UNIT-5

The Transport Layer:-

Transport layer protocols: Introduction ,Services, Port number ,User datagram protocol ,User datagram, UDP services, UDP applications

Transmission control protocol: TCP services, TCP features, Segment, A TCP connection, windows in TCP, Flow control, Error control, Congestion control in TCP.

Application Layer :-

World Wide Web: HTTP, Electronic mail, Architecture, web based mail, email security, TELENET, Local versus Remote logging-

Domain Name System: Name Space, DNS in Internet, Resolution, Caching, Resource Records, DNS messages, Registrars, Security of DNS Name Servers, SNMP.

What is Transport Layer?

- Transport Layer is the fourth layer from the top in OSI Model which provide communication services to the application processes that was running on different hosts.
- Transport Layer provides the services to the session layer and it receives the services from network layer.
- The services provided by transport layer includes error correction as well as segmenting and de-segmenting data before and after it's sent on the network.
- Transport layer also provides the flow control functionality and ensures that segmented data is delivered across the network in the right sequence.

Note: Main duty of transport layer is to provide process to process communication.

Services provided by Transport Layer:-

1. **Process to Process Communication:-**

Transport Layer is responsible for delivery of message to appropriate process.

Transport Layer uses a port number to deliver the segmented data to the correct process amongst the multiple processes that are running on a particular host. A port number is a 16-bit address used by transport layer to identify any client-server program.

2. Multiplexing and De-multiplexing:-

The transport layer provides the multiplexing service to improve transmission efficiency in data communication. At the receiver side, demultiplexing is required to collect the data coming from different processes. Transport Layer provides

a) Upward Multiplexing:-

It means multiple transport layer connections utilizes the connection of same network. Transport layer transmits several transmissions bound for the same destination along the same path in network.

b) Downward multiplexing:-

It means a transport layer connection utilizes the multiple connections. This multiplexing allows the transport layer to split a network connection among several paths to improve the throughput in network.

3. Flow Control:-

Flow control makes sure that the data is transmitted at a rate that is accept table for both sender and receiver by managing data flow.

The transport layer provides a flow control service between the adjacent layers of the TCP/IP model. Transport Layer uses the concept of sliding window protocol to provide flow control.

4. Data integrity:-

Transport Layer provides data integrity by:

- Detecting and discarding corrupted packets.
- Tracking of lost and discarded packets and re-transmit them.
- Recognizing duplicate packets and discarding them.
- Buffering out of order packets until the missing the packets arrive.

5. Congestion avoidance:-

- In network, if the load on network is greater than the network load capacity, then the congestion may occur.
- Congestion Control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

- The transport layer recognizes overloaded nodes and reduced flow rates and take proper steps to overcome this.

Example of Transport Layer:-

- Let us understand transport layer with the help of example. Let us take an example of sending email.
- When we send an email then the email then in OSI model each layer communicates to the corresponding layer of the receiver.
- So when the mail will come at transport layer on sender side then the email is broken down in to small segments. Then that broken segments are sent to network layer and transport layer also specifies the source and destination port.
- At the receiver side, transport layer reassembles all the segment to get the data and use port number to identify the application to deliver data

Working of Transport Layer:-

- The transport layer receives the services from the network layer and then give services to the session layer.
- **At the sender's side:** At the sender's end, transport layer collect data from application layer i.e message and performs segmentation to divide the message into segments and then adds the port number of source and destination in header and send that message to network layer.
- **At the receiver's side:** At the receiver's end, transport layer collects data from network layer and then reassembles the segmented data and identifies port number by reading its header to send that message to appropriate port in the session layer.

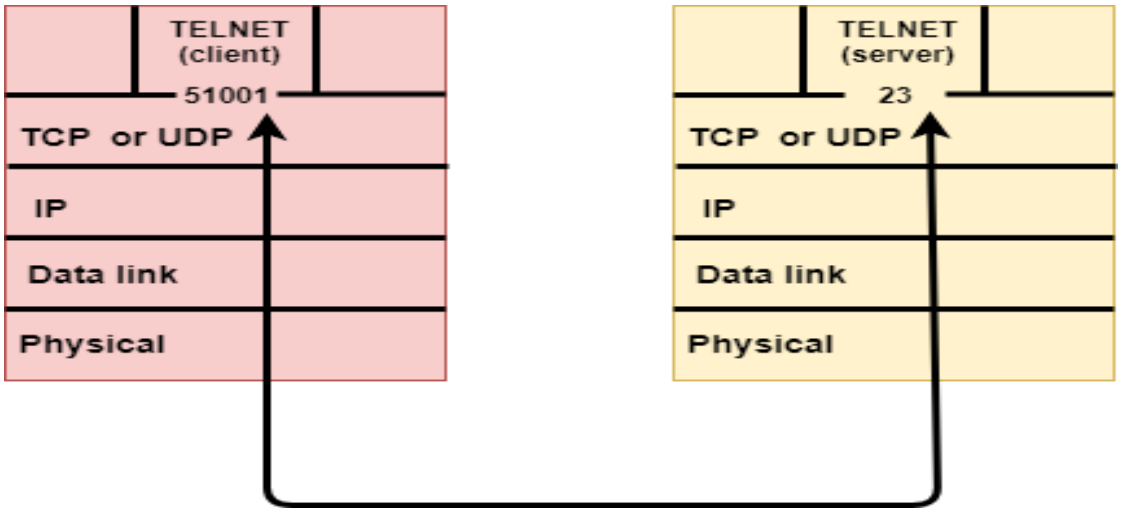
Transport Layer Protocols:-

- UDP (User Datagram Protocol)
- TCP(Transmission Control Protocol)
- SCTP (Stream Control Transmission Protocol)

The transport layer is represented by two protocols:

i)UDP

ii) TCP.



UDP(User Datagram Protocol):-

- UDP is one of the simplest transport layer protocol which provides non sequenced data transmission functionality.
- UDP is consider as connectionless transport layer protocol.
- This type of protocol is referred to be used when speed and size are more important than reliability and security.
- It is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data received from the upper layer.
- User datagram is the packet constructed by the UDP protocol

UDP Services

- Process to Process Communication
- Connectionless Service
- Fast delivery of message

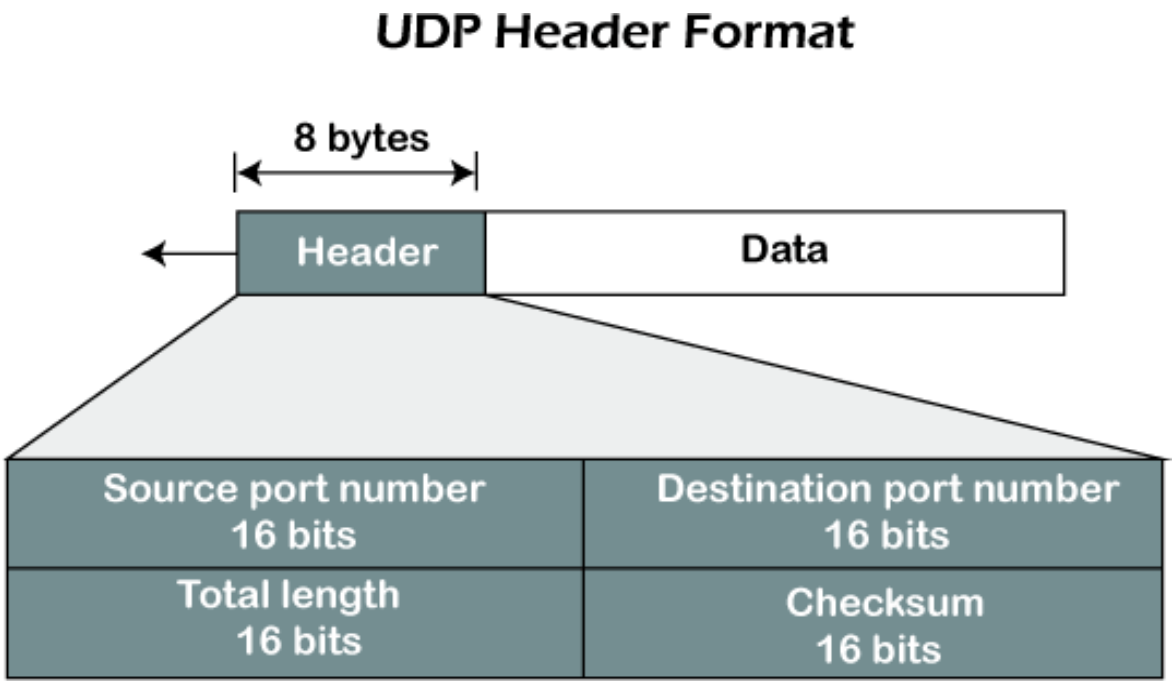
- Checksum

Disadvantages

- UDP delivers basic functions required for the end-to-end transmission of data.
- It does not use any sequencing and does not identify the damaged packet while reporting an error.
- UDP can identify that an error has happened, but UDP does not identify which packet has been lost.

Format of User Datagram

The user datagram has a 16-byte header which is shown below



User datagram have a fixed size header of 8 bytes which is divided into four parts -

Source port address: It defines source port number and it is of 16 bits.

Destination port address: It defines destination port number and it is of 16 bits.

Total length: This field is used to define the total length of the user datagram which is sum of header and data length in bytes. It is a 16-bit field.

Checksum: Checksum is also 16 bit field to carry the optional error detection data.

User Datagram Protocol Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.

UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming

- User Datagram Protocol has attributes that make it beneficial for use with applications that can tolerate lost data. Below are some examples:
- It allows packets to be dropped and received in a different order than they were transmitted, making it suitable for real-time applications where latency might be a concern.
- It can be used for transaction-based protocols, such as DNS or Network Time Protocol (NTP).
- It can be used where a large number of clients are connected and where real-time error correction isn't necessary, such as gaming, voice or video conferencing, and streaming media.

UDP application

Here are few applications where UDP is used to transmit data:

- ❖ Domain Name Services
- ❖ Simple Network Management Protocol
- ❖ Trivial File Transfer Protocol
- ❖ Routing Information Protocol
- ❖ Kerberos

ii) TCP(Transmission Control Protocol):-

- TCP stands for Transmission Control Protocol.
- TCP is a connection-oriented transport layer protocol.
- TCP explicitly defines connection establishment, data transfer, and connection tear down phases to provide connection oriented service for data transmission.
- TCP is the most commonly used transport layer protocol.

Features Of TCP protocol:-

- ❖ Stream data transfer
- ❖ Reliability
- ❖ Flow Control
- ❖ Error Control
- ❖ Multiplexing
- ❖ Logical Connections
- ❖ Full Duplex

1) Segment Numbering System:-

- ➢ TCP keeps track of the segments being transmitted or being received by assigning numbers to each and every single one of them.
- ➢ A specific Byte Number is assigned to data bytes that are to be transferred while segments are assigned sequence numbers.
- ➢ Acknowledgment Numbers are assigned to received segments.

2) Reliability:-

- ➢ TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism, which checks the state and sound arrival of the data.
- ➢ In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.

3) Order of the data is maintained:-

- This protocol ensures that the data reaches the intended receiver in the same order in which it is sent.
- It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.

Connection-oriented:-

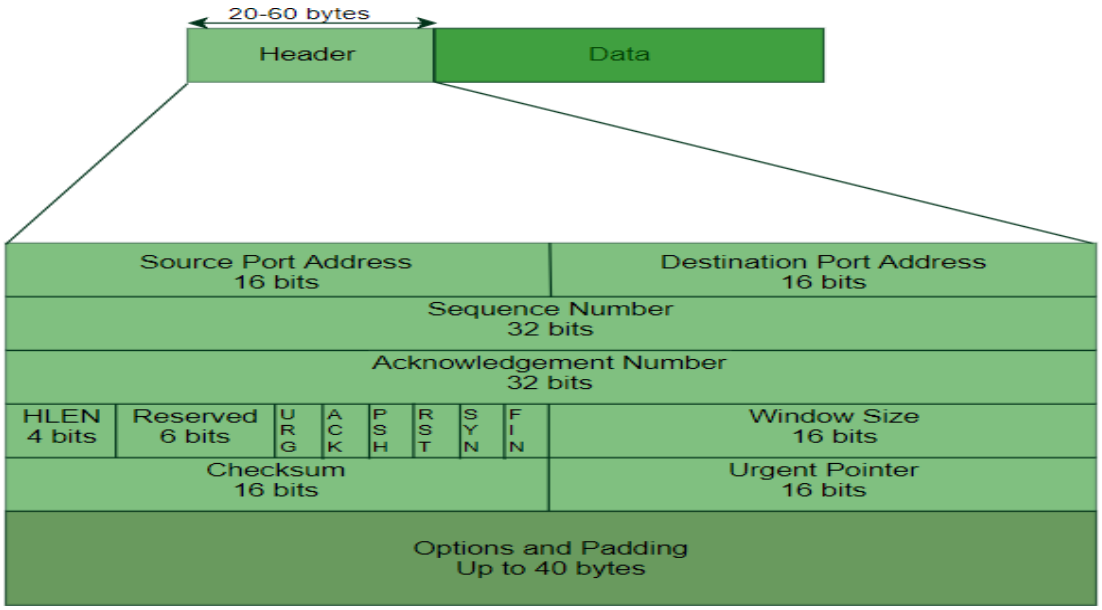
It is a connection-oriented service that means the data exchange occurs only after the connection establishment. When the data transfer is completed, then the connection will get terminated.

4) Full duplex:-

It is a full-duplex means that the data can transfer in both directions at the same time.

5) Stream-oriented:-

- TCP is a stream-oriented protocol as it allows the sender to send the data in the form of a stream of bytes and also allows the receiver to accept the data in the form of a stream of bytes.
- TCP creates an environment in which both the sender and receiver are connected by an imaginary tube known as a virtual circuit.
- This virtual circuit carries the stream of bytes across the internet.



- **Source port address** is a 16 bit field that defines port number of application program that is sending the segment.
- **Destination port address** is a 16 bit field that defines port number of application program that is receiving the segment.
- **Sequence number** is a field of 32 bit that will define the number assigned to data first byte contained in segment.
- **Acknowledgement number** is a 32 bit field that describe the next byte that receiver is looking forward to receive next from sender.
- **Header Length (HLEN)** is a field of 4 bit that specify the number of 4 byte words in TCP header. The header length of TCP header can be between 20 to 60 bytes.
- **Reserved** is a field 6 bit that are reserved for future use.
- **Control bits** are 6 different independent control bits or flags in this field.

There are six in control field:

URG: Urgent pointer

ACK: Acknowledgement number

PSH: Push request

RST: Reset connection

SYN: Sequence number Synchronization

FIN: Connection termination

- **Window Size** is a 16-bit field that defines the size of the window of sending TCP in bytes.
- **Checksum**, 16-bit field contains checksum and used for error detection.
- **Urgent pointer** is a 16 bit field .This flag is set when there is urgent data in the data segment.
- **Options and padding** can be upto 40 bytes field for optional information in TCP header.

3)SCTP(Stream Control Transmission Protocol):-

- SCTP stands for Stream Control Transmission Protocol.
- SCTP is one of the connection oriented transport layer protocols.
- It allows transmitting of data between sender and receiver in full duplex mode.
- This protocol makes it simpler to build connection over wireless network and to control multimedia data transmission.

Features of SCTP

- Unicast with Multiple properties
- Reliable Transmission
- Message oriented
- Multi-homing

Transport Layer- TCP: Error and Flow control

What makes TCP protocol reliable:

TCP has four important feature which makes it reliable:

- Error control and
- Flow control
- Congestion control
- Connection management

Error control is achieved by:

- ❖ Acknowledgement number
- ❖ Re transmission
- ❖ Checksum
- ❖ Sequence number

1) Acknowledgment Number:

- In TCP for every data/segment send to the other end, it requires an acknowledgment in return. The acknowledgment number is nothing but the sequence number of the next bytes the receiver expects to receive.
- In the case of TCP, there is a cumulative acknowledgment number that is acknowledgment number is not send for each byte rather it is sent for a group of bytes that is called a segment.

For example:

- If the acknowledgment number is 1635, means all the bytes before this number are reached and the receiver expects bytes with 1635 as the next sequence number.
- If an acknowledgment number is not received, TCP automatically re-transmits the data(segment) and waits a longer amount of time.
    - The maximum time it can keep trying re transmission is 4 to 10 mins, depending upon implementation.
- TCP does not guarantee that data will be received at other end, its just that it provides reliable delivery of data or reliable notification of failure.
- There is nothing called segment number in TCP, rather each segment is a collection of bytes and each bytes is associated with sequence number.
- Thus acknowledgment number provides reliability to the TCP

2) Retransmission:

This is the heart of the TCP when it comes to reliability that is error control mechanism. If the packets is lost or damaged or corrupted or the ack itself is lost, TCP retransmits the data.

Retransmission takes place in two scenarios:

- Re transmission timer expires: that is it does not get the ack for the send bytes within stipulated time.
- Fast re transmission: This happens when the sender receives three duplicate ACK, in this segment is re transmitted even before RTO.

3)Checksum:

This is one of the features of TCP along with acknowledgment and retransmission which is used for error control mechanisms in TCP.

The checksum is calculated on three fields:

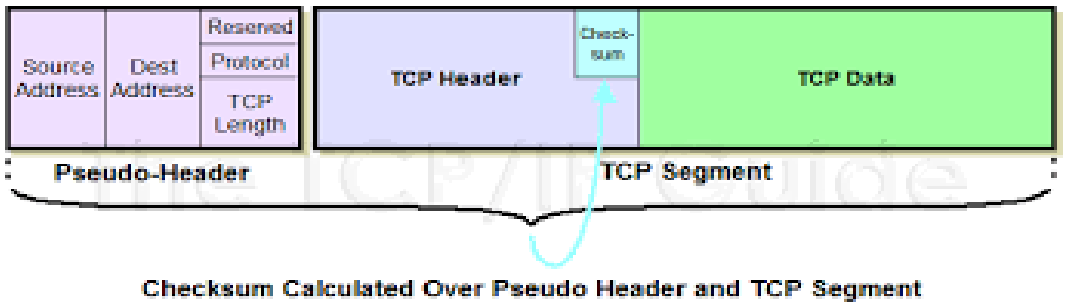
- TCP header
- TCP Body
- Pseudo IP header

The most surprising field out of the above three is the pseudo IP header because the IP header is below the transport header and the values of its fields keep changing when the packet traverses the network.

So the IP fields are used for checksum are those which are constant in the network that is:

- Source IP address
- Destination IP address
- Protocol
- TCP segment size

Fixed of 8 bits



- The total size of the pseudo-header is 12 bytes.
- Once the checksum is calculated with all the three fields, it is placed in the checksum field of TCP header and send to the receiver side and even calculates the checksum on the same fields and compares with what it received from the sender.

If the checksum happens not to be same, segment is considered as corrupted and ack is not being send and TCP autocratically retransmits the same.

4) Sequence number:

TCP associates a sequence number with each bytes it send. For example if the application writes a data of size say 2048 bytes, TCP would send this in two segments where the first segment carries bytes ranging from 1-1024 and the second 1025-2048.

Significance of sequence number:

i) Reassembly of packet at receiver side:

If the segments arrive out of order, the receiving TCP will reorder the two segments on the basis of sequence number before passing it to the application. Hence in TCP segments never reach out of order.

ii) Discard of duplicate data:

If TCP receives duplicate data may be because of lost acknowledgment or delay in receiving ack because of congestion, the receiving TCP can detect the duplicate data with the help of sequence number and discards the data.

iii) Retransmission of lost or corrupted or for damaged data:

Segments which are lost or damaged are re-send on the basis of the sequence number.

Flow Control

- TCP provides a mechanism called flow control by which it always tells its peer how many bytes of data it is willing to accept.
- This is called advertised window which reflects the buffer size of the receiver side so that sender cannot overflow the receiver buffer.

Congestion control

- Important issue in a packet-switched network, such as the Internet, is congestion.

- Congestion in a network may occur if the load on the network—the number of packets sent to the network— is greater than the capacity of the network—the number of packets a network can handle.
- Congestion control refers to the mechanisms and techniques that control the congestion and keep the load below the capacity.

Application Layer

- The application layer is actually an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communication network.
- This layer allows users to interact with other software applications.
- Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
- This layer allows users to access, retrieve and manage files in a remote computer. It allows users to log on as a remote host.
- This layer provides access to global information about various services.

This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.

- It provides protocols that allow software to send and receive information and present meaningful data to users.
- It handles issues such as network transparency, resource allocation and so on.
- This layer serves as a window for users and application processes to access network services.
- Application Layer is basically not a function, but it performs application layer functions.
- In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0's or 1's).
- This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
- This layer also receives and preserves data from it's previous layer, which is Presentation Layer (which carries in itself the syntax and semantics of the information transmitted).

- The protocols which are used in this application layer depend upon what information users wish to send or receive.

This application layer, in general, performs host initialization followed by remote login to hosts.

Features provided by Application Layer Protocols :

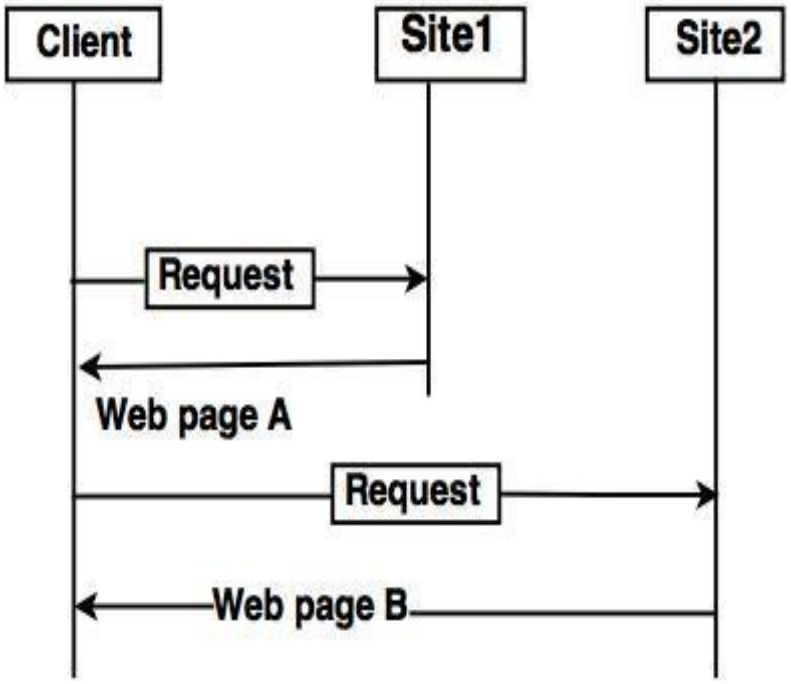
To ensure smooth communication, application layer protocols are implemented the same on source host and destination host.
The following are some of the features which are provided by Application layer protocols-

- The Application Layer protocol defines process for both parties which are involved in communication.
- These protocols define the type of message being sent or received from any side (either source host or destination host).
- These protocols also define basic syntax of the message being forwarded or retrieved.
- These protocols define the way to send a message and the expected response.

These protocols also define interaction with the next level.

World Wide Web:-

- The World Wide Web (WWW) is a collection of documents.
- The pages can be retrieved and viewed by using browser. and other web resources which are identified by URLs, interlinked by hypertext links, and can be accessed and searched by browsers via the Internet.
- World Wide Web is also called the Web and it was invented by Tim Berners-Lee in 1989.
- Website is a collection of web pages belonging to a particular organization



Architecture of WWW

- The client wants to see some information that belongs to site 1.
- It sends a request through its browser to the server at site 2.
- The server at site 1 finds the document and sends it to the client.

Client (Browser):

- Web browser is a program, which is used to communicate with web server on the Internet.
- Each browser consists of three parts: a controller, client protocol and interpreter.
- The controller receives input from input device and use the programs to access the documents.
- After accessing the document, the controller uses one of the interpreters to display the document on the screen.

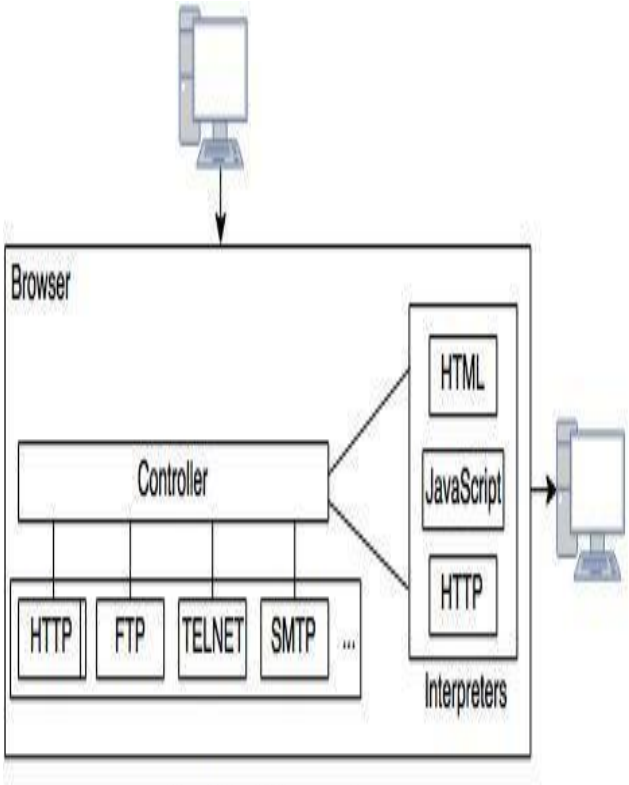


Fig: Client (Browser)

Server:

- A computer which is available for the network resources and provides service to the other computer on request is known as server.
- The web pages are stored at the server.
- Server accepts a TCP connection from a client browser.
- It gets the name of the file required.
- Server gets the stored file. Returns the file to the client and releases the top connection.

Uniform Resource Locater (URL)

- The URL is a standard for specifying any kind of information on the Internet.
- The URL consists of four parts: protocol, host computer, port and path.
- The protocol is the client or server program which is used to retrieve the document or file. The protocol can be ftp or http.
- The host is the name of computer on which the information is located.

- The URL can optionally contain the port number and it is separated from the host name by a colon.
- Path is the pathname of the file where the file is stored.

Hypertext Transfer Protocol (HTTP)

- The **Hypertext Transfer Protocol (HTTP)** is a networking protocol for distributed, collaborative, hypermedia information systems.
- HTTP is the foundation of data communication for the World Wide Web.
- HTTP functions as a request-response protocol in the client-server computing model.
- In HTTP, a web browser, for example, acts as a client, while an application running on a computer hosting a web site functions as a server.
- The client submits an HTTP request message to the server.
- The server, which stores content, or provides resources, such as HTML files, or performs other functions on behalf of the client, returns a response message to the client.
- A response contains completion status information about the request and may contain any content requested by the client in its message body.

Electronic Mail:-

- **Electronic Mail** (e-mail) is one of most widely used services of Internet.
- This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world.
- Message in mail not only contain text, but it also contains images, audio and videos data.
- The person who is sending mail is called **sender** and person who receives mail is called **recipient**.
- It is just like postal mail service.

Architecture of E-Mail System :

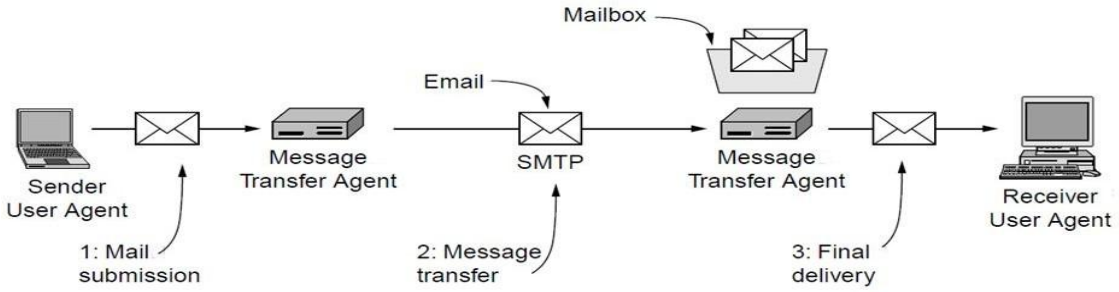
The basic architecture of an email system are : User Agent (UA), Message Transfer Agent (MTA), Message Access Agent(MAA). These are explained as following below:-

1. **User Agent (UA) :**
    - The UA is normally a program which is used to send and receive mail.
    - Sometimes, it is called as mail reader.
    - It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

2. **Message Transfer Agent (MTA) :**
    - MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA.
    - It transfer mail to mailboxes of recipients if they are connected in the same machine.
    - It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.

3. **Message Access Agent(MAA):-**
    - The Simple Mail Transfer Protocol is used for the first and second stages of e-mail delivery.
    - The pull protocol is mainly required at the third stage of e-mail delivery, and the message access agent is used at this point.
    - POP and IMAP4 are the two protocols used to access messages.

Architecture and Services (1)



Architecture of the email system

Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Services provided by E-mail system :

- **Composition –** The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- **Transfer –** Transfer means sending procedure of mail i.e. from the sender to recipient.
- **Reporting –** Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- **Displaying –** It refers to present mail in form that is understand by the user.
- **Disposition –** This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

Webmail:-

- Webmail systems include Google Gmail, Microsoft Hotmail and Yahoo! Mail.
- Webmail is one example of software (in this case, a mail user agent) that is provided as a service using the Web.
- Many of the items on the page showing the mailbox are clickable, so messages can be read, deleted, and so on.
- To make the interface responsive, the Web pages will often include JavaScript programs. These programs are run locally on the client in response to local events

Email Security:-

- Email security is the process of ensuring the availability, integrity and authenticity of email communications by protecting against the risk of email threats.

- Email enables billions of connected people and organizations to communicate with one another to send messages. Email is at the foundation of how the internet is used, and it has long been a target for attacks.

- Since the earliest days of email, it has been abused and misused in different ways with no shortage of email threats.

- Email security aims to help prevent attacks and abuse of email communication systems.

- Within the domain of email security, there are various email security protocols that technology standards organizations have proposed and recommended for implementation to help limit email risks.

- Protocols can be implemented by email clients and email servers, such as Microsoft Exchange and Microsoft 365, to help ensure the secure transit of email.

- Looking beyond just protocols, secure email gateways can help organizations and individuals to protect email from various threats.

TELNET:-

- Telnet is an abbreviation for **Terminal Network**.

- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site.

There are two types of login:-

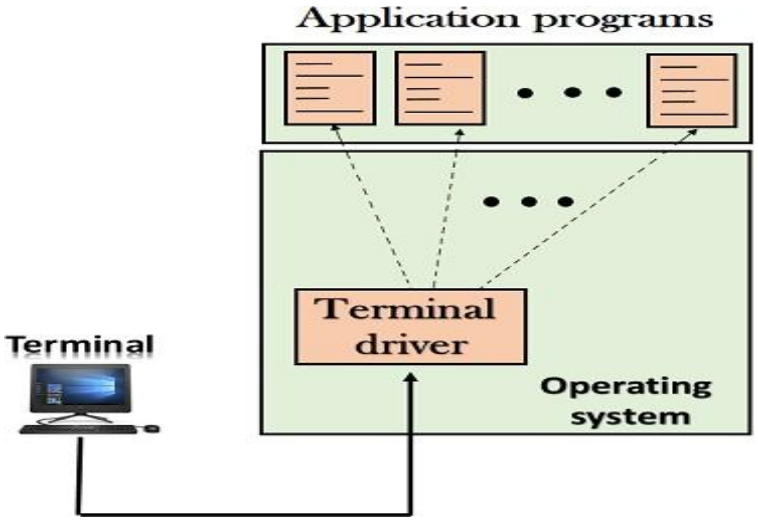
1) Local Login

2) Remote Login

1) Local Login:-

- When a user logs into a local computer, then it is known as local login.
- When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver.

- The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.
- However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters have special meanings such as control character with "z" means suspend.
- Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login



2) Remote Login:-

- When the user wants to access an application program on a remote computer, then the user must perform remote login.

- Remote login occurs at the local site and at the remote site.

- At the Local Site:-

  The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack.

- At the Remote Site:-

The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server.

Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

Domain Name System:-

- 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 addressess 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 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

- To map a name onto an IP address, an application program calls a library procedure called Resolver, passing it the name as a parameter.

- The resolver sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller

- Armed with the IP address, the program can then establish a TCP connection with the destination, or send it UDP packets.

- The Internet is divided into several hundred top level domains, where each domain covers many hosts. Each domain is partitioned into sub domains, and these are further partitioned as so on.

- The top level domains are of two types :-

1)Generic domains:-

The generic domains are com(commercial), edu(educational instructions), mil(the U.S armed forces, government), int (certain international organizations), net(network providers), org(non profit organizations).

2)Country domains:-

The country domain include one entry for every country.Each domain is named by following upward path.The components are separated by dots.

Eg:- eng.sum.com

This is called hierarchical naming.

Domain names:-

Domain names can be either absolute (ends with a period e.g. eng.sum.com) or relative (doesn't end with a period). Domain names are non-case sensitive (i.e) com and COM are same.

Domain:-

A domain may be defined as subtree of DNS.A domain may be divided into subdomain.

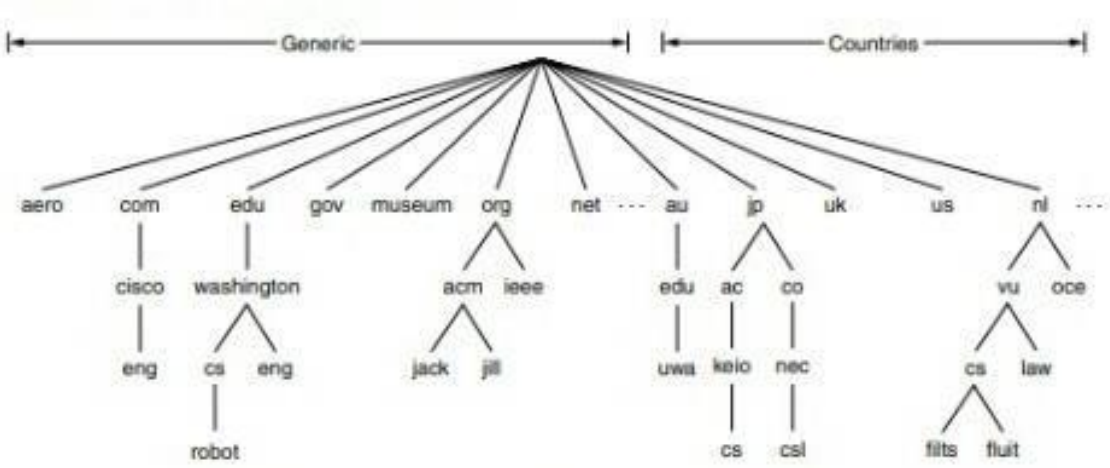


Figure 7-1. A portion of the Internet domain name space.

Resolution:-

The process of mapping a name to an address or an address to a name is called name address resolution.

Resolver:-

- DNS is a client server application. A host which wants to map a name to address called DNS client named resolver.
- The resolver then accesses the closet DNS server with mapping request. If this server has the requested information, it satisfies resolver but if it doesnot have the requested information, then it refers the resolver to other servers or else other servers to provide the information.
- The resolver gives a domain name to server and requests for IP addresses. The server checks the generic or country domains to get mapping.

Name Servers:-

- Name server consists of the DNS database (i.e) various names and their corresponding IP addressing.

- Single name server could contain the entire DNS database. So the information is distributed among many computers called DNS server.

- Then we have to use hierarchy of Name Server. The root can be create many 1st level domains as needed.The first level domains are further divided into second level domains and second level domains into so on.

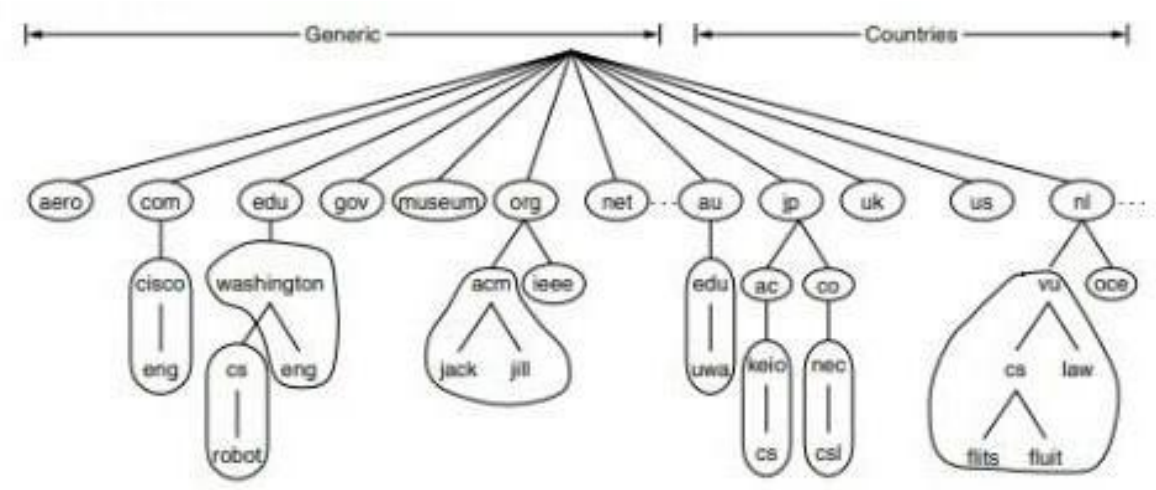


Figure 7-5. Part of the DNS name space divided into zones (which are circled).

The whole DNS namespace is divided into zones. What a server is responsible for has authority over is called zone. The server makes a database called zonefile. It keeps all information about every node underzone.

Security of DNS Name Servers:-

- DNS is organized into a tree-like infrastructure where the first level contains topmost domains, such as *.com* and *.org*.

- The second-level nodes contain general, traditional domain names. The 'leaf' nodes on this tree are known as hosts.

- In DNS attacks, hackers will sometimes target the servers which contain the domain names.
- In other cases, these attackers will try to determine vulnerabilities within the system itself and exploit them for their own good.

Types of Attacks:

1. **Denial of service (DoS) –**
   An attack where the attacker renders a computer useless (inaccessible) to the user by making a resource unavailable or by flooding the system with traffic.
2. **Distributed denial of service (DDoS) –**
   The attacker controls an overwhelming amount of computers (hundreds or thousands) in order to spread malware and flood the victim's computer with unnecessary and overloading traffic. Eventually, unable to harness the power necessary to handle the intensive processing, the systems will overload and crash.
3. **DNS spoofing (also known as DNS cache poisoning) –**
   An attacker will drive the traffic away from real DNS servers and redirect them to a "pirate" server, unbeknownst to the users. This may cause the corruption/theft of a user's personal data.
4. **Fast flux –**
   An attacker will typically spoof his IP address while performing an attack. Fast flux is a technique to constantly change location-based data in order to hide where exactly the attack is coming from. This will mask the attacker's real location, giving him the time needed to exploit the attack. Flux can be single or double or of any other variant. A single flux changes the address of the webserver while double flux changes both the address of the web server and the names of DNS serves.
5. **Reflected attacks –**
   Attackers will send thousands of queries while spoofing their own IP address and using the victim's source address. When these queries are answered, they will all be redirected to the victim himself.
6. **Reflective amplification DoS –**
   When the size of the answer is considerably larger than the query itself, a flux is triggered, causing an amplification effect. This generally uses the same method as a reflected attack, but this attack will overwhelm the user's system's infrastructure further.

Measures against DNS attacks:-

1. Use digital signatures and certificates to authenticate sessions in order to protect private data.
2. Update regularly and use the latest software versions, such as BIND. BIND is open-source software that resolves DNS queries for users. It is widely used by a good majority of the DNS servers on the Internet.
3. Install appropriate patches and fix faulty bugs regularly.

4. Replicate data in a few other servers, so that if data is corrupted/lost in one server, it can be recovered from the others. This could also prevent single-point failure.
5. Block redundant queries in order to prevent spoofing.
6. Limit the number of possible queries.

SNMP(Simple Network Management protocol):-

• It is basically a framework that is used for managing the devices on the internet by using the TCP/IP protocol suite.

• Basically, SNMP provides a set of fundamental operations in order to monitor and maintain the Internet.

• It is an application layer protocol that was defined by the Internet engineering task force.

• This protocol is mainly used to monitor the network, detect the faults in the Network, and sometimes it is also used to configure the remote devices.

Concept of SNMP:-

1. The SNMP protocol makes the use of Manager and Agent; where the manager is usually a host that controls and monitors the set of agents.

2. The SNMP is an application-level protocol and it consists of a few manager stations that mainly controls a set of agents.

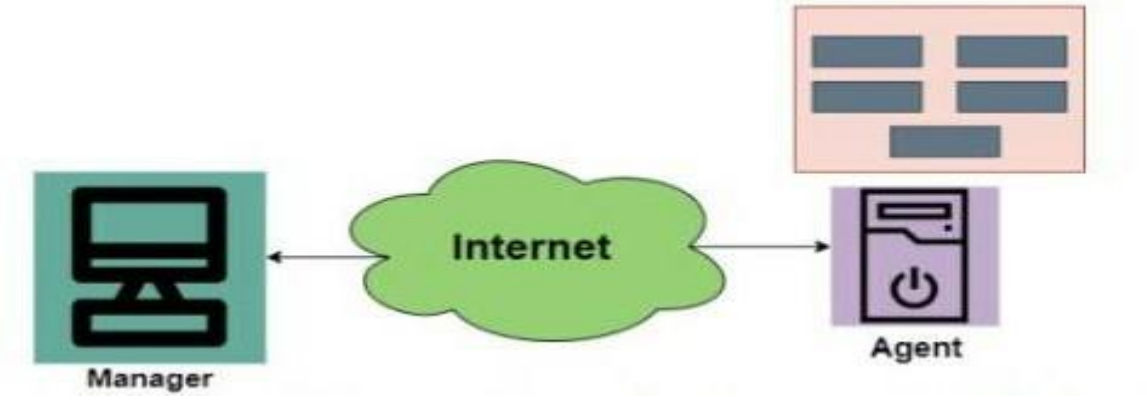
3. This protocol is mainly designed at the application level so that it can monitor the devices that are mainly made by different manufacturers and that are installed on different physical networks.

Thus there are three components in the architecture of the SNMP:

• SNMP Manager

• SNMP Agent

• Management Information Base



1)SNMP Manager:-

It is basically a centralized system and it is mainly used to monitor and manage devices that are connected with the network.SNMP manager is typically a computer and it is used to run one or more network management systems. Given below are the main functions of SNMP Manager:

1. Collects response from the agents.

2. To acknowledge asynchronous events from the agents.

3. To set variables in the agent.

4. Queries the Agent

SNMP Agent:-

SNMP Agent is basically a software program that is packaged within the network element. It is mainly installed on a managed device where managed devices can be switches, servers, routers, PC, etc. Mainly the agents keep the information in the database also the manager has the access to the values present in the database.

Given below are the main responsibilities of the SNMP Agent: • SNMP agents mainly collect the management information about its local environment • The SNMP agent mainly signals an event to the manager. • The SNMP agents also act as a proxy for some non–SNMP manageable network nodes.

Thus the management with SNMP is mainly based on these given ideas:

1. An SNMP manager checks the agent by requesting information that mainly reflects the behavior of the SNMP agent.

2. The SNMP manager also forces the agent to perform the task by resetting the values in the database of the agent.

3. Management process is also contributed by the agent just by warning the SNMP manager about an unusual situation.

Management Components:-

In order to perform the Management tasks, the SNMP protocol makes the use of two other protocols and are SMI and MIB. We can also say that the Management on the Internet is done by the cooperation of three protocols and these are SNMP, MIB, SMI.

Role of SNMP :-

The SNMP protocol performs some specific roles in Network Management;

• It mainly defines the format of the packet that needs to be sent from the manager to the agent or viceversa.

• SNMP is also used to interpret the result and create the statistics.

• The packets that are exchanged between the manager and agent contains the name of the object(variable) and their status(values).

• The SNMP is also responsible for reading and changing these values.

Role of SMI:-

In order to use the SNMP, there is a need for some rules and these rules are for naming the objects. Now its time to take a look at the roles of SMI:

• SMI(Structure of Management Information) is mainly used to define the general rules for naming the objects.

• It is also used to define the type of objects that includes(range and length).

• This is also used to show how to encode the objects and values.

• The SMI does not define the number of objects that should be managed by an entity.

• It also does not define the association between the objects and their values.

Role of MIB:-

In order to manage each entity, this protocol is mainly used to define the number of objects and then to name them according to the rules defined by the SMI and after that associate a type to each named object.

• MIB(Management Information Base) is mainly used to create a set of objects that are defined for each entity that is similar to the database.

• Thus MIB mainly creates a collection of named objects, their types.

Advantages of SNMP Protocol :-

Given below are some of the benefits of using SNMP :

1. It is the standard network management protocol.

2. This protocol is independent of the operating system and programming language.

3. The functional design of this protocol is Portable.

4. The SNMP is basically a core set of operations and it remains the same on all managed devices. Thus SNMP supports extendibility.

5. SNMP is a universally accepted protocol.

6. It is a lightweight protocol.

7. This protocol allows distributed management access.

Disadvantages:-

Some of the drawbacks of SNMP are as follows:

• This protocol leads to the reduction of the bandwidth of the network.

• Access control, authentication, and privacy of data are some largest security issues using this.

• SNMP deals with information that is neither detailed nor enough well organized.