St. JOSEPH'S COLLEGE OF ENGINEERING, CHENNAI – 119
DEPARTMENT OF EEE
CS2363 – COMPUTER NETWORKS - NOTES UNIT – I

Introduction

Computer Network :

- A computer network is a **group of computer systems** and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Networks are used to:

- Facilitate communication via email, video conferencing, instant messaging, etc.
- Enable multiple users to share a single hardware device like a printer or scanner.
- Enable file sharing across the network.
- Allow for the sharing of software or operating programs on remote systems.
- Make information easier to access and maintain among network users.

Requirements for Network design :

- The first step is to identify the **set of constraints** and requirements that influence network design.
- An ***application programmer*** would list the services that his application needs, for example, a guarantee that each message the application sends will be delivered without error within a certain amount of time.
- A ***network designer*** would list the properties of a cost-effective design, for example, that network resources are efficiently utilized and fairly allocated to different users.
- A ***network provider*** would list the characteristics of a system that is easy to administer and manage, for example, in which faults can be easily isolated and where it is easy to account for usage.

Classification Of Communication Networks: - Based on size of networks

LAN:- LOCAL AREA NETWORK LAN is a **Privately owned network** with in a single building of few Kilometers in size. E.g.: office, factory uses LANS to share recourses and exchange information.

- LAN uses **broadcast n/w approach**.
- Speed of LAN **10 to 100 Mbps**.
- If LAN uses bus topology (i.e.) single cable it uses IEEE 802.3 mechanism. If LAN uses ring topology then it uses 802.5 mechanism
- For broadcasting in LAN , channel allocation can be static and dynamic. The channel is common and only one station can transmit.

MAN:

It contains a collection of machines that **spans over a city**. Speed is greater than LAN

WAN:

- It contains a collection of machines that spans over large geographical area.
- This n/w consist of 2 distinct components transaction lines and switching elements that are inter connected.
- Data from source to destination is routed across intermediate nodes.
- The purpose of intermediate nodes is to provide switching facility that move data from node to node until they reach their destination.

LAN	WAN
Scope of LAN is restricted to a small/ single building	**Scope of WAN spans over large geographical area country/ Continent**
LAN is owned by same organization	**A part of n/w asserts are owned or not owned.**
Data rate of LAN 10-100 Mbps.	**Data rate of WAN is Gigabyte.**

NETWORK PERFORMANCE - METRICS

- Network performance is measured in two fundamental ways**:**
  1) B*andwidth / throughput* and 2) *latency /delay*.

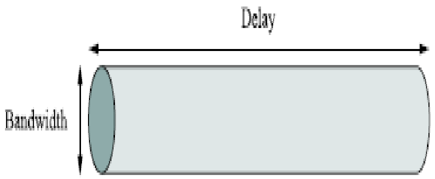
Bandwidth :

- The **bandwidth** of a network is given by the **number of bits that can be transmitted over the network** in a certain period of time. For example, a network might have a bandwidth of 10 million bits/second (Mbps), meaning that it is able to deliver 10 million bits every second.

Latency :

- The second performance metric **latency**, corresponds to **how long** it takes a message to travel from one end of a network to the other.
- Latency is measured strictly in terms of time.

Latency = Propagation + Transmit + Queue
Propagation = Distance/Speed Of Light
Transmit = Size/Bandwidth

Delay × Bandwidth Product	
• Channel between a pair of processes as a **hollow pipe.** • latency - corresponds to the **length of the pipe.** • bandwidth - gives the **diameter** of the pipe. • The delay × bandwidth product - gives the volume of the pipe. • ie)—the maximum number of bits that could be in transit through the pipe at any given instant.	

RTT – Round trip time : In telecommunications, the RTT is the **length of time it takes for a signal to be sent** plus the **length of time it takes for an acknowledgment** of that signal to be received.

<u>NETWORK / PROTOCOL ARCHIECTURE</u>

•Network designers have developed **general blueprints**—usually called ***network architectures***—that **guide the design** and implementation of networks.

Layering and Protocols

- Protocol is the **set of rules** governing the exchange of data between 2 entities. It defines

what is communicated, **how** it is communicated, **when** it is communicated.

Key elements of Protocol

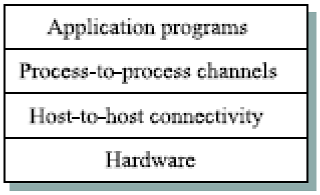
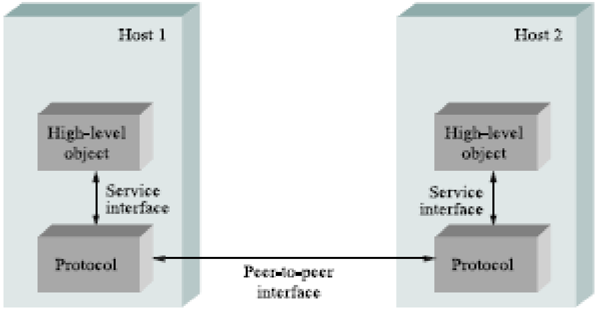
- Syntax – It refers to the structure or format of data meaning the order in which they are presented.
- Semantics – It refers to the meaning of each section of bit. How to do interpretation.
- Timing – When data should be sent and how fast they can be sent.

Layered Protocol Hierarchy: Networks are organized as a **series of layers** each built upon the other one.

Layer n of one machine can communicate with Layer n of another machine.(ie) **Peer-Peer communication.**

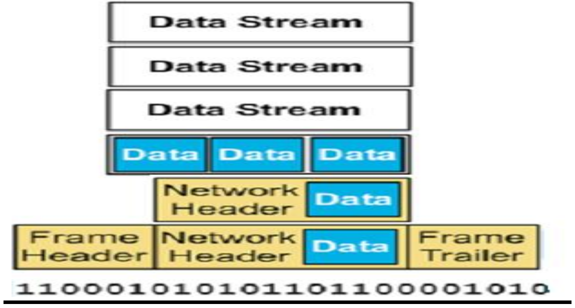
Between each pair of adjacent layers, there are **interfaces**.

- Interface provides **primitive operations and services** that lower layer provides to upper one. A set of **layers and protocol** is called **network architecture**. A list of protocols used by a system is called **protocol stack**.

Layered - Architecture	Service and Peer Interface
	

Encapsulation

High-level messages are **encapsulated** inside of low-level messages. Headers are usually attached to the front of a message.



Advantages of Protocol Layered Architecture:

- It reduces **design complexity**.
- It decomposes the problem of building a network into **more manageable components**.
- It provides a **modular design**, if we want to add some new service, we may only need to modify the functionality at one layer, **reusing the functions** provided at all other layers

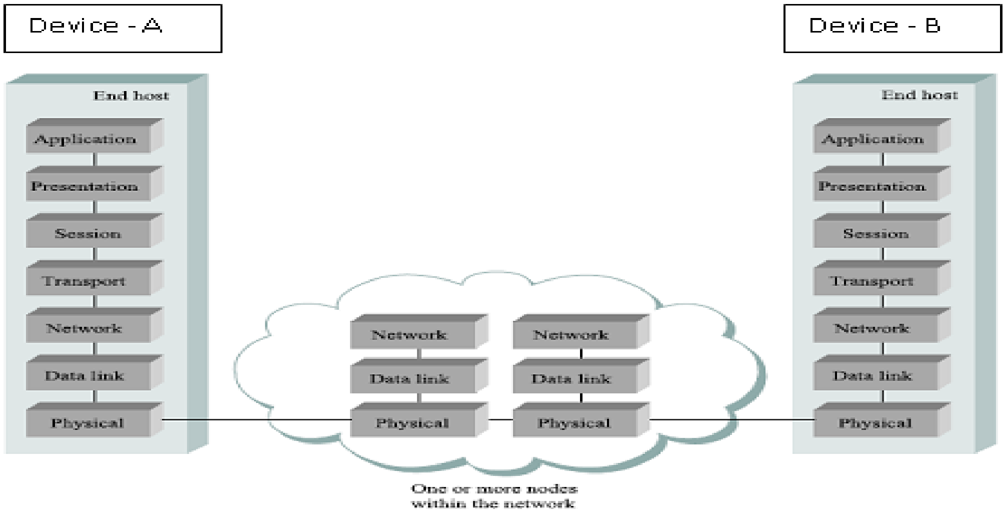
DisAdvantages of Protocol Layered Architecture:

- Creating distinct layers for different level of abstraction is not easy.
- Defining boundaries, interface functions is difficult.

- There are two network architectures
  1. ISO- OSI – International Standards Organization Open Systems Interconnection
  2. TCP / IP - Transmission Control Protocol / Internet Protocol [or]
  Internet Architecture

1. ISO- OSI - Architecture

- **The OSI model is built of Seven ordered layers:** Physical layer, Data link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer.
- The following figure shows the layers involved when a message is sent from device A to device B .
- As the message travels from A to B it may pass through many intermediate Nodes. These **intermediate nodes** usually involve only the **first three layers** of the OSI model.



1. Functions of Physical layer – Data is transmitted **in raw bits.**
The physical layer defines the characteristics of the interface between the device and the transmission medium, **Representation of bits ie)** type of **encoding** to be done, **Date rate** number of bits sent and **Line configuration** to define connection of devices to the medium.

2. Functions of Data link layer – Data is transmitted **in the form of frames.**
This layer is responsible for a **node-to-node delivery.**
The functions carried out by data link layer are framing, flow control , error control and access Control.

- **Framing:-**It divides the stream of bits received into manageable data units called **frames** .
- **Physical addressing**: Adds the header to the frame to define the physical address (MAC address –size 48 – bits) of the sender and / or receiver of the frame.
- **Flow control:** It is the process of managing the **rate of data transmission** between two nodes **to prevent a fast sender** from overwhelming a slow receiver.
- **Error control:** Mechanisms to detect and **retransmit damaged or lost frames** .
- **Access control:** It determines which device has control, When two or more devices are connected to the same link.

3. Functions of Network layer – Data is transmitted **in the form of Packets (data grams).**

- The network layer is responsible for the **source to destination delivery** (end-end) of **a packet.**
- **Logical addressing;** Addressing system to help distinguish the source and destination systems across networks.

- The network layer adds a header to the packet coming from the upper layer includes the logical address of the sender and receiver.
- **Routing:** When independent networks or links are connected together to create an internetwork or a large network, the connection devices route the packet to their final destination.

4. Functions of Transport layer – Data is transmitted **in the form of segments.**

- The transport layer is responsible for source to destination delivery **(end-end)** of **the entire message.**
- **Service-point addressing.** Computers often run several programs at the same time. The transport layer header therefore must include a type of address called a **service point address or port address** to communicate with specific process.
- **Segmentation and reassembly**. A message is divided into transmittable segments, each segment containing a sequence number and reassembled at the receiver side.
- **Connection control:** The transport layer can be either connectionless or connection oriented. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred the connection is terminated.
- **Flow control.** In this layer flow control is performed **end-end** rather than across a single link.
- **Error control**. Like the data link layer, the transport layer is responsible for error control layer. However error control at this layer is performed **end-end** rather than across a single link.

5. Functions of Session layer

- The session layer is the network **dialog controller.**
- **Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place either in **half –duplex of full-duplex**.
- **Synchronization:-** The session layer allows a process to add **checkpoints** (synchronization points) into a stream of data.

6. Functions of Presentation layer

- This layer is concerned with the **syntax and semantics** of the information exchanged .
- **Translation:** The exchanging information in the form of character strings, numbers and so on. The information should be changed to bit streams of types like BCD etc.
- **Encryption:** The sender transforms the original information to **another form** and sends the resulting in scrambled message in the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression:** Data compression reduces the no of bits to be transmitted. Data compression becomes particularly important in the transmission **multimedia such as text, audio and video**.

7. Functions of Application layer

The application layer enables the user whether human or software, too access the network.

- **Network virtual terminal:** A network virtual terminal is a software version of physical terminal and allows a user to logon to a remote host.
- **File transfer, access and management (FTAM)**:This application allows a user to access files in a remote computer, to retrieve files from a remote computer and to manage or control files in a remote computer.
- **Mail services:** This application basis for email forwarding and storage.
- **Directory services** : This application provides distributed database sources and access for global information a about various object and services.

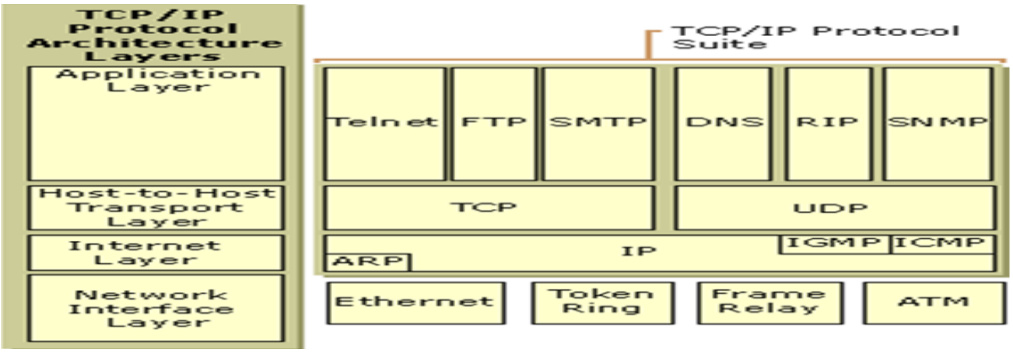
2. Internet Architecture or TCP/IP Protocol Architecture

Transmission control Protocol/ Internet protocol has **5- layers.**

1. Application layer 2. Host-to- Host Transport layer 3. Internet layer 4. Network Access layer
5. Physical layer.

The “Network” layer shown here is sometimes referred to as the “sub-network” or “link” layer

- Three main features
  - Does **not imply strict layering**. The application is free to bypass the defined transport layers and to directly use IP or other underlying networks
  - An **hour-glass shape** – wide at the top, narrow in the middle and wide at the bottom. IP serves as the focal point for the architecture
  - In order for a new protocol to be officially included in the architecture, there needs to be both a protocol specification and at least one (and preferably two) representative implementations of the specification



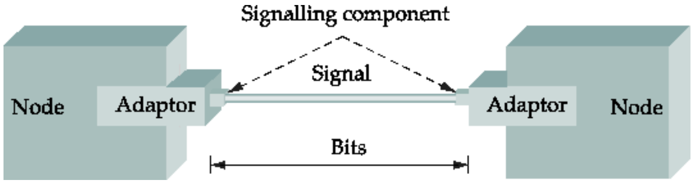
- Several protocols such as telnet for remote login , **FTP** -File Transfer Protocol for downloading files from file server ,**SMTP** – Simple Mail Transfer Protocol for e-mail application , **DNS** – Domain Name System for mapping domain name to IP- address and Routing Information Protocol (**RIP**) for routing, Simple Network Management Protocol (**SNMP**) for Network Management are defined in Application layer.
- In Transport layer TCP- Transmission Control Protocol for connection- oriented service and UDP – User Datagram Protocol for connectionless service are defined.
- In network layer Internet Protocol (IP) that provides connectionless delivery and **error reporting mechanism** provided by **Internet Control Message Protocol (ICMP)** are defined.
- Network interface layer combines the functions of physical and data link layer of ISO-OSI.

PHYSICAL LAYER :- ENCODING & TOPOLOGY

ENCODING

- A digital signal is a sequence of **discrete, discontinuous voltage pulses**. Each pulse is a signal element.
- **Binary data** are transmitted by encoding each **data bit into signal elements.**
- The **network adaptor** contains a **signaling component** that actually encodes **bits into signals** at the sending node and **decodes signals into bits** at the receiving node.
- The obvious thing to do is to map the

data value 1 onto the high signal
and the **data value 0 onto the low signal**.



Encoding Techniques	
NRZ	BIPHASE
NRZ –L 0 – bit → high voltage 1 - bit → low voltage	**Manchester code** 0- bit → Transition from high to low in the middle of interval. 1- bit → Transition from low to high in the middle of interval.
NRZ –I 0 – bit → No transition 1 - bit → transition at the beginning (from low voltage – to high voltage and vice versa)	**Differential Manchester code** Always transition in the middle of interval. 0- bit → Transition at the beginning of interval. 1- bit → No transition at the beginning of interval.

1. NON-RETURN TO ZERO (NRZ)

- The data value 1 map onto the high signal and the data value 0 onto the low signal.
- A **negative voltage** is used to represent one binary value(either for zero or for 1) and a **positive voltage** is used to represent the other.

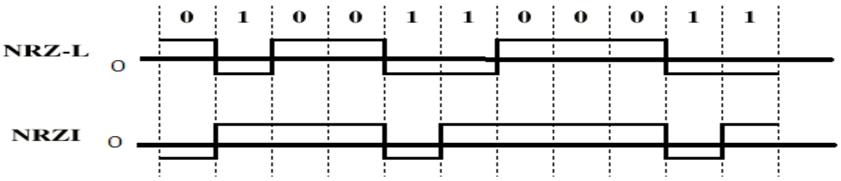
Problem with NRZ

Baseline wander

- The receiver keeps an average of the signals it has seen so far
- Uses the average to distinguish between low and high signal
- When a signal is significantly low than the average, it is 0, else it is 1
- Too many **consecutive 0's and 1's** cause this average to change, making it difficult to detect

Clock recovery

- Frequent transition from high to low or vice versa are necessary to enable clock recovery
- Both the sending and decoding process is driven by a clock
- Every clock cycle, the sender transmits a bit and the receiver recovers a bit
- The sender and receiver have to be precisely synchronized



2. NRZI (Non return to zero, invert on ones)

- To overcome the problems in NRZ , a variation of NRZ known as NRZI is used. As NRZ-L, NRZI maintains a constant voltage pulse for the duration of a bit time.
- The data themselves are encoded as the presence or absence of a signal transition at the beginning of bit time.

- **A transition at the beginning of a bit time denotes a binary 1** for that bit time; **no transition indicates a binary 0**. NRZI is an example of differential encoding.

Advantages of NRZ

- **NRZ codes** are easiest and make efficient use of band width. If an NRZ code is used to generate a signal with data rate of 9600 bps, most of the energy in the signal is concentrated between dc and 4800 Hz.
- Because of their simplicity and relatively low-frequency response characteristics, NRZ codes are commonly used for digital magnetic recording.

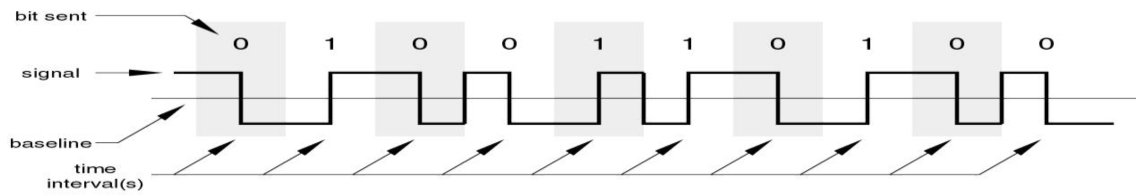
Limitations of NRZ

- The limitations are the presence of dc component and the lack of synchronization capability.

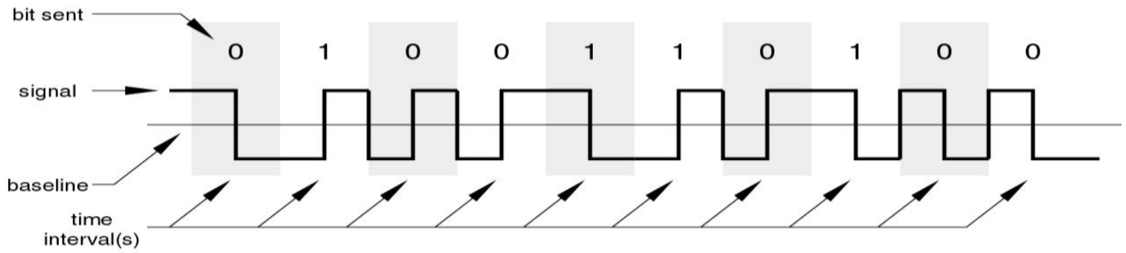
3. BIPHASE:

- Two of these techniques, Manchester and differential Manchester, are in common use
- In **Manchester code,** there is a transition at the middle of each bit period. The mid bit transition serves a clock mechanism and also as data: a low-to-high transition represents a 1, and high-to-low transition represents a 0.
- In **Differential Manchester code**, the mid bit transition is used only to provide clocking. The encoding of a 0 is represented by the absence of transition at the beginning of a bit period, and a 1 is represented by the absence of transition at the beginning of a bit period. Differential Manchester has added advantage of employing differential encoding.
- **Disadvantage:** All of the biphase techniques require at least one transition per bit time and may have as many as two transitions thus, the maximum modulation rate is twice that for NRZ; this means that the bandwidth required is correspondingly greater
- The biphase scheme has several **Advantages**
    - ❖ Synchronization
    - ❖ No dc component
    - ❖ Error detection

Manchester Encoding

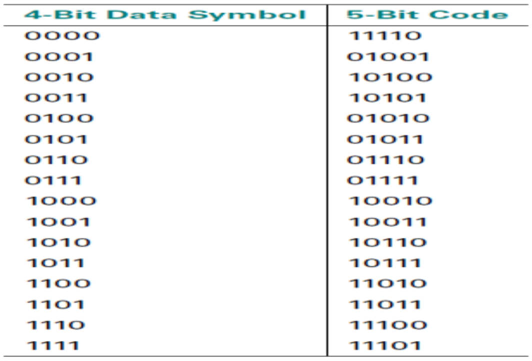


Differential Manchester Encoding



4. 4B/5B encoding

- o Insert extra bits into bit stream so as to break up the long sequence of 0’s and 1’s
- o Every **4-bits of actual data** are encoded in a **5- bit code** that is transmitted to the receiver
- o 5-bit codes are selected in such a way that each one has no more than one leading 0(zero) and no more than two trailing 0’s.
- o No pair of 5-bit codes results in more than three consecutive 0’s



4-Bit Data Symbol	5-Bit Code
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

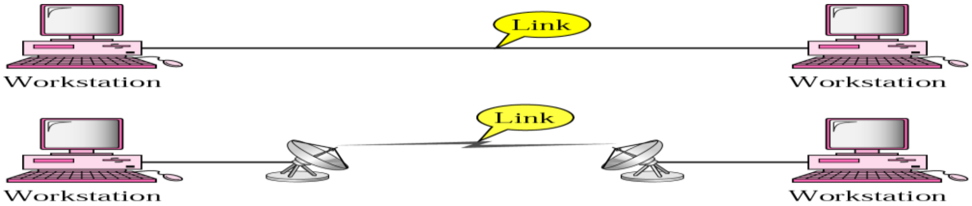
POINT-TO-POINT AND MULTIPOINT CONFIGURATION

Line Configuration /Transmission line

It refers to the way in which two or more communication devices are attached to a link. It is categorized into two types, **Point-to-Point** and **Multi-Point**

Point – to – point

- **Point-to-point** connection provides a **dedicated link** between two devices.
- The entire **capacity of the link is reserved** for transmission between those two devices.
- Most point-to-point connections use an **actual length of wire** or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

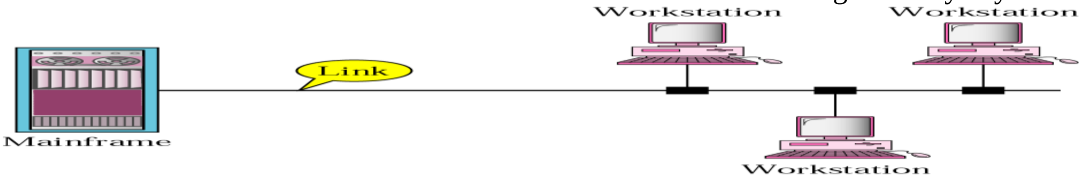


Example

- When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

Multi-Point

- It is one in which **more than two** specific devices share a single channel.
- All the devices connected to the channel/link will receive the message sent by any device.



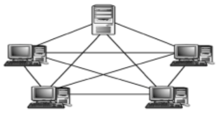
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a ***spatially shared*** **connection.** If users must take turns, it is a ***timeshared*** **connection.**

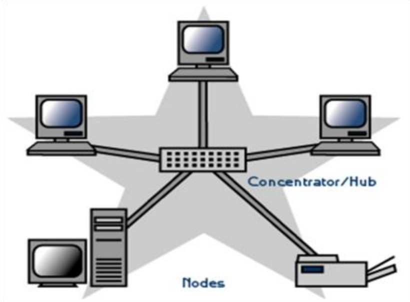
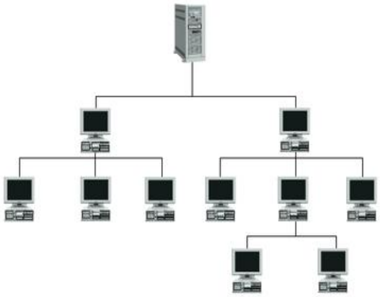
Network Topology:

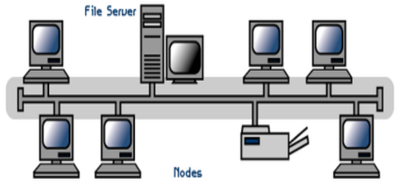
The term "**Topology**" refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected.

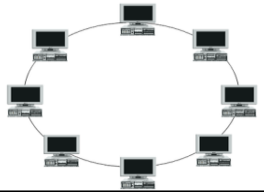
Point-to Point	Multi-point
(1) Mesh topology. (2) Star topology. (3) Tree (Hierarchical) topology.	(4) Bus topology. (5) Ring topology.

- Ring and mesh topologies are convenient for peer to peer transmission.
- Star and tree are more convenient for client server.
- Bus topology is equally convenient for either of them.

Mesh topology	Advantages	Disadvantages
• Every device has a dedicated **point-to-point link** to every other device. • No.of connections needed for n-devices n(n-1)/2 	• Many traffic problems can be eliminated. • It is robust. • Security is more. • Fault identification is easy. • Speed.	• Amount of cabling, cost, space is more. • Number of I/O ports. • Installation and reconfiguration is difficult. •Hardware and requirement is more expensive.

Star Topology	Advantages	Disadvantages
• In a star topology, every computer is connected to a centralized device called a **HUB**. • Each device communicates with the other through the hub.  	• It is less expensive than mesh. • Each device needs only one link and one I/O port. • It is easy to install and reconfigure. • Less cabling is needed. • Robustness. Easy fault identification.	• Failure in centralized hub will severely affect the communication.
Tree (Hierarchical) topology	Advantages	Disadvantages
• It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the **central hub**. • The central hub is the **active hub**.. 	• Less Expensive. • Fault identification is easy. • Every device has only one link and I/O port to the controller. • Installation and reconfiguration is easy. • More devices can be attached to central hub.	• Any problem in central controller will be serious.

Bus topology	Advantages	Disadvantages
• A bus topology connects computers along a single or more cable to connect linearly. 	Mostly used in small networks. Good for LAN.	Security is very low. Fault identification is not easy.

Ring topology	Advantages	Disadvantages
• The ring network is like a bus network, but the "end" of the network is connected to the first node 	• Fault identification is easy. • Adding and deleting devices is easy. • Installation and reconfiguration is easy.	• Unidirectional traffic. • Any failure in the link can disable the network.

LLC- LOGICAL LINK CONTROL - FRAMING , ERROR DETECTION & FLOW CONTROL (RELIABLE TRANSMISSION)

FRAMING

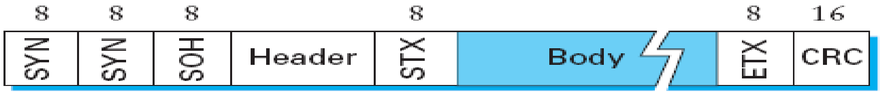
It is a method of **grouping of bits** into manageable unit known as **frame** in data link layer. Framing protocols are categorized into two as shown in the table.

Framing Protocols	
Bit oriented protocol	**Byte oriented protocols**
i) SDLC / HDLC SDLC – **S**ynchronous **d**ata link control . HDLC - High Level Data Link control. Frame boundary is defined by special flag **0 1 1 1 1 1 1 0**	**i)** BISYNC - **Bi**nary **Syn**chronous **C**ommunication **:** Frame boundary is defined by sentinel characters **STX , ETX and DLE** **ii)** PPP - **P**oint to **p**oint **p**rotocol **:** Frame boundary is defined by special flag **0 1 1 1 1 1 1 0** **iii)** DDCMP - **D**igital **D**ata **C**ommunication **M**essage **P**rotocol – **Byte counting** approach.

Byte oriented protocols :

1) <u>BISYNC</u> : - Binary Synchronous Communication protocol.
Supports ASCII , EBCDIC and transcode.

Frame format of BISYNC :



SYN - Synchronization character
The data portion of the frame is then contained between special ***sentinel characters:*** *STX (start of text) and ETX (end of text).*
SOH - Start of header. CRC – Cyclic Redundancy Check.

- **Character stuffing / Byte stuffing** avoids the problem of appearance of special sentinel character ETX in the middle of data by "escaping" the ETX character by preceding it with a data-link-escape (DLE) .

(Ex). ETX – Appears in the middle of data

STX ABCXYETXZACLAM ETX

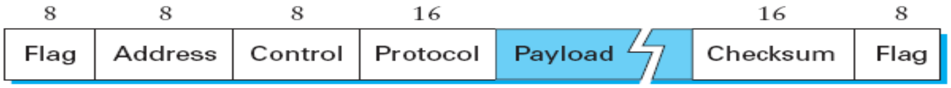
Character stuffing:

STX ABCXY **DLE ETX** ZACLAM ETX

- if **DLE** char appears in the middle then include **another DLE char**.

2) Point – point Protocol

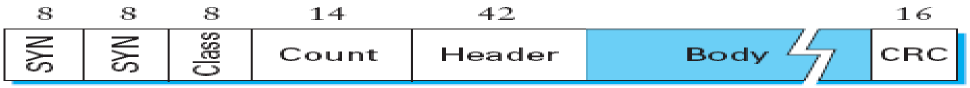
- It uses special sentinel characters.
- It also uses character stuffing.
- FLAG is the special character used



Flag :
It is the **special character** used to identify the starting and ending of the frame.
Flag : **0 1 1 1 1 1 1 0**
Address & Control : Address and control are default characters.
Protocol : It identifies the high level protocol IP / IPX
Payload : It is the msg to be transmitted. Default size 1500 bytes.
Checksum : used to detect the error.

3) <u>DDCMP</u> – Digital Data communication Message Protocol.

- It follows byte **counting** approach.
- It includes a **field "Count**" in the frame header which defines the no. of bytes in the data.

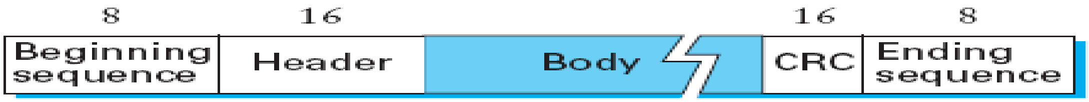


SYN : It synchronizes the sender and receiver and indicate the beginning of the frame.
Count : It specifies the no. of bytes in the data.
Body : The message.

- CRC – It is used to detect the error in the transmission.
- Transmission error could **corrupt the Count field**. In that case the end of the frame would not be correctly detected. This is known as **framing error.**

Bit-oriented protocol

SDLC / HDLC - High Level Data Link control, SDLC – Synchronous data link control .



- Beginning Sequence : it synchronizes the sender's and receiver's clock and indicates beginning of the frame.
- Body : The actual message or data transmitted.
- CRC : It is used to detect the error.
- Ending Sequence : The end of the frame.
- It uses bit stuffing.
- Bit stuffing avoids the problem of appearance of special sequence of bit in the middle of the data.
- Whenever five 1's appear in the body of the message the sender insert a zero before transmitting the next bit.
- Ex: Data : 1 1 1 1 1 1 0 1 0
  Data with bit stuffing : 1 1 1 1 1 **0** 1 0 1 0
- On the receiver side after receiving the five consecutive 1's it looks the 6th bit.
  - Case i) :- if it is zero then it is stuffed bit , it should be removed.
  - Case ii) :- If it is one then it is the end of the data or error.

ERROR DETECTION

ERRORS

- **Single bit error:** One bit in the data unit have changed from 1 to 0 or from 0 to 1.
- The term **burst error** means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.
- **Burst errors does not** necessarily **mean that the errors occur in consecutive bits**, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.
- Error detection means to decide **whether the received data is correct or not without having a copy of the original message.**

Two basic approaches in Error control

1) Error detection and retransmission: If there is error the sender is notified about error. Then the sender will retransmit the copy of a message.

2) FEC –.: This allows the receiver to reconstruct the original message even after the message was corrupted. Detection & correction of errors are handled in advance by sending **redundant bits.**

Detection and Retransmission	Forward Error Correction
It detects errors. T o Correct the error the Message has to be retransmitted from the sender.	It detects the error as well as correct the errors.
Only less no. Of redundant bits are required.	More no. of redundant bits.
It is useful when errors are not occurring frequently.	It is useful when errors are more possible.
Time delay occurs to correct the error until retransmission is over.	Collection of errors can be handled in advance rather than waiting.

- There are 4 error detection methods.

1) VRC – Vertical Redundancy Check. (1- Dimensional parity check)
2) LRC – Longitudinal Redundancy Check. (2-Dimensional parity check)
3) Check sum. / Internet check sum
4) CRC – Cyclic Redundancy Check.

1 . ONE DIMENSIONAL PARITY CHECK (VRC)

- In this technique, a redundant bit known as **parity bit** is appended to every data unit so that total number of bits including that parity bit is even (odd) namely even (odd) parity check.

Sender side - Parity Generator	**Receiver side** - Parity Checker
Data : 0 0 1 0 0 1 1 Parity : **1** Data sent : 0 0 1 0 0 1 1 **1** No. of 1's = 4 – even parity	When the receiver receives the data the number of 1's will be counted. Data received : 0 0 1 0 0 1 1 1 No. of 1's = 4 - No error If data received is 0 0 1 0 0 1 1 **0** No . Of 1' s = 3 which is not even. - Error

PERFORMANCE

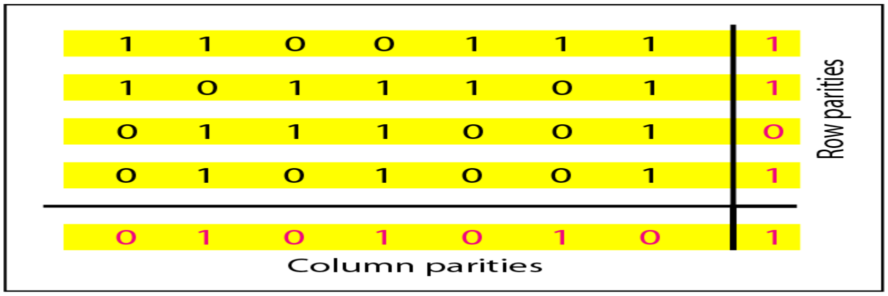
- It detects all single bit errors
- It can detect burst errors only if total number of bits changed is odd
- It can not detect any even number of errors

2. TWO DIMENSIONAL PARITY CHECK (LRC)

- Divide the data into **rows and columns.**
- Include the **parity bit** row wise and column wise.
- ie) the parity bit is introduced corresponding to every row and every column so that the total no. of 1's in every row and column including the parity bit becomes even.
- Either odd or even parity can be used.
- Consider 28 bits data

DATA

- 1100111 1011101 0111001 0101001
- Divide into 4 rows each with 7 bits



1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	1

Row parities
Column parities

a. Design of row and column parities

- LRC detects single as well as burst errors.
- If two bits in one data units are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.
- It needs r+c extra redundant bits for data of rc bits

3. CYCLIC REDUNDANCY CHECK (CRC)

It is the most efficient method. At sender side a sequence of **redundant bits (CRC remainder)** is appended to the end of data unit so that resulting data unit becomes exactly divisible by a predetermined binary number.

At receiver side, the incoming data unit is divided by same number, if reminder =0, the Data is accurate, if reminder is not equal to zero, the data is damaged.

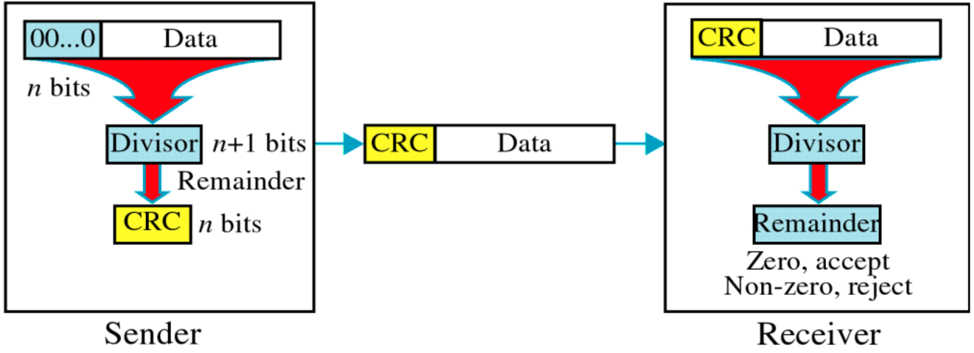
- For Given a **k-bit *message***, the transmitter (sender) generates an **n-bit sequence**, known as a *frame check sequence (FCS)*, the resulting (k+n) bits is exactly divisible by some predetermined number known as *CRC divisor.*

STEPS ON SENDER SIDE:

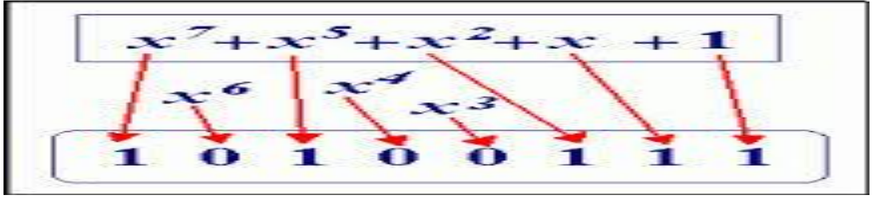
1. Append **n - zeros** to the data unit if the predetermined CRC divisor is of **n+1** bits
2. The new data unit is divided by the **predetermined divisor** and the remainder is found (**CRC remainder**).
3. Replace appended zeros in the data unit by CRC remainder

RECEIVER

- The receiver then divides the incoming data by the same CRC number and,
- if there is **no remainder**, assumes that there was **no error**.
- Otherwise data is corrupted one



Mapping Polynomial and Binary form of Divisor: Every CRC polynomial can be uniquely mapped into a binary sequence and vice versa.

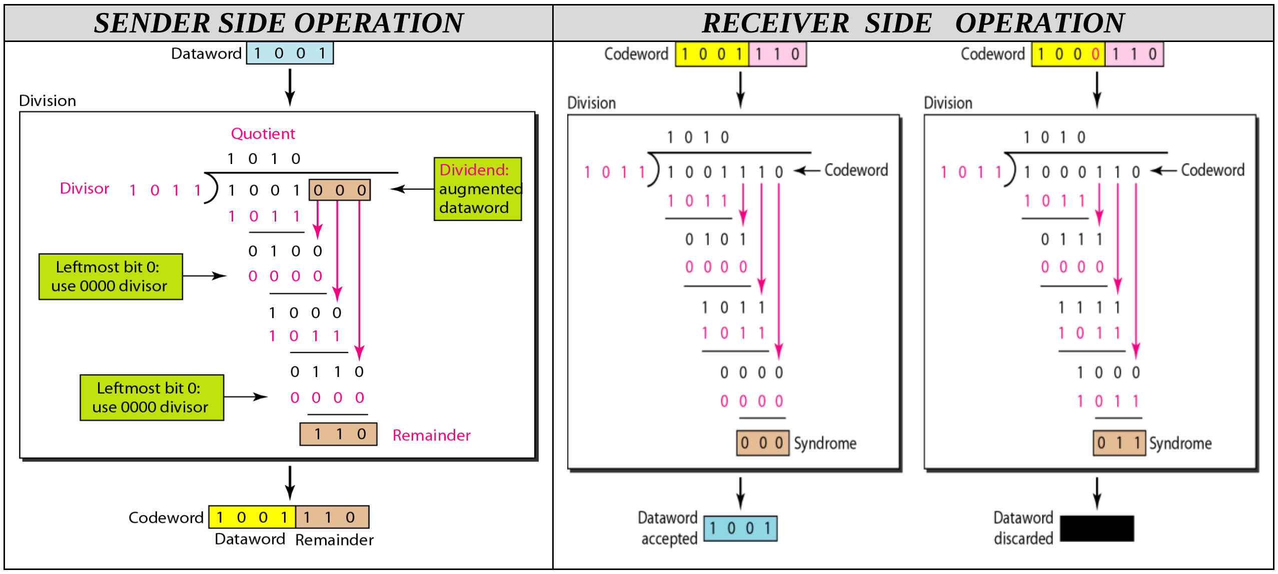


Example:

DATA : 1001

DIVISOR : x^3+x+1 → 1011

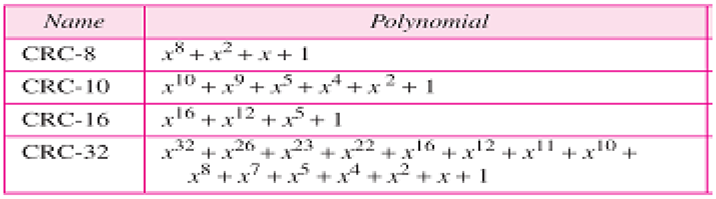
APPENDED DATA : 1001**000** **(since divisor has 4- bits , 3 zeros will be appended)**



PERFORMANCE

- It can detect all single bit errors (x^n and x^0 have non zero coefficient)
- It can detect all burst errors of length less than the length of the predetermined divisor
- It is the most efficient method.
- It uses less number of redundant bits.
- Performance is better than other methods

Some CRC – Polynomials

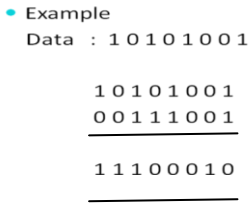


Name	*Polynomial*
CRC-8	$x^8 + x^2 + x + 1$
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$
CRC-16	$x^{16} + x^{12} + x^5 + 1$
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} +$ $x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

4. ***CHECK SUM***

It is used in higher layer protocols. It consists of two components

1. Check sum generator 2. Checksum Checker

Sender - side Check sum generator	**Receiver - side** Check sum Checker
1) The data is divided into block of rows and columns. 2) All sections of data are added together using 1's complement. 3) The resultant sum is complemented and taken as check sum. 4) This check sum is attached with the data and transmitted.  • Example Data : 1010100100111001 10101001 00111001 11100010 ● Take complement of the sum 1 1 1 0 0 0 1 0 **0 0 0 1 1 1 0 1 .** **Data sent is Data + checksum** 1 0 1 0 1 0 0 1 0 0 1 1 1 0 0 1 **<u>0 0 0 1 1 1 0 1</u>**	1) The received data is divided into k +1 sections of n-bits. 2) Add all the sections using 1's complement. 3) complement the resultant sum. 4) If the result is zero , accept the data otherwise reject it. Received data : 1 0 1 0 1 0 0 1 0 0 1 1 1 0 0 1 **<u>0 0 0 1 1 1 0 1</u>** 1 0 1 0 1 0 0 1 0 0 1 1 1 0 0 1 0 0 0 1 1 1 0 1 1 1 1 1 1 1 1 1 Take the complement of the sum. Data is accepted.

Performance

- The checksum detects all errors involving an odd number of bits.
- It detects most errors involving an even number of bits.
- If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.

<u>FLOW CONTROL MECHANISMS:</u>

1. STOP –WAIT protocol:

- Source transmits frame. Destination receives frame and replies with acknowledgement
- Source waits for ACK before sending next frame Destination can stop the flow by not send ACK

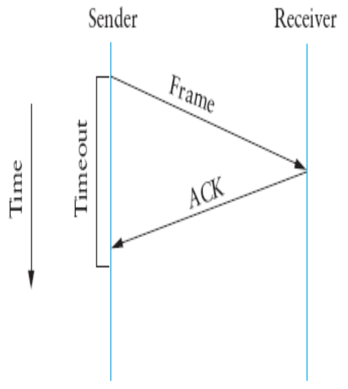
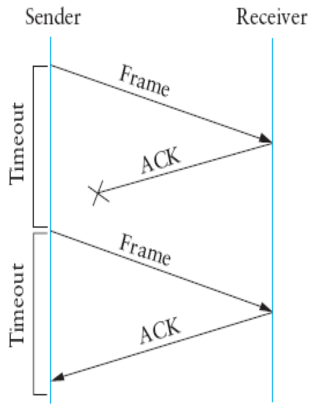
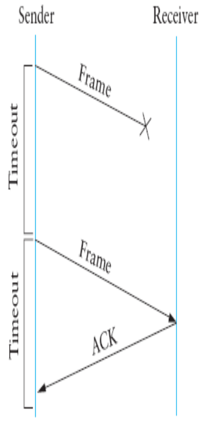
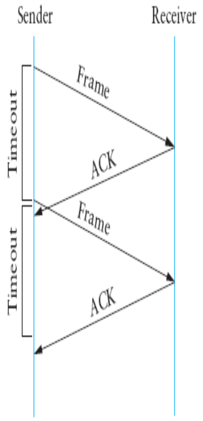
Stop and Wait Time out mechanism:

- When a sender transmits a frame ,it sets a corresponding timer. If the sender does not receive any ACK before the timer expires then it retransmits the original frame. Thus the sender waits for a reasonable time before retransmission.

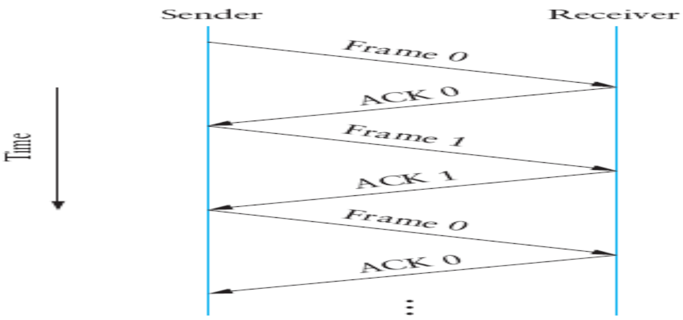
PREFORMANCE – **Limitations of stop and wait**

- It is a simple protocol .Works well for a few transmission of large frames. It is suitable for Half duplex mode
- It is inadequate because it allows the **sender to have only one outstanding frame** on the link at a time resulting **in poor utilization of link capacity and time** . It is not suitable for full duplex mode

Time Line Diagram of Stop and Wait protocol

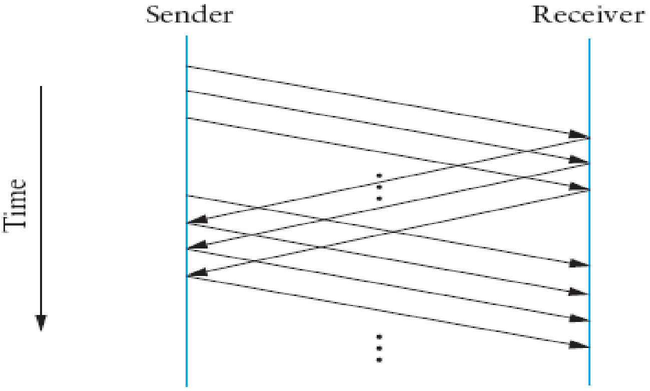
ACK - Received	ACK Lost	Frame lost Time out soon
	 Sender Receiver Frame ACK Timeout Frame ACK Timeout	 Sender Receiver Frame Timeout Frame ACK Timeout Sender Receiver Frame ACK Timeout Frame ACK Timeout

- If the ACK is lost or arrived late , **retransmission of the same frame** will take place. Thus produces **duplicate copy** of the delivered frame.
- To address this problem, the header for a stop-and-wait protocol usually includes a **1-bit sequence number that takes bit value 0 0r 1**.



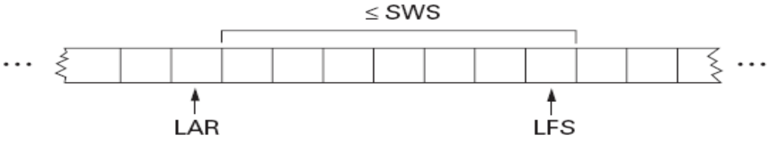
SLIDING WINDOW FLOW CONTROL

- **Allow multiple frames** to be in transit. Receiver has buffer of n frames . Transmitter can send up to n frames without receiving ACK of the first frame. Each frame is numbered. ACK includes number of next frame expected. Sequence number of k bits used to represent frame 0,1,2….. 2^k
- If window size is N , it can send N frames without waiting for ACK



- The sliding window algorithm works as follows..

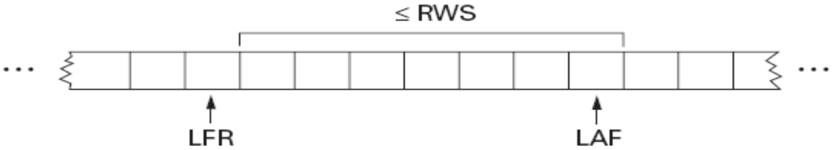
  Sender : The sender maintains three variables such that **LFS − LAR ≤ SWS**
  - ***SWS*** - *sender window size*- gives the upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit;
  - **LAR** denotes the sequence number of the *last acknowledgment received;*
  - ***LFS*** *-denotes the sequence number of the last frame sent.*



- The sender associates a timer with each frame it transmits, and it retransmits the frame should the timer expire before an ACK is received. When an acknowledgment arrives, the sender moves LAR to the right, thereby allowing the sender to transmit another frame.

Receiver: The receiver maintains three variables:

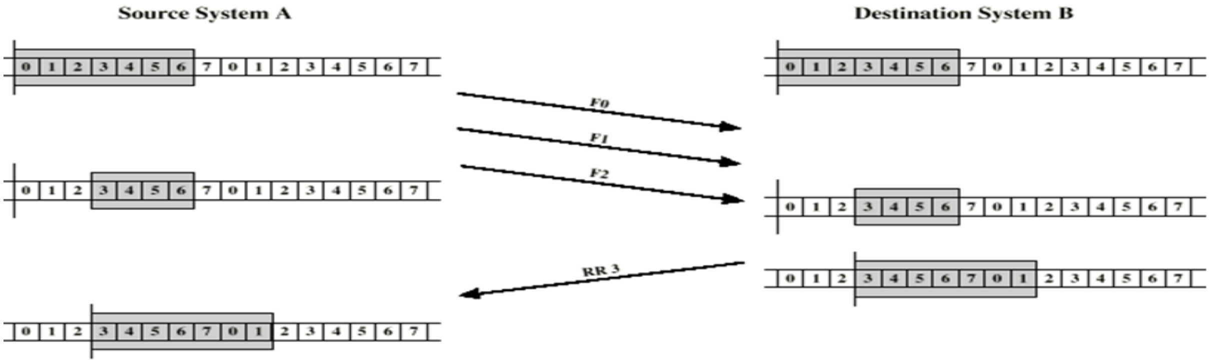
- RWS (*receive window size)* - gives the upper bound on the number of out-of-order frames.
- LAF - the sequence number of the *largest acceptable frame;*
- *LFR - the sequence number of the last frame received.*



The receiver maintains **LAF − LFR ≤ RWS**

- If SeqNum ≤ LFR or SeqNum > LAF, then the frame is outside the receiver's window and it is **discarded.**

- If LFR < SeqNum ≤ LAF, then the frame is within the receiver's window and it is **accepted**.
- The following diagram shows the alternate shrinking and growing of sender/receiver window.



Acknowledgements

1.Cumulative Ack-

- Ack contains the sequence number of the next frame expected to arrive indicating all frames of previous seq .no arrived Suppose Frames are received out of order- before getting 5th frame 6 and 7 are received, receiver will not send the Ack for 6 and 7 but wait for 5th frame .
- Ack of type **RR n** means ready to receive nth frame and cumulative ack for 0,1,2,3…n-1.

2. PIGGYBACKING:

If any station sends as well as receives the data it should maintain two windows. To do it efficiently we can use piggybacking .each data frame includes a filed that holds sequence number of that frame and a field that holds sequence number of the received frame for acknowledgment

3. Selective acknowledgments.

- Receiver could acknowledge exactly those frames it has received.
  (eg)Frames are received out of order say before getting 5th frame 6 and 7 are received
- Ack will be sent for frames 6 and 7 thus inform the non- arrival of frame 5 to the sender.

Finite Sequence Numbers and Sliding Window

- A frame's sequence number is specified in a header field of some finite size and for a 3-bit field means that there are eight possible sequence numbers, 0 . . . 7.
- Reuse of sequence numbers is needed. Therefore receiver / sender is able to distinguish between different incarnations of the same sequence numbers.
- For this send window size may be set to satisfy the following inequality.
  SWS < *(*MaxSeqNum+1*)/*2 . ie for 3- bit field sequence number SWS < (7+1)/2.
  ie) Sequence number is divided into 2 halves. First half 0,1,2,3 and 2nd – 4,5,6,7.

Advantages

- Sliding window protocol reliably deliver frames across an unreliable link.
- Preserve the order in which frames are transmitted.
- Flow control.

MAC- MEDIA ACCESS CONTROL - IEEE 802.3 ETHER NET , IEEE 802.5 TOKEN RING , FDDI , WIRELESS NETWORKS

IEEE802.3--- ETHERNET

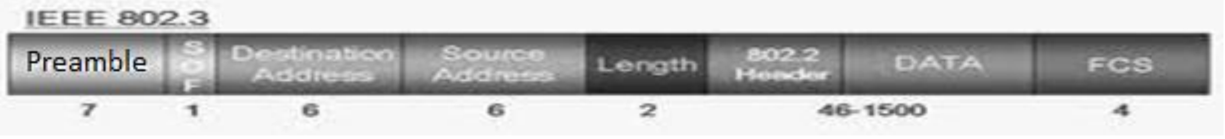
ACCESS METHOD CSMA/CD :- (Ethernet transmitter Algorithm)

- Whenever multiple user access a single line, there is a danger of overlapping and destroying called collision. As traffic increases collisions increases.
- The access mechanism used in Ethernet is called **Carrier Sense Multiple Access with Collision Detection(CSMA/CD).**
- Here any workstation that wishes to transmit, listen for existing traffic on the line. If the line is idle, it will transmit otherwise it waits until there is no traffic.
- **1- persistent CSMA** - The Ethernet is said to be a ***1-persistent* protocol** because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes **idle**.
- In general, a ***p-persistent* algorithm** transmits with probability $0 \leq p \leq 1$ after a line becomes idle, and defers with probability $q = 1 - p$.
- To detect collision after transmission, it checks the line for the line extremely **high voltage** that indicates a collision.
- If it finds any **collision** it quits current transmission and **waits a predetermined amount** of time for the line to clear and sends its data again.

Binary Exponential BACKOFF Algorithm

- It deals with **contention of a network**. If two hosts find the medium as idle then they start the transmission at the same time, it leads to collision.
- When the station detects that its frame **collide** with another frame , it will send **runt frame**(jam sequence) to inform to all other hosts about the collision.
- **Runt frames** - A runt frame is an Ethernet frame of 96 bits with preamble framing sequence.
- After the **first collision** each station waits for a predetermined time - **time slot [0,1**] retransmission at the beginning of that slot
- After the second collision each station waits for a predetermined time [0,1,2,3]
- In general after the **k-th** collision the slots available are $[0,1,2,\ldots 2^k - 1]$

FRAME FORMAT & FRAME ADDRESSING



PREAMBLE: It contains 7 bytes of alternate 0's and 1's that altering receiver about coming frame.

SFD: The second field 10101011 of the 802.3 frame signals the beginning of the frame SFD/SOF(Start of Frame) tells the receiver everything that follows is data , starting with address.

DESTINATION ADDRESS: DA field is allotted six bytes and contains physical address of the packets next destination

SOURCE ADDRESS It is also allotted 6 bytes and contains physical address of the last device to forward the packet.

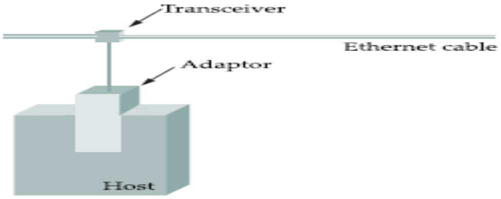
LENGTH/ TYPE OF PDU Next 2 bytes indicate number of bytes in the coming PDU. If the length of PDU is fixed, then this field can be used to indicate Type or base for other protocol.

DATA AND PAD Data may contain 0 to 1500 bytes. To identify valid frame from garbage, valid the full format should contain 64 bytes from destination address to checksum. So if the data portion is less than 46 bytes, pad field is used to fill out the frame to minimize size**.**

CRC The last field in 802.3 frame contains error detection information, in this case a CRC – 32 **.**

Physical properties of Ethernet

- A transceiver (a small device directly attached to the tap) detects when the line is idle and drives signal when the host is transmitting.

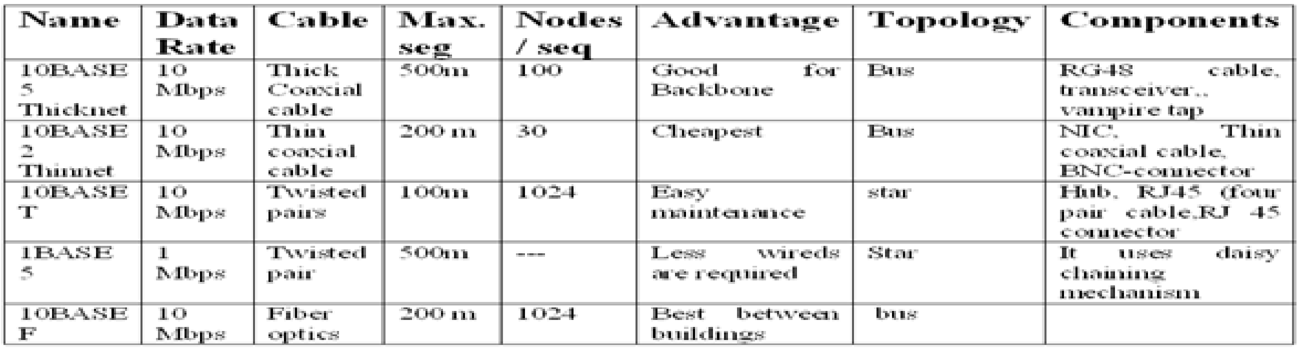


It **uses Manchester Encoding.** It supports data rate between 1 and 100 mps

Connecting Devices

- **Repeater:** It is operating at physical layer. A repeater **receiving** the weak signal regenerates the original strength bit pattern. So it helps to extend the length of physical n/w.
- **HUB:** when a station sends frame to hub, the frame is sent to all ports and every station will receive it. If 2 stations try to send frames simultaneously there is a collision.
- **SWITCH :**It at can recognize the destination address and can route the frame to that particular port to which the destination station is connected and the rest of the media are not involved in the transmission process.
- **Ethernet works on BUS Topology and STAR Topology**

Ethernet Technologies



Name	Data Rate	Cable	Max. seg	Nodes / seq	Advantage	Topology	Components
10BASE 5 Thicknet	10 Mbps	Thick Coaxial cable	500m	100	Good for Backbone	Bus	RG48 cable, transceiver.., vampire tap
10BASE 2 Thinnet	10 Mbps	Thin coaxial cable	200 m	30	Cheapest	Bus	NIC, Thin coaxial cable, BNC-connector
10BASE T	10 Mbps	Twisted pairs	100m	1024	Easy maintenance	star	Hub, RJ45 (four pair cable,RJ 45 connector
1BASE 5	1 Mbps	Twisted pair	500m	---	Less wireds are required	Star	It uses daisy chaining mechanism
10BASE F	10 Mbps	Fiber optics	200 m	1024	Best between buildings	bus	

The “10” in 10Base2 means that the network operates at 10 Mbps, “Base” refers to the fact that the cable is used in a *baseband* system, and the “2” means that a given segment can be no longer than 200 m.

- Another cable technology is 10BaseT
  - network operates at 10 Mbps
  - T stands for twisted pair
  - Limited to 100 m in length

Types of Ethernet LANs

- Fast Ethernet (100Base-T) :Operates at 100 Mbps
- Gigabit Ethernet : Operates at 1 Gbps and Uses fiber optic cable
- 10 Gbps Ethernet: Latest development of ethernet . IT Uses fiber optic cable
- Wireless Ethernet : IEEE 802.11 standard. It Operates at around 2.4 Gbps

TOKEN RING - 802.5

Access Method : Token passing – **delayed token release**

- All workstations are connected in a ring or star topology. Access method is a **token-passing scheme.**
- It is used to prevent the collision. **Token** is a special **three-byte frame** that travels around the ring.

Token

It is a simple frame of size 3 – bytes or 24 – bits.

SFD	AC	EFD

SFD - Starting frame delimiter
AC – Access control
EFD – Ending frame delimiter

It circulates around the ring from host to host. A host can **transmit** the data only when it **possess the token.**

How does token ring work? /Access Method (Token Passing)

- A station that wants to transmit a frame will capture token, Token frame is converted into data frame.
- Frame proceeds around the ring, being regenerated by each station. Each intermediate station examines the destination address, if the data is not for it, it sends to its neighbor.
- The receiver recognizes its own address copies the message, checks for errors and changes bits in the last byte of the frame to indicate its copying. The full packet continues around the ring until it returns to the station that sent it.
- The sender discards the data frame after checking address and copy bits of the frame and releases the token in the ring. This is known as **delayed token release**

Token ring Data frame format

SFD	AC	FC	DA	SA	DATA	CRC	EFD	FS
8 bits	8 bits	8 bits	48 bits	48 bits	up to 18200x8 bits	32 bits	8 bits	8 bits

STARTING DELIMITER: It is 1 Byte. It is used to alert the receiver and to mark starting of frame.

AC – Access Control: It is 1 Byte

First 3- bits – Priority bits 4th bit – token bit
M- bit set by the Monitoring station to discard the garbage frame.
R – bit to reserve the ring with priority.

FC – Frame control – to indicate whether control/data frame.

DESTINATION ADDRESS: The 2 to 6 bytes contains the physical address of the frames next destination.

SOURCE ADDRESS:The SA is also 2 to 6 bytes and contain the physical address of the sending station

DATA : The sixth field. Data can be of any length to be transmitted within the token holding time.

CHECKSUM: The CRC field is 4 bytes long and contains CRC-32 error detection sequence.

ENDING DELIMITER: The ED is the second flag field of 1 byte and indicates the end of the sender’s data and control information. It contains an E bit which is set if an interface detects an error.

FRAME STATUS: It is the last byte. It contains an A and C bits. When a frame arrives interface of a station of destination address, the interface turns on the A bit it passes through. If it copies the frame to the station it turns on C bit.

A = 1 --- Address recognized **C** = 1 ---- Frame copied
A = 0 ---- Destination is not present **C** = 0 ---- Frame not copied
A = 1 Address recognized **C** = 0 ---- Frame not copied due to error

Priority handling

- The priority is defined by the frame's priority and reservation fields. When a station wants to transmit a frame of priority n , then it must wait for a token of priority less than or equal to n. However if a higher priority has already been set, the station may not make a reservation
- When the current frame is finished, the next token is generated at high priority that has been reserved.

Active and standby monitors / Ring Maintenance

- AM – Active monitor Station and SM - Stand by Monitor are present in the ring
- The monitor contention process is initiated when a loss of signal on the ring is detected. . when a particular timer on an end station expires such as the case when a station hasn't seen a token frame in the past t sec.

Active monitor selection - Claim token

Claim token will be transmitted by a station that wants to become a Monitor station.
If there is a competition then the station with **highest MAC address** will win.

Monitor Functions

- To insert a 24-bit delay into the ring, to ensure that there is always sufficient buffering in the ring for the token to circulate.
- To ensure that exactly one token circulates..
- To detect a broken ring.
- To remove the damaged frame/ orphan frame

Control Frames :

Name	Control field	Purpose
BEACON	0000 0010	Takes action during ring failure
CLAIM-TOKEN	0000 0011	Electing Monitor station
ACTIVE-MONITOR PRESENT	0000 0101	Transmitted by AM periodically

Compare Ethernet Vs Token ring

<u>802.3</u>	<u>802.5</u>
Widely used	It uses point to point connection
It is simple	It is easy and fully digital
Non deterministic- **random access protocol**	deterministic- **controlled access protocol**
Minimum valid frames is 64 B	Short frames are possible
At high load efficiency is less	Throughput efficiency are high at high load
Manchester encoding	Differential Manchester
Access- CSMA/CD	Access method – token passing
No priorities	It supports priorities

FDDI - FIBER DISTRIBUTED DATA INTERFACE

- It is a local area network protocol standardized by ANSI and ITU-T.
- It supports data rates of 100 Mbps and provides a high-speed alternative to Ethernet and token ring.
- The copper version of FDDI is known as CDDI.

Frame Format : FDDI has two frames . i) Token frame ii) Data frame

Token Format

SD	FC	ED
8bits	8bits	8bits

- SD start delimiter (flag)
- FC frame control (indicates frame type ie)– token or data frame)
- ED end delimiter (flag)

Data Format

Preamble	SD	FC	DA	SA	INFO	FCS	ED	FS

- PREAMBLE: to synchronize the frame with each stations clock.
- STARTING DELIMITER (SD): indicates the starting of the frame.
- FRAME CONTROL (FC): it lets whether it is data frame or control frame.
- DESTINATION ADDRESS: specifies where the frame should go.
- SOURCE ADDRESS: specifies the station that sent the frame.
- INFORMATION: contains data unit or control information.
- FRAME CHECK SEQUENCE: 32bit CRC
- ENDING DELIMITERS: marks end of the frame.
- FRAME STATUS: It contains 3 special bits A , E C
- **A -- address recognized C --- frame copied E ---Error detected**

Access Method - Token Passing (Early Token Release)

- Medium access control is provided by a small frame, **the token -three-byte frame**, that circulates around the ring when all stations are idle.
- When a station wishes to transmit, it must wait for token to pass by and ***seize the token***. Only the station possessing the token is allowed to transmit.
- At the end of the frame it should append the token known as early token release. The next station who wants to transmit can seize the token and sends frame. So at any time **multiple frames** circulate the ring. Each station is responsible for absorbing its own frame.

Time Registers - control the circulation of token

- FDDI defines three time registers to control circulation of the token and distribute link access opportunities among the nodes equitably
  - **TTRT and AMT**
- Target token rotation time (TTRT) The TTRT register indicates the average time required for a token to circulate around the exactly once (the elapsed time between a token 's arrival at a given station and its next arrival at the same station).

  TTRT >= time required to transmit a token +
  Propagation time for one complete circuit of the ring +
  Time required to transmit a maximum length frame +
  Synchronous allocation for station i.
- Absolute maximum time (AMT) The AMT register holds a value equal to twice the TTRT. A token may not take longer than this time to make one rotation of the ring.
- AMT = 2 TTRT

Timers

- Each station contains a set of timers that enable it to compare actual timings with the values contained in the registers.
- The two timers used by FDDI are **token rotation timer (TRT) token holding timer (THT).**

- Token Rotation Timer (TRT): The TRT runs continuously and measures the actual time taken by token to complete a cycle.
- Token Holding Timer (THT): The THT begins running as soon as the token is received. Its function is to show how much time remains for sending asynchronous frames once the synchronous frames have been sent.

Working Principle

- FDDI defines two classes of traffic: *synchronous* and *asynchronous*. When a node receives a token, it is always allowed to send synchronous data, without regard for whether the token is early or late. Synchronous here refers to information is delay sensitive. Ex: audio/video transfer. Asynchronous concentrates on throughput. Ex; File transfer
- Late Counter (LC)
- All stations have
  - same value of TTRT (Target Token Rotation Time)
  - a separately assigned value of synchronous allocation (SA_I)
- **Initially, TRT is set equal to TTRT, LC=0**.
- TRT begin to count down.

Case 1:

If TRT becomes zero before a token is received,

LC is incremented to 1.

TRT is set again equal to TTRT.

if TRT expires again before receiving a token,

LC is incremented to 2.

The token is considered as lost.

Case 2:

If token arrives earlier before TRT becomes zero.

The station saves TRT in THT [THT ← TRT]

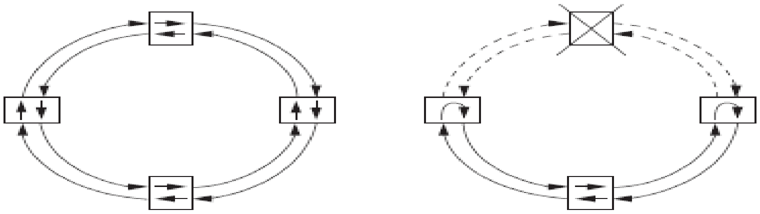
The station Resets TRT = TTRT [TRT ← TTRT]

TRT is enabled and the station can transmit syn, frame for allotted time SAi.

After transmitting synchronous frame, THT is enabled. The station may begin transmission of asynchronous frame as long as THT > 0.

Physical properties

- Two independent rings that transmit data in opposite directions, as illustrated in Figure.
- The second ring is not used during normal operation but instead comes into play only if the primary ring fails.



SWITCHING NETWORKS

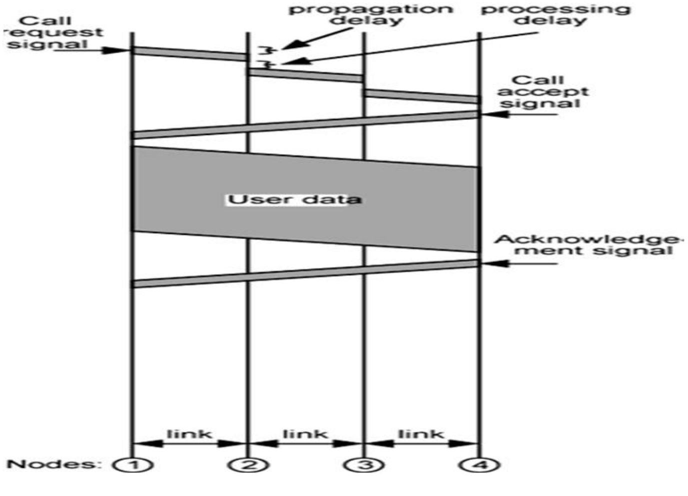
- **Switching is a mechanism** that allows us to **interconnect links to form a larger network**.
- A switched network consists of a series of inter linked nodes, called switches.
- **Switches -** Switches are hardware devices capable of creating temporary dedicated connections between two or more devices linked to the switch but not to each other.

TYPES of Switching techniques 1) Circuit switching	
2) Packet switching - 3 - techniques 2.1 Data gram Approach - (Connectionless) 2.2 Virtual circuit - (Connection-oriented) 2.3 Source Routing	a) PVC - Permanent Virtual Circuit b) SVC - Switched Virtual Circuit

CIRCUIT SWITCHING

1) **Circuit Switching: Dedicated** communication path between two stations

- Three phases
  - — Establish
  - — Transfer
  - — Disconnect
- We have to setup a path . Once the **path is setup**, the delay time is the propagation time for signals from sender to receiver. Once a call has been setup . a dedicated path between both ends exists and will continue to exist until the call is finished No traffic congestion occurs. No loss of data occurs. **Call request and call accept** are the major actions
- **Inefficient**
  - — **Channel capacity dedicated** for duration of connection
  - — If no data, capacity wasted. Set up (connection) takes time, Once connected, transfer is transparent, Developed for voice traffic (phone)



PACKET SWITCHING

2.1 DATAGRAM APPROACH

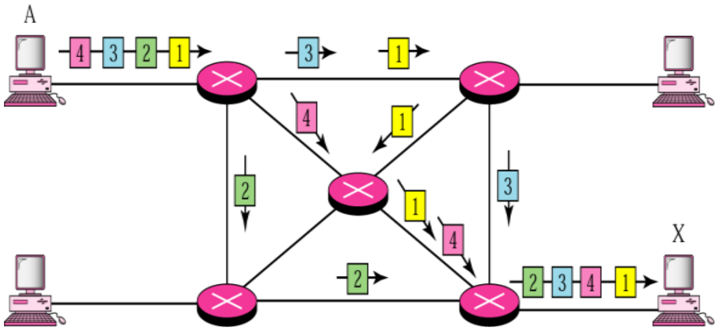
- In packet-switching **data** are is broken up into multiple discrete units of variable length block called **packets**. The network establishes the maximum length of packet. .
- Each packet contains not only data but also a **header** with control information **(source, destination address)**. The packet is sent over the network node to node.

- At each node the packet is stored briefly then routed according to the information in its header.
- Each packet is treated **independently** and can take **any route.**
- Packets may arrive out of order and s may go missing
- It is up to receiver to re-order packets and recover from missing packets

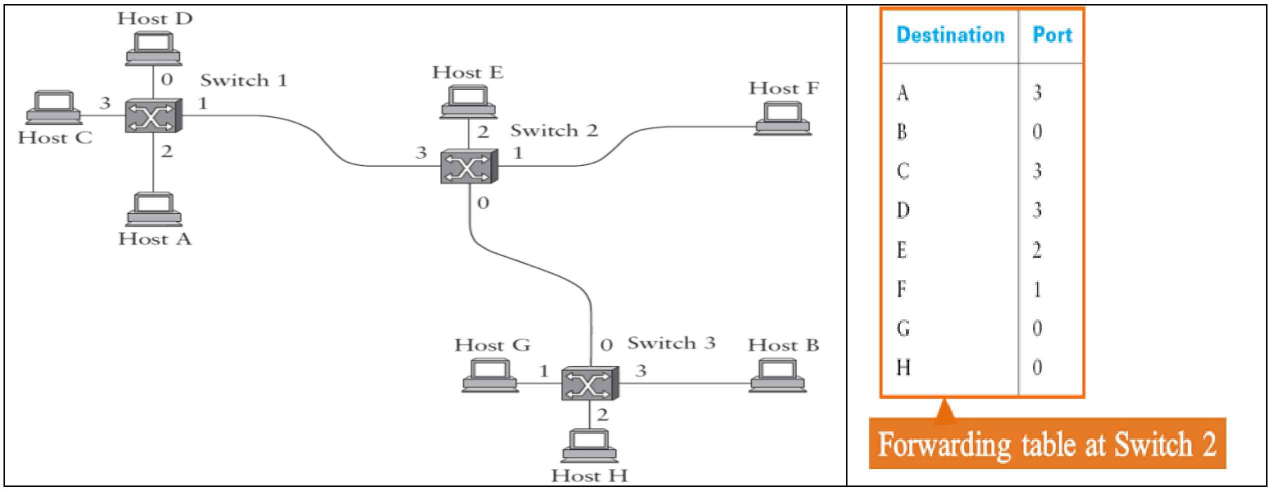
Advantages

- **Line efficiency**
  - Single link can be shared by many packets over time
- **Data rate conversion**
  - Nodes buffer data if required to equalize rates
- **Packets are accepted even when network is busy**
  - Delivery may slow down
- **Priorities can be used**

Datagram approach



The hosts have addresses A,B,C, and so on .To decide how to forward a packet ,a switch consults a forwarding table(routing table).This particular table shows the forwarding information that switch 2 needs to forward data grams in the example network.



Destination	Port
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

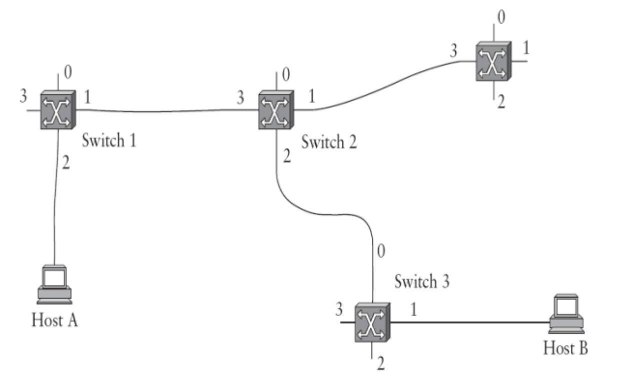
Forwarding table at Switch 2

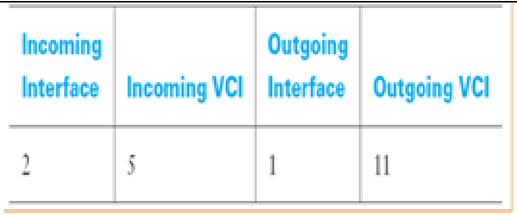
2.2 VIRTUAL CIRCUIT SWITCHING

Virtual Circuit Approach

- **Preplanned route is logically established** before any packets sent. Call request and call accept packets establish connection (handshake). Clear request is used to drop circuit
- Each packet contains a **virtual circuit identifier instead of destination address**. No routing decisions is required for each packet. VC table is available on a single switch contains.

- Incoming virtual circuit identifier(VCI) that uniquely identifies the connection at this switch , and which will be carried inside the header of the packets that belong to this connection.
- An incoming interface on which packets for this VC arrive at the switch
- An outgoing interface in which packets for this VC leave the switch
- Outgoing VCI A potentially different VCI that will be used for outgoing packets.
- The combination of the VCI of packets and the interface identifies the virtual connection.





Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
2	5	1	11

Type 1) Permanent virtual Circuit(PVC)

- It is a **long lived VC**. Virtual Connection is configured manually. **Virtual Connection** is maintained by the **administrator**. Usually persists for months between particular source and destination.

Type 2) Switched Virtual Circuit (SVC)

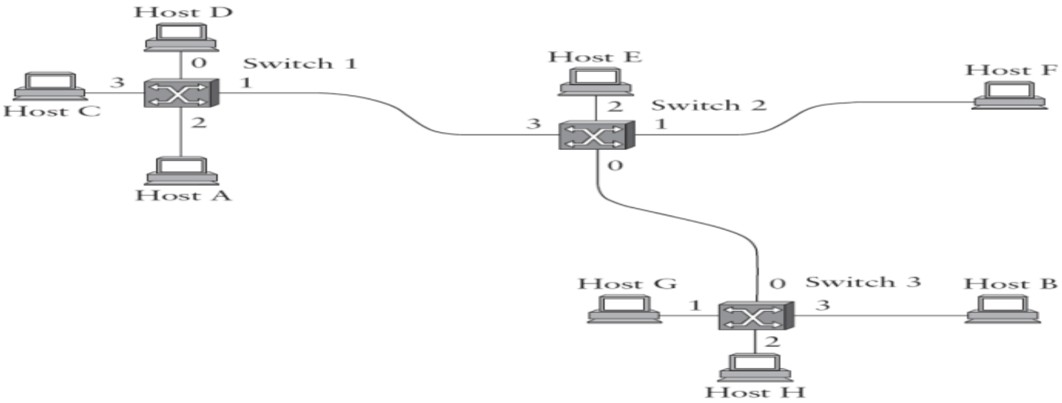
- Host sender can send messages into the network and configure the connection state.
- It is known as Signaled VC. A host may set up and delete a VC dynamically without administrator. Application initiated and Terminated when application ends

Permanent virtual Circuit - Uses Virtual Circuit Table (VC)

- Data is sent from host A to host B through a switched network with three switches. The administrator picks a VCI value that is currently unused. VCI value 5 is chosen for the link from host A to switch 1, and that 11 is chosen for the link from switch 1 to switch 2. VCI of 7 is chosen to identify this connection on the link from switch 2 to switch3,and that a VCI of 4 is chosen for the link from switch 3 to host B. VC tables have been set up for any packet to send to host B.

Virtual circuit table – for switches

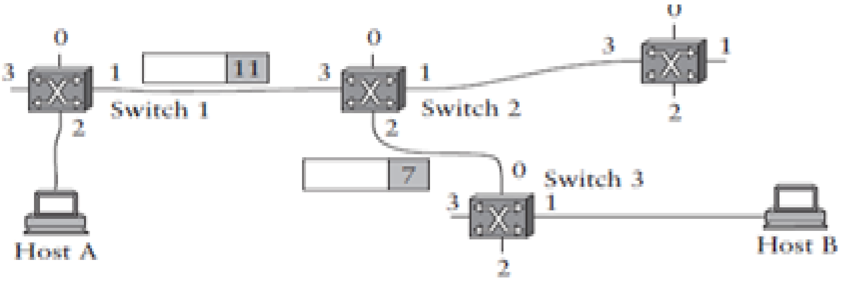
Switch	Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
Switch 1	**2**	**5**	**1**	**11**
Switch 2	**3**	**11**	**2**	**7**
Switch 3	**0**	**7**	**1**	**4**



- Host A puts the VCI value of 5 in the header of that packet and sends it to switch 1 through interface 2. Switch 1 receives the packet on interface 2, and it use the combination of the interface and the VCI to find the appropriate VC table entry. As shown in the table entry, switch1 forwards it through interface 1 with VCI 11. Thus the packet will arrive at switch 2 on interface 3 with VCI 11.
- Switch 2 looks up interface 3 and VCI 11 in and sends the packet on to switch 3 after updating the VCI value in the packet header appropriately. This process continues until it arrives at host B with the VCI Value of 4 in the packet . To host B, this identifies the packet as having come from host A.

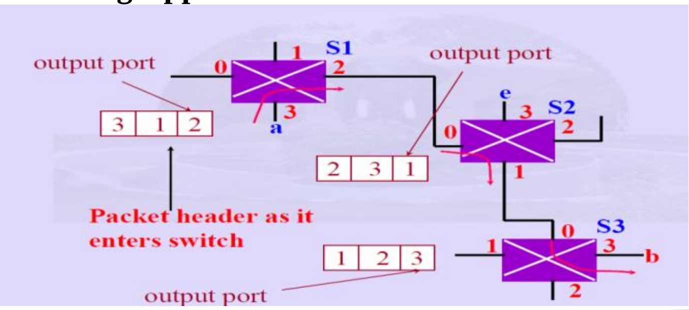
Switched virtual circuit

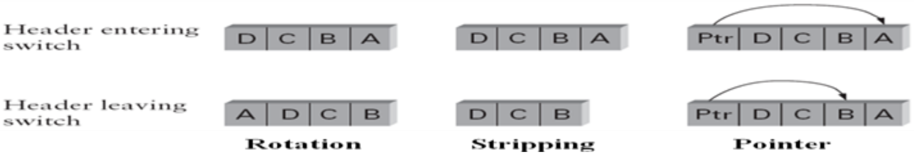
- Data is sent from host A to host B through a switched network with three switches.
- Before sending message Host A sends a set up message to switch 1. The set up message needs to get all the way to B to create the connection in every switch on the way.
- When the switch 1 receives the set up connection request, it picks In VCI as 5. It creates a new entry in its VC table for this new connection. The virtual circuit table now has the following information.: Incoming interface 2 with identifier 5, send them out on port 1.
- When switch 2 receives the setup message, it performs a similar process and picks the value 11 as the incoming VCI value. Similarly switch 3 picks 7 as the value for its incoming VCI. Each switch can pick any number it likes, as long as that number is not currently in use. An unused VCI 4 is used by B to identify all packets coming from host A.



- Host B sends an acknowledgement for setup including chosen VCI 4 to switch 3.Now switch 3 can complete the virtual circuit table entry for this connection by entering outgoing VCI as 4. Switch 3 sends the acknowledgement on to switch 2, specifying a VCI of 7. Switch 2 sends the message on to switch 1, specifying a VCI of 11.
- Finally , switch 1 passes the acknowledgement on to host A, telling it to use the VCI of 5 for this connection. At this point , VC table is complete and data transmission begins.

2.3 Source Routing Approach

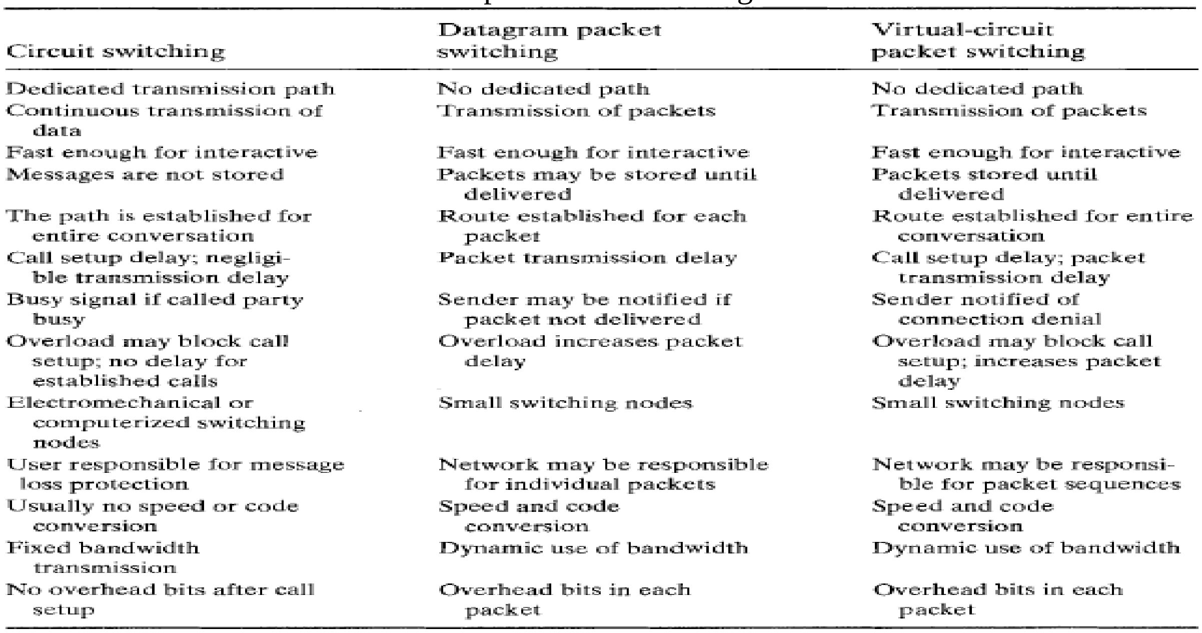




Source Routing

- Source specifies the entire route to reach the destination. Source includes Address in the packet that contains sequence of ports on path from source to destination. Here, the Source host must know entire topology. Variable size header causes switches to be slow. This approach includes rotation, stripping, pointers to read the ports in the packet header. It is impractical for large networks.

Comparison of switching networks



Circuit switching	Datagram packet switching	Virtual-circuit packet switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; packet transmission delay
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packet	Overhead bits in each packet

LAYER - 2 (DATA LINK) CONNECTING DEVICE - BRIDGES

- It is a network **connecting device**. It does **forwarding & filtering frames** using LAN destination address.
- Bridges are used to connect **LAN or WAN**. It works at DLC Layer.

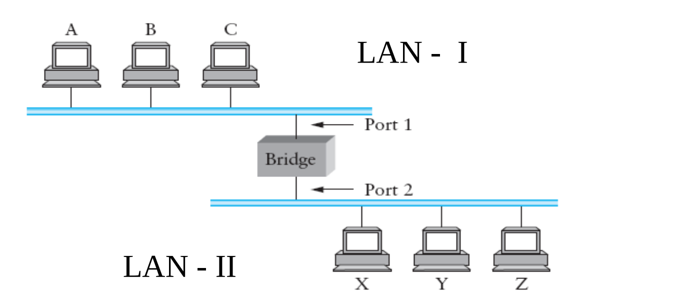
Uses of bridges: It improves Reliability , Performance ,Security and geographical connection

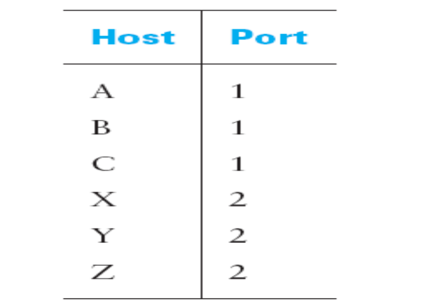
Types Of Bridge

i) **Simple Bridge** - connect 2 LANs

ii) **Multiport Bridge** connect more than 2 LANs

iii) Transparent Bridge It **learns on its own** about **connected LANs**. When frame is received, bridge "learns" location of sender: incoming LAN segment and records sender location in **filtering or forwarding table.**





Host	Port
A	1
B	1
C	1
X	2
Y	2
Z	2

The forwarding table may be maintained by human(n/w administrator) or by the bridge itself.

Forwarding table construction

- When a bridge first boots, **forwarding table is empty**, entries are added over time.
- Each bridge will inspect the ***source* address** in all the frames it receives. Thus, when **host A** sends a frame to a host on either side of the bridge, the bridge receives this frame and records that a frame from host A was just received on **port 1**.
- Thus the bridge can build a table as shown in the following example. Also, a **timeout** is associated with each entry, and the **bridge discards the entry** after a specified period of time.
- Timeout is used to protect against the situation in which a host—and as a consequence, its LAN address—is moved from one network to another.

Function Of Bridge between LAN -I and LAN -II

It read all frames transmitted by LAN- I and accept those for Stations in LAN- II using MAC . It retransmits the frame to stations in LAN II. Does the same for frames from LAN II to I

Design Issue /Functions:

- Bridge should have enough buffer space at a peak time and that is to store frame until it is transmitted
- able to find and distinguish address of station on different LAN.
- connect more than one LAN.
- bridges can maintain information about other bridges.
- a control mechanism to overcome congestion.

Limitations of LAN Bridges

- **Scalability –** Connecting more LANs using a single bridge decrease the efficiency.
- **Heterogeneity**

Routing Strategies for bridges: A bridge must be equipped with a routing capacity . When a bridge receives a frame, it must decide whether or not to forward it. It should be able to find a path of smaller cost and avoid loops.

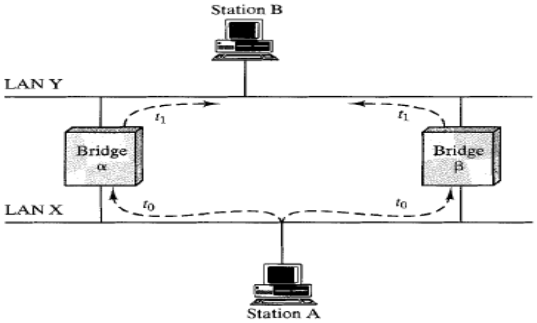
Types

- Fixed routing
- Spanning tree algorithm
- Source routing

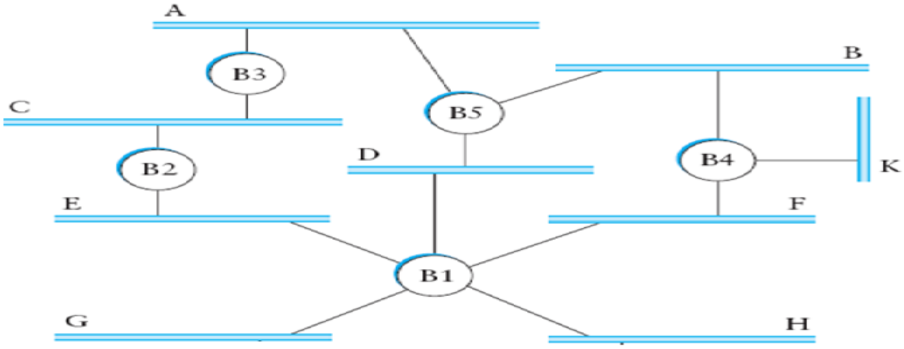
Fixed routing : A route is allotted for each source-destination pairs of LANs. It is maintained in the **form of matrix.**
Spanning Tree Algorithm: Bridge connects n/w and **removes loop in the path** using spanning tree algorithm.
Source Routing_Source specifies **which bridges** to forward the frame. **Route** is inserted in the **frame header** following the source address. Forwarding tables are not necessary.

SPANNING TREE ALGORITHM:
Bridge connects n/w and removes **loop in the path using spanning tree algorithm.** It constructs a spanning tree of edges that maintain connectivity of the graph with no loops. It is a dynamic algorithm.
The algorithm works as follows

- **FRAME FORWARDING**:
  If a bridge receives a MAC frame on port x
  Step1:search in database if destination MAC address is listed for any Port other than x.
  Step2:if not found ,flood it through all other ports
  Step3:determine whether any port is blocked or not
- **ADDERESS LEARNING:**
  When a frame arrives on a particular port, the bridge updates its data base, by entering MAC address of source & corresponding port no and an aging timer. Time is set to admit any change in topology. If timer expires the record to be deleted before timer expires ,any change comes it is to be recorded
- **LOOP RESOLUTION:**
  At time t_o A transmit a frame to B. It is captured by both bridges B1 and B2. Each bridge update its data base for source address,B1 retransmit it at t_1 to B2 .So every bridge gets the same packet in opposite directions which confuses it.



Extended LAN

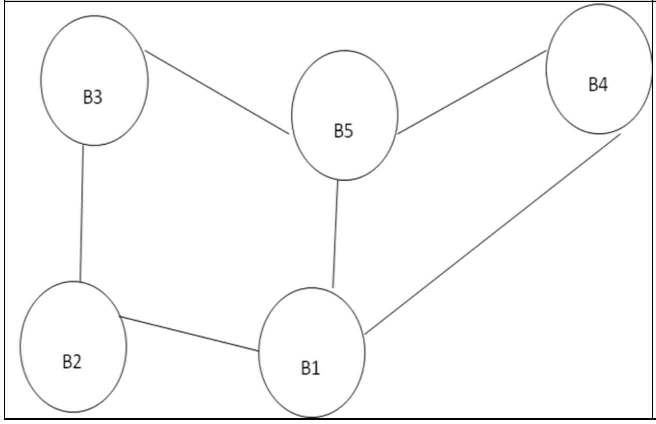
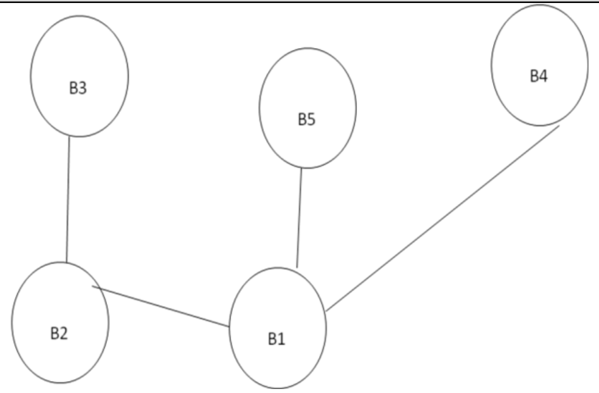


- **Terminology**
  - **Root bridge: Lowest value of bridge identifier**
  - **Path cost: Associated with each port**

    - **Root port: Port to the root bridge**
    - **Root path cost: Cost of the path to root bridge**
    - **Root and designated bridges will forward frames to and from their attached LANs**
    - **All other ports are in the blocking state**

Assumption:

- Each bridge is assigned with unique identifier. Each port is assigned with unique port identifier.
- Root port: through which the first HOP to root bridge is made with minimum cost.
- Root path cost: for each bridge the minimum cost of path to root bridge

Bridges with Loop	**Spanning tree of bridges**
	

STEP1: **Determine root bridge**

- Initially, each bridge considers itself to be the root bridge. Bridges send frames to its attached LANs
    - The ID of the sending bridge
    - ID of the bridge that the sending bridge considers root
    - The root path cost for the sending bridge
    - Best one (lowest root ID/cost/priority) wins

STEP 2: Selecting Root Ports

- Each bridge selects one of its ports which has the minimal cost to the root bridge
- In case of a tie, the lowest port ID is used

STEP3: Selecting Designated Bridge

- Each bridge considers itself to be the designated bridge
- Bridges send BDPU frames to its attached LANs
- Best one wins (lowest ID/cost/priority)

Example:

- B3 receives (B2 , 0 , B2)
- Since 2 is less than 3, B3 accepts that B2 as root.
- B3 sends to B5 as (B2, 1, B3) by incrementing the distance.
- Mean while B2 and B5 accepts that B1 as the root.
- B2 sends (B1 , 1 , B2) to B3.
- B5 sends (B1, 1 , B5) to B3.
- Thus now B3 accepts B1 as root and finds B2 & B5 are closer to the root and it stops forwarding any messages to the root.

Source Routing Bridges

- **Source Routing**_Source specifies **which bridges** to forward the frame. **Route** is inserted in the **frame header** following the source address. Forwarding tables are not necessary.
- Bridge need not maintain routing tables.
- The bridge makes decision whether or not to forward a frame on to the basis of routing information in that frame.
- So a bridge is enough to know its identifier and identifies of each LAN to which it is attached.

  Eg: A frame contains routing - LAN1, B1, LAN3, B3, LAN2

WIRELESS LAN - IEEE 802.11

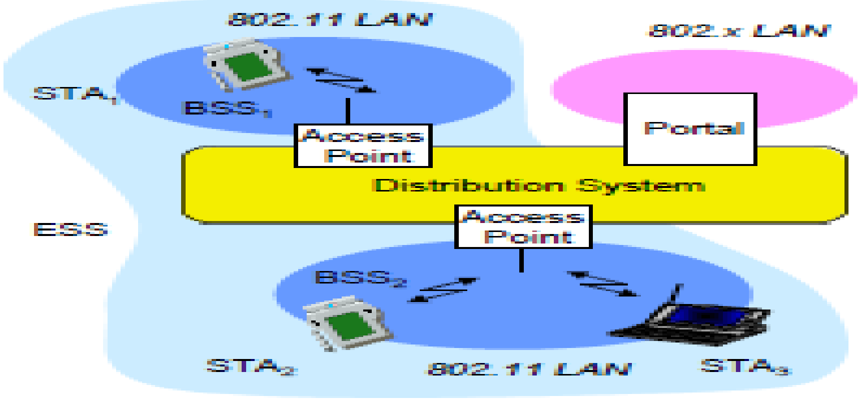
Model of 802.11 Architecture

BSS:T he smallest building block of wireless LAN is a Basic Service Set BSS. Each BSS consists of some number of stations executing same MAC and competing for access to same shared medium.

Access point :A BSS may be isolated or connected to a backbone DS through **an access point**.

Distribution system: A distribution system is a wired backbone LAN.

ESS An extended service ESS consists of 2 or more basic set connected by a distribution system.



Types of Station:

No transition: A station is either stationary or moves within a single BSS

BSS transition: A Station moves fro m one BSS to another BSS with in same ESS.

ESS transition: A station moves from a BSS in one ESS to BSS with in another ESS.

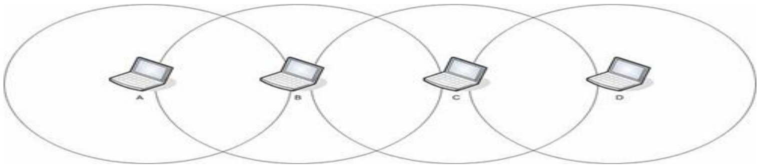
•**Physical medium**:

- Frequency Hopping Spread Spectrum
- Direct Sequence Spread Spectrum
- Infrared

Hidden station problem and exposed station problem:

Hidden station problem:

1. A is transmitting to B.
2. C senses the medium, does not hear anything as it is out of range of A/hidden station of A
3. Decides to transmit to B, creates an interference at B.

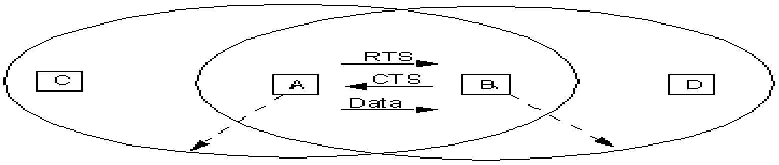


<u>Exposed station problem:</u>

1. B is transmitting to A.
2. C- a exposed station of B senses the medium, sees it is occupied.
3. C postpones its intended transmission to D, which is actually possible.

CSMA/CD(802.3) as it is cannot be used for wireless LANs.

<u>Multiple access with collision avoidance (MACA):</u>
To solve hidden and exposed problem.
<u>Phases:</u>
1. A sends a RTS (request to send) frame to B, indicating the length of data.
2. B answers CTS (clear to send), indicating the expected length of data, copied from RTS.
3. A sends data.
4.C receives RTS (but no CTS), must not send during CTS, after that it is free to transmit.
5. D receives (not RTS, but) CTS, has to wait with the transmission until the end of the data is reached.



Medium Access Control It consists of 2 control mechanism.
A distribution access protocol.DCF
An optimal centralized access protocol on top of it. PCF

Distributed Access Protocol: Using it nodes sense of an ad-hoc network of peer stations and transmit.
Centralized Access Protocol: It regulates the transmission by a centralized decision maker. It is useful to send data which are time sensitive and high priority.

DISTRIBUTED COORDINATION FUNCTION:
DCF –A delay is known as an inter frame space IFS.
A station with a frame to transmit senses the medium. If the medium remains idle for a time equal to IFS (inter frame space- delay) , then the station can transmit. If a medium is busy, the station defers transmission and continues to monitor the medium until transmission is over. Once the transmission is over, station delays another IFS. If the medium remains idle, then station senses the medium using exponential back off scheme. If the medium is still idle. It may transmit.
There are 3 different type of IFS.

SIFS (Short IFS) : It is used for all immediate response action.
PIFS (Point Coordination IFS) : A middle length IFS, used by centralized controller in PCF scheme when issuing polls.
DIFS (Distributed Coordination IFS) : A longest IFS used as a minimum delay for asynchronous frames .
When SIFs used?

ACK: When a station receives a frame addressed only to itself, it responds with ACK after SIFS gap.

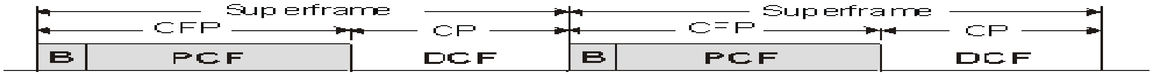
CTS: All other stations receive RTS defer any transmission for a SIFS gap.

POINT COORDINATION FUNCTION : It provides contention free service. PCF is built on DCF. An alternative method implemented on top of PCF. Point coordinator makes use of PIFS when issuing polls. It seizes the medium and lockout all asynchronous traffic while it issues polls and receives responses.

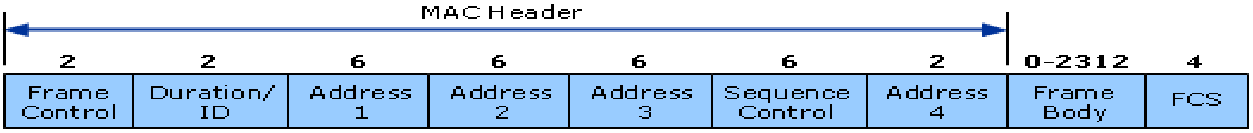
Super Frame : At its beginning the point coordinator may optionally size medium and issue polls for a given period of time. The responding stations send variable size frames.

The remainder of super frame is available for contention based access. At the end of super frame it uses PIFS delay. If medium is idle, point coordinator gains immediate access and full super frame period follows. Suppose medium is busy, PCI must wait ant it results in foreshortened super frame.

SuperFrame



FRAME FORMAT



2	2	6	6	6	6	2	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Frame contains four addresses
- How these addresses are interpreted depends on the settings of the **ToDS** and **FromDS** bits in the frame's Control field
- This is to account for the possibility that the frame had to be forwarded across the distribution system which would mean that,
- the original sender is not necessarily the same as the most recent transmitting node
- Same is true for the destination address

BLUETOOTH

Bluetooth Architecture:

The Bluetooth technology is used in **ad-hoc piconets**, which are local area networks with a very limited coverage and without the need for an infrastructure.

It is needed to connect different small devices in close proximity (about 10 m) without expensive wiring or the need for a wireless infrastructure Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band. Bluetooth operates on 79 channels with 1 MHz carrier spacing

Simple Bluetooth piconet

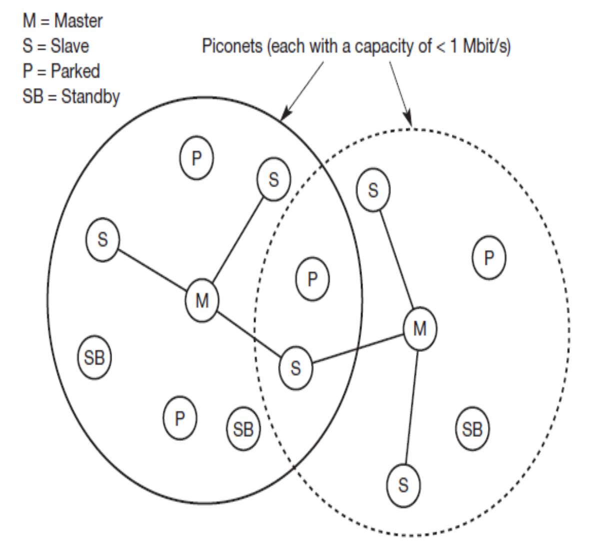
A very important term in the context of Bluetooth is a **piconet**. A piconet is a collection of **Bluetooth devices** which are synchronized to the same hopping sequence. The Figure shows a collection of devices with different roles.

One device in the piconet can act as **master** (M), all other devices connected to the master must act as **slaves** (S).

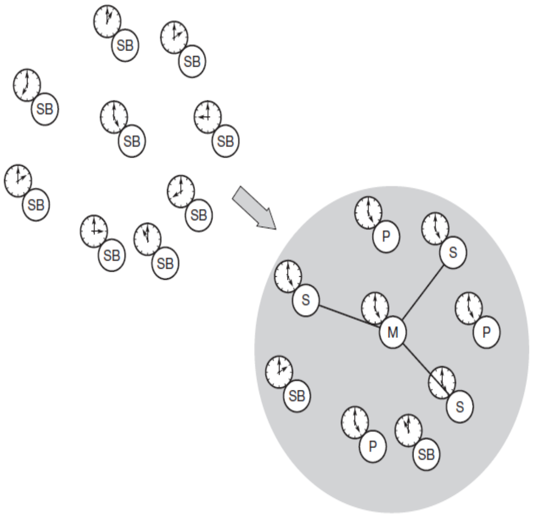
The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern.

Two additional types of devices are shown: parked devices (P) can not actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds .

- As all active devices have to use the same hopping sequence they must be synchronized. The first step involves a master sending its clock and device ID.
- All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave.



Bluetooth scatter net



Forming a Bluetooth Piconet

- All active devices are assigned a 3-bit **active member address** (AMA). All parked devices use an 8-bit **parked member address** (PMA). Devices in stand-by do not need an address.
- All users within one piconet have the same hopping sequence and share the same 1 MHz channel. As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate). (Only having one piconet available within the 80 MHz in total is not very efficient.) This led to the idea of forming groups of piconets called **scatternet**

Bluetooth protocol stack

The Bluetooth protocol stack can be divided into a **core specification** (Bluetooth, 2001a), which describes the protocols from physical layer to the data link control together with management functions, and **profile specifications** (Bluetooth, 2001b).

The **core protocols** of Bluetooth comprise the following elements:

● **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power .

● **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters

Protocols :

Link manager protocol: Link set-up and management between devices including security functions and parameter negotiation.

Logical link control and adaptation protocol (L2CAP): Adaptation of higher layers to the baseband (connectionless and connection-oriented services).

Service discovery protocol: Device discovery in close proximity plus querying of service characteristics .

The **telephony control protocol specification – binary** (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls between Bluetooth devices. It also describes mobility and group management functions.