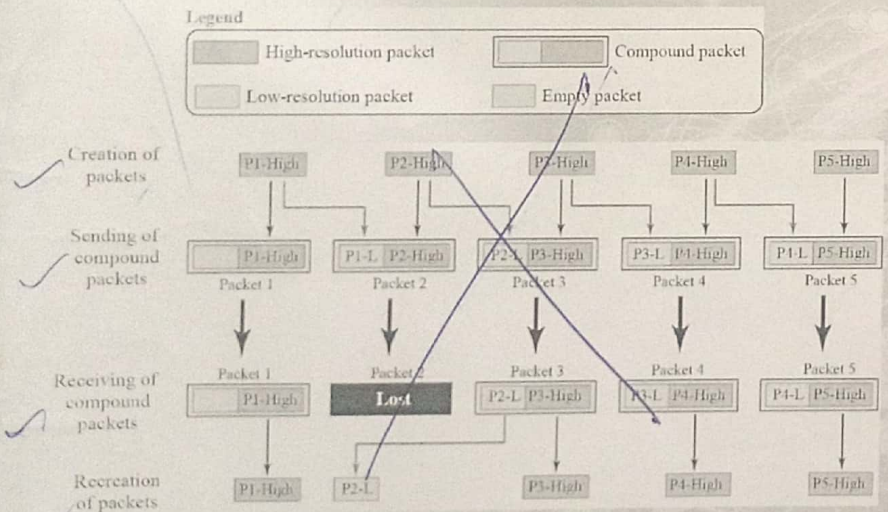
Combining Hamming Distance & Interleaving

- Hamming distance and interleaving can be combined
- We can first create n-bit packets that can correct t-bit errors
- Then we interleave m rows and send the bits column by column
- Possible to correct burst errors up to m × t bits of errors

Compounding High & Low Resolution Packets

- Creation of a duplicate of each packet with a low-resolution redundancy and combine the redundant version with the next packet
- For example, we can create four low-resolution packets out of five high-resolution packets and send them

Compounding High-and-Low resolution Packets



Data Link Control (DLC) Services

- The data link control (DLC) deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast
- Data link control functions include framing, flow control and error control

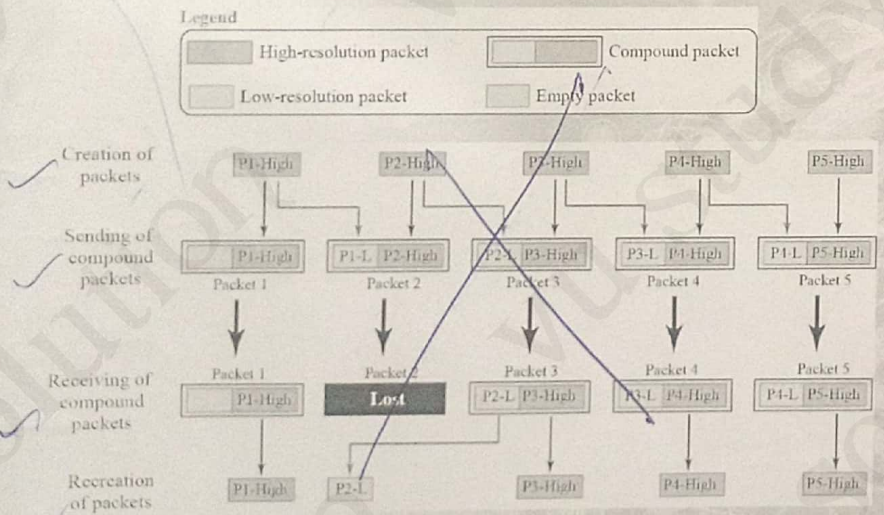
Combining Hamming Distance & Interleaving

- Hamming distance and interleaving can be combined
- We can first create n-bit packets that can correct t-bit errors
- Then we interleave m rows and send the bits column by column
- Possible to correct burst errors up to m × t bits of errors

Compounding High & Low Resolution Packets

- Creation of a duplicate of each packet with a low-resolution redundancy and combine the redundant version with the next packet
- For example, we can create four low-resolution packets out of five high-resolution packets and send them

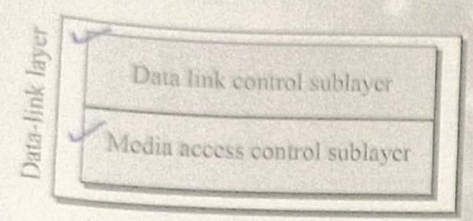
Compounding High-and-Low resolution Packets



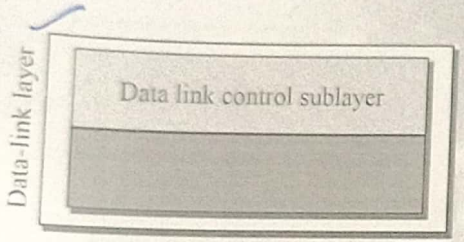
Data Link Control (DLC) Services

- The data link control (DLC) deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast
- Data link control functions include framing, flow control and error control

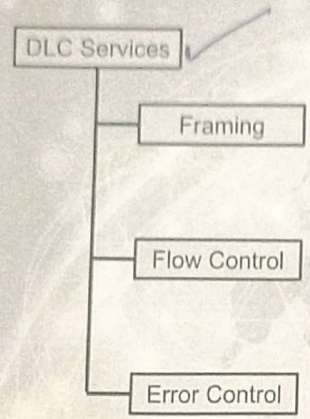
DLC Services



a. Data-link layer of a broadcast link



b. Data-link layer of a point-to-point link



Imp to view

Framing

- Data-link layer needs to pack bits into frames, so that each frame is distinguishable from another

- Our postal system practices a type of framing

- Framing separates a message by adding a sender address and a destination address

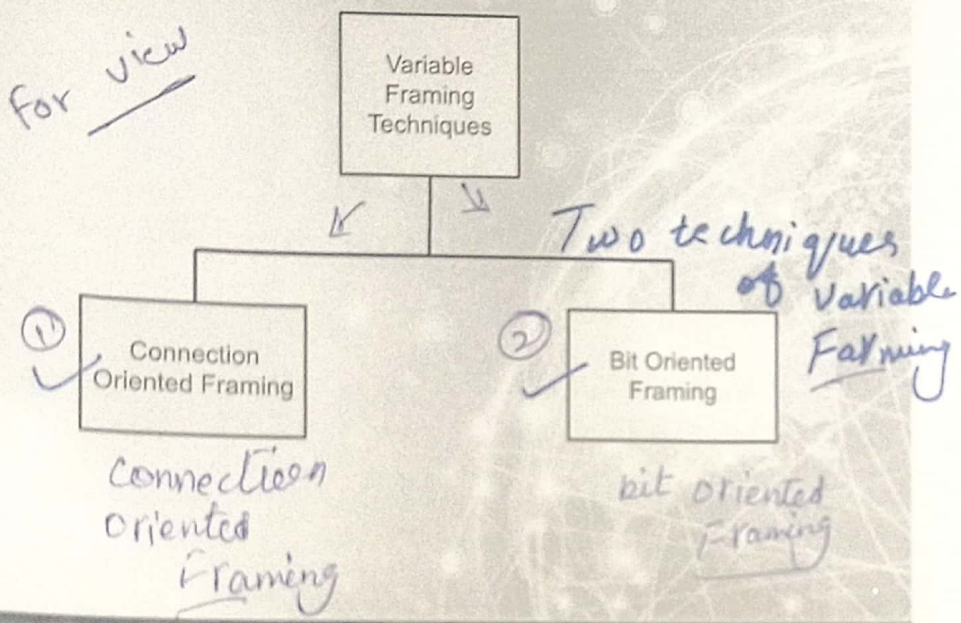
Framing

- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt

Frame Size

- Why not one BIG Frame?
- Frames can be of:
  - ✓ Fixed Size
    - ➢ Size acts as a boundary/delimiter
  - ✓ Variable Size
    - ➢ How to define Beginning and End of a Frame?

Variable Framing Techniques



For view

Two techniques of Variable Farming

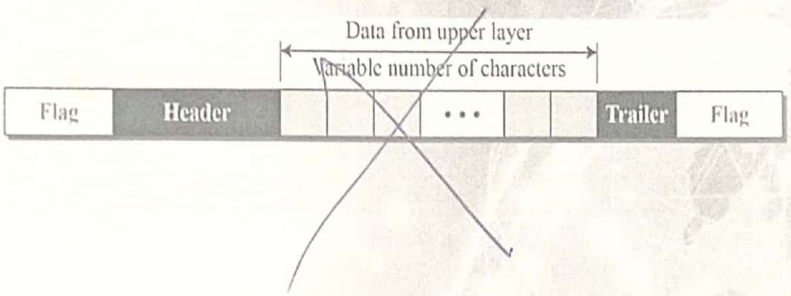
1 Connection Oriented Framing

2 Bit Oriented Framing

Connection oriented Framing

bit oriented Framing

A Frame in a Character-Oriented Protocol



Connection Oriented Framing

- Data to be carried are 8-bit characters

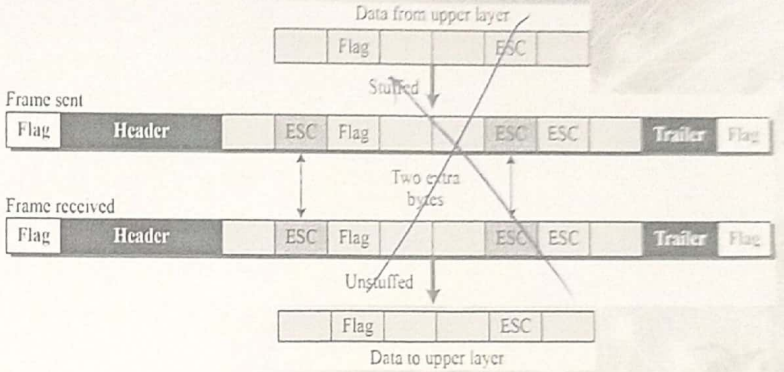
Byte Stuffing in Connection-Oriented Framing

- Connection-oriented Framing used text characters as flags
- Nowadays any character used for flag can also be a part of the data
- In order to avoid confusing the receiver, we use Byte Stuffing

Byte Stuffing in Connection-Oriented Framing

- Several Issues:
  - ✓ One or more escape characters followed by a byte with same pattern as a flag?
  - ✓ Unicode (16/32 bit) vs. 8-bit characters
- Data is stuffed with a pre-defined Escape Character (byte) when there is a character with same pattern as a flag

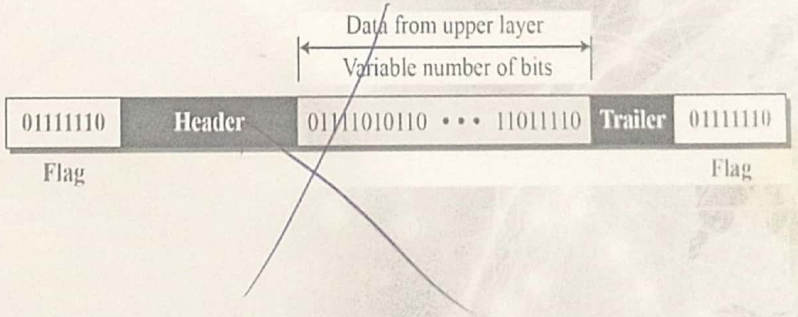
Byte Stuffing and Unstuffing



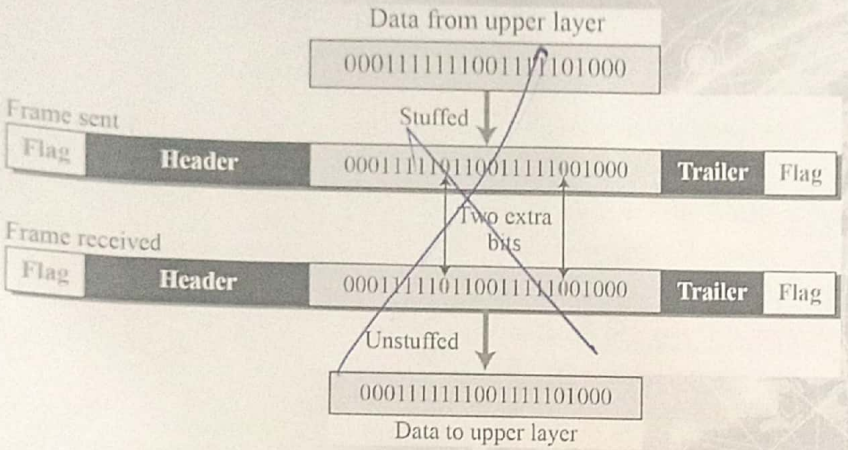
Bit-Oriented Framing

- Data section of frame is a sequence of bits
- We need a delimiter to separate one frame from the other
- A special 8-bit pattern (01111110) to define beginning and end of a frame
- Same issue as Connection-oriented Framing

A Frame in a Bit-Oriented Protocol



Bit Stuffing and Unstuffing



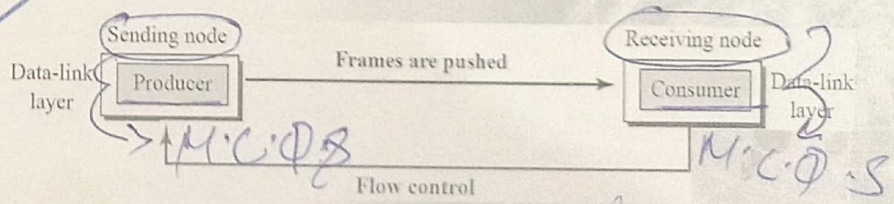
Flow and Error Control

- One of the responsibilities of the data-link control sublayer is flow and error control at the data-link layer.

Flow Control

- Balance between production and consumption rates
- If frames are produced faster than they are consumed at the receiving data link layer, the frames will be discarded
- Use of buffers; one at sending end and other at receiving end

Flow Control at the Data Link Layer



Example

- Consumers need to communicate with the producers on two occasions:
  - ✓ When the buffer is full; &
  - ✓ When there are vacancies

✓ If the two parties use a buffer with only one slot, the communication can be easier

Error Control

- Error Control at Data Link layer uses CRC in one of the two ways:

✓ If a frame is corrupted, it is silently discarded and if it is good, it is delivered to network layer

✓ If frame is corrupted, it is silently discarded and if it is good, an acknowledgement is sent to sender

Connectionless and Connection-Oriented

- A DLC protocol can be either connectionless or connection-oriented

✓ Connectionless: No relationship between the frames

- Connection-Oriented: Frames are numbered and sent in order

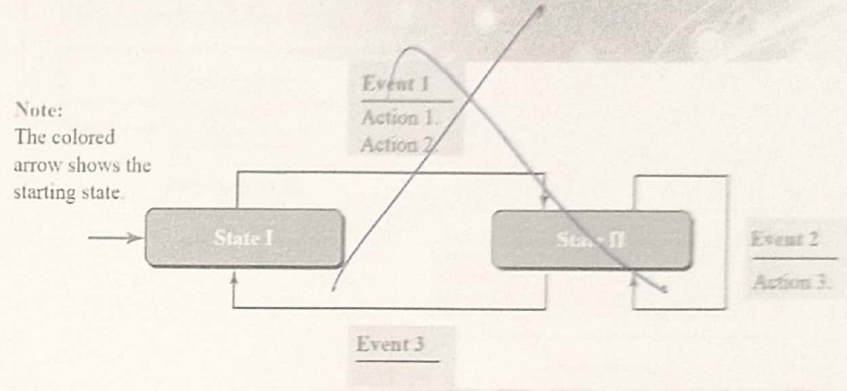
DATA-LINK LAYER PROTOCOLS

- Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:
  - ✓ Simple Protocol
  - ✓ Stop-and-Wait Protocol
  - ✓ Go-Back-N Protocol
  - ✓ Selective-Repeat Protocol
- Last two protocols have almost disappeared completely

Finite State Machine (FSM)

- A machine with a finite number of states
- Machines stays in one of the states until an event occurs
- Each event is associated with 2 reactions:
  - ✓ List of actions to be performed
  - ✓ Determining the next state

Finite State Machine (FSM)



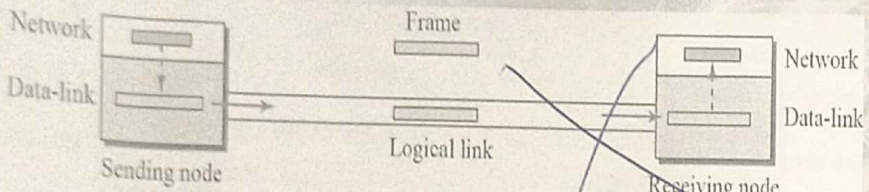
DATA-LINK LAYER PROTOCOLS

- Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:
  - ✓ Simple Protocol
  - ✓ Stop-and-Wait Protocol
  - ✓ Go-Back-N Protocol
  - ✓ Selective-Repeat Protocol

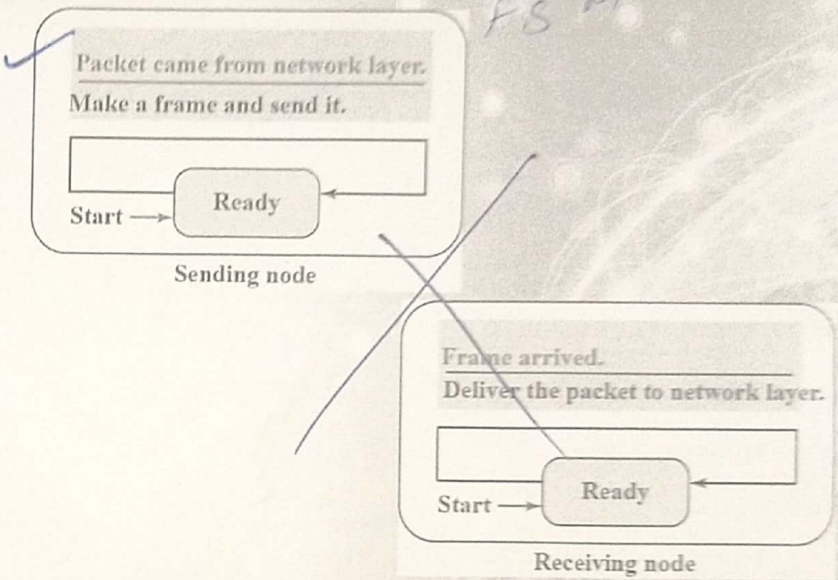
Simple Protocol

- Simple protocol has neither flow nor error control
- Assumption: The receiver can immediately handle any frame it receives
- The receiver can never be overwhelmed with incoming frames

Simple Protocol

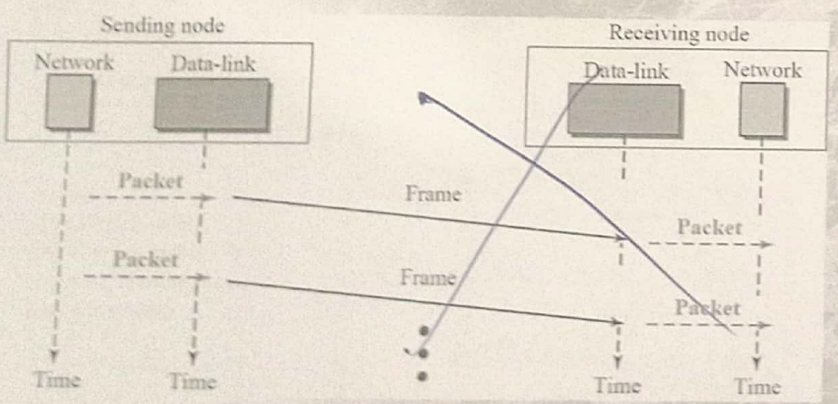


FSM for Simple Protocol



Example

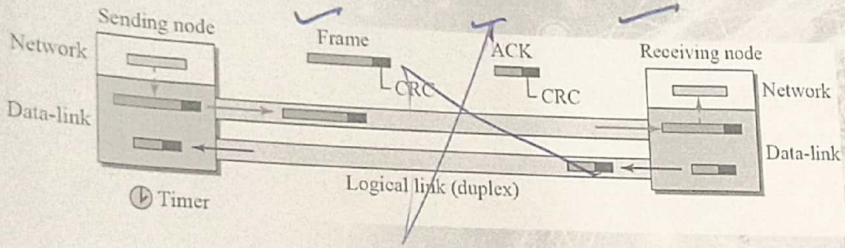
Here is an example of communication using this protocol. It is very simple. The sender sends frames one after another without even thinking about the receiver.



Stop-and-Wait Protocol

- Stop-and-Wait protocol uses both flow and error control
- The sender sends one frame at a time and waits for an acknowledgment before sending the next one
- To detect corrupted frames, we add a CRC code

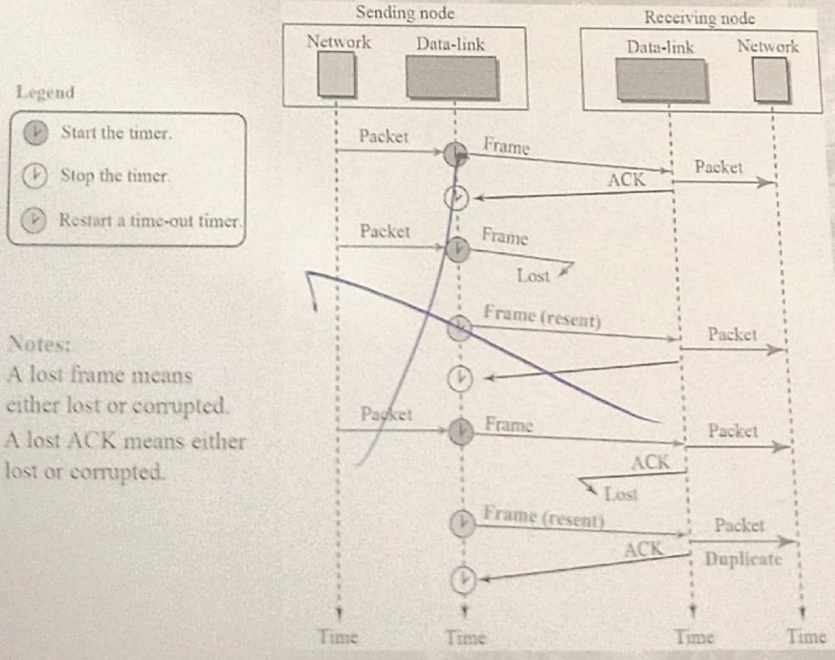
Stop-and-Wait Protocol



Stop-and-Wait Protocol

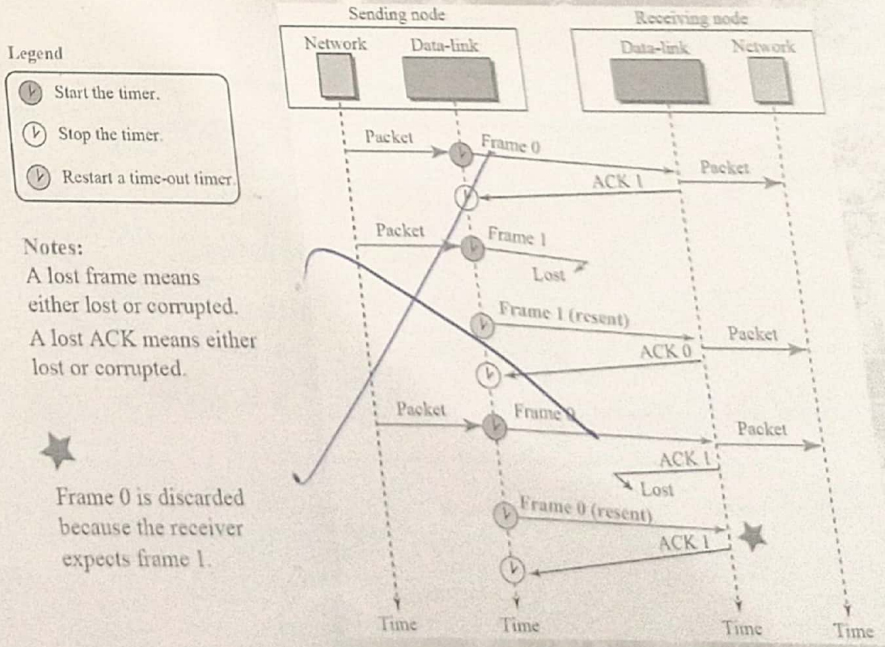
- Stop-and-Wait protocol uses both flow and error control
- The sender sends one frame at a time and waits for an acknowledgment before sending the next one
- To detect corrupted frames, we add a CRC code

Example



Notes:
A lost frame means either lost or corrupted.
A lost ACK means either lost or corrupted.

Example



Notes:
A lost frame means either lost or corrupted.
A lost ACK means either lost or corrupted.

Frame 0 is discarded because the receiver expects frame 1.

Piggybacking

- Both Simple and Stop-and-wait protocols are designed for unidirectional communication
- Data flows in one direction and ACK travels in the other
- To make the system efficient, the data in one direction is piggybacked with the acknowledgment in the other direction

High-level Data Link Control (HDLC)

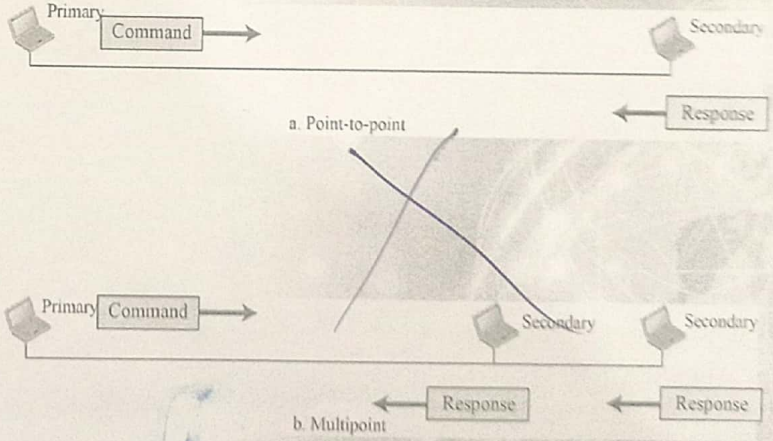
- Bit -oriented protocol for communication over point-to-point and multipoint links
- It implements Stop-and-Wait protocol
- Most of the concepts defined in this protocol is the basis for other protocols such as PPP, Ethernet, or wireless LANs

Configurations & Transfer Modes in HDLC

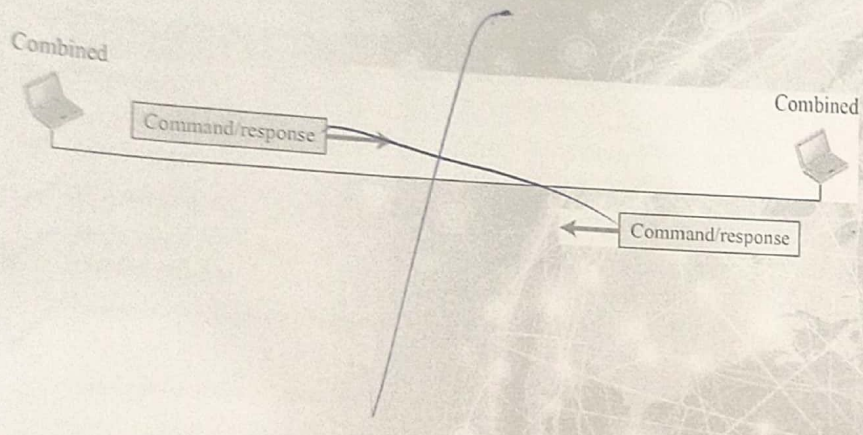
- HDLC provides two common transfer modes that can be used in different configurations:
  - ✓ Normal Response Mode (NRM) &
  - ✓ Asynchronous Balanced Mode (ABM)

Normal Response Mode
Asynchronous Balanced Mode

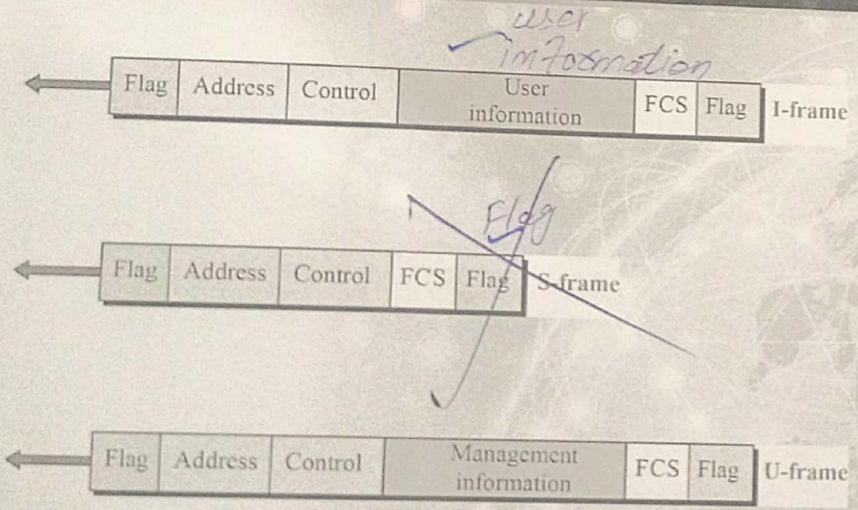
Normal Response Mode



Asynchronous Balanced Mode



HDLC Frames



Framing

- HDLC defines three types of frames:
  - ✓ information frames (I-frames)
  - ✓ Supervisory frames (S-frames)
  - ✓ Unnumbered frames (U-frames)

Point-to-Point Protocol (PPP)

- Most common protocol for point-to-point access
- Millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP
- To control and manage the transfer of data, there is a need for a PPP at the data-link layer

Services provided by PPP

The designers of PPP have included several services to make it suitable for a point-to-point protocol, but have ignored some traditional services to make it simple

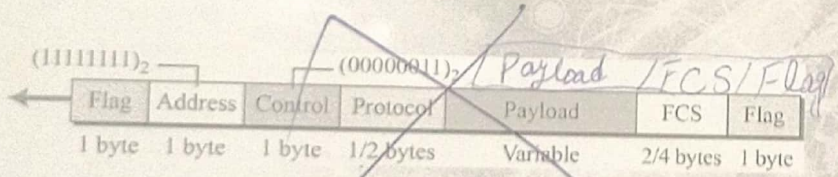
Services Included	Services Not Included
Framing	Flow Control
Link Establishment and Data Exchange	Error Correction (PPP has CRC detection only)
Authentication	No Sequence Numbering
Multilink PPP Address configuration	Absence of sophisticated Addressing Mechanism
Network Address configuration	

Point-to-Point Protocol (PPP)

- Most common protocol for point-to-point access
- Millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP
- To control and manage the transfer of data, there is a need for a PPP at the data-link layer

PPP Frame Format

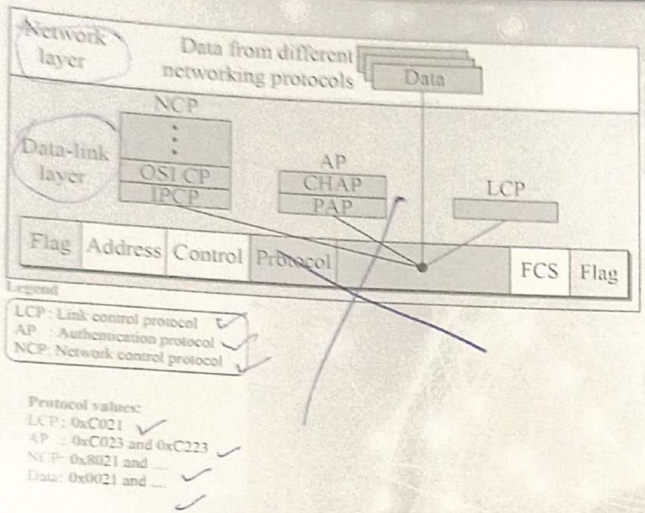
PPP uses a character-oriented (or byte-oriented) frame



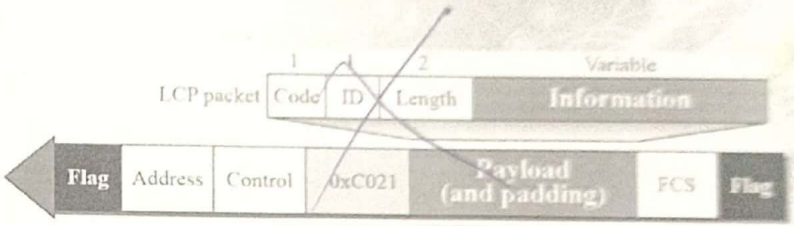
Multiplexing in PPP

- Although PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate and carry the network-layer data
- Three sets of protocols are:
  - Link Control Protocol (LCP)
  - Two Authentication Protocols (APs)
  - Several Network Control Protocols (NCPs)

Multiplexing in PPP



LCP Packet encapsulated in a Frame



LCP Packets

Code	Packet Type	Description
0x01	Configure-request	Contains the list of proposed options and their values
0x02	Configure-ack	Accepts all options proposed
0x03	Configure-nak	Announces that some options are not acceptable
0x04	Configure-reject	Announces that some options are not recognized
0x05	Terminate-request	Request to shut down the line
0x06	Terminate-ack	Accept the shutdown request
0x07	Code-reject	Announces an unknown code
0x08	Protocol-reject	Announces an unknown protocol
0x09	Echo-request	A type of hello message to check if the other end is alive
0x0A	Echo-reply	The response to the echo-request message
0x0B	Discard-request	A request to discard the packet

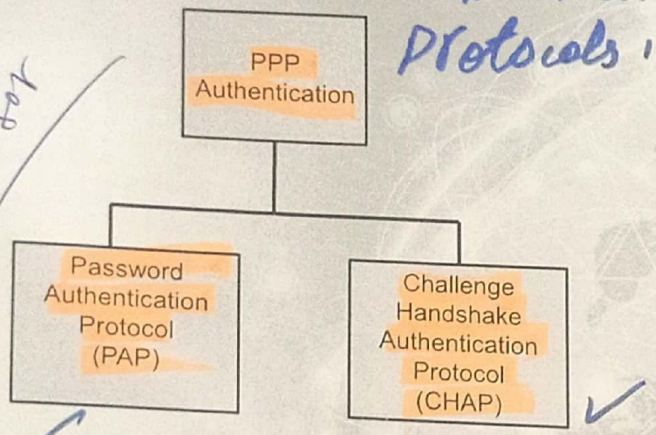
Multiplexing in PPP

- Although PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate and carry the network-layer data
- Three sets of protocols are:
  - Link Control Protocol (LCP)
  - Two Authentication Protocols (APs)
  - Several Network Control Protocols (NCPs)

Authentication Protocols in PPP

Two Authentication Protocols in PPP.

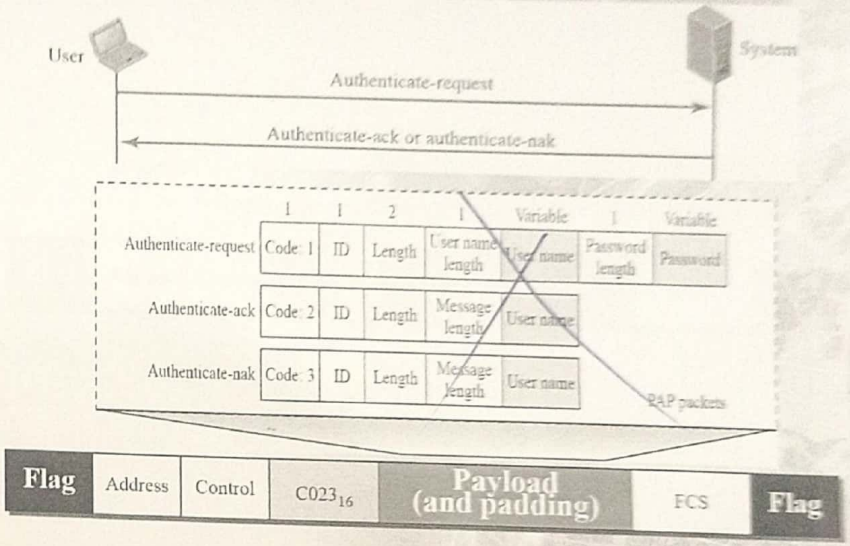
Full form + Stand for



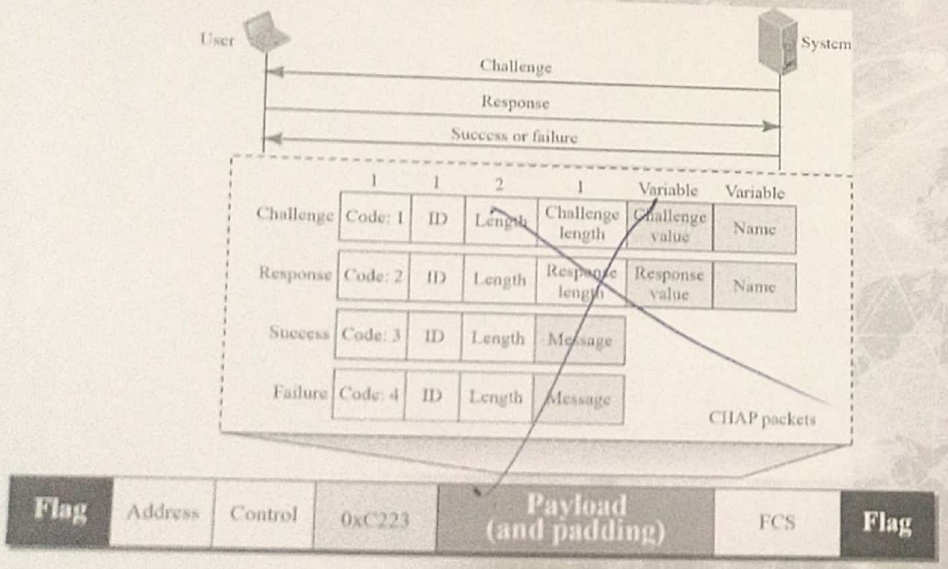
Password Authentication Protocol

Challenge Handshake Protocol

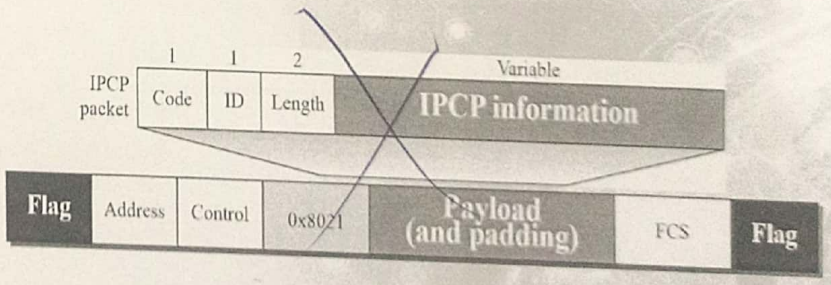
PAP packets encapsulated in a PPP frame



CHAP Packets encapsulated in a PPP frame



Internet Protocol Control Protocol (IPCP)



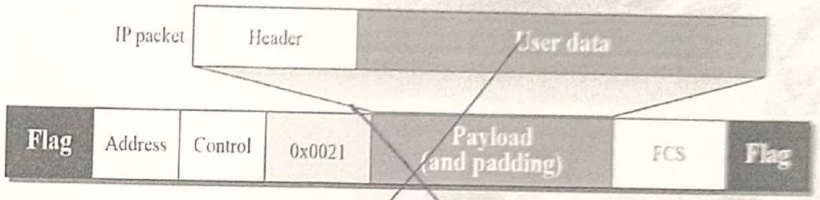
Code values for IPCP Packets

Internet Protocol control Protocol

Code	IPCP Packet
0x01	Configure-request
0x02	Configure-ack
0x03	Configure-nak
0x04	Configure-reject
0x05	Terminate-request
0x06	Terminate-ack
0x07	Code-reject

on Your choice for MCQs

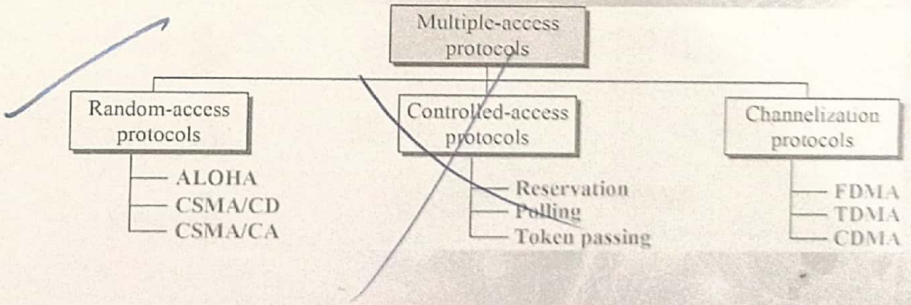
IP datagram encapsulated in a PPP frame



Media Access Control (MAC) Sub-Layer

- When nodes use a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link
- Many protocols have been devised to handle access to a shared link
- All of these protocols belong to Media Access Control (MAC) sub-layer

Taxonomy of Multiple-Access Protocols



Random Access

CTP#12

- In random-access or contention no station is superior to the other and none is assigned control over the other
- Station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send
- This decision depends on the state of the medium (idle or busy)

ALOHA

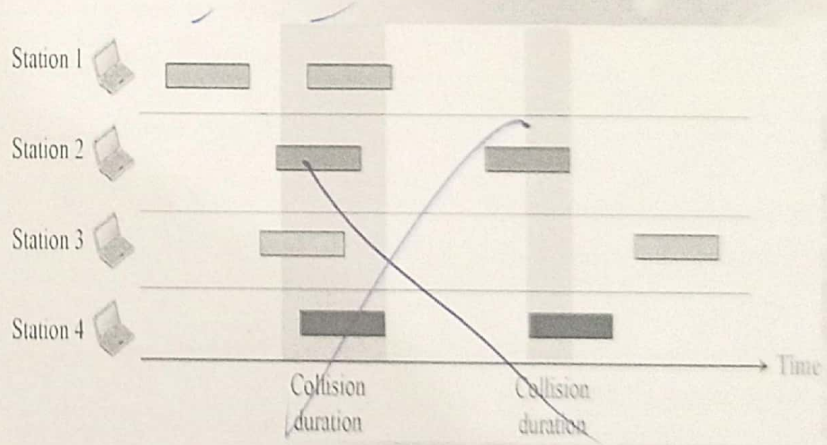
- ALOHA, the earliest random access method, was developed in early 1970s
- Designed for a radio (wireless) LAN, but it can be used on any shared medium
- Potential collisions in this arrangement as the medium is shared between the stations

ALOHA

- When a station sends data, another station may attempt to do so at the same time
- The data from the two stations collide and become garbled

گندا / ٹکرانا / collide

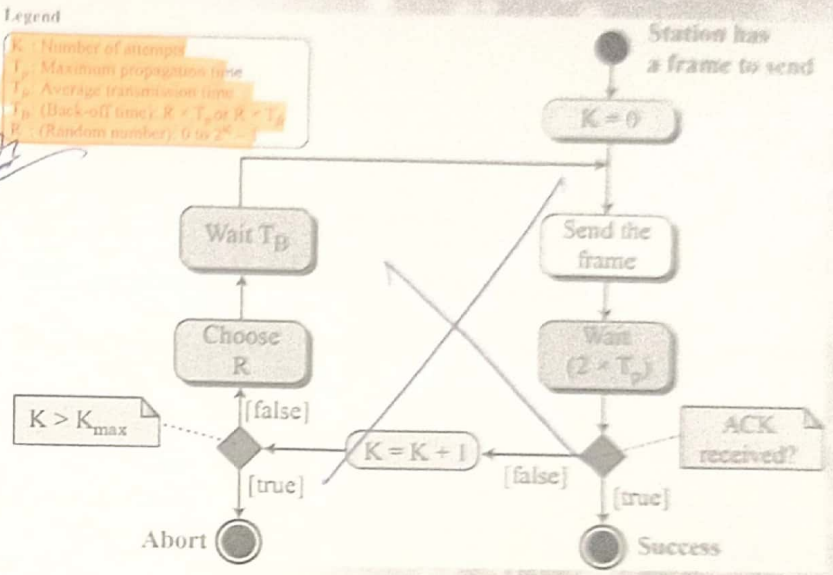
Frames in a pure ALOHA network



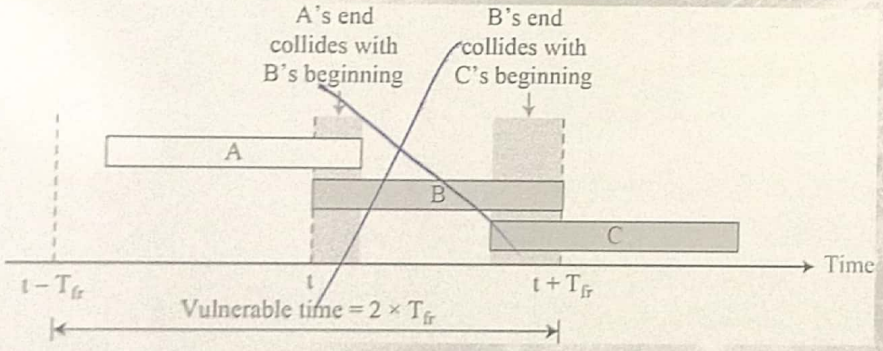
ALOHA

- ALOHA, the earliest random access method, was developed in early 1970s
- Designed for a radio (wireless) LAN, but it can be used on any shared medium
- Potential collisions in this arrangement as the medium is shared between the stations

Procedure for pure ALOHA protocol



Vulnerable Time for pure ALOHA protocol



Slotted ALOHA

Vulnerable Time = T_{fr}

$T_{fr+} = t + T_{fr}$

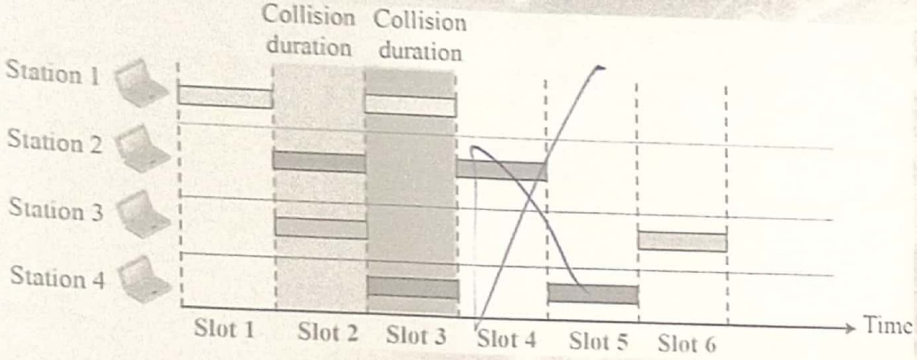
$T_{Pr} = t - T_{fr}$

Vulnerable Time = Propagation Time

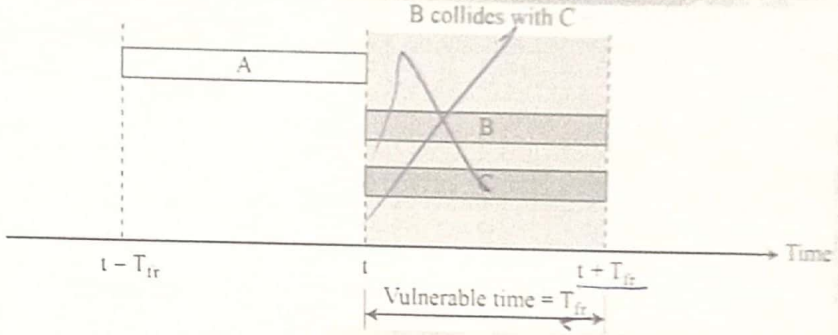
T_{fr} LVS $2 \times T_{fr}$

- We divide time into slots of T_{fr} sec and force the station to send only at the beginning of the slot
- Invented to improve the efficiency of pure ALOHA
- If a station misses the time slot, it must wait until beginning of next time slot reducing vulnerable time to T_{fr} (vs. 2 x T_{fr} for pure ALOHA)

Frames in a Slotted ALOHA Network



Vulnerable Time for Slotted ALOHA



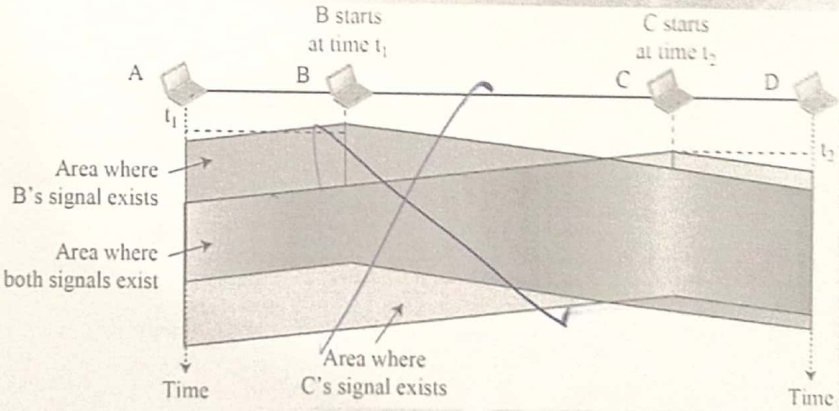
Carrier Sense Multiple Access (CSMA)

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

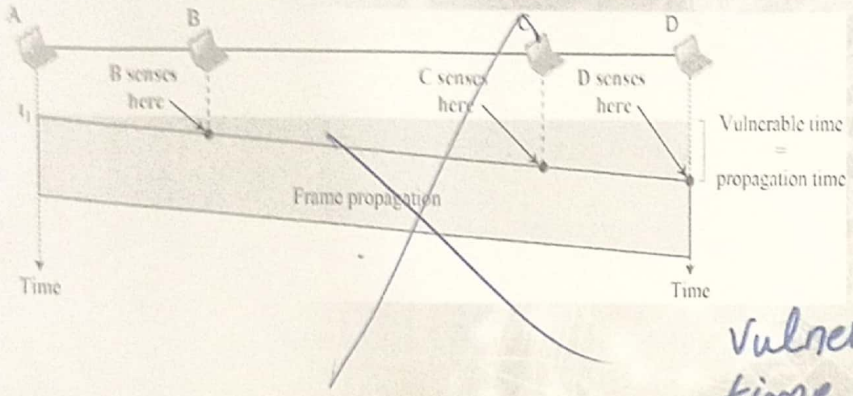
The chance of collision is reduced as the station is required to sense/listen to the medium before sending data

- 'sense before transmit' or 'listen before talk'

Space/Time Model of a Collision in CSMA

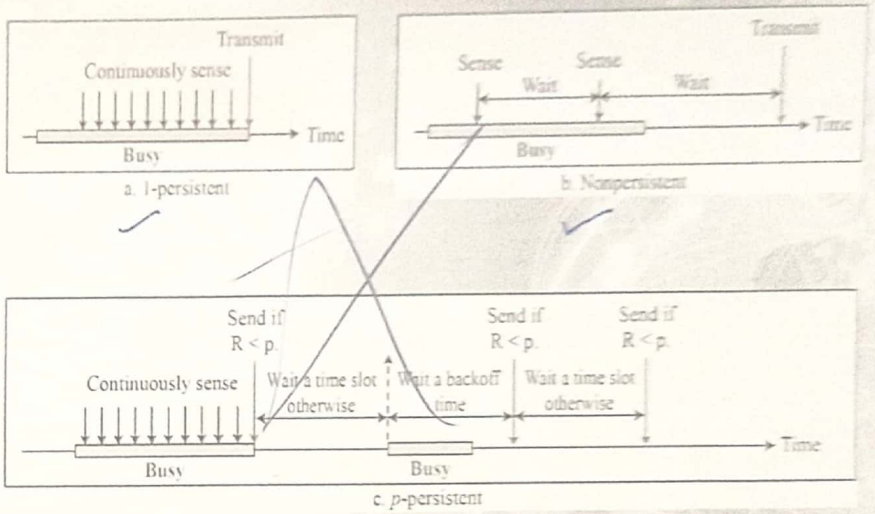


Vulnerable Time in CSMA



Vulnerable time = propagation Time

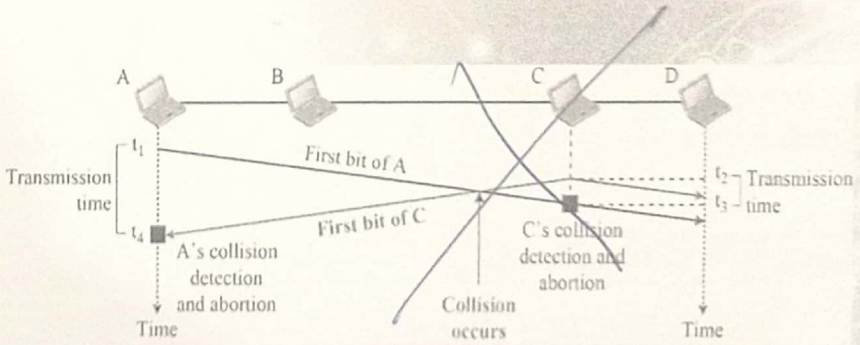
Behavior of Three Persistence Methods



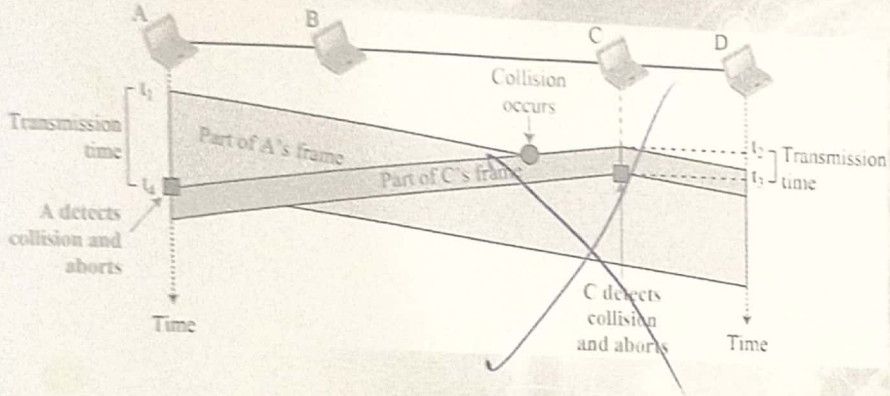
Carrier Sense Multiple Access/Collision Detection

- CSMA method does not specify the procedure following a collision
- CSMA/CD augments the algorithm to handle the collision
- The station monitors the medium after it sends a frame to see if the transmission was successful. If there is a collision, the frame is sent again

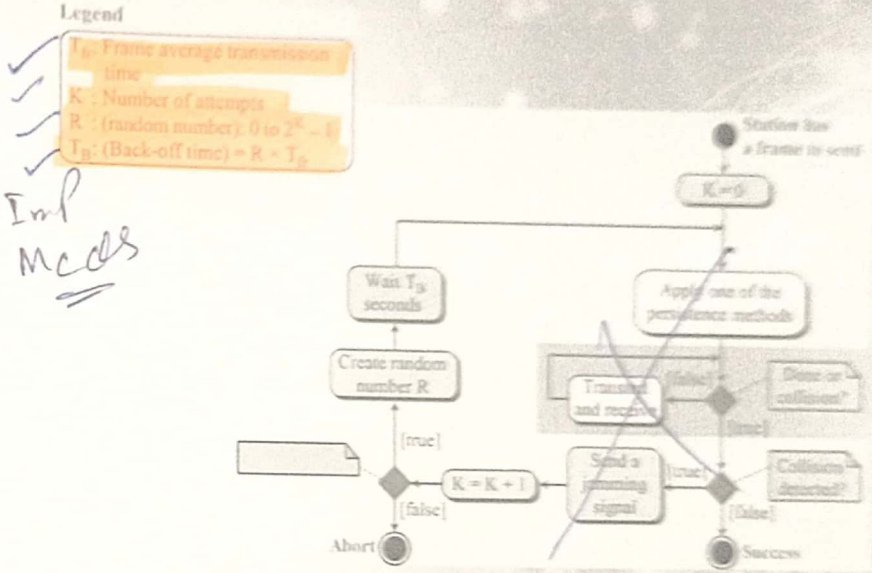
Collision of the First Bits in CSMA/CD



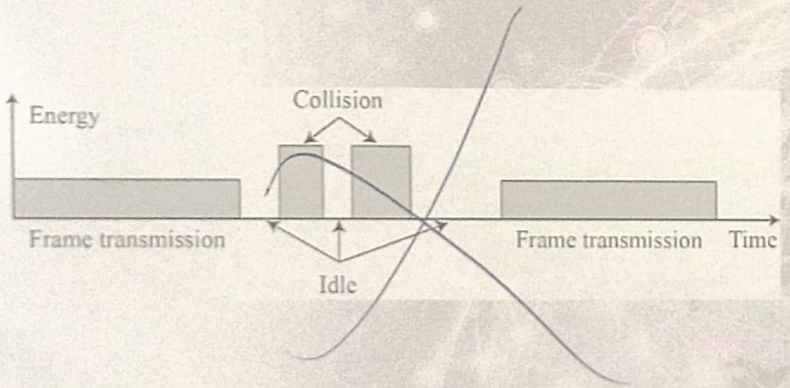
Collision and Abortion in CSMA/CD



Flow Diagram for the CSMA/CD



Energy Level During Transmission, Idleness and Collision

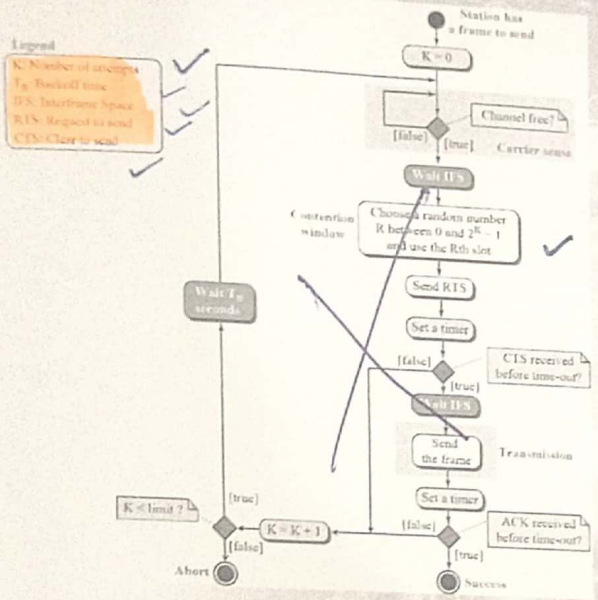


Carrier Sense Multiple Access/Collision Avoidance

- CSMA/CA was invented for Wireless Networks
- Collisions are avoided through the use of three strategies:

1. ✓ The Interfame Space
2. ✓ The Contention Window
3. ✓ Acknowledgements

Flow Diagram for CSMA/CA



Carrier Sense Multiple Access/Collision Avoidance

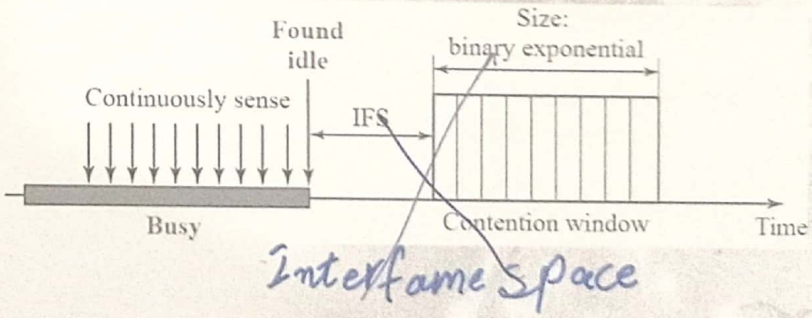
- CSMA/CA was invented for Wireless Networks

- Collisions are avoided through the use of three strategies:
  - The Interframe Space
  - The Contention Window
  - Acknowledgements

CSMA/CA

- Interframe Space (IFS): Collisions are avoided by deferring transmission even if the channel is idle
- Contention Window: Amount of time divided into slots. Station chooses a random number of slots as its wait time (one slot first time and double each time system cannot detect an idle channel)

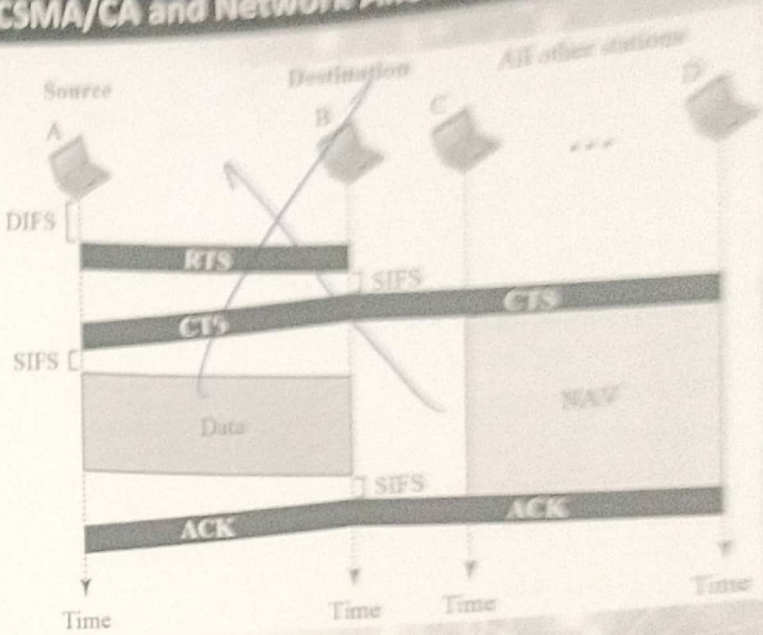
Contention Window



CSMA/CA

- Acknowledgement: Positive acknowledgement and time-out timer can help guarantee that the receiver has received the frame

CSMA/CA and Network Allocation Vector (NAV)



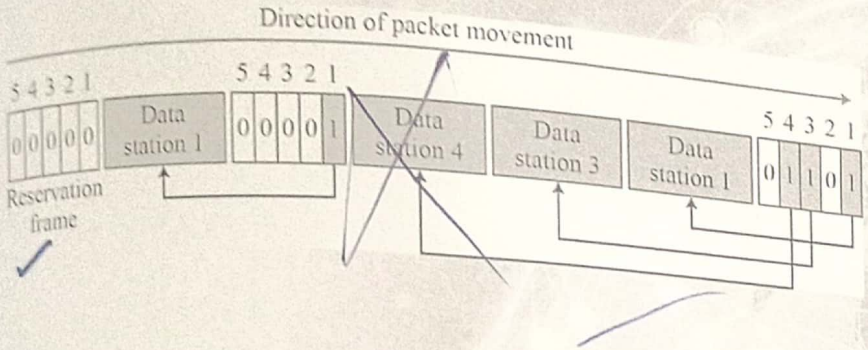
CONTROLLED ACCESS

- The stations consult one another to find which station has the right to send
- A station cannot send unless authorized by other stations
- We discuss three controlled-access methods:
  - ✓ Reservation
  - ✓ Polling
  - ✓ Token Passing

Reservation

- In the reservation method, a station needs to make a reservation before sending data
- Time is divided into intervals
- In each interval, a reservation frame precedes the data frames sent in that interval

Reservation Access Method



Polling

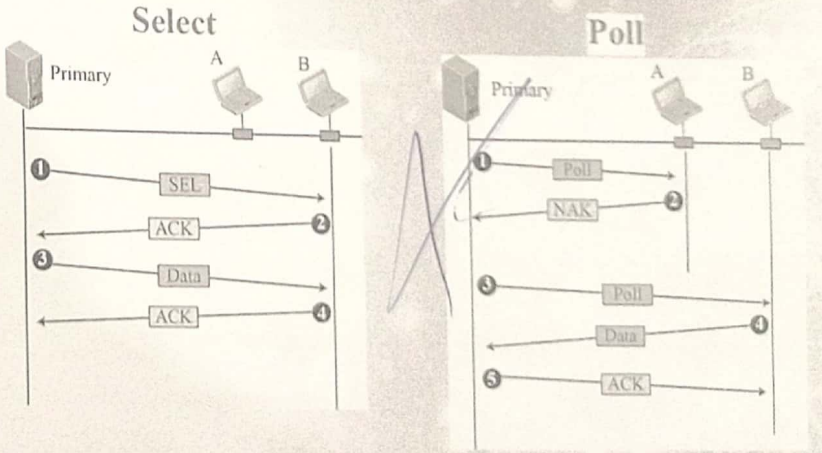
- The primary device controls the link; the secondary devices follow its instructions.

Polling

Sq) what is Polling?

- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.
- All data exchanges must be made through primary device even when the ultimate destination is a secondary device.

Select and Poll Functions in Polling-Access Method



CONTROLLED ACCESS

- Three controlled-access methods:
  - ✓ Reservation
  - ✓ Polling
  - ✓ Token Passing

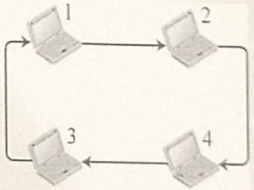
Token Passing

- In the token-passing method, the stations in a network are organized in a logical ring
- For each station, there is a predecessor and a successor
- The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring

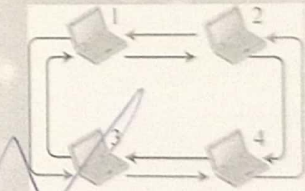
Token Passing

- Special packet called TOKEN circulates through the ring
- Possession of TOKEN gives the station the right to send the data
- TOKEN Management is required to manage possession time, Token monitoring, priority assignment etc.

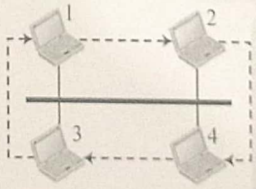
Logical Ring & Physical Topology in Token-Passing Method



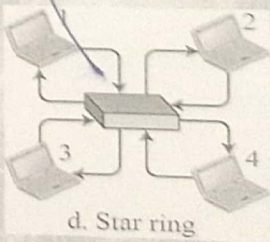
a. Physical ring



b. Dual ring



c. Bus ring



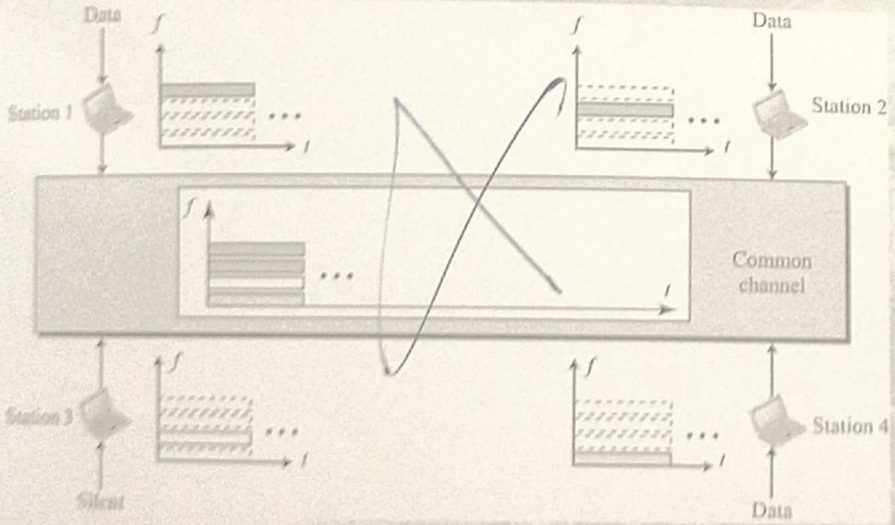
d. Star ring

CHANNELIZATION (Channel Partition)

- The available bandwidth of a link is shared in time, frequency, or through code, among different stations

- We discuss three protocols:
  - ✓ Frequency Division Multiple Access (FDMA)
  - ✓ Time Division multiple Access (TDMA)
  - ✓ Code Division Multiple Access (CDMA)

Frequency-Division Multiple Access (FDMA)



Frequency-Division Multiple Access (FDMA)

- In FDMA, the available bandwidth is divided into frequency bands

- Each station is allocated a band to send its data. i.e. each band is reserved for a specific station, and it belongs to the station all the time

- Each station also uses a bandpass filter to confine the transmitter frequencies

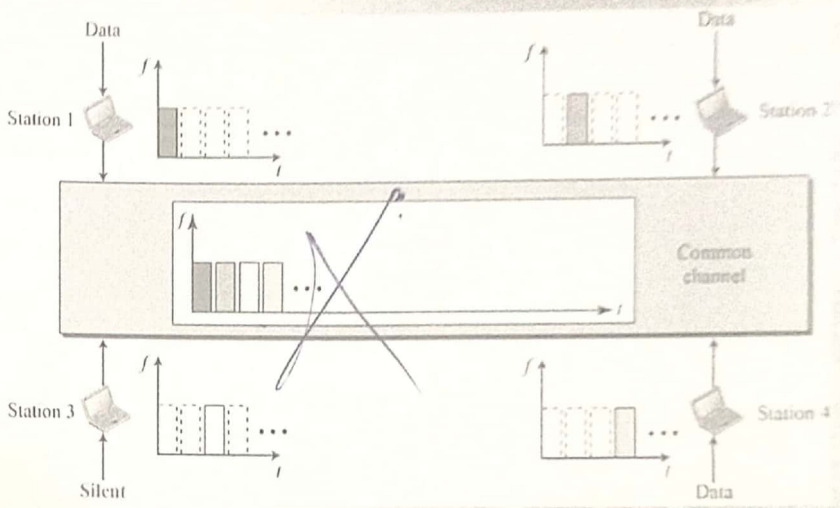
CHANNELIZATION (Channel Partition)

- Three protocols:
  - ✓ Frequency Division Multiple Access (FDMA)
  - ✓ Time Division Multiple Access (TDMA)
  - ✓ Code Division Multiple Access (CDMA)

TDMA

- Stations share the bandwidth of the channel in time
- Each station is allocated a time slot during which it can send data
- Each station transmits its data in its assigned time slot

Time-Division Multiple Access (TDMA)



CHANNELIZATION (Channel Partition)

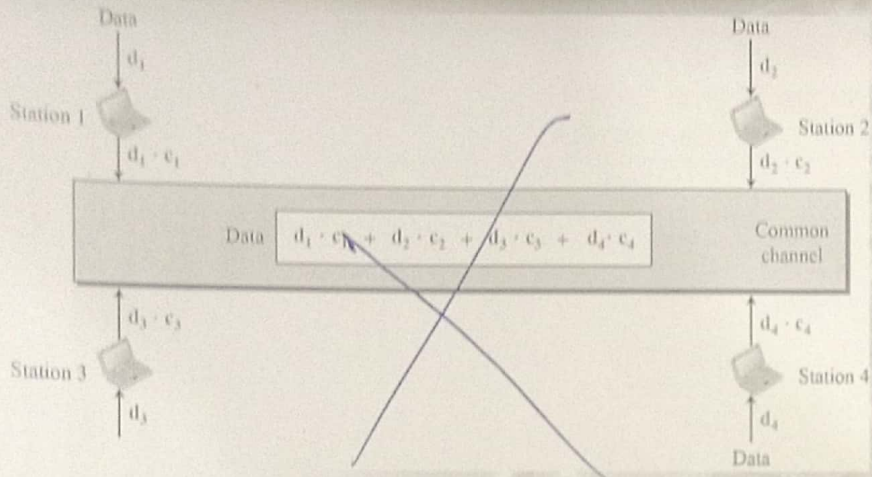
- Three protocols:
  - ✓ Frequency Division Multiple Access (FDMA)
  - ✓ Time Division Multiple Access (TDMA)
  - ✓ Code Division Multiple Access (CDMA)

Code Division Multiple Access (CDMA)

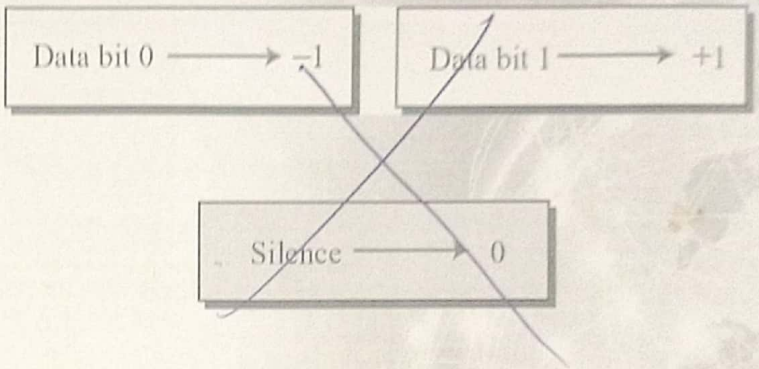
- CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link
- CDMA differs from TDMA in that all stations can send data simultaneously; there is no timesharing

ایک ہی وقت میں

Simple idea of Communication with Code



Data Representation in CDMA



Data Rep

Ethernet Protocol

APP #13

- Data-link layer and the physical layer are the territory of the local and wide area networks
- We can have wired or wireless networks

territory

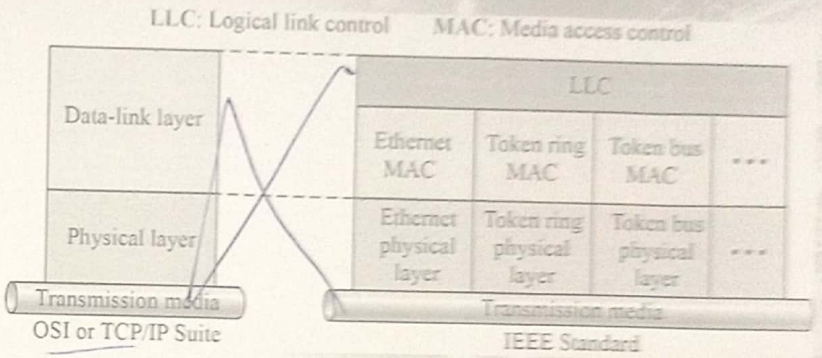
IEEE Project 802

- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable inter-communication among equipment from a variety of manufacturers
- Project 802 did not seek to replace any part of the OSI model or TCP/IP protocol suite

IEEE Project 802

- A way of specifying functions of the physical layer and the data-link layer of major LAN protocols

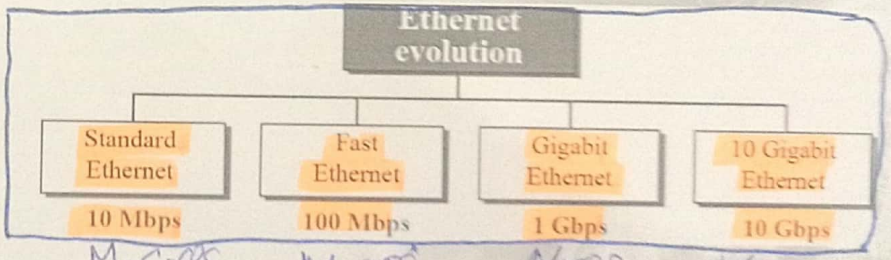
IEEE Standard for LANs



Ethernet Evolution

- The Ethernet LAN was developed in the 1970s
- Since then, it has gone through four generations:
  - ✓ Standard Ethernet (10 Mbps)
  - ✓ Fast Ethernet (100 Mbps)
  - ✓ Gigabit Ethernet (1 Gbps)
  - ✓ 10 Gigabit Ethernet (10 Gbps)

Ethernet Evolution



Standard Ethernet

- The original Ethernet technology with the data rate of 10 Mbps is called Standard Ethernet
- Most implementations have moved to later evolutions
- Still some features of the Standard Ethernet that have not changed during the evolution

Connectionless & Unreliable Service

- Each frame is independent of other
- No connection establishment or tear down process
- The sender may overwhelm receiver with frames and frames are dropped
- If frame drops, sender will not know about it unless we are using TCP (Transport)

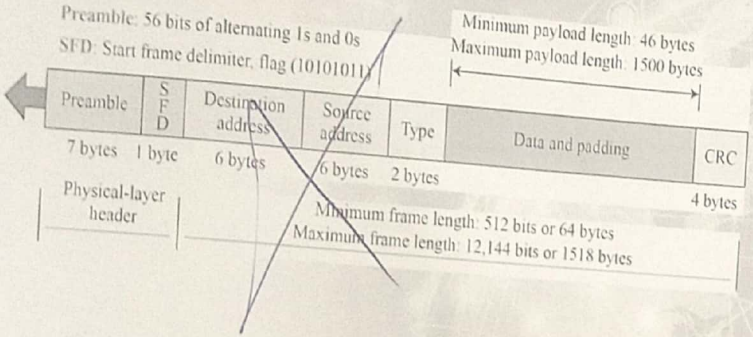
Connectionless & Unreliable Service

- Ethernet is unreliable like IP and UDP
- If a frame is corrupted, receiver silently drops it
- Left to high level protocols to find out abut it

Standard Ethernet

- The original Ethernet technology with the data rate of 10 Mbps is called Standard Ethernet

Ethernet Frame Format



Addressing

- For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

Addressing in Standard Ethernet

- Each station on Ethernet has its own network interface card (NIC)
- The NIC fits inside the station and provides the station with a link-layer/physical address
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes

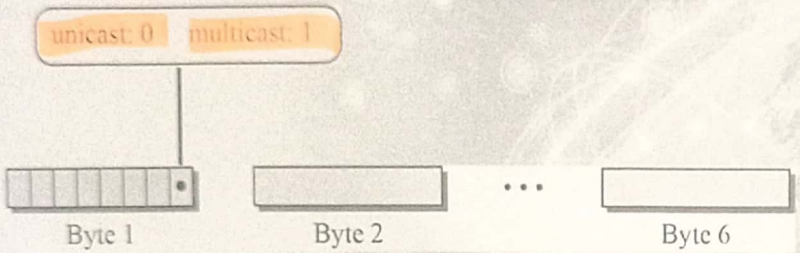
Transmission of Address Bits

How the address 47:20:1B:2E:08:EE is sent out online.

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

Hexadecimal	47	20	1B	2E	08	EE
Binarys	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast and Multicast Addresses



Example 13.2

Define the type of the following destination addresses:

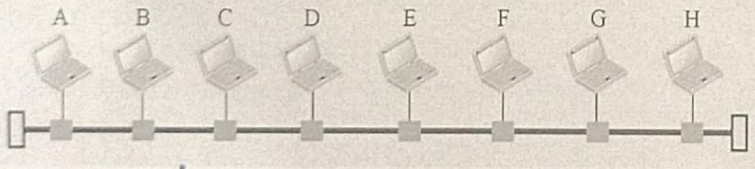
a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

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 Fs, the address is broadcast. Therefore, we have the following:

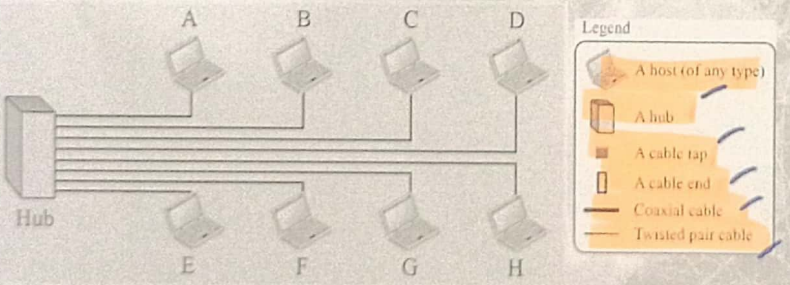
a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are Fs in hexadecimal.

Must very Imp Example

Implementation of Standard Ethernet



a. A LAN with a bus topology using a coaxial cable

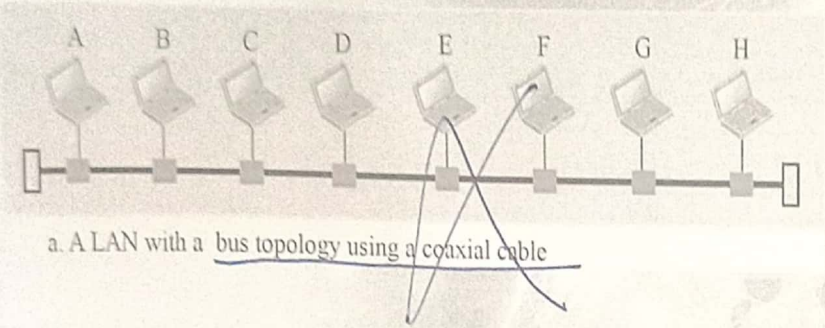


b. A LAN with a star topology using a hub

Access Method in Standard Ethernet

- Since the network that uses the standard Ethernet protocol is a broadcast network, we need to use an access method to control access to the sharing medium
- The standard Ethernet chose CSMA/CD with 1-Persistent Method

Access Method in Standard Ethernet



a. A LAN with a bus topology using a coaxial cable

Efficiency of Standard Ethernet

- The ratio of the time used by a station to send data to the time the medium is occupied by this station
- The practical efficiency of standard Ethernet has been measured to be:

Efficiency = 1/(1+ 6.4 x a)

where a = number of frames that can fit on a medium

Example

In the Standard Ethernet with the transmission rate of 10 Mbps, we assume that the length of the medium is 2500 m and the size of the frame is 512 bits. The propagation speed of a signal in a cable is normally 2×10^8 m/s.

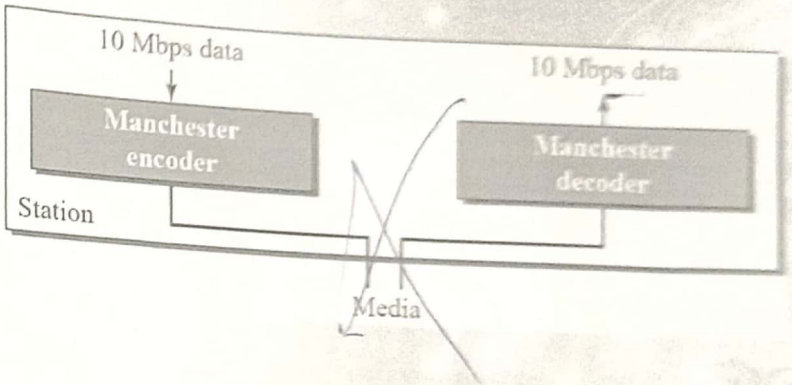
Implementation of Standard Ethernet

- The Standard Ethernet defined several implementations, but only four of them became popular during the 1980s

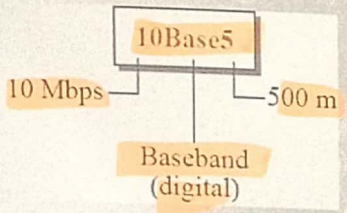
Summary of Standard Ethernet implementations

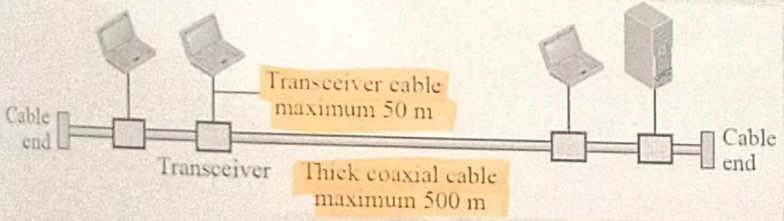
Implementation	Medium	Medium Length	Encoding
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000	Manchester

Encoding in Standard Ethernet

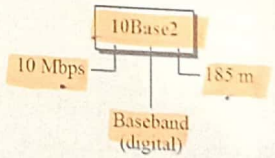


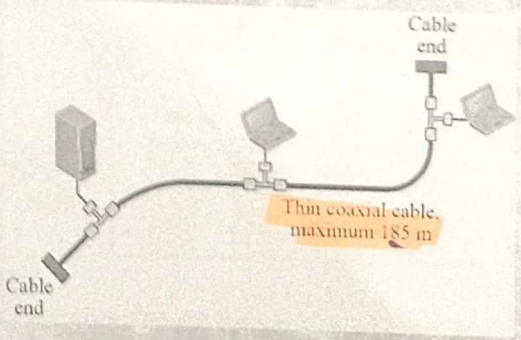
10Base5 implementation



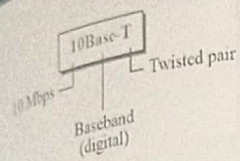


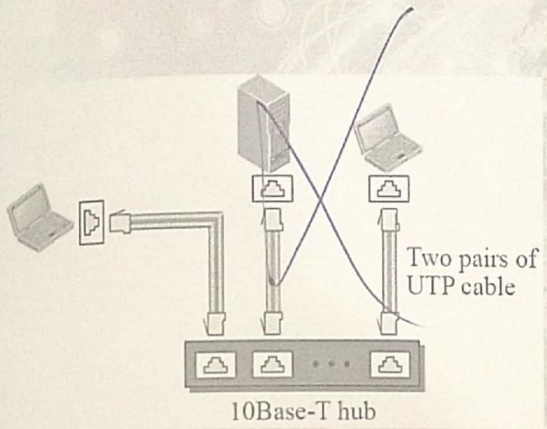
10Base2 implementation





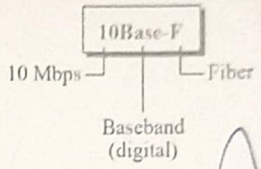
10Base-T implementation

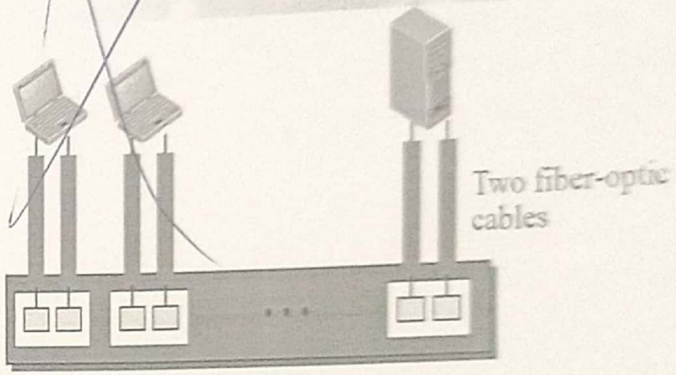




10Base-T hub

10Base-F implementation





10Base-F hub

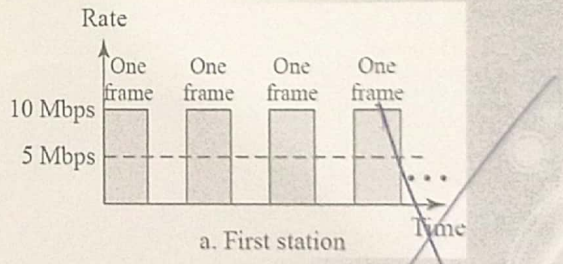
Changes in the Standard

- The changes that occurred to the 10-Mbps Standard Ethernet opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs

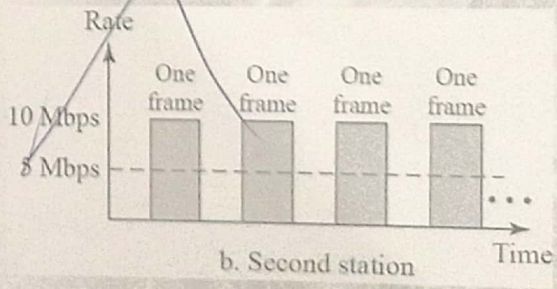
  ✓ Bridged Ethernet
  ✓ Switched Ethernet
  ✓ Full-Duplex Ethernet

✓ Bridged Ethernet
✓ Switched Ether

Bridged Ethernet- Sharing Bandwidth

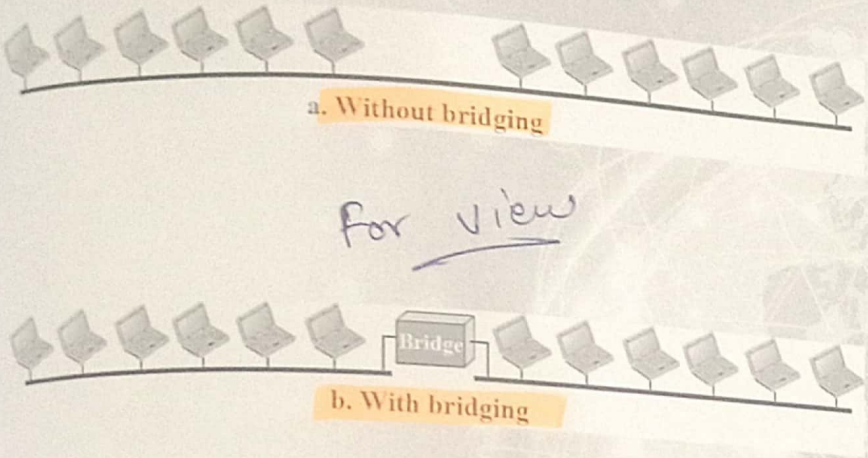


a. First station



b. Second station

A Network with and without Bridging

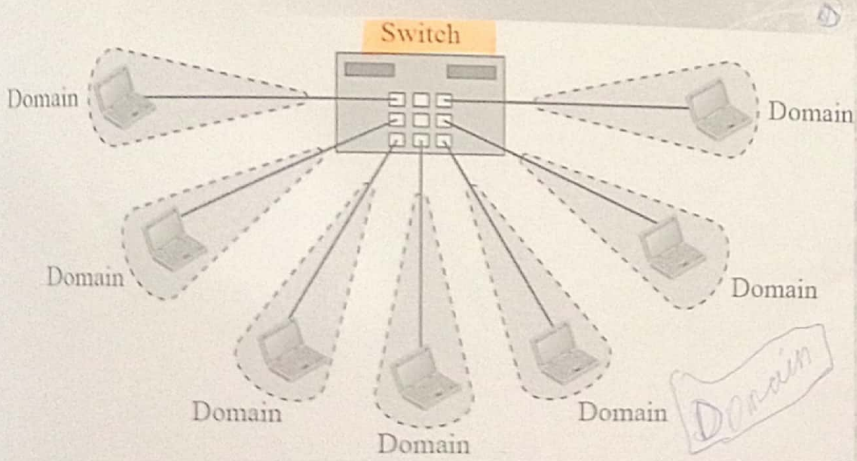


Changes in the Standard

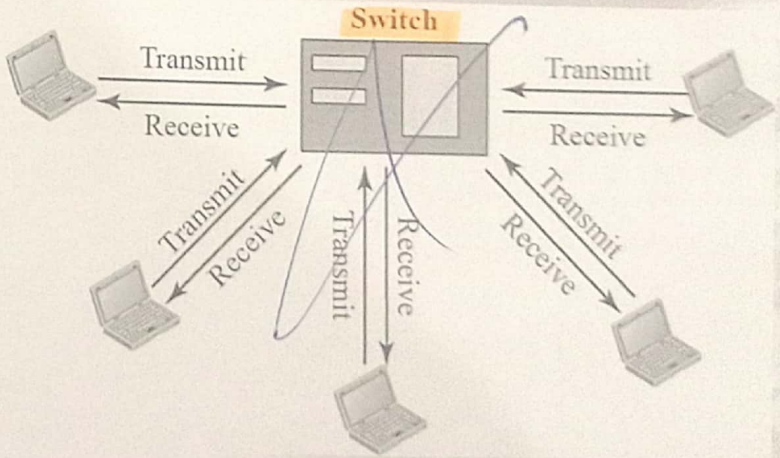
- The changes that occurred to the 10-Mbps Standard Ethernet opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs

  - ✓ Bridged Ethernet
  - ✓ Switched Ethernet
  - ✓ Full-Duplex Ethernet

Switched Ethernet



Full – Duplex Switched Ethernet



Fast Ethernet

- In the 1990s, Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet
- To make it compatible with the Standard Ethernet, the MAC sublayer was left unchanged

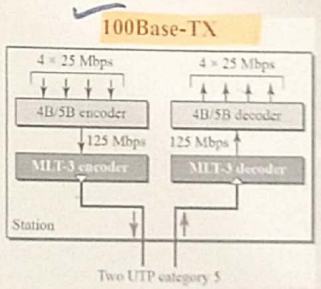
Physical Layer

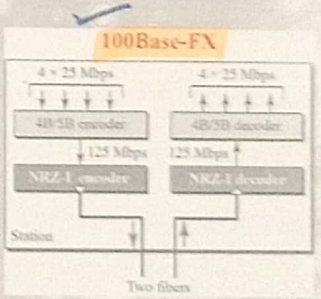
- To be able to handle a 100 Mbps data rate, several changes need to be made at the physical layer

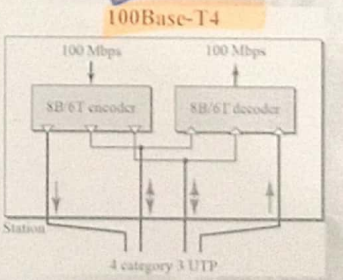
Fast Ethernet

- But the features of the Standard Ethernet that depend on the transmission rate, had to be changed
- Goals of Fast Ethernet:
  - ✓ Upgrade data rate to 100Mbps
  - ✓ Make it compatible with Standard Ethernet
  - ✓ Keep same 48-bit address
  - ✓ Keep same frame format

Encoding for Fast Ethernet







For View

Implementation of Fast Ethernet implementations

Implementation	Medium	Medium Length	Wires	Encoding
100Base-TX	STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

100Base-TX | STP | 100m | 2 | 4B5B+MLT-3

100Base-FX | Fiber | 185m | 2 | 4B5B+NRZ-I

100Base-T4 | UTP | 100m | 4 | Two 8B/6T

Gigabit Ethernet

- Need for an even higher data rate resulted in the design of IEEE Standard 802.3z Gigabit Ethernet Protocol (1000 Mbps)

Gigabit Ethernet

- The goals of the Gigabit Ethernet were:
  - ✓ Upgrade the data rate to 1 Gbps
  - ✓ Make it compatible with standard or Fast Ethernet
  - ✓ Use same 48 bit address
  - ✓ Use the same frame format
  - ✓ Keep same minimum and maximum frame lengths

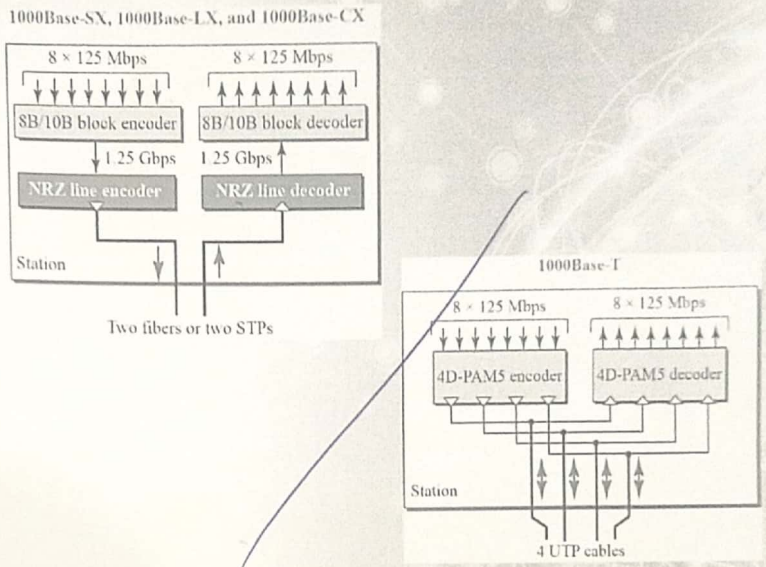
MAC Sub-layer

- A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched
- To achieve a data rate of 1 Gbps, this was no longer possible
- Gigabit Ethernet has two distinctive approaches for medium access:
  - ✓ Half-duplex
  - ✓ Full-duplex

Physical Layer

- The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet
- We briefly discuss some features of this layer:

Encoding in Gigabit Ethernet



Summary of Gigabit Ethernet Implementations

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

10-gigabit Ehternet

- The idea is to extend the technology, the data rate, and the coverage distance so that the Ethernet can be used in LANs and MANs (metropolitan area network)
- The IEEE committee created 10 Gigabit Ethernet and called it Standard 802.3ae

Implementation

- 10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention; CSMA/CD is not used in 10 Gigabit Ethernet
- Four implementations are most common:

Implementation

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

Other Wired Networks

CHP # 14

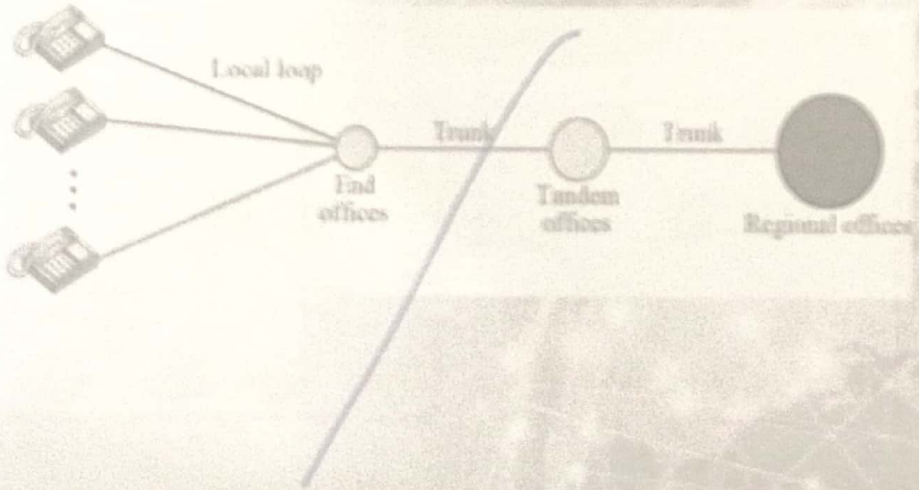
- Access Networks
  - ✓ Networks that connect a small LAN to an ISP
- Wide Area Networks
  - ✓ Wired networks used to transfer data over long distances

Telephone Network

- The telephone network had its beginnings in the late 1800s
- Plain Old Telephone System (POTS) was originally an analog system using analog signals to transmit voice
- With the advent of the computer era, the network, in the 1980s, began to carry data in addition to voice

- During the last decade, the telephone network has undergone many technical changes and the network is now Digital as well as Analog

A Telephone System



- The telephone network is made of three major components:
  - ✓ Local Loops
  - ✓ Trunks
  - ✓ Switching offices

- The telephone network has several levels of switching offices:
  - ✓ End offices
  - ✓ Tandem offices
  - ✓ Regional offices

Local-Access Transport Areas (LATAs)

- A LATA can be a small or large metropolitan area

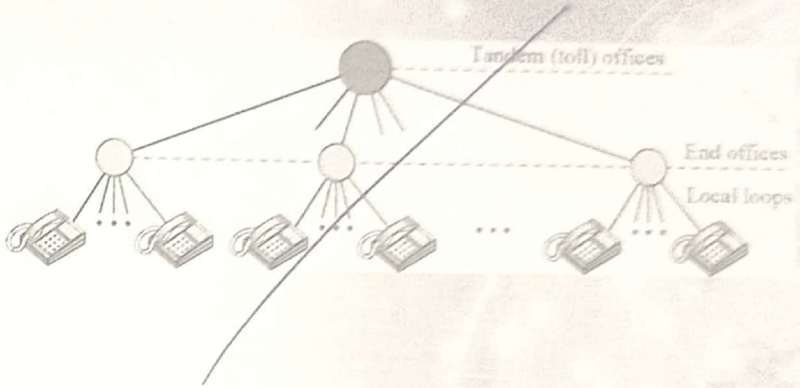
- A small state may have a single LATA; a large state may have several LATAs

- A LATA boundary may overlap with state boundary; part of a LATA can be in one state, part in another state

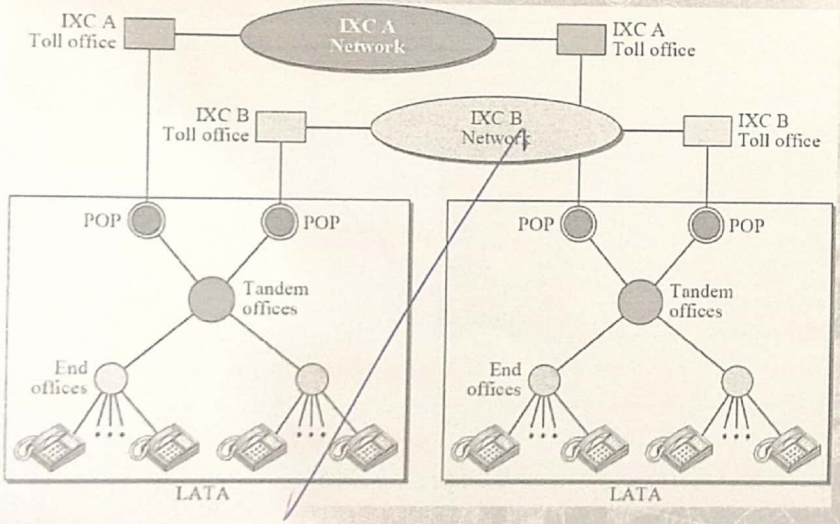
Intra-LATA and Inter-LATA Services

- Services offered by Telephone companies inside a LATA are called Intra-LATA services and between LATAs are called Inter-LATA services
- Carrier that handles Intra-LATA are called a Local Exchange Carrier (LEC) and the ones that handle Inter-LATA are called Interexchange Carriers (IXCs)

Switching Offices in a LATA



Points of Presence (POPs)



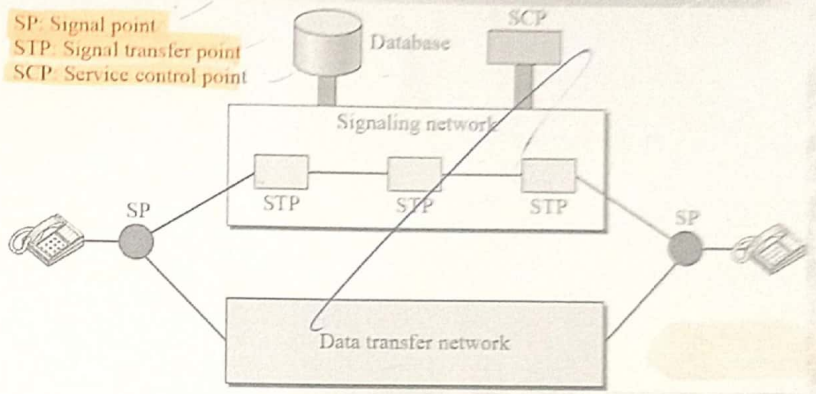
Signaling

- The telephone network in the beginning, used a circuit-switched network with dedicated links to transfer voice communication
- The operator connected the two parties by using a wire with two plugs inserted into the corresponding two jacks
- Later, the signaling system became automatic

Signaling

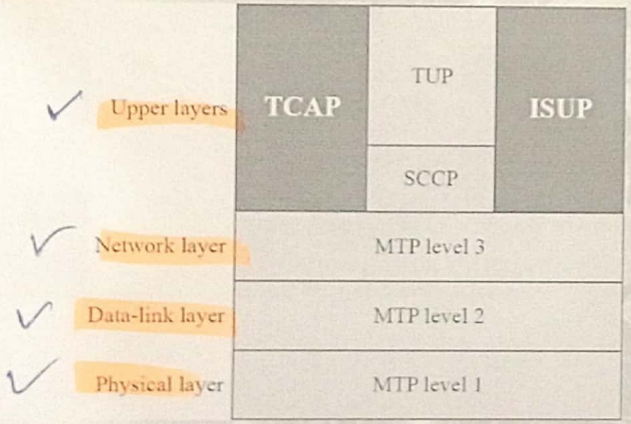
- Rotary telephones were invented that sent a digital signal defining each digit in a multi-digit telephone number
- As telephone networks evolved into a complex network, the functionality of the signaling system increased

Data Transfer and Signaling Network



Layers in SS7

MTP: Message transfer part
SCCP: Signaling connection control point
TCAP: Transaction capabilities application port
TUP: Telephone user port
ISUP: ISDN user port



Services

- Telephone companies provide two types of services:
  - ✓ Analog Services
    - ➢ Analog Switched Services
    - ➢ Analog Leased Services
  - ✓ Digital Services
    - ➢ Switched /56 Service
    - ➢ Digital Data Service

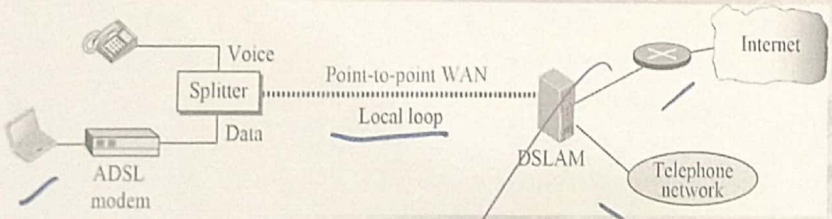
Digital Subscriber Line (DSL)

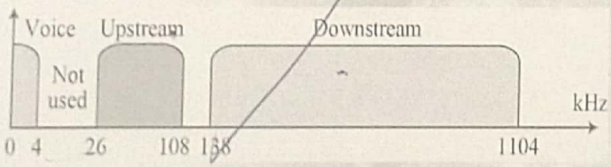
- After traditional dial-up modems reached their peak data rate, telephone companies developed another technology, DSL, to provide higher-speed access to the Internet
- DSL supports high-speed digital communication over the existing telephone

Digital Subscriber Line (DSL)

- DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL)

ADSL Point-to-Point Network





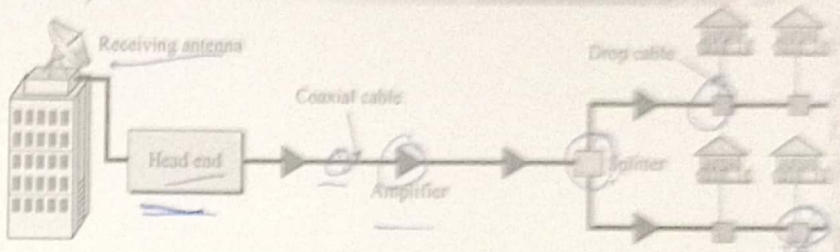
Cable Network

- The Cable TV networks were initially created to provide remote subscribers access to TV programs
- Cable networks enabled access to remote broadcasting stations via microwave connections
- Cable TV also found a good ISP market by using some of the channels originally designed for video

Traditional Cable Networks

- Cable TV started to distribute broadcast video signals to locations with poor or no reception in the late 1940s
- It was called community antenna television (CATV) because an antenna at the top of a tall hill or building received the signals from the TV stations

Traditional Cable TV Network

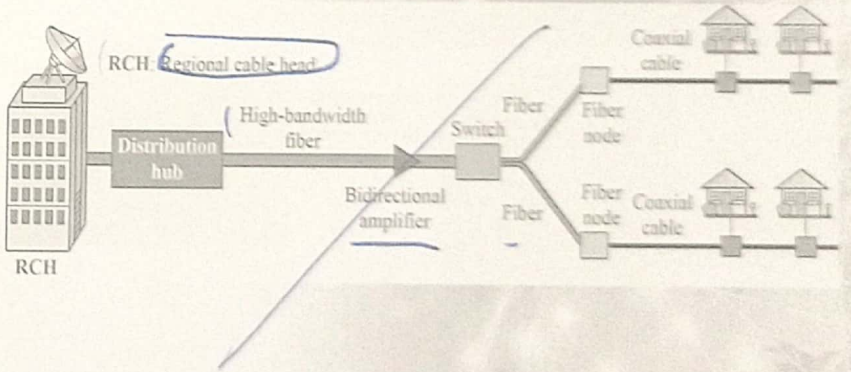


For view

Hybrid Fiber Coaxial (HFC) Network

- Second generation of cable network is called a Hybrid Fiber-Coaxial (HFC) network
- The network uses a combination of fiber-optic and coaxial cable

Hybrid Fiber-Coaxial (HFC) Network



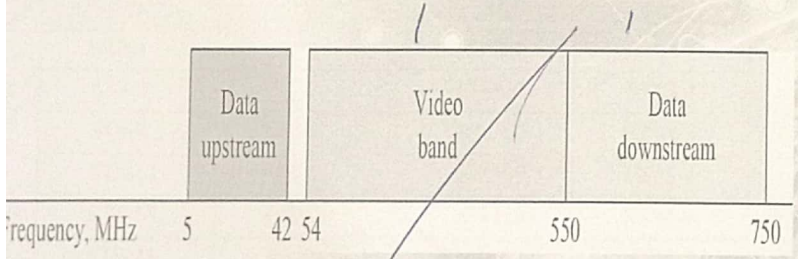
Cable TV for Data Transfer

- Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer
- DSL technology provides high-data-rate connections for residential subscribers over the local loop BUT UTP is susceptible to Interfence

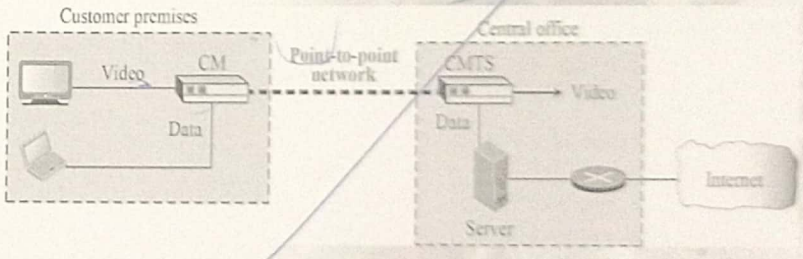
Cable TV for Data Transfer

- This imposes an upper limit on the data rate. A solution is the use of the cable TV network

Division of Coaxial Cable Band by CATV



Cable Modem Transmission System (CMTS)



Synchronous Optical Network (SONET)

- A wide area network (WAN) that is used as a transport network to carry loads from other WANs
- ITU–T standard called Synchronous Digital Hierarchy (SDH)
- Architecture of a SONET system consists of signals, devices, and connections

SDH
Synchronous
Digital Hierarchy.

SONET Architecture

- Signals
  - ✓ Synchronous Transport Signals (STS)
  - ✓ Optical Carriers (OCs)
  - ✓ Synchronous Transport Module (STM)
- SONET Devcies
  - ✓ STS Mux/Demux
  - ✓ Regenerators
  - ✓ Add-Drop Multiplexer and Terminals
- Connections
  - ✓ Section
  - ✓ Line
  - ✓ Path

SONET Signals

(Imp for M.C.A)

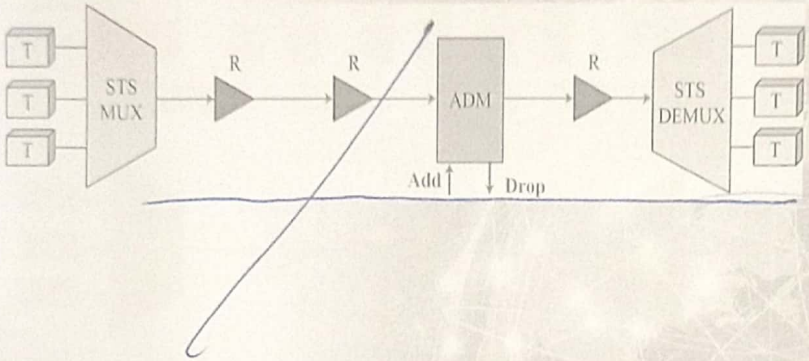
STS	*OC*	*Rate (Mbps)*	*STM*
STS-1	OC-1	51.840	
STS-3	OC-3	155.520	STM-1
STS-9	OC-9	466.560	STM-3
STS-12	OC-12	622.080	STM-4
STS-18	OC-18	933.120	STM-6
STS-24	OC-24	1244.160	STM-8
STS-36	OC-36	1866.230	STM-12
STS-48	OC-48	2488.320	STM-16
STS-96	OC-96	4976.640	STM-32
STS-192	OC-192	9953.280	STM-64

SONET Architecture

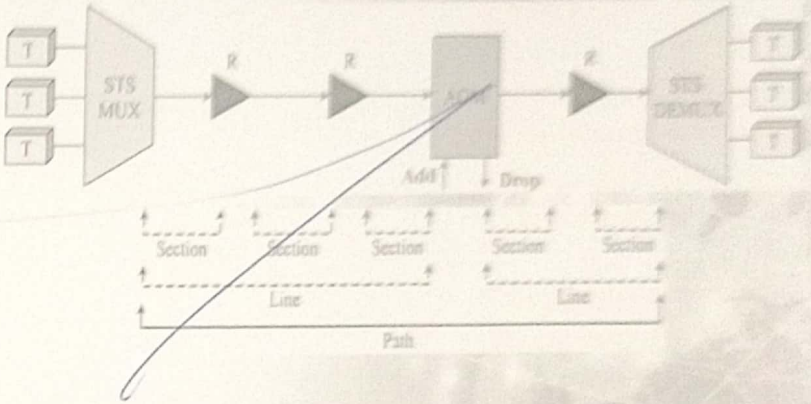
- Signals
  - ✓ Synchronous Transport Signals (STS)
  - ✓ Optical Carriers (OCs)
  - ✓ Synchronous Transport Module (STM)
- SONET Devcies
  - ✓ STS Mux/Demux
  - ✓ Regenerators
  - ✓ Add-Drop Multiplexer and Terminals
- Connections
  - ✓ Section
  - ✓ Line
  - ✓ Path

SONET Devices

ADM: Add/drop multiplexer
STS MUX: Synchronous transport signal multiplexer
STS DEMUX: Synchronous transport signal demultiplexer
R: Regenerator
T: Terminal



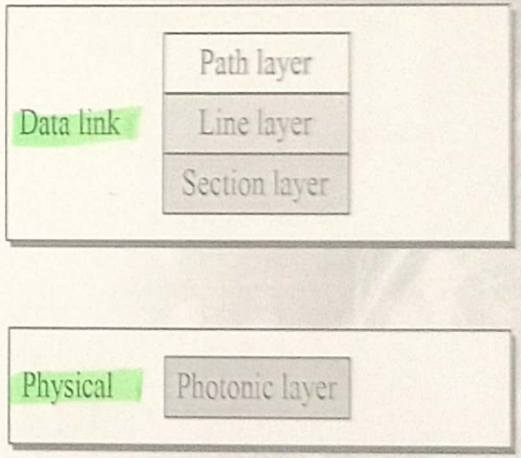
SONET Connections



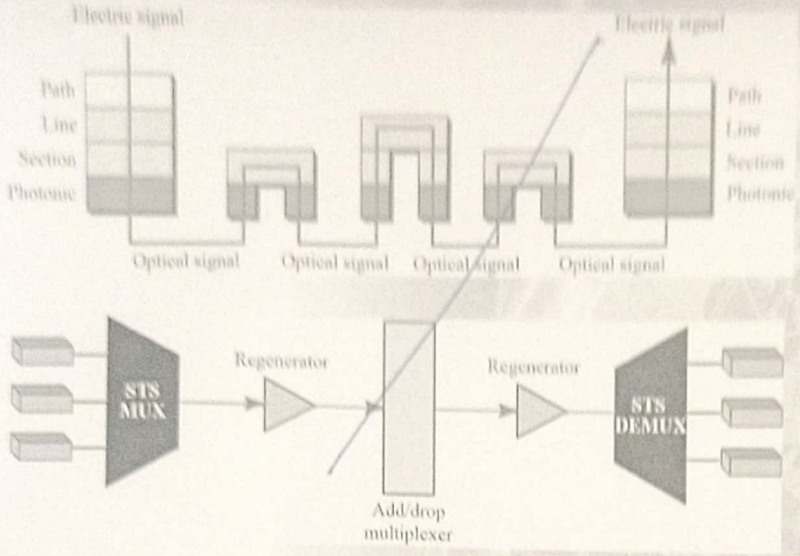
SONET Layers

- The SONET standard includes four functional layers:
  - ✓ The Path Layer
  - ✓ The Line Layer
  - ✓ The Section Layer
  - ✓ The Photonic Layer
- The layers correspond to both the physical and the data-link layers

SONET Layers



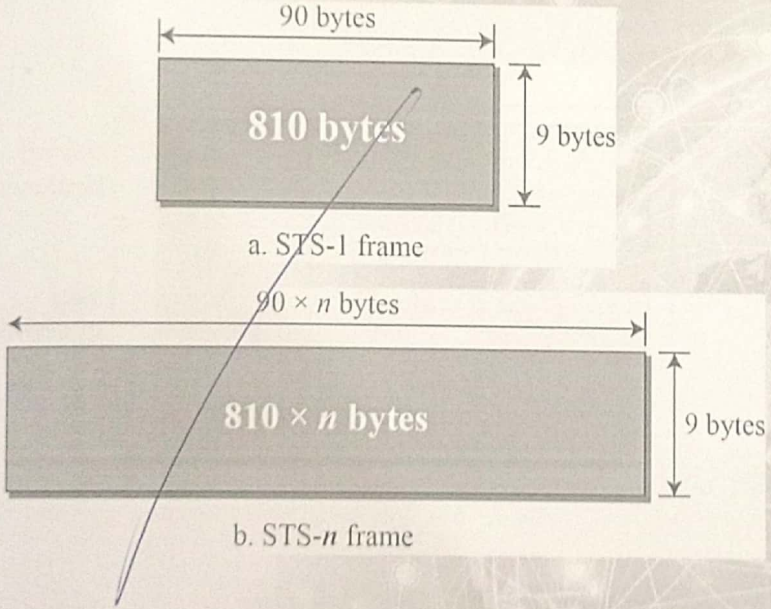
Device-Layer Relationship in SONET



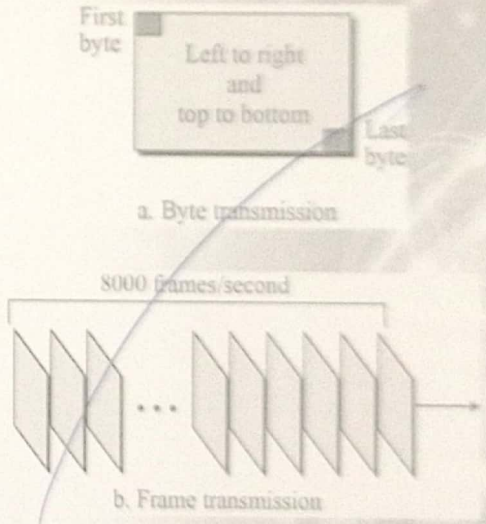
SONET Frames

- Each synchronous transport signal STS-n is composed of 8000 frames
- Each frame is a two-dimensional matrix of bytes with 9 rows by 90×n columns
- STS-1 frame is 9 rows by 90 columns (810 bytes), and an STS-3 is 9 rows by 270 columns (2430 bytes)

An STS-1 and an STS-n Frame



STS-1 Frames in Transition



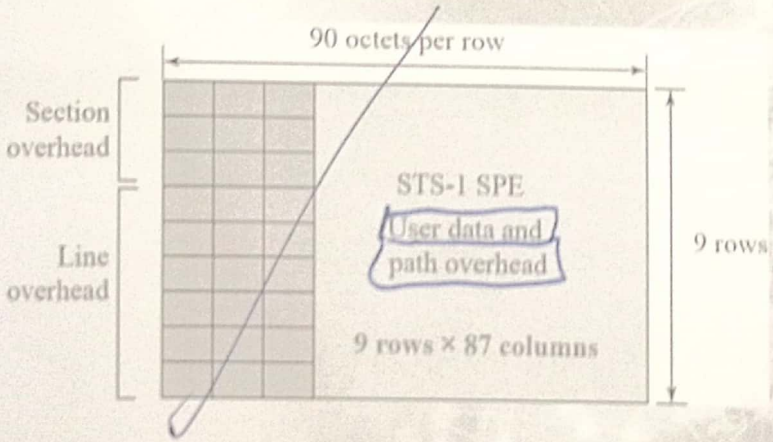
Example

Find the data rate of an STS-1 signal

Example

Find the data rate of an STS-3 signal

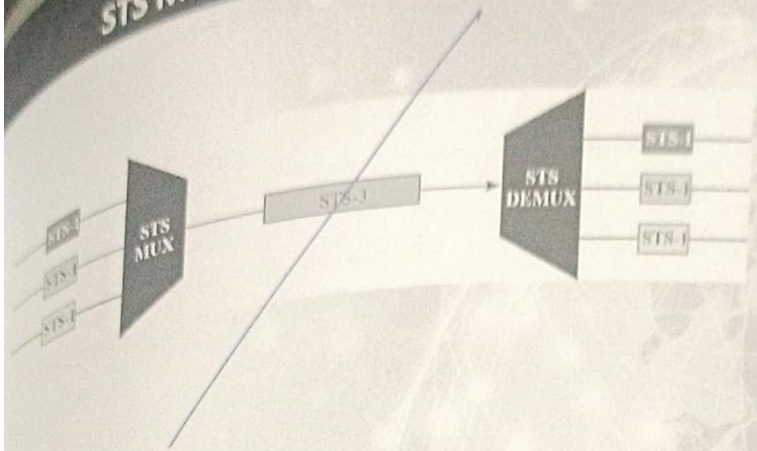
STS-1 Frame Format



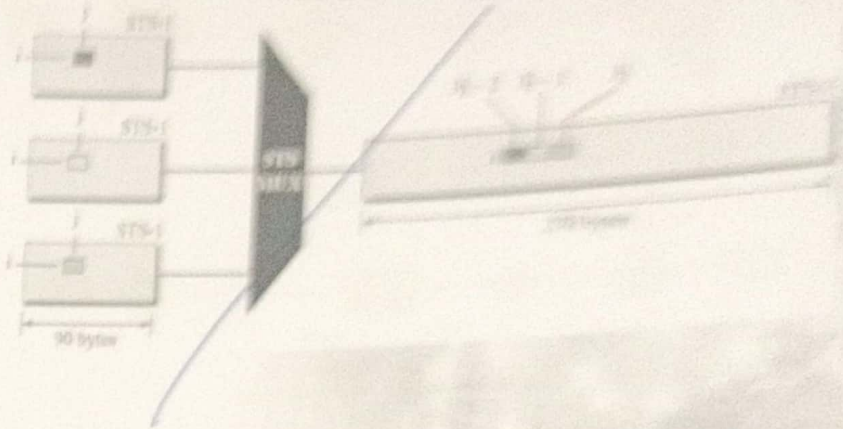
STS Multiplexing

- In SONET, frames of lower rate can be synchronously time-division multiplexed into a higher-rate frame.
- For example, three STS-1 signals (channels) can be combined into one STS-3 signal (channel), four STS-3s can be multiplexed into one STS-12, and so on.

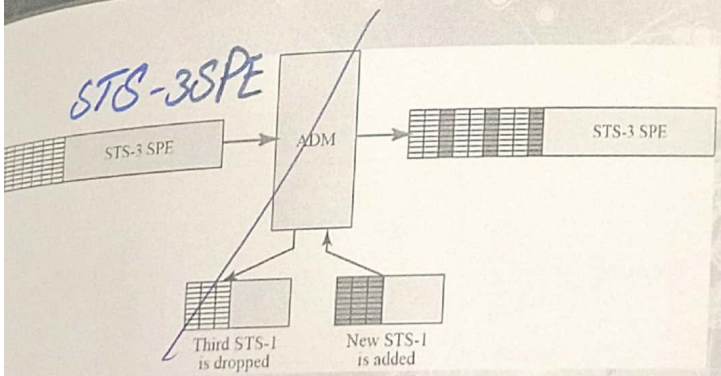
STS Multiplexing/Demultiplexing



Byte Interleaving



Add/Drop Multiplexer



SONET Networks

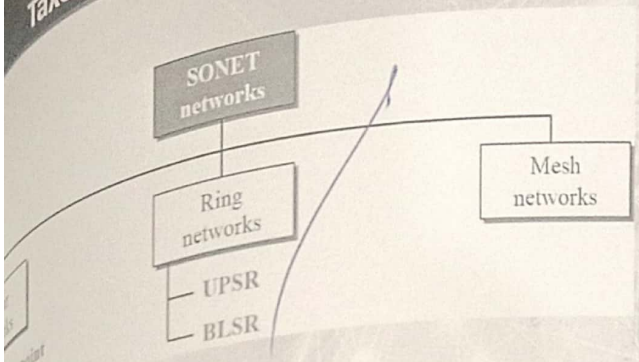
- SONET network can be used as a high-speed backbone carrying loads from other networks such as ATM or IP

(i) Point-to-Point
(ii) multipoint

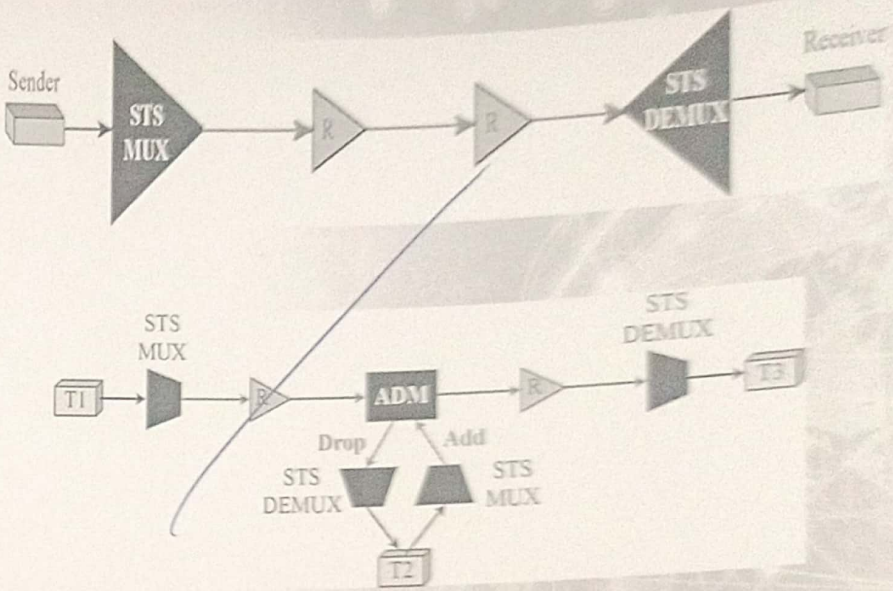
- We can roughly divide SONET networks into three categories:
  - ✓ Linear Networks
  - ✓ Ring Networks
  - ✓ Mesh networks

(1) UPSR
(2) BCLR

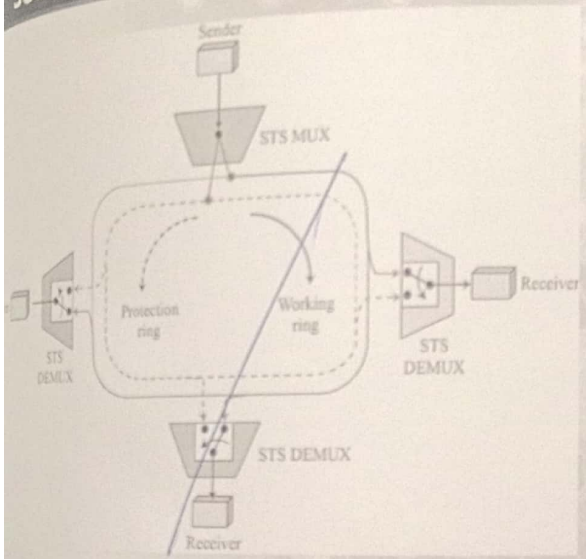
Taxonomy of SONET Networks



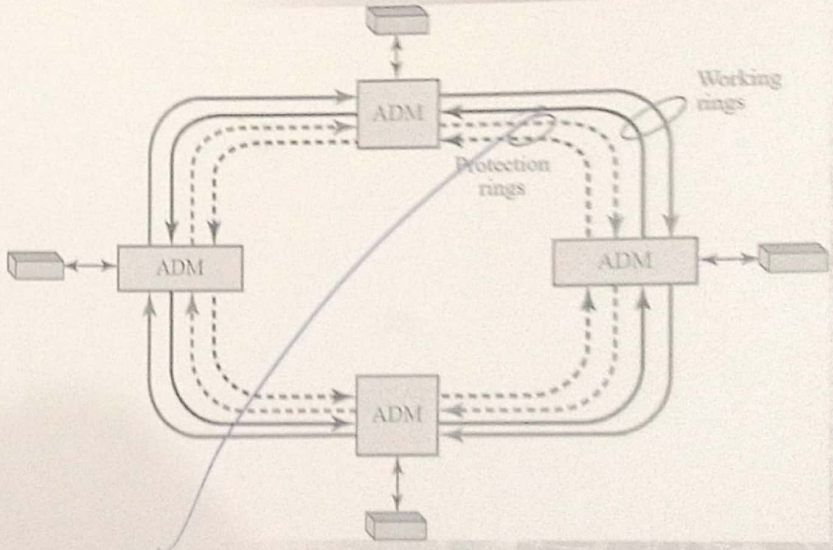
SONET Networks – Linear Networks



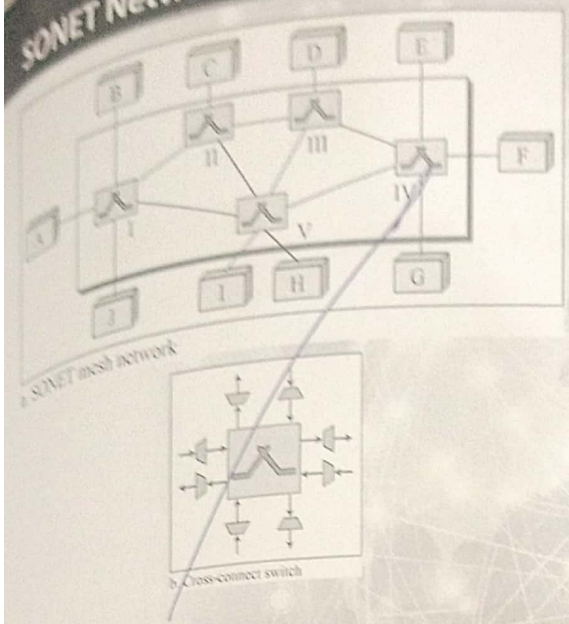
SONET Networks – Ring Networks



SONET Networks – Ring Networks



SONET Networks – Mesh Networks



a. SONET mesh network

b. Cross-connect switch

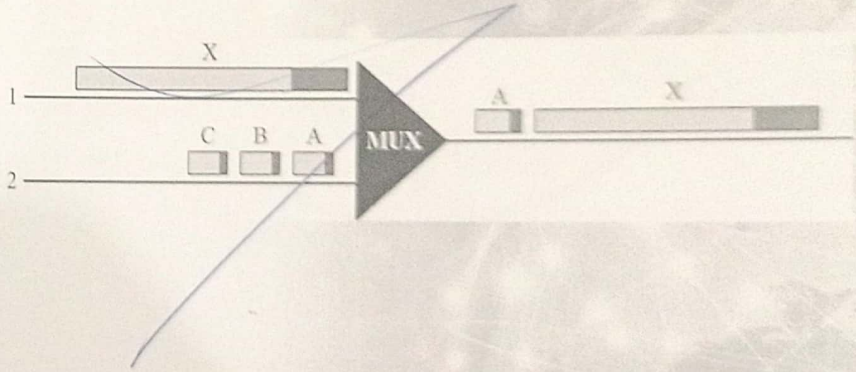
ATM

- Asynchronous Transfer Mode (ATM) is a switched wide area network based on the cell relay protocol designed by the ATM forum
- The combination of ATM and SONET will allow high-speed interconnection of networks

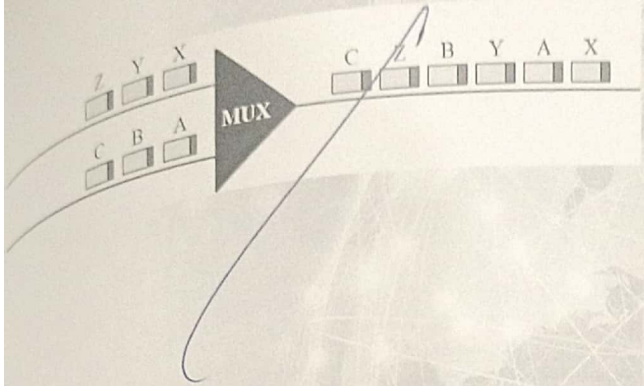
Problems

- Some of the problems associated with existing systems are:
  - ✓ Frame Networks
  - ✓ Mixed Network Traffic
- Solution
  - ✓ Cell Networks
  - ✓ Asynchronous TDM

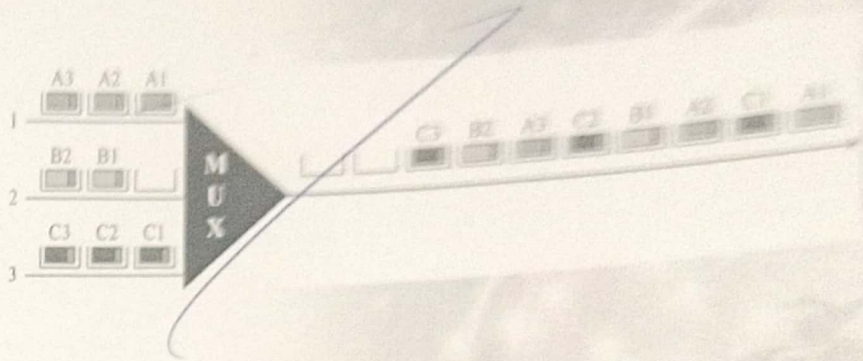
Multiplexing using Different Frame Size



Multiplexing using Cells



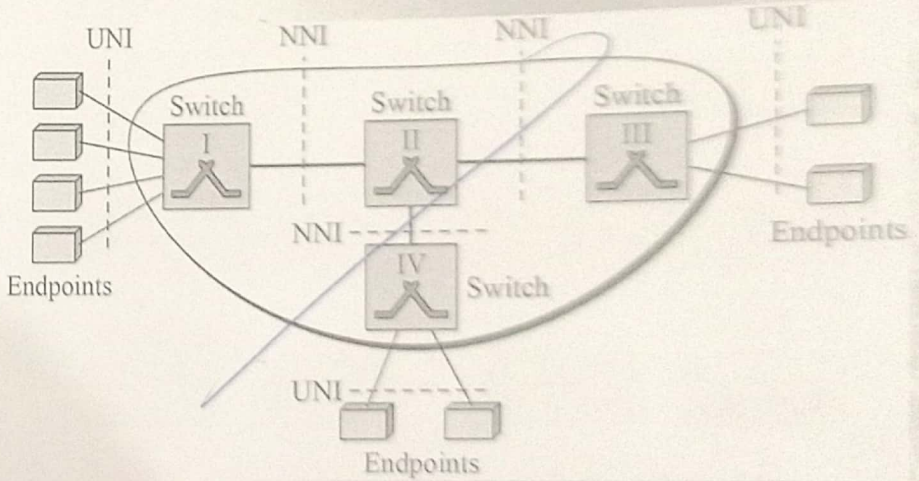
ATM Multiplexing



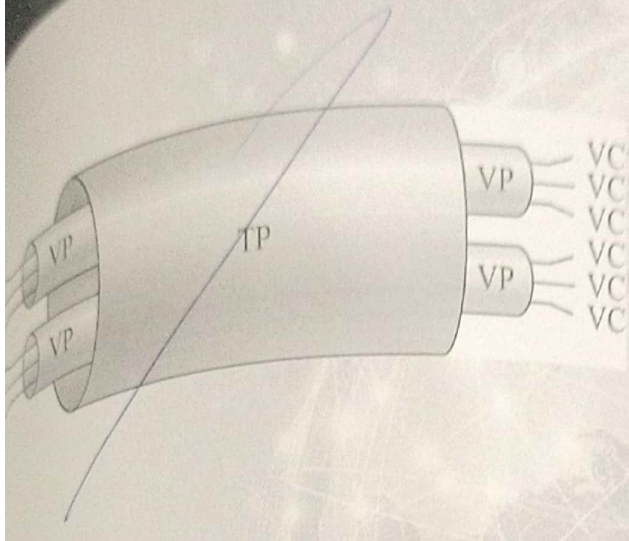
Architecture

- ATM is a cell-switched network
- The user access devices, called the endpoints, are connected through a user-to-network interface (UNI) to the switches inside the network
- The switches are connected through network-to-network interfaces (NNIs)

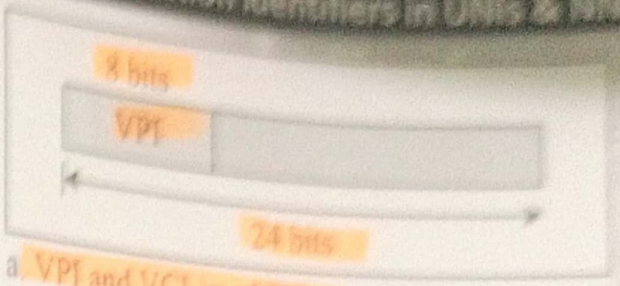
Architecture of an ATM Network



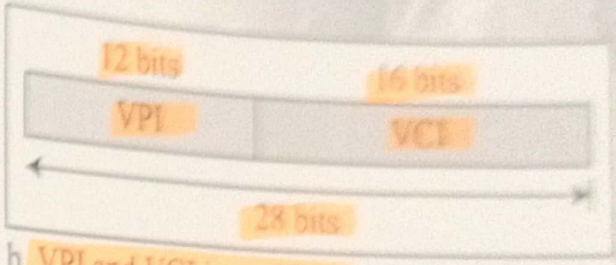
TP, VP, VC



Virtual connection identifiers in UNIs & NNIs

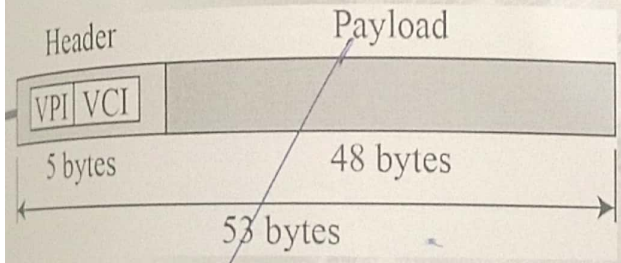


a. VPI and VCI in a UNI

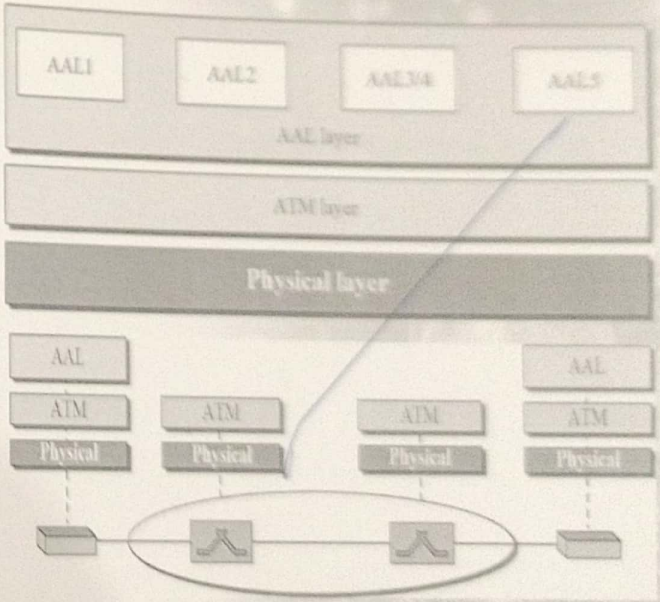


b. VPI and VCI in an NNI

An ATM Cell



ATM Layers



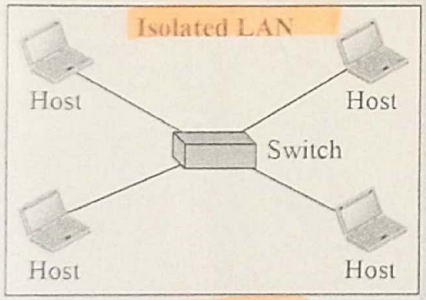
CPP#15

- Wireless communication is one of the fastest-growing technologies
- The demand for connecting devices without the use of cables is increasing everywhere
- Wireless LANs can be found on college campuses, in office buildings, and in many public areas

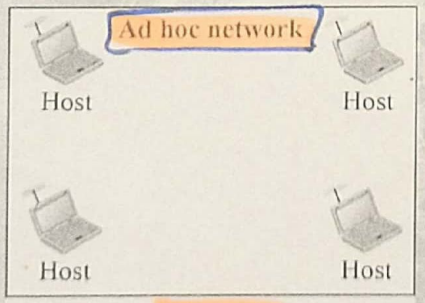
Ameen

- Architecture comparison of wired and wireless LANs
  - ✓ Medium
  - ✓ Hosts
  - ✓ Isolated LANs
  - ✓ Connection to other Networks
  - ✓ Moving between Environments

Isolated LANs: Wired versus Wireless

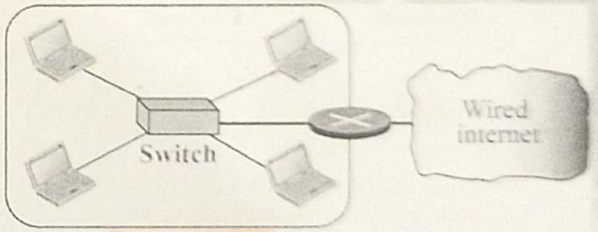


Wired

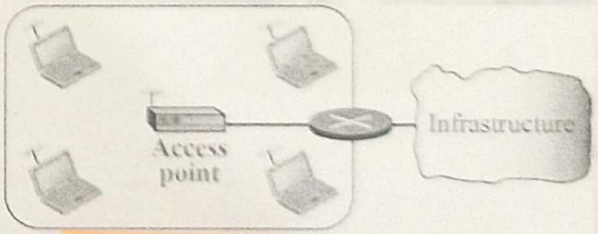


Wireless

Connection of a Wired/Wireless LAN to other networks



Wired LAN



Infrastructure network

Characteristics of a Wireless LAN

- Several characteristics of wireless LANs either do not apply to wired LANs or the existence of these is negligible and can be ignored

MCQs

- ✓ Attenuation
- ✓ Interference
- ✓ Multipath Propagation
- ✓ Error

Access Control

- Most important issue in a wireless LAN is how a wireless host can get access to the shared medium (air)

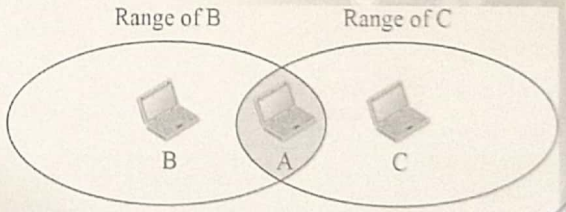
S.Q)

- CSMA/CD does not work in wireless LANs for three reasons:
  1. Wireless hosts don't have power to send and receive at the same time

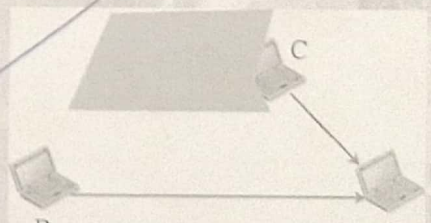
Access Control

2. The hidden station problem prevents collision detection
3. The distance between stations can be large

Hidden Station Problem



a. Stations B and C are not in each other's range.



b. Stations B and C are hidden from each other.

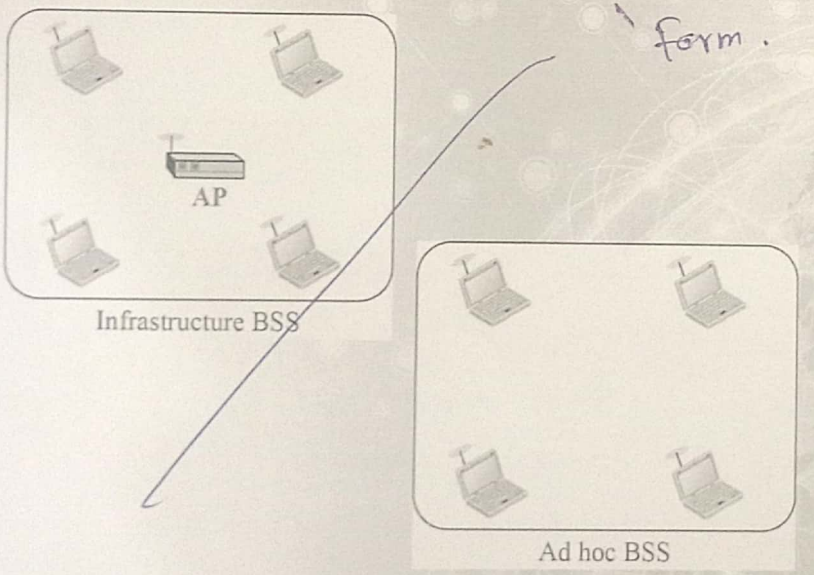
IEEE 802.11 PROJECT

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers
- It is sometimes called Wireless Ethernet
- The term WiFi (short for wireless fidelity) as a synonym for wireless LAN (certified by WiFi alliance)

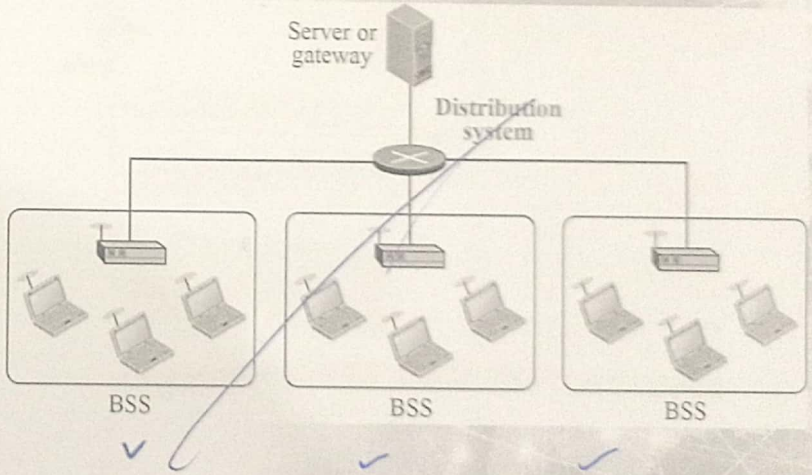
Architecture

- The standard defines two kinds of services:
  - ✓ The basic service set (BSS); and
  - ✓ The Extended service set (ESS)

Basic Service Sets (BSSs)



Extended Service Set (ESS)



Types of Stations

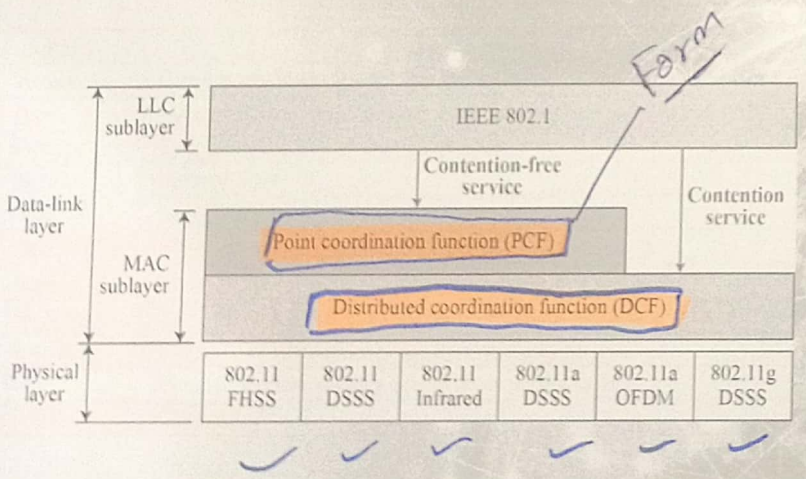
Three type of Stations.

- No-Transition Mobility
- BSS-Transition Mobility
- ESS-Transition Mobility

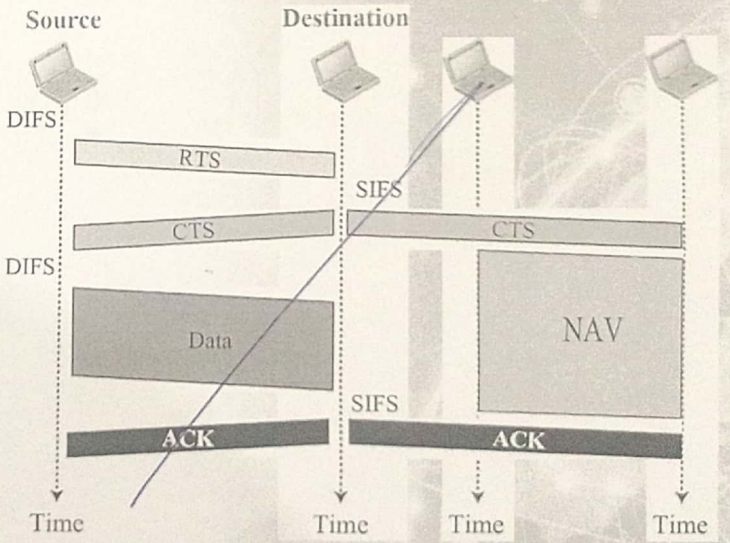
MAC Sub-layer

- IEEE 802.11 defines two MAC sub-layers:
  - ✓ The Distributed Coordination Function (DCF); and
  - ✓ The Point Coordination Function (PCF)

MAC Layers in IEEE 802.11 Standard



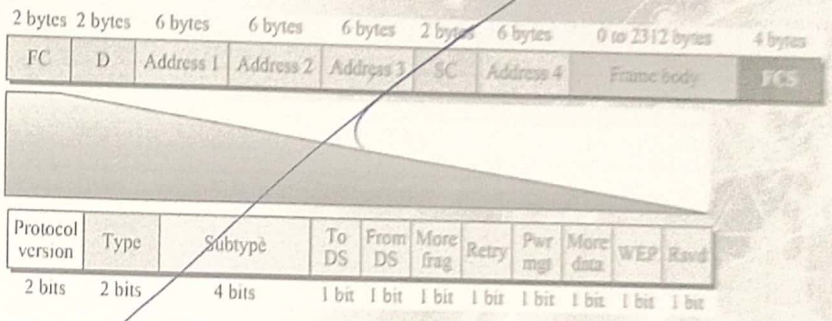
CSMA/CA and NAV



MAC Sub-layer

- IEEE 802.11 defines two MAC sub-layers:
  - ✓ The Distributed Coordination Function (DCF) ; and
  - ✓ The Point Coordination Function (PCF)

Frame Format



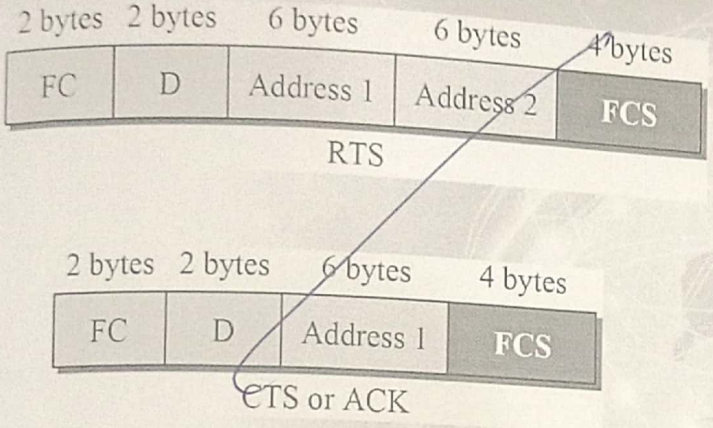
Subfields in FC field

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 6.2)
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

- ✓ Management Frames
- ✓ Control Frames
- ✓ Data Frames

Control Frames



Values of Subfields in Control Frames

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

Physical Layer

- All physical implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines 3 unlicensed bands in 3 ranges:
  - 902–928 MHz
  - 2.400–4.835 GHz
  - 5.725–5.850 GHz

Specifications

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

BLUETOOTH

Bluetooth defines
Piconet
Scatternet

- Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other

Bluetooth uses several layers.

- A Bluetooth LAN is an ad hoc network
- The devices, sometimes called gadgets, find each other and make a network called a Piconet

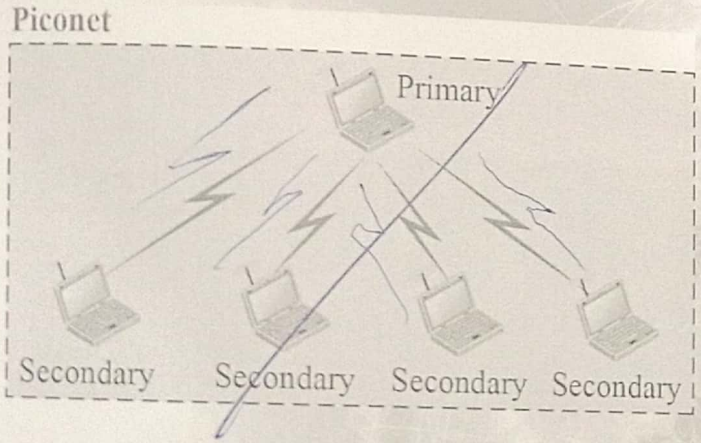
Architecture

Bluetooth device has built-in short range radio transmitter.

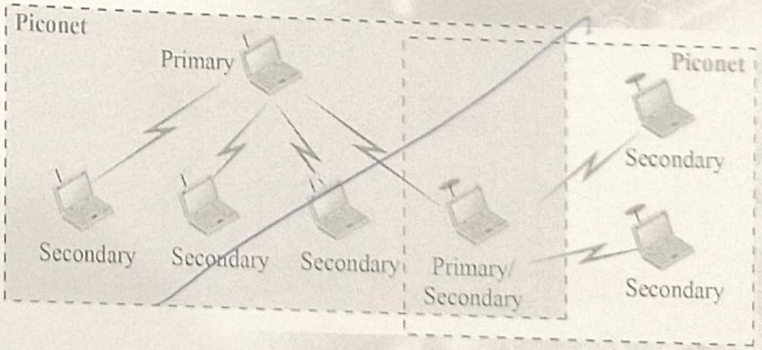
- Bluetooth defines two types of networks:
  - ✓ Piconet
  - ✓ Scatternet

✓ Piconet
✓ Scatternet

Piconet



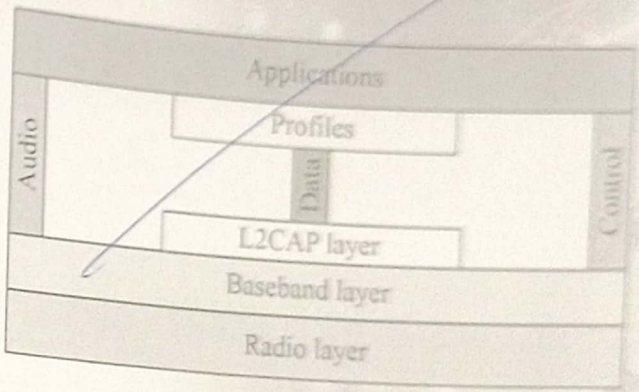
Scatternet



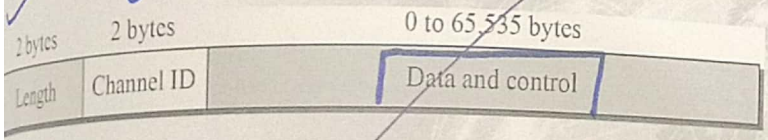
Bluetooth Layers

- Bluetooth uses several layers that do not exactly match those of the Internet model we have defined in this book

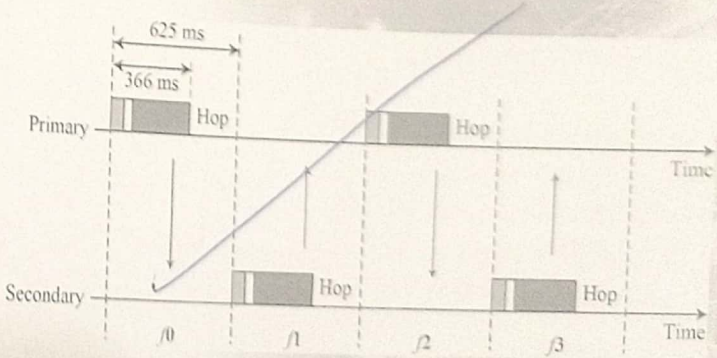
Bluetooth Layers



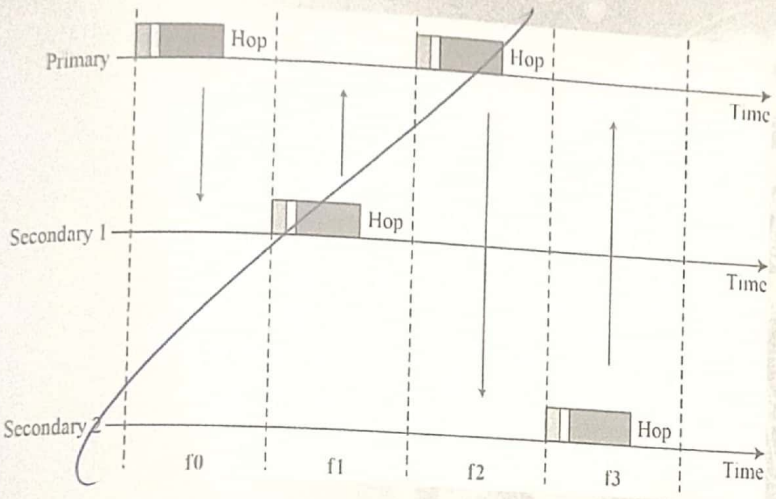
L2CAP Data Packet Format



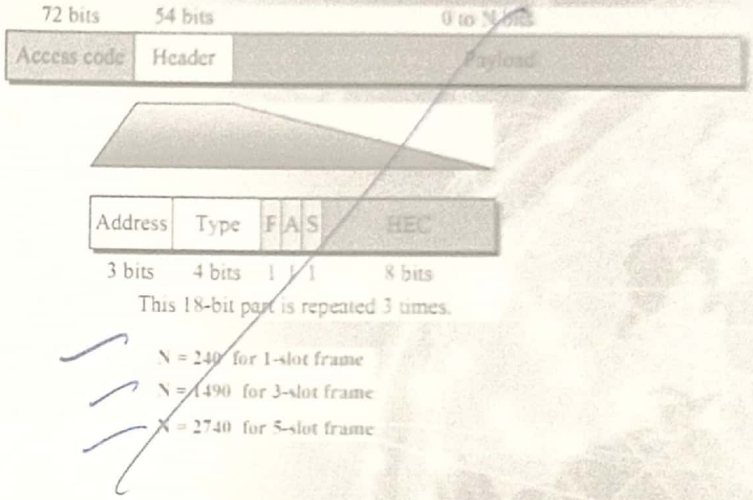
Single-Secondary Communication



Multiple-Secondary Communication



Frame Format Types



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

Bluetooth

- Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other
- A Bluetooth LAN is an ad hoc network
- The devices, sometimes called gadgets, find each other and make a network called a Piconet

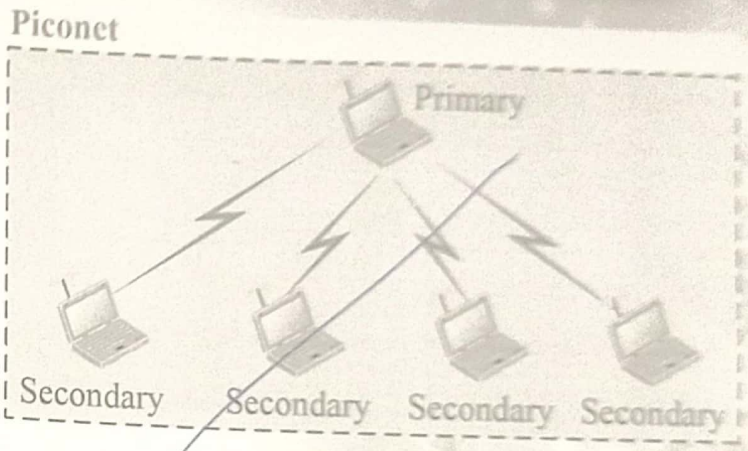
Bluetooth

- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard
- The standard defines a wireless Personal-Area Network (PAN) operable in an area the size of a room or a hall

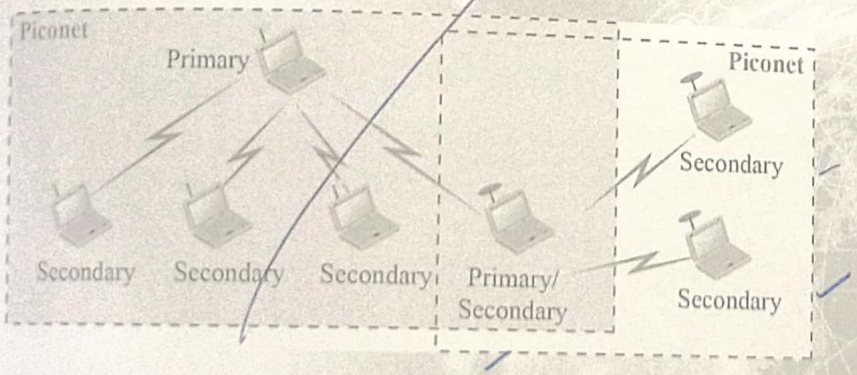
Architecture

- Bluetooth defines two types of networks:
  - Piconet
  - Scatternet

Piconet



Scatternet



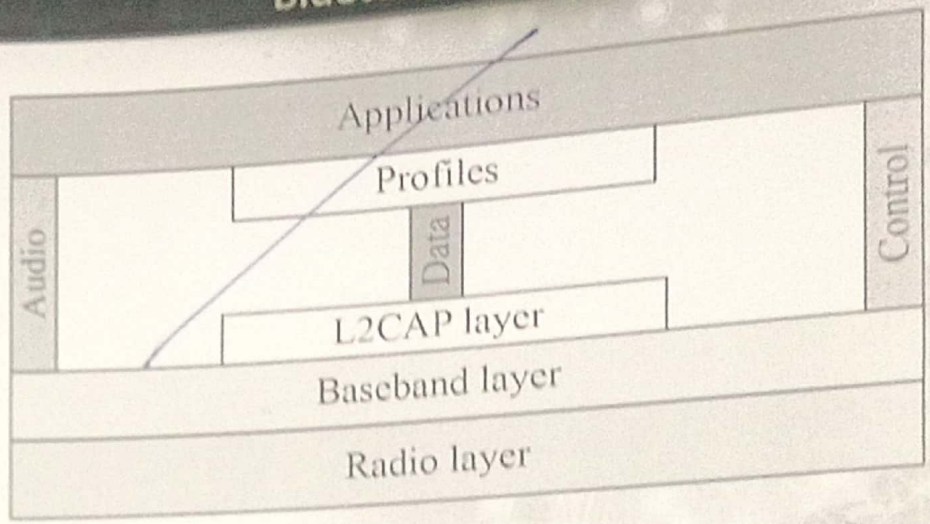
Bluetooth Devices

- A Bluetooth device has a built-in short-range radio transmitter
- The current data rate is 1 Mbps with a 2.4-GHz bandwidth
- This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs

Bluetooth Layers

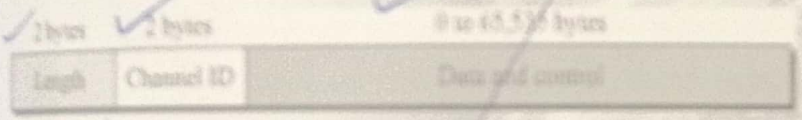
- Bluetooth uses several layers that do not exactly match those of the Internet model we have defined already

Bluetooth Layers

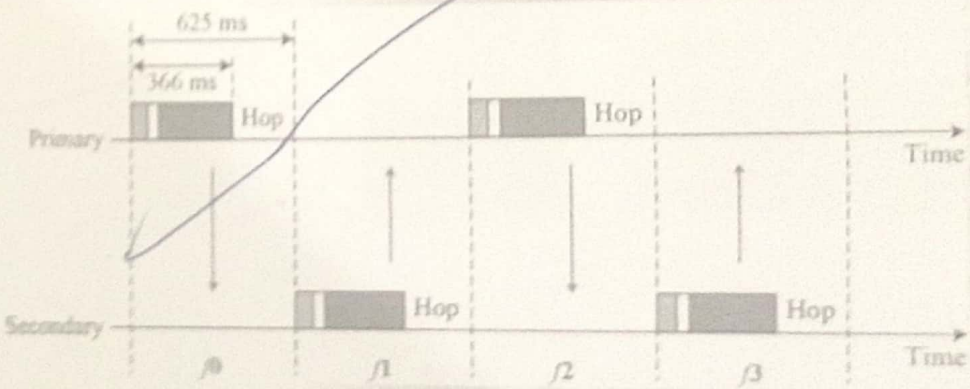


L2CAP Data Packet Format

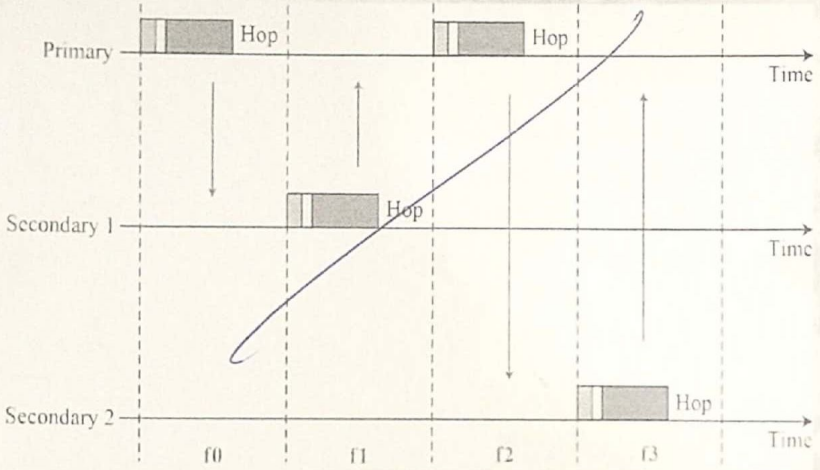
L2CAP Data Packet format



Single-Secondary Communication



Multiple-Secondary Communication



Connecting Devices

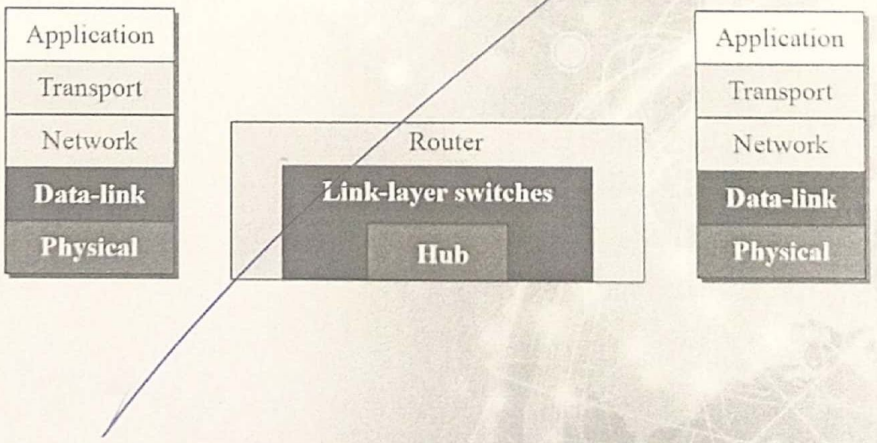
CHP #16

- Hosts and networks do not normally operate in isolation
- Connecting devices connect hosts together to make a network or connect networks together to make an internet
- Connecting devices can operate in different layers of the Internet model

Connecting Devices

- Three kinds of connecting devices:
  - ✓ Hubs
  - ✓ Link-layer switches
  - ✓ Routers

Three Categories of Connecting Devices



Hubs

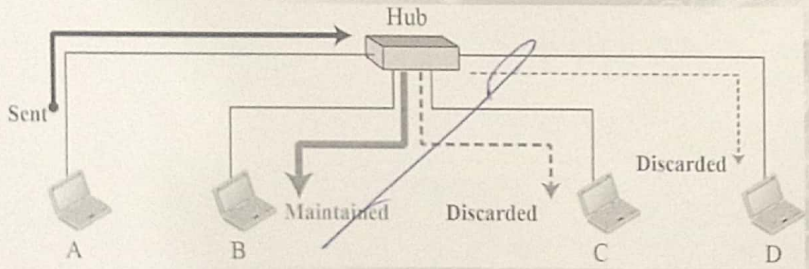
- Hub is a device that operates only in the physical layer
- Signals that carry information within a network can travel a fixed distance before attenuation impacts the data
- A hub (repeater) receives a signal and, before it becomes too weak or corrupted, regenerates it

Hubs

- Hub is a device that operates only in the physical layer

17

Hub



Link-Layer Switches

- A link-layer switch (or switch) operates in both the physical and the data-link layers
- As a physical-layer device, it regenerates the signal it receives
- As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame

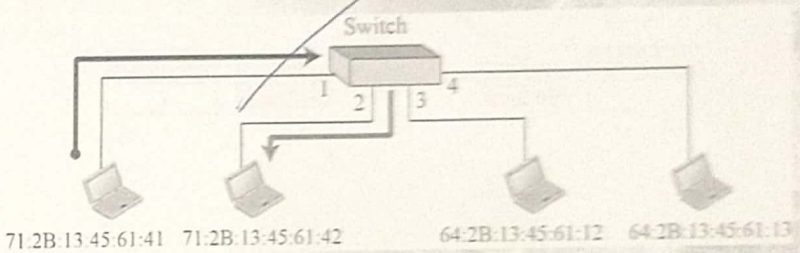
Switch versus Hub

- Switch has the 'Filtering' capability
- Unlike hub, a switch can check the destination address of a frame and decide on outgoing port
- Switch eliminates collisions and does not require carrier sensing
- Switches connect heterogeneous devices

Link-Layer Switch

Switching table

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



Link-Layer Switches

- A link-layer switch (or switch) operates in both the physical and the data-link layers

Learning Switch

a. Original

Address	Port

b. After A sends a frame to D

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

c. After D sends a frame to B

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

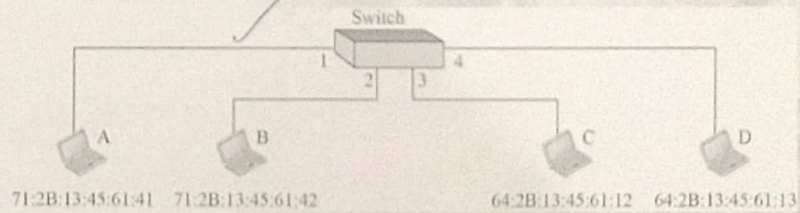
d. After B sends a frame to A

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

e. After C sends a frame to D

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

Gradual building of Table

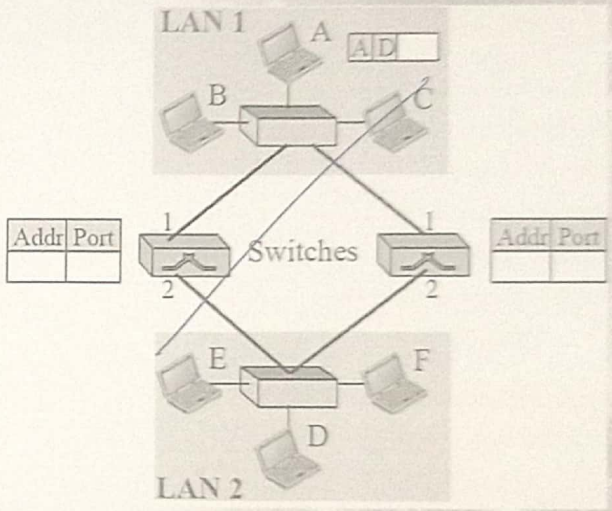


Loop Problem in a Switch

- Redundant switches create Loops in the system
- Created when two or more broadcasting LANs are connected by more than one switch

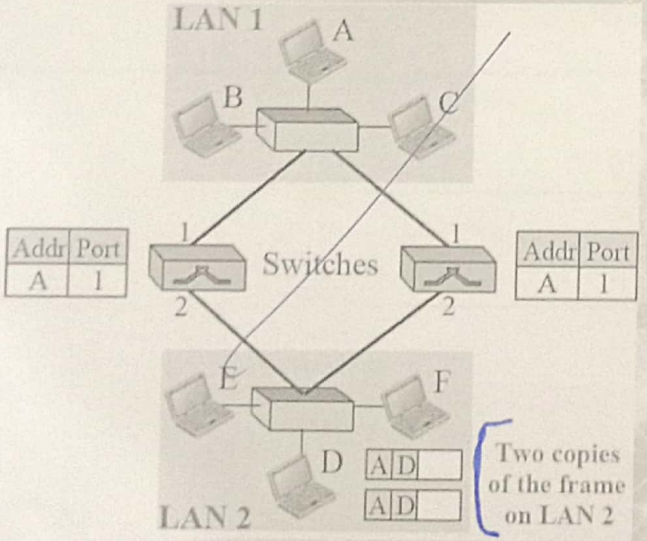
Loop Problem in a Learning Switch (Part a)

a. Station A sends a frame to station D



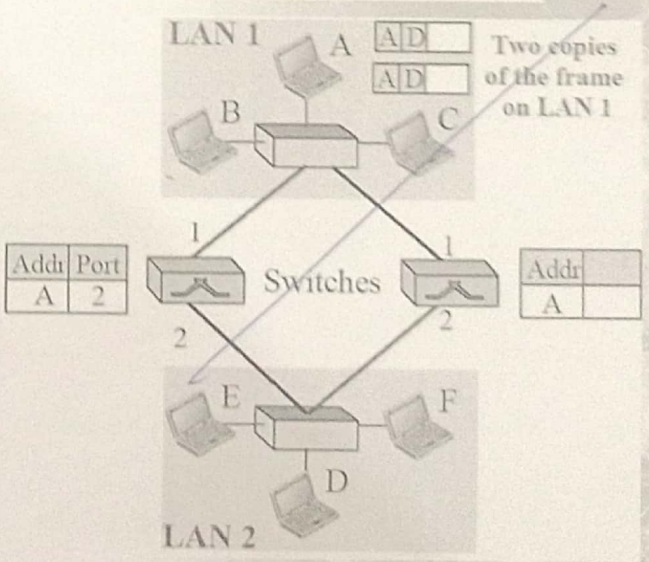
Loop Problem in a Learning Switch (Part b)

b. Both switches forward the frame



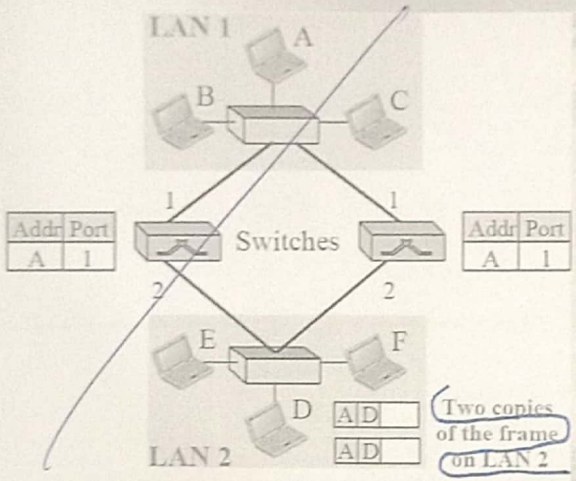
Loop Problem in a Learning Switch (Part c)

c. Both switches forward the frame



Loop Problem in a Learning Switch (part d)

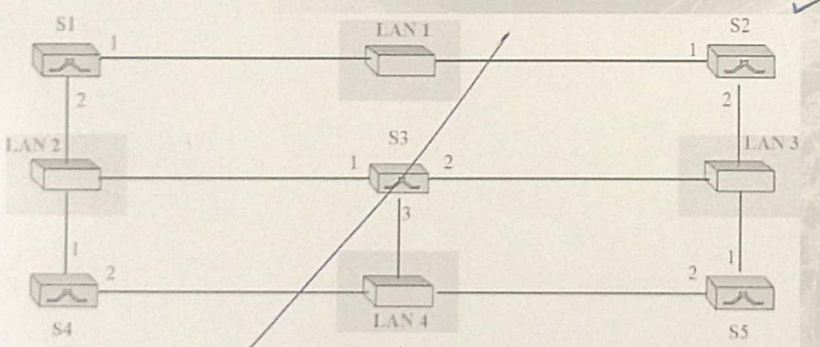
d. Both switches forward the frame



Spanning Tree Algorithm

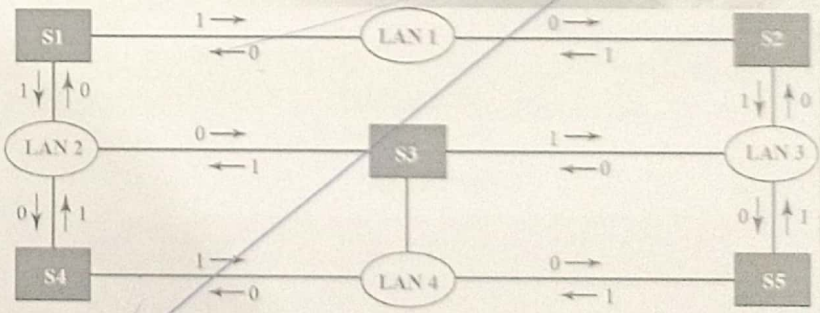
- In graph theory, Spanning Tree is a graph in which there is no loop
- In a switched LAN, this means creating a topology in which each LAN can be reached from any other LAN through one path only (no loop)
- To find the spanning tree, we assign a cost (metric) to each LAN link

A system of Connected LANs and its Graph (Part a)



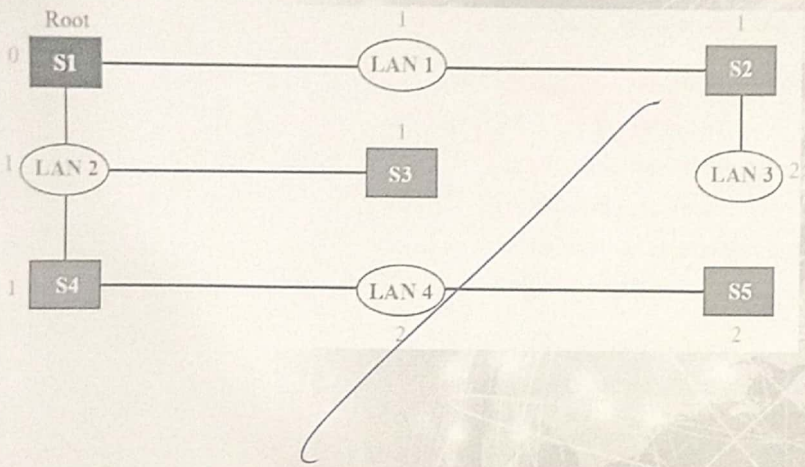
a. Actual system

A System of Connected LANs and its Graph (Part b)

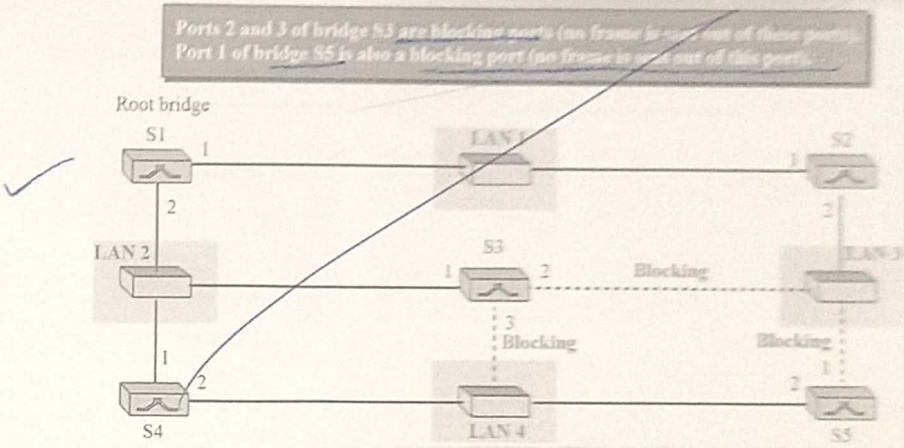


b. Graph representation with cost assigned to each arc

Finding Shortest Path/Spanning Tree for a Switch



Forwarding & Blocking Ports after using Spanning Tree



Routers

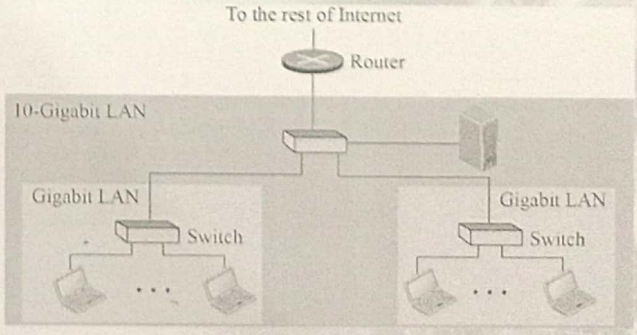
- We compare routers to two-layer switch and a hub

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

Router vs. Switch

Three differences between a router and a repeater or a switch:

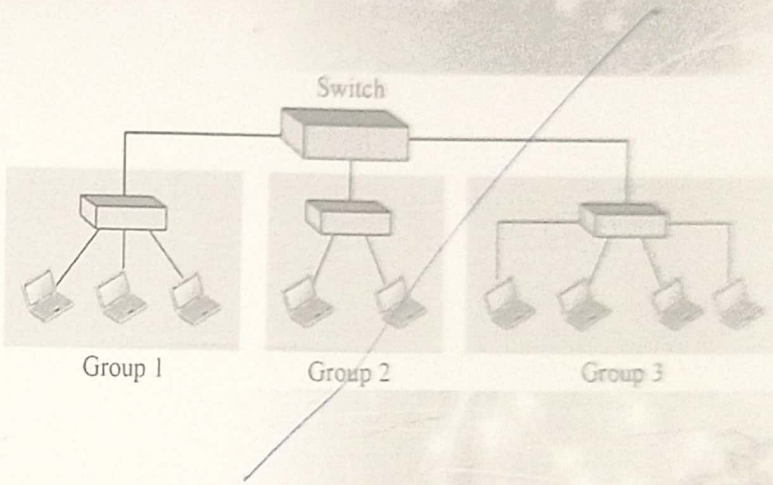
1. A router has a physical and logical (IP) address for each of its interfaces.
2. A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives.
3. A router changes the link-layer address of the packet (both source and destination) when it forwards the packet.



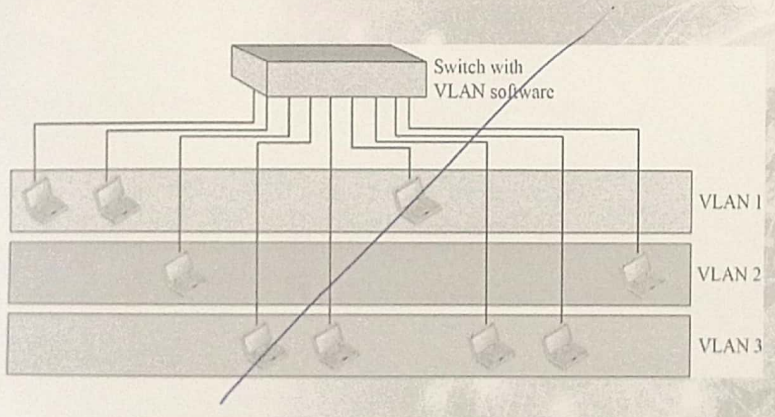
VIRTUAL LANS (VLAN)

- A VLAN is a LAN configured by software, not by physical wiring
- A station is considered part of a LAN if it physically belongs to that LAN i.e. The criterion of membership is geographic
- Provides a virtual connection between two stations belonging to two different physical LANs

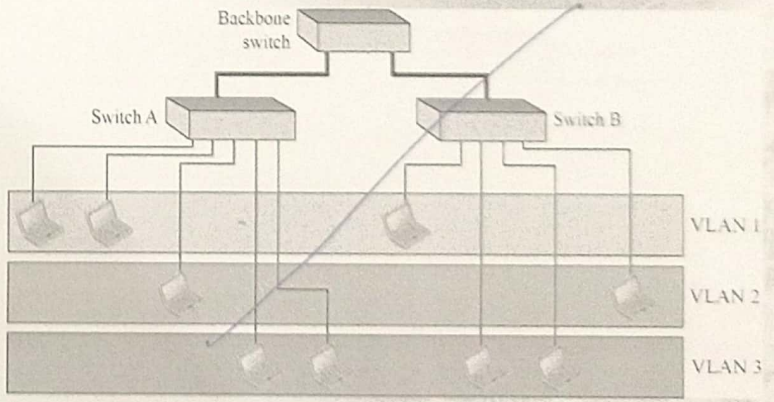
A Switch Connecting three LANs



A Switch using VLAN Software



Two Switches in a Backbone using VLAN Software



Membership of a VLAN

What characteristic can be used to group stations in a VLAN?

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

Configuration of a VLAN

How are the stations grouped into different VLANs?

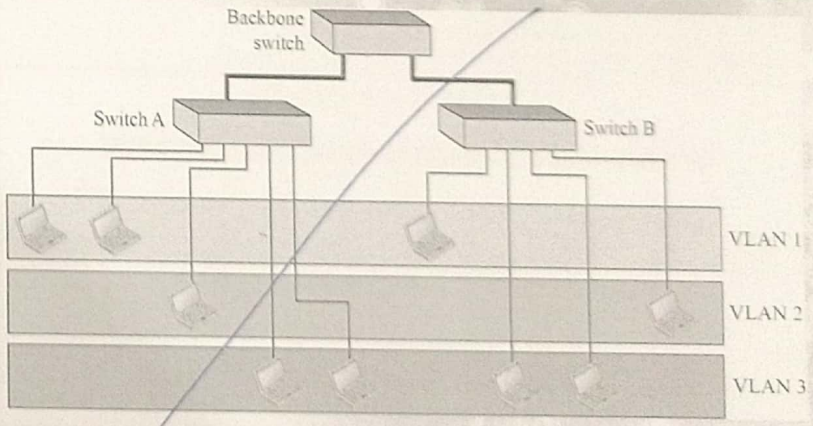
Stations are configured in one of three ways:

- ✓ Manually
- ✓ Semi-Automatically
- ✓ Automatically

Communication between Switches

- In a multi-switched backbone, each switch must know:
  - ✓ Which station belongs to which VLAN; and
  - ✓ The membership of stations connected to other switches

Communication between Switches



Switch A must know the membership status of stations connected to switch B, and switch B must know the same about switch A. Three methods have been devised for this purpose: table maintenance, frame tagging, and time-division multiplexing.

Advantages of using VLANs

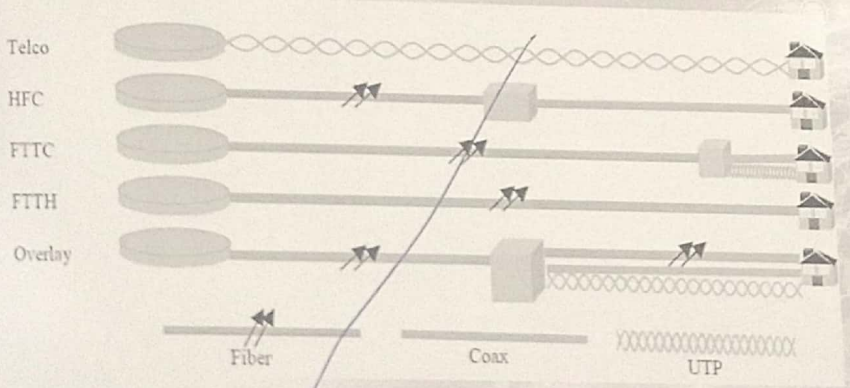
- Cost and Time Reduction
- Creating virtual Workgroups
- Security

Comparison of Modern Access Technologies

- Telco
- HFC
- FTTx

Telco
HFC
FTTx

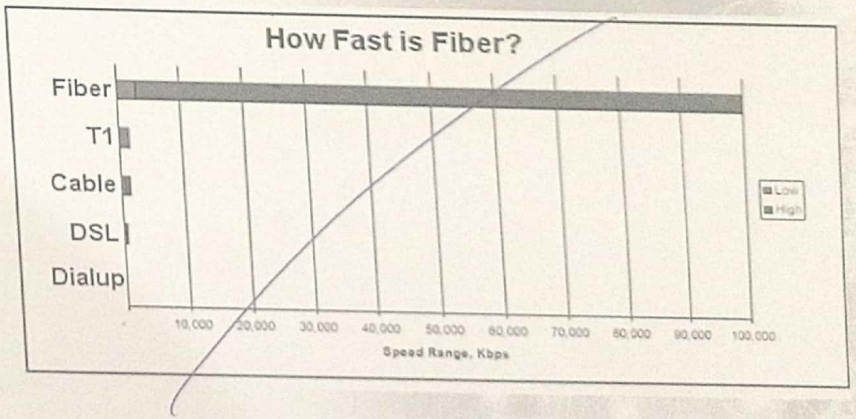
Comparison of Modern Access Technologies



FTTC
Fiber To the curb.

FTTC

Fiber – The Medium of the Future!



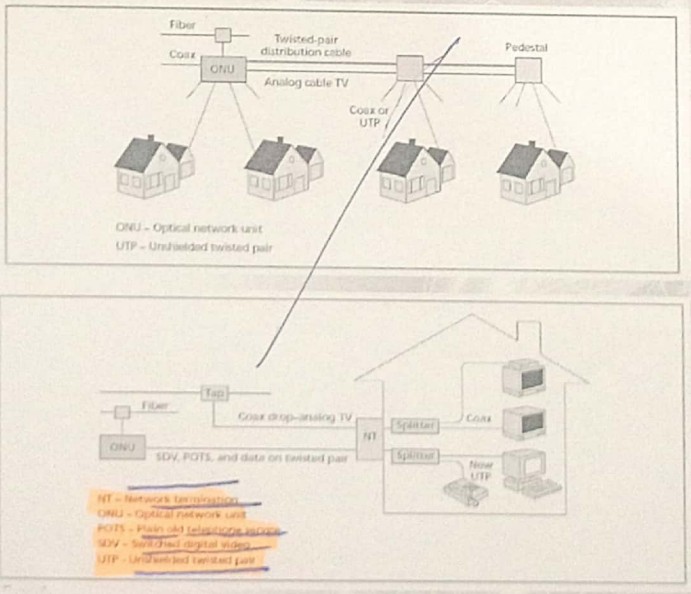
Fiber To The Curb (FTTC)

- An access network in which fiber is used for part, but not the entire link from the provider to the end-user
- An optical to electrical (O/E) conversion takes place somewhere near the end-user
- The terminal network segment of a FTTC network is usually twisted pair or coaxial cable

Fiber To The Curb (FTTC)

- The final optical receiver in a FTTC network typically serves several customers

Fiber To The Curb (FTTC)



Fiber To The Home (FTTH)

- Need: High-speed data, reliable voice and high-quality video

Problems:

- ✓ How to get high speed lines out to each customer?
- ✓ How to future-proof the architecture?

Solution: FTTH

Fiber to the home!

Fiber To The Home (FTTH)

- Fiber-to-the-home (FTTH) is the installation of optical fiber from a telephone switch directly into the subscriber's home
- It is one of the latest access technologies
- FTTH is also referred to as Fiber-to-the-Building (FTTB)

Fiber-to-the Building

Fiber To The Home (FTTH)