Computer Networks

Published By:

Physics Wallah

ISBN: 978-93-94342-39-2

Mobile App: Physics Wallah (Available on Play Store)

Website: www.pw.live

Email: support@pw.live

Rights

Disclaimer

A team of PW experts and faculties with an understanding of the subject has worked hard for the books.

While the author and publisher have used their best efforts in preparing these books. The content has been checked for accuracy. As the book is intended for educational purposes, the author shall not be responsible for any errors contained in the book.

The publication is designed to provide accurate and authoritative information with regard to the subject matter covered.

(This Module shall only be Used for Educational Purpose.)

Computer Networks

INDEX

1 IP ADDRESSING, SUBNETTING & SUPERNETTING

1.1 IP Addressing

Class A : 0 → (1 - 126), No. of IP Addresses = 2^{31}
Class B : 10 → (128 - 191), No. of IP Addresses = 2^{30}
Class C : 110 → (192 - 223), No. of IP Addresses = 2^{29}
Class D : 1110 → (224 - 239), No. of IP Addresses = 2^{28}
Class E : 1111 → (240 - 255), No. of IP Addresses = 2^{28}

1.2 Default subnet Mask

Class A : 255.0.0.0
Class B : 255.255.0.0
Class C : 255.255.255.0

1.3 Private Addresses Range

10.0.0.0 to 10.255.255.255 → 1 class A Network.
172.16.0.0 to 172.31.255.255 → 16 class B Network.
192.168.0.0 to 192.168.255.255 → 256 class C Network.

Class	Number of Networks	Number of hosts per Network
Class A	$2^7 - 2 = 126$	$2^{24} - 2 = 1,67,77,214$ hosts
Class B	$2^{14} = 16,384$	$2^{16} - 2 = 65,534$ hosts
Class C	$2^{21} = 20,97,125$	$2^8 - 2 = 254$ hosts
Class D	No NID and HID, all 28 remaining bits are used to define multicast address	
Class E	No NID and HID, it is meant for research and future purpose	

Note:
The IP address 127.x.y.z is known as loop back address and it is used to check the connectivity.

1.4 Types of Communication

(i) Unicast communication (1 : 1)

(ii) Broadcast communication (1 : All)

(iii) Multicast Communication (1: Many)

1.5 Unicast Communication

1. Transmitting the data from one computer to another computer is called as unicast communication.
2. It is one to one transmission.
3. In Unicast communication both source and destination either present in the same network or in the different network.

1.6 Broadcast Communication

1.6.1 Limited Broadcasting

1. Transmitting data from one computer to all other computer in the same network is called as Limited Broadcasting.
2. Limited Broadcast Address = 255.255.255.255
3. Limited broadcast address can't be used as a source IP Address.
4. Limited broadcast Address will always be used as a Destination IP.

1.6.2 Direct Broadcasting

1. Transmitting data from one computer to all other computer in the different network is called as Limited Broadcasting.
2. Direct broadcast address can't be used as a source IP Address.
3. Direct broadcast Address will always be used as a Destination IP.

	NID	**HID**		
1.	–	0's	→	Network ID
2.	–	1's	→	Direct Broadcast Address (DBA)
3.	1's	1's	→	Limited Broadcast Address (LBA)
4.	0's	–	→	Host with in the Network
5.	1's	0's	→	Network Mask or Subnet Mask

1.7 Multicast communication

Transmitting a packet from one computer to many computers (0 or more) is called Multicast communication.

1.8 CIDR Rules

1. All the IP Address in the Block must be contiguous.
2. Block size must be a power of 2.
3. First IP address of the block must be divisible by size of the block.

1.9 Supernetting

The process of combining two or more network to get a single network is called as supernetting.

1.10 Advantage of Supernetting

1. Super netting Reduce Routing table entry.
2. Router will take less time for processing the packet.
3. It improve flexibility of IP Address Allotment i.e. If someone required 500 Address, then no need to purchase class B network we can combine two class C network.

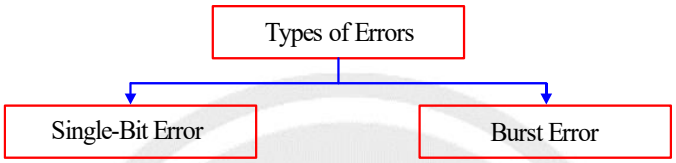
1.11 Rules of Supernetting

1. Network ID must be contiguous.
2. Size of the Network must be same and number of Network must be a power of 2.
3. First Network ID must be divisible by size of the supernet.

❑❑❑

2 ERROR CONTROL

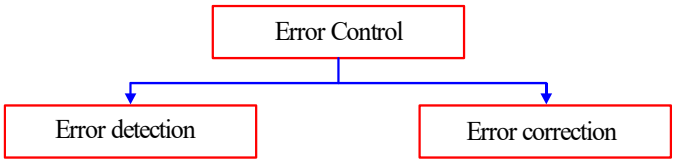
2.1 Error Control



Note:

- The number of corrupted bits or affected bits depends on the data rate and duration of noise.
- The number of corrupted bits or affected bits =Data rate * Noise duration.
- Burst error is more likely to occur than a single bit error.
- Error correction is more difficult than error detection.

	Error Detection	Error Correction
1.	Once noticed error simply discard.	Capability of correcting error.
2.	Ask for retransmission.	Does not required retransmission.



1.	Simple Parity	1.	Hamming code
2.	2D parity		
3.	Check sum		
4.	CRC		

2.1.1 Hamming distance

Hamming distance between two Binary string of same size is the number of differences between corresponding bits.
Hamming distance between two Binary string is denoted by d(x, y)

$$d(000, 011) = 2$$

d(100, 011)=3
d(10101, 11110)=3

Hamming distance can easily be found if we apply XOR operation (⊕) on the two words and count the Number of 1's in the result.

2.1.2 Minimum Hamming distance

In a set of codewords, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of code words.

Valid code word					
0	1	0	(a)	d (a, b) = 3	Minimum Hamming distance = 1
1	0	1	(b)	d (a, c) = 1	
1	1	0	(c)	d (a, d) = 2	
0	0	1	(d)	d (b, c) = 2	
				d (b, d) = 1	
				d (c, d) = 3	

2.1.3 Minimum Hamming distance for Error detection

To detect 'd' bit error minimum hamming distance required =d+1

2.1.4 Min. Hamming distance For Error Correction

To Correct 'd' bit error minimum hamming distance required =2d+1

2.2 Simple Parity Check Code

Simple parity

In the Simple parity concept one extra bit (parity bit) is added to each dataword.
Simple parity check can detect all single bit error .
Simple parity check can not detect an even number of errors.
Simple parity check can detect an odd number of errors .

2.3 2D Parity Check Code

2D parity

Two dimensional parity check can detect and correct all single bit error and detect two or three bit error that occur any where in the matrix.
However only some pattern with four or more Errors can be detected.
In a 2D-parity check code, the information bits are organized in a matrix consisting of rows and columns.
For each row and each column one parity check bits is calculated.

2.4 CRC

Length of the dataword = n
Length of the divisor = k
Append (k-1) Zero's to the original message
Perform modulo 2 division
Remainder of division = CRC
Codeword = dataword with Appended (k-1) Zero's + CRC

Note:

1. CRC must be (k-1) bits.
2. If the generator has more than one term and coefficient of x^0 is 1, all single bit error can be detected.
3. If a generator can't divide $x^t + 1$ (t between 0 and n – 1) then all isolated Double error can be detected.
4. The generator that contains a Factor of x + 1 can detect all odd numbered errors.

2.4.1 A good polynomial generator needs to have the following characteristics

1. It should have at least two terms.
2. The coefficient of the term x^0 should be 1.
3. It should not divide $x^t + 1$, for t between 2 and n – 1.
4. It should have the factor x + 1.

2.5 Hamming Code

1. Hamming code is used for error correction.
2. Hamming code can correct 1 bit error only.
3. Hamming code can detect upto 2 bit error.
   m = Massege bits
   r = redundant bits or Check bits or parity bits or extra bits
   n = m + r (n = codeword)

According to the hamming code, number of redundant bits

$$\boxed{m + r + 1 \leq 2^r}$$

where r = lower limit

❑❑❑

3 FLOW CONTROL

3.1 Delay in Computer Network

(1) Transmission Delay (T_d)
(2) Propagation Delay (P_d)
(3) Queuing Delay (Q_d)
(4) Processing Delay (P_{rd})

3.2 Transmission Delay

Amount of time taken to transfer a packet on to the outgoing link is called as Transmission delay.

$$\text{Transmission delay}\,(T_d) = \frac{\text{Length of packet}}{\text{Bandwidth}}$$

$$T_d = \frac{L}{B}$$

3.3 Propagation Delay

Amount of time taken to reach a packet from one (sender) point to another (receiver) point is called as propagation delay.

$$\text{Propagation delay}\,(P_d) = \frac{\text{distance}}{\text{velocity}}$$

$$P_d = \frac{d}{v}$$

3.4 Stop wait Protocol

3.4.1 Sender Side Rule

Rule 1 : Sender can send one data packet at a time.
Rule 2 : Sender can send the next data packet only after receiving the ACK of the previous packet.

3.4.2 Receiver Side Rule

Rule 1: Receiver will receive and consume the data packet.
Rule 2 : After consuming the data packet, Ack need to be sent.

3.5 Efficiency OR Line utilization OR Link utilization OR Sender utilization

$$\text{Efficiency} = \frac{\text{Useful time}}{\text{Total time}}$$

$$\text{Efficiency} = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2*P_d + Q_d + P_{rd} + T_d(\text{ACK})}$$

3.6 Throughput Or Effective Bandwidth Or Bandwidth Utilization Or Maximum Data Rate Possible

$$\text{Throughput} = \frac{\text{Length of the Frame}}{\text{Total time}}$$

$$\boxed{\text{Throughput} = \frac{L}{T_d(\text{frame}) + 2*P_d + Q_d + P_{rd} + T_d(\text{ACK})}} \quad \text{OR} \quad \boxed{\text{Throughput} = \eta * B}$$

3.7 Sliding Window

In the sliding window concept instead of sending one packet and wait for the acknowledgement, we send 'w' packet and wait for the Acknowledgement. Where 'w' is the sender window size.

3.7.1 GB–N(N>1)

1. In the GB – N the sender window size is N itself.
2. In the GB-N the receiver window size is equal to one always.

Note:

(1) Out of order packet is not received by Receiver.

(2) Timer is maintained only for the first frame (Rightmost) in window because if its timer expires then sender assume that rest of the frame are also not received by receiver (because out of order delivery is rejected).

Note:

GB–N uses cumulative Acknowledgement and Acknowledgement number defines the number of the next expected frame.

Ack timer < Time out timer

Window Receiver (W_R) size:

In the GB-N the window receiver size is equal to one always irrespective of window sender size (Wr=1).

Window Sender (W_S) Size:

Window sender size is calculated based on the following formula:

$Ws + W_R \leq$ Available Sequence Number

$Ws + 1 \leq$ Available Sequence Number

$Ws \leq$ Available Sequence Number – 1

3.7.2 Efficiency and Throughput in GBN

$$\text{Efficiency} = \frac{\text{Useful time}}{\text{Total time}}$$

$$\boxed{\text{Efficiency} = \frac{N*T_d(frame)}{T_d(frame)+2*P_d+Q_d+P_{rd}+T_d(ACk)}}$$

$$\text{Throughput} = \frac{N*\text{Length of Frame}}{\text{Total time}}$$

$$\boxed{\text{Throughput} = \frac{N*\text{Length of Frame}}{T_d(frame)+2*P_d+Q_d+P_{rd}+T_d(ACk)}} \quad \text{OR} \quad \boxed{\text{Throughput} = \eta * B}$$

3.8 Selective Repeat ARQ

3.8.1 Selective Repeat/Selective Reject ARQ

(1) In SR Protocol window sender size is equal to window receiver size ($W_S = W_R$).

(2) SR Protocol uses independent acknowledgement, and acknowledgement number defines number of error free packet received.

(3) SR receiver can receive out of order packet but packets are delivered to upper layer in sorted order.

(4) In SR protocol searching and sorting logic is required. Searching is done by sender and sorting is done by receiver.

(5) Timer is maintained for each and every frame in the window at sender side.

(6) For 1st out of order delivery or if packet received is corrupted then Negative acknowledgment (NACK) for respective packet is sent by receiver to sender.

(7) When sender receive NACK 3 then it will search in the window for packet 3 & immediately packet 3 is retransmitted even though its timer is not expired.

3.8.2 Efficiency and Throughput of SR

$$\text{Efficiency} = \frac{\text{Useful time}}{\text{Total time}}$$

$$\boxed{\text{Efficiency} = \frac{Ws \times T_d(frame)}{T_d(frame)+2*P_d+Q_d+P_{rd}+T_d(ACK)}}$$

$$\boxed{\text{Throughput} = \eta * B}$$

$$\text{Throughput} = \frac{W_s * \text{Length of the frame}}{\text{Total time}}$$

$$\boxed{\text{Throughput} = \frac{W_s * \text{Length of the frame}}{T_d(frame)+2*P_d+Q_d+P_{rd}+T_d(ACK)}}$$

3.9 Comparison among Stop and Wait, GBN and SR protocols

	Stop & wait	GBN	SR
Efficiency	$\eta = \frac{\text{Useful time}}{\text{Total time}}$ or $\eta = \frac{T_d(frame)}{\text{Total time}}$	$\eta = \frac{\text{Useful time}}{\text{Total time}}$ or $\eta = \frac{N*T_d(frame)}{\text{Total time}}$	$\eta = \frac{\text{Useful time}}{\text{Total time}}$ or $\eta = \frac{W_s*T_d(frame)}{\text{Total time}}$
Throughput	$\frac{\text{Length of frame}}{\text{Total time}}$ or $\eta * B$	$\frac{N*\text{Length of the frame}}{\text{Total time}}$ or $\eta * B$	$\frac{W_s*\text{Length of the frame}}{\text{Total time}}$ or $\eta * B$
Buffer	1 + 1	N + 1	N + N
Seq No.	2	N + 1	2N
Seq. No. = K bit		$W_S = 2^K - 1$ $W_R = 1$	$W_S = 2^{K-1}$ $W_R = 2^{K-1}$

$$\boxed{\text{RTT or Total Time} = T_d(frame)+ 2*P_d + T_d(ACK)+ P_{rd} + Q_d}$$

❑❑❑

4 IPv4 HEADER

4.1 IPv4 Header

VER (4 bits)	HL (4 bits)	Services (8 bits)	Total Length (16 bits)
Identification number (16 bits)		Flags (3 bits)	Fragment offset (13 bits)
Time to Live (8 bits)		Protocol (8 bits)	Header checksum (16 bits)
Source IP Address (32 bits)			
Destination IP Address (32 bits)			
Option (0-40 bytes)			

4.1.1 Version (4 Bit)

It is used to indicate IPv4 or IPv6.

4.1.2 Header Length(4 Bit)

Header length is a 4 bit field that contains the length of header.

Minimum Header size is 20 byte.

Maximum Header size is 60 byte.

4.2 Services [8 bit]

In this Interpretation the first 3 bit are called precedence bit (Priority bit) and Next 4 bit are called types of services bits and last bit is Not used.

4.2.1 Priority

It is a 3-bit subfield ranging from 0 to 7 (000 to 111 in binary). Priority field is needed if a router is congested and need to discard some datagram, those datagrams which have the lowest priority are discarded first.

4.2.2 Types of Services

It is a 4 bit subfield. Each bit having a special meaning, although a bit can be 0 or 1. One and only one of the bits can have the value 1 in each datagram.

4.3 Total length (16 bits)

Total length = Data + Header

4.4 Identification Number (16 bits)

1. Each datagram is associated with a sequence number is called as datagram number or identification number.
2. It is used to identify all the fragment of same datagram.
3. All the fragment of same datagram will have the same identification number.

4.5 Flags

It is the 3 bit field shown in the figure.

X	D F	M F
Not Used	Don't Fragment	More Fragment

4.6 Fragment offset (13 bits)

Fragment offset indicate no of data byte ahead of this fragment in that particular packet.

4.7 TTL (8 bits)

1. TTL is used to avoid infinite looping.
2. TTL field is used to control the maximum number of hops visited by datagram.
3. When a source host sends a datagram, it stores a number in this field. Each router that process the datagram decrements this number by one. If TTL field reaches zero before the datagram arrives at its destination, then the datagram is discarded and an ICMP message is sent back to sender.

4.8 Protocol (8 bits)

1. This 8 bits field tell us which protocol is encapsulated in the IP packet.
2. At the time of traffic, some packet must be discarded. In this case it will be advantageous to know which protocol data it contains.
3. The order in which router eliminate the datagram from buffer is-
   ICMP>IGMP>UDP>TCP
   (01) (02) (17) (06)

4.9 Header Checksum

1. It is calculated only for header part not the data because rest of the component in packet already covered by TCP checksum.
2. Header checksum is calculated at each and every Router because IP Header might be change when packet is moving from one router to another.
3. Every router makes one modification i.e. TTL so Header checksum is calculated at every Router.
4. Fragment offset, MF, Total length, option all may be changed at a Router.

4.10 Source Address (32 bits)

This 32 bit defines the IPv4 address of source. This field remain unchanged during the time the IPv4 datagram travel from the source Host to destination Host.

4.11 Destination Address (32 bits)

This 32 bits Field defines the IPv4 address of the destination. This field remain unchanged during the time the IPv4 datagram travel from source host to destination host.

4.12 Option

The Header of IPv4 data gram is made of two parts a fixed part and a variable part. The fixed part is 20 bytes long and variable part that can be maximum of 40 bytes.

There are 5 options

1. Strict source Routing
2. Loose source Routing
3. Record Routing
4. Time stamp
5. Padding

4.12.1 Strict Source Routing

A strict source routing is used by the source to predetermine a route for data gram as it travel through the internet.

4.12.2 Loose Source Routing

A loose source route option is similar to strict source route but it is less rigid. Each router in the list must visited, but the data gram can visit other router as well.

4.12.3 Record Routing

A record route option is used to record the internet routers that handle the data gram. It can list up to 9 router Address.
All the Router are supposed to record their IP Address on their IP packets.

Note:
First 16 bits (2 byte) are reserved for option type (8 bit) and length (8 bit). Out of 40 bytes only 38 bytes are remaining for storing IPv4 addresses. In 38 bytes we can store 9 IPv4 addresses as each IPv4 address is of 4 byte

4.12.4 Time Stamp

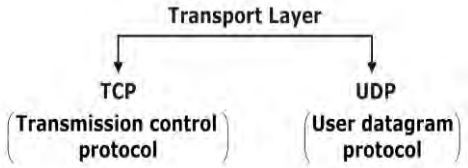
It is used to find out delays at each router. Every router should record incoming time and outgoing time.

❑❑❑

5 TCP & UDP

5.1 Introduction

Transport Layer can be connection oriented or connection less.



1. TCP is reliable process to process delivery of entire message.
2. TCP is a connection oriented.
3. TCP connection are full duplex and point to point.
4. TCP connection has 3 phases
   i. Connection establishment
   ii. Data transfer
   iii. Connection termination
5. Each TCP connection is identified uniquely by Source Port + Destination Port + Source IP + Destination IP.
6. Each TCP connection is associated with Four window.
7. TCP uses three way “Handshake” to establish TCP connection.
8. TCP is not useful for Broadcasting and Multicasting.
9. TCP Header size is 20 bytes but if option (40 bytes) is added it will become 60 bytes.
10. TCP provide end to end error control and flow control.
11. Data will be received at the destination in order.
12. Data may arrive out of order and be temporarily stored by receiving TCP, but TCP guarantee that no out of order data delivered to the process.

5.2 TCP header

<table>
<tr><td colspan="8">Source Port (16 bits)</td><td>Destination Port (16 bits)</td></tr>
<tr><td colspan="9">Sequence number (32 bits)</td></tr>
<tr><td colspan="9">Acknowledgement number (32 bits)</td></tr>
<tr><td>Header Length (4 bits)</td><td>Reserved bits (6 bits)</td><td>URB</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Window Size (Advertisement Window) (16 bits)</td></tr>
<tr><td colspan="8">Check sum (16 bits)</td><td>Urgent Pointer (16 bits)</td></tr>
<tr><td colspan="9">Options
(0 - 40 bytes)</td></tr>
</table>

Port Number	Name
0 – 1023	Well known port No.
1024 – 49151	Registered Port No.
49152 – 65535	Dynamic Port No.

$$\text{Wrap Around time (WAT)} = \frac{\text{Total sequence No.}}{\text{Bandwidth}\left[\text{Bytes / Sec}\right]}$$

- Minimum sequence number required to Avoid wrap Around time with in Life time = B × LT
- Minimum number of bits required to Avoid wrap Around time with in LT = $\lceil \log_2 B * LT \rceil$

SYN = 1 → Consume one sequence number.

Ack = 1 → Consume zero sequence number.

FIN = 1 → Consume one sequence number.

1 Data byte → Consume one sequence number.

SYN	Ack	Meaning
1	0	request
1	1	reply
0	1	Ack
0	0	Data

Time out timer in TCP

Basic Algorithm	Jacobson's Algorithm
Time Out Timer = 2 * RTT Next Round Trip Time (NRTT) = α(IRTT) + (1 – α)ARTT $0 \le \alpha \le 1$	Time Out Timer = 4 * ID + RTT Next Round Trip Time (NRTT) = α (IRTT) + (1 – α) ARTT $0 \le \alpha \le 1$ Actual Deviation (AD) = |IRTT – ARTT| Next Deviation (ND) =α (ID) + (1 – α) AD

5.3 Congestion Control

1. $W_s = \min (Wc, W_R)$

Slow start	Congestion Avoidance	Congestion Detection
1. If ACK Arrives $W_c = W_c + 1$	1. IF ACK Arrives $W_c = W_c + \frac{1}{W_c}$	1. Time out
2. After one RTT $W_c = 2 * W_C$	2. After one RTT $W_c = W_c + 1$	2. 3 duplicate ACK

5.4 Token Bucket

- Token bucket algorithm allows ideal hosts to accumulate credit for the future in the form of tokens.
- In regular interval, tokens are thrown into the bucket.
- Bucket has a maximum capacity.
- If there is a ready packet a token is removed from bucket and packet is sent.
- If there is no token in the bucket, the packet cannot be sent.

Let the capacity of token bucket is 'C' token and token enter into the bucket at rate of 'r' tokens per second.
The maximum number of packet that can be enter into the network during the time interval 't' is

Maximum number of packet = $C + rt$

Maximum average rate for token bucket $M = \frac{C + rt}{t}$

$$Mt = C + rt$$
$$Mt - rt = C$$
$$(M - r)t = C$$
$$t = \frac{C}{M - r}$$

C → token Bucket capacity
r → Token Arrival rate

5.5 UDP

1. UDP is message oriented connection less Datagram protocol.
2. It is unreliable Transport protocol.
3. It does not provide Flow control and Error control & congestion control.
4. It does not add anything to the services except process to process delivery of data.
5. Header is simple and fixed in size i.e. 8 byte.

UDP Header

Source port (16 bit)	Destination port (16 bit)
Length (16 bit)	Checksum (16 bit)

Note:
Unlike TCP, the checksum calculation is not mandatory in UDP. No error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

5.5.1 Optional inclusion of checksum

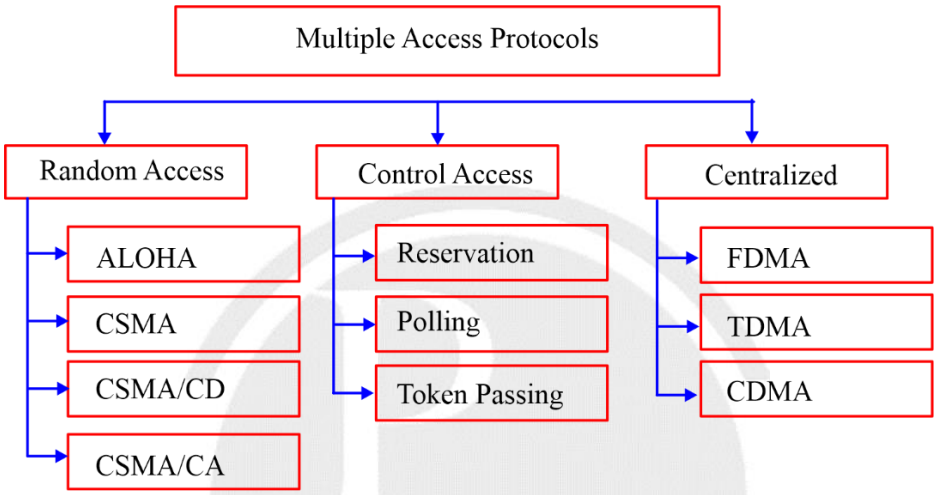
The sender of UDP packet can choose not to calculate the checksum. In this case the checksum field is filled with all 0's before being sent.

5.5.2 Need of UDP

[1] The application that required one request one reply. TCP is not suitable hence we use UDP.
[2] Application that required constant dataflow TCP is not suitable hence we use UDP.
[3] Application that required multimedia data transfer we cannot use TCP hence we use UDP.
[4] Application that required fastness and then reliability TCP is not suitable hence we use UDP.
[5] UDP used for management process such as SNMP (simple network management protocol).
[6] UDP is used for some route updating protocol such as RIP.
[7] For broadcasting & multicasting application TCP is no suitable hence we use UDP.
[8] UDP is normally used for interactive real time applications.
[9] UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer protocol(TFTP) process include flow and error control. It can easily use UDP

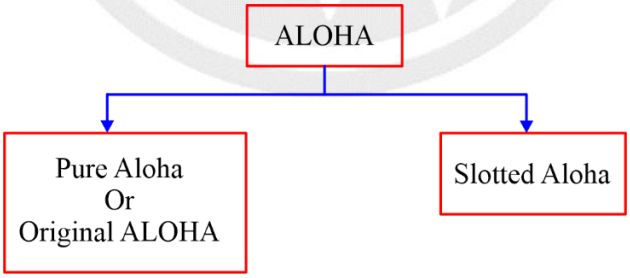
TCP	UDP
Connection-oriented	Connectionless
Reliability in delivery of message	Not reliable
Sequence Number.	No sequence number.
ACK number.	No ACK number.
Overhead is high(Header size 20-60 Bytes)	overhead is less(Header size = 8 Bytes)
Keep track of order (sequence)	No order
Protocols: HTTP, FTP, SMTP, POP	Protocol: DNS, SNMP, TFTP, DHCP, All real time protocol

6 MEDIUM ACESS CONTROL[MAC]



6.1 Aloha

Aloha was developed at university of Hawaii in 1970's.
It was designed for wireless LAN but it can be used in any shared medium.
Each station sends equal size frame.



Pure Aloha	Slotted Aloha
Any station transmits the data at any time.	Any station can transmit the data at the beginning of any time slot.
Vulnerable time in which collision may occur = 2 * T_f (T_f - Transmission time for single frame)	Vulnerable time in which collision may occur = T_f
Throughput of pure aloha = $G * e^{-2G}$	Throughput of slotted Aloha = $G * e^{-G}$
Maximum throughput s_{max} = 18.4 % (When G = 1/2)	Maximum throughput s_{max} = 36.8 % (When G = 1)
The main advantage of pure aloha is it simplicity in implementation	The main advantage of slotted aloha is that it reduces the number of collisions to Half and double the throughput of pure aloha

6.2 CSMA (Carrier Sense multiple access)

CSMA requires that each station, first sense the carrier before transmitting the data.
Vulnerable time for CSMA = Propagation time.

6.3 Persistence methods in CSSMA

Persistent
Non-persistent
P-persistent

6.4 CSMA/CD (Carrier Sense multiple access/Collision Detection)

1. Minimum size of frame to detect the collision in Ethernet (CSMA/CD)
   $T_d \geq 2 * P_d + T_d$(Jam signal)
2. Backoff Algorithm
   Waiting time = K * Slot duration
   = K * RTT
   = K * 2 * P_d

   K is any random number in between 0 to $2^n - 1$.
   n is collision number (Collision number is respect to data packet).

3. Efficiency in Ethernet (CSMA/CD)

$$\eta = \frac{1}{1 + 6.44a} \quad \text{or} \quad \eta = \frac{\text{useful time}}{\text{Total time}} = \frac{T_d}{\text{Collision time} + T_d + P_d}$$

4. $P(1-P)^{N-1}$ → Probability of success for single station(Throughput of Host)

$NP(1 - P)^{N-1}$ → Probability of success for any station among all stations [Throughput of channel]

5. Ethernet Frame Structure:

Preamble	SFD	DA	SA	Length Of Data	Data	CRC
7B	1B	6B	6B	2B	(46B – 1500B)	4B

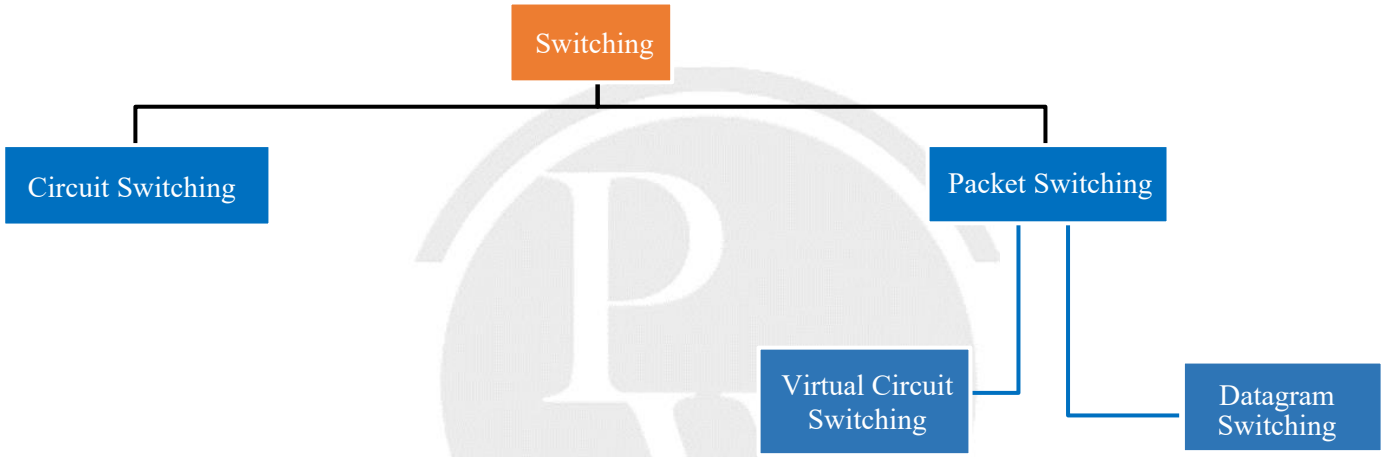
PL DLL DLL

Ethernet uses Manchester encoding technique for converting data bits into signal.
(Baud rate = 2 ∗ bit rate)
Bit rate = 1/2 baud rate

❑❑❑

7 ROUTING ALGORITHMS, SWITCHING & IP SUPPORT PROTOCOL

7.1 Switching



Circuit Switching	Packet switching
(I) It has three phases-connection establishment, Data transfer and Connection termination.	It has only one phase-Data transfer
(2) Physical path between source and destination	No physical path
(3) All packets use same path	Packet may follow different path (travel independently)
(4) Reserves the entire bandwidth in advance	Does not reserve
(5) Bandwidth wastage	No Bandwidth wastage
(6) No store and forward transmission	Supports store and forward transmission
(7) Congestion can happen during connection establishment phase	Congestion can happen during data transfer phase

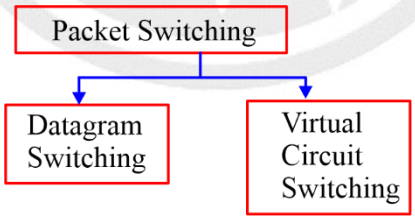
(8) It is reliable	Not reliable
(9) Better for sending large messages	Better for sending small messages
(10) Not fault tolerant technique	Fault tolerant technique
(11) Circuit switching is implemented at physical layer.	Packet switching is implemented at network layer
Total time= Setup time + T_d + P_d + Tear down time $TT=S+\frac{L}{B}+X.\frac{d}{V}+T$	For X Hop and N packet Total time= $X[T_d + P_d] + X-1[P_{rd} + Q_d] + N-1(T_d)$

7.2 Generalized Formula for optimal packet size(P)

M = Message size
h = Header size
p = Payload/Packet data size
No. of Hops = X

$p = \sqrt{\frac{Mh}{X-1}}$

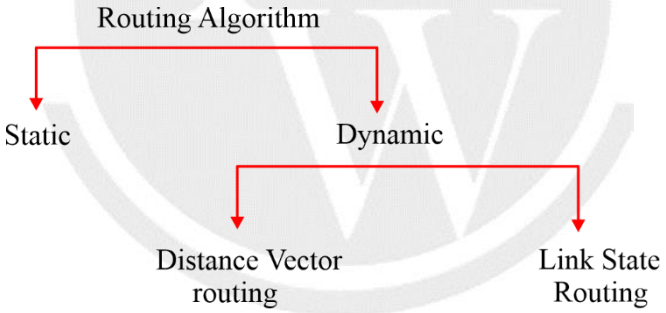
So optimum packet size P = p + h



Datagram Switching	Virtual circuit switching
(1) It is a connection less service.	It is connection-oriented service.
(2) All the packets may follow different path.	All the packet follows the same dedicated path.
(3) Data may appear out of order at the destination since the packets may follow different paths.	Data appears in order at the destination since all the packets take the same dedicated path.
(4) It is not reliable since packets may be discarded.	It is highly reliable.

(5) Cheap	Costly
(6) No resource reservation is done.	First packet reserves the resources (CPU, bandwidth and buffer) for the subsequent packets.
(7) All the packets require a global header which contains full information about the destination.	Only first packet requires a global header which identifies the path from one end to another end. All the following packets require a local header which identifies the path from hop to hop.
(8) The packets may be discarded at intermediate switches if sufficient resources are not available to process the packets.	The packets are never discarded at intermediate switches and immediately forwarded since resources are reserved for them.
(9) IP Networks uses datagram switching.	ATM (Asynchronous Transfer Mode) uses virtual circuit switching.
(10) Datagram switching is normally implemented at network layer.	Virtual circuit switching is normally implemented at data link layer.

7.3 Routing Algorithm



Distance vector Routing	Link state Routing
1. 1980's	1. 1990's
2. Bandwidth required is very less because we sent only distance vector packet.	2. Band width required is high because we sent entire link state packet
3. Local knowledge	3. Global knowledge
4. Bellman Ford algorithm	4. Dijkstra algorithm
5. Traffic is very less	5. Traffic is very high

6. Convergence is very low	6. Convergence is faster
7. Count to infinity Problem	7. No problem of count to infinity
8. Persistent Loops	8. Transient Loops
9. RIP	9. OSPF

The maximum Hop count allowed For RIP is 15 and Hop count of 16 is considered as Destination unreachable.

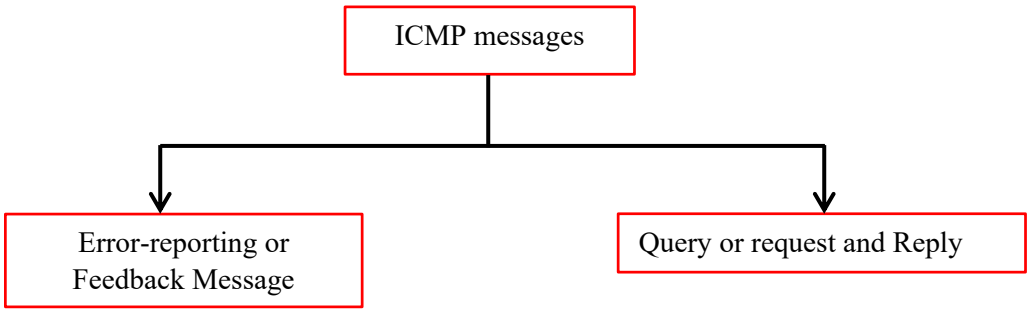
Note:
RIP uses UDP as its transport protocol with the port number – 530

7.4 IP Support Protocol

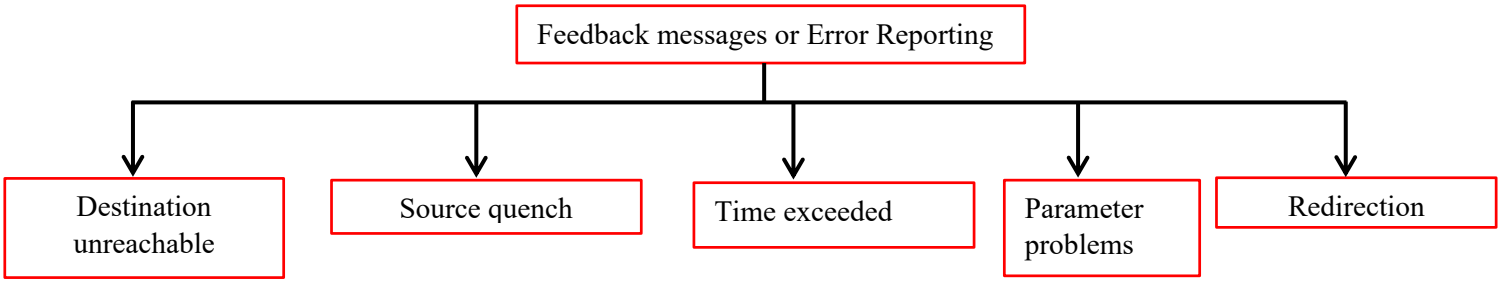
7.4.1 ARP

1. Address Resolution Protocol(ARP) is used to find the MAC(Media Access Control) address of a device from its IP address.
2. **ARP request:** ARP request is broadcasting
3. **ARP response/reply:** ARP reply is unicasting.

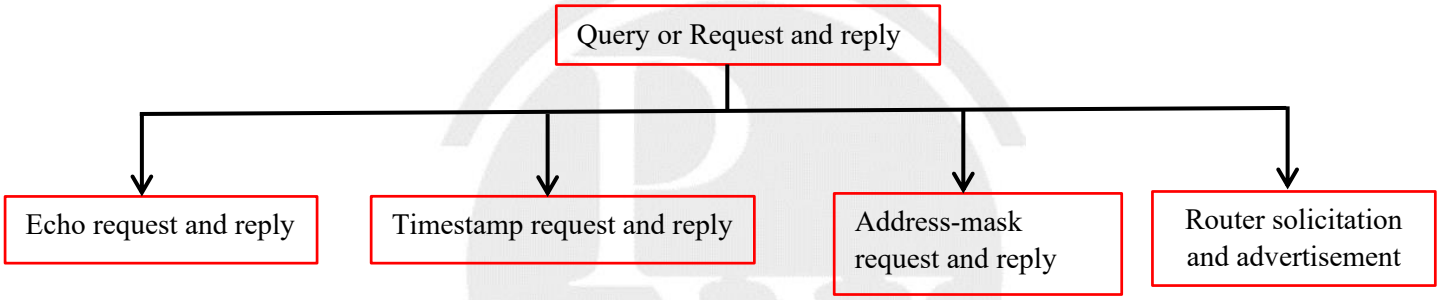
7.4.2 Internet Control Message Protocol (ICMP)



7.4.3 Internet Control Message Protocol (ICMP)



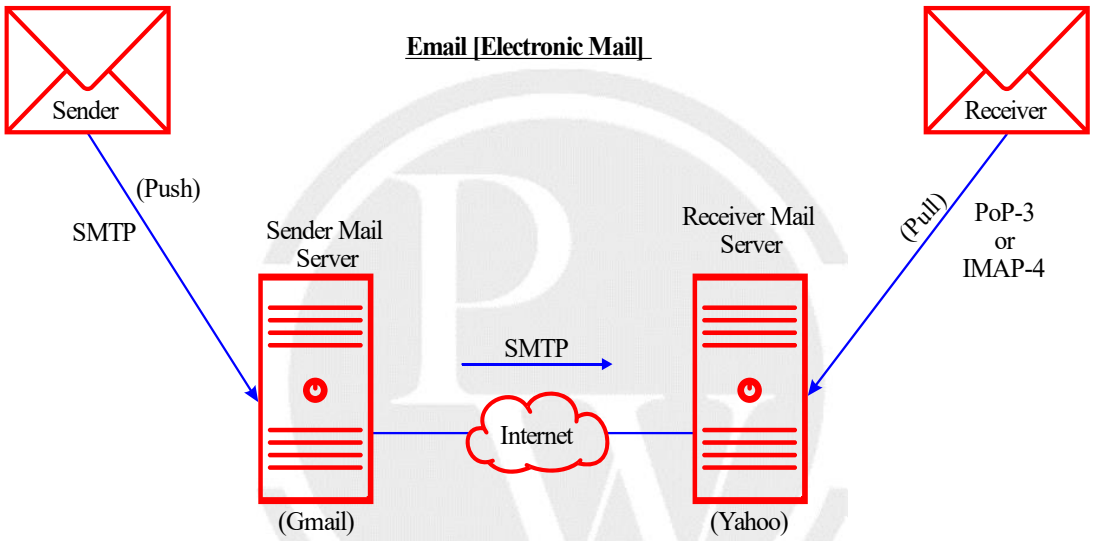
7.4.4 Internet Control Message Protocol (ICMP)



❑❑❑

8 APPLICATION LAYER PROTOCOL

8.1 E-MAIL



SMTP transfer the mail from sender's mail server to receiver's mail server.
While sending the mail ,SMTP is used two times-.

(i) Between the sender and sender's mail server
(ii) Between the sender's mail server and receiver's mail server

8.1.1 To receive or download the email,

Another protocol is needed between the receiver mail server and receiver.
The most commonly used protocols are POP3 and IMAP4.

8.1.2 SMTP(Simple mail transfer protocol)

1. The objective of SMTP is to transfer the email reliably and efficiently.
2. It uses port number-25 at TCP.
3. In SMTP there are two components:
   (i) User Agent (UA)
   (ii) Mail transfer Agent (MTA)
4. User Agent prepares the message, creates the envelope and put the message in the envelope.
5. Mail transfer Agent transfer the mail across the internet i.e. Actual mail transfer is done through MTA.
6. To send mail, system must have a client MTA and to receive the mail. it must have a server MTA.

7. SMTP is text based protocol.
8. With the help of SMTP & POP we can send only text messages.
9. SMTP can only handle the message containing 7 bit ASCII text.
10. SMTP cannot transfer other types of data like images, video, audio, etc.
11. SMTP cannot transfer binary files or executable files.
12. SMTP cannot transfer the text data for the language other than English (such as French, Japanese, and Chinese etc.).
13. Only SMTP is not sufficient to send binary files or to send videos or audio so we require MIME (Multipurpose Internet mail extension).
14. MIME is a supplementary protocol that allows non-ASCII data to send through SMTP.
15. MIME is a set of software function that transforms non-ASCII data to ASCII data or viceversa.
16. MIME is used to convert non text data to text data and text data to non text data.
17. SMTP is stateless protocol. It does not maintain any information of user. If an e-mail is asked to be sent twice, then server resends it without saying that e-mail has already been sent.
18. SMTP is a connection-oriented protocol.
19. SMTP uses persistent TCP connections, so it can send multiple e-mail at once.
20. SMTP is an “In-Band” protocol.
21. SMTP is used for Push the e-mail.
22. SMTP Pushes the mail from client to server on other hand, It needs a pull protocol(Download).
23. POP3 and IMAP4 are used for Pulling the e-mail.

8.2 POP3(Post office Protocol version-3)

1. It is a message access protocol.
2. It is a pull protocol.
3. POP3 uses port number-110 at TCP.
4. POP3 is a connection-oriented protocol.
5. POP3 uses persistent TCP connection.
6. POP3 is a stateful protocol.
7. POP3 is an “In-Band” protocol.
8. POP3 does not allow users to partially check the content of the mail before downloading.
9. POP3 does not allow user to organize the mail on the mail server.

8.2.1 IMAP-4(Internet Mail Access Protocol version-4)

1. IMAP-4 is similar to POP3 but it has more features. IMAP-4 is more powerful and more complex.
2. IMAP-4 provides the following extra functions.
3. A user checks the email header prior to downloading.
4. A user can search the content of the email for a specific string of characters prior to downloading.
5. A user can partially download the email.

6. A user can create, delete, or rename the mail box on the mail server.
7. A user can create a hierarchy of mailbox in a folder for email storage.

8.2.2 Characteristics of IMAP

1. IMAP is a pull protocol.
2. IMAP uses port number-143 at TCP.
3. IMAP is a connection-oriented protocol.
4. IMAP uses persistent TCP connection.
5. IMAP is a tasteful protocol.
6. IMAP is an "In-Band" Protocol.

POP3	IMAP
(1) Mails can only be accessed from a single device.	Mails can be accessed from multiple device.
(2) Download the email from server to a single computer and the copy at the server is deleted.	The email message is stored on the mail server itself.
(3) User cannot organize the mails in the mail box of the mail server.	User can organize mails on the mail server.
(4) It does not allow user to sync emails.	It allows user to sync their emails.
(5) It is unidirectional i.e all the changes made on a device does not effect the content present on the server.	It is bidirectional i.e all the chances made on server or device are made on the other side too.

8.3 File Transfer protocol (FTP)

8.3.1 FTP (File Transfer Protocol)

1. File transfer protocol is a standard internet protocol for transferring files b/w computers over TCP/IP connection.
2. It uses port number - 20 & 21 on TCP.
3. It has two types of connection
   (i) Control connection (port number. - 21)
   (ii) Data connection (port number - 20)
4. Control connection remains connected during the entire interactive FTP session.
5. The data connection is opened and closed for each file transfer activity.
6. When user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.
7. FTP uses persistent TCP connections for control information.
8. FTP uses Non-persistent TCP connections for data information.
9. FTP is a connection-oriented protocol.
10. FTP is an "out of band" protocol as data and control information flow over different connection.
11. Some protocols send their request and data in the same TCP connection for this reason they are called as In-bound protocol.
12. HTTP & SMTP are In-Band protocol.
13. FTP is state full protocol.

8.3.2 Transmission mode

FTP can transfer a file across the data connection using one of the following three transmission modes.

(i) Stream mode
(ii) Block mode
(ii) Compressed mode

8.3.3 File Type

FTP can transfer one of the following file types across the data connection:

(i) ASCII file
(ii) EBCDIC file (File format used by IBM)
(ii) Image file

8.3.4 Data structure

FTP can transfer a file across the data connection using one of the following interpretation of the structure of the data:

(i) File structure
(ii) Record structure
(iii) Page structure

8.4 HTTP Protocol

1. HTTP protocol is used mainly to access data on world wide web (www).
2. It is client server protocol using port number - 80 on TCP.
3. HTTP is "In-Band" protocol i.e. both request and data we will send only in one connection.
4. HTTP is a stateless protocol i.e. It does not maintain any information of user.
5. There are two types of HTTP protocol
   (i) Non persistent (1.0)
   (ii) Persistent (1.1)

8.5 Non Persistent (1.0)

In a Non persistent connection one TCP connection is ade for each request/response. This strategy follow the following steps :-

(i) The client opens a TCP connection and sends a request.
(ii) Server sends the response and closes the connection.
(iii) In this strategy , If a file contains link to N-different pictures in different files(all located on same server) the connection must be opened and closed N+1 times.

8.6 Persistent (1.1)

1. In a persistent connection the server leaves the connection open for more request after sending a response.
2. The server closes the connection at the request of client or time out has been reached.

8.6.1 Important Table

SHORT TRICK	DNS	HTTP	SMTP	POP	IMAP	FTP
Stateful/ Stateless	Stateless	Stateless	Stateless	Stateful	Stateful	Stateful
Transport Protocol Used	UDP	TCP	TCP	TCP	TCP	TCP
Connectionless/ Connection oriented	Connection less	Connection less	Connection oriented	Connection oriented	Connection oriented	Connection oriented
Persistent/Non-persistent	Non-persistent	HTTP 1.0 is non persistent HTTP 1.1 is persistent.	Persistent	Persistent	Persistent	Control connection is persistent. Data connection is non-persistent.
Push/Pull	-	-	Push	Pull	Pull	Can't
Port Number Used	53	80	25	110	143	20 for data connection. 21 for control connection.
In band/ Out-of-band	In band	In band	In band	In band	In band	Out-of- band

Application	Port Number.	Transport Protocol
DNS	53	UDP
HTTP	80	TCP
FTP	20 (Data connection) 21(Control connection)	TCP
SMTP	25	TCP
POP	110	TCP
SNMP	161, 162	UDP
TFTP	69	UDP
IMAP	143	TCP
Telnet	23	TCP
DHCP	67 (DHCP Server) 68 (DHCP Client)	UDP

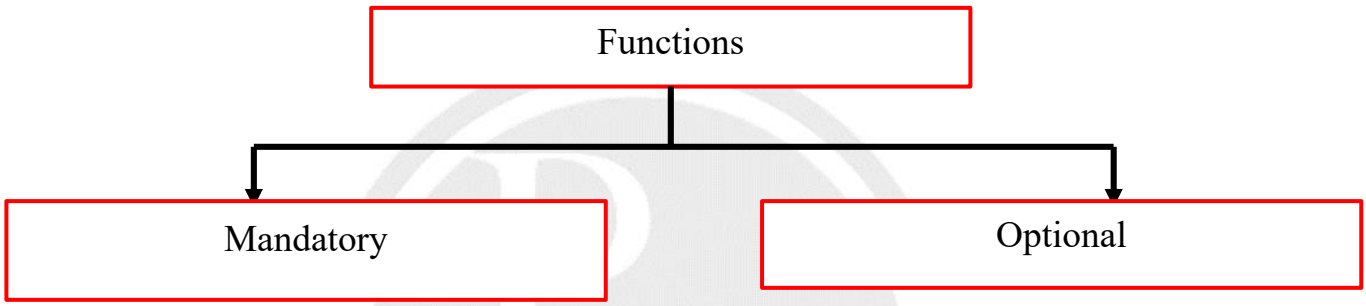
8.6.2 Commands

HTTP	FTP	SMTP
GET	USER	HELO
HEAD	PASS	MAIL FROM
PUT	ACCT	RCPT TO
POST	CWD	DATA
TRACE	REIN	QUIT
DELETE	QUIT	RSET
CONNECT	PORT*	VRFY
OPTIONS	PASV	NOOP
	TYPE	TURN
	MODE	EXPN
	PROMPT	HELP
	STRU	SEND FROM
		SMOL FROM
		SMAL FROM

❑❑❑

9 OSI AND TCP/IP PROTOCOL STACK

9.1 Functions of Computer Network



- Error control
- Flow control
- Access control
- Multiplexing and Demultiplexing
  :
  :

- Encryption & Decryption
- Check pointing
- Routing
  :
  :

9.2 OSI/ISO

OSI : Open systems Interconnection model.
ISO : International Standards Organization. It is a multinational body dedicated to worldwide agreement on international standard.

9.2.1 OSI Mode

- This model has been proposed by ISO.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture (Hardware/Software).
- The purpose is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware & software.
- This model has got 7 separate but related layers.

9.3 Functions of Physical layer

9.3.1 Physical Layer

Physical Layer is responsible for movement of individuals bits from one Hop to next Hop.

9.3.2 Functions of physical Layer

1. It is used to define electrical, mechanical, functional and procedural characteristic of physical link. (physical Link)
   Copper → Electrical signal
   Fiber → Light signal
   Wireless comm. → Electromagnetic signal.

2. It defines transmission mode:
   a. Simplex
   b. Half duplex
   c. Full duplex

3. It defines topology configuration:
   - Bus topology
   - Star topology
   - Mesh Topology
   - Tree Topology

4. It is totally Hardware layer.

5. It defines link configuration:
   i Point to Point Link
   ii Broadcast Link
6. It defines Encoding.
7. Bits Synchronization.
8. Bit rate control.

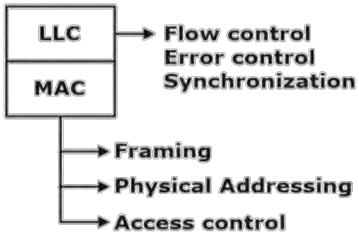
9.4 Data Link Layer

Data link layer is responsible for moving frames From One Hop (Node) to Next Hop (Node).

9.4.1 Function of data link layer

1. Flow control
2. Error control
3. Access control
4. Framing
5. Physical Addressing

Data Link Layer is divided into two parts



9.5 Network Layer

The network layer is responsible for the delivery of individual packet from source to destination.

9.5.1 Function of Network Layer

1. Host to Host connectively
2. Logical Addressing
3. Switching
4. Routing
5. Fragmentation
6. Congestion control:

9.6 Transport Layer

Transport Layer is responsible for process to process delivery. A process is an application program running on a host.

9.6.1 Function of Transport Layer

1. End to end connectively
2. Service point Addressing
3. Flow control
4. Error control
5. Segmentation and Reassembly
6. Congestion control
7. Connection Control
8. Multiplexing and Demultiplexing.

9.7 Session Layer

Session layer also known as **network dialog controller.** It establishes, maintains, synchronizes and terminates the interaction b/w sender and receiver.

9.7.1 Function of Session Layer

1. Authentication & Authorization
2. Check point or synchronization
3. Dialog control

9.8 Presentation Layer

This layer take care of syntax and semantics of the information exchange in between two communicating systems.

9.8.1 Function of Presentation Layer

1. Character translation
2. Encryption/Decryption
3. Compression

9.9 Application Layer

Application Layer is responsible for providing services to users. Users such as:

1. Mail services
2. File sharing
3. File transfer and many more

9.10 TCP/IP Model

This mode has got 5 different layer

Physical : No specific protocol

Data Link : No specific protocol

Network : ARP, RARP, ICMP, IGMP

Transport : TCP, UDP,SCTP

Application : DNS, SMTP, HTTP, FTP, POP,IMAP, SNMP , Telnet etc.

❑❑❑