Page No:
Date:

Network

A network is the interconnection of a set of devices capable of communication.

- A device can be a host such as large computer, desktop, laptop, workstation, cellular phone or security system.
- A device can be a connecting device such as router, a switch, a modem that changes the form of data.

- Local Area Networks (LAN)
- Wide Area Networks (WAN)
  - Point-to-point WANs
  - Switched WANs
- Internetwork

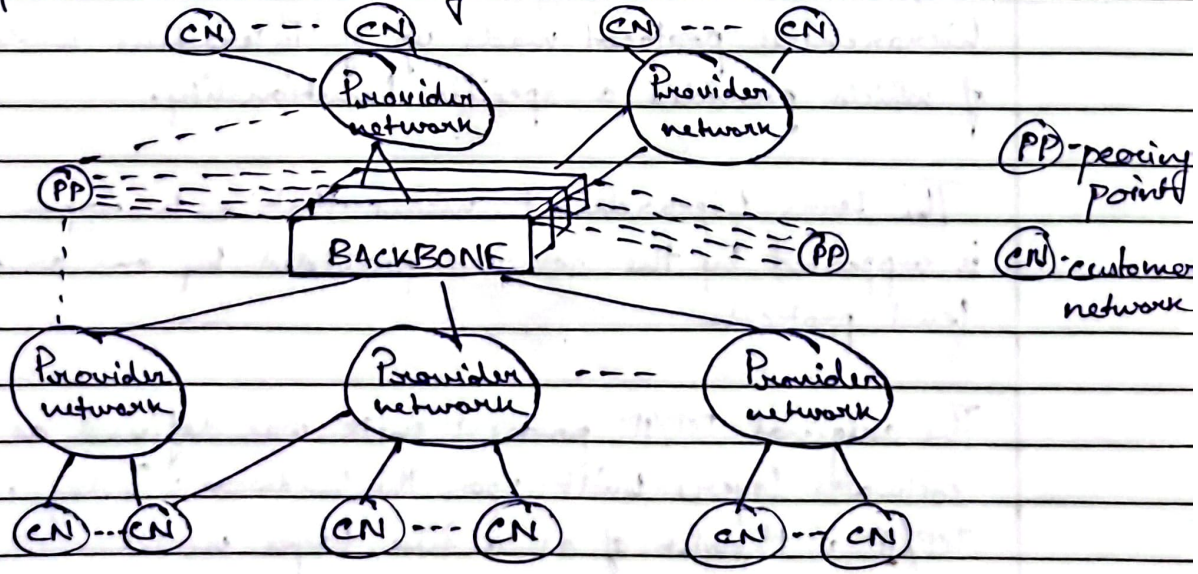
Switching

An internet is a switched network in which a switch connects atleast two links together. A switch needs to forward data from a link to another link when required.

- Circuit Switched Network
- Packet Switched Network

Internet

The most notable internet is called the Internet and is composed of thousands of interconnected networks.



Accessing the internet

The internet today is an internetwork that allows any user to be a part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point to point WAN

- Using telephone networks
  - Using dial up service
  - DSL
- Using cable networks
- Using wireless networks
- Direct connection

* Protocol layering - Defines the rules that both the sender and receiver and all the intermediate devices need to follow to be able to communicate effectively.

When communication is simple, we may need only one simple protocol; when the communication is complex, we need a protocol at each layer or protocol layering

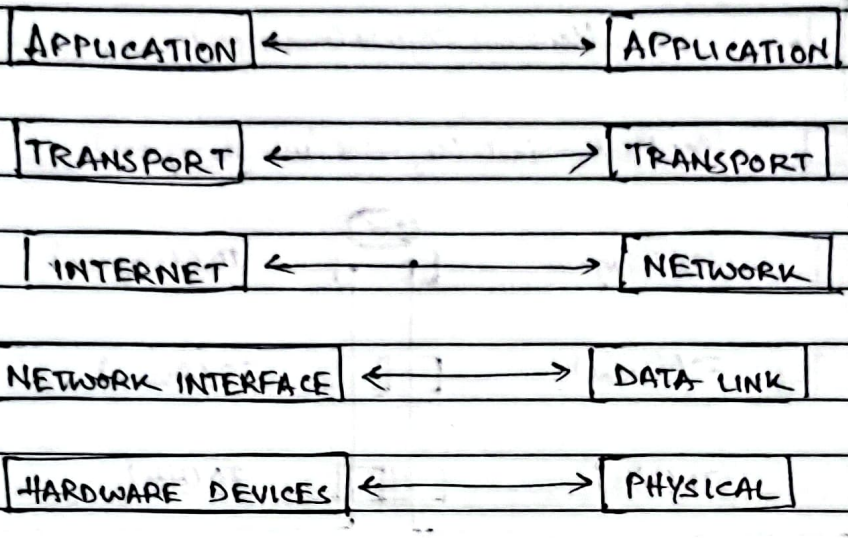
* TCP/IP Protocol Suite

TCP/IP Protocol Suite used in the internet today is a hierarchical protocol made up of interactive modules each of which provides a specific functionality.

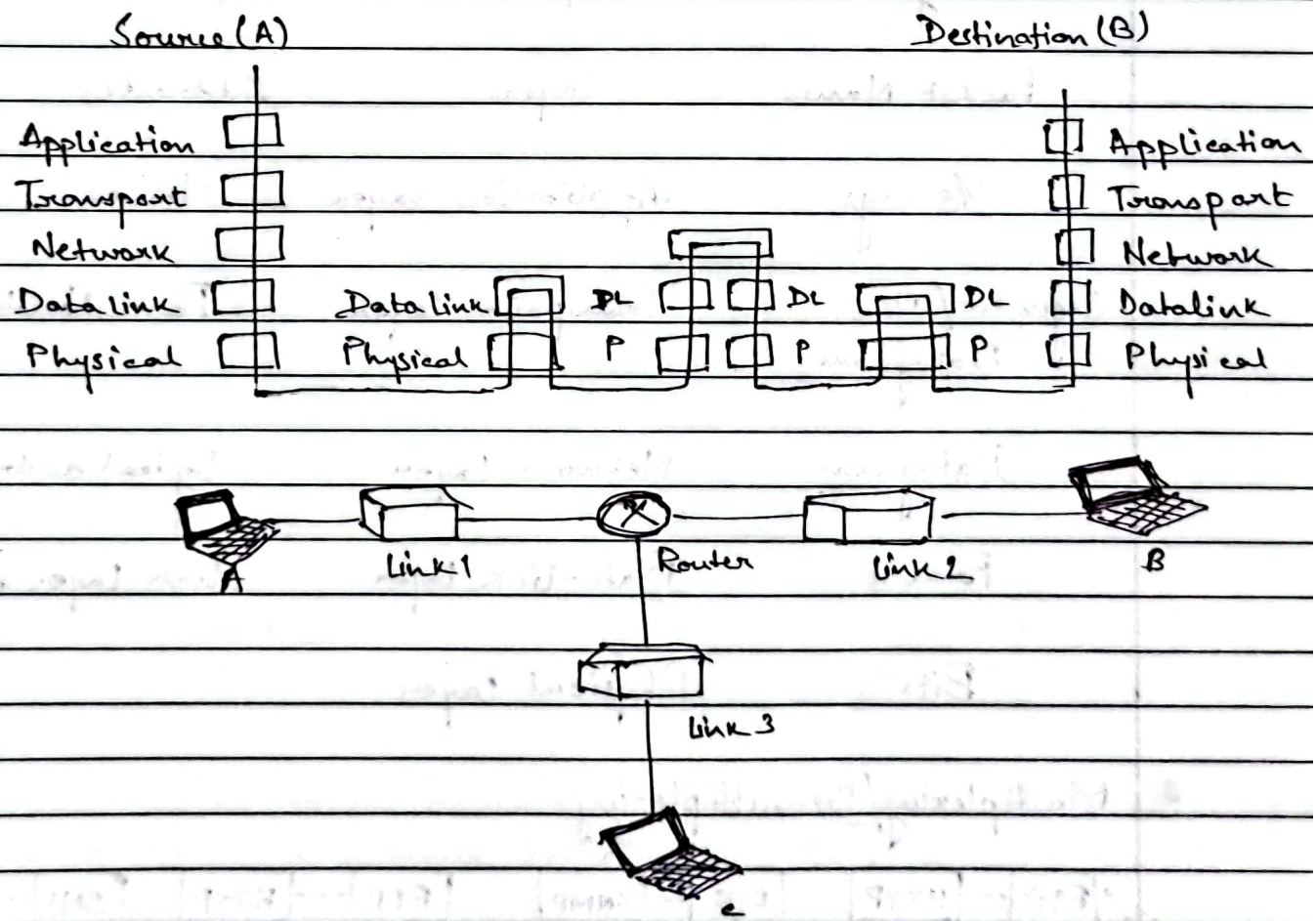
The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols

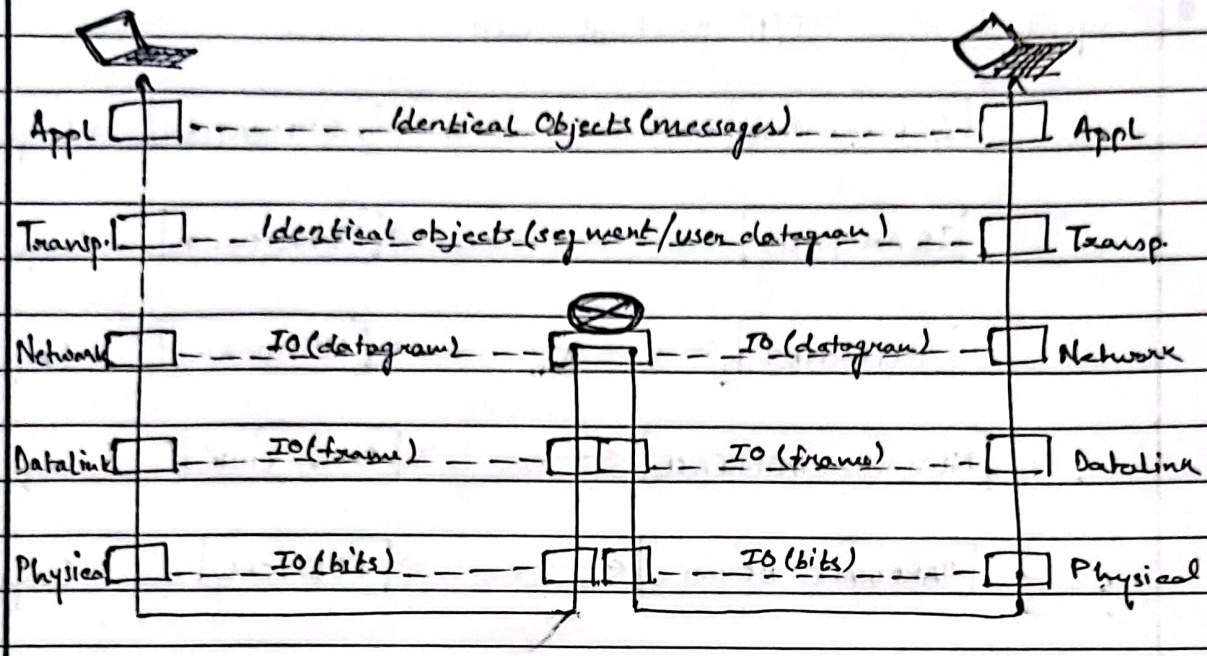
The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however TCP/IP is thought of as a five layer model

Layers in the TCP/IP protocol suite



Communication through an internet

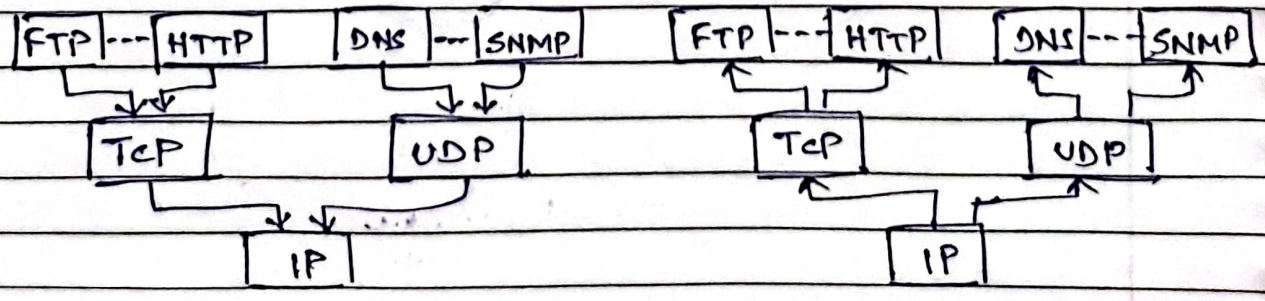




Addressing in the TCP/IP protocol suite

Packet Names	Layers	Addresses
Message	Application Layer	Names
Segment/User Datagram	Transport layer	Port Numbers
Datagram	Network Layer	Logical addresses
Frame	Data-Link layer	Link Layer address
Bits	Physical layer	

Multiplexing/Demultiplexing



multiplexing at source demultiplexing at destination

Page No:
Date:

The OSI Model

Established in 1947, ISO is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data link
Layer 1	Physical

TCP/IP and OSI Model

Application	Application	} General application protocols
Presentation		
Session		
Transport	Transport	} General transport pro
Network	Network	} IP & helping protocol
Data link	Data link	} Underlying LAN and WAN tech.
Physical	Physical	

OSI Model — TCP/IP protocol suite

There were some communication networks such as telegraph and telephone network before 1960s. These network were suitable for constant rate communication at that time which means that after a connection was made b/w two users, the encoded message (telegraphy) or voice (telephony) could be exchanged.

Page No:
Date:

In 1972, Vint Cert and Bob Kahn both of whom were part of ARPANET Groups collaborated on what they called the Internetting Project.

* They wanted to link dissimilar networks so that a host on one network could communicate with a host on another. But there were many problems to overcome-
  - Diverse packet sizes
  - Diverse interfaces
  - Diverse transmission rates
  - Differing reliability requirements.

• TCP/IP • MILNET • CSNET • NSFNET • ANSNET

* The internet today is a set of pier network that provide services to the whole world.
  - World Wide Web
  - Multimedia
  - Peer-to-peer applications

Encapsulation

- It is used to describe a process of adding headers and trailers around some data.

- It is the process of taking data from one protocol and translating it into another protocol so that data can continue across a network.

- The lower layer encapsulates the higher layer's data b/w a header

- Example - A TCP/IP packet contained within an ATM frame is a form of encapsulation.

Page No:
Date:

Decapsulation

Decapsulation is the process of opening up encapsulated data that are usually sent in the form of packets over a communication network.

Data decapsulation is simply the reverse of encapsulation.

As the data moves up from the lower layer to the upper layer of TCP/IP protocol stack, each layer unpacks the corresponding header and uses the information contained in the header to deliver the packet to the exact network application waiting for the data.

Types of connections

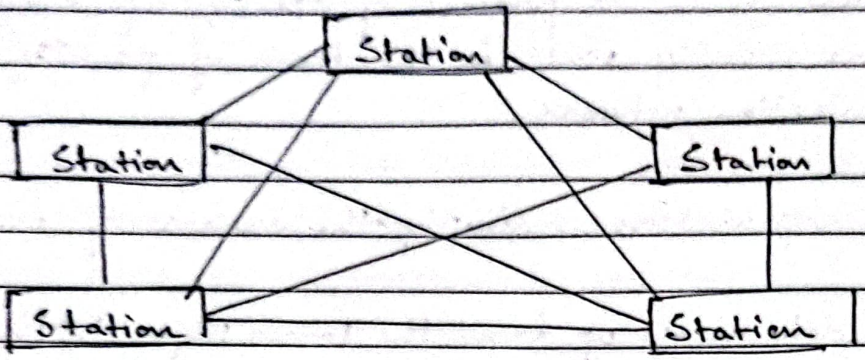
① Point-to-point Connection provides a dedicated link b/w two devices.
The entire capacity of the link is reserved for transmission b/w those two devices.

② Multipoint / Multidrop connection in which more than two specific devices share a single link. In a multipoint env, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is spatially shared connection. If user must take turns, it is timeshared connection.

Network Topology

- Arrangement with which computer systems or network devices are connected to each other.
- Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in the same network.

- Mesh topology



In mesh topology, every device has a dedicated point to point link to every other device
- In fully connected mesh network, total number of physical links required for n devices are $n(n-1)$
- If each link is duplex, total physical links required will be $n(n-1)/2$

Advantages

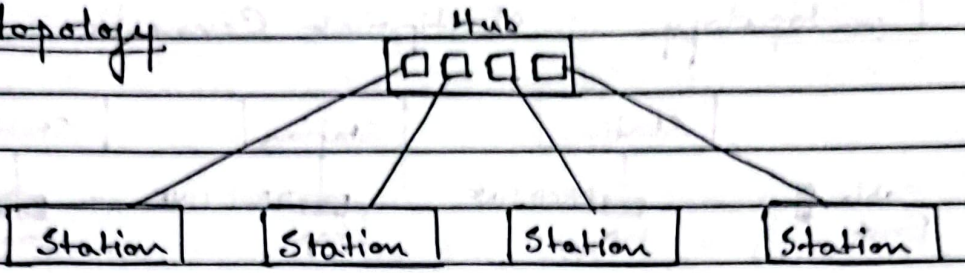
(i) The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when the links must be shared by multiple devices.

(ii) Point to point links make fault identification and fault isolation easy. So traffic can be routed to avoid links with suspected problems

Disadvantages
- Amount of cabling and number of I/O ports required
- Since every device must be connected to every other device, installation and reconnection are difficult.
- The sheer bulk of the wiring can be greater than available space to accomodate
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Page No:
Date:

• Star topology



- In star topology, each device has a dedicated point to point link only to a central controller usually called a hub. Unlike a mesh topology, a star topology does not allow direct traffic b/w devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device

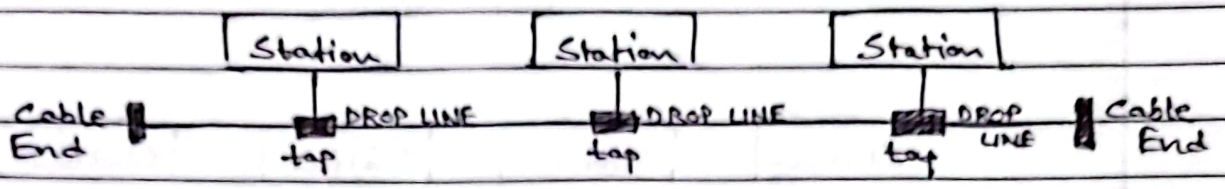
Advantages

- Since less # of dedicated links, it is less expensive than a star topology.
- Each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Robustness - if one link fails, only that link is affected. This factor also lends itself to easy fault identification and isolation.

Disadvantages

- If the hub goes down, the whole system is dead. This is because the whole system depends upon a central controller called Hub.

- **Bus topology** - Multipoint Connection



- One long cable acts as a backbone to link all the devices in the network.

Nodes are connected to the bus cable by drop lines and taps.

A drop line is a connection running b/w the device and the main cable, whereas tap is a controller.

Advantages

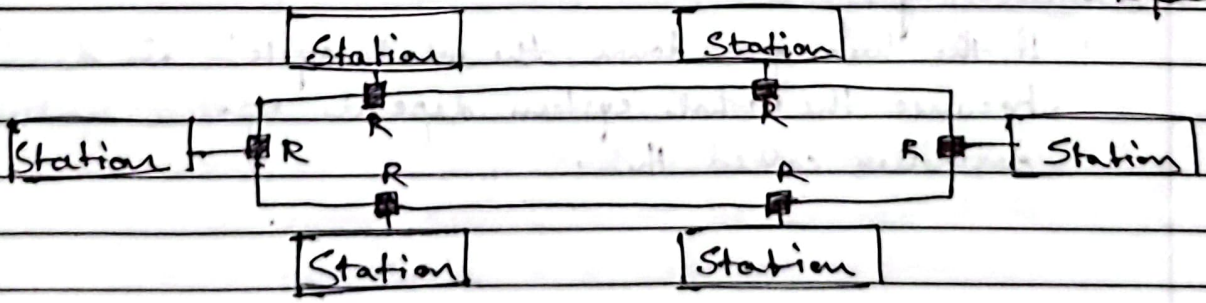
- Easy installation
- A bus uses less cabelling than mesh/star topology

Disadvantages

- Reconnection and fault isolation are difficult
- Adding new devices is difficult. This is because of a bus is usually designed to be optimally efficient at installation.

- **Ring Topology**

R - Repeater



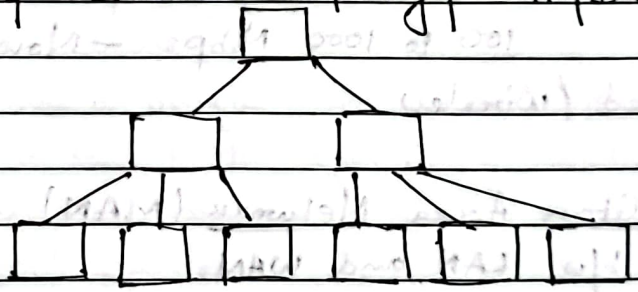
- In ring topology, each device has a dedicated point to point connection with only the two devices on the either side of it.

- A signal is passed along the ring in one direction from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Advantages
- A ring is relatively easy to install and reconfigure
- Since each device is linked to only its immediate neighbours To add or delete a device requires changing only two connections.

Disadvantages
- Since traffic is unidirectional, in a simple ring, a break in the ring can disable the entire network.

- Tree topology - Star bus topology - Hybrid topology



- A tree topology is a special type of structure in which many connected elements are arranged like branches of a tree.
- Tree topologies form a natural parent and child hierarchy
- Tree topology also known as star bus topology

Advantages
- Scalable as leaf nodes can accomodate more nodes in the hierarchical chain
- Other hierarchical networks not effected if any of them gets damaged

Disadvantage
- Huge cabling needed
- A lot of maintainance required

* For point to point connection, star topology is better.
* For multipoint connection, bus topology is better

PAN (Personal Area Network)

- It is a network with a size covering few meters of area.
- Normally covers area inside of a room
- Designed to communicate devices nearby a person.
- Can be -
  - Wired: USB, FireWire
  - Wireless: Bluetooth, Zigbee
- Ex: Firestick, Gaming consoles etc.

LAN (Local Area Network)

- Covers few kilometers
- Usually privately owned, links devices in single office, building or campus.
- Speed: 4 to 16 megabits per second (Mbps) - Earlier
  100 to 1000 Mbps - Nowadays
- Wired / Wireless

Metropolitan Area Network (MAN)

- Size b/w LAN and WAN
- Area - A whole town / city
- Designed for customers who need high speed internet connectivity, normally to the internet and have endpoints spread over city or part of city.
- Ex- telephone customer network, cable TV network

Wide Area Network (WAN)

- Provides long distance transmission of data, image, video, information over large geographic area
- Comprise a country, continent or whole world
- Ex: Asynchronous transfer mode (ATM)

Page No:
Date:

Types of connecting devices in a network

① Repeater / Hub

- It doesn't know anything about the packets i.e. to whom does it belong to.
- It sends packets to each device connected to it.
- It is the simplest and cheapest way to create a network
- Generates a lot of unnecessary traffic
- Wastage in bandwidth
- Security is an issue

② Switch / Bridge

- It is smarter brother of hub
- It sends packets to the exact destination without spanning the entire network.
- Each device has NIC card with unique MAC address

How does switch behave?

Every device has a unique MAC address printed on NIC card.
Every packet is sent to the specific destination only.
Thus, no flooding of packets.
No traffic (B.W) problem.
Not only the ethernet connection but also WIFI uses it

Router

- It is a glue that ties network together
- Hubs and switches are devices used to create networks
- If we want to send packets b/w those networks then routers come into picture
- We need routers to send packets from our laptop to search engine server over the internet.
- Once we send packets to our ISP, routers make sure that packets is passed on from network to network to reach search engine servers.

Page No:
Date:

Switching

i) Circuit Switching
ii) Message Switching
iii) Packet Switching

* CIRCUIT SWITCHING

- It is a technique that directly connects the sender and the receiver in unbroken path.

- Once a connection is established, a dedicated path exists b/w both ends until the connection is terminated.

- Three phases: Establish, Transfer, Disconnect

- Routing decisions must be made when the circuit is first established, but there are no decisions made after that time.

- **Advantages**
  - The communication channel (once established) is dedicated.

- **Disadvantages**
  - Possible long wait to establish a connection during which no data can be transmitted.
  - More expensive than any other switching techniques.

Page No:
Date:

* MESSAGE SWITCHING

- A message switching node is typically a general purpose computer
- The device needs sufficient secondary storage capacity to store the incoming messages, which could be long
- A time delay is introduced using this type of scheme due to store-and-forward time, plus the time required to find the next node, in the transmission path.

• Advantages

- Channel efficiency can be greater compared to circuit switched systems because more devices are sharing the channel

- Traffic congestion can be reduced, because messages may be temporarily stored in route

• Disadvantages

- Message switching is not compatible with interactive applications

- Store and forward devices are expensive because they must have large disks to hold potentially long messages

* PACKET SWITCHING

- Message needs to be divided into packets of fixed or variable size

- The size of the packet is determined by the network and governing protocol

- Resources are allocated on the basis of FCFS basis

- Packets are handled in two different approaches
  - Datagram Service (connection less)
  - Virtual circuit (connection oriented)

Datagram Switching

- Each packet contains full destination address
- Packets can take any practical route
- Each packet is treated independently
- Packets may arrive & out of order (so receiver may require reordering)
- Packets may go missing (and node handles recovery of missing packets)
- It is a best effort network.
- Store and forward operation required at each node for each packet.
- Connection less protocol : Ethernet, IP, UDP

** If there are no setup or teardown phases, how are the packets routed to their destination in datagram network?

→ In this type of network, each switch has a routing table based on destination address. The routing tables are dynamic and updated periodically

Packet Switching : Virtual Circuit

- In this, a pre planned route is established before any data packets are sent
- A logical (virtual) connection is established when
  - Sender sends a "call request packet" to the receiver
  - Receiver sends back an acknowledgement packet "call accepted packet" to the sender the receiver agrees on conversational parameters

The conversational parameter can be maximum packet size, path to be taken, and other variables necessary to establish and maintain the conversation.

In virtual circuit approach, routing decision is not made every time for all packets. It is made only once for all packets using that virtual circuit.

It basically involves three steps:

i) Connection establishment
ii) Data transfer
iii) Connection release

Advantages

- Maximize link efficiency by making optimal use of link bandwidth.
- Robust against link and node failure
- Nodes buffer the data if required to equalize rates

Disadvantages

- Protocols for packet switching are typically more complex
- Packet switched systems cannot deliver the same quality as delivered by circuit switched system.
- Some initial cost in implementation.

Item	Circuit Switched	Packet S
Call Setup	Required	NA
Dedicated physical path	Y	N
Each packet follows same route	Y	N
Packets arrive in order	Y	N
Is a switch crash fatal	Y	N
When congestion can occur	At setup time	ON EVERY PACKET
Potentially wasted bandwidth	Y	N
Store & forward transmission	N	Y
Transparency	Y	N
Charging	per minute	per packet

Page No:
Date:

Circuit Switching	Virtual Circuit Packet
Dedicated path established	No dedicated path
Message sent as it is	Message broken into small parts called packets
No store & forward transmission	Store & forward transmission
Constant data rate	Constant data rate is not guaranteed because of store and forward of packets at all nodes
Money is charged as per minute	Money is charged as per packets

- Performance metrics for packet switched network
  - (i) Throughput - It is a measure of how fast we can actually send data through a network
  - (ii) Latency (delay) - It defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

Latency = Propagation time + Transmission time + Queuing time + Processing delay

- Propagation time - Measures the time required for a bit to travel from source to destination

$$PT = \frac{\text{Distance}}{\text{Velocity}}$$

Page No:
Date:

- Transmission time - Time required to send a complete message
  TT = Message Size / Bandwidth
- Queuing time - Time needed for each intermediate or end device to hold the message before it can be processed
  - It changes with load imposed on the network
- Processing time - Time required to process the message like error detection, acknowledgement, correction etc

Page No:
Date:

APPLICATION LAYER

- Application layer provides services to the user
- Communication is provided using logical connection, which means that the two application layers assume that there is an imaginary connection through which they communicate the data.
- Communication at application layer is logical and not physical.
- Protocols in this layer do not provide services to any other protocols in the suite, they only receive services from the protocols in the transport layer.

Application Layer Paradigm

Two application programs must be developed with each other in order to communicate the data:

- One running on a computer somewhere in the world
- The other running on another computer somewhere else in the world

(i) Traditional paradigm: Client-Server
(ii) New paradigm: Peer-to-Peer
(iii) Hybrid:

Client Server Paradigm

- It has two systems
  (i) Client
    - It requests the server for connection and communication
    - It doesn't run all the time, runs only when it needs to receive service

(ii) Server
- It runs continously, waiting for another application program called client
- It runs all the time

Peer to peer paradigm (P2P)
- There is no need for a server process running all the time and waiting a client process to connect
- The responsibility is shared b/w peers
- A computer connected to the internet can either
  - Provide service at one time and receive at another time
  - Can provide and receive the service at same time

How can a client process communicate with a server process?
Using Application Programming Interface (API):
- It is used to represent a set of instructions to tell the lowest four layers of TCP/IP suite to open the connection, send and receive the data from the other end, and close the connection.

• Interface – A set of instructions b/w two entities
In this case, one of the entities is the
- process at the application layer and the other is
- operating system that encapsulates the first four layers of the TCP/IP suite.

In other words, a computer manufacturer needs to build the first four layers of the suite in the operating system and include an API.

In this way, the processes running at the application layer and are able to communicate with the operating system when sending or receiving message through the internet.

Ex: Socket interface, Transport layer Interface (TLI), STREAM

Page No:
Date:

Sockets

It is a data structure created and used by the application program

From the application layer POV, the communication b/w client process and server process takes place through sockets created at the two ends

Socket Address

In two way communication, we need a pair of addresses:

- Local (sender) address
- Remote (receiver) address

Local address in one address is remote address in other direction and vice versa

Socket Address is a combination of 32 bit IP address (to uniquely identify the device) and 16 bit port number (to identify the process)

- Port number: It is 16 bit integers b/w 0 and 65535
- Client port number: Client chooses its port number randomly from 0 to 65535 using the transport layer software running on the client host. This is called ephemeral (temporary) port number
- Server port number: Server process is also defined by a port number. But its not randomly chosen. If its random, then client will not know the port number in order to access the server. They are called as well known port number.

Page No:
Date:

Transport layer protocols

Three protocols are defined at the transport layer:

(i) TCP
- Connection oriented
- Reliable → Supports flow and error control mechanism
- Supports full duplex
- It is a byte stream oriented protocol.

(ii) UDP
- Connection less
- Unreliable → No flow and error control mechanism

(iii) STCP - Streams Transmission Control Protocol
- Provides service which is a combination of TCP and UDP
- Connection oriented
- Reliable
- But its not byte stream oriented protocol. It is message oriented protocol like UDP.

Page No:
Date:

World Wide Web (WWW)

- **Web Client (Browser)** – Its responsibility is to interpret and display a web page.

  Each browser typically has three parts -

  1. Controller - It receives input from the keyboard and mouse and uses the client program to access the documents
  2. Client Protocol - Client protocols are like HTTP, FTP, SSH etc.
  3. Interpreter - It can be HTML, Java or JavaScript depending upon the type of document

- **Web Server** The web pages are stored at the server which are expected to run all the time. To improve the efficiency, a cache memory is used generally. For example, Apache, Microsoft Information Centre

- Uniform Resource Locator (URL) It is an identifier which is used to distinguish one webpage from another. It has three fields - host, port and path

  However before defining the web page, we must tell the browser which client server application we want to use. Therefore there are 4 identifiers instead of 3

  1. Protocol - Its like a vehicle which is used to access the web page
  2. Host - Its the IP address / unique name of server
  3. Port - It is a 16 bit integer which is normally predefined for client server based application.

     Example - If HTTP is used, then port number is 80
  4. Path - It is the location of the file in underlying operating system.

protocols://host/path → used for most of the time

protocols://host:port/path → used when port number is needed

- Web Documents

① Static - Fixed content document that are created and stored in the server
- Content of the file is decided when it is created
- Static documents are created using HTML, XML, XSL, XHTML

② Dynamic - Created by a web server whenever a browser requests the documents
- They are created using Java Server Page (JSP), Active Server Page (ASP), Cold fusion.

③ Active - For many applications we need a program or a ~~direct~~ script to be run at the client side. They are called active documents.
- Java applets are used to create such documents

Hyper Text Transfer Protocol (HTTP)

It is a protocol which is used to define how the client server programs can be written to retrieve web pages from the web.

Server uses port number 80 whereas client uses a temporary port number.

HTTP uses TCP service of a transport layer which is reliable

Page No.
Date:

Q. How a file on the web page be accessed?

- It is accessed by establishing a connection (TCP) between client and server.
- The data is retrieved based on request and response method where the client sends request and server responds to the clients request.
- Since its TCP connection, the connection has to be released once data transmission is over.

• Non persistent connection

Here, the TCP connection is made for each request/response in the following stages

- Client opens a TCP connection and sends request
- Server sends the response & closes connection
- Client reads the data until it encounters and end of file marker, then closes the connection

• Persistent Connection

Here, the server leaves the connection open for more requests after sending a response

The server can close the connection either

- at request of the client
- if timeout has been reached.

• Proxy Server

- The proxy server is installed in the local network.
- When an HTTP request is created by any of the clients, the first request is directed to the proxy server.
- If the proxy server already has the corresponding web page, it sends the response to the client. Otherwise the proxy server acts as a client and sends the request to the web server in the internet.
- When response is returned, the proxy server makes a copy and stores it in the cache before sending it to the requesting client.

Page No:
Date:

File Transfer Protocol (FTP)

It is standard protocol provided by the TCP/IP to copy a file from one host to another.

Although HTTP can be used to transfer the file ; FTP is a better choice for large file / file with different formats

FTP is not secure as the data transfer takes place in the form of plain text which is insecure. Although, FTP requires a password, the password is sent in plaintext (unencrypted), which means it can be intercepted. For security one can add Secure Socket layer (SSL) b/w the FTP layer and TCP layer. Here this is called SSL-FTP

FTP can transfer → ASCII file, EBCDIC file, image file etc.

- Basic Model of FTP

The client has three components

(i) User Interface
(ii) Client control process → Remains connected for entire FTP session
(iii) Client Data transfer process → It is opened and then closed for each file transfer activity.

Server has two components

(i) Server control process
(ii) Server data trasfer process

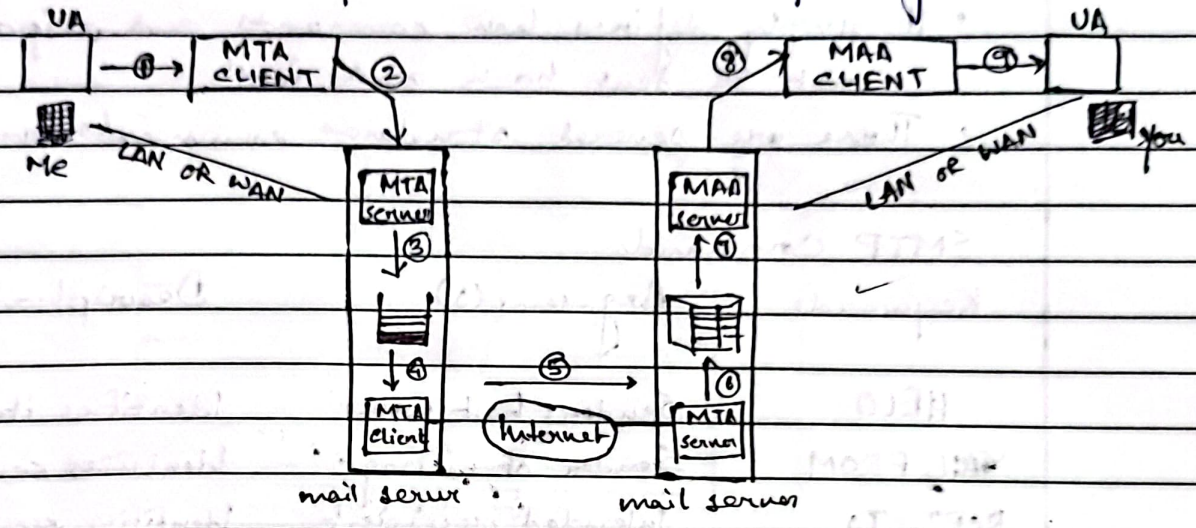
⊛ FTP uses two well known ports of TCP

(i) Port 21 - Used for control connection
(ii) Port 20 - Used for data connection

Page No:
Date:

Client Server Application : EMail

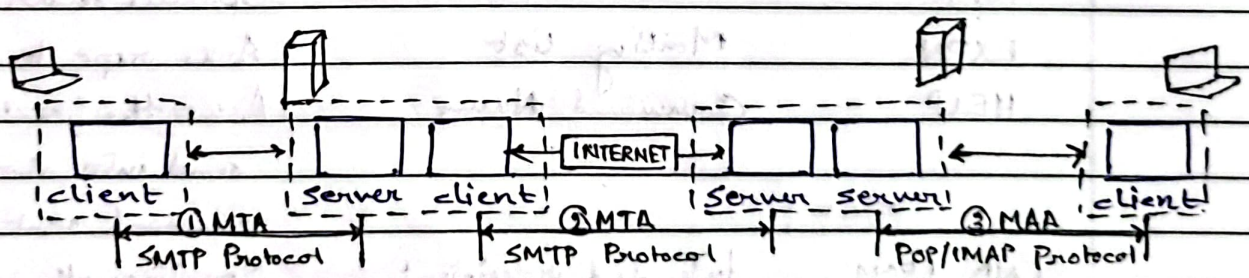
In HTTP or FTP, the server program is running all the time. When a request come to the server, server provides service to the client → Typical client server paradigm.



UA – User Agent
MTA – Message transfer agent
MAA – Message access agent

– Email system requires → Two UAs, Two pair MTA, One pair MAA

Protocols used in email



SMTP → Used two times
(i) B/w sender and senders mail server
(ii) B/w two mail server

POP and IMAP → Used only one time

EMail Address: Local part @ Domain Name
Local part: mailbox address of the recipient
Domain Name: The domain name of the mail server

(1) Simple Mail Transfer Protocol (SMTP)

- SMTP is message transfer agent
- It is a push protocol, which pushes the message from client to server.
- It simply defines how commands and responses must be sent back and forth
- There are several standards commands and responses

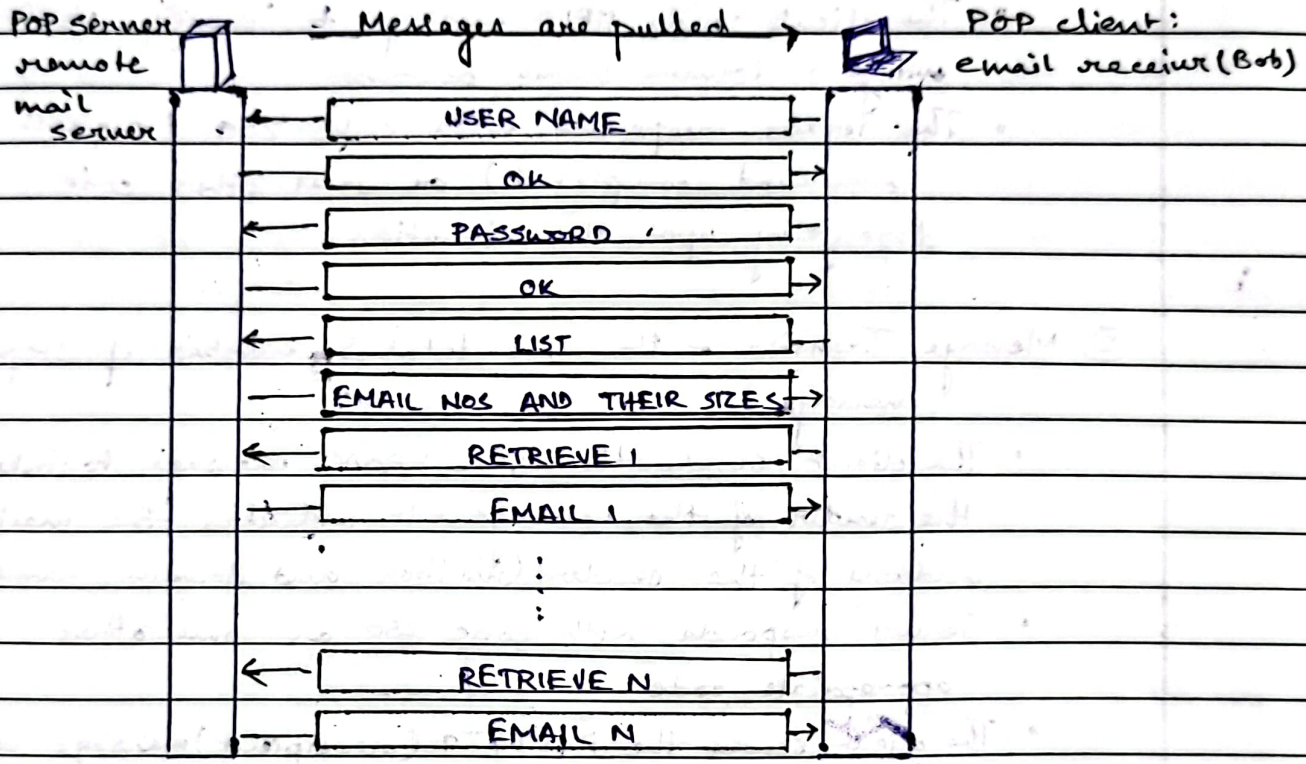
SMTP Commands

Keywords	Argument(s)	Description
HELO	Senders host name	Identifies itself
MAIL FROM	Sender of message	Identifies sender of msg
RCPT TO	Intended receipient	Identifies receipient of msg
DATA	Body of mail	Sends actual msg
QUIT		Terminates the msg
RSET		Aborts current mail txn
VRFY	Name of receipient	Verifies address of rcpt
NOOP		Checks status of rcpt
TURN		Switches sender & reciepient
EXPN	Mailing list	Asks rcpt to expand mail list
HELP	Command Name	Asks the receipient to send info about the command sent as argument
SEND FROM	Intended receipient	Specifies that mail be delivered only to the terminal of receipient and not to the mailbox
SMOL FROM	"	... terminal/maibox
SMAL FROM	"	... terminal & maibox

Page No:
Date:

POST OFFICE PROTOCOL (POP)

- POP is a message access agent
- It is a pop protocol which pulls the message from server to the client.
- The client POP3 software is installed on recipient computer, whereas, server POP3 software is installed on mail the server.



Internet Mail Access Protocol (IMAP)

POP3	IMAP4
• User can not have different mail folder on the mail server.	• User can create, delete, rename mailboxes on the mail server
• Does not allow user to partially check the content of the mail.	• Allows user to check email header, search content of email prior to downloading, partial downloading email.
• Cannot create hierarchy of mailboxes in a folder for email storage.	

Page No:
Date:

Mail Transfer Phase

The process of transmission of a mail occurs in following three phases :

① Connection Establishment - First client makes a TCP connection to well known port 25. then SMTP server starts the connection phase.

- The server sends code 220 (service ready)
- The client sends HELO message to identify itself using a domain name address
- The server responds with code 250 (request command completed) or some other code depending upon the situation.

② Message Transfer - It takes total 8 number of steps for message

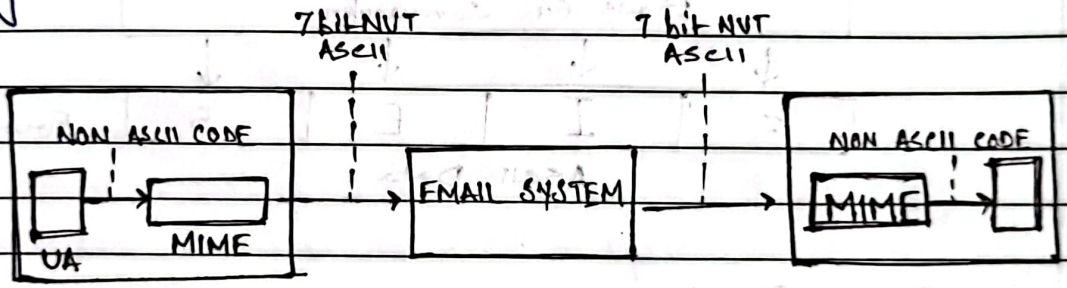
- The client sends the MAIL FROM message to introduce the sender of the message. It includes the mail address of the sender (mailbox and domain name)
- Server responds with code 250 or some other appropriate code
- The client sends the RCPT TO (receipient) message which includes the mail address of the receipient
- Server responds with code 250 or some other appropriate code.
- Client sends DATA message to initialize the message transfer.
- Server responds with code 354 (start mail input) or some appropriate message
- Client sends the content of the message in the consecutive lines. Each line is terminated by a two character end of line token. The message is terminated by the line containing just one period.
- Server responds with code 250 (OK) or some other appropriate code

③ Connection Termination - After the message is transferred successfully, the client terminates the connection. This phase involves two steps:

- The client sends the .QUIT command
- The server responds with code 221 or some other appropriate code.

MIME (Multipurpose Internet Mail Extension)

It is a supplementary protocol that allows the non ASCII data to be transferred through EMail. MIME transforms the non ASCII data at sender site to NVT ASCII data and delivers it to the client MTA to be sent through the internet. The message at the receiving site is transformed back to the original data.



- **MIME Header**

  MIME Version: 1.1
  Content-Type: type/subtype
  Content-Transfer-Encoding: encoding type
  Content-ID: message ID
  Content-Description: textual explanation of non textual contents

- **MIME Description**

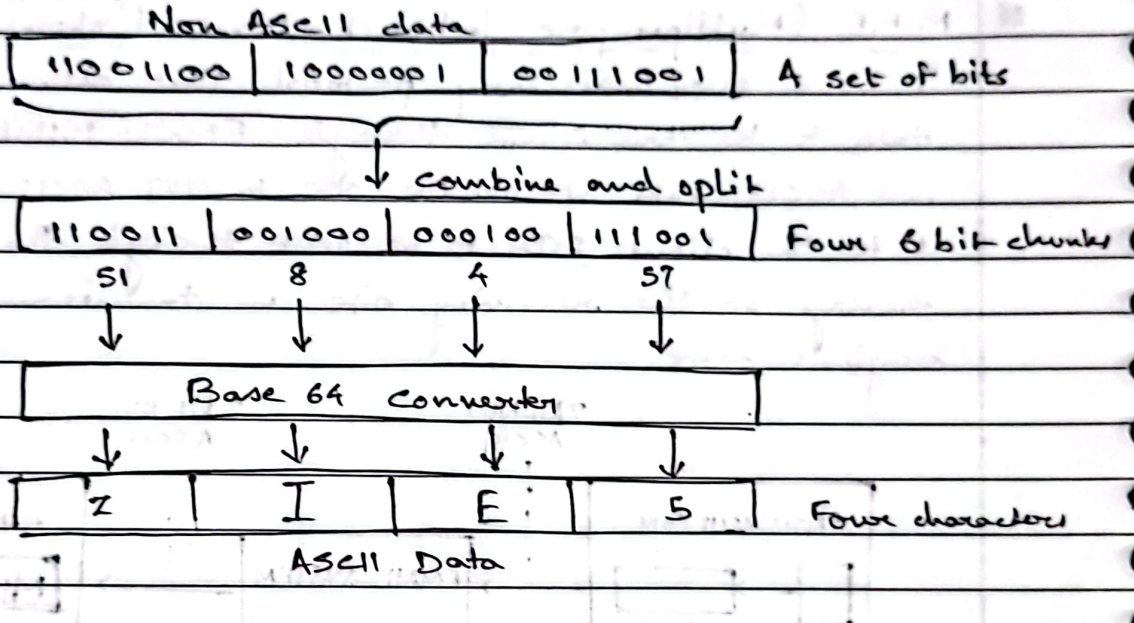
  Version → Current Version is 1.1
  Content type/subtype → Text, multipart, message, image, video, audio, application
  Content transfer encoding → 7bit → NVT ASCII
  8bit → Non ASCII
  Binary, Base64, Quoted printable

Page No:
Date:

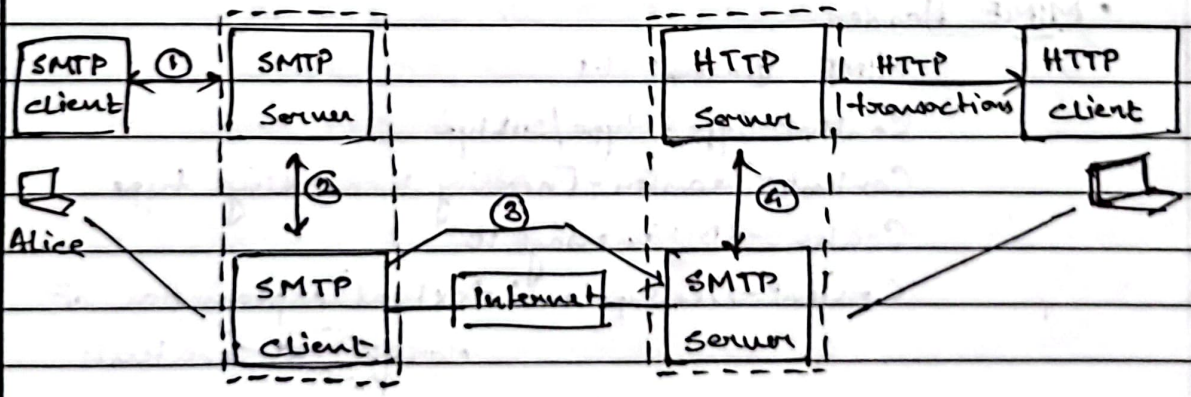
Content ID ⟶ To uniquely identify whole message in multi message environment

Content Desc ⟶ Defines whether the body is image, audio or video

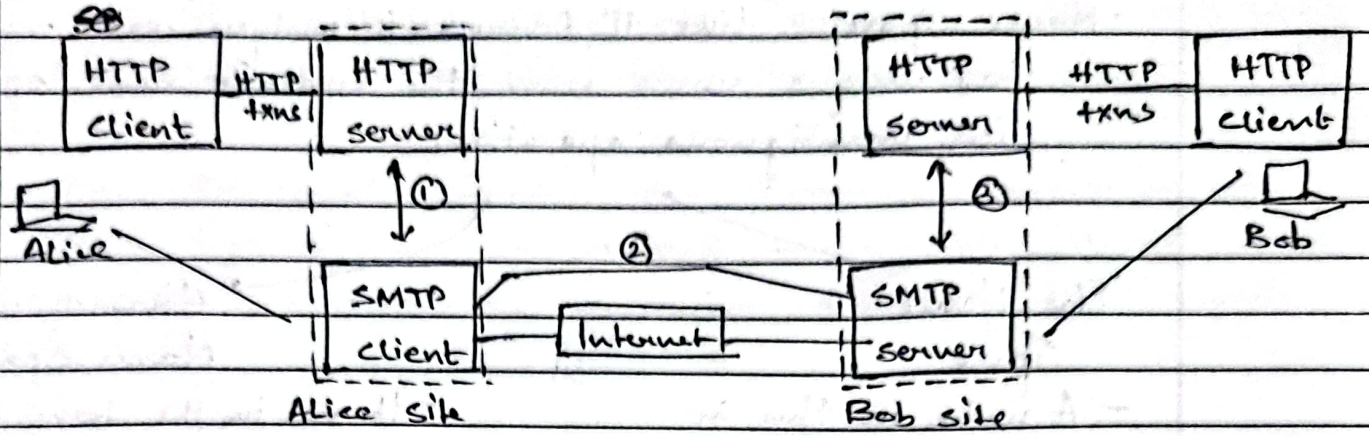
Base 64 conversion



Web Based EMail



Only receiver uses HTTP

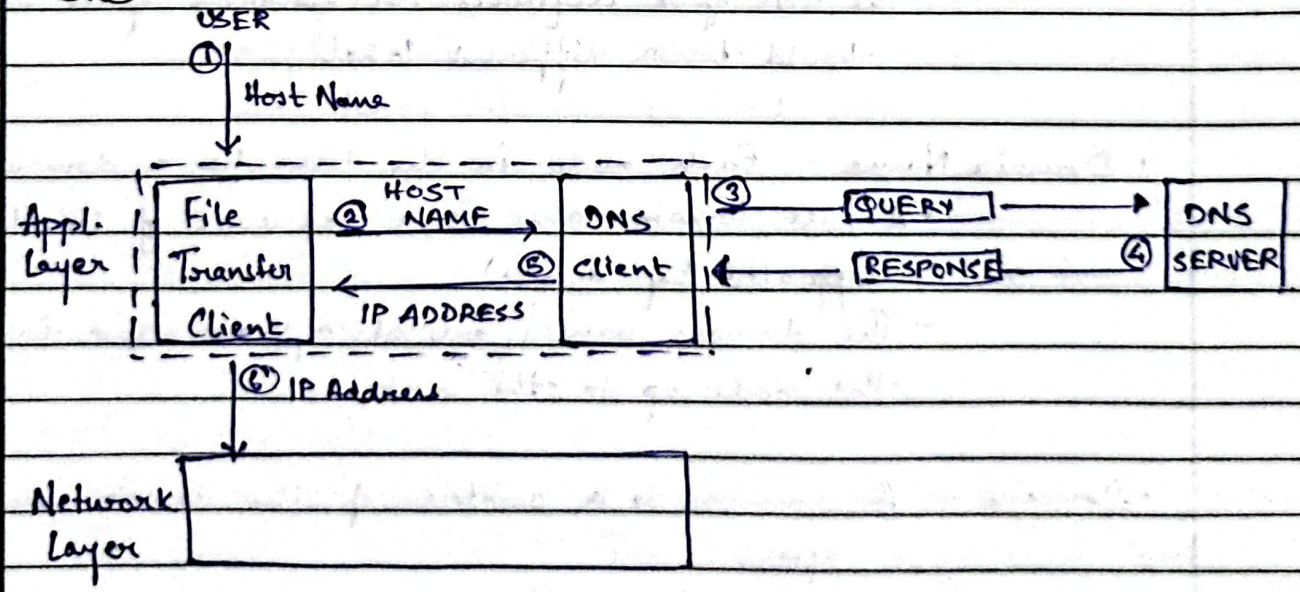


Both sender and receiver uses HTTP

Domain Name System (DNS)

To identify an entity, TCP/IP protocols use the IP address which uniquely identifies the connection of a host to the internet.

However, people prefer to use names instead of numeric addresses. Therefore we need a system that can map a name to an address or an address to a name. It is done by DNS.



DOMAIN NAME SPACE

- Name Space - Like IP Address is unique each machines has unique name from the available name space for unambiguous operation.

Flat Name Space

- A name in this is a sequence of characters without structures. So it must be centrally controlled to avoid the duplication of ambiguity.

Hierarchical Name Space

- It is in the form of structures. Name consist of many parts each having significance. So it is not centrally controlled to avoid the duplication of ambiguity. thus decentralized from administrative POV

- Label - Each node in the tree has a label; which is a string with max of 63 characters
  - Root label is a null string
  - The DNS requires the children of a node should have different labels

- Domain Name - Each node in the tree has a domain name
  - A full domain name is a sequence of labels separated by dots (.)
  - The domain names are always read from the node up to the root.

- Domain - A domain is a subtree of the domain name space
  - Name of the domain is the name of the node at the top of the tree.

Page No:
Date:

Name space is distributed in hierarchy manner. The name space is distributed among many computers called DNS servers DNS allows to be divided further smaller domains.

Since the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers. What a server is responsible for or has authority over is called a zone.

Root Server It is a server whose zone consists of the whole tree. The root server doesn't store any information about domain but delegates its authority to other servers, keeping references to those servers.

DNS defines two types of servers

① Primary Server – It is server that stores a file about the zone for which it has an authority. It is responsible for creating, maintaining and updating the zone file. It stores zone file on local disk

② Secondary Server – It is a server that transfers the complete information about a zone from another server and stores file on its local disk

* A primary server loads all information from the disk files; the secondary server loads all information from the primary server

DNS in the internet

DNS is a protocol that can be used in different platforms

① Generic Domain – They define registered hosts according to their generic behaviour. Each node in the tree defines the domain, which is an index to the domain name space database

② Country domains - The country domain section uses two character country abbreviations (India → in) The second labels can be organisational or they can be more specific (academic → ac)

DNS Types

A	A 32 bit IPv4 address
NS	Identifies the authorative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the begining of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address

Page No:
Date:

TRANSPORT LAYER

Transport Layer Services

The transport layer is responsible for

- Providing services to the application layer and to receive the service from network layer.
- Providing process-to-process communication b/w two application layers
- Providing communication using logical connection
- Providing multiplexing at the source and demultiplexing at the destination host
- Provide flow and error control services
- Providing congestion control.

Client/Server Paradigm

- Addressing — like MAC and IP addresses at DLL and the network layer, we need transport layer address, called a port number, to choose among the multiple processes running on the destination host.

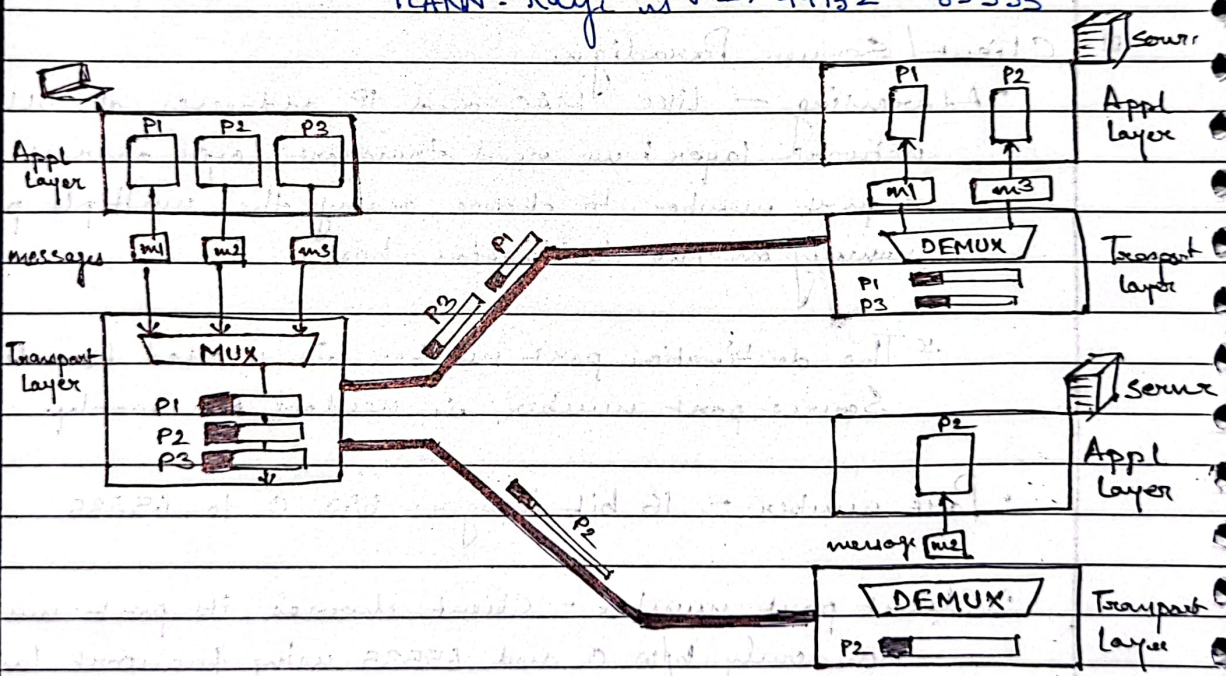
  * The destination port number is needed for delivery
    Source port number is needed for reply.

- Port number — 16 bit integers b/w 0 to 65535

- Client port number — Client chooses its port number randomly b/w 0 and 65535 using transport layer software running on the client host. This is called the ephemeral (temporary) port number
  It is recommended to be greater than 1023

Page No:
Date:

- **ICANN Ranges** It has categorized the port numbers into three parts - well known, registered and dynamic (private)
  - Well Known - It is assigned and controlled by the ICANN. Range is from 0 - 1023
  - Registered - These ports are neither assign nor controlled by ICANN. They are only registered by ICANN so that the duplication of the port can be avoided
    Range → 1024 - 49151
  - Dynamic - These are temporary port numbers. They are neither assigned nor registered by ICANN. Range is → 49152 - 65535



- Connectionless Service : Packets are sent from one party to another with no need for the connection establishment or connection release. The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment
  Eg. UDP (User Datagram Protocol)

Page No:
Date:

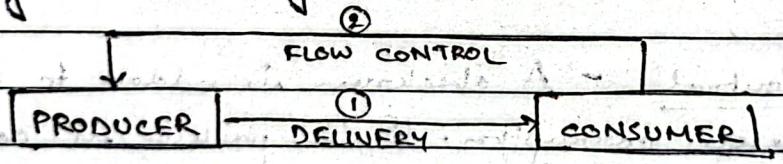
Connection oriented service - In connection oriented service a connection is first established b/w sender and the receiver. Data is transferred. At the end, the connection is released. Ex. TCP, SCTP

Reliable Service - If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service.

Unreliable Service If the application program does not need reliability because it uses its own flow and error control mechanisms as it needs fast service or the nature of the service does not demand flow and error control, then an unreliable protocol can be used.

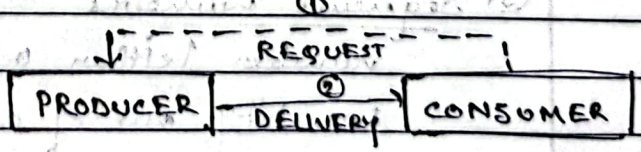
* UDP is connectionless and thus unreliable; TCP and SCTP are connection oriented and thus reliable.

Pushing and pulling



(a) Pushing

- Data loss
- Duplicate data transmission
- Out of order delivery
- Data corrupt

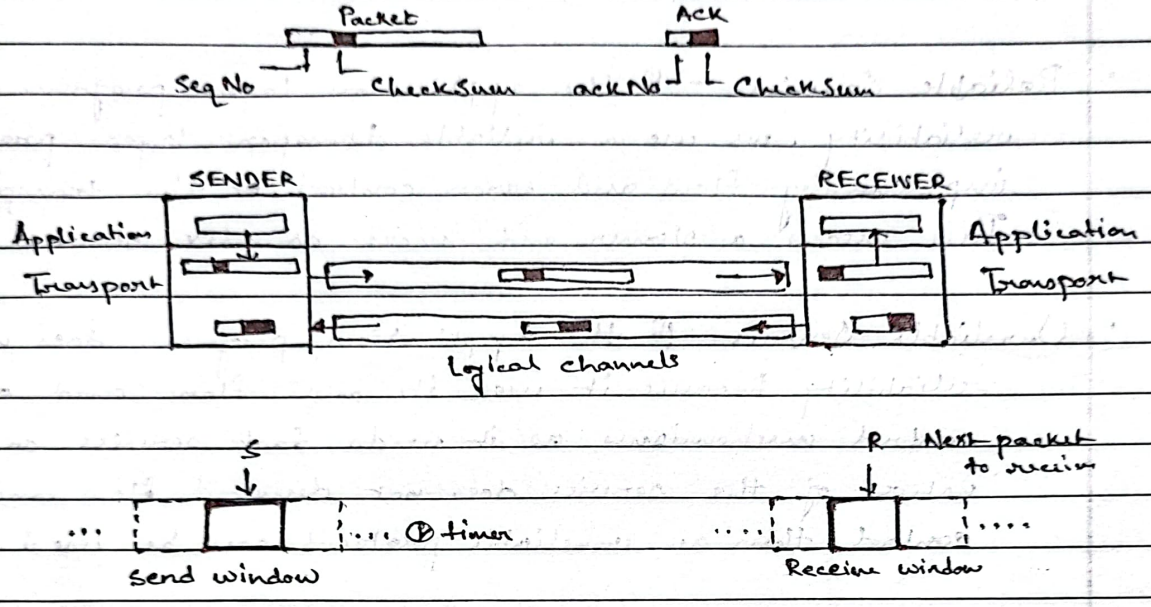


(b) Pulling

Page No:
Date:

Stop and Wait Protocol

It is a basic connection oriented protocol primarily used for flow and error control in data transmission.



① Flow Control – After sending a packet, the sender waits for an acknowledgement (ACK) before sending the next packet.

② Error Control – A checksum is added to each packet to detect corruption. If the packet is corrupted, it's discarded and the sender resends the packet after a timeout.

③ Sequence numbers – Each packet is assigned a sequence number (either 0 or 1 in this case) which helps to identify out of order or duplicate packets.

④ Acknowledgement Numbers – The acknowledgement contains the sequence number of the next expected packet, allowing the receiver to handle potential duplicate packets.

Page No:
Date:

- Practical Use in Noisy Channels

① In real world noisy channels, packet corruption, loss or out of order issues can occur. For handling these, protocols like Go-Back-N and Selective Repeat are more efficient algorithms / alternatives to Stop-and-wait.

② CheckSum - Both data packets and acknowledgements contain checksums to detect errors

③ If a packet or ACK is lost or corrupted, the sender uses a timer to resend the packet

- Stop and Wait ARQ (Automatic Repeat reQuest):

① Advantages

- Easy to implement
- Requires minimal buffer size since the send and receive window size is just 1.

② Disadvantages

- Inefficient use of communication link, especially when dealing with high bandwidth channels
- If the round trip time (RTT) is long, the sender spends a lot of time waiting, which results in low link utilization.

Page No:
Date:

Go Back N Protocol

It enhances the efficiency of the Stop-and-wait protocol by allowing multiple packets to be in transit before requiring an acknowledgement, improving link utilization.

① Efficiency improvement - GBN allows multiple packets to be sent consecutively without waiting for acknowledgements. This increases the pipe filling of communication link, improving overall efficiency

② Sequence numbers - Since multiple packets are sent, more bits are required to represent the sequence numbers. If header allows m bits for sequence number, the sequence number ranges from 0 to $2^m - 1$, following a modulo 2^m pattern. The sequence numbers are repeated cyclically.

③ Cumulative Acknowledgement - GBN uses cumulative acknowledgements. The acknowledgement number (ackNo) indicates the sequence number of the next packet the receiver expects, acknowledging all packets up to that number.

Sender Sliding Window

① WINDOW SIZE - The senders sliding window is of size $2^m - 1$ (where m is the no. of bits used for the sequence number). It has three important variables:

- Sf (Send First): The sequence number of the first outstanding packet
- Sn (Send Next): The sequence number of the next packet to be sent.
- Ssize (Window size): The size of the sending window which can hold multiple packets in transit.

(ii) SLIDING MECHANISM The window slides when acknowledgements for packets are received. Multiple slots can slide at once, depending on how many packets can be acknowledged.

- Receiver Sliding Window

The receivers window size is 1. It only accepts a packet if its sequence number matches the expected sequence number (R_n). When a correct packet is received, the window slides by one slot and the next expected packet is updated.

- Timers

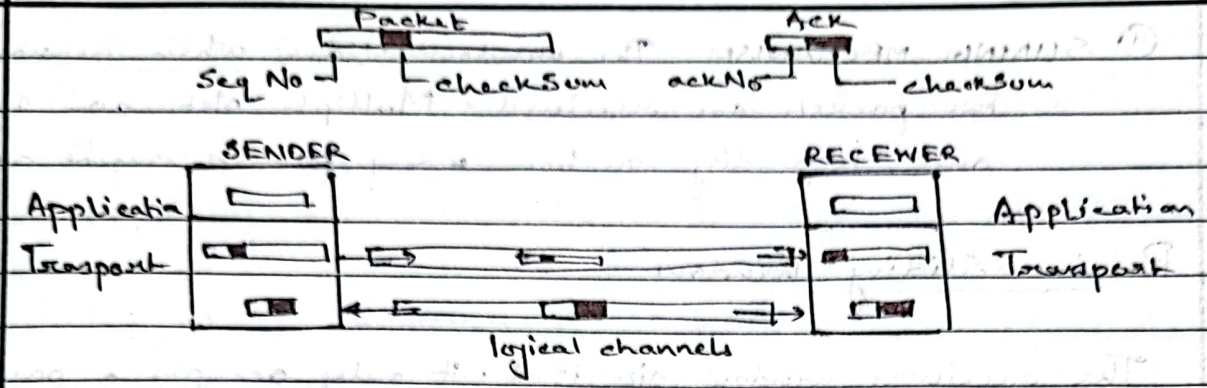
Instead of using individual timers for each packet, GBN maintains a single timer for first outstanding frame. When this timer expires (due to no acknowledgement), all unacknowledged packets are sent.

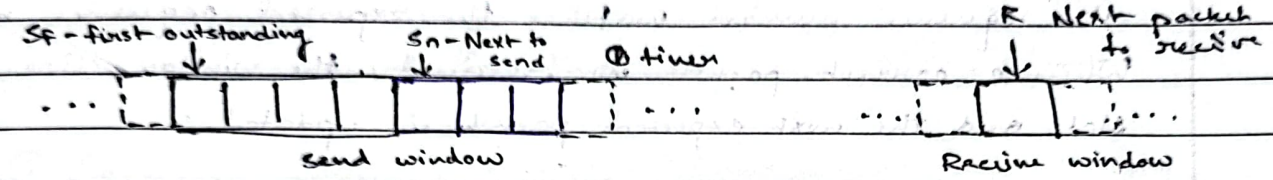
- Acknowledgements

(i) Positive Acknowledgements - Sent when a packet is correctly received in order.

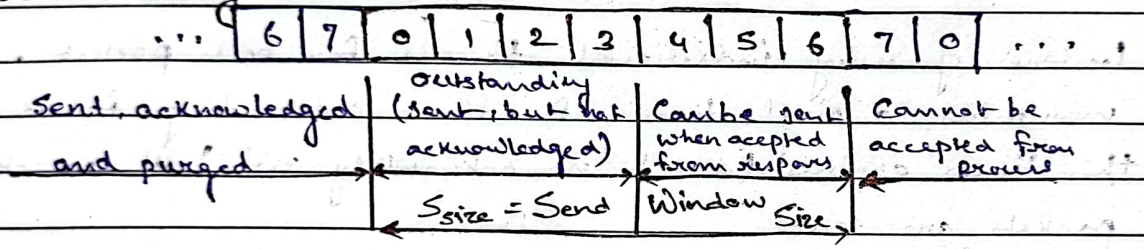
(ii) Silence for errors - If a packet is damaged or received out of order, the receiver discards it and remains silent, waiting for expected packet.

(iii) Resending mechanism - If the timer expires before an acknowledgement is received the sender resends all outstanding packets starting from the first unacknowledged one, hence the name - Go Back N

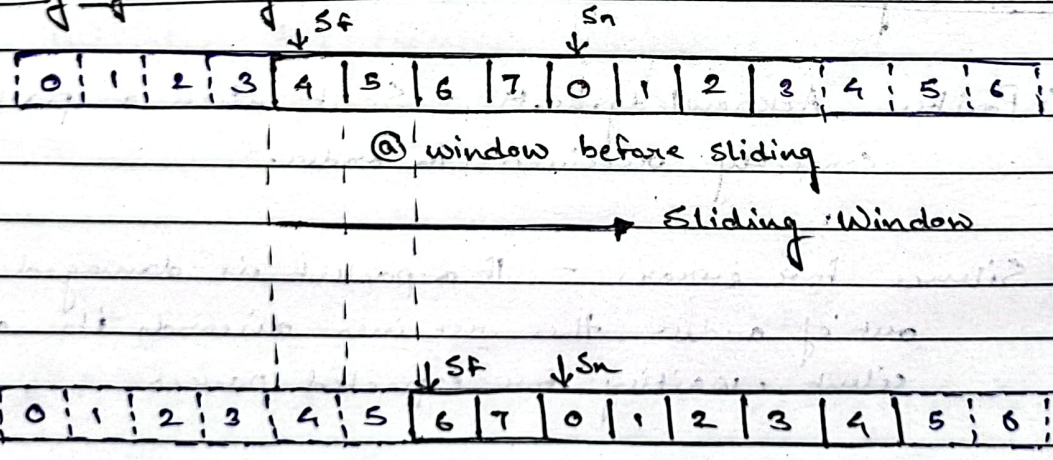




- Sender Sliding Window



- Sliding of sliding window



Page No:
Date:

Selective Repeat Protocol

It enhances efficiency by allowing the receiver to accept out of order packets and only request retransmission of missing or corrupted packets. Unlike Go-Back-N, where the sender resends all outstanding frames when an error is detected, SR resends only the specific problematic frame.

- **Sender and receiver window size**

  In SR, the sender and receiver windows are of same size which is typically $2^m - 1$, where m is the number of bits used for sequence numbering.

  For example, if $m = 4$, sequence numbers ranges from 0 to 15 but window size is 8

- **Handling out of order packets**

  The receiver can store out of order packets and wait for the missing packets to complete the sequence before delivering them to the application layer. This reduces the need for retransmitting unnecessary packets and makes the protocol more efficient in handling errors.

- **Sliding Windows**

  (i) S_f - The sequence number of the first outstanding (unacknowledged) frame.

  (ii) S_n - The sequence number of the next frame to be sent

  (iii) S_{size} - Window size, typically $2^m - 1$

The receiver sliding window has a size equal to the senders window and expects packets in sequence. It only delivers a packet to the upper layer once the packet has been received correctly and all packets have been received.

- Timers

Each packet has its own timer, unlike Go-Back-N where a single timer for the first outstanding frame is maintained. If a timer expires before an acknowledgement is received, only that specific packet is resent

- Acknowledgement (ACK) Mechanism

Each ACK in SR is specific to the packet being acknowledged. For example: if a packet with sequence number 3 is received correctly, an acknowledgement (ACK) for that packet (ackNo = 3) is sent.

This contrasts with the Back N where the ACK indicates the next expected packet acknowledging all previous packets.

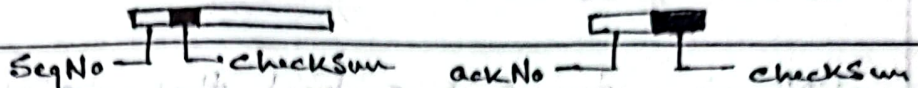
(Ex) If the sender sends 6 packets (0, 1, 2, 3, 4, 5) and receives an acknowledgement for packet 3,

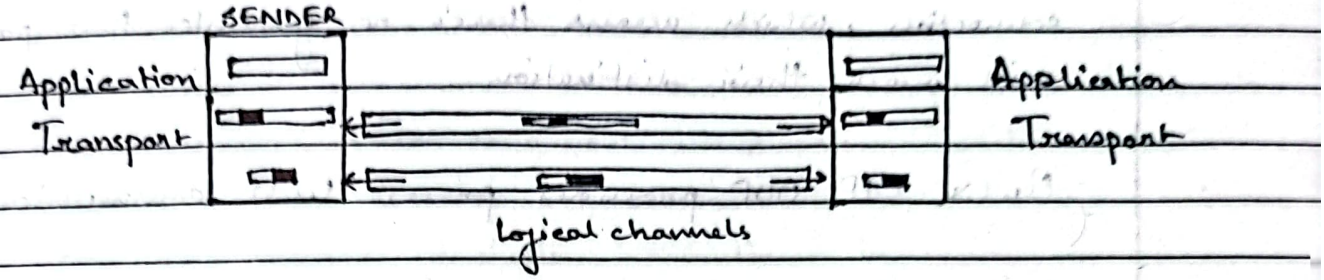
⇒ In Go Back N, packets 0, 1 and 2 are considered acknowledged and the receiver is expecting packet 3

⇒ In selective Repeat, only packet 3 is acknowledged and nothing can be inferred about packets 0, 1 and 2.

Piggybacking

- In unidirectional protocols, data flows in one direction with control information (ACK, NAK) flows in other direction.
- In real world bidirectional communication, piggybacking is used to improve efficiency. A data packet travelling from A to B can carry acknowledgment info. about packets received from B and vice versa. This reduces overhead of sending separate control frames.

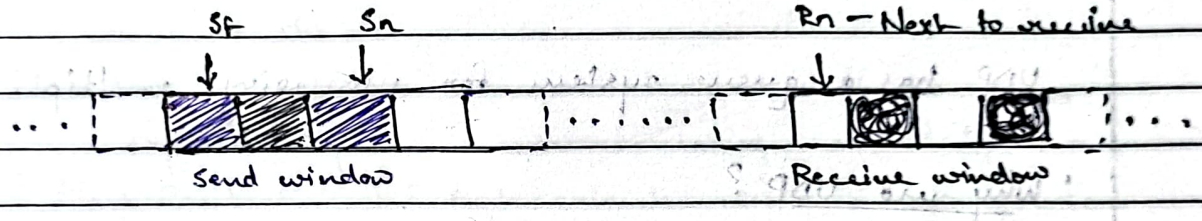




Sent but not acknowledged

Acknowledged out of order

Packet received out of order.



Page No:
Date:

User Datagram Protocol (UDP)

UDP is a transport protocol that doesn't require a connection, which means there's no guarantee that packets will reach their destination.

Unlike IP, UDP provides process to process communication.

UDP doesn't include a mechanism to control the flow of data between sender and receiver.

The only error control provided is via the checksum

UDP has a queue system for managing multiple processes

- **Why use UDP?**
  Processes that don't require reliability and want to send small, simple messages can use UDP. Its simplicity and efficiency are ideal for scenarios where low overhead is more critical than reliability.

- **Applications of UDP**

- Suitable for simple request response communication with little concern for flow or error control.

- Trivial File Transfer Protocol (TFTP) - Uses UDP because it has its own error control mechanisms

- UDP supports multicasting which is not available in TCP.

- Used in network management. SNMP and DNS

- Routing protocols - Such as Routing Information Protocol (RIP)

Page No:
Date:

Transmission Control Protocol (TCP)

TCP requires a connection to be established before data can be sent. Like UDP, it allows communication between processes. TCP includes mechanisms for flow control, error control and congestion control. TCP delivers data as a continuous stream in contrast to UDP's datagram. Data can flow in both directions simultaneously.

TCP features

1. Numbering System - Data bytes are numbered sequentially
2. Sequence Number - Represents the number of the first byte in the segment
3. Acknowledgement Number - Indicates the next byte expected by the receiver, making acknowledgement cumulative
4. Flow Control - TCP byte oriented system ensures that data is not sent faster than the receiver can handle.
5. Error Control - TCP ensures reliable delivery by using acknowledgement and retransmission mechanisms
6. Congestion Control - TCP adjusts the data transmission to prevent network congestion.

Three Way Handshake for TCP connection establishment

1. Client sends SYN - The client sends a SYN segment to initiate a connection, synchronising sequence numbers.
2. Server responds with SYN + ACK - The server responds with a SYN+ACK segment, acknowledging the client's request and synchronisation sequence numbers for its own data.
3. Client sends ACK - The client sends an ACK to complete a handshake, establishing the connection.

Page No:
Date:

Connection Termination in TCP

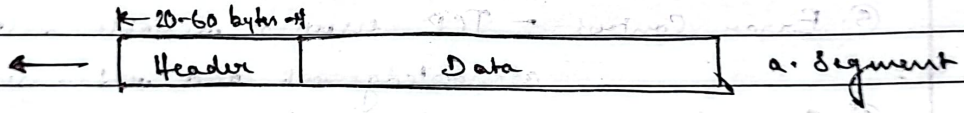
① Client sends FIN – The client initiates termination by sending a FIN segment

② Server responds with FIN + ACK – The server acknowledges the FIN and sends its own FIN to close the connection from its side.

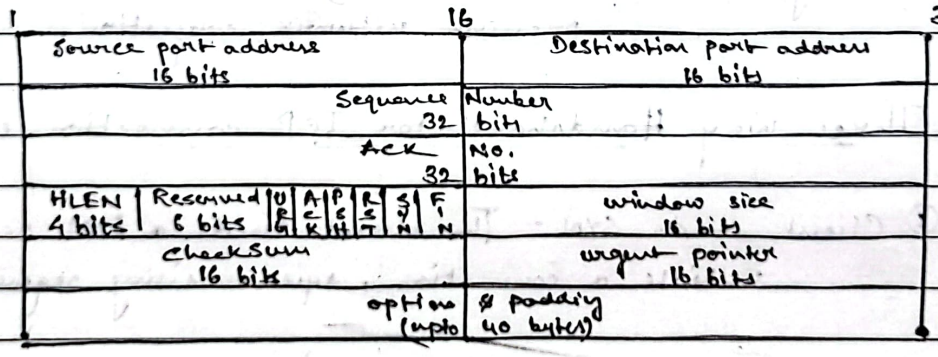
③ Client Sends ACK – The client acknowledges the servers FIN and connection is terminated.

Half Close – It allows one side of the connection to stop sending data while still receiving data from the other side.

TCP Segment Format



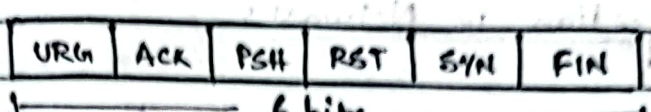
a. Segment



b. Header

Page No:
Date:

Control Field



URG - Urgent pointer is valid
ACK - Acknowledgement is valid
PSH - Request for push
RST - Reset the connection
SYN - Synchronize sequence numbers
FIN - Terminate the connection

- Header length (HLEN) - This 4 bit field indicates the length of the header in the units of 4 byte word
- Reserved - 6 bit field reserved for future use
- Control - This field defines 6 different control bits / flags.
- Window size - Defines size of the window, in bytes, that the other party must maintain. As the length of this field is 16 bits, max. size of window is 65535 bytes.
- Checksum - The calculation for checksum for TCP follows the same procedure as the one described for UDP. However, the inclusion of the checksum in the UDP is optional while in TCP is mandatory.
- Urgent Pointer - This 16 bit field is only valid iff the urgent flag is set and is used when segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

Page No:
Date:

Congestion in Networks

- Congestion occurs when the networks load ~~exceeds~~ exceeds its capacity.
- Routers and switches have buffers that temporarily store packets before processing which can lead to congestion.

Congestion control in TCP

- Congestion control involves techniques to either prevent or manage congestion. It aims to keep the networks load below its capacity

- TCP uses a congestion window (cwnd) that adjusts based on network conditions, alongside the receiver window (rwnd)

Congestion Detection - It detects congestion through two main signals

① Timeout - Severe congestion
② Three duplicate ACKs (mild congestion)

Congestion Control Mechanisms

① Slow Start (SS) - Starts with a small congestion window (cwnd = 1 MSS) and exponentially increases the size with each ACK until a threshold (ssthresh) is reached.

② Congestion Avoidance (CA) - After reaching the threshold, cwnd grows linearly to avoid overwhelming the network

③ Fast Recovery (FR) - Triggered after receiving three duplicate ACKs. Cwnd is halved (multiplicative decrease) and then incremented linearly as duplicate ACKs are received, signalling mild congestion.

- AIMD (Additive Increase, Multiplicative Decrease)
  After congestion is detected, TCP reduces the congestion window multiplicatively and then increases it additively forming a saw tooth pattern of congestion control.

- TCP Variants

① Tahoe TCP - Uses only slow start and congestion avoidance. It treats both timeout and duplicate ACKs the same by resetting to slow start.

② Reno TCP - Differentiates b/w timeouts (which lead to slow start) and duplicate ACKs (which lead to fast recovery)

③ New Reno TCP - An optimized version of Reno TCP for improved congestion recovery.

Congestion v/s network performance