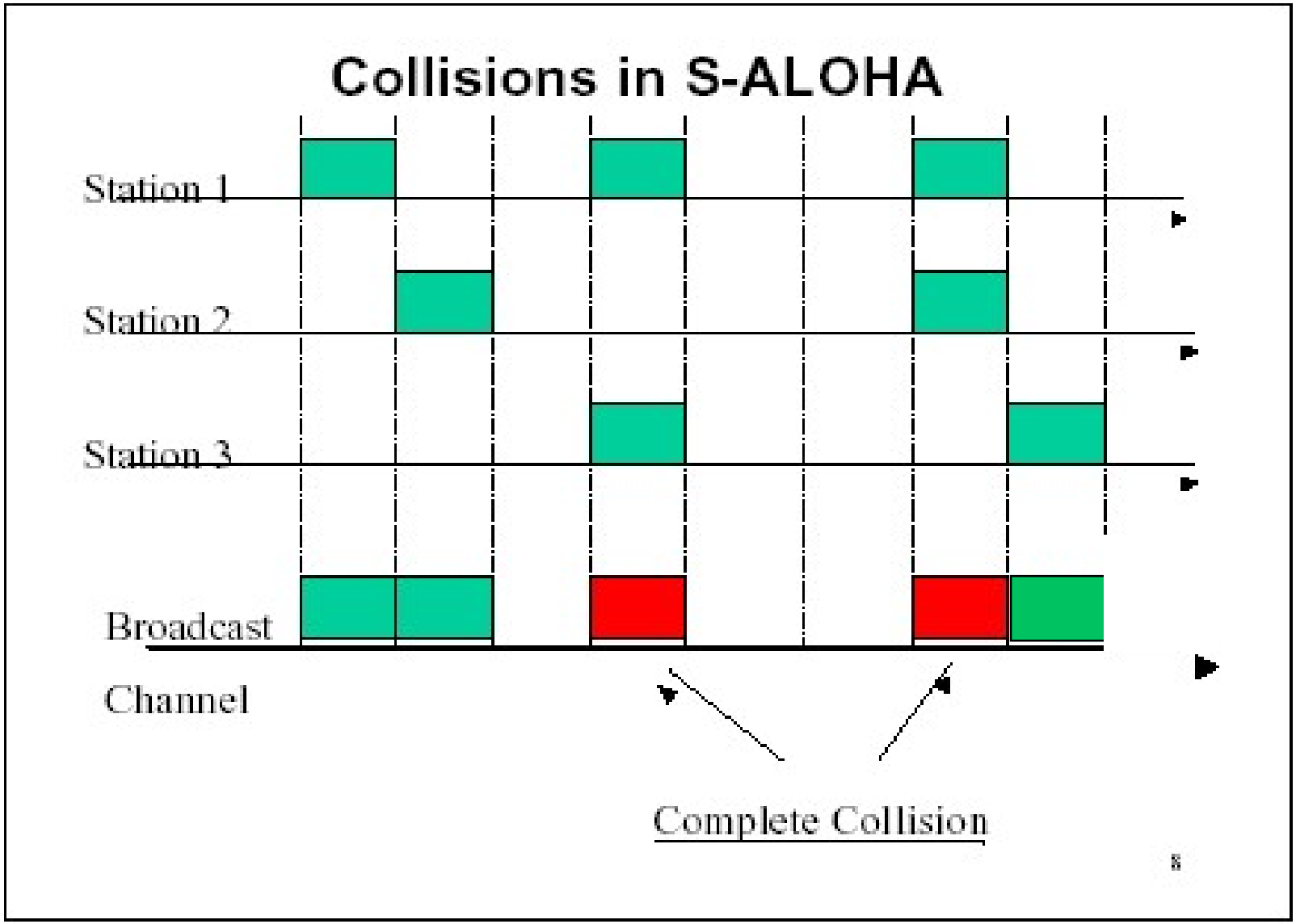
Critical time for pure ALOHA protocol

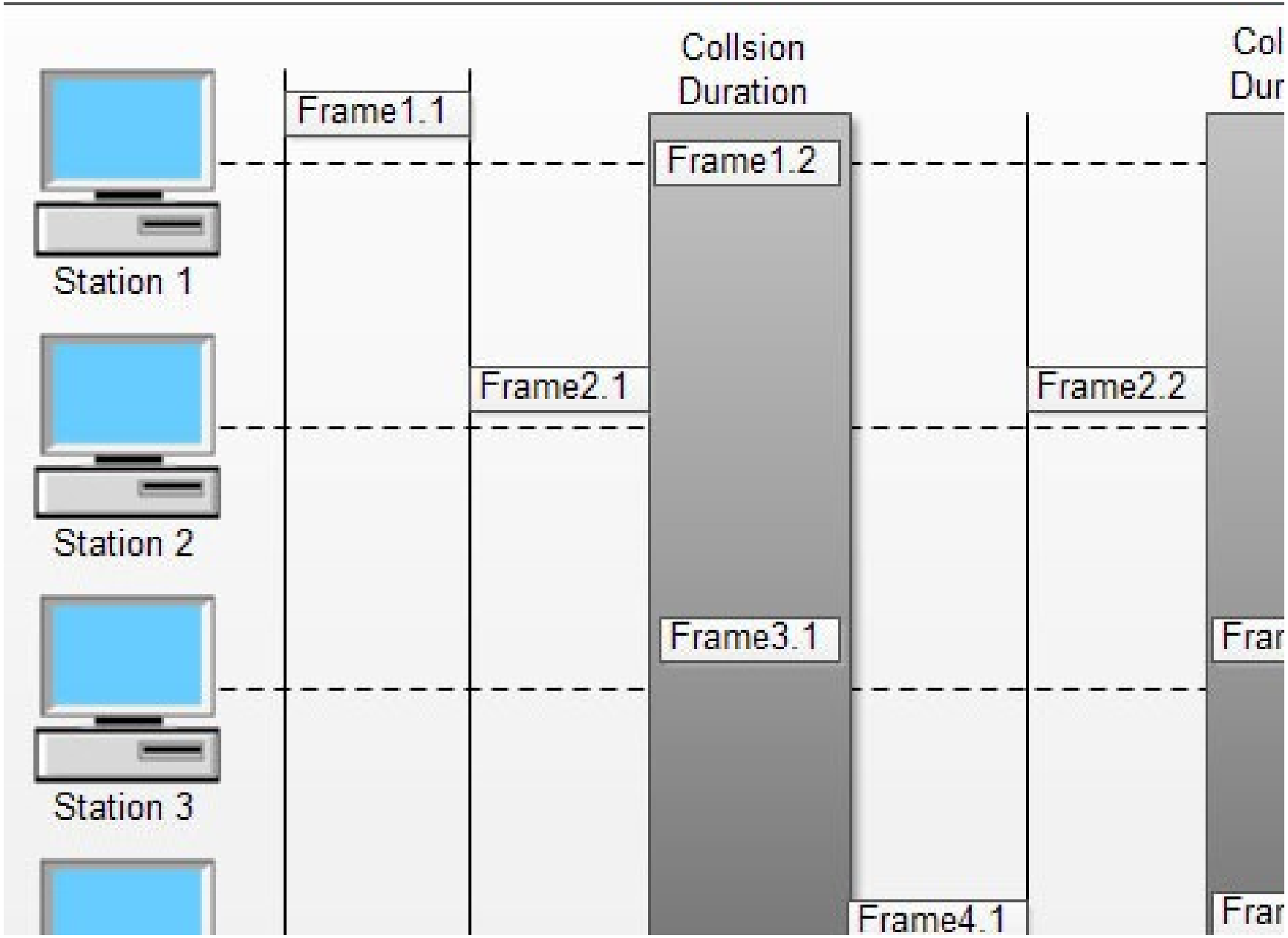


Slotted aloha :

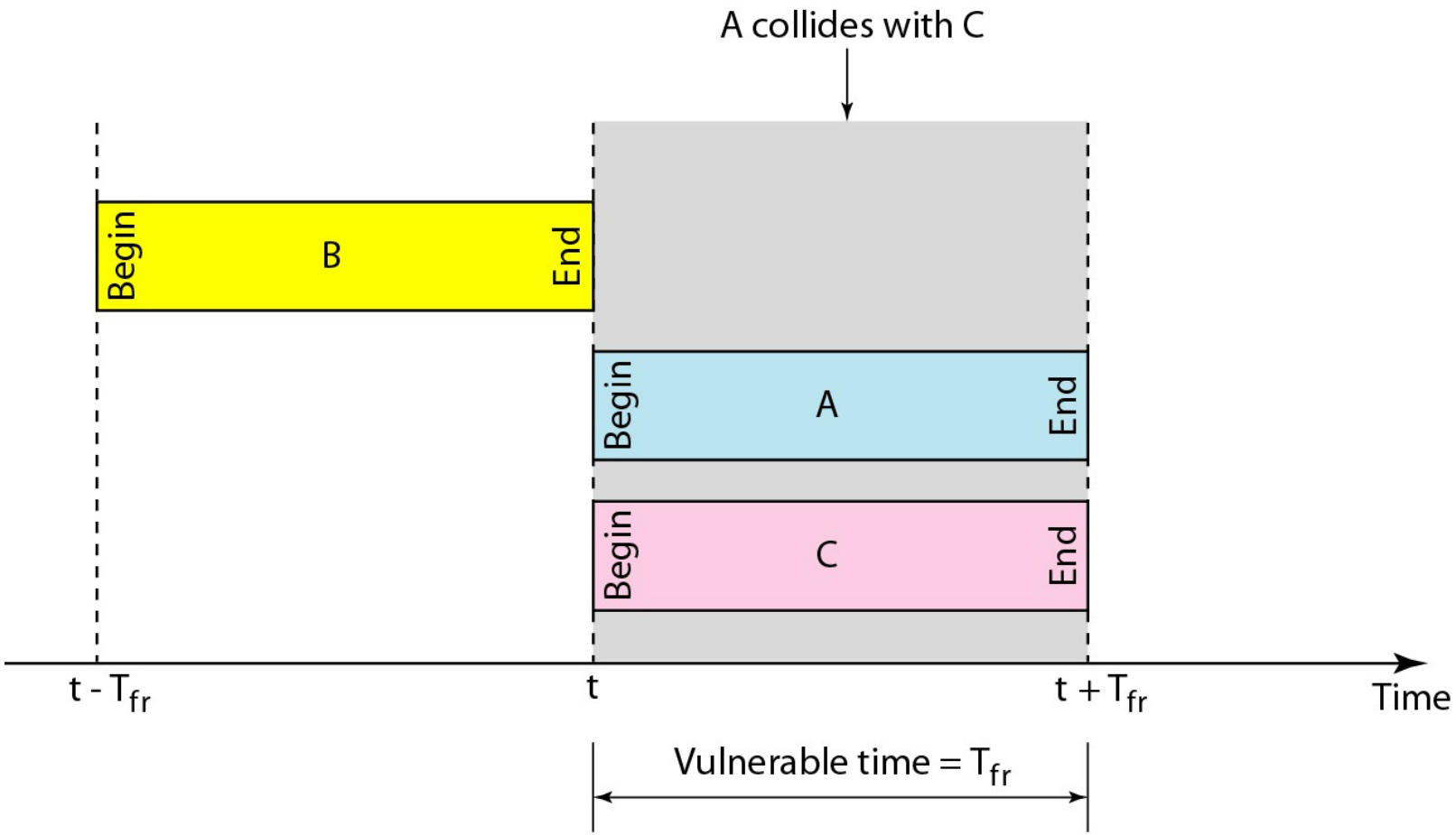
- Time is divided into slots equal to a **frame transmission time (T_{fr})**
- A station can transmit at the beginning of a slot only
- If a station misses the beginning of a slot, it has to wait until the beginning of the next time slot.
- **A central clock** or station informs all stations about the start of a each slot

Random Access – Slotted ALOHA

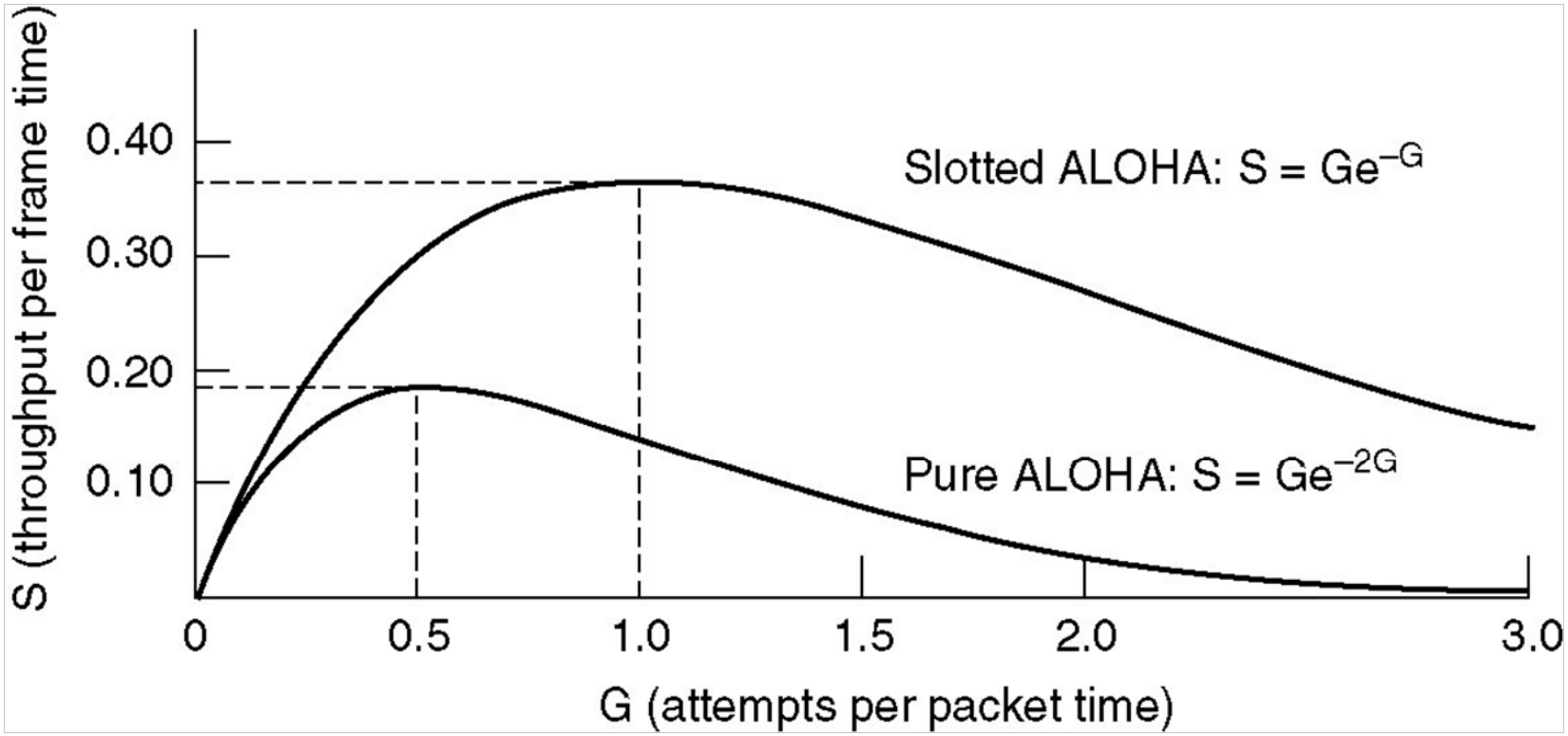



Collsion
Duration
Frame1.1
Frame1.2
Station 1
Frame2.1
Frame2.2
Station 2
Frame3.1
Station 3
Frame4.1

In danger time for slotted ALOHA protocol



Efficiency of Aloha



G = offered load rate= new frames+ retransmitted
= **Total frames presented to the link per the transmission time of a single frame**

Fig. Throughput versus offered traffic for ALOHA systems

Note

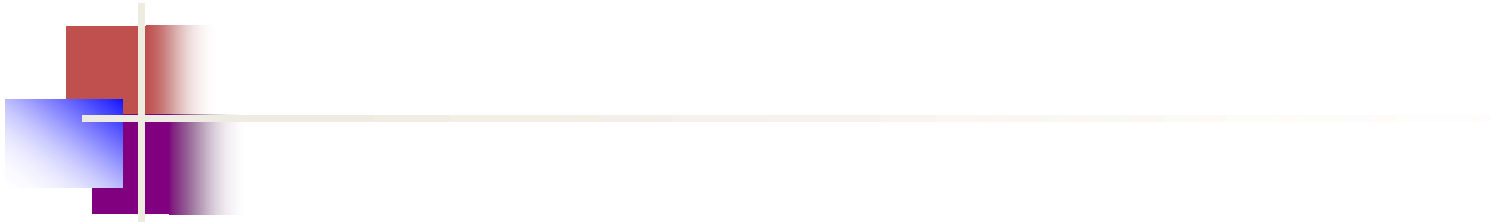
The throughput (S) for pure ALOHA is

$$S = G \times e^{-2G} .$$

The maximum throughput

$$S_{max} = 0.184 \text{ when } G = (1/2).$$

G = Average number of frames generated by the system (all stations) during one frame transmission time



Note

The throughput for slotted ALOHA is $S = G \times e^{-G}$.

The maximum throughput $S_{max} = 0.368$ when G = 1.

Differences Between Pure ALOHA and Slotted ALOHA

Pure ALOHA	Slotted ALOHA
When a first frame arrives, the node immediately transmits	When a node has a fresh frame to send, it waits until the beginning of the next slot
Nodes can transmit frames at Random Times.	Nodes can transmit frames in their respective slot boundaries only at the beginning of the Slot.
Does not require Synchronization of slots of any nodes.	Requires synchronization between slots of nodes.
Mode of Transfer is Continuous.	Mode of transfer is Discrete

Carrier Sense Multiple Access (CSMA)

- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- The chance of collision can be reduced if a station **senses the medium before trying to use** it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

CSMA: Carrier Sense Multiple Access

Advantage:

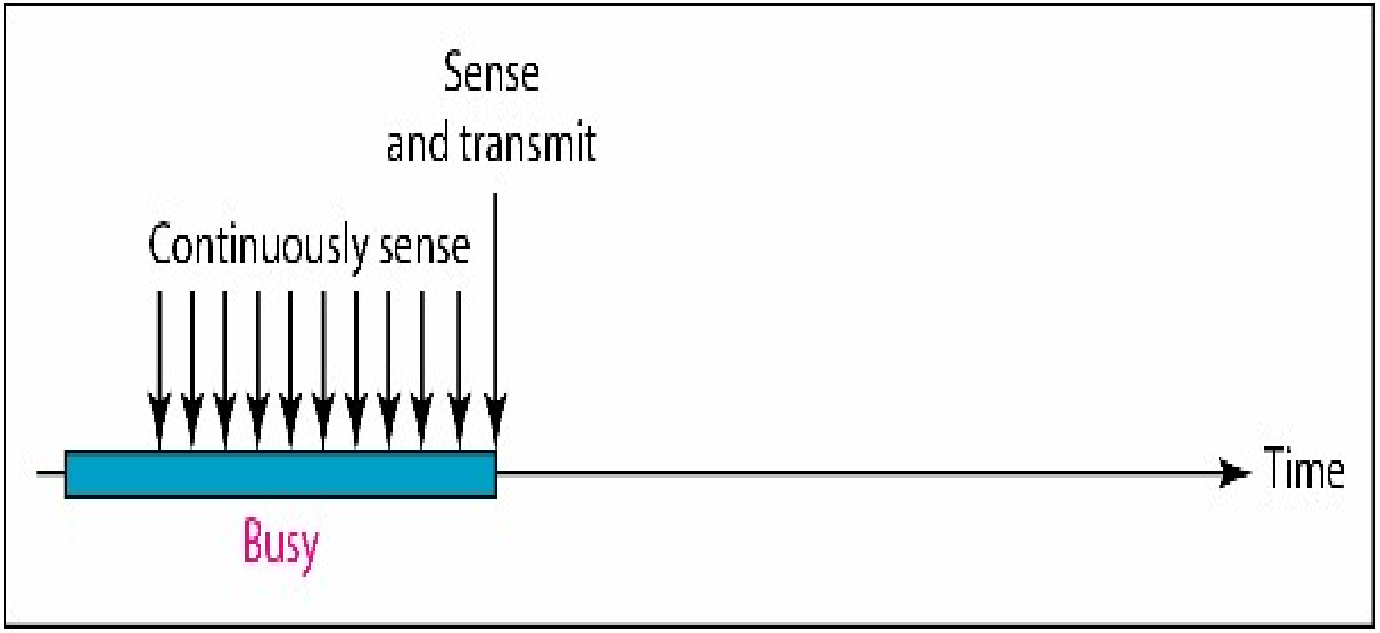
- Minimize the chance of collision
- Increases the performance.

CSMA Methods

- 1-persistent CSMA
- non-persistent CSMA
- p-persistent CSMA

1-persistent

- When a station has data to send, it first listens to channel to see if any one else is transmitting at that moment.
- If the channel is busy, the station continuously senses until it becomes idle.
- When the station detects an idle channel, it transmits a frame.
- If a collision occurs, the station waits a random amount of time and starts all over again.
- The station transmits with a probability of 1 whenever if finds the channel idle.



a. 1-persistent

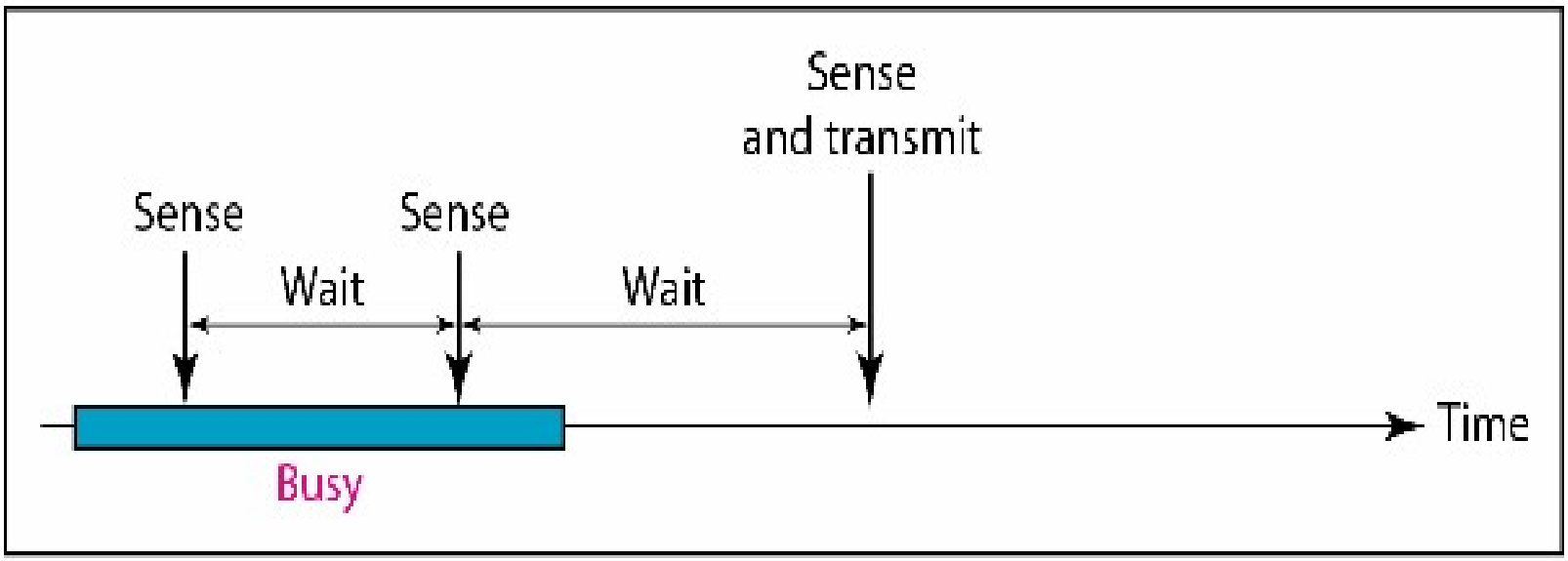
- Performance
  - 1-persistent stations are **selfish**
  - If two or more stations becomes ready at the same time, **collision guaranteed**

1-persistent

- Propagation delay and zero propagation delay.
  - The propagation delay has an important effect on the performance of the protocol.
  - There is a small chance that just after a station begins sending, another station will become ready to send and sense the channel. If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision
  - Even if the propagation delay is zero, there will still be collisions. If two stations become ready in the middle of a third station's transmission, both will wait politely until the transmission ends and then both will begin transmitting exactly simultaneously, resulting in a collision.

Non-persistent CSMA

- *A station that has a frame to send it senses the line.*
- *If the line is idle, it sends immediately.*
- *If the line is not idle,* ***it waits a random amount of time and then senses the line again.***
- *This algorithm should lead to better channel utilization and longer delays than 1-persistant CSMA*



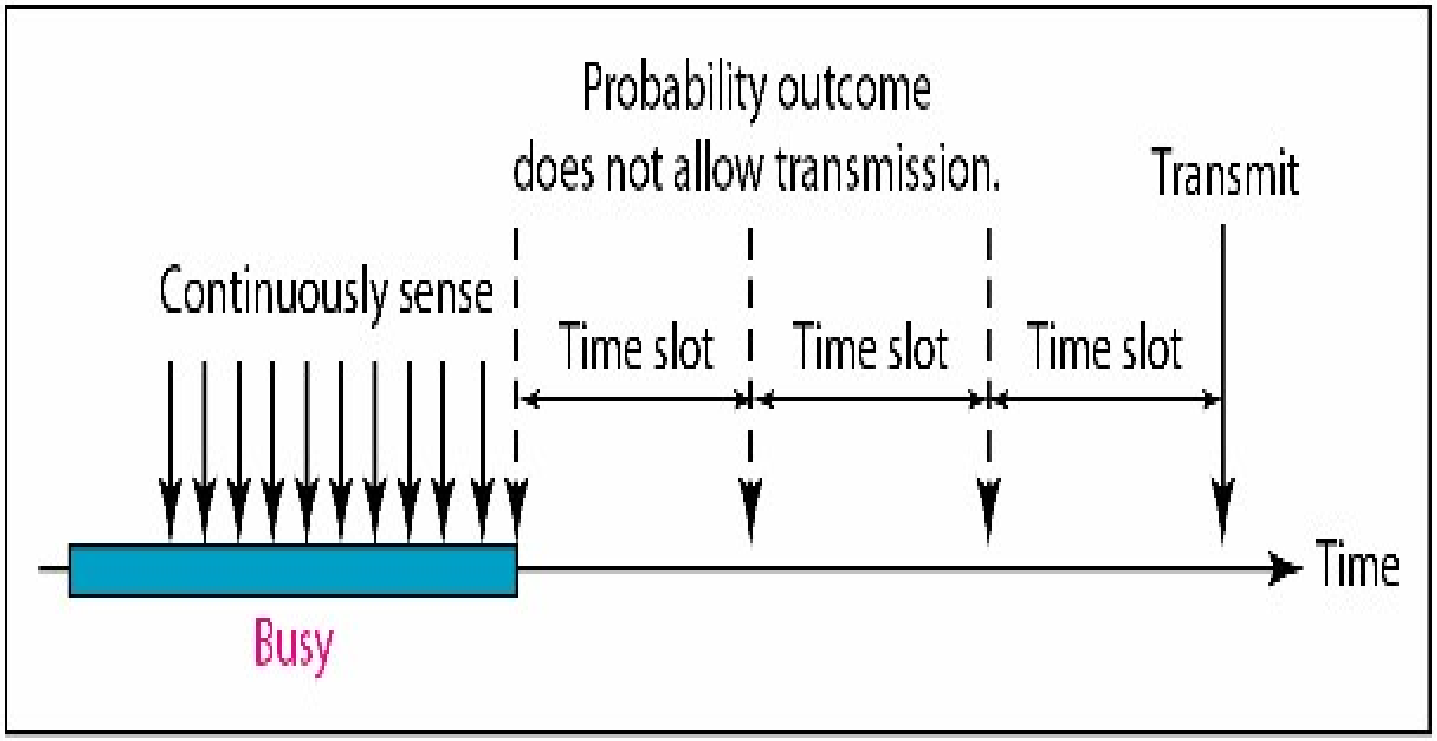
b. Nonpersistent

- Performance:
  - Random delays reduces probability of collisions because two stations with data to be transmitted will wait for different amount of times.
  - Bandwidth is **wasted** if waiting time (backoff) is large because medium will remain idle following end of transmission even if one or more stations have frames to send

P-persistent CSMA

- Time is divided to slots where each Time unit (slot).
- Station wishing to transmit listens to the medium:

1. If medium idle,
   - transmit with probability (**p**), OR
   - wait **one time unit (slot)** with probability (**1 – p**), then repeat 1.
2. If medium busy, **continuously listen until idle** and repeat step **1**

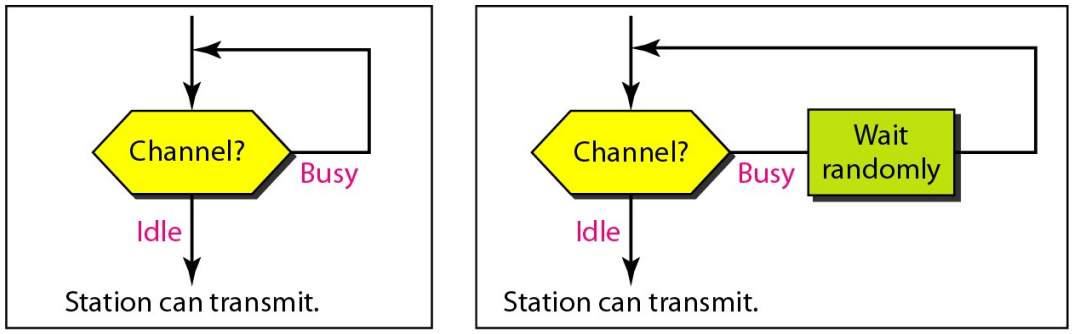


c. p-persistent

Performance

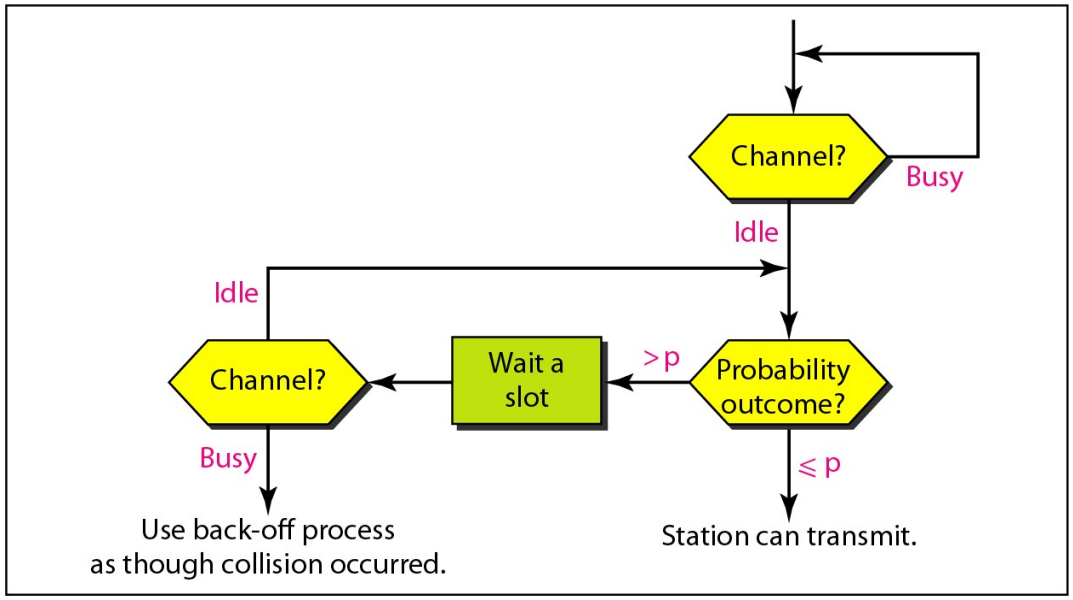
- Reduces the possibility of collisions like **nonpersistent**
- Reduces channel idle time like **1-persistent**

Flow diagram for three persistence methods



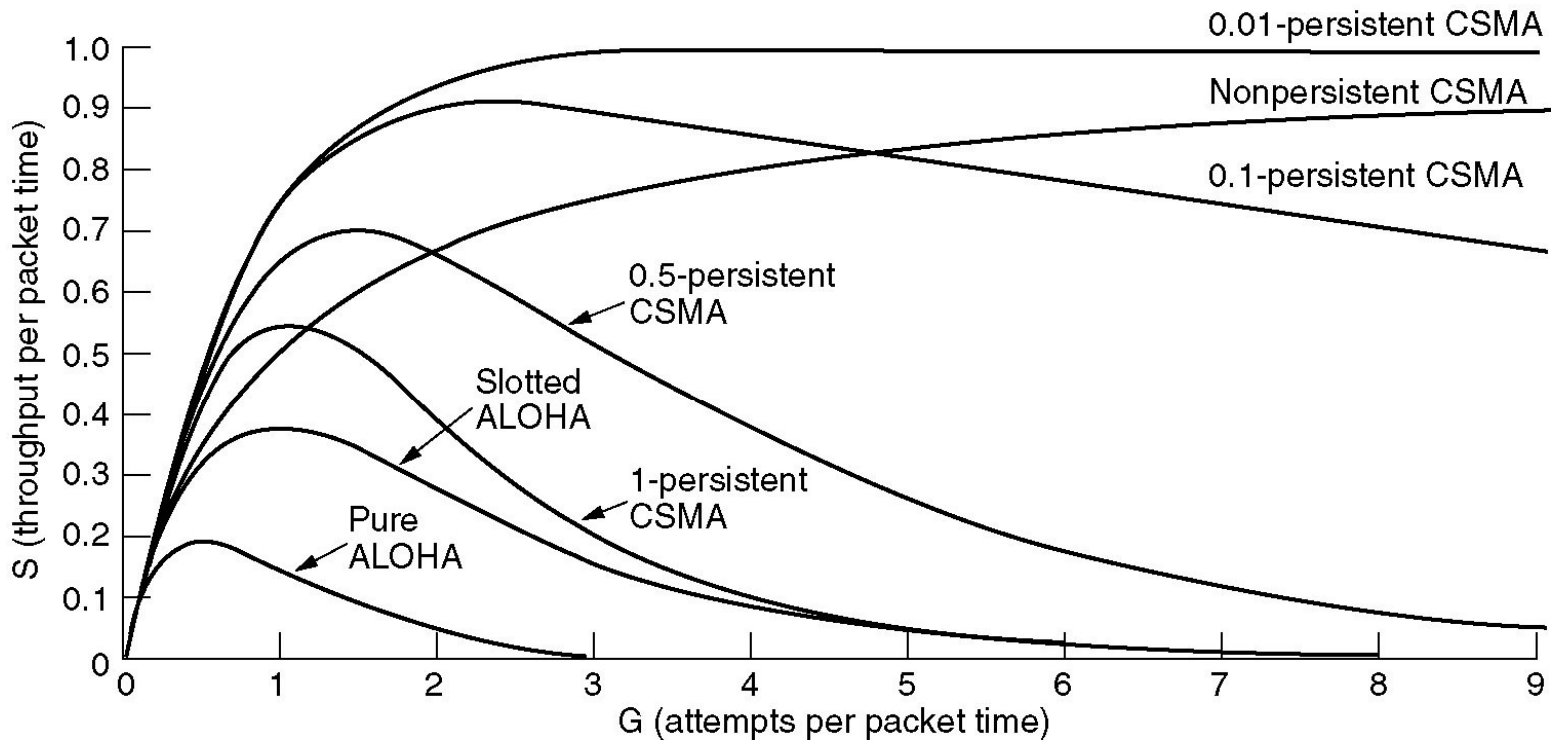
a. 1-persistent

b. Nonpersistent



c. p-persistent

Persistent and Nonpersistent CSMA



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

CSMA with Collision Detection

- In this method a station monitors the medium after it sends a frame it check if the transmission was successful.
- station aborts their transmissions as soon as they detect a collision . To save time and bandwidth.
- If collision occurs a special signal has to be send,so that other stops transmitting the data .this signal is called jamming signal

CSMA/CD Protocol

- Use one of the CSMA persistence algorithm

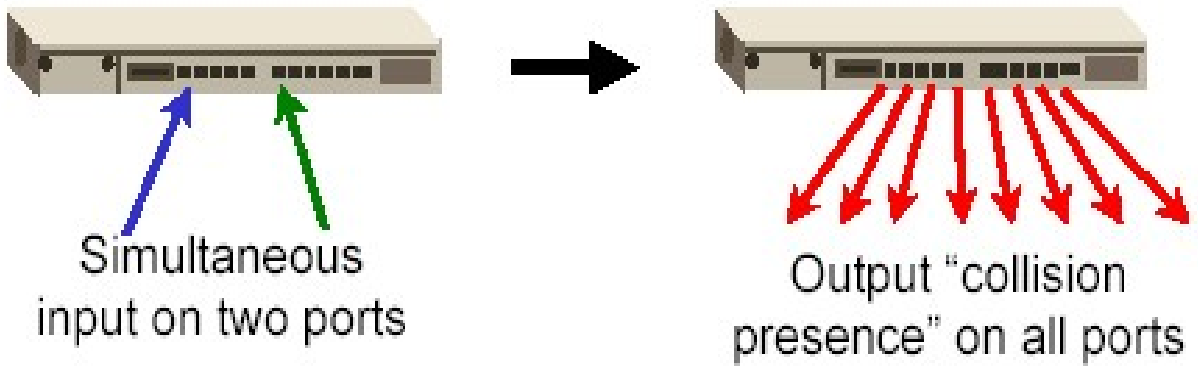
(non-persistent, 1-persistent, p-persistent) for transmission

- If a collision is detected by a station during its transmission then it should do the following:
  - **Abort transmission** and
  - **Transmit** a ***jam signal*** to notify other stations of collision so that they will **discard the transmitted fra**me also to make sure that the collision signal will stay until detected by all the station
  - After sending the ***jam signal***, **backoff (wait) for a *random*** amount of time, then
  - Transmit the frame again

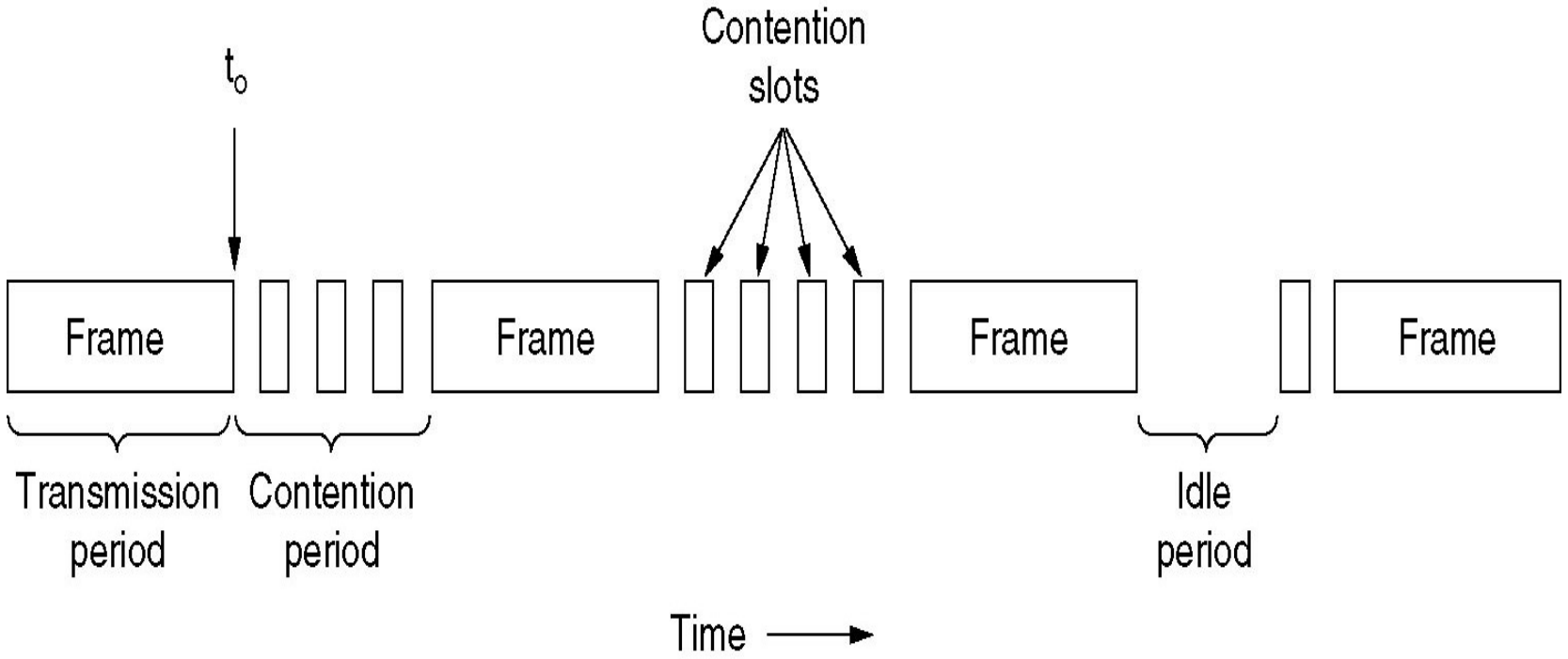
How does a node detect a collision?

Transceiver: **A node monitors the media while transmitting. If the observed power is more than transmitted power** of its own signal, it means collision occurred

Hub: **if input occurs simultaneously on two ports, it indicates a collision. Hub sends a collision presence signal on all ports.**

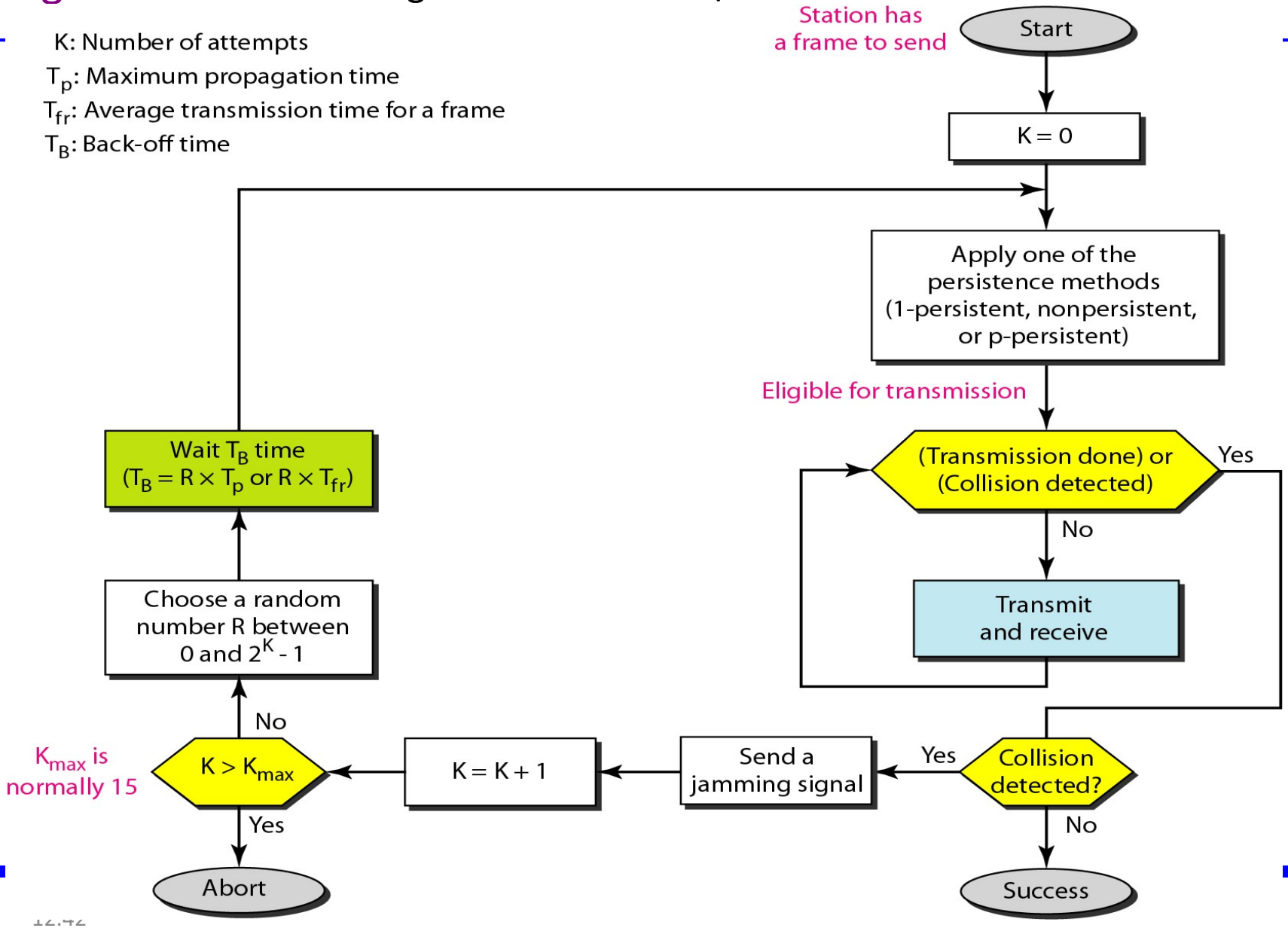


CSMA with Collision Detection



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

Figure 12.14 Flow diagram for the CSMA/CD

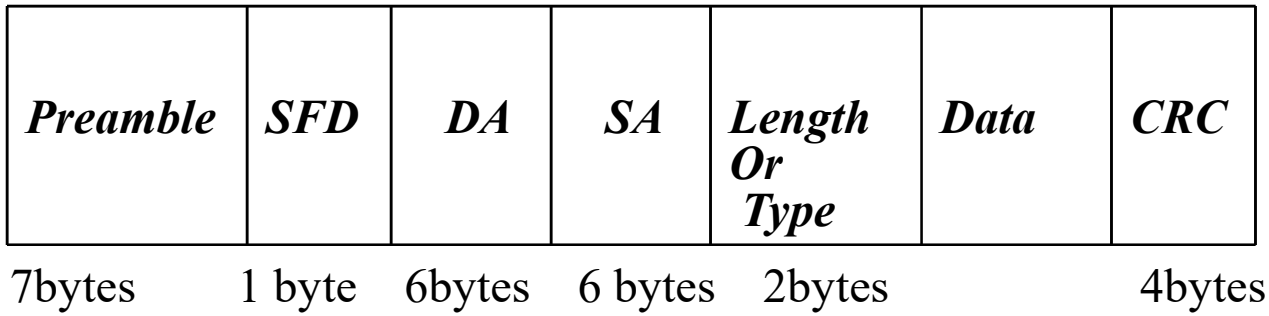


Wired LANs: *Ethernet*

MAC Sublayer

- In Standard Ethernet, the MAC sublayer governs the operation of the access method.
- It also frames data received from the upper layer and passes them to the physical layer.
- Frame Format
  - The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC
  - It does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.

IEEE 802.3 MAC FRAME FORMAT:



Preamble: The first field of the 802.3 frame Contain 7bytes (56 bits) of alternating 0's and 1's.that alerts the receiving system to the coming frame and enables it to synchronize.

The preamble is actually added at the physical layer and is not formally part of the frame.

IEEE 802.3 MAC FRAME FORMAT:

•Start frame delimiter (SFD). The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

•Destination address (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

•Source address (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet.

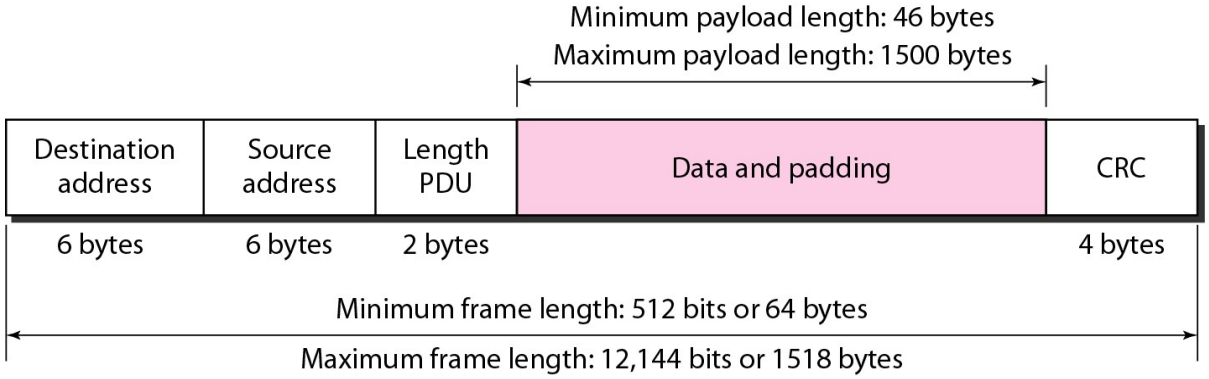
•Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

•Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes

•CRC. The last field contains error detection information, in this case a CRC-32

FRAME LENGTH

- Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame



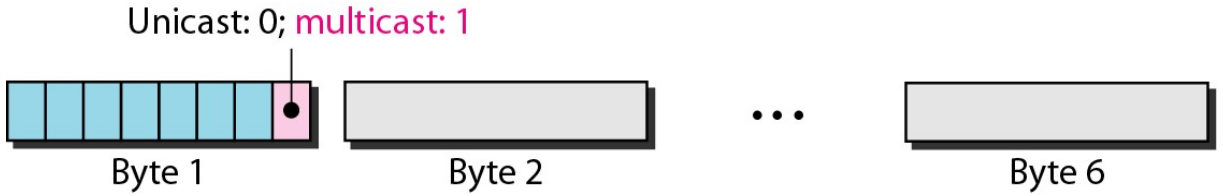
Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address.

Addressing

- Ethernet address in hexadecimal notation

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

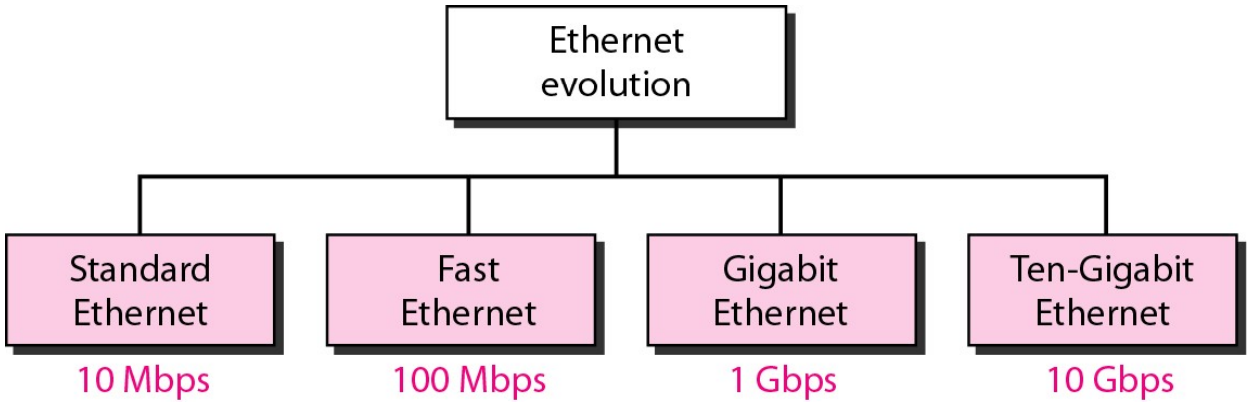


Unicast, Multicast & Broadcast Addressing

- **Source Address** is always **Unicast** means, frame comes from only one station.
- **Destination Address can be Unicast, Multicast , Broadcast**
- **Unicast Addressing** : Defines only one recipient. Sender & Receiver relationship is one-one.
- **Multicast Addressing**: Defines a group of addresses. Sender & Receiver relationship is one-many.
- **Broadcast Addressing**: Defines a special case of Multicast Address in which destination address is forty eight 1's .

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



Physical Layer: Ethernet

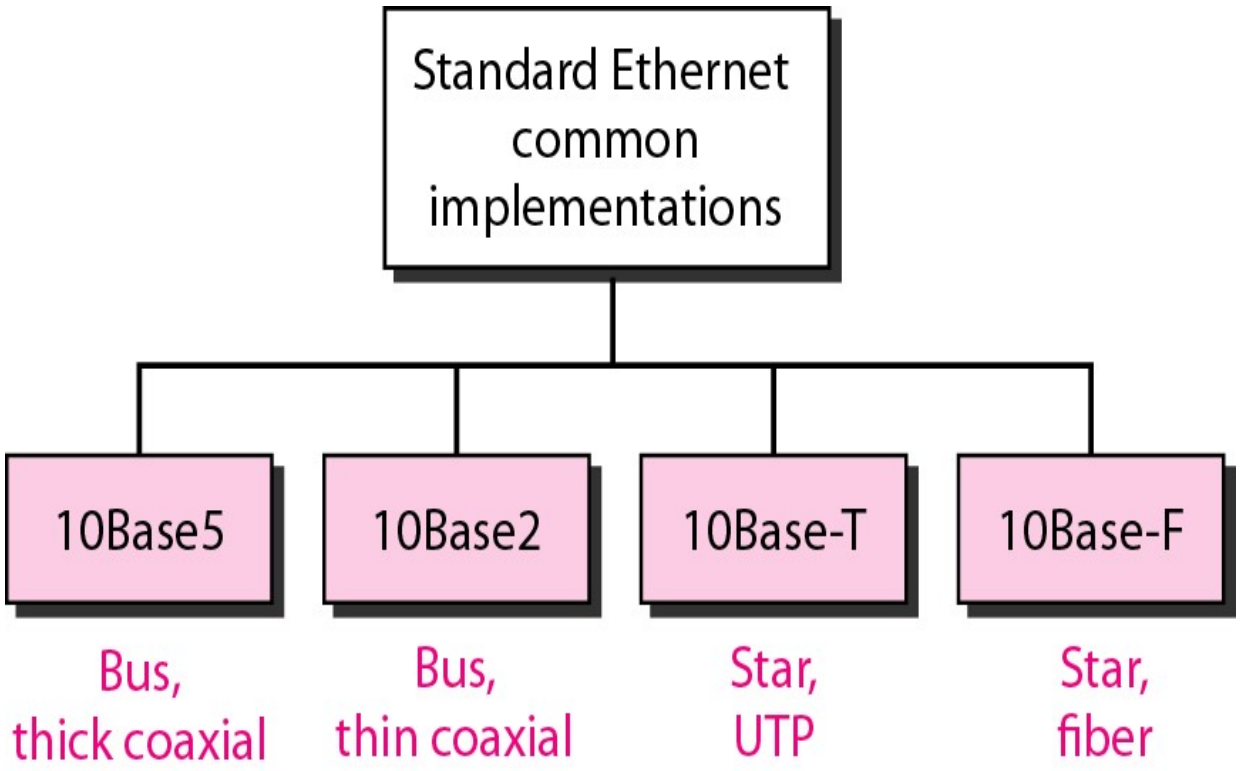
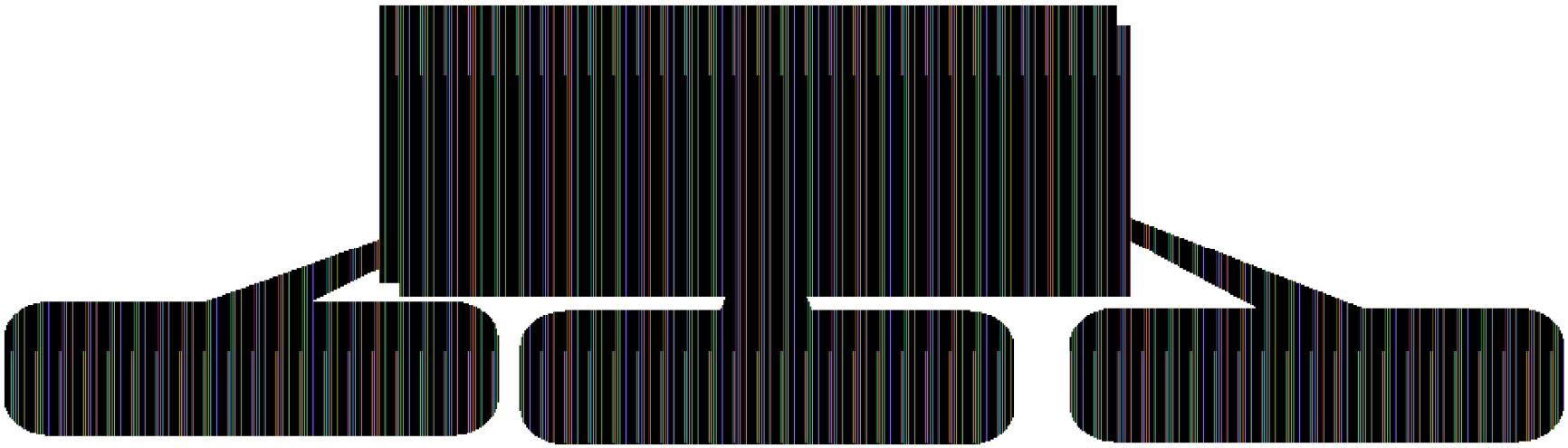


Figure 12-9



The **transceiver** is responsible for transmitting, receiving, and detecting collisions.

The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.

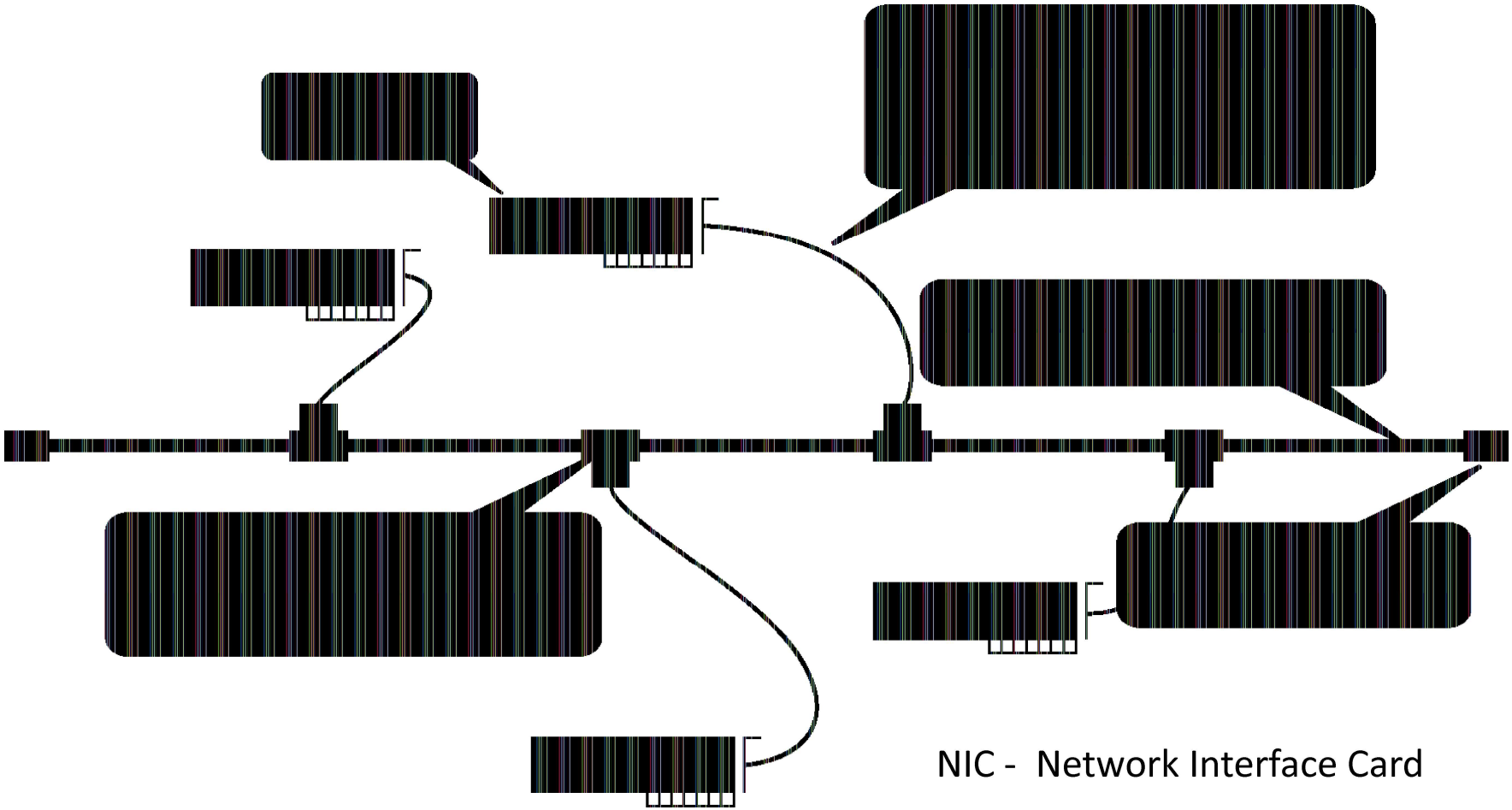
The maximum length of the coaxial cable must not exceed *500 m, otherwise, there* is excessive degradation of the signal. If a length of more than *500 m is needed, up to* five segments, each a maximum of 500-meter, can be connected using repeaters.

NIC - Network Interface Card

The NIC fits inside the station and provides the station with a link-layer address.

Figure 12-9-continued

10BASE5



NIC - Network Interface Card

Figure 12-11

- The second implementation is called lOBase2, **thin Ethernet, or Cheapernet.**
- **lOBase2** also uses a bus topology, but the cable is much thinner and more flexible.
- The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.
- Note that the collision here occurs in the thin coaxial cable. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed *185 m (close to 200 m) due to the high level of attenuation in thin coaxial* cable.

Figure 12-11-continued

10BASE2

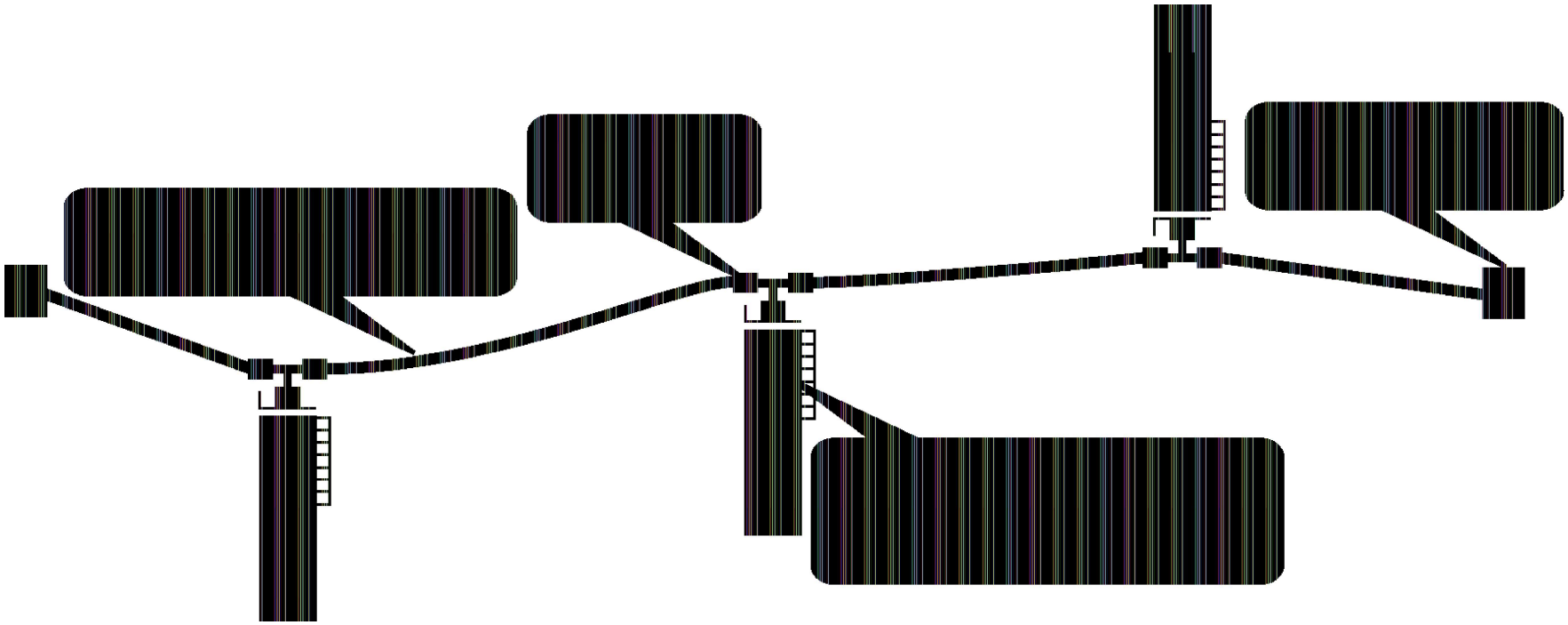
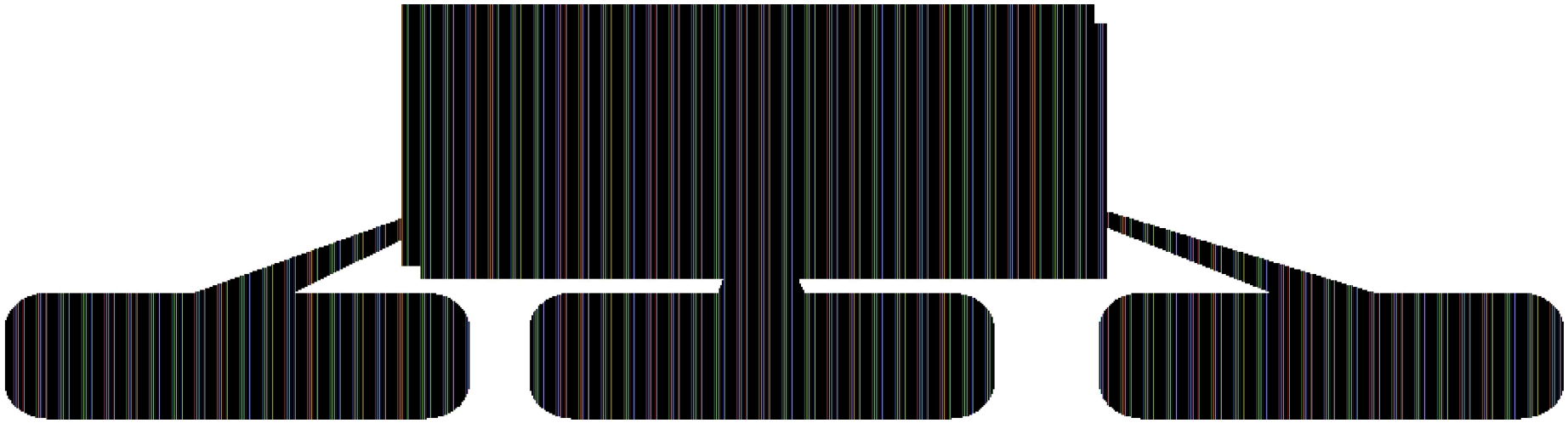
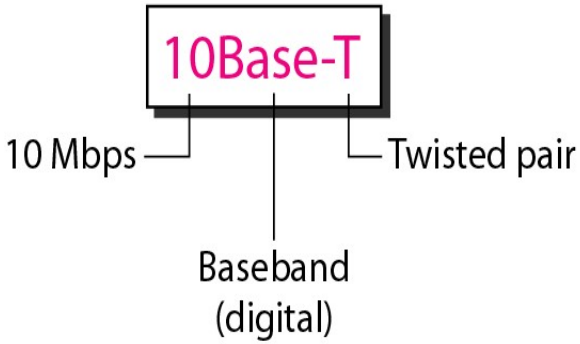
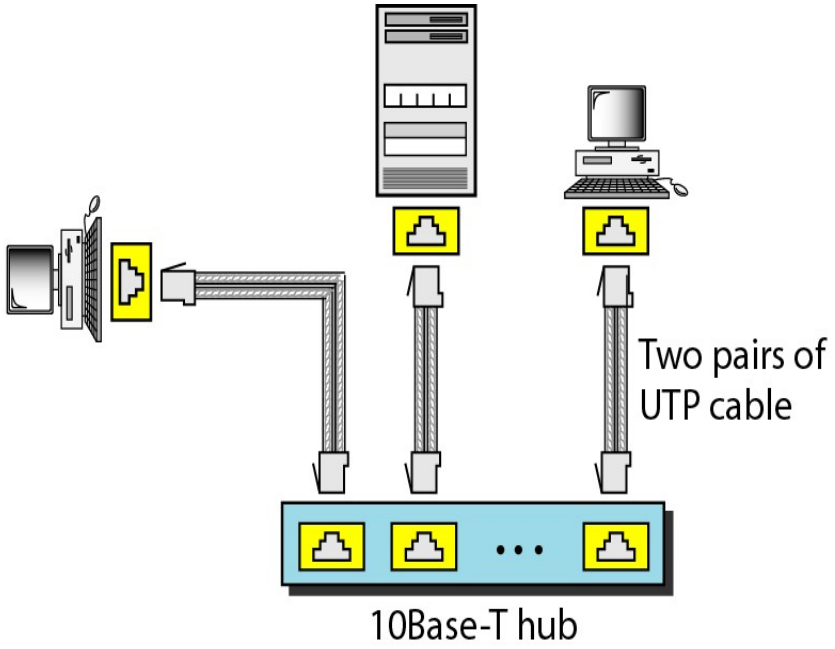


Figure 12-12



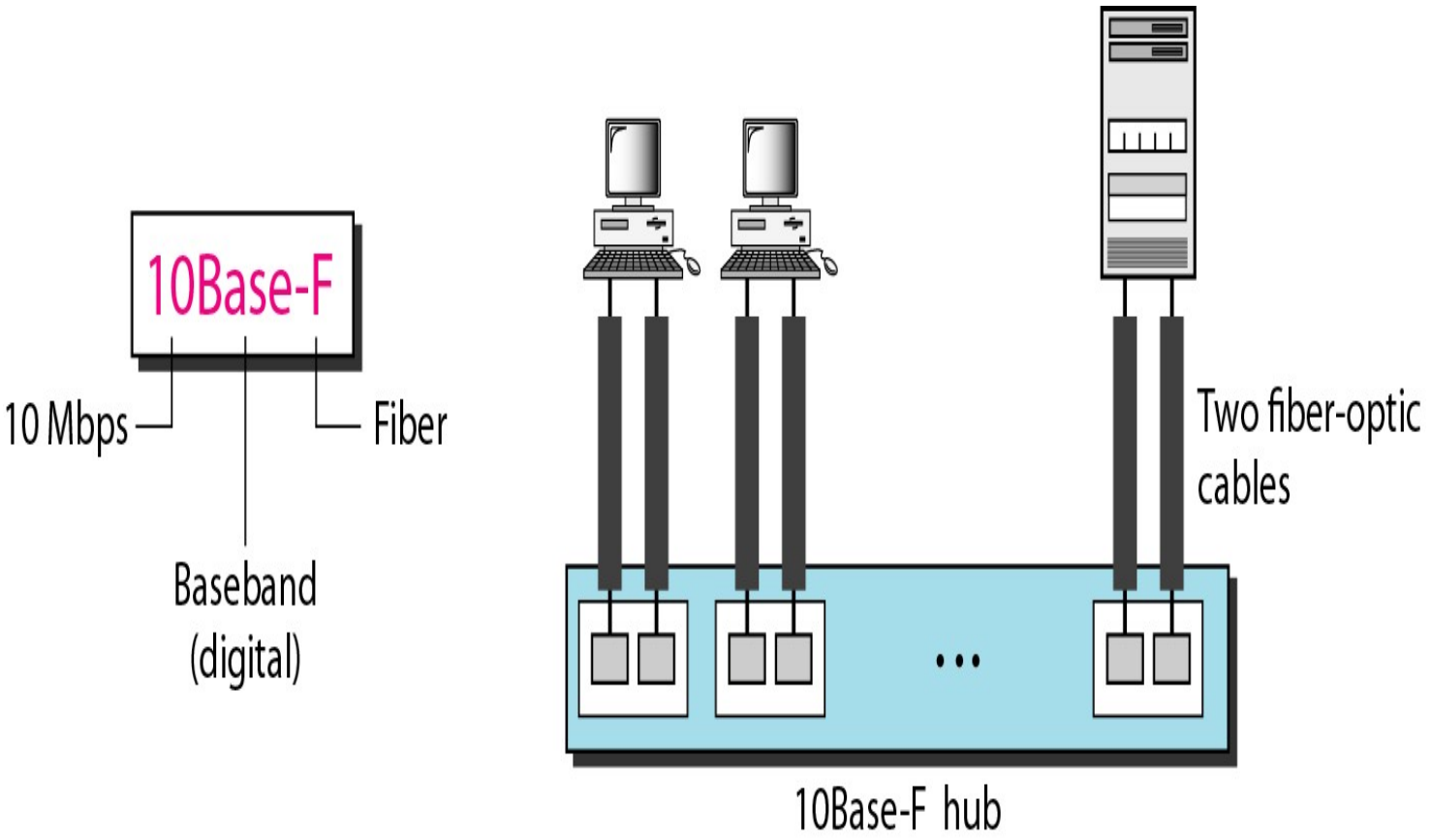
- The third implementation is called lOBase-T or twisted-pair Ethernet. 1OBase-T uses a physical star topology.
- The stations are connected to a hub via two pairs of twisted cable
- Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub.


10Base-T
10 Mbps
Twisted pair
Baseband
(digital)


Two pairs of
UTP cable
10Base-T hub

10BASE -F

- Although there are several types of optical fiber lO-Mbps Ethernet, the most common is called 10Base-F.
- lOBase-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables


10Base-F
10 Mbps
Fiber
Baseband
(digital)
Two fiber-optic
cables
10Base-F hub

Name	Cable	Max. seg.	Nodes/seg.	Adv
10Base5	Thick coax	500 m	100	Original cab
10Base2	Thin coax	185 m	30	No hub nee
10Base-T	Twisted pair	100 m	1024	Cheapest sy

Fast Ethernet

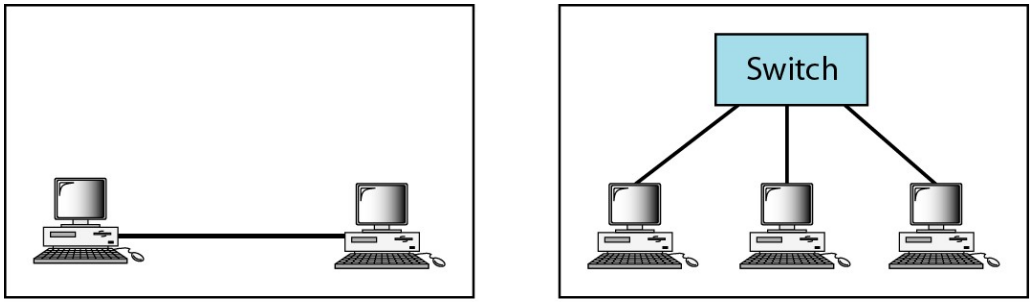
- Under the name of IEEE 802.3u
  - Upgrade the data rate to 100 Mbps
  - Make it compatible with Standard Ethernet
  - Keep the same 48-bit address and the same frame format
  - Keep the same min. and max. frame length

- MAC Sublayer
  - CSMA/CD for the half-duplex approach
  - No need for CSMA/CD for full-duplex Fast Ethernet

- Autonegotiation: allow two devices to negotiate the mode or data rate of operation

Fast Ethernet: Physical Layer

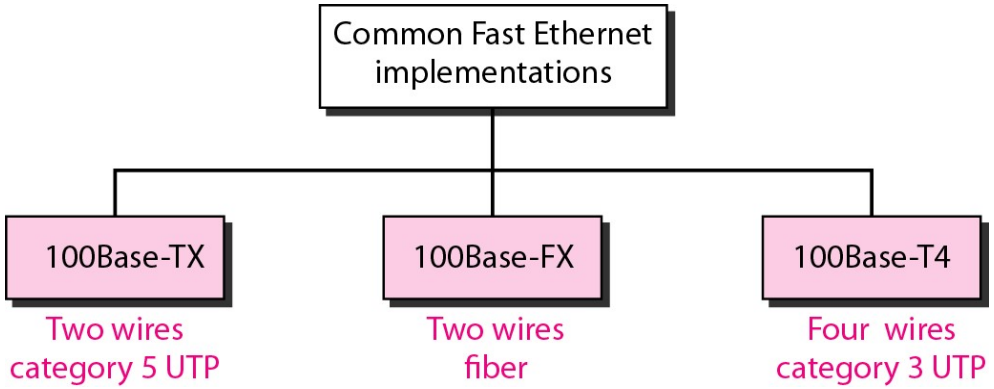
- Topology



a. Point-to-point

b. Star

- Implementation

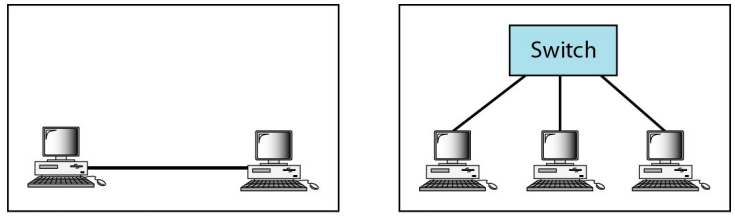


Gigabit Ethernet

- Under the name of IEEE 802.3z
  - Upgrade the data rate to 1 Gbps
  - Make it compatible with Standard or Fast Ethernet
  - Keep the same 48-bit address and the same frame format
  - Keep the same min. and max. frame length
  - Support autonegotiation as defined in Fast Ethernet
- MAC Sublayer
  - Most of all implementations follows full-duplex approach
  - In the full-duplex mode of Gigabit Ethernet, there is no collision; the maximum length of the cable is determined by the signal attenuation in the cable.
- Half-duplex mode (very rare)
  - Traditional: 0.512 μs (25m)
  - Carrier Extension: 512 bytes (4096 bits) min. length
  - Frame bursting to improve the inefficiency of carrier extension

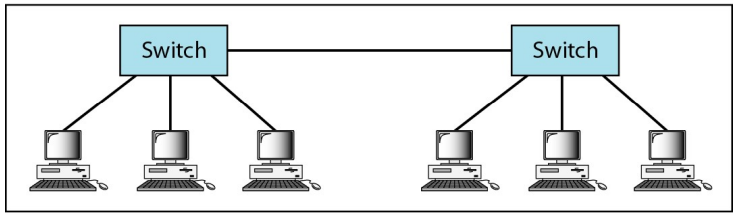
Gigabit Ethernet: Physical Layer

- Topology

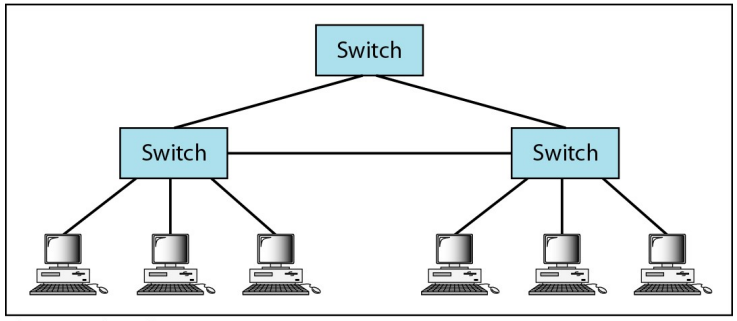


a. Point-to-point

b. Star



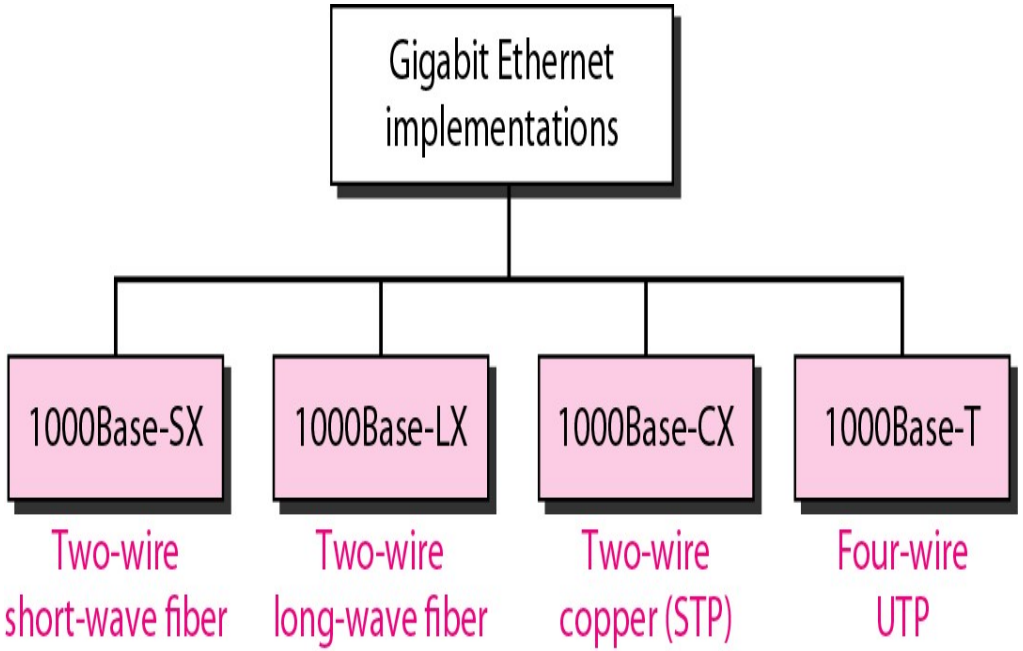
c. Two stars



d. Hierarchy of stars

Gigabit Ethernet: Physical Layer

- Implementation



Gigabit Ethernet: Summary

Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Ten-Gigabit Ethernet

- Under the name of IEEE 802.3ae
  - Upgrade the data rate to 10 Gbps
  - Make it compatible with Standard, Fast, and Giga Ethernet
  - Keep the same 48-bit address and the same frame format
  - Keep the same min. and max. frame length
  - Allow the interconnection of existing LANs into a MAN or WAN
  - Make Ethernet compatible with Frame Relay and ATM

- MAC Sublayer: Only in full-duplex mode → no CSMA/CD

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

WIRELESS LANS

IEEE 802.11 : WIRELESS LANS

- The transmission techniques:

  - Infrared

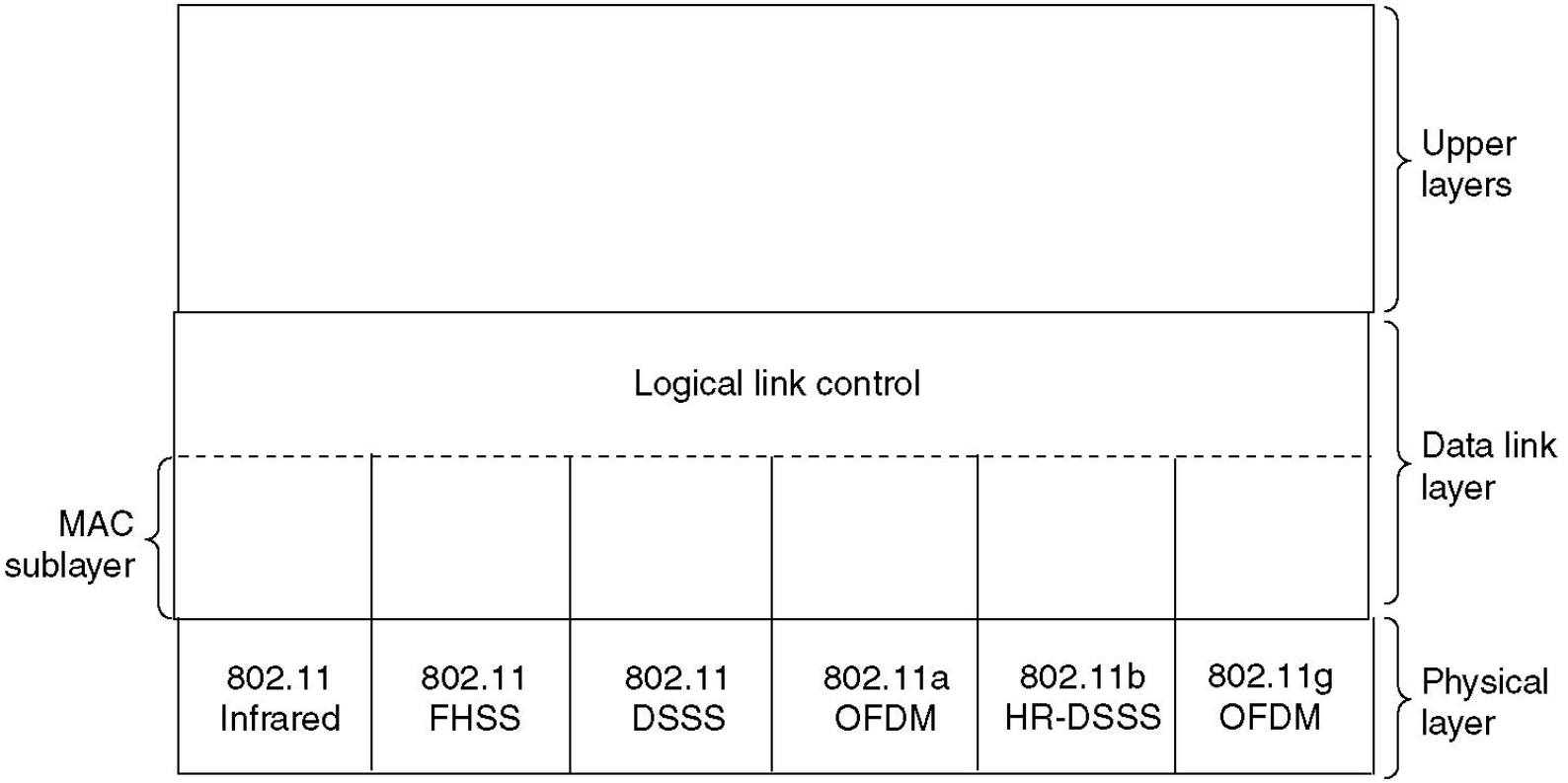
  -FHSS (Frequency Hopping Spread Spectrum)

  -DSSS (Direct Sequence Spread Spectrum).

  -OFDM (Orthogonal Frequency Division Multiplexing)

  - HR-DSS (High Rate Direct Sequence Spread Spectrum)

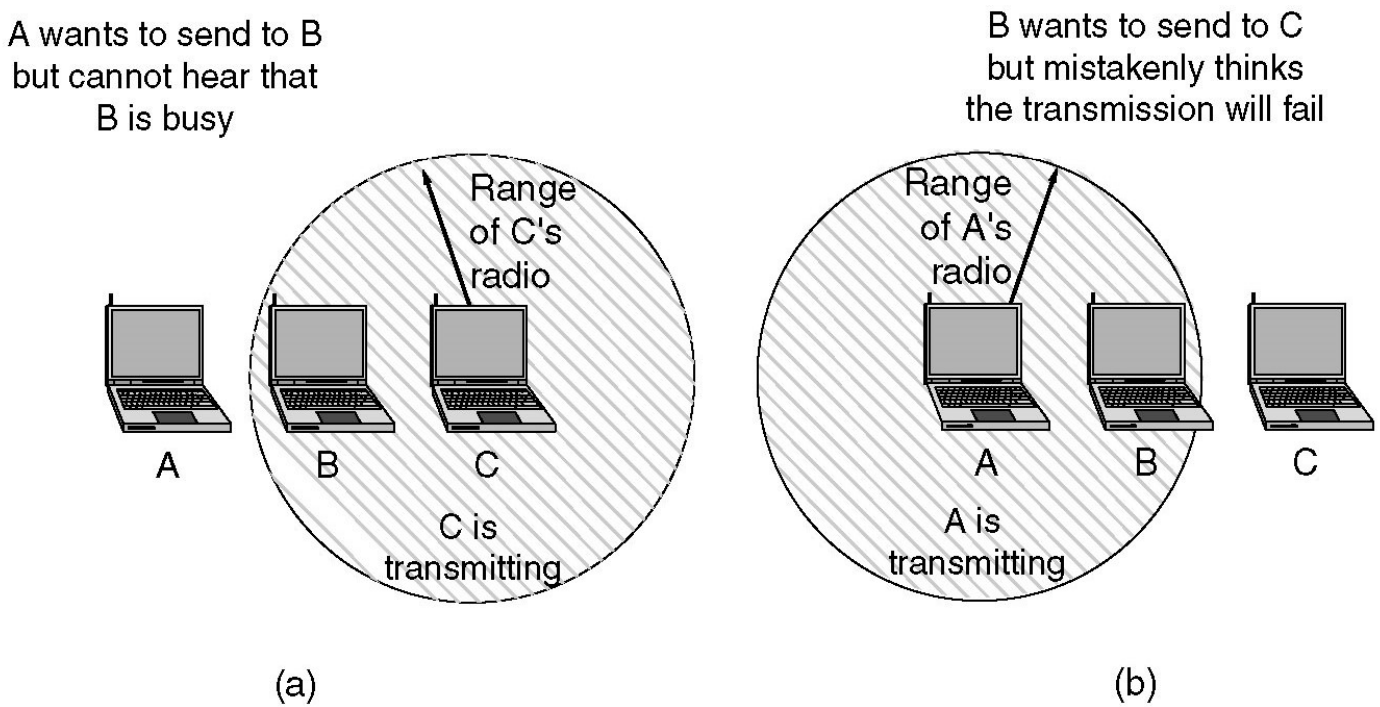
The 802.11 Protocol Stack



The 802.11 MAC Sublayer Protocol

(a) The hidden station problem.

(b) The exposed station problem.



Hidden Station Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- C transmits to B.
- If A "*senses*" the channel, it will not hear C's transmission and falsely conclude that A can begin a transmission to B.

Exposed station Problem

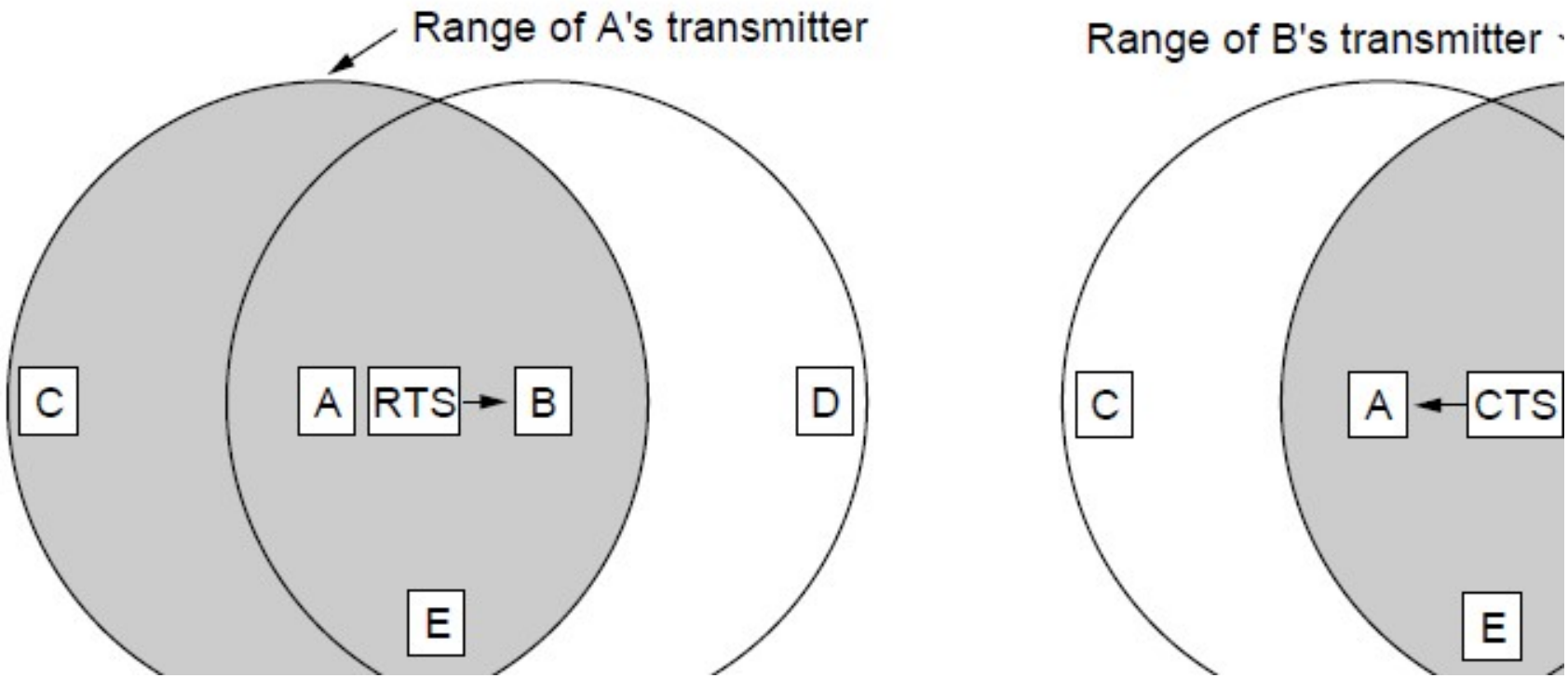
- This is the inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A’s transmission, B falsely assumes that it cannot send to C.

Wireless LAN Protocols

- *MACA* (Medium Access with Collision Avoidance)
- *MACAW*(Medium Access with Collision Avoidance for Wireless)

Wireless LAN Protocols

- ***MACA*** (Medium Access with Collision Avoidance) protocol solved hidden and exposed terminal problems:
  - Sender broadcasts a Request-to-Send (***RTS***) and the intended receiver sends a Clear-to-Send (***CTS***).
  - Upon receipt of a ***CTS,*** the sender begins transmission of the frame.
  - RTS, CTS helps determine who else is in range or busy (Collision Avoidance).
  - Can a collision still occur?



The MACA protocol. (a) *A sending an RTS to B. (b) B responding* with a CTS to *A.*

Wireless LAN Protocols

- MACA protocol is fine tuned to improve the performance and new protocol is renamed as **MACAW** (**MACA for Wireless**)
- MACAW - new features
  - added ACKs,
  - Carrier Sense and
  - Back off algorithm runs for every stream and **not** per station.

- These changes improved the fairness of the protocol.

THE 802.11 MAC SUBLAYER PROTOCOL

- 802.11 Supports 2 modes of operations to deal with problems.
- The two modes are :

  * DCF (Distributed Coordination Function)

    -does not use any kind of central control

  * PCF(Point Coordination Function)

    -uses the base station to control all activity in its cell.

Distribute Coordination Function (DCF)

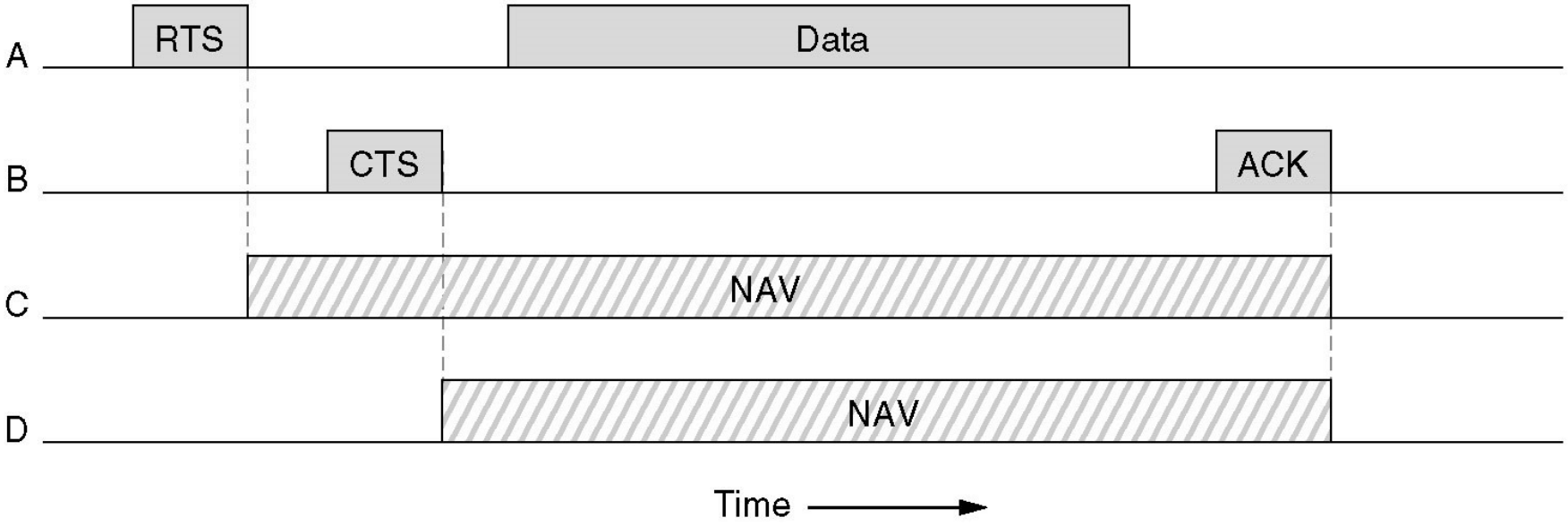
- Uses *CSMA/CA* (*CSMA* with *C*ollision *A*voidance).
  - Uses one of two modes of operation:
    - ***virtual carrier sensing***
    - physical carrier sensing
- The two methods are supported:

1. ***MACAW*** **(Multiple Access with Collision Avoidance for Wireless) with virtual carrier sensing.**
2. **1-persistent physical carrier sensing.**

1-Persistent Physical Carrier Sensing

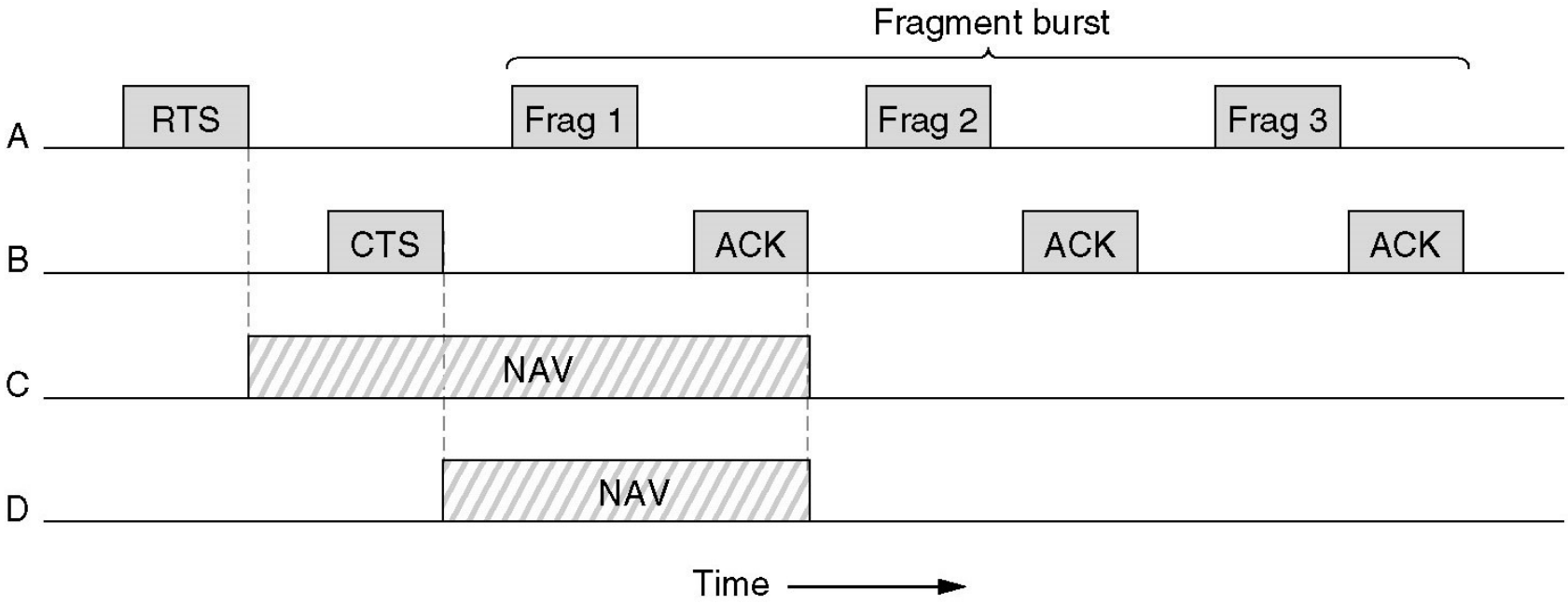
- The station **senses** the channel when it wants to send.
- If idle, the station transmits.
  - *A station does not sense the channel while transmitting.*
- If the channel is busy, the station defers until idle and then transmits (1-persistent).
- Upon collision, wait a *random time* using binary exponential backoff algorithm.

Virtual Channel Sensing in CSMA/CA



- In this example, *A* wants to send to *B*. C is a station within range of *A* (and possibly within range of *B*, but that does not matter). *D* is a station within range of *B* but not within range of *A*.
- C (in range of A) *receives the RTS and based on information in RTS creates a* ***virtual channel busy*** **NAV(Network Allocation Vector).**
- D (in range of B) *receives the CTS and creates a shorter* **NAV.**

Fragmentation in 802.11



- High wireless error rates ➔ long packets have less probability of being successfully transmitted.
- Solution: MAC layer fragmentation with stop-and-wait protocol on the fragments.

- To deal with the problem of noisy channels, 802.11 allows frames to be fragmented into smaller pieces, each with its own checksum.
- The fragments are individually numbered and acknowledged using a stop-and-wait protocol (i.e., the sender may not transmit fragment *k +*1 until it has received the acknowledgment for fragment *k).*
- *Once the channel has been* acquired using RTS and CTS, multiple fragments can be sent in a row, sequence of fragments is called a **fragment burst.**
- The NAV mechanism keeps other stations quiet only until the next acknowledgement

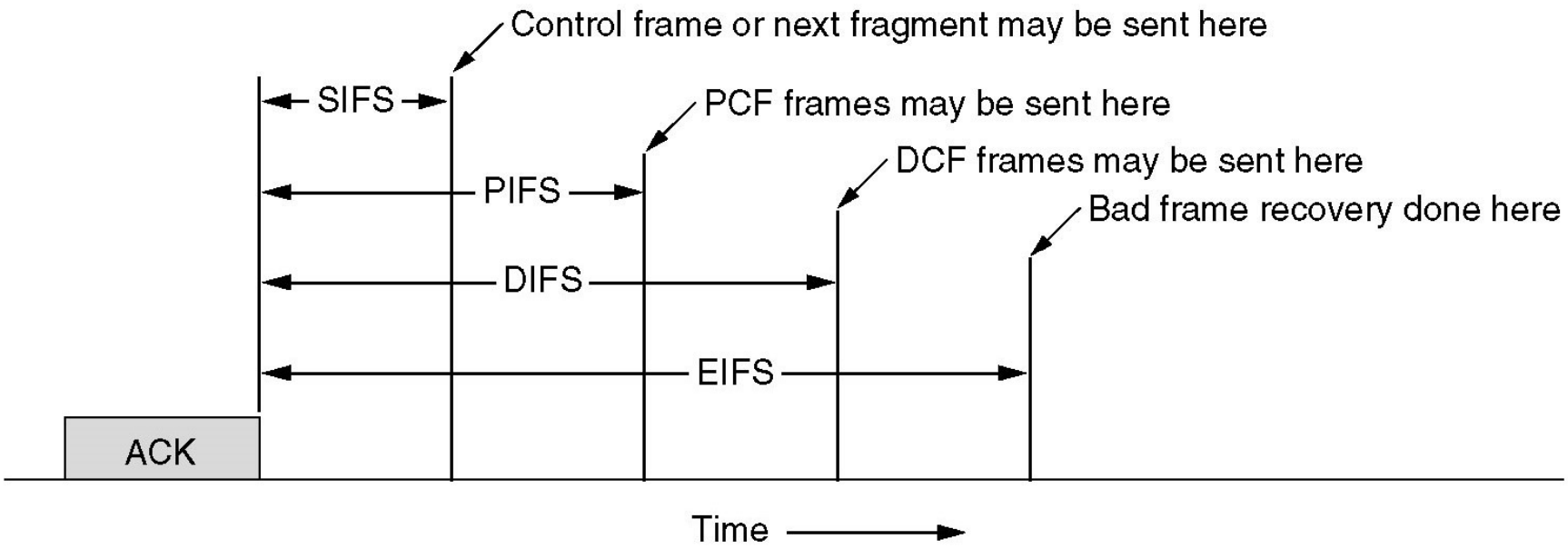
PCF(Point Coordination Function)

- PCF mechanism uses **base station to control all activity** in its cell.
- Base station polls the other station asking them if they have any frame to send.
- In PCF, as it is centralized, **no collision will occur**.
- In polling mechanism, the base station broadcasts a **beacon frame periodically (10 to 100 times per second).**
- Base station can tell another station to ***sleep*** to save on batteries and base stations holds frames for sleeping station.

DCF and PCF Co-Existence

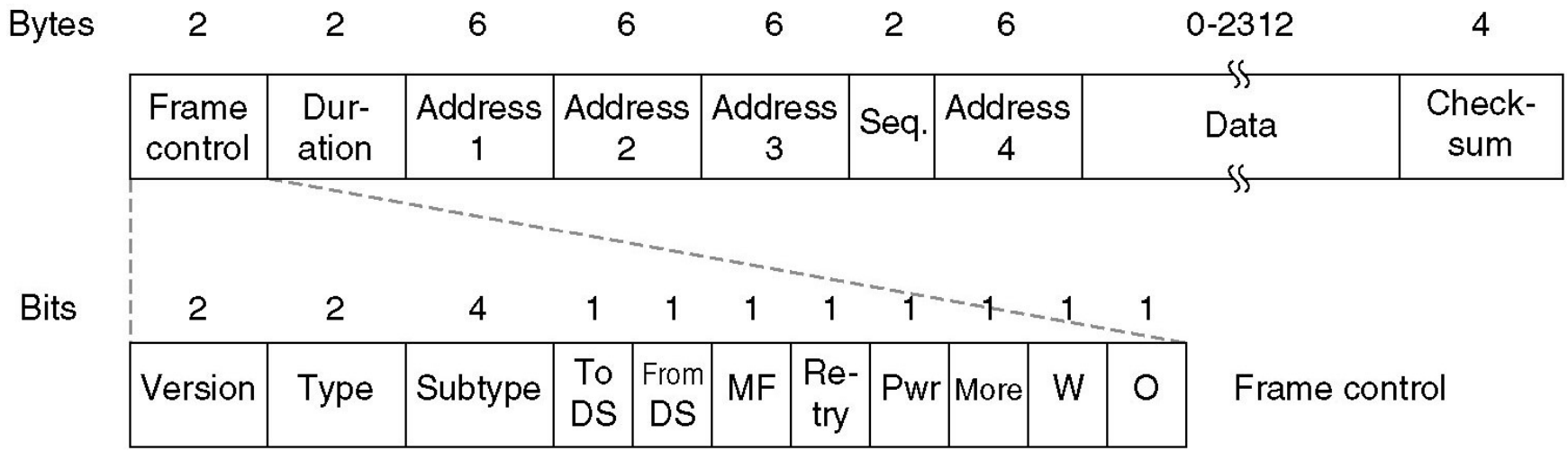
- Distributed and centralized control can co-exist using InterFrame Spacing.
- SIFS (Short IFS) :: is the time waited between packets in an ongoing dialog (RTS,CTS,data, ACK, next frame)
- PIFS (PCF IFS) :: when no SIFS response, base station can issue beacon or poll.
- DIFS (DCF IFS) :: when no PIFS, any station can attempt to acquire the channel.
- EIFS (Extended IFS) :: lowest priority interval used to report bad or unknown frame.

Interframe Spacing in 802.11.



The 802.11 Frame Structure

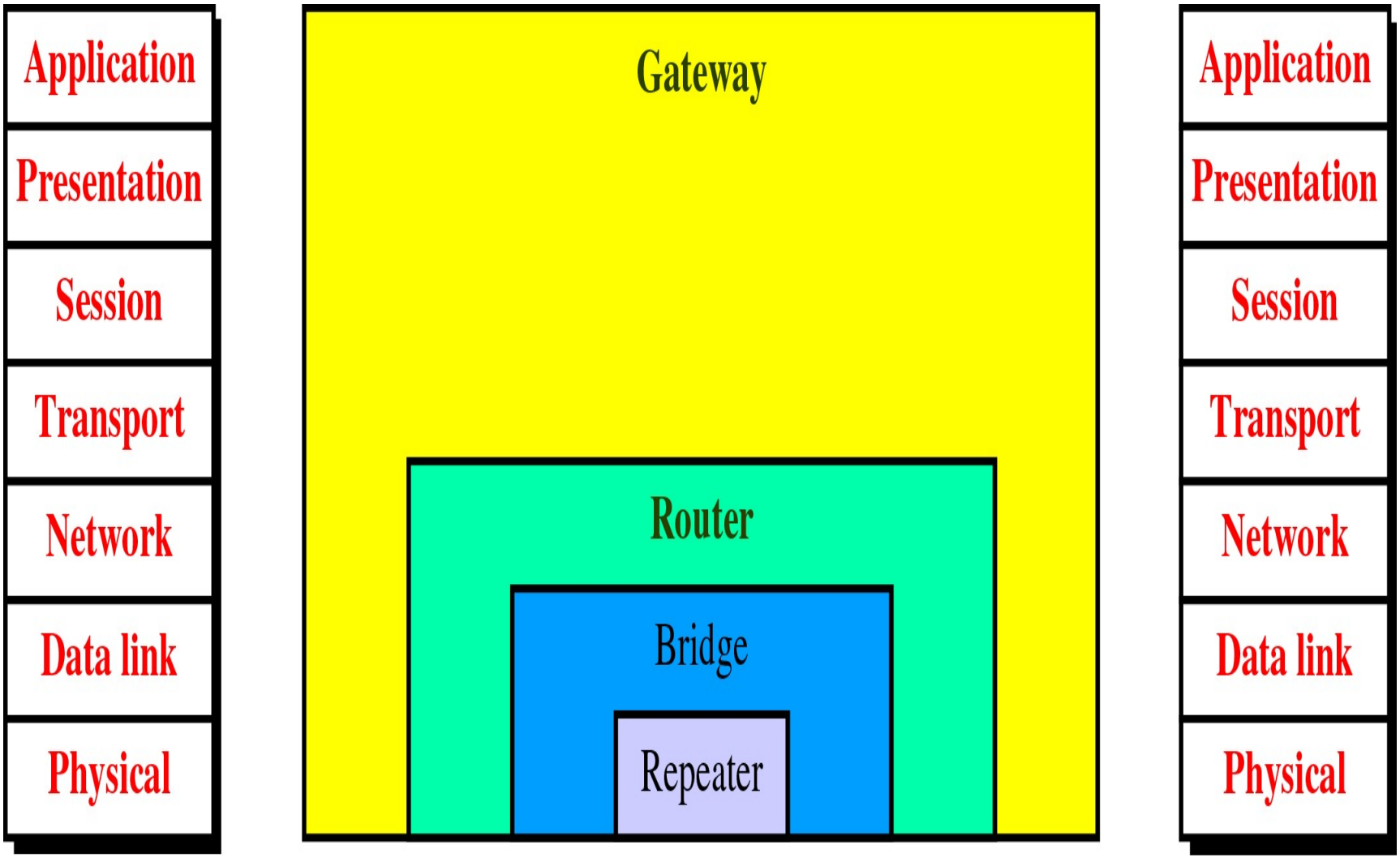
- The 802.11 data frame.



- First comes the *Frame Control field. It* itself has 11 subfields. The first of these is the *Protocol version, which allows two versions of* the protocol to operate at the same time in the same cell.
- Then come the *Type (data, control,*or management) and *Subtype fields (e.g., RTS or CTS). The To DS and From DS bits indicate* the frame is going to or coming from the intercell distribution system (e.g., Ethernet).
- The *MF* bit means that more fragments will follow. The *Retry bit marks a retransmission of a frame* sent earlier. The *Power management bit is used by the base station to put the receiver into* sleep state or take it out of sleep state. The *More bit indicates that the sender has additional* frames for the receiver.
- The *W bit specifies that the frame body has been encrypted using the* **WEP (Wired Equivalent Privacy) algorithm. Finally, the *O bit tells the receiver that a*** sequence of frames with this bit on must be processed strictly in order.

- The second field of the data frame, the *Duration field, tells how long the frame and its* acknowledgement will occupy the channel. his field is also present in the control frames and is how other stations manage the NAV mechanism.
- The frame header contains four addresses, all in standard IEEE 802 format. The source and destination are obviously needed. The other two addresses are used for the source and destination base stations for intercell traffic.
- The *Sequence field allows fragments to be numbered. Of the 16 bits available, 12 identify the* frame and 4 identify the fragment. The *Data field contains the payload, up to 2312 bytes,* followed by the usual *Checksum.*

Connecting Devices and the OSI Model

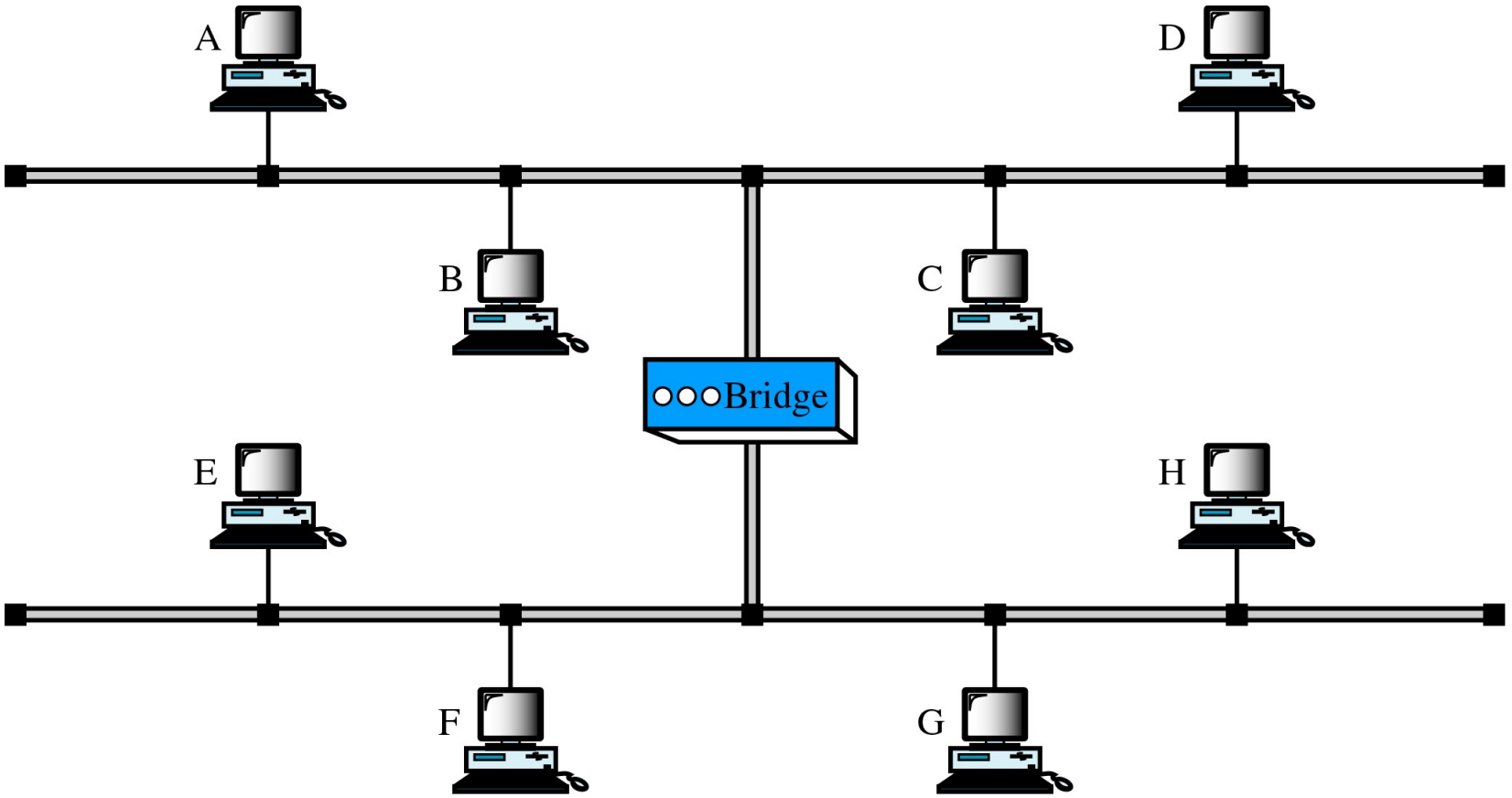


Bridges and its types

- LANs can be connected by devices called **bridges**
- A bridge operates in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame

Figure 21-7

A Bridge

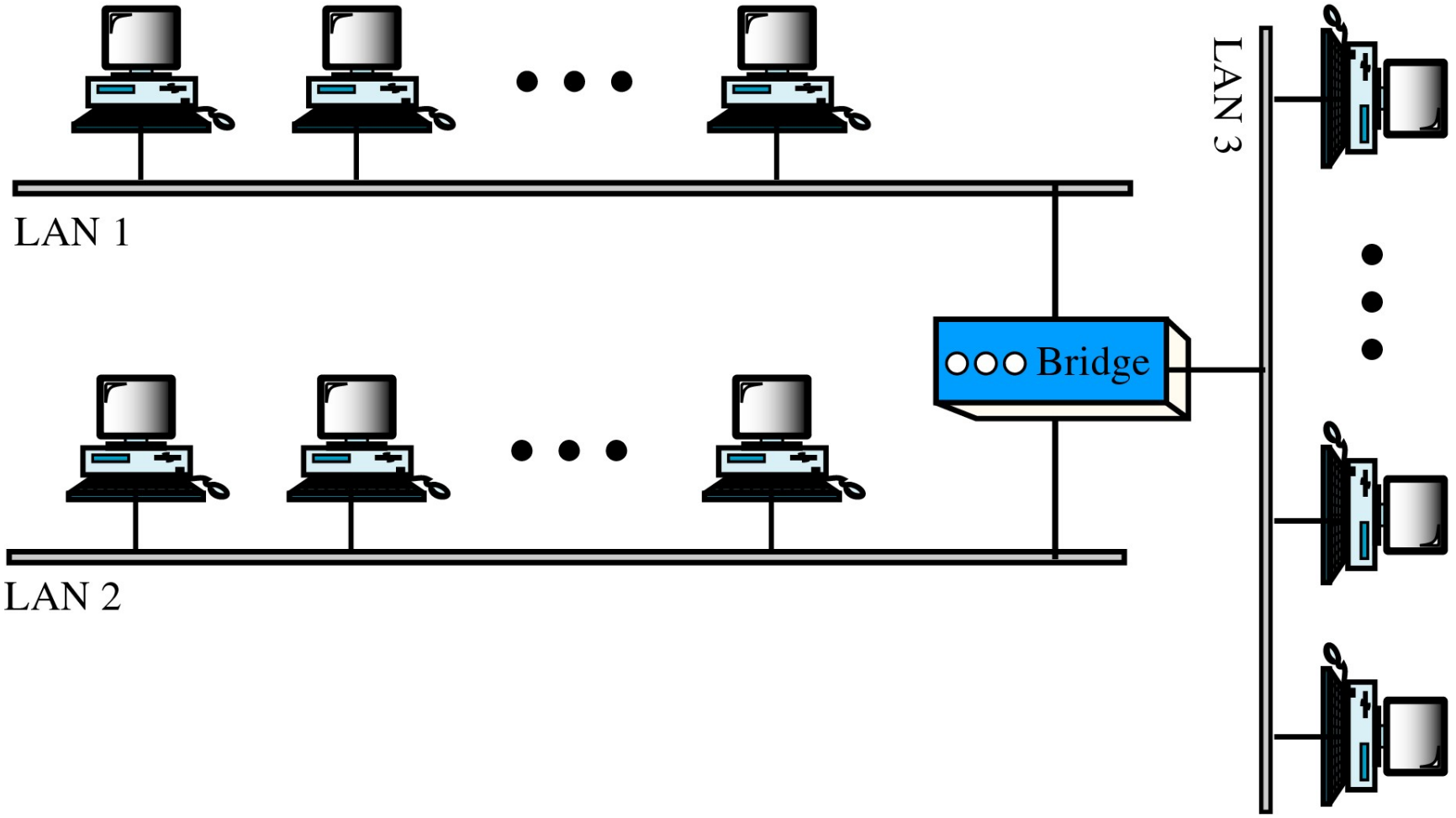


A bridge connecting two LANs

A bridge does not change the physical (MAC) addresses in a frame.

Figure 21-9

Multiport Bridge



- Filtering:
  - A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
  - If the frame is to be forwarded, the decision must specify the port.
  - A bridge has a table that maps addresses to ports.

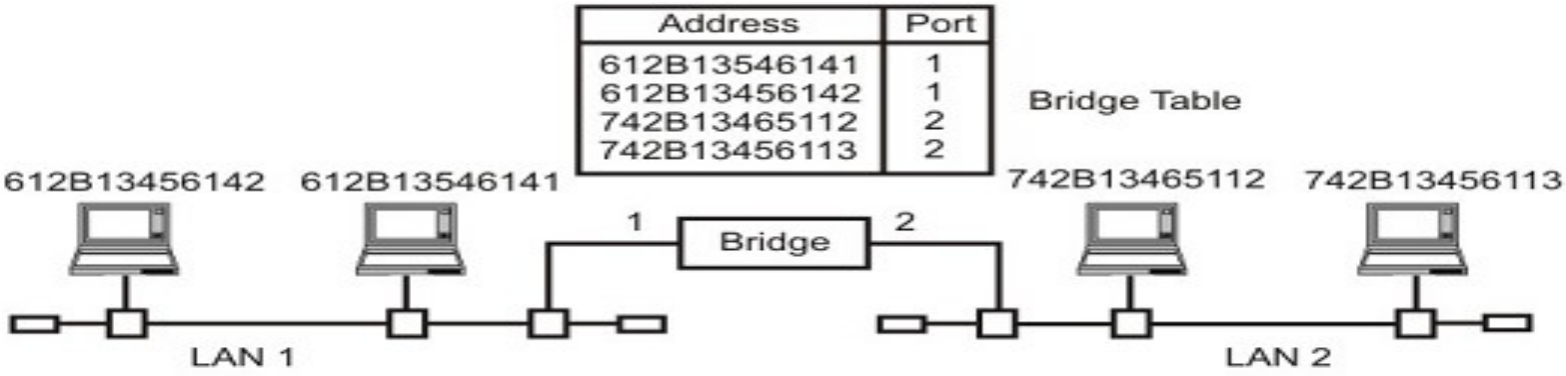


Figure 6.1.4 A bridge connecting two separate LANs

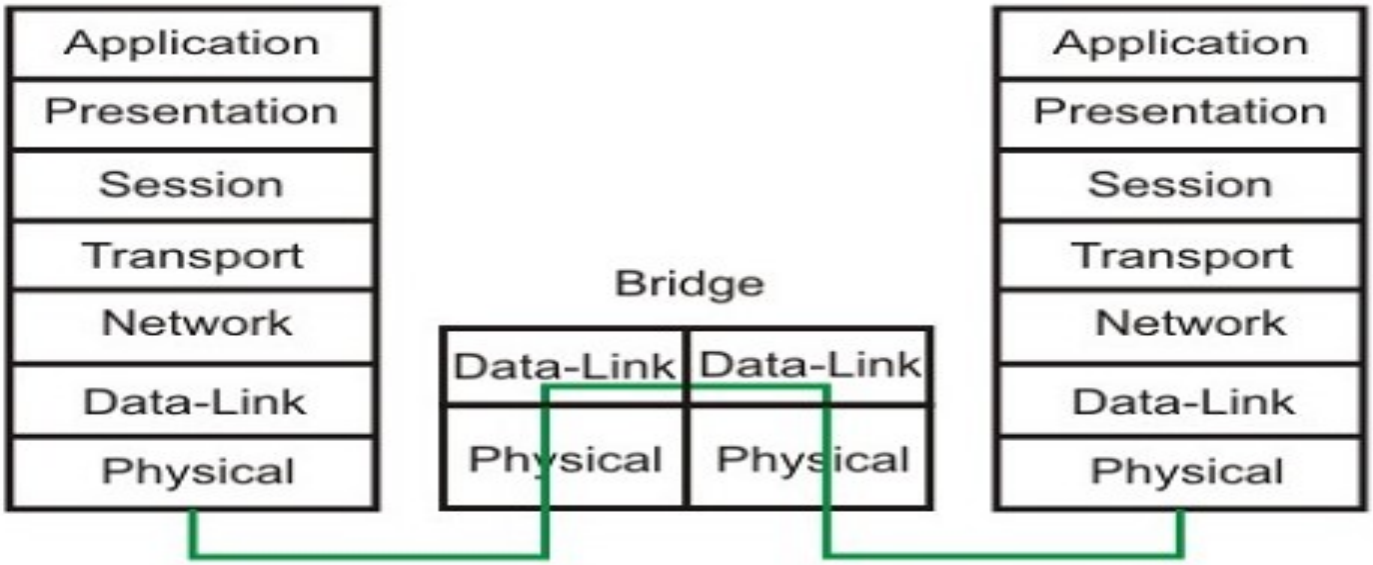


Figure 6.1.5 Information flow through a bridge

Types of Bridges:

- Transparent Bridges.
- Source Routing Bridges.

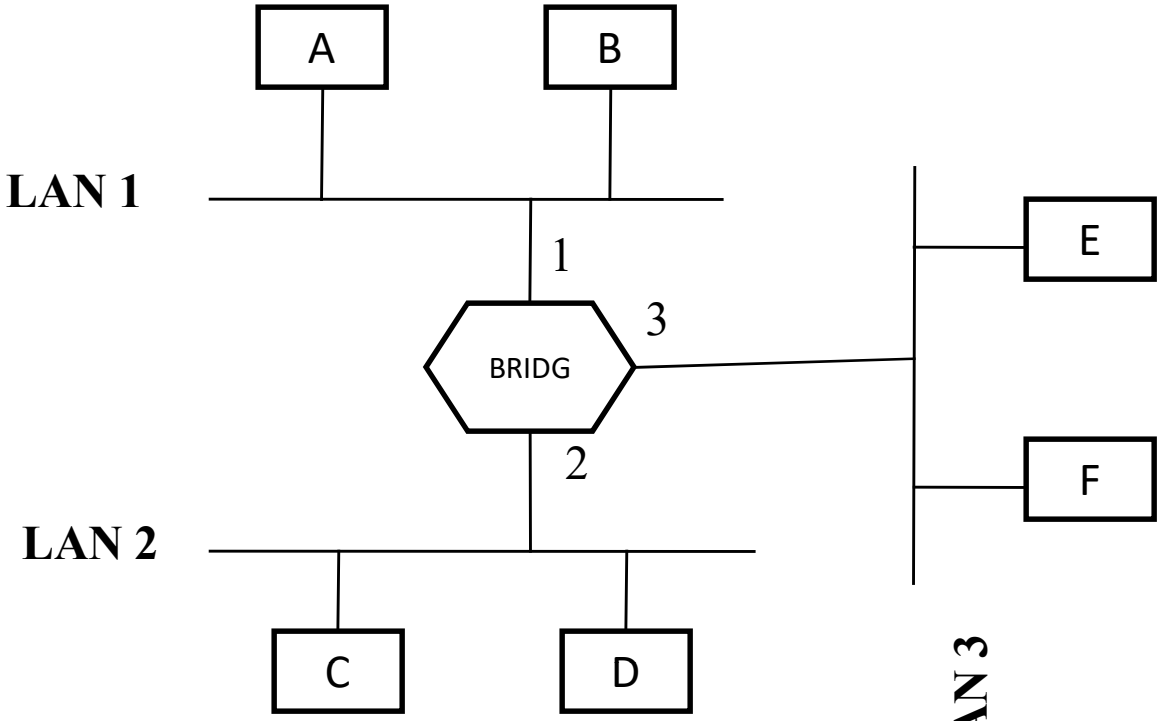
Transparent Bridges

- A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence.
- If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary.
- Basic Function:
  - Forwarding: Frames must be forwarded from one station to another.
  - Learning: The forwarding table is automatically made by learning frame movements in the network.
  - Prevention of Looping: Loops in the system must be prevented.

- Forwarding - 3 **rules** for forwarding the frame.
  - If destination and source LANs are the same discard the frame.
  - If destination and source LANs are different , forward the frame.
  - If the destination LAN is unknown, use flooding.

Learning:

- The earliest bridges had forwarding tables that were static. If a station was added or deleted, the table had to be modified manually.
- A better solution to the static table is a dynamic table that maps addresses to ports automatically.
- To make a table dynamic, we need a bridge that gradually learns from the frame movements.
- To do this, the bridge inspects both the destination and the source addresses. The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes.



ADDRESS	PORT

(a) original

ADDRESS	PORT
A	1

(b) If A to D

ADDRESS	PORT
A	1
E	3

(c) If E to A

ADDRESS	PORT
A	1
E	3
B	1

(d) If B to C

Prevention of Looping:

- Transparent bridges work fine as long as there are no redundant bridges in the system.
- Systems administrators, however, like to have redundant bridges (more than one bridge between a pair of LANs) to make the system more reliable. If a bridge fails, another bridge takes over until the failed one is repaired or replaced.
- Redundancy can create loops in the system, which is very undesirable
- To solve the looping problem, the IEEE specification requires that bridges use the spanning tree algorithm to create a loopless topology.

Source Routing Bridges

- In source routing bridges, a sending station defines the bridges that the frame must visit.
- The addresses of these bridges are included in the frame.
- In other words, the frame contains not only the source and destination addresses, but also the addresses of all bridges to be visited.
- The source gets these bridge addresses through the exchange of special frames with the destination prior to sending the data frame.
- Token Ring networks mainly use source-routing bridges.