Computer Network

Transport Layer

Ms. Pooja Sisodiya

Assistant Professor CE & IT

Transport Layer

- To provide reliable, cost effective data transfer from source to destination
- This layer deals with end to end transfer of data
- Here transport entity deals with other host’s transport entity
- transport layer deals with processes running on host

Elements of Transport Protocol

- **Addressing**
- **Connection Establishment**
- **Connection release**
- **Flow control and buffering**
- **Multiplexing**
- **Crash Recovery**

Elements of Transport Protocol

ADDRESSING:

- When an application (e.g., a user) process wishes to set up a connection to a remote application process, it must specify which one to connect to.
- The method normally used is to define transport addresses to which processes can listen for connection requests.
- In the Internet, these endpoints are called ports.
- There are two types of access points
- TSAP (Transport Service Access Point) to mean a specific endpoint in the transport layer.
- The analogous endpoints in the network layer (i.e., network layer addresses) are not surprisingly called NSAPs (Network Service Access Points).
- IP addresses are examples of NSAPs.
- Application processes, both clients and servers, can attach themselves to a local TSAP to establish a connection to a remote TSAP.
- These connections run through NSAPs on each host.

Elements of Transport Protocol

ADDRESSING: Continue..

•The purpose of having TSAPs is that in some networks, each computer has a single NSAP, so some way is needed to distinguish multiple transport endpoints that share that NSAP.

A possible scenario for a transport connection is as follows:

1.A mail server process attaches itself to TSAP 1522 on host 2 to wait for an incoming call.

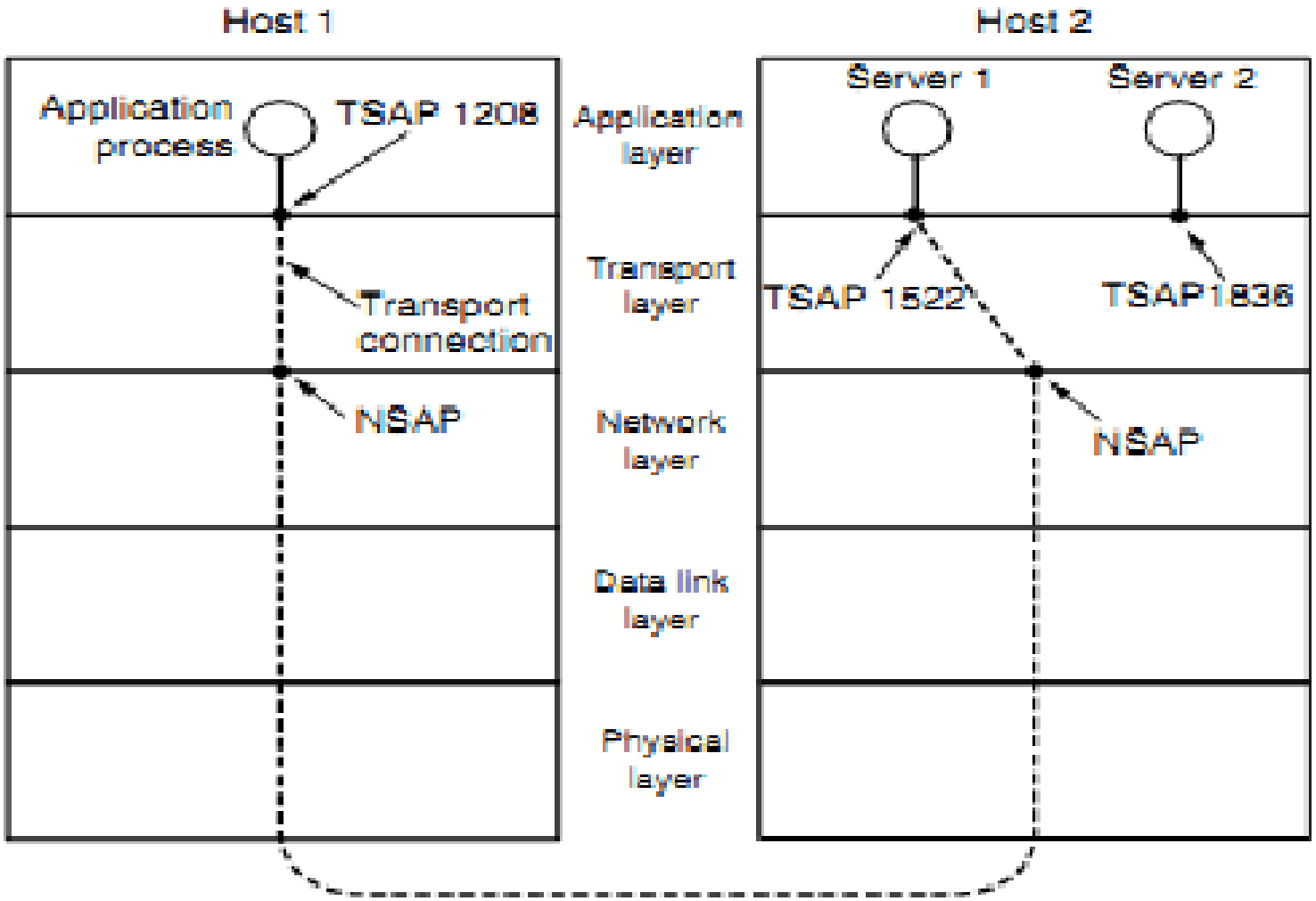
- How a process attaches itself to a TSAP is outside the networking model and depends entirely on the local operating system.
- A call such as our LISTEN might be used, for example.

2.An application process on host 1 wants to send an email message, so it attaches itself to TSAP 1208 and issues a CONNECT request.

- The request specifies TSAP 1208 on host 1 as the source and TSAP 1522 on host 2 as the destination.
- This action ultimately results in a transport connection being established between the application process and the server.

Elements of Transport Protocol

ADDRESSING: Continue



Elements of Transport Protocol

ADDRESSING: Continue

4.The application process sends over the mail message.

5.The mail server responds to say that it will deliver the message.

6.The transport connection is released

CONNECTION ESTABLISHMENT:

•With packet lifetimes bounded, it is possible to devise a fool proof way to establish connections safely.

Packet lifetime can be bounded to a known maximum using one of the following techniques:

- Restricted subnet design
- Putting a hop counter in each packet
4. Time stamping in each packet

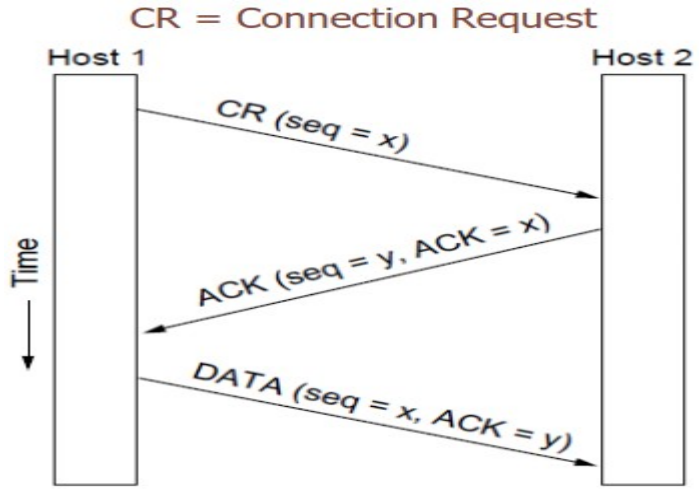
4.Using a 3-way hand shake, a connection can be established.

5.This establishment protocol doesn't require both sides to begin sending with the same sequence number.

Elements of Transport Protocol

CONNECTION ESTABLISHMENT:

- This establishment protocol involves one peer checking with the other that the connection request is indeed current.
- Host 1 chooses a sequence number, x , and sends a CONNECTION REQUEST segment containing it to host 2.
- Host 2replies with an ACK segment acknowledging x and announcing its own initial sequence number, y.
- Finally, host 1 acknowledges host 2's choice of an initial sequence number in the first data segment that it sends



Elements of Transport Protocol

CONNECTION RELEASE:

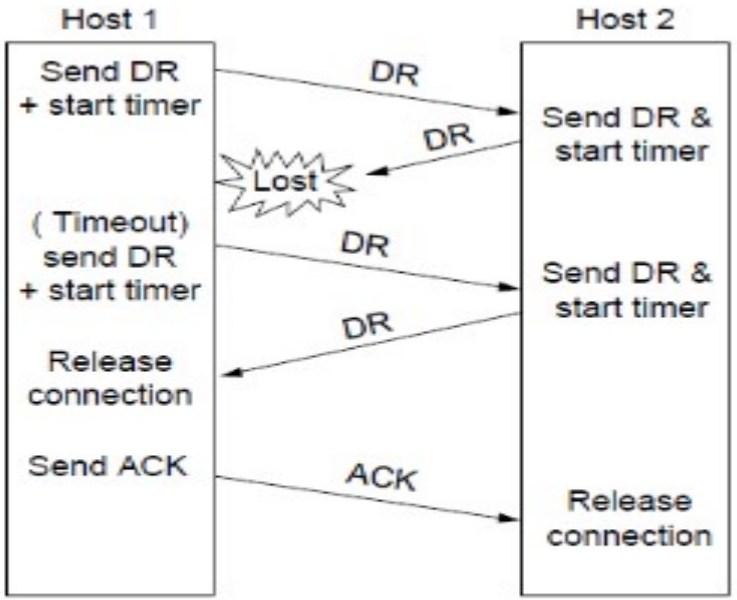
- A connection is released using either asymmetric or symmetric variant.
- But, the improved protocol for releasing a connection is a 3-way handshake protocol.
- **There are two styles of terminating a connection:**

1) Asymmetric release: Asymmetric release is the way the telephone system works: when one party hangs up, the connection is broken.

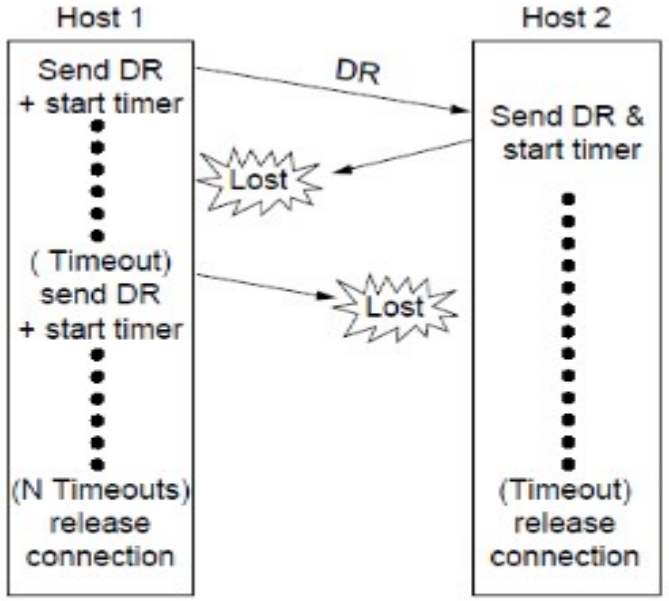
2) Symmetric release: Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately.

Elements of Transport Protocol

CONNECTION RELEASE:



Lost DR:
H1 starts over



Extreme:
Many lost DRs
both release after N

Elements of Transport Protocol

FLOW CONTROL AND BUFFERING:

- Flow control is done by having a sliding window on each connection to keep a fast transmitter from over running a slow receiver.
- Buffering must be done by the sender, if the network service is unreliable.
- The sender buffers all the TPDUs sent to the receiver.
- The buffer size varies for different TPDUs. They are:

a) Chained Fixed-size Buffers

b) Chained Variable-size Buffers

c) One large Circular Buffer per Connection

MULTIPLEXING:

- In networks that use virtual circuits within the subnet, each open connection consumes some table space in the routers for the entire duration of the connection.
- If buffers are dedicated to the virtual circuit in each router as well, a user who left a terminal logged into a remote machine, there is need for multiplexing.
- There are 2 kinds of multiplexing: **UP-WARD and DOWN-WARD MULTIPLEXING**

Transmission Control Protocol (TCP)

- TCP stands for Transmission Control Protocol.
- It is a transport layer protocol that facilitates the transmission of packets from source to destination.
- It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network.
- This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.
- Features of TCP protocol**:**
- **Transport Layer Protocol**
- **Reliable**
- **Order of the data is maintained**
- **Connection-oriented**
- **Full duplex**

Transmission Control Protocol (TCP)

The different issues to be considered are:

1.The TCP Service Model 2. The TCP Protocol 3. The TCP Segment Header 4. The Connection Management 5. TCP Transmission Policy 6. TCP Congestion Control 7. TCP Timer Management.

The TCP Service Model:

- TCP service is obtained by having both the sender and receiver create end points called SOCKETS. Each socket has a socket number(address)consisting of the IP address of the host, called a "PORT" (=TSAP)
- To obtain TCP service a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine
- All TCP connections are full duplex and point to point i.e., multicasting or broadcasting is not supported.
- A TCP connection is a byte stream, not a message stream i.e., the data is delivered as chunks

Transmission Control Protocol (TCP)

Sockets:

- A socket may be used for multiple connections at the same time.
- In other words, 2 or more connections may terminate at same socket.
- Connections are identified by socket identifiers at same socket.
- Connections are identified by socket identifiers at both ends.

Some of the sockets are listed below:

Primitive	Meaning
SOCKET	Creat new communication end points
BIND	attached a local address to a socket
LISTEN	announced williness to accept connection, give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	actively attempt to established connection
SEND	Send some data over the connection

Transmission Control Protocol (TCP)

The TCP Protocol:

- A key feature of TCP, and one which dominates the protocol design, is that every byte on a TCP connection has its own 32-bit sequence number
- When the Internet began, the lines between routers were mostly 56-kbps leased lines, so a host blasting away at full speed took over 1 week to cycle through the sequence numbers.
- The basic protocol used by TCP entities is the sliding window protocol.
- When a sender transmits a segment, it also starts a timer.
- When the segment arrives at the destination, the receiving TCP entity sends back a segment (with data if any exist, otherwise without data) bearing an acknowledgement number equal to the next sequence number it expects to receive.
- If the sender's timer goes off before the acknowledgement is received, the sender transmits the segment again.

Transmission Control Protocol (TCP)

The TCP Segment Header:

- Every segment begins with a fixed-format, 20-byte header.
- The fixed header may be followed by header options.
- After the options, if any, up to 65,535 - 20 - 20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header.
- Segments without any data are legal and are commonly used for acknowledgements and control messages.

Source port: It defines the port of the application, which is sending the data. So, this field contains the source port address, which is 16 bits.

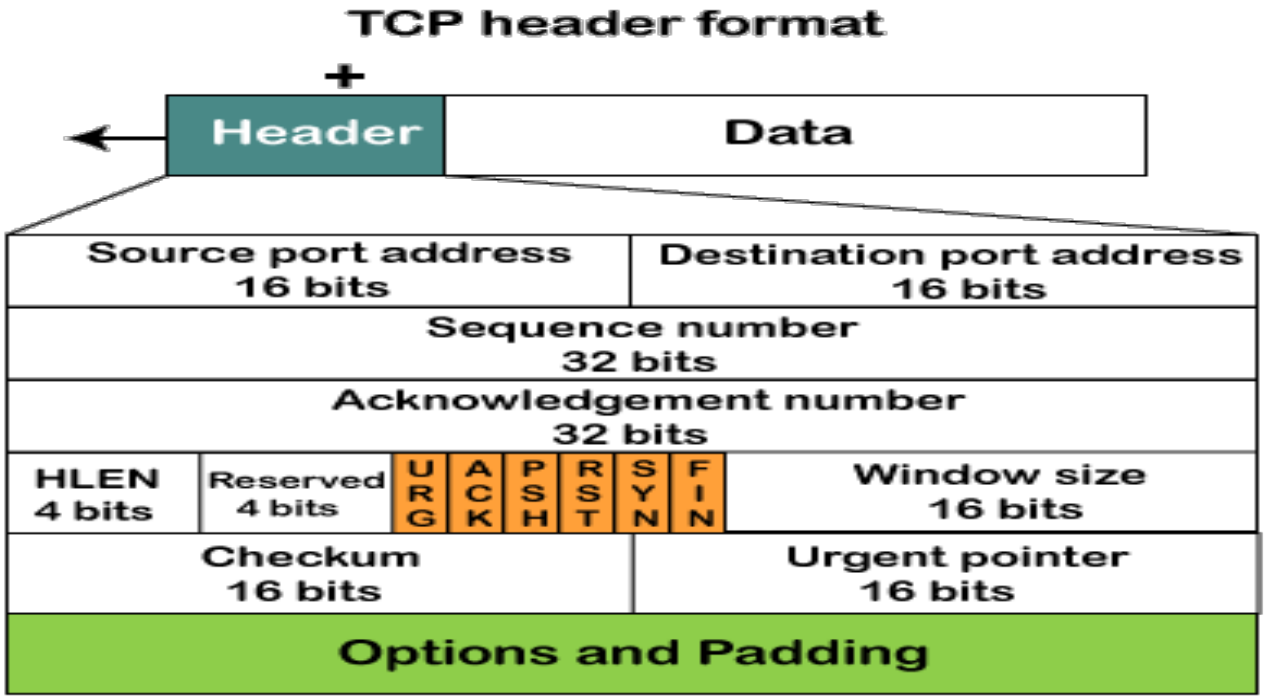
Destination port: It defines the port of the application on the receiving side. So, this field contains the destination port address, which is 16 bits.

Sequence number: This field contains the sequence number of data bytes in a particular session.

Transmission Control Protocol (TCP)

The TCP Segment Header:

Acknowledgment number: When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received. For example, if the receiver receives the segment number 'x', then it responds 'x+1' as an acknowledgment number.



Transmission Control Protocol (TCP)

HLEN: It specifies the length of the header indicated by the 4-byte words in the header.

- The size of the header lies between 20 and 60 bytes. Therefore, the value of this field would lie between 5 and 15
- Reserved: It is a 4-bit field reserved for future use, and by default, all are set to zero.

Flags: There are six control bits or flags:

URG: It represents an urgent pointer. If it is set, then the data is processed urgently.

ACK: If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.

PSH: If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.

RST: If it is set, then it requests to restart a connection.

SYN: It is used to establish a connection between the hosts.

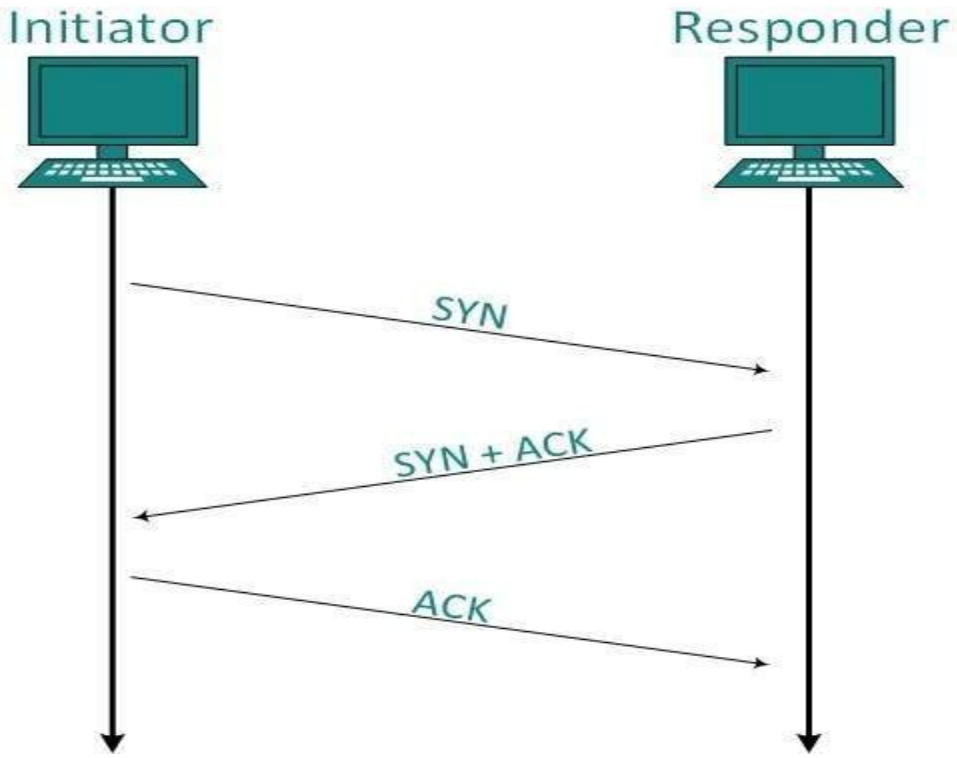
FIN: It is used to release a connection, and no further data exchange will happen.

Transmission Control Protocol (TCP)

- **Window size:** It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment. The value of this field is determined by the receiver.
- **Checksum:** It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.
- **Urgent pointer:** It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.
- **Options:** It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.

Transmission Control Protocol (TCP)

Connection Management:TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



Transmission Control Protocol (TCP)

- **Establishment:** Client initiates the connection and sends the segment with a Sequence number.
- Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number.
- Client after receiving ACK of its segment sends an acknowledgement of Server's response.
- **Release:** Either of server and client can send TCP segment with FIN flag set to 1.
- When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

Congestion control

Congestion Control: When large amount of data is fed to system which is not capable of handling it, congestion occurs.

- TCP controls congestion by means of Window mechanism.
- TCP sets a window size telling the other end how much data segment to send.

TCP may use three algorithms for congestion control:

1.Additive increase, Multiplicative Decrease

2.Slow Start

3.Timeout React

- TCP reacts to congestion by reducing the sender window size.
- The size of the sender window is determined by the following two factors-
  - Receiver window size
  - Congestion window size

Receiver Window Size: Receiver window size is an advertisement of- "How much data (in bytes) the receiver can receive without acknowledgement?"

- Sender should not send data greater than receiver window size.

Transmission Control Protocol (TCP)

- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.
- So, sender should always send data less than or equal to receiver window size.
- Receiver dictates its window size to the sender through TCP Header.

Congestion Window:

- Sender should not send data greater than congestion window size.
- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.
- So, sender should always send data less than or equal to congestion window size.
- Different variants of TCP use different approaches to calculate the size of congestion window.
- Congestion window is known only to the sender and is not sent over the links.

Transmission Control Protocol (TCP)

TCP Congestion Policy:

1.Slow Start

2.Congestion Avoidance

3.Congestion Detection

Transmission Control Protocol (TCP)

Congestion prevention policies:

I) Retransmission Policy:

- The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.
- However retransmission increases the congestion in the network.
- But we need to implement good retransmission policy to prevent congestion.
- The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

II) Window Policy:

- To implement window policy, selective reject window method is used for congestion control.
- Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver.
- Thus, this duplication may make congestion worse.
- Selective reject method sends only the specific lost or damaged packets.

Transmission Control Protocol (TCP)

III) Acknowledgement Policy:

- The acknowledgement policy imposed by the receiver may also affect congestion.
- If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.
- Acknowledgments also add to the traffic load on the network.
- Thus, by sending fewer acknowledgements we can reduce load on the network.
- To implement it, several approaches can be used:
- A receiver may send an acknowledgement only if it has a packet to be sent.
- A receiver may send an acknowledgement when a timer expires.
- A receiver may also decide to acknowledge only N packets at a time.

Transmission Control Protocol (TCP)

IV) Discarding Policy:

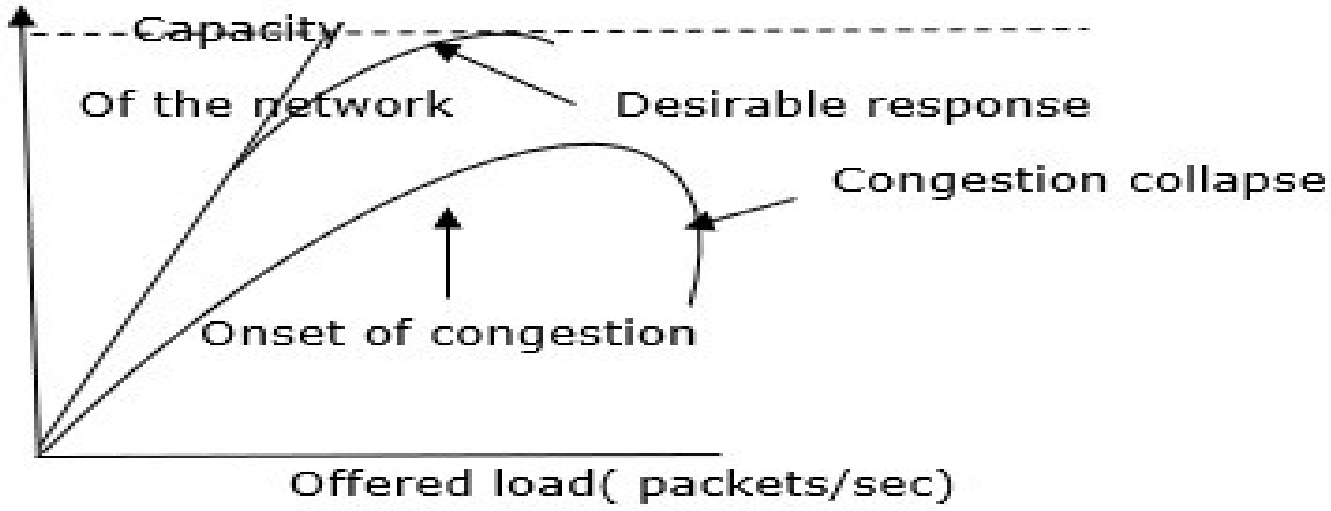
- A router may discard less sensitive packets when congestion is likely to happen.
- Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

V) Admission Policy:

- An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.
- Switches in a flow, first check the resource requirement of a flow before admitting it to the network.
- A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Leaky bucket and token bucket algorithms

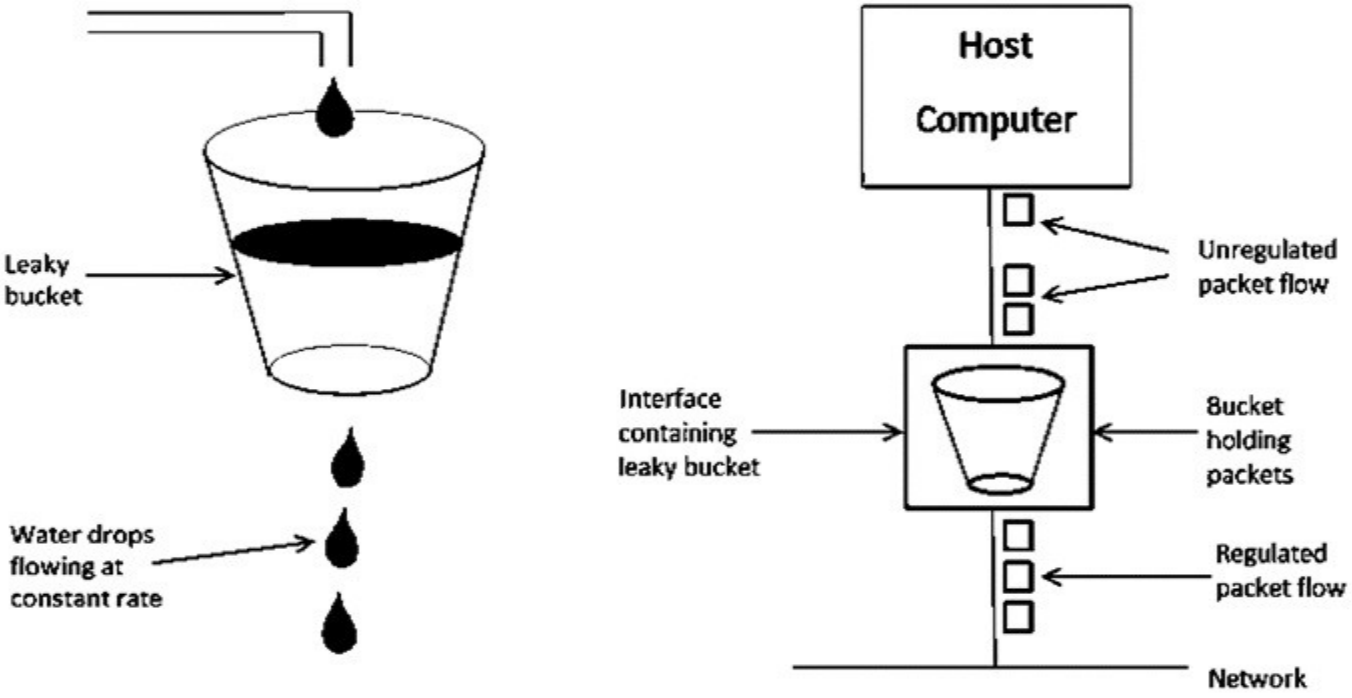
- The network layer and transport layer share the responsibility for handling congestions.
- One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network.
- To maintain this, the network and transport layers have to work together.
- With too much traffic, performance drops sharply.



Leaky bucket and token bucket algorithms

- There are two types of Congestion control algorithms, which are as follows −
- Leaky Bucket Algorithm.
- Token Bucket Algorithm.

Leaky Bucket Algorithm: Let see the working condition of Leaky Bucket Algorithm −



Leaky bucket and token bucket algorithms

Leaky Bucket Algorithm: Continue...

- Leaky Bucket Algorithm mainly controls the total amount and the rate of the traffic sent to the network.
- Step 1 − Let us imagine a bucket with a small hole at the bottom where the rate at which water is poured into the bucket is not constant and can vary but it leaks from the bucket at a constant rate.
- Step 2 − So (up to water is present in the bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.
- Step 3 − If the bucket is full, additional water that enters into the bucket that spills over the sides and is lost.
- Step 4 − Thus the same concept applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 10 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 8 Mbps for 2 seconds. Thus, in a time span of 8 seconds, 68 Mb data has been transmitted.

Leaky bucket and token bucket algorithms

Token Bucket Algorithm: The leaky bucket algorithm enforces output patterns at the average rate, no matter how busy the traffic is.

- So, to deal with the more traffic, we need a flexible algorithm so that the data is not lost. One such approach is the token bucket algorithm.
- Let us understand this algorithm step wise as given below −

Step 1 − In regular intervals tokens are thrown into the bucket f.

Step 2 − The bucket has a maximum capacity f.

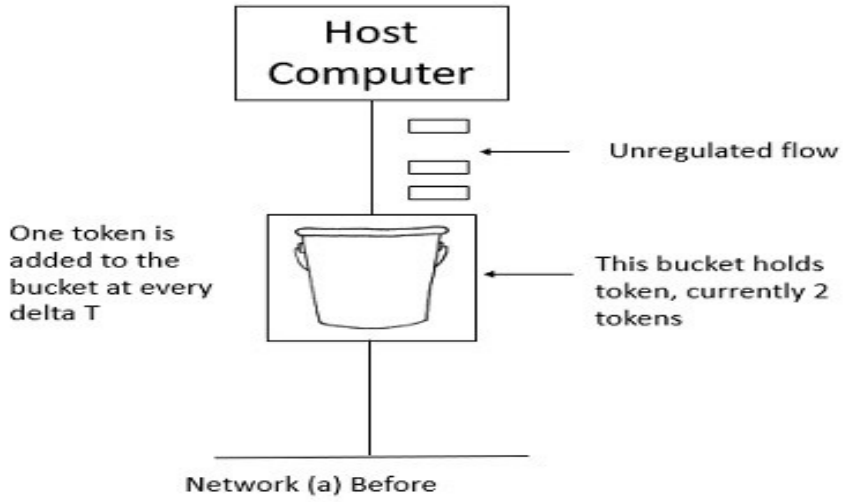
Step 3 − If the packet is ready, then a token is removed from the bucket, and the packet is sent.

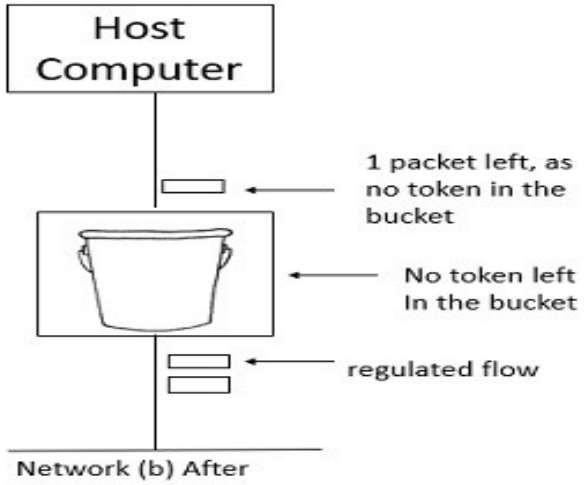
Step 4 − Suppose, if there is no token in the bucket, the packet cannot be sent.

Leaky bucket and token bucket algorithms

Example:

- Let us understand the Token Bucket Algorithm with an example −:
- In figure (a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface.
- In Figure (b) two packets have been sent out by consuming two tokens, and 1 packet is still left.





Hyper Text Transfer Protocol (HTTP)

- HTTP stands for Hypertext Transfer Protocol and is mainly used to access the data on the world wide web i.e (WWW).
- The HTTP mainly functions as the combination of FTP(File Transfer Protocol) and SMTP(Simple Mail Transfer Protocol).
- HTTP is one of the protocols used at the Application Layer.
- The HTTP is similar to FTP because HTTP is used to transfer the files and it mainly uses the services of TCP.
- Also, HTTP is much simpler than FTP because there is only one TCP connection.
- In HTTP, there is no separate control connection, as only data is transferred between the client and the server.
- The HTTP is like SMTP because the transfer of data between the client and server simply looks like SMTP messages. But there is a difference unlike SMTP, the HTTP messages are not destined to be read by humans as they are read and interpreted by HTPP Client(that is browser) and HTTP server.

Hyper Text Transfer Protocol (HTTP)

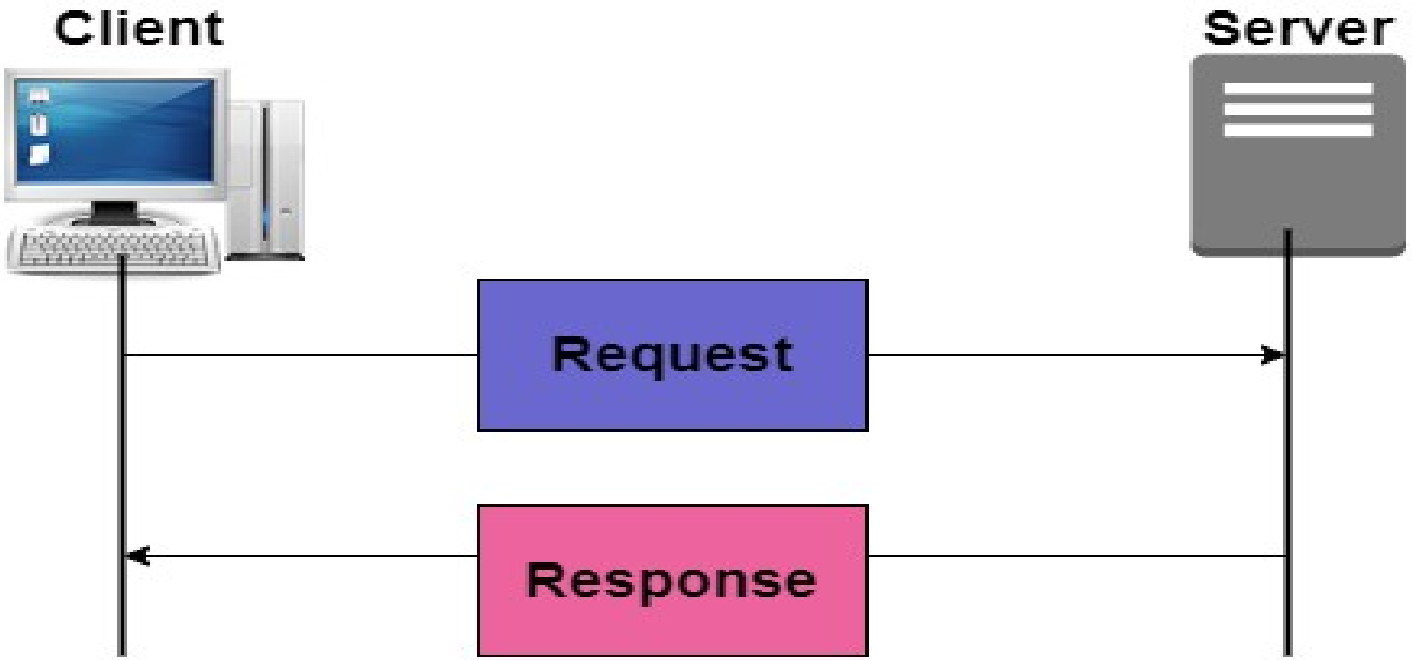
- Also, SMTP messages are stored and then forwarded while the HTTP messages are delivered immediately.
- The HTTP mainly uses the services of the TCP on the well-known port that is port 80.
- HTTP is a stateless protocol.
- In HTTP, the client initializes the transaction by sending a request message, and the server replies by sending a response.
- This protocol is used to transfer the data in the form of plain text, hypertext, audio as well as video, and so on

Working of HTTP:

- The HTTP makes use of Client-server architecture.
- As we have already told you that the browser acts as the HTTP client and this client mainly communicates with the webserver that is hosting the website.

Hyper Text Transfer Protocol (HTTP)

- The format of the request and the response message is similar.
- The Request Message mainly consists of a request line, a header, and a body sometimes.
- A Response message consists of the status line, a header, and sometimes a body.

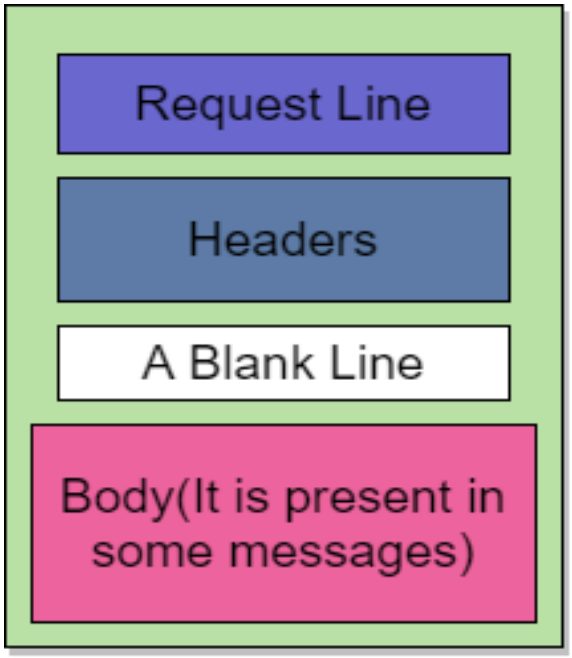


Hyper Text Transfer Protocol (HTTP)

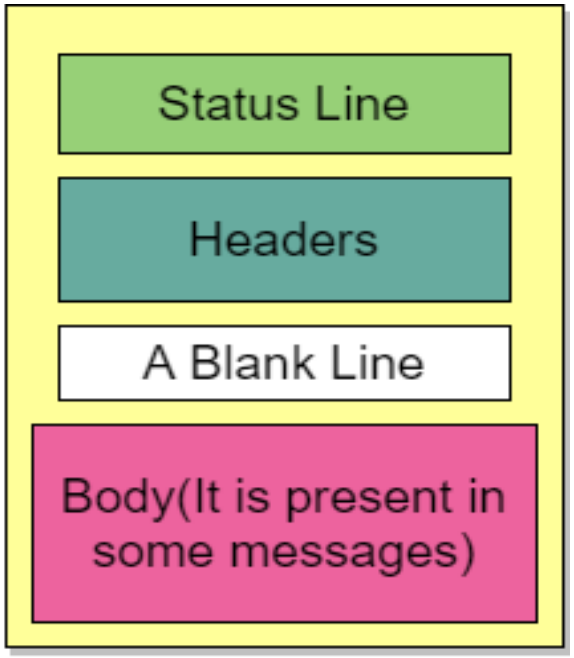
- At the time when a client makes a request for some information (say client clicks on the hyperlink) to the webserver.
- The browser then sends a request message to the HTTP server for the requested objects.
- After that the following things happen:
  - There is a connection that becomes open between the client and the webserver through the TCP.
  - After that, the HTTP sends a request to the server that mainly collects the requested data.
  - The response with the objects is sent back to the client by HTTP
  - At last, HTTP closes the connection.

Hyper Text Transfer Protocol (HTTP)

- Let us take a look at the format of the request message and response message



Request Message

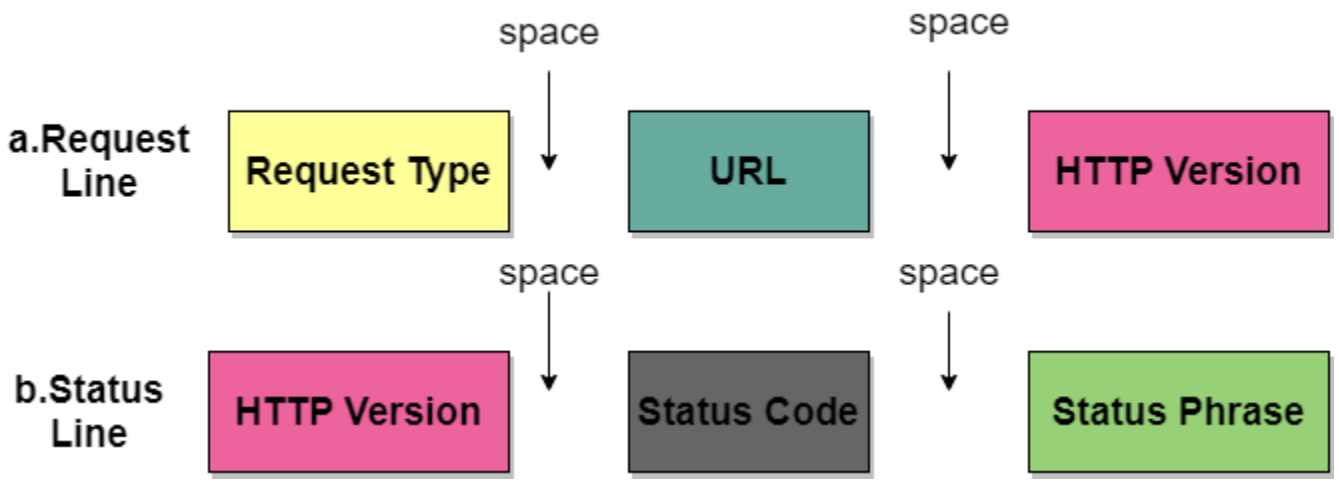


Response Message

Hyper Text Transfer Protocol (HTTP)

1. Request Line and Status line:

•The first line in the Request message is known as the request line, while the first line in the Response message is known as the Status line.



Where,

1.1 Request Type:

•This field is used in the request line. The are several request types that are defined and these are mentioned in the table on next slide

Hyper Text Transfer Protocol (HTTP)

- **Request Type:**

Name of Method	Actions
GET	This method is used to request a document from the server.
HEAD	This method mainly requests information about a document and not the document itself
POST	This method sends some information from the client to the server.
PUT	This method sends a document from the server to the client.
TRACE	This method echoes the incoming request.
CONNECT	This method means reserved
OPTION	In order to inquire about the available options.

Hyper Text Transfer Protocol (HTTP)

1.2 URL: URL is a Uniform Resource locator and it is mainly a standard way of specifying any kind of information on the Internet.

1.3 HTTP Version: The current version of the HTTP is 1.1.

1.4 Status Code: The status code is the field of the response message.The status code consists of three digits.

1.5 Status Phrase: This field is also used in the response message and it is used to explain the status code in the form of text.

2. Header: The header is used to exchange the additional information between the client and the server.

- The header mainly consists of one or more header lines. Each header line has a header name, a colon, space, and a header value.

•The header line is further categorized into four:

2.1 General Header: It provides general information about the message and it can be present in both request and response.

2.2 Request Header: It is only present in the request message and is used to specify the configuration of the client and the format of the document preferred by the client

Hyper Text Transfer Protocol (HTTP)

2.3 Response Header: This header is only present in the response header and mainly specifies the configuration of the server and also the special information about the request.

2.4 Entity Header: It is used to provide information about the body of the document.

3. Body: It can be present in the request message or in the response message. The body part mainly contains the document to be sent or received.

Hyper Text Transfer Protocol (HTTP)

Features of HTTP:

•The HTTP offers various features and these are as follows:

- HTTP is simple The HTTP protocol is designed to be plain and human-readable.
- HTTP is stateless Hypertext transfer protocol(HTTP) is a stateless protocol, which simply means that there is no connection among two requests that are being consecutively carried out on the same connection.
  - Also, both the client and the server know each other only during the current requests and thus the core of the HTTP is itself a stateless one, On the other hand, the HTTP cookies provide in making use of stateful sessions.
- HTTP is extensible The HTTP can be integrated easily with the new functionality by providing a simple agreement between the client and the server.
- HTTP is connectionless As the HTTP request is initiated by the browser (HTTP client) and as per the request information by the user, after that the server processes the request of the client and then responds back to the client

Hyper Text Transfer Protocol (HTTP)

Advantages of HTTP:

- Given below are the benefits of using HTTP:
- There is no runtime support required to run properly.
- As it is connectionless so there is no overhead in order to create and maintain the state and information of the session.
- HTTP is usable over the firewalls and global application is possible.
- HTTP is platform-independent.
- HTTP reports the errors without closing the TCP connection.
- Offers Reduced Network congestions.

Disadvanatges of HTTP:

- HTTP is not optimized for mobile.
- HTTP is too verbose.
- It can be only used for point-to-point connections.
- This protocol does not have push capabilities.
- This protocol does not offer reliable exchange without the retry logic.

File Transfer Protocol (FTP)

- FTP stands for 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.

Objectives of FTP:

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

- Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems.
- For example, two systems may have different file conventions.

File Transfer Protocol (FTP)

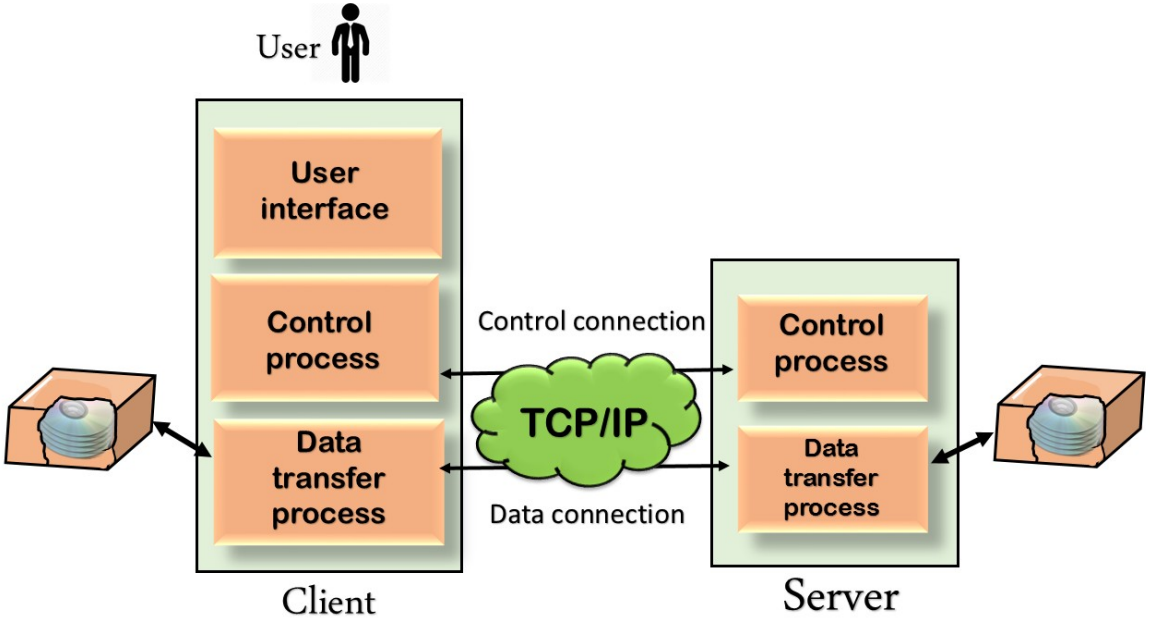
Why FTP?

- Two systems may have different ways to represent text and data.
- Two systems may have different directory structures.
- FTP protocol overcomes these problems by establishing two connections between hosts.
- One connection is used for data transfer, and another connection is used for the control connection.

File Transfer Protocol (FTP)

Mechanism of FTP:

- The below figure shows the basic model of the FTP.
- The FTP client has three components: the user interface, control process, and data transfer process.
- The server has two components: the server control process and the server data transfer process.



File Transfer Protocol (FTP)

There are two types of connections in FTP:

- **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.

File Transfer Protocol (FTP)

FTP Clients:

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

Domain Name System (DNS)

- 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.
- For example, suppose the FTP site at indusuni had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.indusuni.ac.in.
- Therefore, the domain name is more reliable than IP address.

Domain Name System (DNS)

- 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.
- Generic Domains
- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers

Domain Name System (DNS)

Country Domain:

•The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., in for India) in place of three character organizational abbreviations.

Inverse Domain:

•The inverse domain is used for mapping an address to a name.

•When the server has received a request from the client, and the server contains the files of only authorized clients.

•To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS:

•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.

Domain Name System (DNS)

- 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.
- DHCP can be implemented on local networks as well as large enterprise networks.
- DHCP is the default protocol used by the most routers and networking equipment.
- DHCP is also called RFC (Request for comments) 2131.

Dynamic Host Configure Protocol (DHCP)

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol).
- DHCP automates and centrally manages these configurations.
- There is no need to manually assign IP addresses to new devices.
- Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

Dynamic Host Configure Protocol (DHCP)

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network.
    - The server acknowledges by providing an IP address to the client/node/device.
- DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.
- There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

Dynamic Host Configure Protocol (DHCP)

How DHCP works:

•DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients.

- Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

•DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows:

•First of all, a client (network device) must be connected to the internet.

•DHCP clients request an IP address. Typically, client broadcasts a query for this information.

•DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.

•When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Dynamic Host Configure Protocol (DHCP)

Components of DHCP: When working with DHCP, it is important to understand all of the components. Following are the list of components:

DHCP Server: DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

DHCP client: DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.

IP address pool: IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.

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

Dynamic Host Configure Protocol (DHCP)

Lease: Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.

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

- The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Dynamic Host Configure Protocol (DHCP)

Benefits of DHCP:

- **Centralized administration of IP configuration:** DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.
- **Dynamic host configuration:** DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.
- **Seamless IP host configuration:** The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.
- **Flexibility and scalability:** Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.