MODULE 2

Chapter Outline

3.1 Wired Local Area Network

3.2 Wireless LANs

3.3 Point-to-Point WANs

3.4 Switched WANs

3.5 Connecting Devices

Wired LAN: IEEE Standards-Frame Format-Addressing-Ethernet evolution. **Wireless LANS**: IEEE802.11, MAC Sub layer, Addressing Mechanism, Bluetooth-Architecture, Frame format, **Switched WANS**: X.25, ATM-ATM Architecture, ATM Layers. **Network Layer:** Introduction, Switching-Circuit switching, Packet switching, connection oriented and connectionless service, services provided by network layer.

3-1 WIRED LOCAL AREA NETWORKS

- **A local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus.**
- **Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet.**
- **The LAN market has seen several technologies such as Ethernet, token ring, token bus, FDDI, and ATM LAN, but Ethernet is by far the dominant technology.**

IEEE Standards

The architecture developed by the IEEE 802 LAN standards committee is known as IEEE 802 reference model.

It specifies the functions of the physical layer and data link layer of major LAN protocols.

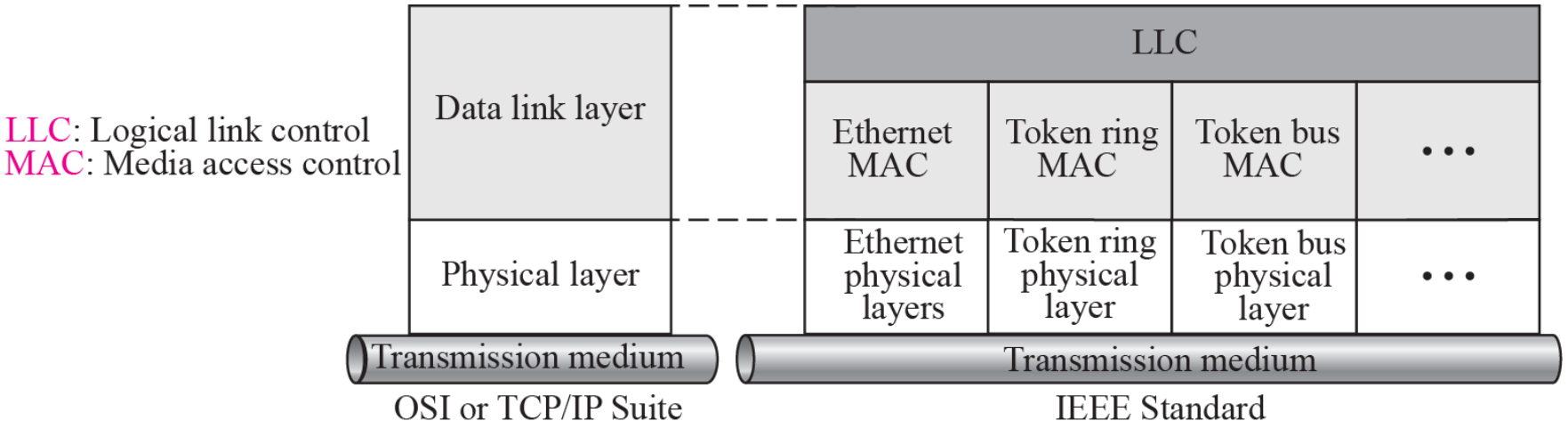
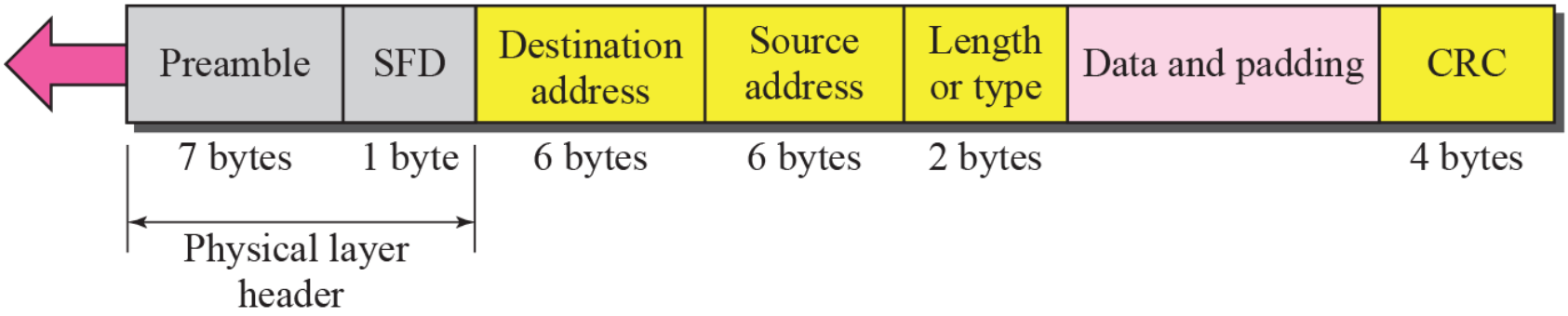


Figure 3.2 *Ethernet Frame*

Frame Format

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

SFD: Start frame delimiter, flag (10101011)

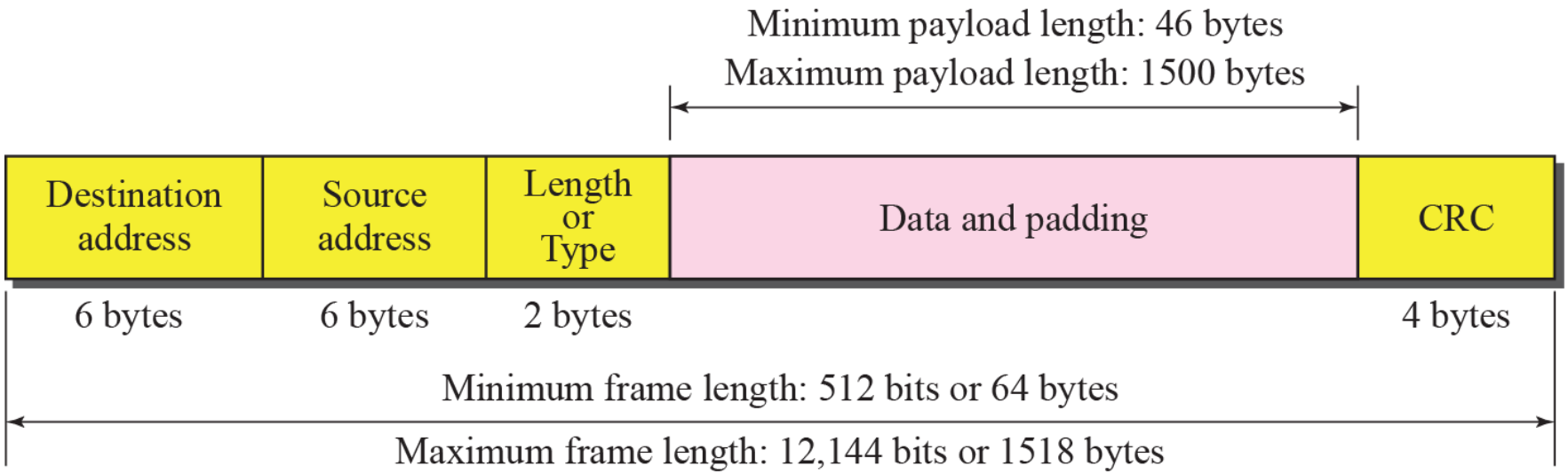


Preamble:-Consists alternate 0's and 1's that alerts the receiving system about the coming frame.

SFD:-Signals the beginning of the frame.

Figure 3.3 *Maximum and minimum lengths*

Frame Length



Note

Minimum length: 64 bytes (512 bits)

Maximum length: 1518 bytes (12,144 bits)

Figure 3.4 *Ethernet address in hexadecimal notation*

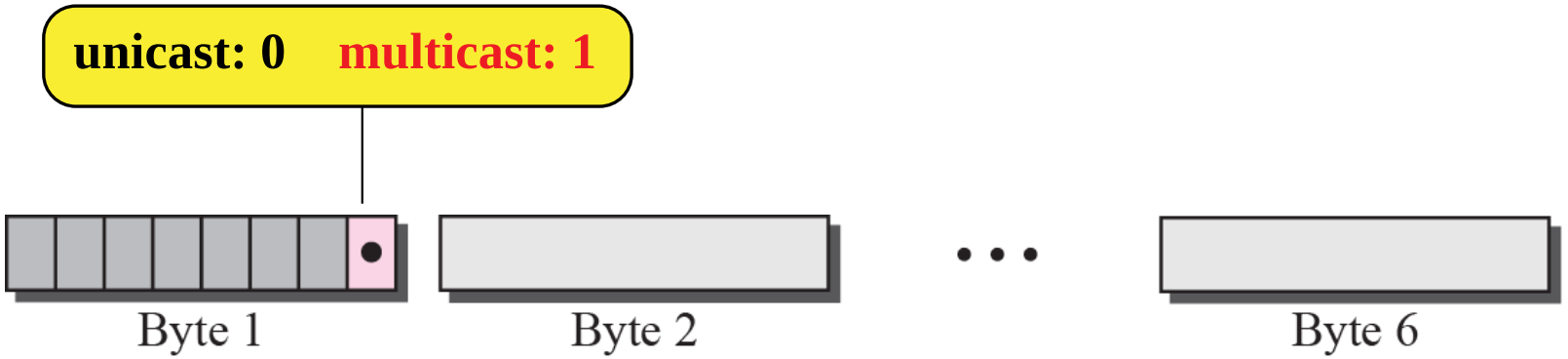
d: Hexadecimal digit

$$d_1d_2 : d_3d_4 : d_5d_6 : d_7d_8 : d_9d_{10} : d_{11}d_{12}$$

6 bytes = 12 hexadecimal digits = 48 bits

Data link address,Physical address, MACaddress

Figure 3.5 *Unicast and multicast addresses*



The LSB of the first byte defines the type of address.
If the bit is 0,the address is unicast;otherwise multicast

Note

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

Example 3.1

Define the type of the following destination addresses:

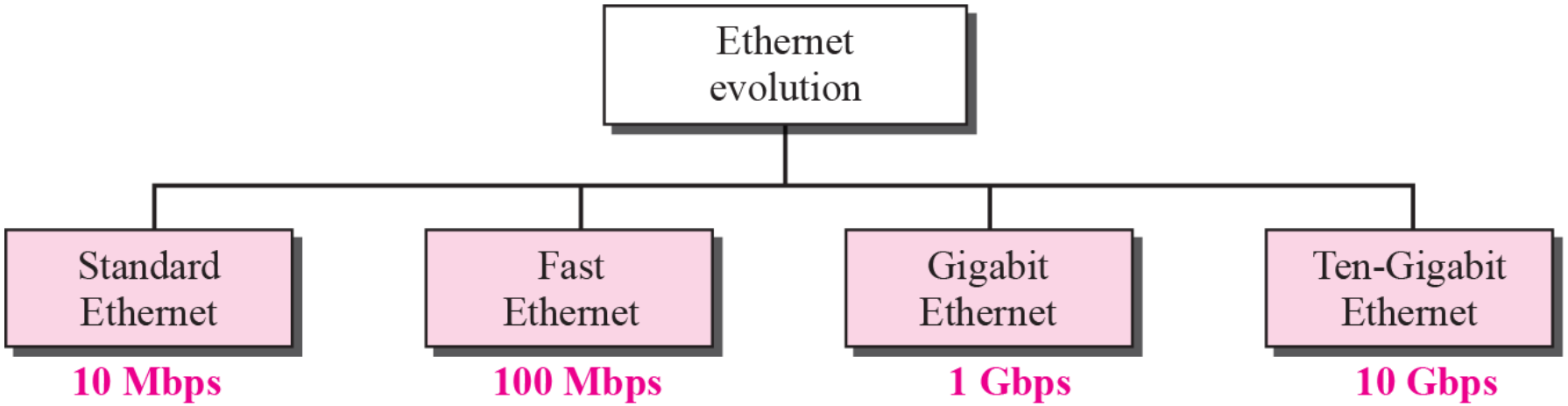
a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution

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

a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are F's.

Figure 3.6 *Ethernet evolution through four generations*



Standard Ethernet

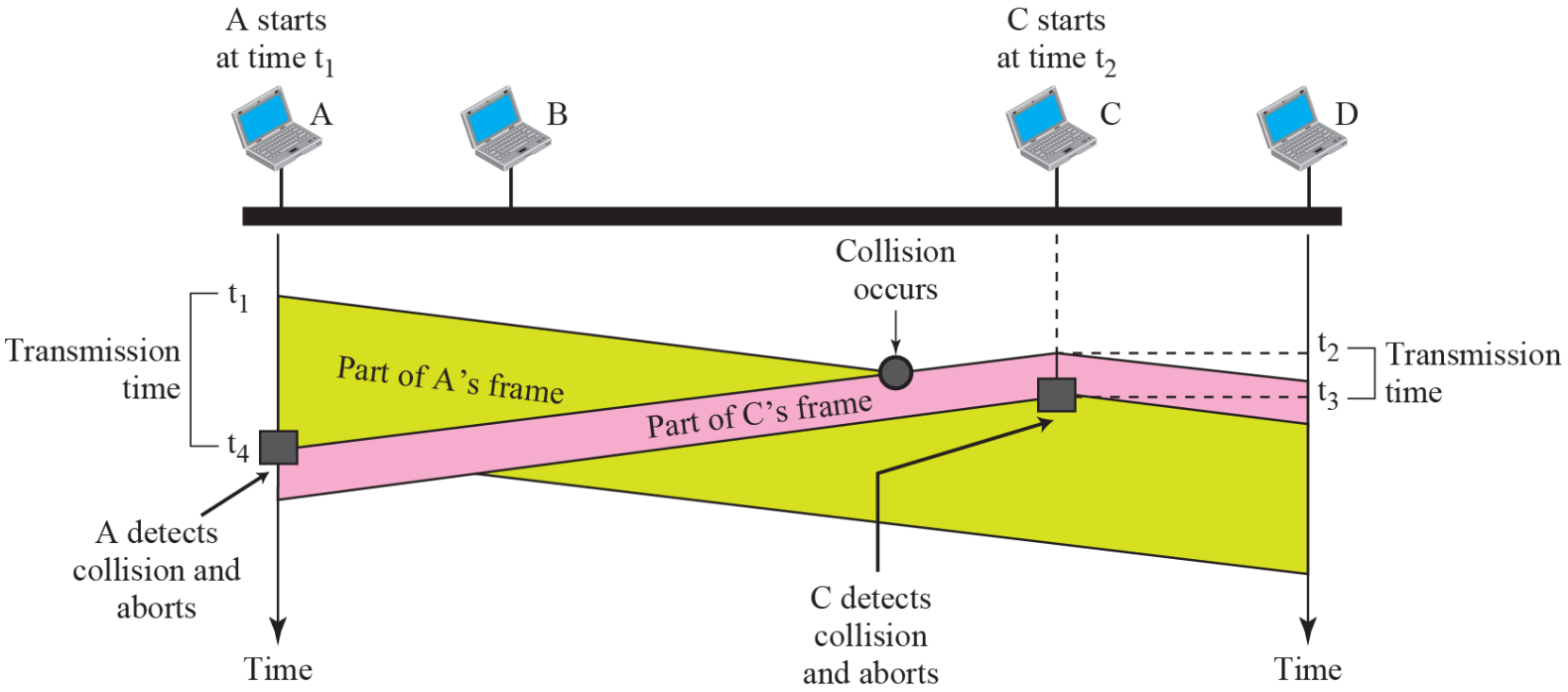
Access Method:CSMA/CD

- **Protocols that listen for a carrier and act accordingly are called carrier sense protocols.**
- **CSMA method minimise the collision and increase the performance.**
- **The chance of collision can be reduced if a station senses the medium before trying to use it.**
- **CSMA can reduce collision but it cannot eliminate it .**
- **When a station sends a frame it takes time to sense it by other stations.**

CSMA – Carrier Sense Multiple Access, which senses the medium before transmission.
CSMA/CD - Carrier Sense Multiple Access with Collision Detection, which tells the station what to do when a collision is detected.

Frame transmission time=2*Propagation time

Figure 3.8 *Collision of the first bit in CSMA/CD*



Example 3.3

In the standard Ethernet, if the maximum propagation time is 25.6 μs, what is the minimum size of the frame?

Solution

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

Figure 3.9 *CSMA/CD flow diagram*

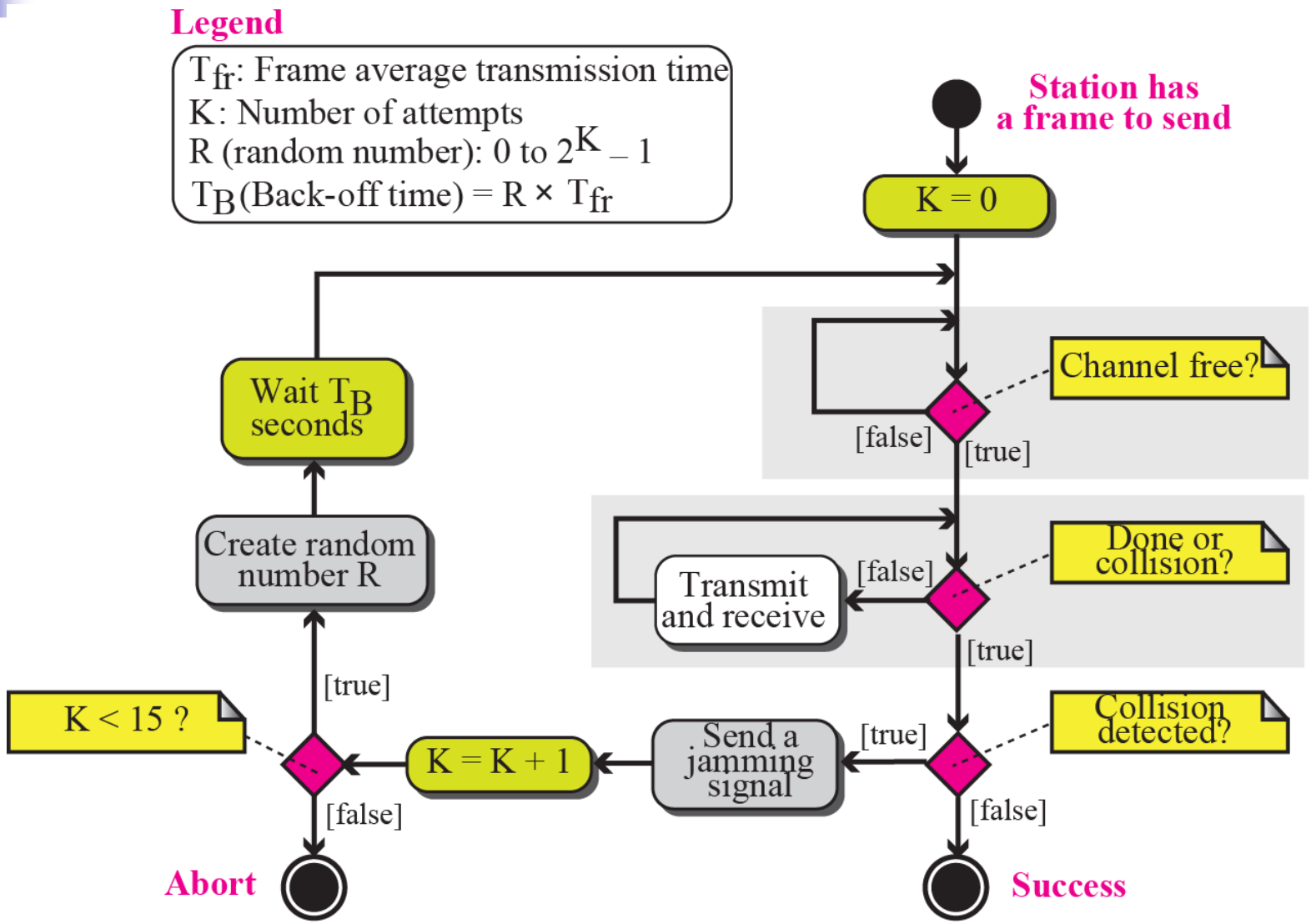
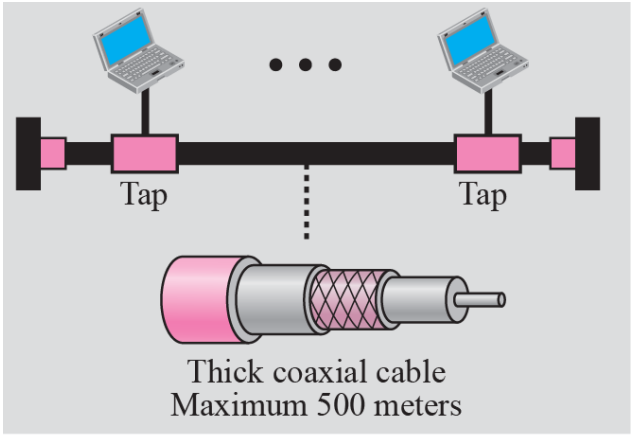


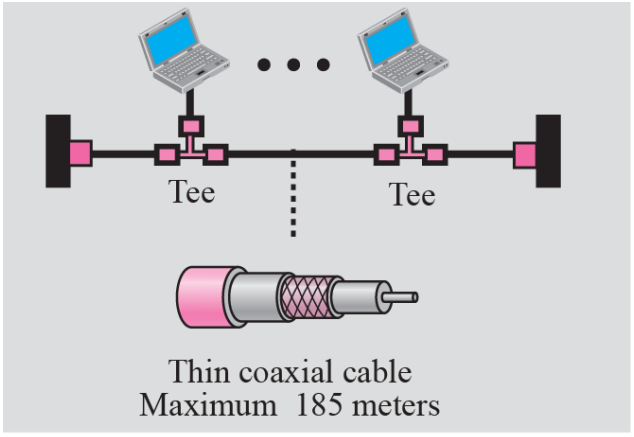
Table 3.1 *Summary of Standard Ethernet implementations*

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10B*
Medium	Thick coax	Thin coax	2 UTP	2
Maximum length	500 m	185 m	100 m	20

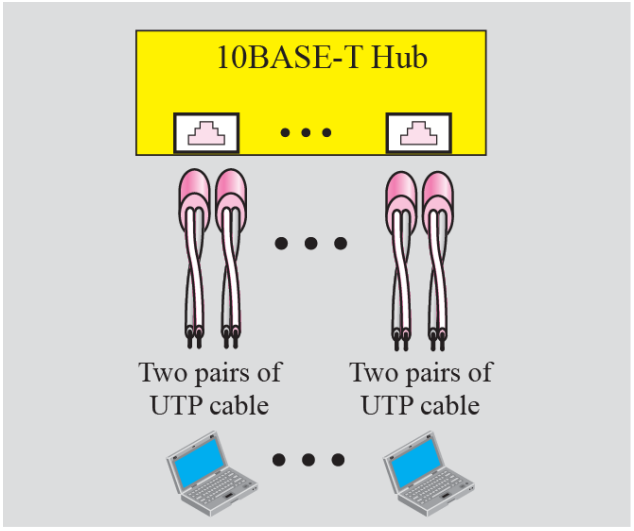
Figure 3.10 *Standard Ethernet implementation*



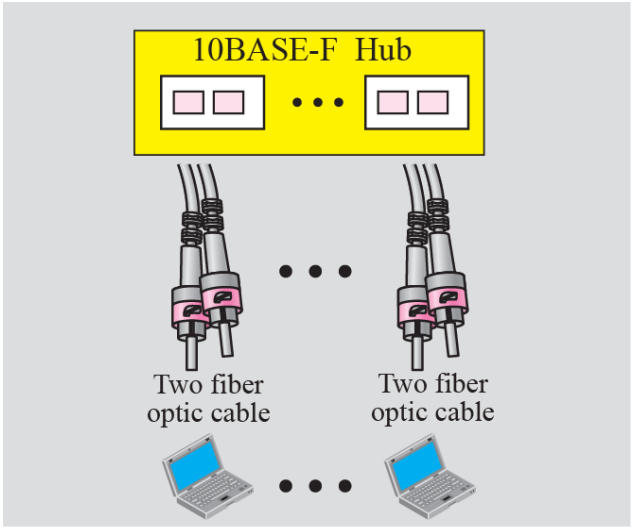
a. 10BASE5



b. 10BASE2



c. 10BASE-T



d. 10BASE-F

FAST ETHERNET

- IEEE created Fast Ethernet under the name 802.3u (enhanced standard of 802.3 standard.
- Fast Ethernet 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.

MAC sublayer

- MAC sublayer of fast Ethernet dropped the bus topologies and kept only two choices of star topology ie, half duplex and full-duplex.
- In a 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.
- For half duplex Fast Ethernet, the access method is CSMA/CD.
- For full duplex Fast Ethernet there is no need for CSMA/CD, but it keeps CSMA/CD for backward compatibility with Standard Ethernet.

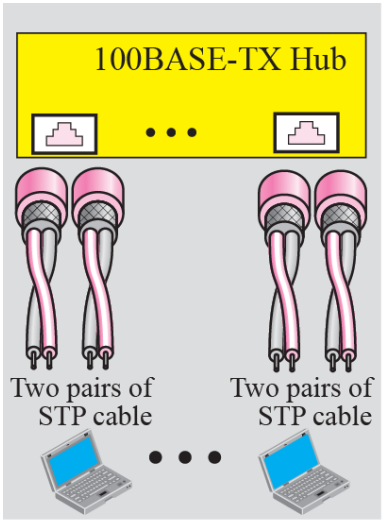
Autonegotiation

- Fast Ethernet has a feature called autonegotiation.
- It allows two devices to negotiate the mode or data rate of operation.
- It allow incompatible devices to connect to one another.
- Example
- A device with 10 Mbps capacity can communicate with a device with 100 Mbps capacity.
- It allow one device to have multiple capabilities.

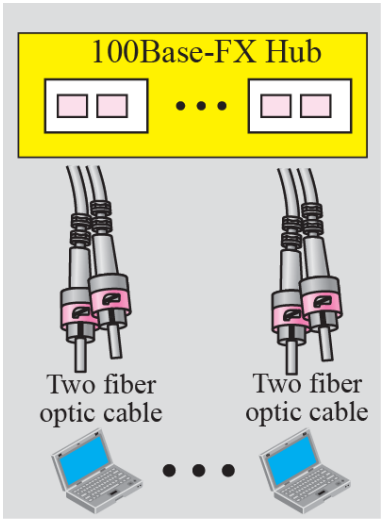
Table 3.2 *Summary of Fast Ethernet implementations*

Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	STP	Fiber	UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m

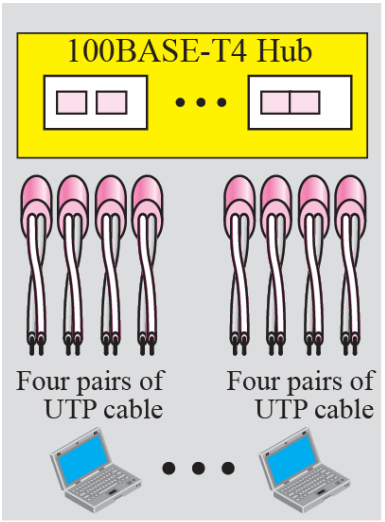
Figure 3.11 *Fast Ethernet implementation*



a. 100BASE-TX



b. 100BASE-FX



c. 100BASE-T4

GIGABIT ETHERNET

- IEEE created Gigabit Ethernet under the name 802.3z (enhanced standard of 802.3 standard).
- It can transmit data at a higher data rate of 1000 Mbps (1 Gbps).
- It is compatible with Standard or Fast Ethernet.
- It keep the same 48-bit address, same frame format and same minimum and maximum frame lengths.
- It support autonegotiation as defined in Fast Ethernet.
- Gigabit Ethernet has two approaches for medium access : half-duplex mode and full-duplex mode.

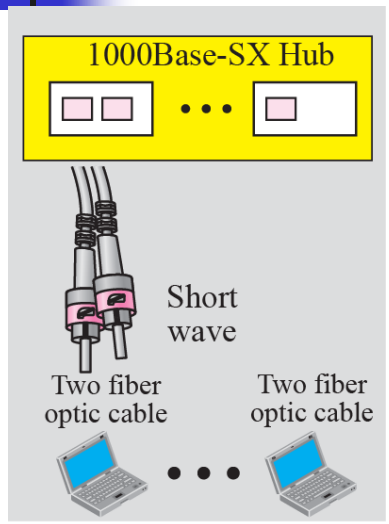
Table 3.3 *Summary of Gigabit Ethernet implementations*

Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000*
Media	Fiber short-wave	Fiber long-wave	STP	Cat
Number of wires	2	2	2	
Maximum length	550 m	5000 m	25 m	1

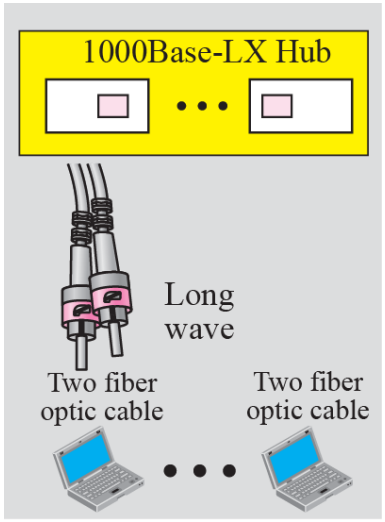
Note

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.

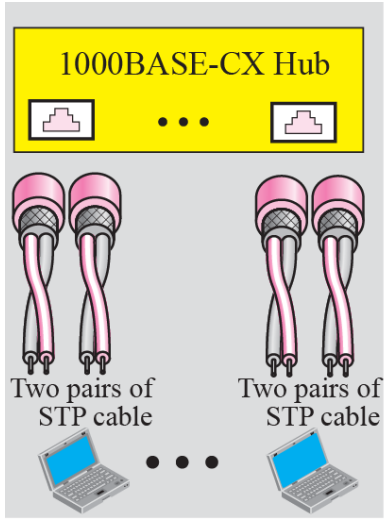
Figure 3.12 *Gigabit Ethernet implementation*



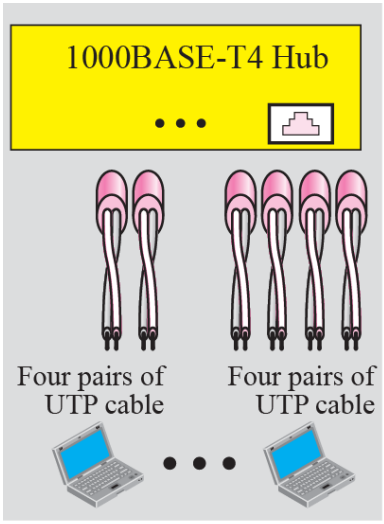
a. 1000BASE-SX



b. 100BASE-LX



c. 1000BASE-CX



d. 1000BASE-T4

- **TEN-GIGABIT ETHERNET**
- The IEEE committee created Ten-Gigabit Ethernet and called it standard 802.3ae.
- Its data rate is 10 Gbps.
- It is compatible with Standard, Fast and Gigabit Ethernet.
- It keep the same 48-bit address, same frame format and the same minimum and maximum frame lengths.
- It allow the interconnection of existing LANs into MAN or a WAN.
- MAC sublayer
- It operates in full duplex mode. So there is no need for CSMA/CD.

Table 3.4 *Ten-Gigabit Ethernet Implementation*

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	multi-mode fiber	single-mode fiber	single-mode fibe
Number of wires	2	2	2
Maximum length	300 m	10,000 m	40,000 m

3-2 WIRELESS LANS

Wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere.

In this section, we concentrate on two wireless technologies for LANs: IEEE 802.11 wireless LANs, sometimes called wireless Ethernet, and Bluetooth, a technology for small wireless LANs.

IEEE 802.11

The std defines two kinds of services

1)BSS(basic service set)
2)ESS(extended service set)

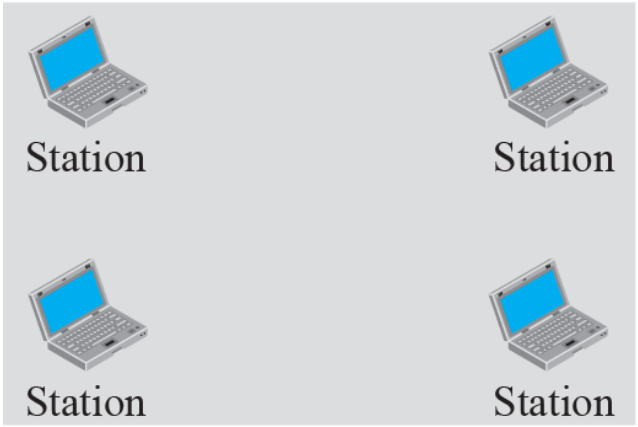
The smallest building block of a wireless LAN is a BSS.
BSS consists of some stations executing the same MAC protocol
A BSS may connect to a backbone 'distribution system' (DS) through an access point (AP).

If one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the source station to the AP and then from AP to the destination station.
A MAC frame from a station in the BSS to a remote station is sent from the source station to the AP and then to the destination over the DS.

An 'extended service set' (ESS) consists of two or more basic service sets interconnected by a distribution system.

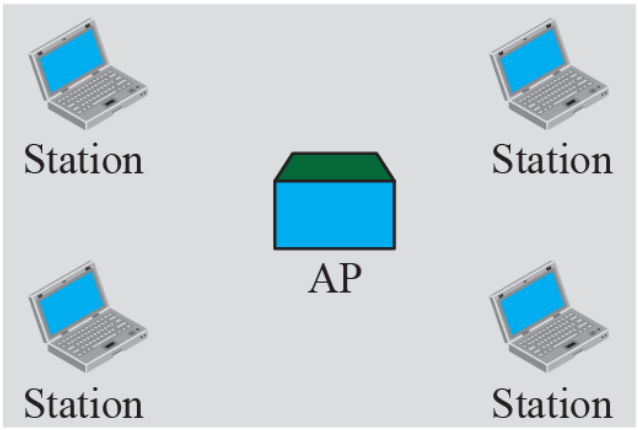
Figure 3.13 *Basic service sets (BSSs)*

BSS: Basic service set



Ad hoc network (BSS without an AP)

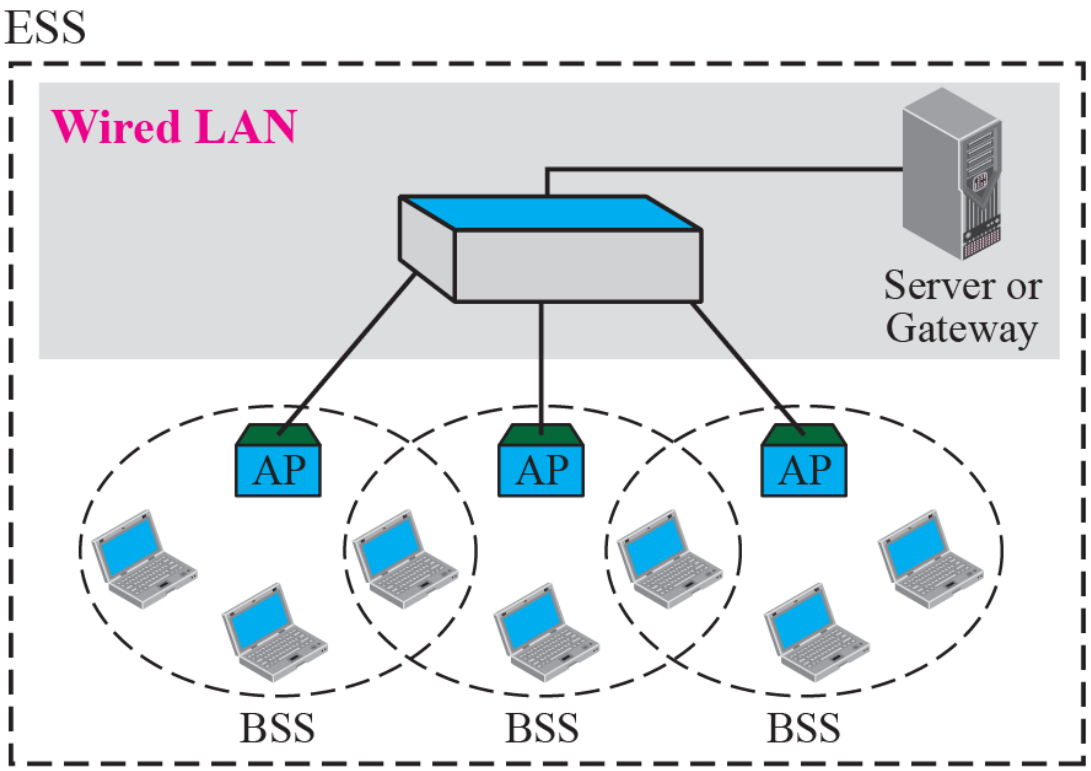
AP: Access point



Infrastructure (BSS with an AP)

Figure 3.14 *Extended service sets (ESSs)*

ESS: Extended service set
BSS: Basic service set
AP: Access point



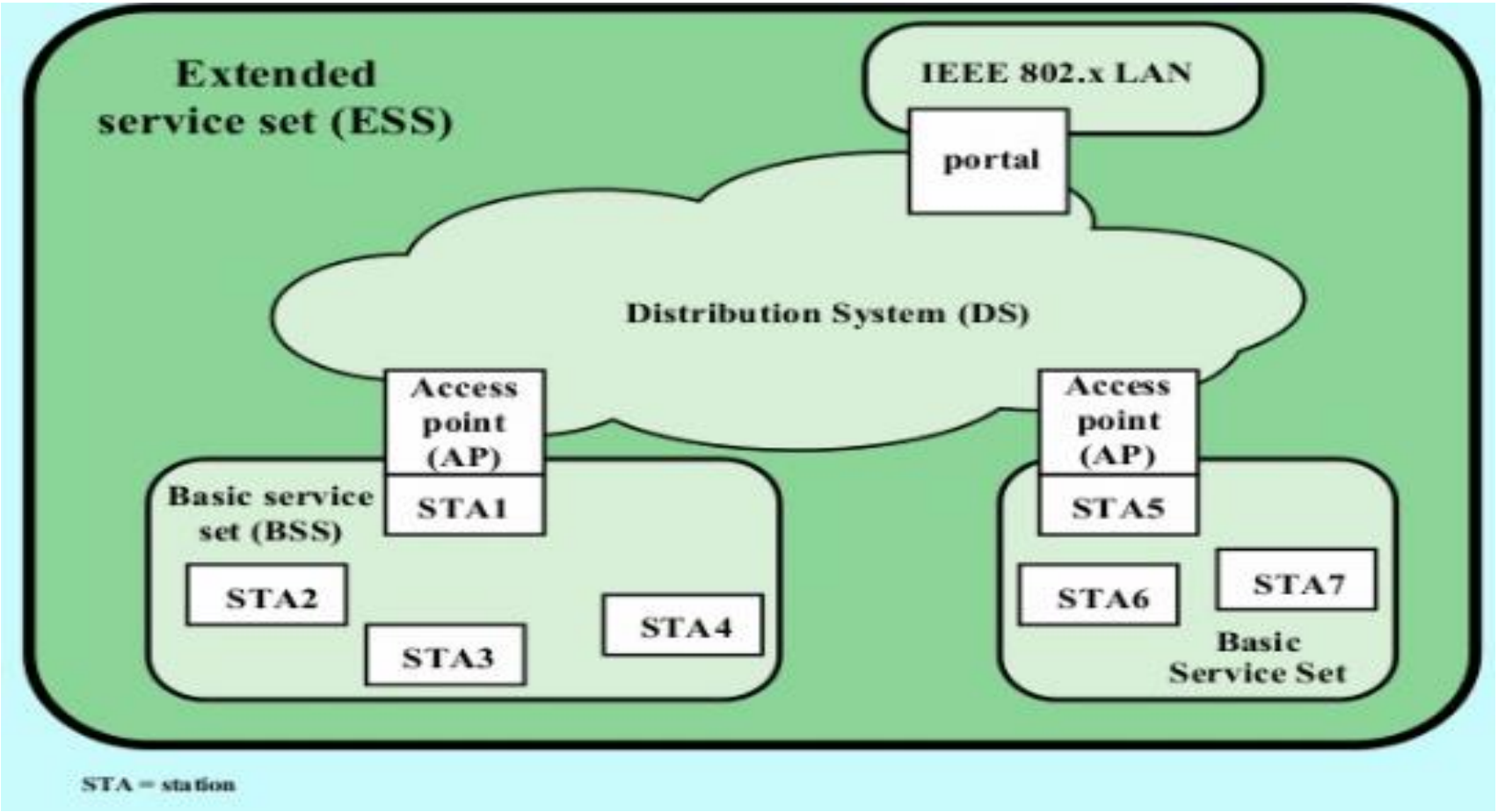

Extended
service set (ESS)
IEEE 802.x LAN
portal
Distribution System (DS)
Access
point
(AP)
Access
point
(AP)
Basic service
set (BSS)
STA1
STA5
STA2
STA3
STA4
STA6
STA7
Basic
Service Set
STA = station

Figure 3.15 *CSMA/CA flow diagram*

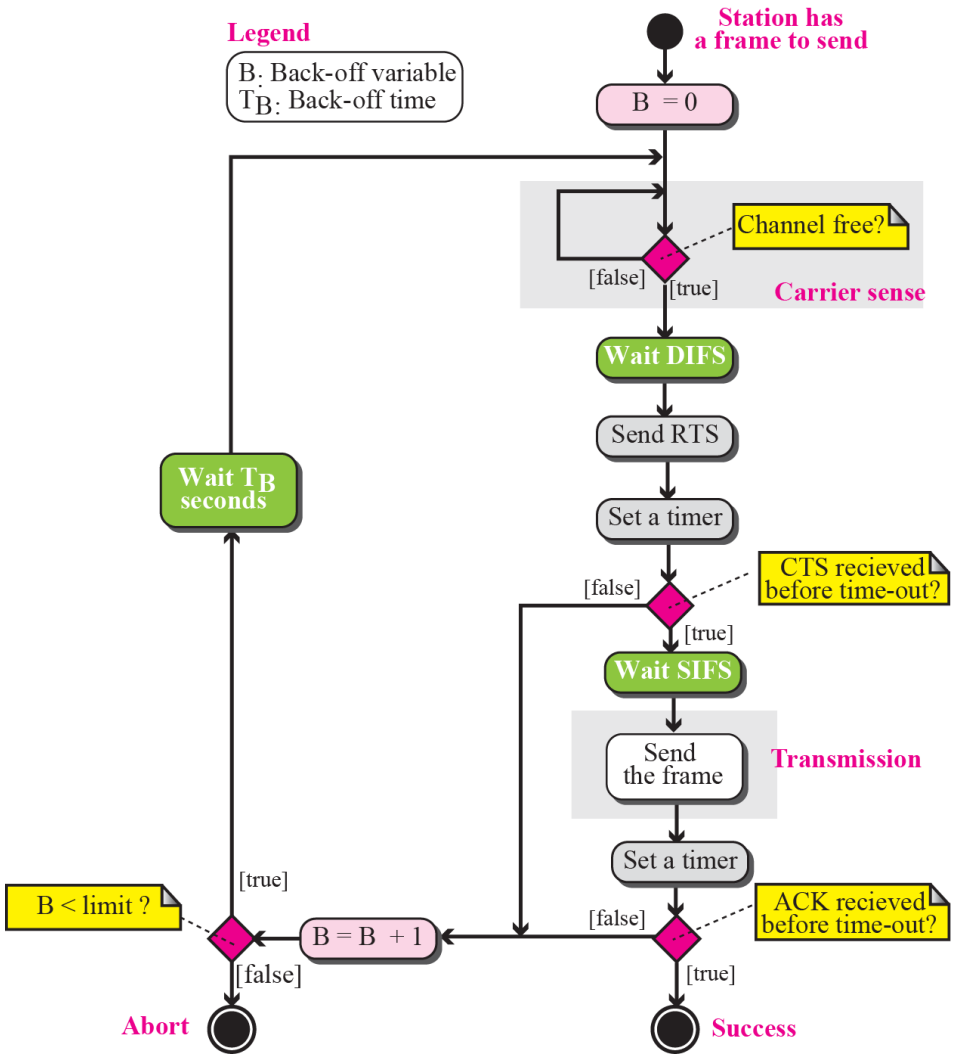


Figure 3.16 *CSMA/CA and NAV*

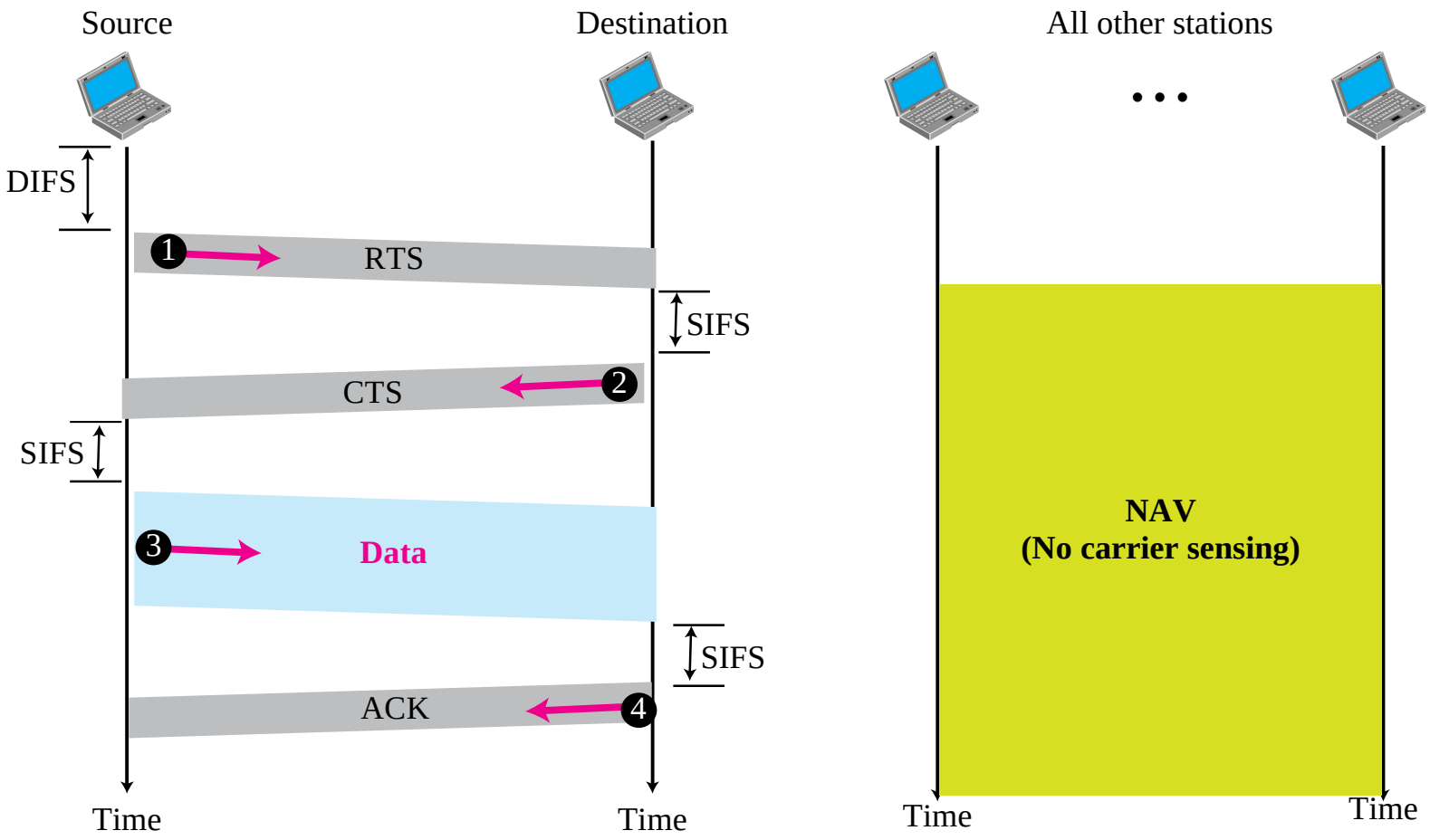


Figure 3.17 *Frame format*

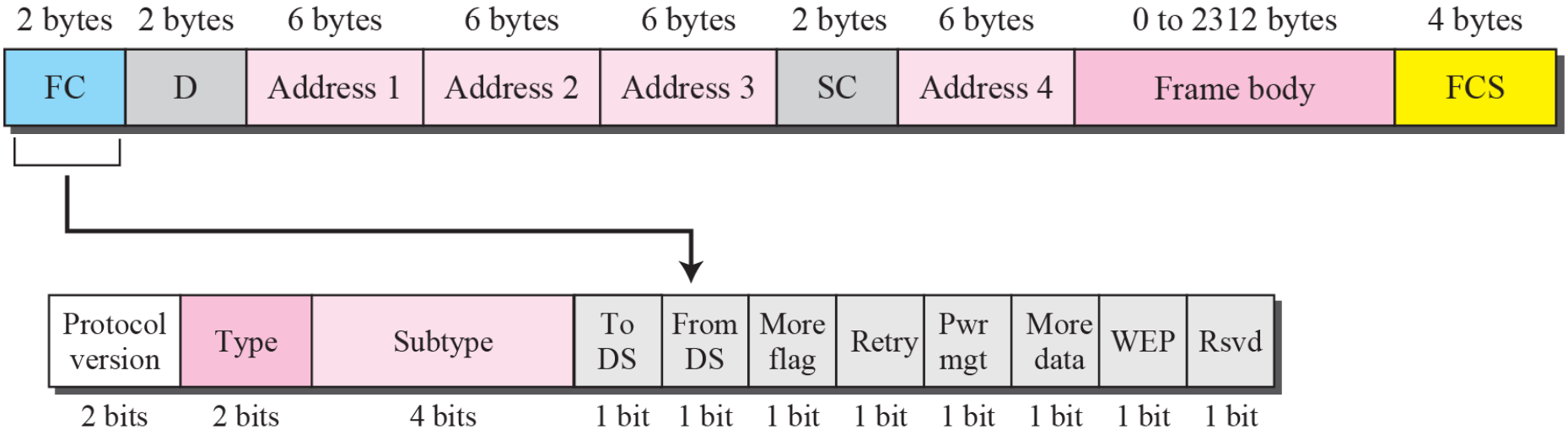


Table 3.5 *Subfields in FC field*

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 3.6)
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

More Fragments:

★ A single bit subfield which when set to 1 indicates that more fragments would follow.

Retry:

★ A single bit subfield which when set to 1 specifies a retransmission of a previous frame.

Power Management:

★ A single bit subfield indicating that the sender is adopting power-save mode.

More Data:

★ A single bit subfield showing that sender has further data frames for the receiver.

WEP:

★ A single bit subfield indicating that this is an encrypted frame.

Order:

★ The last subfield, of one – bit, informs the receiver that to the higher layers the frames should be in an ordered sequence.

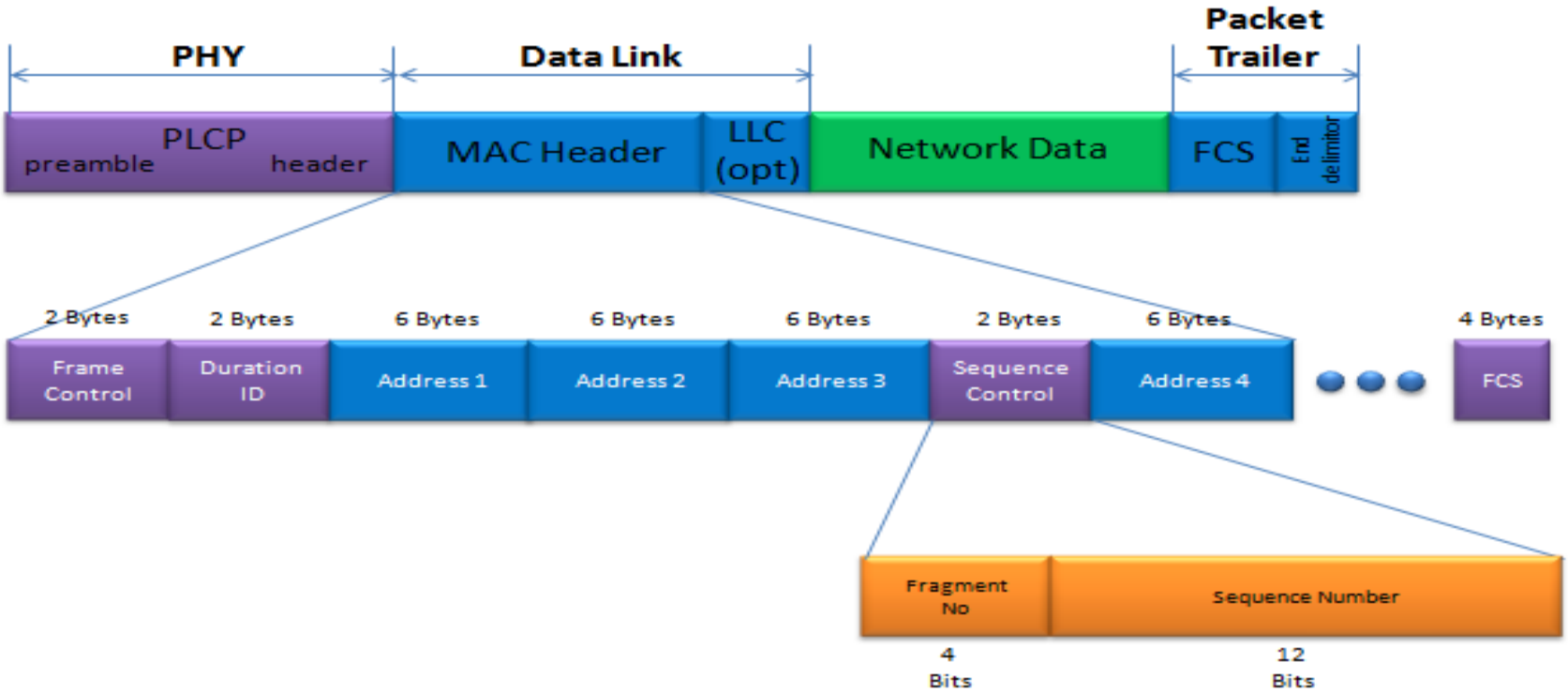
Duration:

★ It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Reciever	Transmitter	Destination	Source

Sequence

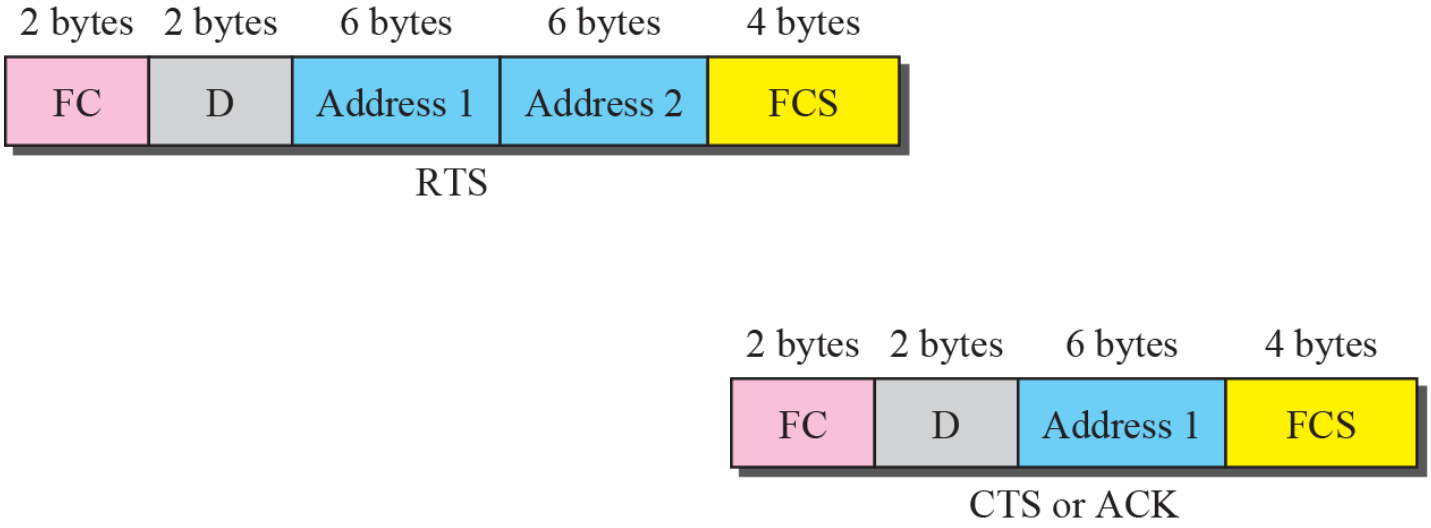
- **It is a 2 byte field that stores the frame numbers.**
- **It detect the duplicate frames and determines the ordr of frames for higher layers.**
- **Among the 16 bits,the first 4 bits provides identification to the fragment and the rest 12 bits contain the seq number that increments with each transmission**



MAC Frame Types

- 1. Management Frames – They are used to manage communications between stations and access points.
- 2. Control Frames – They are used for accessing the channel and acknowledging frames.
- 3. Data Frames – They are used for carrying data and control information.

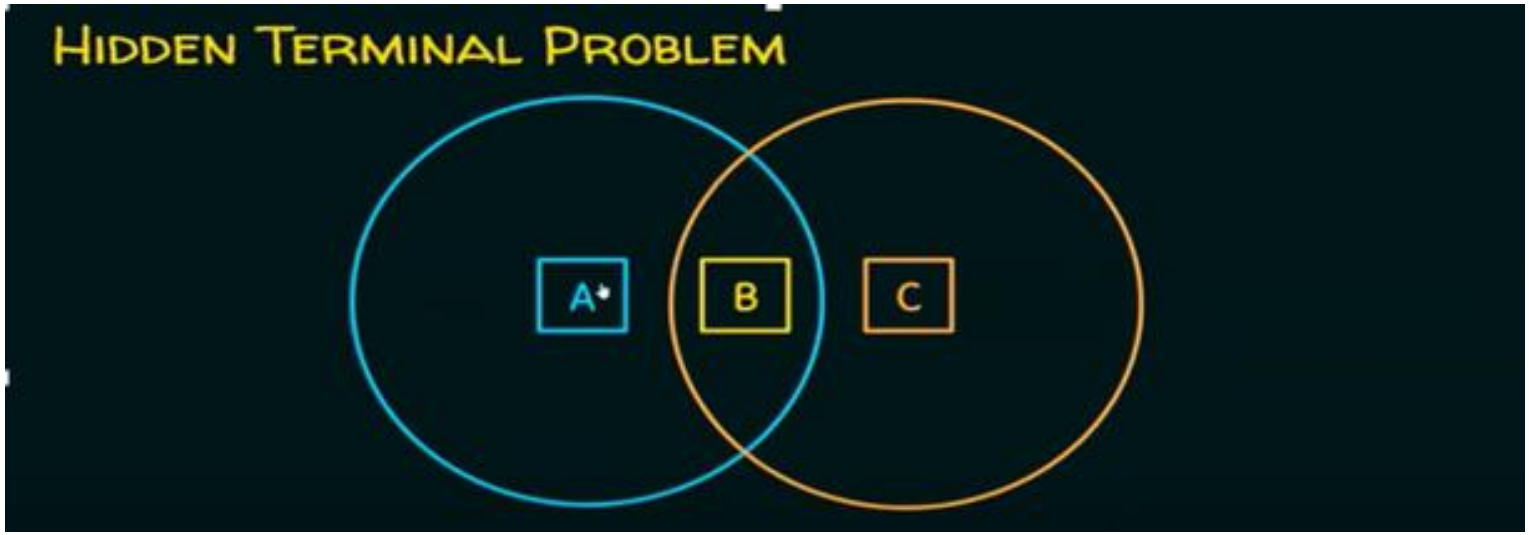
Figure 3.18 *Control frames*



HIDDEN TERMINAL PROBLEM

Suppose both A and C want to communicate with B and so they each send it a frame.

- **A and C are unaware of each other since their signals donot carry that far.**
- **These two frames collide with each other at B(unlike on Ethernet,neither A nor C is aware of this collision**
- **A and C are said to be hidden nodes with respect to each other.**

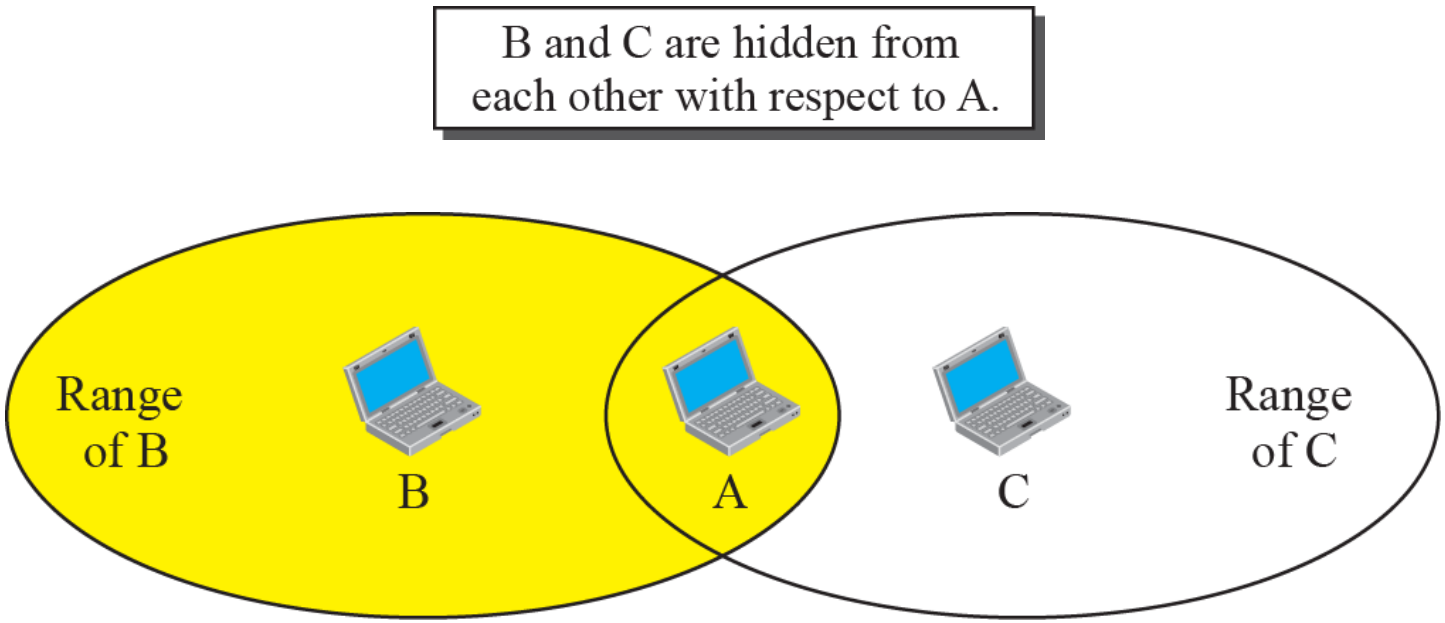


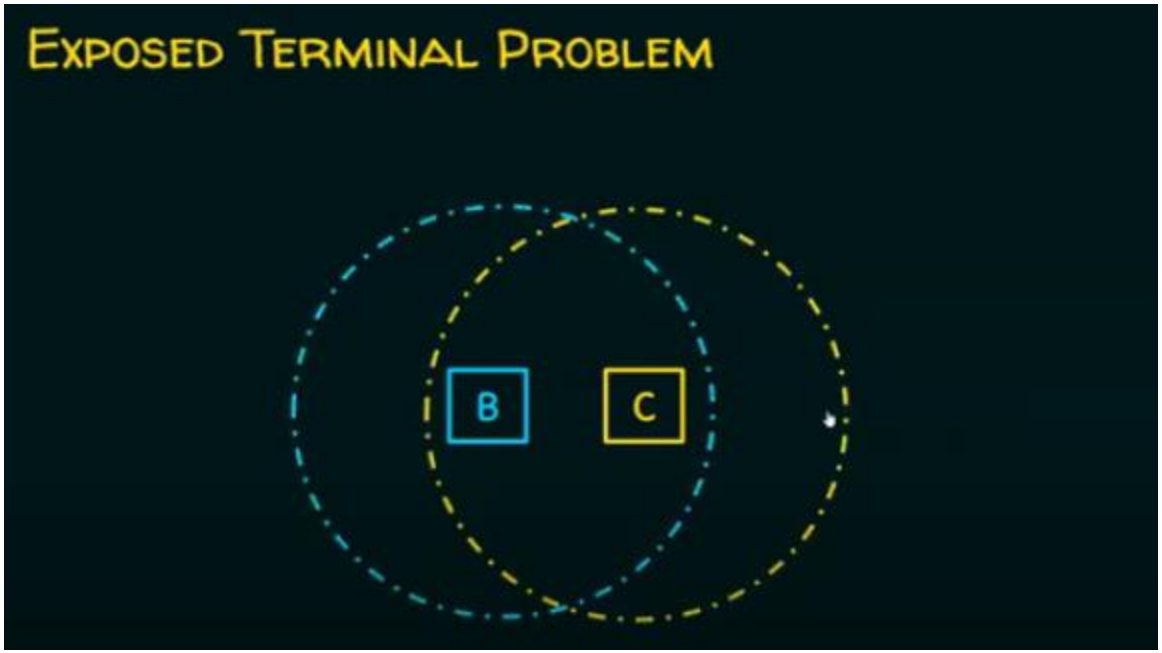
Hidden Terminal Problem – Solution

Multiple Access Collision Avoidance (MACA) Algorithm – RTS and CTS frames

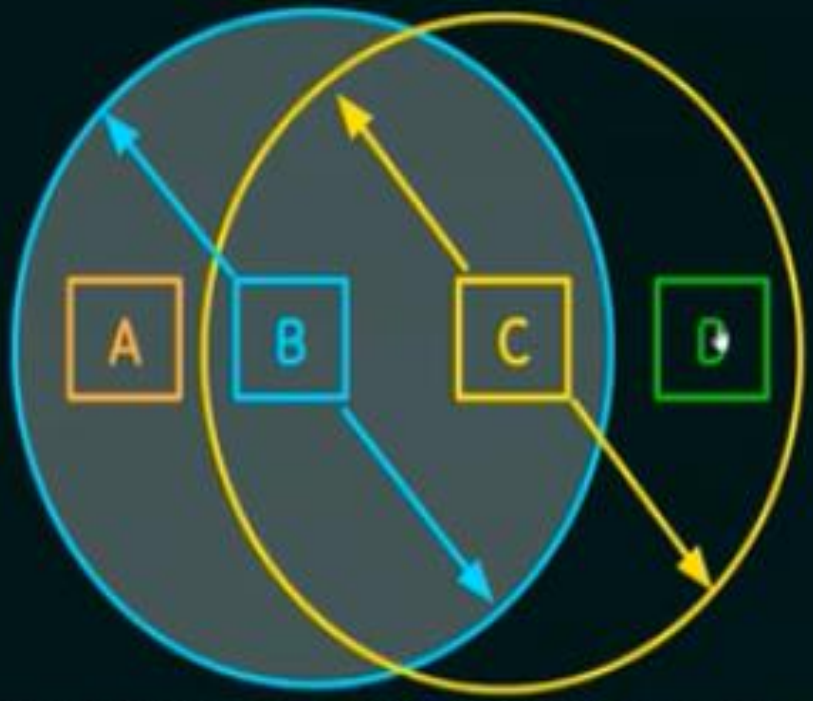
These two are the control frames.

Figure 3.19 *Hidden station problem*




EXPOSED TERMINAL PROBLEM
B
C

Exposed Terminal Problem



Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.

- ★ It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
- ★ Suppose C wants to transmit to node D.
- ★ This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.

Exposed Terminal Problem – Solution

Multiple Access Collision Avoidance (MACA) Algorithm – RTS and CTS

IEEE 802.11 – Collision Avoidance

- ★ 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).

Key Idea

- ★ Sender and receiver exchange control frames with each other before the sender actually transmits any data.
- ★ This exchange informs all nearby nodes that a transmission is about to begin.
- ★ Sender transmits a Request to Send (RTS) frame to the receiver.
  - The RTS frame includes a field that indicates how long the sender wants to hold the medium. Length of the data frame to be transmitted.
- ★ Receiver replies with a Clear to Send (CTS) frame
  - This frame echoes this length field back to the sender

- **There may be some nodes near the sender and some near the receiver.**

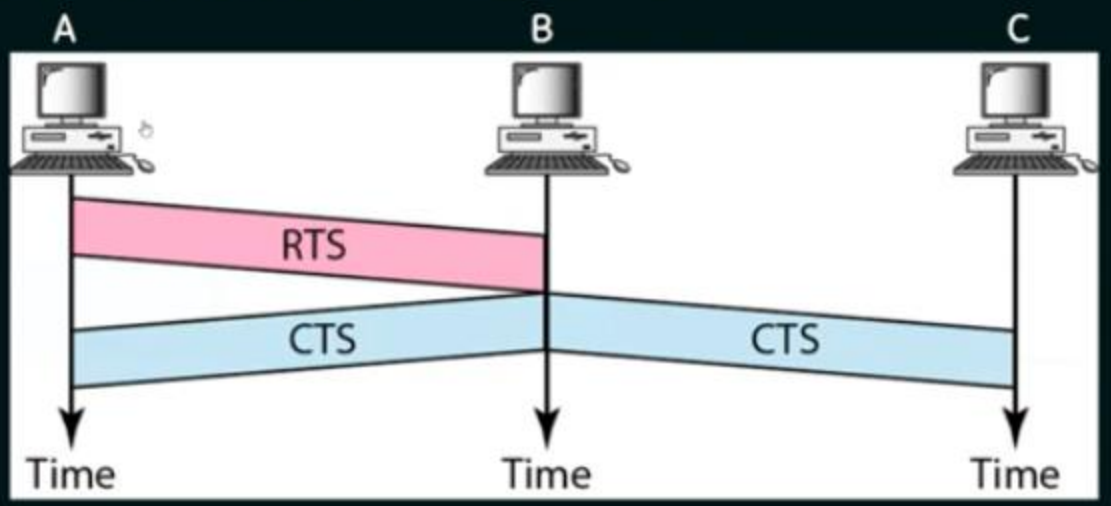
IEEE 802.11 – Collision Avoidance

- ★ Any node that sees the CTS frame knows that
  - it is close to the receiver, therefore
  - cannot transmit for the period of time it takes to send a frame of the specified length
- ★ Any node that sees the RTS frame but not the CTS frame
  - is not close enough to the receiver to interfere with it, and
  - so is free to transmit

IEEE 802.11 – Collision Avoidance

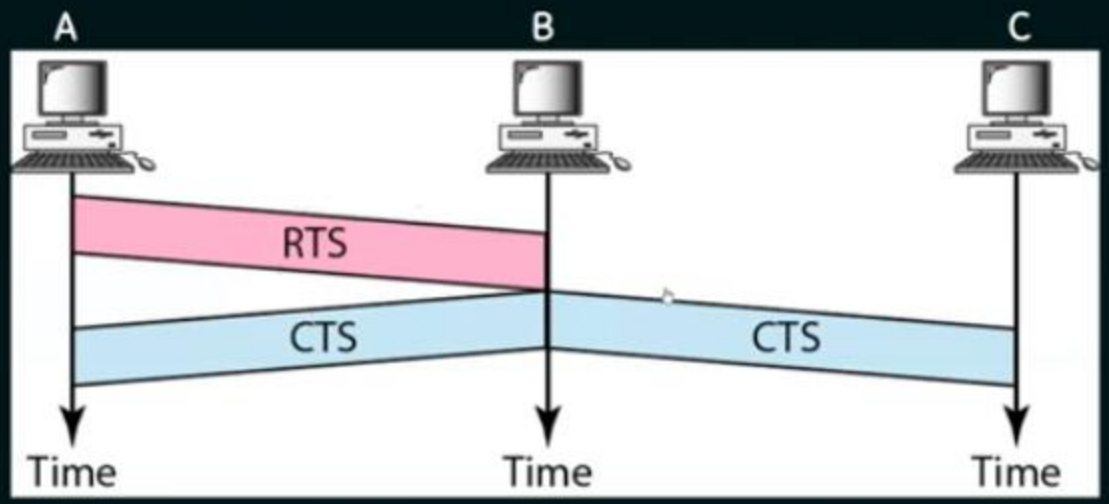
- The idea of using ACK in MACA is Proposed in MACAW: MACA for Wireless LANs.
- Receiver sends an ACK to the sender after successfully receiving a frame.
- All nodes must wait for this ACK before trying to transmit.
- If two or more nodes detect an idle link and try to transmit an RTS frame at the same time
  - Their RTS frame will collide with each other
- 802.11 does not support collision detection
  - So the senders realize the collision has happened when they do not receive the CTS frame after a period of time
  - In this case, they each wait a random amount of time before trying again.
  - The amount of time a given node delays is defined by the same exponential backoff algorithm used on the Ethernet.

USE OF RTS/CTS HANDSHAKING



Station C doesn't hear RTS from A, but it does hear CTS from B, so it knows something is up.

USE OF RTS/CTS HANDSHAKING



Station C doesn't hear RTS from A, but it does hear CTS from B, so it knows something is up.

Note

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

Figure 3.20 *Use of handshaking to prevent hidden station problem*

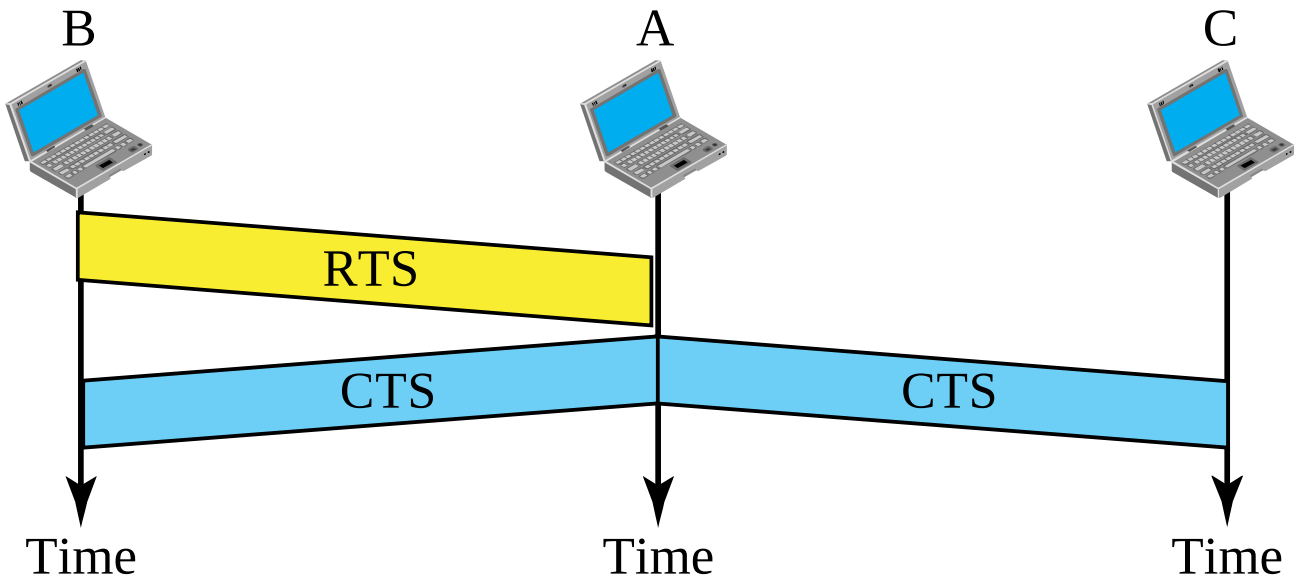


Figure 3.21 *Exposed station problem*

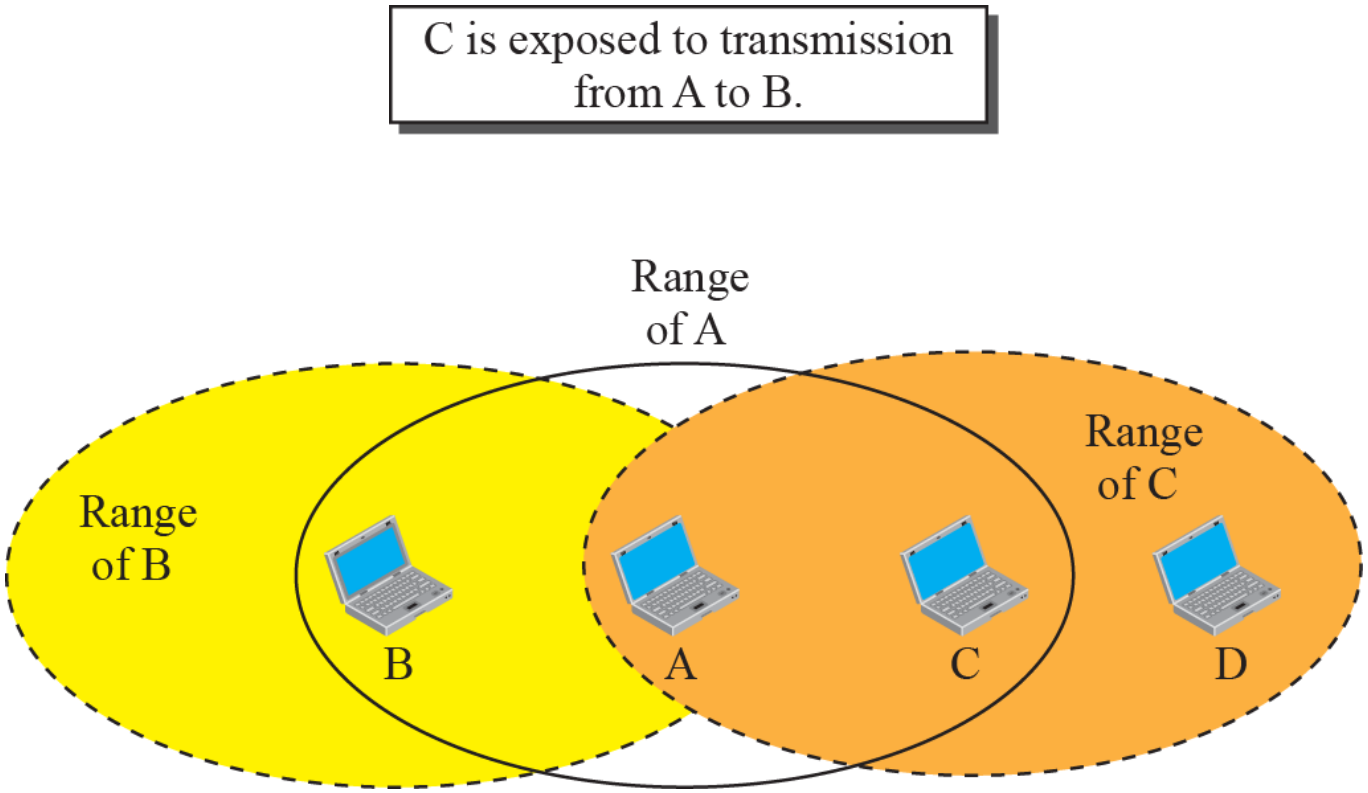
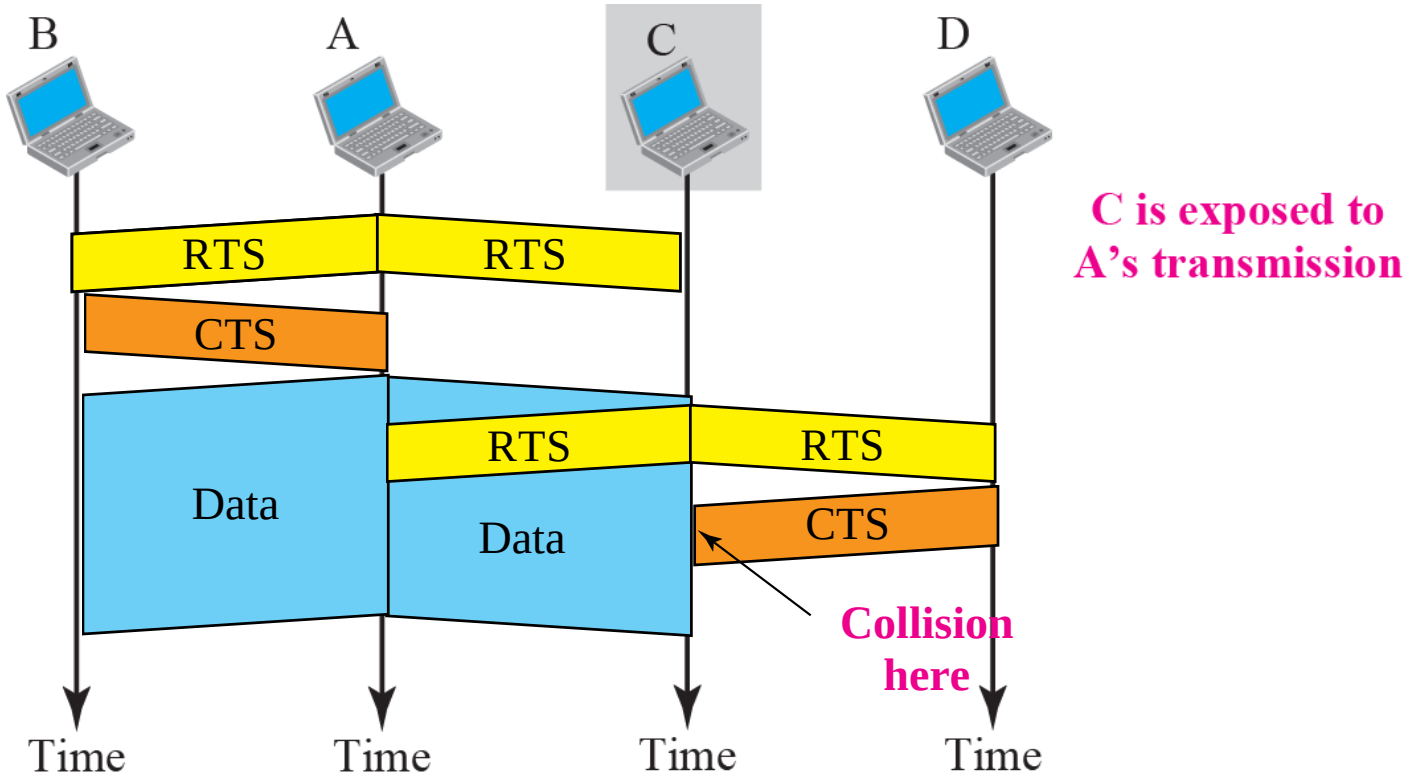


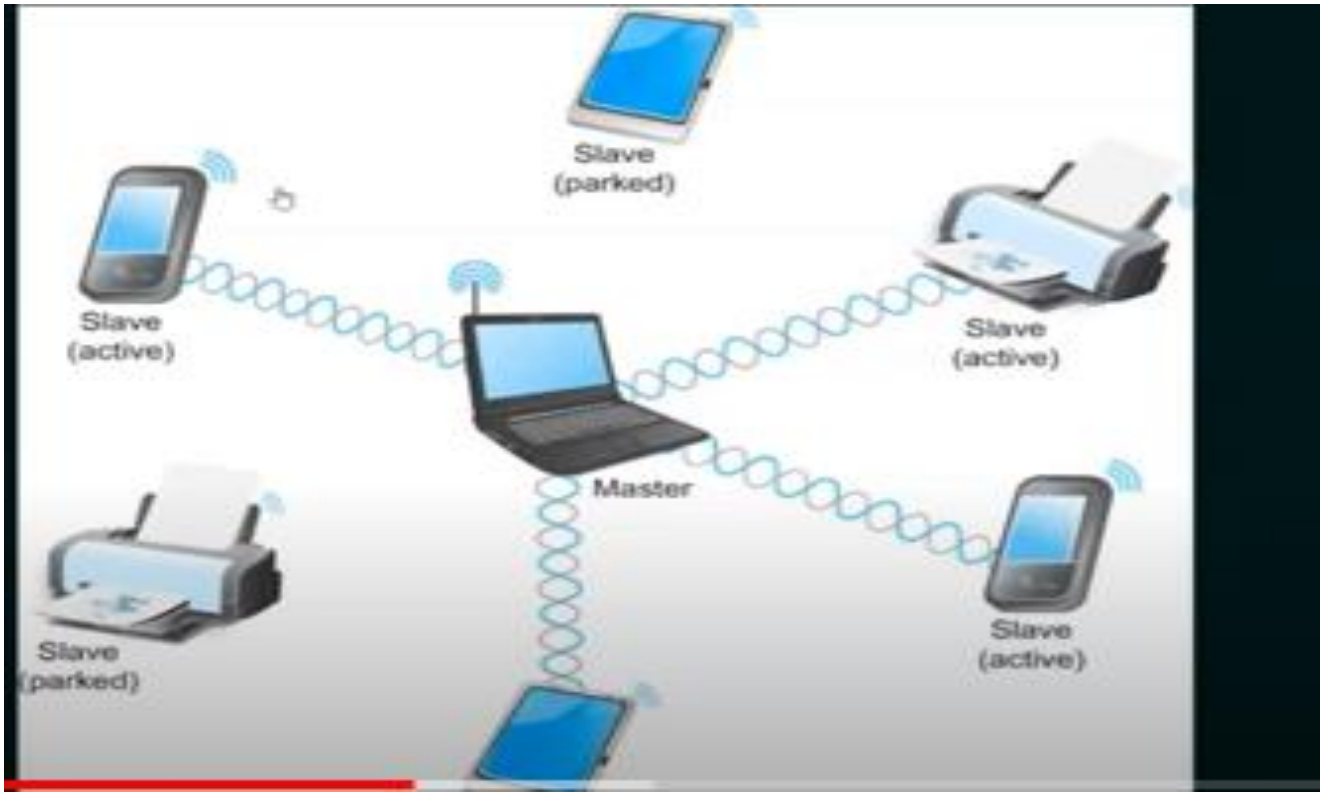
Figure 3.22 *Use of handshaking in exposed station problem*



BLUETOOTH

- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers etc.
- The connected device are called gadgets.
- They find each other and make a network called a Piconet.

Consists of a master device and upto 7 slave devices.
Any communication is between the master and the slave.
The slaves donot communicate directly with each other
A slave can be parked:ie it can be set to an inactive low power state.



BLUETOOTH ARCHITECTURE

- Two types of Bluetooth networks are Piconet and Scatternet.

- Piconets
- A Bluetooth network is called a Piconet or a small net.
- A Piconet can have up to eight stations, one of which is called the primary and the rest are called secondaries.
- An additional eighth secondary can be in the parked state, which is synchronized with the primary, but cannot take part in communication until it is moved from the parked state by moving an active station to the parked state.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

Piconet and Scatternet

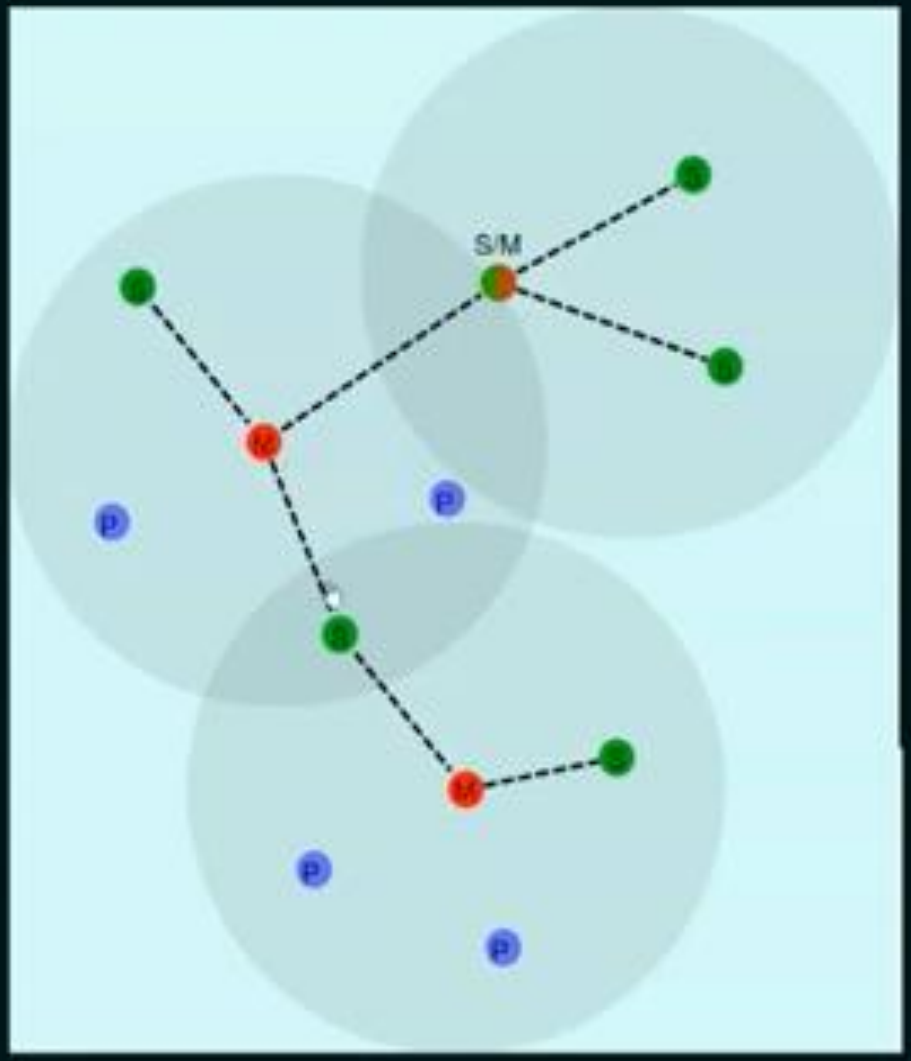
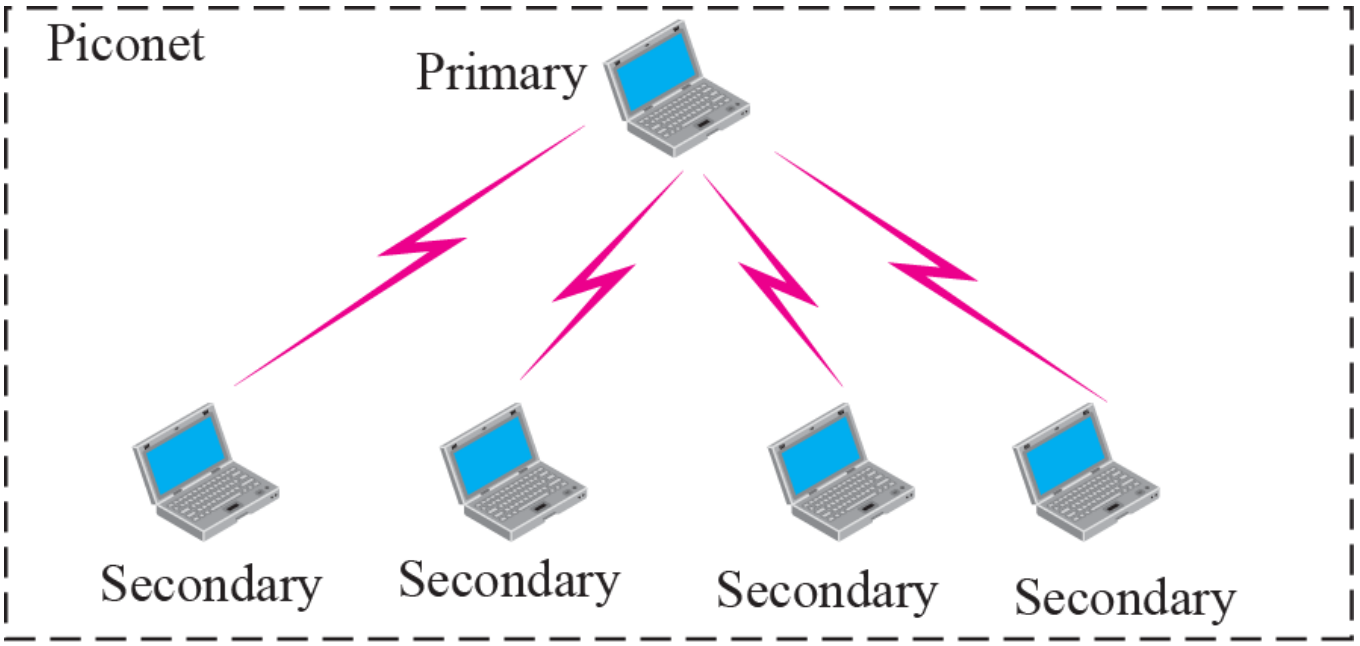


Figure 3.23 *Piconet*



- Scatternet
- Piconets can be combined to form a scatternet .
- A secondary station in one piconet can be the primary in another Piconet.
- A Station can be a member of two piconets.

Pros

- ★ Low cost.
- ★ Easy to use.
- ★ It can also penetrate through walls.
- ★ It creates an ad-hoc connection immediately without any wires.
- ★ It is used for voice and data transfer.

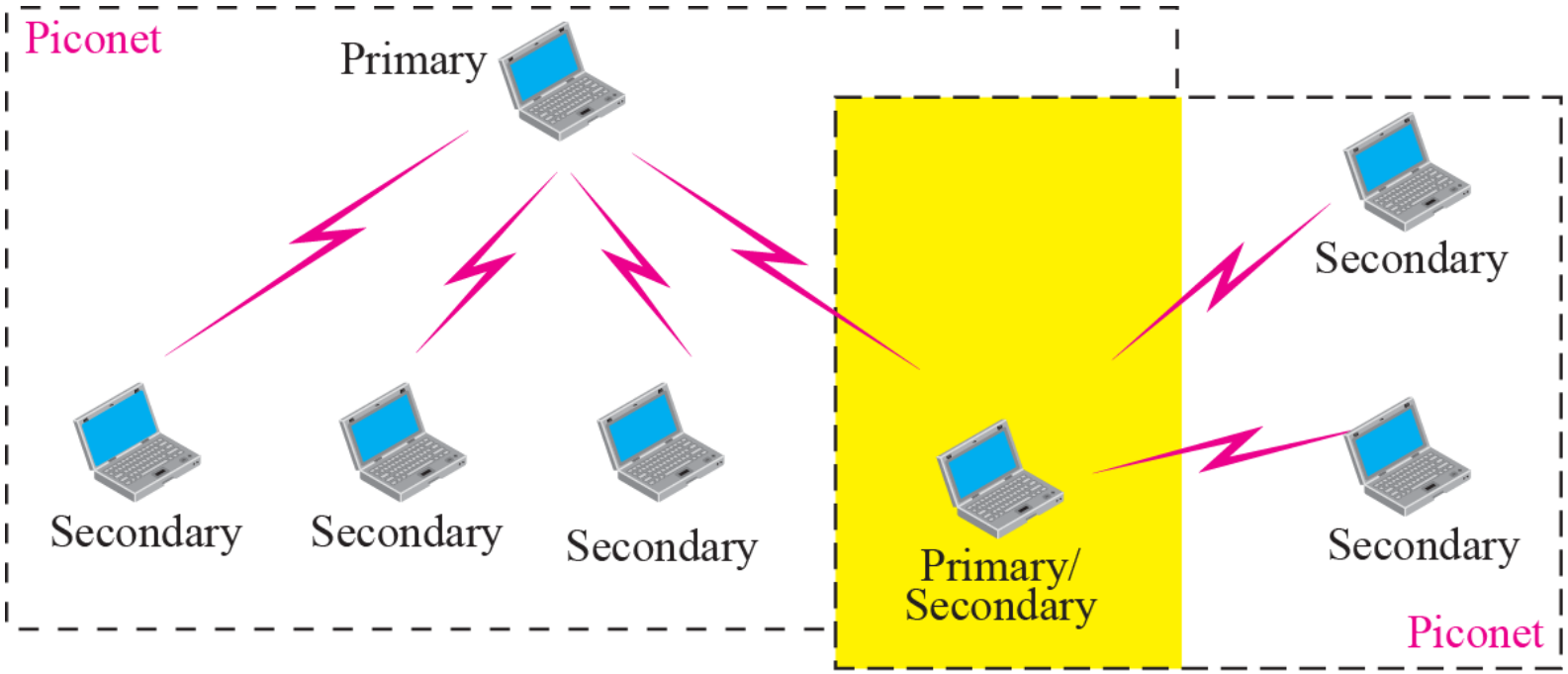
Cons

- ★ It can be hacked and hence, less secure.
- ★ It has slow data transfer rate.
- ★ It has small range: 10 meters.

BLUESNARFING

- ★ Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs.
- ★ This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.
- ★ Bluesnarfing is the theft of information from the target device.

Figure 3.24 *Scatternet*



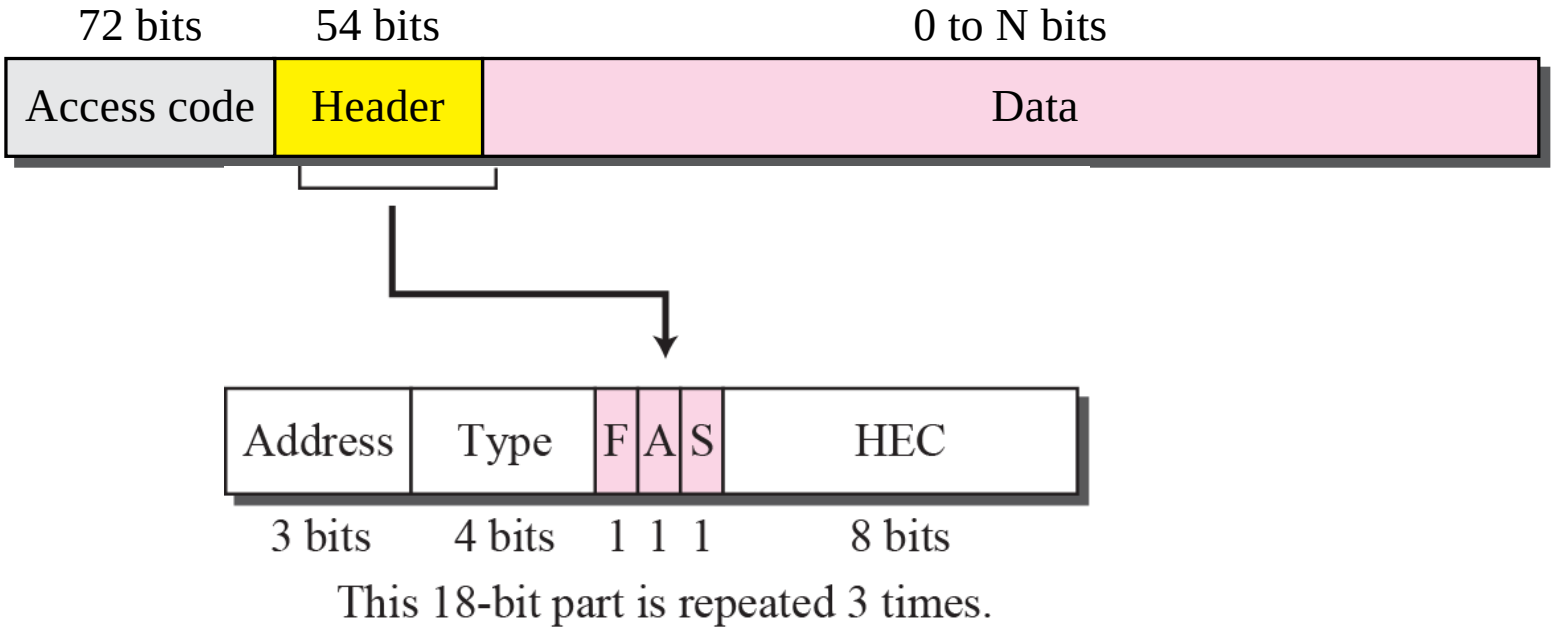
Bluetooth Frame Format with Basic Data Rate

A Bluetooth frame with basic rate has three parts, access code, header and data as shown in the following diagram−

The various fields are−

•**Access Code**− A 72-bit field containing synchronization bits to identify the master.

•**Header**− A 54-bit field containing 18-bit patterns repeated thrice, having the following subfields−



- **Address**− A 3 bit-field that can identify a maximum of seven slaves numbered 1 to 7. An address 0 depicts broadcast.
- **Type**− A 4-bit field that identifies the type of data from upper layers. It identifies whether the frame is ACL, SCO, null.(asynchronous connectionless,synchronous connection oriented

- **F**− A bit for flow control. When the device cannot receive more frames, F is set to 1.
- **A**− A bit for acknowledgement, for piggybacking an ACK to the end of the frame.
- **S**− A bit denoting sequence number of the frame for detect retransmission. Only a single bit suffices since stop and wait protocol is used.
- **Checksum**− An 8-bit field containing checksum for error detection.

•**Data**− A variable length field ranging from 0 to 2744 bits that contains data or control information from upper layers.

Bluetooth Frame Format with Enhanced Data Rate

The frame for enhanced data rate contains additionally a guard field and a trailer as shown in the following diagram−

The additional fields and changes in data field are−

•**Guard**− A 16-bit field containing a synchronization pattern that enables to switch to higher data speed while transmitting the data field.

•**Trailer**− A 2-bit field denoting end of the variable length data field.

•**Data**− A variable length field ranging from 0 to 2744 bits that contains high volume payload from upper layers.

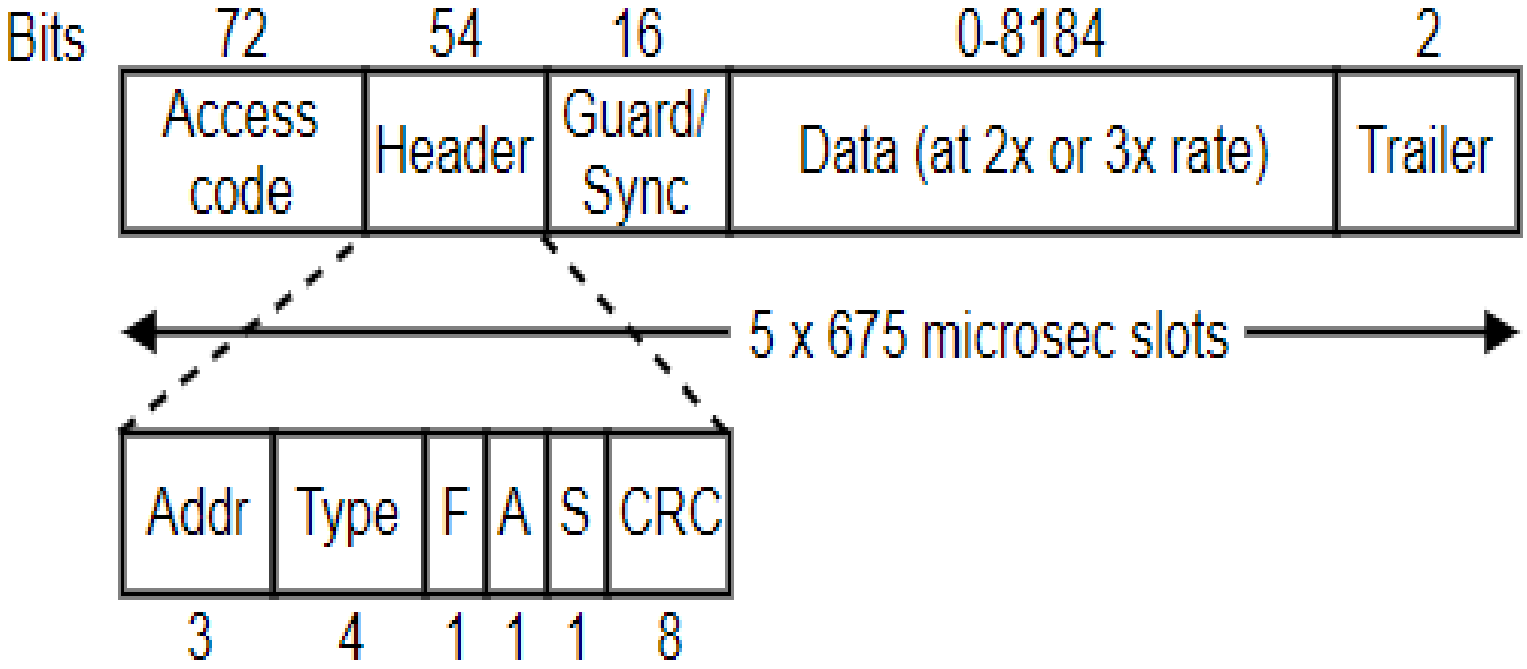
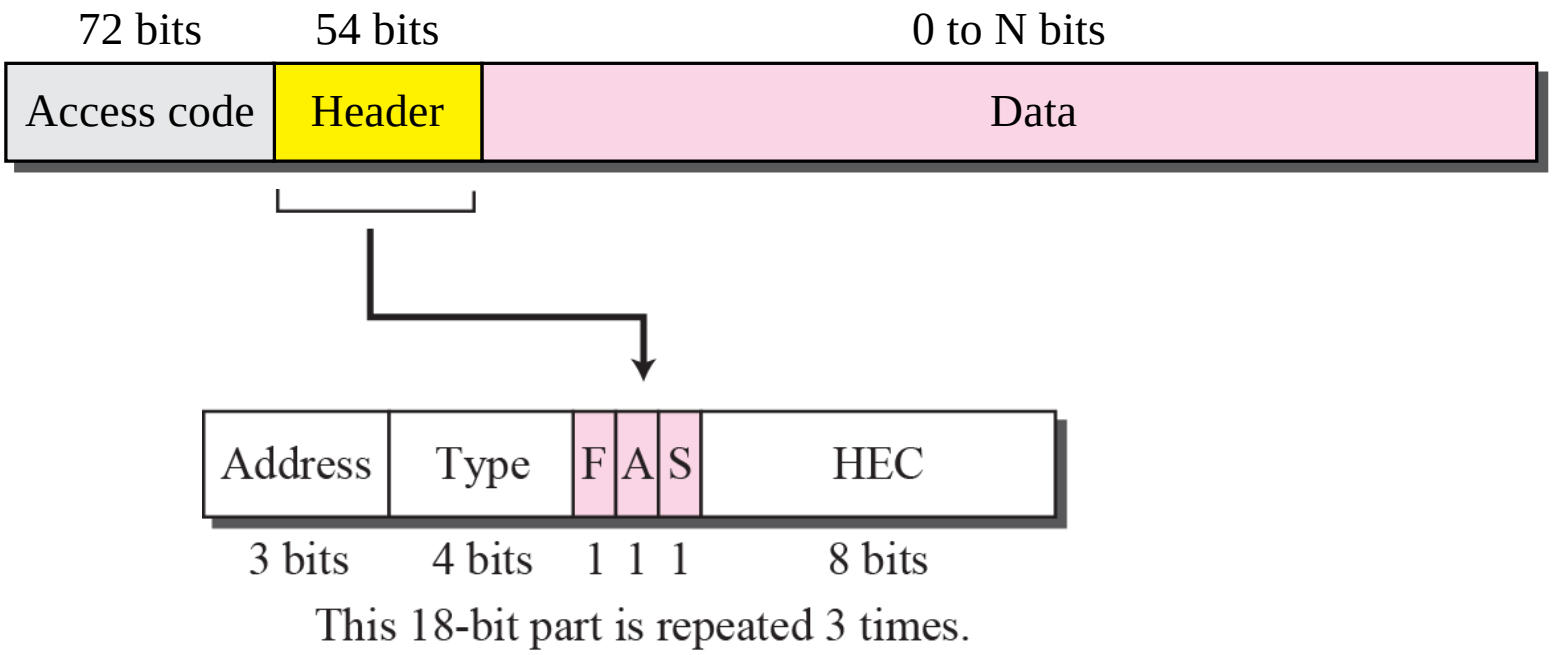

Bits
72
54
16
0-8184
2
Access code
Header
Guard/ Sync
Data (at 2x or 3x rate)
Trailer
5 x 675 microsec slots
Addr
Type
F
A
S
CRC
3
4
1
1
1
8

Figure 3.25 *Frame format types*

N = 240 for 1-slot frame
N = 1490 for 3-slot frame
N = 2740 for 5-slot frame

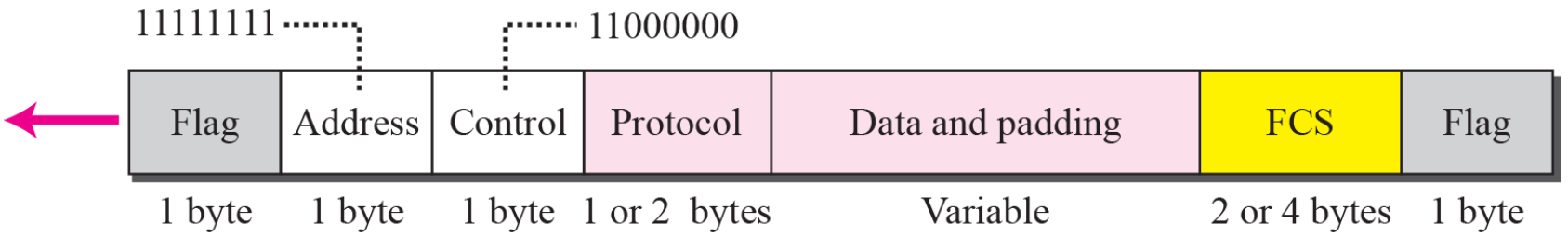


3-3 POINT-TO-POINT WANS

A second type of network we encounter in the Internet is the point-to-point wide area network. A point-to-point WAN connects two remote devices using a line available from a public network such as a telephone network. We discuss traditional modem technology, DSL line, cable modem, T-lines, and SONET.

Figure 3.31 *PPP frame*

***To control and manage the transfer of data,a special protocolcalled point – to-point Protocol was designed.**
***PPP has only physical and data link layers.**
***PPP defines the frame format.**



***Link Control Protocol(LCP)**
***Network Control Protocol(NCP)**

3-4 SWITCHED WANS

The backbone networks in the Internet can be switched WANs. A switched WAN is a wide area network that covers a large area (a state or a country) and provides access at several points to the users. Inside the network, there is a mesh of point-to-point networks that connects switches. The switches, multiple port connectors, allow the connection of several inputs and outputs.

Switched WAN technology differs from LAN technology in many ways.

Note

A cell network uses the cell as the basic unit of data exchange.
A cell is defined as a small, fixed-size block of information.

Introduction

In the early 1970's there were many data communication networks (also known as Public Networks), which were owned by private companies, organizations and governments agencies. Since those public networks were quite different internally, and the interconnection of networks was growing very fast, there was a need for a common network interface protocol. In 1976 X.25 was recommended as the desired protocol by the **International Consultative Committee for Telegraphy and Telephony** (CCITT) called the **International Telecommunication Union** (ITU) since 1993.

X.25 is a standard for WAN communications that defines how connections between user devices and network devices are established and maintained. X.25 is designed to operate effectively regardless of the type of systems connected to the network. It is typically used in the packet-switched networks (PSNs) of common carriers, such as the telephone companies. Subscribers are charged based on their use of the network.

X.25 Devices and Protocol Operation

X.25 network devices fall into three general categories: data terminal equipment (DTE), data circuit-terminating equipment (DCE), and packet-switching exchange (PSE) as shown in Fig.

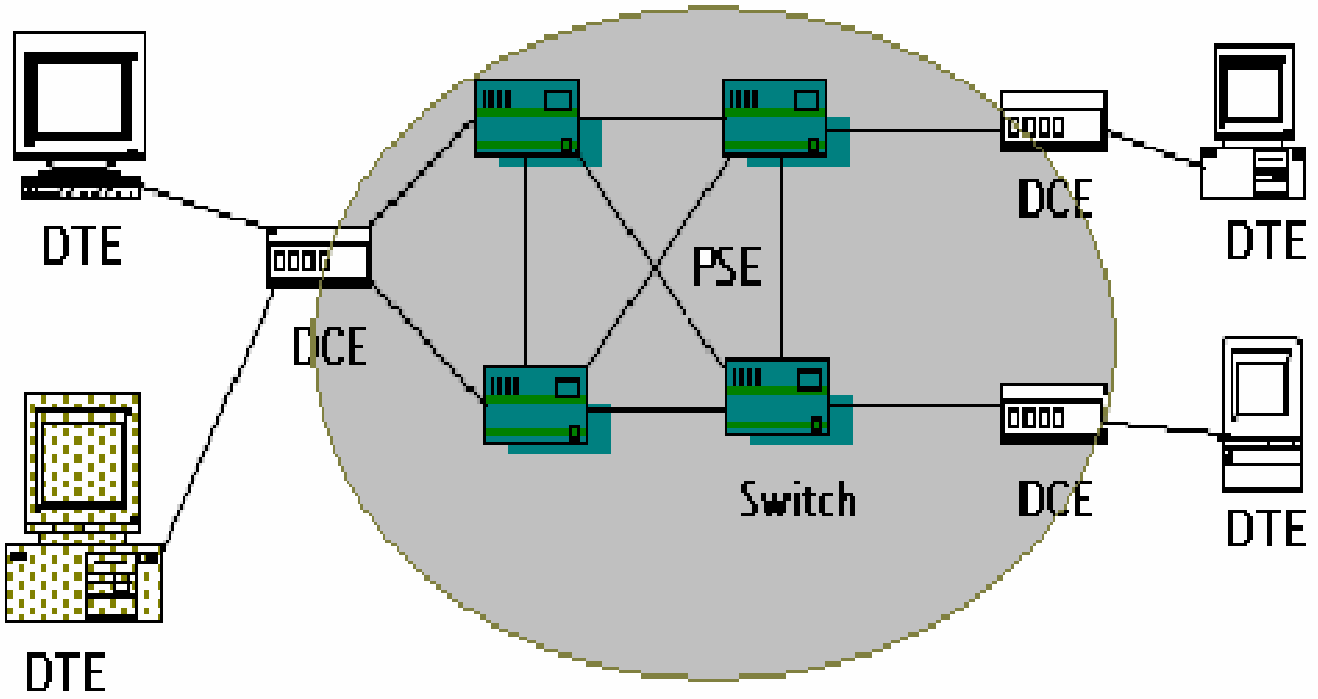


Figure 4.4.1 X.25 network

Data terminal equipment (DTE) devices are end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers. Data communication Equipments (**DCEs**) are communications devices, such as modems and packet switches that provide the interface between DTE devices and a PSE, and are generally located in the carrier's facilities.

PSEs are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 PSN. Figure 4.4.1 illustrates the relationships among the three types of X.25 network devices

Packet Assembler/Disassembler

The *packet assembler/disassembler (PAD)* is a device commonly found in X.25 networks. PADs are used when a DTE device, such as a character-mode terminal, is too simple to implement the full X.25 functionality. The PAD is located between a DTE device and a DCE device, and it performs three primary functions: buffering (storing data until a device is ready to process it), packet assembly, and packet disassembly. The PAD buffers data sent to or from the DTE device. It also assembles outgoing data into packets and forwards them to the DCE device. (This includes adding an X.25 header.) Finally, the PAD disassembles incoming packets before forwarding the data to the DTE. (This includes removing the X.25 header) Figure 4.4.2 illustrates the basic operation of the PAD when receiving packets from the X.25 WAN.

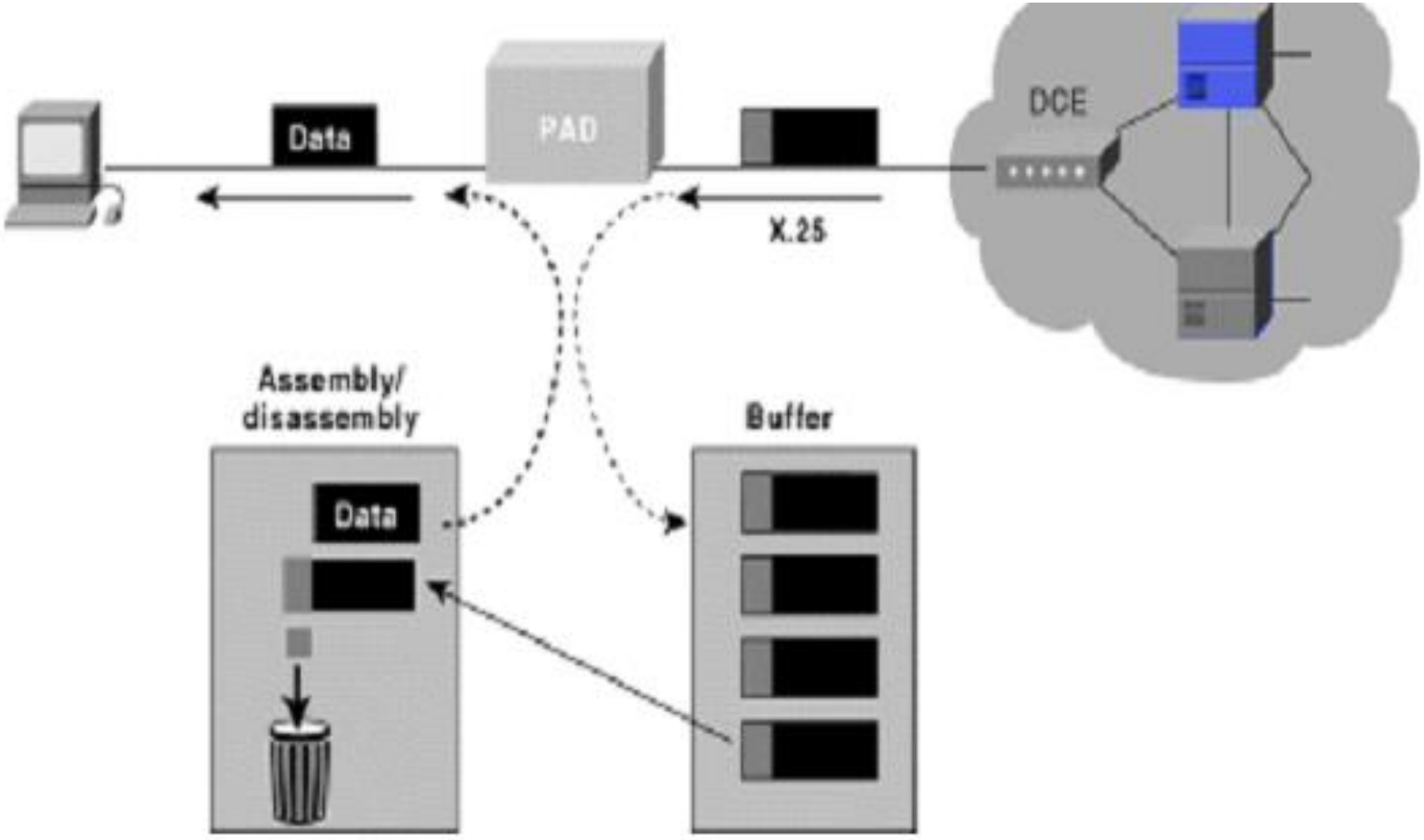


Figure 4.4.2 PADs

X.25 session establishment and virtual circuits

Session Establishment X.25 sessions are established when one DTE device contacts another to request a communication session. It's up to the receiving DTE whether to accept or refuse the connection. If the request is accepted, the two systems begin full-duplex communication. Either DTE device can terminate the connection. After the session is terminated, any further communication requires the establishment of a new session.

Virtual Circuits The X.25 is a **packet-switched** virtual circuit network. A *virtual circuit* is a logical connection created to ensure reliable communication between two network devices. A virtual circuit denotes the existence of a logical, bidirectional path from one DTE device to another across an X.25 network. Physically, the connection can pass through any number of intermediate nodes, such as DCE devices and PSEs. Virtual circuits in X.25 are created at the network layer such that multiple virtual circuits (logical connections) can be multiplexed onto a single physical circuit (a physical connection). Virtual circuits are demultiplexed at the remote end, and data is sent to the appropriate destinations.

TC

Figure 4.4.3 illustrates separate virtual circuits being multiplexed onto a single physical circuit.

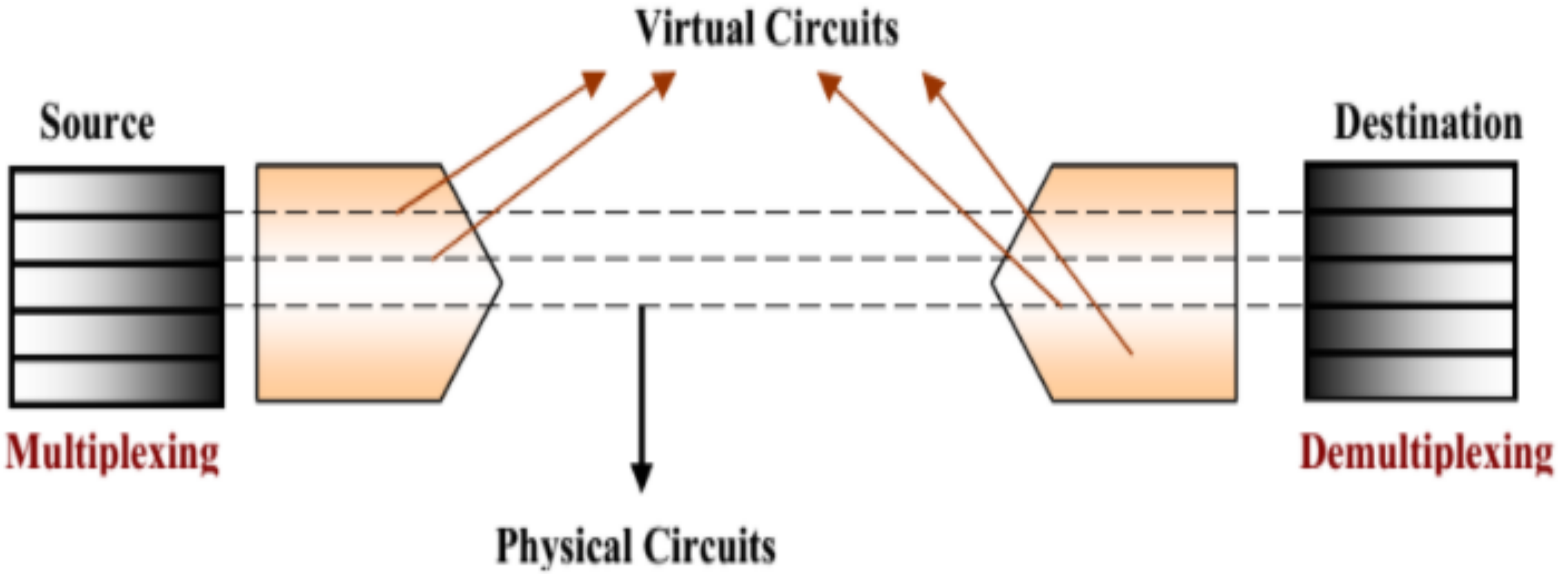
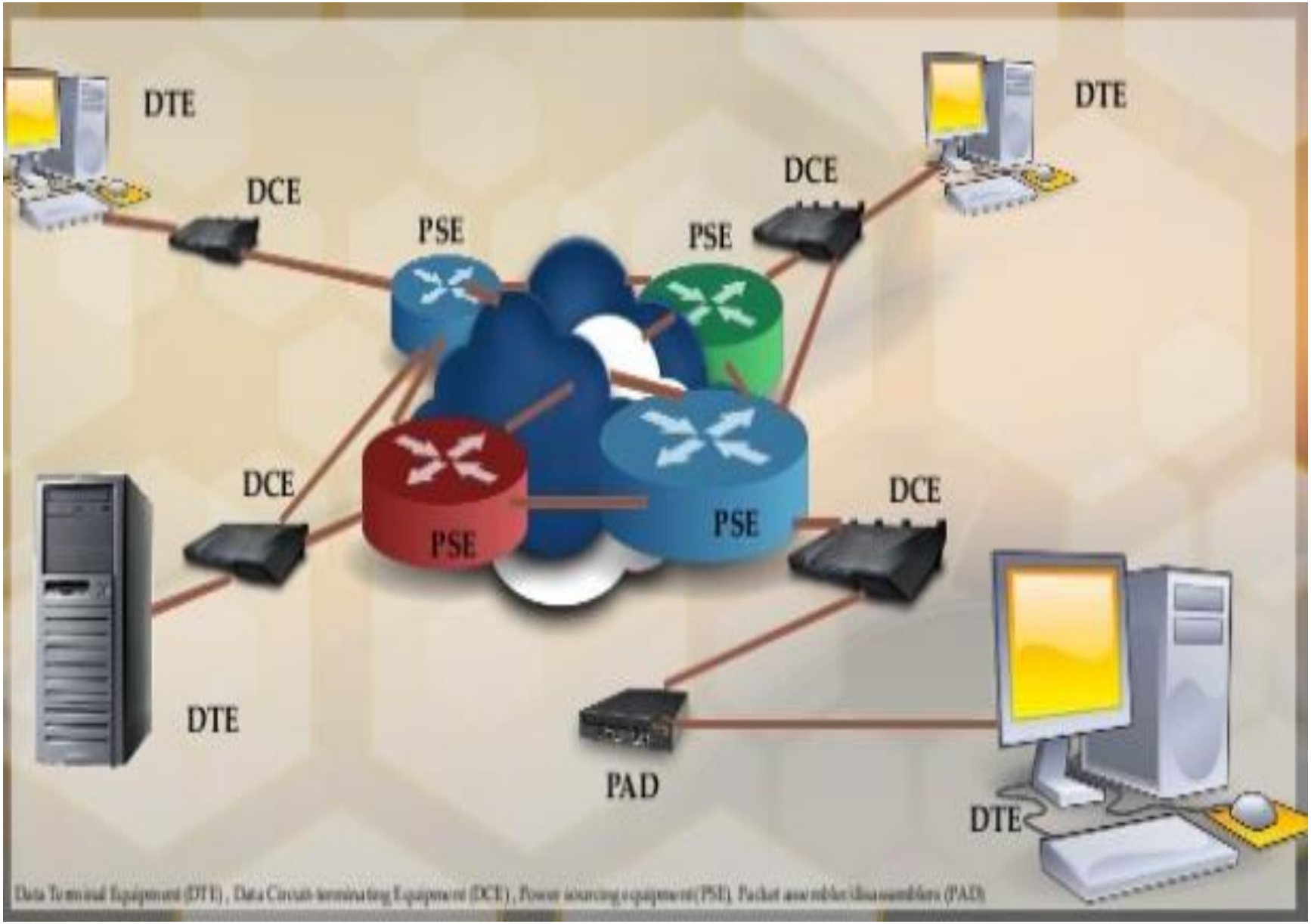


Figure 4.4.3 Physical Circuits and Virtual Circuit

X.25 Protocol Suite

The X.25 protocol suite maps to the lowest three layers of the OSI reference model as shown in Figure 4.4.4. The layers are:

- **Physical layer:** Deals with the physical interface between an attached station and the link that attaches that station to the packet-switching node. o X.21 is the most commonly used physical layer standard.
- **Frame layer:** Facilitates reliable transfer of data across the physical link by transmitting the data as a sequence of frames. Uses a subset of HDLC known as Link Access Protocol Balanced (LAPB), bit oriented protocol.
- **Packet layer:** Responsible for end-to-end connection between two DTEs. Functions performed are: o Establishing connection o Transferring data o Terminating a connection o Error and flow control o With the help of X.25 packet layer, data are transmitted in packets over external virtual circuits.


DTE
DTE
DCE
DCE
PSE
PSE
DCE
DCE
PSE
PSE
DTE
PAD
DTE

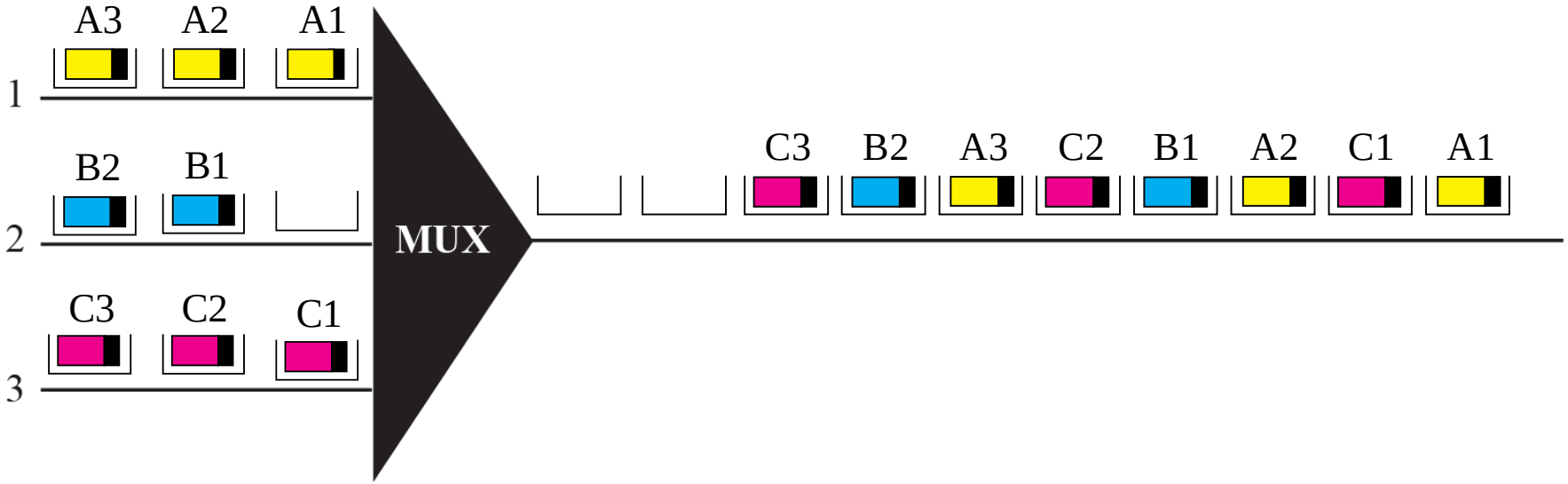
Characteristics of X.25

- Maximum packet sizes vary from 64 bytes to 4096 bytes,
  - 128 bytes is default on most networks.
- X.25 is optimized for low speed lines:
  - 100kbps and below.
  - At line speeds above 100 kbps the effects of latency.
- X.25 has been development of packet switched protocols
  - TCP/IP and ATM.

Asynchronous Transfer Mode (ATM)

- ATM, also known as **cell relay**, involves the transfer of data in discrete chunks called cells.
- Multiple logical connections can be multiplexed over a single path
- This is similar to packet switching except that the packets are variable sized and cells are of a fixed size.
- ATM is used in the WANs and is not constrained to a particular physical medium or data rate .
- ATM has minimal error and flow control capabilities to reduce the overhead of cells the overhead of protocol processing, enabling ATM to operate at high data rates.

ATM multiplexing



ATM Protocol Architecture

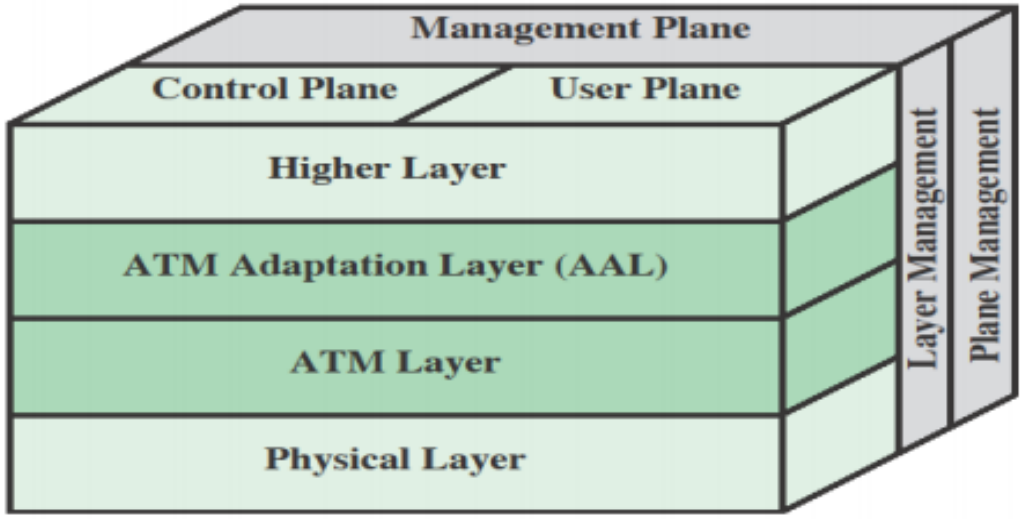


Figure 11.1 ATM Protocol Architecture

ATM Protocol Architecture …

- **Physical Layer**

Concerned with specifications of the transmission medium and signal encoding . Data rates specified include 155 and 622 Mbps with other data rates possible.

- **ATM Layer**

Defines transmission of data in fixed size cells and also defines the logical connections (Virtual circuits and virtual paths).

• **ATM Adaptation Layer (AAL)**

Supports transfer protocols not based on ATM. It maps higher layer information into ATM cells to be transported over an ATM network, then collects information from ATM cells for delivery to higher layers (e.g. a IP packet can be mapped to ATM cells).

- (There are 3 planes in the protocol architecture: the User plane is for user traffic including flow and error control; the Control plane is for connection control; the Management plane manages the system as a whole and coordinates the planes and layers).

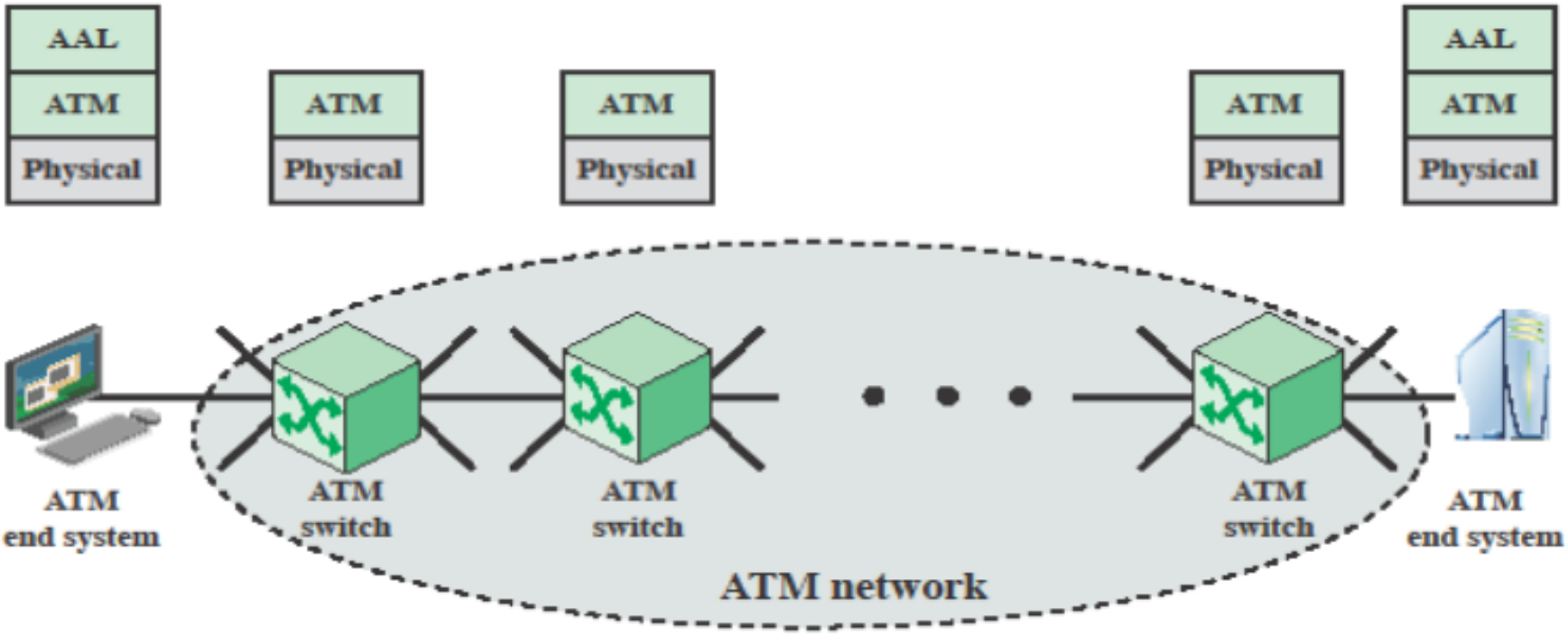


Figure 11.2 ATM Protocol Layers

Virtual Paths (VPs) and Virtual Circuits (VCs)

Figure 11.4 ATM Connection Relationships

- In ATM (Asynchronous Transfer Mode) logical connections are known as **virtual channel connections or VCCs**. The VCC is similar to virtual circuit (VC) in packet switched network. It is unit of switching used in ATM network.

  • Initially VCC is established between end users in the network.

  • After the VCC connection is established variable rate and fixed size cells are exchanged.

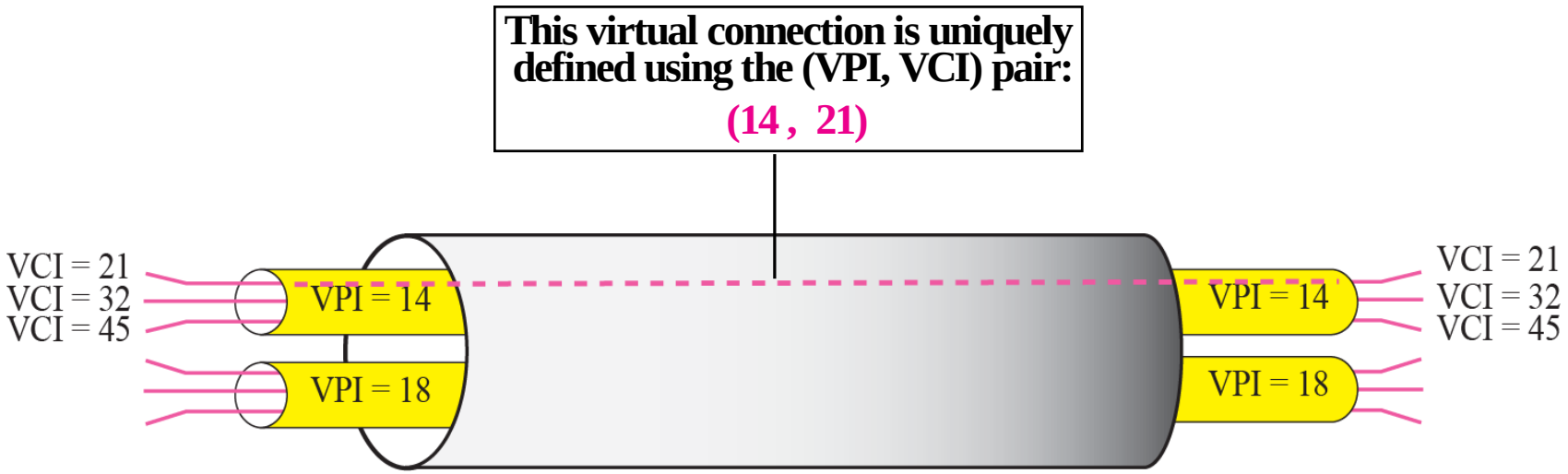
  • Here VPC i.e. Virtual Path Connection is combination of VCCs having same end points or destinations. Hence all the ATM cells travelling through VCCs in one common VPC are switched together.

  • Virtual path is identified by VPI and Virtual Channel is identified by VCI as mentioned below.

  ➡VPI (Virtual Path Identifier) identifies virtual path (8/12 bits in size).

  ➡VCI (Virtual Channel Identifier) identifies virtual channel in a virtual path (16 bits).

Figure 3.34 *Virtual circuit*



Note

A virtual connection is defined by a pair of numbers: the VPI and the VCI.

ATM Cell Format

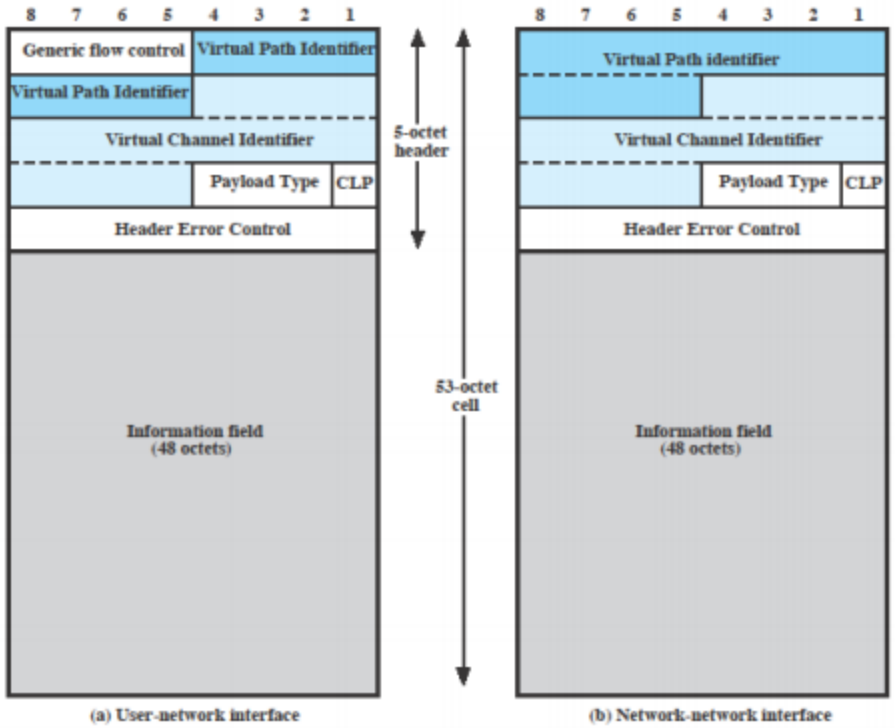


Figure 11.6 ATM Cell Format

Generic Flow Control (GFC)
provides flow control at the UNI level

Virtual Path Identifier (VPI)
identifies the cell's next VP to pass through a series of network.

Virtual Channel Identifier (VCI)
Identifies the cell's next VC inside the VP.

Payload Type (PT)
The first bit indicates whether the cell contains user data (bit 0) or control data (bit 1).
The second bit indicates congestion (0 = no congestion, 1 = congestion), and
The third bit indicates whether the cell is the last in a series of cells (1 = last cells for the frame)

Cell Loss Priority (CLP)
Indication if the cell should be discarded if it encounters extreme congestions as it moves through the network (bit 1 = discarded in referenced to cells with CLP equal to 0)

Header Error Control (HEC)
Calculates checksum only on the first 4 bytes of the header. HEC can detect error and correct a single bit error in these bytes—thus preserving the cell rather than discarding it.

Figure 3.33 *Architecture of an ATM network*

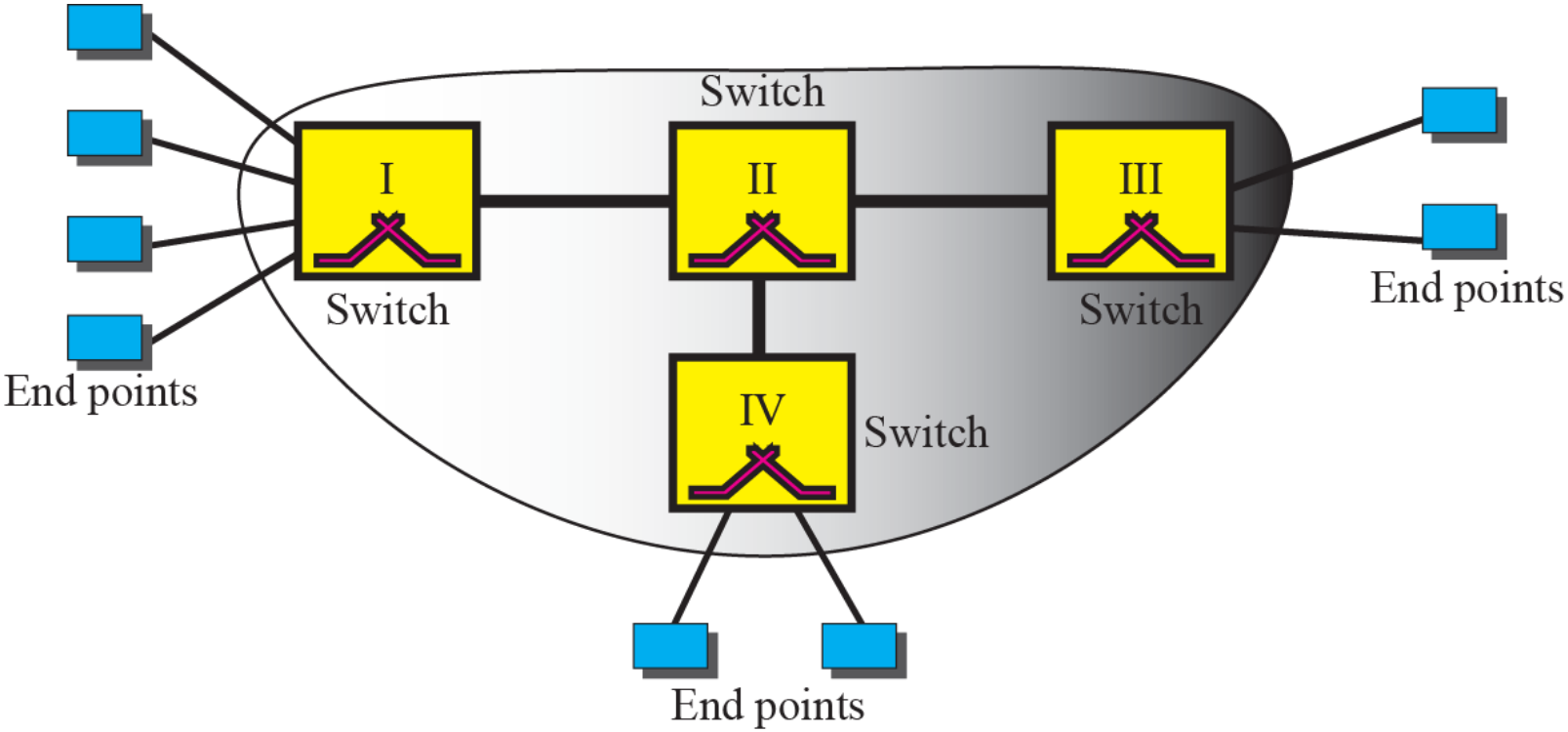


Figure 3.35 *ATM layers*

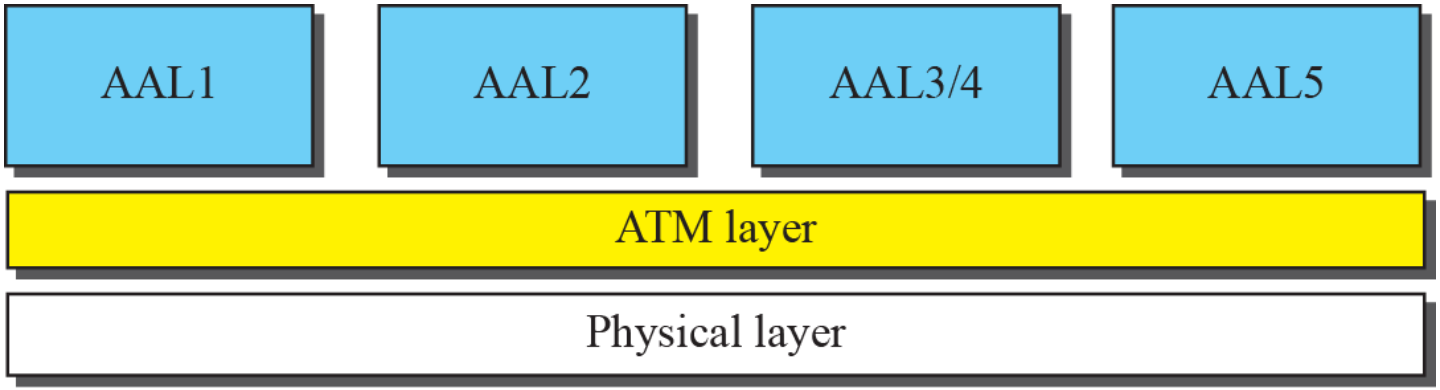


Figure 3.36 *Use of the layers*

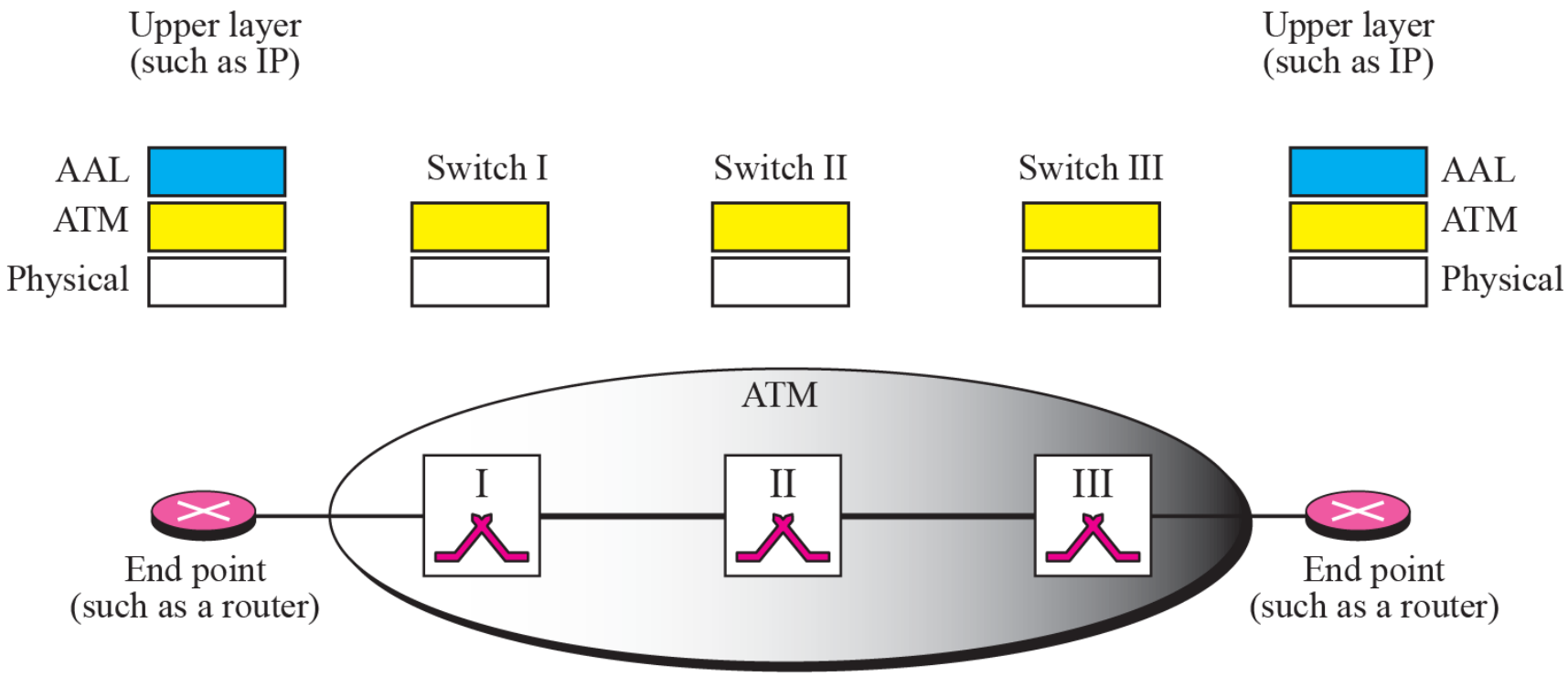


Figure 3.37 *AAL5*

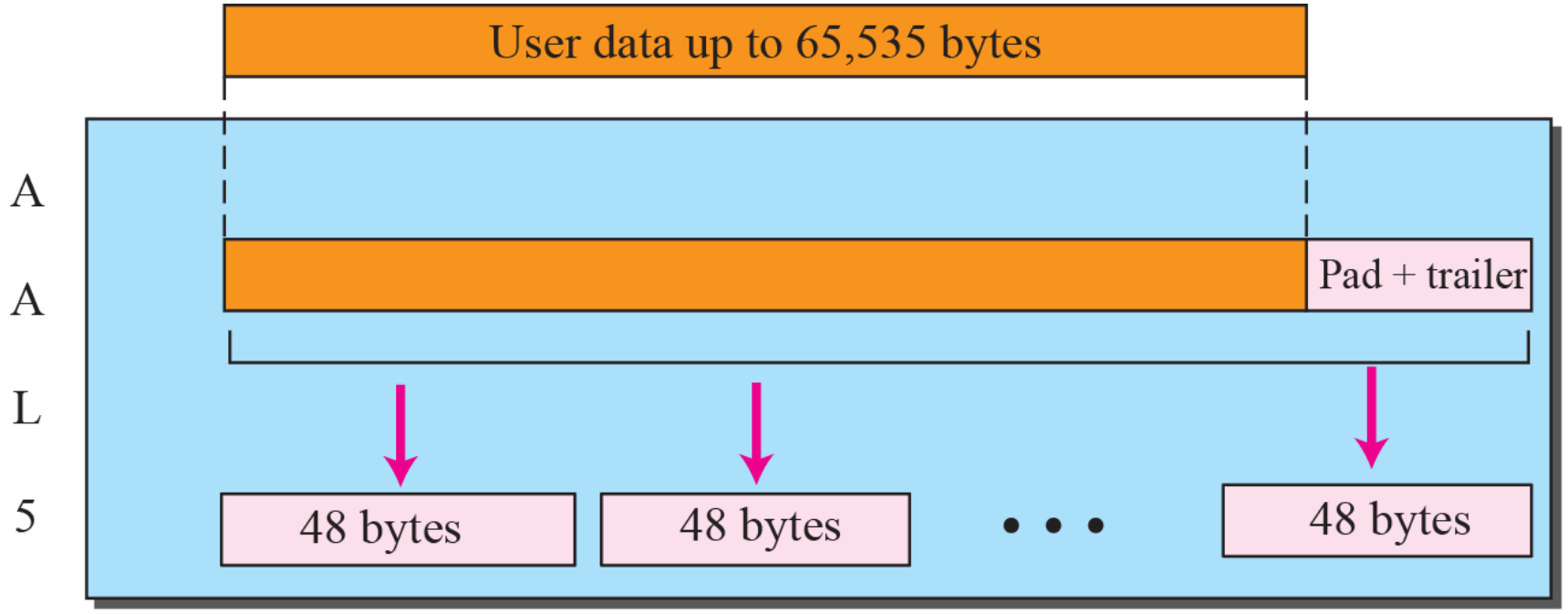


Figure 3.38 *ATM layer*