Name:
Roll No:

CN Assignment-2

Q1) What is logical addressing? Explain IPV4 classful and classless addressing?

Logical Addressing :-

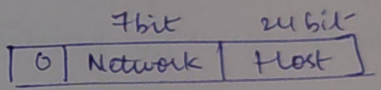
It is also refered to as IP address. This address facilitates universal communication that are not dependent on the underlying physical networks.

Classful addressing :-

The 32-bit IP addres is divided into five sub-classes. There are

- **class A**

IP addresses belonging to class-A are assigned to the networks that contain a large number of hosts.



Network ID – 8 bits host ID – 24 bits

The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine ID.

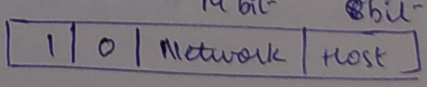
24 bits used to determine the host in any N/w

- **Class B**

IP address belonging to class B is assigned to N/w's that range from medium-sized to large-sized N/w's.

Network ID – 16 bits

Host ID – 16 bits

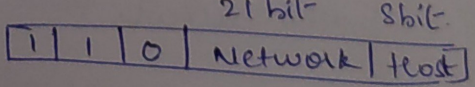


- **Class C**

IP addresses belonging to class C are assigned to small-sized Networks

Network ID – 24 bits

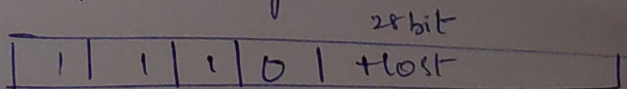
Host ID – 8 bits



- **Class D**

IP address belonging to class D is reserved for multi-casting.

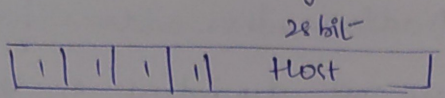
It does not possess any subnet mask



• Class E

IP addresses belonging to class E are reserved for experimental and research purposes.

This class doesn't have any subnet mask.



Classless Addressing

It is a method of IP address that allows for more flexible allocation of IP addresses than the traditional class-based addressing (class A, B, C)

In CIDR, IP addresses are represented in the form of a prefix followed by a slash and a number, indicating number of bits used for N/w position.

This enables efficient use of IP addresses and better allocation of address space, especially in context of internet routing.

Addres Depletion :-

It is designed to overcome address depletion and give more organization access to internet.

In this schema there are are not classes but addresses are still granted in blocks

The size of block varies based on ~~[illegible]~~ nature & size of organization

Q2) Explain in detail about IPV4 header format.

Q3) Compare TCP and UDP Protocols.

TCP

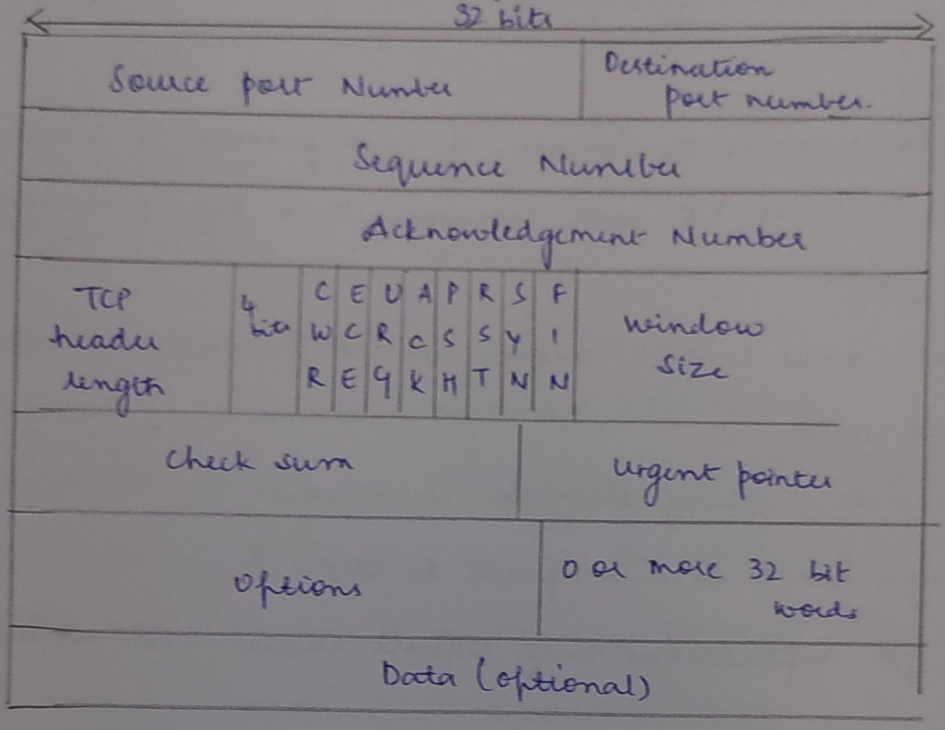
- Connection-oriented protocol. It establishes a reliable and full-duplex connection before data transfer.
- Reliable and ensures the delivery of data. It uses mechanisms like acknowledgement, retransmission and flow control to achieve reliability.
- Guarantees the order of delivery of data packets. If packets arrive out of order, TCP will rearrange them before delivering to application layer
- Implements flow control mechanism to prevent overwhelming the receiver with data.
- Performs error checking through checksums.
- Has a larger header size compared to UDP.
- Suitable for applications that require reliable and accurate data delivery
- Three-way handshake is used to establish a connection.
- HTTP, HTTPS, FTP, Telnet etc.

UDP

- Connectionless protocol
- Unreliable in terms of data delivery
- Doesn't guarantee the order of delivery.
- No inherent flow control mechanism
- UDP uses checksums for error detection, but it doesn't request retransmission.
- Has a smaller header size
- Suitable for real-time applications.
- No connection setup is required.
- DNS, DHCP, SNMP etc

Q4) Discuss in detail about TCP Segment header.

Every TCP segment consists of a 20 byte mixed format header. Header options may follow the fixed header. With a header so that it can tag up to 65535 data bytes.



Source Port

It is a 16-bit source port number used by the receiver to reply

Destination Port - 16 bit destination port no.

Sequence Number - SN of 1st data byte in this segment.

Acknowledgement Number - If the ACK control bit is set, this field contains the next number that the receiver expects to receive.

~~Data offset~~-

URG - It indicates an urgent pointer field that data type is urgent or not

ACK - It indicates that the acknowledgement field in a segment is significantly

PUSH - It is set or reset according to a data type i.e sent immediately or not.

RST - resets the connec?.

SYN - synchronizes the sequence number.

FIN- This indicate no more data from the sender.

window- It is used in Acknowledgement segment.

checksum- It is used for error detection

Options- The IP datagram options provide additional punctuality. It can use several optional parameters between a TCP sender & receiver.

Data- This field, connected with the TCP header fields, constitute a TCP segment.

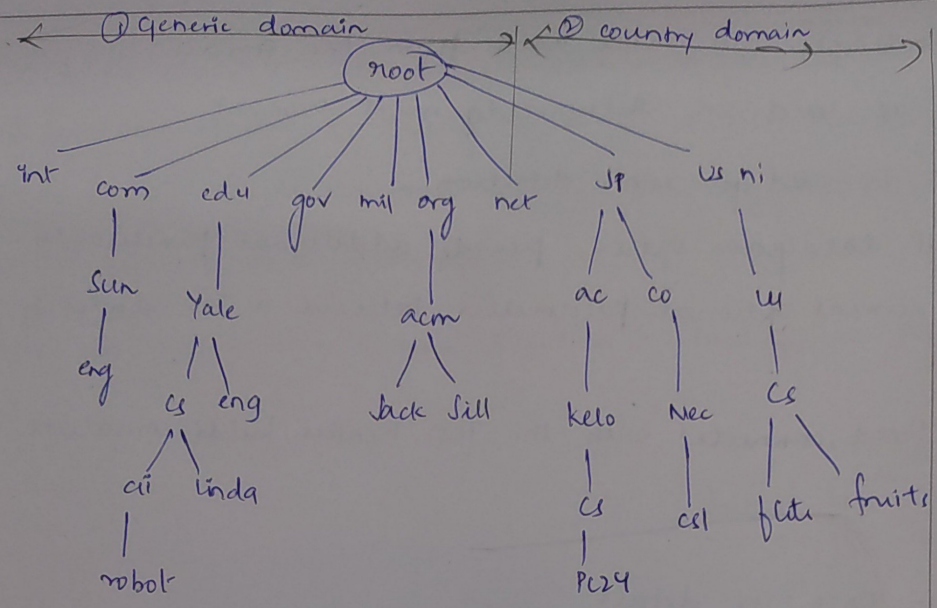
Qs) Write about DNS in detail.

The N/w only understands numerical addresses, so some mechanism is required to convert the ASCII string to N/w addres. To solve this DNS was invented, it is used to map the ASCII string to N/w addres. To map the name on to IP Application program calls a library procedure called "resolver" passing it the name of the parameter.

DNS Namespace

Managing a large constantly changing set of names is a non-trivial problems. To solve this DNS uses hierarchical addressing The internet is divided into over 200 top level domains, each domain covers many hosts, each domain partitioned into sub-domain and these are further partitioned and so on. All these domains can be represented by a tree.

It has 128 levels, uses labels, domain names.



Q6) Write in detail about ICMP Protocol.

Internet control Message Protocol is a N/w Layer protocol used to diagnose communication errors by performing an error control mechanism. IP depends on ICMP to provide error control.

It is a supporting protocol & is used by N/w devices.

ICMP Packet Format:

Type (8 bit)	Code (8 bit)	CheckSum (16 bit)
Extended Header (32 bit)		
Data / Payload (Variable length)		

Uses of ICMP:-

ICMP is used for error reporting if 2 devices connect over the internet and some error occurs. So, the router sends an ICMP error message to the source informing about the error.

Another important use of is used to perform network diagnosis by making use of traceroute & ping utility.

Working:-

The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol.

FIN- This indicates no more data from the sender.

window - It is used in Acknowledgement segment.

checksum - It is used for error detection

Options - The IP datagram options provide additional punctuality. It can use several optional parameters between a TCP sender & receiver.

Data - This field, connected with the TCP header fields, constitute a TCP segment.

Q5) Write about DNS in detail.

The N/w only understands numerical addresses, so some mechanism is required to convert the ASCII string to N/w address. To solve this DNS was invented, it is used to map the ASCII string to N/w address. To map the name on to IP Application program calls a library procedure called "resolver" passing it the name of the parameter.

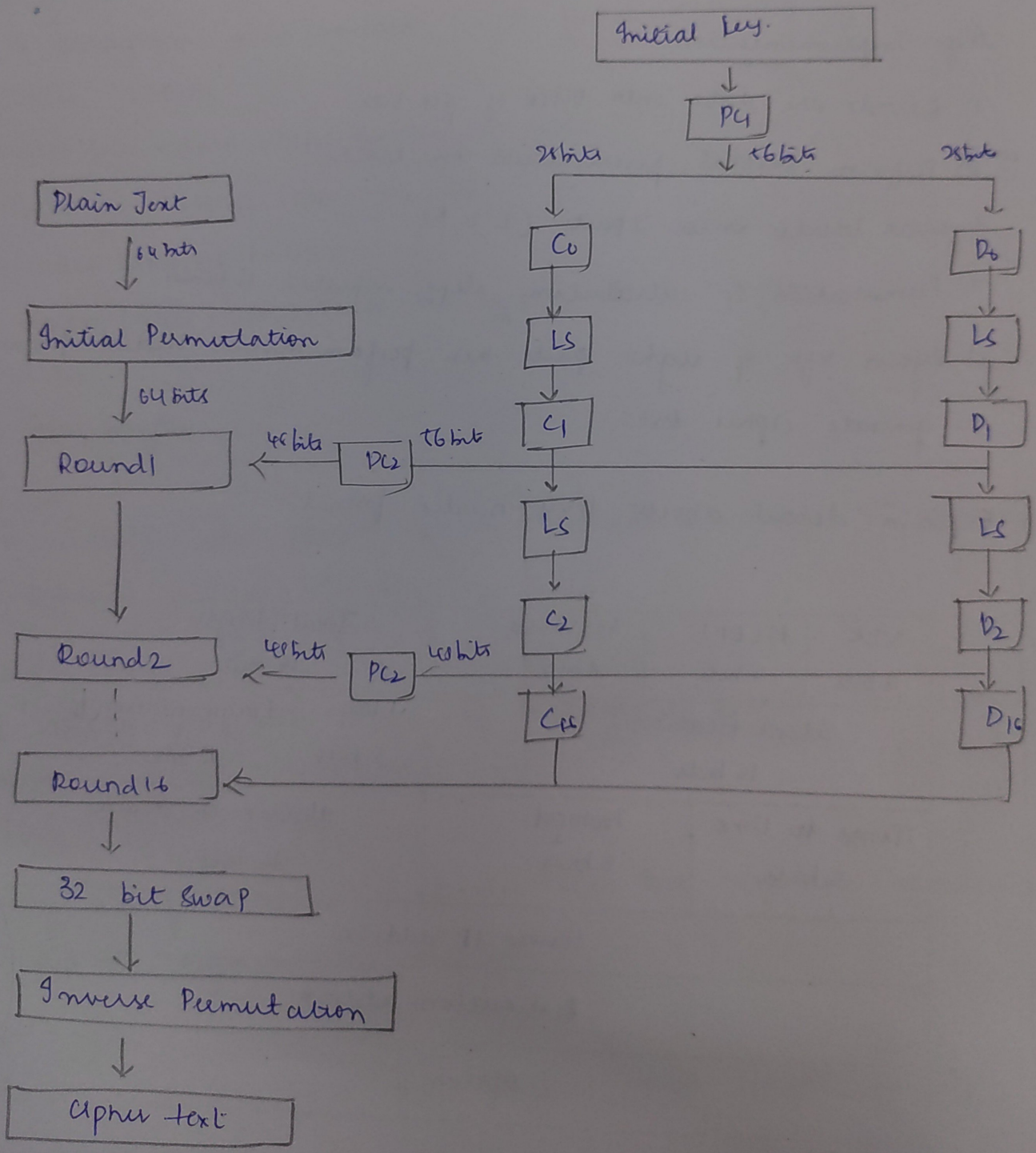
DNS Namespace

Managing a large constantly changing set of names is a non-trivial problems. To solve this DNS uses hierarchical addressing The internet is divided into over 200 top level domains, each domain covers many hosts, each domain partitioned into sub-domain and these are further partitioned and so on. All these domains can be represented by a tree.

It has 128 levels, uses labels, domain names.

Whenever a connection is established before the message sending, both devices must be ready through a TCP Handshake. ICMP packets are transmitted in the form of datagrams that contain an IP header with ICMP data.

Q7) Write in detail about how symmetric encryption algorithm DES works.



Des is a symmetric encryption Algorithm which involves encrypting carrying out combinations, substitutions and permutations. It is a block ciphering technique where

block-size = 64 bits No. of round = 16

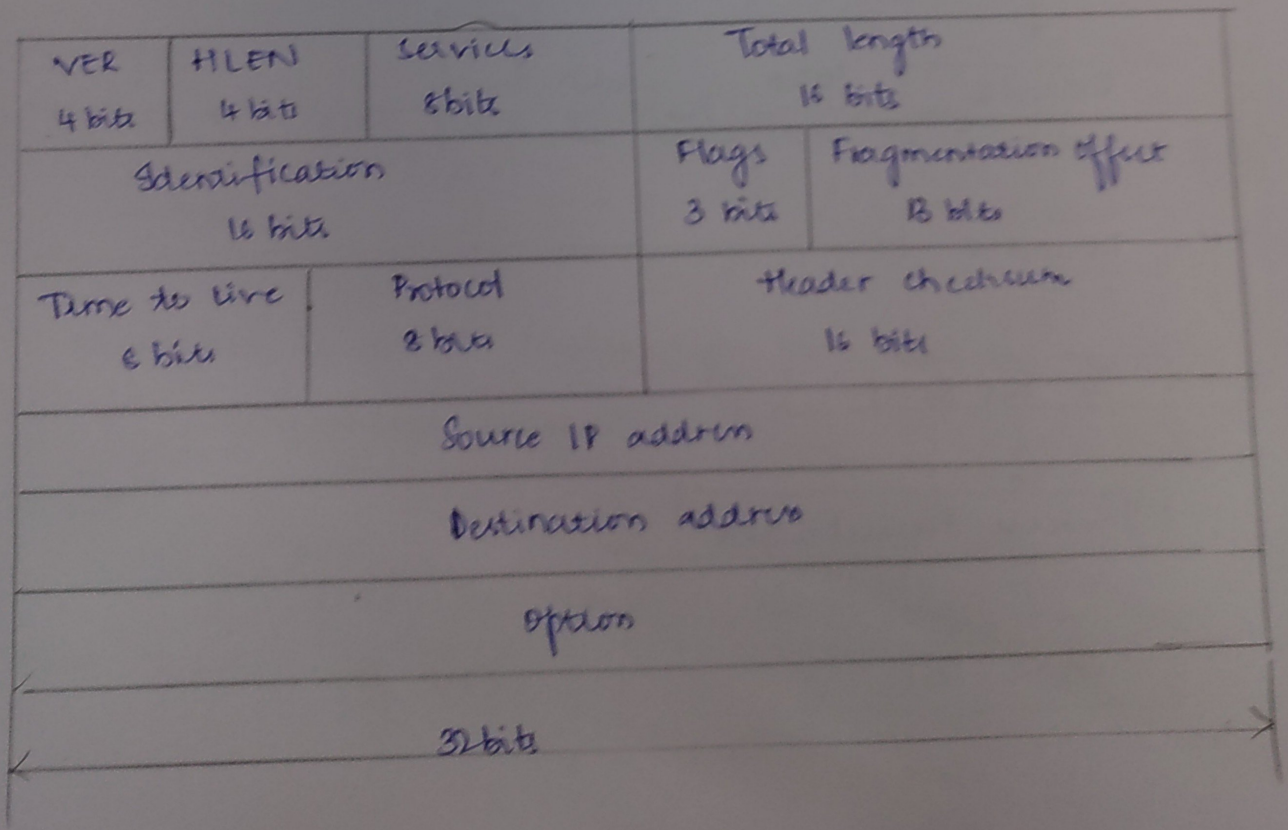
key size = 64 bits

16 sub keys are generated from K_1 to K_{16} which are used for 16 rounds.

Algo Implementation:

1) Divide the data into block of 64 bits
2) Perform initial permutation on blocks
3) Break blocks into 2 parts (L & R)
4) Permutation & substitutions steps repeated 16 times
5) Rejoin left & right parts then perform inverse initial permutation to generate cipher text.

Q2) Explain detail about IPv4 header format.



→ Header can extend upto 64 bytes.

→ IPV4 delivery mechanism is used in TCP/IP protocols.

→ It is an unreliable and connectionless datagram protocol.

→ If reliability is important IPV4 must be paired with reliable protocol such as TCP.

Packets in IPV4 are datagrams

Datagram

A datagram is a variable length packet consisting of 2 parts

1) Header 2) Data.

Packet size + data - header = size of data.

Header is divided into 4 sections

1) Header LENGTH (4 bits)

2) Version (4 bits - 0100). Each bit equivalent to 4 bytes

3) Service

4) Total length

Version

It identifies the version of the protocol. Currently 4th version of Internet protocol is using.

Header length

It defines the total length of datagram header in 4 byte words.

Service

Prvsly this field is called service type but now the name changed to 'differentiated services'.

Total length

It is a 16 bit field that defines total length of IPV4 data gram interms of bytes.