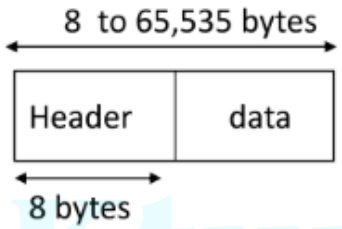
1. What is UDP? Draw and explain UDP Datagram format.

- User Datagram Protocol (UDP) is a Simple Transport Layer protocol,UDP is a part of the Internet Protocol .
- Unlike TCP, it is an unreliable and connectionless protocol.
- UDP provides a way for applications to send encapsulated IP datagrams and send them without having to establish a connection.
- The UDP enables process to process communication.
- A unique characteristics of UDP is that it provides no inherent on many platforms,an application can send unique interface at the line rate on the link interface.
- Does not guaranteed delivery of ordered data and no flow control.
- UDP packets are called user datagram

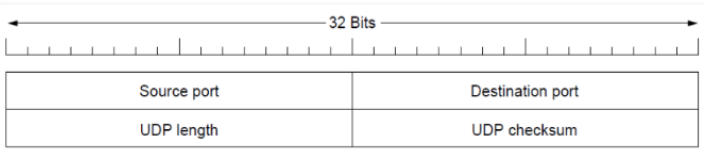


UDP Datagram Format:

- UDP packet consists of header and data
- UDP header is an **8-bytes** fixed and simple header.
- UDP port number fields are each 16 bits and range of port numbers is defined from 0 to 65535.

The UDP header format

8 bytes header consist of
- Source port number
- Destination port number
- UDP Length
- UDP Checksum

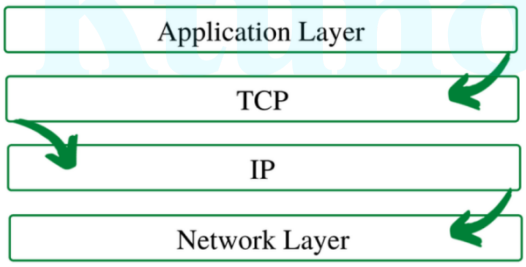


1. **Source Port:** Source Port is a **2 Byte** long field used to identify the port number of the source.
2. **Destination Port:** It is a **2 Byte** long field, used to identify the port of the destined packet.
3. **Length:** It is the length of UDP including the header and the data. It is a **16-bits field.**

4. **Checksum:** Checksum is **2 Bytes** long field. It is to verify that the end to end data is not been corrupted by routers or bridges in the network.the algorithm to compute this is known as the standard checksum algorithm.

2. What is TCP? Draw and explain TCP segment format. Explain TCP connection establishment process

- It is a connection-oriented & reliable protocol for communications that helps in the exchange of messages between different devices over a network.
- It lies between the Application and Network Layers
- It is a full duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.
- It consist flow control mechanism,error checking and recovery of messages.
- TCP also implements a congestion-control mechanism.



TCP/IP Layer

- It provides good quality of services.
- TCP has packets called as **segments**(consists of header and data).
- The segment consist of 20-60 bytes header and the rest of data from application programme.
- TCP provides the following facilities to:

1. **Stream Data Transfer**:From the application's viewpoint, TCP transfers a contiguous stream of

2.Flow Control

Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.

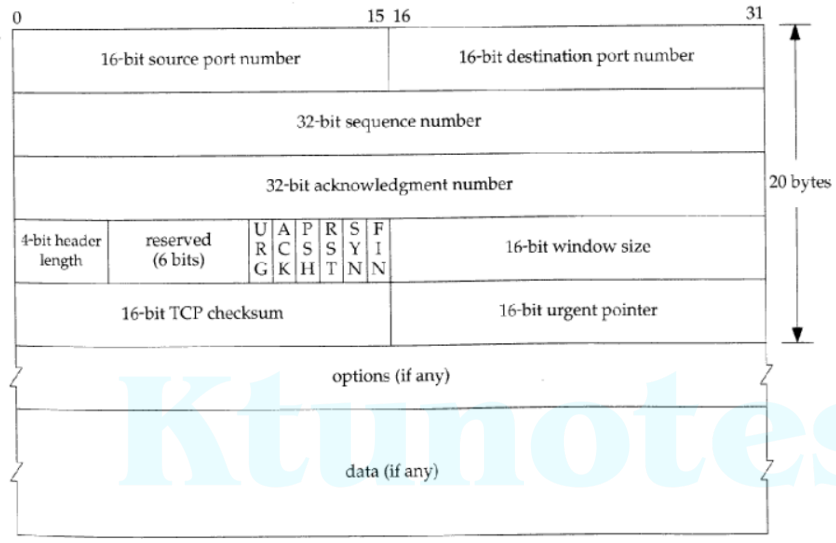
3.Multiplexing

- To allow for many processes within a single host to use TCP communication facilities simultaneously, the TCP provides a set of addresses or ports within each host.
- Whenever an entity accepts items from more than one source, this is

referred to as multiplexing (many to one). • whenever an entity delivers items to more

TCP HEADER FORMAT

TCP data is encapsulated in an IP datagram.



- **Source Port Address –**

  A 16-bit field that holds the port address of the application that is sending the data segment.

- **Destination Port Address –**

  A 16-bit field that holds the port address of the application in the host that is receiving the data segment.

- **Sequence Number –**

  A **32-bit field** that holds the sequence number.. It is used to reassemble the message at the receiving end of the segments that are received out of order.

- **Acknowledgement Number –**

  A **32-bit field** that holds the acknowledgement number, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

- **Header Length (HLEN) –**

  This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header.This is needed because the options field is of variable length.

- **Control flags –**

  These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:

  - URG: Urgent pointer is valid
  - ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)
  - PSH: Request for push
  - RST: Reset the connection
  - SYN: Synchronize sequence numbers
  - FIN: Terminate the connection

- **Window size –**

  This field tells the window size of the sending TCP in bytes.

- **Checksum –**

  This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

- **Urgent pointer –**

  This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

- The TCP in the client then proceeds to establish a TCP connection with the TCP in the server in the following manner

Step1.

- The client-side TCP first sends a special TCP segment to the server-side TCP. This special segment contains no application-layer data.
- But one of the flag bits in the segment's header, the SYN bit, is set to 1.
- For this reason, this special segment is referred to as a SYN segment.
- In addition, the client randomly chooses an initial sequence number (client_isn) and puts this number in the sequence number field of the initial TCP SYN segment.
- This segment is encapsulated within an IP datagram and sent to the server.

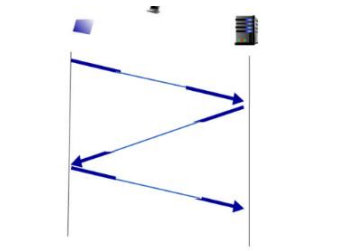
Step2.

- Once the IP datagram containing the TCP SYN segment arrives at the server host, the server extracts the TCP SYN segment from the datagram, allocates the TCP buffers and variables to the connection, and sends a connection-granted segment to the client TCP.

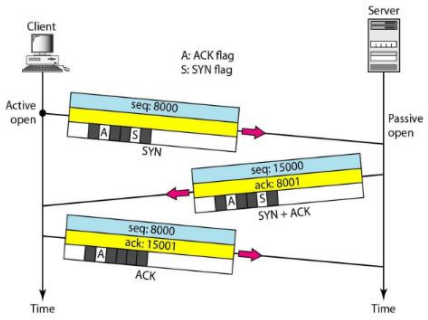
- This connection-granted segment also contains no application layer data.
- However, it does contain three important pieces of information in the segment header.
  - First, the SYN bit is set to 1.
  - Second, the acknowledgment field of the TCP segment header is set to client_isn+1.
  - Finally, the server chooses its own initial sequence number (server_isn) and puts this value in the sequence number field of the TCP segment header.
- The connection granted segment is referred to as a **SYN ACK segment**.

Step 3

- Upon receiving the SYN ACK segment, the client also allocates buffers and variables to the connection.
- The client host then sends the server yet another segment; this last segment acknowledges the server's connection-granted segment (the client does so by putting the value server_isn+1 in the acknowledgment field of the TCP segment header).
- The SYN bit is set to zero, since the connection is established.
- This third stage of the three-way handshake may carry client-to-server data in the segment payload
- *This connection establishment procedure is often referred to as a* ***three-way handshake***



TCP three-way handshake: segment exchange

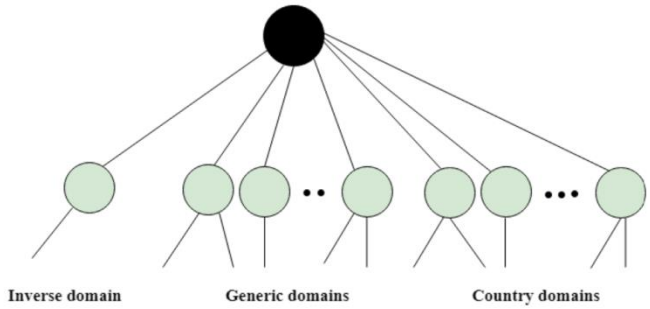


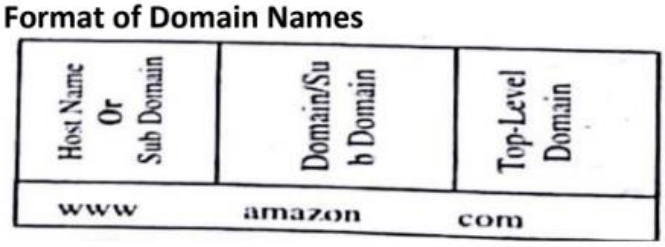
3.What is DNS? Explain resource record and name server. Illustrate DNS working.

An application layer protocol defines how the application processes running on different systems, pass the messages to each other:

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses.
- This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- The **domain name space** is divided into three different sections: generic domains, country domains, and inverse domain.

—DNS is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address.





Name Servers

- Name servers are the repositories of information that make up the domain database. The database is divided up into sections called zones, which are distributed among the name servers.
- Name servers can answer queries in a simple manner.
- The response can always be generated using only local data, and either contains the answer to the question or a referral to other name servers "closer" to the desired information.
- The simplest mode *for the server* is non-recursive, since it can answer queries using only local information.
- The simplest mode *for the client* is recursive, since in this mode the name server acts in the role of a resolver and returns either an error or the answer, but never referrals.

Recursive Query vs. Iterative Query

If the server is supposed to answer a **recursive query** then the response is either the resource record data or an error code.

In **iterative mode**, on the other hand, if the server does not have the information requested locally then it return the address of some name server who might have the information about the query. .

Resource Records: Each domain name is associated with a record called the resource record. The server database consists of resource records.

The resource records are used in the answer, authoritative and additional information section of the response message.These are 4-tuples:(Name, Value, Type, TTL)

A: Name is hostname, Value the IP address
NS: Name is a domain
CNAME: Name is an alias hostname, Value its canonical name
MX: Name is an alias name for a mail server

DNS WORKING:

- DNS is a client/server network communication protocol. DNS clients send requests to the.server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname.
- If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

4.Explain SNMP basic components and their functions. Describe the basic commands used in SNMP

The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite.

It provides a set of fundamental operations for monitoring and maintaining an internet.

SNMP components –

There are 3 components of SNMP:

SNMP Manager –

It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

defines the format of packets exchanged between a manager and agent. It reads and changes the status (values) of objects (variables) in SNMP packets.

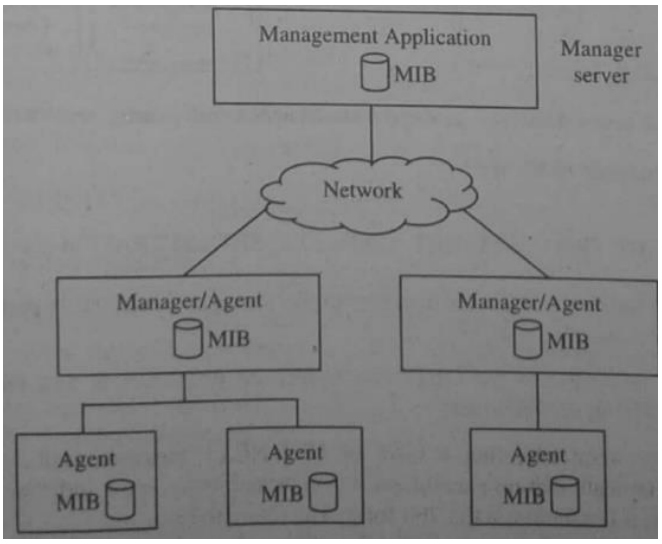
SNMP agent –

It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.Defines the general rules for naming objects, defining object types (includingrange and length), and showing how to encode objects and values.

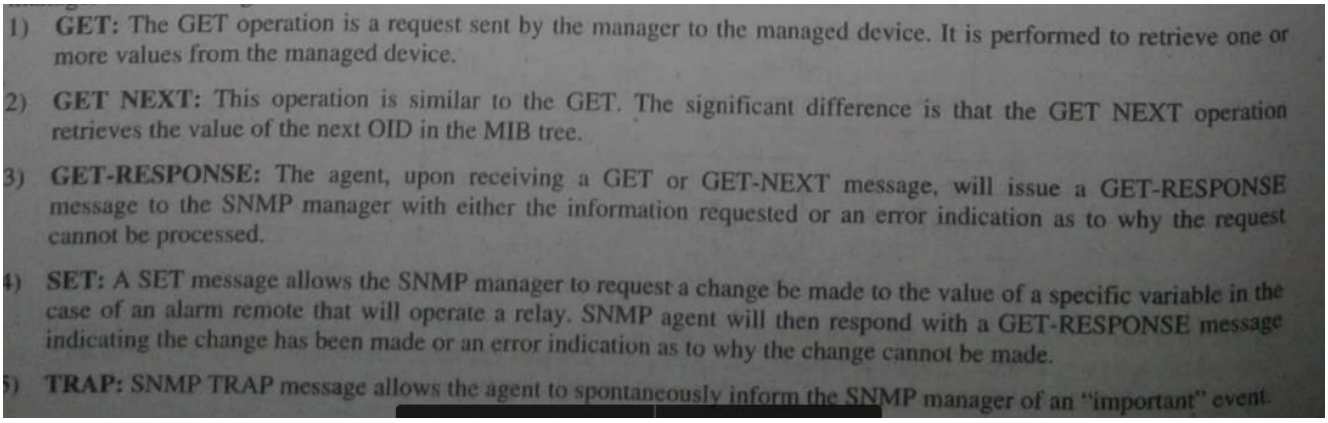
Management Information Base(MIB) –

MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

MIB creates a collection of named objects, their types, and their relationships to each otherin an entity to be managed.



The basic commands used in SNMP:



1) **GET:** The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.

2) **GET NEXT:** This operation is similar to the GET. The significant difference is that the GET NEXT operation retrieves the value of the next OID in the MIB tree.

3) **GET-RESPONSE:** The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the SNMP manager with either the information requested or an error indication as to why the request cannot be processed.

4) **SET:** A SET message allows the SNMP manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. SNMP agent will then respond with a GET-RESPONSE message indicating the change has been made or an error indication as to why the change cannot be made.

5) **TRAP:** SNMP TRAP message allows the agent to spontaneously inform the SNMP manager of an "important" event.

5.What is FTP? Explain its working in detail with the comments involved.

- File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another.
- Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.
- For example, two systems may use different file name conventions.
- Two systems may have different ways to represent text and data.
- Two systems may have different directory structures.
- All of these problems have been solved by FTP in a very simple and elegant approach.

WORKING OF FTP:

- The FTP connection is established between two systems and they communicate with each other using a network.
- So, for the connection, the user can get permission by providing the credentials to the FTP server or can use anonymous FTP.
- When an FTP connection is established, there are two types of communication channels are also established and they are known as **command channel** and **data channel**.

- The command channel is used to transfer the commands and responses from client to server and server to client.
- As soon as the server and the client get connected to the network, the user logins using User ID and password.
- The server verifies the user login and allows the client to access the files.

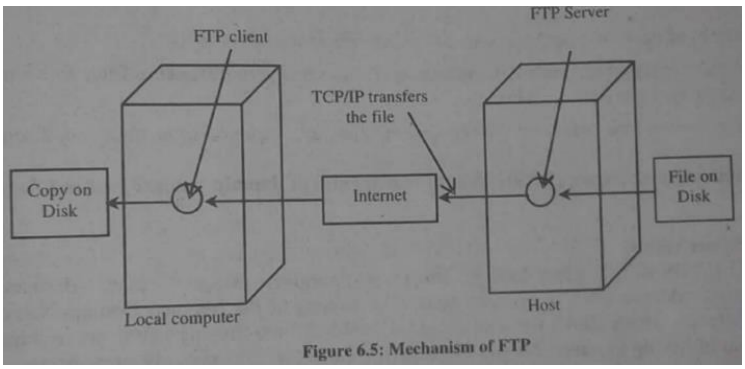


Figure 6.5: Mechanism of FTP

6.Explain MIME and its various features.

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:

1.Text in character sets other than ASCII .

2.Non-text attachments: audio, video, images, application programs etc.

3.Message bodies with multiple parts.

4.Header information in non-ASCII character sets Virtually all human-written Internet email and a fairly large proportion of automated email is transmitted via SMTP in MIME format.

MIME defines five new message headers, as shown in Fig. The first of these simply tells the user agent receiving the message that it is dealing with a MIME message, and which version of MIME it uses.

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

FEATURES OF MIME

1. It is able to send multiple attachments with a single message.
2. Unlimited message length.
3. Binary attachments (executables, images, audio, or video files) may be divided if needed.
4. MIME provided support for varying content types and multi-part messages.

7.Distinguish between TCP and UDP.

Characteristics	UDP	TCP
General Description	Simple, high speed, low functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliable without worrying about network layer issues.
Data Interface to Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
Retransmission	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Managing flow of data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
Overhead	Very low	Low ,but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quality	Small to moderate amounts of data(up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
Protocol Connection Setup	Connections less; details sent without setup.	Connection-oriented; connection must be established prior to transmission.
Applications and Protocols	Multimedia applications, DNS,BOOTP,DHCP,TFTP, SNMP,RIP,NFS	FTP, Telnet, SMTP, DNS,HTTP POP,NNTP,IMAP,BGP, IRC,NFS

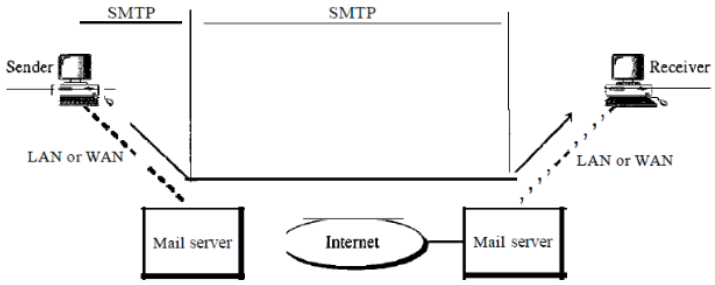
8. What are the email protocols?

There are two email protocols used

1. SMTP
2. MIME

SMTP—Simple Mail Transfer Protocol

- SMTP is a simple ASCII protocol.
- The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.
- The server starts by sending a line of text giving its identity and telling whether it is prepared to receive mail.
- SMTP simply defines how commands and responses must be sent back and forth. Each network is free to choose a software package for implementation.



- SMTP defines 14 commands. The first five are mandatory; every implementation must support these five commands.
- The next three are often used and highly recommended. The last six are seldom used.
- Responses are sent from the server to the client. A response is a three digit code that may be followed by additional textual information.

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:

1.Text in character sets other than ASCII .

2.Non-text attachments: audio, video, images, application programs etc.

3.Message bodies with multiple parts.

4.Header information in non-ASCII character sets Virtually all human-written Internet email and a fairly large proportion of automated email is transmitted via SMTP in MIME format.

MIME defines five new message headers, as shown in Fig. The first of these simply tells the user agent receiving the message that it is dealing with a MIME message, and which version of MIME it uses.

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content