Module 3

Local Area Networks

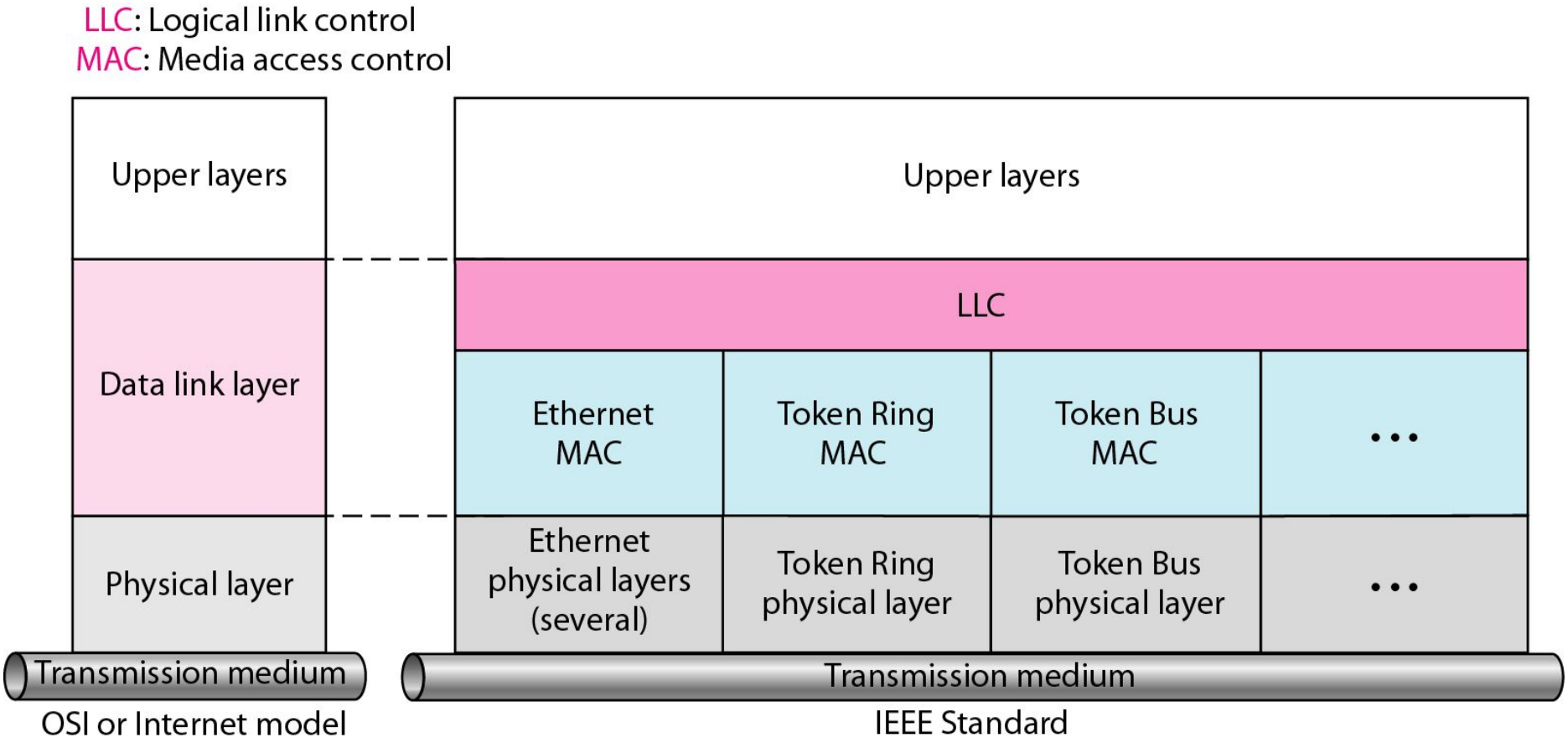
- A **local area network** (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus.
- The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN.

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.
- The standard was adopted by the **American National Standards Institute** (ANSI).
- In 1987, the **International Organization for Standardization** (ISO) also approved it as an international standard under the designation ISO 8802.

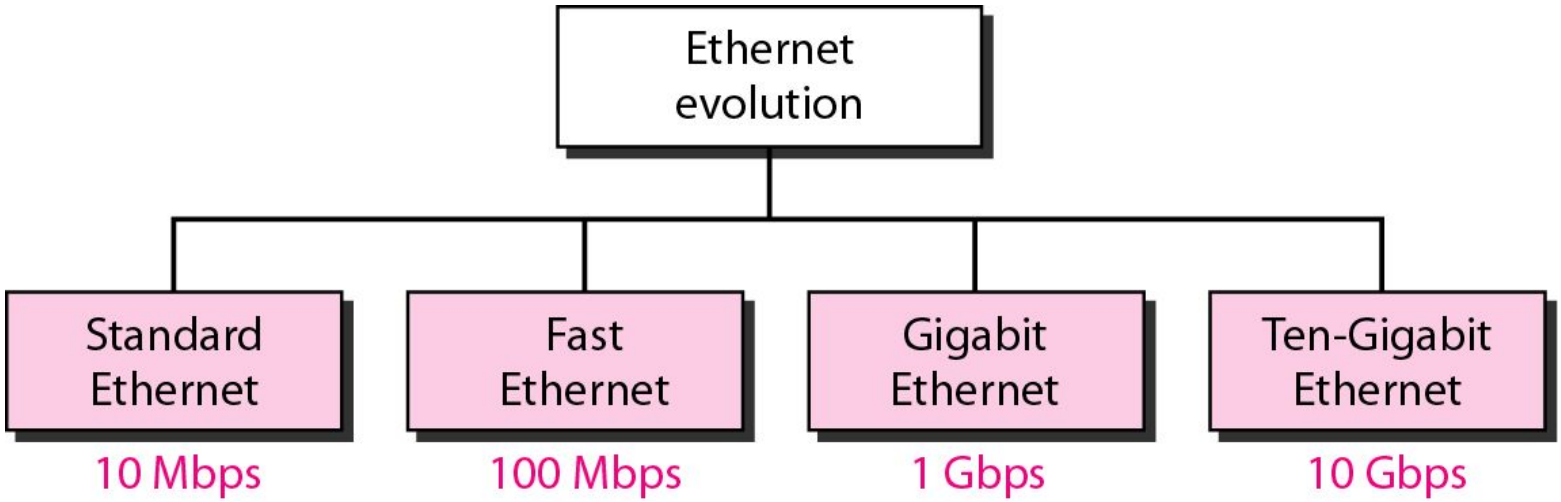
Relationship of the 802 Standard to the traditional OSI model

- The IEEE has subdivided the data link layer into two sublayers:
  - logical link control (LLC) and media access control (MAC).
- IEEE has also created several physical layer standards for different LAN protocols.



STANDARD ETHERNET

- The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC).
- The 4 standards are:



STANDARD ETHERNET

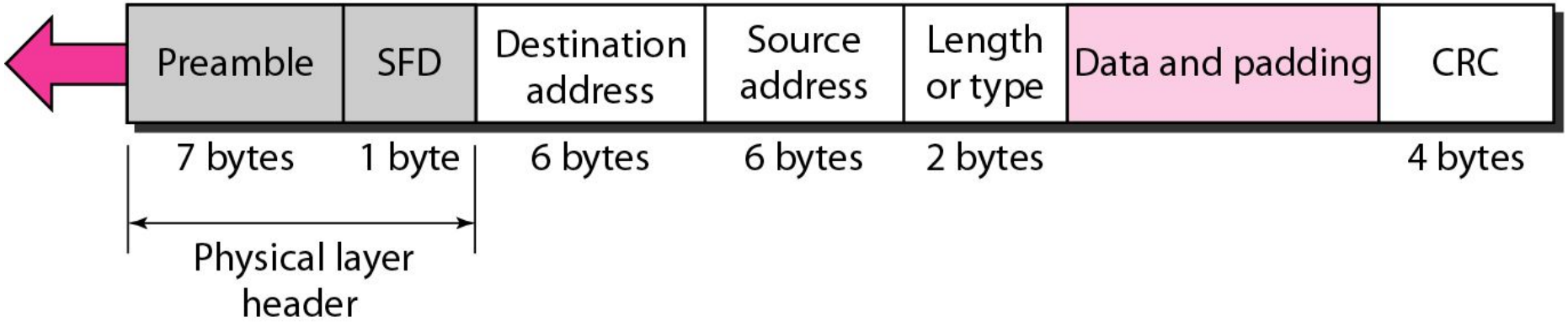
- In Standard Ethernet, the MAC sublayer governs the operation of the access method.
- It also frames data received from the upper layer and passes them to the physical layer.

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.
- Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers.

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

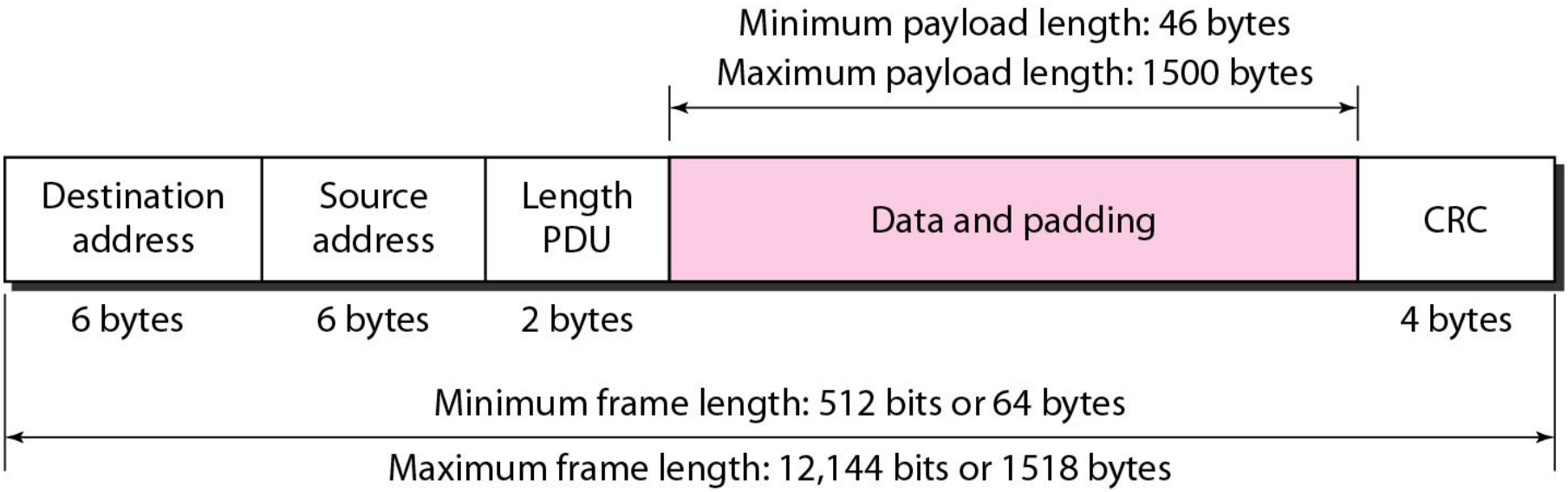
SFD: Start frame delimiter, flag (10101011)



- **Preamble:** The first field of the 802.3 frame contains **7 bytes (56 bits) of alternating 0s and 1s** that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD):** The second field (**1 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.
- **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

- The minimum length restriction is required for the correct operation of *CSMA/CD*
- An Ethernet frame needs to have **a minimum length of 512 bits or 64 bytes**. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.
- The standard defines the **maximum length of a frame** (without preamble and SFD field) as **1518 bytes**. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.



Note

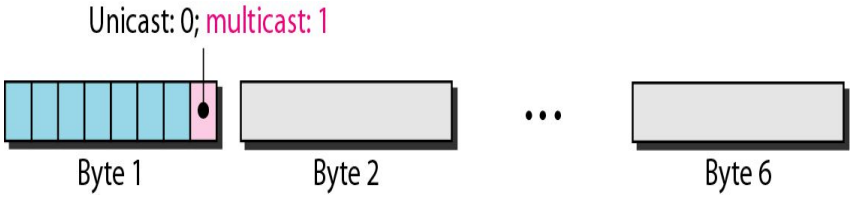
Frame length:

Minimum: 64 bytes (512 bits)

Maximum: 1518 bytes (12,144 bits)

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**.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.



Unicast, Multicast, and Broadcast Addresses

- A **source address** is always a **unicast address**-the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. If the **least significant bit of the first byte** in a **destination address** is **0,** the address is **unicast**; otherwise, it is **multicast**.
- A **unicast destination address defines only one recipient**; the relationship between the **sender and the receiver is one-to-one**.
- A **multicast destination address** defines a **group of addresses**; the relationship between the sender and the receivers is **one-to-many**.
- The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A **broadcast destination address is forty-eight 1s**.

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.

Note

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

Example

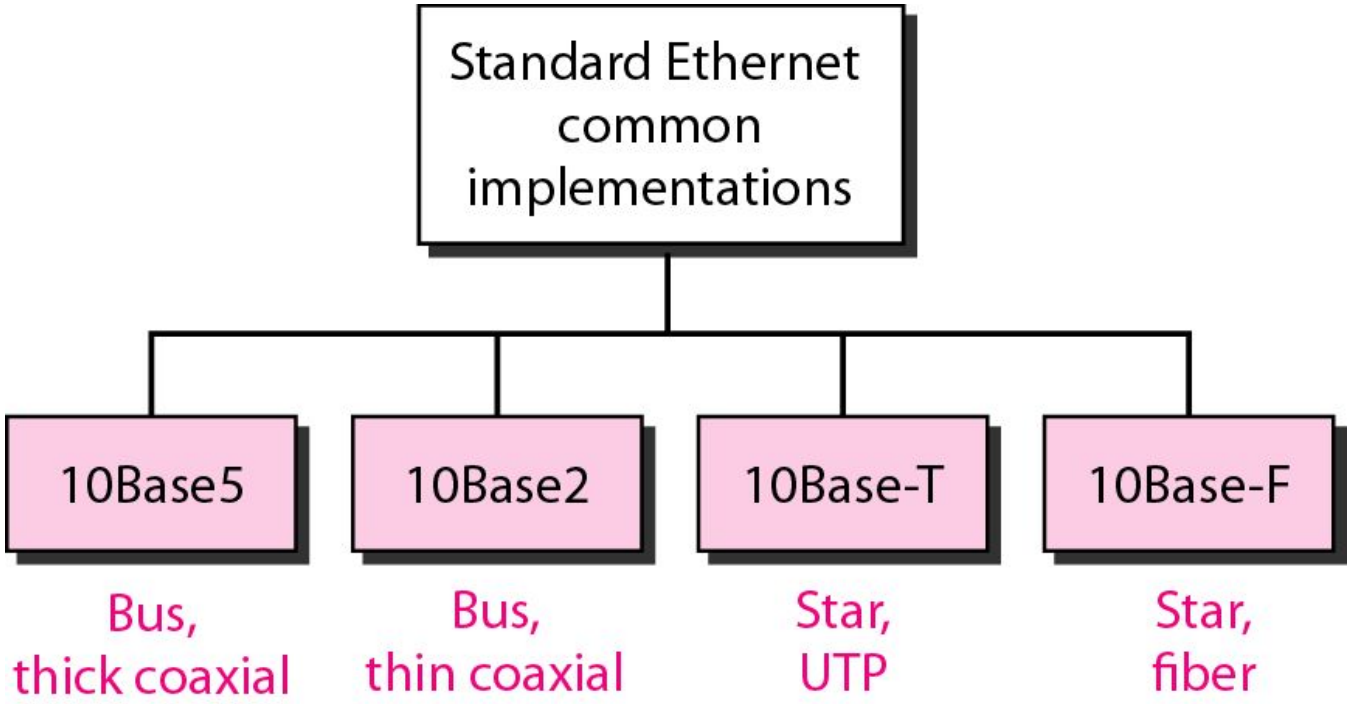
Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A

b. 47:20:1B:2E:08:ED

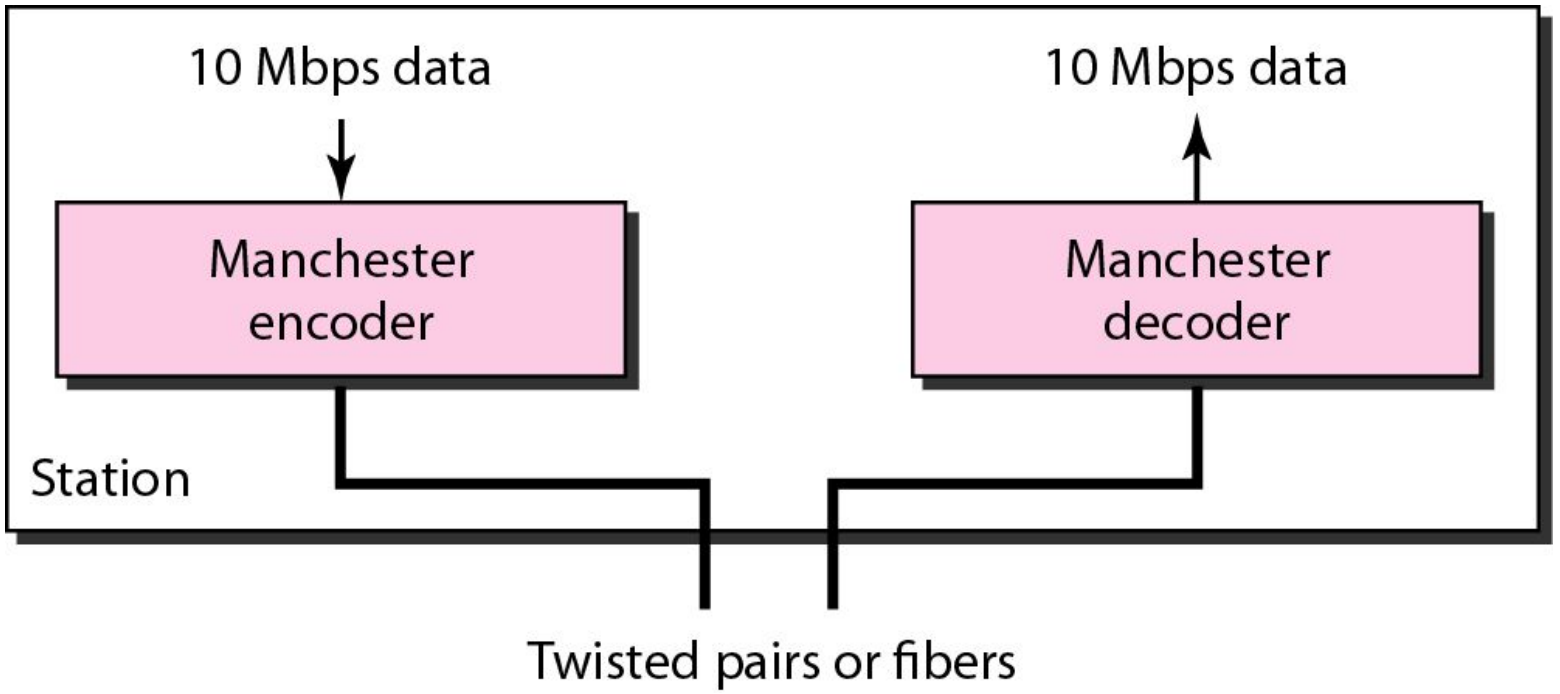
c. FF:FF:FF:FF:FF:FF

Categories of Standard Ethernet



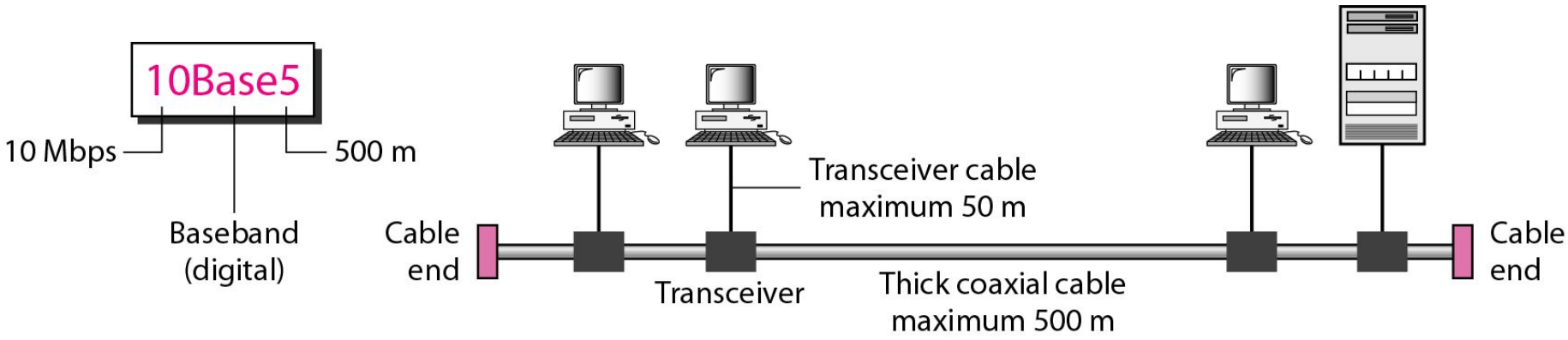
Encoding and Decoding

- All standard implementations use digital signaling (baseband) at 10 Mbps.
- At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data.
- Manchester encoding is self-synchronous, providing a transition at each bit interval.



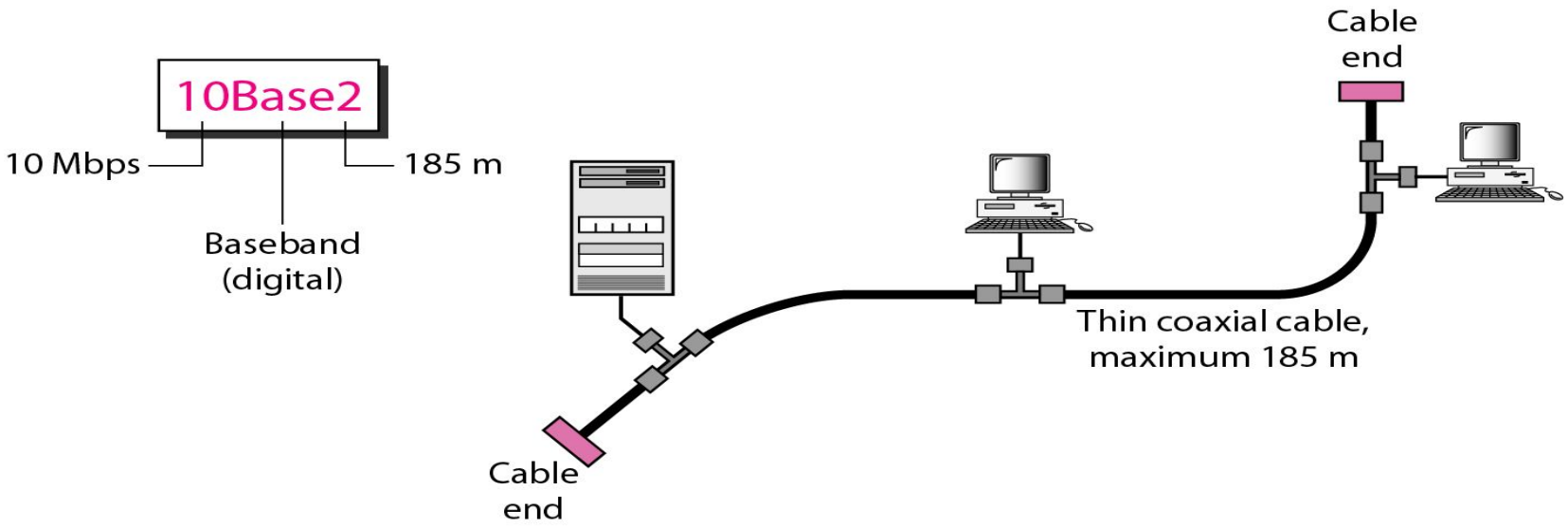
10Base5: Thick Ethernet

- The first implementation is called **10Base5, thick Ethernet, or Thicknet.**
- The nickname derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands.
- 10Base5 was the first Ethernet specification to use a bus topology with an external **transceiver** (transmitter/receiver) connected via a tap to a thick coaxial cable.
- 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.



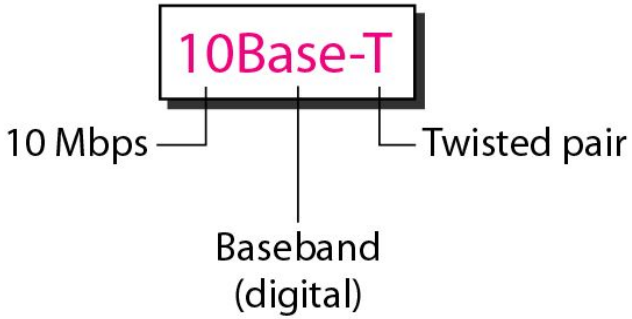
10Base2: Thin Ethernet

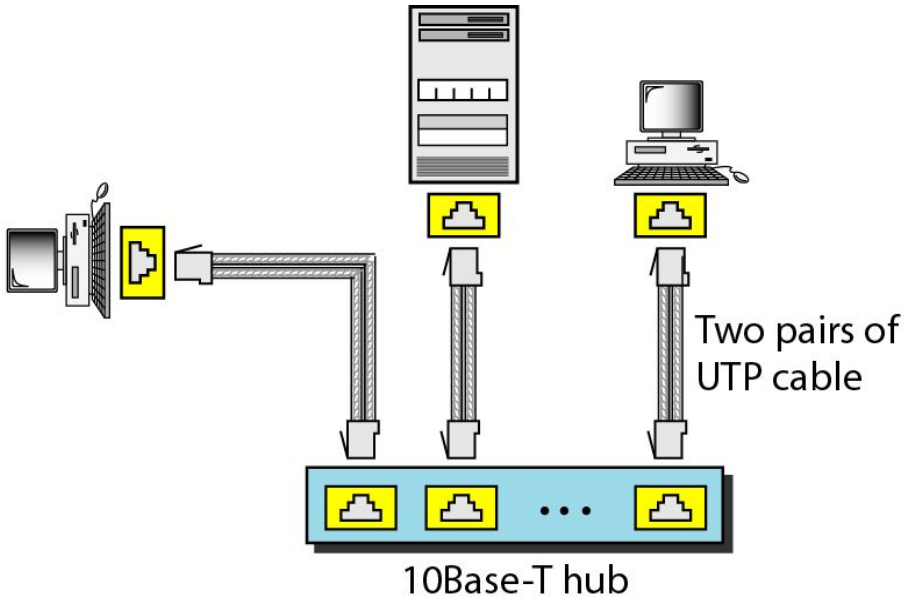
- The second implementation is called 10Base2, thin Ethernet, or Cheapernet.
- 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
- The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.
- The collision occurs in the thin coaxial cable.
- This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps.
- Installation is simpler because the thin coaxial cable is very flexible.
- The **length of each segment cannot exceed *185* m** (close to 200 m) due to the high level of **attenuation** in thin coaxial cable.



10Base-T: Twisted-Pair Ethernet

- The third implementation is called 10Base-T or twisted-pair Ethernet.
- 10Base-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**.
- Compared to 10Base5 or 10Base2, the hub actually replaces the coaxial cable as far as a collision is concerned.
- The **maximum length of the twisted cable is 100 m**, to minimize the effect of attenuation in the twisted cable.





10Base-F: Fiber Ethernet

- 10Base-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables.

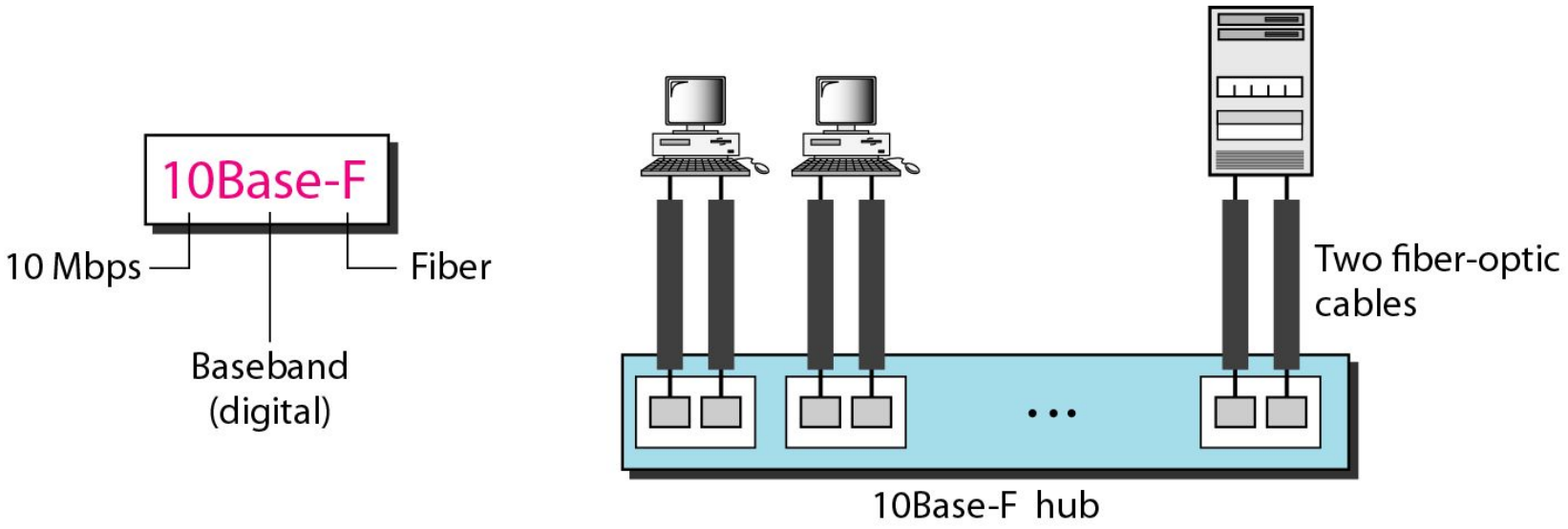
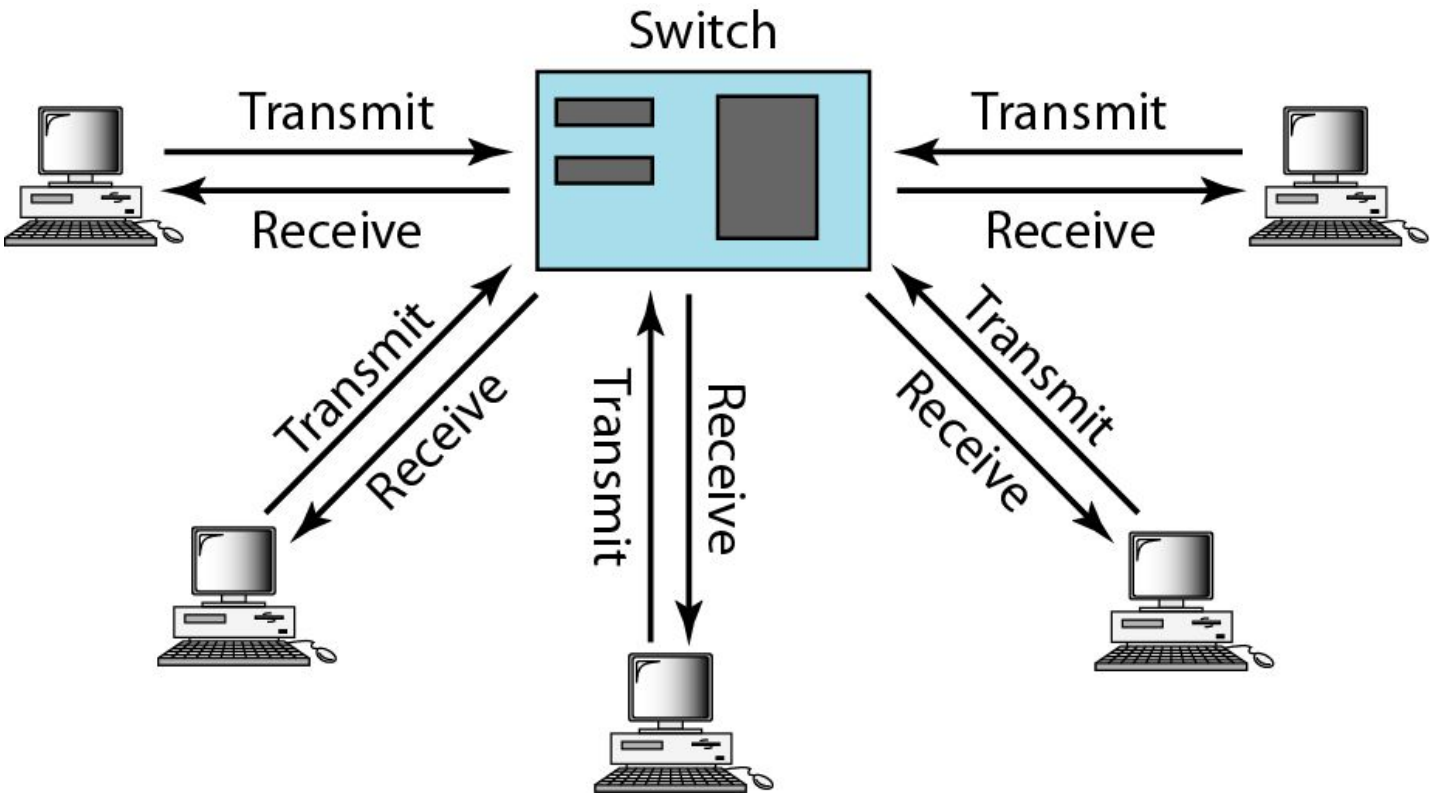


Table 13.1 *Summary of Standard Ethernet implementations*

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

Full-duplex switched Ethernet

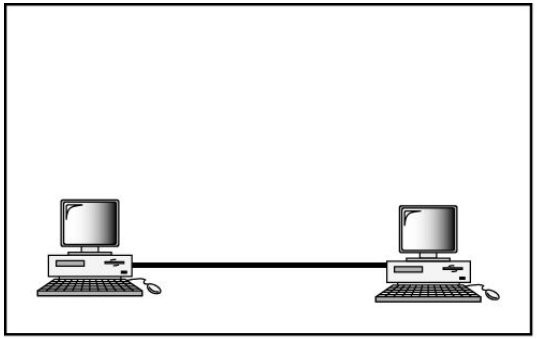


FAST ETHERNET

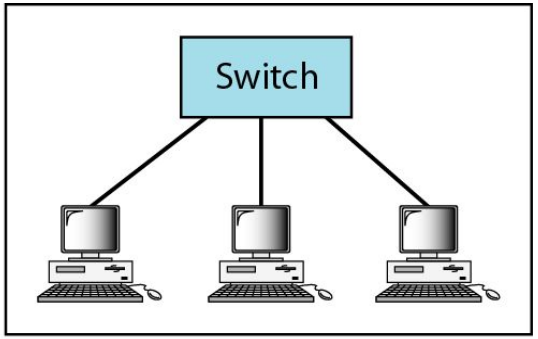
- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
- IEEE created Fast Ethernet under the name **802.3u**.
- Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.
- The goals of Fast Ethernet can be summarized as follows:

  1. Upgrade the data rate to **100 Mbps**.
  2. Make it compatible with Standard Ethernet.
  3. Keep the same 48-bit address.
  4. Keep the same frame format.
  5. Keep the same minimum and maximum frame lengths.

- A decision was made to drop the bus topologies and keep only the star topology. For the **star topology**, there are two approaches**: half duplex and full duplex**.
- In the **half-duplex approach**, the stations are connected via a **hub**.
- In the **full-duplex approach**, the connection is made via a **switch** with buffers at each port.
- A new feature added to Fast Ethernet is called **auto negotiation**. It allows a station or a hub a range of capabilities.
- **Auto negotiation** allows two devices to **negotiate the mode or data rate of operation**. It was designed particularly for the following purposes:
  - To allow **incompatible devices to connect to one another**. For example, a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).
  - To **allow one device to have multiple capabilities**.
  - To **allow a station to check a hub's capabilities**.
- Fast Ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected **point-to-point.** Three or more stations need to be connected in a star topology with a hub or a switch at the center.



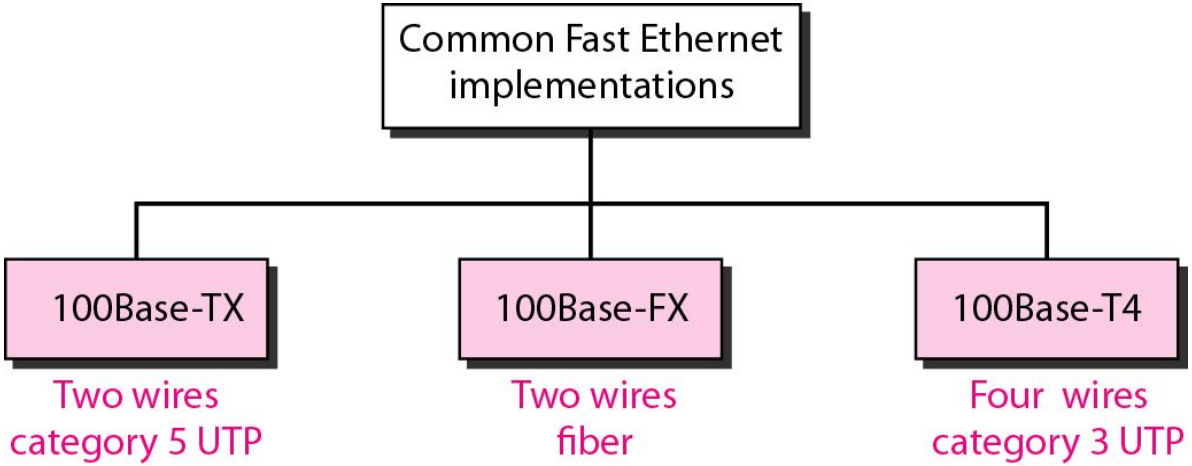
a. Point-to-point



b. Star

Fast Ethernet implementations

- Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.
- The two-wire implementation can be either category 5 UTP (100Base-TX) or fiber-optic cable (100Base-FX).
- The four-wire implementation is designed only for category 3 UTP (l00Base-T4).



- **100Base-TX** uses two pairs of twisted-pair cable (either category 5 UTP or STP).
- **100Base-FX** uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes. The designers of 100Base-FX selected the NRZ-I encoding scheme for this implementation. However,
- NRZ-I has a bit synchronization problem for long sequences of Os (or Is, based on the
- encoding. To overcome this problem, the designers used 4B/5B encoding.
- A new standard, called **100Base-T4,** was designed to use category 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps.

Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

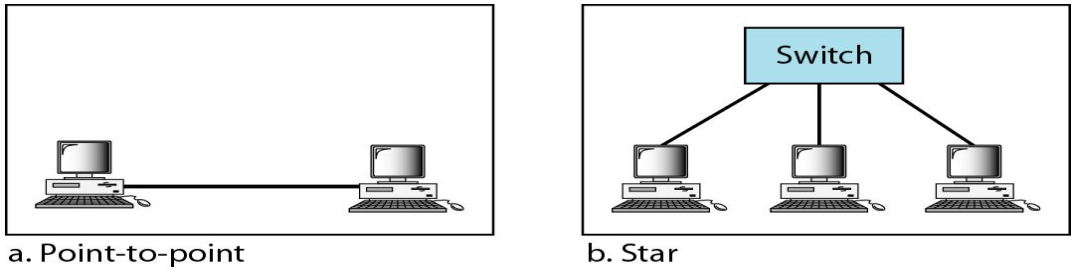
GIGABIT ETHERNET

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps).
- The IEEE committee calls the standard **802.3z.**
- The goals of the Gigabit Ethernet design can be summarized as follows:
  1. Upgrade the data rate to 1 Gbps.
  2. Make it compatible with Standard or Fast Ethernet.
  3. Use the same 48-bit address.
  4. Use the same frame format.
  5. Keep the same minimum and maximum frame lengths.
  6. To support auto negotiation as defined in Fast Ethernet.

- Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex.
- In **full-duplex mode**, there is a central switch connected to all computers or other switches. In this mode, each switch has buffers for each input port in which data are stored until they are transmitted. There is no collision in this mode.
- In **half-duplex mode**, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses *CSMAlCD.*

- Three methods have been defined: traditional, carrier extension, and frame bursting.
- **Traditional:** In the traditional approach, we keep the minimum length of the frame as in traditional Ethernet (512 bits). The reduced slot time means that collision is detected 100 times earlier. This means that the maximum length of the network is 25 m. This length may be suitable if all the stations are in one room, but it may not even be long enough to connect the computers in one single office.
- **Carrier Extension:** To allow for a longer network, we increase the minimum frame length. The carrier extension approach defines the minimum length of a frame as 512 bytes (4096 bits). This means that the minimum length is 8 times longer. This method forces a station to add extension bits (padding) to any frame that is less than 4096 bits. In this way, the maximum length of the network can be increased 8 times to a length of 200 m. This allows a length of 100 m from the hub to the station.
- **Frame Bursting:** Carrier extension is very inefficient if we have a series of short frames to send; each frame carries redundant data. To improve efficiency, frame bursting was proposed. Instead of adding an extension to each frame, multiple frames are sent. However, to make these multiple frames look like one frame, padding is added between the frames (the same as that used for the carrier extension method) so that the channel is not idle. In other words, the method deceives other stations into thinking that a very large frame has been transmitted.

- Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another.



a. Point-to-point

b. Star

c. Two stars

d. Hierarchy of stars

Implementation

- Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation.
- The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX).
- The four-wire version uses category 5 twisted-pair cable (1000Base-T).
- 1000Base-T was designed in response to those users who had already installed this wiring for other purposes such as Fast Ethernet or telephone services.

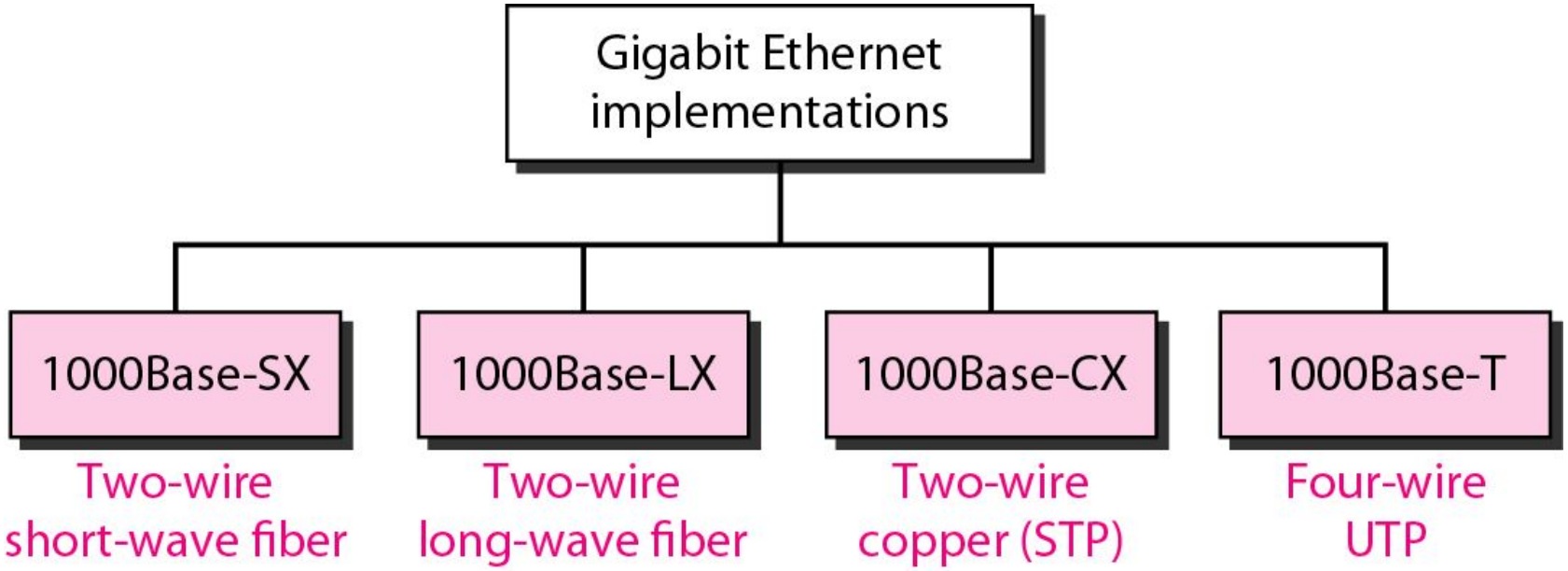


Table 13.3 *Summary of Gigabit Ethernet implementations*

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

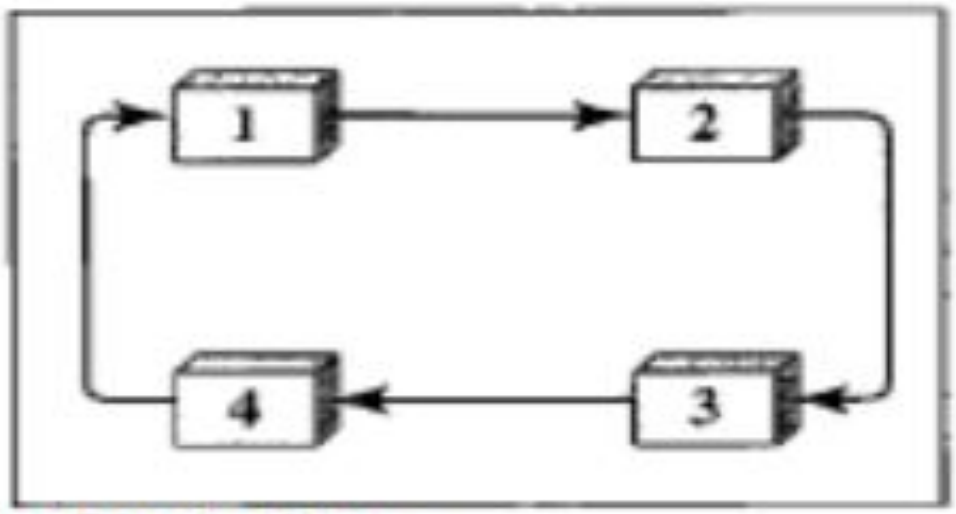
- The IEEE committee created Ten-Gigabit Ethernet and called it **Standard 802.3ae**.
- The goals of the Ten-Gigabit Ethernet design can be summarized as follows:
  - Upgrade the data rate to 10 Gbps.
  - Make it compatible with Standard, Fast, and Gigabit Ethernet.
  - Use the same 48-bit address.
  - Use the same frame format.
  - Keep the same minimum and maximum frame lengths.
  - Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
  - Make Ethernet compatible with technologies such as Frame Relay and ATM.
- Ten-Gigabit Ethernet operates only in **full duplex mode** which means there is no need for contention.
- The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances.
- Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase-E.

Ten-Gigabit Ethernet implementations

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

Token Ring

- In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.

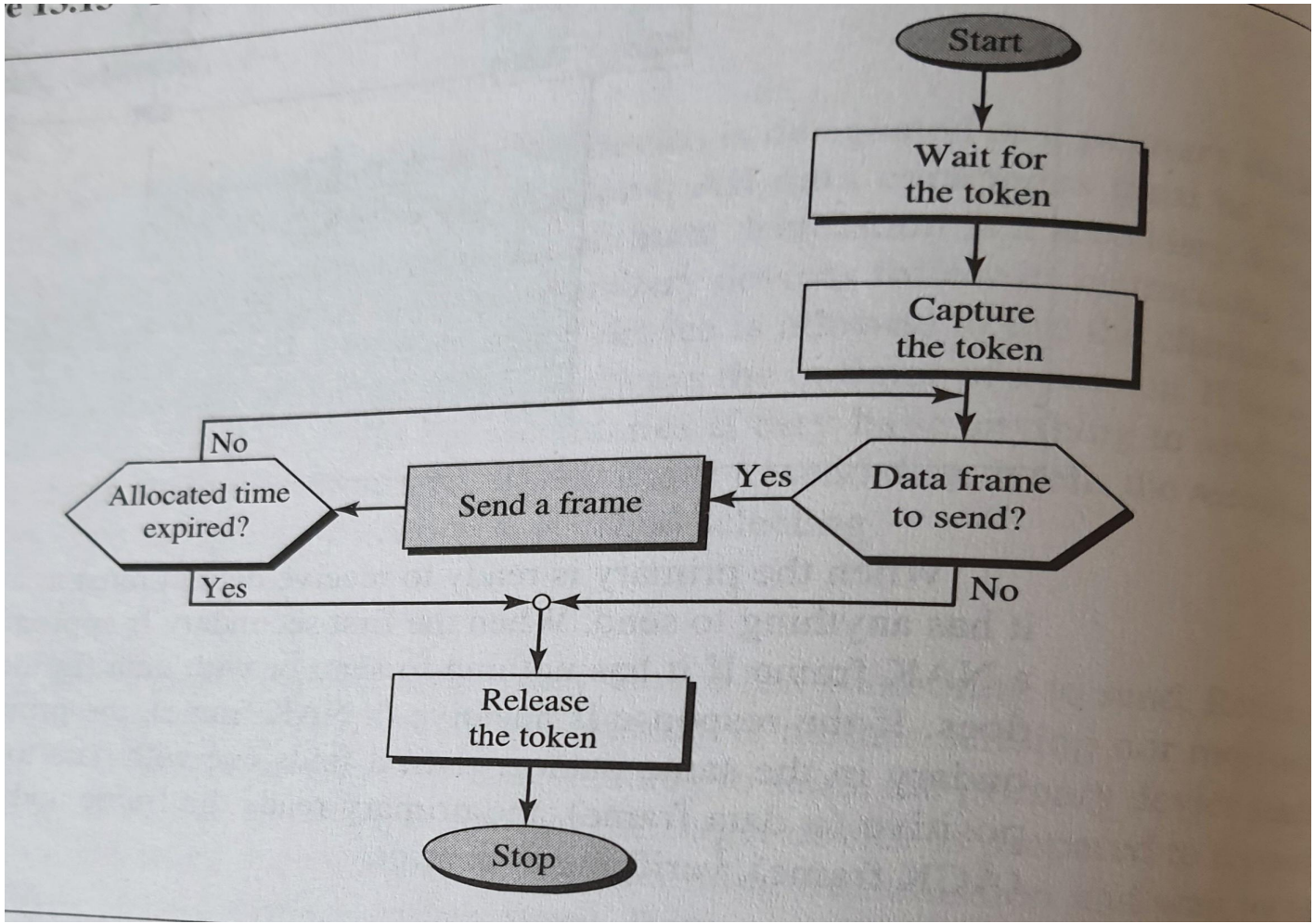


a. Physical ring

- In the physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line. This means that the token does not have to have the address of the next successor. The problem with this topology is that if one of the links-the medium between two adjacent stations fails, the whole system fails.

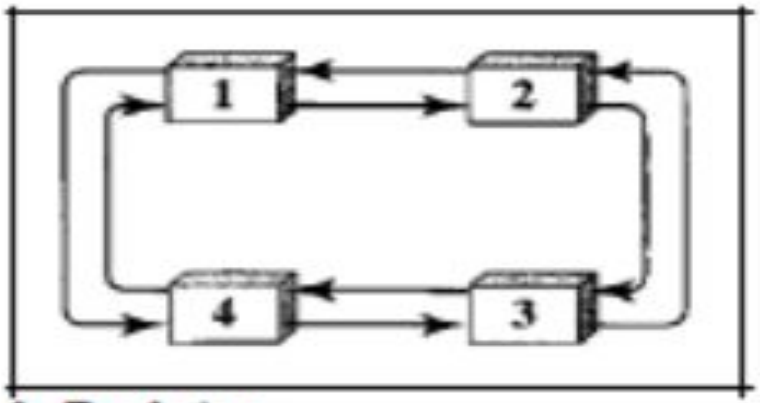
Token passing procedure

- In the token-passing method, a station is authorized to send data when it receives a special frame called a token.
- When no data are being sent, the token circulates in the network.
- If a station needs to send data, it waits for the token.



Dual ring topology

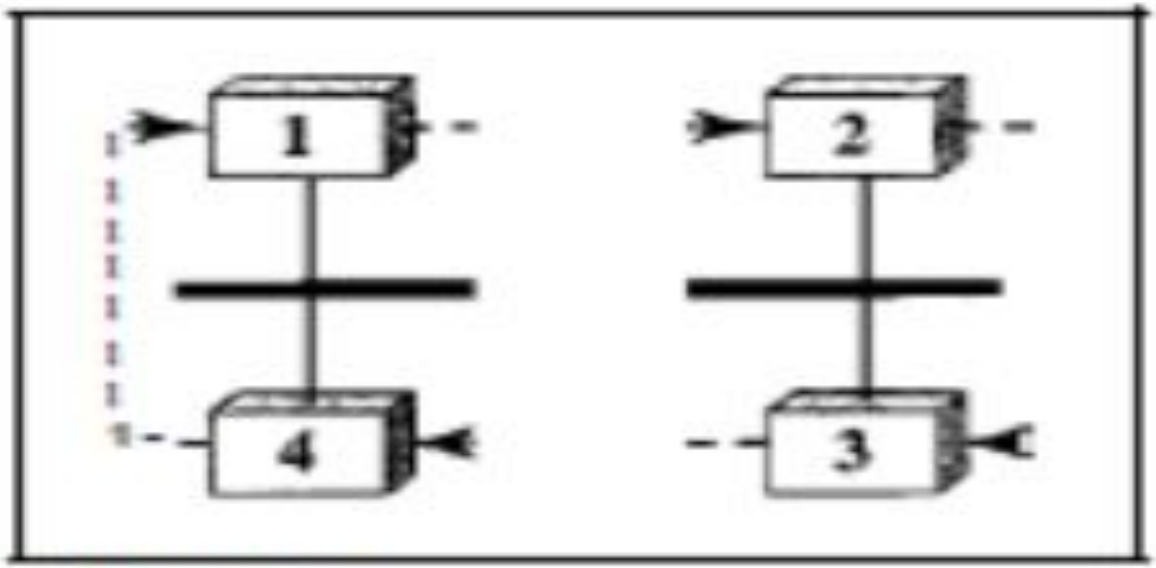
- The dual ring topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring.
- The second ring is for emergencies only.
- If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring.
- After the failed link is restored, the auxiliary ring becomes idle again.
- Note that for this topology to work, each station needs to have two transmitter ports and two receiver ports.
- The high-speed Token Ring networks called FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) use this topology.



b. Dual ring

Token Bus

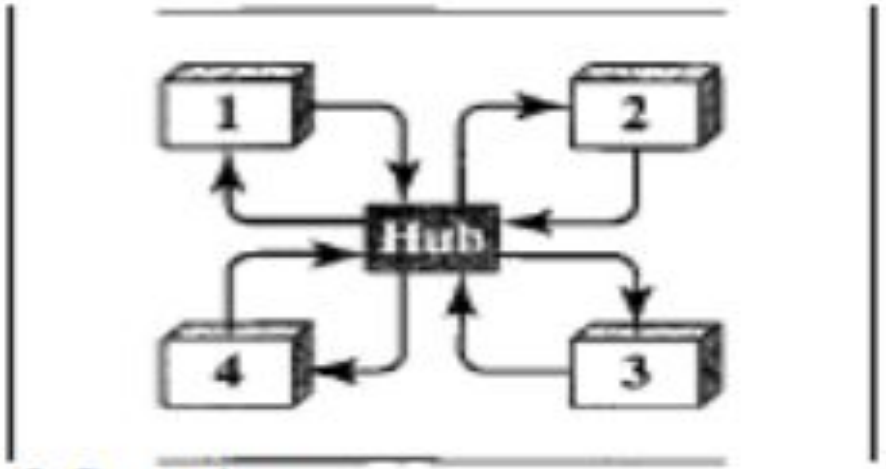
- In the bus ring topology, also called a **token bus**, the stations are connected to a single cable called a bus. They, however, make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes).
- When a station has finished sending its data, it releases the token and inserts the address of its successor in the token.
- Only the station with the address matching the destination address of the token gets the token to access the shared media.
- The Token Bus LAN, standardized by IEEE, uses this topology



c. Bus ring

Star Ring topology

- In a star ring topology, the physical topology is a star.
- There is a hub acts as the connector.
- The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections.
- This topology makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate.
- Also adding and removing stations from the ring is easier.
- This topology is still used in the Token Ring LAN designed by IBM.

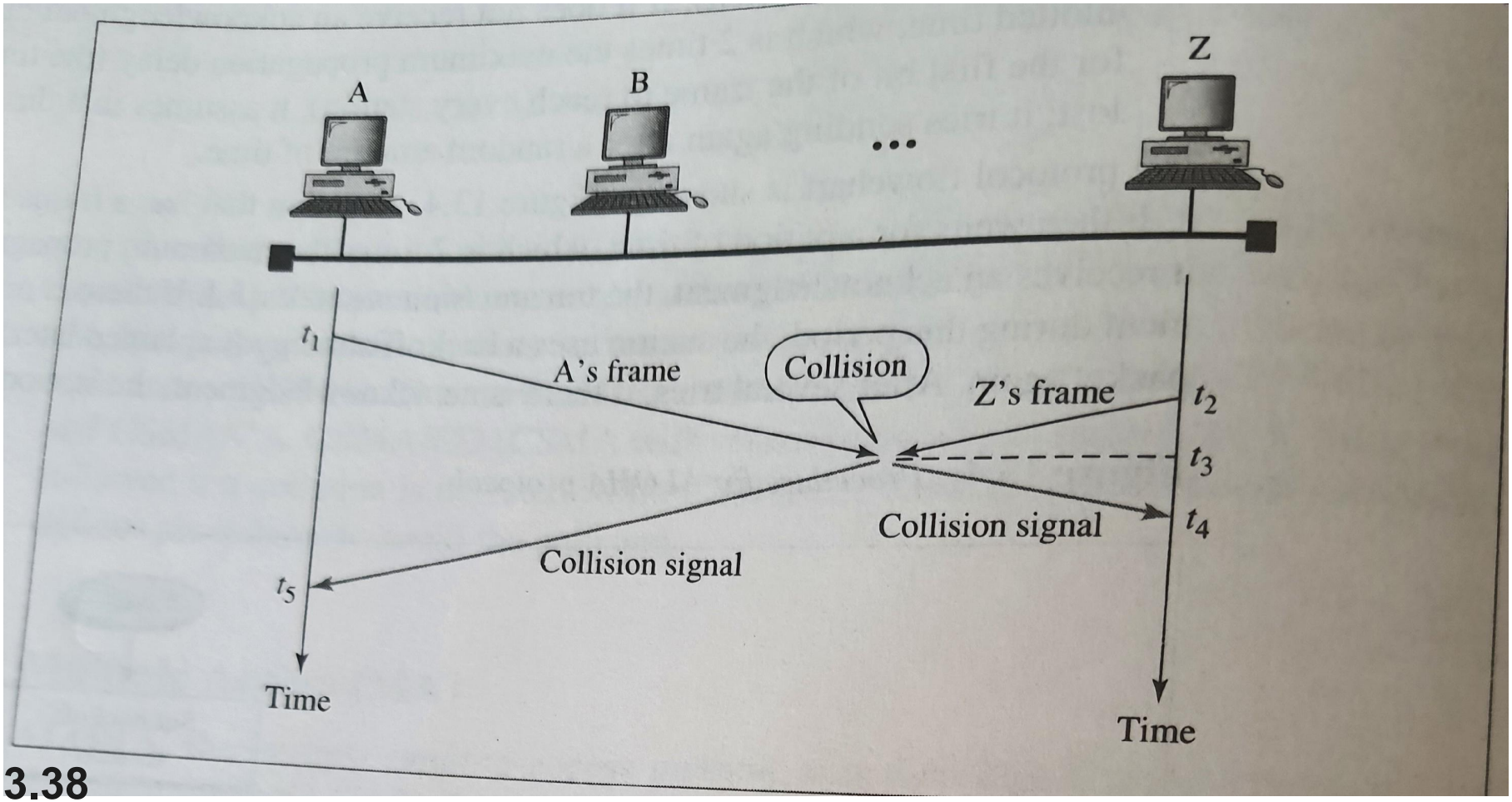


d Star ring

CSMA

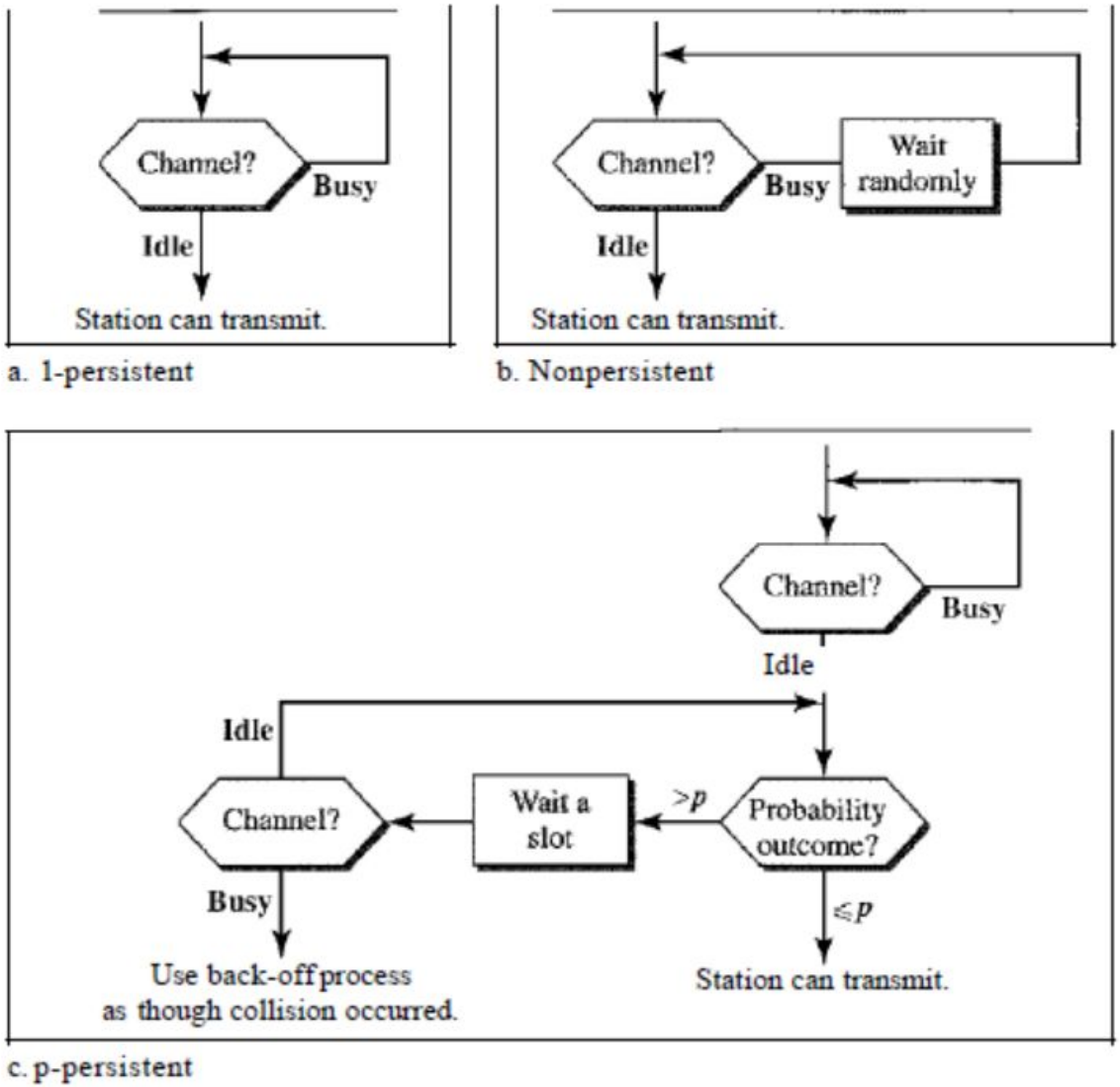
requires that each station first listens to the medium before sending.
CSMA is based on the principle "sense before transmit" or "listen before talk".

To minimize the chance of collision and increase the performance, the CSMA method was developed.



Persistence strategy

- defines the procedures for a station that senses a busy medium.

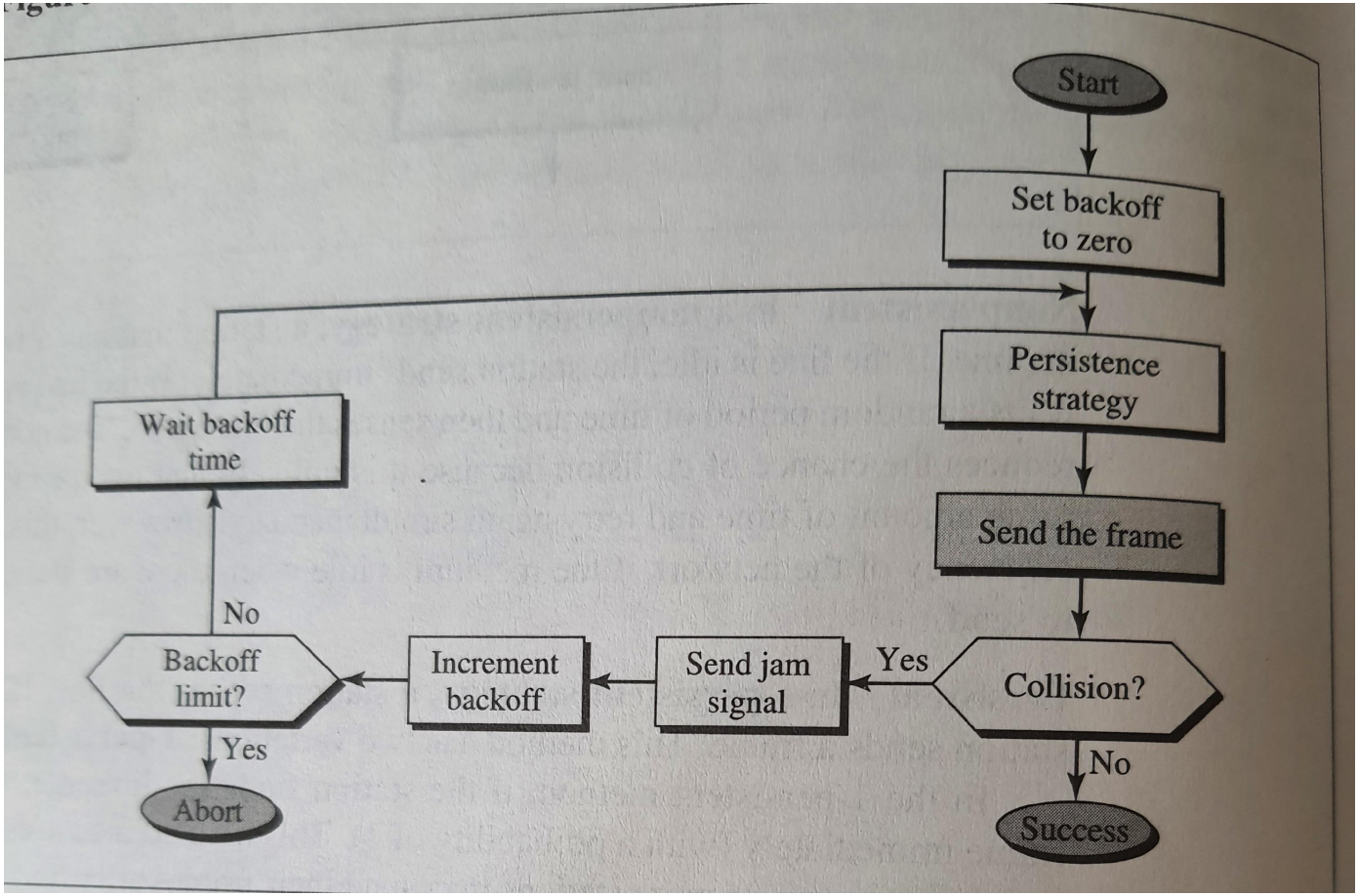


CSMA/CD

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.
- It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free.
- The collision detection technology detects collisions by sensing transmissions from other stations.
- On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

CSMA/CD procedure

- To reduce the probability of collision, the station waits – it needs to **back off**.
- In exponential back off method, the station waits an amount of time between 0 and 2^N * maximum _propagation time.



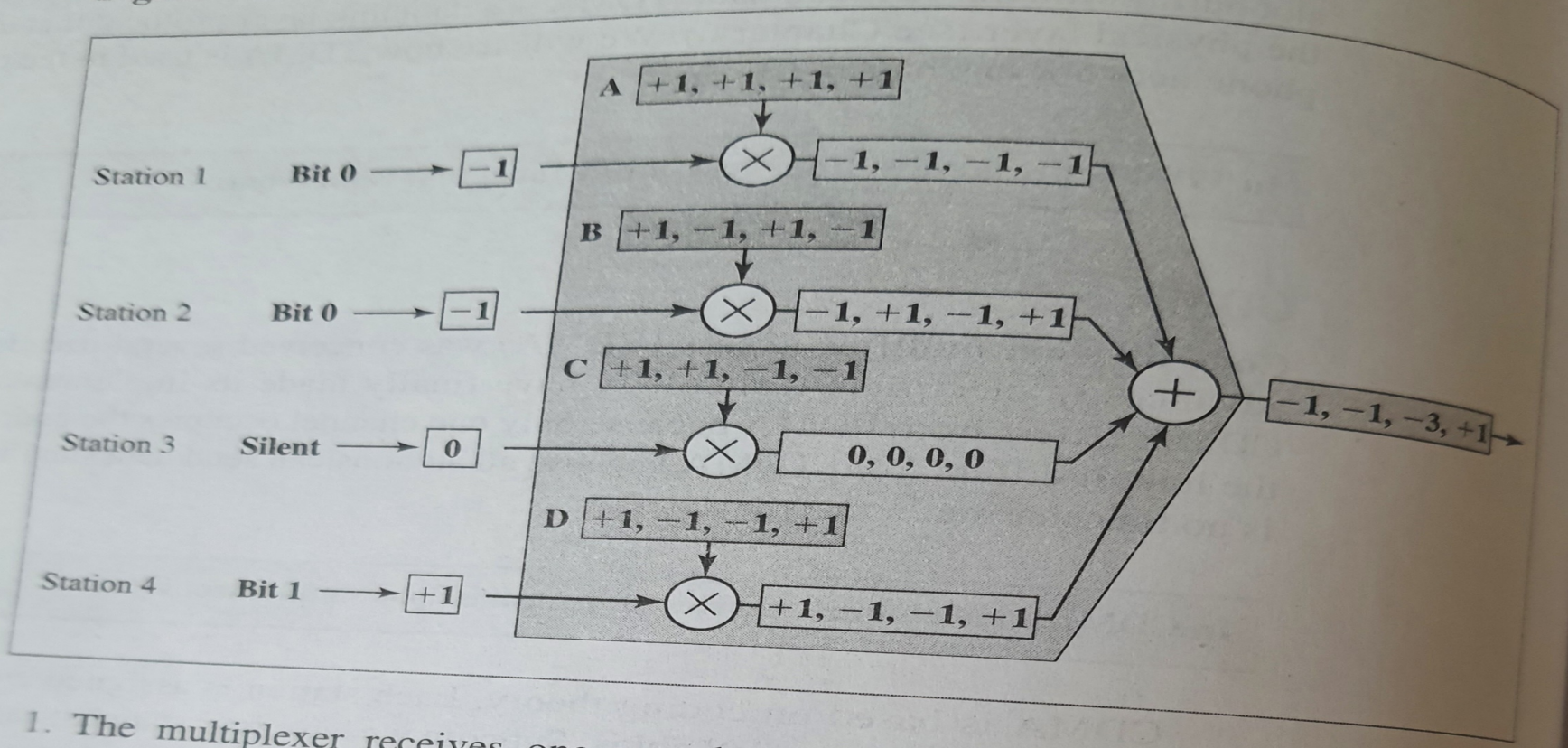
Multiple access method - Channelization

- **Channelization** is a multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations.
- 3 channelization protocols: FDMA, TDMA & CDMA
- FDMA, TDMA related to physical layer.
- CDMA – data link layer.
- **Frequency Division Multiple Access (FDMA)**
  - The available bandwidth is shared among all stations
  - Each station uses its own allocated bandwidth to send its data.
  - Each band is reserved for a particular station – the band belongs to the station all the time.
- **Time Division Multiple Access (TDMA)**
  - The entire bandwidth is just one channel.
  - The stations share the capacity of the channel in time.
  - Each station is allotted a time slot during which it can send data.

- **Code Division Multiple Access (CDMA)**
  - CDMA differs from FDMA as only one channel occupies the entire bandwidth of the link.
  - Differs from TDMA as all stations can send data simultaneously- there is no timesharing.
  - Based on coding theory – each station is assigned with a code – a sequence of numbers called **chips**.
  - Suppose there are 4 stations – each has a sequence of chips which are designated as A, B, C, D.
    - A (+1,+1,+1,+1)
    - B (+1, -1,+1, -1)
    - C (+1,+1, -1, -1)
    - D (+1, -1, -1, +1)
  - Rules for encoding – If a station needs to send a 0 bit, it sends a-1.
  - If a station needs to send a 1 bit, it sends a+1.
    If a station is idle, it is represented by 0.

CDMA Multiplexer

Figure 13.16 *CDMA multiplexer*

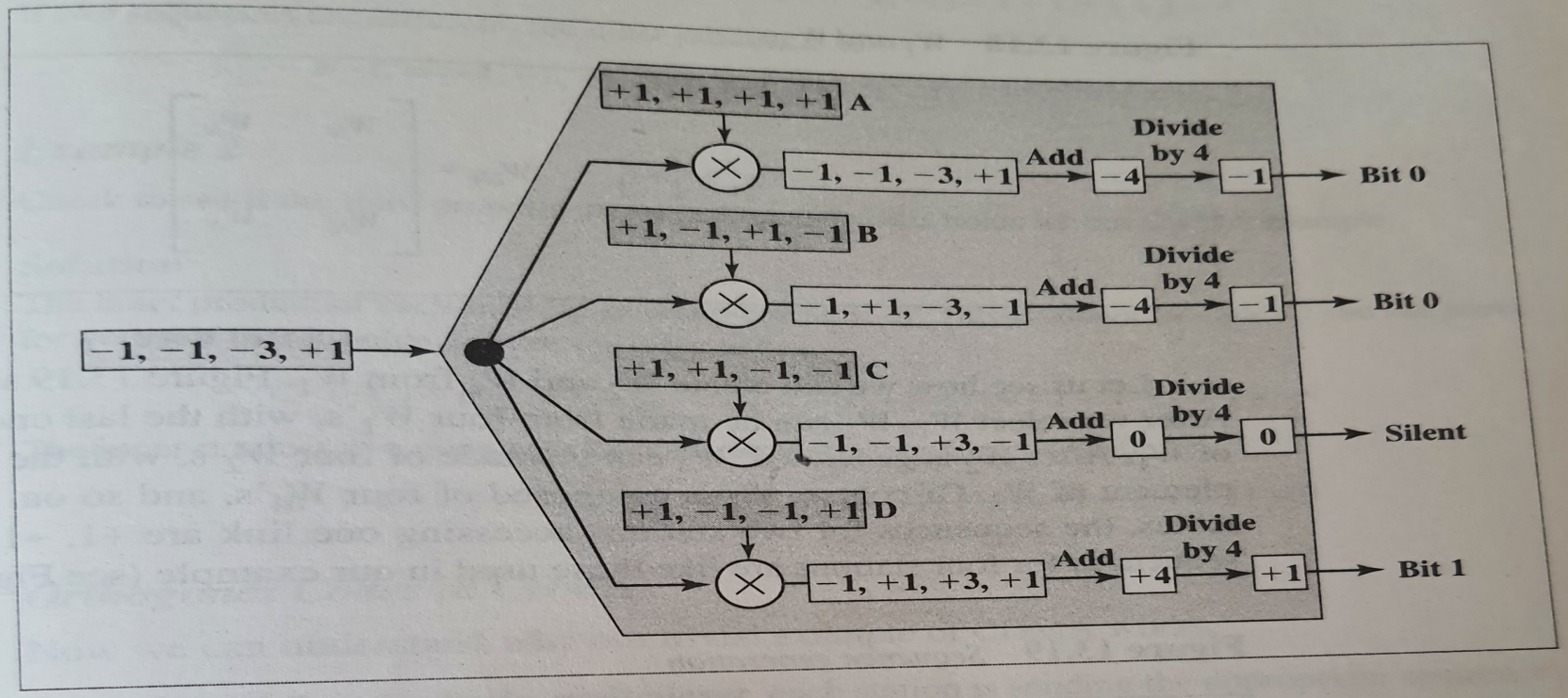


1. The multiplexer receives one encoded number from each station (−1, −1, 0, and +1).
2. The encoded number sent by station 1 is multiplied by each chip in sequence A. A new sequence is the result (−1, −1, −1, −1). Likewise, the encoded number sent by station 2 is multiplied by each chip in sequence B. The same is true for the remaining two encoded numbers. The result is four new sequences.
3. All first chips are added, as are all second, third, and fourth chips. The result is one new sequence.
4. The sequence is transmitted through the link.

CDMA Demultiplexer

Figure 13.17 shows the situation at the demultiplexer. The steps are as follows:

Figure 13.17 *CDMA demultiplexer*



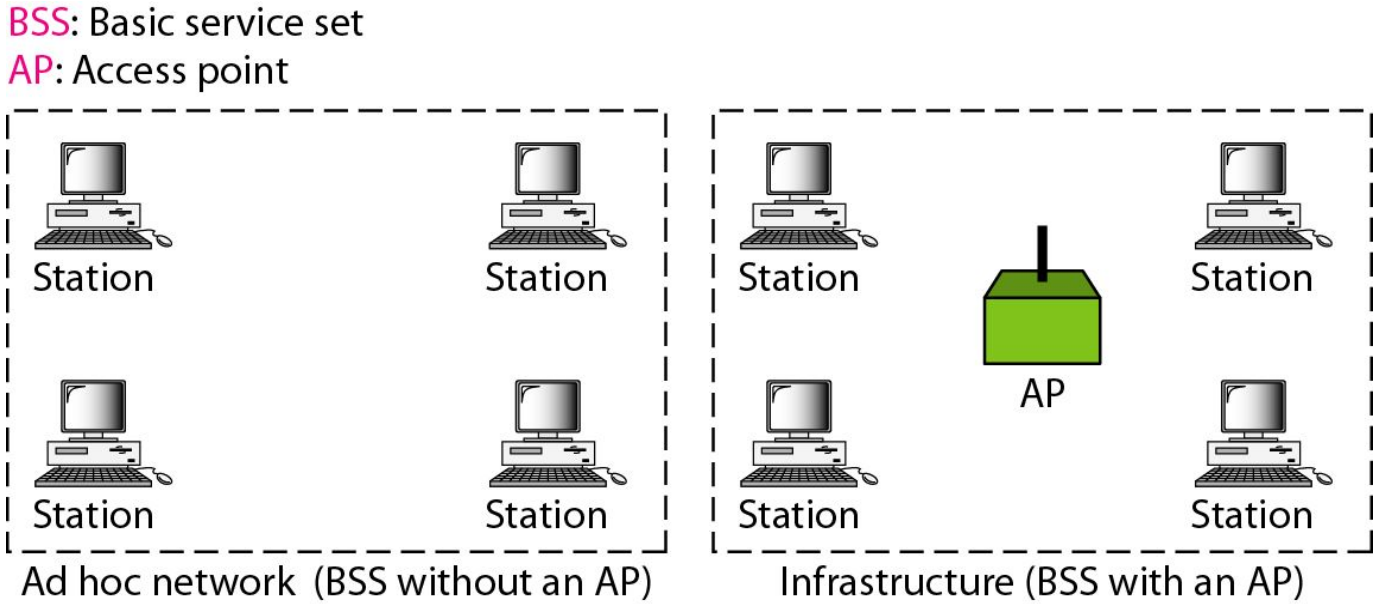
1. The demultiplexer receives the sequence sent across the link.
2. It multiplies the sequence by the code for each receiver. The multiplication is done chip by chip.
3. The chips in each sequence are added. The result is always +4, −4, or 0.
4. The result of step 3 is divided by 4 to get −1, +1, or 0.
5. The number in step 4 is decoded to 0, 1, or silence by the receiver.

Wireless LAN - IEEE 802.11

- Wireless communication is one of the fastest-growing technologies.
- The demand for connecting devices without the use of cables is increasing everywhere.
- Wireless LAN can be found on college campuses, in office buildings, and in many public areas.
- IEEE has defined the specifications for a wireless LAN, called **IEEE 802.11**, which covers the physical and data link layers.

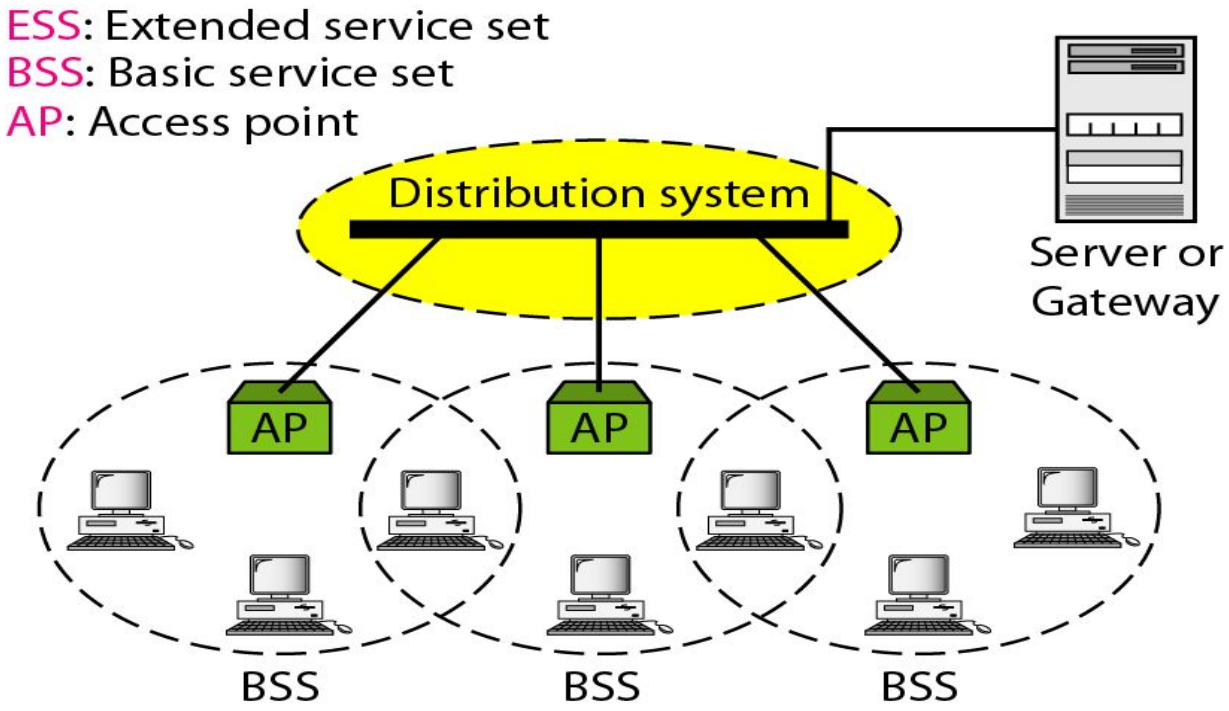
Architecture-BSS

- The standard defines **two kinds of services**: the basic service set (BSS) and the extended service set (ESS).
- **Basic Service Set**
- IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- The **BSS without an AP** is a **stand-alone network** and cannot send data to other BSSs.
- It is called **an *ad hoc architecture***. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS.
- A **BSS with an AP** is sometimes referred to as an ***infrastructure* network**.



Architecture-ESS

- An extended service set (ESS) is made up of **two or more BSSs with APs**.
- The BSSs are connected through a ***distribution system***, which is usually a **wired LAN**.
- The distribution system connects the APs in the BSSs.
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- Note that the extended service set uses two types of stations: mobile and stationary.
- The **mobile stations** are **normal stations** inside a BSS.
- The **stationary stations are AP stations** that are part of a wired LAN.

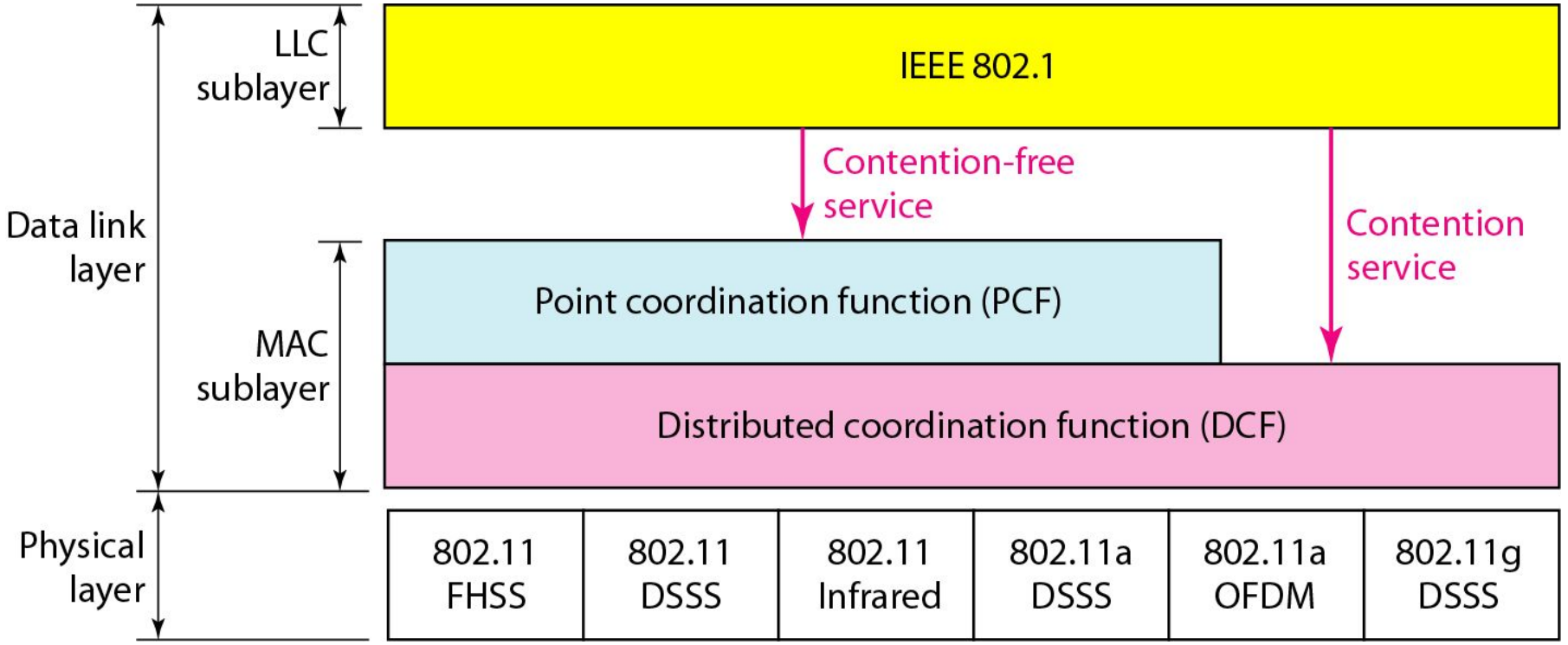


Station Types

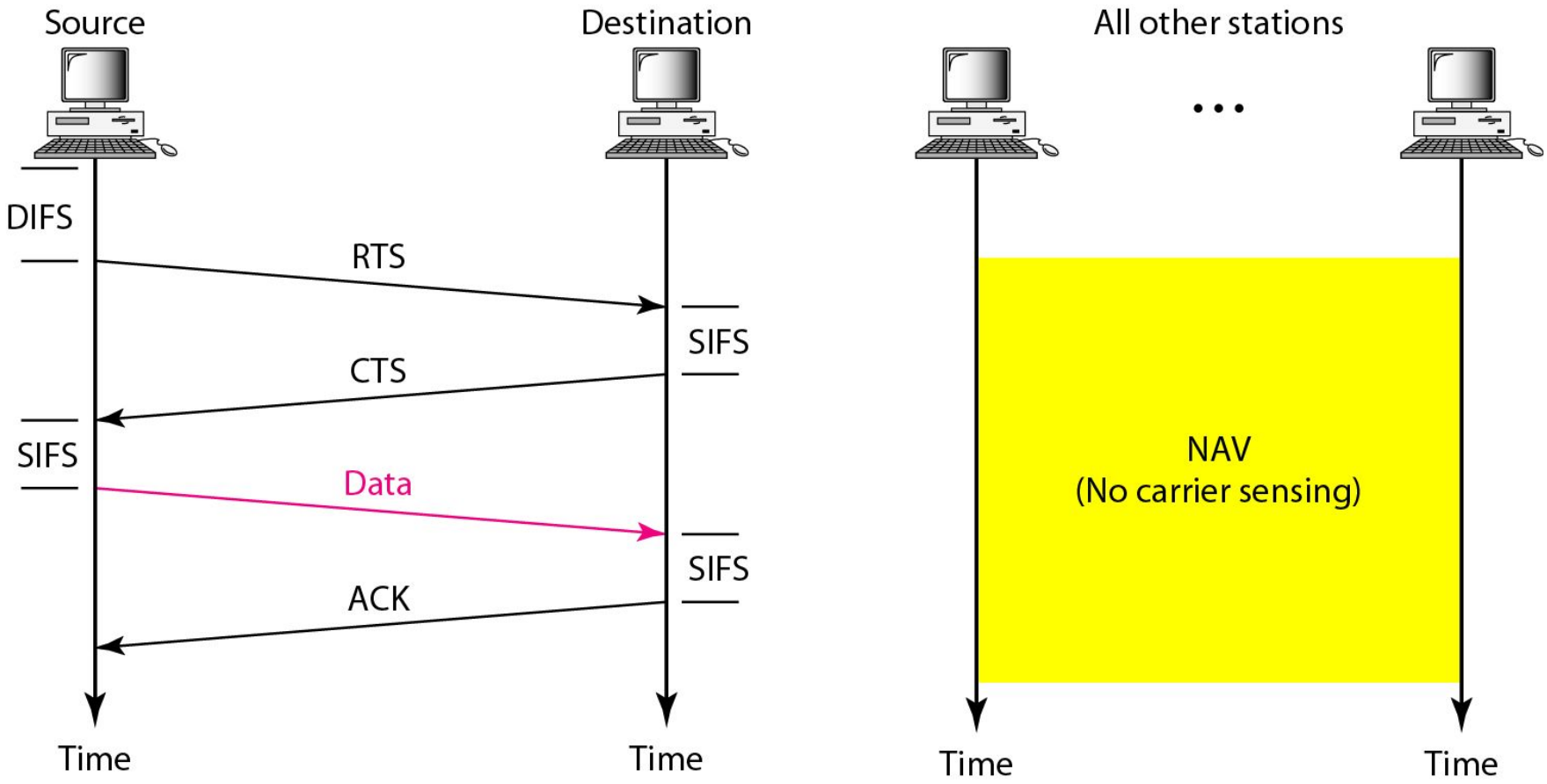
- IEEE 802.11 defines **three types of stations** based on their mobility in a wireless LAN:
  - **no-transition, BSS-transition, and ESS-transition mobility**.
- A station with **no-transition mobility** is either stationary (not moving) or moving only inside a BSS.
- A station with **BSS-transition mobility** can move from one BSS to another, but the movement is confined inside one ESS.
- A station with **ESS-transition mobility** can move from one ESS to another.

MAC Sublayer

- IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).



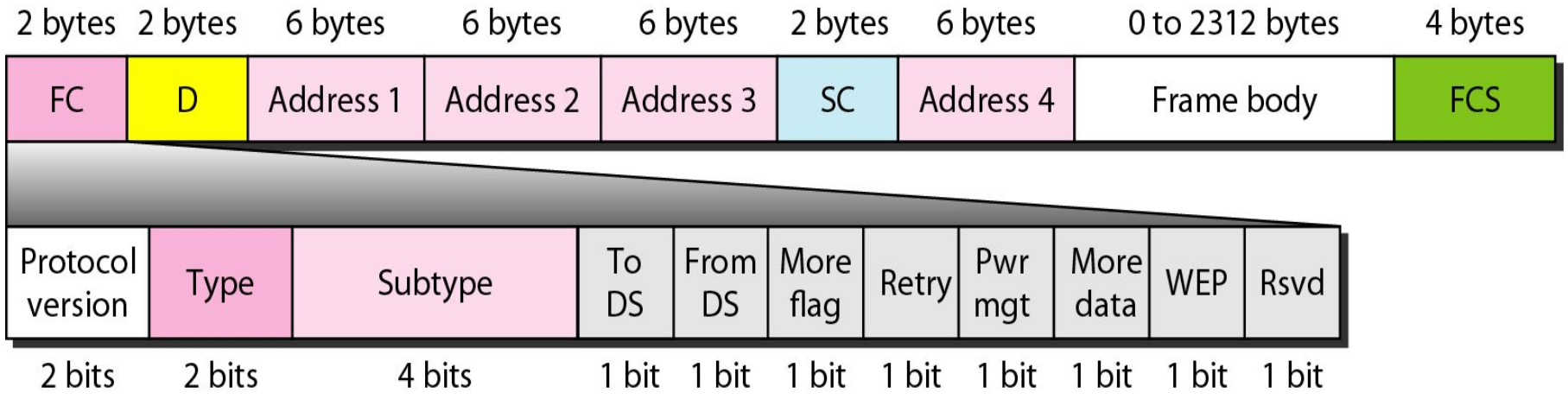
CSMA/CA and NAV



Frame Format

The MAC layer frame consists of nine fields:

- Frame control (FC): The FC field is 2 bytes long and defines the type of frame and some control information.
- D: In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAY. In one control frame, this field defines the ID of the frame.
- Addresses: There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the *To* DS and *From* DS subfields.
- Sequence control: This field defines the sequence number of the frame to be used in flow control.
- Frame body: This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.
- FCS. The FCS field is 4 bytes long and contains a CRC-32 error detection sequence

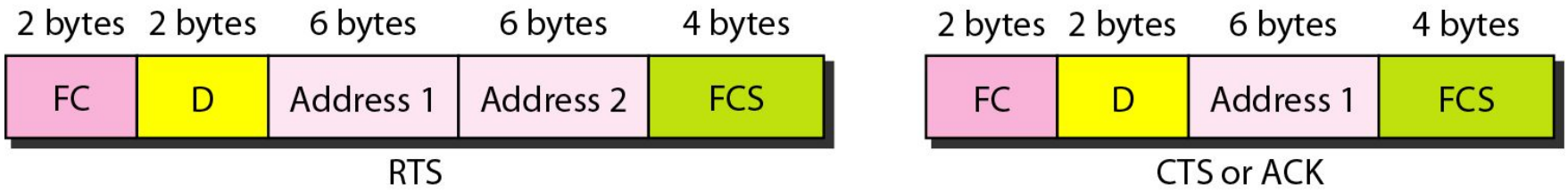


Subfields in FC field

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

Frame Types

- A wireless LAN defined by IEEE 802.11 has three categories of frames:
  - **Management frames, control frames, and data frames.**
- **Management frames** are used for the **initial communication between stations and access points.**
- **Control frames** are used for **accessing the channel and acknowledging frames.**



- For control frames the value of the type field is 01; the values of the subtype fields for frame

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

- **Data frames** are used for **carrying data and control information**.

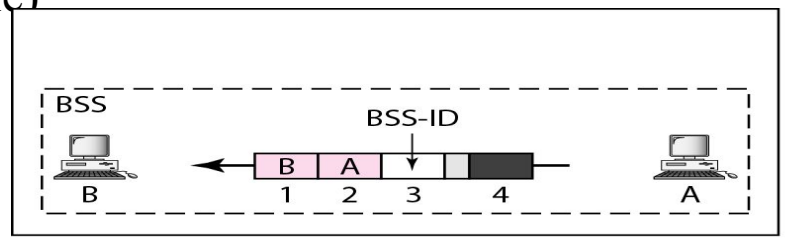
Addressing mechanism

- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, *To DS* and *From DS*. Each flag can be either 0 or 1 resulting in four different situations.
- The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags.

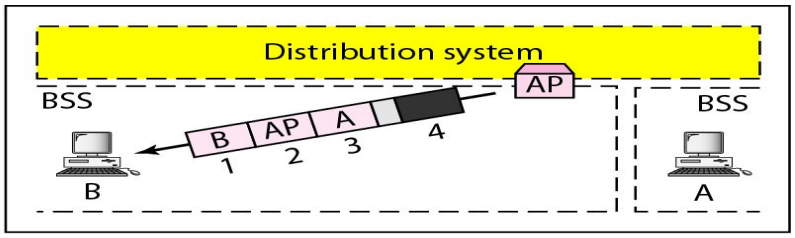
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

- Address 1 is always the address of the next device.
- Address 2 is always the address of the previous device.
- Address 3 is the address of the final destination station if it is not defined by address 1.
- Address 4 is the address of the original source station if it is not the same as address 2.

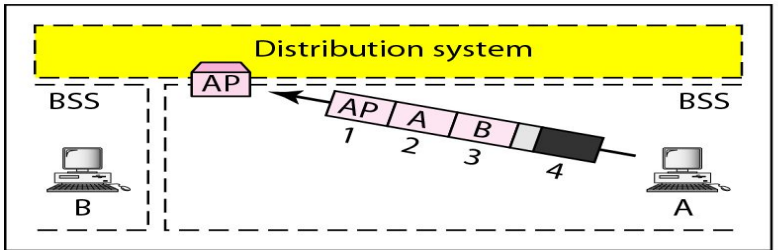
- Case 1: 00 In this case, *To DS* = 0 and *From DS* = 0. This means that the frame is not going to a distribution system *(To DS* = 0) and is not coming from a distribution system *(From DS* =0). The **frame is going from one station in a BSS to another without passing through the distribution system. The ACK frame should be sent to the original sender**.
- Case 2: 01 In this case, *To DS* = 0 and *From DS* = 1. This means that the **frame is coming from a distribution system** *(From* DS = 1). The frame is **coming from an AP** and going to a **station.** The **ACK should be sent to the AP**.
- Case 3: 10 In this case, *To DS* =1 and *From DS* =0. This means that the frame is going to a distribution system *(To DS* = 1). The frame is **going from a station to an AP**. The **ACK is sent to the original station**.
- Case 4:11 In this case, *To DS* =1 and *From DS* =1. This is the case in which the distribution system is also wireless. The frame is going from **one AP to another AP** in a wireless distribution system. We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example)

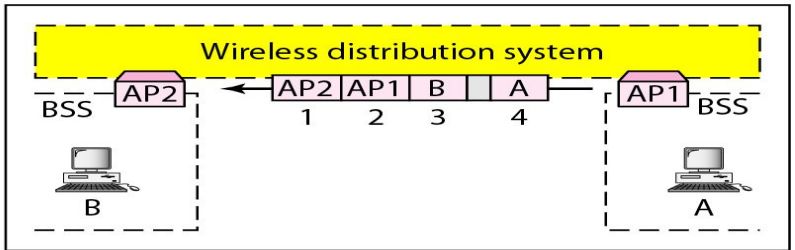


a. Case 1



b. Case 2

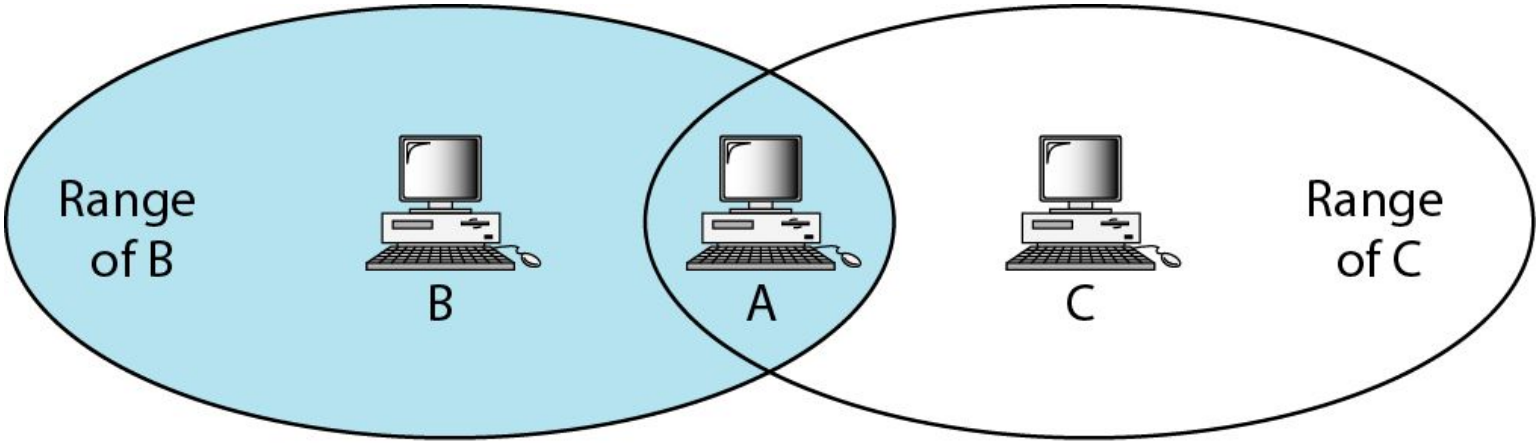




Hidden and Exposed Station Problems

- Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C. Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C. Station A, however, is in the area covered by both Band C; it can hear any signal transmitted by B or C.
- Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations Band C are hidden from each other with respect to A.
- **Hidden stations can reduce the capacity of the network because of the possibility of collision.**

Hidden station problem



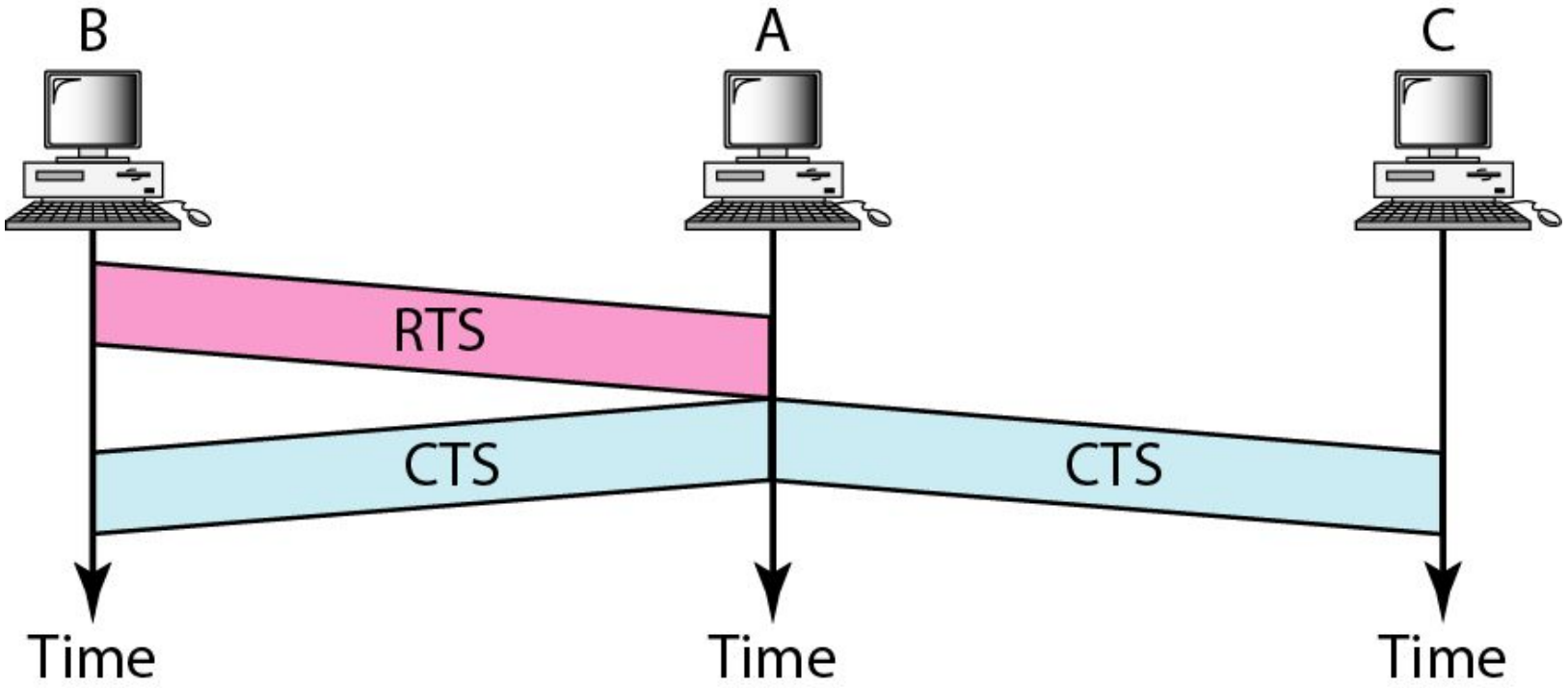
B and C are hidden from each other with respect to A.

Note

The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

Use of handshaking to prevent hidden station problem

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS) which shows that the RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C.
Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.



- Station A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.
- The handshaking messages RTS and CTS cannot help in this case, despite what you might think.
- Station C hears the RTS from A, but does not hear the CTS from B.
- Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D.
- Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state.
- Station B, however, responds with a CTS. The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data

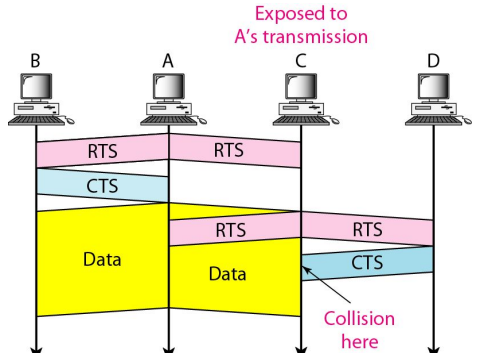


Figure 14.12 *Exposed station problem*

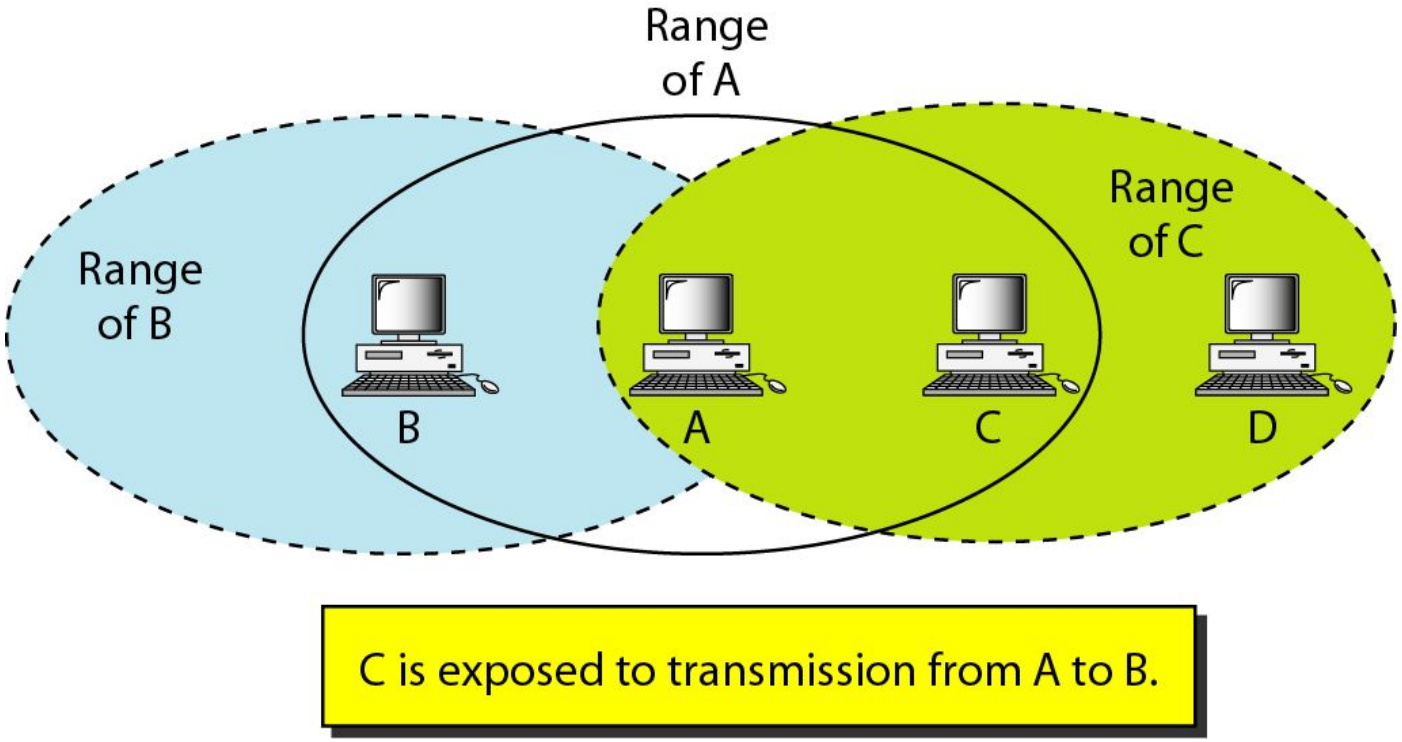
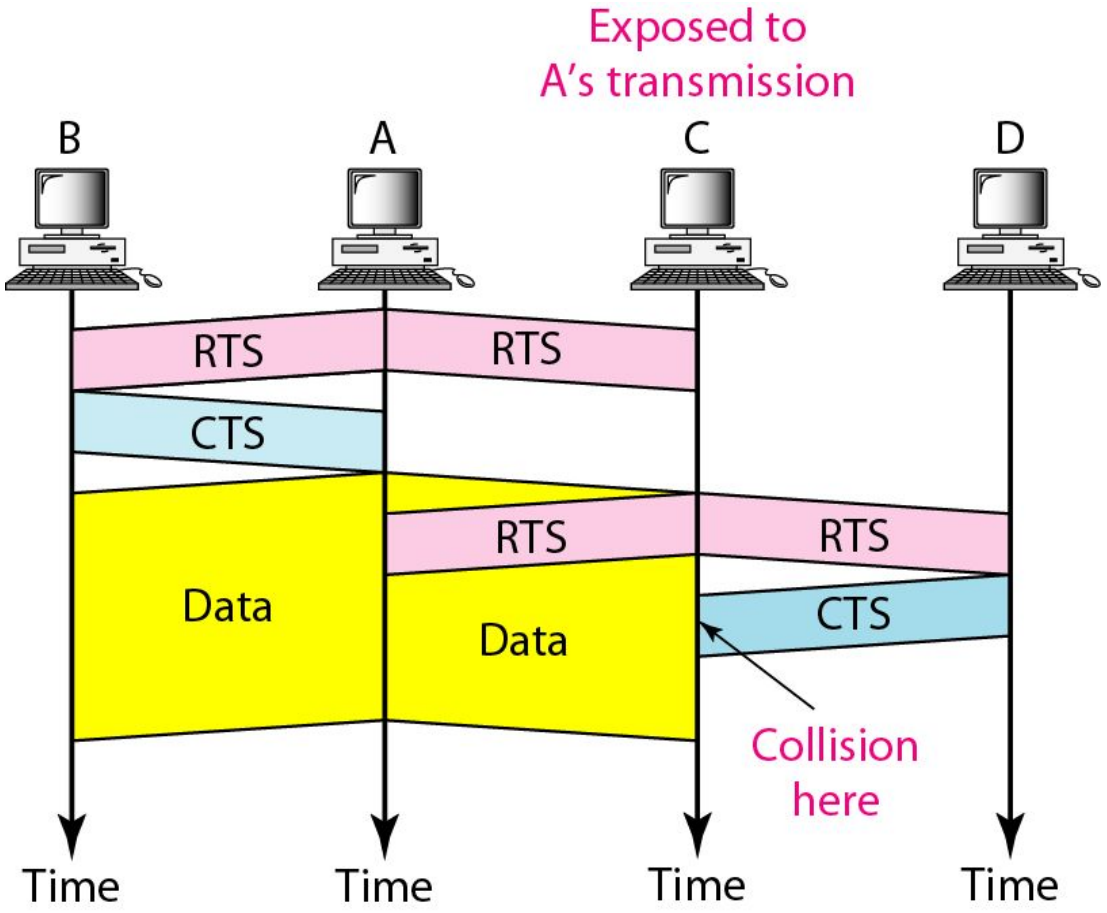


Figure 14.13 *Use of handshaking in exposed station problem*



- IEEE 802.11 FHSS
- IEEE 802.11 FHSS uses the frequency-hopping spread spectrum (FHSS) method.
- FHSS uses the 2.4-GHz ISM band. The band is divided into 79 subbands of 1 MHz (and some guard bands). A pseudorandom number generator selects the hopping sequence. The modulation technique in this specification is either two-level FSK or four-level FSK with I or 2 bitslbaud, which results in a data rate of 1 or 2 Mbps.
- IEEE 802.11 DSSS
- IEEE 802.11 DSSS uses the direct sequence spread spectrum (DSSS) method. DSSS uses the 2.4-GHz ISM band. The modulation technique in this specification is PSK at 1 Mbaud/s. The system allows 1 or 2 bitslbaud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps.
- IEEE 802.11 Infrared
- IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm. The modulation technique is called pulse position modulation (PPM). For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0. For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0. The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

- ***IEEE 802.lla OFDM***
- IEEE 802.Ila OFDM describes the orthogonal frequency-division multiplexing
- (OFDM) method for signal generation in a 5-GHz ISM band. OFDM is similar to
- FDM as discussed in Chapter 6, with one major difference: All the subbands are used
- by one source at a given time. Sources contend with one another at the data link layer
- for access. The band is divided into 52 subbands, with 48 subbands for sending 48
- groups of bits at a time and 4 subbands for control information. The scheme is similar
- to ADSL. Dividing the band into subbands diminishes the effects of interference. If the subbands are used randomly, security can also be increased. OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps (PSK) and 54 Mbps (QAM).
- ***IEEE 802.llb DSSS***
- IEEE 802.11 b DSSS describes the high-rate direct sequence spread spectrum (HRDSSS)
- method for signal generation in the 2.4-GHz ISM band. HR-DSSS is similar to
- DSSS except for the encoding method, which is called complementary code keying
- (CCK). CCK encodes 4 or 8 bits to one CCK symbol. To be backward compatible with
- DSSS, HR-DSSS defines four data rates: 1,2, 5.5, and 11 Mbps. The first two use the
- same modulation techniques as DSSS. The 5.5-Mbps version uses BPSK and transmits
- at 1.375 Mbaudls with 4-bit CCK encoding. The II-Mbps version uses QPSK and transmits
- at 1.375 Mbps with 8-bit CCK encoding.

- *IEEE 802.11g*
- This new specification defines forward error correction and OFDM using the 2.4-GHz
- ISM band. The modulation technique achieves a 22- or 54-Mbps data rate. It is backwardcompatible
- with 802.11b, but the modulation technique is OFDM.

Physical layers

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

14-2 BLUETOOTH

***Bluetooth** is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.*

Topics discussed in this section:

Architecture
Bluetooth Layers
Baseband Layer
L2CAP

Piconet

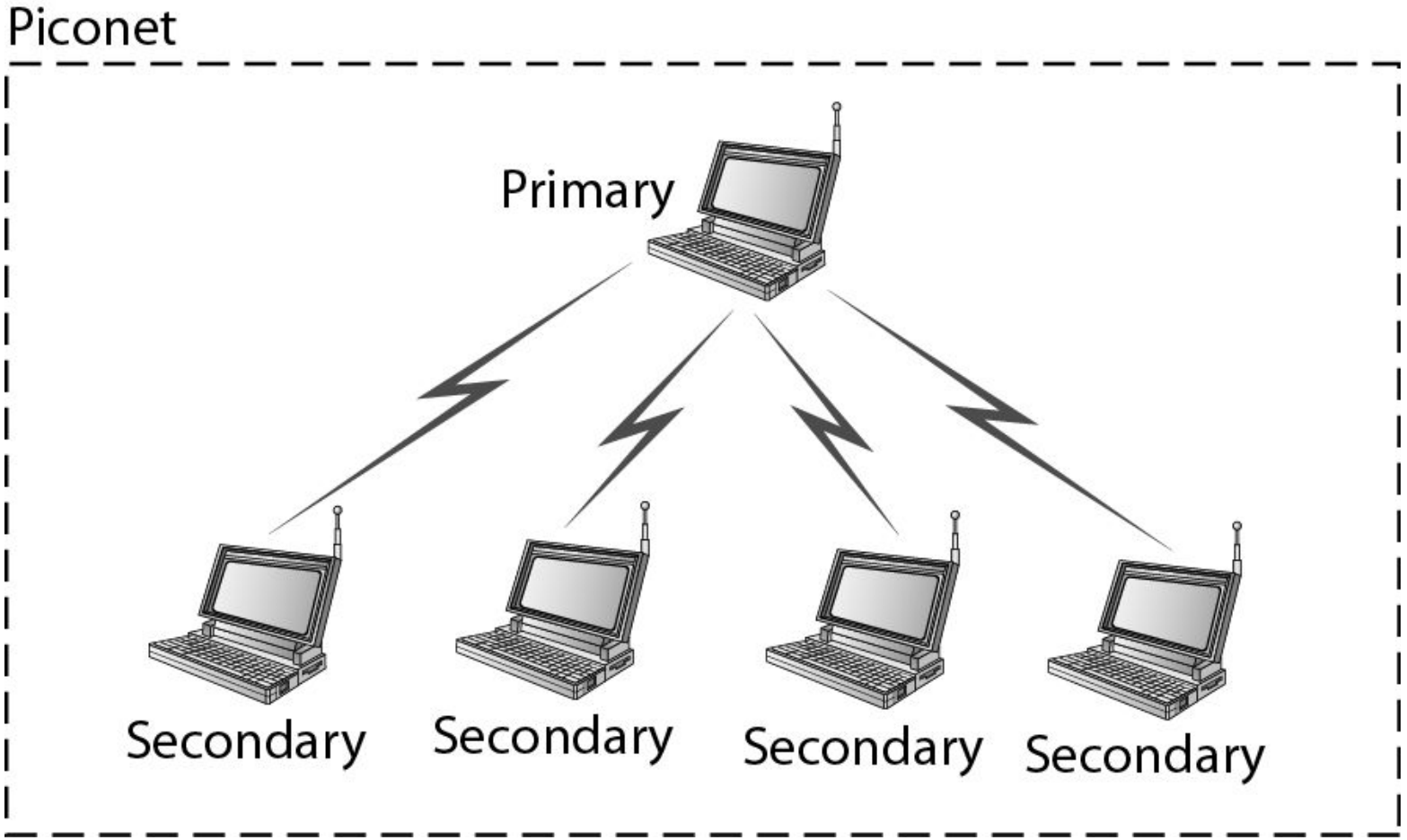
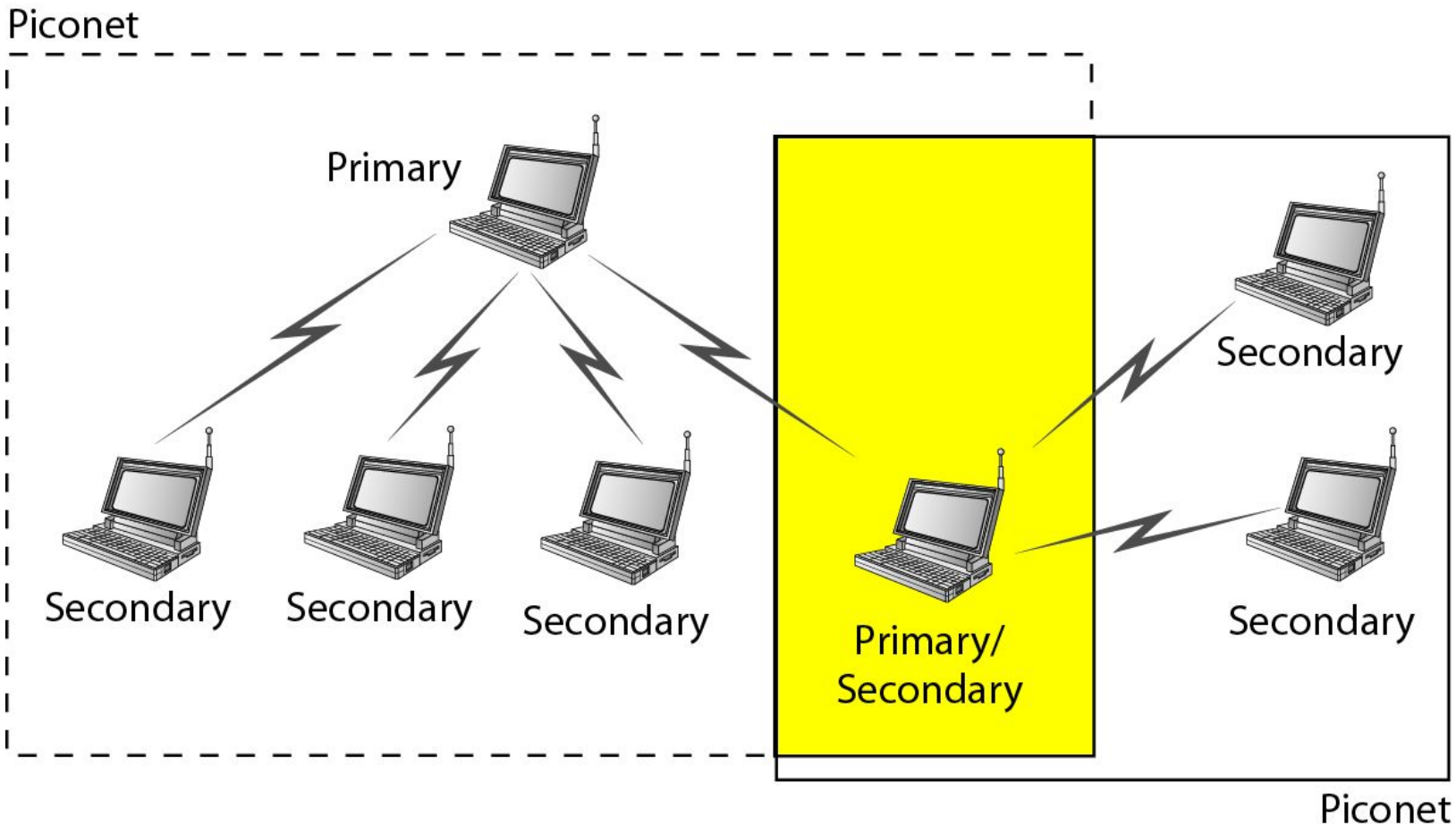
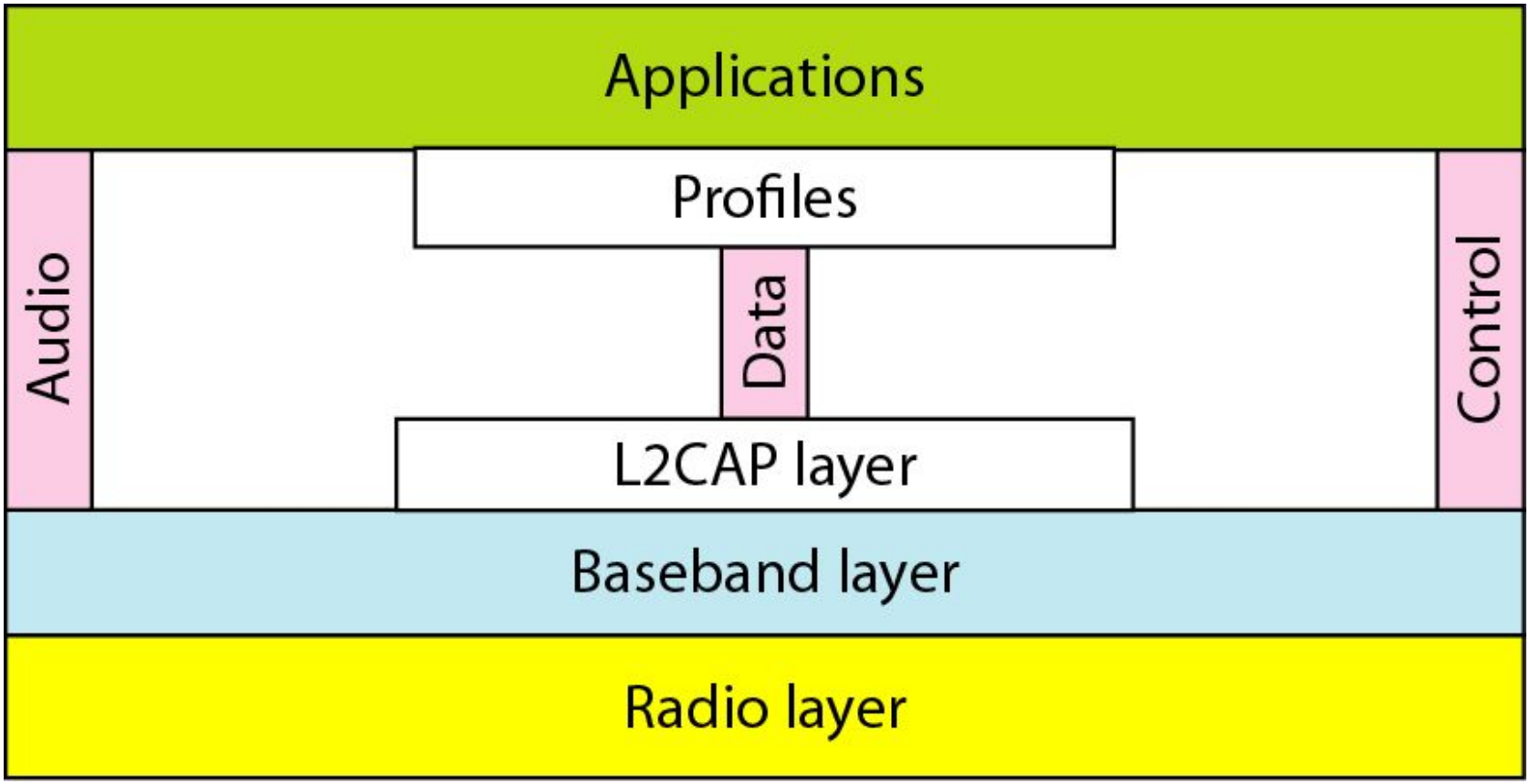

Piconet
Primary
Secondary
Secondary
Secondary
Secondary

Figure 14.20 *Scatternet*



Bluetooth layers

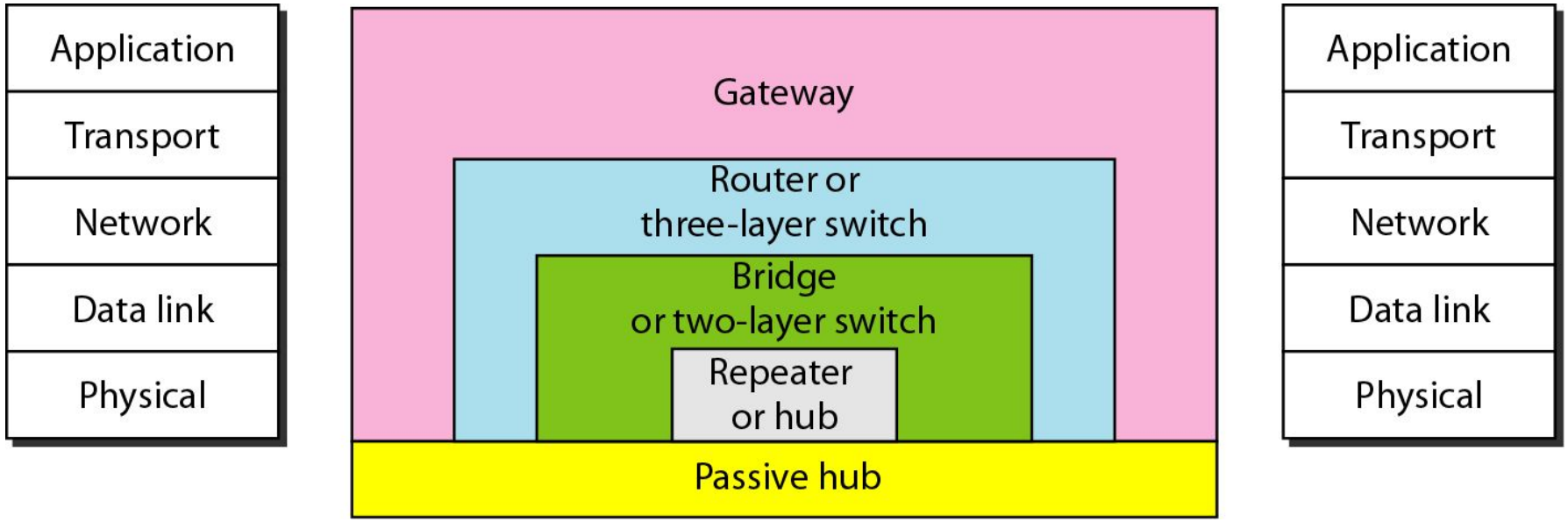


CONNECTING DEVICES

- LANs do not normally operate in isolation. They are connected to one another or to the Internet.
- To connect LANs, or segments of LANs, we use connecting devices. Connecting devices can operate **in** different layers of the Internet model.
- The five categories contain devices which can be defined as

  1. Those which operate below the physical layer such as a passive hub.
  2. Those which operate at the physical layer (a repeater or an active hub).
  3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).
  4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
  5. Those which can operate at all five layers (a gateway).

Five categories of connecting devices

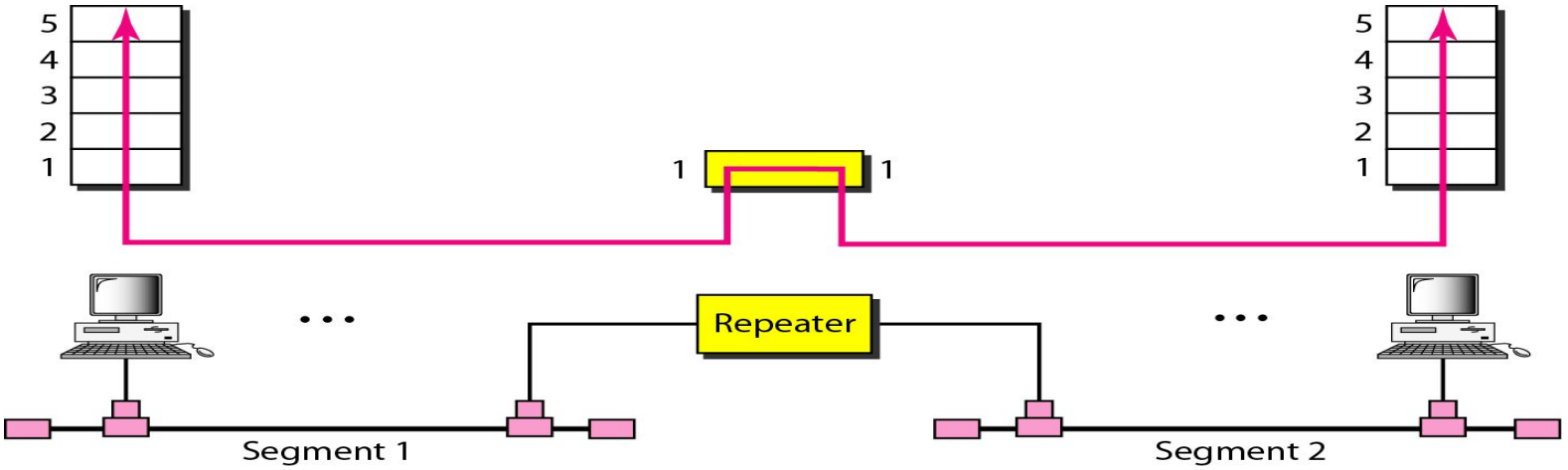


Passive Hubs

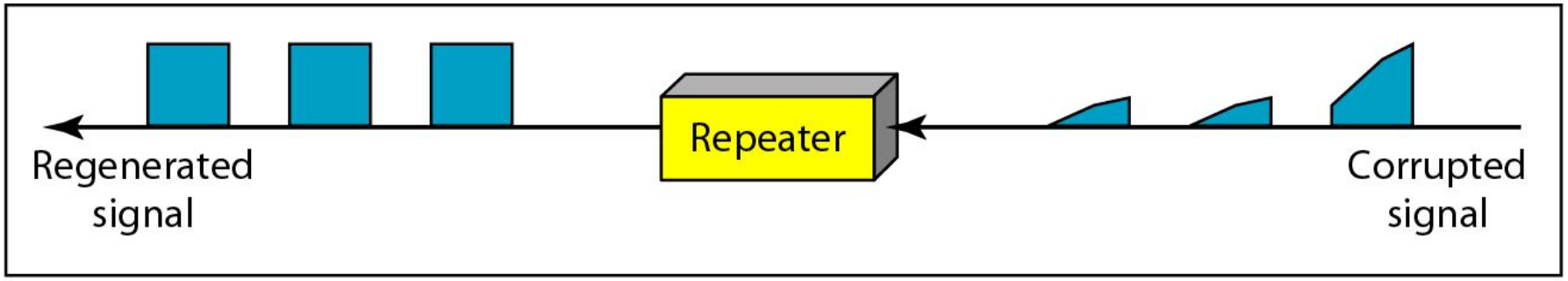
- A **passive hub** is just a connector.
- It connects the wires coming from different branches.
- In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; **the hub is the collision point**.
- This type of a hub is part of the media; its location in the Internet model is below the physical layer.
- Broadcast signals onto the network without amplifying or regenerating.

Repeaters

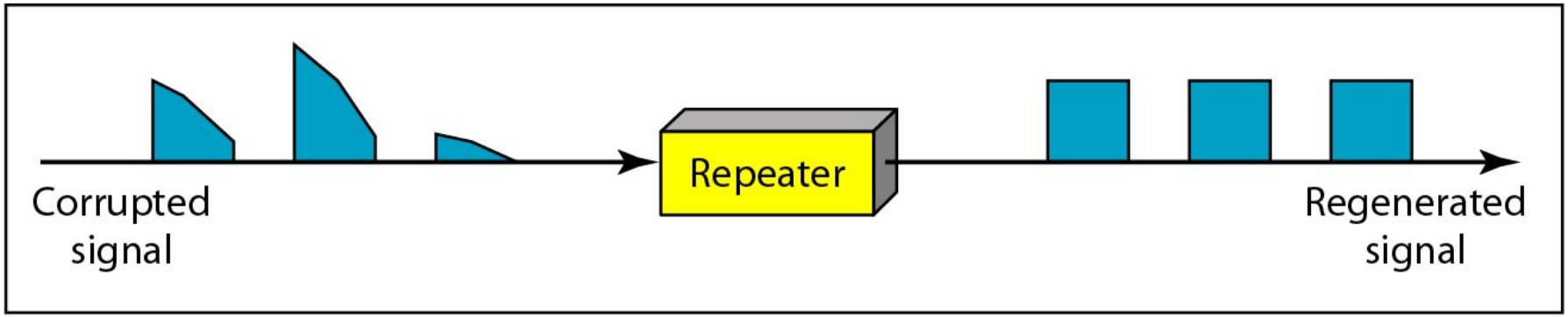
- A repeater is a device that operates only in the physical layer.
- Signals that carry information within a network can travel a **fixed distance** before attenuation endangers the integrity of the data.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern.
- The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN.
- A repeater **connects segments of a LAN**.
- A repeater **forwards every frame; it has no filtering capability**.
- A repeater is a **regenerator, not an amplifier**.



Function of a repeater



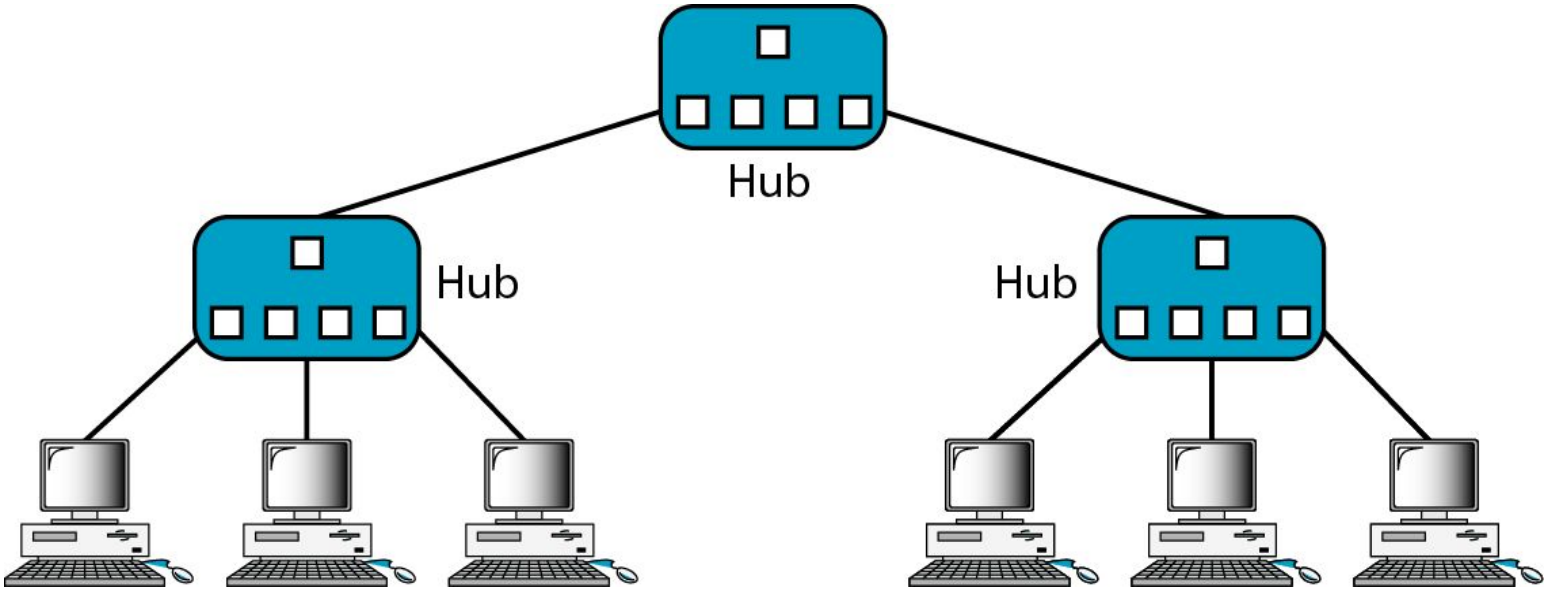
a. Right-to-left transmission.



b. Left-to-right transmission.

Active Hubs

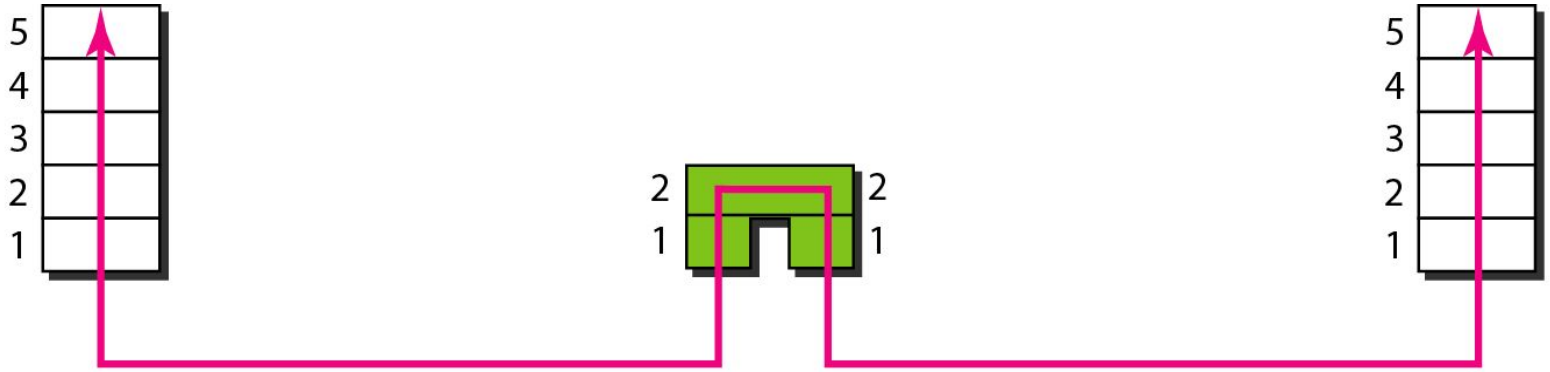
- An active hub is actually a **multiport repeater**.
- It is normally used to create connections between stations in a physical star topology. We have seen examples of hubs in some Ethernet implementations (10Base-T, for example).
- Hubs can also be used to create multiple levels of hierarchy.
- The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).
- Amplify or regenerate the incoming signals before broadcasting.



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.
- 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.

A bridge connecting two LANs



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

Bridge Table

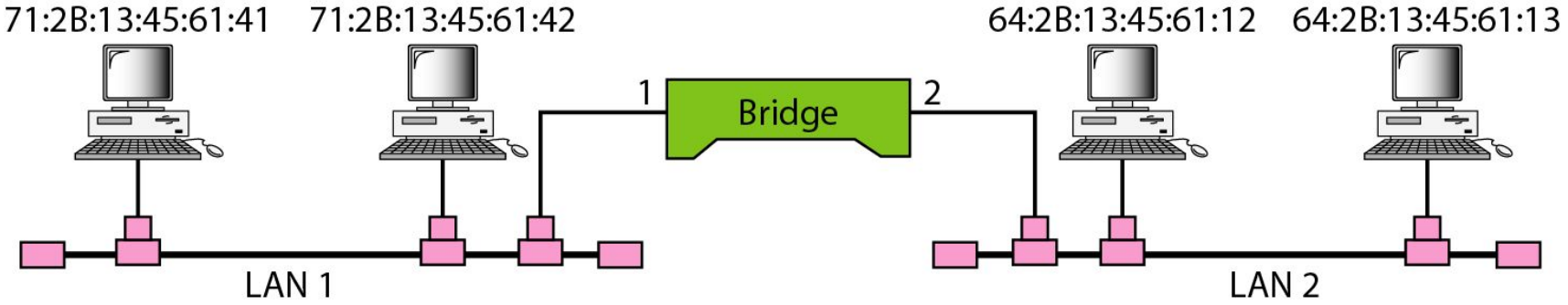
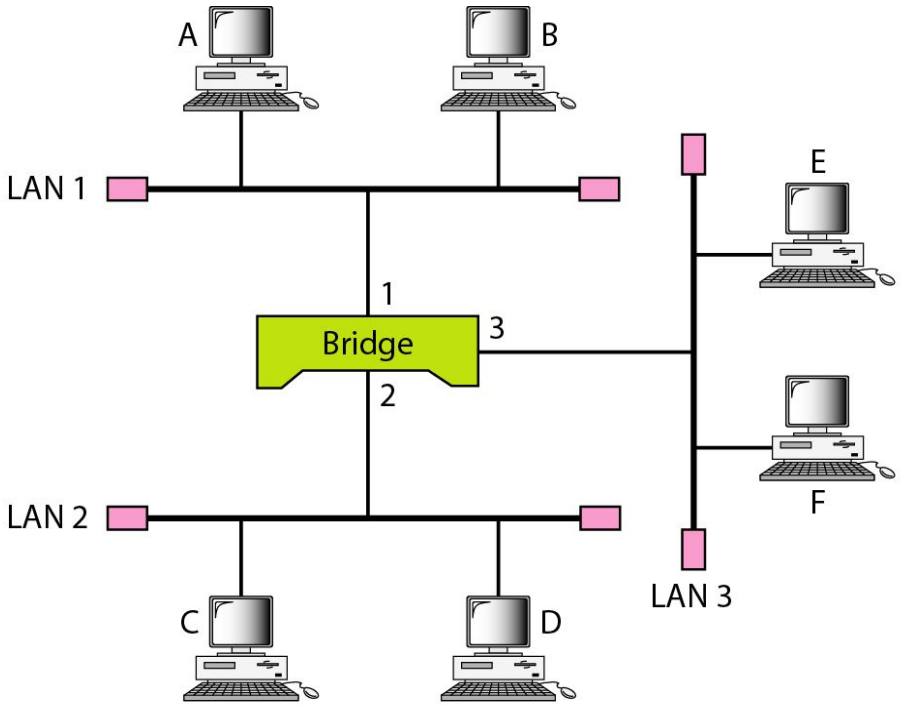


Figure 15.6 *A learning bridge and the process of learning*



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

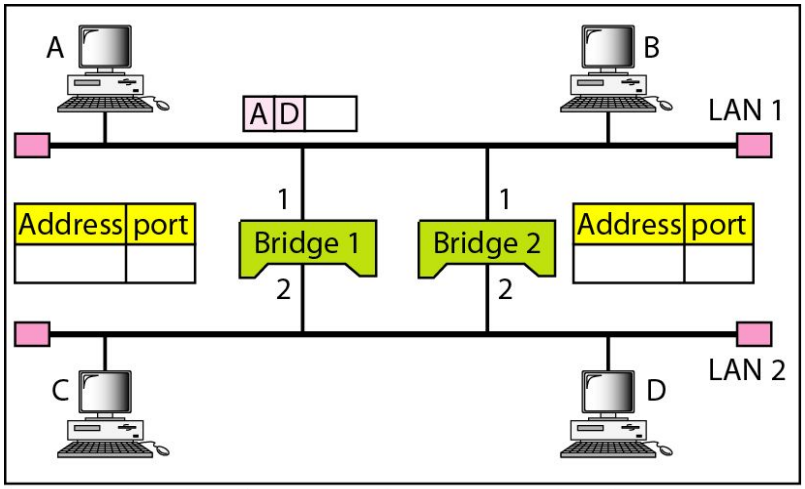
Address	Port
A	1
E	3

c. After E sends a frame to A

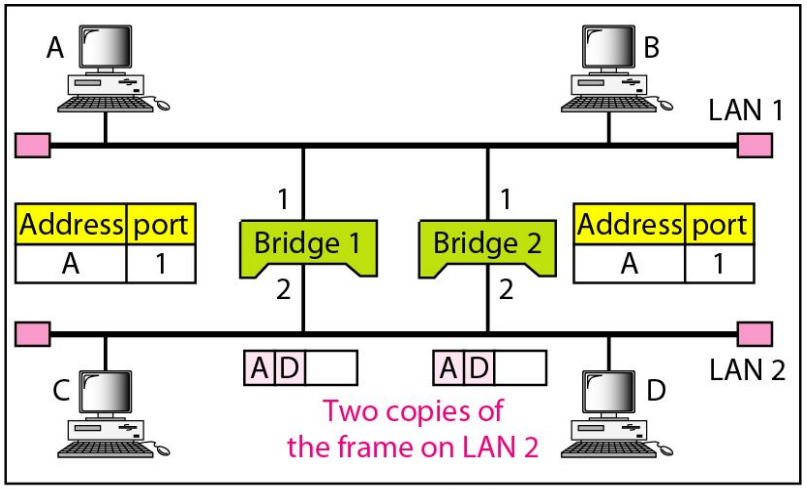
Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

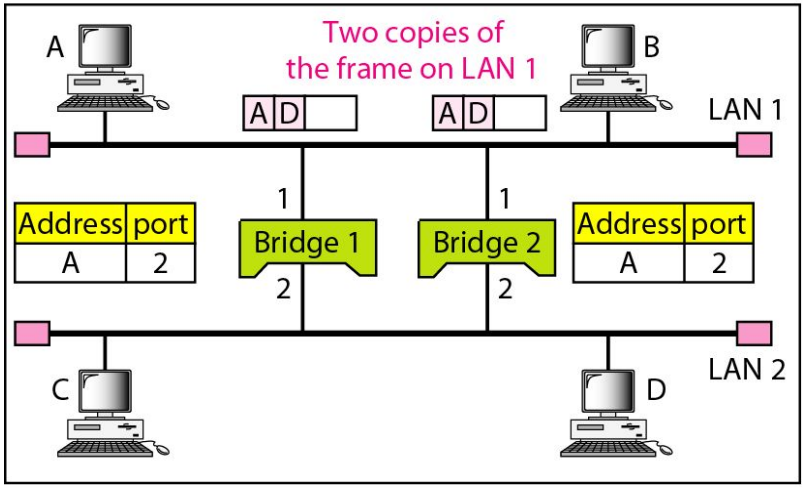
Figure 15.7 *Loop problem in a learning bridge*



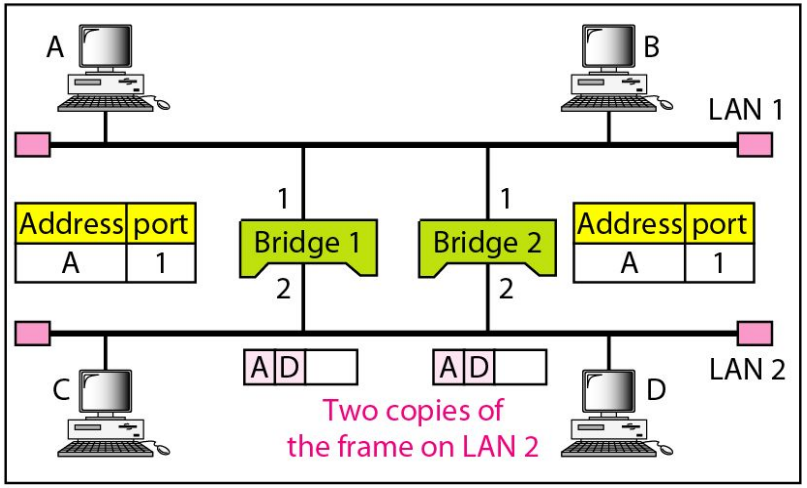
a. Station A sends a frame to station D



b. Both bridges forward the frame

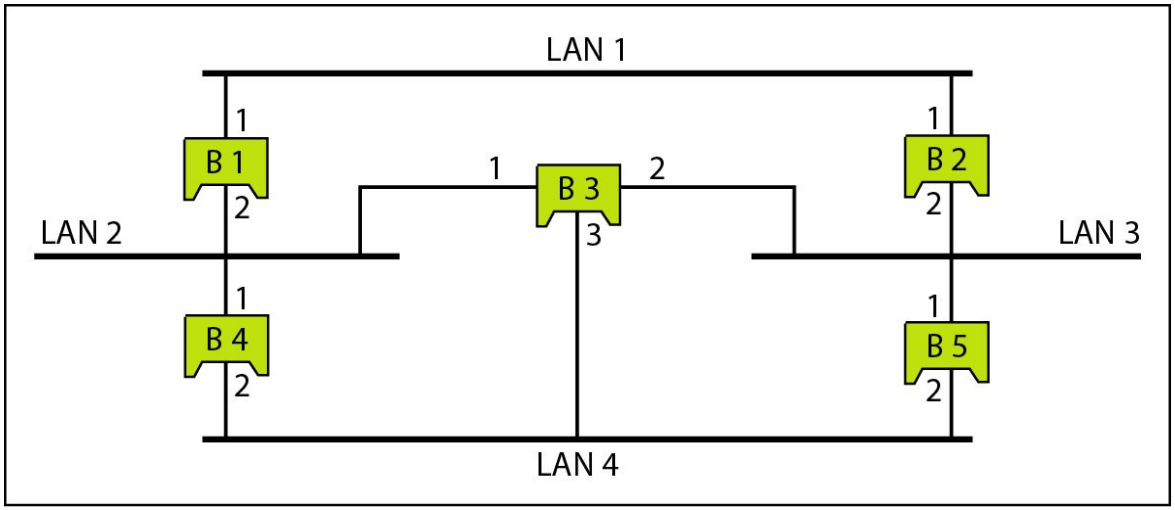


c. Both bridges forward the frame

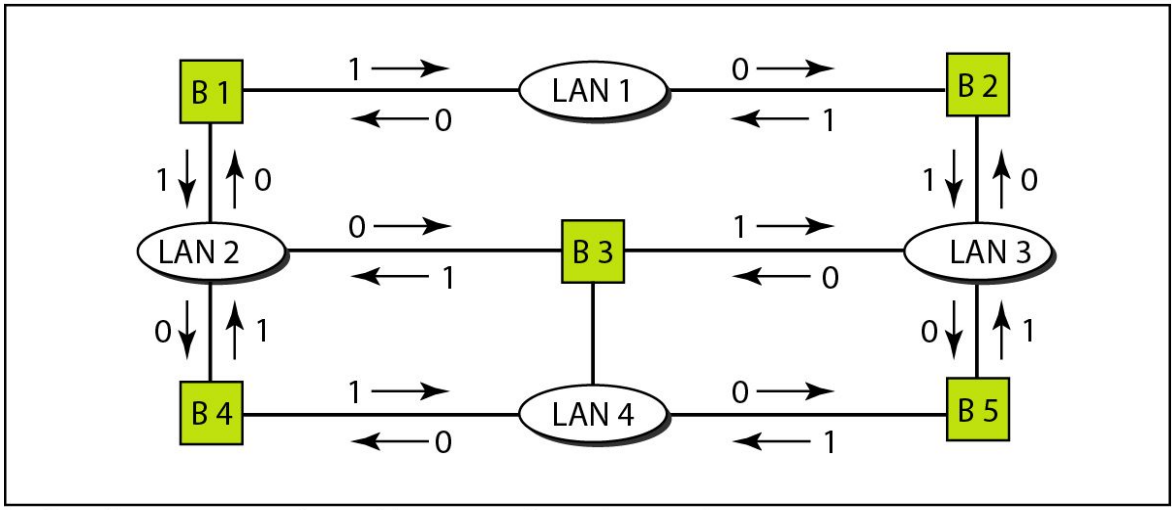


d. Both bridges forward the frame

Figure 15.8 *A system of connected LANs and its graph representation*

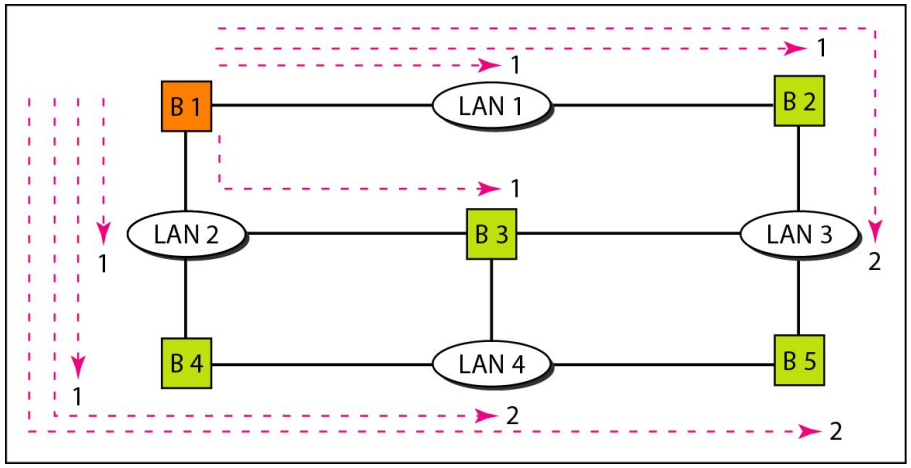


a. Actual system

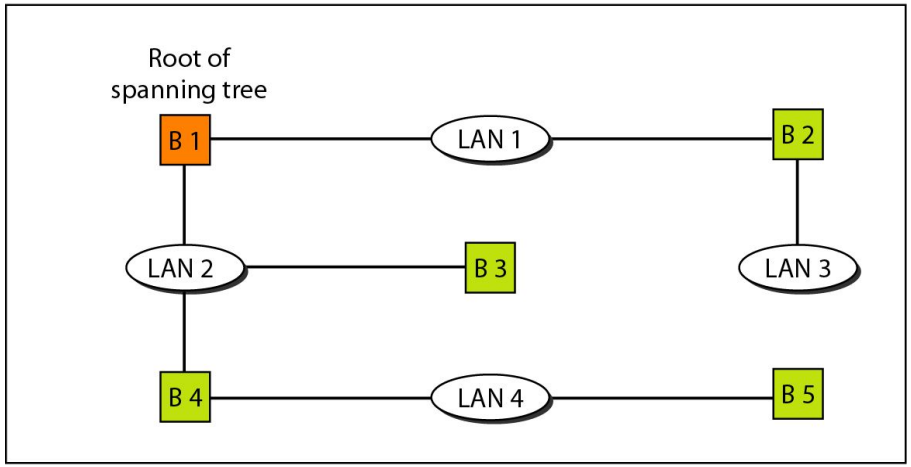


b. Graph representation with cost assigned to each arc

Figure 15.9 *Finding the shortest paths and the spanning tree in a system of bridges*

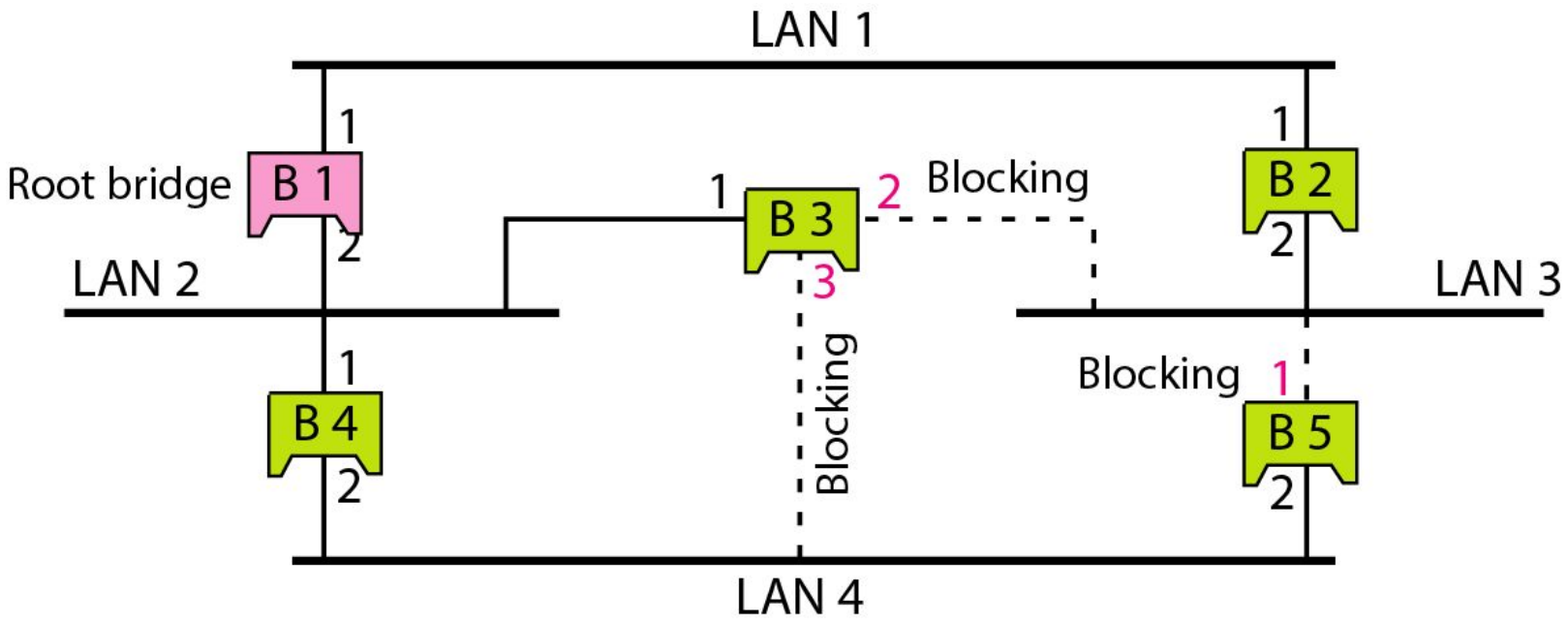


a. Shortest paths



b. Spanning tree

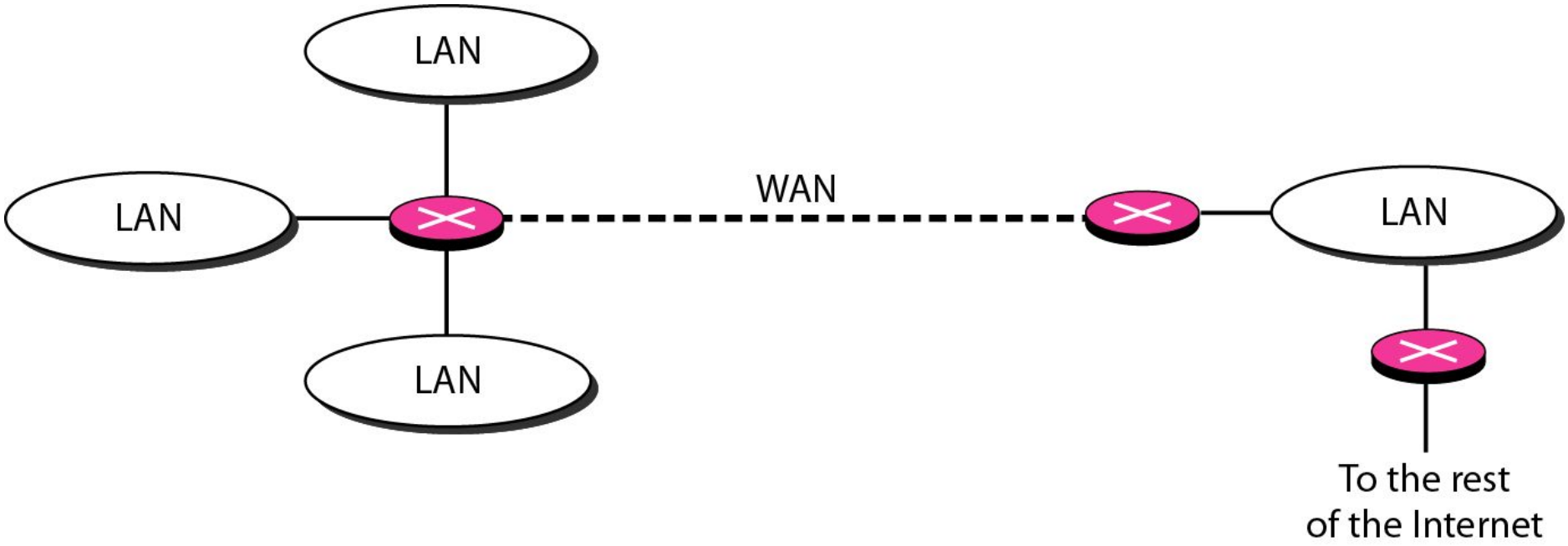
Figure 15.10 *Forwarding and blocking ports after using spanning tree algorithm*



Ports 2 and 3 of bridge B3 are blocking ports (no frame is sent out of these ports).
Port 1 of bridge B5 is also a blocking port (no frame is sent out of this port).

Routers

- A router is a **three-layer device** that routes packets based on their **logical addresses** (host-to-host addressing).
- A router normally **connects LANs and WANs** in the Internet and has a **routing table** that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols.



Gateway

- A gateway is normally a computer that operates in all **five layers of the Internet** or seven layers of OSI model.
- A gateway takes an application message, reads it, and interprets it. This means that it can be used as a **connecting device between two internetworks** that use different models.
- For example, a network designed to use the OSI model can be connected to another network using the Internet model.
- The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message.

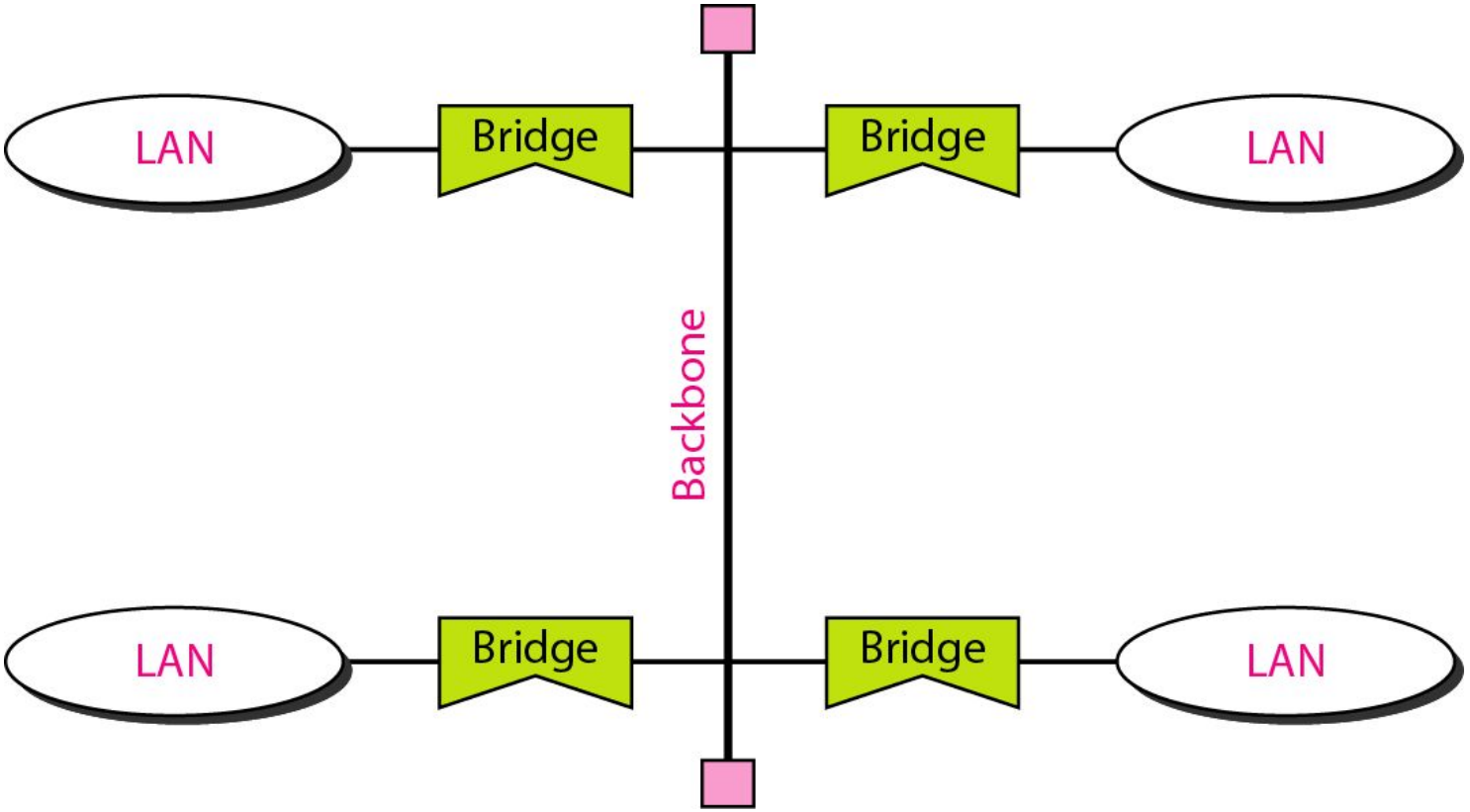
BACKBONE NETWORKS

A backbone network allows several LANs to be connected. In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN, and the backbone connects the LANs.

Note

In a bus backbone, the topology of the backbone is a bus.

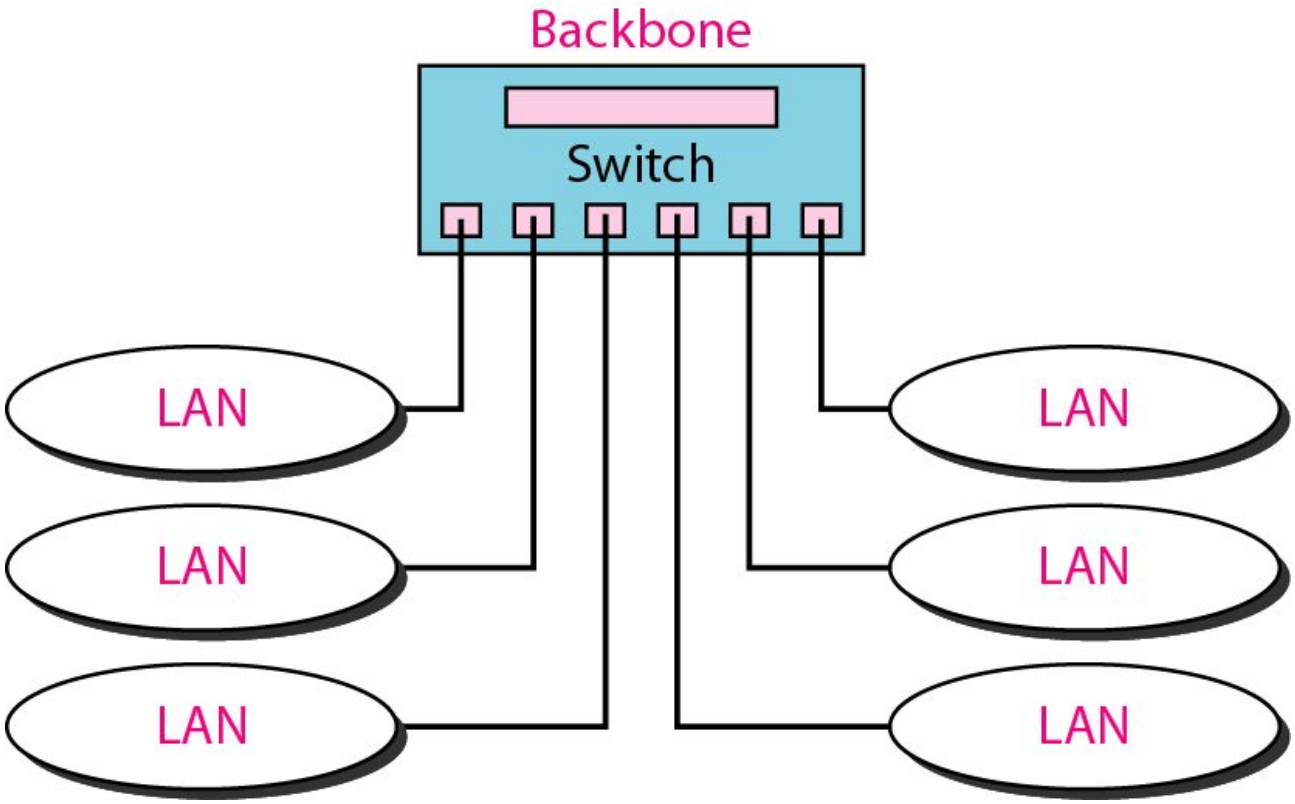
Bus backbone



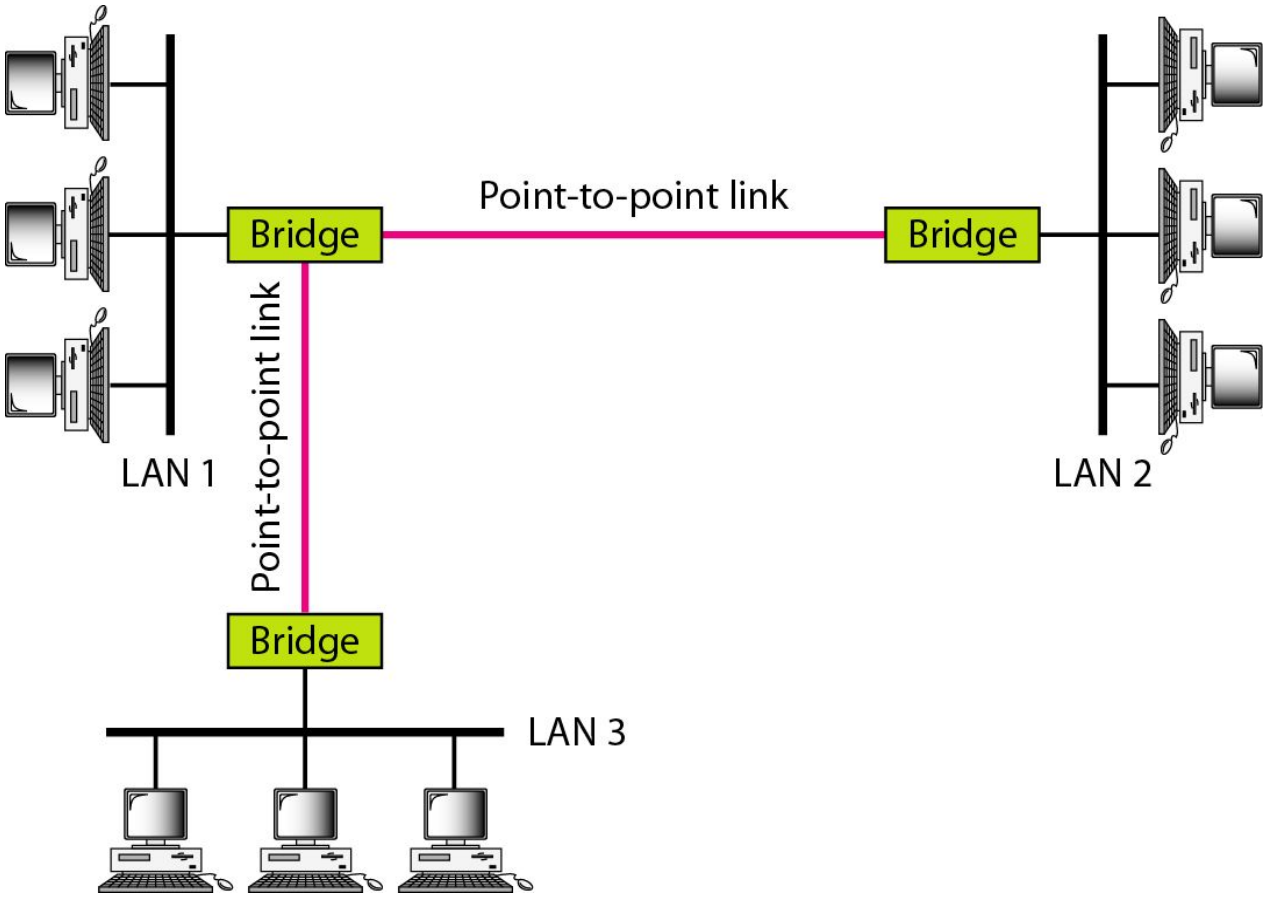
Note

In a star backbone, the topology of the backbone is a star; the backbone is just one switch.

Star backbone



Connecting remote LANs with bridges

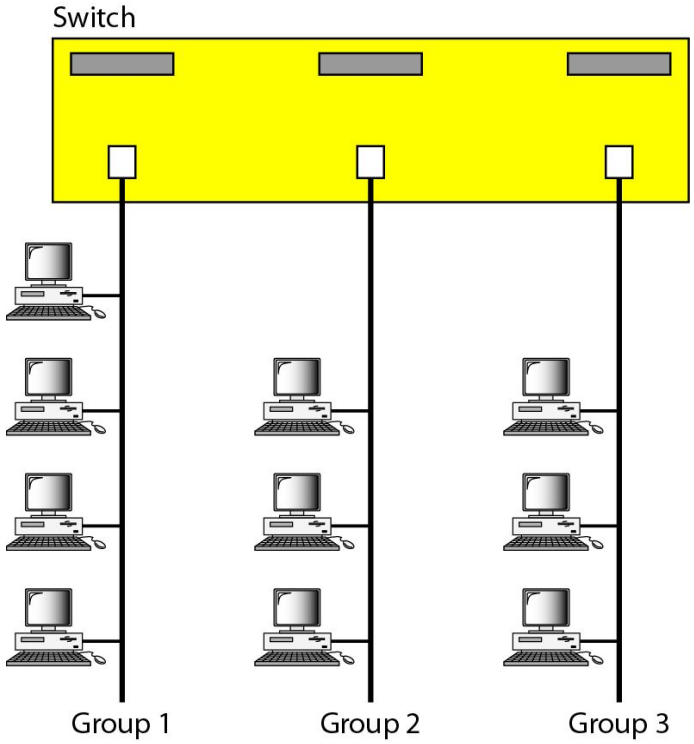


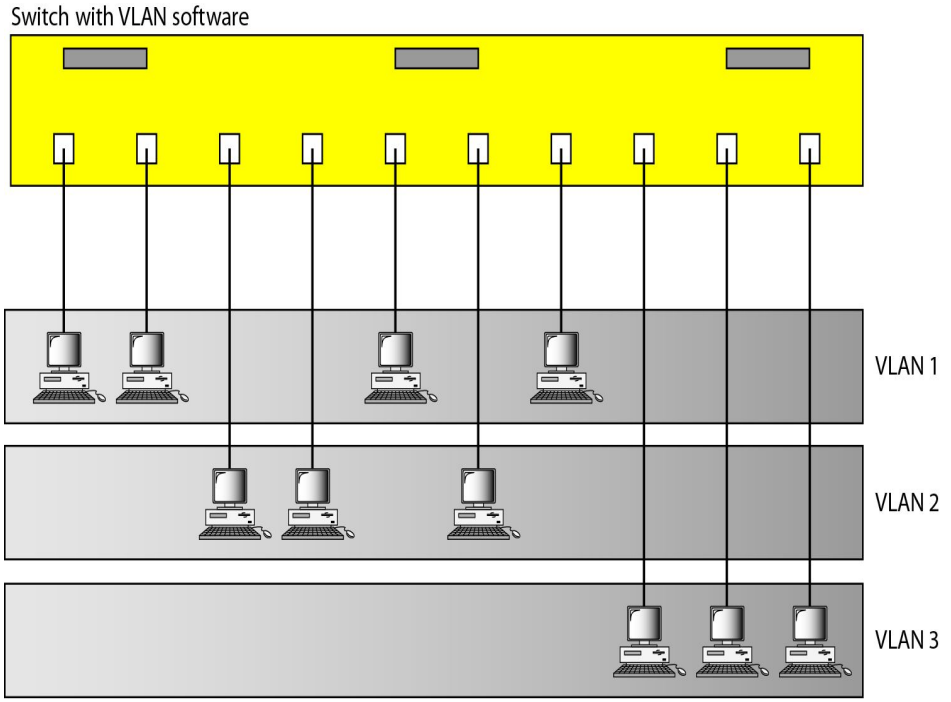
Note

A point-to-point link acts as a LAN in a remote backbone connected by remote bridges.

VIRTUAL LANs

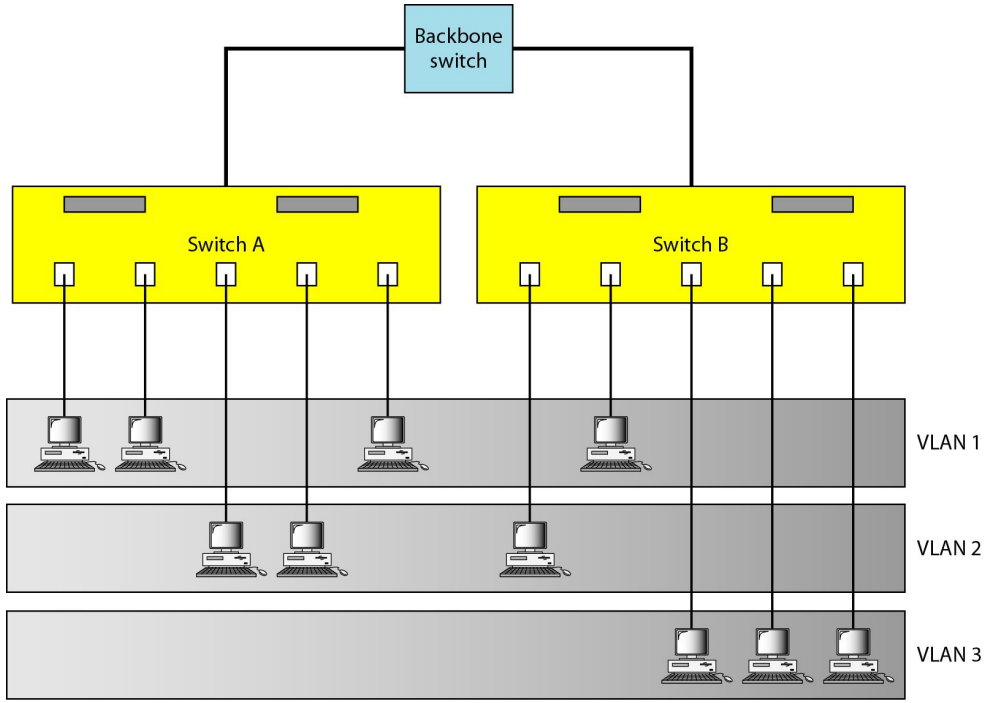
- **VLAN** is a **custom network** which is created from **one or more local area networks**. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN.
- A virtual local area network (VLAN) is defined as a local area network configured by software, not by physical wiring.





VLANs

- A LAN can be divided into several logical LANs called VLANs.
- Each VLAN is a work group in the organization. If a person moves from one group to another, there is no need to change the physical configuration. The group membership in VLANs is defined by software, not hardware. Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN.
- This is a good configuration for a company with two separate buildings. Each building can have its own switched LAN connected by a backbone. People in the first building and people in the second building can be in the same work group even though they are connected to different physical LANs.
- VLANs **create broadcast domains**.



Membership

- Vendors use different characteristics such as **port numbers, MAC addresses, IP addresses, IP multicast addresses**, or a combination of two or more of these.

Port Numbers

- Some VLAN vendors use switch port numbers as a membership characteristic. For example, the administrator can define that stations connecting to ports 1, 2, 3, and 7 belong to VLAN 1; stations connecting to ports 4, 10, and 12 belong to VLAN 2; and so on.

MAC Addresses

- Some VLAN vendors use the 48-bit MAC address as a membership characteristic. For example, the administrator can stipulate that stations having MAC addresses E21342A12334 and F2A123BCD341belong to VLAN 1.

IP Addresses

- Some VLAN vendors use the 32-bit IP address as a membership characteristic. For example, the administrator can stipulate that stations having IP addresses 181.34.23.67, 181.34.23.72, 181.34.23.98, and 181.34.23.112 belong to VLAN 1.

Multicast IP Addresses

- Some VLAN vendors use the multicast IP address as a membership characteristic. Multicasting at the IP layer is now translated to multicasting at the data link layer.

Configuration

- Stations are configured in one of three ways: manual, semiautomatic, and automatic.

Manual Configuration

- In a manual configuration, the network administrator uses the VLAN software to manually assign the stations into different VLANs at setup.
- Later migration from one VLAN to another is also done manually.
- This is not a physical configuration; it is a logical configuration.
- The term *manually* here means that the administrator types the port numbers, the IP addresses, or other characteristics, using the VLAN software.

Automatic Configuration

- In an automatic configuration, the stations are automatically connected or disconnected from a VLAN using criteria defined by the administrator.
- For example, the administrator can define the project number as the criterion for being a member of a group. When a user changes the project, he or she automatically migrates to a new VLAN.

Semiautomatic Configuration

- A semiautomatic configuration is between a manual configuration and an automatic configuration. Usually, the initializing is done manually, with migrations done automatically.

Communication Between Switches

- In a multi-switched backbone, each switch must know not only which station belongs to which VLAN, but also the membership of stations connected to other switches.
- **Three methods have been devised for this purpose:** table maintenance, frame tagging, and time-division multiplexing.

Table Maintenance

- In this method, when a **station sends a broadcast frame** to its group members, the switch creates an **entry in a table and records station membership.** The switches send their **tables to one another periodically for updating.**

Frame Tagging

- In this method, when a **frame is traveling between switches**, an **extra header** is added to the **MAC frame** to define the destination VLAN. The frame tag is used by the receiving switches to determine the VLANs to be receiving the broadcast message.

Time-Division Multiplexing (TDM)

- In this method, the connection (trunk) between switches is divided into timeshared channels. For example, if the total number of VLANs in a backbone is five, each trunk is divided into five channels. The traffic destined for VLAN 1 travels in channel 1, the traffic destined for VLAN 2 travels in channel 2, and so on. The receiving switch determines the destination VLAN by checking the channel from which the frame arrived.

IEEE standard

- **IEEE 802.1Q**, often referred to as **Dot1q**, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network.
- In 1996, the IEEE 802.1 subcommittee passed a standard called 802.1Q that defines the format for frame tagging.
- The standard also defines the format to be used in multi-switched backbones and enables the use of multivendor equipment in VLANs.
- **Advantages**

Cost and Time Reduction

- VLANs can reduce the migration cost of stations going from one group to another.
- Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software.

Creating Virtual Work Groups

- VLANs can be used to create virtual work groups. For example, in a campus environment, professors working on the same project can send broadcast messages to one another without the necessity of belonging to the same department. This can reduce traffic if the multicasting capability of IP was previously used.

Security

- VLANs provide an extra measure of security. People belonging to the same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.

VLAN

- State the IEEE standard for VLAN.
- How does a VLAN save a company time and money?
- List the advantages for VLAN.
- How does a VLAN reduce network traffic?
- What is the basis for membership in a VLAN?