S. No.	Date	Title	Page No.	Teacher's Sign / Remarks

www.ankurgupta.net

Computer NETWORS

* These notes have been prepared from the following book:-

Data Communications and Networking
by Behrouz A Forouzan

Kindly refer above book for more details

Physical Layer

To be transmitted, data must be transformed to electromagnetic signals.

Analog data are continuous, while Digital data have discrete states.

Analog signals can have an infinite number of values in a range, while digital signals can have only a limited number of values.

In data communications, we commonly use periodic analog signals (because they need less bandwidth) and non periodic digital signals (because they can represent variation in data).

Periodic Analog Signals can be classified as simple or composite. A composite analog ~~signal~~ periodic signal is composed of multiple sine waves.

The peak amplitude of a signal is the absolute value of its highest intensity.

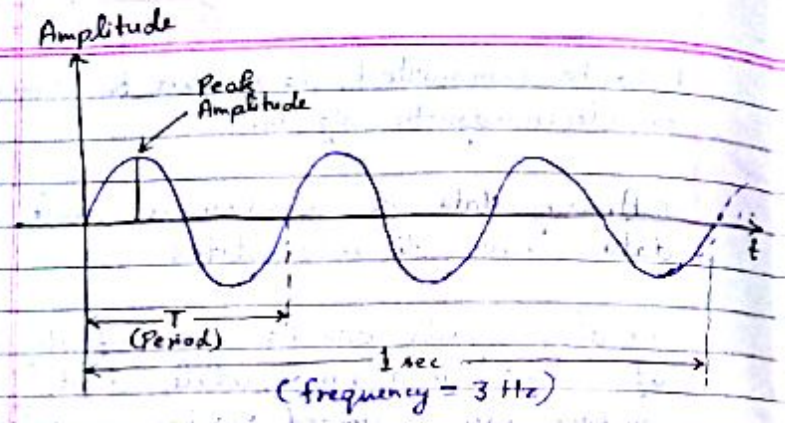
Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.

Frequency refers to the number of periods in 1 sec.

Period → seconds

Frequency → Hz → cycles per second.

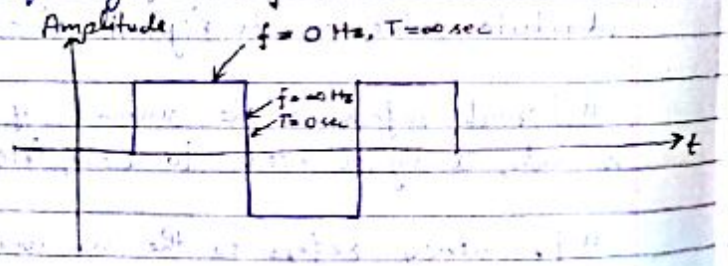
$f = 1/T$



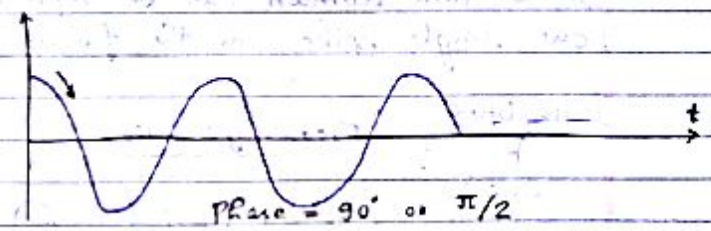
Frequency is the rate of change with respect to time. Change in a short span of time means high frequency. Change over a long span of time means low frequency.

If a signal does not change at all its frequency is zero.

If a signal changes instantaneously, its frequency is infinite.



Phase describes the position of the waveform relative to time 0.



The wavelength is the distance a simple signal can travel in one period.

Wavelength = Propagation Speed × Period

$$\boxed{\lambda = c \cdot T = c/f}$$

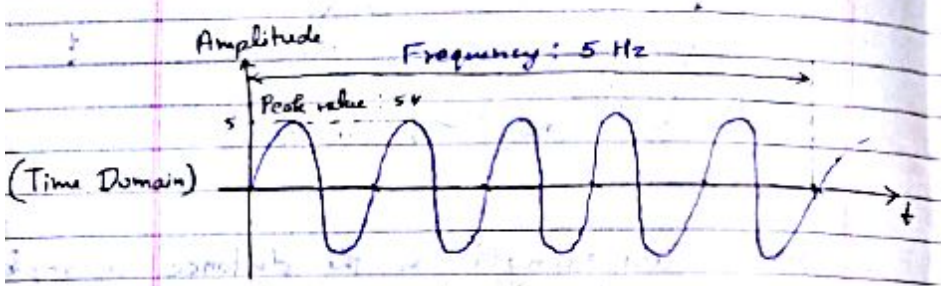
While the frequency of a signal is independent of the medium, the wavelength depends on both the frequency and the medium.

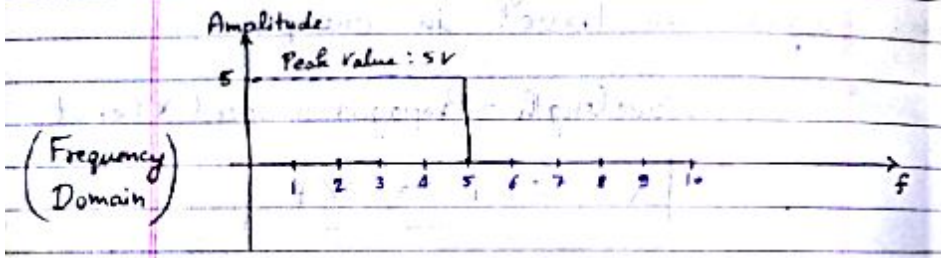
A single-frequency sine wave is not useful in data communications. We need to send a composite signal, a signal made of many simple sine waves.

A normal human being can create a continuous range of frequencies between 0 and 4 kHz.

Time and Frequency Domain :-

A complete sine wave in the time domain can be represented by one single spike in the frequency domain.





Bandwidth :-

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

$$\boxed{B = f_h - f_l}$$

Digital Signals :-

If a signal has L levels, each level needs $\lceil \log_2 L \rceil$ bits.

$$\boxed{\text{No. of bits per level} = \lceil \log_2 L \rceil}$$

→ Most digital signals are non-periodic, and thus period and frequency are not appropriate characteristics for digital signals.

→ Bit Rate (instead of frequency) is used to describe digital signals.

→ Bit Rate is the number of bits sent in 1 sec, expressed in bits per second (bps).

Bit Length :-

The bit length is the distance one bit occupies on the transmission medium.

$$\boxed{\text{Bit length} = \text{Propagation Speed} \times \text{bit duration}}$$

$$\boxed{= \text{Propagation Speed} / \text{Transmission Speed}}$$

A digital signal is a composite analog signal, with infinite bandwidth.

Transmission of Digital Signals :-

(1) Baseband Transmission :-

Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal.

→ Baseband transmission requires that we have a low-pass channel, a channel with a bandwidth that starts from zero.

(2) Broadband Transmission :-

Broadband transmission or modulation means changing the digital signal to an analog signal for transmission.

→ Modulation allows us to use a bandpass channel - a channel with a bandwidth that does not start from zero.

Transmission Impairment :-

(1) Attenuation :-

$dB = 10 \log_{10} \frac{P_2}{P_1}$

Attenuation means a loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium.

→ To compensate for this loss, amplifiers are used to amplify the signal.

(2) Distortion :-

Distortion means that the signal changes its shape.

→ Distortion can occur in a composite signal made of different frequencies because each signal component has its own propagation speed through a medium, and therefore, its own delay in arriving at the final destination.

(3) Noise :-

Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

→ Induced noise comes from sources such as motors and appliances.

→ Crosstalk is the effect of one wire on other.

→ Impulse noise is a spike that comes from power lines.

Signal-to-Noise Ratio (SNR) :-

$$SNR = \frac{\text{Average Signal Power}}{\text{Average Noise Power}}$$

→ A high SNR means, the signal is less corrupted by noise.

→ A low SNR means, the signal is more corrupted by noise

$$SNR_{dB} = 10 \log_{10} SNR$$

Data Rate Limits :-

Data Rate depends on three factors:-

(1) The bandwidth available
(2) The level of signal we use
(3) The quality of channel (the level of noise)

(a) Noiseless Channel :-
(Nyquist Bit Rate)

$$\text{Bit Rate} = 2 \times BW \times \log_2 L$$

Here, BW is the bandwidth of the channel, L is the no. of levels to represent data, and Bit Rate is the bit rate in bits per second.

→ Theortically, if we have given a specific bandwidth, we can have any bit rate we want by increasing the number of signal levels.

→ Increasing the levels of a signal may reduce the reliability of the system.

(b) Noisy Channel :-
(Shannon Capacity)

$$\text{Capacity} = BW \times \log_2 (1 + SNR)$$

Capacity ⇒ Capacity of the channel in bits per second.

→ The shannon's capacity gives us the upper limit. The nyquist formula tells us how many signal levels we need.

Question :- We have a channel with a 1-MHz BW. The SNR for this channel is 63. What are the appropriate bit rate and signal level?

Solution :- Using Shannon formula :-

$$C = B \log_2 (1 + SNR)$$
$$= 10^6 \log_2 (1 + 63) = 10^6 \times 6$$
$$= 6 \text{ Mbps} \Rightarrow \text{Ans}$$

Shannon formula gives us 6 Mbps, the upper limit. For better performance, we choose something lower, 4 Mbps.

Using Nyquist Formula :-

$$4 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 L$$
$$\Rightarrow 2 = \log_2 L \Rightarrow L = 2^2 = 4 \Rightarrow \text{Ans}$$

Performance of a Network :-

(a) Bandwidth :-

In networking, we use the term bandwidth in two contexts :-

(i) Bandwidth in hertz, refers to the range of frequencies in a composite signal.

(ii) Bandwidth in bits per second, refers to the speed of bit transmission in a channel.

→ Basically an increase in bandwidth in Hz means an increase in bandwidth in bps.

(b) Throughput :-

The throughput is a measure of how fast we can actually send data through a network.

$$\boxed{\text{Throughput} < \text{Bandwidth}}$$

→ The bandwidth is a potential measure of a link. The throughput is an actual measurement of how fast we can send data.

www.ankurgupta.net

(c) Latency (Delay) :-

The time taken for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

$$\boxed{\text{Latency} = \text{Propagation time} + \text{transmission time} + \text{queuing time} + \text{processing delay}}$$

(i) Propagation time :-

The time required for a bit to travel from the source to the destination

$$\boxed{\text{Propagation Time} = \frac{\text{Distance}}{\text{Propagation Speed}}}$$

(ii) Transmission Time :-

$$\boxed{\text{Transmission Time} = \frac{\text{Message Size}}{\text{Bandwidth}}}$$

(iii) Queuing Time :-

The time needed for each intermediate or end device to hold the message before it can be processed.

Question:- What are the propagation time and the transmission time for a 5 MB message if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/sec.

Solution:-

$$\text{Propagation Time} = \frac{12{,}000 \times 10^3}{2.4 \times 10^8}$$

$$= 5 \times 10^{-2} \text{ sec}$$

$$= 0.05 \text{ sec.}$$

$$\text{Transmission Time} = \frac{5 \times 10^6 \times 8}{1 \times 10^6}$$

$$= 40 \text{ sec.}$$

Latency = Propagation time + transmission time

$$= 40 + 0.05$$

$$= 40.05 \text{ sec.} \Rightarrow \text{Ans}$$

(d) **Bandwidth-Delay Product:-**

It is the number of bits that can fill the link.

(e) **Jitter:-**

Jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time sensitive (audio and video data).

Signal Element Versus Data Element :-

A data element is the smallest entity that can represent a piece of information: this is the bit.

In data communications, a signal element carries data elements. A signal element is the shortest unit of a digital signal.

→ We define a ratio r, which is the number of data elements carried by each signal element.

Data Rate Versus Signal Rate :-

The data rate defines the number of data elements (bits) sent in 1 sec. The unit is bits per second (bps).

The signal rate is the number of signal elements sent in 1 sec. The unit is the baud.

For digital signal :-

$$S = c \times N \times \frac{1}{r} \text{ baud}$$

For analog signal :-

$$S = N \times \frac{1}{r} \text{ baud}$$

where, S = Signal Rate (baud), c = Case factor,
N = data rate (bps),
r = No. of data elements per signal element

Asynchronous Transmission :-

In Asynchronous Transmission the timing of a signal is not important. Instead, information is received and translated by agreed upon patterns.

→ In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.

Synchronous Transmission :-

In synchronous transmission we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.

→ Synchronous transmission is faster than asynchronous transmission.

Multiplexing :-

→ Multiplexing is the set of techniques that allow the simultaneous transmission of multiple signals across a single data link.

→ There are three basic multiplexing techniques :-
(i) Frequency Division
(ii) Wavelength Division
(iii) Time Division

→ The first two are designed for analog signals, and the third for digital signals.

→ We can divide Time Division Multiplexing into two different schemes :-
(i) Synchronous TDM
(ii) Statistical TDM

→ In Synchronous TDM, each input has a reserved slot in the output frame, even if it is not sending data.

→ In Statistical TDM, slots are dynamically allocated.

Transmission Media :-

Transmission media can be divided into two broad catagories :-
(i) Guided Media
(ii) Unguided Media

→ Guided media include twisted pair cable, coaxial cable, and fiber-optic cable.

→ Unguided medium is free space.

Twisted Pair Cable :-

→ RJ45 connector is used.
→ Used in telephone lines, DSL lines, and LANs.

Coaxial Cable :-

→ Carries signals of higher frequency ranges than those in twisted-pair cable.
→ BNC connector is used.
→ Used in Cable TV, Thin Ethernet, and Thick Ethernet.
→ Attenuation is much higher in coaxial cable than in a Twisted pair cable.
→ Coaxial cable has much higher bandwidth.
→ It requires the frequent use of repeaters

We can divide wireless transmission (Unguided media) into three broad categories :-

(i) Radio Waves, (ii) Micro Waves, (iii) Infrared Waves.

Radio Waves :-

→ Radio Waves have frequencies between 3 kHz and 1 GHz.

→ Radio Waves are omnidirectional.

→ Used for long-distance broadcasting.

→ Can panetrate walls.

→ Have low data rate for digital communication.

Microwaves :-

→ have frequencies between 1 and 300 GHz.

→ Microwaves are unidirectional.

→ Very high frequency microwaves can not penetrate walls.

→ High data rate for digital communication is possible.

→ Used for unicast (one-to-one) communication such as cellular phones, satelite networks and wireless LANs.

Infrared :-

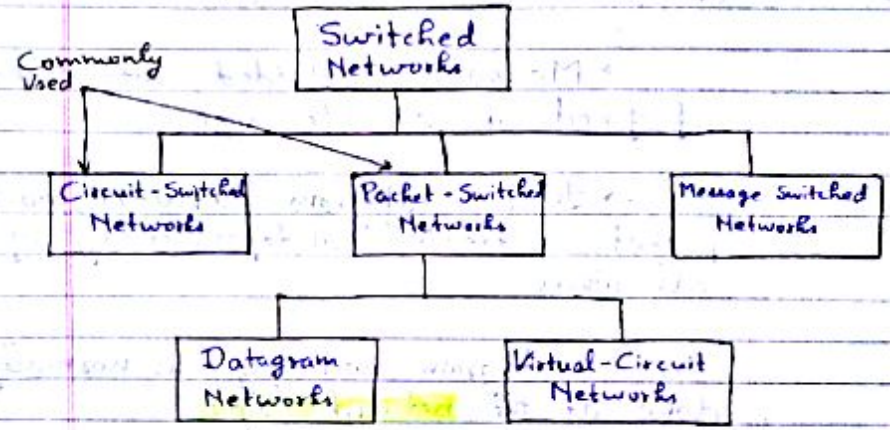
→ have frequencies b/w 300 GHz to 400 THz.

→ Used for short range communication.

→ Can not penetrate walls.

Switching :-

→ A switched network consists of a series of interlinked nodes, called switches.



Circuit-Switched Networks :-

It is made of a set of switches connected by physical links, in which each link is divided into n-channels.

→ Circuit Switching takes place at physical layer.

→ The resources need to be reserved during the setup phase, and remain dedicated for the entire duration of data transfer until the teardown phase.

→ There is no addressing involved during data transfer.

Datagram Networks :-

→ In a packet-switched networks there is no resource reservation; resources are allocated on demand.

→ Message is divided into packets of fixed or variable size.

→ In a datagram network, each packet is treated independently of all others.

→ Datagram switching is normally done at the network layer.

→ The switches in a datagram network are reffered to as routers.

→ Datagram networks are sometimes reffered to as connectionless networks.

Virtual Circuit Networks :-

A virtual-circuit network is a cross between a circuit-switched network and a datagram network

→ All packets follow the same path established during the connection.

→ It is implemented in the data link layer.

www.ankurgupta.net

Network Topologies

Bus Topology :-

→ Single cable connects all computers.

→ Each computer has connector to shared cable

→ Computers must synchronize and allow only one computer to transmit at a time.

→ Cable segment must end with a terminator

→ Uses thin coaxial cable (backbones will be thick coaxial cable)

→ Standard is IEEE 802.3

Advantages :-

(i) Inexpensive to install
(ii) Easy to add stations
(iii) Use less cable than other topologies
(iv) Works well for small networks.

Disadvantages :-

(i) No longer recommended
(ii) Backbone breaks, whole network down.
(iii) Limited no. of devices can be attached.
(iv) Difficult to isolate problems.
(v) Sharing same cable slows response rate.

Star Topology :-

→ Each device has a dedicated point-to-point link to a hub.

→ Easier to maintain.

→ Very flexible and the most preferred topology by Industries.

→ Requires more cable than bus topology.

→ If hub goes down, the whole system is dead.

→ Used in high speed LANs.

→ Twisted Pair Cable is used.

→ The hub can be used in two ways:-
(i) As a repeater, where a frame from one node is retransmitted on all of the outgoing links.
(ii) As a switch, where a frame from one node is retransmitted only on an outgoing link to the destination station.

Ring topology :-

→ Computers connected in a closed loop.

→ Most common type is Token Ring (IEEE 802.5)

→ Single Ring :- Data travels in one direction only.

→ Double Ring :- Allows fault tolerance.

Advantages :-
→ Data packets travel at great speed.
→ No collisions
→ Easier to find faults.
→ No terminators required.

Disadvantages :-
→ A break in the ring will bring it down.
→ Not as common as the bus-less devices available.

Widely used in Wide Area Networks.

Mesh Topology :-

→ Not common on LANs.

→ Most often used in WANs to interconnect LANs.

→ Each node is connected to every other node.

→ It is fault tolerant.

Advantages :-

→ Improves fault tolerance

→ Can carry more data

Disadvantages :-

→ Expensive

→ Difficult to install, manage and troubleshoot

Physical versus Logical Topology :-

→ The actual layout of a network and its media is its Physical Topology.

→ The way in which the data accesses the medium and transmits packets is the Logical Topology.

→ A glance at a network is not always revealing. Cables emerging from a Hub does not make it necessarily a Star Topology - it may actually be a bus or a ring.

Combination of topology and transmission media :-

→ Twisted pair is suitable for use in star and ring topologies.

→ Coaxial Cable is suitable for use in bus topology.

→ Fiber Optics is suitable for use in ring and star topology.

→ Unguided media are suitable for star topology.

ISO/OSI Stack

Protocol Hierarchy :-

→ Most Networks are organized as a series of layers.

→ The task of each layer is to give some services to the upper layer.

→ Any layer maintains a virtual connection with the corresponding layer in a peer.

→ The interface between the layers in the same node is well defined.

→ The implementation of each layer in each node is transparent to other nodes.

→ The protocols between the peer layers can be changed if the peers all agree. However it need not be referred to other layers.

→ The Service definitions tell what the layer does and nothing else.

→ The Interface tells the process above it how to access it. It specifies what the parameters are and what results to expect.

www.ankurgupta.net

List of protocols used by certain system is called protocol stack.

Set of layers and protocols is the Network Architecture.

Architecture :-

→ Architecture is a set of rules and conventions used to build something

→ It does not specify implementation details

Open System Interconnection Reference Model :-
(OSI - ISO)

→ The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions.

→ It was developed by the International Organization for Standardization (ISO)

→ The OSI model is not a protocol.

Responsibility of the host	Application	7
	Presentation	6
	Session	5
	Transport	4
Responsibility of the network	Network	3
	Data-Link	2
	Physical	1

→ The upper layers of the OSI model generally are implemented only in software.

→ The physical layer and the data link layer are implemented in software and hardware.

→ A given layer in the OSI model generally communicates with three other OSI layers :-

(i) The layer directly above it.
(ii) The layer directly below it.
(iii) Its peer layer in other network systems.

→ OSI is a model, not a protocol.

→ The OSI model provides a conceptual framework between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols.

→ A protocol implements the functions of one or more of the OSI layers.

Functions of the OSI Layers :-

(1) Physical Layer :-

Physical layer is concerned with transmission of raw bits over a communication channel.

The physical layer is also concerned with the following :-

(i) Physical characteristics of interfaces and medium :-

Number of pins and functions of each pin of the network connector (Mechanical)

(ii) Representation of bits :-

How 0s and 1s are changed to electrical signals.

(iii) Data Rate and Synchronization of bits :-

Sender and receiver must use the same bit rate and both must have synchronized clocks.

(iv) Establishing and breaking of connection.

(v) Transmission Mode :-

Simplex, half-duplex or full-duplex.

(vi) Physical Topology :- Bus/Star/Ring/Mesh

(2) Data Link Layer :-

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.

It makes the physical layer appear error-free to the upper layer (network layer).

The data link layer is responsible for moving frames from one hop (node) to the next.

Other responsibilities of the data link layer include the following:-

(i) Framing :-

The DLL divides the stream of bits received from the network layer into manageable data units called frames.

(ii) Physical Adressing :-

The DLL adds a header to the frame to define the address of the next hop in the route.

Next hop (node) may be the receiver or some intermediate node.

Communication at the data link layer occurs between two adjacent nodes.

(iii) Flow Control :-

Deals with the data rate mismatch between the sender and the receiver.

(iv) Error Control :-

Uses mechanisms to detect and retransmit damaged or lost frames.

It also uses mechanism for ordering frames and reorganizing duplicate frames.

(v) Access Control :-

Uses protocols like ALOHA and CSMA to control access on a shared medium.

(vi) Synchronization :-

Synchronize and initialize send and receive sequence numbers with its peer at the other end.

(3) Network Layer :-

The network layer is responsible for the source-to-destination delivery of a packet.

→ If two systems are connected to the same link, there is usually no need for a network layer.

→ Thus source-to-destination delivery is performed using two basic approaches known as connection oriented or connectionless network layer services.

Other responsibilities of the network layer include the following :-

(i) Logical Addressing :-

The network layer adds a ~~packet~~ header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

(ii) Routing :-

The routing algorithm is the piece of software that decides where a packet goes next.

→ For connectionless (datagram) networks the routing decision is made for each packet.

→ For connection-oriented (virtual connection) networks, the decision is made once at circuit setup time.

(iii) Dealing with Congestion :-

Congestion occurs in a network when more packets enter an area, than can be processed.

(iv) Dealing with Internetworking :-

→ Packets may travel through many different networks.

→ Each network may have a different frame format.

→ Some networks may be connectionless, other connection-oriented.

Source-to-Destination delivery is also called as ~~End-to-End delivery~~. Host-to-Host delivery.

(4) Transport Layer :-

The transport layer is responsible for process-to-process delivery of the entire message.

The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Some of the services of transport layer are similiar to those provided by data link layer.

Other responsibilities of the transport layer include the following :-

(i) Service Point Addressing :-

The transport layer header includes a type of address called a Service Point Address or Port Address to deliver the entire message to the correct process on the computer

(ii) Segmentation and Reassembly :-

A message is divided into transmittable segments with each segment containing a sequence number, that is used for reassembly the message correctly.

(iii) Connection Control :-

The transport layer can be either connection-less or connection oriented. A connection-less transport layer treats each segment as an independent packet A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.

(iv) Flow Control :-

Flow control at this layer is performed end-to-end.

(v) Error Control :-

Error control at this layer is performed process to process. Error correction is usually achieved through retransmission.

(vi) Negotiation of Quality and Type of Service :-

The user and transport protocol may need to negotiate as to the quality or type of service to be provided.

(vii) Guarantee Service :-

The transport layer may have to overcome service deficiencies of the lower layers (e.g. providing reliable service over an unreliable network layer).

Process-to-Process delivery is also called as end-to-end delivery.

(5) Session Layer :-

This layer allows users on different machines to establish session between them. A session allows ordinary data transport but it also provides enhanced services useful in some applications.

A session may allow a user to log into a remote time-sharing machine or to transfer a file between two machines.

Some of the session related services are :-

(i) Dialogue Control :-

Session can allow traffic to go in both direction ~~in both direction~~ at the same time, or in only one direction at one time.

It also decides who speaks, when and how long.

(ii) Token Management :-

Allows only one side that is holding token to perform the critical operation.

(iii) Synchronization :-

Allows a process to add checkpoints, or synchronization points to a stream of data, so that after a crash, only the data transferred after the last checkpoint have to be repeated.

Session layer establishes, maintains and synchronizes the interaction among communication systems.

(6) Presentation Layer :-

This layer is concerned with Syntax and Semantics of the information transmitted, unlike other layers which are interested in moving data reliably from one machine to other.

Few of the services that presentation layer provides are :-

(i) Translation :-

Encoding data in a standard agreed upon way.

(ii) Encryption and Decryption

(iii) Compression and Decompression.

www.ankurgupta.net

(7) Application Layer :-

The application layer enables the user, to access the network.

Various services provided by application layer are :-

(i) File Transfer (FTP)

(ii) Remote login (telnet)

(iii) Mail (SMTP)

(iv) News (NNTP)

(v) Web (HTTP).

www.ankurgupta.net

Data Link Layer

Specific responsibilities of the data link layer include framing, addressing, flow control, error control, and media access control.

Error Detection and Correction

Types of Errors:-

(i) Single-bit error

(ii) Burst error

The length of the burst is measured from the first corrupted bit to the last corrupted bit.

Redundancy:-

To detect or correct errors, we need to send extra (redundant) bits with data.

Forward Error Correction:-

The receiver tries to guess the message by using redundant bits.

In Backward Error Correction we retransmit the frame

Modulo-2 Arithmetic:-

$0+0=0$, $0+1=1$, $1+0=1$, $1+1=0$

$0-0=0$, $0-1=1$, $1-0=1$, $1-1=0$

Block Coding :-

In block coding, we divide our message into blocks, each of k bits, called datawords. We add r-redundant bits to each block to make the length $n = k + r$. The resulting n-bit blocks are called codewords.

Hamming Distance :-

The hamming distance between two words is the number of differences between corresponding bits.

$d(10101, 11110) = 3$

Minimum Hamming Distance :-

The smallest Hamming distance between all possible pairs in a set of words.

Minimum Distance for Error Detection :-

To guarantee the detection of up to s errors in all cases, the minimum Hamming distance in a block code must be $d_{min} = s + 1$.

Minimum Distance for Error Correction :-

To guarantee correction of upto t errors in all cases, the minimum Hamming distance in a block code must be $d_{min} = 2t + 1$.

Error Detection Techniques :-

(1) Simple Parity Check :-

→ Appends a parity bit to the end of the data.

→ There are two types of parity :- even parity and odd parity.

→ It can detect all single-bit errors.

→ It can also detect burst errors, if the number of bits in error is odd.

(2) Two dimensional parity check :-

→ Organizes the block of bits in the form of a table.

→ Parity check bits are calculated for each row, and after that for all columns.

→ It can detect upto three errors that occur anywhere in the table, however, errors affecting 4 bits may not be detected.

(3) Checksum :-

(a) The sender's end :-

→ The data is divided into k segments each of m-bits.

→ The segments are added using 1's complement to get the sum.

→ The sum is complemented to get the checksum.

→ The checksum segment is sent along with data segment

(b) The receiver's end :-

→ All recieved segments are added using 1's complement arithmetic to get the sum.

→ The sum is complemented.

→ If the result is zero, the recieved data is accepted; otherwise discarded.

Example :-

Sender :-

k = 4, m = 8

(i) → 10110011
(ii) → 10101011
0101111 0
1
0101111 1
(iii) → 01011010
10111001
(iv) → 11010101
10001110
1
Sum :- 10001111
Checksum :- 01110000

Receiver :-

(i) → 10110011
(ii) → 10101011
0101111 0
1
0101111 1
(iii) → 01011010
10111001
(iv) → 11010101
10001110
1
10001111
Checksum :- 01110000
Sum :- 11111111
Complement :- 00000000
Conclusion :- Accept data.

Performance of Checksum:-

→ Detects all errors involving an odd number of bits.

→ Detects most errors involving even number of bits.

(4) Cyclic Redundancy Check (CRC):-

→ One of the most powerful and commonly used error detecting codes.

Basic Approach:-

→ Given a m-bit block of bit sequence, the sender generates an n-bit sequence, known as a Frame Check Sequence (FCS), so that the resulting frame consists of m+n bits.

→ The receiver divides the incoming frame by the number, used for generating FCS. If there is no remainder, the receiver assumes that there is no error.

Generating FCS:-

To generate n-bit FCS, the following steps are followed:-

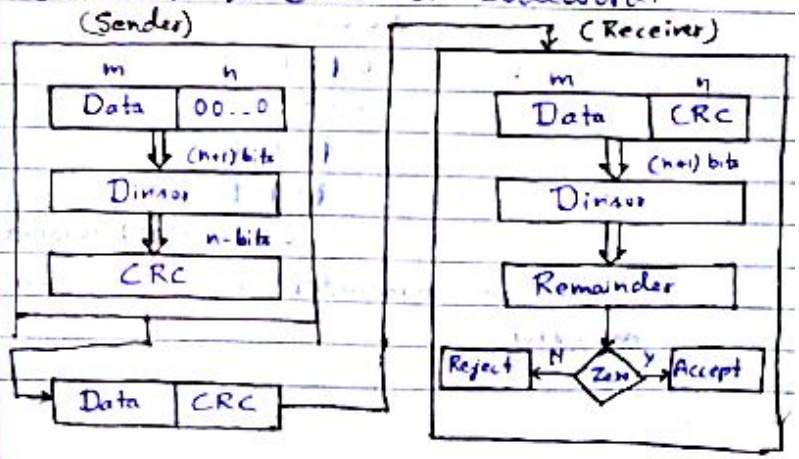
(i) Append n 0s to the right-hand side of the m-bit dataword.

(ii) The (m+n)-bit result is fed into the generator.

(iii) The generator divides the augmented dataword by the divisor (modulo 2 division), of size n+1, that is predefined and agreed upon.

(iv) The n-bit remainder of the division is called the frame check sequence (FCS).

(v) This FCS is appended to the dataword to create a codeword.



Example:- Data :- 1010, Divisor :- 1011

At sender:-

```
        1001  → Quotient
1011 | 1010000
       1011
       00010
        0000
         0100
         0000
          1000
          1011
           011  → Remainder
```

Data to be sent :-

1011011

Data + CRC

At Receiver :-

```
        1001
1011 | 1010011
       1011
       00110
        0000
         0101
         0000
          1011
          1011
           000  → Remainder
```

→ Since remainder is 000, there is no error.

Polynomials :-

→ All the values can be expressed as polynomials of a dummy variable x.

$$P = 11001 \Rightarrow x^4 + x^3 + 1$$

→ CRC process can be expressed as :-

$$\frac{x^n M(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)}$$

n → No. of bits in FCS; $M(x)$ → Message; $P(x)$ → Characteristic Polynomial; $Q(x)$ → Quotient; $R(x)$ → Remainder; $P(x)$ → Characteristic Polynomial

Example:-

Data = 1010 = $x^3 + x$

Divisor = 1011 = $x^3 + x + 1$

$M(x) = x^3(x^3+x) = x^6 + x^4$

At sender:-

$$x^3+x+1 \,\big)\, x^6+x^4 \,\big(\, x^3+1$$
$$x^6+x^4+x^3$$
$$x^3$$
$$x^3+x+1$$
$$x+1 \Rightarrow \text{CRC.}$$

Data to be sent :- $x^6 + x^4 + x + 1$

CRC

At Receiver :-

$$x^3+x+1 \,\big)\, x^6+x^4+x+1 \,\big(\, x^3+1$$
$$x^6+x^4+x^3$$
$$x^2+x+1$$
$$x^2+x+1$$
$$0 \Rightarrow \text{No error.}$$

Performance of CRC :-

→ CRC can detect all single-bit errors.

→ CRC can detect all double-bit errors (provided there are minimum three 1's or terms in the characteristic polynomial P(x))

→ CRC can detect all odd number of errors (P(x) should be divisible by (x+1)).

→ CRC can detect all burst errors of less than the degree of the characteristic polynomial (n).

→ CRC detects most of the larger burst errors with a high probability.

Error Correction Technique :-

Requirement for error detection :-

The minimum Hamming distance between any two codewords should be two.

Requirement for error correction :-

The minimum Hamming distance between any two codeword must be more than two.

Number of additional bits should be such that it can point the position of the bit in error.

If k is the number of additional bits, the condition is :-

$$2^k \geq m + k + 1$$

Number of Data Bits (m)	Number of Redundancy Bits (k)	Total Bits (m+k)
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11
8	4	12

Hamming Code :-

→ To each group of m information bits, k-parity bits are added to form (m+k) bit codeword.

→ Location of each of the (m+k) bits is assigned a decimal value.

→ The k-parity bits are placed in positions $1, 2, 4, \ldots 2^{k-1}$.

→ k parity checks are performed on selected digits of the codeword.

→ At the receiving end, the parity bits are recalculated. The decimal value of k-parity bits provides the bit position in error, if any.

$p_1 \rightarrow 1, 3, 5, 7$

$p_2 \rightarrow 2, 3, 6, 7$

$p_3 \rightarrow 4, 5, 6, 7$

Error Position	Position Number $C_3\ C_2\ C_1$
0 (no error)	0 0 0
1	0 0 1
2	0 1 0
3	0 1 1
4	1 0 0
5	1 0 1
6	1 1 0
7	1 1 1

Example :-

Data ⇒ 1 0 1 1

Hamming Code ⇒

7	6	5	4	3	2	1
d_4	d_3	d_2	p_3	d_1	p_2	p_1

Codeword ⇒ 1 0 1 0 1 0 1

⇓ Sent to Receiver

Received Codeword ⇒ 1 0 $\boxed{0}$ 0 1 0 1

Error.

Calculating parity bits :-

C_3	C_2	C_1	
1	0	1	= 5

Location of error

After error correction → 1 0 $\boxed{1}$ 0 1 0 1

http://users.cis.fiu.edu/~downeyt/cop3402/hamming.html

Flow Control

Flow control is the set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

Various protocols used in flow control are :-

(1) Stop-and-Wait Flow Control :-

→ The simplest form of flow control.

→ The source transmits a data frame.

→ After receiving the frame, the destination indicates its willingness to accept another frame by sending back an ACK frame acknowledging the frame just received.

→ The source must wait until it receives the ACK frame before sending the next data frame.

With the use of multiple frames for a single message, the stop-and-wait protocol does not perform well because only one frame can be in transit at a time.

(2) Sliding Window Flow Control :-

→ In Sliding Window Protocol, we allow multiple frames to be in transit at the same time.

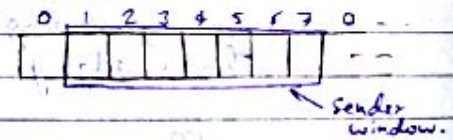
→ To keep track of the frames, sender sends sequentially numbered frames.

→ The sequence numbers range from 0 to $2^k - 1$.

→ Sender maintains a list of sequence numbers that it is allowed to send (sender window).

→ The size of the sender window is at most $2^k - 1$.

For $k = 3$,



→ The receiver also maintains window of size 1

→ The receiver acknowledges a frame by sending an ACK frame that includes the sequence number of next frame expected.

→ This scheme can be used to acknowledge multiple frames.

Piggybacking :-

→ If two station exchange data, each need to maintain two windows. To save communication capacity, a technique called piggybacking is used.

→ When a frame is carrying data from A to B, it can also carry ~~data from~~ control information about arrived (or lost) frames from B and vice-versa.

→ If a station has an ACK but no data to send, it sends a seperate ACK frame.

Performance of Flow Control Protocols :-

(i) Stop and Wait Protocol :-

Utilization, or effiency, of the line is :-

$$U = \frac{t_{transmission}}{2\, t_{propagation} + t_{transmission} + t_{ACK}}$$

Assuming transmission time of ACK to be negligible ($t_{ACK} = 0$) :-

$$\boxed{U = \frac{t_{transmission}}{2\, t_{propagation} + t_{transmission}}}$$

(ii) Sliding Window Protocol :-

$$\boxed{U = \frac{W\,(t_{transmission})}{2\, t_{propagation} + t_{transmission}}}$$

where, W = Window size $(2^k - 1)$

$t_{propagation}$ = Propagation time

$t_{transmission}$ = Transmission time

For maximum utilization, $U = 1$

If $W \times t_{transmission} \geq 2\, t_{propagation} + t_{transmission}$

then $U = 1$

Backward Error Control

During frame transmission, following two types of error may occur :-

(i) Lost Frame :-

A noise burst may damage a frame to such an extent that it is not recognizable at the receiving end.

(ii) Damaged Frame :-

A recognizable frame does arrive, but some of the bits are in error.

Error control in the data link layer is based on automatic repeat request (ARQ), which is the retransmission of data.

Three versions of ARQ are :-

(i) Stop-and-Wait ARQ

(ii) Go-back-N ARQ

(iii) Selective Repeat ARQ

(1) Stop-and-Wait ARQ :-

→ Based on the stop-and-wait flow control technique.

→ The source transmits a single frame and then waits for an ACK.

→ No other data frame can be sent until the ACK arrives at source.

→ A timer is used to take care of lost and damaged frames, and lost ACK.

→ The sender will timeout and resend the same frame, if the ACK is lost.

→ The receiver receives the same frame twice. How to identify duplicate frames?

↳ A modulo-2 numbering scheme is used, where frames are alternately labeled with 0 or 1, and positive acknowledgements are of the form ACK0 or ACK1.

→ The ACK always announces the sequence number of the next frame accepted.

(2) Go-back-N ARQ :-

→ Based on sliding window protocol and most widely used.

Basic Concept :-

→ A station may send a series of frames sequentially up to a maximum number.

→ In case of no error, the destination will acknowledge incoming frames as usual.

→ If the destination detects error in frame, or it received a frame out-of-order (frame lost), it sends a NAK for that frame (using reject or REJ frame).

→ The destination will discard the frame in error and all future frames until the frame in error is correctly received.

→ The source, on receiving a REJ, must retransmit the frame in error plus all succeeding frames.

→ For lost ACK, the sender, after timeout, resends the frames that are still unacknowledged.

→ For k-bit sequence number, the maximum sender window size is limited to $(2^k - 1)$

→ The size of the receiver window is 1.

(3) Selective Repeat ARQ :-

→ In this case, only those frames are retransmitted for which negative ACK has been received (called selective reject SREJ) or time out has occured.

→ Receiver requires storage buffers to contain out-of-order frames until the frame in error is correctly received.

→ The sender and receiver window must be at most one-half of 2^k.

$$\Rightarrow 2^k/2$$

$$= 2^{k-1}$$

Data Link Layer Protocols :-

(1) HDLC
- → High-level Data Link Control
- → Bit oriented protocol.
- → Communication over point-to-point and multipoint links.

(2) Point-to-Point Protocol
- → Point-to-point access.
- → Byte-Oriented Protocol.

www.ankurgupta.net

Ethernet -(IEEE-802.3)

Multiple Access Protocols :-

(i) Pure Aloha :-

A station may transmit a frame at any time. The station then listens for an amount of time equal to the maximum possible round trip propagation delay ($2t_p$). for an acknowledgement.

If the station does not hear an acknowledgement, it resends the frame.

→ The maximum utilization of the channel is only about 18%.

(ii) Slotted Aloha :-

Here the channel is organized into uniform slots whose size equals the frame transmission time.

Transmission is permitted only at a slot boundary.

→ The maximum utilization of the system is about 37%.

Both ALOHA and slotted ALOHA fail to take advantage of one of the key properties of networks which is that propagation delay b/w stations may be very small compared to frame transmission time.

(iii) Carrier Sense Multiple Access (CSMA) Protocol :-

→ It is based on the property that propagation time is very less compared to frame transmission time.

→ When a station sends a packet, other knows about it within a fraction of packet transmission time.

→ With CSMA, a station wishing to transmit first listens to the medium to determine if another transmission is in progress (Listen before talk).

Types of CSMA :-

(a) Nonpersistent CSMA :-

→ If the medium is idle, transmit.

→ If medium is busy, wait random period and then reserve medium.

The use of random delays reduces the probability of collision.

(b) 1-persistent CSMA :-

→ If the medium is idle, transmit.

→ If medium is busy, continue to listen until the channel is sensed idle, then retransmit immediately.

(c) p-persistent CSMA :-

→ If the medium is idle, transmit with probability p, and delay one time unit with probability (1-p).

→ If the medium is busy, continue to listen until the channel is idle.

Limitations of CSMA :-

When two frames collide, the medium remains unusable for the duration of transmission of both damaged frames.

For long frames, compared to propagation time, the amount of wasted capacity can be considerable.

(iv) CSMA/CD (Carrier-Sense-Multiple-Access with Collision Detection) :-

In CSMA/CD, the station listens to the medium while transmitting (Listen while talking).

The steps in CSMA/CD are :-

→ If the medium is idle, transmit.

→ If the medium is busy, continue to listen until the channel is idle, then transmit immediately (1-persistent).

→ If a collision is detected during transmission, transmit a jamming signal to assure that all stations know that there has been a collision and then cease transmission.

→ After transmitting the jamming signal, wait a random amount of time, reffered to as backoff, then attempt to transmit again.

In CSMA/CD, the amount of time to detect a collision is no greater than twice the propagation delay ($2t_p$).

The frames should be long enough to allow collision detection prior to end of transmission.

$$\boxed{\text{Frame transmission time } (t_f) \geq 2t_p}$$

The Binary Exponential Backoff Algorithm :-

→ This algorithm is used to calculate random amount of time (backoff) to wait ~~before an~~ after a collision.

→ In this algorithm, after k^{th} collision, each station waits r-slot times where $0 \leq r < 2^k$.

→ We choose r randomly from the interval 0 to $2^k - 1$.

If k-stations transmit during a contention slot with probability p, the probability A that some station acquires the channel in that slot is :-

$$\boxed{A = kp(1-p)^{k-1}}$$

Manchester encoding requires twice as much bandwidth as straight binary encoding.

$$\boxed{\text{Bit Rate} = \text{Baud Rate}/2}$$

www.ankurgupta.net

Routing Algorithms

Types of Routing Algorithms :-

(1) Non-adaptive / Fixed / Static Routing

(2) Flooding

(3) Random Routing

(4) Flow-based Routing

(5) Adaptive / Dynamic Routing

www.ankurgupta.net

Fixed Routing or Non-adaptive Routing :-

→ A route is selected for each source-destination pair of nodes in the network.

→ The routes are fixed; they may only change if there is a change in the topology of the network.

→ Algorithms used are :-

(i) Dijkstra's Algorithm

(ii) Bellman-Ford Algorithm

Advantages:-

→ Simple

→ Works well in a reliable network with stable load.

→ Same for virtual circuit and Datagram

Disadvantages:-

→ Lack of flexibility

→ Does not react to failure or network congestion.

Flooding:-

→ Requires no network information.

→ Every incoming packet to a node is sent out on every outgoing line except the one it arrived on.

Measures to improve Flooding:-

→ Hop-count :- A hop counter may be contained in the packet header, which is decremented at each hop, with the packet being discarded when the counter becomes zero.

→ Use sequence number to avoid sending them out a second time.

Selective Flooding:-

The routers do not send every incoming packet out on every line, only on those lines that go in approximately in the direction of destination.

Flow-based Routing:-

→ Uses both topology and load information for routing.

→ Flow between a pair of nodes is relatively stable and predictable.

→ For a given line if the capacity and average flow is known, it is possible to compute mean packet delay using queuing theory.

→ From the mean delays of all the lines, it is easy to calculate the flow-weighted average to get the mean delay for the whole subnet.

→ Then the routing algorithm finds the path of minimum average delay.

Adaptive Routing :-

→ Routing decisions change as conditions on the network change.

→ Two principle conditions that change routing decisions are :-

(i) Failure :-
When a node fails.

(ii) Congestion

→ For adaptive routing to be possible, network state information must be exchanged among the nodes.

→ Algorithms used are :-
(i) Distance Vector Routing
(ii) Link-state Routing.

Distance Vector Routing :-

Key characteristics :-
→ Knowledge about the entire network
→ Routing only to neighbours
→ Information sharing at regular interval

→ Each node maintains a routing table having one entry for each node with two other fields; preferred next node and a cost estimate of the distance, based on one of the metrices.

Network Id	Cost	Next Router

This algorithm is also called as the Distributed Bellman-Ford algorithm and the Ford-Fulkerson algorithm.

→ Here each node receives the routing tables from all of its neighbours and updates its own routing table accordingly.

The main issue with Distance Vector Routing algorithm is that it reacts rapidly to good news, but leisurely to bad news (Count-to-infinity problem).

Link-State Routing :-

Basic Steps :→

→ Identify the neighboring nodes.

→ Measure the delay or cost to each of its neighbors.

→ Form a packet containing all the information.

→ Send the packet to all other nodes (flooding).

→ Compute the shortest path to every other node (Dijkstra's Algorithm).

Link-State Versus Distance Vector Routing :-

→ Link state routing converges more quickly.

→ Link state routing requires more CPU power and memory than distance vector routing algorithm.

→ Link-state protocols are generally more scalable than distance vector protocols.

Hierarchial Routing :-

The routers are divided into regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

For huge networks, we usually create multilevel hierarchy.

www.ankurgupta.net

Congestion Control

Common Causes of Congestion :-

→ As packets arrive at a node, they are stored in an input buffer. If packets arrive too fast, an incoming packet may find that there is no available buffer space.

→ Even very large buffer can not prevent congestion, because of delay, timeout and retransmissions.

→ Slow processors may lead to congestion.

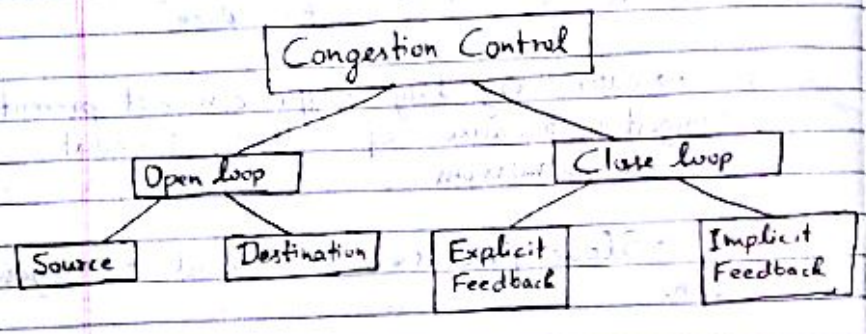
→ Low bandwidth line may also lead to congestion.

Congestion :-

→ When too many packets arrive in a part of the subnet, performance degrades. This situation is called congestion.

Congestion Control :-

Congestion Control refers to the mechanisms and techniques used to control congestion and keep the traffic below the capacity of the network



Open Loop Congestion Control :-

The basic objective is to prevent congestion by adopting suitable policies for :-

- → Flow Control
- → Acknowledgement
- → Retransmission (Timeout interval)
- → Caching
- → Packet discard
- → Routing

Traffic Shaping :-

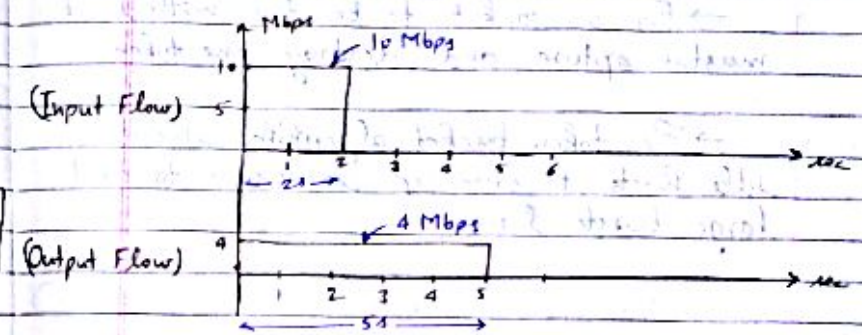
- → Leaky bucket algorithm
- → Token bucket algorithm.

→ Traffic shaping is about regulating the average rate of data transmission.

The Leaky Bucket Algorithm :-

→ It shapes bursty traffic into fixed ~~shape~~ rate traffic.

→ Packets are dropped when the bucket is full.



Limitation :- Enforces rigid output pattern even when the traffic in the network is small.

Token Bucket Algorithm :-

→ In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every ΔT sec.

→ For a packet to be transmitted, it must capture and destroy one token.

→ The token bucket algorithm allows idle hosts to save up permission to send large bursts later.

Close Loop Congestion Control :-

Three basic steps :-

(1) Monitor the system for detection of congestion.

(2) Pass the information to proper place for taking action to control congestion.

(3) Adjust system parameters to get out of congestion.

Congestion Control Versus Flow Control :-

Congestion Control	Flow Control
→ It is a global issue. It is a joint responsibility of the users and the network	→ Flow control is local issue. between a sender-receiver pair.
→ It occurs because of the combined behaviour of the stations, switches, routing etc.	→ Its primary function is to ensure that a fast sender does not overwhelm a slow receiver.
→ Its job is to ensure that the subnet is able to carry the offered load.	

www.ankurgupta.net

Hubs, Switches, Gateways & Routers

Repeaters and Hubs work in Physical Layer.

Bridge works in Data-Link Layer.

Router works in Network Layer.

Gateway works in Application Layer.

Repeaters :-

→ Connects different segments of a LAN.

→ It forwards every frame it receives.

→ It is a regenerator, not an amplifier.

Hub :-

→ Hub is a generic term, but commonly refers to a multiport repeater.

→ It can be used to create multiple levels of hierarchy.

→ Easy to maintain and diagnose.

Bridge :-

→ A bridge operates both in physical and data-link layer.

→ A bridge uses a table for filtering/routing.

→ It does not change the physical (MAC) addresses in a frame.

→ The difference between hub and bridge is that the hub forwards a frame from the input port to all other ports, while bridge forwards the frame only to the destination port.

There are two types of bridges :-

(1) Transparent Bridges

(2) Source Routing Bridges.

(1) Transparent Bridge :-

→ The stations are unaware of the presence of a transparent bridge.

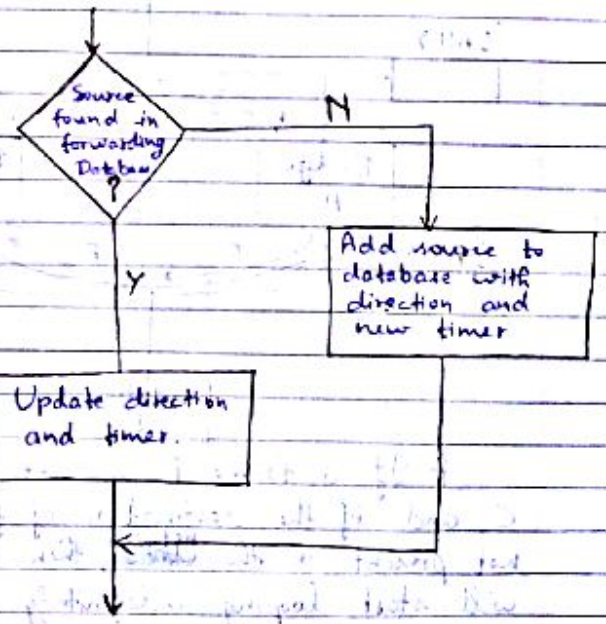
→ Reconfiguration of the bridge is not necessary; it can be added/removed without being noticed.

→ It performs two functions :-

(a) Forwarding of frames.

(b) Learning to create the forwarding table.

Learning in Transparent Bridge :-

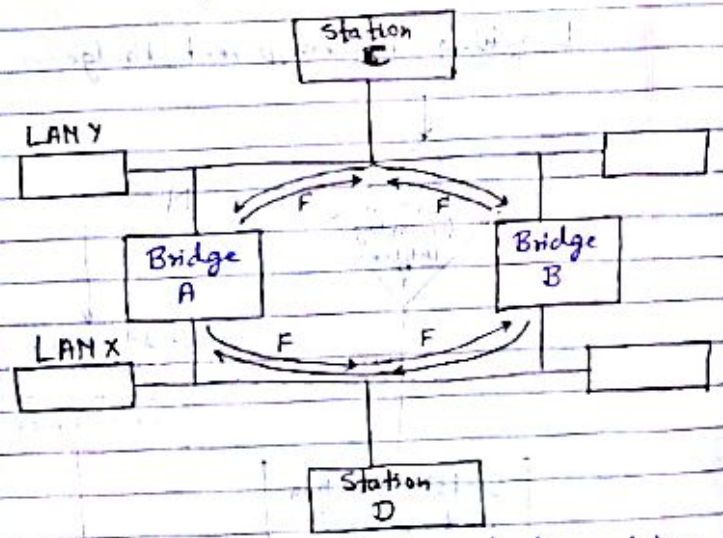


Loop problem in Transparent Bridges :-

→ Forwarding and learning processes work fine as long as there is no redundant bridge in the system.

→ On the other hand redundancy is desirable from the viewpoint of reliability so that the function of a failed bridge is taken over by a redundant bridge.

→ As redundancy creates loop problem in the system, it is very undesirable.



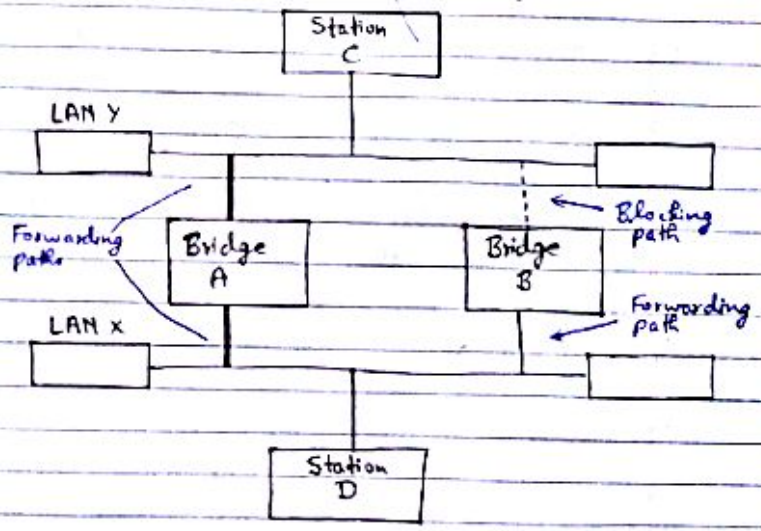
If a frame F is sent from station C, and if the destination of frame F is not present in the ~~station~~ network, then the frame will start looping indefinitely between the bridges in the network.

Solution to Loop Problem :-
(Spanning Tree Topology)

→ To solve the looping problem, the IEEE specification requires that the bridges use a special topology.

→ Such topology is known as spanning tree (a graph where there is no loop) topology.

→ Without changing the physical topology, a logical topology is created that over-lays the physical one.



(2) Source Routing Bridge :-

→ Another way to prevent loops in a system with redundant bridges is to use source routing bridges.

→ Here the source station provides all the routing information about intermediate bridges in the frame.

→ The routing information provides the sequence of bridges, that will be used to forward the frame from source to destination.

Switch :-

→ Switching is a fast bridge.

→ Switch performs the forwarding operation using hardware, while bridges use softwares to forward the frame.

→ Ports are provided with buffer.

→ Each frame is forwarded after examining the # address and forwarded to the proper port #.

Three forwarding approaches :-

(i) Cut-through → No collision or error detection

(ii) Collision-Free → No error detection

(iii) Fully buffered → Both collision and error detection.

Router :-

→ Works in Network layer.

→ It uses IP addresses.

→ A router has four basic components :-
(i) Input Ports, (ii) Output ports,
(iii) Routing Processor, (iv) Switching Fabric

→ Input Port performs physical and data-link layer functions of the router.

→ Output Port performs the same functions as the input port, but in reverse order.

→ The routing processor performs the function of the network layer. The process involves the table lookup.

→ The switching fabric moves the packet from the Input Queue to the output queue by using specialized mechanisms.

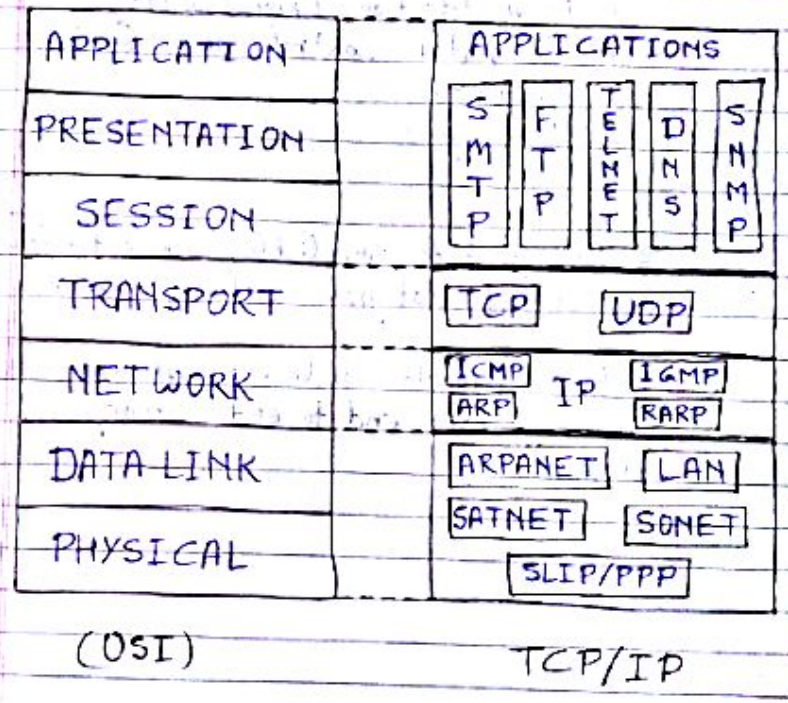
www.ankurgupta.net

TCP / IP

TCP/IP :-

Acts as a glue to link different types of LAN and WAN to provide Internet, a single integrated network for seamless communication.

TCP/IP and OSI Model :-



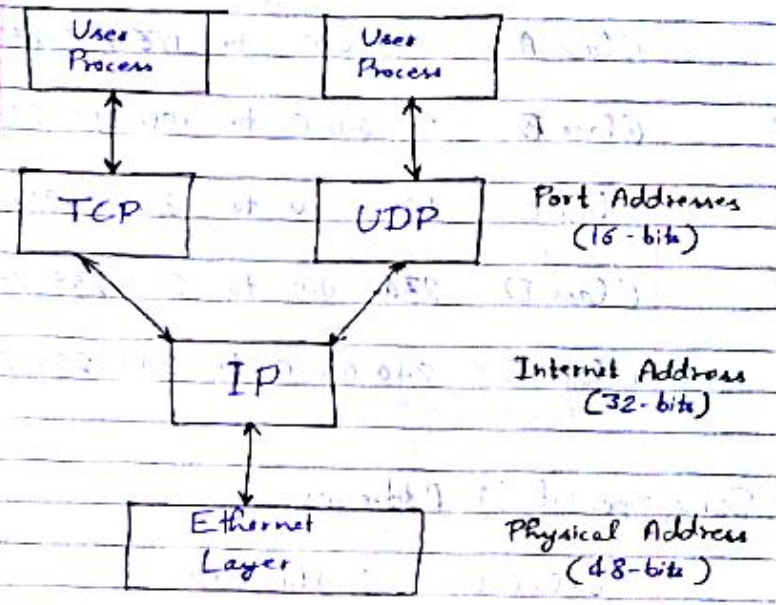
Internetworking Issues :-

(1) Addressing
(2) Packetizing
(3) Fragmentation and Re-assembly
(4) Routing
(5) Flow Control
(6) Error detection / Error Control
(7) Congestion Control and QoS
(8) Security
(9) Naming.

IP provides unreliable, connectionless best-effort datagram delivery service.

TCP provides reliable, efficient and cost-effective end-to-end delivery of data.

Addresses in TCP/IP :-



Classful Addressing :-

Class A	0 Net Id	Host Id		
Class B	10 Net Id	Host Id		
Class C	110 Net	Id	Host Id	
Class D	1110 Multicast Address			
Class E	1111 Provide for future.			
	8-bits	8-bits	8-bits	8-bits

The concept of Net Id and Host Id does not apply to classes D and E.

Dotted Decimal Notation :-

Class-A	1.0.0.0	to	127.255.255.255
Class-B	128.0.0.0	to	191.255.255.255
Class C	192.0.0.0	to	223.255.255.255
Class D	224.0.0.0	to	239.255.255.255
Class E	240.0.0.0	to	254.255.255.255

Some Special IP Addresses :-

0.0.0.0 ⇒ This host

255.255.255.255 ⇒ Broadcast on this network (when net-id is unknown)

00 - - - 00	host id

⇒ A host on this network.

netid	111 - - - - 111

⇒ Broadcast on a distant N/W

127.x.y.z ⇒ Loop-back

Masking :-

A mask is a 32-bit number made of contiguous 1s followed by contiguous 0s.

The mask helps to find the netid and the hostid.

Default masks for classful addressing :-

Class	Binary	Dotted-Decimal
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Example :-

144.16.5.210 (IP-Address) → | MASK: 255.255.0.0 | → 144.16.0.0 (Network Address)

www.ankurgupta.net

Subnetting :-

A subnet is a logically visible subdivision of an IP Network.

The practice of dividing a network into subnetworks is called subnetting.

→ Subnetting increases the number of 1s in the mask.

Classless Addressing :-

In this scheme, there are no classes, but the addresses are still granted in blocks.

Restrictions on classless address blocks :-

(i) The addresses in a block must be contiguous.

(ii) The number of addresses in a block must be power of 2 (1, 2, 4, --)

(iii) The first address must be evenly divisible by the number of addresses.

Mask :-

A block of addresses can be defined as :-

$$x.y.z.t \ /n$$

in which x.y.z.t defines one of the addresses and the /n defines the mask.

First address :-

Set the rightmost (32−n) bits to 0s.

Last address :-

Set the rightmost (32−n) bits to 1s.

Number of Addresses :-

$$2^{(32-n)}$$

Example :- Calculate first address, last address and no. of Addresses for 205.16.37.39/28.

Solution :- $n = 28$, $(32-n) = 4$

$(39)_{10} = (00100\underline{111})_2$

First Address ⇒

$(00100\underline{0000})_2 = (32)_{10}$

⇒ 205.16.37.32 Ans

Last Address ⇒

$(00100\underline{1111})_2 = (47)_{10}$

⇒ 205.16.37.47 Ans

No. of Addresses :

⇒ $2^4 = 16$ Ans

Network Address:-

The first address in a block is normally not assigned to any device; it is used as the network address that represents the organization to the rest of the world.

Hierarchy:-

(1) Two-level Hierarchy : No Subnetting :-

The n left-most bits of the address x.y.z.t/n defines the network; the (32-n) rightmost bits define the particular host.

(2) Three-levels of Hierarchy : Subnetting :-

Here the rest of the world sees the organization as one entity; however, internally there are several subnets.

All messages are sent to the router address that connects the organization to the rest of the Internet, the router routes the message to the appropriate subnets.

(3) More level of hierarchy :-

There can be any number of hierarchical levels in classless addressing

Example of three level of hierarchy :-

Q:- An organization is given the block 17.12.40.0/26, which contains 64 addresses. The organization has three offices and needs to divide the addresses into three sub-blocks of 32, 16, and 16 addresses.

Solution:-

(1) Suppose the mask for the first subnet is n_1, then

$$2^{32-n_1} = 32 \Rightarrow n_1 = 27$$

(2) Suppose the mask for the second subnet is n_2, then:-

$$2^{32-n_2} = 16 \Rightarrow n_2 = 28$$

(3) Similiarly for third subnet :-

$$n_2 = 28$$

This means we have the masks 27, 28, 28 with the organization mask being 26.

Address range for subnet 1 :-

17.12.14.0 to 17.12.14.31 /27

Address range for subnet 2 :-

17.12.14.32 to 17.12.14.47 /28

Address range for subnet 3 :-

17.12.14.48 to 17.12.14.63 /28

Private Subnets :-

(1) 10.0.0.0 /8

or

10.0.0.0 to 10.255.255.255

(2) 172.16.0.0 /12

or

172.16.0.0 to 172.31.255.255

(3) 192.168.0.0 /16

or

192.168.0.0 to 192.168.255.255

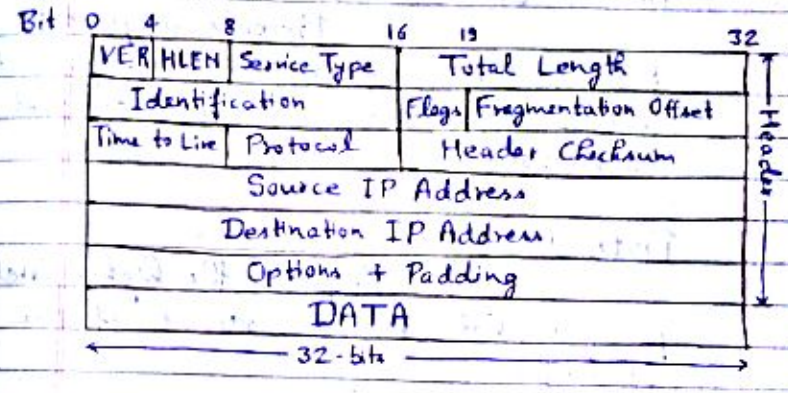
www.ankurgupta.net

Internet Protocol (IP) :-

Communication at the network layer in the internet is connectionless.

Packets in IPv4 layer are called datagrams.

IPv4 datagram :-



A brief description of each field is given below :-

VER (4 bits) :- Version of the IP protocol in use

HLEN (4 bits) :- Length of the header, expressed as the number of 32-bit words. Minimum size is 5, and maximum 15.

Total Length (16 bits) :- Length in bytes of the datagram (including header). Maximum datagram size is $(2^{16}-1)$ or 65535 bytes.

Service Type (8-bits):-
Allows packet to be assigned a priority.

Identification, Flags, Fragment Offset:-
Used for handling fragmentation.

Time to Live (8-bits):-
Prevents a packet from travelling forever in a loop. Sender sets a value, that is decremented at each router.

Protocol (8 bits):-
Defines the higher level protocol that uses the service of the IP layer.

Options (Variable Width):-
Can be used to provide more functionalities to the IP datagram.

Header Checksum (16 bits):-
Covers only the header of the IP datagram.

~~If Fragment offset is multiple of~~ Fragments must be multiple of 8-octets.

ARP:-

→ ARP is used for finding a physical address for a known IP address
→ An ARP request is broadcast to all stations in the network.
→ An ARP reply is unicast to the host requesting the mapping.

RARP, BOOTP, DHCP:-

→ All of these are used to find the IP address for a known physical address.
→ The issue with RARP is that, broadcasting is done at the data link layer.

→ BOOTP is an application layer protocol. The issue with BOOTP is that it is not dynamic configuration protocol.

→ DHCP provides static and dynamic address allocation.

ICMP :-

→ IP has no error-control mechanism.

→ IP also lacks mechanism for host and management queries.

→ Internet Control Message Protocol (ICMP) has been designed to compensate for the above deficiencies.

→ ICMP messages are divided into two broad categories :-

(i) Error-reporting messages.

(ii) Query messages.

→ ping and traceroute commands are part of ICMP.

IGMP :-

→ Internet Group Management Protocol (IGMP) is used for multicasting.

ICMP and IGMP are companion protocols of IP.

User Datagram Protocol (UDP) :-

UDP is a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.

→ The multiplexing and demultiplexing operation are performed using the port mechanism.

→ UDP messages can be lost, duplicate delayed and can be delivered out-of-order.

UDP Datagram Format :-

Bit 0	16	32
Source Port	Destination Port	
Total Length	Checksum	← Options

Total Length (16-bits) :-

The 16-bits can define a total length of 0 to 65,535 bytes.

Actual UDP Length = IP Length − IP Header's Length

UDP is suitable transport protocol for multicasting.

Transmission Control Protocol (TCP) :-

→ TCP provides a connection-oriented, full duplex, reliable, streamed delivery service using IP to transport messages between two processes.

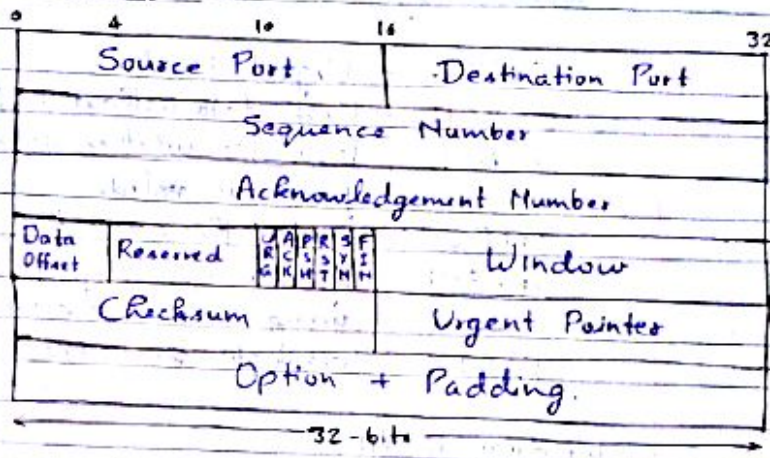
→ Reliablity is ensured by :-

(i) Connection-Oriented service.
(ii) Flow control using sliding window protocol.
(iii) Error detection using checksum
(iv) Error Control using Go-Back-N ARQ technique
(v) Congestion Avoidance Algorithm :-
→ Multiplicative decrease
→ Slow-start.

→ Other functionalities implemented by TCP are :-

(i) Recovery from packet losses
(ii) Detection of duplicate packets
(iii) Packet delivery in correct order

TCP Frame :-



TCP Header Fields :-

Sequence Number (32-bits) :-
It defines the number assigned to the first byte of data contained in this segment. TCP assigns a sequence number to each byte.

Acknowledgement Number (32-bits) :-
It defines the byte number that the receiver of the segment is expecting to receive from the other party.

HLEN (Data-Offset) [4-bits] :-
It specifies the number of 32-bit words present in TCP header.

Control Flag Bits (6-bits):-

(i) URG - Urgent Pointer
(ii) PSH - Push data without buffering.
(iii) ACK - Indicates whether acknowledge field is valid.
(iv) RST - Reset the connection
(v) SYN - Synchronize sequence numbers during connection establishment.
(vi) FIN - Terminate the connection.

Window (16-bits):-

Specifies the size of window

Checksum (16-bits):-

Used for error detection.

Urgent Pointer (16-bits):-

Used only when URG flag is valid.

Options:-

Optional 40-bytes of information

Broadcasting and multicasting are not applicable to TCP.

Important Points related to TCP/IP:-

The unit of information passed by TCP to IP is called a segment.

In IP, there is also an option of source routing, in which the source specifies a list of IP addresses that must be traversed by the datagram.

In TCP, for connection establishment, a three way handshake is used.

In TCP, for connection termination, a four way handshaking protocol is necessary for termination of connection in both directions.

www.ankurgupta.net

Congestion Control in TCP :-

There are three algorithms :-

(i) Slow start : Exponential Increase :-

In the slow-start algorithm, the size of the congestion window increases exponentially until it reaches a threshold.

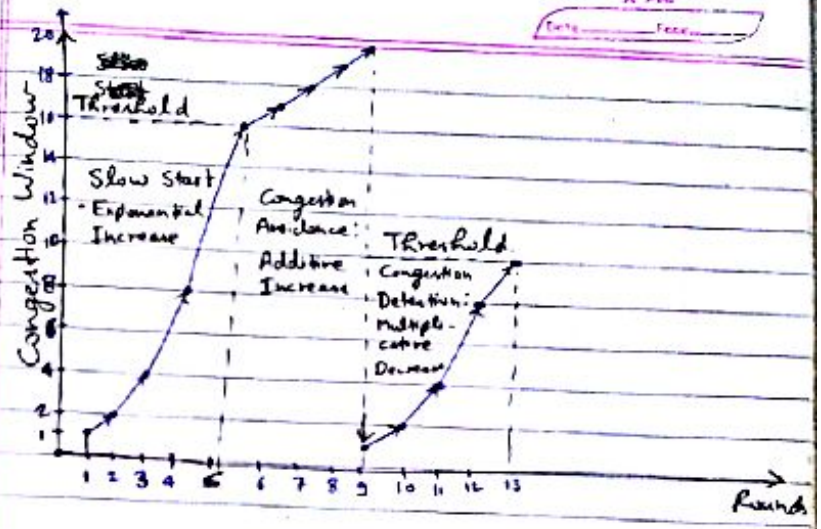
(ii) Congestion Avoidance : Additive Increase :-

After reaching the threshold (in previous algo), the size of the congestion window starts increasing additively until congestion is detected to avoid congestion.

(iii) Congestion Detection : Multiplicative Decrease :-

If congestion occurs in previous algo, the congestion window size must be decreased.

The size of the threshold is dropped to one half : a multplicative decrease.



Socket Address :-

→ The combination of IP address and the port number is called a socket address.

Application Layer

TELNET :-

→ TELNET ⇒ TErminaL NETwork

→ General purpose client-server application program for remote log-in.

→ Communication takes place using NVT (Network Virtual Terminal) character set.

→ Telnet uses only one TCP connection.

→ The server uses the well-known port 23 and the client uses an ephemeral port.

→ To distinguish data from control characters, each sequence of control characters is preceded by a special control character called Interpret as Control (IAC)

→ NVT uses two sets of characters, both 8-bit bytes :-

(i) for Data (highest-order bit is 0)
(ii) for Control (highest-order bit is 1).

www.ankurgupta.net

MIME (Multipurpose Internet Mail Extension) :-

It is a supplementary protocol that allows non-ascii data to be sent through e-mail.

MIME defines 5 headers :-

(i) MIME - Version - Current is 1.1
(ii) Content - Type - Content_Type/Content_Subtype
(iii) Content - Transfer - Encoding
(iv) Content - Id
(v) Content - Description

The email system, we use today is based on ARPANET

SMTP (Simple Mail Transfer Protocol) :-

→ SMTP simply defines how commands and responses must be sent back and forth.

→ Uses Port - 25 of destination machine.

→ Commands are sent from the client to the server.

→ It defines 14 - commands :-

(i) HELO - Sender's host name.
(ii) MAIL FROM - Sender of the message.
(iii) RCPT TO - Intended receipent of message.
(iv) DATA - Body of the mail.

→ Responses are sent from the server to the client. It is a 3-digit code.

→ The process of transferring a mail message occurs in three phases :-

(i) Connection Establishment
(ii) Mail Transfer
(iii) Connection Termination

POP3 (Post Office Protocol, version-3) :-

→ The client POP3 S/W is installed on the receipent computer; the server POP3 S/W is installed on the mail server.

→ Uses TCP port 110 on the server.

→ Two modes of the operation :-
(a) Delete Mode
(b) Keep Mode.

IMAP4 (Internet Mail Access Protocol version-4) :-

→ Uses TCP port 143.

→ IMAP4 provides the following extra functions :-
(i) Checking email header prior to downloading.
(ii) Searching in the contents of the e-mail prior to downloading.
(iii) Partially download e-mail.
(iv) Create, delete, or rename mailboxes on the mail server.
(v) Creating a hierarchy of mailboxes in a folder for email storage.

FTP (File Transfer Protocol) :-

→ Uses TCP/IP.

→ Establishes two connections b/w the hosts :-
(i) For Data transfer (Port 20)
(ii) For Control Information (Port 21).

→ The control connection uses very simple rules of communication, while the data connection uses more complex rules due to the variety of data types transferred.

→ The control connection remains connected during the entire FTP session.

→ The data connection is opened and then closed for each file transferred.

Communication over Control Connection :-

→ FTP uses the same approach as SMTP to communicate across the control connection.

→ It uses the 7-bit Ascii character set.

POP3 (Post Office Protocol, version-3) :-

→ The client POP3 S/W is installed on the receipent computer; the server POP3 S/W is installed on the mail server.

→ Uses TCP port 110 on the server.

→ Two modes of the operation :-
(a) Delete Mode
(b) Keep Mode.

IMAP4 (Internet Mail Access Protocol version 4) :-

→ Uses TCP port 143.

→ IMAP4 provides the following extra functions :-
(i) Checking email header prior to downloading.
(ii) Searching in the contents of the e-mail prior to downloading.
(iii) Partially download e-mail.
(iv) Create, delete, or rename mailboxes on the mail server.
(v) Creating a hierarchy of mailboxes, in a folder for email storage.

FTP (File Transfer Protocol) :-

→ Uses TCP/IP.

→ Establishes two connections b/w the hosts :-
(i) For Data transfer (Port 20)
(ii) For Control Information (Port 21).

→ The control connection uses very simple rules of communication, while the data connection uses more complex rules due to the variety of data types transferred.

→ The control connection remains connected during the entire FTP session.

→ The data connection is opened and then closed for each file transferred.

Communication over Control Connection :-

→ FTP uses the same approach as SMTP to communicate across the control connection.

→ It uses the 7-bit Ascii character set.

Communication over Data Connection :-

→ RETR command is used to retrieve a file from a server to the client.

→ STOR command is used to store a file from client to the server.

→ LIST command is used to show the content of a directory.

HTTP Protocol :-

→ It is a stateless protocol.

→ HTTP methods are case-sensitive, i.e. GET is a legal method but get is not.

→ HTTP 1.1 supports persistence connection. It is also possible to pipeline requests, i.e. sending request-2 before the response to request-1 has arrived.

→ HTTP supports proxy servers. A proxy server is a computer that keeps copies of responses to recent requests.

DNS Lookup :-

(i) Reverse DNS Lookup :-
Determination of Domain Name from IP-address.

(ii) Forward DNS Lookup :-
Determination of IP address from domain-name.

www.ankurgupta.net

Network Security

Public Key Cryptography :-

→ The public key used for encryption is different from the private key used for decryption

RSA :-

Inventors :- Rivest, Shamir, and Aldeman.

→ Based on number theory.

→ The private key is a pair of numbers (d, n) and the public key is also a pair of numbers (e, n).

Steps :-

(i) Choose two large primes p and q.

(ii) Compute :-

$$n = p \times q \quad \& \quad z = (p-1) \times (q-1)$$

(iii) Choose a number d, relatively prime to z.

(iv) Find e, such that :-

$$(e \cdot d) \bmod z = 1$$

(v) For encryption :-

$$C = P^e \pmod n$$

(vi) For decryption :-

$$P = C^d \pmod n.$$

Diffie-Hellman Key Exchange Algorithm:-

Given:- (i) Prime Number - $p = 7$
(ii) Base - $g = 7$

~~Alice chooses a secret integer a = 2, then sends~~
~~Bob $A = g^a \bmod p$~~

Deffie-Hellman Key Exchange Algorithm:-

Given:- (i) Prime Number - p
(ii) Base - g

Alice has a secret integer a
Bob has a secret integer b

Secret Key $= g^{ab} \bmod p$

Example:- Modulus $= 7$, Primitive Root $= 3$
$a = 2$, $b = 5$

Key $= 3^{(2\times5)} \bmod 7$
$= 4$

Base = Primitive Root = g
Prime No = Modulus = p

www.ankurgupta.net