TCP/IP Reference Model:

The TCP/IP model **does not same** as OSI model. It is a **set of protocols** that allow communication across multiple different networks.
It always provides a kind of environment where transferring of packets perform in appropriate manner. It is also known **as internet protocol suite** which is a networking model and a set of communication protocol used for the internet.

TCP/IP model provides **end to end connectivity** and specify how data should be formatted, addressed, transmitted, routed and received at the destination.
These functionalities have been organized into **4 layers** which is known as layers of TCP/IP model. Layers are

1) The Host to Network Layer
2) Internet layer
3) Transport layer
4) Application Layer

1) The Host to Network Layer:

It is the lowest layer of TCP/IP reference model which is concerned with the network specific aspect of the transfer of packets. It always helps to connect to the network using some protocols, so it can transmit IP packets over it.
This protocol is not specified and may vary host to host and network to network. Here, the host has connect to the network using some protocol so it can transmit IP packets over it. Protocols like ARP, RARP etc that help in transmission.

Address Resolution Protocol (ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an **ARP broadcast** message asking, “Who has this IP address?”
Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it.
ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.
Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both

sending and receiving hosts. Next time, if they require communicating, they can directly refer to their respective ARP cache.
Reverse ARP is a mechanism where host knows the MAC addresses of remote host but requires knowing IP address to communicate.

2) Internet layer:

This layer is also known as connectionless internetwork layer. It is the upper layer of network interface layer that handles the transfer of information across multiple network.

It transfers packets into any network and have them to deliver independently to the destination. They may appear in a different order than they were sent but also rearrange them in order to deliver them to proper destination.

The internet layer specifies an **official packet format** and protocol known as **internet protocol.** The job of internet layer is to transport IP packets to appropriate destination.

Packet routing is very essential task in order to avoid congestion. For these reason it is said that TCP/IP internet layer perform same function as that of OSI network layer.

IP (Internet Protocol) is the main protocol if internet layer and provides communication between hosts on different kind of networks. It is a connectionless, unreliable, packet delivery service. That means, there is no guarantee that a packet gets delivered.
IP defines an addressing scheme that is independent of the physical address or MAC address. It has two classifications like:

a. Internet Protocol Version 4 (IPv4)
b. Internet Protocol Version 6 (IPv6)

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable. Though IP is not reliable one; it provides '**Best-Effort-Delivery**' mechanism.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP Address divided into two parts:
– Prefix (network ID) identifies network to which host attaches
– Suffix (host ID) identifies host on that network

IP addresses are divided into many categories:

Class A- It uses first octet for network addresses and last three octets for host addressing, that means Network ID is 8 bits and Host ID is 24 bits.

NID 8 bits	HID 24 bits

Class B - it uses first two octets for network addresses and last two for host addressing, means that means Network ID is 16 bits and Host ID is 16 bits

NID 16 bits	HID 16 bits

Class C - it uses first three octets for network addresses and last one for host addressing, means that means Network ID is 24 bits and Host ID is 8 bits

NID 24 bits	HID 8 bits

Class D - it provides flat IP addressing scheme and used for multicasting.

Class E - It is used as experimental and for future use.

Internet Protocol Version 6 (IPv6)
IPv6 is a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

3) Transport layer:
In the TCP/IP model, the layer above the internet layer is known as transport layer. It is developed to permit entities on the source and destination hosts to carry on a conversation.

It is a connection oriented protocol that always makes a connection then start communication. It is a reliable connection that allows a byte to byte transfer from one machine to another machine without any error.

It specifies 2 end-to-end protocols
1)TCP (Transmission Control Protocol)
2)UDP (User Datagram Protocol)

i) TCP
It is a reliable connection-oriented protocol that permits a byte stream originating on one machine to be transported without error on any machine in the internet. It divides the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination, the receiving TCP process collects the received message into the output stream. TCP deals with flow control to make sure a fast sender cannot swamp a slow receiver with more message than it can handle.

ii) UDP

It is an unreliable, connectionless protocol for applications and there is no guarantee to deliver the message. It is widely used where accuracy doesn't matter and requires quick delivery.

It is also used for client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery.

4) Application Layer:

In TCP/IP model, session or presentation layer are not present. Application layer is present on the top of the Transport layer. It includes all the higher-level protocols and some common are:

1. Hyper Text Transfer Protocol (HTTP)
2. File transfer Protocol (FTP)
3. Simple mail Transfer Protocol (SMTP)
4. Simple Network Management Protocol (SNMP)
5. Dynamic Host Configuration Protocol (DHCP)

Hyper Text Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is an application layer protocol for distributing information in the World Wide Web (WWW). Hypertext Transfer Protocol (HTTP) is based on the **client–server architecture**.

Hypertext Transfer Protocol (HTTP) is the protocol that enables the connection between a web server and a client. A Hypertext Transfer Protocol (HTTP) server (commonly called as a web server) uses the well-known port number 80.

HTTP permits applications such as browsers to upload and download web pages. It makes use of TCP at the transport layer again to check reliability.

HTTP is a connectionless protocol that sends a request, receives a response and then disconnects the connection. HTTP delivers HTML documents plus all the other components supported within HTML such as JavaScript, Visual script and applets.

Hypertext Transfer Protocol (HTTP) operates on a request-response model. A browser sends a request to a server for a file, and the server responds with the requested file if it is available. HTTP messages are English based and it converts it into their logical address or IP address to make interface.

File Transfer Protocol (FTP)

It was designed to permit reliable transfer of files over different platforms. FTP offers simple commands and makes the differences in storage methods across networks transparent to the user.

The FTP client is able to interact with any FTP server; therefore the FTP server must also be able to interact with any FTP client.

FTP does not offer a user interface, but it does offer an application program interface for file transfer. The client part of the protocol is called FTP and the server part of the protocol is known as FTPd. The suffix "d" means Daemon where a daemon is a piece of software running on a server that offers a service.

Simple Mail Transfer Protocol (SMTP)

SMTP is the Application Layer protocol that handles message services over TCP/IP networks. It is based on end-to-end message delivery.

SMTP sends email to other computers that support the TCP/IP protocol suite. It supervises the email sending from the local mail host to a remote mail host. It is not reliable for accepting mail from local users or distributing received mail to recipients this is the responsibility of the local mail system.

SMTP makes use of TCP to establish a connection to the remote mail host, the mail is sent, any waiting mail is requested and then the connection is disconnected. It can also return a forwarding address if the intended recipient no longer receives email at that destination. To enable mail to be delivered across differing systems, a mail gateway is used.
After the sending is completed, the client can follow any of these actions.

Terminate Session: If the current Simple Mail Transfer Protocol **(SMTP)** client has no more messages to send, the connection can be closed with a **QUIT** command.

Exchange Roles: If the current Simple Mail Transfer Protocol **(SMTP)** client has no more messages to send, but is ready to receive any messages from the current Simple Mail Transfer Protocol **(SMTP)** server, it can issue the **TURN** command. Now the SMTP client and the SMTP server will switch their role of sender/receiver, and the sender (previous receiver) can now send messages by issuing a **MAIL** command.

Send Another Mail: If the Simple Mail Transfer Protocol **(SMTP)** client (sender) has another message to send, it can issue a new **MAIL** command

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol, also known as SNMP, is a vital protocol for Network Administrators. The SNMP protocol allows an Administrator to request information about one or more network devices hardware, software or configuration

SNMP is used as standardized protocol that manages network devices. The SNMP Protocol uses IP with UDP or TCP.

The SNMP Protocol has **two** sides, the **agent and the management** stations.
The agent sends data about itself to the management station.
The management station collects data from all the agents on the network.

The agent sends alerts called traps and answers requests that were sent by the management station.
The management station catches and decodes the traps.
The management station also requests specific information from the agent.
The agent is a server, router, printer, bridge or workstations.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is used to dynamically (automatically) assign TCP/IP configuration parameters to network devices (IP address, Subnet Mask, Default Gateway, DNS server etc.)

A computer that gets its configuration information by using DHCP is known as a DHCP client.

DHCP clients communicate with a DHCP server to obtain IP addresses and related TCP/IP configuration information.

DHCP server should be configured properly by the DHCP administrator. The **DHCP** client software is not configured with a static IP address and it is configured to obtain an IP address dynamically from a DHCP Server.

Dynamic Host Configuration Protocol (DHCP) server involves four steps as listed below.

1. **DHCPDISCOVER:** The DHCP client broadcasts a DHCP discover message on the network containing its MAC address. This first datagram is known as a DHCPDISCOVER message, which is a request to any DHCP server that receives the datagram for configuration information.

2. DHCPOFFER: Each DHCP server on the network that receives the request responds with a DHCP offer message as broadcast to the computer that issued the DHCPDISCOVER.

3. DHCPREQUEST: The DHCP client accepts an offer and broadcasts a DHCPREQUEST datagram. The DHCPREQUEST datagram contains the IP address of the server that issued the offer and the physical address of the DHCP client.

4. DHCPACK: When the DHCP server from which the offer was selected receives the DHCPREQUEST datagram, it constructs a DHCPACK datagram. This datagram is known as a DHCPACK (DHCP ACKNOWLEDGEMENT). The DHCPACK includes an IP address for the DHCP client.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. In OSI model the transport layer guarantees the delivery of packets	2. In TCP/IP model the transport layer does not guarantees delivery of packets.
3. OSI model has a separate presentation layer	3. TCP/IP does not have a separate presentation layer
4. Network layer of OSI model provide both	4. The Network layer in TCP/IP model

connection oriented and connectionless service.	provides connectionless service.
5. OSI model has a problem of fitting the protocols in the model	5. TCP/IP model does not fit any protocol
6. Protocols are hidden in OSI model and are easily replaced as the technology changes.	6. In TCP/IP replacing protocol is not easy.
7. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	7. In TCP/IP it is not clearly separated its services, interfaces and protocols.
8. It has 7 layers	8. It has 4 layers