# UNIT V

- UDP The Internet Transport Protocols:
- Introduction to UDP
- Remote Procedure Call(RPC)
- TheReal-TimeTransport Protocol (RTP)


- The Internet Transport Protocols :UDP
- The Internet has two main protocols in the transport layer, a connectionless protocol and a connection-oriented one.
- UDP is the connectionless protocol.
- TCP is the connection-oriented protocol

- Introduction to UDP

- The Internet protocol suite supports a connectionless transport protocol, UDP (User Datagram Protocol).

- UDP provides a way for applications to send encapsulated IP datagrams and send them without having to establish a connection.

- UDP transmits segments consisting of an8- byte header followed by the payload.

- The two ports serve to identify the end points with in the source and destination machines.

# Introduction to UDP

| ← 32 Bits → | |
|---|---|
| Source port | Destination port |
| UDP length | UDP checksum |
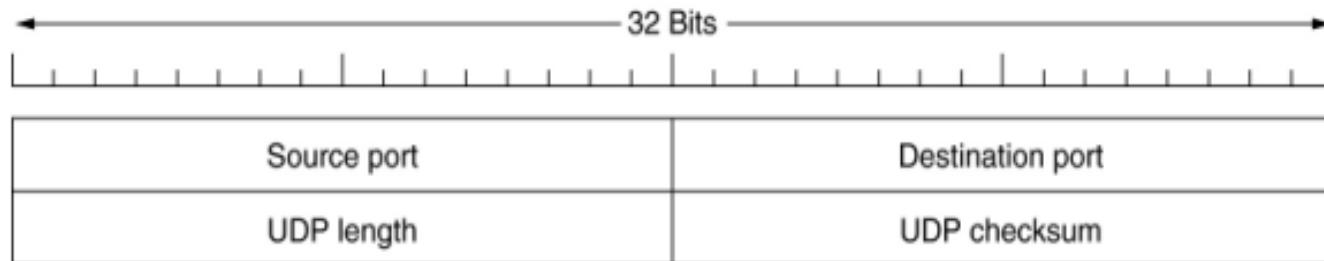
The UDP header.

UDP does not do flow control, error control, or retransmission up on receipt of a bad segment.

What UDP does do is provide an interface to the IP protocol with the added feature of demultiplexing multipleprocesses using the ports.

- **Remote Procedure Call** – In a certain sense, sending a message to a remote host and getting a reply back is a lot like making a function call in programming language. – In both cases you start with one or more parameters and you get back a result. This observation has led people to try to arrange request-reply interaction on networks to be cast in the form of procedure calls.

Steps in making a remote procedure call. The stubs are shaded
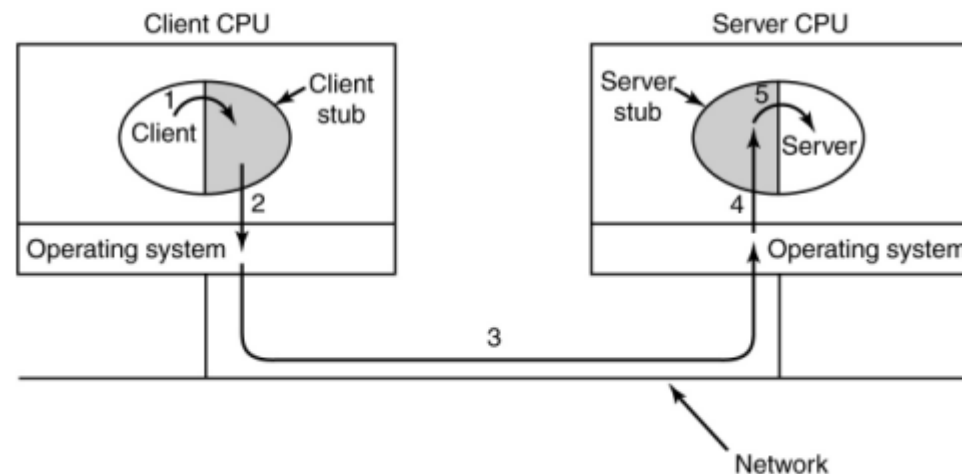
- This technique is known as RPC (Remote Procedure Call) and has become the basis form any networking applications.

- Traditionally, the calling procedure is known as the client and called procedure is known as the server

- **The Real-Time Transport Protocol** – Another one is real-time multimedia application. – In particular, as Internet radio, Internet telephony, music-on-demand, video conferencing, video-ondemand,…

- People discovered that each application was re inventing more or less the same real-time transport protocol.

- The basic function of RTP is to multiplex several real-time data streams onto a single stream of UDP packets.

- # The Real-Time Transport Protocol
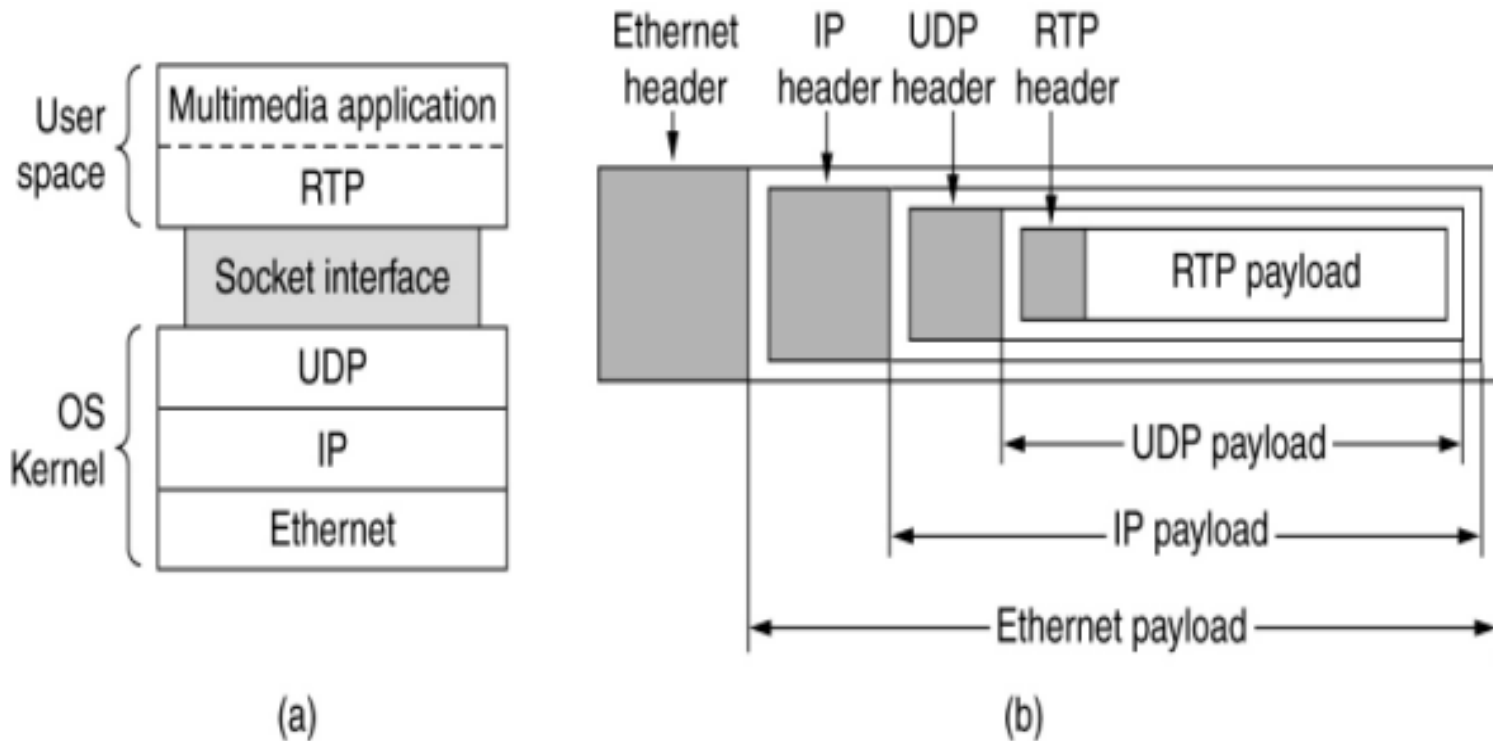


(A)The position of RTP in the protocol stack.
(b)Packet nesting.

- The UDP stream can be sent to a single destination (unicasting) or to multiple destinations (multicasting)

- Each packet sent in an RTP stream is given a number one higher than its predecessor.

- RTP has no flow control, no error control, no acknowledgements, and no mechanism to request retransmission.

- Introduction to TCP

- Transmission Control Protocol TCP was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork.

- An Internetwork differs from a single network because different parts may have widely different topologies, bandwidths, delays, packet sizes, and other parameters.

- TCP was designed to dynamically adapt to properties of the internetwork and to be robust in the face of many kinds of failures

- Each machine supporting TCP has a TCP transport entity.

- In both cases, it manages TCP streams and interfaces to the IP layer.

- IP layer gives no guarantee that datagrams will be delivered properly, so it upto TCP to time out and retransmit them as need be.

# The TCP Segment Header
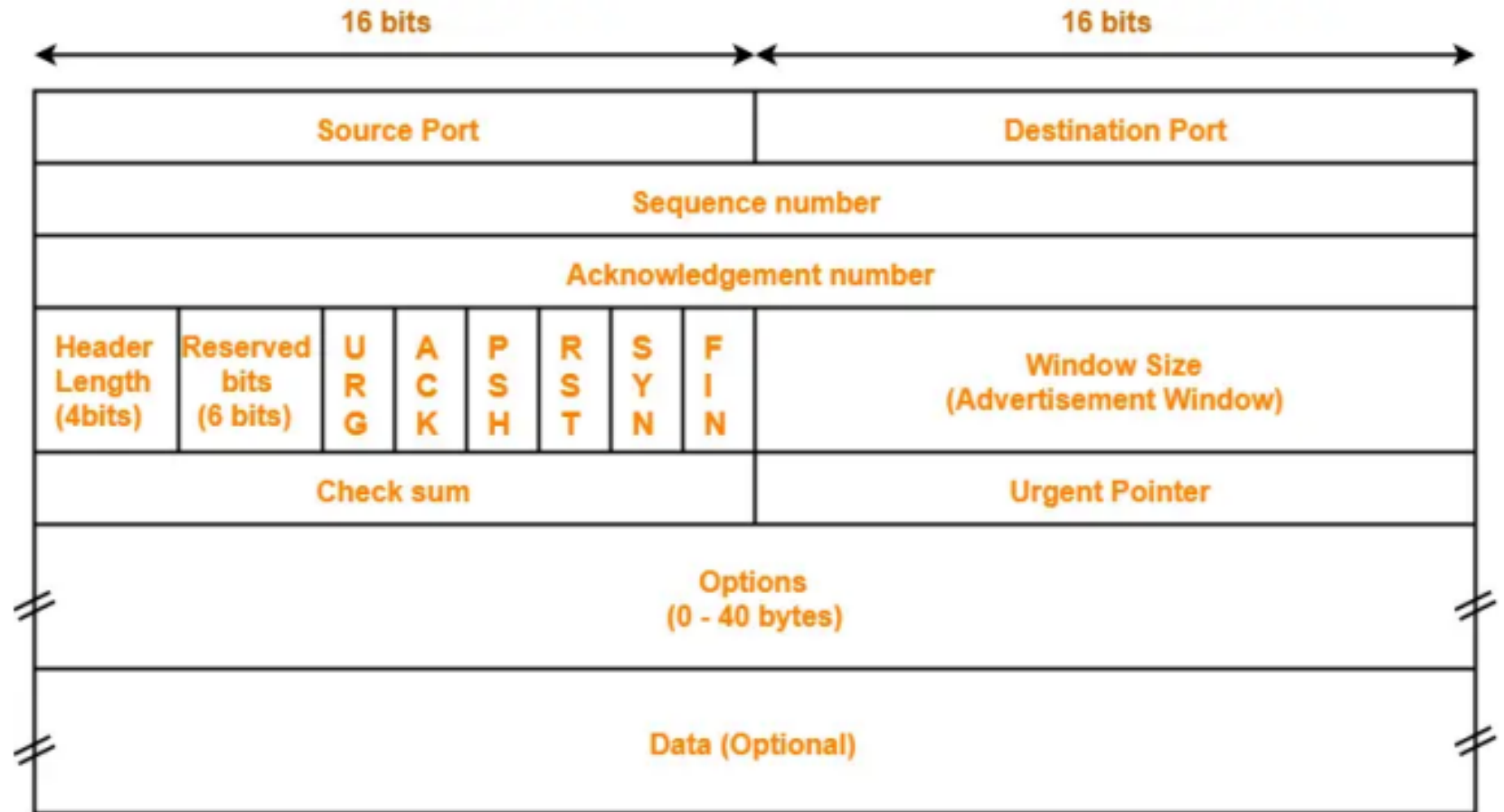


**TCP Header**

- **The TCP Segment Header**

- **Source Port** It is a 16-bit field that indicates the port number of the sending device where the data originates It is a randomly assigned field.

- **Destination Port** This field indicates the port number on the receiving device where the data should be delivered. It is 16 bits field

- **Sequence Number** TCP converts data into bytes and the collection of bytes is known as segment. Each TCP segment is assigned a sequence number, which helps the receiving end to reassemble the data in the correct order. It is a 32-bit value.

- **Acknowledgment Number** In TCP, data transmission is acknowledged to ensure reliability. This field contains the sequence number that the receiving device expects to receive next. Acknowledgment no is always an incremental value i.e., if the sequence number is x, than Acknowledgment no is set to x+1.

- **Data Offset** This field determines the size of the TCP header. It is necessary to locate the start of the data payload. It is a 4 bits field.

- Reserved These bits are reserved and are currently set to zero.

- **Control Bits (Flags)** It is also called flags or TCP flags which are used to control and manage aspects of TCP connection and data transmissio

- Some common flags include:
- 1. URG (Urgent) This bit can be 0 or 1. When this bit is 1, it implies that the data should be treated as a priority. For example, data is always sent in a seq. but we have some urgent data bits that should be sent first. In that case, the Urgent bit is set ON for that particular data, and that data is sent first.
- 2. ACK (Acknowledgment) Indicates whether the acknowledgment number field is valid or not. If ACK is 1 it implies that the acknowledgment number is valid and if ACK is 0, it means that the segment is missing acknowledgment.
- 3. PSH (Push) In general, applications collect a certain number of data and then process it. When the Push flag is set ON, it tells the application to transmit the data immediately and not wait for data to stack to fill the entire TCP segment

- 4. RST (Reset) Resets the connection. If it is set to 1, the connection is abruptly reset.

- 5. SYN (Synchronize) Initiates a connection and synchronizes sequence numbers. It is used in the 3-way handshake process.

- 6. FIN (Finish) The fin flag is used to terminate the TCP connection. Whenever Host wants to end the connection with the receiving end, it sends data with FIN flag 1. Since TCP works in a full duplex mode, receiving end should also set its FIN flag as 1.

- **Window Size**: This field indicates the size of the receiving device's receive window, which helps in flow control. It is a 16- bit field. It is used for flow control between the sender and receiver

- **Checksum**: checksum is a 16-bit field numerical value calculated from the TCP header and data payload to detect errors during transmission.

- **Urgent Pointer**: If the URG flag is set, this field points to the last urgent data byte in the TCP segment i.e., it tells about the sequence number of the last urgent data byte. It is a 16 bit field.

- **Options**: This field is optional and can contain additional parameters or information related to the TCP connection

- **Hyper Text Transfer Protocol.**

• HTTP stands for Hyper Text Transfer Protocol.

• It is a protocol used to access the data on the World Wide Web (www).

• The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

• This protocol is known as Hyper Text Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document

**Hyper Text Transfer Protocol.**

HTTP Client                                    HTTP Server

HTTP Request →

← HTTP Reply
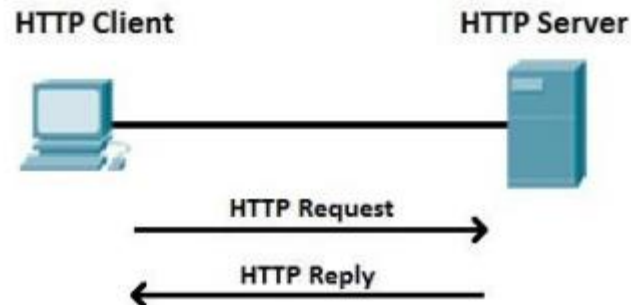
- **Features of HTTP:**

- **Connectionless protocol**: HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection.

- **Media independent**: HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content.

- **Stateless**: HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages

- **File transfer protocol**

• FTP 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 servers.

**There are two types of connections in FTP:**

FTP Connections

Control Connection
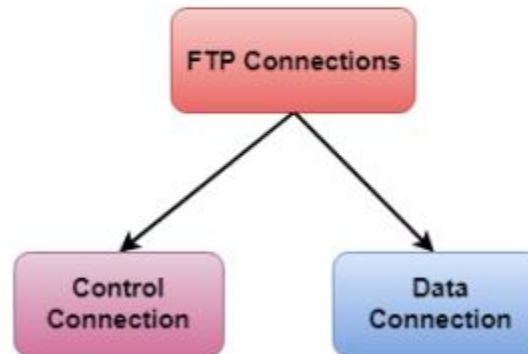
Data Connection

- **Control Connection**: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

- **Data Connection**: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred
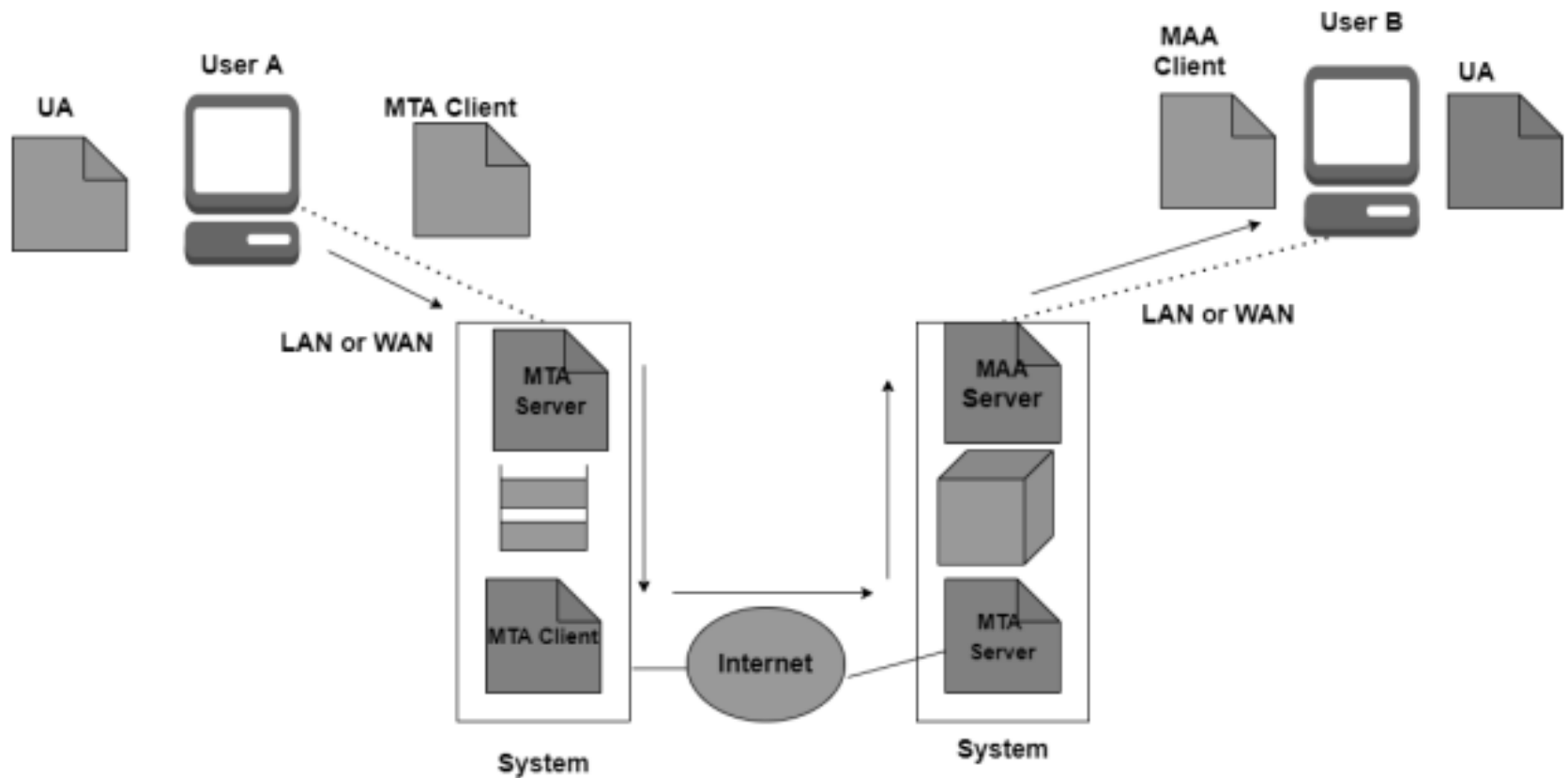
- <span style="color:red">Electronic Mail</span>

- Electronic mail is computer network one of the most well-known network services. Electronic mail is a computer-based service that allows users to communicate with one another by exchanging messages.

- Email information is transmitted via email servers and uses a variety of TCP/IP protocols. For example, the simple mail transfer protocol (SMTP) is a protocol that is used to send messages

- Services offered by Electronic Mail

• **Composition**: Creating messages and responses is referred to as composition.

• **Transfer**: Sending mail from the sender to the receiver is known as a transfer.

• **Reporting**: Mail delivery confirmation is known as reporting. It allows users to see if their mail has been delivered, misplaced, or rejected.

• **Displaying**: It refers to presenting messages so that the user can understand them.

• **Disposition**: This stage concerns the recipient's actions after receiving mail, such as saving it, deleting it before reading it, or after reading it

# Electronic Mail

- **Components Of Electronic Mail**
- The following are the essential components of an e-mail system:
- User Agent (UA) : Reading a Message , Sending a reply to a Message , Message Composition.
- Message Transfer Agent (MTA) : The Message Transfer Agent manages the actual email transfer operation (MTA). Simple Mail Transfer Protocol sends messages from one MTA to another.
- Message Access Agent: The Simple Mail Transfer Protocol is used for the first and second stages of e-mail delivery.

- TELNET

- TELNET stands for Teletype Network. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the local computer.
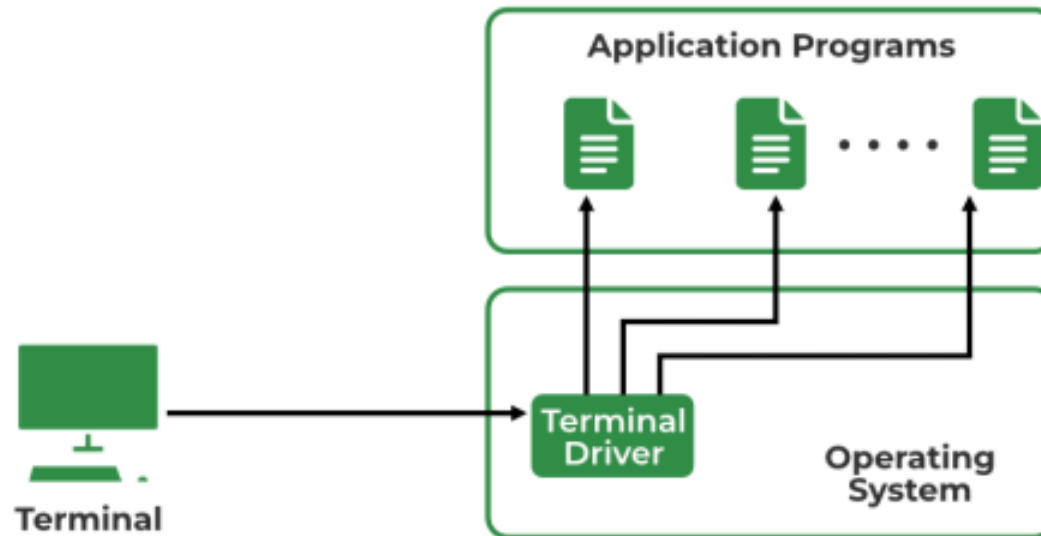
- Logging

The logging process can be further categorized into two parts

- Local Login

- Remote Login

- 1. Local Login: Whenever a user logs into its local system, it is known as local login.

- 2. Remote Login: Remote Login is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer.

- **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

- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Inverse domain      Generic domains      Country domains
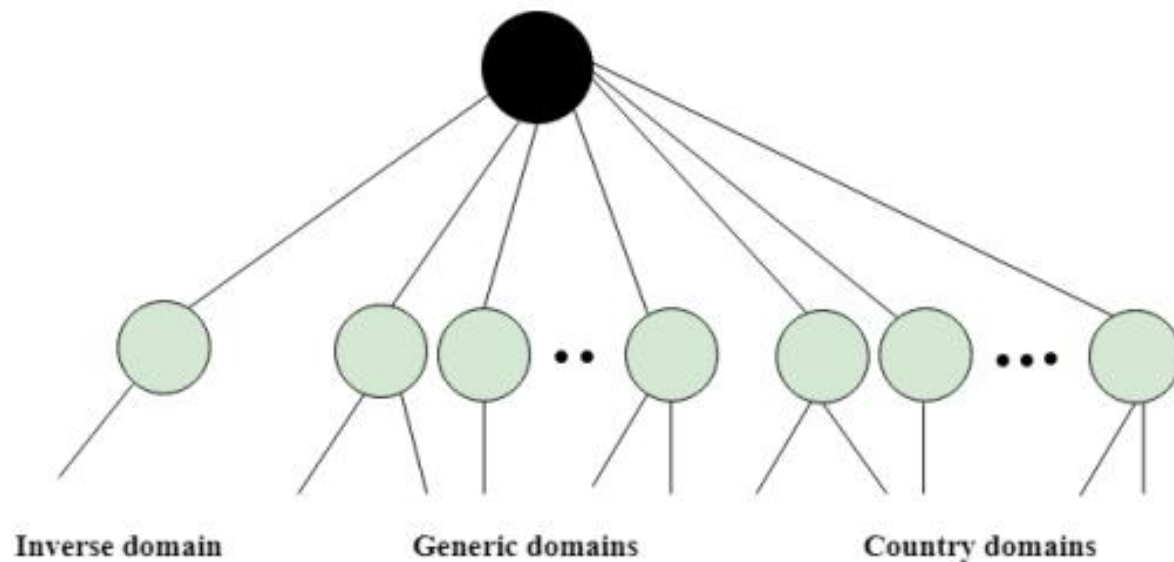
- SNMP: Simple Network Management Protocol.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.

**SNMP Concept**
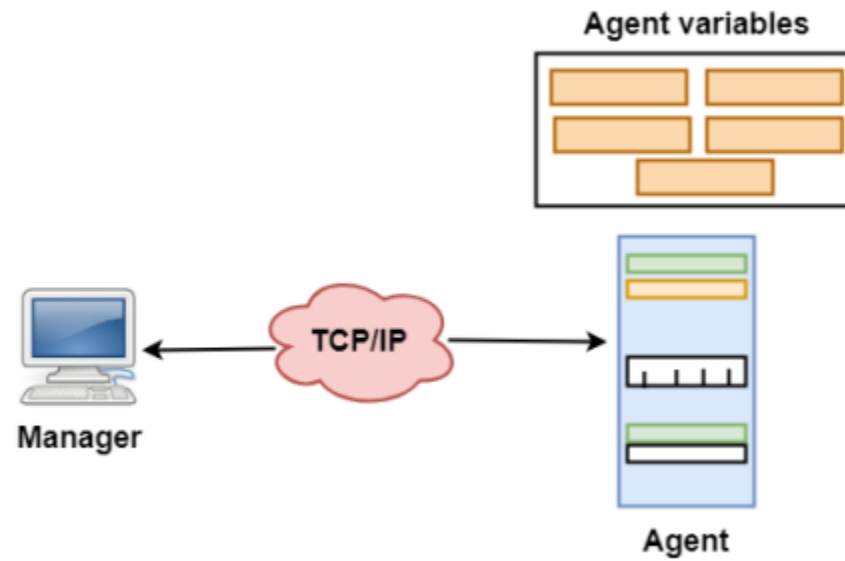
- SNMP has two components Manager and agent. The manager is a host that controls and monitors a set of agents such as routers.

- It is an application layer protocol in which a few manager stations can handle a set of agents.

- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.

- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways

- **World Wide Web**

- The World Wide Web or Web is basically a collection of information that is linked together from points all over the world. It is also abbreviated as WWW.

- World wide web provides flexibility, portability, and user-friendly features.

- It mainly consists of a worldwide collection of electronic documents (i.e, Web Pages).

- It is basically a way of exchanging information between computers on the Internet.

- The WWW is mainly the network of pages consists of images, text, and sounds on the Internet which can be simply viewed on the browser by using the browser software.

- It was invented by Tim Berners-Lee.

- **Architecture of WWW**

- The WWW is mainly a distributed client/server service where a client using the browser can access the service using a server.

- The Service that is provided is distributed over many different locations commonly known as sites/websites.

- Each website holds one or more documents that are generally referred to as web pages.

# Architecture of WWW