Short Notes:

CS 601 Data Communication & Networking

TOPIC 124 – 125

Chap….#...9

Data link Layer + Nodes & Links:

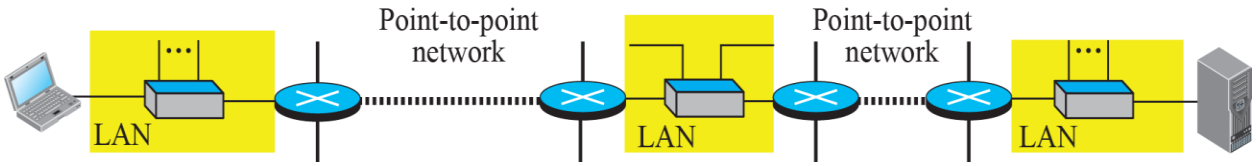
- The Internet is a combination of networks glued together by connecting devices (routers or switches)
- If a packet is to travel from a host to another host, it needs to pass through these networks
- Data Link layer controls node-to-node communication

The data link layer, or layer 2, is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between nodes on a network segment across the physical layer. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. Data link layer control Node-to-Node communication.

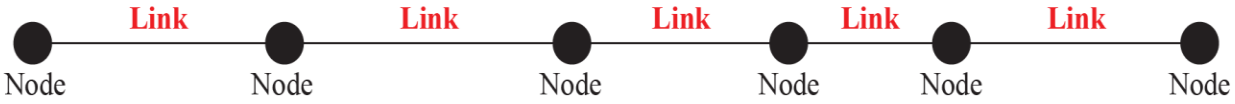
Example of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections. In the Internet Protocol Suite (TCP/IP), the data link layer functionality is contained within the link layer, the lowest layer of the descriptive model, which is assumed to be independent of physical infrastructure.

Nodes & Links:

As we study before that communication in data link layer is nod to node. We also know about data unit from one point to another point in Internet needs to pass through many networks like (LANs and WANs) to reach another point.
We refer to the two endpoints that are called hosts and the router as notes and the networks in between as links.



a. A small part of the Internet



b. Nodes and links

Topic 126 - 127. Serves provided by Data link Layer:

Data link layer provides the following services:

- framing
- flow control
- error control
- congestion control

Framing: First and foremost function of data link layer is framing. Date link layer divides data packets into small frames. Framing is a primary service of data link layer.

In case of framing we gone talk about two processes encapsulation and de capsulation, both combined are call framing. We know that data travel in the form of packets. Data link layer encapsulate this Packets into multiple frames. Encapsulation means breakdown of a packet into multiple frames which is stream of bit for transmission. Data Link Layer is also add its own header to each off frame .When data receive data link layer de-capsulate these frames. It Takes multiple frames and combined it in form of packet.

Example of Encapsulation & De Capsulation:

Suppose you have to travel from one city to another, the first thing you will do is you will take taxi for railway station and get off here for the train, and get on the train and go to another city. After landing in another city, you will take the taxi again and reach your destination.

Flow Control: Second Services flow control the transmission of frames from the source Host to the destination it actually needs some sort of control .Whenever your sender is transmitting data and your receiver is consuming the data we need to make sure some sort of control between sender and receiver. So that the speed of Data transmitting and the speed of data consuming they are same and data get not loss.

In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node.

Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to the sending computer, or if the receiving computer has less processing power than the sending computer.

Error Control: Data link layer is the layer where deploy some sort of error correction first of all detection and then error correction as well.

Congestion control: is a method used for monitoring the process of regulating the total amount of data entering the network so as to keep traffic levels at an acceptable value. This is done in order to avoid the telecommunication network reaching.

Topic 128 two types of DLL

There are two types of DLL:

- Point-to-point link
- Broadcast link

Point -to-point link: A point-to-point link refers to a communications connection between two communication endpoints or nodes. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other.

The term is also used in computer networking and computer architecture to refer to a wire or other connection that links only two computers or circuits, as opposed to other

network topologies such as buses or crossbar switches which can connect many communications devices. Point-to-point is sometimes abbreviated as P2P.

Broadcast link: Broadcast links connect two or more nodes and support broadcast transmission, where one node can transmit so that all other nodes can receive the same transmission. Ethernet is an example.

Sub layers of DLL:

There are two sub layers of Data link layer:

Data link control (DLC): it deals with point-to-point link as well as broadcast link.

Media Access Control (MAC): it deals with only broadcast link.

Topic 129 - 130 Link Addressing:

Link layer addresses

- IP addresses:
- Link layer addresses / physical addresses / MAC addresses:

IP Addresses: IP addresses are the identifiers at the network layer in Internet we cannot make a packet reach its destination using only IP addresses.

Link Layer Addresses: Source and destination IP addresses Define Two ends but cannot Define which links the packet and path will take. Encapsulation and de capsulation processes are involved In these link layer addresses. In process of encapsulation also involve header. This header contains the link layer addresses of the source and destination.

Topic 131 Types of address

Three types of address

i. Unicast
ii. Multicast
iii. Broadcast

Unicast: one to one communication. Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.

Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet. All LANs (e.g. Ethernet) and IP networks support the unicast transfer mode, and most users are familiar with the standard unicast applications (e.g. http, smtp, ftp and telnet) which employ the TCP transport protocol.

Multicast: Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers.

Multicasting is the networking technique of delivering the same packet simultaneously to a group of clients. IP multicast provides dynamic many-to-many connectivity between a set of senders (at least 1) and a group of receivers.

Broadcast: Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.

Broadcast transmission is supported on most LANs (e.g. Ethernet), and may be used to send the same message to all computers on the LAN (e.g. the address resolution protocol (arp) uses this to send an address resolution query to all computers on a LAN, and this is used to communicate with an IPv4 DHC server). Network layer protocols (such as IPv4) also support a form of broadcast that allows the same packet to be sent to every system in a logical network (in IPv4 this consists of the IP network ID and an all 1's host number). This is defined in network layer.

Topic 132 Address Resolution Protocol (ARP)

In networking if a host send data to another host then it must have IP address. This process is done by using DNS. DNS finding IP address of the destination. IP address is very good, but it is not enough to find out the destination nodes.

In this case IP address is not helpful for moving the frame through different nodes and links that make up the rote from the source to the destination. Here we need address resolution protocol.

Any time a host or a router needs to find the link layer address to other hots it will send an ARP request to the subsequent node. This packet will include the link layer and IP address of the source node, because the sender does not know the link layer address of the receiver the query is actually broadcast over the network.

Topic 133 – 134 Address Resolution Protocol (ARP) Operation

ARP Operation:

ARP broadcast request package to all the machines on LAN and ask if any of the machine know they are using particular IP address. when a Machinery can recognize the IP address as it's own it sends a reply. So to ARP can update the cash for future reference and proceed with communication.

Note: ARP request is always broadcast. ARP reply is always Unicast.

Caching:

In caching system A the link layer address of system B once it received. If once store address in cash then all the Future transactions from system A to system B are normally unit cost.

Topic 135 – 136
Chap…#...10

Types of Error

Data transmission suffers unpredictable change because of interference. This interference can change the shape of signal.

There are two types of errors:

- Single bit error
- Burst error

Single bit Error: means that only one bit of given data unit is changed from 1 to 0 or 0 to 1.

Example:

0	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**

0	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**

Burst Error: means that two or more bits in data unit have change from 1 to 0 or from 0 to 1.

0	1	0	0	1	0	0	1	0	1	0

0	1	1	0	1	1	0	1	1	0	0

Length of burst error is 8 bits.

Number of impacted bits actually depends on two things:

- Data rate
- Duration of rate

Note: higher data rate cause of more bits impacted. And more duration of noise is source of higher number of bits going to be impacted. Because of these two things burst error is common then single bit error.

Topic 137 Redundancy

Redundancy

Central concept of detecting or correcting error is redundancy to be able to detect or correct error we send some extra bits with our data. The presence of these redundant bits allowed the receiver to detect or correct corrupted bits.

Error detection VS Error correction

Error Detection:

Error detection is simple while error correction is complex. In error detection we are only looking to see if error has occurred (yes or no). We are not interested in the number of corrupted bits. In error detection single bit error is same as burst errors.

Error Correction:

In error correction we need to know:

- The exact numbers of corrupted bits, and
- The location of corrupted bits.

Topic 138 – 139 Coding Schemes

Coding schemes can be derived into two broad categories:

- Block coding
- Convolution coding

Block coding: In block coding we divide our message into blocks, each of them has 'k' bits, called as data word. Here "k" means a certain number of bits. Then we add 'r' redundant bits to each block to make the length **n = k + r**. The resulting 'n' bit blocks are called code word.

Note: sender sends code words to receiver and receiver checks code words.

Block coding in error detecting:

If the following two conditions are met, the receiver can detect a change in the original code words:

- The receiver has a list of valid code words
- The original code word has changed to an invalid one.

Topic 140 Block Coding

Example:

Let us assume that k = 2 and n = 3, table below shows that list of code word and data word. Letter we will see how to derive a code from a data word.

$$2^n = 2^3 = 8$$

Data word	Code word	Data word	Code word
00	000	10	101
01	011	11	110

Look at 2nd code word that is '011':

Let suppose:

i. If receiver get '011' and this is valid code word, then '01' is extracted and it is passed to receiver.
ii. If we send '011' and received as '000' this is invalid code word. It is corrupted code word. This will not be processed by the receiver, and this will be discarded.

iii. If code word is corrupted during transmission and we receive the corruption of two bits. We receive '011' instead of '000'. In this case this matches with a valid code word in given data.

Topic 141 Hamming Distance

Hamming distance is a metric for comparing two binary data strings. While comparing two binary strings of equal length, Hamming distance is the number of bit positions in which the two bits are different. The Hamming distance between two strings, x and y is denoted as *d*(x,y).

Hamming Distance between receiver code word and sent code word is actually number of bits that are corrupted.

Example:

1. **d (000, 011) ; 000 is x and 011 is y.**

d (000, 011); 0 0 0 , 0 1 1

Here hamming distance is 2 because two bits are different:

2. **d (10101, 11110) =>** '10101' is x and '11110' is y

   d(10101, 11110) => 1 0 1 0 1 , 1 1 1 1 0

   Here hamming distance is 3 because 3 bits are corrupted:

In simple words hamming distance tells us how many bits are corrupted.

If d (x,y) ≠ 0 → that means there is an error in our data.

Topic 142 Minimum Hamming Distance

Minimum Hamming distance is a smallest hamming distance between all possible pair of code words.

dmin = *s* + 1
Where s → no of detected error

dmin → minimum hamming distance:

Example:

A code scheme has a hemming distance *dmin*=4. This code guarantees the detection. Up how to many errors.

dmin = 4

dmin = s + 1

s = *dmin* - 1

S = 4 – 1

S = 3

If you got a block code which has got a minimum hamming distance 4, it means that this block code guarantees error detection up to three bears in the cold word.

Linear block code: Is all subsets of block code in which the exclusive OR of two valid code words creates another world code.

Data word	Code word	Data word	Code word
00	000	10	101
01	011	11	110

If we do exclusive OR ⊕ between two code words:

001 ⊕10 =110 → linear block code.

Topic 143 Parity check code

Parity check is a simple way to add redundancy bits to the packets such that the total number of 1's is even or odd.

- Most common error detecting code.
- Linear block code (n = k + 1).
- The extra parity bits is selected to make total number of 1s coed word even.

Example:

C (5, 4) => k= 4, n=5

Data word (k)	Code word (n)	Data word (k)	Code word (n)
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
1010	10100	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

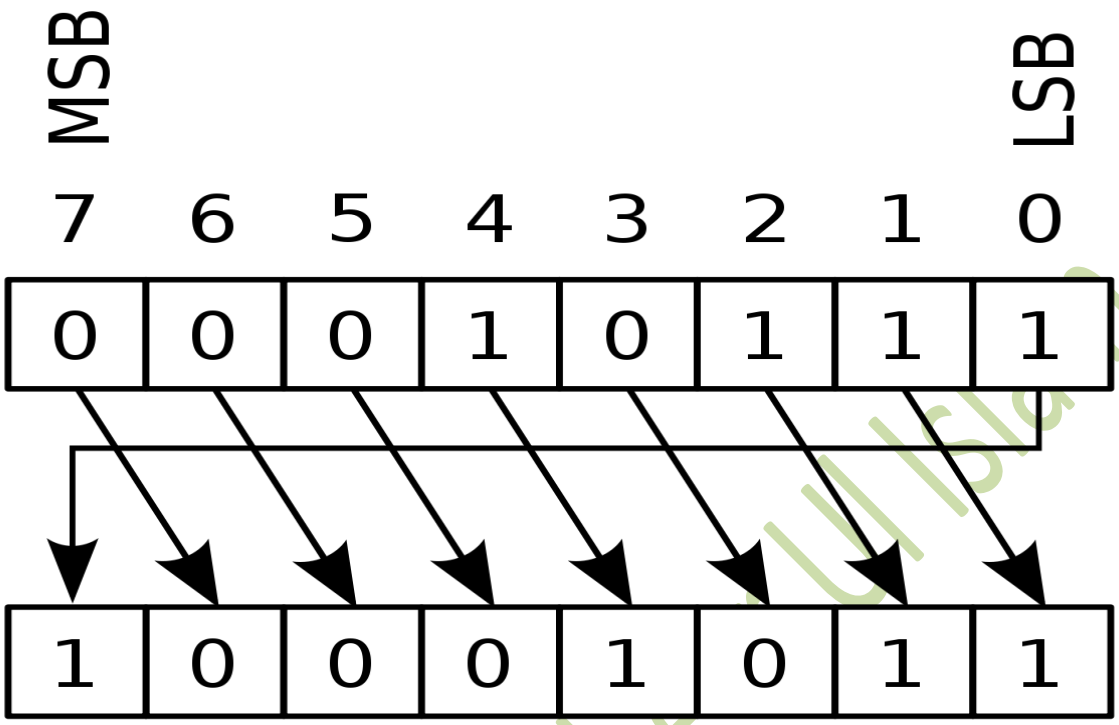
n > k → no of code word > no of data word

If total number of 1s is odd then our extra parity bit is 1 to make our total number of 1 is even. If the total number of 1s is already even then extract parity bit that we are adding to our code word is 0.

Topic 144 to 145 CYCLIC CODES:

In coding Theory a cyclic code is a block code where the circular shift of each codeword gives another word that belongs to the code. They are error correcting codes that have algebraic properties that are convenient for efficient error detection and correction.

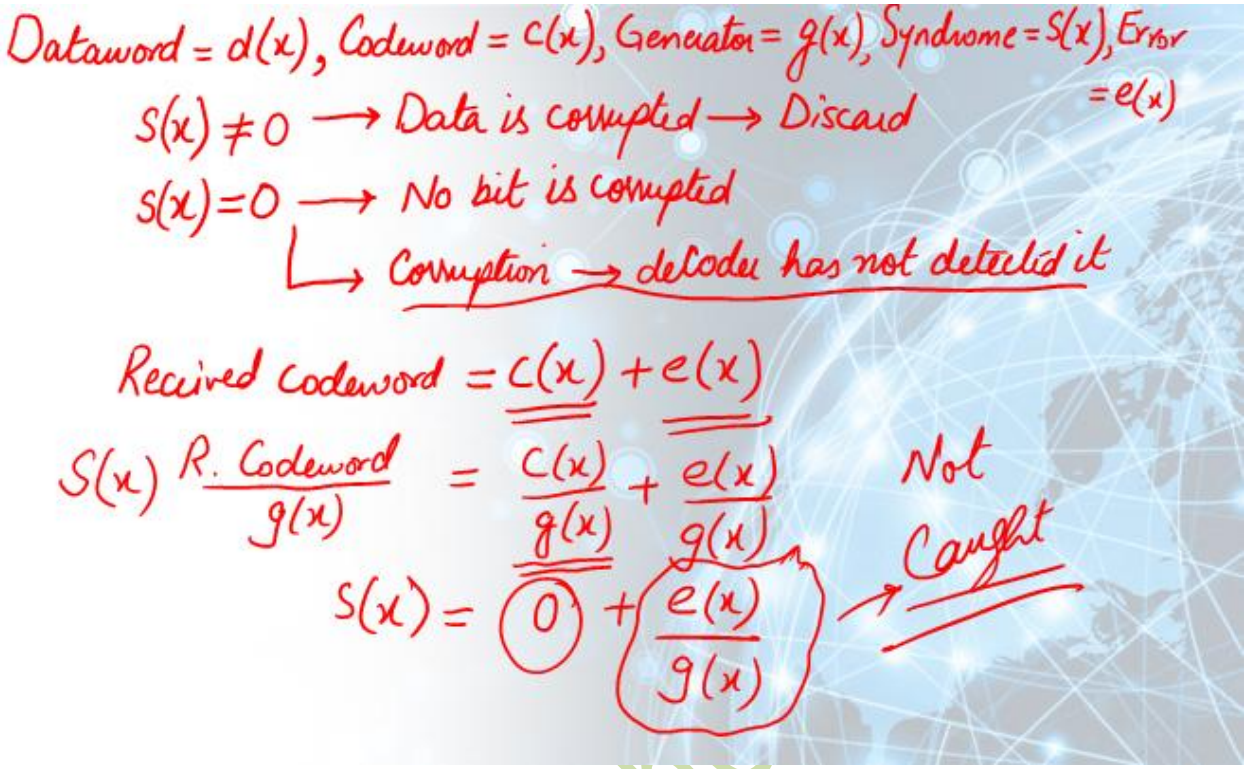
Example:



CRC

- CRC is an error detection technique to detect change to Raw data and is used widely in today's computer networks
- CRC codes are also known as polynomial codes since it is possible to view the bit string to be sent as a polynomial.

Cyclic Code Analysis using Polynomials



Advantages of Cyclic Codes

i. Good performance in detection:
   - Single-bit errors
   - Double errors
   - Odd number of errors
   - Burst errors

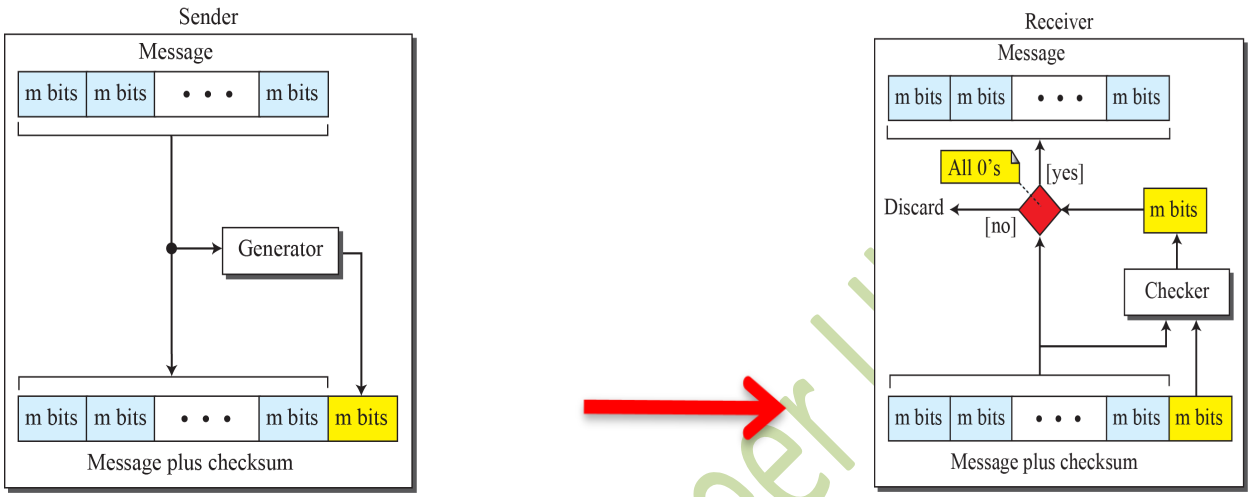
ii. Easy Implementation

iii. Fast Implementation

Topic 146 CHECKSUM:

A checksum is a small-sized block of data derived from another block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage.

- Error-detection technique that can be applied to a message of any length.
- Checksum mostly used at the network and transport layer rather than the data-link layer



Watch topic 146 for this diagram:

Concept behind Checksum

- The idea of the traditional checksum is simple. We show this using a simple example:

Suppose the message is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers.

Set of numbers is (7, 11, 12, 0, 6)

Example:

7 + 11 + 12 + 0 + 6 = 36

We should to send as follow (7, 11, 12, 0, 6, 36) but here five 4–bit word that are (7, 11, 12, 0, 6) and 36 is not 4 bit number. So for sending 36 with our data we shout convert it 4 bit number first as following method:

In the previous example, the decimal number 36 in binary is (100100)2. To change it into a 4-bit number we add the extra leftmost bit to the right four bits as shown below

$(10)_2 + (0100)_2 = (0110)_2$

$(6)_{10}$

So instead of sending (7, 11, 12, 0, 6, 36) we will send (7, 11, 12, 0, 6, 6) now checksum is in 4 bit form. Now receiver again add these numbers and if the result is 6 then it will accepted otherwise rejected.

Topic 147-148 Forward Error Correction (FEC)

- Retransmission of corrupted and lost packets is not useful for real-time multimedia transmission
- We need to correct the error or reproduce the packet immediately
- Several techniques developed and are commonly called Forward Error Correction techniques

1. Using Hamming Distance

- For error detection, we definitely need more distance
- It can be shown that to correct 't' errors, we need to have: $d_{min} = 2t + 1$
- If we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits
- A lot of redundant bits need to be sent with the data

Example:

If we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits

$d_{min} = 2t + 1$

$d_{min} = 2(10) + 1$

$d_{min} = 21$ this is amount of redundant bits that you send with your data word.

2. Using XOR

Another recommendation is to use the property of the exclusive OR operation as shown below.

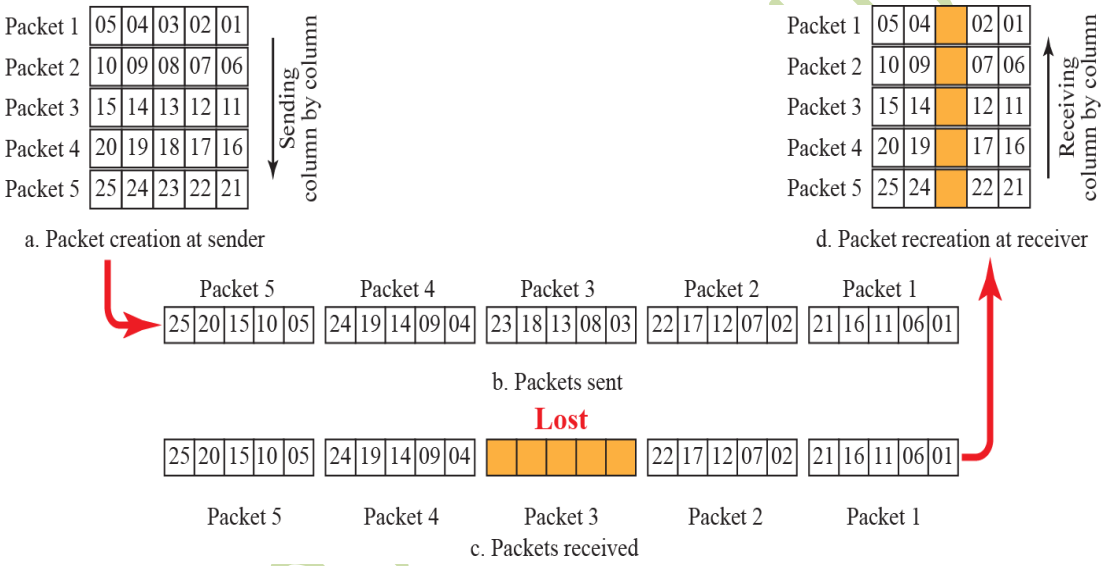
$R = P_1 + P_2 + \ldots + P_i + \ldots + P_N$

This means:

$$P_i = P_1 + P_2 + \ldots + R + \ldots + P_N$$

Chunk Interleaving

- Another way to achieve FEC in multimedia is to allow some small chunks to be missing at the receiver
- We cannot afford to let all the chunks belonging to the same packet be missing; however, we can afford to let one chunk be missing in each packet.



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.

Topic 149 – 151
Chap…#...11

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.

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. 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?

  If we make one big size frame it creates a problem. In case of error if we have one big frame our whole data will be lost. That is why we make number of small frames instead of one big frame.

- Frames can be of:

✓ **Fixed Size**
- Size acts as a boundary/delimiter
- In fix size every frame have same size

The problem with fixed size framing is that, error detection, error correction, flow control and all these kind of functions become very difficult.

✓ **Variable Size**
- How to define Beginning and End of a Frame?

In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

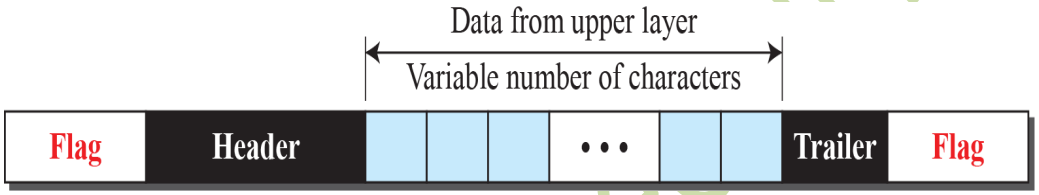
i. **Character-Oriented Protocols:**
ii. **Bit-Oriented Protocols:**

Topic 151 – 153

Character (Byte) Oriented Protocols or:

- In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII.
- The header, which normally carries the source and destination addresses and other control information.

- The trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.
- Figure shows the format of a frame in a character-oriented protocol.

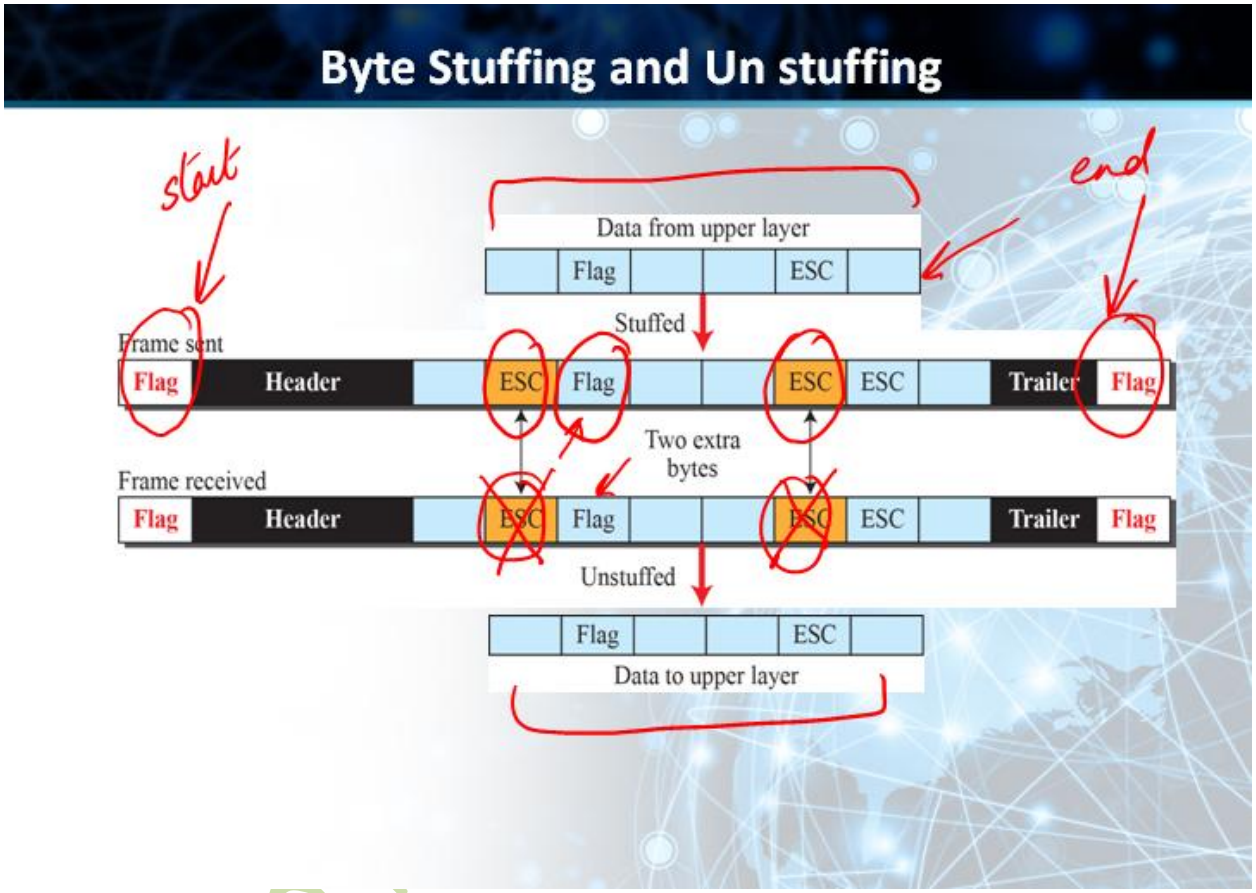


- Character-oriented framing was popular when only text was exchanged by the data link layers.
- The flag could be selected to be any character not used for text communication.
- Now, however, we send other types of information such as graphs, audio, and video. Any pattern used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame. To fix this problem, a byte stuffing strategy was added to character-oriented framing.

Byte stuffing (or character stuffing):

- In this sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data.
- The data link layer on the receiving end removes the escape byte before the data are given to the network layer.
- This technique is called byte stuffing or character stuffing.
- Thus, a framing flag byte can be distinguished from one in the data by the absence or presence of an escape byte before it.
- Of course, the next question is: What happens if an escape byte occurs in the middle of the data?
- The answer is that it, too, is stuffed with an escape byte.
- Thus, any single escape byte is part of an escape sequence, whereas a doubled one indicates that a single escape occurred naturally in the data.

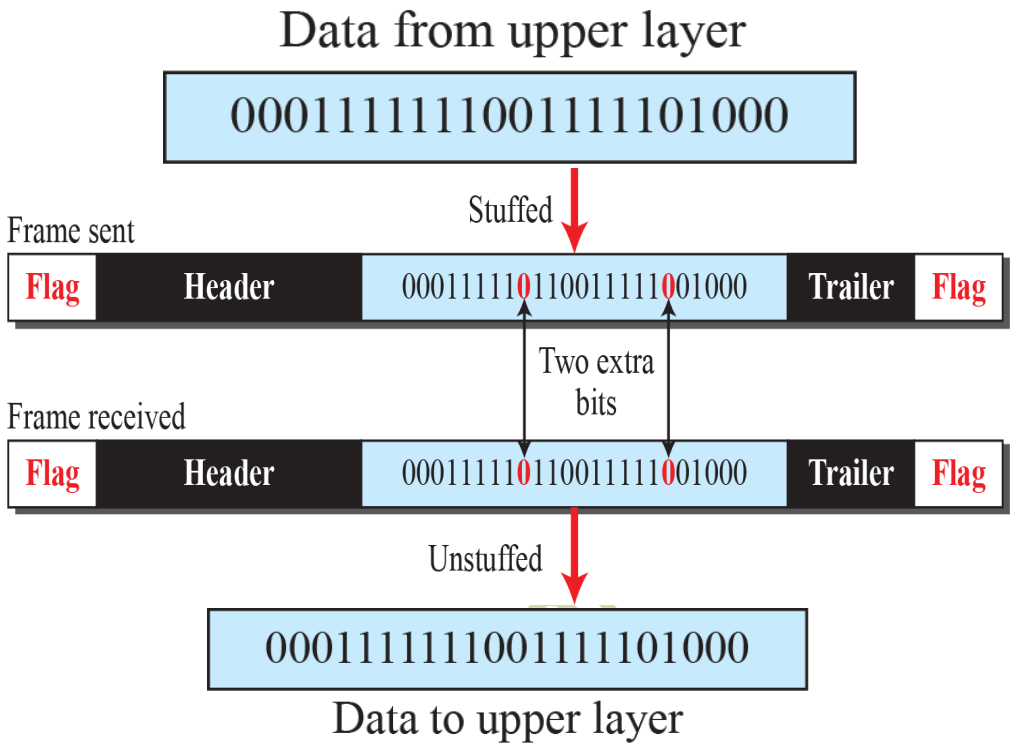
- **Major disadvantage** of Character-oriented protocols is it use 8-bits characters. The universal coding systems in use today, such as Unicode, have 16-bits and 32-bits characters that conflict with 8-bits characters.



Bit-Oriented Protocols:

- In this data frames contains an arbitrary number of bits and allows character codes with an arbitrary number of bits per character.
- It works like this. Each frame begins and ends with a special bit pattern, **01111110** (in fact, a flag byte).
- Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.
- This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically un stuffs (i.e., deletes) the 0 bit.
- Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing.
- If the user data contain the flag pattern, 01111110, this flag is transmitted as **011111010** but stored in the receiver's memory as **01111110.**

Look at the Slide below



Topic 154

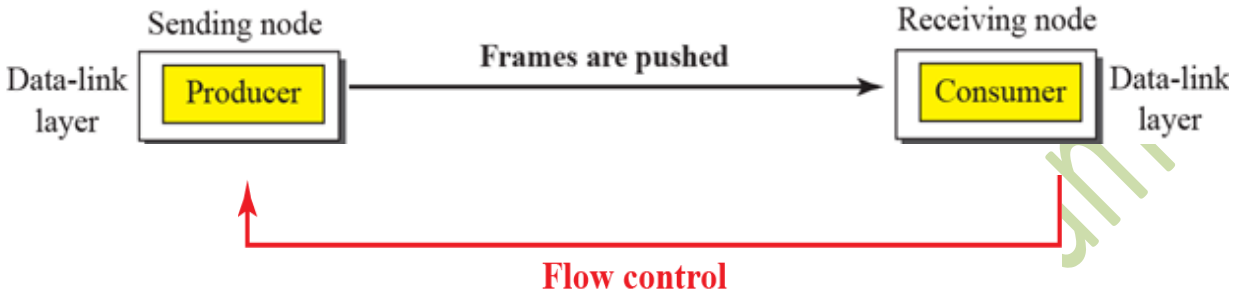
FLOW Control:

- **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**

In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually occurred.

Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to

the sending computer, or if the receiving computer has less processing power than the sending computer.



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

Topic 155

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 that the frame is received safely.

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.**

Connectionless:

All frames are independent. Connectionless doesn't mean that no physical connection between frames, but it means that you don't have any relationship between frames that you are sending so you have one frame for one message and other frame for another message.

Connection-Oriented:

In this particular case as we discussed in data link layer connection oriented protocol as those that actually establish a connection first, then they do the setup, then they do the data transmission and then they have to do connection dare down.

In this particular case the frames are sent in particular order. They have got a transmission with another when a frame is successfully received. Receiver sends acknowledgement back to the sender to tell the sender that this Frame is received successfully and error free now send the Next one.

Topic 156

DATA-LINK LAYER PROTOCOLS:

Traditionally four protocols have been dsefined 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

Note: Before we have to discussion Data link layer protocol we have to discuss Finite State Machine **(FSM)**.

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

Definition:

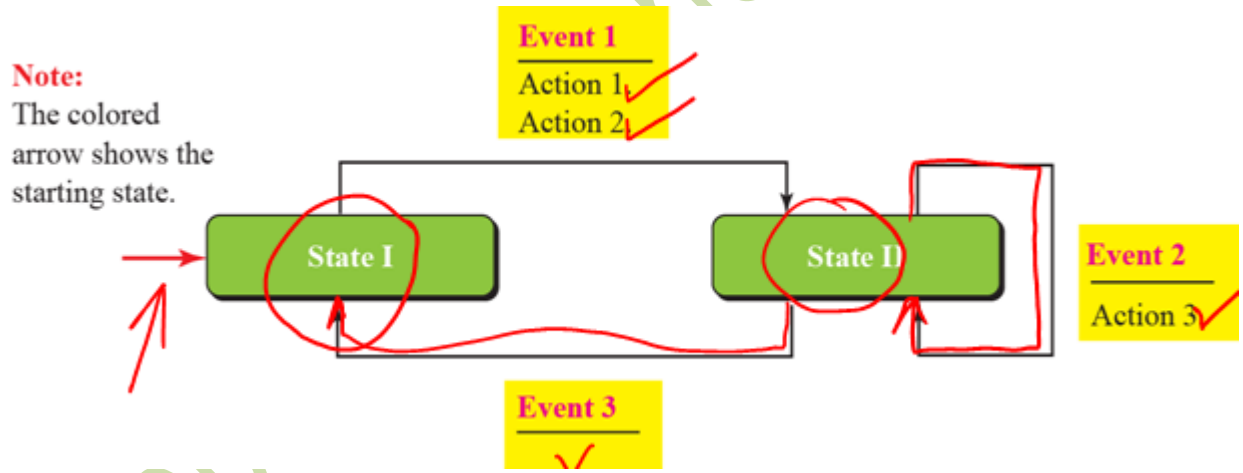
A state-of-the-art machine is a model of counting based on a fictitious machine consisting of one or more states. Only one mode of this machine can be activated at a time. This means that the machine has to be moved from one state to another to perform various functions.

Explanation:

Let's supposed the State is standing that is your starting stat you stay at your standing State until a force applied to you.

Same concept of FSM it starts from a particular Stat and stay in this stat until a specific event happens. When event is occurred there are two things your FSM does.

- List of actions to be performed
- Determining the next state

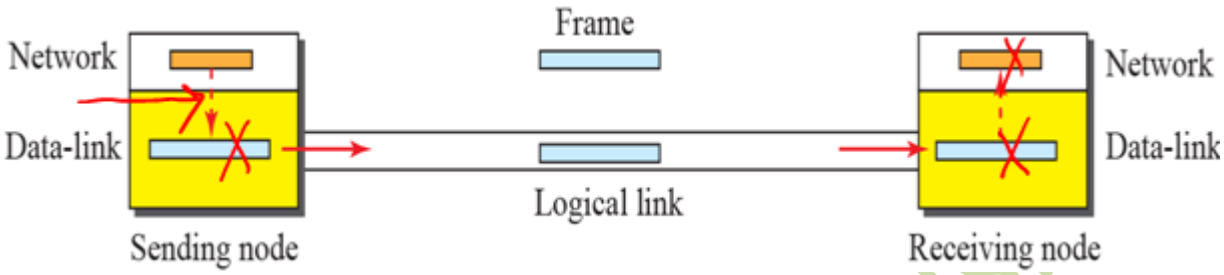


Topic 157

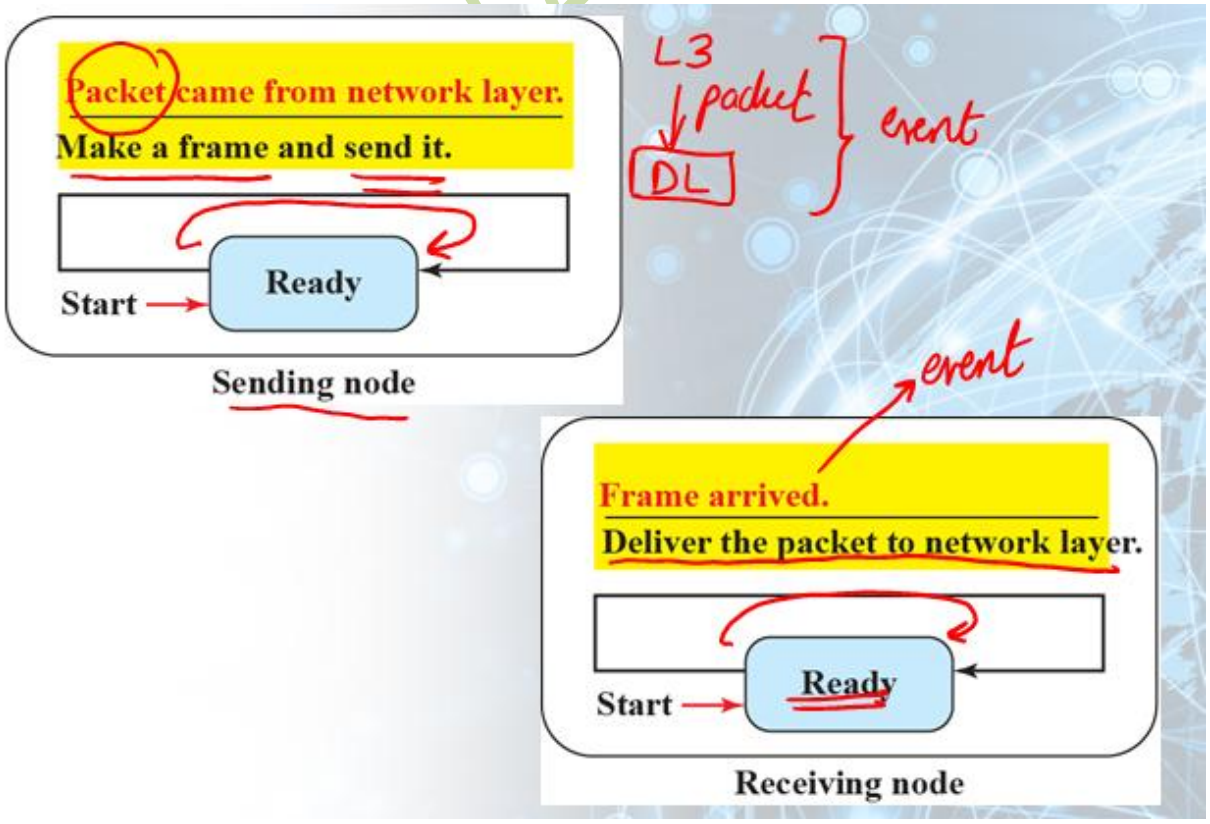
Simple Protocol

- 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.

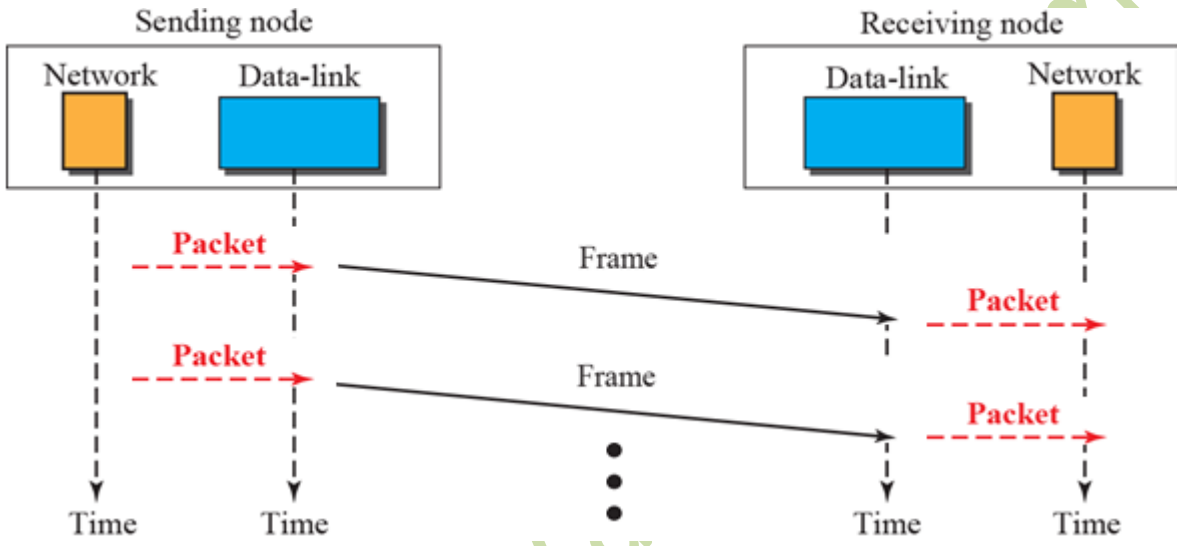


FSM for Simple Protocol:



Example

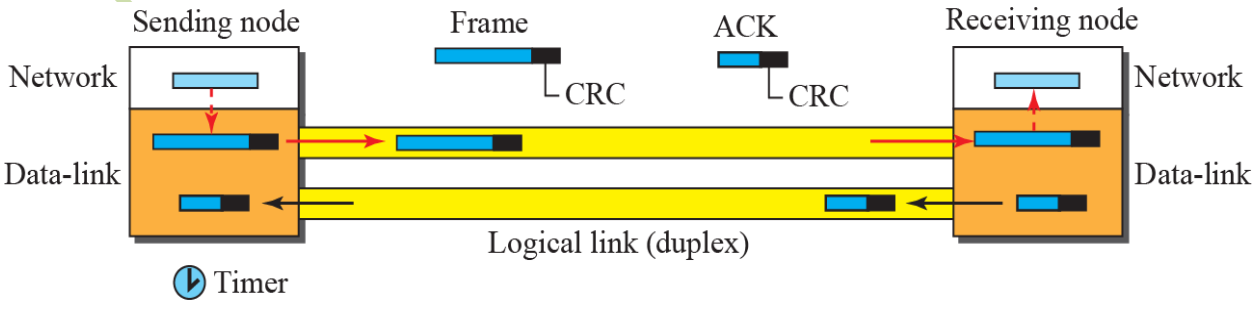
Here is an example of communication using this protocol. It is very simple. The sender sends frames one after another without even thinking about the receiver.



Topic 158

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.

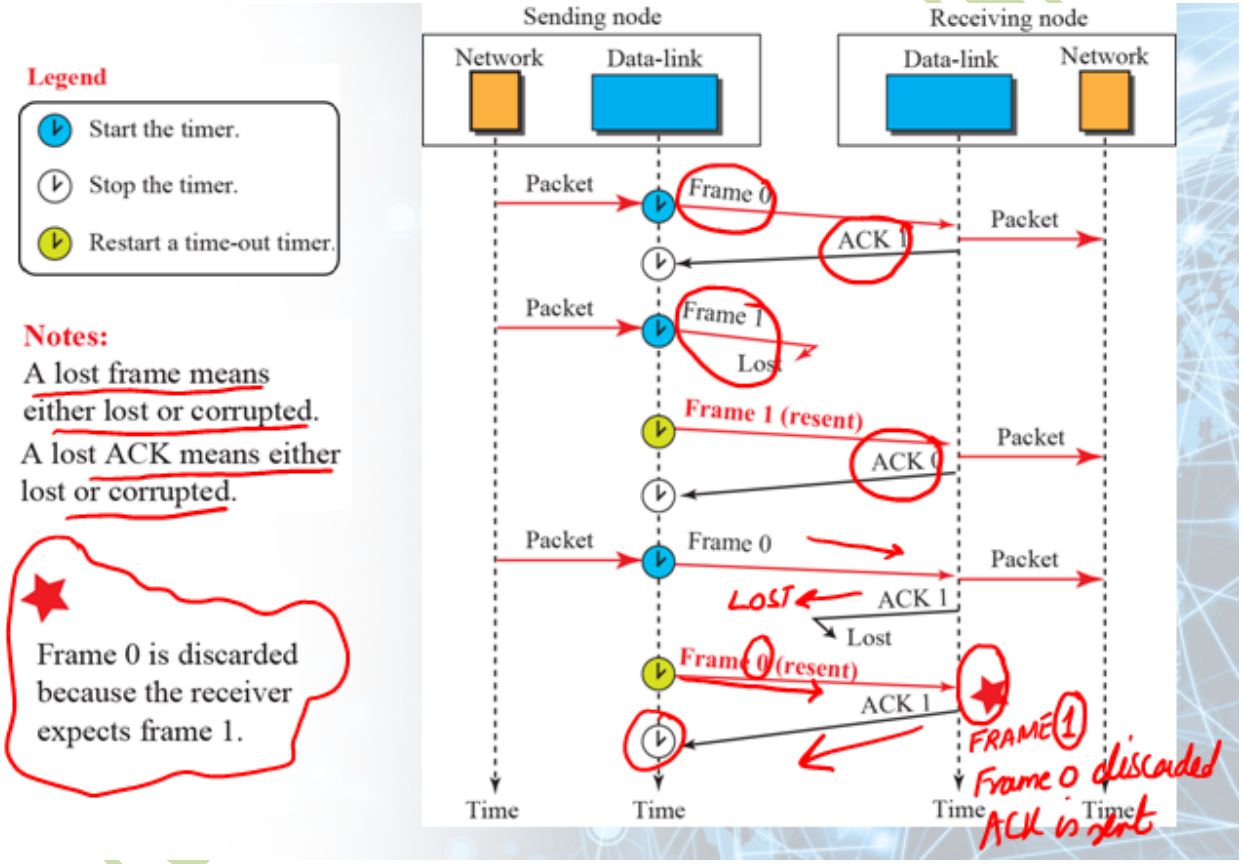


Acknowledgement caring with two messages:

- I have received the previous frame please send next one.
- The frame that we have sent previously he has been received error free.

Topic 159

Example:



Topic 160

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)

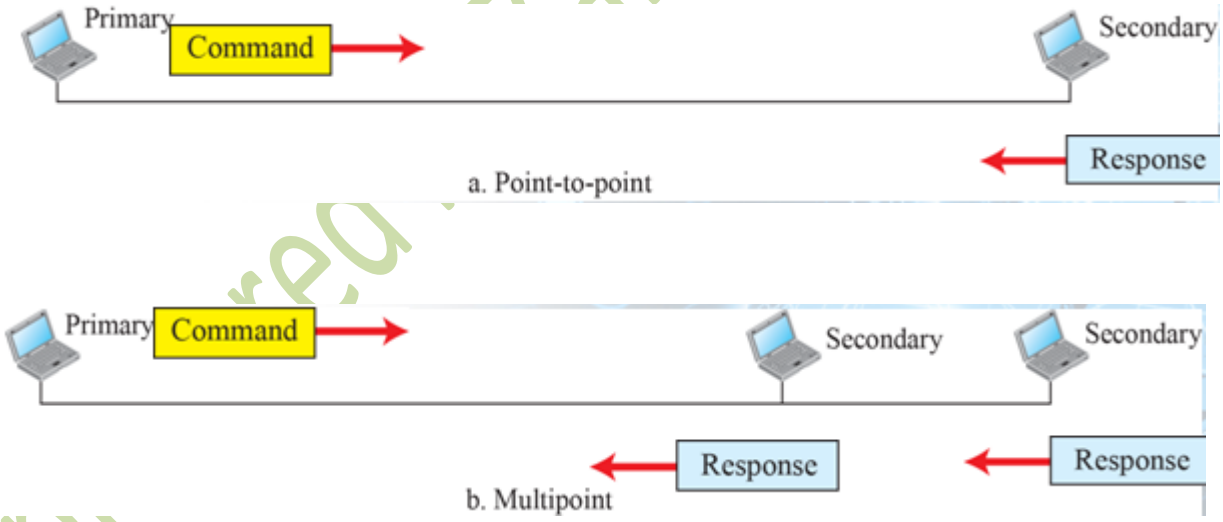
- Bit -oriented protocol for communication over point-to-point and multipoint links
- It implements Stop-and-Wait protocol
- Most of the concepts defined in this protocol is the basis for other protocols such as PPP, Ethernet, or wireless LANs

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 (NRM)



Asynchronous Balanced Mode (ABM)

Topic 161

HDLC Framing

HDLC defines three types of frames:

- **information frames (I-frames)**

  Information frames, or **I-frames**, transport user data from the network layer. They can also include flow and error control information piggybacked on data.

- **Supervisory frames (S-frames)**

  Supervisory frames, or **S-frames**, are used for flow and error control whenever piggybacking is impossible or inappropriate, such as when a station does not have data to send. S-frames **do not** have information fields.

- **Unnumbered frames (U-frames)**

  Unnumbered frames, or **U-frames**, are used for various miscellaneous purposes, including link management. Some U-frames contain an information field, depending on the type.

Topic 162

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

Topic 163

Services provided by PPP

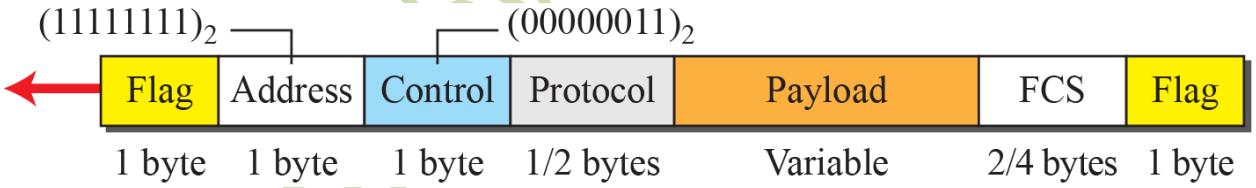
The designers of PPP have included several services to make it suitable for a point-to-point protocol, but have ignored some traditional services to make it simple

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	

PPP Frame Format

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



Topic 164

Multiplexing in PPP

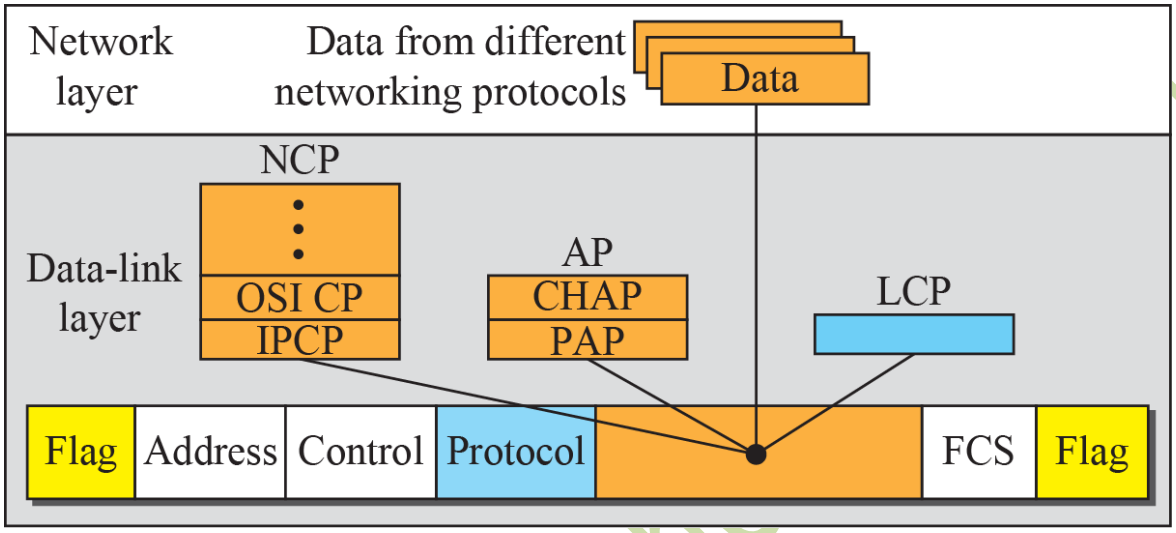
Although PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate and carry the network-layer data

Three sets of protocols are:

- **Link Control Protocol (LCP):** This is responsible for establishing, maintaining, configuring and terminating our PPP links.

- **Two Authentication Protocols (APs):** AP has two types: **PAP** stands for Password Authentication Protocol.
  CHAP stands for Challenge handshake Authentication protocol.

- **Several Network Control Protocols (NCPs):** It has OSI, CP and IPCP.s

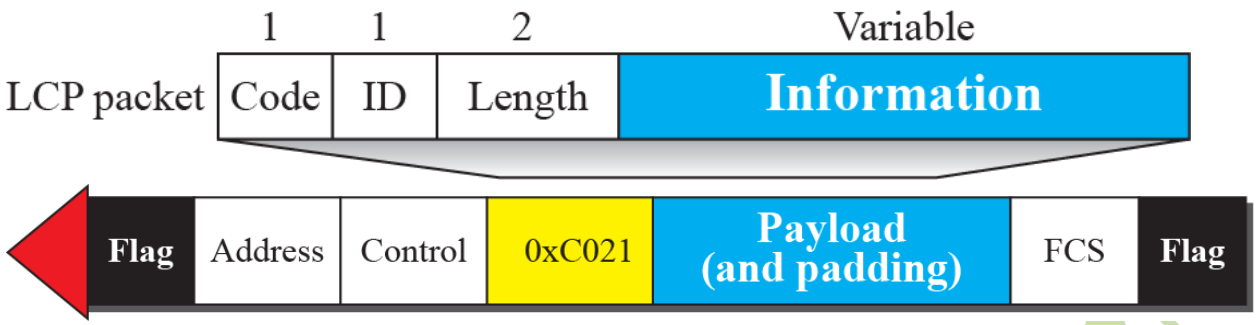


Legend

LCP : Link control protocol
AP : Authentication protocol
NCP: Network control protocol

Protocol values:
LCP : 0xC021
AP : 0xC023 and 0xC223
NCP: 0x8021 and ....
Data: 0x0021 and ....

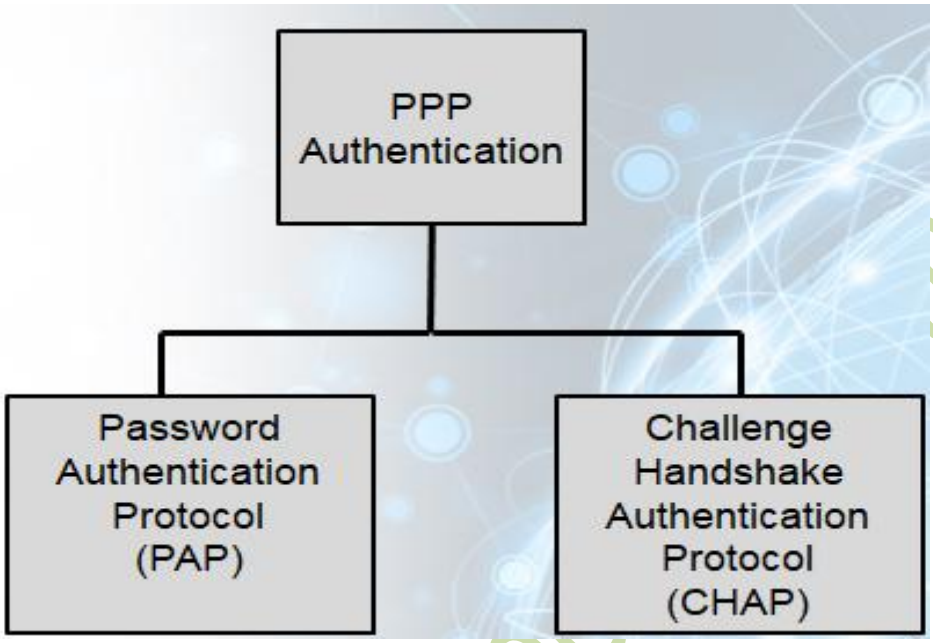
LCP Packet encapsulated in a Frame



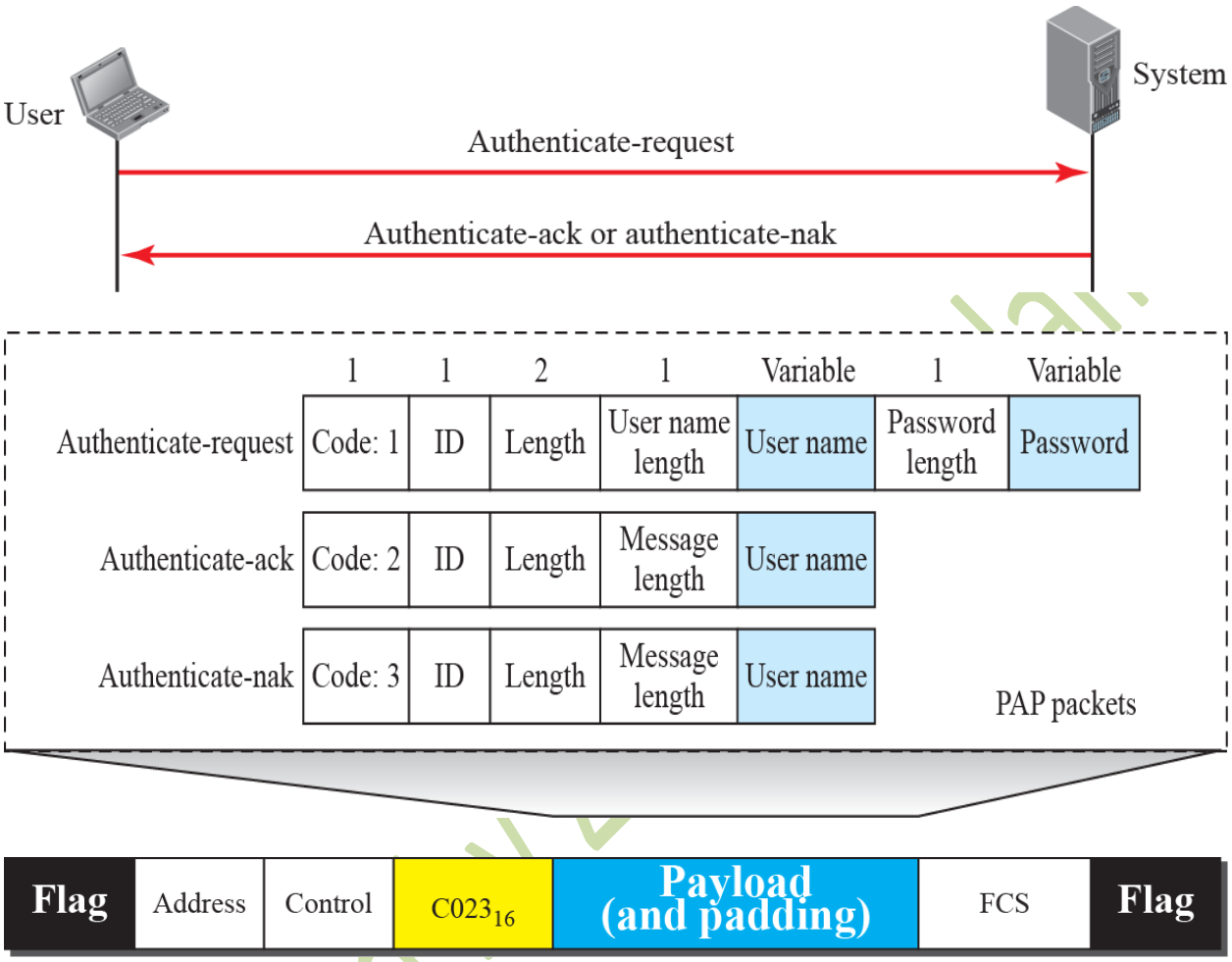
LCP Packets

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

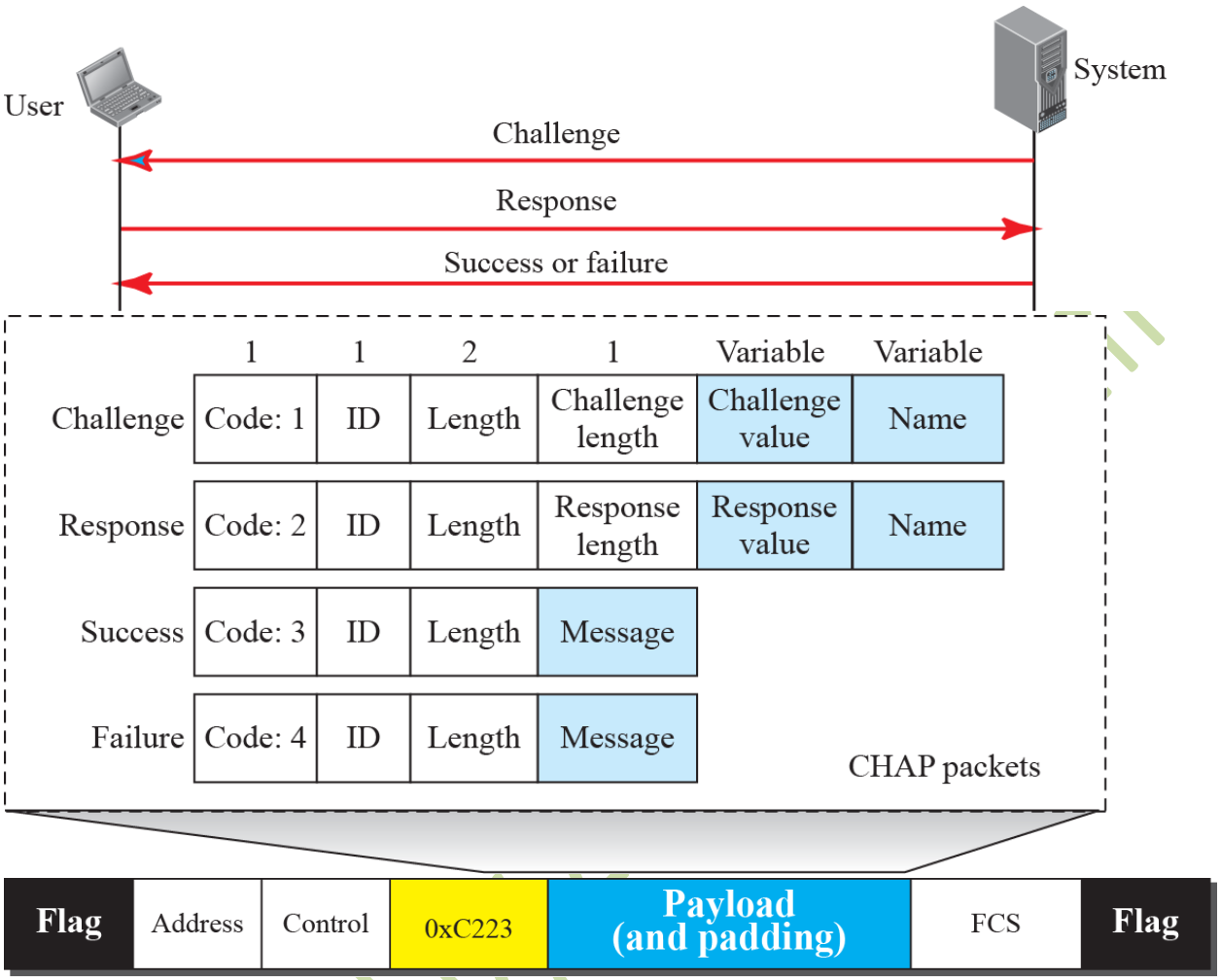
Authentication Protocols in PPP



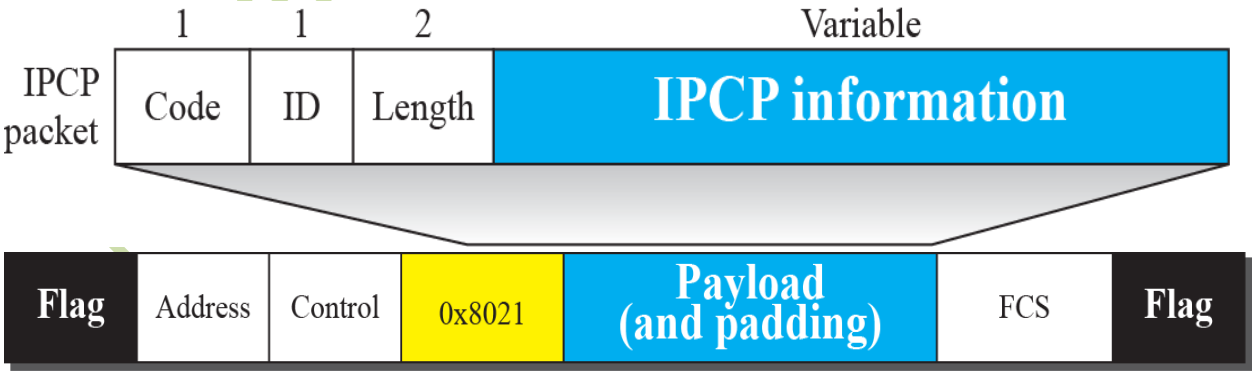
PAP Packets encapsulated in a PPP frame



CHAP Packets encapsulated in a PPP frame



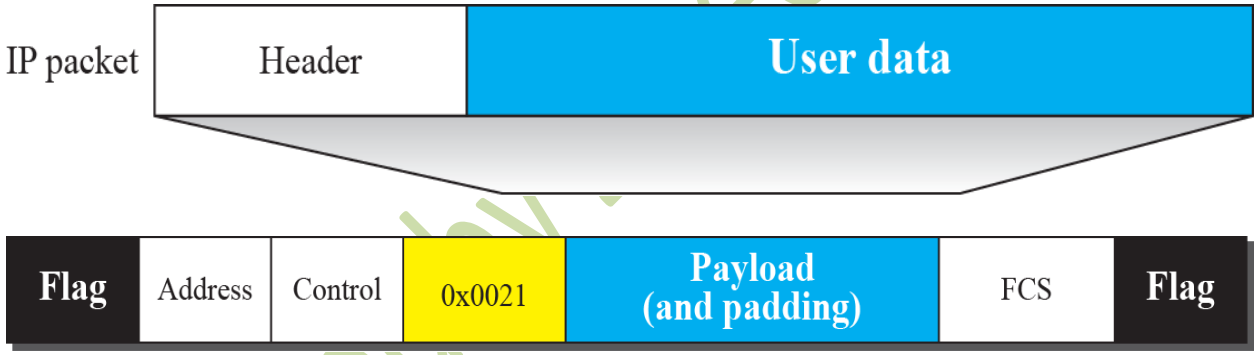
Internet Protocol Control Protocol (IPCP)



Code values for IPCP Packets

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

IP datagram encapsulated in a PPP frame

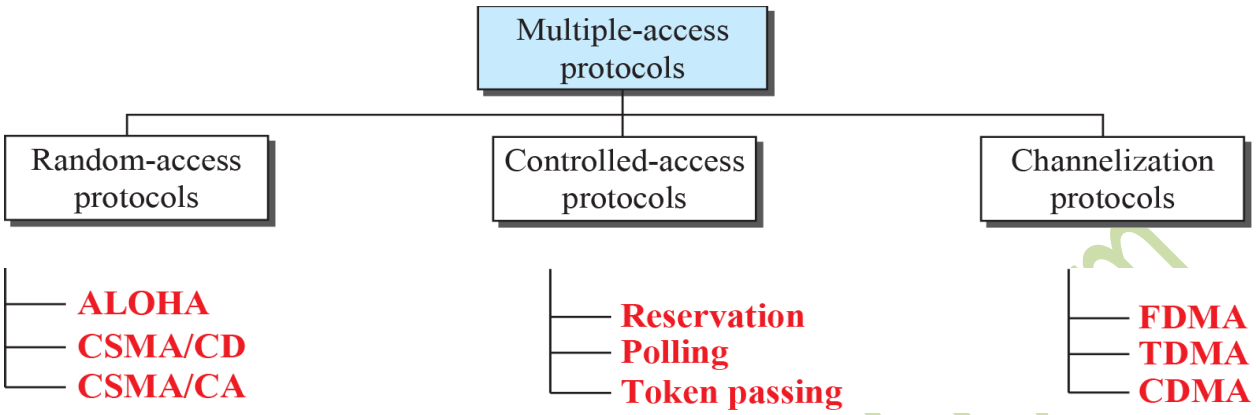


Topic-166
Chap#12

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



Topic 167

Random Access Protocol

- 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).
- It has three types:
  - ❖ Aloha
  - ❖ CSMA/CD
  - ❖ CSMS/CA

Topic 168

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.

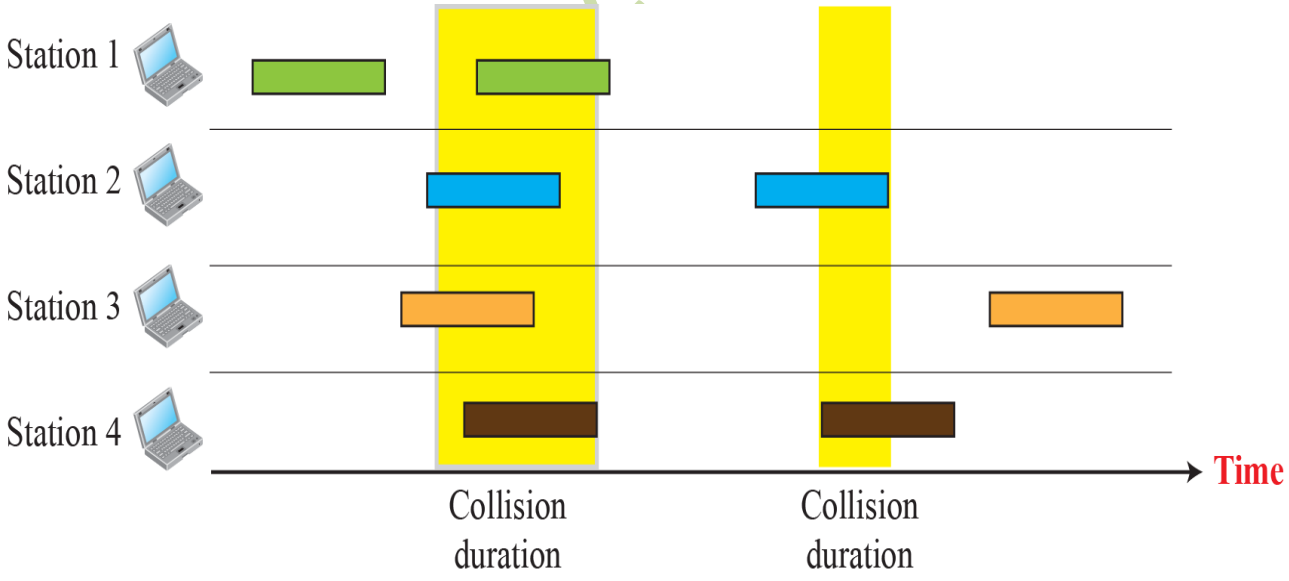
- When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled and we will lose that data.

ALOHA is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sub-layer (MAC sub-layer) of the open systems interconnection (OSI) model. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.

In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy. If the channel is idle, then the frames will be successfully transmitted. If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded. These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

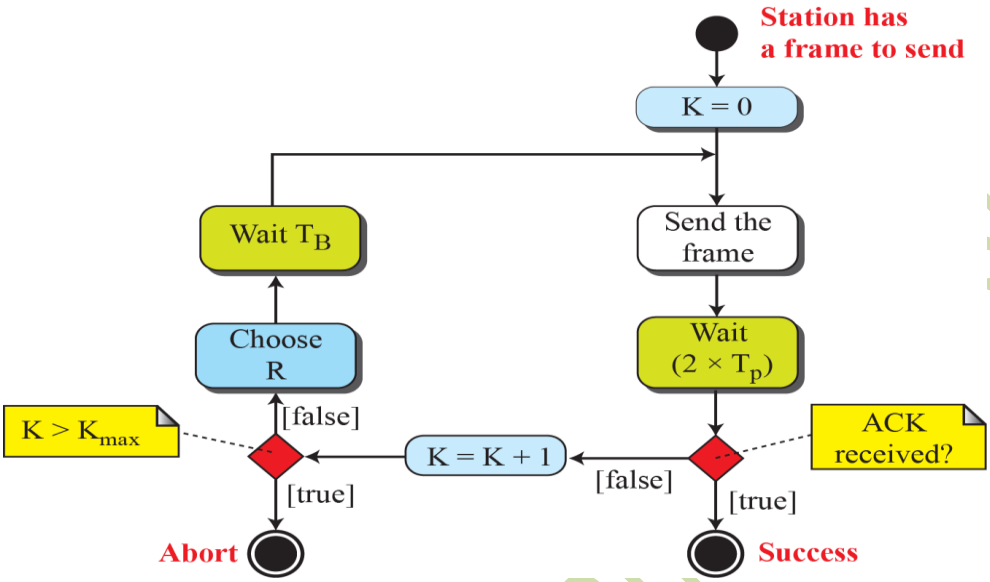
Frames in a pure ALOHA Network:

In pure ALOHA, the time of transmission is continuous. Whenever a station hasn't available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.



Topic 169

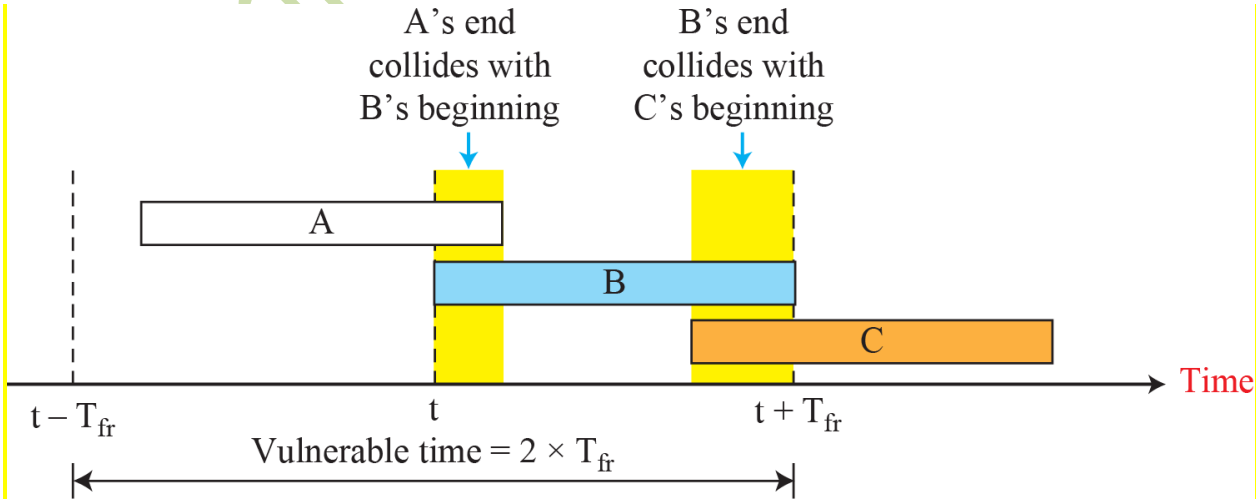
Procedure for pure ALOHA protocol:



Legend

K : Number of attempts
T_p : Maximum propagation time
T_{fr}: Average transmission time
T_B: (Back-off time): $R \times T_p$ or $R \times T_{fr}$
R : (Random number): 0 to $2^K - 1$

Vulnerable Time for pure ALOHA protocol:



Topic 170

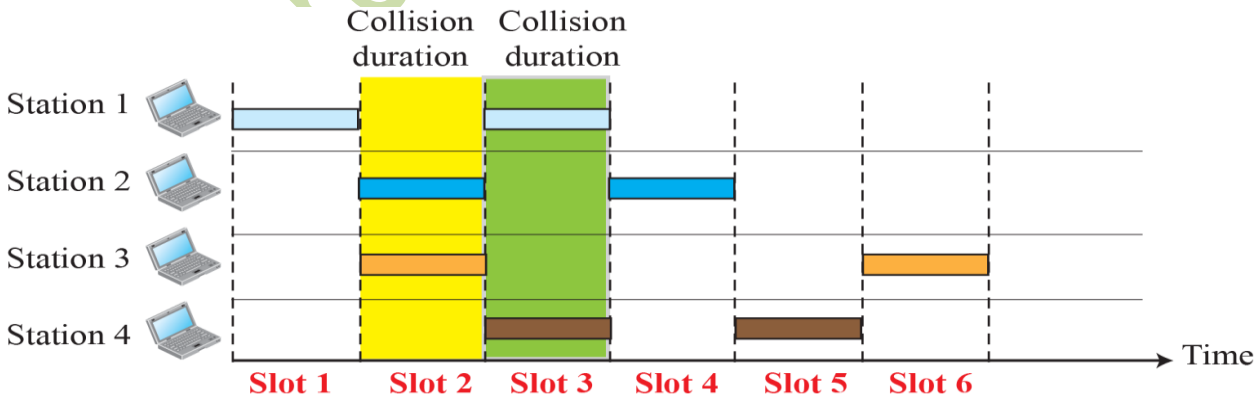
Slotted ALOHA:

- We divide time into slots of Tfr 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 Tfr (vs. 2 x Tfr for pure ALOHA)

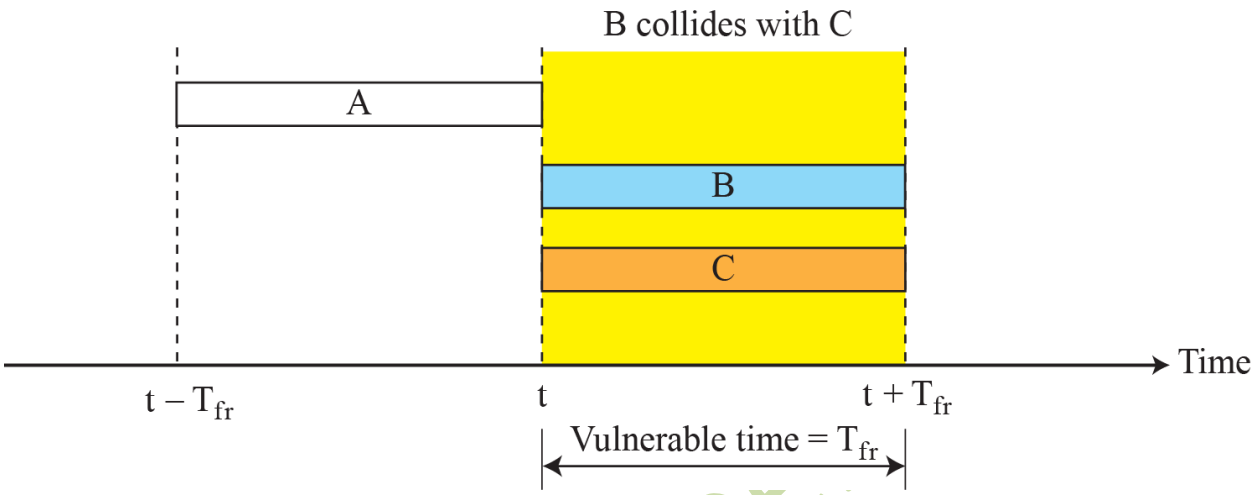
The communicating stations agree upon the slot boundaries. Any station can send only one frame at each slot. Also, the stations cannot transmit at any time whenever a frame is available. They should wait for the beginning of the next slot.

However, there still can be collisions. If more than one frame transmits at the beginning of a slot, collisions occur. The collision duration is 1 slot. The situation is depicted in the following diagram.

Frames in a Slotted ALOHA Network:



Vulnerable Time for Slotted ALOHA:



Topic 171

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'.

CSMA / CD (Career Sense Multiplus / Collision Detection) is a way to control media access that was widely used in early Ethernet technology / LAN, when shared bus topology And each node (computer) was connected by coaxial cables. Now a days

Ethernet is full duplex and CSMA / CD is not used because the topology is either star or point to point but still They are supported.

Consider a scenario where there are "n" stations on a link and everyone is waiting for data to be transmitted through this channel. In this case, all N stations will want to access their link / channel to transfer their data. The problem arises when more than one station transmits data at a time. In this case, the data from different stations will clash.

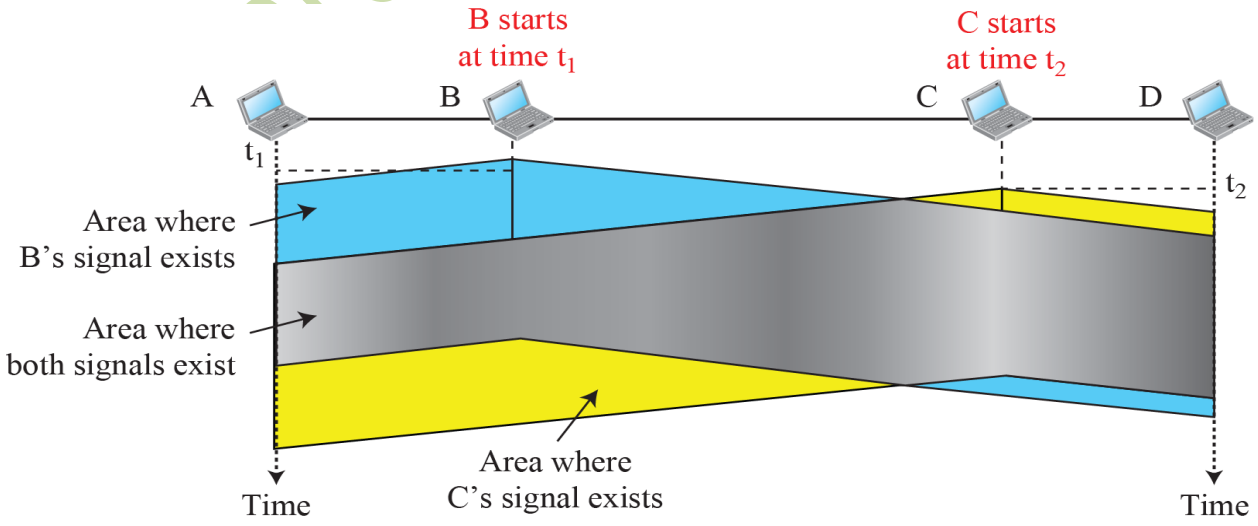
CSMA / CD is one such technique where the various stations following this protocol agree on certain conditions and collision detection measures for effective transmission. This protocol decides which station to move when the data reaches its destination without any corruption.

But even this technique doesn't completely eliminate collisions because propagation delay.

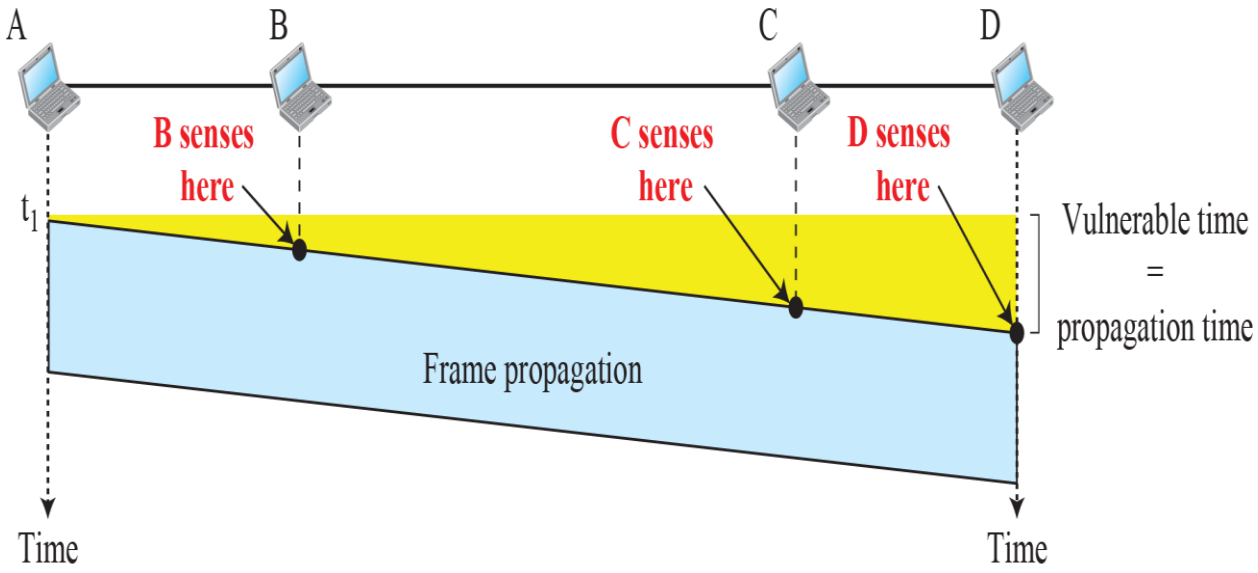
When a station sends a frame in CSMA/CD it still takes some time before this frame gets to all the other stations that are sharing the medium.

The time that takes first bit of a frame that sent on medium to reach all the other stations is called propagation delay.

Space/Time Model of a Collision in CSMA:



Vulnerable Time in CSMA:



Behavior of Three Persistence Methods:

I-persistence:

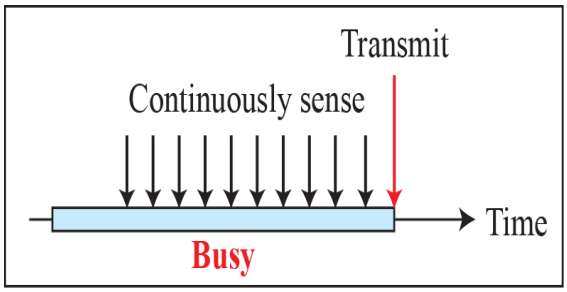
This is a simplest method. In this method after the station find link ideal it sends immediately without waiting. This method has got highest chance of collision.

Non-persistence:

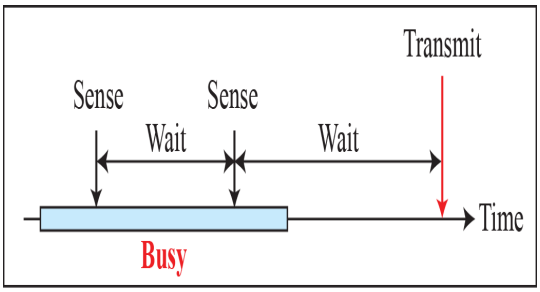
In this method the channel has time slots. A station that has frame to send, it sense the link. If the link is Idle it send frame immediately. If links are not idle, it waits for a random amount of time and the sense that link again. So Collision rate in this case goes down as compared to I-persistence but the efficiency goes also down.

P-persistence:

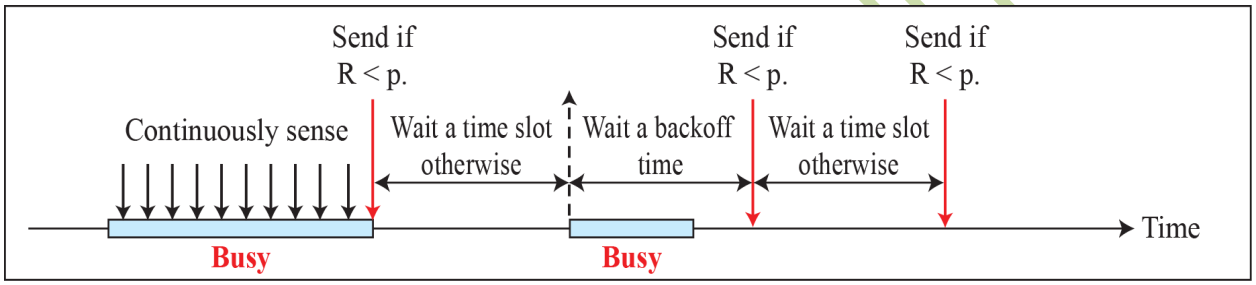
In this case we have got a slot duration which is equal to or greater than the maximum propagation time. This approach combined the advantages of both I-persistence and Non-persistence.



a. 1-persistent



b. Nonpersistent

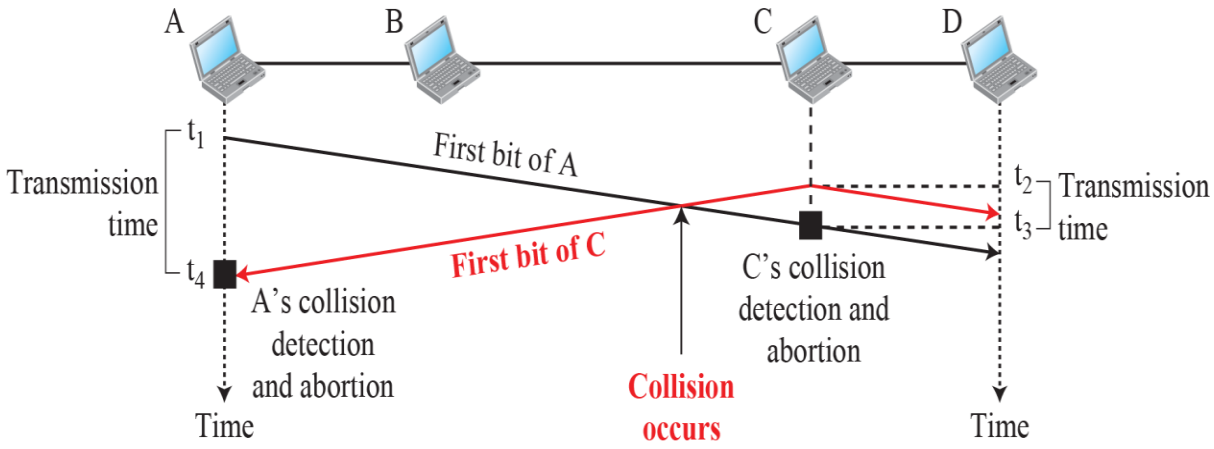


c. *p*-persistent

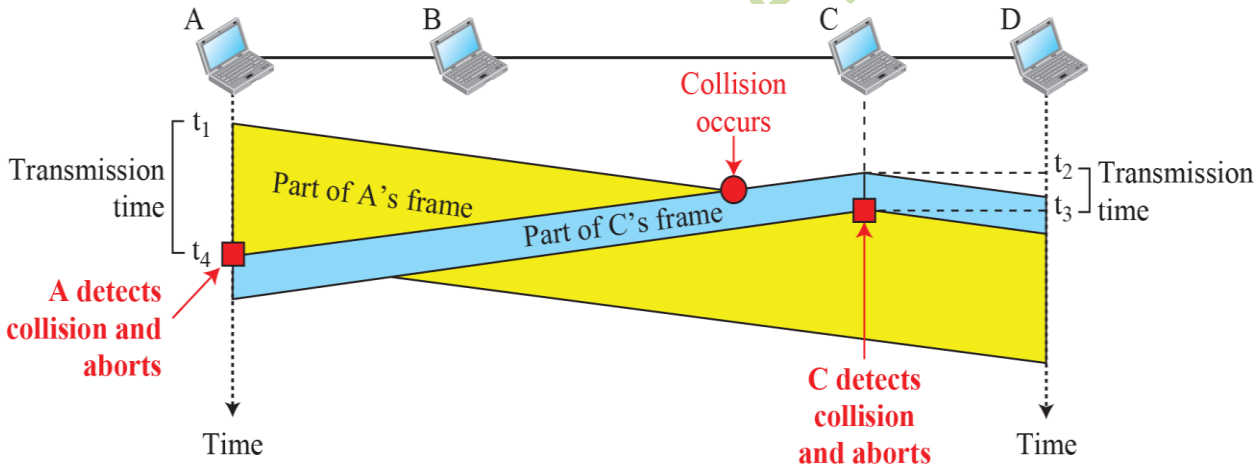
Topic 172

- CSMA method does not specify the procedure following a collision.
- CSMA/CD arguments 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.

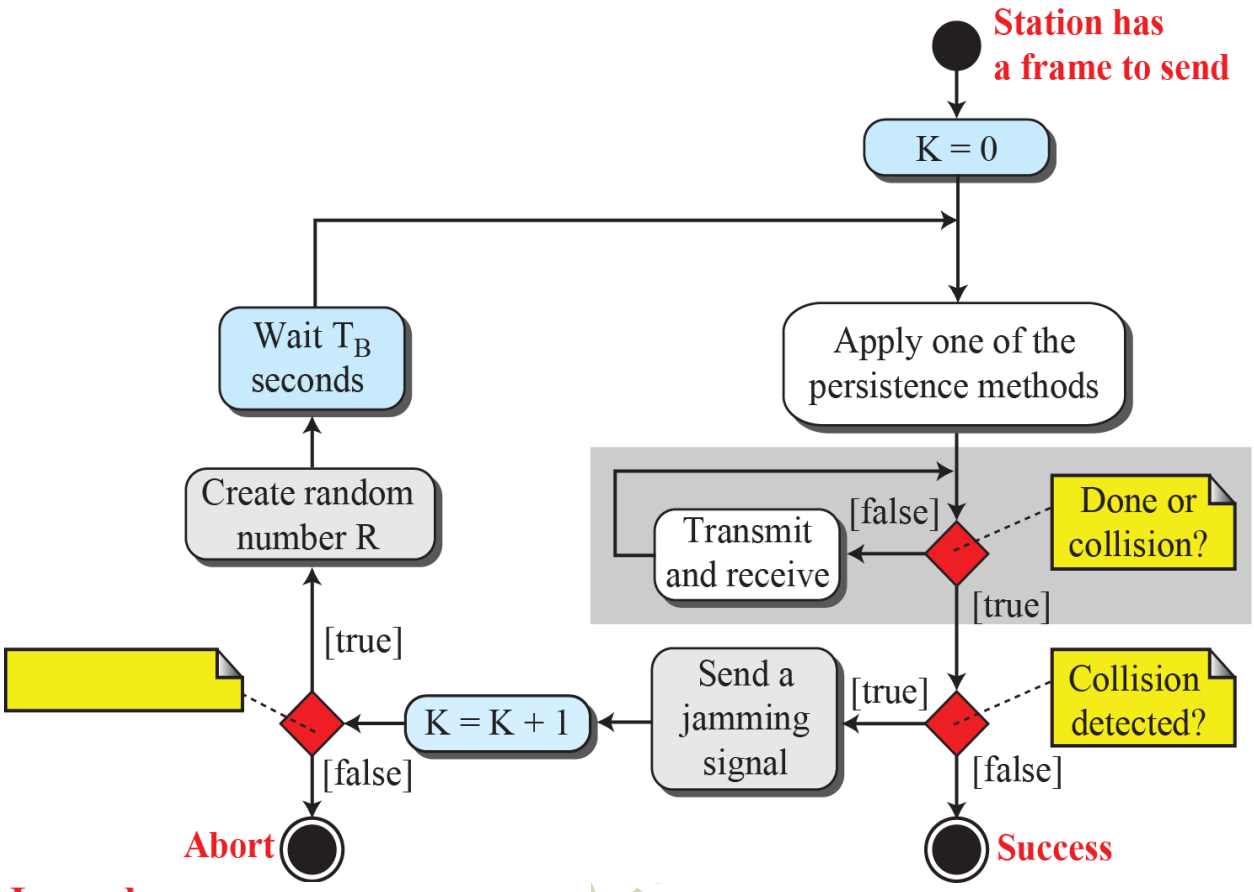
Collision of the First Bits in CSMA/CD:



Collision and Abortion in CSMA/CD:



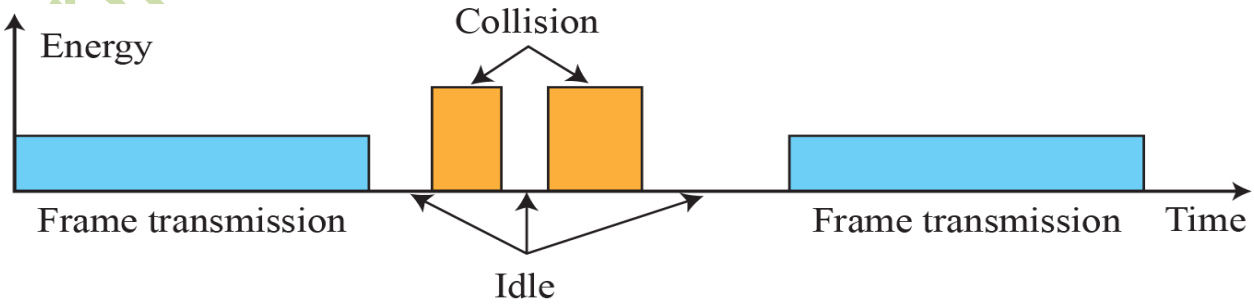
Flow Diagram for the CSMA/CD:



Legend

T_{fr}: Frame average transmission time
K : Number of attempts
R : (random number): 0 to $2^K - 1$
T_B: (Back-off time) = R × T_{fr}

Energy Level During Transmission, Idleness and Collision:



Topic 173

CSMA/CA

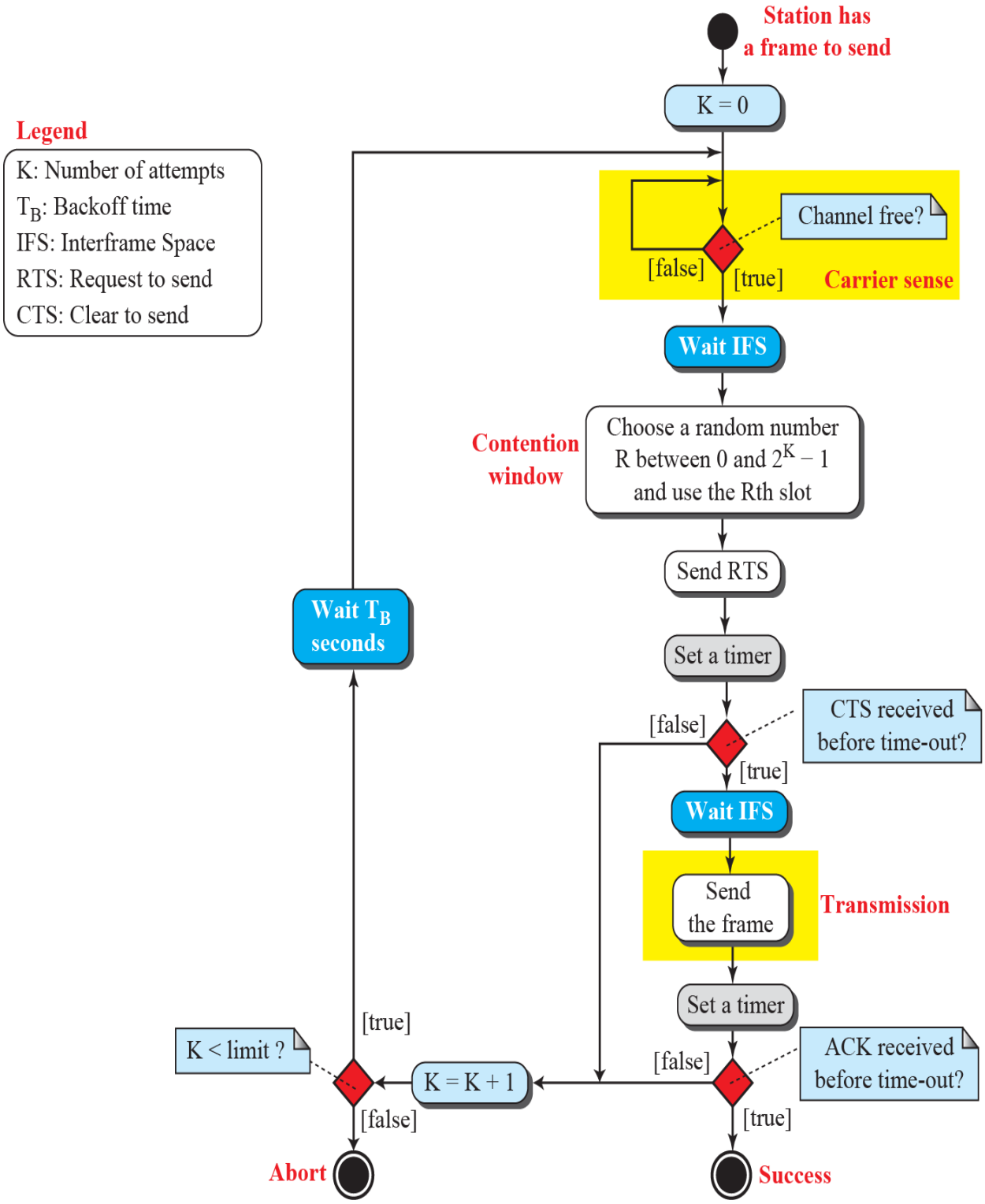
- CSMA/CA was invented for Wireless Networks
- Collisions are avoided through the use of three strategies:
    - The Inter frame Space
    - The Contention Window
    - Acknowledgements

Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".

The algorithm of CSMA/CA is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
- Otherwise, it waits for a back-off time period and restarts the algorithm.

Flow Diagram for CSMA/CA:



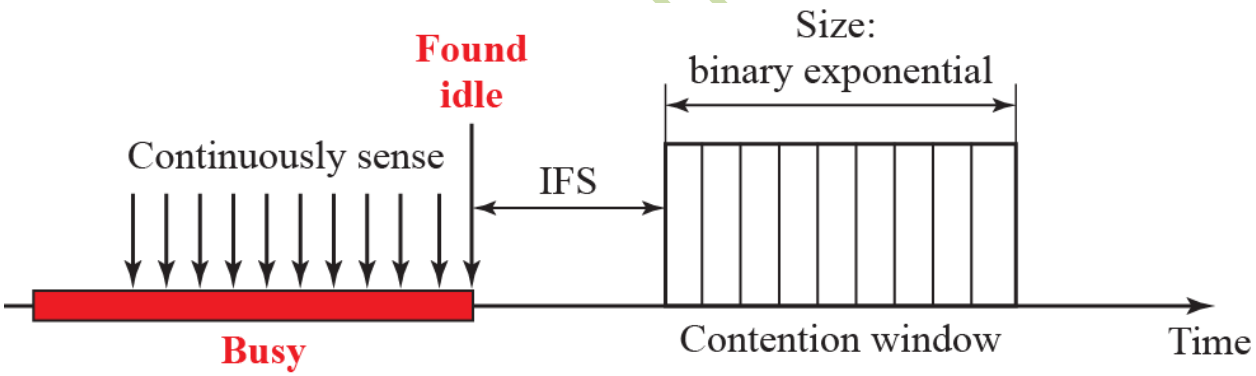
Topic 174

CSMA/CA

- **Inter frame 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)**

Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".

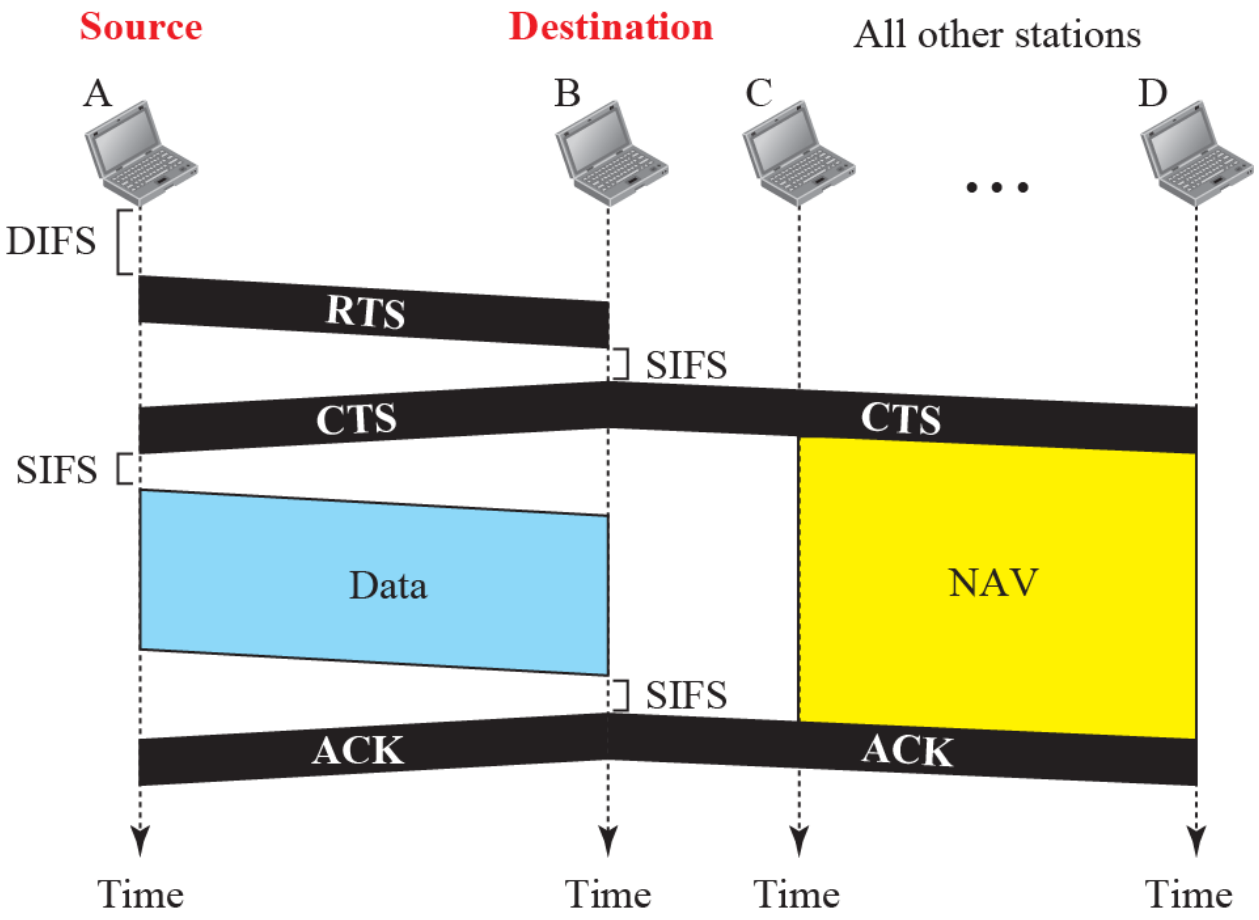
Contention Window



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)



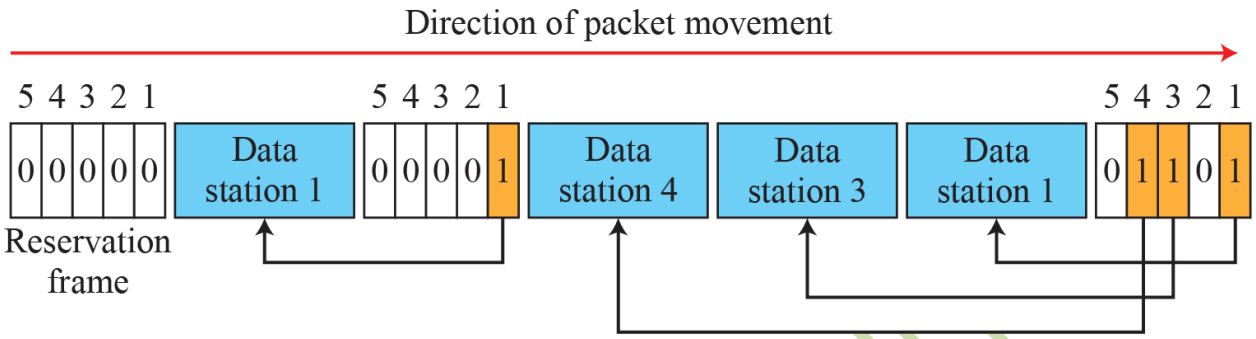
Topic 175

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
- 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

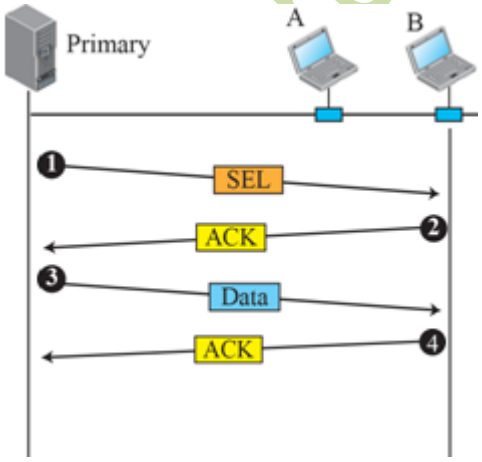


Polling

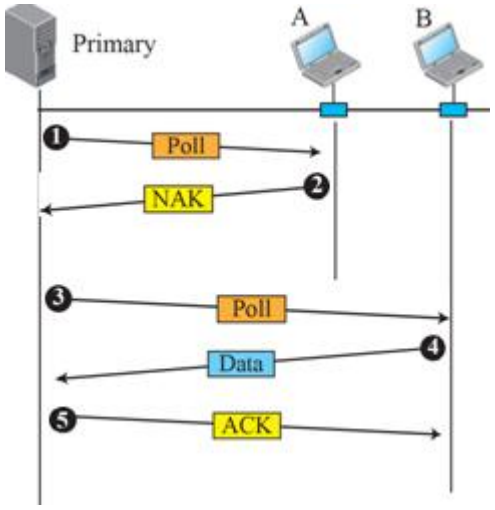
- **Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.**
- **All data exchanges must be made through primary device even when the ultimate destination is a secondary device.**
- **The primary device controls the link; the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

Polling is the process where the computer or controlling device waits for an external device to check for its state.

Select

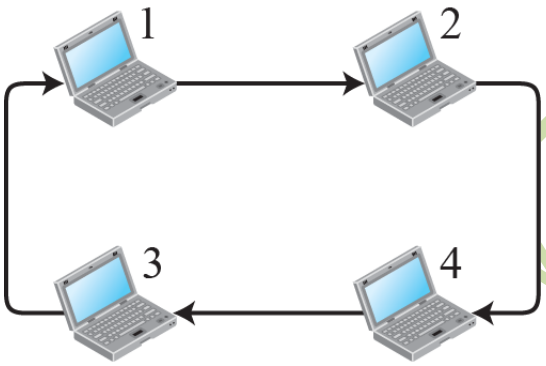


Poll

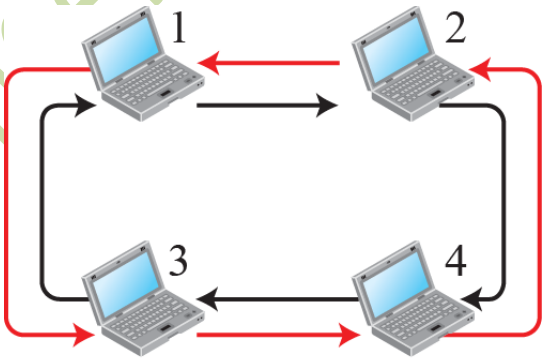


Token Passing

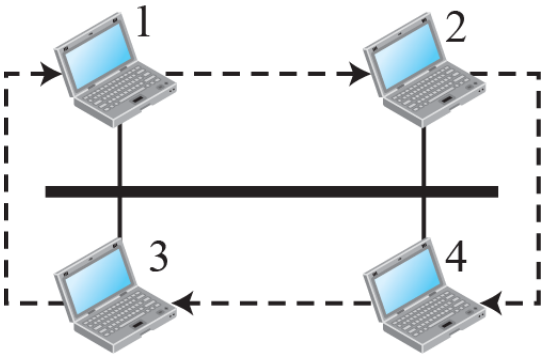
- In the token-passing method, the stations in a network are organized in a logical ring
- For each station, there is a predecessor and a successor
- The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring
-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



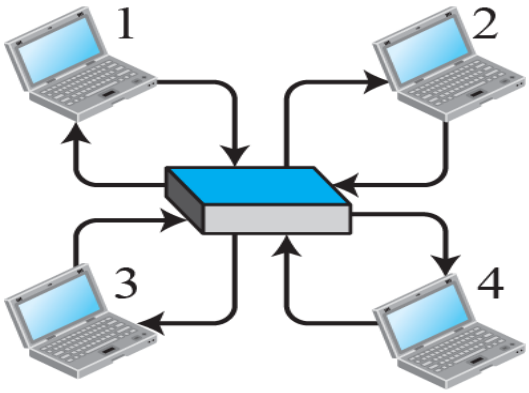
a. Physical ring



b. Dual ring



c. Bus ring



d. Star ring

Topic 177

CHANNELIZATION (Channel Partition)

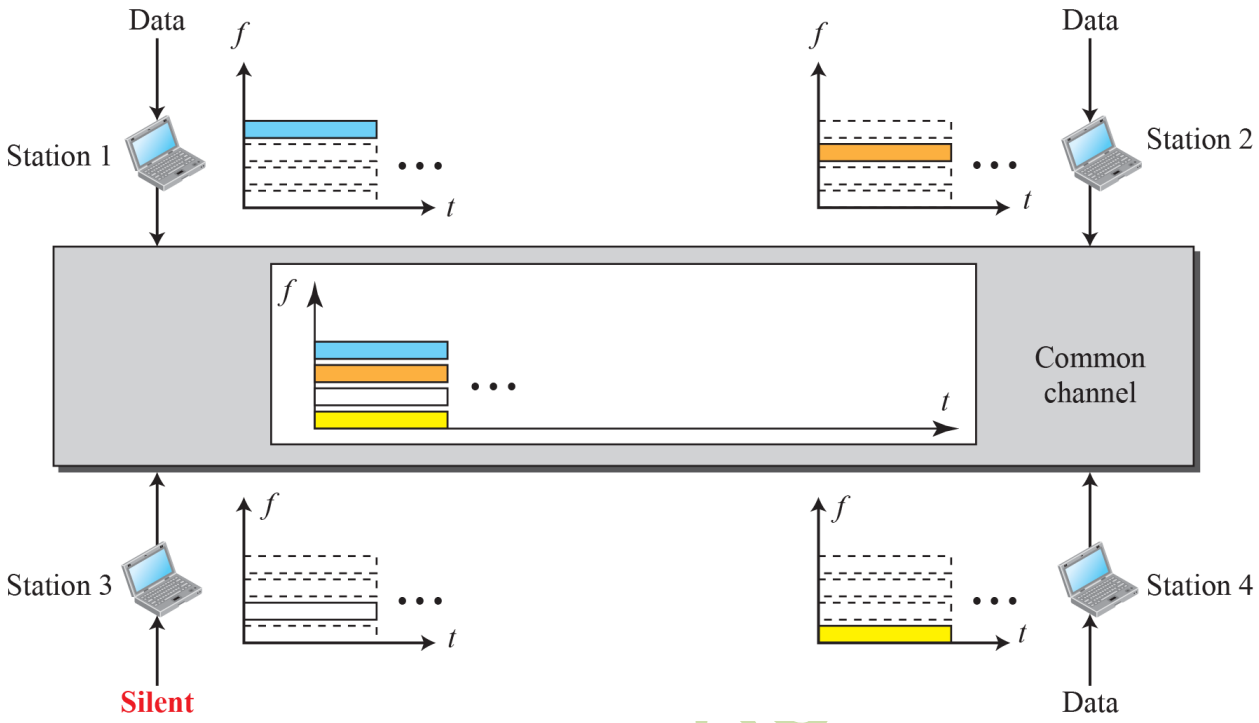
- The available bandwidth of a link is shared in time, frequency, or through code, among different stations
- We discuss three protocols:
    - Frequency Division Multiple Access (FDMA)
    - Time Division multiple Access (TDMA)
    - Code Division Multiple Access (CDMA)

Frequency-Division Multiple Access (FDMA)

- 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 band pass filter to confine the transmitter frequencies.

Frequency-division multiple access (FDMA) is a channel access method used in some multiple-access protocols. FDMA allows multiple users to send data through a single communication channel, such as a coaxial cable or microwave beam, by dividing the bandwidth of the channel into separate non-overlapping frequency sub-channels and allocating each sub-channel to a separate user. Users can send data through a sub-channel by modulating it on a carrier wave at the sub-channel's frequency. It is used in satellite communication systems and telephone trunk lines.

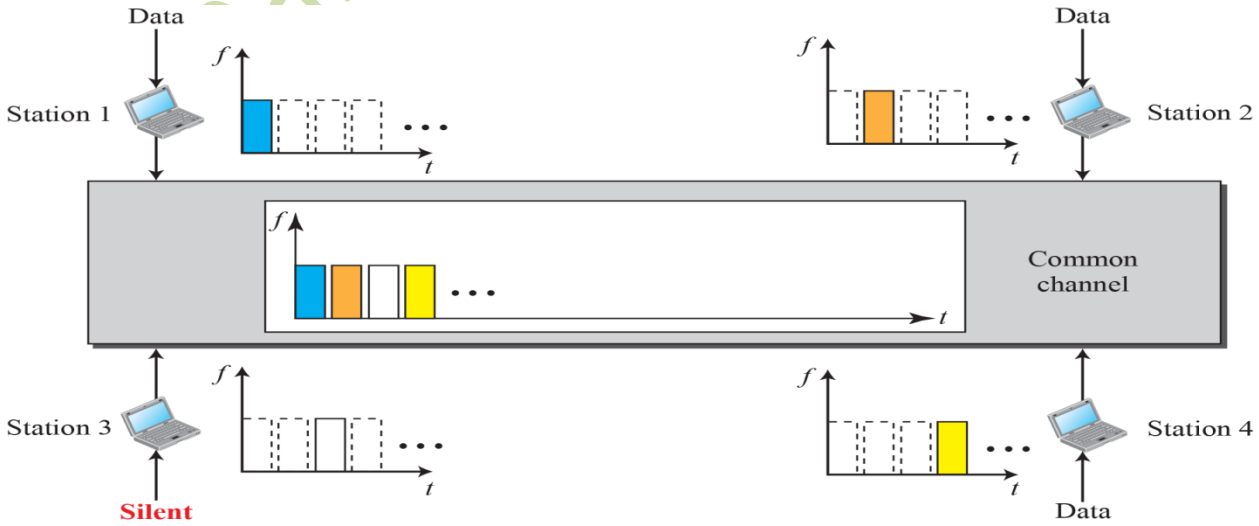
Frequency-Division Multiple Access (FDMA)



Topic 178

TDMA

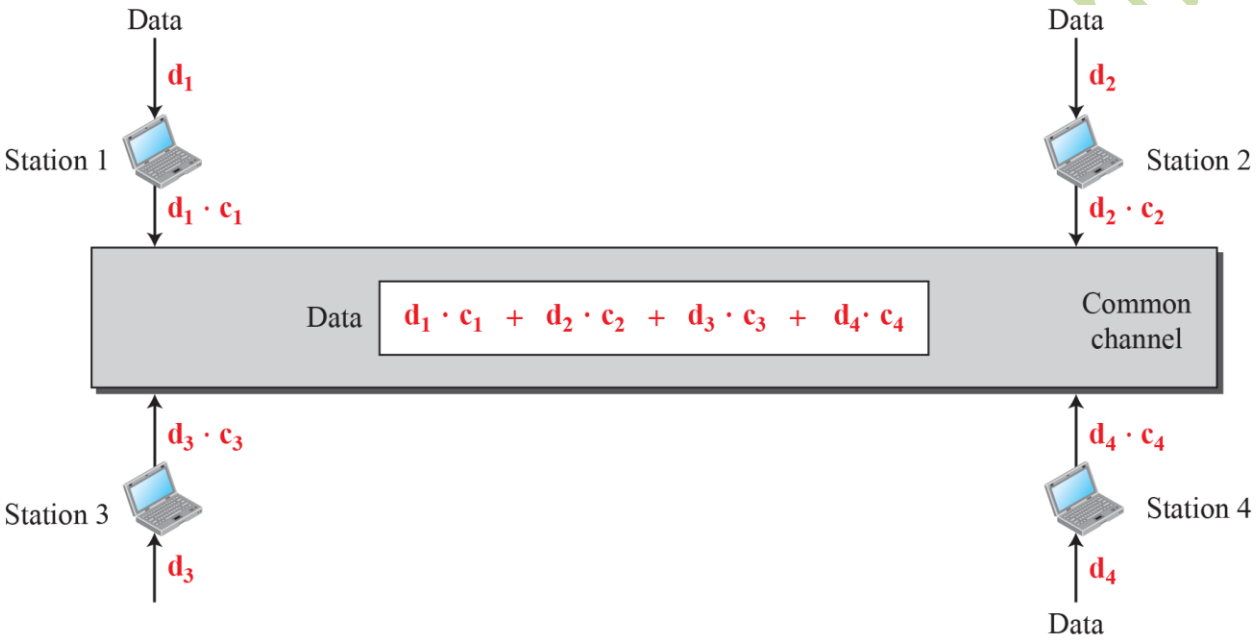
- **Stations share the bandwidth of the channel in time**
- **Each station is allocated a time slot during which it can send data**
- **Each station transmits its data in its assigned time slot**



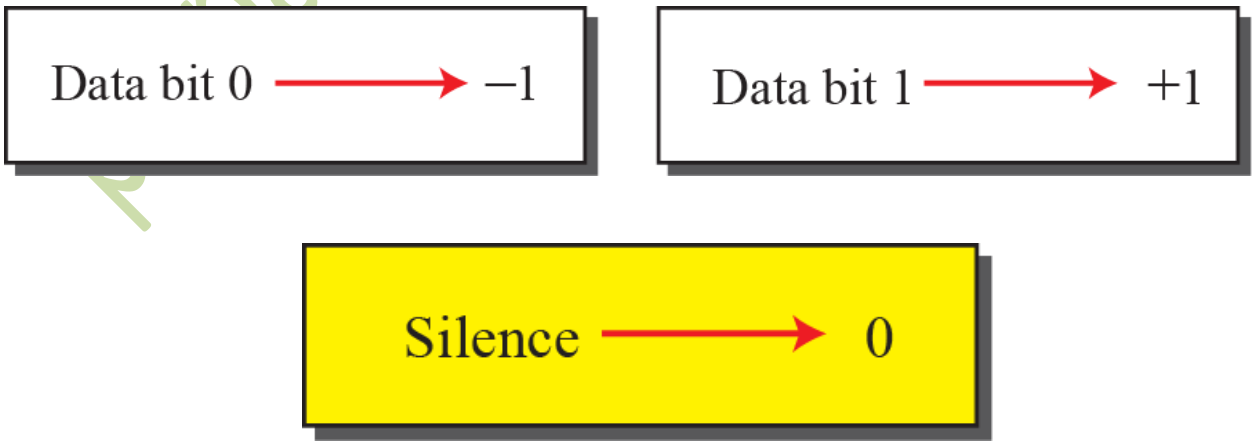
Topic 179

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.



Data Rep-resentation in CDMA



TOPIC 180
Chap..#..13

If two computers send data at the same time, a collision will occur. When this happens, the data sent is not usable. In general, both computers will stop sending, and wait a random amount of time, before they try again. A special protocol was developed to deal with such problems. It is called CSMA/CD.

Ethernet Protocol

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

Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3. Ethernet has since been refined to support higher bit rates, a greater number of nodes, and longer link distances, but retains much backward compatibility. Over time, Ethernet has largely replaced competing wired LAN technologies such as Token Ring, FDDI and ARCNET.

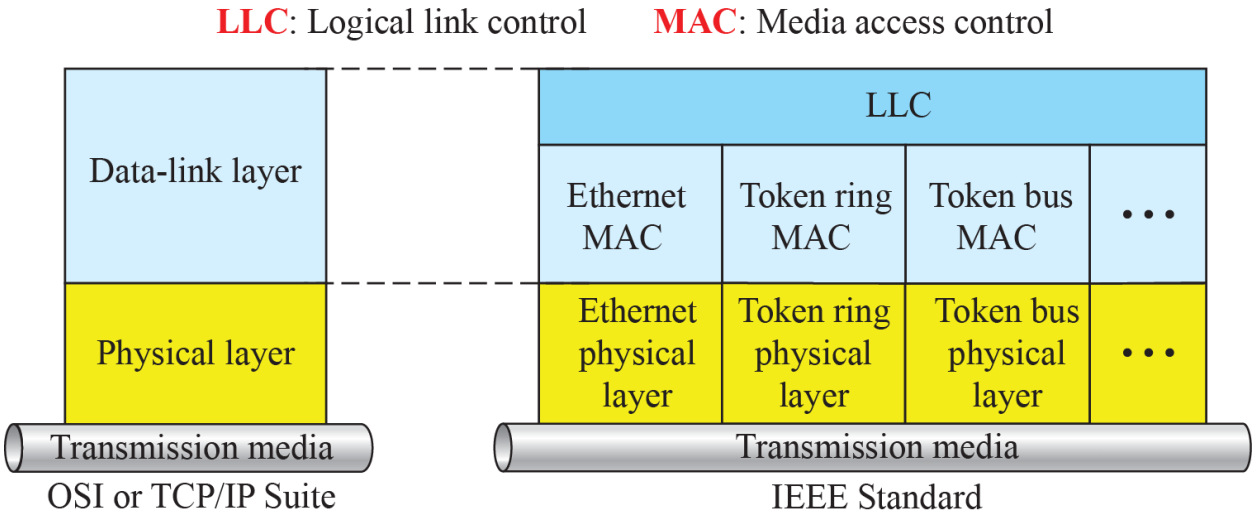
It is a way of connecting computers together in a LAN. It has been the most widely used method of linking computers together in LANs since the 1990. The basic idea of its design is that multiple computers have access to it and can send data at any time.

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

IEEE 802 is a family of **Institute of Electrical and Electronics Engineers** (IEEE) standards for LAN, PAN, and MAN. The IEEE 802 LAN/MAN Standards Committee (LMSC) maintains these standards. The IEEE 802 family of standards has twelve members, numbered 802.1 through 802.12, with a focus group of the LMSC devoted to each.

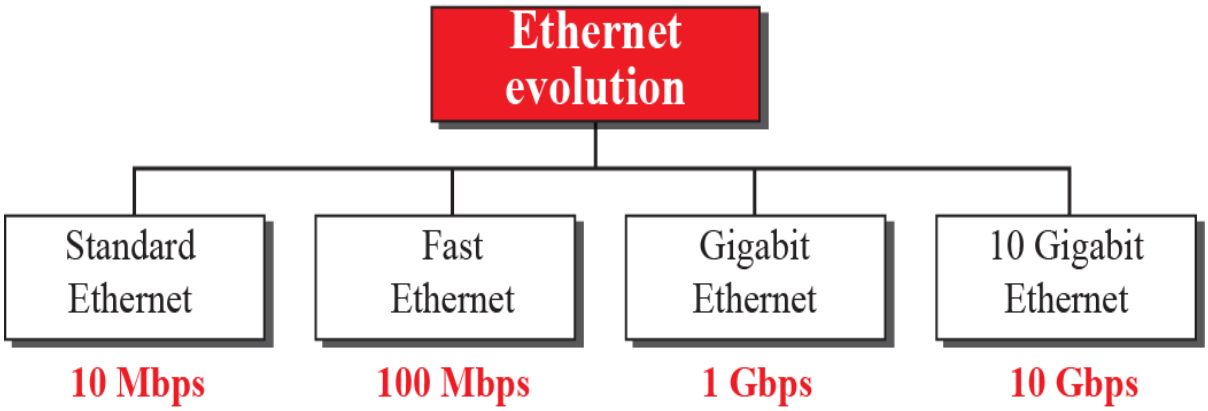
IEEE Standard for LANs



TOPIC 181

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)



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 has not changed during the evolution.

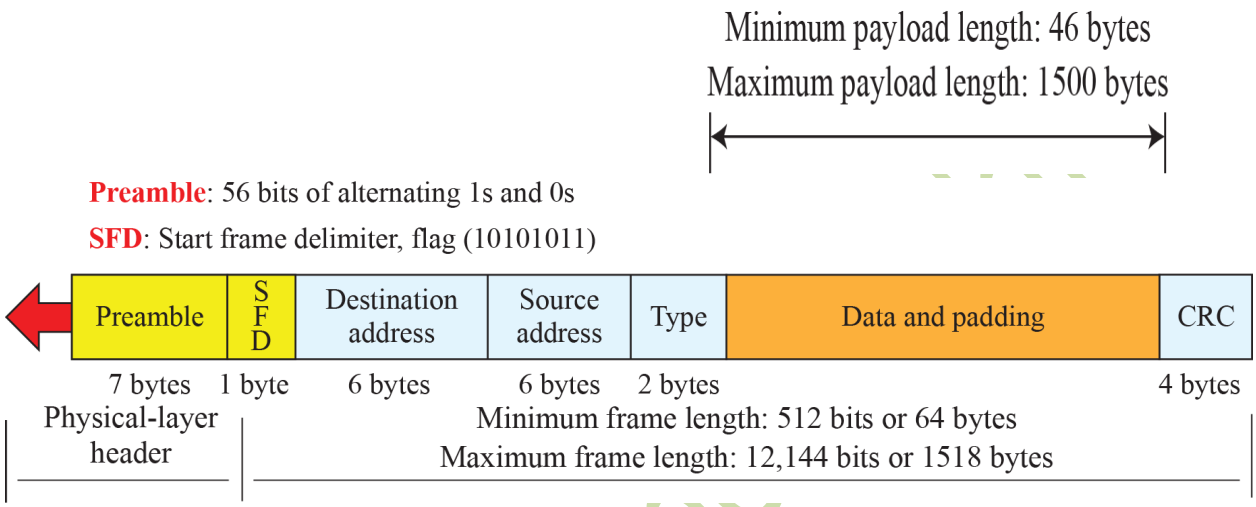
A standard Ethernet network can transmit data at a rate up to 10 Mbps per second. Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and Local Talk.

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

TOPIC 182

Ethernet Frame Format



TOPIC 183

Addressing in Standard Ethernet

- Each station on Ethernet has its own network interface card (NIC).
- Every NIC has got a unique link-layer address.
- 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.
- For example, the following shows an Ethernet MAC address: 4A:30:10:21:10:1A.

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:

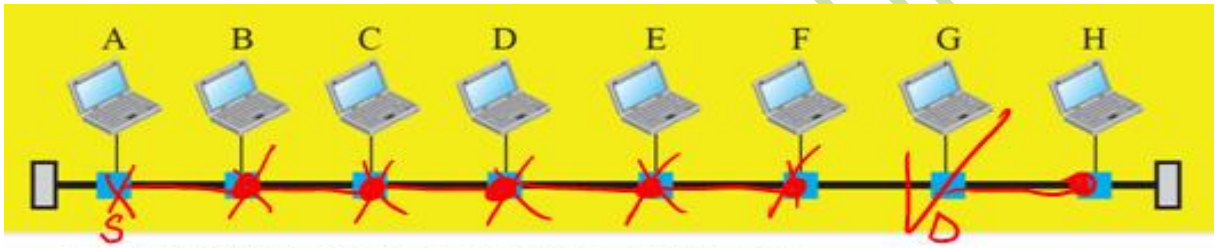
a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are Fs in hexadecimal.

Implementation of Standard Ethernet

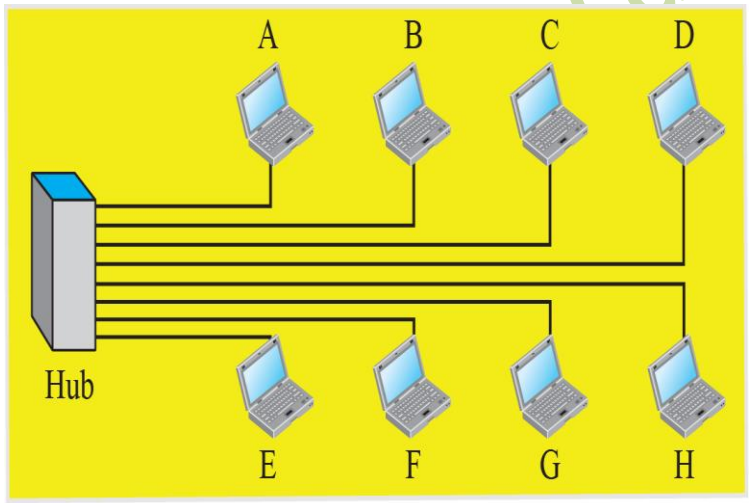
As we know all the frames in Ethernet by nature is broadcast. If the all frame are broadcast then how we know which of the unicast or multicast.

The answer is we know that by specifying the way these frame are actually treated when they reach at destination.

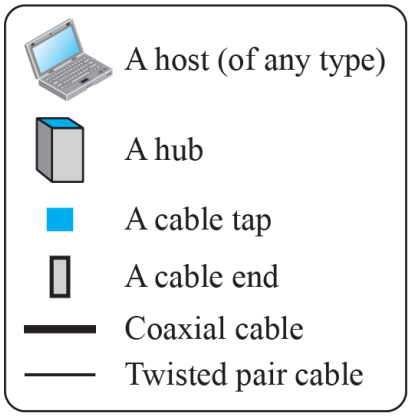
Example:



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



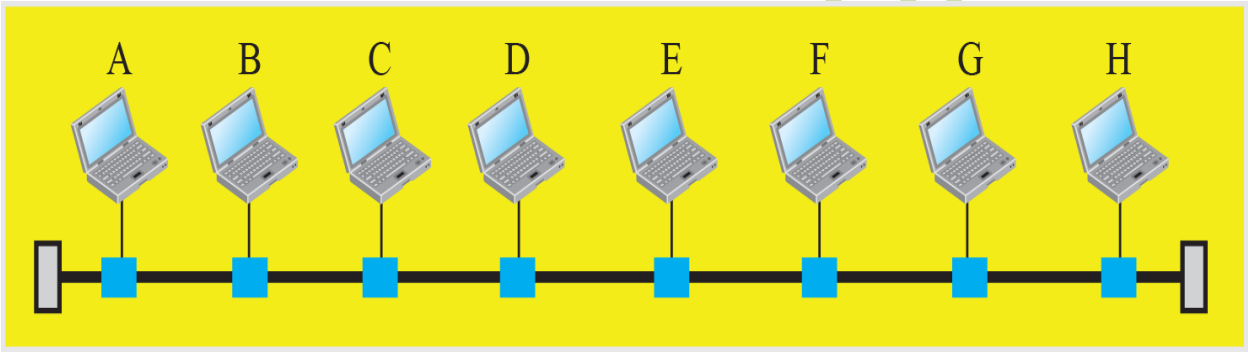
b. A LAN with a star topology using a hub



TOPIC 184

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.



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

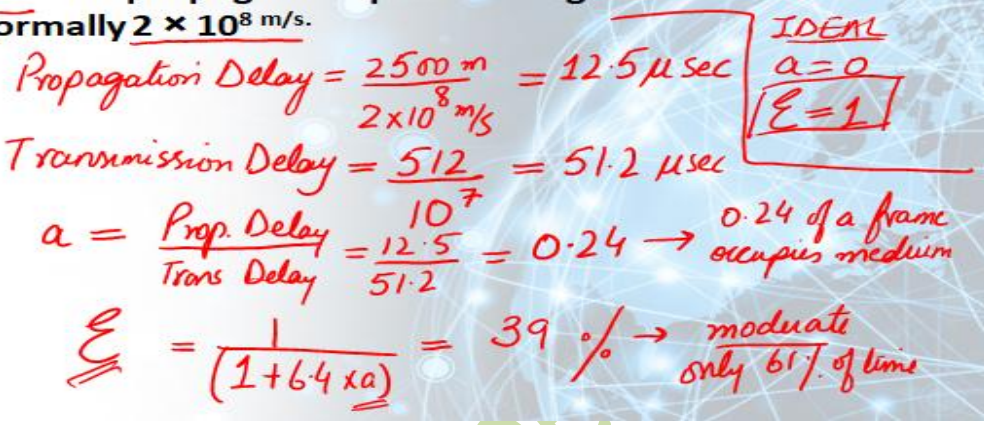
TOPIC 185

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.



TOPIC 186

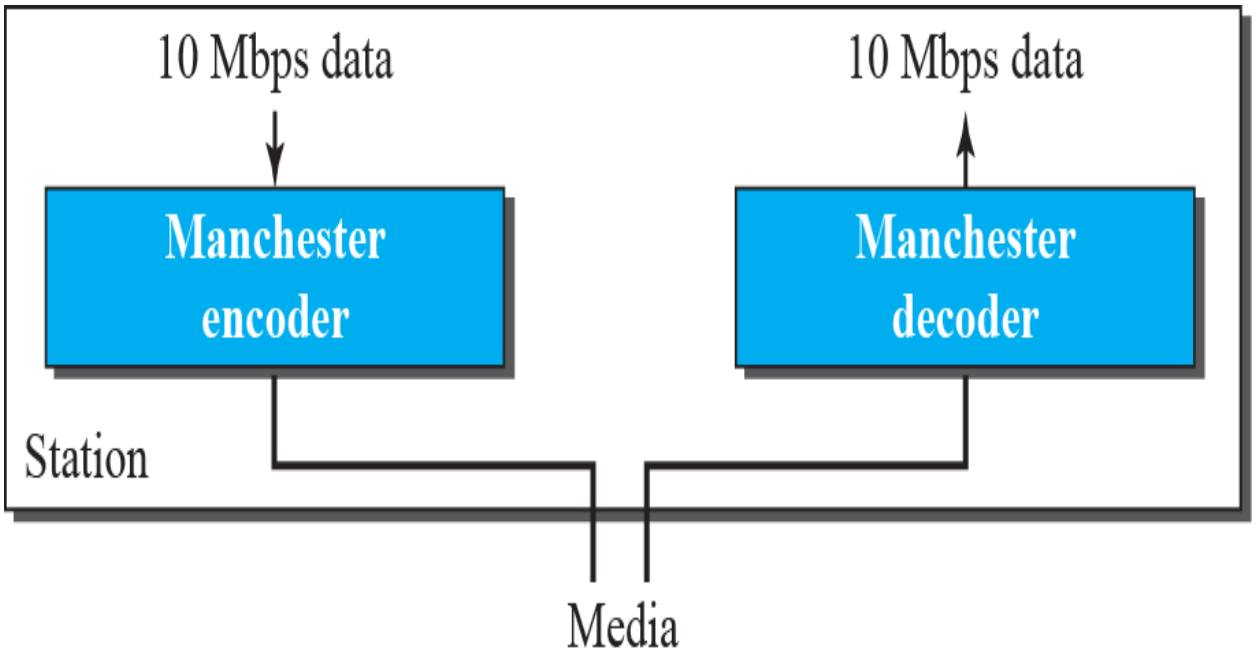
Implementation of Standard Ethernet

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

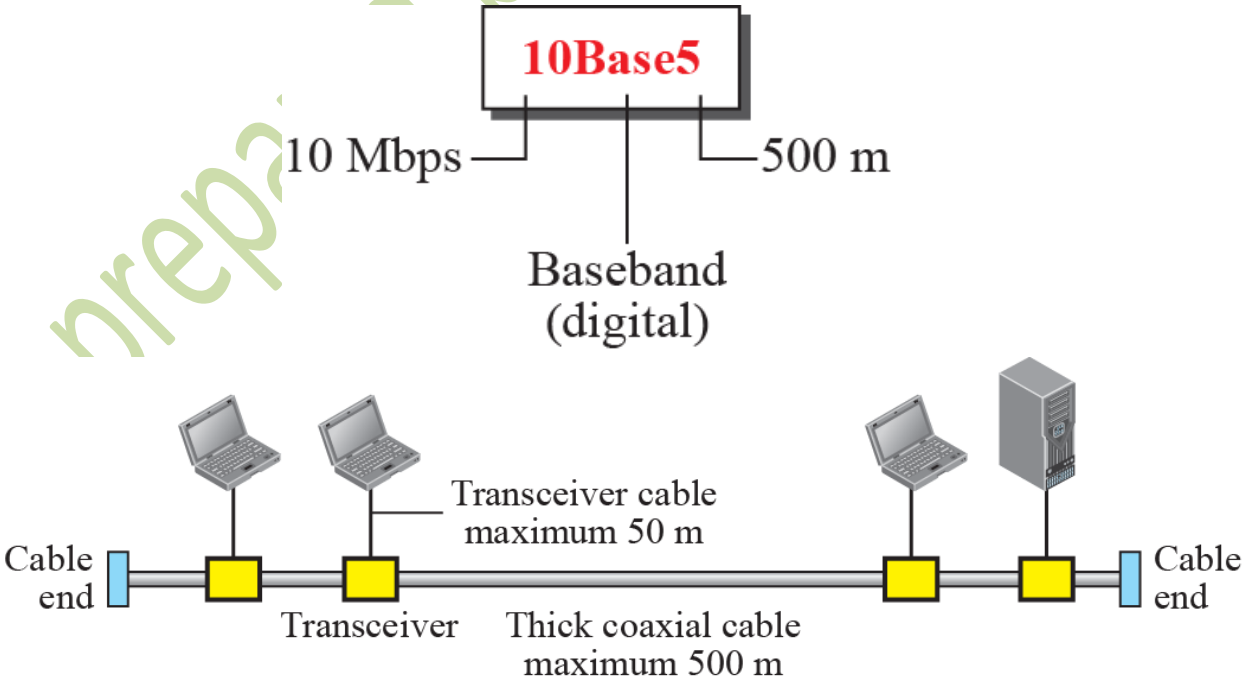
Summary of Standard Ethernet implementations

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

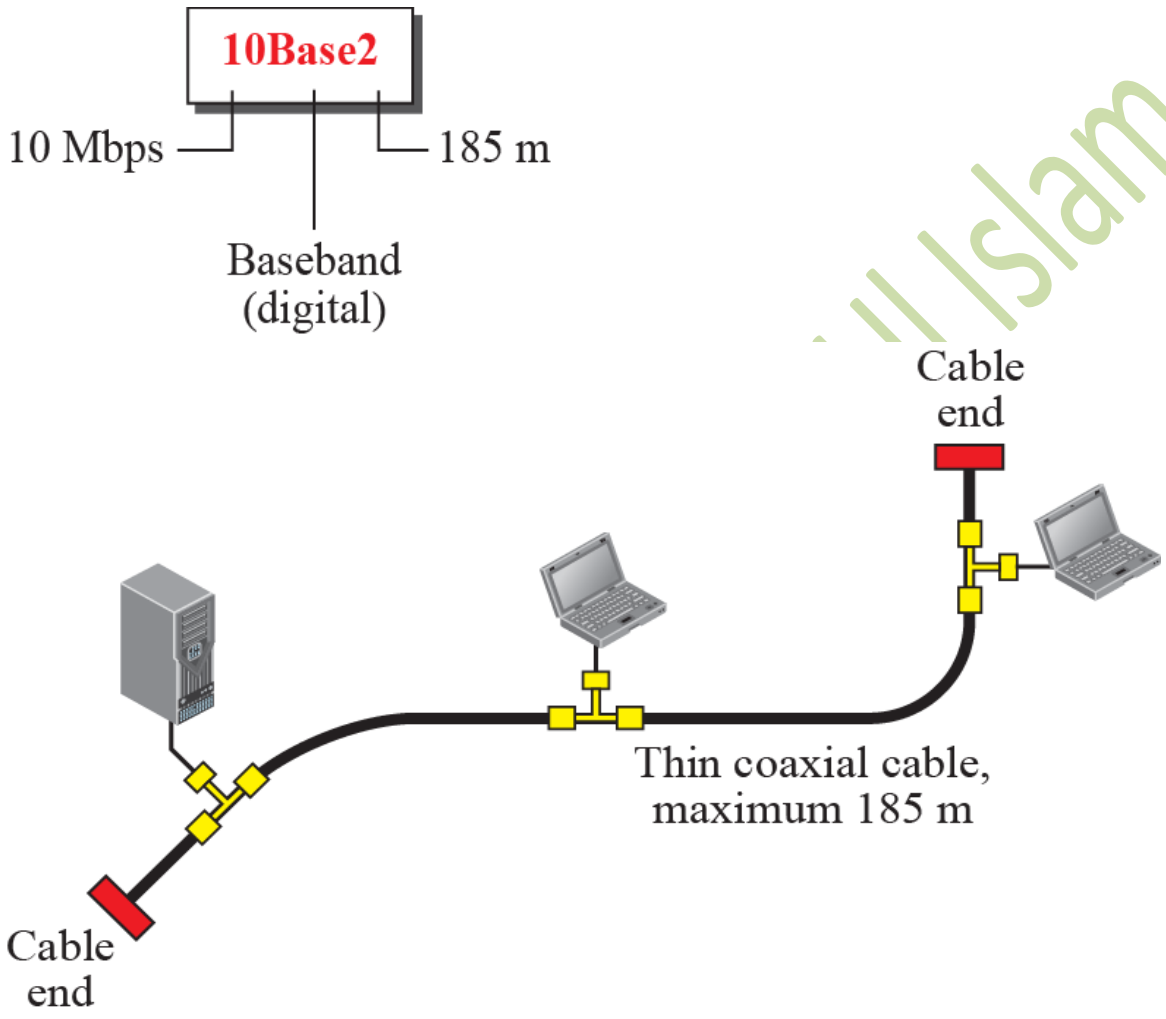
Encoding in Standard Ethernet



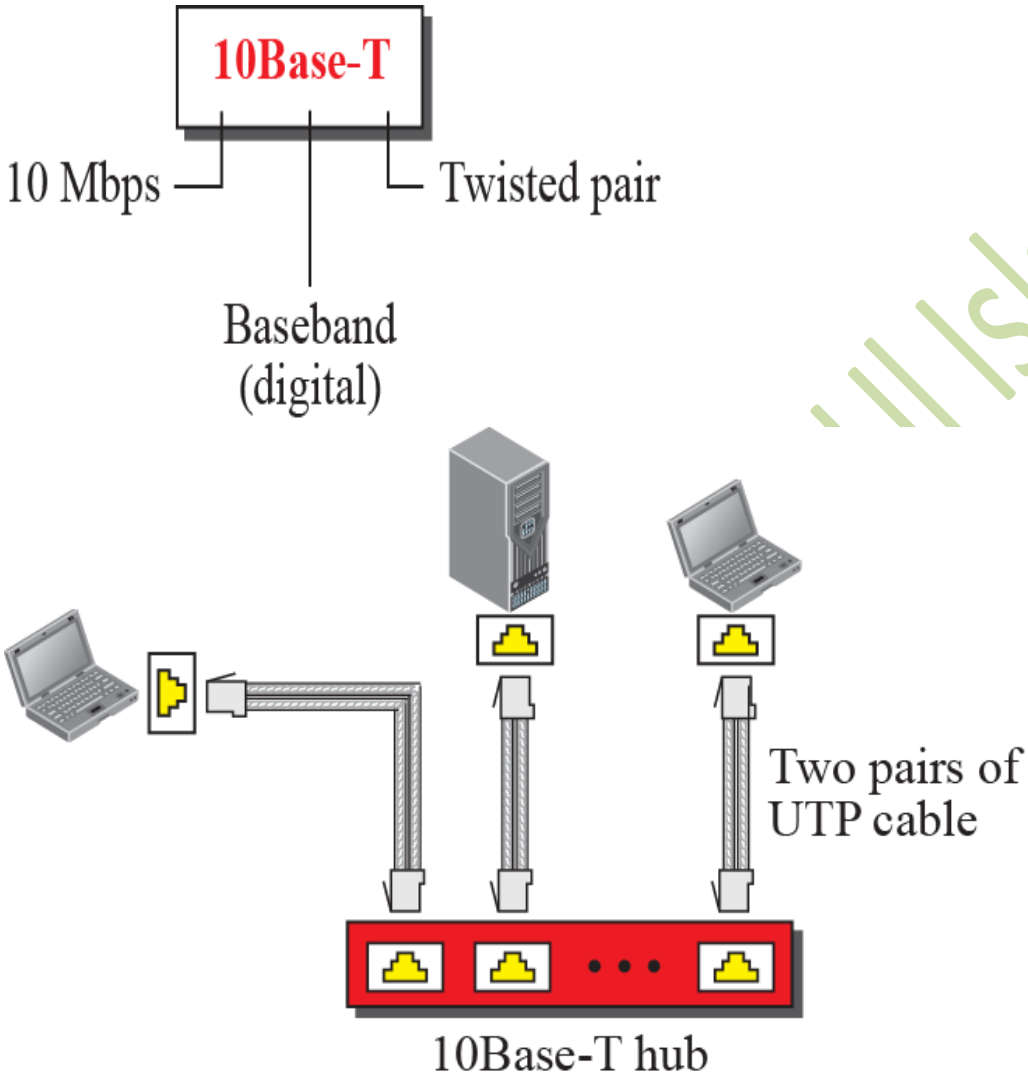
10Base5 Implementation



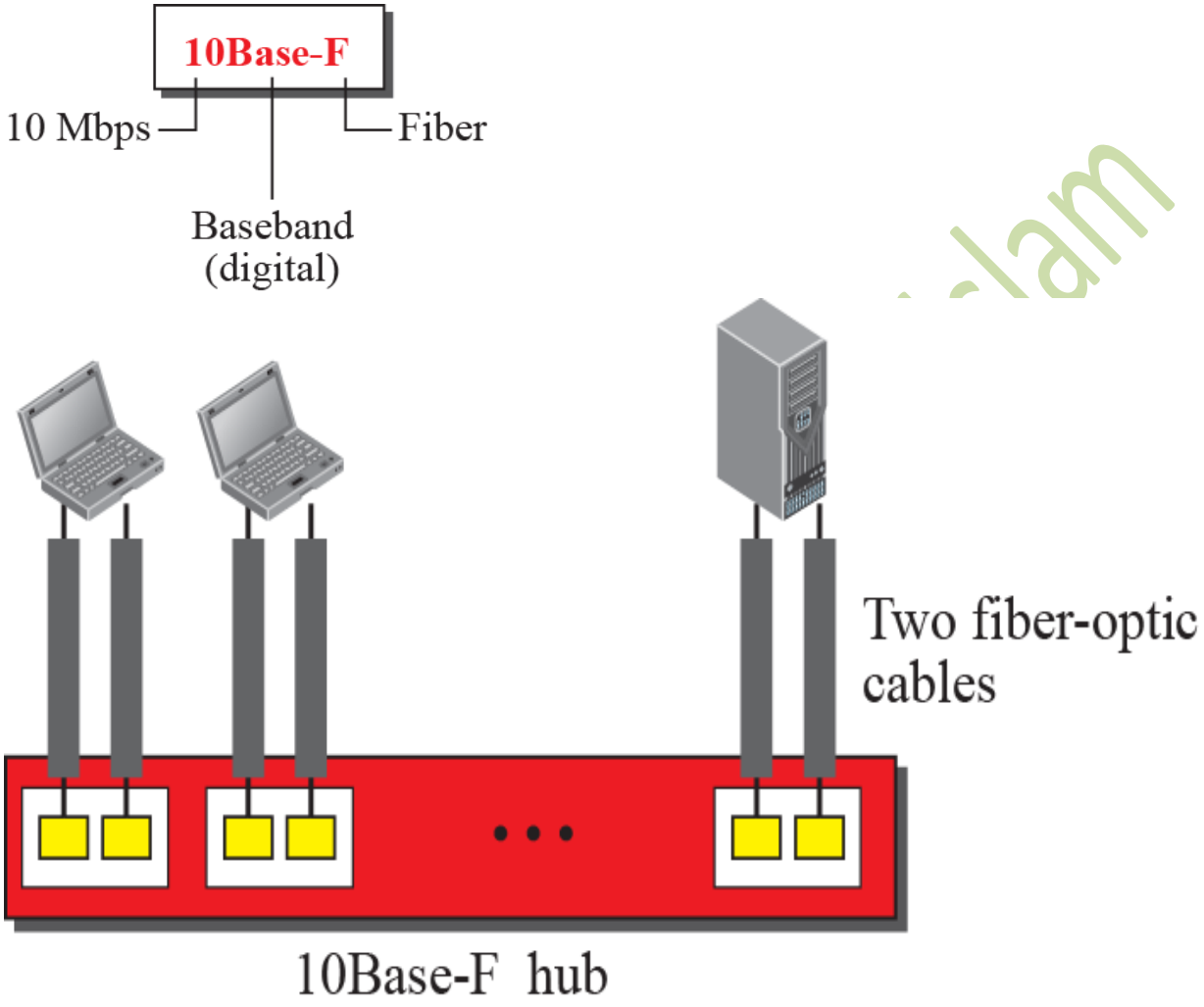
10Base2 Implementation



10Base-T Implementation



10Base-F Implementation

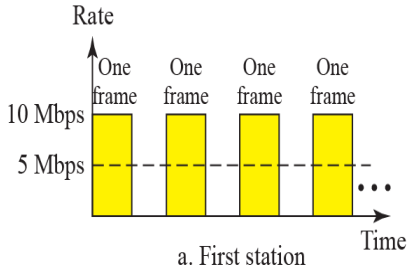


TOPIC 187

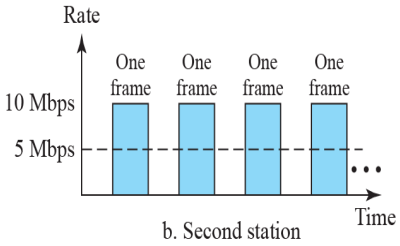
Changes in the Standard

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



a. First station



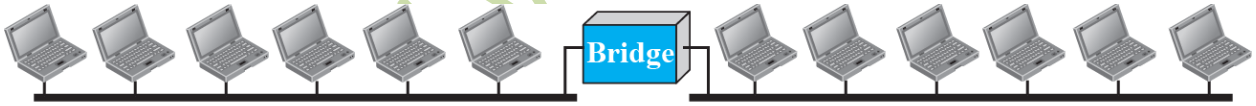
b. Second station

Bridged Ethernet

An Ethernet network bridge is a device which connects two different local area networks together. Both networks must connect using the same Ethernet protocol. Bridges can also be used to add remote computers to a LAN. Many bridges can connect multiple computers or other compatible devices with or without wires**.**

A Network with and without Bridging:

a. Without bridging



b. With bridging

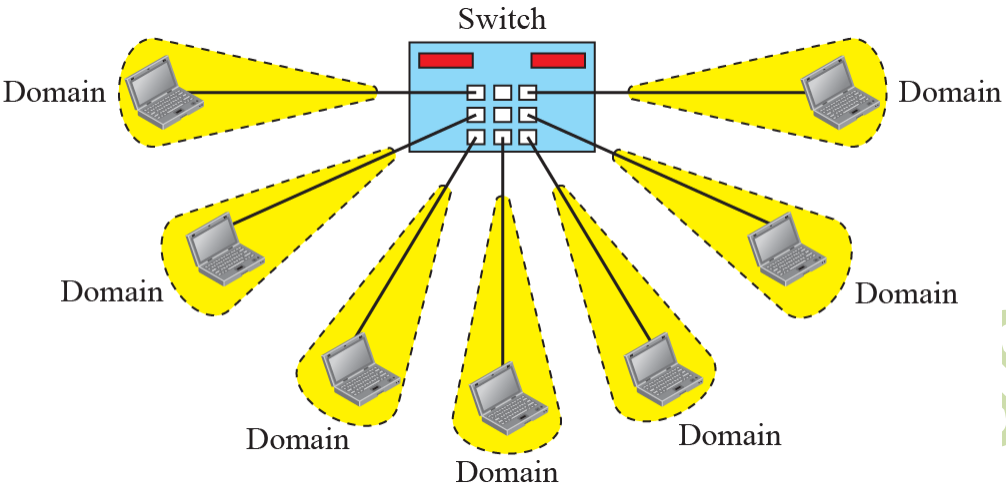
Advantages:

- The basic advantage of bridging is that we can now divide 10Mbps capacity.
- We also separate the collision domains as well.

TOPIC 188

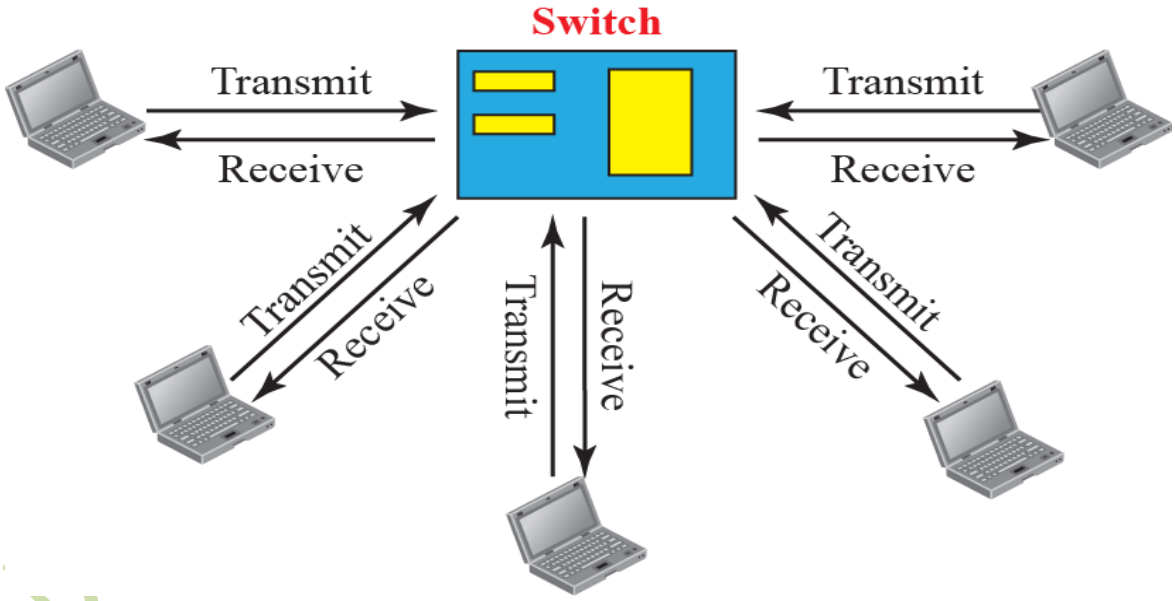
Switched Ethernet:

A network switch (also called switching hub, bridging hub, and, by the IEEE, MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.



Full – Duplex Switched Ethernet (FDSE)

The Ethernet switch or Ethernet FDSE (Full Duplex Switched Ethernet), was born in the early 1990s before the advent of switched Ethernet, shared Ethernet networks were cut into shared subnets autonomous, interconnected by bridges. Therefore, the traffic was multiplied by the number of subnets.



Advantages of FDSE

- This increases the direct capacity from 10MBS to 20MBS.
- Instead of using one link between stations, we use two links.
- CSMA / CD is not required.

TOPIC 189

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 sub-layer was left unchanged.
- But the features of the Standard Ethernet that depend on the transmission rate, had to be changed.
- To be able to handle a 100 Mbps data rate, several changes need to be made at the physical layer.

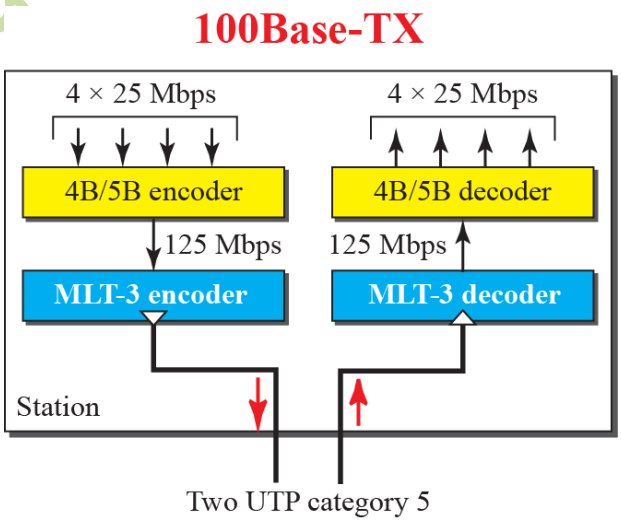
In computer networking, Fast Ethernet physical layers carry traffic at the nominal rate of 100 Mbs. The prior Ethernet speed was 10 Mbs. Of the Fast Ethernet physical layers, 100BASE-TX is by far the most common.

Goals of Fast Ethernet:

- Upgrade data rate to 100Mbps
- Make it compatible with Standard Ethernet
- Keep same 48-bit address
- Keep same frame format

100BASE - TX

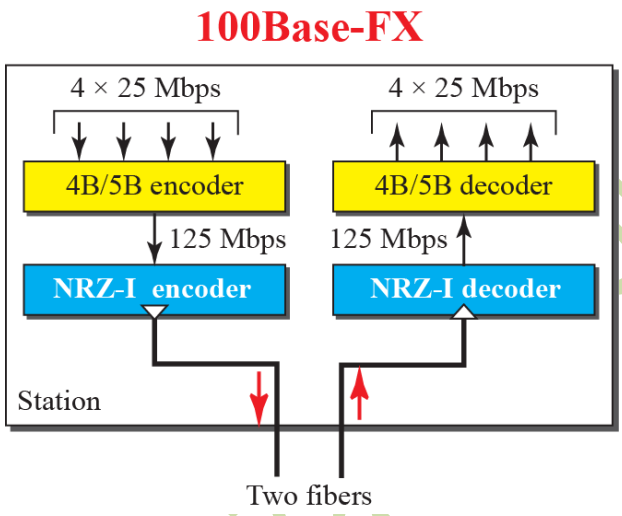
The 100BASE-TX is a prominent form of Fast Ethernet, and connects more than two wires within a category of 5 or higher cable. Each network segment can have a maximum cabling distance of 100 meters (328 feet). One pair is used for each direction, providing full duplex operation with 100 Mbps in each direction.



100BASE - FX

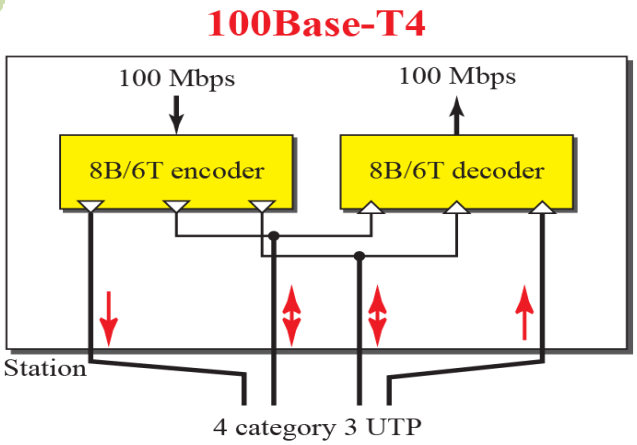
100BASE-FX is a version of Fast Ethernet over optical fiber. The 100BASE-FX Physical Medium Dependent (PMD) sublayer is defined by FDDI's PMD, so 100BASE-FX is not compatible with 10BASE-FL, the 10 Mbits version over optical fiber.

100BASE-FX is still used for existing installation of multimode fiber where more speed is not required, like industrial automation plants.



100BASE - T4

100BASE-T4 was an early implementation of Fast Ethernet. It requires four twisted copper pairs of voice grade twisted pair, a lower performing cable compared to category 5 cable used by 100BASE-TX. Maximum distance is limited to 100 meters. One pair is reserved for transmit, one for receive, and the remaining two switch direction. The fact that 3 pairs are used to transmit in each direction makes 100BASE-T4 inherently half-duplex.



TOPIC 190

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 (GbE or 1 GigE) is a term used in computer networking to transmit Ethernet frames at gigabits per second (1 billion bits per second). The most popular variety 1000BASE-T is defined by the IEEE 802.3ab standard. It came into use in 1999, and due to its significant improvement over Fast Ethernet, as well as the use of cables and equipment, Fast Ethernet was converted to wired local networks. Which are more widely available than previous standards, economical and soon.

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
- The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet.

MAC Sub-layer

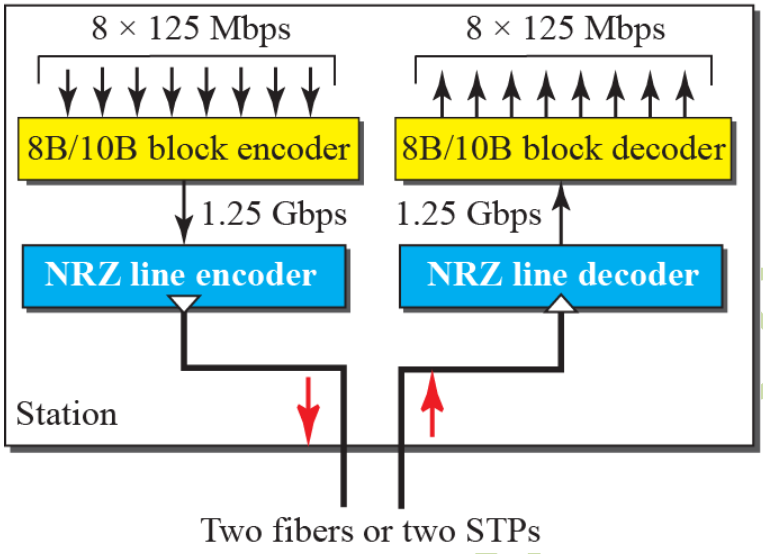
- A main consideration in the evolution of Ethernet was to keep the MAC sub-layer untouched
- To achieve a data rate of 1 Gbps, this was no longer possible
- Gigabit Ethernet has two distinctive approaches for medium access:
    - Half-duplex
    - Full-duplex

Encoding in Gigabit Ethernet:

Giga bit Ethernet is either a 2 wire or 4 wire Implementation.

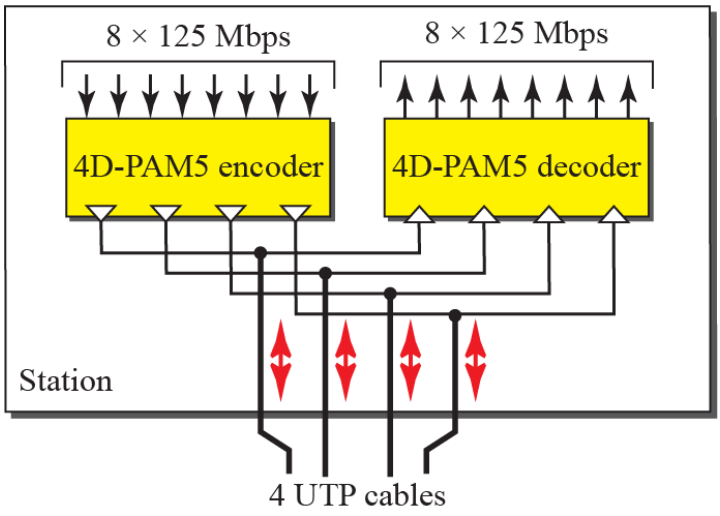
In case of 2 wire implementation it uses the fiber optic cable for 1000 Mbps or 1 gigabit. 1000 base SX is use for short waves and 1000 base XL for long waves.

1000Base-SX, 1000Base-LX, and 1000Base-CX



In case of 4 wire version, It uses 1000 Base-T and it was designed and responds to users who already installed the twisted pair cable for fast Ethernet. It uses UTP for 1000 Base-T.

1000Base-T



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	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

TOPIC 191
Chap..#..14

Other Wired Networks

- 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

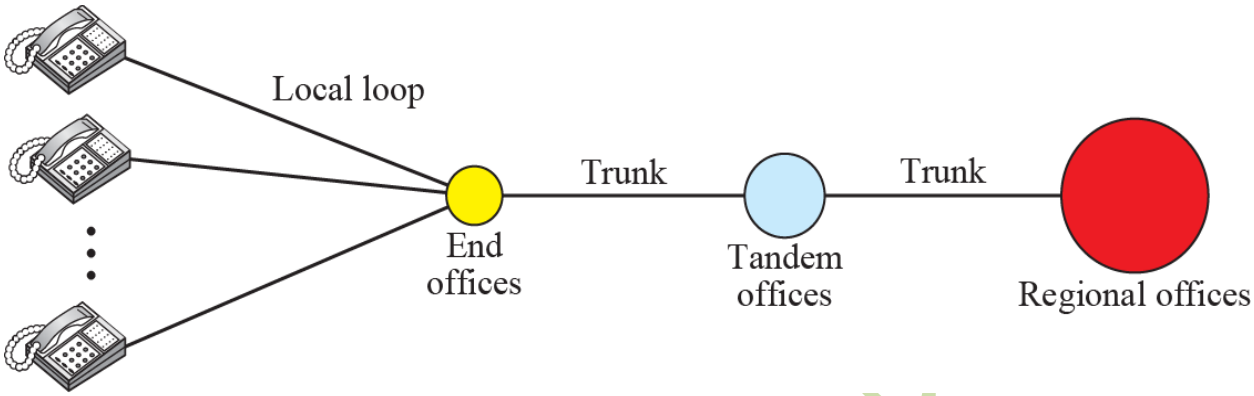
- The telephone network had its beginnings in the late 1800s.
- Plain Old Telephone System (POTS) was originally an analog system using analog signals to transmit voice.
- With the advent of the computer era, the network, in the 1980s, began to carry data in addition to voice.
- During the last decade, the telephone network has undergone many technical changes and the network is now Digital as well as Analog.

Major Components

- The telephone network is made of three major components:
  - **Local Loops** it is twisted pair cable (4 khz) (first 3 office last 4 exact local loop)
  - **Trunks** they are optical fiber cables
  - **Switching offices**

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

A Telephone System



TOPIC 192

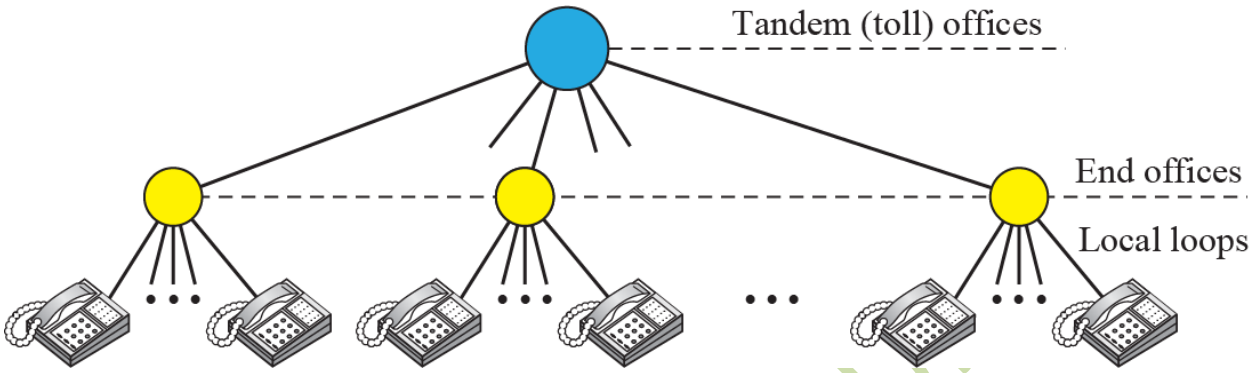
Local-Access Transport Areas (LATAs)

- 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.

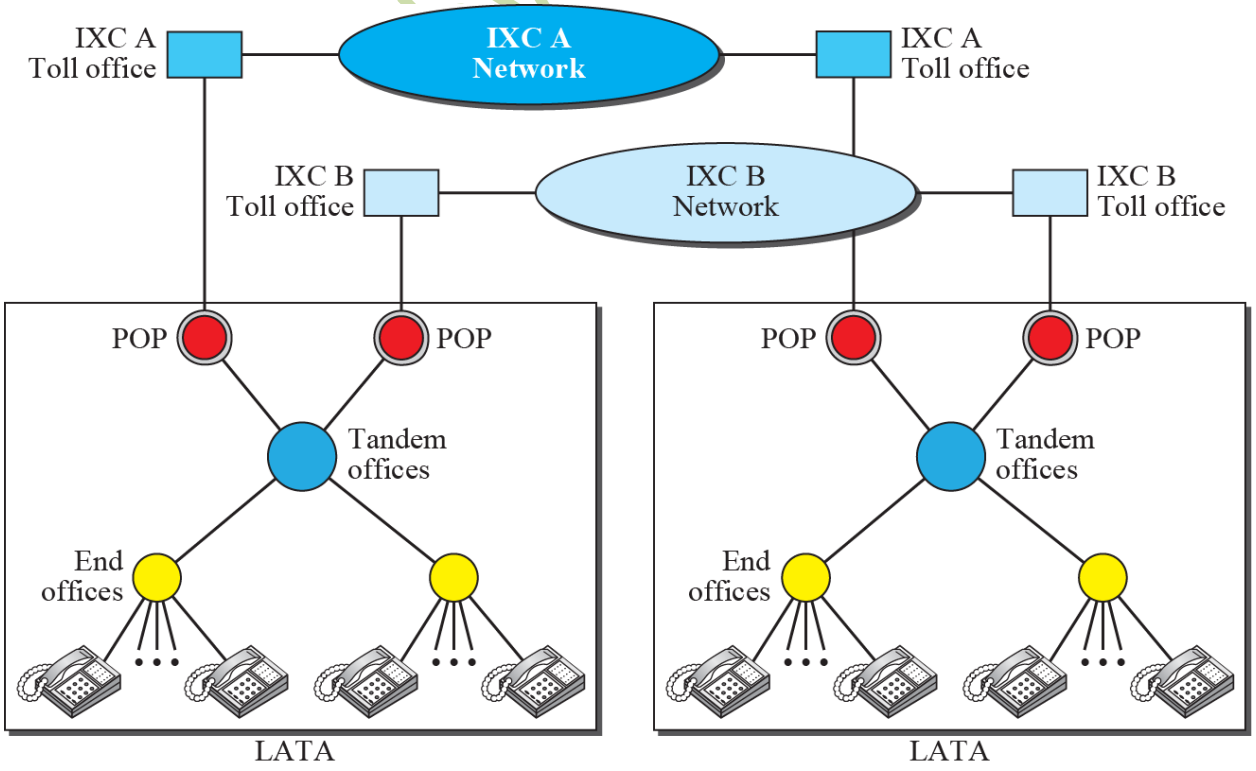
Intra-LATA and Inter-LATA Services

- 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)

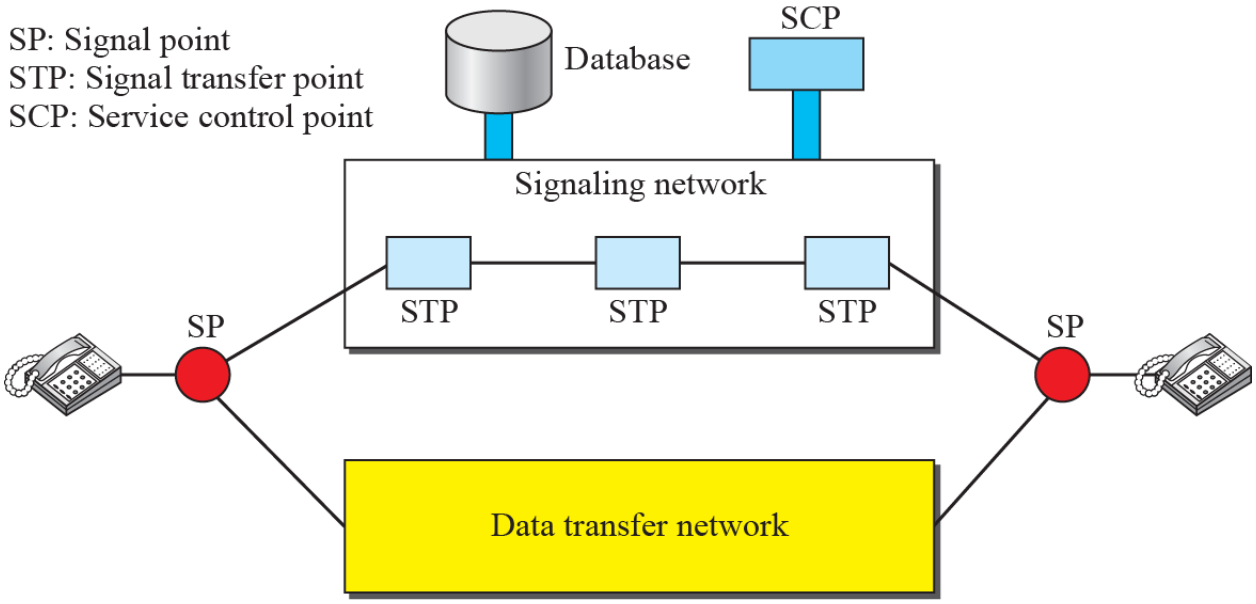


TOPIC 193

Signaling

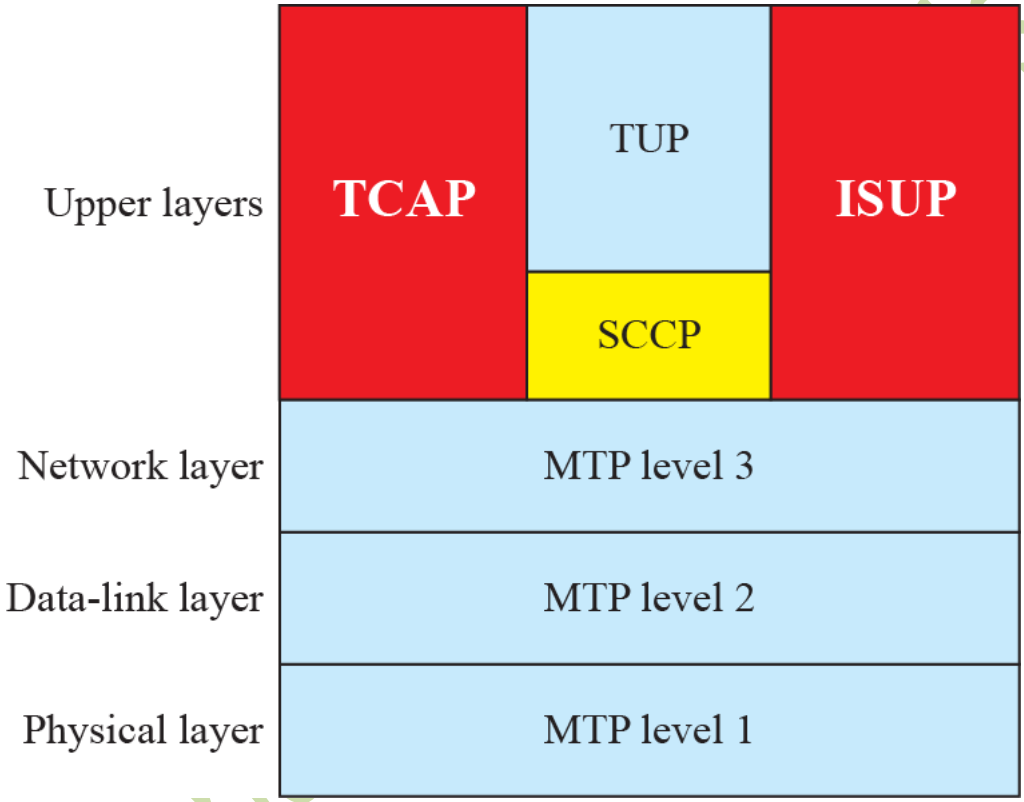
- The telephone network in the beginning, used a circuit-switched network with dedicated links to transfer voice communication.
- The operator connected the two parties by using a wire with two plugs inserted into the corresponding two jacks.
- Later, the signaling system became automatic.
- Rotary telephones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



TOPIC 194

Services

Telephone companies provide two types of services:

- Analog Services
  - Analog Switched Services
  - Analog Leased Services
- Digital Services

- Switched /56 Service
- Digital Data Service

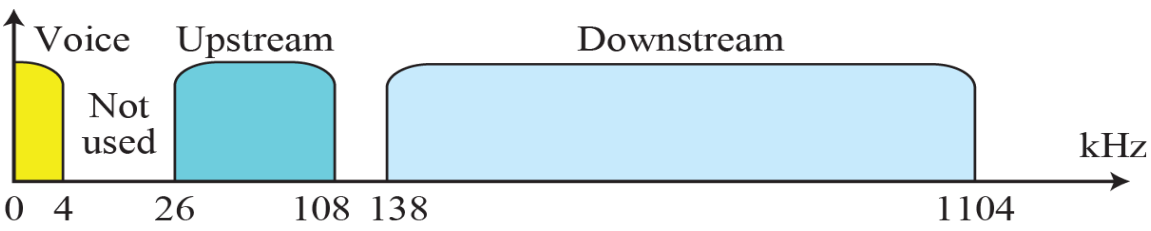
Digital Subscriber Line (DSL)

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

ADSL Point-to-Point Network

In case of ADSL to use existing telephone lines as the local loop. So, your subscriber is using the same local loop for voice. But as you can see below given figure ADSL that was not able to achieve by using the same twisted pair with dial-up modem. the reason for that is the telephone line is actually capable for getting approximately 1.1 MHz, But in the case of dial-up modems we used to have some filters that are installed at the end offices and when those filters were employed we used to have bandwidth confined to 4 kHz only which we use for our voice channels.

If these filters are removed we can use available bandwidth of approximately 1.104 MHz for high-speed. Out of this 1.104 MHz 0-4 KHz is used for voice and the rest of it, then you can use 26 to 108 KHz for Upstream Channel and 138 to 1104 KHz for Downstream Channel.



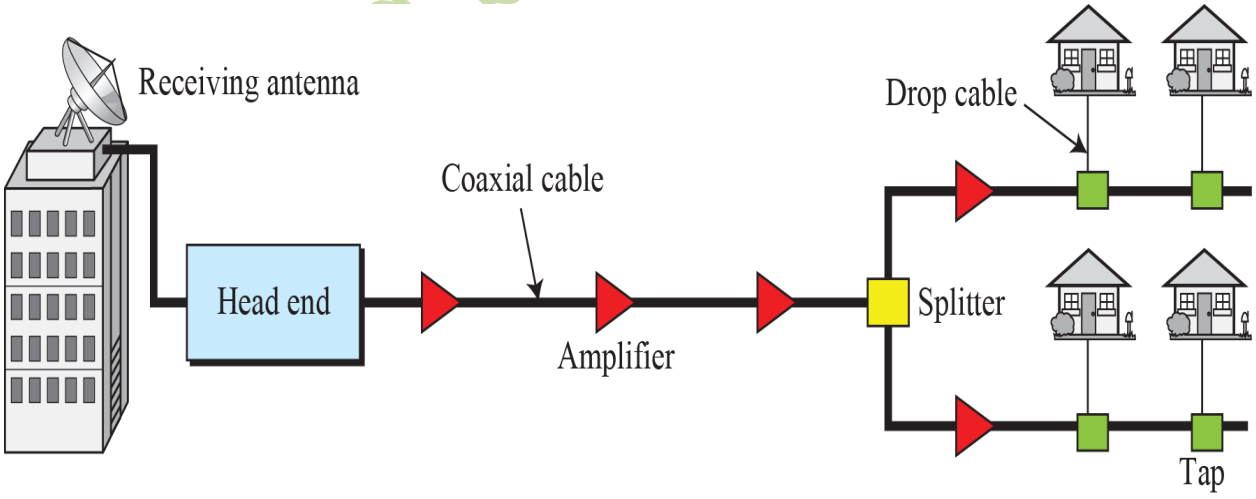
TOPIC-195

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.

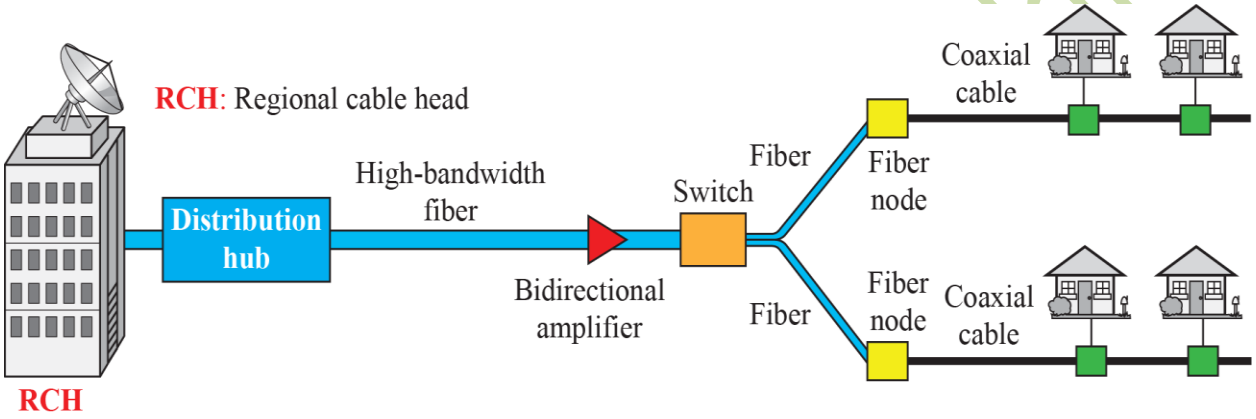
Traditional Cable Networks

- 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.
- CATV is transmission is only unidirectional.
- There are 35 amplifiers are used between Head end and end user.



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.
- One distribution hub can actually have up to 40,000 subscribers.
- In this type of Cable network we have multidirectional communication.



TOPIC 196

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

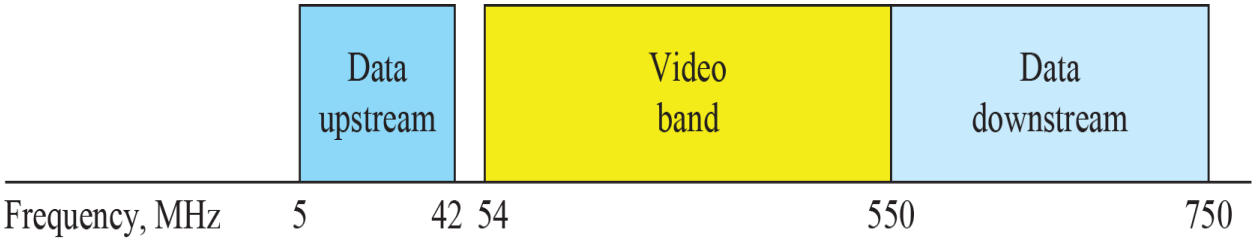
Division of Coaxial Cable Band by CATV

This band is divided into three different Sub-bands.

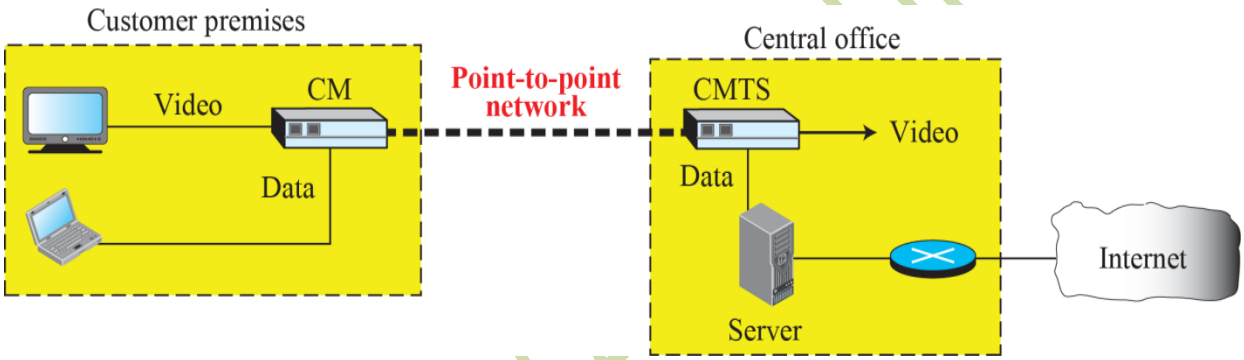
1st band is video band and we have got This video band from 54 to 550 MHz which means our video band has 496 MHz. Each of our TV channel takes 6 MHz. This essentially means that actually use this video band to carry 80 TV channels.

2nd band is upstream and it carries from 5 to 42 MHz this is also divided into 6 MHz.

3rd band is data Down-stream band its range is 550 to 750 MHz this is also divided into 6 MHz.



Cable Modem Transmission System (CMTS)



TOPIC 197

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.
- Fiber optic cables are used in SONET.

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
- **SONET Layers / Connections**
  - Section
  - Line
  - Path

TOPIC 198

SONET Signals

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 Devices

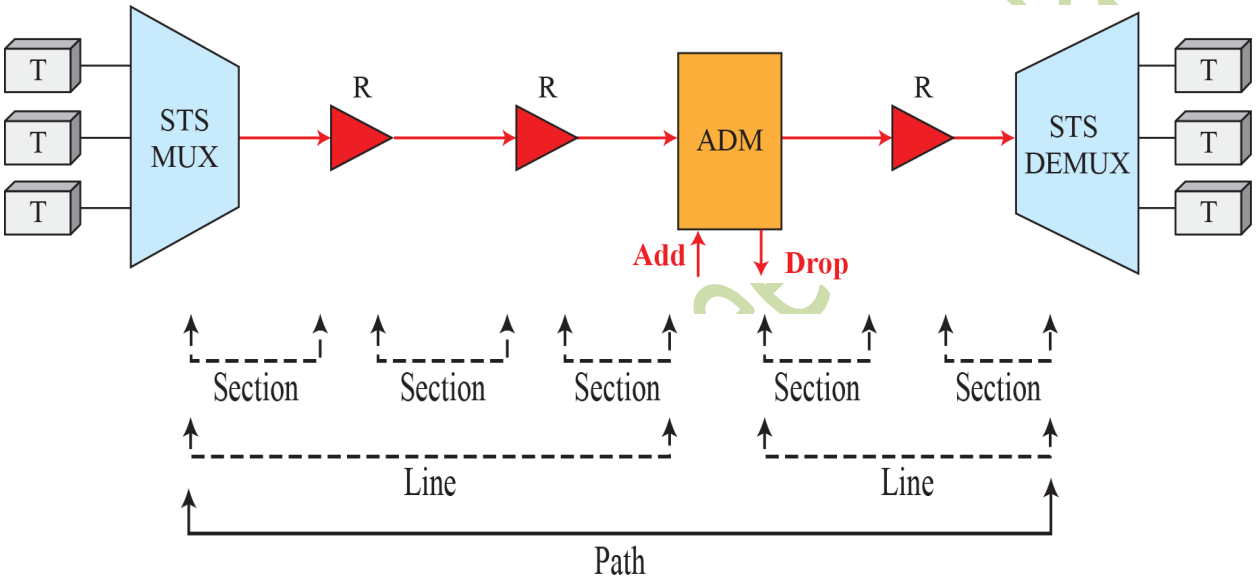
ADM: Add/drop multiplexer

STS MUX: Synchronous transport signal multiplexer

STS DEMUX: Synchronous transport signal demultiplexer

R: Regenerator

T: Terminal



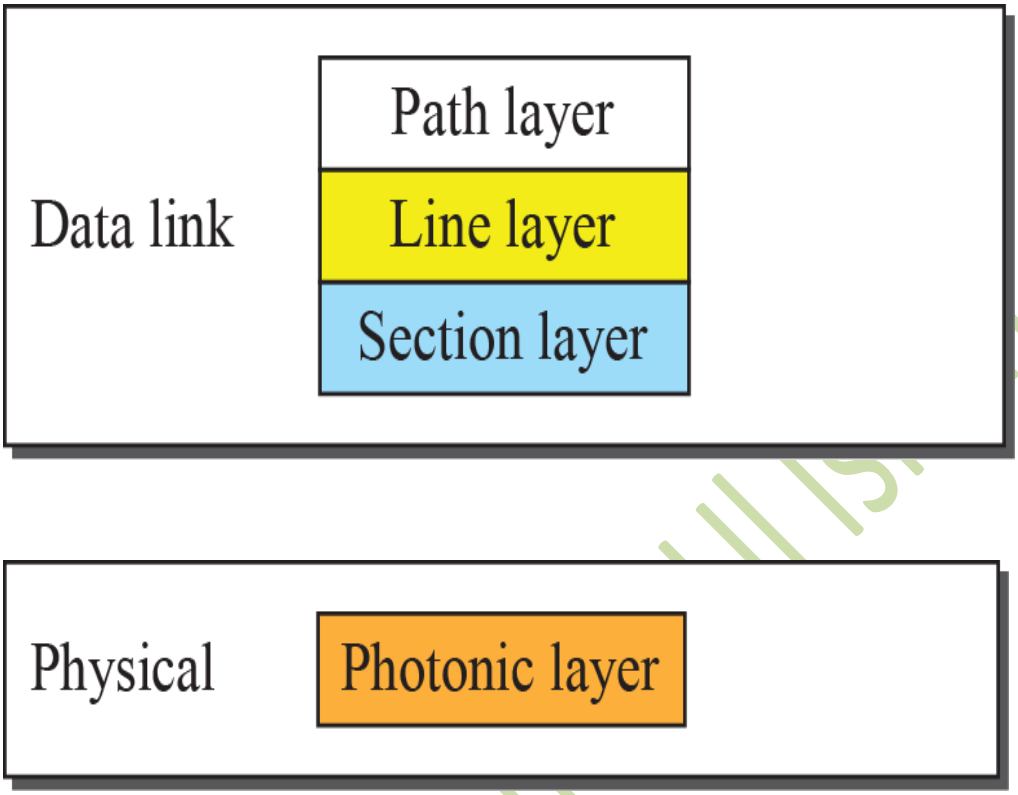
TOPIC 199

SONET Layers / Connections

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.



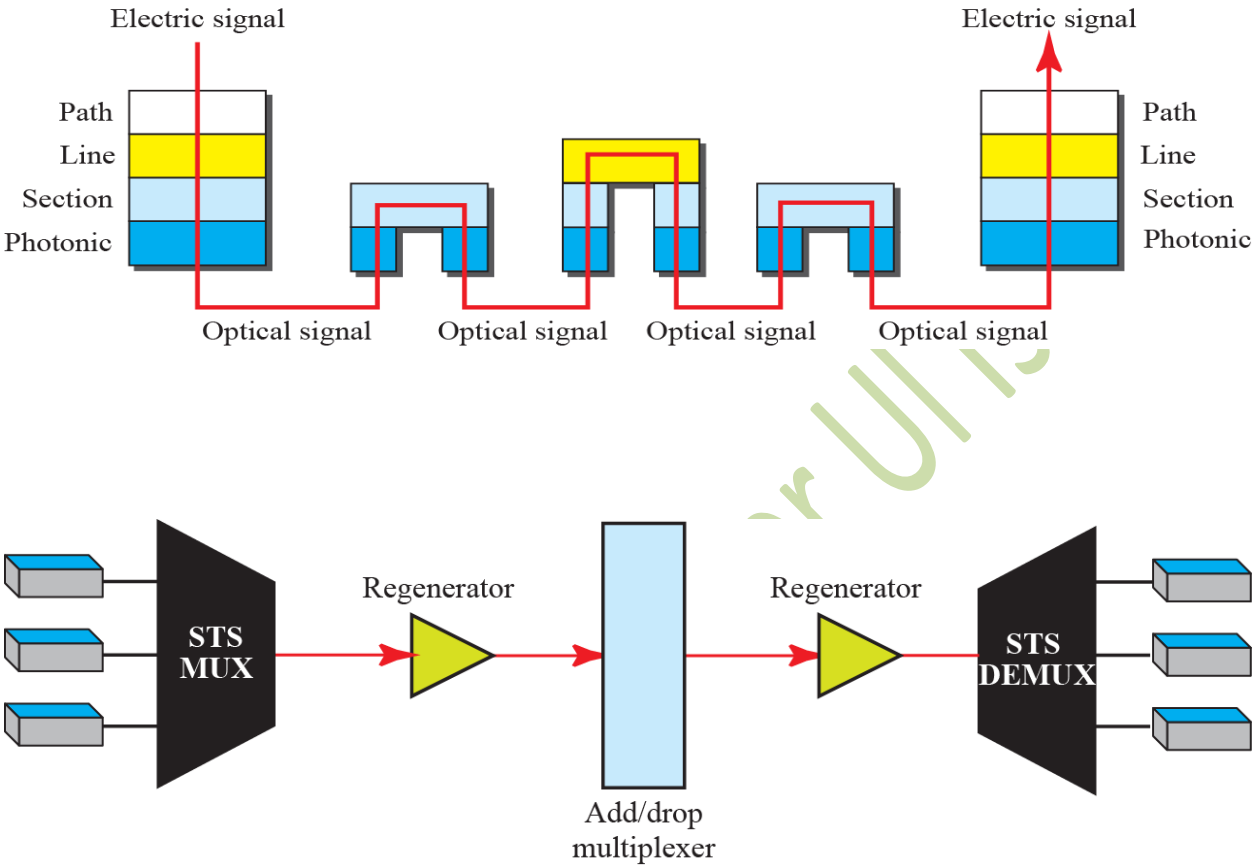
Path Layer is responsible for the movement of a signal from source to the destination.

Line layer is a particular type of connection it is responsible for the movement of the signal across a physical line.

Section layer is responsible for the movement of the same signal across the physical section.

Photonic layer is equivalent to physical layer of OSI model. In this case use and encoding and encoding here presence of light is represent 1 in binary and absence of light is a represent 0.

Device-Layer Relationship in SONET

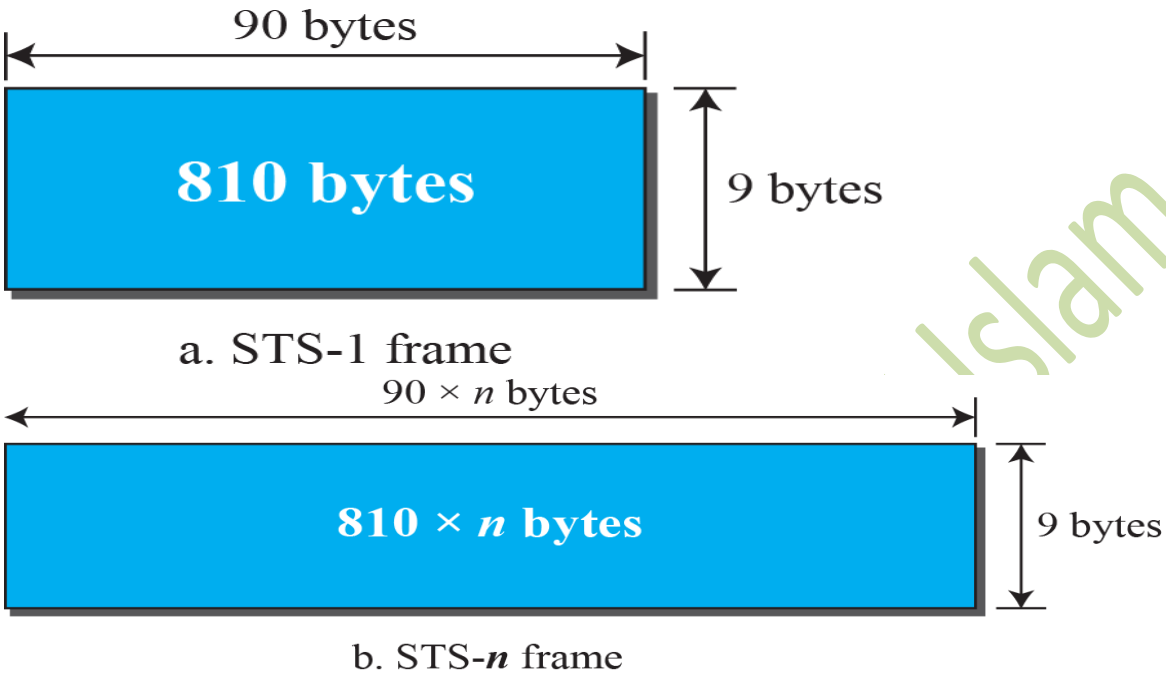


TOPIC 200

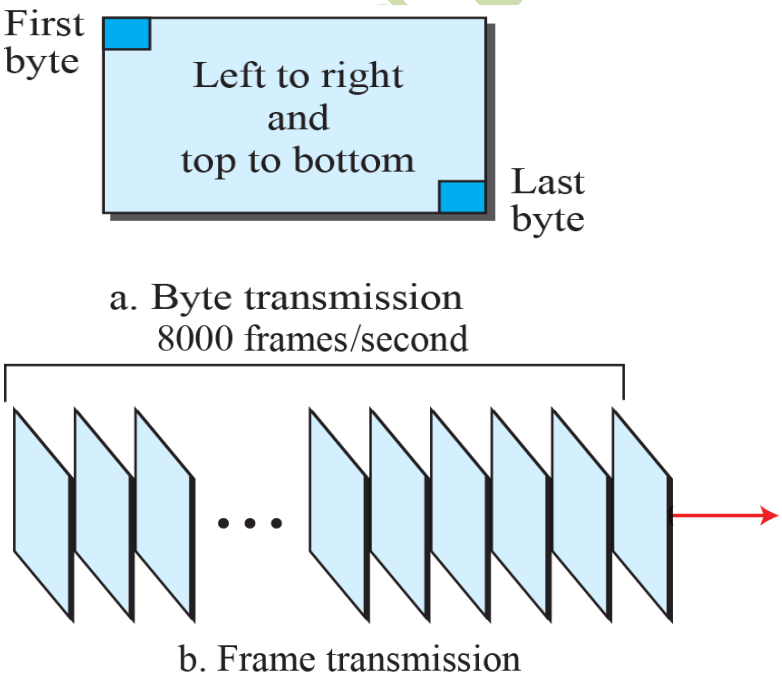
SONET Frames

- 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

8000 frames per second

9 bytes x (1 x 90) bytes

Data Rate = 8000 x 9 (1 x 90)

= 51.84 Mbps

Find the data rate of an STS-3 signal

n = 3

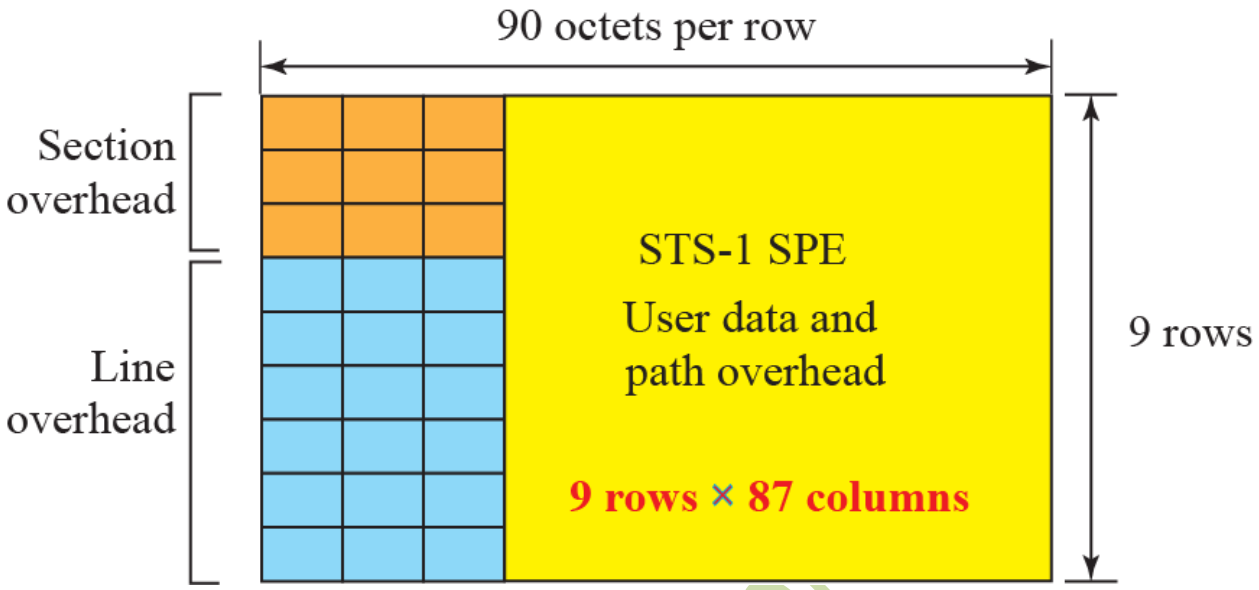
Data Rate = 8000 x 9 (3 x 90)

= 155.52 Mbps

STS-1 Data Rate x 3

= STS-3 Data Rate.

STS-1 Frame Format

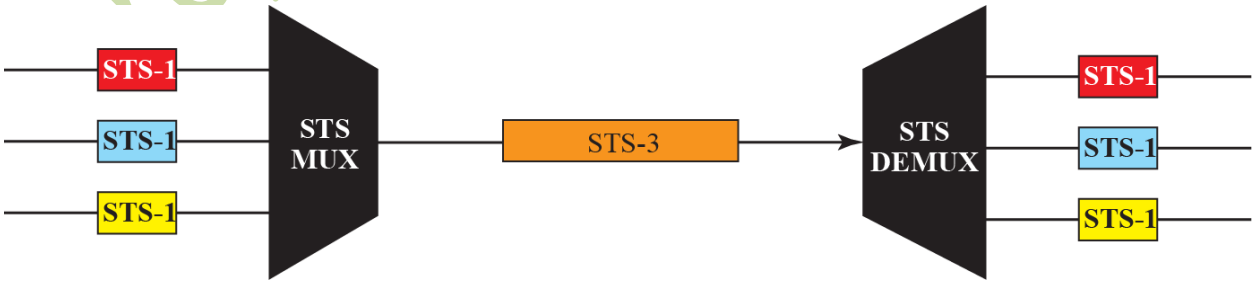


TOPIC 201

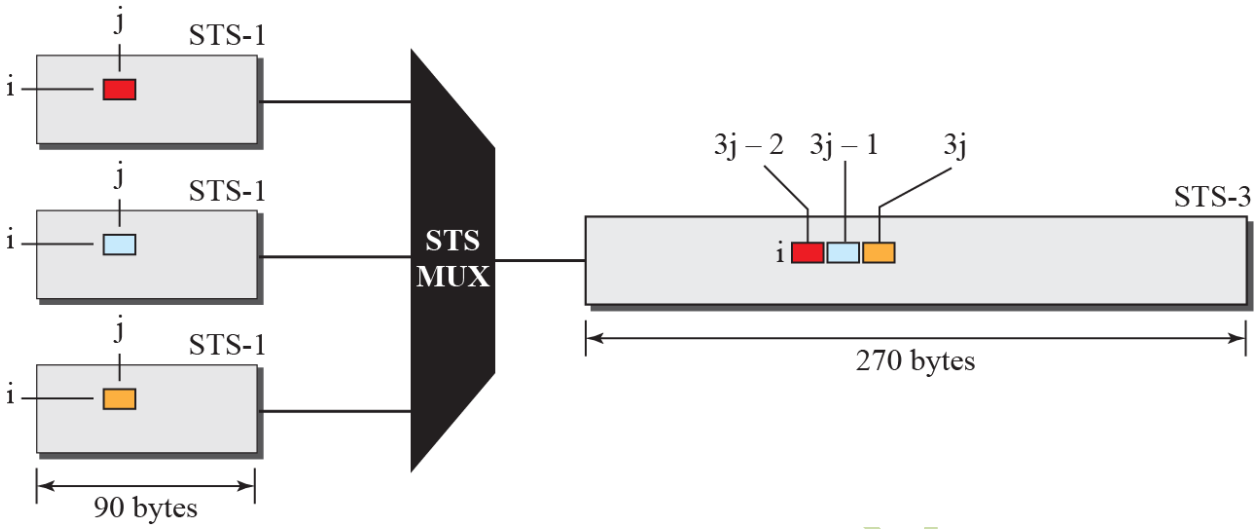
STS Multiplexing

- 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.

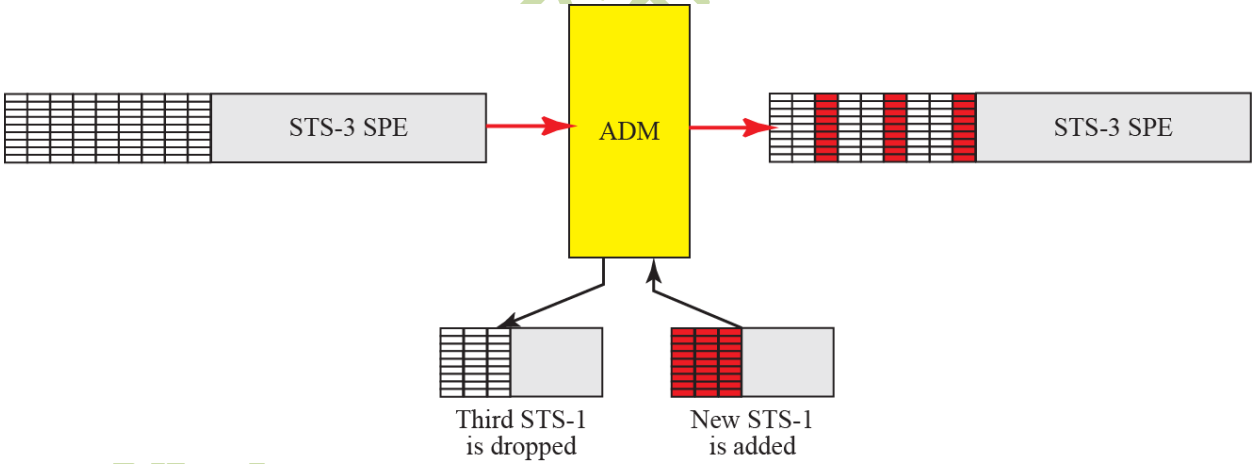
STS Multiplexing/De-multiplexing



Byte Interleaving



Add/Drop Multiplexer

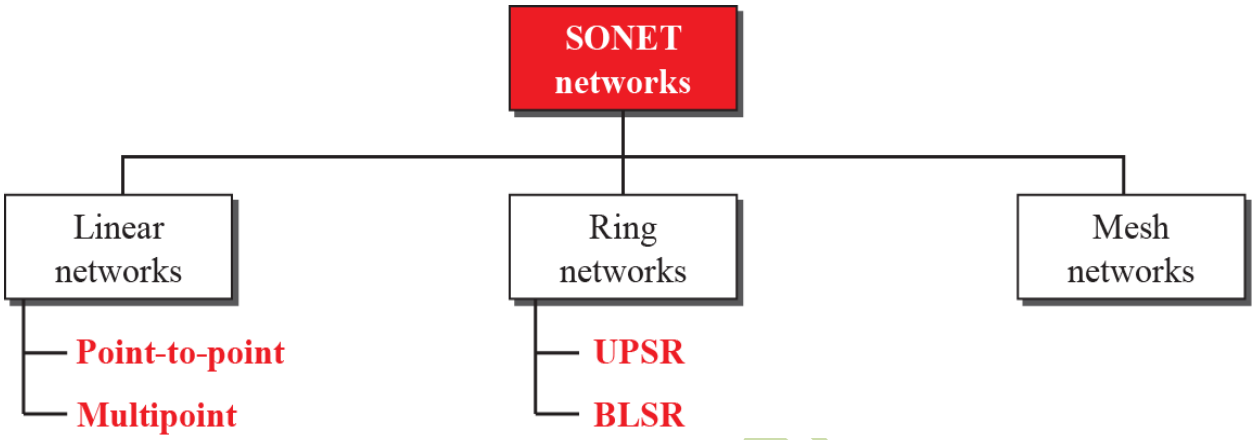


SONET Networks

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

We can roughly divide SONET networks into three categories:

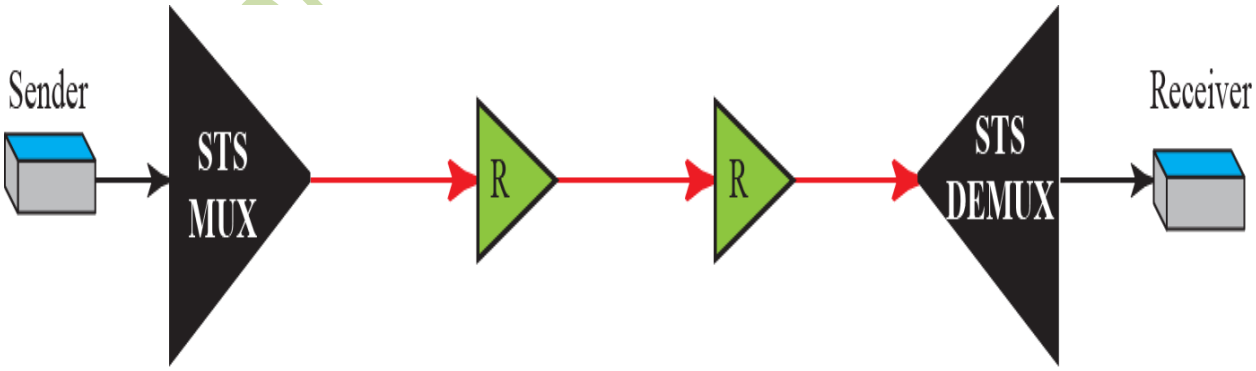
- Linear Networks
- Ring Networks
- Mesh networks



1st type of SONET is Linear Networks.

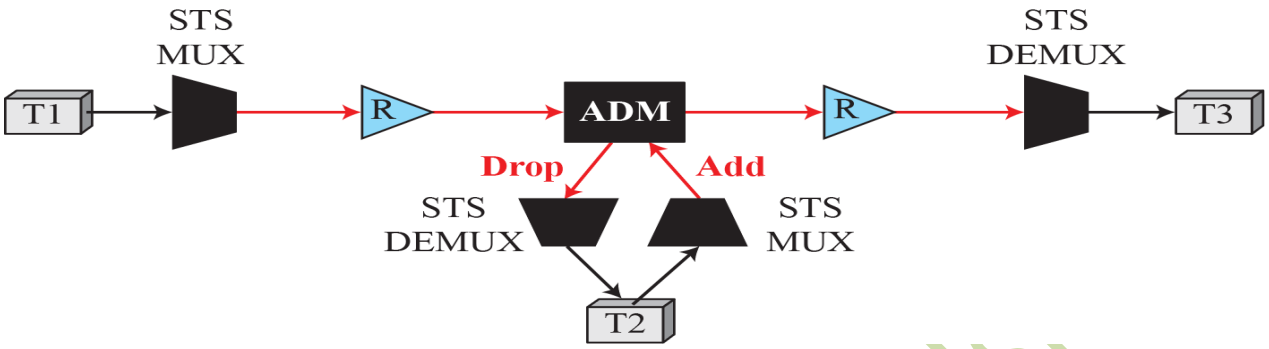
It has two types:

Point-to-Point is a simple Network which is made up of an STS Mux and De-mux and a couple of generators. In this case signals can flow unidirectional or bi-directional. We can have both, but in the case of figure below we only have the data traveling in Down-stream therefore this is unidirectional by Nature.



Multi-point network we use in this type "ADD & drop" multiplexer. In this case each terminal can send the data one or more Down-stream channels. We can have a multi-

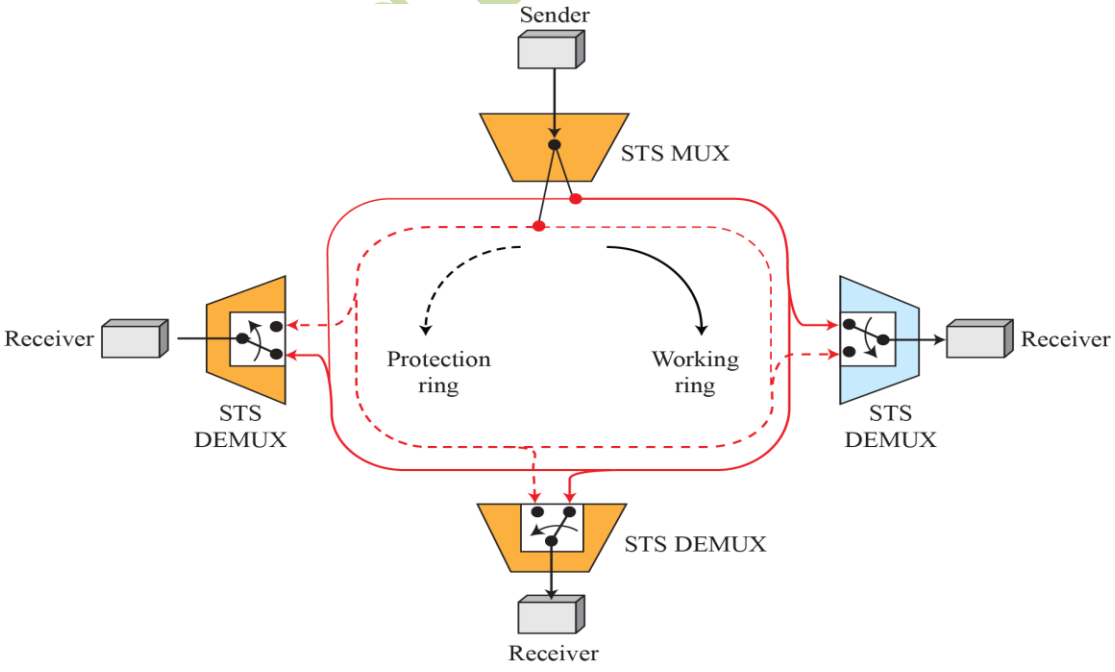
point network Bi-directional, but in this case we have our unidirectional multi-point Channel.



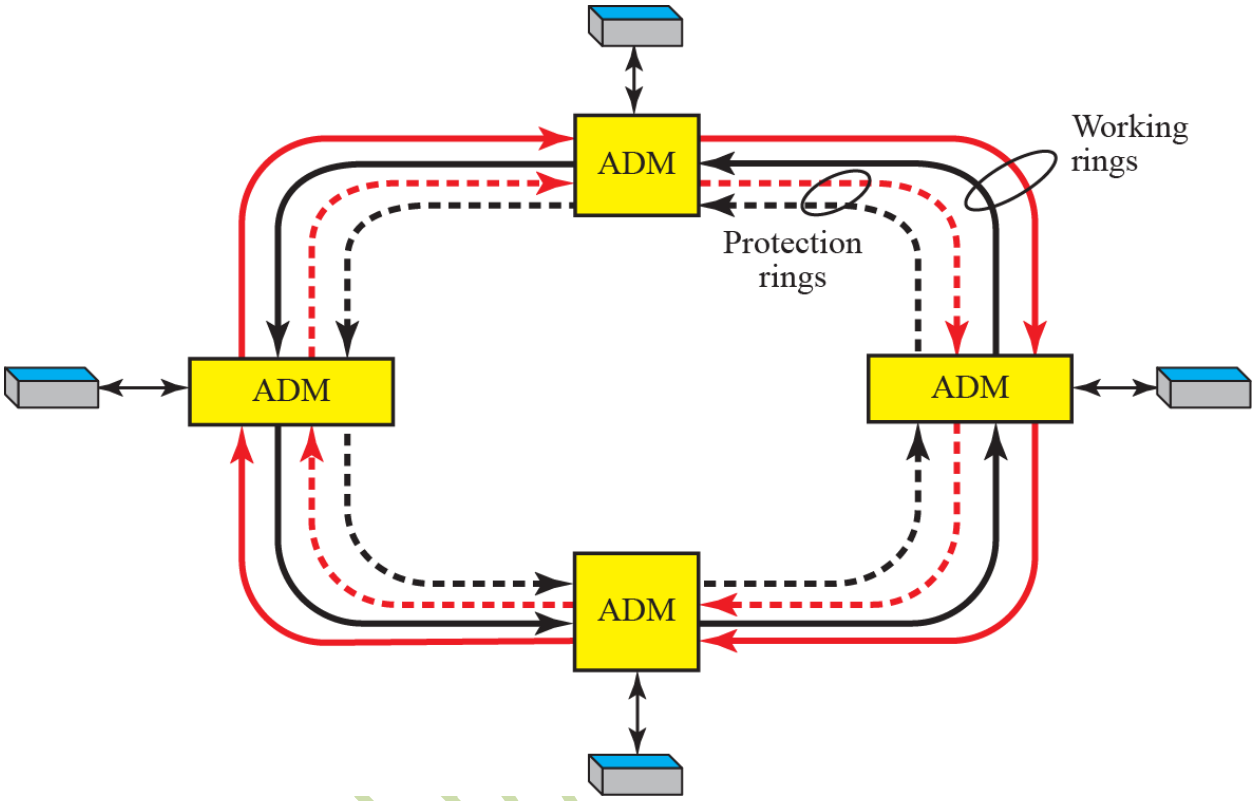
2nd Type of SONET Networks is Ring Networks

It has two types:

UPSR stands for unidirectional path switching ring. We call it path switching ring because it has two rings one is working ring which is clock wise and another is protection ring which is anti-clock wise. Both these Rings carry the exact same type of data. So each node which is connected to this kind of ring receives two different data streams of same data. UPSR compare both data strings and choose the best one. We have fast failure recovery rate in the case of UPSR and in general ring Network, but as you can see because two rings doing the same job. One half the band-width is wasted, there for efficiency is low as compared to linear Network.

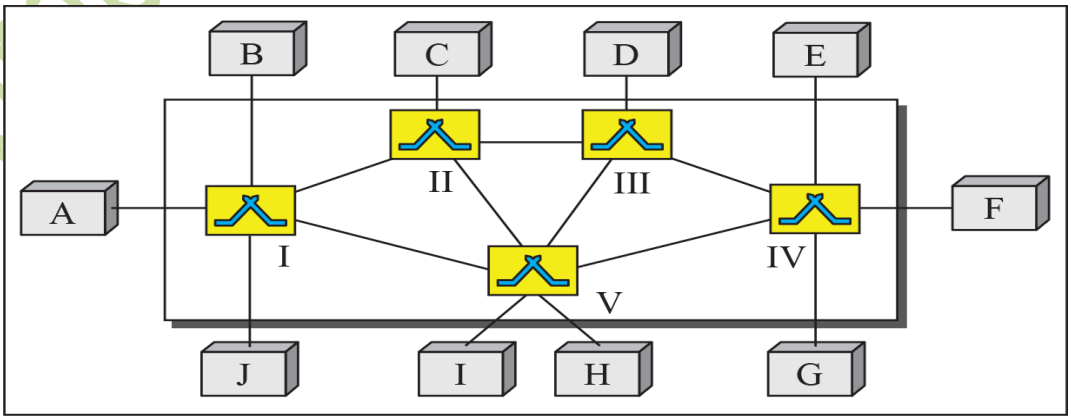


BLSR stands for bi-directional line switching ring. In this case communication is bi-directional. It means tha two rings for working line and also two rings for protection line as well. BLSR used 4 Rings totally, and as you can imagine the Rate of faliure is improve and efficiency more down**.**

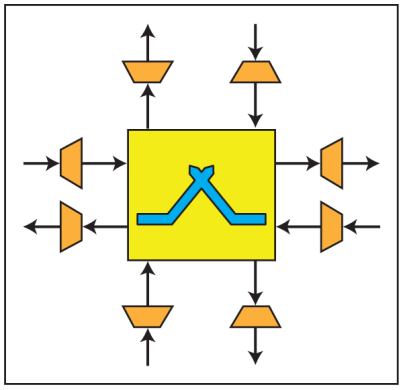


3rd type of SONET Networks is Mesh Networks:

In mesh Network it is used switch which is known as a cross connected switches multiple input and output force in this case.



a. SONET mesh network



b. Cross-connect switch

TOPIC 203

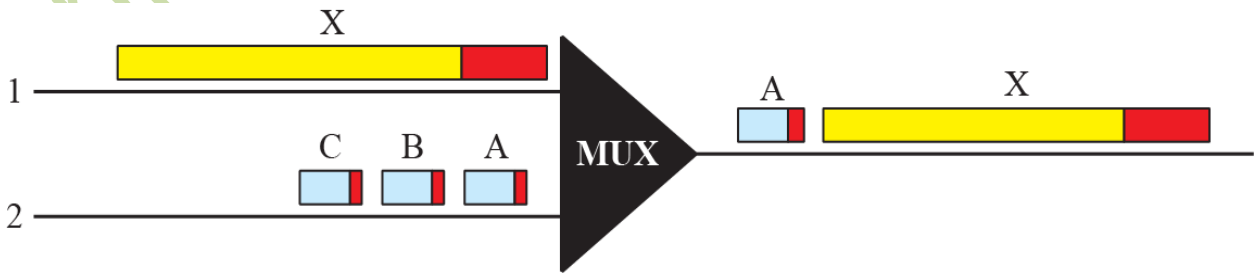
ATM

- 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.

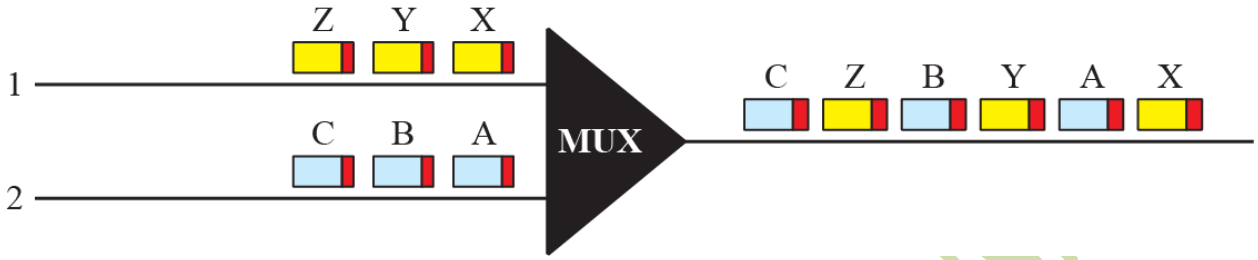
Problems

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

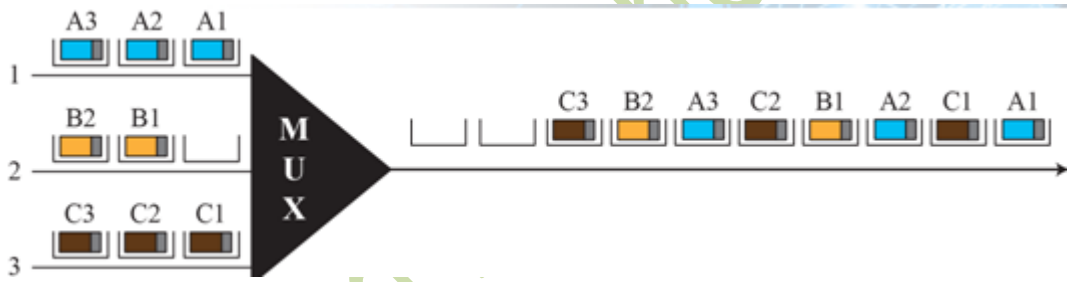
Multiplexing using Different Frame Size



Multiplexing using Cells



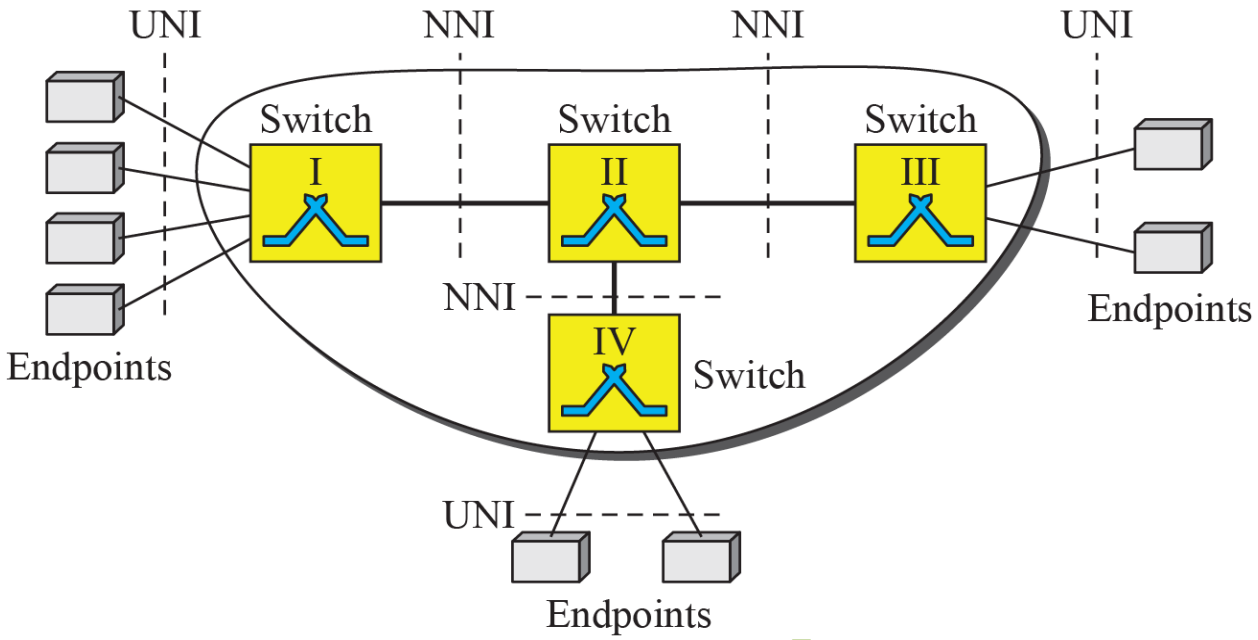
ATM Multiplexing



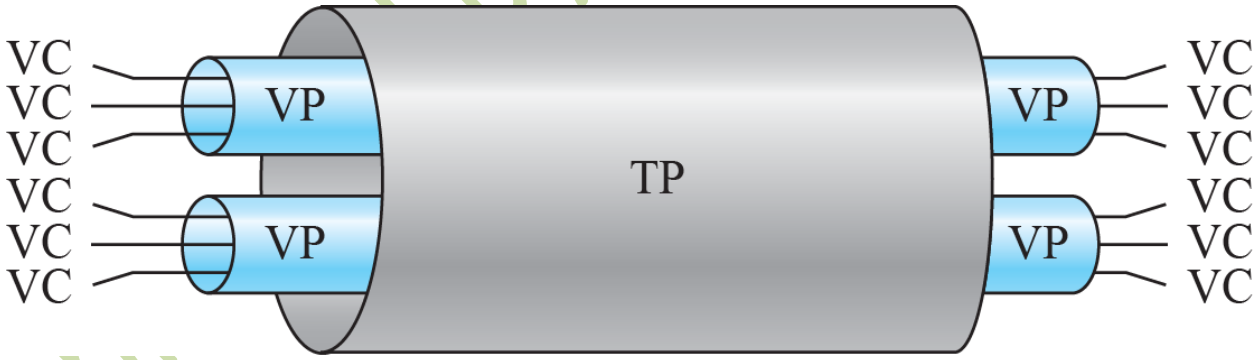
TOPIC 204

Architecture

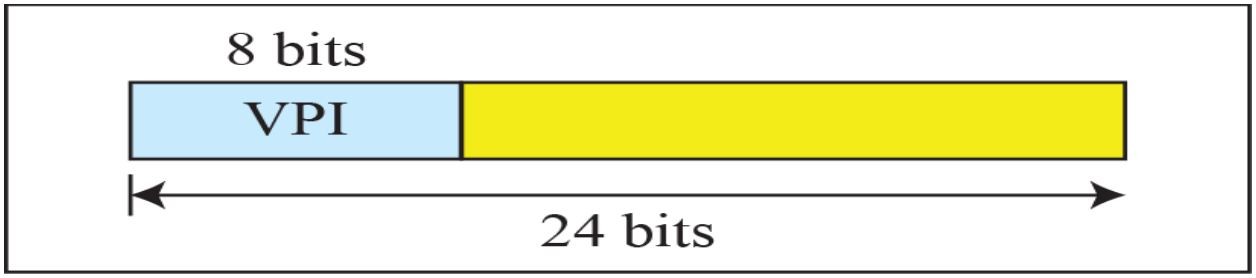
- ATM is a cell-switched network.
- The user access devices, called the endpoints, are connected through a user-to-network interface (UNI) to the switches inside the network.
- The switches are connected through network-to-network interfaces (NNIs).



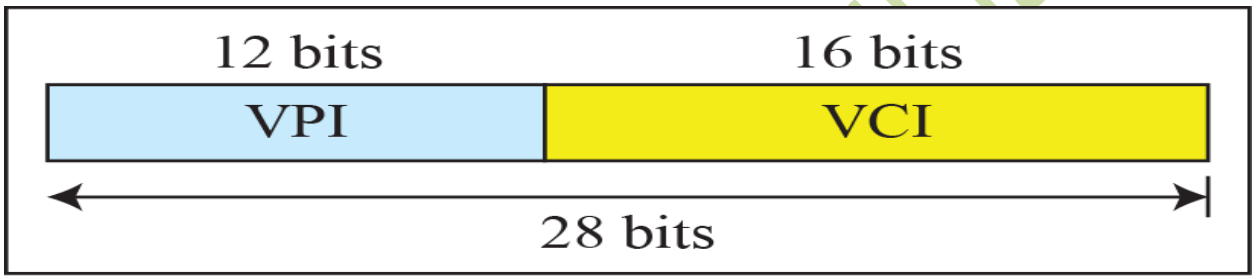
TP, VPs, and VCs



Virtual connection identifiers in UNIs & NNIs

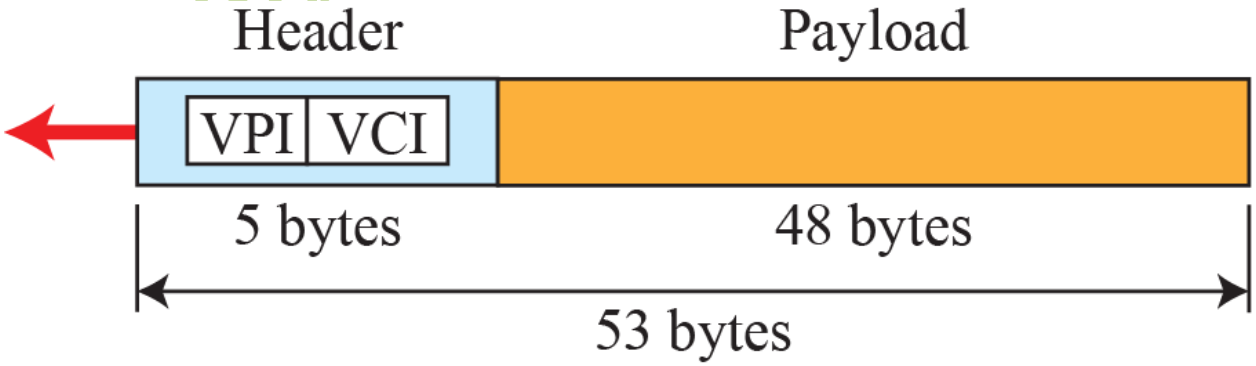


a. VPI and VCI in a UNI

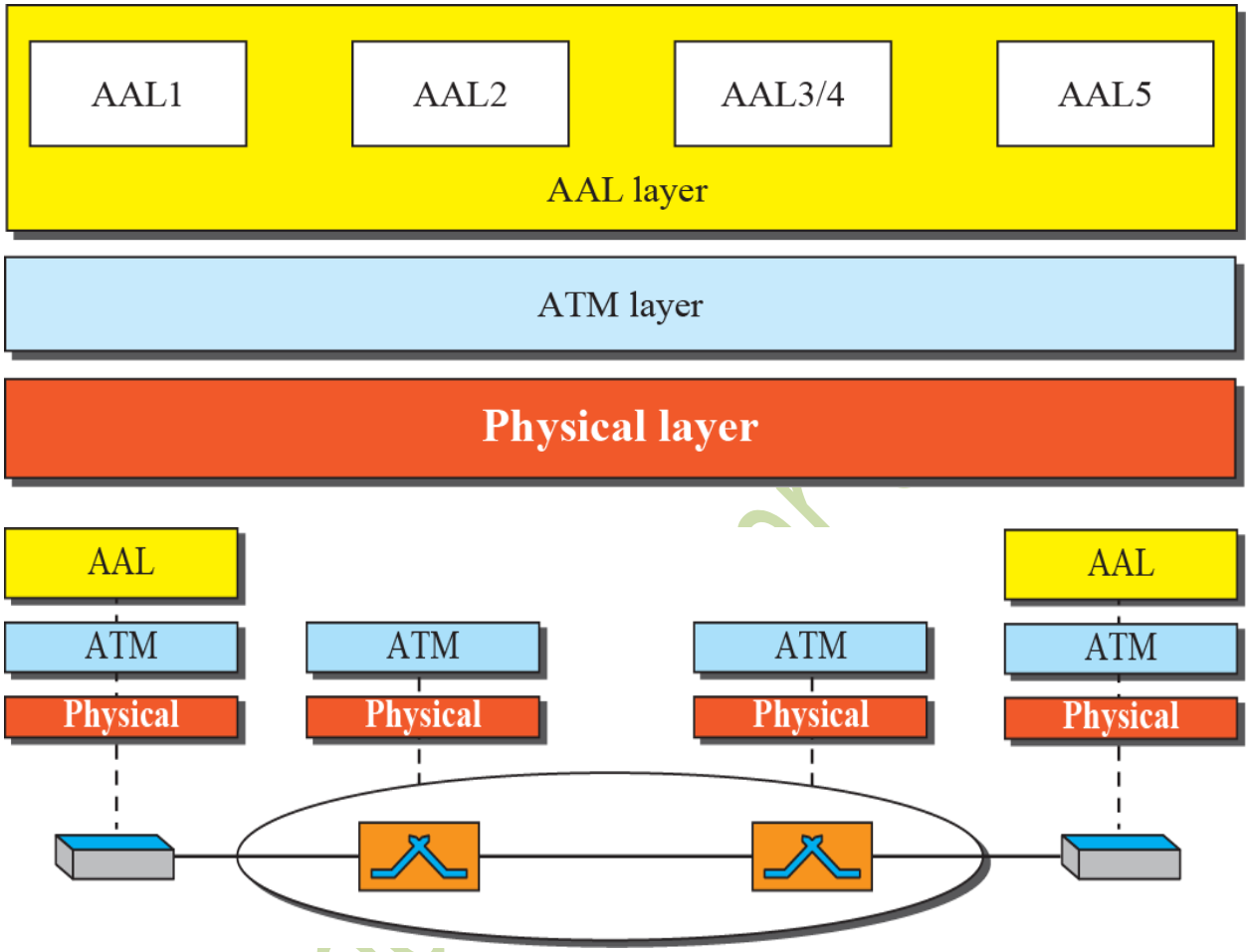


b. VPI and VCI in an NNI

An ATM Cell



ATM Layers


AAL1
AAL2
AAL3/4
AAL5
AAL layer
ATM layer
Physical layer
AAL
ATM
Physical
AAL
ATM
Physical
ATM
Physical
ATM
Physical

TOPIC 205
Chap….15

Introduction to Wireless

- 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.

Architectural Comparison

Architecture comparison of wired and wireless LANs

- **Medium** in the case of wired Networks we need cables to connect our nodes. While on the wireless network we don't need cables.

- **Hosts** as we know in wired network our nodes are connected with switch through a wire. So, we can't move easily our nodes. While in case of wireless we can easily move nodes.

- Isolated LANs

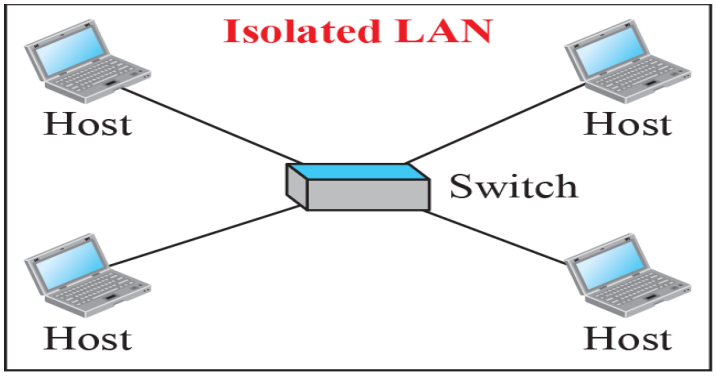
- Connection to other Networks

- Moving between Environments**.**
  Just by doing two things we can move our wired network into wireless:

  - Remove link layer switch and replace it with wireless access point.
  - We will replace wired NIC with wireless NIC.

NOTE: wireless LAN exists bottom two layers (Layer 1 & Layer 2)

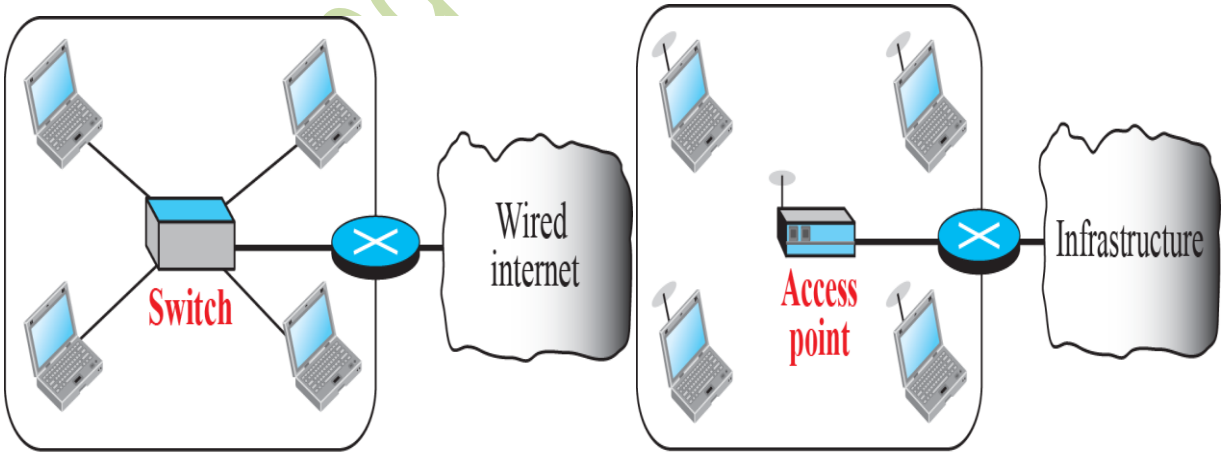
Isolated LANs: Wired versus Wireless



Wired

Wireless

Connection of a Wired/Wireless LAN to other networks



Wired LAN

Infrastructure network

TOPIC 206

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

- **Attenuation**
  Attenuation is the loss of signal strength in networking cables or connections. This typically is measured in decibels (dB) or voltage and can occur due to a variety of factors. It may cause signals to become distorted or indiscernible. An example of this is Wi-Fi signal and strength getting noticeably weaker the further that your device is from the router.

- **Interference**
  Because the air is shared by all transmitters, transmissions by any device at the same frequency as an access point's radio can cause interference.

- **Multipath Propagation**
  In the case of multipath propagation the actual signals that you want to receive you have to receive. But you also receive some multiple other versions of same signals. Actually original signals reflected from ground, from walls or any other things and create a noise. This noise is called Multipath propagation.

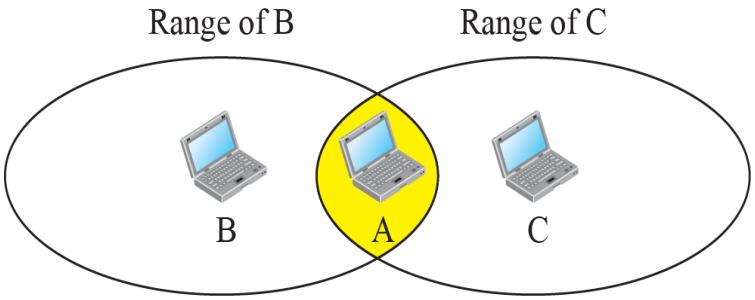
- **Error**

TOPIC 207

Access Control

- Most important issue in a wireless LAN is how a wireless host can get access to the shared medium (air).
- CSMA/CD does not work in wireless LANs for three reasons:
  - Wireless hosts don’t have power to send and receive at the same time.
  - The hidden station problem prevents collision detection.
  - 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.

TOPIC 208

IEEE 802.1 PROJECT

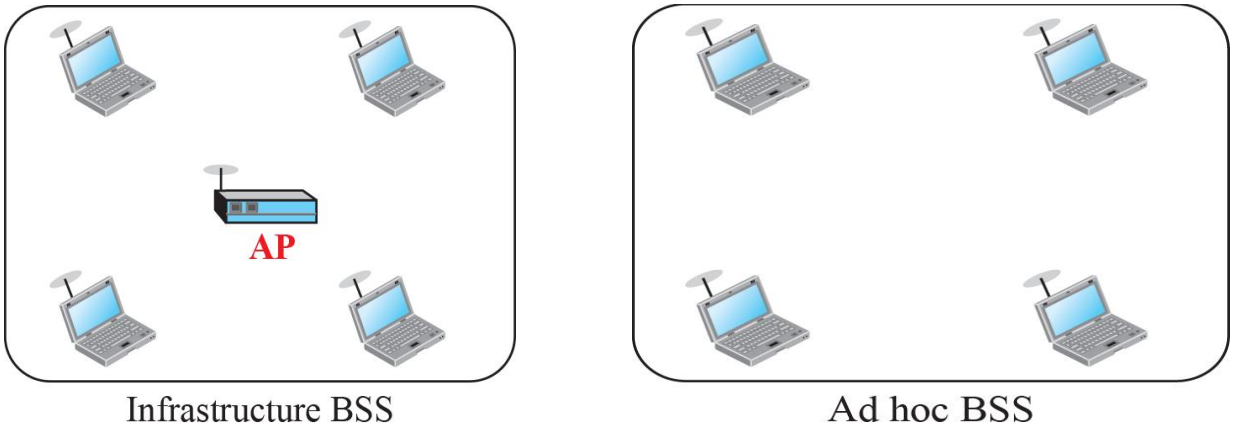
- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers.
- It is sometimes called Wireless Ethernet.
- The term WiFi (short for wireless fidelity) as a synonym for wireless LAN (certified by WiFi alliance).

Architecture

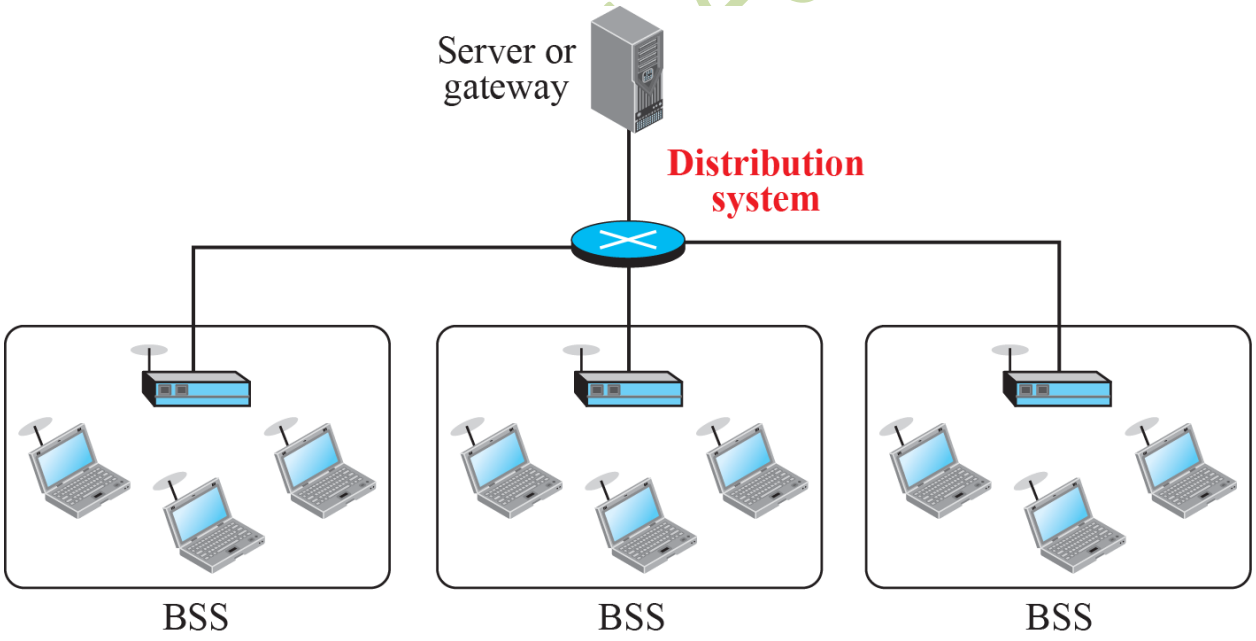
The standard defines two kinds of services:

- The basic service set (BSS)
- The Extended service set (ESS)

Basic Service Sets (BSSs)



Extended Service Set (ESS)



Types of Stations

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

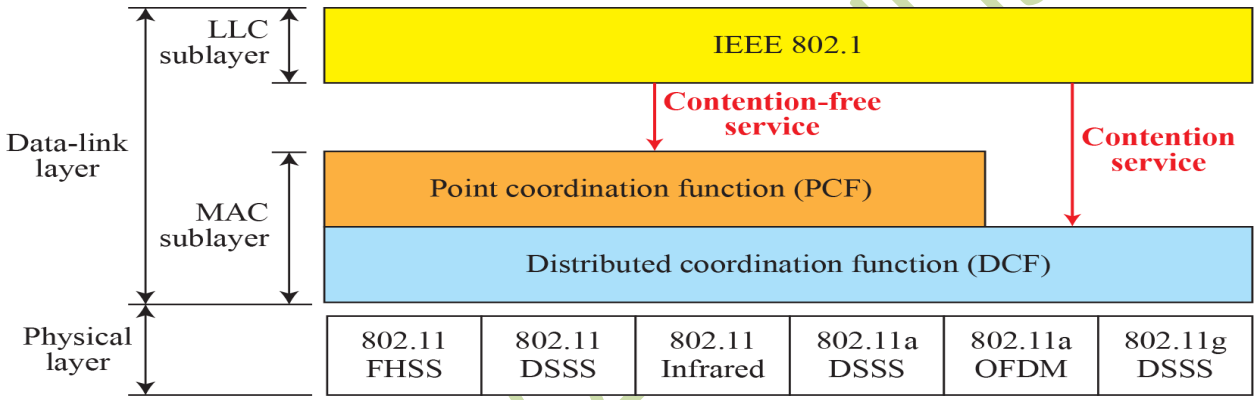
TOPIC 209

MAC Sub-layer

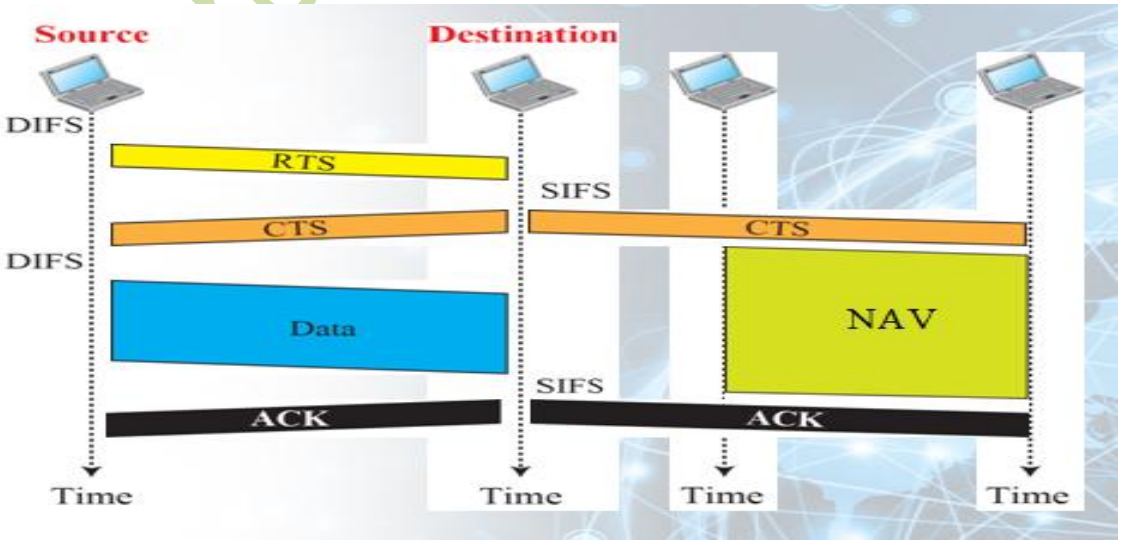
IEEE 802.11 defines two MAC sub-layers:

- The Distributed Coordination Function (DCF)
- The Point Coordination Function (PCF)

MAC Layers in IEEE 802.11 Standard

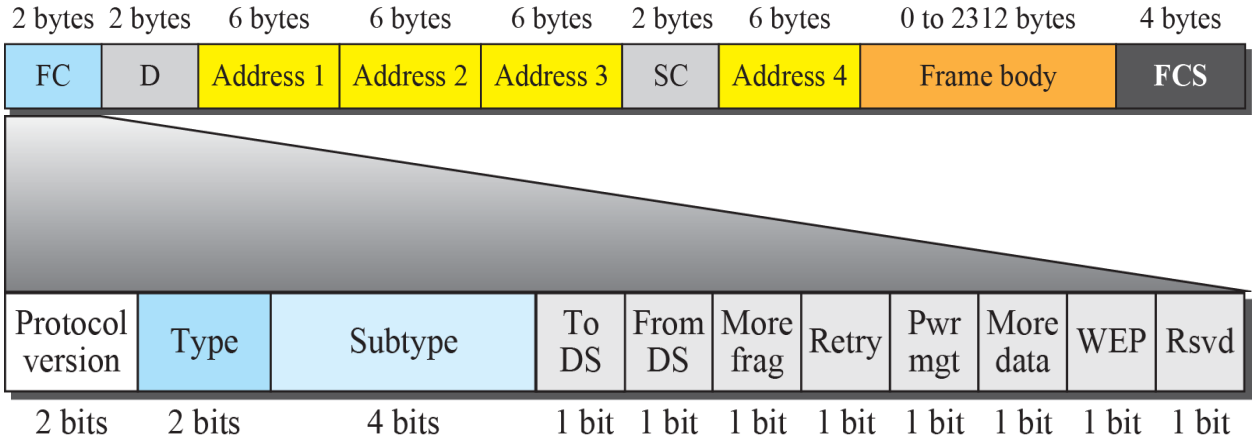


CSMA/CA and NAV



TOPIC 210

Frame Format of Point Coordination Function (PCF)



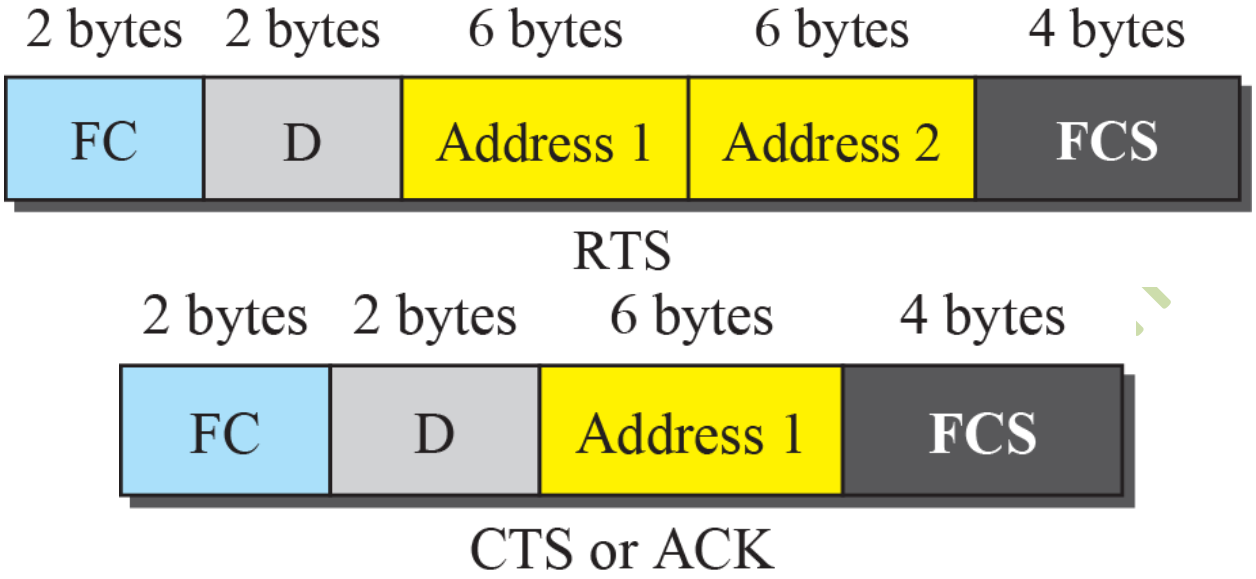
Subfields in FC field

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 frame



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

TOPIC 211

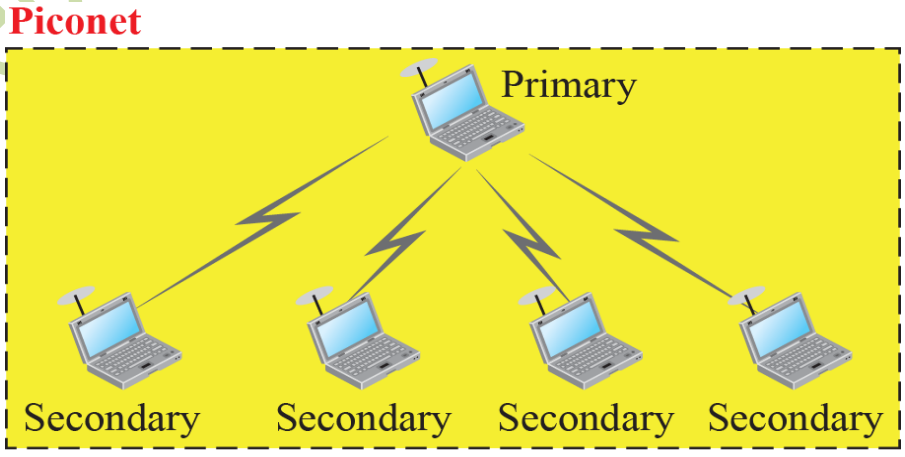
BLUETOOTH

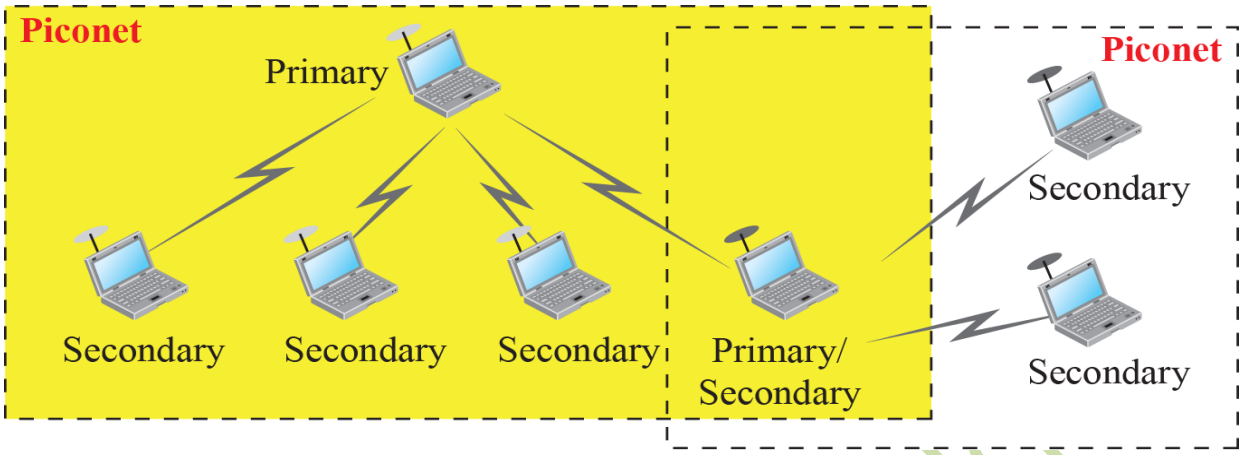
- Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other.
- A Bluetooth LAN is an ad hoc network.
- The devices, sometimes called gadgets, find each other and make a network called a Piconet.

Architecture

Bluetooth defines two types of networks:

- **Piconet** in this case we can have up 8 active devices in a single time one of them is primary and other 7 is secondary.
- **Scatternet** multiple piconet is connected with each other is called scatternet.





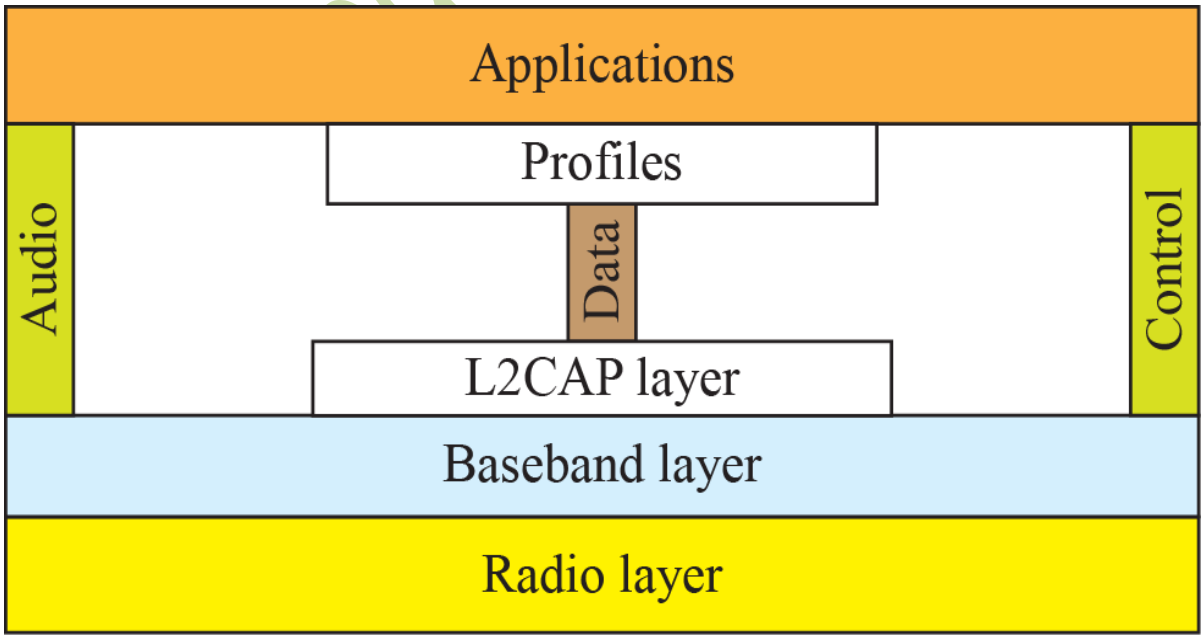
TOPIC 212

BLUETOOTH devises

- A Bluetooth device has a built-in short-range radio transmitter.
- The current data rate is 1 Mbps without 2.4 gigahertz bandwidth.
- This means there is a possibility of interference between the IEEE 802. 11 Wireless LAN's and Bluetooth LAN's

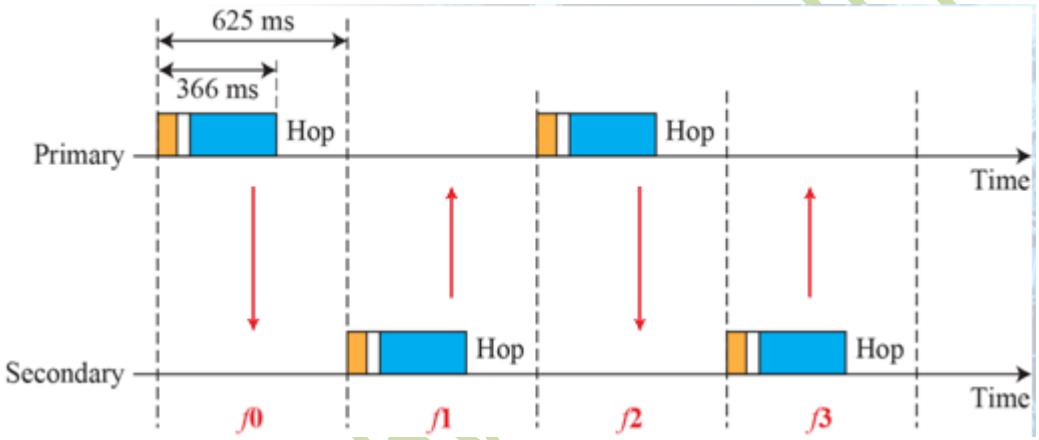
Bluetooth Layers

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

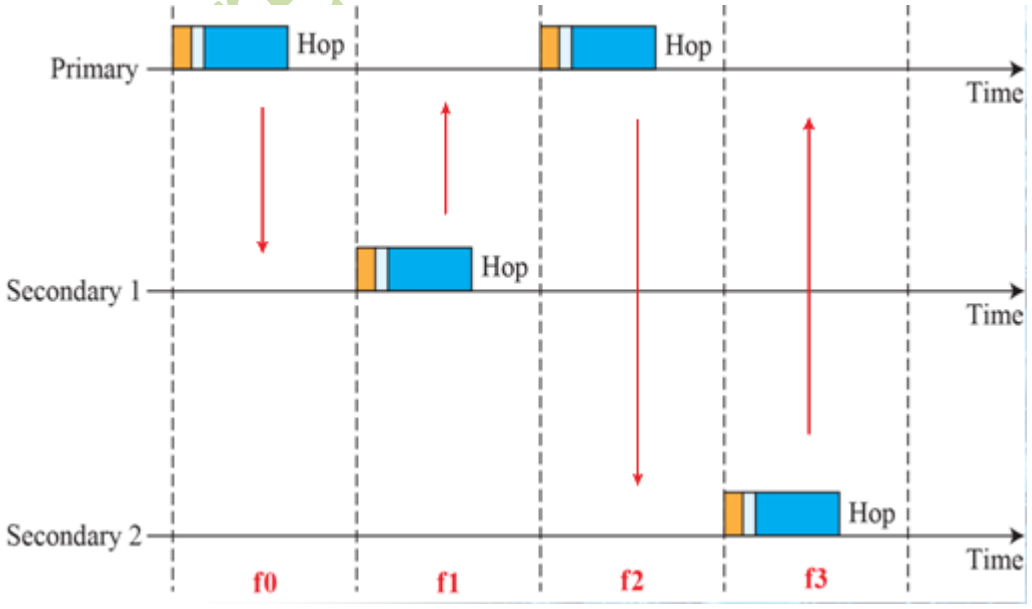


L2CAP Data Packet Format

Single-Secondary Communication



Multiple-Secondary Communication



Frame Format Types