Friends
Date | Page No.

IMRAN KHALID

Diploma in Computer Engineering I^{th} sem.
Roll No. → 15DCS0019
Subject → Data Communication & Networking

Friends
Date: 24/7/17

Data Communication

Data communication means the transfer of data from place to another by various means.
Data communication includes sorting, processing and storing of data before its transmission.

- **Data**
  Data is raw, unorganized facts that need to be processed. Data can be something simple and useless until it is organized.
- **Information**
  When data is processed, organized, structured to make it useful, it is called information.
  For example, no. of visitors to a ~~country~~ website by country is example of data.
  Finding out that visitors from USA is increasing and while from India is decreasing is meangful information.
- **Computer Networks**
  A large no. of seperate but inter-connected computers are called computer networks.

Computer networks means an inter-connected collection of autonomous computers.

Friends
Date 27/7 Page No.:

Two computers are said to be interconnected if they are able to exchange information.

- **Need of Computer Networks**

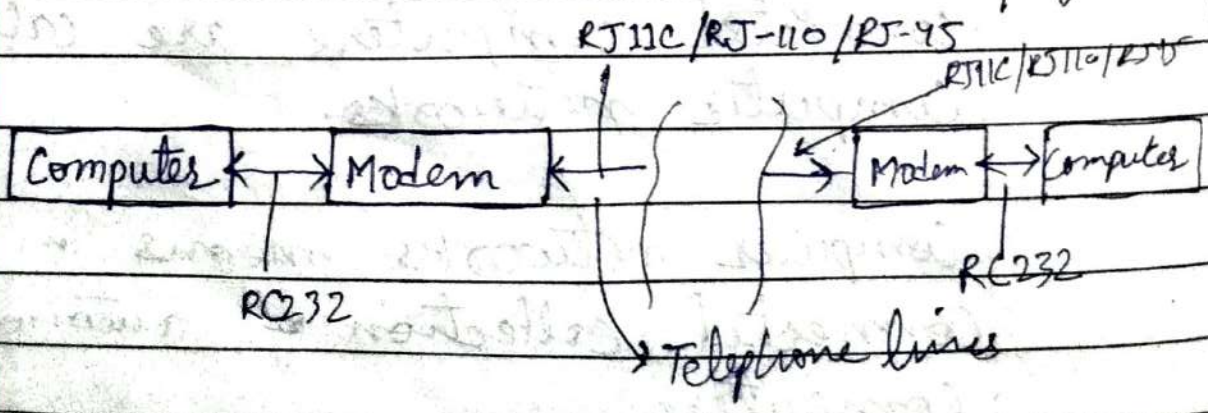
i) **Communication** :→ To provide communication among users.

ii) **Resource sharing** :→ Resource sharing is the most common objective for provide networks. To reduce the cost we use resource sharing.

iii) To increase the reliability of processing capacity through backup and redendancy.

iv) Centralized Management :- To provide centralized management and allocation of resources.

- **Data Communication Networks/systems**



A data communication network / system is a combination of pair of communication devices, a transmission medium in between and a method of translating the signal generated by the computers into a form which is acceptable / suitable to the transmission medium.

① A computer is a source or destination of information.

② Modems are devices which converts digital information generated by computers into analog information suitable for transmission on the telephone link.

③ A telephone link is a medium to provide physical connectivity b/w two computers.

- Types of Data

Data is send in the form of changing electrical signals over the transmission medium. There are two types of signal available in nature.

① Analog signal
② Digital signal

Analog and Digital signals are the types of signals carrying information. The major difference between both signals is that the analog signals that has a continuous electrical, while digital signals non-continuous electrical.

Analog signals

The analog signals were used in many systems to produce signals to carry information. These signals are continuous in both values and time. The use of analog signals has been declined with the arrival of digital signals. In short, to understand the analog signals - all signals that are natural or comes naturally are analog signals.

Digital signals

Unlike analog signals, digital signals are not continuous but signals are discrete in value and time. These signals are represented by binary numbers and consist with different voltage values.

	Analog signal Vs	Digital signal
1.	Continuous signal	Discrete signal
2.	Represented by sine waves	Repr. by square waves.
3.	Human voice, natural sound, etc.	Computers, optical drives, etc.
4.	Continous range of values.	Discontinious values.
5.	Records sound waves as they are	converts into a binary waveform.
6.	Only in analog devices	suited for digital electronics devices.

Friends
Date: 25/7 Page No.

Data Representation

In computer systems logical 0's & 1's are physically represented by two voltage labels most of the time. But we intend to transmit these signals over a long distance, it is very difficult to use DC voltage for the purpose. so we use some other paramaters to represents these descrete states.

It can be frequency, phase or amplitude of wave or a combination of these physical parameters.

1. PAM (Pulse Amplitude Modulation)
2. PCM (Pulse code Modulation)
3. FSK (Frequency shift Keying)
4. PSK (Phase shift Keying)

PAM (Pulse Amplitude Modulation)

Pulse amplitude modulation (PAM) is the transmission of data by varying the amplitude (voltage or power levels) of the individual pulses in a regularly timed sequence of electrical or electromagnetic pulses. The number of possible pulse amplitudes can be infinite (in the case of PAM), but is usually some power of two so that the resulting output signal can be digital.

PCM (Pulse Code Modulation)

PCM is a method used to digitally represent sampled analog signals. It is the standard form of digital audio in computers, compact discs, digital telephony and other digital audio applications. In a PCM stream, the amplitude of the analog signal is sampled regularly at uniform intervals and each sample is quantized to the nearest value within a range of digital steps.

Frequency shift Keying (FSK)

FSK is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier signal. The technology is used for communication systems such as amateur radio, caller ID and emergency broadcasts.

Phase-shift Keying (PSK)

Phase-shift Keying (PSK) is a digital modulation process which conveys data by changing (modulation) the phase of a reference signal (the carrier wave). The modulation occurs by varying the sine and cosine inputs at a precise time. It is widely used for wireless LAN's, RFID and bluetooth communication.

Data Transmission Modes

Based on the no. of bits transmitted at a time, there are two different ways of data transmission.

1. Serial Transmission

When data is transmitted serially, 1 bit at a time it is called serial transmission. 1 wire is used for the data transmission in any particular direction. Data bits are transmitted one after another. For transmitting 8 bit of transmission it will take 8 unit of time.

2. Parallel Transmission

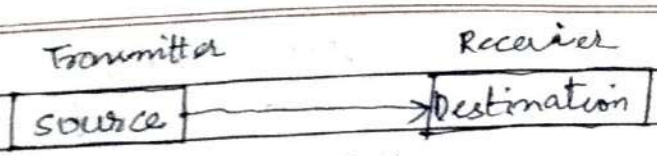
In P.T several bits are transmitted simultaneously over multiple transmission lines. The no. of bits which are transmitted simultaneously depends on the design of the system.

Simplex, Half & Full Duplex Transmission

There are another ways of classifying transmission system which are based on the direction of data transmission / flow.

1. simplex

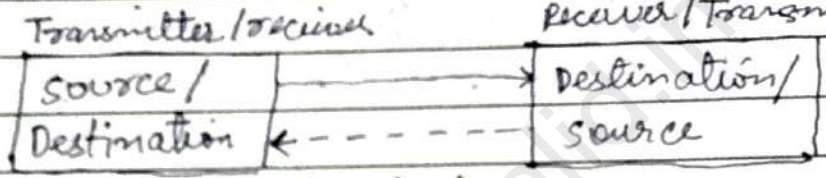
In this mode data is transmitted in one direction only. This means one end will always remain be transmitter and other always be a receiver.



(simply)

2. Half Duplex

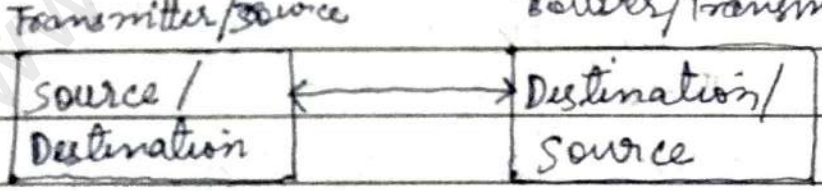
In this mode data is permitted to flow in either direction but not simultaneously. At the given time the transmission take place only in one direction



(Half)

3. Full Duplex

A transmission system in which data can be transmitted in both direction simultaneously its called a full Deplex system.



(Full Duplex)

- Data Transmission speed

In data communication over long distances There are two general terms used to convey the speed of communication system

1. BPS (Bits Per second)
It is a unit that indicates the no. of bits transmitted from source to destination in a second.

2. Baud
Baud is the numerical expression of the no. of times per second, the signal changes its value

- Asynchronous serial Transmission
There data is transmitted 1 bit at a time, usually in a group of characters. The receiver is provided with the information about the begining and end by adding a 'start' signal before the character and adding a 'stop' signal after a character.
The transmission protocol is called a 'start-stop' protocol and it uses a single channel for transmission.
The main advantage of asynchronous serial transmission is that the character is self contain with all the information and the two ends of the link need not be synchronized.
The main disadvantage is the over head of start & stop signals.

Date: 25/7 Page No.:

- Synchronous Transmission
It refers to the transmission of data with some time reference signal. It consist of a string of bits transmitted on a channel.
S.T uses synchronizing information on group of characters instead of on each character. The receiving station operation in steps with the transmitting station through the recognization of specific bit pattern at the beginning of each transmission. The two ends of the link are synchronized by receiver clock with a transmitter clock

→ Transmission Technologies
There are two types of transmission technologies:
1) Broadcast Network
Broadcast networks have single communication channel that is shared by all the machines on the network. Short messages called packets in certain context, send by any machine are received by all the others.

2) Point to point Networks
P.T.P.N consist of many connections b/w individual pair of machines. To go from

the source to the destination a packet on this type of network may have to first visit one or more intermediate machines.

→ Types of Networks (Computer Networks)
One way to catogories diff. type of computer network designs is by their scope or scale. Common type of area network are:

1. LAN (Local Area Network)
2. MAN (Metropolitan Area Network)
3. WAN (wide Area Network)
4. WLAN (wireless Local Area Network)
5. SAN (Storage Area Network)
6. CAN (Campus Area Network)
7. PAN (Personnel Area Network)

LAN
Local Area Network covers a small physical area like a home, office, or a small group of buildings, such as a school or airport.

MAN
Metropolitan Area Networks enable are very large network that covers an entire city. It usually ranges from 5 to 50 kms. The MAN can be used to provide services including telecoms, internet access, television and CCTV.

Friends
Date : Page No. :

WAN

Wide Area Network covers a broad area, like communication links that cross metropolitan, regional or national boundaries. The internet is the best example of a WAN.

WLAN

Wireless Local Area Networks enable users to move around within a larger coverage area, but still be wirelessly connected to the network.

SAN

Storage Area Network help attach remote computer storage devices, such as disk array, tape libraries to servers in such a manner that they appear to be locally attached to the operating system.

CAN

Campus Area Network provides wireless or LAN for the users located intwo or more buildings or limited geographical Area. CAN usually set in campus of a university.

PAN

Personal Area Network are used for communicating among various devices such as fax machine, printers to a single user.

Friends
Date 31/7/17

- **Protocol**
  A protocol is an agreement b/t the communication parties on how communication is to proceed.

- **Interface**
  The interface defines which prempitive operations and services the lower layer offers to the upper one

- **Layer**
  To reduce the network complexity, most networks are organized as a series of layers or labels, each one build upon it. The purpose of each layer is to offer certain services to the share layer.

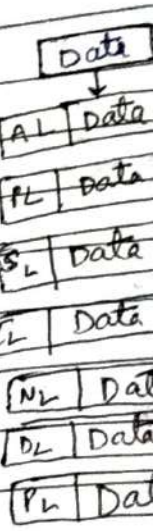
- **Header**
  Header is used to put by the layer in font of message/data to identify the message and passes the result to global layer. The header includes control information such as sequence no. to allow to source machine to deliver message in right order if the lower layer don't maintain the sequence.

V. good. Sunil 1/8/17 (A1)

Friends
Date: 1/2/17 Page No.:

Standards

A standard is a prescribed set of rules, conditions, admissions or requirements concerning definition of terms; classification of components; specification of materials, performance or operations, delination of procedures; measurement of quality and quantity in describing material, products, systems, services or practices. A standard allows products from multiple vendors to communicate with each other, giving the purchaser more flexiblity in equipment selection and views.



The OSI Model (Reference Model)

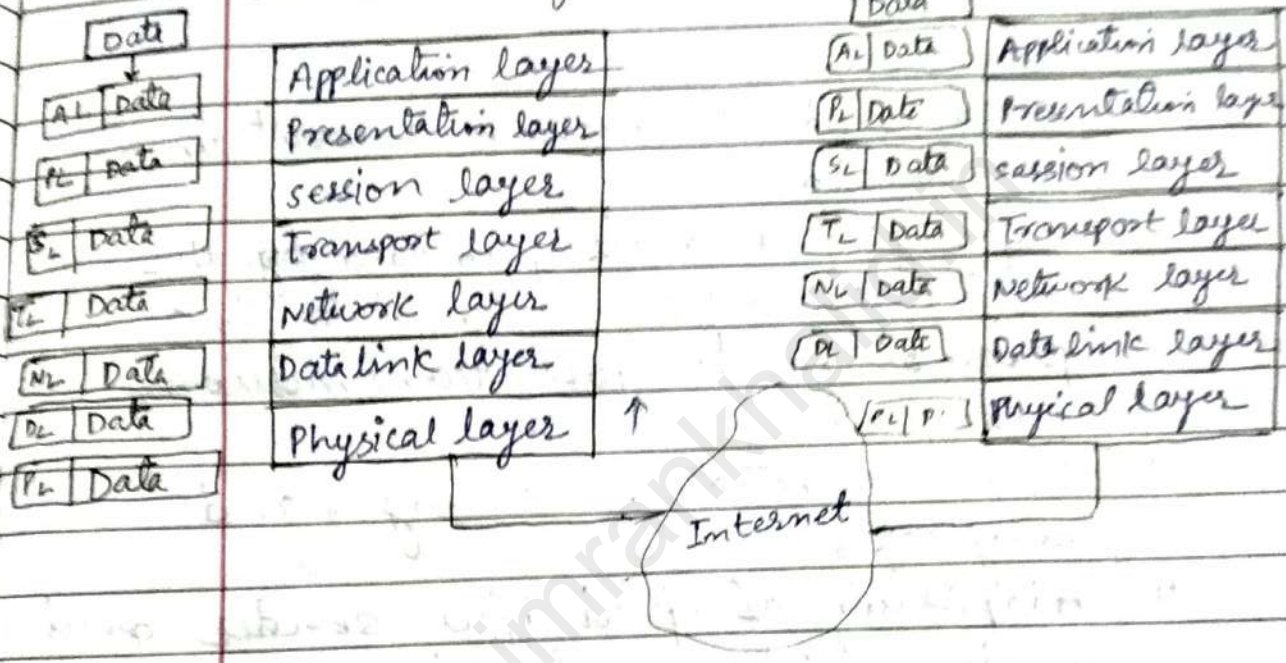
The ISO (International standards organisation) has promoted the open systems intercommections (OSI) model. The purpose of this International standard reference modal is to provide a common basis for the coordination development of standard for the purpose of system Inter-connection.

- **Advantage of Open system:-**

Open system is important to have support for multiple hardware platforms, multiple GUI platforms, multiple operating system,

multiple database-Management system, multiple connection protocols & multiple LAN operating systems for implementing an effective client/server environment.

The OSI Layers



1). Physical Layer

The physical layer covers the physical interface between devices & the rules by which bits are passed from one into another

Function of physical layer

1. RAW bits transfer
2. Allocation of pins
3. Establishing connection
4. Bit error controll
5. Electrical & mechanical specification of interface.

Friends
Date: 8/8/17

Data link layer

The task of data link layer is to take a raw transmission facility and transform it into a line that is free of transmission error and deliver it to the network layer.

Functions of this layer

1. Data link connection activation & deactivation.
2. Mapping data units provided from the network layer into data link protocol units for transmission. (frames)
3. Error detection, recovery, and notification
4. Adaptation of speed b/w sender and receiver. (flow control).

Network layer

The basic service of network layer is to provide the transparent transfer of data between transport entities. It release the transport layer of the need to know anything about the data transmission and switching technologies used to connect system.

Functions of Network layer

1. Network addressing and point identification.
2. Multiplexing network connection onto data link.
3. Service selection when different services are available.
4. Error detection and data recovery to support desired quality of service.
5. Flow control.

4. Transport layer

It provides a reliable mechanism for the exchange of data between processes in different systems. It provides end-to-end error recovery and flow control.

Function of this layer :-

1. selection of functions used during data transfer.
2. Transport of data from higher layers
3. Process to process delivery.

5. session layer

It allows users on diff. machine to stablish connection (session). A session allows ordinary data transport and some enhanced services useful in some applications

Function of session layer

1. session correction connection establishment.
2. session connection released.
3. Normal data exchange.
4. Interaction management.
5. Address transmission.

6. Presentation layer

The presentation layer performs certain function that are requested sufficiently often. These are conserned with syntax and symantic of the information transmitted.

Function of this layer:

1. session initiation and termination request.
2. Negeotation and Re-negeotation presentation image.
3. Data transformation.
4. Data formatting.
5. syntax selection.
6. Inception to ensure security.

7. Application layer

This layer contains the variety of protocols that are commonly needed

Friends
Date: 8/8/2017

Function of this layer :-

1. Identification of intended communication partners and there ability and authenticity.
2. Establishment of authority to communicate.
3. Agerment on data validity commitment.
4. Information transfer.

Local Area Networks

LANs provides a means for users to interconnect a wide range of devices together into united resources sharing systems, using a high bandwidth communication system over relatively inexpensive transmission media. LAN makes possible the sharing of all software and hardware resources.

Classification of LANs

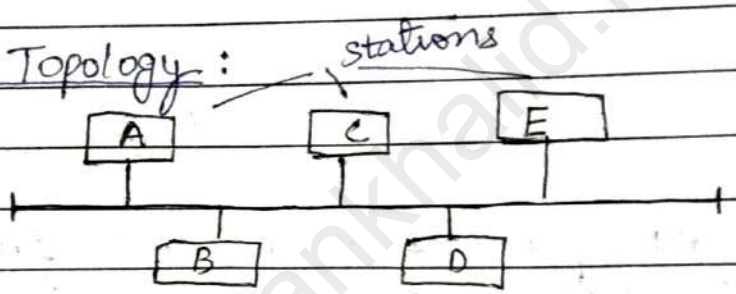
A large variety of Hardware & software system are available for LAN. All of them shared the genral characteristics but are implemented in different ways. LANs are classified according to following criteria :

Friends
Date: 21/08/17

1. Network Topology
2. Transmission medium
3. Transmission Technique
4. Access Protocol

- **Network Topology**
The network topology relates the logical way in which systems are interconnect.

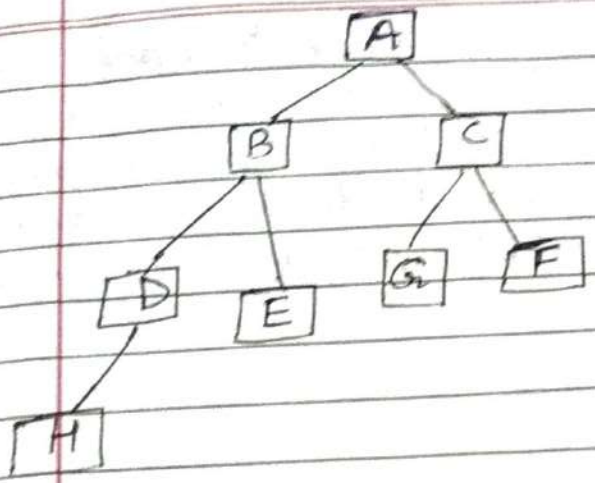
1. **Bus Topology:**



The bus topology uses a single common cable or link to connect the nodes of the network.. Stations connected to the common media through a series of tabs located at specified distances from one another along the common cable but only one station transmitt along the common medium at only one time.

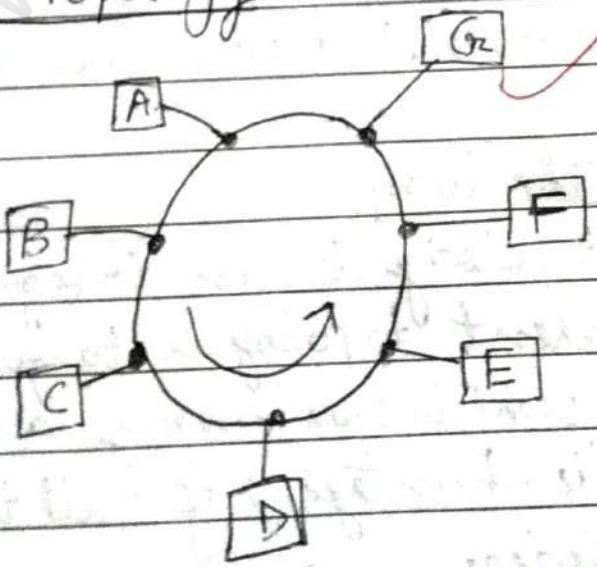
2. **Tree Topology**

Friends
Date: 21/02/2017



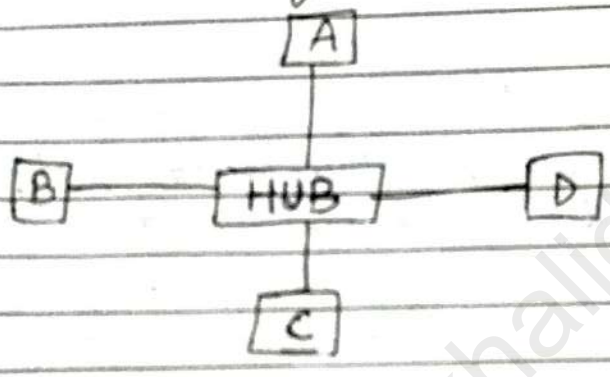
The tree topology arranges links & nodes into distinct hierarchies in order to allow better control and easier troubleshooting. In order to function well, Networks using tree topology must in coorporate some form of traffic control to determine when to allow traffic to travel up and down the branches of tree.

3: Ring Topology



The ring topology connects each node to the next one to form a closed loop. Each station has a transmitter and receiver, and data is transmitted in one direction around the ring.

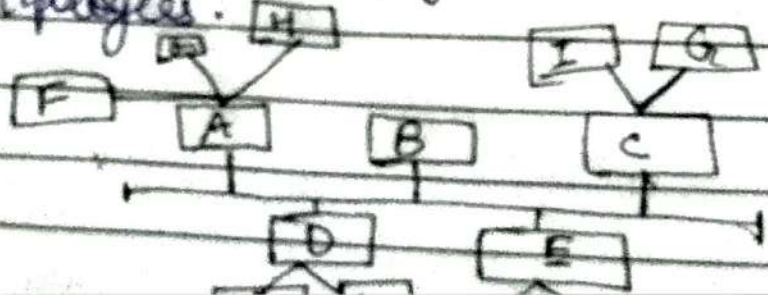
4. Star Topology



The star topology consist of a no. of individual nodes which connect to a common central point. The common central point in star topology network is often concentrated device or HUB.

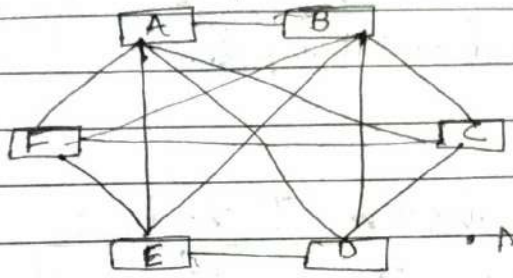
5. Hybrid Topology

Hybrid topology is an integration of two or more different topologies to form a resultant topology which has many advantages (as well as disadvantages) of all the constituent basic topologies.



Friends
Date 21/4/2017

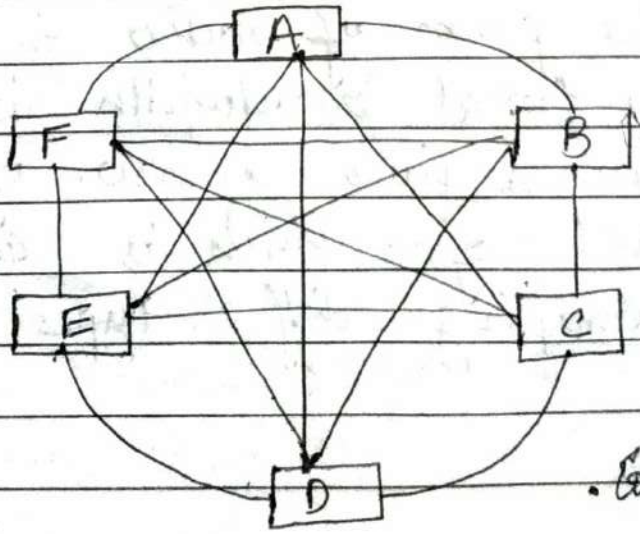
6. Mesh Topology
A network setup where each computer and network device is interconnected with one another, allowing for most transmission to be distributed, even if one of the connection go down.



• Mesh Topology

Full mesh, in this every computer in the network has a connection to each of the other computers in that network.
Partially connected mesh, atleast two of the computers in the network have connections to multip other computers in that network.

7. Complete Topology
A complete topology is a network topology in which there is a direct link between all pairs of nodes. In a fully connected network with n nodes, there are $n(n-1)/2$ direct links.



• Complete Topol.

- **Transmission Medium**
It defines the type of transmission medium that is used to interconnect systems. For example co-axial, twistedpair, twin-axial, fibre optics, unsheilded twisted pair wires, shielded multiple twisted pair wires.

- **Transmission Technique**
It defines the method that is used for transmissionting the signals over the cable

1. **Baseband**
In the baseband technique of signal transmission a digital signal is directly applied onto the cable and the entire cable is used to propogate a single digital signal

2. **Broadband**
In the broadband techniqure information is transmitted over the cable in the form of radio frequency signals. The total bandwidth is usually is divided into a no. of channels, each of which is capable of carrying diff. types of information

Friends
Date: 22/08/2017

4) Access Protocol

The fourth area in which LANs are classified in according to the protocol that governs the way individuals station access the transmission medium.

i) CSMA/CD

This stands for carrier sense multiple Access with Collision detection. It is also reffered to as listen while talk (LWT). Under this protocol all nodes attached to the network (monitor) listen to the transmission medium at all the time. When a station needs to transmitt data it waits untill the medium is free and then transmitt if two or more nodes transmit at the same time, a collision occurs/results each nodes detect the collision at waits for a random amount of time and tries to again to retransmit.

ii) CSMA/CA

This stands for carrier sence multiple access with collision avoidance. It is similar to CSMA/CD except that all nodes implement an algorithm that helps to avoid collision rather than simply

detect, wait and then retransmit.

iii) Token Passing

This technique (protocol) is commonly used on ring structure network but used on Bus structure networks also. A special message packet called the token is passed from one node to another node around the ring. when a node receives a token, it either transmit the message if it has message to send, by capturing the token and then releases it for the next node after transmission is over or it passes the unused token to next node on the ring. Each station receives one chance to transmit during the time that it takes for the token to circulate around the ring.

LAN Standards

Some sort of standardisation is always necessary for any technology or product line to be economically & technically feasible.

IEEE 802 Standards

This is an important set of standards for Local Area Networks. It has been documented by the Intitute of Electrical & Electronics Engg. (IEEE). The IEEE LAN standards deal with layer 1 & layer 2 of the OSI Reference model (Physical & Data link layer).

It divides the OSI data link layer into two sub layers.

1. MAC (Medium Access Control)
2. LLC (Logical Link Control)

i) MAC

The MAC sub layer perform the access function for the particular access control method employed by the network. Typical access control method are CSMA/CD & CSMA/CA, token passes.

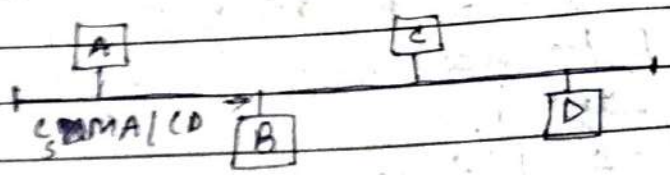
ii) LLC

The LLC sub layer performs function comparable to conventional data link protocols. These includes framing, addressing and error control

Date: 22/08/2017

IEEE 802.3 standard

This standard describes MAC sub layer and physical layer functions for a Bus structured network that uses CDMA/CD as an access protocol.



The initial development on CSMA/CD was done at Xerox Corporation. The physical link lable portion of the standard specifies connector hardware to the voltage waveform to algorithms for carrier sensing. Ethernet which is widely used type of LAN is based on the IEEE 802.3 base standard. It operates at 10 MBPS or 100 MBPS of speed.

byte

7	1	2/6	2/6	2	0-1500	0-46	4
Preamble	start of frame	Destination Address	source Address	length of Data	Data	Pad	check sum

(Frame format of IEEE 802.3 standard)

Preamble :-

This feild is used to synchorize the receivers clock

Friends
Date : Page No. :

Start of frames
It denotes the start of the frame itself.

Destination Address
It shows the address of the destination.

source Address
It shows the address of the source.

Length of Data
It tells how many bytes are present in data feild.

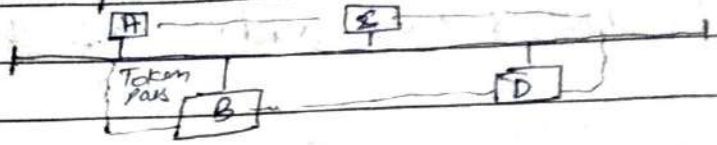
Data
It contains the actual data of max limit 1500 bytes.

PAD
It is used to fill the frame of min. size 64 bytes.

Checksum :→
It is used to detect the communication errors.

11) IEEE 802.4 standard (Bus Token)

This standard describes the mac sub layer & physical layer system for a bus structured network that uses token passes on an access protocol.



A token bus is a logically ordered group of communicating nodes which access the medium in a round robin function

byte

1	1	1	2/6	2/6	0-8182	4	1
Preamble	Start of frame	Frame Control	Destin. Addr.	Source Add	Data	check sum	End of frame

(Frame Format of IEEE 802.4 standard)

Preamble :-

It is used to synchronize the receiver clock

Start of Frame :

It denotes the start of frame itself.

Frame Control :-

It specify frame type.

Friends
Date: 27/08/2017

Destination Address:
It shows the address of the destination.

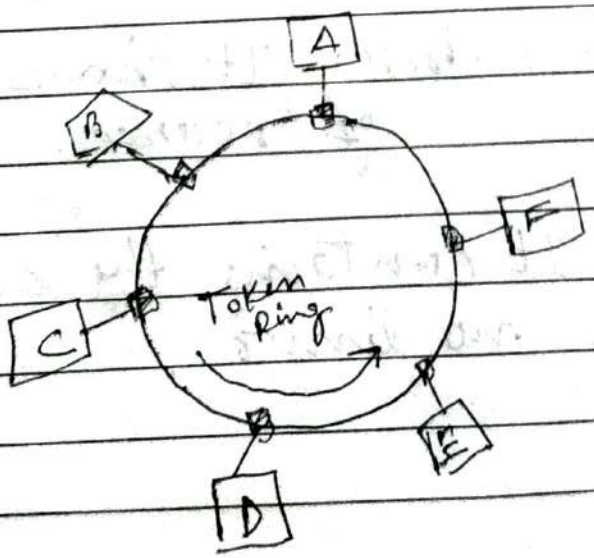
Source Address:-
It shows the address of the source.

Data:-
It contains the actual data of max. 8182 byte.

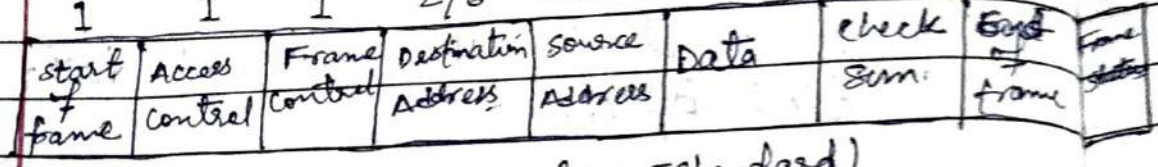
Checksum:-
It is used to detect the communication errors.

End of Frames:-
It represents the end of frame.

IEEE 802.5 standard (Token Ring):->
This standard describes mac sublayer & physical layer function for a ring-structured network that uses token passing as an access protocol.



A data receiver-transmitter pair is present at each node of the network. All network traffic must pass through them. The Ring architecture is a store and forward type of system.



(Frame format of 802.5 standard)

- Start of frame :- It represents state of frame itself.

- Access Control :- It contains token bit monitor bit, priority bit & reservation bit.

- Frame Control :- It specify the frame type.

- Destination Address - It shows the address of destination.

- Source Address - It shows the address of source.

- Data - It contains the actual data of no limit.

- Checksum:- It is used to detect the communication errors.

- End of frame:- It represents the end of frame.

Frame status - It contains two bit A and C.
A = destination present
C = Frame copied.

A	C	Result
0	0	F
0	1	F
1	0	F
1	1	T

When A = 1 & C = 1 then transmission is said to be successful.

Data link layer

Function of Data link layer :-

1. It provides a well defined service interface to the network layer.

2. It determines how the bits of the physical layer are grouped into frames. (framing).

3. It deals with transmission errors.

4. It regulates the flow of frame so that slow receivers are not swamped by the past sender (frame control).

(1)

- Services provided to the network layer by data link layer :-

There are mainly three services are provided by data link layer to the network layer that are :→

1. Unacknowledged connectionless services
2. Acknowledged connection less service
3. Acknowledged connection oriented services.

(2)

- Unacknowledge connectionless service:

Unacknowledge connectionless service, it consist of having the source machine send independent machine frames to the destination machine without having the destination machine acknowledged them.

If the frame lost, No attempt to recover it.

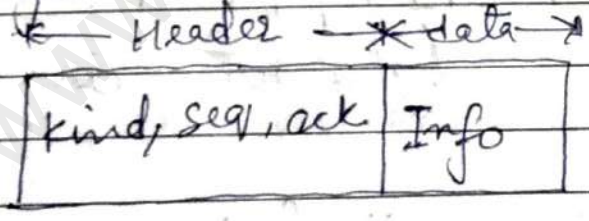
- Acknowledge connectionless service.

IN this no connection use but each frame send is individually knowledge sending again of frame is done when not receive.

Friends Date: 29/8/2017

Acknowledge Connection Oriented service.
In this service source & destination machine establish a connection before any data transfer. Each frame send over the connection is no. and data link layer guarantees that each frames send is received. Further more it guarentees that each frame receive exactly once and all frames received in right order.

(2) • Frames :→
A frame is composed of four feilds
1. Kind
2. SEQ
3. ACK
4. Info

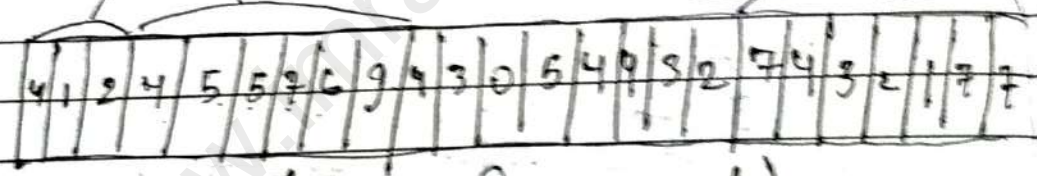


The first three which contain control information called frame Header and the last contains actual data to be transfer.
Kind feilds tells whether or not there is any data in the frame. SEQ, ACK feilds are used for sequence no. & acknowledgement.

Framing :→
In this the data link layer break the bit stream into discrete frames and compute the checksum for each frame. When the frame arrived at the destination the checksum is re-computed. If the newly computed checksum is diff. from the I contained in the frame, the data-link layer knows that an error has occured and takes steps to deal with it.
There are 4 methods of framing:

1). Character count

Data: 124,576,9,30,54,3,2,4,3,2,177,



(character count)

In this method, it uses a feed in the header to specify the no. of characters in the frame

2) starting & ending characters with character stuffing:
In this each frame start with the ASCII character sequence DLE SIX and end with the

sequence:
DLE SIX
DLE ETX
DLE - Data link Escape
STX - Start of Text
ETx - End of Text

Data : ABCD

DLE	STX	A	DLE	B	DLE	C	DLE
D	DLE	ETX					

3) Starting and ending flags with bit stuffing
In this senders data link layer encounters 5 consicative 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

Data : 1 00111111 11001010 11111 00 000 101

1 00111110 11001010 11111 000 000 1111

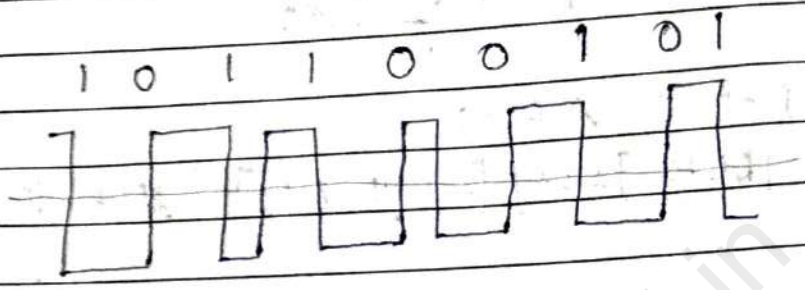
stuffed bits

4) Physical layer coding violations:
In this LAN encode one bit of data by using two physical bit. Normally a 1 bit is highly low pair and 0 bit is a low high bit. In this every

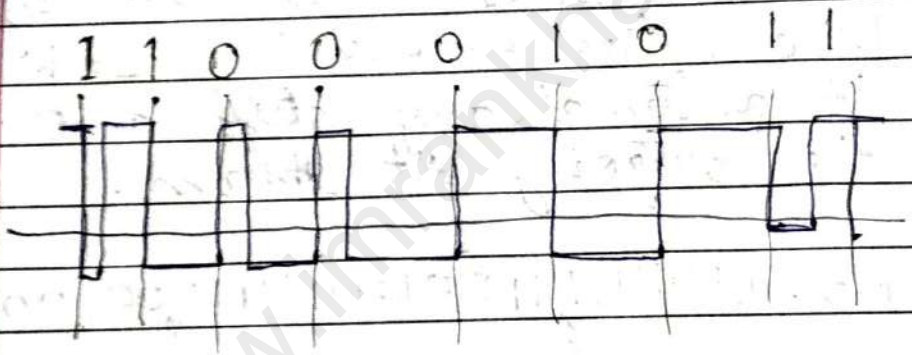
Friends
Date: 05/09/2017

data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries.

Data: 101100101



Data 11000 1011



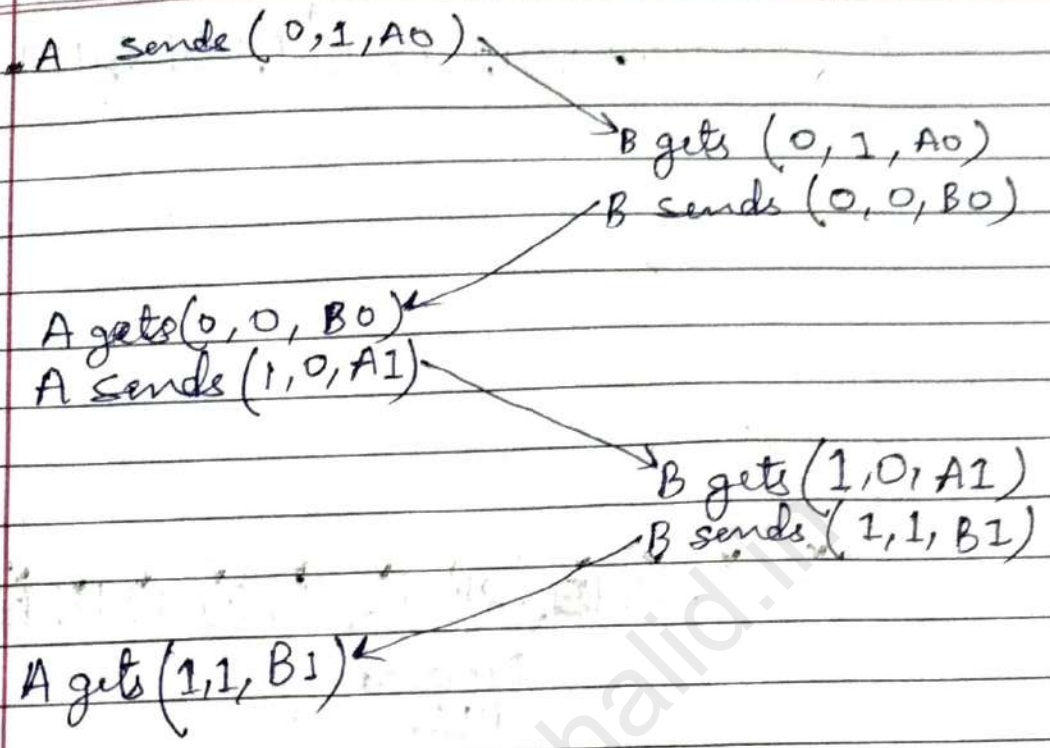
- Data link layer protocols:

Sliding Window Protocol

(A). A one bit sliding window protocol

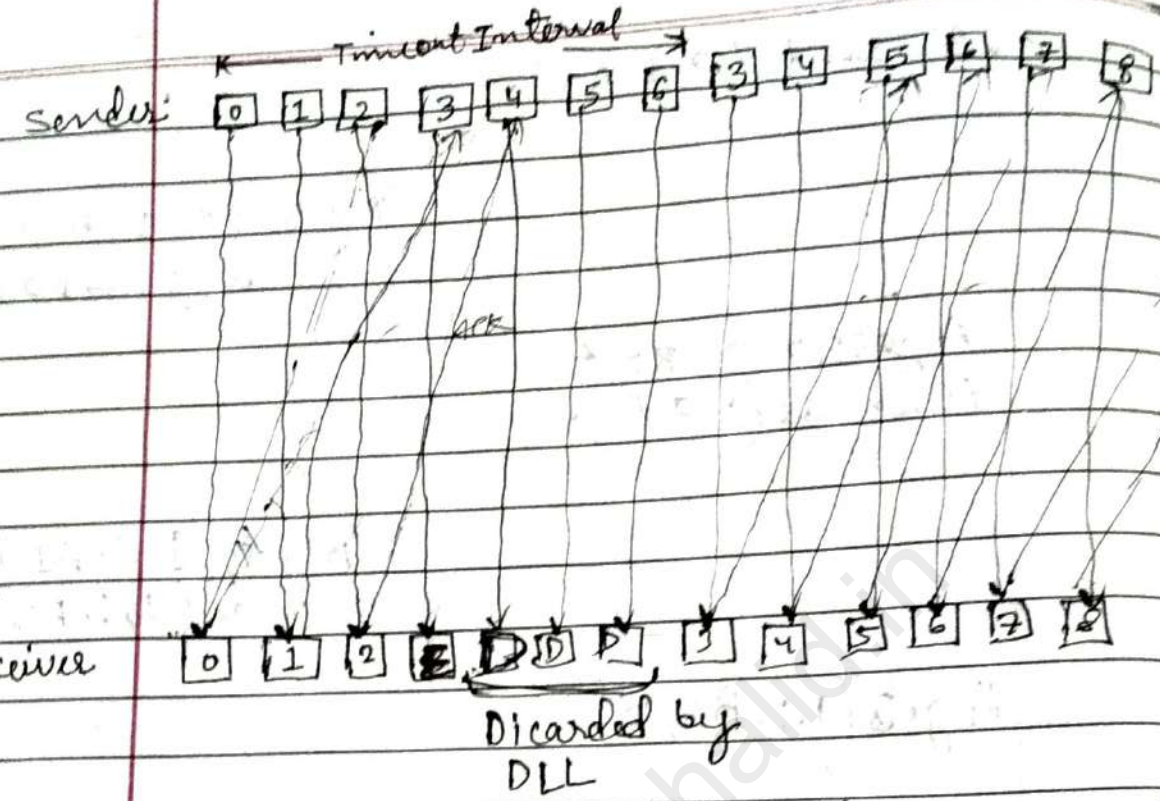
This protocol contains a max. window size of one. Such a protocol uses stop and wait, since the sender transmits a frame and waits for its acknowledgment before sending the next one.

A S



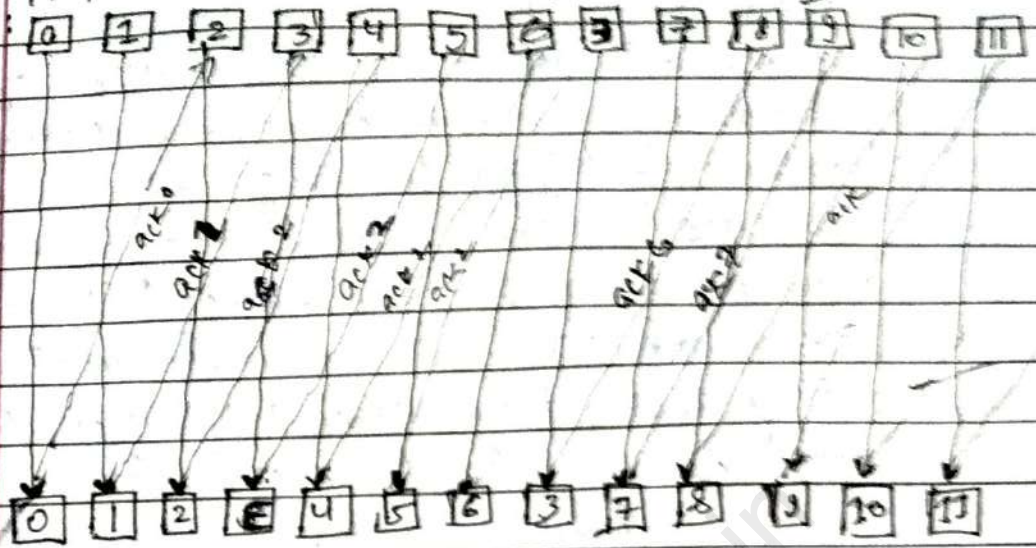
1B) A protocol using Go back-in :: In this the receiver simply discards all sub sequent frame, sending no acknowledgements for the discarded frame. The Data link layer refuses to accept all other sub sequent frame after a frame with error receives. If the senders window fills up before the timer runout the pipeline will ~~become~~ began to empty. Eventually the sender will time out and retransmit all unacknowledge frames in order, starting with the damaged or lost one.

Friends
Date: 05/09/2017



(c) A protocol using selective Repeat

In this the receiving DLL stored all the correct frames following the bad one when the sender finally notices that something is wrong it just retransmit the one ~~back~~ frame not all the its successors. If the second ~~try~~ succeed, the receiving DLL will now have many correct frames in sequence, so they can all be ended off to the network layer quickly and highest no. acknowledge.



12/09/2017

→ Error Detection and correction

• Types of errors

(a) single bit error →

In single bit error, only one bit in the data unit has changed.

e.g → Data : 1010
Data with error received : 1110 (E)

(b) Burst error →

In burst error, two or more bits in the data unit have changed.

e.g → Data : 1010
Data with error received : 1100 (EE)

Redundancy

Error detection uses the concept of redundancy which means adding extra bits for detecting errors at the destination. This technique is called because the extra bit are redundant to the information, they are discarded as soon as the accuracy of transmission has been determined.

→ **Error detection Method:**

(a) Parity check:→

In parity check, a parity bit is added to every data unit so that total no. of 1's even is even parity and total no. of 1's is odd is odd parity.

In this technique, a redundant bit called a parity bit is added to every unit so that to make the total no. of 1's even or odd.

Eg → Even Data 10101 ! ← parity bit (calculation) → send → 1010101 ✓

10101 01 → send → 1010111 ✗

1's is not even

(b) CRC [cyclic Redundancy check]:-
CRC is a based on binary division. The redundancy bit used by CRC are derived by dividing the data unit by a pre determined divisor, the remainder is CRC. The remainder is appended to the end of the data unit so that the resulting data unit becomes exactly divisible by the second predetermined binary number.
At its destination, the incoming data-unit is divided by same number if at this step, there is no remainder the data unit is assumed to be intact and is therefore accepted.

- Steps to calculate CRC:-

1. First are string of n zero is appended to the data unit, The number of zeroes (n) is less than 1 as no. of digits in divisor.

2. Second the newly data unit is divided by the divisor by using binary divisor. The reminder result is the CRC.

3. Then put CRC is place of zeroes in last of data and send the data.

4. At distination, we divided the received data by some divisor and if we get

zeroes as remainder then data is acceptable:

For Eg:-

- calculate CRC for the given data

Data : 1010011110

Divisor : $x^3 + x + 1$

⇒ 1011

3210
1011

$n+1 = 4$

$n = 3$

At the sender's end,

Data : 10100111110000

```
          100 1000111
1011) 10100111110000
      1011↓↓↓
      0001011
         1011
         0000 1100
              1011
               1110
               1011
               1010
               1011
               0001
```

A	B	R
0	0	0
0	1	1
1	0	1
1	1	0

001 CRC

Data 1010011110001 sends → Re-checked

At the receiver end:
Re-checked procedure by receiver →

```
1011 ) 10100111 0001
       1011
       -----
        0001011
           1011
           ----
           01100
            1011
            ----
            01110
             1011
             ----
             0101 1
              1011
              ----
              0
```

Q → calculate CRC for the given data:
Data : 1011000
Divisor : x^3+x

At the sender: 1010 (no. of digits = 4)

$n+1=4$

$\boxed{n=3}$

Data = 1011000 11000

(a)

```
1010 | 1011000 | 110000
       1010
        1000
        1010
          0010 11
          1010
          0001000
             1010
             00100
```

CRC

At receiver end data received:

1101001011010

Divisor: x^3+1

3210
1001

```
          1100 1011
1001 | 1101001011010
       1001
        01000
        1001
          0001010
          1001
            0011 11
            1001
              0111 00
              1001
                0101 1
                1001
                  100 0
```

Friends
Date: 12/9/2019

- Error detection and correction Methods:-

@ Hamming code: (only for 7 bits)
At the receiver end, we can correct the error by using hamming code technique. By using hamming code technique we can correct a single bit error.

i) At the sender End

11	10	9	8	7	6	5	4	3	2	1
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

r_1 : bits 1, 3, 5, 7, 9, 11
r_2 : bits 2, 3, 6, 7, 10, 11
r_4 : bits 4, 5, 6, 7
r_8 : bits 8, 9, 10, 11

At the sender's end, let we have data: 1001101, calculating the even parity to each corresponding values associated with r_1, r_2, r_4 and r_8 and write these values to their places and send this calculated code.

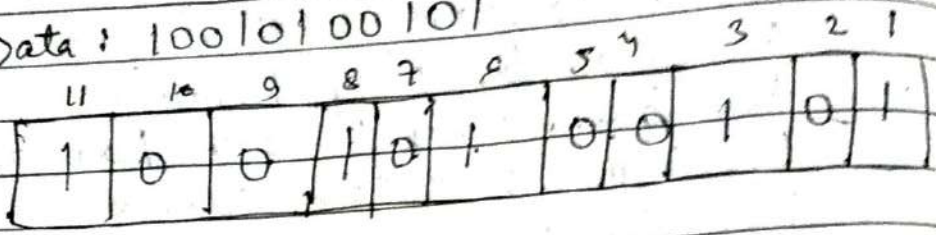
11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	1	1	0	0	1	0	1

Hamming code: 10011100101 → send

Q.17

→ At the receiver end :→

Data : 1001|0|100|101



r_1 – 1, 3, 5, 7, 9, 11
1 (110001)

r_2 – 2, 3, 6, 7, 10, 11
(0, 1, 1, 0, 0, 1)

r_4 → 4, 5, 6, 7
1 (0, 0, 1, 0)

r_8 → 8, 9, 10, 11
0 (1, 0, 0, 1)

$(r_8, r_4, r_2 r_1)$

$(0111)_2 \longrightarrow (7)_{10}$

Error is at 7 bit in hamming code w/c recevid by receiver.

(10011000101) code

Data: 1001101

Ans.

Friends Date: 12/9/2017

Q1 → calculate the hamming code for the given data.

Data : 1100101

11	10	9	8	7	6	5	4	3	2	1
1	1	0	r_8	0	1	0	r_4	1	r_2	r_1

$r_1 = 0 \ (1, 0, 0, 0, 1)$

$r_1 : 1, 3, 5, 7, 9, 11$

$r_2 = 0 \ (1, 1, 0, 1, 1)$

$r_2 = 2, 3, 6, 7, 10, 11$

$r_4 = 1 \ (0, 1, 0)$

$r_4 : 4, 5, 6, 7$

$r_8 : 8, 9, 10, 11$

11	10	9	8	7	6	5	4	3	2	1
1	1	0	0	0	1	0	1	1	0	0

hamming code : 11000101100

At the receiver end, the received hamming code is.

Data : 10100111001

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	1	1	1	0	0	1
			r_8				r_4		r_2	r_1

1010110

r_1 = 1, 3, 5, 7, 9, 11
0 (1, 0, 1, 0, 1, 1)

r_2 = {2, 3, 6, 7, 10, 11
0 = (0, 0, 1, 0, 0 1)

r_4 = 4, 5, 6, 7
1 (1, 1, 1, 0)

r_8 = 8, 9, 10, 11
0 (0, 1, 0, 1)

$(r_8\ r_4\ r_3\ r_1) \rightarrow (0100)_2 \rightarrow (4)_{10}$ VR

(10100110001) → Hamming code
↓ Data
10|0110

b) LRC and VRC :→
LRC = Longitudinal Redundancy code
VRC = Vertical Redundancy code

In this method, a block of bits are organized in a table (rows, columns). First we calculate the parity bit for each data unit. Then we calculate the parity bit for each column and create a new row of 8 bits. They are the parity bit for whole block.

[28 bits block → 7 bits]

Friends
Date: 12/09/2017

Data: 11010111100 11111011111110 111

Data: 1101011, 1100111, 1101111, 1110011,
b_1 b_2 b_3 b_4

1	1	0	1	0	1	1	1	b1
1	1	0	0	1	1	1	1	b2
1	1	0	1	1	1	1	0	b3
1	1	0	0	1	1	1	1	b4
VRC → 0	0	0	0	1	0	0	1	b5

↑ LRC

sende:
→ 1101011 1100111 1101111 1110011

check error at receiver ende →

1	1	0	1	0	1	1	1	
1	1	0	0	1	0	1	1	error
1	1	0	1	1	1	1	0	
1	1	0	0	1	1	1	1	
0	0	0	0	1	1	1	1	

Q → calculate LRC and VRC

Data → 1101101 1110001 1000001 1010011

Friends Date: 12/9/2017

LRC

1	1	0	1	1	0	1	1	
1	1	1	0	0	0	1	0	
1	0	0	0	0	0	1	0	
1	0	1	0	0	1	1	0	
1	0	1	0	0	1	1	1	← VRC
0	0	0	1	1	1	1	0	

LRC = 10001

VRC = 00011101

Data : 11011011 11100010 10000010
10100110 00011101

Friends
Date: 26/09/2017

Network layer

Network layer is responsible for carrying a packet from one computer to another, it is responsible for Host-to-Host delivery.
The network layer is a packet switched network that uses connectionless communication.

- **Network layer at source :-**
The network layer at source is responsible for creating a packet that carries two universal addresses. at destination & source address.
The source network layer receives data from the transport layer at the universal address and adds universal of Host A (sender) and adds the universal address of Host B (destination), and makes sure that the packet is of correct size for passing through the next link.

- **Network layer at destination :-**
At destination if the packet is a fragment, the network layer waits until all fragment arrived, and then it re-assembles them and deliver to the transport layer.
reassembled packets to

Friends
Date 26/09/2017

Addressing:-
At the network layer we need to uniquely identify each device on the internet to allow global communication b/w all devices.

(i) Internet Addresses
The identifier used in the network layer of the internet model to identify each devices connected to the internet is called internet address or IP Address and IP is 32 bit address. The IP addresses are unique and universal.

Notations of IP Addresses:
There are two common notations to show an IP address:

① Binary notation
In Binary notation the IP address is displayed as 32 bits. To make the address more readable one or more spaces are usually inserted b/w each octet (8 bit).

e.g→ 00000001 11001100 11111100 01011100

② Dotted Decimal Notation:-
In this addressed is written in decimal form with a decimal point (.) seperating the bytes.

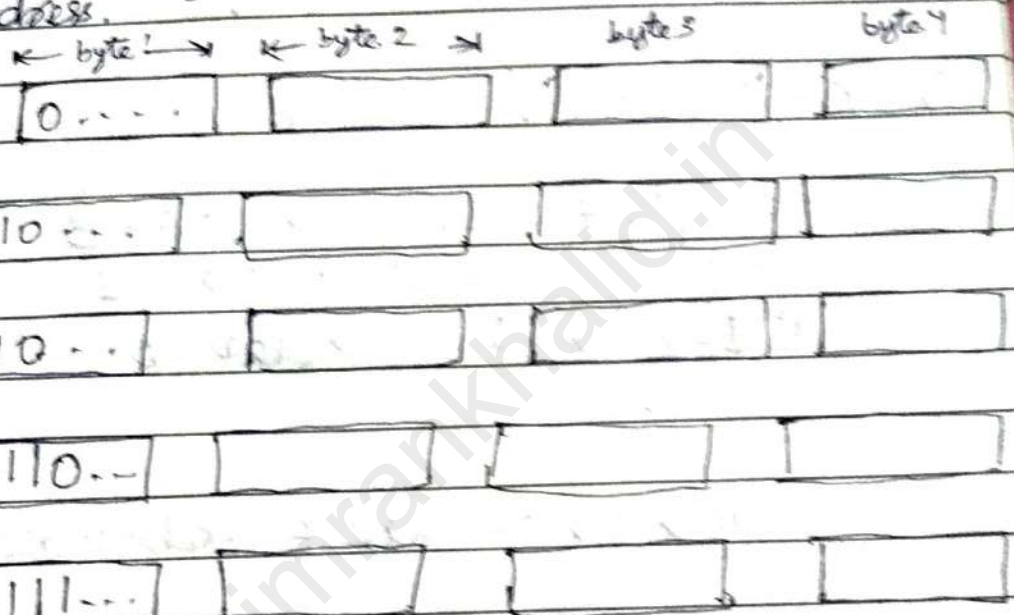
e.g→ 10.2.0.10 , 129.7.15.11

class A
class B
class C
class D
class E
class
class

Date 03/10/2017

Classful Addressing

In classful addressing the IP Address space is divided into five classes, class A, B, C, D & E. If the address is given in binary notation the first few bits can immediately tell us the class of the Address.



class C → 11010101.10110101.11010111.11011111

class D → 11100010.10111011.01110111.00111101

class A → 01001011.10110111.10111011.10001011

Finding the class in dotted decimal notation; in this each class has a specific range of number.

(a) 191.7.5.19 → class B
(b) 240.9.11.15 → class E
(c) 129.7.5.11 → class B

H.W → where class E Address are used?

- Unicast and Multicast, Reserved Addres

Unicast Addresses

Addresses in class A, B and C are for unicast communication, from one source to one destination. A Host needs to have atleast one unicast address to be able to recieve and send packets.

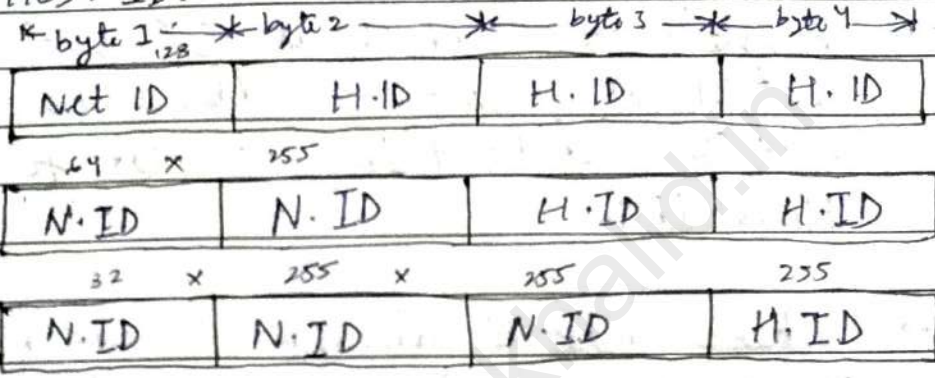
Multicast Addresses

Addresses in class D are for multicast communication, from one source to a group of destinations.

Friends
Date: 3/12/2017

Reserved Address :-
Address in class E are reserved for future use.

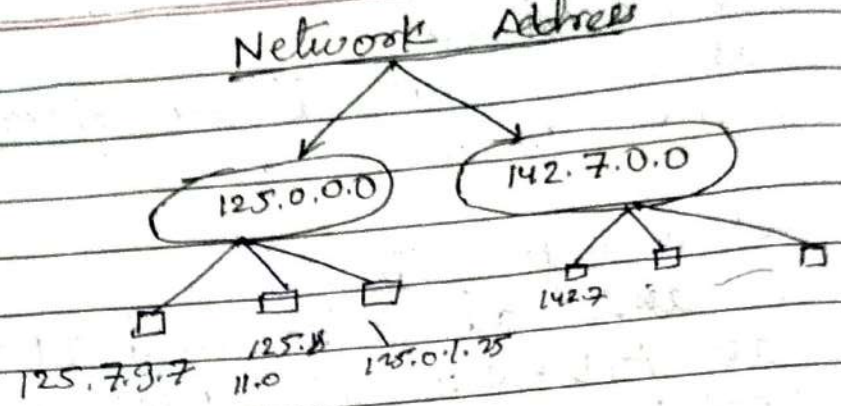
Net ID & Host ID
In classful addressing and IP address in class A, B & C is divided into Net ID & Host ID.



H.W → How many internet connection are availale in worldwide and list according to country (max 10).

Network Address
The network address is an address that defines the network itself it can not assigned to a Host.
In classful addressing is the one that is asign to the organization.

Date: 3/10/2017



A network address is different from a net ID. A network address has both net ID and HOST ID with 0s for the Host ID.

Q → Where class E Addresses are used?

Ans → Network stack implementations are written to support the FRC, and hence will not sent or accept packets from IPs that are reserved for future use. Besides the networking stack services have to support them as well; DHCP has to be able to distribute them, DNS has to be able to store them, the software at IANA and your ISP must be able to actually support the creation and usage of that block.

By the time we all support this class E block, we will have made big progress switching to IPV6 so it'll no longer be worth it. Developers ISPs and consumer better invest in switching to IPV6 instead.

No network stacks are tested to work with class E addressess, and there is no reason that router would treat them as unicast. Assuming you updated the network stacks on every device on the internet to treat class E as unicast, you'll get a year or so of run rate. Youre better off investing in IPv6.

Q → How many internet connections are available in worldwide and list according to country (max. 10):

Ans → Total internet connections in world wide are: 3,746,332,421 on 9-october-2017 at 12:12:01.

1.	China	721,434,547
2.	India	462,124,989
3.	U.S	286,942,362
4.	Brazil	139,111,185
5.	Japan	115,111,595
6.	Russia	102,258,256
7.	Nigeria	86,219,965
8.	Germany	71,016,605
9.	U.K	60,273,385
10.	Mexico	58,016,997
11.	France	55,860,330
12.	Indonesia	53,236,719
13.	Viet Nam	49,063,762
14	Turkey	46,196,720

source: www.internetlivestats.com

A4 (only one side)

Friends
Date: 10/10/2017
Page No.

Assignment No. 1

L.D → 25/10/2017

Q1 → Draw the TCP/IP network architecture model and explain the features of various layers.

Q2 → How does ATM works? Explain in detail through a diagram.

Q3 → write in detail about working functionality of
(i) Bluetooth
(ii) wireless Transmission
(iii) Optical fibre
(iv) Infrared

Q4 → write in detail about these terms:
① ISDN
② FDDI
③ HDLC
④ Multimedia File Transfer

Friends
Date: 10 | 10 | 2017

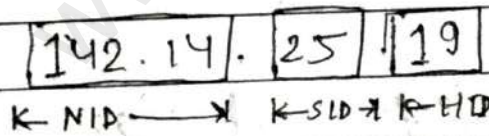
Q → which algo. is used by Google for searching?

Subnetting

In subnetting a network is divided into several smaller group with each subnetwork having its own subnetwork address.

For example, a university may owns to group its hosts according to department. In this case, a university has one network address, but needs several subnetwork addresses. The outside world knows the organization by its network address. Inside the organization each network is recognized by ~~each~~ its subnetwork address.

(without subnetting)



(with subnetting)

Supernetting

In supernetting an organization can combine several class C blocks to create a large range of addresses. Several networks are combine to create a super network.

Friends
Date: 10/10/2017

Mask

The router outside the organization has a routing table with one column based on the network addresses, the router inside the organization has a routing table based on the subnetwork addresses. A 32 bit key is called mask. The router outside the organization uses a default mask. The outer inside a organization uses a subnet mask.

Default mask is a 32 bit binary number that gives the network address when ANDed with the address in the block.

For example the packet has address 190.245.7.90 find the network address to root the packet.

Steps for find Network address:

step 1. Find its class
⇒ Class B

2. Default mask for all class
Class A = 255.0.0.0
B = 255.255.0.0
C = 255.255.255.0

3. Then router ANDs this mask with IP address and get its network address

Friends
Date: 31/10/2017

190.245.7.90

↓

10111110 11110101 00000111 10110100

11111111 11111111 00000000 00000000

= 10111110 11110101 00000000 00000000

= 190.245.0.0

Routing Techniques

Routing requires a host or a router to a have a routing table. when a host has a packet to sent or when a router receives a packet to be forwarded, it looks at this table. to find the route to the final destination.

As the internet has no. of entries in the routing table makes table lookups inefficient. so techniques are made to make the size of the routing table managable and handle issue such as security.

Some routing techinques are:

(1) Next-Hop Routing

To reduce the contents of a routing table technique used next-Hop routing. In this, the routing

table holds only information that leads to the next of HOP instead of holding of information all route.

(2). Network specific Routing
Here instead of having 2nd entry for every host connected to some physical network, we have only one entry to define the address of the network itself.

(3). Host specific Routing
In this the destination Host address is given the routing table.

(4). Default Routing
In this when there is a 500 big network is connected to the router and upto a host and the route is frequently used and we make entry of network as default.

Static & Dynamic Routing Table
- Static Routing Table
It contains information entered manually. The administrator enter the route for each destination into the table. when this type of table is created It cannot update automatically

when there is a change in internet.

Dynamic routing Table:
A dynamic routing table is updated periodically using one of the dynamic protocol such as (RIP) Routing Information protocol), OSPF (open shortest path first), whenever there is a change in internet, such as a shut down of a router or breaking of a link, the dynamic routing protocol update all the tables in the routers.

Routing Algorithm

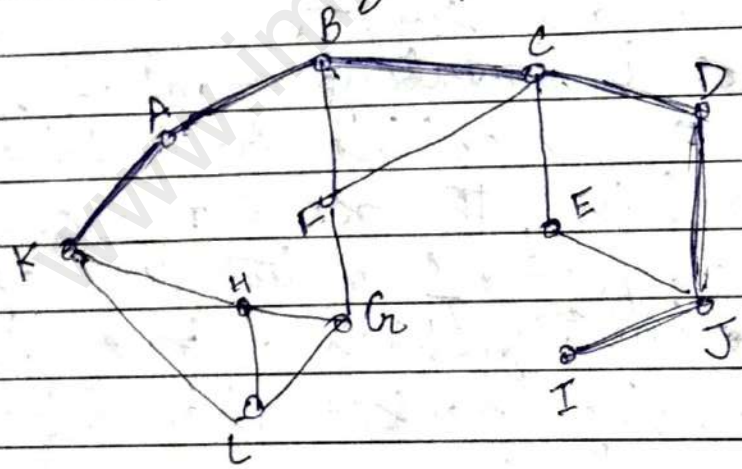
The main function of a network layer is routing packet from the source machine to destination machine. The routing algorithm is a part of network layer software responsible for deciding which output line and incoming packet should be transmitted on.
The routing algo's can grouped into two major class:
(1) Non adaptive Algorithms:
It do not based their routing decision on measurement or estimate the current traffic and topology.

Friends
Date: 31/10/2017

Instant the choice of the rule to use get from source to destination is computed in advanced, offline and downloaded to the routers when the network is booted, it is also called static routing.

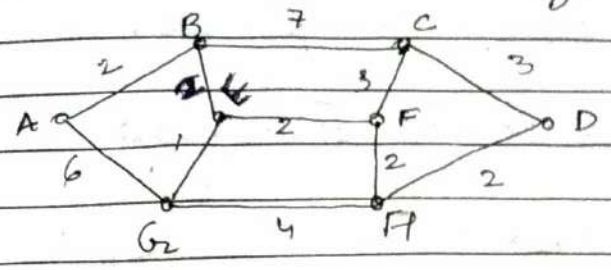
Adaptive Algorithms
It changes their routing decision to reflect changes in the topology and usually traffic as well.
Adaptive algo differ in pair they get their information when they change the routes and what metric is used for optimization.

(1.) The optimality principle



It states that if router "J" is on the optimal path from router "K" to router "I", then the optical path from "K" to "J" also fall along the same route.

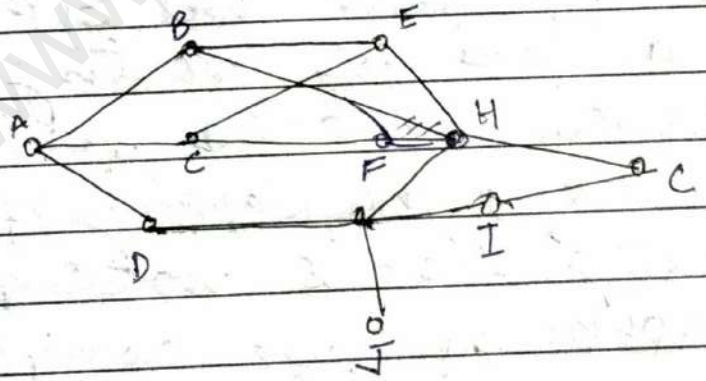
(2). Shortest Path Routing Algorithm



In this each node of the graph representing a ~~routing~~ router and each arch of the graph representing a communication line to choose a route b/w a given pair of routers the algorithm just find a shortest path b/w that graph.
To go from "A" to "H" we choose a given path.

$$A \xrightarrow{2} B \xrightarrow{2} E \xrightarrow{2} F \xrightarrow{2} H$$

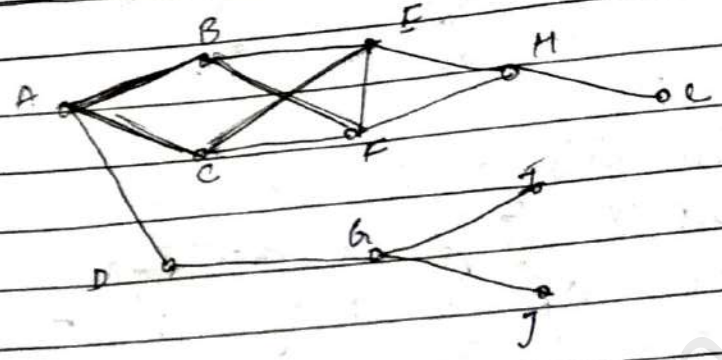
(3.) Flooding



In this every incoming packet is send out in every outgoing line except the one it arrive on.
Flooding generate a vast no. of duplicate packets and infinite

no. unless some measure are taken to damp the process.

(3) Selective Flooding



In this algo, the routes don't send every incoming packet on every line, it only send on those lines that are going approx. the right direction.

(4). Flow - Based Routing

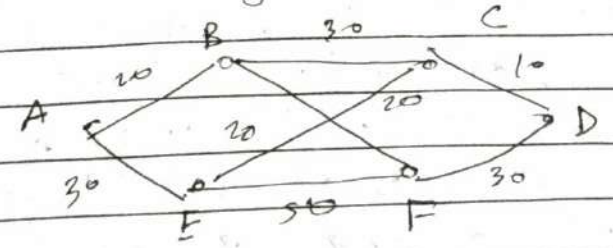
The algo that uses both topology and load for routing is called flow based routing.

In this, the capacity of ~~every~~ ~~avaga~~ flow is ~~note~~ we known an we compare the mean ~~com~~ packet delay on the line.

$$T = \frac{1}{\mu C - \lambda}$$

T delay time.

$1/\mu$ – mean packet size in bit
C – capacity in bps
λ = mean flow packet/sec.



(5). Distance vector Routing

This algo. operates by having each router maintained a table (Vector) Giving the best known distance to each destination and which line to use to get their. These tables are updated by exchanging information with neighbours.

To	A	B	C	D	E	F
A	0	10	20	15	30	15
B	10	0	15	25	30	45
C	20	15	0	15	20	25
D	15	25	25	0	15	20
E	30	15	40	20	0	15

Friends Date: 3/10/2017

(6). Link state Routing

The idea behind L.S.R is simple and can be stated as 5-parts.

Host (i) Discover its neighbours and learn their network address.

(ii) Measured the delay or cost to each of its neighbours.

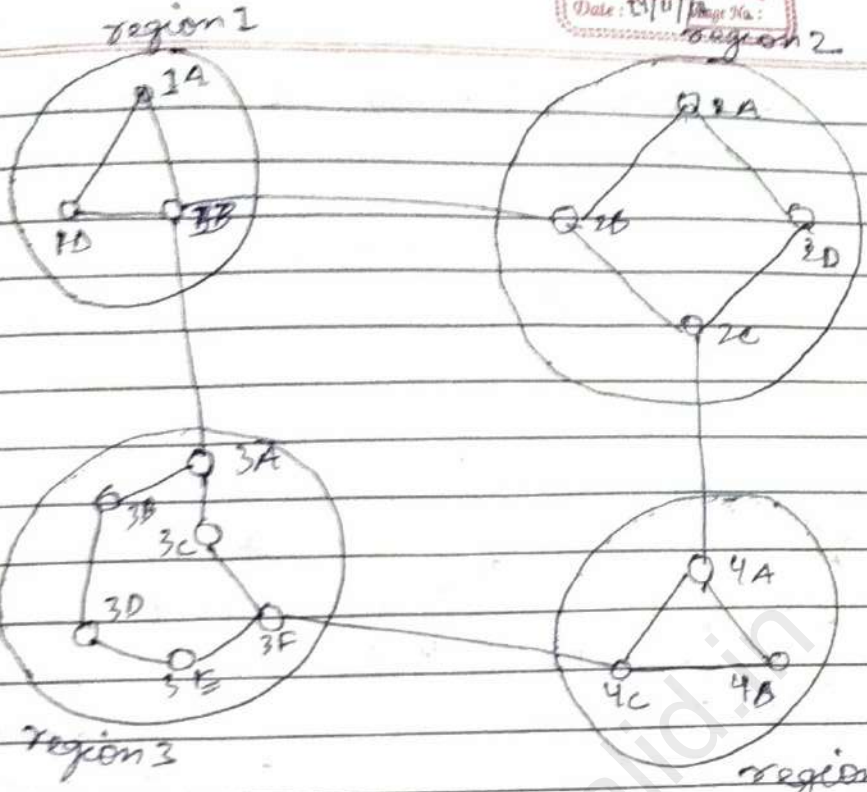
(iii) Construct a packet telling all it has just learned.

(iv) send this packet all other neighbouring routers.

(v) Compute the shortest path to every other router.

(7) Heirachical Routing

As network grow in size the router's routing table grow proportionally. Not only is router memory consume by ever increasing tables but more CPU time is needed to scan them and for more bandwith is needed to send status report about them. It is no longer feasable for every router to have an entry for every other router, so the routing will have to be heirarchical.

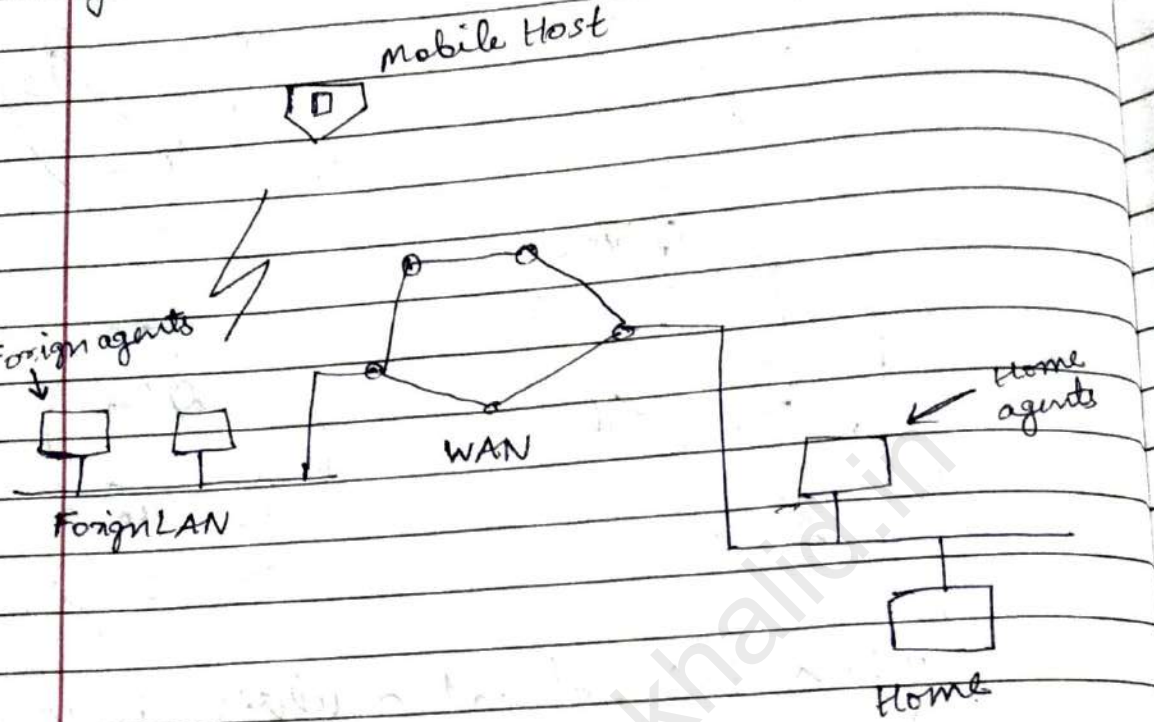


when Heirarchical routing is used, the routers are divided into regions with each router knowing all the details about how to route packets to destination within its own region but knowing nothing about the internal structure of other region.

B). Routing for Mobile Host

Millions of people have portable computers now a days and they generally wants to Read their email and acces their normal file system wherever in the world they may be these mobile host introduced a new complications, to route a packet to a

mobile host, the network first has to find it



To reserve the situation, each area has one or more foreign agents which keep track of all mobile users visiting the area. In adding each area has a home agent which keep track of users whose home is in the area but who are currently visiting another area. After mutual communication service are provided to the mobile host.

(9). Broadcast Routing

For some applications host needs to send messages to many or all other hosts for example a service distributing weather reports

stock market updates or live radio programs.
Sending a packet to all destination simultaneously is called broadcasting.

(10.) Multicast Routing
For some applications widely seperated process work together in groups. for example a group of process mipleting a distrted database system.
It frequently is necessary for one process to send a message to all the other member of the group. Sending a message to such a group is called multicasting and its routing algorithm is called multicast routing.

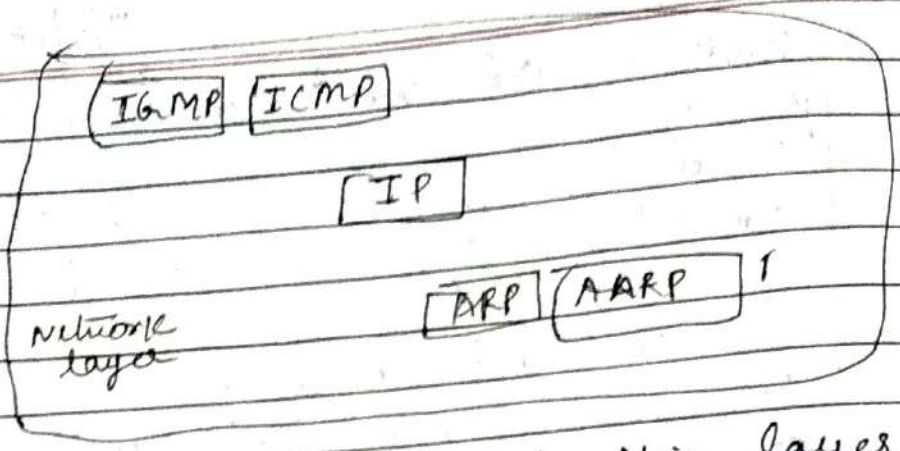
Network Layer Protocol

1. IGMP
Internet ~~control~~ Group Mongenet pro.to)

2. ICMP
Internet control Message protocol

3. ARP
Address resolution protocol

4. RARP
Reverse address resolution protocol



The main protocol in this layer is IP which is responsible for Host to Host delivery of data grams from a source to a destination.
IP needs a protocol called ARP to find the MAC address of next HOP.
During datagram delivery, IP needs the services of ICMP to handle unusual situation such as occurance of an error.
For multicasting IP uses the services of another protocol called IGMP.

ARP

Address resolution protocol a packet starting from a source host may pass through several diff. physical network before finally reaching a destination host. The host and router are recognized at the network level by their IP address.
At the physical network level the host and router are recognized by their MAC addresses. A MAC

address is a local address. It should be unique locally but not necessarily universally.
This means the delivery of a packet to a host or a router requires two levels of address. (IP & MAC)
We need to be able to map an IP address to its corresponding MAC address. These mapping are called dynamic mapping, here once a machine knows of the two addresses it can use a protocol to find the other one.
These protocols have been designed to perform dynamic mapping (ARP & RARP).
The ARP map an IP address to a mac address. The RARP map the MAC address to an IP address.

→ IGMP & ICMP H.W

IGMP (Internet Group Management Protocol)
IGMP is a group of management protocol that mainly manages the group membership in a multitask network. In a multicast network, multicast routers are used to write packets to all the computers that are having membership of a particular group.
The multicast router used the information from IGMP to determine which host are having

membership of which group. A multicast router generally receives thousands of multicast packets that have to be transmitted to various groups. If a router has no knowledge about the group membership, it will broadcast packet to every host and this will increase the load on the network.

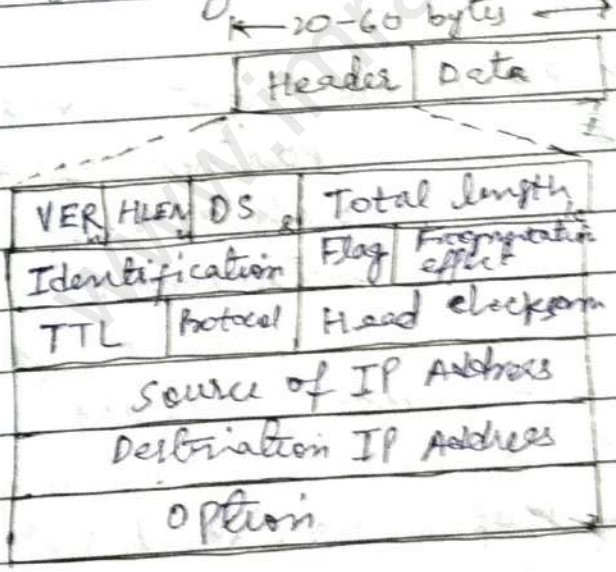
ICMP (Internet Control Message Protocol)
ICMP is a TCP/IP network layer protocol that provides troubleshooting control and error message services. ICMP is most frequently used in operating system for networked computers, where it transmits error messages. ICMP for Internet protocol version 4 is called ICMP v4 and for Internet protocol version 6 is called ICMP v6. ICMP is also known as RFC 792. An ICMP message is created as a result of errors in an IP ~~diagram~~ datagram or for diagonstic routing purposes.
These errors are reported to the ~~original~~ originating datagram's source IP address. An ICMP message is encapsulated directly within a single IP datagram and reports error in the processing of datagrams. An ICMP header begins after the IP v4 header. An ICMP packet has an eight byte header, followed by a variable-sized data section. The first four bytes of the header are fixed.

IP

The internet protocol (IP) is the Host-to-Host network layer delivery protocol for the internet. IP is an unreliable and connectionless datagram protocol, a best effort delivery service.

Datagram

Packets in the IP layer are called datagram. Its a variable length packet consisting of two parts Header & Data.
The Header is 20-60 bytes in length and contains information essential to routing and delivery.



VER
It defines the version of the IP.
HLEN → It defines the length of the datagram Header (Header length).
DS → Differentiated services

It defines the class of Datagram for quality of services purposes.

- **Total length** → It defines the total length of the Datagram in bytes (length = total length of data + Header length).

- **Identification** → This field identify the datagram orginating from the source host.

- **flag** → It is a three bits. 1st bit is reserved, 2nd bit is for fragmentation. (0 or 1 for allow and not allow for the fragmentation), 3rd bit is for to allow more fragment.

- **Fragmentation offset** → It shows the relative position of fragment with resp. to the whole datagram.

- **TTL** → TTL (Time To leave). It is used to control the max. no. of Hops (Routers) visited by the datagram. Going 1 to other router, the value is decremented in the datagram.

- **Protocal** → It defines the higher level protocal that uses the

Friends
Date: Page No.:

suvices of IP layer.

- Headerchecksum → Header checksum covers the header only, it is calculated for the header related errors.

- Source address → It defines the IP address of source

- Destination Address → IP address of destination.

- Option → This field is not required for every datagram, this is used for network testing and debugging.

- Fragmentation HW

When an IP datagram travels from one host to another, it can pass through different physical layer networks. Each physical network has a maximum frame size. This is called the maximum transmission unit (MTU). It limits the length of a datagram that can be placed in one physical frame. IP implements a process to fragment datagrams exceeding the MTU. The process creates a set of datagram

within the maximum size. The receiving host reassembles the MTU. IP requires that each link support a minimum MTU of 68 octets. This is the sum of the max. IP header length (60 octets) and min. possible length of data in a non-final fragment (8 octets). If any network provides a lower value than this, fragmentation and reassembly must be implemented in the network interface layer. This must be transparent to IP. IP implementation are not required to handle unfragmented datagrams larger than 576 bytes. In practice, most implementation will accomodate larger values.

- The following steps fragment the datagram:

① The DF flag bit is checked to see if fragmentation is allowed. If the bit is set, the datagram will be discarded and an ICMP error returned to the originator.

② Based on the MTU value, the data field is split into two or more parts. All newly created data portions must have a length that is a multiple of 8 octets, with the exception of the last data portions.

③. Each data portion is placed in an IP datagram. The headers of these datagrams are minor modification of the original.

Friends
Date: 21/11/2017

IPv6 (Internet Protocol Version 6) or IPng (Internet Protocol next generation)

The network layer protocol in the internet is currently IPv4. It has some deficiencies.

1. IPv4 has 2 level of address structure (Net ID & Host ID). The use of address space is efficient.
2. The Internet must accomodate real time audio & video transmission. Reservation of resource is not provided here for minimum delay.
3. No security mechanism was provided.

To overcome these deficiency, IPv6 was proposed and is now a standard. IPv6 has following advantages.

1. Large address space of 128 bits long.
2. Better header format to speedup routing process.
3. New options for additional function.
4. Allowance of extention, to allow the extention of

(5) support of resource allocation that is used to support traffic such as real time audio video transmission.
(6) support for more security.

IPv6 addressing

- Hexadicamal colon notation. Here 128 bytes means 16 bytes equalls to 32 Hexa digits. Two byte in each coloumn, 4 digits seperated by a ~~Colomn~~ colon is used for notation.

for ex. →

FADI : AB71 : 3740 : AFF3 : A770 :
7976 : 0632.

← 128 bit = 16 bytes = 32 Hex digit →

IPv6 Packet Format :

VER	PRI	Flow label	
Payload length		Next Header	Hop limit
source address			
Destination Address			
Payload			

Friends
Date: 21/10/2017

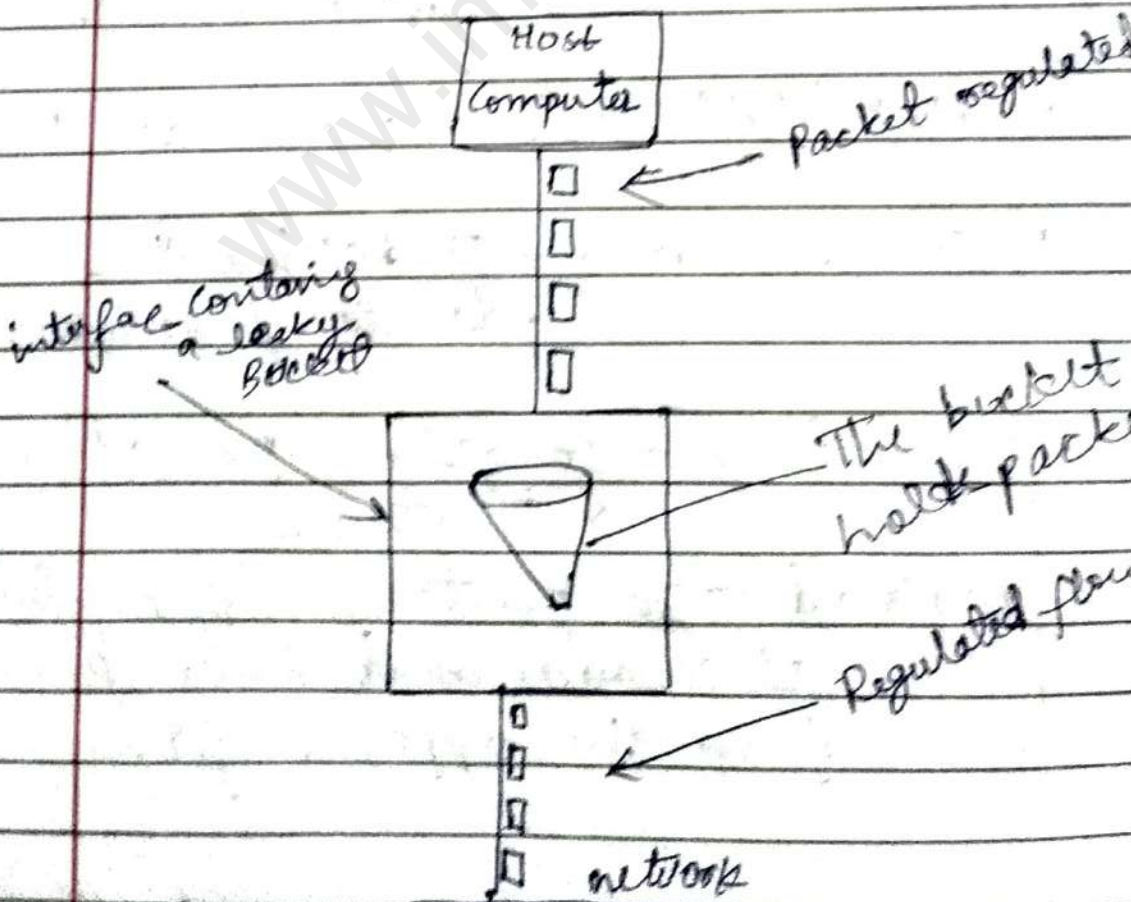
- VER → It defines the version for IPv6. its value is 6.
- PRI → It defines the priority of packet with resp. to traffic congestion.
- Flow label → It is designed to provide special handling for a special particular flow of data.
- Payload → It defines the total length of IP datagram.
- Next Header → It defines the header that follows the base header in the datagram.
- HOP limit → It is same as TTL.
- Source address → It defines the address of source.
- Destination → It defines the address of destination.
- Payload → It contains extention of Header and data packet from the upper layer.

Congestion

When too many packets are present in a part of packet network (subnet) performance degrades. This situation is called congestion.

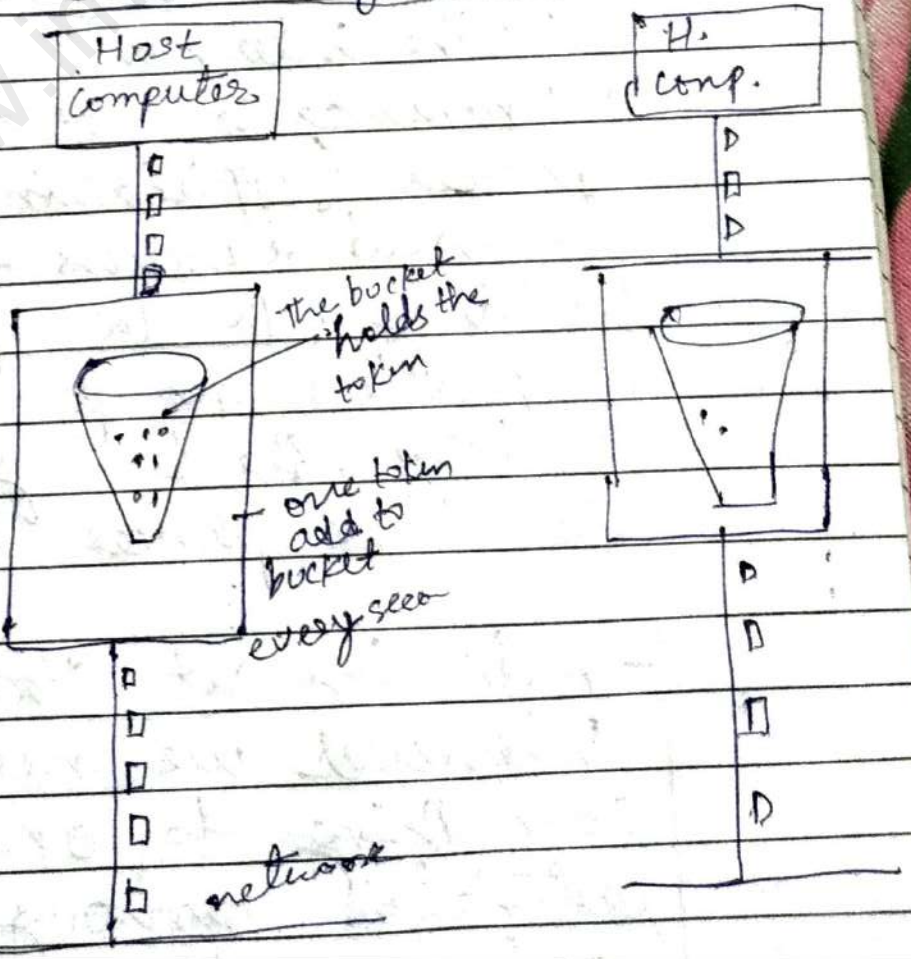
As the traffic increases too far, the routers are no longer able to cope and they become loosing packets. This tends to make matter worse. At very high traffic performance collapses completely and almost no packet are deliver. Over this congestion control algorithms are designed.

① The leaky Bucket Algorithm →



In this each host is connected to the network by an interface containg a leaky bucket that is a finite internal queue. It is just a single server queing system with constant service time. This method is mechanism to control uneven flow packets from the user processess inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion. Here lost of data exist when the bucket is full.

(2) The token Bucket Algorithm →



It is more flexible algo. that never loses data for token bucket algorithm. In this algo. the bucket holds token, generated by a clock at the rate of 1 token every ΔT second. For a package to be transmitted it must capture and destroy one token

Transport Layer

It is need for process to process delivery. The internet modal has two protocol at the transport layer.

① UDP (User Datagram Protocol)
② TCP (Transmission Control Protocol)

- Process to Process Delivery

In the internet communication real communication takes place b/w two process (application programs). We need a process - to - process delivery. The transport layer is responsible for process to process delivery, the delivery of message, from one process to another.

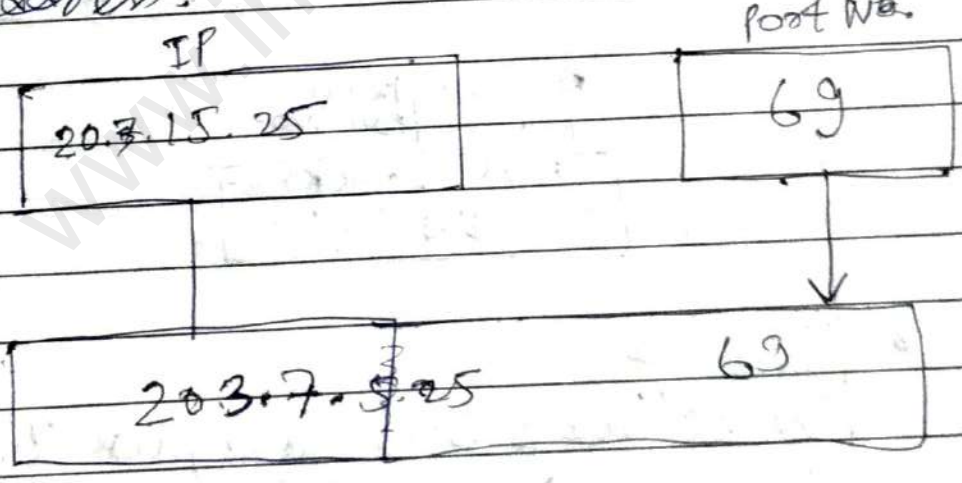
- Addressing at Transport layer

Whenever we need to deliver something to one specific destination among many we need an address. At the

transport layer, we need a transport layer address called a port no., to choose among multiple process running on the destination host. The destination p.no. is needed for delivery, the source port no. is needed for reply. In the internet model, the port no. are 16 bit integer, it means b/w 0 to 65535.

- Socket Address

Process to process delivery needs to identify, IP & port no., at each end to make a connection. The combination of IP address & Port no. is called socket address.

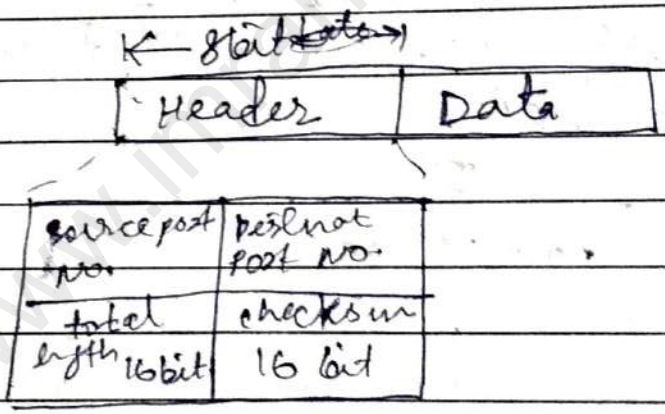


UDP

Connectionless protocol, The simple unreliable transport layer protocol is called user datagram protocol.

UDP is connectionless reliable. It doesn't add anything to services of IP except for providing process to process communication. It performs very limited error checking. UDP is very simple protocol with min of overhead. UDP is a convient protocol for multimedia & multitasking application.

- User Datagram
UDP packet called user datagram having a fixed size of header of 8 bytes



- TCP →
The reliable but complex T.L protocol in the internet is called TCP. TCP is called a stream connection oriented & reliable transport layer protocol.

Friends
Date : Page No. :

segment format :-

[Header | Data]

Source Port No. 16	Destination Port No. 16
Segment No. 32	
Acknowledgement No. 32	
HLEN 4	Reserved 6	Control with flag 6	window size 16
Checksum 16	Urgent Pointer 16
Option 32	

S.P.N → Defines port no. of source.

D.P.N → Defines port no. of destination

Segment No. → It defines the no. assigned to the first byte of data contain in the segment.

Ack. NO. → It contains the source no. of ACK.

HLEN →

Reserved → Reserved for future use

Control with flag → Defines 6 dif. control bits of flags.

W.S → It defines the size of the window.

checksum → Used for error detection

urgent pointer → It is used when contain urgent data.

option → It contains optional information for other uses.

(1)

Application Layer

The A.L allows email to use the internet. The A.L receives services from the various layers and provide services to the user. It provides user interface & support for services such as e-mail, remote file access and transfer and access to the world wide web. The internet is based on client-server model to do a task there must be a client and a server. Although there are several ways to allow a server & client to communicate, the most common one is socket interface. Two computers that are connected by an ethernet must be each run a program one to provide

Friends
Date: 21/11/2017

a service and other request to a server.

1. DNS (Domain Name Server)
2. E-mail
3. FTP
4. HTTP
5. WWW
6. SMTP

① DNS

The Domain Name system (DNS) translates internet domain and host names to IP addresses and vice-versa.
On the Internet, DNS automatically converts between the names we type in our web browser address bar to the IP addresses of web servers hosting those sites. Larger corporation also use DNS to manage their own company intranet. Home networks use DNS when accessing the internet but do not use it for managing the names of home computers.

DNS clients send requests to and receive responses from DNS servers. The DNS database resides on a heirarchy of special database servers. When client like web browsers issue request involving internet host names, a piece of software called the DNS resolver first contacts a DNS

server to determine the server's IP address

② Email

Short for electronic mail, e-mail or email is information stored on a computer that is exchanged between two users over telecommunications. More plainly, e-mail is a message that may contain text, files, images or other attachments sent through a network to a specified individual or group of invidivals. The first e-mail was sent by Ray Tomlinson in 1971. By 1996, more electronic mail was being sent than postal mail.

support@imran.com

- The first portion all e-mail addresses, the part before the @ symbol, contains the alias, user, group, or department of a company. In our above example support is the technical support department at imran.

- Next, the @ (at sign) is used as a divider in the email addresses. It is required for all SMTP e-mail addresses.

- Finally, imran.com is the domain name to which the user belongs.

③ FTP

The File Transfer Protocol (FTP) is the standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client - server model architecture and uses separates control and data connections between the clients and the server. FTP users may authenticates themselves with a clear-text sign in protocol, normally in the form of a username and password, but can connect automatically anonymously if the server is configured to allow it.

FTP is often secured with SSL/TLS (FTPS).

④ HTTP

The HyperText Transfer Protocol (HTTP) is an application protocol for distributed, collaborative and hypermedia information system. HTTP is the foundation of data communication for the world wide web.

HyperText is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989.

HTTP functions as a request-response protocol in the client-server computing model. A web browser for example may be the client and an application running on a computer hosting a website may be the server.
The client submits an HTTP request message to the server. The server which provides resources such as HTML files and other contents or performs other functions on behalf of the client, returns a response message to the client.

(5) WWW

The World Wide Web (WWW) is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the internet. It was invented in 1989. He wrote the first web browser program in 1980 while employed at CERN in switzland.
The world wide web has been central to the development of the information Age and is the primary tool billions of people use to interact on the internet.

Friends
Date: Page No.:

⑥ SMTP

Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the users save message in a server mail-box and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix based systems, send mail is the most widely used SMTP server for e-mail. SMTP usually is implemented to operate over internet port 25.