UNIT-I INTRODUCTION AND APPLICATION (CS3591)

PROTOCOL LAYERING

S. NIMMIDEVI ,AP
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
ADHIPARASAKTHIN ENGINEERING COLLEGE

Define

1. Communication service where the process is used to exchange the messages.
2. Communication is simple, we can use only one simple protocol.
3. When the communication is complex, we must divide the task between different layers, so, we need to follow a protocol at each layer, this technique we used to call protocol layering.
4. This layering allows us to separate the services from the implementation.

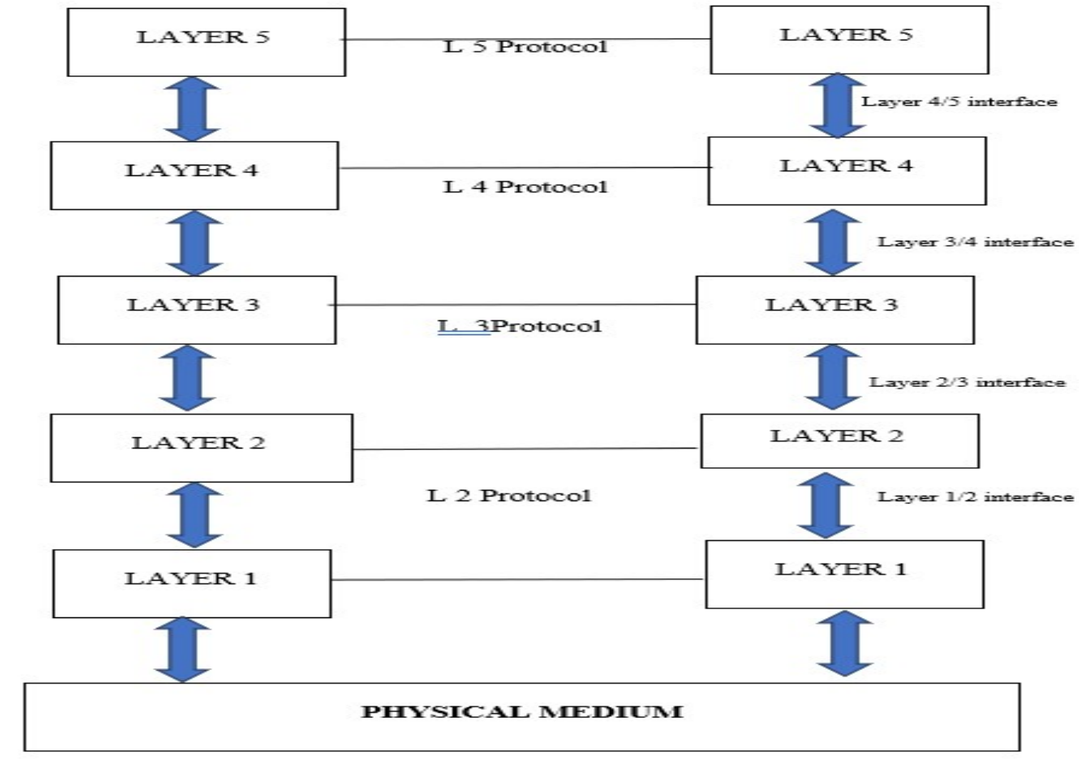
Basic Elements of Layered Architecture

Service − Set of actions or services provided from one layer to the higher layer.

Protocol − It defines a set of rules where a layer uses to exchange the information with its peer entity. It is concerned about both the contents and order of the messages used.

Interface − It is a way through that the message is transferred from one layer to another layer.

BASIC FIVE LAYER ARCHITECTURE



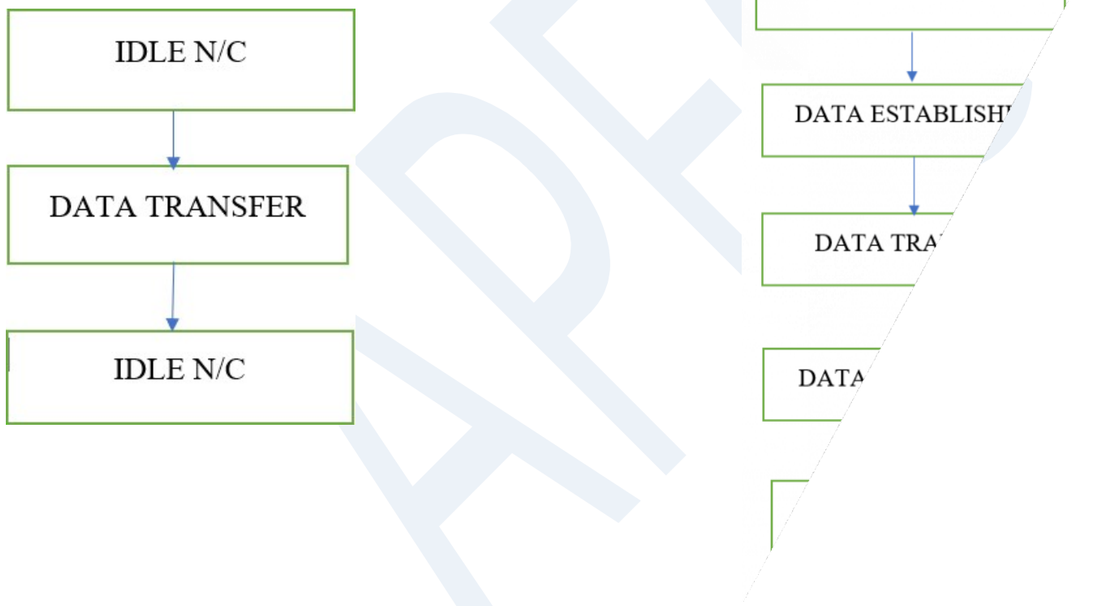
Benefits

1. Breaking the unmanageable task into several manageable task
2. Modularity and clear interface
3. We can change or modify with out affecting another layer
4. Each layer is analyzed and tested independently

Interfaces and services

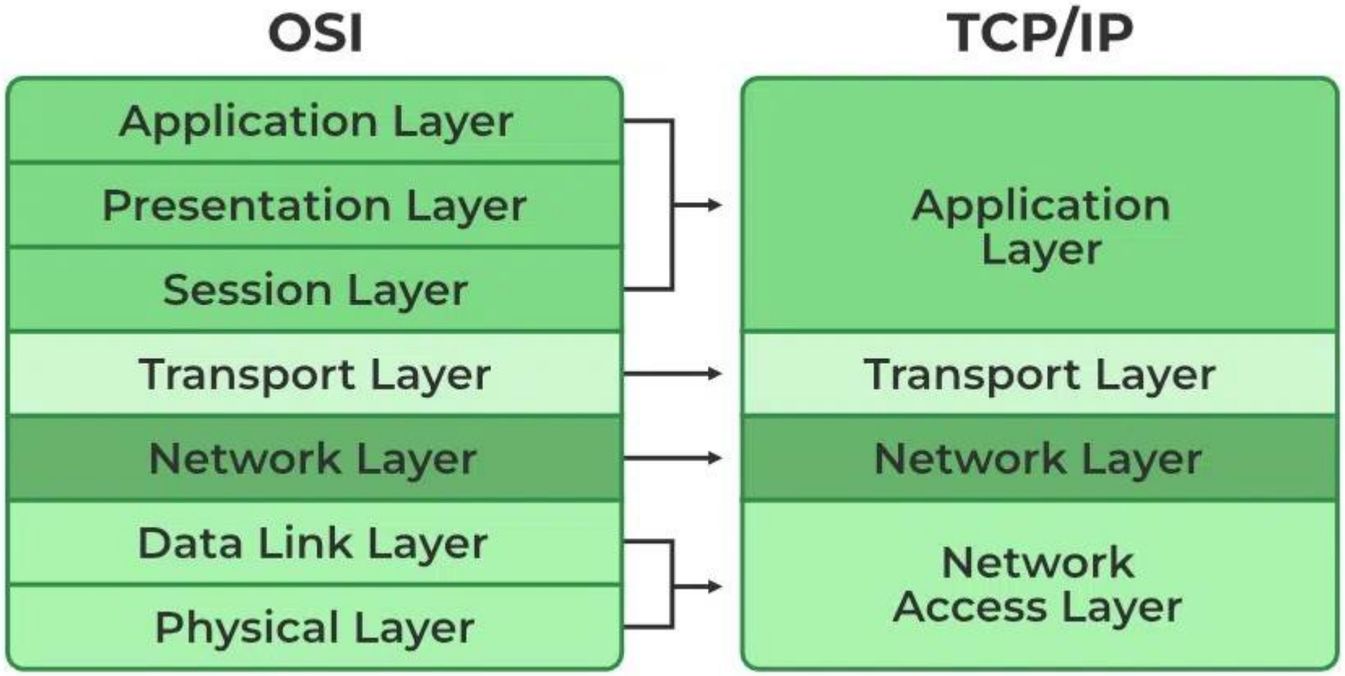
- Common technique for each layer to communicate with each other.
- N-1,N+1 and N layers
- SDU-T/F Data from N+1 to N-1 &N layers.
- PCI-Perform Service function
- Used to exchange infn by peer entities at different sites of network
- PDU- Combination of SDU and PCI
- ICI- It passes the temporary parameter between N& N-1 to invoke service function
- IDU-Total unit of infn transferred across the layer boundaries

Connection oriented and connection less Service



TCP/IP PROTOCOL SUITE

- Internet Architecture
- This model defines how data is transmitted over networks, ensuring reliable communication between devices.
- It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.
- Host to network-Physical & DLL
- Appln Layer-session, Presentation, appln of OSI Layer
- TCP/IP- two Protocol at TP layer-TCP & UDP


OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer

Network Access Layer

- This layer is responsible for generating the data and requesting connections.
- It is responsible for accepting & Transmitting IP datagrams.
- Host to Network Layer/Network Interface Layer
- Cannot Define any Protocol

Internet or Network Layer

It defines the protocols which are responsible for the logical transmission of data over the entire network.

IP: It is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers

ICMP: It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.

ARP: Its job is to find the hardware address of a host from a known IP address.

Transport Layer

- Exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.
- End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

Application Layer

- It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.

Differences

OSI MODEL	TCP/IP
Open System Interconnection.	Transmission Control Protocol.
OSI model has been developed by ISO (International Standard Organization)	It was developed by ARPANET (Advanced Research Project Agency Network).
the transport layer provides a guarantee for the delivery of the packets.	does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
vertical approach.	horizontal approach.
the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It consists of 7 layers.	It consists of 4 layers.
The usage of this model is very low.	This model is highly used.

TCP/IP MODEL

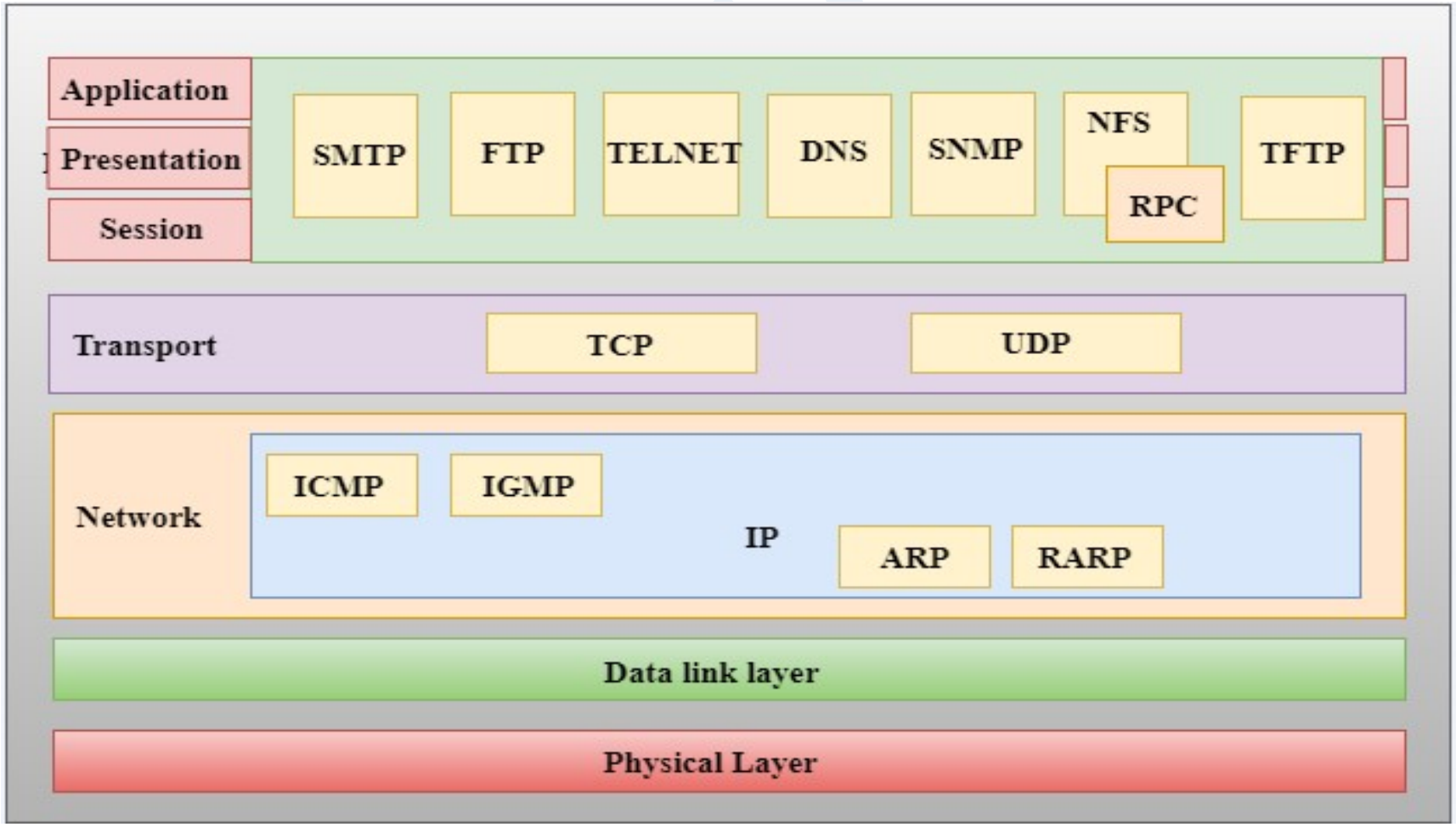


TCP

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- Internet Model

APEC

TCP/IP MODEL


Application
Presentation
Session
SMTP
FTP
TELNET
DNS
SNMP
NFS
RPC
TFTP
Transport
TCP
UDP
Network
ICMP
IGMP
IP
ARP
RARP
Data link layer
Physical Layer

APPLICATION LAYER

- It transports the data and deliver the data
- TELNET-Remote Login
- FTP-Interactive file transfer
- SMTP
- SNMP Delivers the electronic mail



TRANSPORT LAYER

- Appln pgm's send data to Transport Layer
- Incoming Byte Stream------Discrete message
- Handles flow control
- Synchronize b/w Fast sender and Slow Receiver
- Prompt Delivery



INTERNET LAYER

- IP,ARP,ICMP handle machine to machine communication
- Used to move the data
- 2 types
  - Addressing
  - Fragmentation

APEC

HOST TO NETWORK LAYER

- Network Interface layer
- Same as Physical &Data link
- Not Define any protocol

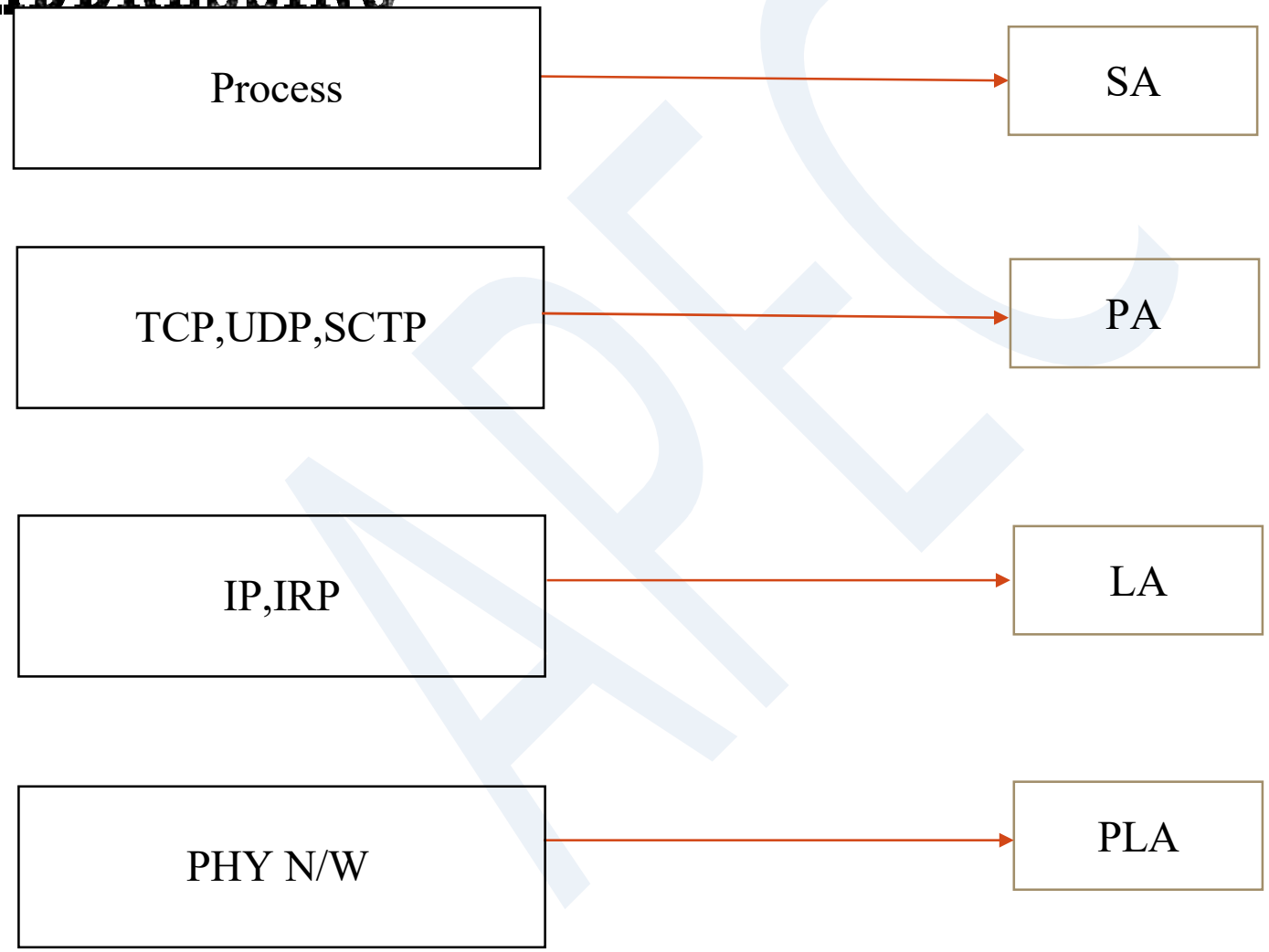
APEC

DIFFERENCE

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.



ADDRESSING



PA &LA

- HOP-HOP
- Lowest level of address
- LAN/WAN➔ address of node 1

- Independent of underlying physical networks
- Necessary for universal communication
- 32 bits
- Remains Change



PA &SA

- Single appln on a single computer
- Port number is used to identify the process
- 16 bits in length

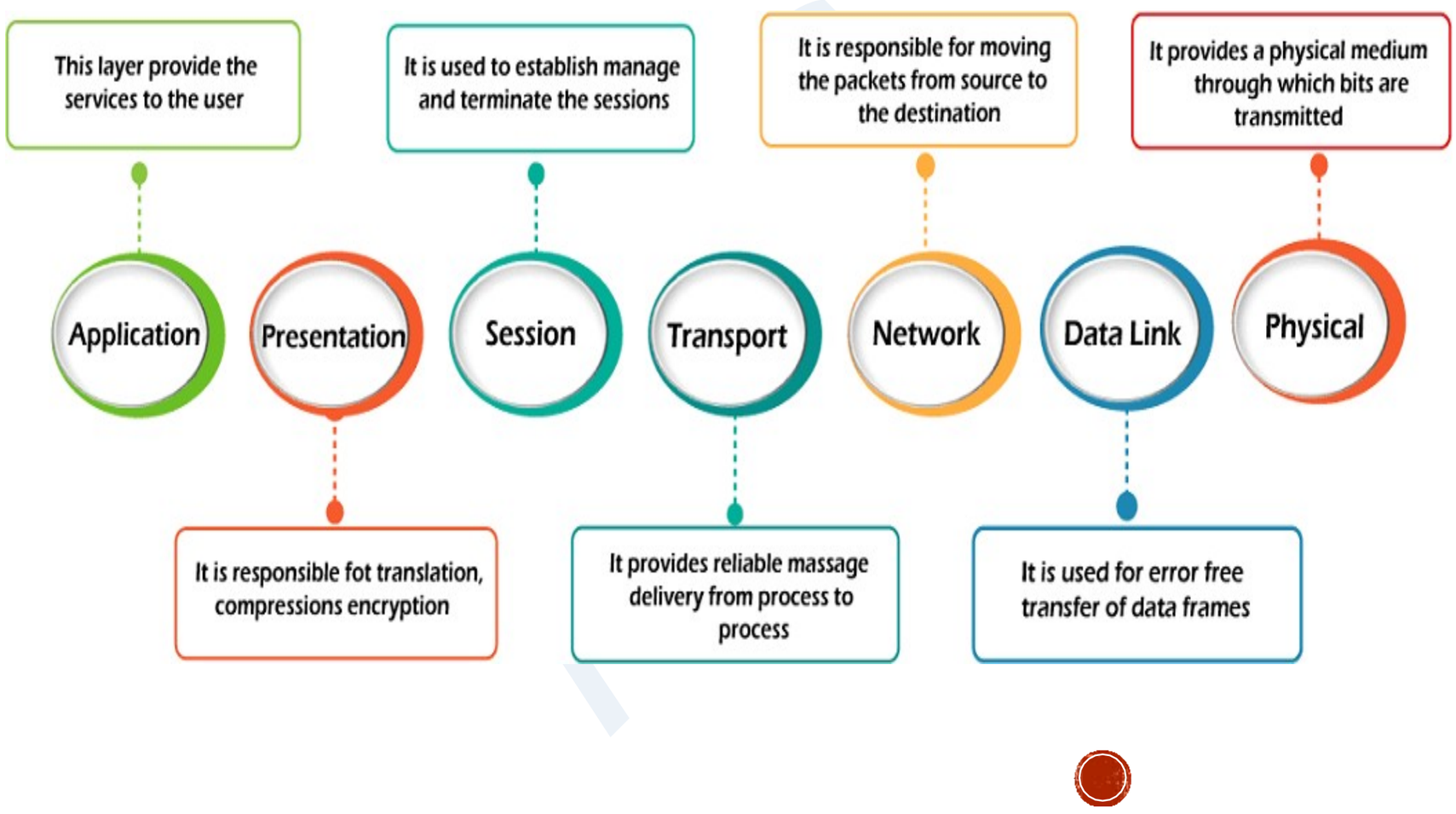
- User friendly address used for specific appln
- Eg-email address and URL

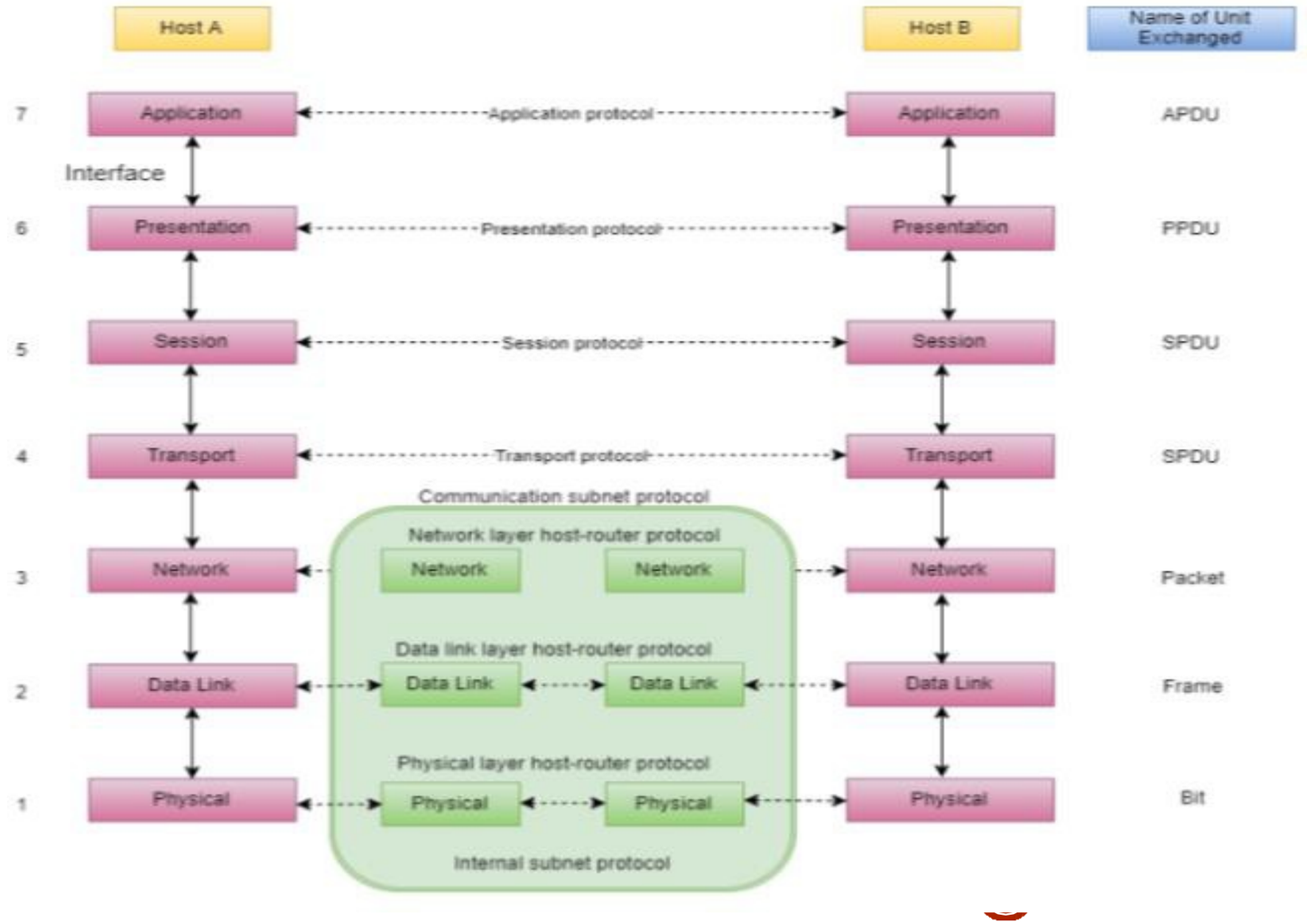
OSI MODEL

- OSI ➔ Open System Interconnection
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI ➔Developed-----ISO in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

Services

- Provides peer to peer logical services(decentralized network, allow users to interact directly with each other without a central authority or server)
- Standards for communication between system
- Each layer should perform a well defined function


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames


Host A
Host B
Name of Unit Exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
SPDU
Communication subnet protocol
Network layer host-router protocol
3
Network
Network
Network
Network
Packet
Data link layer host-router protocol
2
Data Link
Data Link
Data Link
Data Link
Frame
Physical layer host-router protocol
1
Physical
Physical
Physical
Physical
Bit
Internal subnet protocol

Physical Layer

- It is responsible for the actual physical connection between the devices.
- It contains information in the form of **bits.**
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

❖ **FUNCTIONS**

•**Bit Synchronization: P**roviding a clock. This clock controls both sender and receiver receiver thus providing synchronization at the bit level.

•**Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

•**Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

- *Hub, Repeater, Modem, and Cables are Physical Layer devices*

Data link layer

- The data link layer is responsible for the node-to-node delivery of the message.
- Main Function: Data transfer is error-free from one node to another, over the physical layer
- It provides a reliable and efficient communication between two or more devices.

FUNCTIONS

Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame.

- **Flow Control:** It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's . If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time

Switch & Bridge are Data Link Layer devices

Network Layer

- ✓ Responsible for the delivery of Packets from source to destination.
- ✓ It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- ✓ Responsible for routing and forwarding the packets.
- ✓ The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

FUNCTIONS:

•**Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

•**Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

•**Routing:** Routing is the major component of the network layer, and it determines the

best optimal path out of the multiple paths from source to the destination

- *Segment in the Network layer is referred to as **Packet** .*

Transport Layer

- Responsible for delivery of messages from one process to another
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

FUNCTIONS

- ✓ Segmentation and reassembly-msg is divided in to segments – it contains a sequence number which enables the transport layer
- ✓ Connection Control-connection oriented or connection less
- ✓ Flow control
- ✓ Error Control

Data in the Transport Layer is called ***Segments*** *.*

Session Layer

- Network Dialog Controller
- This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.
- **FUNCTIONS**

•**Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes // we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

•**Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the

checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two system
- data translator for a network.
- It converts the data from one presentation format to another format.
- syntax layer.

FUNCTIONS

✓ Translation-Different computers used different encoding system

✓ Encryption-privacy while transmission

✓ Compression-compress the data. it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

- Accessing the network by user
- An application layer is not an application, but it performs the application layer functions.
- Provides user interfaces and other supporting services- email, remote file access

FUNCTIONS

•**File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

•**Mail services:** An application layer provides the

facility for email forwarding and storage.

INTRODUCTION TO SOCKETS



INTRODUCTION

- One end point of a two way communication link between 2 pgms running on a n/w
- Client and server➔ establish connection & Commn – via sockets
- A process sends a message and receive messages from the n/w through a software interface- socket



- Sockets--- host address & port address
- HA-IP address of the host where client and server program is loaded
- PA-Communication port used by client or server program
- Before an application program can transfer any data means 1st create a end point--- sockets



- C language
- <type.h>, <socket.h>----Header file
- Socket---- int socket(int family, int type, int protocol)
- Bind---assign the address to socket
- Int bind(int sd, struct sockaddr,*name, int namelen) 0-success ,1- failure
- Connect----establish a connection on socket
- Int connect(int sd, stucture sockaddr*name, int namelen)



- Listen ----indicates its response to receive connection
- Int listen(int sd,int backlog);
- Backlog---maximum no of connections should be in queue while it waits for server to accepts them
- Accept-accept the connection request
- Int accept(int sd,struct socktaddr *addr,int*addrlen);



- Close—Socket is closed by using close system call
- Int close(int sd)
- 0-return
- 1-failure



Function Call	Description
Socket()	To create a socket
Bind()	It's a socket identification like a telephone number to contact
Listen()	Ready to receive a connection
Connect()	Ready to act as a sender
Accept()	Confirmation, it is like accepting to receive a call from a sender
Write()	To send data
Read()	To receive data
Close()	To close a connection

HTTP

APEC



Introduction

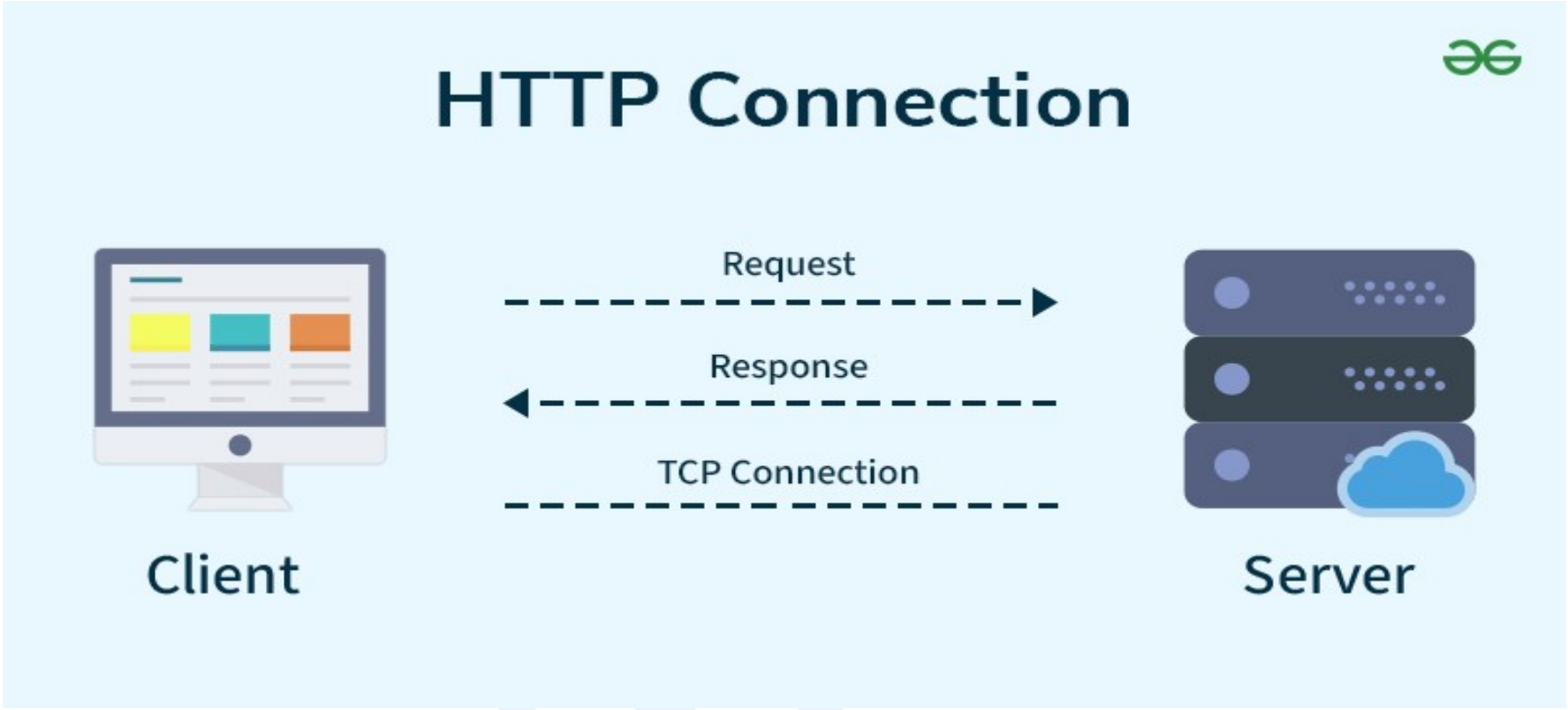
- Standard web transfer protocol
- The protocol used to transfer hypertext between two computers is known as Hypertext Transfer Protocol.
- It is a set of rules for transferring data from one computer to another
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on
- 2 fairly distinct items
  - 1. Set of request from browsers-server
  - 2. Set of responses going back to other way



Working

- **Open a website**
- **Type the URL(www.linkedin.com)**
- **URL ->SENT->DNS**
- **DNS -➔Check the record ->database**
- **URL sent**
- **Connection closed**
- **Search ->Reestablish**




HTTP Connection
Request
Response
TCP Connection
Client
Server

HTTP MESSAGES

- 2 type
- 1. Request
- 2. Response
- Same format
- The request message is sent by the client that consists of a request line, headers, and sometimes a body.
- The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

Request line
Header information
Blank line

URL

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.




URL
Uniform Resource Locator
Method
://
Host
:
Port
/
Path

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored
- **Port:** The URL can also contain the port number of the server, but it's an optional field.
- **Path:** Path is the pathname of the file where



the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

APEC

- HTTP (Hypertext Transfer Protocol) specifies a collection of request methods to specify what action is to be performed on a particular resource.

GET	is used to read/retrieve data from a web server.
HEAD	Used when Client wants some information about the document
POST	used to send data (file, form data, etc.) to the server.
PUT	used to modify the data on the server. It replaces the entire content at a particular location with data that is passed in the body payload. If there are no resources that match the request, it will generate one.
PATCH	PATCH is similar to PUT request, but the only difference is, it modifies a part of the data. It will only replace the content that you want to update.
DELETE	used to delete the data on the server at a specified location



HTTP headers

- ✓Header may be one or more header lines
- ✓Header line-Name, Colon, Space and Header value
- ✓4 Categories
- ✓General Header-General infn abt the msg(Request & Response)
- ✓Response Header-It specifies the server configuration and special infn abt the request
- ✓Request Header-It specifies the Client configuration and client preferred document
- ✓Entity Header-Infn abt the body of the document



HTTP types

- Non Persistent Connections
  - One TCP connection is made for each request/response.
  - Base HTTP file and 10 JPEG -> 11Objects reside on the same server
  - WWW.vtubooks.com /ITDept/home.index
  - HTTP client– initiates the a TCP connection to the sever
  - HTTP client send an HTTP request message to the server via socket
  - HTTP server receives the request message via socket
  - HTTP server tells TCP to close the TCP connection
  - HTTP client receives the response message. TCP connection termination



RTT & Hand shake

- It is the time it takes for a small packet to travel from client to server and then back to client
- Packet propagation delay, Packet queuing delay in intermediate routers, switches and packet processing delays
- RTT=2xPropogation time
- Total=2RTT+Transmit time
- TCP Connection establishes in 3 ways,
- Requesting the server for the connection.
- The server responds to whether the connection can be established or not.
- Acknowledgment by the client on the response sent by the server.



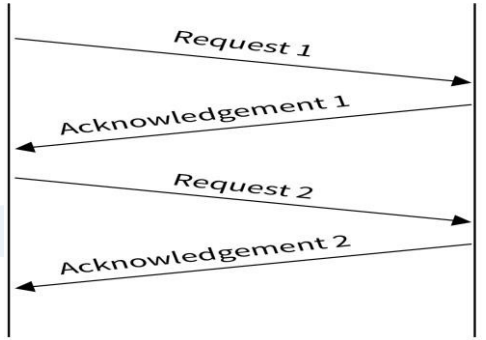
Disadvantage

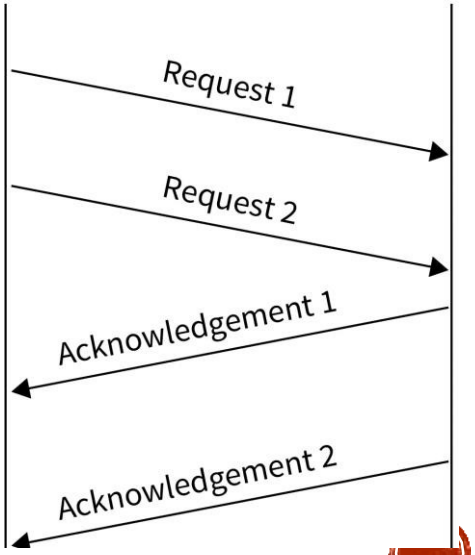
- TCP processing and memory resource wasted in the server and the client
- It requires delay with the transfer of each object

APEC

Persistent Connection

- HTTP 1.1
- Server now keeps the TCP connection open for a certain period of time after sending a response
- Types
- 1. Without Pipelining 2. With Pipelining
- Without Pipelining: The client can send a request to the server only if the previous request that was sent by the client has been acknowledged by the server.
- With Pipelining: The client can send a request to the server even if the previous request that was sent by the client has not been acknowledged by the server.





Proxy Server

- The **proxy server** is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server.
- It works as a gateway between the end-user and the internet.
- It has its own IP address.
- The proxy server accepts the request from the client and produces a response based on the following conditions:

1. If the requested data or page already exists in the local cache, the proxy server itself provides the required retrieval to the client.
2. If the requested data or page does not exist in the local cache, the proxy server forwards that request to the destination server.
3. The proxy servers transfer the replies to the client and also being cached to them.

- Therefore, it can be said that the proxy server acts as a client as well as the server.



Persistent & Non Persistent- Difference

Persistent Connection	Non-Persistent Connection
The Persistent Connection is the second version of the HTTP, and it is also called as HTTP/1.1	The Non-Persistent connection was the first version of HTTP, and it is also called as HTTP/1.0
It will always be in the default mode.	It will always be in the non-default mode.
The Persistent connection requires only one round trip time for all the objects.	The Non-Persistent connection requires two RTT's for every object present in the connection.
TCP is not closed	Closed(request-response)
For downloading the multiple objects, the Persistent connection only uses a single connection	For downloading the multiple objects, the non-Persistent connection requires multiple connections

FTP

- FTP --- 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.
- Downloading the files to computer from other servers.
- Designed for distributing files to a number of users

Objectives

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

COMMAND	PURPOSE
OPEN	Connect to a remote computer
GET	Retrieve a file from the computer

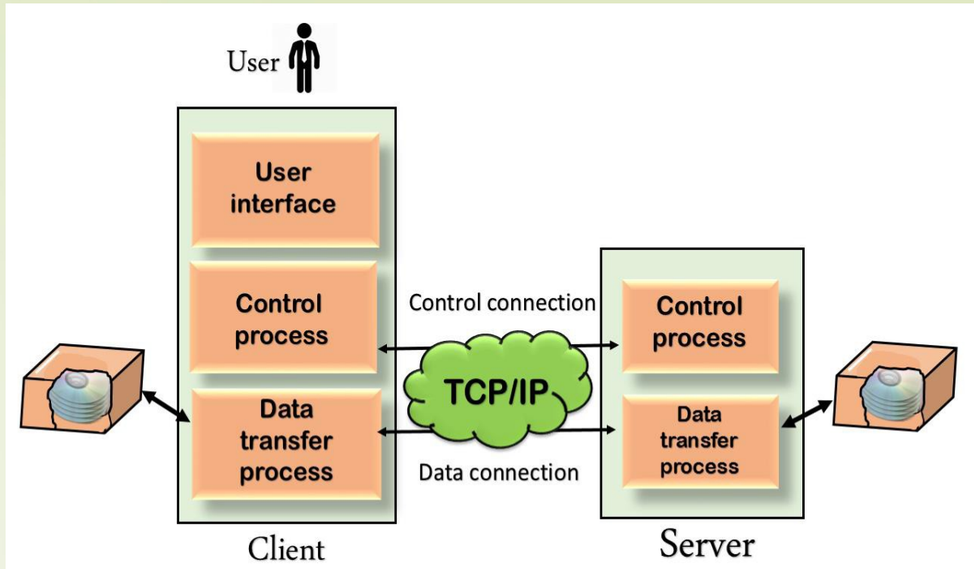
- 2 types of modes
- 1. ASCII 2. Binary(image)mode
- ASCII-used for transferring a text files including HTML files.
- FTP software automatically adjusts line endings for the system to which the file is transferred
- Binary-transferring of files consists of anything but

unformatted text.

- FTP software does not not make changes in the content of the file during transfer

FTP mechanism

- 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.



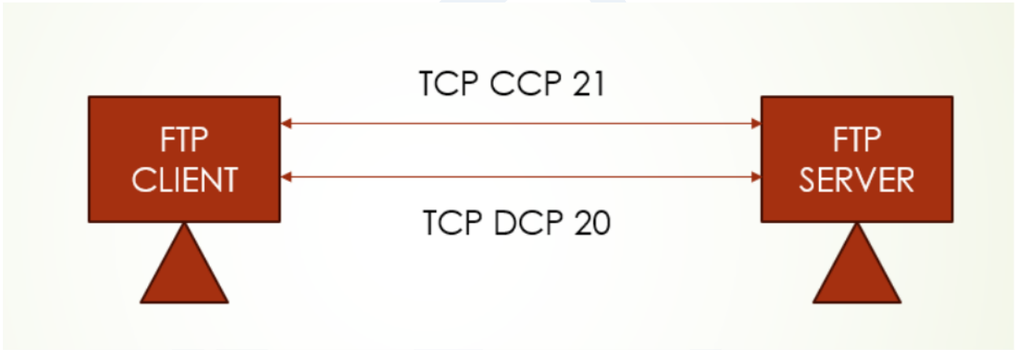
Types of Connection

- **Control Connection:** Simple. 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.
- **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.

Detail steps of FTP

- FTP client contacts FTP server at port 21 specifying TCP as transport protocol
- Client obtain authorization over control connection
- Client browse remote directory by sending commands over control connection
- When server receives a command for a file transfer, the server open a TCP data connection to client
- After transferring one file server closes connection.

- Server open a second TCP data connection to transfer another file



- FTP server maintains state

FTP Commands

S.NO	Command	Meaning
1	Cd	Changes the working directory on the remote host
2	Close	Closes the FTP connection
3	Pwd	Displays the current working directory on the remote host
4	Remotehelp	Displays a list of all server FTP commands
5	Help	Displays a list of all Client FTP commands
6	Type	Allows the user to specify the file type

TFTP

- It is a siample protocol that is commonly used for file transmission.
- TFTP employs the ***User Datagram Protocol (UDP)*** to transport data from one end to the other.
- Fixed length -512 bytes
- It operates on Port number 69, and its service is given by UDP.

Difference b/w FTP and TFTP

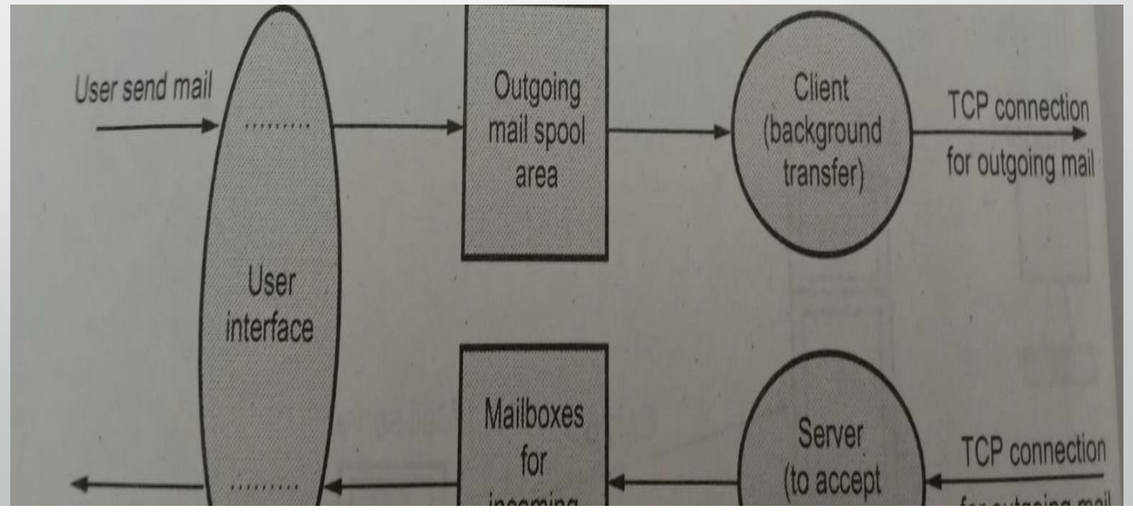
FTP	TFTP
It supports user authentication.	It doesn't support user authentication.
It uses TCP port numbers 20 and 21.	It uses UDP port number 69.
FTP protocol is a connection-oriented service.	TFTP protocol is a connection-less service.
It is mainly based on the TCP.	It is mainly based on the UDP.
It utilizes a lot of commands to perform tasks.	It utilizes five messages to perform tasks.
It is more complex.	It is less complex.
It needs more memory.	It needs less memory.
Remote users utilize the FTP protocol to download and upload files.	TFTP is mainly used to transfer configurations to network devices.
FTP software is larger in size. So, it is heavier than TFTP.	TFTP software is smaller in size. So, it is lighter than FTP.
It is slower.	It is faster.

EMAIL AND EMAIL PROTOCOLS

- Email is a asynchronous communication medium.
- Used for sending a single message, that includes text, voice to one or more recipients
- Fast, easy to distribute and inexpensive
- Not connection oriented
  - Web based email service
  - Email through LAN
  - Unix Shell account
  - Using mail client

Compon
ents

- 1. User agents
- 2. Mail Servers
- 3. SMTP



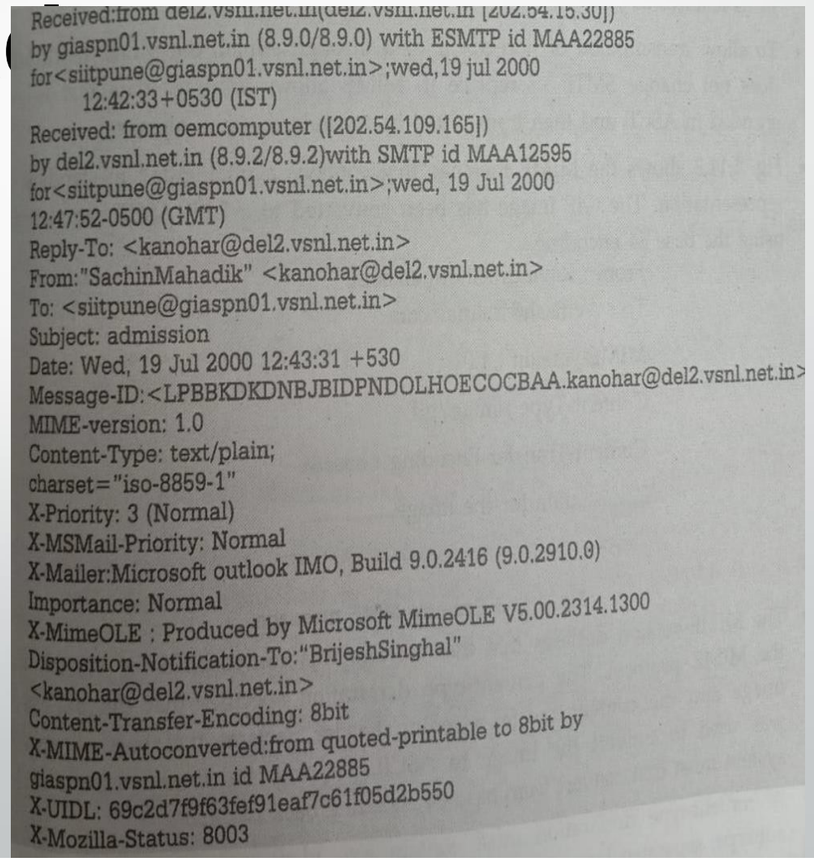
Email Addressing

- To send email to some one, the internet email address must be known to sender vilas@hotmail.com

- Vilas-User name
- Hotmail- host or domain name

Message Hea

- Include the address of the receiver and the sender



Formatted E-mail

- HTML-Just like web pages.
- Rich Text-Read by most word processing applications
- MIME-just created for email
- MS Word format- Microsoft word

Sr. No.	Content type	Use
1.	Text	Textual (document)
2.	Image	Photograph
3.	Audio	A sound recording
4.	Video	A video recording including motion
5.	Application	Raw data for program

Functions of E-mail

- 5 basic functions
- 1. Composition-Process of creating messages and answers
- 2. Transfer 3.Reporting 4. Displaying 5. Disposition

User Agent and Message Transfer Agent

- User agent-It allows user to read and send email. Local programs that provide a command based, menu based or graphical method for interacting with the email system

- Message transfer agent-Move the messages from source to destination

DNS

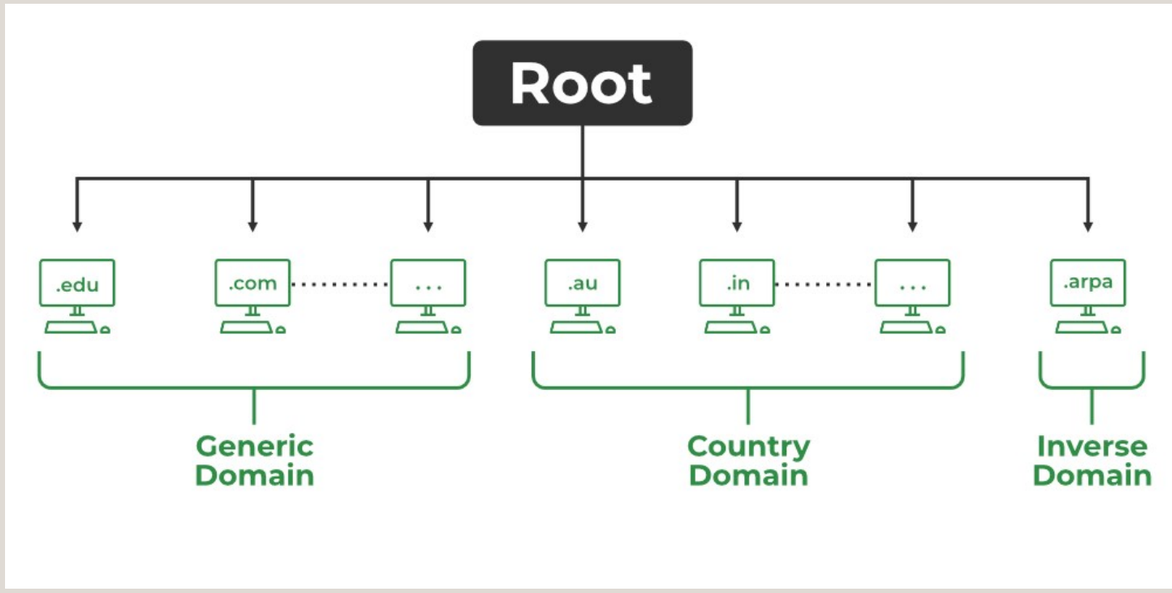
INTRODUCTION

- **Goal- Assign meaningful high level names to a large set of machines and handle the mapping of those names to a machine IP address**
- Case Insensitive com/COM
- Runs over the UDP and uses port 53
- DNS –Application Layer Protocol
- 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 EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

COMPONENTS

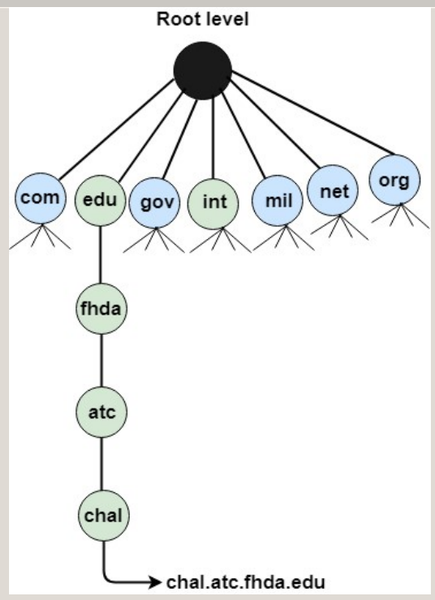
- 6 components
- 1.Domain 2. Domain name 3.Name Server 4.Name Resolver 5.Name Cache 6. Zone
- Vtubooks.com com-domain
- Vtubooks-domain name
- Name sever-Mapping domain names into IP addresses
- Name resolver-software –client interacting with server
- Name cache- Storage used by the name resolver to store information frequently
- Zone-Contigous part of a domain

TYPES


Root
.edu
.com
...
.au
.in
...
.arpa
Generic Domain
Country Domain
Inverse Domain

GENERIC DOMAIN

- 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.



COUNTRY AND INVERSE DOMAIN

- The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States)
- Used to map the address of a name
- 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

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.

NAME SPACES

- 2 types 1. Flat 2. Hierarchical
- Flat-Original set of machines on the internet . It consists of sequence of characters with no further structure
- Name is assigned to address
- Adv-Names are convenient and short
- Disadvantage-Flat name cannot generalize to large set of machines because they are large set of identifiers

- Hierarchical names-partitioning of name spacing
- Provides is simple yet flexible naming structure
- Partitioned at top level
- A tree can have only 128 levels
- Top level domain -3 types
- Arpa-Special domain used for address to name mappings
- 3 characters –generic
- 2 Characters –Country domains

DOMAIN NAME SPACE

- Inverted tree structure with the root at the top.Tree -128(0-127)
- Each node in a tree has a label , which is a string with maximum of 63 characters .Root label-null string/empty
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- Domain name-2 1.FQDN 2. PQDN

HIERARCHY OF NAME SERVERS

- To distribute the information of many computers , DNS servers are used
- Creates many domains as there are first level of nodes
- ZONE-Server have some authority and also responsible for operation . Server creates a database, called zone file. Server maintain all the infn abt the node
- 2 condition-1. Domain and zone –same –Server accept the responsibility for a domain and not divide the domain into sub domain
- 2.Domain and Zone-not same-divide

- Root server –if Zone consists of a full tree then that zone server is called root server.Doesnot maintain information about the domain
- 2 types of server 1. Primary server 2. Secondary server
- Primary-Server keeps the file about the zone for which is responsible and have authority. Operations-create, Update and maintaining
- Secondary- Loads all information from the primary server

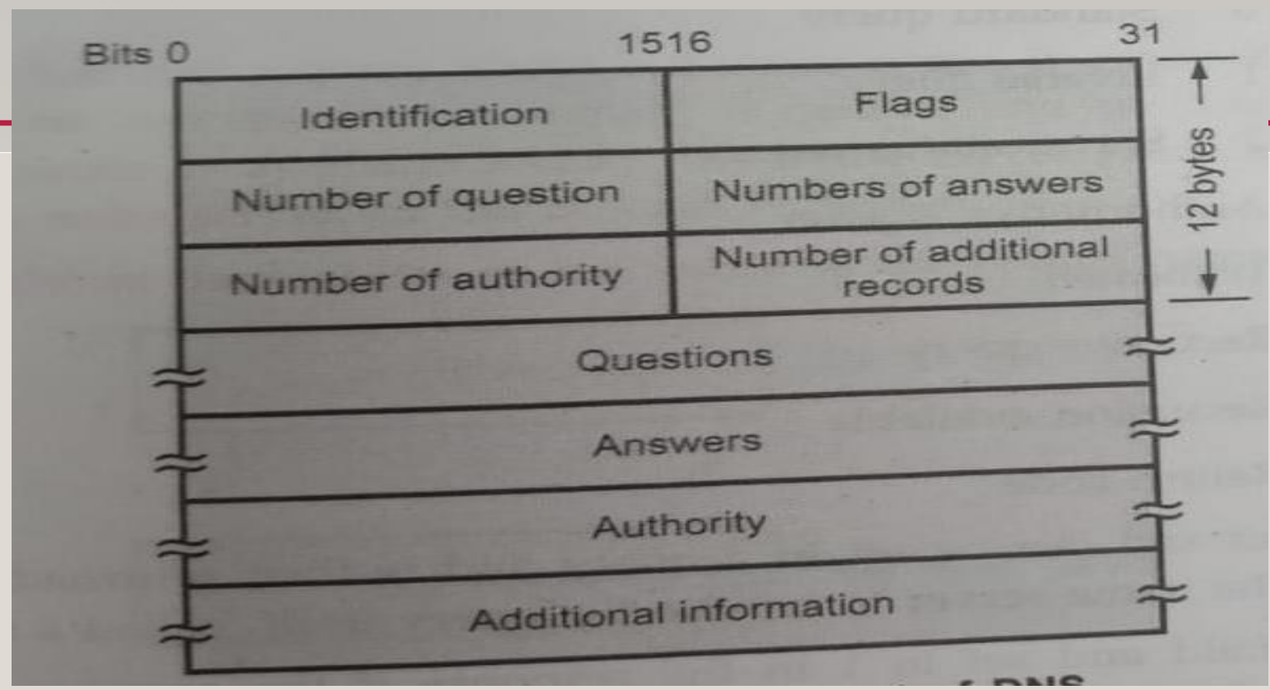
RECURSIVE AND ITERATIVE RESOLUTION

- Recursive-A client request complete translation. If server authority for the domain name, it check it database and respond.
- If the Server is not authority, it sends the request to another server and wait for the response
- When query is finally resolved finally travel back until finally reaching the requesting client
- Non Recursive-Only a single resolution is made and returned.
- If the server is an authority for the name it sends the answer .If it is not it returns to the IP address of the server that it thinks can resolve the query

MESSAGE FORMAT

- Query message
- Response message.
- The information is held up in up to five different sections of DNS message format. The query message is having two sections- header and question records.
- The response message consists of five sections:
- Header
- Question
- Records
- Answer records
- Authoritative records
- Additional records

- **Identification:** The identification field is made up of 16 bits which are used to match the response with the request sent from the client-side.
- **Flags:** It is 16 bits and is divided into the following Fields .
- **Number of Questions-** It is a 16-bit field to specify the count of questions in the Question Section of the message. It is present in both query and response messages.


Bits 0
1516
31
Identification
Flags
Number of question
Numbers of answers
Number of authority
Number of additional records
12 bytes
Questions
Answers
Authority
Additional information

LDAP

- Light weight directory access protocol
- Application level protocol-implement on top of TCP
- It stores entries, which is similar to objects. Each entry must have a distinguished name
- LDAP provides binary, string and time types.
- It defines a network protocol for carrying out definition and manipulation

DDNS

- Dynamic Domain name system
- Service that maps internet domain name to IP addresses
- Allows anyone hosting a web or FTP server to advertise a public name to prospective users
- DNS-Static IP addresses work
- DDNS-Dynamic IP addresses work

ADVANTAGE

- Easy to remember
- An integral part of the internet
- Search engine friendly
- Change in IP address
- Very fast
- Easy and flexible
- High security

--









