Q.1 a. Compare OSI reference model with TCP/IP model. (4)

Answer:

Comparison between OSI and TCP/IP

OSI MODEL	TCP/IP
OSI has seven layers	TCP/IP has four layers.
Model first and then next protocol	Protocols comes first and model next
Three concepts are central to OSI model services, interfaces, protocols	Services, interfaces and protocols are not distinguished properly
OSI supports both connectionless and connection oriented communication in the network layer	TCP/IP model has connectionless in the Internet layer and both modes in the transport layer

b. What is the difference between a physical address, and network address? (4)

Answer:

The **physical address** is the unique hardware address that identifies an interface of a machine on a physical network such as a LAN. Physical addresses are used in the data link layer.

A **network address** is a machine's logical address on a network. The network address is used in the network layer. The network address used on the Internet is the IP address

c. What is the Shannon channel capacity for a telephone channel with bandwidth of 3400 Hz and SNR of 40db? (4)

Answer:

Note that

SNR (dB) = 40 dB

SNR = Antilog(40)=10000

$C = 3400 \log_2 (1 + 10000)$

$= 3400 \log_{10} (10001)/\log_{10}2 = 45200$ bps

d. Find the error, if any, in the following IPv4 addresses. (4)

i) 111.56.045.78
ii) 221.34.7.8.20
iii) 75.45.301.14
iv) 11100010.23.14.67

Answer:

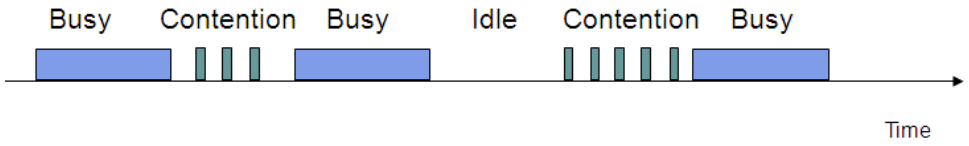
i) There must be no leading zero (045).
ii) There can be no more than four numbers in an IPv4 address.
iii) Each number needs to be less than or equal to 255 (301 is outside this range).
iv) A mixture of binary notation and dotted-decimal notation is not allowed.

e. Explain the working of CSMA/CD protocol. (4)

Answer:

Assumptions

- Collisions can be detected and resolved in $2t_{prop}$
- Time slotted in $2t_{prop}$ slots during contention periods
- Assume n busy stations, and each may transmit with probability p in each contention time slot
- Once the contention period is over (a station successfully occupies the channel), it takes X seconds for a frame to be transmitted
- It takes t_{prop} before the next contention period starts.



- Contention is resolved ("success') if exactly 1 station transmits in a slot:
  - $P_{success} = np(1-p)^{n-1}$
- At maximum throughput, systems alternates between contention periods and frame transmission times

$$\rho_{\max} = \frac{X}{X + t_{prop} + 2et_{prop}} = \frac{1}{1+(2e+1)a} = \frac{1}{1+(2e+1)Rd/vL}$$

where:

R bits/sec, *L* bits/frame, X=*L/R* seconds/frame $a = t_{prop}/X$

n meters/sec. speed of light in medium ***d*** meters is diameter of system

$2e+1 = 6.44$

f. What is birth death process? Briefly describe the Laws of Motion for Birth-Death. (4)

Answer:

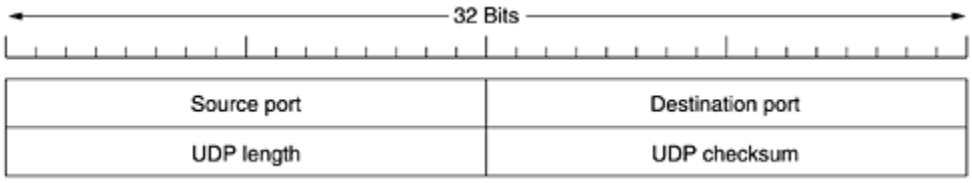
A **birth-death process** is a continuous-time stochastic process for which the system's state at any time is a nonnegative integer.

- Law 1
  - With probability $\lambda_j\Delta t+o(\Delta t)$, a birth occurs between time t and time $t+\Delta t$. A birth increases the system state by 1, to $j+1$. The variable λ_j is called the **birth rate** in state j. In most queuing systems, a birth is simply an arrival.
- Law 2
  - With probability $\mu_j\Delta t+o(\Delta t)$, a death occurs between time t and time $t+\Delta t$. A death decreases the system state by 1, to j-1. The variable μ_j is the death rate in state j. In most queuing systems, a death is a service completion. Note that $\mu_0 = 0$ must hold, or a negative state could occur.
- Law 3

  Births and deaths are independent of each other.

g. Briefly explain the user Datagram protocol. (4)

Answer:



- The characteristics of UDP are as follows
  - UDP service is unreliable
  - UDP does not guarantee the delivery of datagram to the destination
  - UDP does not required connection establishment prior to data transfer
  - UDP computes the checksum for the entire header plus data
  - No segmentation
  - No buffering

The UDP header format is as shown in fig. UDP header is only 8 bytes long. Source Port number and Destination Port Number are two byte fields specifies the source and destination applications for the encapsulated data;

UDP length indicates the length of the entire segment in bytes.

The checksum is optional in case of UDP, checksum covers the entire datagram (header + Data). When no checksums are used all the bits are set to 0's in the checksum field.

Q.2 a. Explain the functions performed by the following layers of OSI model
(i) Physical layer
(ii) Data link layer
(iii) Presentation layer (9)

Answer:

Layer 1:Physical Layer

It is the layer concerned with the transmission of raw bits over the communication path. It relates to the setting up of a physical circuit for the movement of bit stream over the circuit.
Physical layer has the following characteristics.

i) **Electrical** – deal with voltage levels and timing of voltage change
ii) **Procedural** – Specifies the sequence of events for transmitting data based on characteristic of interface.

Some of the design issues are ;

i) Correct transmission of 1's and 0's
ii) **Transmission media** – Twisted pair, co-axial cable, Fiber Optics, satellites.
iii) Network connections and pin details**.**
iv) **Transmission Type** - Duplex / Simplex, Analog / Digital, FDM / TDM

Layer 2 : Data link Layer.

The data link layer is concerned with issues like;

i) Transmission block starting and ending.[Frame formation]

ii) Transmission error detection
iii) Error control to get an error free link.

The design of data layer involves;
a) Framing and link management
b) Error control and flow control
c) Service to the network layer
d) Error detection and correction
e) Error correcting codes and detecting codes
f) Data link protocols and protocol performance

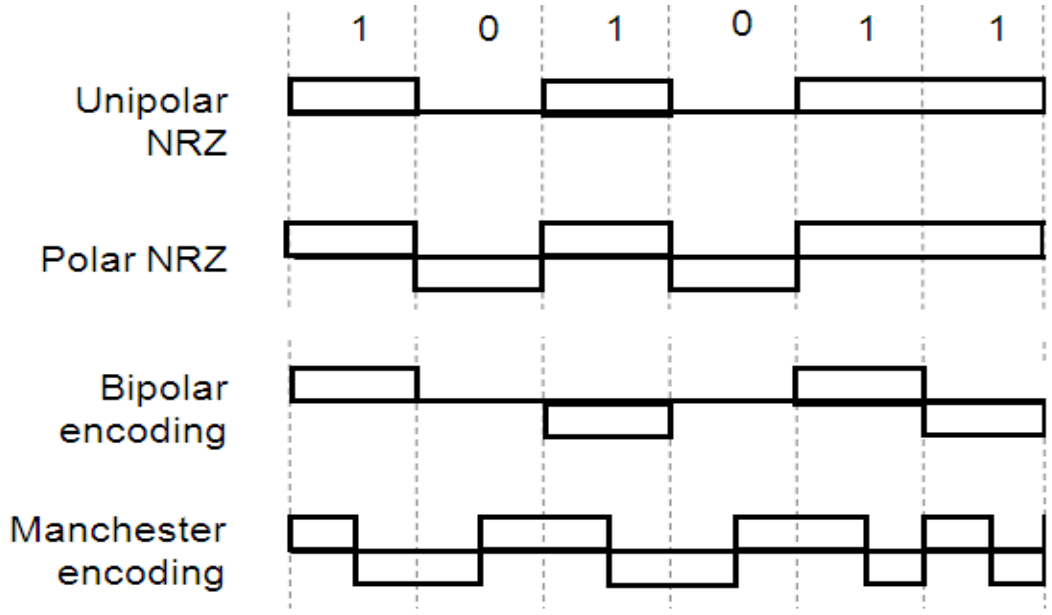
Standards; HDCL, ADCCP,.

Layer 6: Presentation layer:

The presentation layer is concerned with the syntax and semantics of the data exchange between application entities. It resolves differences in format and data presentation. Proper presenting is needed as most user programs exchange names, dates, number, amount of money, etc. and not the binary bit strings. Presentation layer does the conversion and meaning of the information is preserved. Some design issues of this layer are;
i) data representation, data compression
ii) Conversion between the virtual terminal and the real terminal.
iii) Conversion of character stream so that devices with different character sets can communicate.
iv) Network security and privacy.

b. Represent the binary data 101011 in
(i) NRZ-unipolar
(ii) NRZ-polar
(iii) Bipolar
(iv) Manchester, encoding format **(4)**

Answer:



c. Explain 'Flooding' and 'Deflection Routing' . (5)

Answer: Refer page 520 of Reference Book

Q.3 a. Explain selective repeat ARQ and obtain an expression for its efficiency (9)

Answer:

Selective Repeat ARQ:

Selective repeat ARQ protocol is an extension of the Go-Back-N with two new features. They are:

- The receive window is made larger than one frame-capacity
- Retransmission mechanism is modified such that only the individual frames that are required are retransmitted.

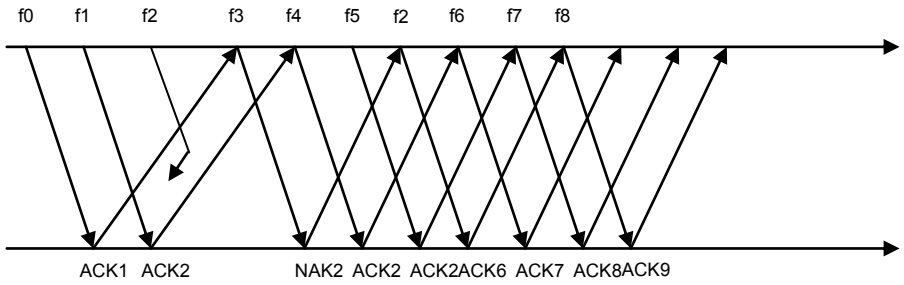


Fig.: Error recovery in Selective Repeat ARQ

Function of the transmitter:

When the send window is empty, the transmitter is in the ready state, waiting for a request from a process in a higher layer. When the transmitter receives a request for transmission, it accepts a packet from the upper layer and prepares a frame for transmission; the sequence number (S_{recent}) is set to the lowest number available in the send window. Suitable error detection codes are also added. The frame is transmitted and a timer is started. If $S_{recent} = W_S - 1$ then the send window is empty, and the transmitter goes back into the blocking state. Else the transmitter stays in the ready state. If an ACK frame is received with value of R_{next} between S_{last} and S_{recent}, then the send window slides forward by setting $S_{last} = R_{next}$ and limit of send window number to $S_{last} + W_S - 1$. If a NAK frame is received with value of R_{next} between S_{last} and S_{recent} then, the frame with sequence number R_{next} is retransmitted. The send window slides forward by setting $S_{last} = R_{next}$ and limit of send window number to $S_{last} + W_S - 1$; else the frame is discarded. The transmitter is in the blocking state when the send window is empty.

Function of the receiver:

The receiver process is always in the ready state waiting for the arrival of a frame from the transmitter. On reception of the incoming frame, the frame is checked for errors. If there are no errors and if the sequence number of the frame is within the range of the send window, then the frame is accepted, buffered, and an acknowledgement is sent. If an arriving packet has no errors, but the sequence number is outside the range of the sending window, then the frame is discarded and a NAK frame is transmitted to the transmitter

Maximum window size

The maximum size of the send window is half the sequence number space, i.e.,

$Ws = Wr = 2^m - 1$

Efficiency of Selective Repeat ARQ

It is said to be the most efficient of all the ARQ protocols that have been discussed.

The probability of a frame being received in good order is 1-Pf. Thus the average number of times a frame has to be sent is the reciprocal of the probability, i.e.,

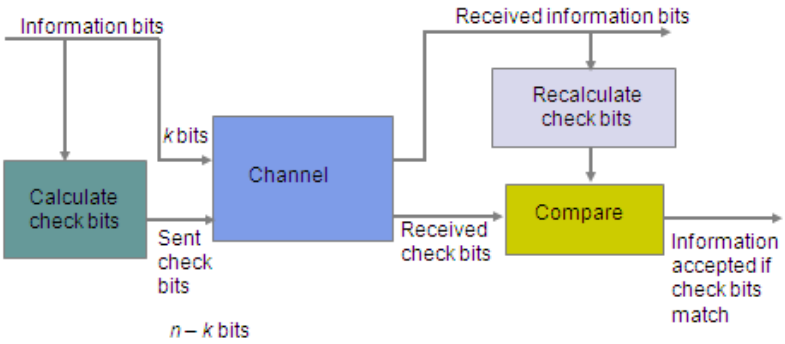
$t_{sr}=t_f/(1-p_f)$

Thus efficiency of selective repeat ARQ is $\eta_{sr} = [(n_f - n_{o))/ t_{SR]/R}$

$= [1 -(n_o/ n_{f)]/[1-} P_{f]}$

b. With neat block diagram explain Error detection system using check bits. (5)

Answer:



- *Redundancy*: Single parity check code adds 1 redundant bit per k information bits: overhead = $1/(k + 1)$
- *Coverage*: all error patterns with odd number of errors can be detected
  - An error patten is a binary $(k + 1)$-tuple with 1s where errors occur and 0's elsewhere
  - Of 2^{k+1} binary $(k + 1)$-tuples, ½ are odd, so 50% of error patterns can be detected
- Is it possible to detect more errors if we add more check bits?

c. Measurements of a slotted ALOHA channel with an infinite number of users show that 10% of the slots are idle.
(i) What is the channel load, G?
(ii) What is the throughput?
(iii) Is the channel under loaded or overloaded? (4)

Answer:

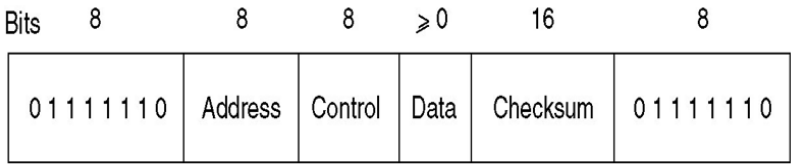
(i) Proportion of slots that go idle in Slotted ALOHA system = P_0 = P[0 transmission] = $[G^0/0!]e^{-G} = e^{-G}$, therefore $G = -\ln P_0 = -\ln 0.1 = - (-2.303) = 2.303$

(ii) $S = Ge^{-G} = 2.303 \times 0.1 = 0.2303$

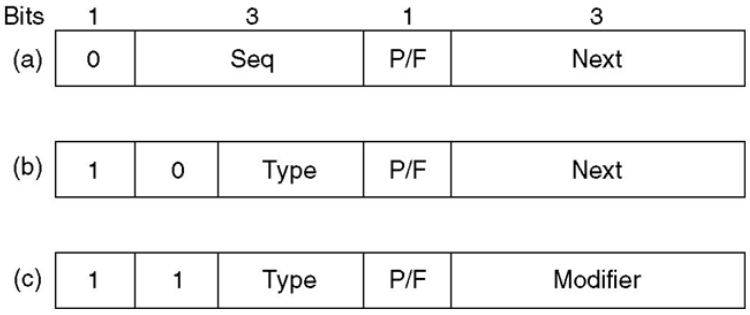
(iii If G > 1, then the channel is said to be overloaded, since G = 2.303, the channel is overloaded.

Q.4 a. With neat format explain HDLC protocol. (6)

Answer:



- Address field: used to identify one of the terminals
- Control field: Used for sequence numbers, acknowledgement and other purpose
- Data Field: Contain any information
- Checksum field: Uses CRC



Control field of
(a) An information frame.(b) A supervisory frame. (c) An unnumbered frame

- The protocol uses a sliding window, with 3 bit sequence number. Up to 7 unacknowledged frames may be outstanding at a time.
- The next field is piggybacked acknowledgement.
- P/F: Poll/Final

All the frames send by the terminal, except the final one, have P/F bit set to P, the final one is set to F.

b. Briefly explain Markov chain model and explain M/G/1 queues (6)

Answer:

Markov chain:-

A **Markov chain** is a discrete random process with the property that the next state depends only on the current state. It is a mathematical tool for statistical modeling in modern applied mathematics, particularly information sciences.

A Markov chain is a discrete random process with the Markov property that goes on forever. A discrete random process means a system which is in a certain state at each "step", with the state changing randomly between steps. The steps are often thought of as time but they can equally well refer to physical distance or any other discrete measurement; formally, the steps are just the integers or natural numbers, and the random process is a mapping of these to states. The Markov property states that the conditional probability distribution for the system at the next step (and in fact at all future steps) *given* its current state depends only on the current state of the system, and not additionally on the state of the system at previous steps:

$$P(X_{n+1}|X_1, X_2, \ldots, X_n) = P(X_{n+1}|X_n).$$

Since the system changes randomly, it is generally impossible to predict the exact state of the system in the future. However, the statistical properties of the system's future can be predicted. In many applications it is these statistical properties that are important.

M/G/1 Queue:-

The M/G/1 queue has exponentially distributed interarrival times and an arbitrary distribution for service times. The increase in generality compared to the M/M/1 queue comes with a price: the M/G/1 queue does not have a general, closed form distribution for the number of jobs in the queue in steady state. It does, however, admit a general solution for the *average* number of jobs in the queue, and application of Little's Theorem provides the corresponding result for the average time spent in the queue. Collectively, these results are known as the *Pollaczek-Khinchin* mean value formulae.

The following derivation of the Pollaczek-Khinchin mean value formulae for the M/G/1 queue assumes FCFS scheduling, to simplify the analysis. However, the formulae are valid for any scheduling discipline in which

1. the server is busy if the queue is non-empty,
2. no job departs the queue before completing service, and

the order of service is not dependent on knowledge about job service times

c. Suppose that a group of 10 stations is serviced by an Ethernet LAN. How much bandwidth is available to each station if
(i) the 10 stations are connected to a 10 Mbps Ethernet hub;
(ii) the 10 stations are connected to a 100 Mbps Ethernet hub;
(iii) the 10 stations are connected to a 10 Mbps Ethernet switch. (6)

Answer:

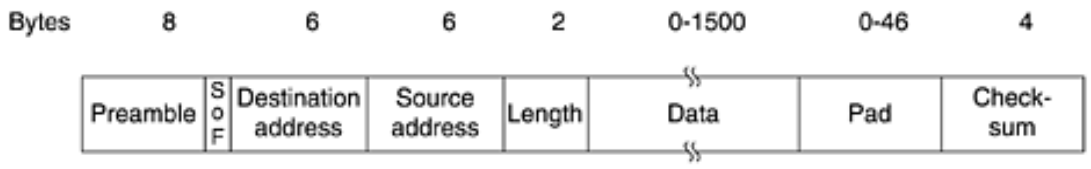
(i). Assuming essentially 100% efficiency, the 10 Mbps are shared equally by the 10 stations, so each station can receive a maximum of 1 Mbps on average.

(ii). Assuming essentially 100% efficiency, the 100 Mbps are shared equally by the 10 stations, so each station receives a maximum of 10 Mbps on average.

(iii). The bit rate available to each station depends on the number of collision domains that are configured in the switch. In the best case, each station has nearly 10 Mbps to the Ethernet switch. Each station will have full access to the 10 Mbps if the switch capacity can handle the aggregate rate from all the stations.

Q.5 a. Explain with neat format IEEE 802.3 protocol. (7)

Answer:



Preamble. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.

Start frame delimiter (SFD). The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address

Destination addresses (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet

Source addresses (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet.

Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

CRC. The last field contains error detection information

b. Give the comparisons between circuit switching and datagram. (7)

Answer:
The comparisons are

Factors	**Circuit Switching**	**Datagram**
Path	Dedicated transmission path	No dedicated path
Data type	Continuous transmission data	Transmission of packets
Speed	Only path set up time is required	path set up time is not required
Storage of data	Message are not stored	Packets may be stored until delivered.
Routing	The same path is establishes for entire conversation	Each packet is routed independently.

c. T1 carrier has a channel capacity of 1.544X106 bits / sec. If 3000 km long T1 trunk is used to transmit 64 byte frames using Go – back – N protocol. How many bits the sequence number should be if the propagation speed is 6μs/km. (4)

Answer:

The propagation delay for 3000 km is: $3000 \times 6\mu = 18 \times 10^{-3} = 18ms$

Two way delay = 18X2 = 36 ms

Time taken for the frame to be transmitted $= \frac{64 \times 8}{1.544 \times 10^6} = 0.33ms$

Total time taken = 0.33 + 18 + 18 = 36.33 ms

(two way delay for frame +acknowledgement)

36.33 ms is required to transmit a frame.

Q.6 a. With neat diagram explain IPv4 header format. (10)

Answer:

|<---------- 32 bits----------→

Version	IHL	Type of service	Total length			
Identification				DF	MF	Fragment offest
Time to live		Protocol	Header checksum			
Source address						
Destination address						
Option						

Fig: IP-4 header format

Figure shows the IP-4 header format. The IP header is built up in blocks of 32 bits. It will always be an integral number of 32-bit words. The IP header is divided up into fields.

The ***version field*** is 4 bits long. It indicates the release version of the IP that is used in this datagram.

The ***header length***[IHL] field is 4 bits long. It identifies the length of the IP header in multiples of 32. The minimum value for a valid header is 5 (means 5*32Bit = 20 Bytes), Maximum is 15 (means 15*32Bit = 60 Bytes).

The ***Service Type*** *TOS (Type of Service)* Specifies the parameters for the type of service requested. The parameters may be utilized by networks to define the handling of the datagram during transport.

Total length. 16 *bits* contains the length of the datagram**.**

Identification: This field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same identification value.

DF: This flag indicates whether fragmentation is allowed or not. It is called the ***don't fragment (DF)*** bit. If the flag is set to 1 fragmentation is not allowed, and if it is set to 0 fragmentation is allowed. If the flag is set to 1, datagrams will be lost if they have to cross networks that can only handle smaller datagrams than the one presented to it. For this reason, it is prudent to set the flag to 0 and allow fragmentation.

MF: This flag is called the ***more fragments (MF)*** bit. It is used to indicate that there are more fragments to follow, so if a datagram is fragmented this is set on all but the last fragment. In the fragmentation process the header information in the original datagram must be copied into each of the fragments.

The ***fragment offset*** field is 13 bits long and is used to indicate the relative position of the fragment to the original datagram when fragmentation is carried out

This is a 13-bit field, so offsets are calculated in units of 8 bytes, corresponding to the maximum packet length of 65,535 bytes. Using the identification number to indicate which message a receiving datagram belongs to, the IP layer on a receiving machine can then use the fragment offset to reassemble the entire message.

The ***TTL field*** indicates the "time to live" for the datagram. This field is used to limit packet lifetime. When it becomes zero, the packet is destroyed. The unit of time is second, allowing maximum lifetime of 255 sec.

The ***protocol field*** is 8 bits long and is used to identify the upper layer protocol that is to receive the IP data portion of the datagram. Higher- level protocol that provide data.

Source and destination address: The address is of 32 bits, which indicated both network address and host address. As the *Internet address* gets you to the correct host. The protocol identifier gets you to the correct service within the host.

The ***header checksum*** is 16 bits long. It holds the error check result for the entire header, which includes options, if they are present .

The ***option field*** is used for security, source routing, error reporting, debugging, time stamping and other information.

b. Compare IPv4 and IPv6 protocol (4)

Answer:

Subjects	IPv4	IPv6
Address Space	32 bit address	128 bit address
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast
Any cast support	Not part of the original protocol	Explicit support of anycast
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility

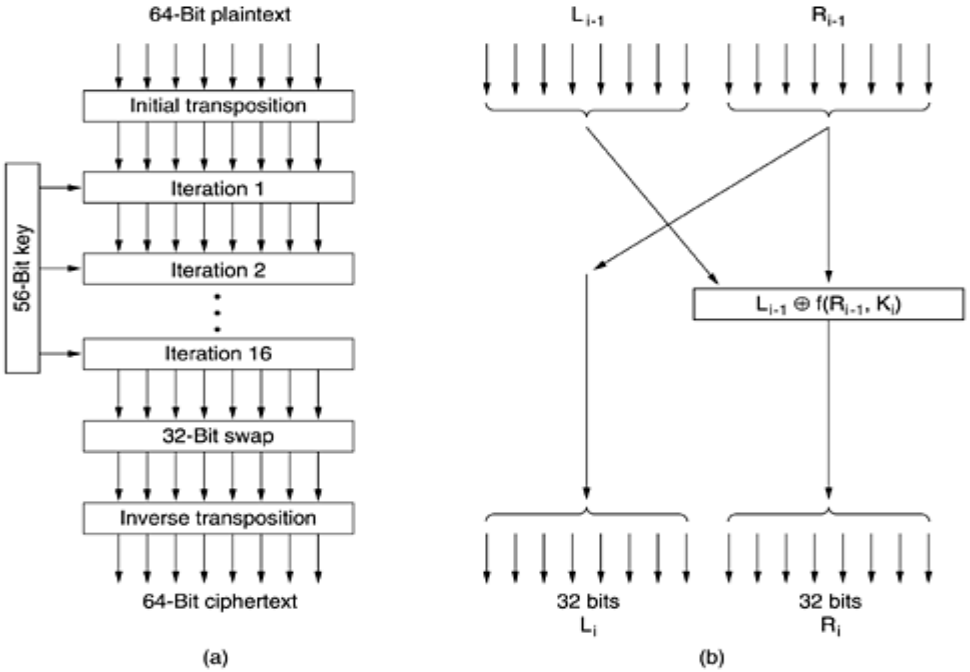
c. Mention the type of address for the following IP address
(i) 126.33.44.56
(ii) 195.55.23.96
(iii) 132.133.134.136
(iv) 251.252.253.259 **(4)**

Answer:
The type of address for the following IP address

126.33.44.56	Class A
195.55.23.96	Class C
132.133.134.136	Class B
151.252.253.250	Class B

Q.7 a. With neat diagram explain DES encryption algorithm. **(10)**

Answer:

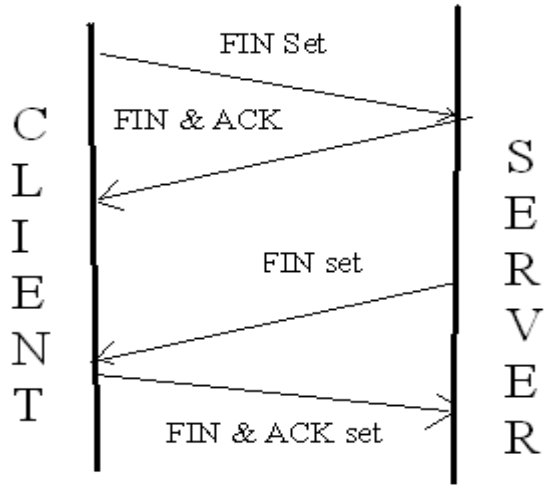


- DES is the Most widely-used secret key system and Efficient hardware implementation
- **Encryption**: Electronic Codebook (ECB) Mode
  - Message broken into 64-bit blocks
  - Each 64-bit plaintext block encrypted separtely into 64-bit cyphertext
  - Original version of DES uses a 56-bit key
- **Decryption:** Encryption operations performed in reverse order
- Initial permutation is independent of key
- Final permutation is inverse of initial permutation
- Penultimate step swaps 32-bits on left with 32-bits on the right
- Intermediate 16 iterations apply a different key that is derived from the original 56-bit key. 64-bit block divided into L_{i-1} and R_{i-1} halves
- Left output $L_i = R_{i-1}$, Right output $R_i = L_{i-1}$ XOR $f(R_{i-1}, K_i)$
- bitwise XOR $f(.,.)$ as follows:

- R_{i-1} expanded to 48 bits using fixed re-ordering & duplication pattern XORed with K_i Each resulting group of 6-bits is mapped into 4-bit output according to substitution mapping

b. With neat diagram explain how the connection will be released in a TCP. (8)

Answer:



When a TCP connection has to be released either client or server can initiate the release. The connection can be thought of as 2 connections from each of server and client.

One connection at the client can be thought of as for sending data from client to server and the other for receiving data from server to client.

This data transfer takes place concurrently. The server also could be visualized to have 2 half duplex connections, one for receiving and one for sending. So when a connection is released each of these 2 half duplex connections must be individually released.

For example as shown the client sends a release request with FIN bit in tcp header set. The server acknowledges back with a segment with both FIN and ACK bits set closing the connection which receives from client. The client on receipt releases the client send connection.

The server then flushes out any data it needs to send to the client and then sends a segment with FIN bit set requesting for a release of its send connection.

The client replies back with a segment with both Fin and ACK bits set in the tcp header , releasing the server send and the client receive connection.

The connection port numbers will not be reused for some time proportionate to the network delay to prevent fresh connections from interfering with old connections which are being closed.

TEXT BOOK

I. Leon Garcia and Indra Widjaja, Communication Networks: Fundamental Concepts and Key Architecture, 2nd ed., Tata McGraw-Hill, 2004