INSWA

Assignment - I

IS12401160001
Vishwas Acharya

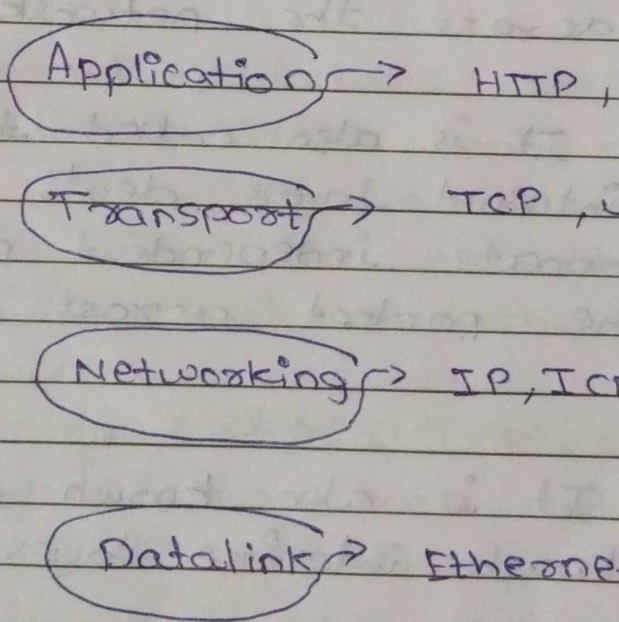
Page No.: 1
Date: / /

1) Explain TCP/IP model in detail with protocals.

Ans. TCP/IP stands for Transmission Control Protocal/ Internet Protocal.

- TCP is the component that collects and reassembles the packets of data, while
- IP is responsible for making sure the packets are sent to the right destination
- It was developed in the 1970s and adopted as the protocol standard for ARPANET in 1983.

- Figure



- TCP/IP uses the client-server model of communication in which a user or machine (a client) is provided a service, like sending a webpage, by another computer in the network

- Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests.
- Being stateless frees up network paths so they can be used continuously.

1) Application layer :- It provides applications with standardized data exchange.

2) Transport layer :- It is responsible for maintaining end-to-end communications across the network.

3) Network layer :- It is also called the internal layer, deals with packets and connects independent networks to transport the packet across network boundaries

4) Physical layer :- It is also known as the network interface layer or data link layer.

2) Write notes on IP addressing schemes giving one example of each.

- TCP/IP includes an Internet addressing scheme that allows users and applications to identify a specific network or host with with to communicate.

- An Internet address works like a postal address, allowing data to be routed to the chosen destination.

- TCP/IP provides standards for assigning addresses to networks, subnetworks, hosts, and sockets, and for using special addresses for broadcasts and local loopback.

- Internet addresses are made up of a network address and a host address. This two-part addresse allows a sender to specify the network as well as a specific host on the network.

- A unique, official network address is assigned to each network when it connects to other Internet networks.

- Internet addressing scheme consists of Internet Protocol (IP) addresses and two special cases of IP addresses:

broadcast addresses and loopback addresse

- Internet addresses
  ↳ The IP uses a 32-bit, two-part addres field.
-
- Subnet addresses
  ↳ Subnet addressing allows an autonomus system made up of multiple network to share the same Internet address.

- Broadcast addresses
  ↳ The TCP/IP can send data to all hosts on a local network or to all hosts on all directly connect networks.

- Local loopback addresses
  ↳ The IP defines the special networ address, 127.0.0.1, as a local loopback address.

3) Discuss TCP or UDP Frame format.

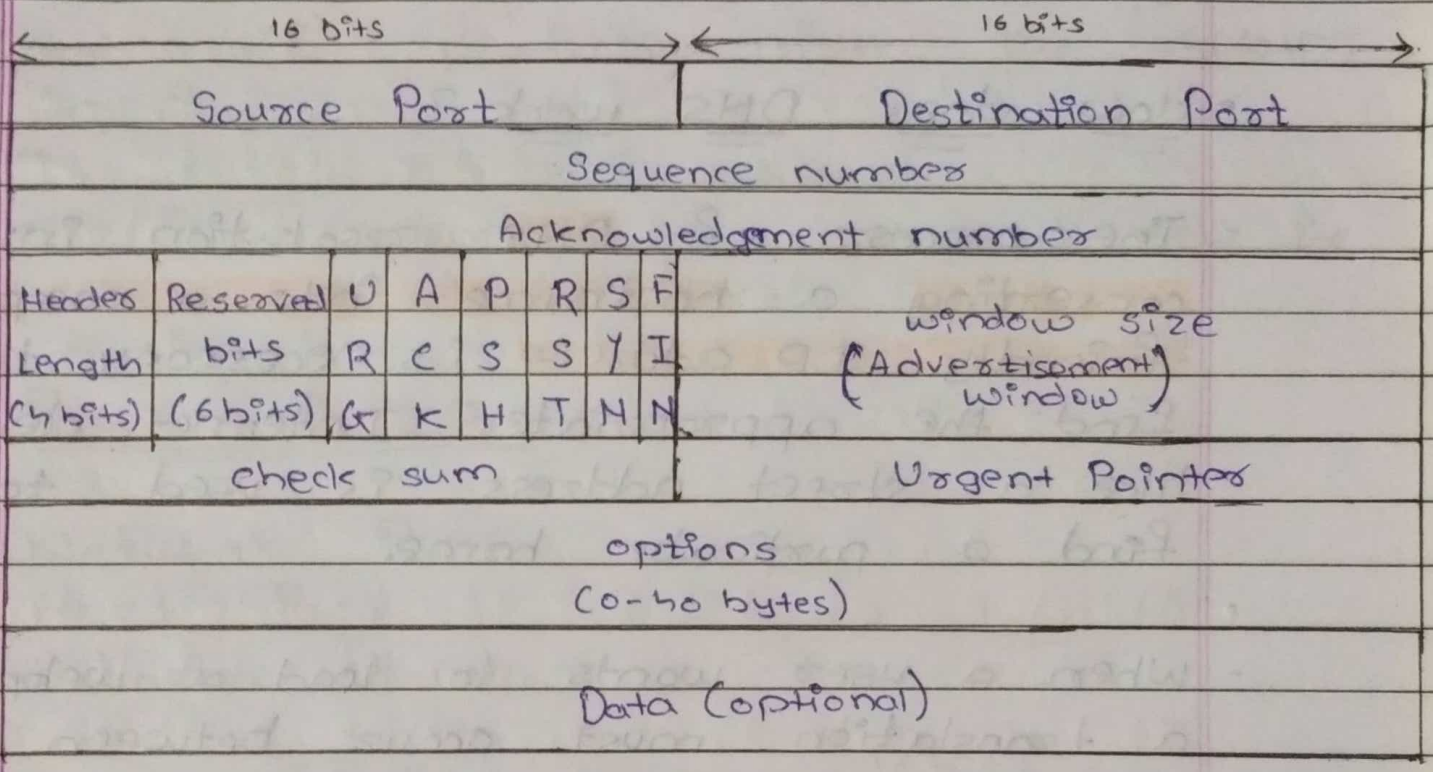
Ans. TCP/UDP is a transport layer protocol. It continuously receives data from th application layer. It divides the data into chunks where each chunk is a collection of bytes.

- It then creates TCP segments by adding a TCP header to the data chunks. TCP segments are encapsulated in

the IP datagram.

- Figure:

TCP header format



4) Describe DNS.

Ans - The Domain Name System (DNS) is the phonebook of the Internet.
- Humans access information online through domain names, like nytimes.com or espn.com
- Web browsers interact through Internet Protocol (IP) addresses
- DNS translates domain names to IP addresses so browsers can load Internet resources.
- Each device connected to the Internet has a unique IP address which other machines

use to find the device.

- DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1, or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2

- How does DNS work?

- The process of DNS resolution involves converting a hostname into a computer-friendly IP address is necessary to find the appropriate Internet device- like a street address is used to find a particular home.

- When a user wants to load a webpage, a translation must occur between what a user types into their web browser and the machine-friendly address necessary to locate the example.com webpage.

- In order to understand the process behind the DNS resolution, it's important to learn about the different hardware components a DNS query must pass between.

- For the web browser, the DNS lookup occurs "behind the scens" and requires no interaction from the user's compute

apart from the initial request

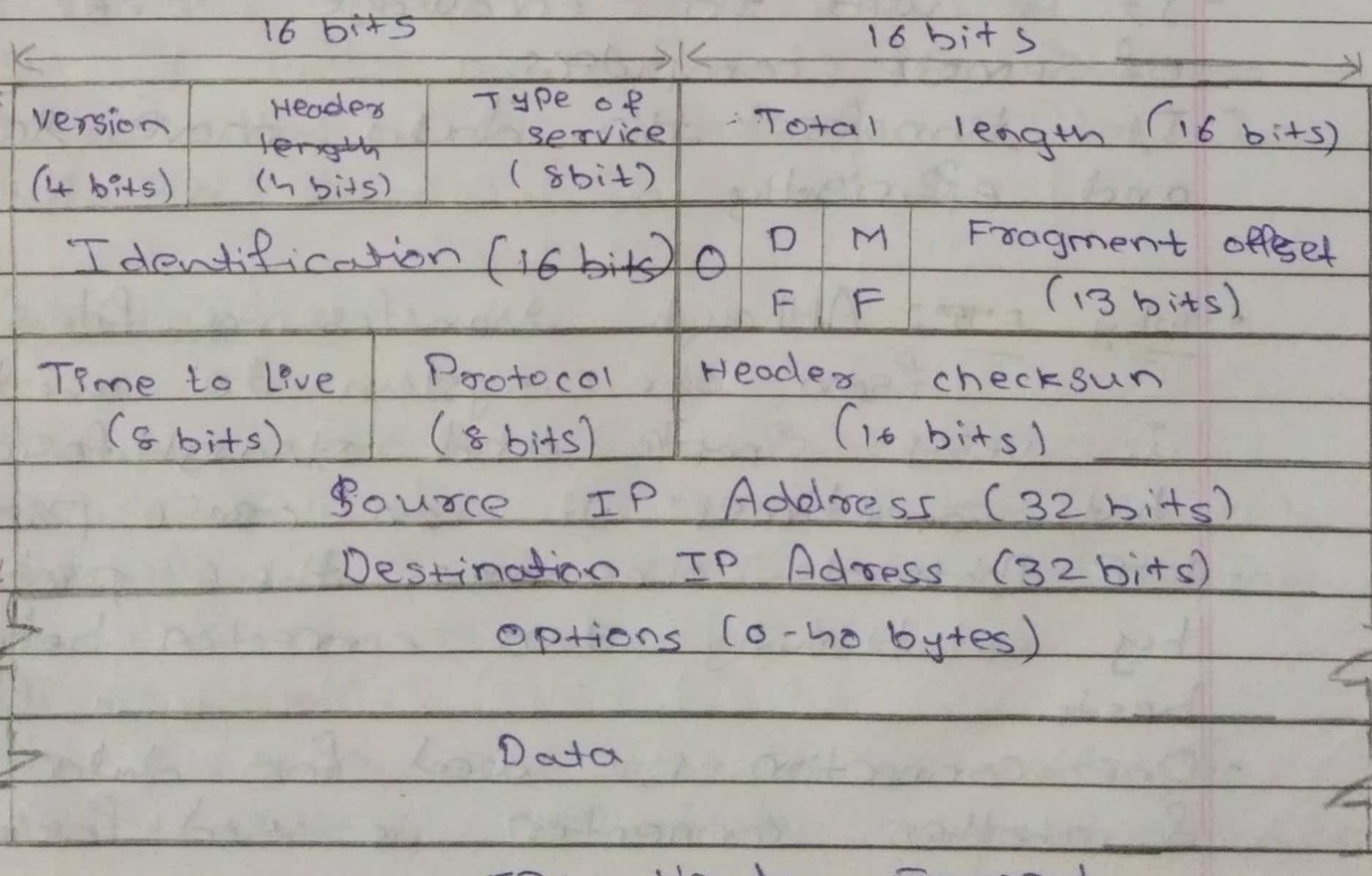
5) Draw IPv4 header format.

Ans IP stands for Internet protocol & v4 stands for Version Four (IPv4).

- It was the primary version brought into action for production with the ARPANET in 1983.
- It is 32-bit IP address
- It is a connectionless protocol used for packet-switched networks.

- Parts of IPv4 :-

1) Network Part
2) Host Part
3) Subnet number:



IPv4 Header Format

6 Explain FTP

Ans FTP stands for File Transfer Protocol.
- It is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other severs.

- Objectives of FTP: It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfer the data move reliably and efficiently

- Why FTP: Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems.
- FTP Protocols overcomes these problems by establishing two connection between hosts.
- One connection is used for data transfer & another connection is used for the

control connection

- Type of FTP Connections:-

1) Active 2) Passive

OR

1) Control 2) Data

- FTP transfer files using any of the following modes:

1) Stream mode
2) Block mode
3) Compressed mode

- Applications of FTP: It is used by IT companies to provide backup files at disaster recovery sites.
- It is used by different big business organizations for transferring files in between them.

- Advantages:-

- Multiple transfers → simple
- Efficiency → speed
- Security → Continuous transfer

- Disadvantages:-

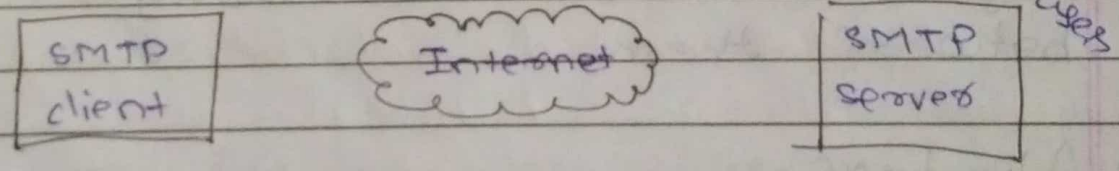
- less security - virus - memory & programming
- old technology - limited

7) Explain the working of electronic mail protocol. SMTP, IMAP & POP3 in brief with suitable diagram.

- E-mail protocols are set of rules that help the client to properly transmit the information to or from the mail servers.
- E-mail working follows the client servers approach. In this client is the mailer i.e the mail application or mail program and servers is a device that manages emails.

- **SMTP: Simple Mail Transfer Protocol**

- SMTP is a set of communication guidel that allow software to transmit an electronic mail over the internet is called simple mail transfer Protocol.



→ Working of SMTP:-

(i) Composition of Mail:- A user sends an email by composing an electronic mail message using a Mail user Agent (MUA). It is a progra which is used to send & receive mail.

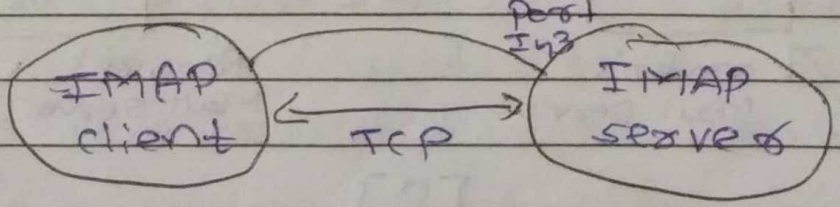
(ii) Submission of Mail: After composting an email, the mail client then submits the completed e-mail to the SMTP servers by using SMTP on TCP port 25.

(iii) Delivery of Mail :- E-mail addresses contain two parts : username of the recipient and domain name.

(iv) Receipt & Processing of Mail: Once the incoming message is received, the exchange severs delivers it to the incoming severs (Mail Delivery Aget) which stores the e-mail where it waits for user to retrieve it.

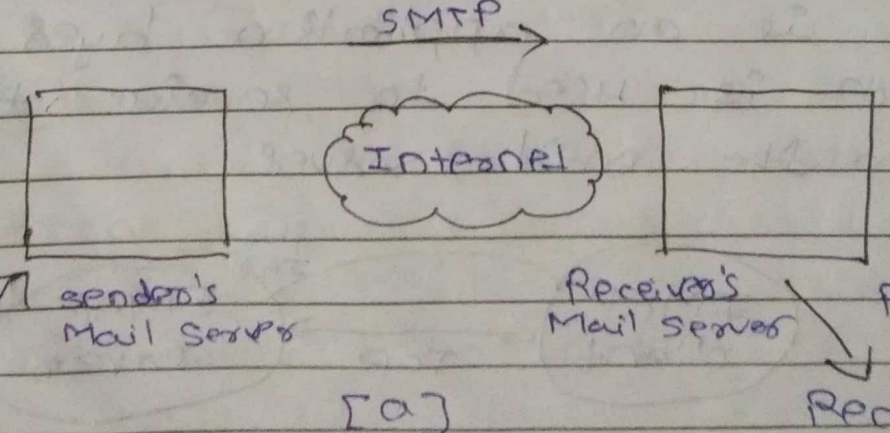
(v) Access & Retrieval of Mail: The stored email in MDA can be retrieved by using MDA. It can be accessed by using login & password.

- IMAP :- Stands for Internet Message Access Protocol
- It is an application layer Protocol which is used to receive the emails from the mail server.



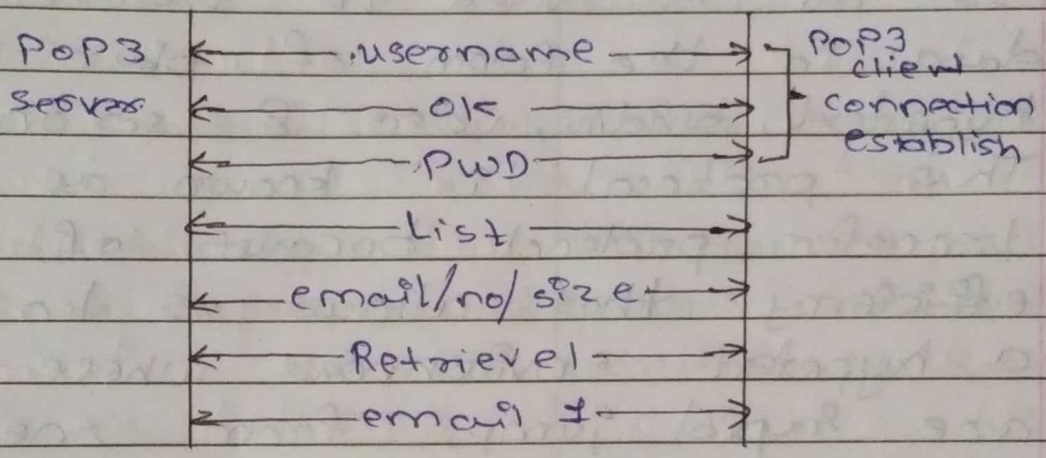
→ Working of IMAP:- It follows client-server architecture & is the most commonly used email protocol
- It is a combination of client & server process running on other computers that are connected through a network
- This protocol resides over the TCP/IP protocol for communication.
- Once the communication is set up the server listens on port 143 by default which is non-encrypted.
- For the secure encrypted communication port, 993 is used.

• POP3:- Post Office Protocol or Point of Presence.
- The POP3 is a simple protocol & having very limited functionalities.
- In the case of the POP3 Protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server.



[a]

- **Working:-** POP's working is based on it's five important equipment which are
1) Base Stations
2) Client equipment
3) Network Switches
4) Routers
5) Firewall



[b]

- To establish the connection between the POP3 server & POP3 client, the POP3 server asks for the user name to the POP3 Client.
- If the username is found in the POP3 server, then it sends the OK message.
- It then asks for the password from the POP3 Client; then the POP3 client sends the password to the POP3 server.
- If the password is matched, then the POP3 server sends the OK message, & the connection gets established.

8) What is HTTP? Differentiate its pessistent & non-pessistent types with the sequest & response behaviour of HTTP.

Ans HTTP stands for HyperText Transfer Protocol.

- It is a Protocol used to access the data on the World wide Web (www)
- It can be used to transfer, the data in the form of plain text, hypertext, audio, video & so on.
- This protocol is known as Hypertext transfer protocol because of its efficiency that allows us to use in a hypetext environment where there are rapid jumps from one document to another document.
- Communication between client computers & web severs is done by sending HTTP requests & receiving HTTP responses.
- Communication between clients & severs is done by sequests & responses

1) A client sends an HTTP request to the web.
2) A web server recives the quest
3) The severs runs an application to proc the request
4) The severs returns an HTTP response to the browser

5) The client receives the response.

Persistent HTTP	Non-Persistent HTTP
1) The server leaves the TCP connection open after sending response	1) It is one that is closed after the server sends the requested object to the client.
2) Default mode is HTTP/1.1	2) Default mode is HTTP/1.0
3) It has two types: pipelined & non-pipelined	3) It has 2 types with parallel connection & without parallel connection
4) It requires 2 TT for connection establishment	4) It requires 2RTT per object.
5) On same TCP connection server parses request responds, parses new request	5) Server parses request responds & closes TCP connection
6) Fewer RTTs & less slow start	6) Each object transfer suffer from slow start.

9) Explain the concept of DHCP

Ans - DHCP :- Dynamic Host Configuration Protocol.
- It is a network management protocol used on IP networks

- It is used to assign an IP address & other configurations to the connected devices on the network to communicate with others
- DHCP is based on a client - server model & based on discovery, offer, request & Ack
- DHCP port number for server is 67 and for the client is 68.
- DHCP servers allows a system to request IP addresses & other networking parameters automatically from the internet service provider. It reduces the network admin work
- It can be implemented on local network's as well as large enterprise networks.
- It is the default protocol used by the most routers & networking equipment.
- DHCP is also called RFC [Request for Comments] 2131
- It manages the provision of all the nodes or devices added or dropped from the network.
- It maintaines the unique IP address of the host using a DHCP server.
- DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes & to allocate

TCP/IP configuration information to the DHCP clients

- Components of DHCP :-

- DHCP Server :- It is a networked device running the DHCP service that holds IP address & related configuration information.

- DHCP Client :- It is the endpoint that receive configuration information from a DHCP server.

- IP address Pool :- It is the range of addresses that are available to DHCP clients

- Subnet :- It is partitioned segments of the IP networks. It is used to keep networks manageable.

- Lease :- It is the length of time for which a DHCP client holds the IP address information.

- DHCP relay :- A host or routes that listens for client messages being broadcast on that network & then forwards them to a configured server.

- Benefits of DHCP:-

- Dynamic Host configuration
- Seamless IP host configuration
- Flexibity & Scalability
- Centralized administration of IP configuraty

- Advantages of DHCP:-

- Centralized management of IP addresses
- Reduced IP address conflicts.
- Efficient change management.
- Automation of IP address administratin

- Disadvantages of DHCP:-

- IP conflict can occurs.

10. Write a Client sesver program for TCP and UDP connection (Explain Socket Programming with TCP and UDP). Write only program and attached screenshot of output in this.

Ans Socket programming is a way of connecting two nodes on a network to communication with each other.

- Select function is used to select between TCP & UDP sockets. This function gives instruction to the kernel to wait for any of the multiple events to occur & awakes the process only after one

or more events occur or a specified time passes.

- Servers:-

1) Create TCP i.e listening socket
2) Create UDP
3) Bind both socket to the server address
4) Initialize a description set for select and calculate a maximum of 2 descripter for which we will wait.
5) Call select & get the ready descriptor (TCP or UDP)
6) Handle new connection if ready descriptor is of TCP or receive date gram if ready descriptor is UDP

- UDP Client.

1) Create UDP socket
2) Send message to server
3) Wait until response from server is received.
4) Close socket descriptor & exit.

- TCP Client :-

1) Create a TCP Socket
2) Call connect to establish connection with servers
3) When the connection is accepted write

message to server.
4. Read response of server
5. Close socket descriptors & exit.