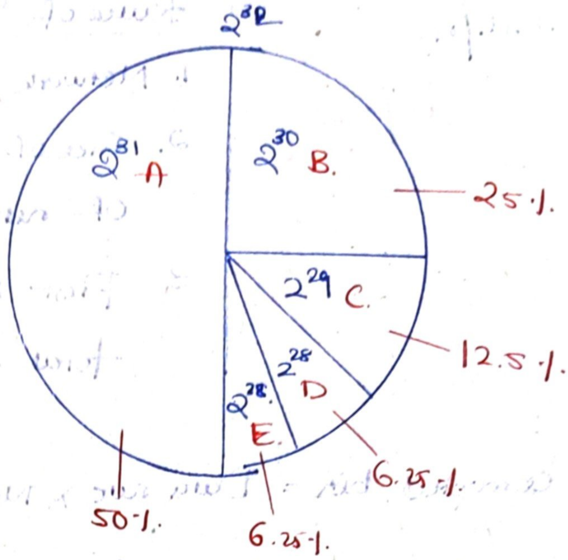
Computer Networks

Classful Addressing:

- Class A : 0
- Class B : 10
- Class C : 110
- Class D : 1110
- Class E : 1111.

Fixed bits.



Class	NID	HID	Host/subnet.	Range
A	2^7-2	24 bits.	$2^{24}-2$	1–126
B.	2^{14}.	16 bits.	$2^{16}-2$.	128–191
C.	2^{21}.	8 bits.	$2^{8}-2$	192–223
D.	—	—	—	224–239
E	—	—	—	240–255

0.0.0.0 – default route / DHCP client.

127.x.x.x

- self connecting
- loopback
- testing
- Inter process Communication.

also 127.x.x.x can't be used as S.IP only D.IP.

* ARP request → Broadcasting

* ARP reply → Unicasting

Types of Communication

1. Unicast (1 to 1)
2. Broadcast (1 to All)
3. Multicast (1 to Many)

Direct Broadcasting: transmitting data from one to all computer.

DBA : HID part all 1's

LBA : 255.255.255.255 — Same for All.

NID	HID	
valid	0's	– Network Id of entire n/w.
valid	1's	– DBA
1's	1's	– LBA

Subnetting: borrowing bits from HID.

'n' bits borrow = 2^n subnets possible

→ for each subnet = $2^{HID-n\text{ bits}}-2$ hosts/subnet possible.

Classless Addressing

a.b.c.d./n.

NID / Subnet mask

Supernetting : Combining two or more networks.

Rules of Supernetting :

1. Network IDs must be contiguous
2. Size of N/w must be same and number of networks must be power of 2.
3. First NID must be divisible by the total size of the Supernet.

* No. of corrupted bits = Data rate x Noise Duration.
* Hamming distance = distance between two binary strings of same size is the no. of differences between corresponding bits.
* To detect 'd' bit error, minimum hamming distance required is (d+1)
* To correct 'd' bit error, minimum HD required = (2*d+1)

CRC

Length of dataword = n

Length of divisor = k

Append (k-1) zeros to original msg

Perform modulo 2 division

Remainder of division = CRC

Codeword = n + k-1

Codeword = dataword with appended (k-1) zeros + CRC.

Polynomial Notation in CRC

Dataword = d(x)

Codeword = c(x)

Generator = g(x)

Syndrome = s(x)

Error = e(x)

(1.) Determine degree of 'r' of g(x) (highest power)

(2.) Determine $x^r d(x)$

(3.) Get the remainder by dividing $x^r d(x)$ by g(x)

(4.) Codeword = $x^r d(x)$ + remainder.

* A generator that contains a factor of $(x+1)$ can detect all odd numbered errors.

* If generator has more than 1 term and co-efficient of x^0 is 1, all single bit error can be detected

* If a generator cannot divide (x^t+1) (t b/w 0 to n-1) then all isolated double error can be detected.

A good polynomial generator should have:

1. Atleast two terms.
2. Coefficient of x^0 should be 1.
3. It should divide x^t+1 (t b/w 2 and n-1)
4. It should have the factor $x+1$.

	Data	Bandwidth
k	2^{10}	10^3
M	2^{20}	10^6
G	2^{30}	10^9.

* According to hamming code,

→ Redundant bits = $m+r+1 \le 2^r$

r = lower limitation

→ Redundant bit position = 2^i ($i \ge 0$)

Transmission delay - Td = $\frac{L}{B}$ (L = Frame/packet size, B = Bandwidth)

Propogation delay - Pd = $\frac{\text{distance}}{\text{velocity}}$.

Total Time / RTT = Td (Frame) + 2* pd + Qd + Prd + Td (Ack).

Efficiency of "Stop and wait" = $\frac{\text{Td (Frame)}}{\text{Total time}}$

Throughput = efficiency × Bandwidth.

* Stop and wait uses independent acknowledgement.

In Stop and wait ARQ :

1. Efficiency ↓ when Pd ↑ and Td ↓
2. Efficiency ↑ when Td ↑ and Pd ↓
3. Efficiency ↓ when distance ↑ and bandwidth ↑
4. Efficiency ↑ when pkt size ↑ and distance ↓

Sliding window:

* Max window size = $(1+2a)$ pkt.
* Min sequence no = $(1+2a)$ $\left\{ a = \frac{Pd}{Td} \right\}$
* Min no of bits required for sequence no. = $\lceil \log_2 (1+2a) \rceil$

Selective Repeat / Selective Reject

* Window Sender Size = Window reciever Size.
* Seq. no = k bit
  $W_S = 2^{k-1}$, $W_R = 2^{k-1}$

$$\text{Efficiency} = \frac{W_s \times \text{Frame Size}}{\text{Total Time}}$$

Go-back-N $(N>1)$

Sender window size = N

Reciever window size = 1.

– It use cumulative acknowledgement.

$W_S + W_R \le$ Avail. Seq Number

→ $W_S + 1 \le ASN$

→ $W_S \le ASN - 1$

$$\text{Efficiency} = \frac{N \times Td\ (\text{frame})}{\text{Total time}}$$

Sequence no = k bit

$W_S = 2^k - 1$, $W_R = 1$.

	Stop and wait	Go-Back N	Selective Repeat
Efficiency.	$\eta = \frac{Td}{\text{Total time}}$	$\eta = \frac{Td \times N}{\text{Total time}}$	$\eta = \frac{Td \times W_S}{\text{Total time}}$
Buffer.	1+1	N+1	N+N
Sequence no.	2 (0 and 1)	N+1 (0–N)	2N (0–(2N–1))
Seqno = k bit.	--	W_S $2^k - 1$, W_R 1	W_S 2^{k-1}, W_R 2^{k-1}

IPv4 Header

VER 4	HL 4	Service 8	Total length 16	— 32 bit
Identif. no. 16	Flags 3	Frag Offset 13		— 32 bit
TTL 8	Protocol 8	Header Checksum 16		— 32 bit
Source Ip Address 32				— 32 bit
Destination Ip address 32				— 32 bit
Options (0-40 Byte)				— variable 40 Byte

20 Byte

Min Header size = 20B.

Max Header size = 60B.

Scaling factor = 4

* Ip is a packet stream protocol.
* TCP is a byte stream protocol.
* Order of elimination of datagrams from buffer:

ICMP > IGMP > UDP > TCP.
(01) (02) (17) (06)

Not Change	May be changed	Definitely Changed
1. VER	1. Total length	1. TTL
2. Service	2. MF	2. Header Checksum
3. Identif. no.	3. Frag offset	
4. DF	4. Header length	
5. Protocol	5. Options.	
6. SIP		
7. DIP		

MTU: maximum amount of data that can be stored in any data link layer.

* Fragmentation is done by Intermediate devices such as "Routers"

* $\text{Fragmentation overhead} = (\text{Total \# fragment} - 1) * \text{size of Ip header}$.

TCP Header:

Source port 16		Destination port 16		→ 4B
Sequence No. 32				→ 4B
Acknowledgement No. 32				→ 4B
HL 4	Reserved 6	1 1 1 1 1 1	Window Size 16	→ 4B
Checksum 16		Urgent pointer 16		→ 4B
Options (0-40 Bytes)				

* Min header size = 20 B
* Max header size = 60 B

0 → 1023 } Well known port no

0 → 49,151 } Reserved / Registered port no

49,152 → 65,535 } Dynamic port no

* Time out Timer (TCP) = $Td + 2 * pd$

* **Basic Algorithm** : $NRTT = \alpha(IRTT) + (1-\alpha) ARTT$

  $0 \leq \alpha \leq 1, \quad \alpha = \frac{1}{2} = 0.5$

* **Jacobson's Algorithm** : $T.O = 4 \times Do + RTT$

* **Congestion window size** = min { Network Capacity, Recieve Capacity }

TCP Checksum = TCP data + TCP Header + IP pseudo Header

Token Bucket

→ Max no of packets = $C + rt$

→ Max avg rate of token bucket = $\frac{C + rt}{t}$

→ $t = \frac{C}{m - r}$

C = Capacity of token bucket

r = rate of tokens entering

t = max no of packets enter into network during time interval 't'

UDP Header

Source port 16	Destination Port 16	4B
Length 16	Checksum 16	4B
		8B

TCP	UDP
Dynamic header	Fixed header
Error and flow control	No error/flow control
Connection oriented	Connectionless
Reliable	Not reliable
High Overhead	Low overhead
Order maintained	No order
Protocols : HTTP, FTP, SMTP.	Protocols : DNS, SNMP

Congestion Control Algorithm (TCP)

1. Slow Start phase (exponential increase)
2. Congestion avoidance (additive increase)
3. Congestion detection (multiplicative decrease)

* Total length in UDP $= 2^{16} - 1$
$= 65,535$

* Practical data size at Transport layer at UDP = 65,507

$\{65,535 - 20 - 8\}$ — $65,535$: TL; 20: IP header; 8: UDP header

* When destination port is "well known port no", data moving Client → Server

* When Source port is "well known port no", data is moving from Server → Client.

WAP $= \frac{\text{total seq. no}}{\text{Bandwidth (B/sec)}}$

Min seq no to avoid
WAP $= LT \times B$

* Min bits required
$= \lceil \log_2 (LT \times B) \rceil$

Pure Aloha.

Backoff time = K × slot time.
K: (0 to $2^n - 1$, n = collision no)

→ Vulnerable time $= 2 * T_F$

→ Transmission time of single frame — $T_F = \frac{\text{Frame Size}}{\text{Bandwidth}} = \frac{L}{B}$

→ Throughput $= S = G \times e^{-2G}$

G = no of frames generated in one frame transmission

* Max throughput (Pure aloha) = 18.4% (when G = 1/2)

Slotted Aloha.

→ Vulnerable time = T_f.

→ Throughput $= S = G \times e^{-G}$

* Max throughput = 36.8% (when G=1)

CSMA

Vulnerable time = Pd.

CSMA/CD

* $Td\,(\text{Jam Signal}) = \dfrac{\text{Jam Signal Size}}{\text{Bandwidth}}$

* $Td\,(\text{Frame}) \geq 2 \times pd + Td\,(\text{Jam Signal})$

* $\text{Frame Size} \geq 2 \times pd + Td\,(\text{Jam signal}) \times \text{Bandwidth}$.

Ethernet

* Connectionless communication
* No flow control and per level error control.
* No acknowledgment
* Uses bus topology
* Uses CSMA/CD as access Control method.
* Uses Manchester Encoding

→ Baud rate = 2 × Bit rate

→ Bit rate = $\frac{1}{2}$ Baud rate

Ethernet:

Preamble	SFD	DA	SA	Length of Data or Type	Data	CRC
7B.	1B	6B	6B	2B.	(46-1500)	4B.

max data in Ethernet

Destination MAC Address.

1. Unicast MAC address: last bit of first byte is 0.
2. Multicast MAC address: last bit of first byte is 1.
3. Broadcast MAC address: if all 48 bits are 1.

In ethernet: * Efficiency ↑ when pd ↓ and Td ↑

* Efficiency ↓ when pd ↑ and Td ↓.

→ Efficiency of ethernet = $\eta = \dfrac{1}{6.44a+1}$ $\left\{ a = \dfrac{Pd}{Td} \right\}$

* Probability of station not to transfer data pkt is (1-P)
* For successful transmission of one station, remaining (N-1) Packets should not transfer the data pkt.

N = stations in ethernet, P = probability of station to transfer data pkt.

* Probability of (N-1) stations not to transfer data put = $(1-p)^{N-1}$
* Probability of success of single transmission = $p(1-p)^{N-1}$
* Probability of success of any station = $N.p(1-p)^{N-1}$
* Avg no of collisions that might occur before a successful transmission = e

→ Throughput of host = $p(1-p)^{N-1}$

→ Throughput of channel = $Np(1-p)^{N-1}$.

Controlled Access Protocols

1. Polling
2. Reservations
3. Token passing.

Polling

→ Efficiency = $\frac{Td}{T_{poll}+Td+Pd}$

→ Throughput = $\eta \times B$

TDMA

→ Efficiency = $\frac{1}{1+a}$ $\left(a = \frac{Pd}{Td}\right)$

Circuit Switching

Total time = $S + \frac{m}{B} + x.\frac{d}{v} + T$.

S = Setup time.

m = message; B = bandwidth.

X — #hops

T – teardown time.

Packet Switching

Total time = $x.\frac{m}{B} + x.\frac{d}{v} + x-1 \times (Qd + Prd)$

Total time for 'x' hops and 'N' packets.

→ Total time = $x[Td + Pd] + (x-1)[Qd + Prd]$

→ Optimal packet size = P = p + h — header size

p — payload/packet data size

→ If no. of hops/link = x, the no of routers = x-1

Protocols :

SMTP → Email

DNS → Domain name to Ip addr.

FTP → File transfer.

HTTP → Web Services

POP → Download email.

Application	Port No.
DNS	53
HTTP.	80
FTP.	20 (DC), 21 (CC)
SMTP.	25
POP	110
SNMP	161, 162
TFTP	69
IMAP.	143
Telnet	23
DHCP	67 (S), 68 (C)

* By default DNS uses UDP at transport layer.
* DNS Query Size < 512B → UDP
* DNS Query Size > 512B → TCP

TCP	UDP
SMTP	DNS
HTTP	SNMP
FTP	TFTP
POP	DHCP
IMAP	– All realtime and multimedia protocols
Telnet	

HTTP Commands :

GET

HEAD

PUT

POST

TRACE

DELETE

CONNECT.

Stateful	Stateless
DNS	POP
HTTP	IMAP
SMTP	FTP

ARP : Communication protocol to find MAC address of a device from its IP address.

Feedback / Error Reporting ICMP messages.

1. Destination unreachable
2. Source quench
3. Time exceeded
4. Parameter problems
5. Redirection.

Query or Request and Reply ICMP messages

1. Echo request and reply
2. Time Stamp request and reply
3. Address mask request and reply
4. Router solicitation and advertisement.

No Icmp message will be generated if

* in response to a datagram carrying an Icmp
* for a fragmented datagram that is not first fragment.
* for a datagram having multicast address
* for a data gram having special address like 127.0.0.0

Distance Vector Routing	Link State Routing
1. Bandwidth required is less because we send only distance vector.	Bandwidth required is very high because we send entire link state packet.
2. Local knowledge.	Global knowledge
3. Bellman Ford Algorithm	Dijkstra's Algorithm
4. Traffic is less.	High traffic.
5. Count to infinity problem	No count to infinity problem
6. Convergence low	Convergence is faster
7. RIP	OSPF

OSI model:

Application layer
Presentation layer } user support layer
Session layer

Transport layer — interface

Network layer
Data link layer } network support layer
Physical layer.

Physical layer: responsible for movement of bits from one hop to next hop.

Data link layer: responsible for moving frames from one hop to next hop (node).

Network layer: delivery of individual packet from source to destination

Transport layer: for process to process delivery

Session layer: It establish, maintain, synchronise and termi-nate the interaction between sender and reciever.

Presentation Layer: It take care of syntax and semantics of information exchanged b/w two communicating systems.

Application layer: providing service to users such as mail service, file transfer and many more.