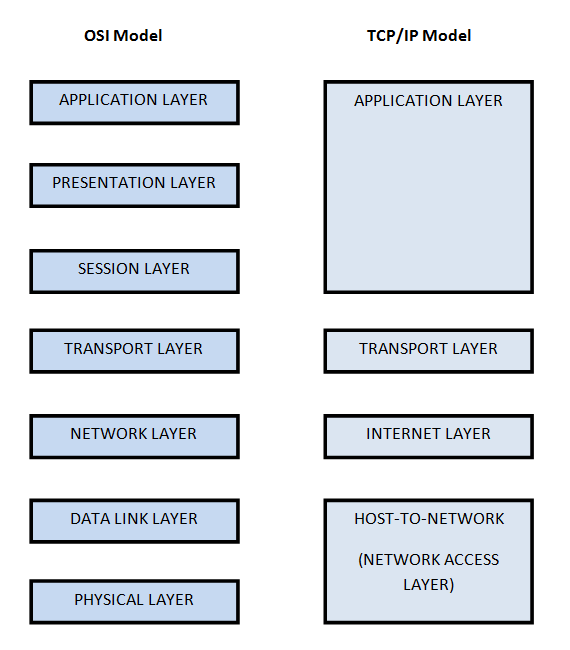
**1. Comparison between OSI and TCP/IP models.**

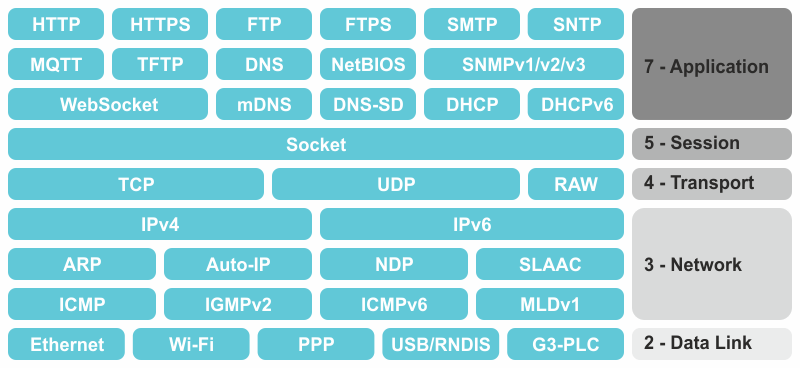
|  |  |
| --- | --- |
| **OSI** | **TCP/IP** |
| OSI or open system interconnection standard is protocol independent and works as a gateway between the user and its network | TCP/IP (transmission control protocol/internet protocol) standard are built on standard communication protocols and lets the hosts connect over the networks |
| OSI follows a vertical approach in its model | TCP/IP follows a horizontal approach in its model |
| In the OSI model the transport layer is responsible for the delivery of the packets | Where as in the TCP/IP model there is no guarantee that the transport layer would deliver the packets. |
| Within the OSI model the session and presentation layers are different | In TCP/IP there are no different layers of presentation and session. |
| The OSI model is often used as a reference while building a new network. | TCP/IP is kind off an implementation of the OSI model |
| In OSI model there are 7 layers | In TCP/IP there are 4 layers |
| In OSI there are different data link layer and physical layer | In TCP/IP there is only one layer that is Network access layer |
| The OSI model is new as compared to the TCP/IP model | The TCP/IP model is older than the OSI model when compared. |
| The OSI model is a conceptual model and is used for understanding the network functions | The TCP/IP model is designed to function to solve set of problems and not to act as a reference guide for other networks |
| The network layer of OSI model gives both mode of service i.e. connectionless and as well as connection oriented. | The network layer of TCP/IP gives only one mode of service i.e. connectionless. |
| In OSI model the protocols are hidden from user and can be replaced easily as and when technology is changed | In TCP/IP the changes in protocol is not that easy as compared to the OSI model. |
| The transport layer in this model is connection oriented in nature. | The transport layer in this model provides both connectionless and connection-oriented services. |



(Fig. Refrence: <https://www.quora.com/What-is-OSI-model-and-TCP-model>)

**2. Transmission control protocol:**

* The transmission control protocol is a major part of the internet protocol model.
* TCP is reliable, ordered and uses checking system for the delivery of stream of packets between the applications that are running on hosts in an IP network.
* The TCP protocol lies in the intermediate level between the internet protocol and the application layer.
* The transport layer is responsible for host to host connectivity.
* The TCP protocol is used widely by many applications like world wide web and email system.
* TCP takes care from start to end connections in a state table where it stores all the internet IP address and ports.



**TCP protocol**

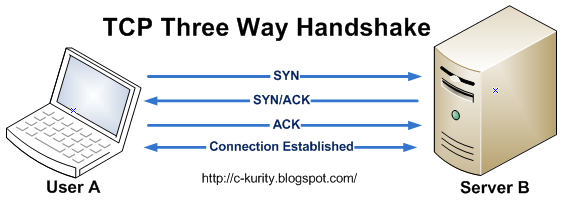
(Fig. Reference: <https://www.oryx-embedded.com/cyclone_tcp.html>)

**Different ports of TCP:**

* Source port: size: 16 bits, it’s the local TCP port through which the connection is made.
* Destination port: size: 16 bits, it’s the remote machines port to which the connection is mode.
* Sequence number: size: 32 bits, it’s the number which keeps the track of the order of the packets.
* Acknowledgement number: size: 32bits, the previous acknowledged sequence number of the packet.
* Header length: size: 4bits, the number of the words in header of 32bits.
* Reserved bits: Size: 6bits, it is kept for the future use.
* Flags: size: 6bits totally.
* URG: urgent field pointer
* ACK: this packet includes an acknowledgement or is the acknowledgement itself.
* PSH: push function
* RST: reset the connection or when required terminate it.
* SYN: synchronization packet or start connection.
* FIN: final packet, or to start the hang-up sequence.
* Window size: size: 16 bits, it has the acknowledgement field that the receiving side will accept it.
* Checksum: size:16 bit, it is a checksum of the header and data of the TCP.
* Urgent pointer: size:16 bits: an offset from the sequence number that points to the data following urgent data.

Three-way hand shake:

* TCP uses a 3 way handshake method to establish connection with another machine in a network
* For eg. If machine A wants to connect to machine B then the machine B has to be in passive open state.
* Machine A will send a synchronization message (SYN) to the machine B which has the sequence number.
* The machine B sends an acknowledgement message (ACK) and its synchronization message (SYN) to the machine A.
* The machine A sends the acknowledgement message (ACK) to the machine B and then the connection is established between the two machines.

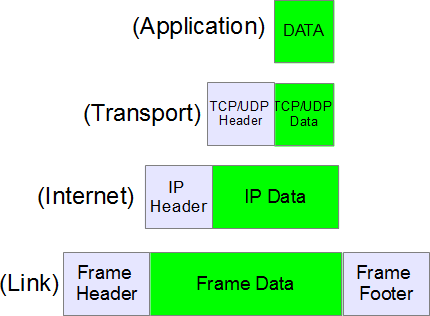


(Fig. Reference: http://c-kurity.blogspot.ca/2010/06/three-way-handshake-process-to.html)

**3. Internet protocol in detail:**

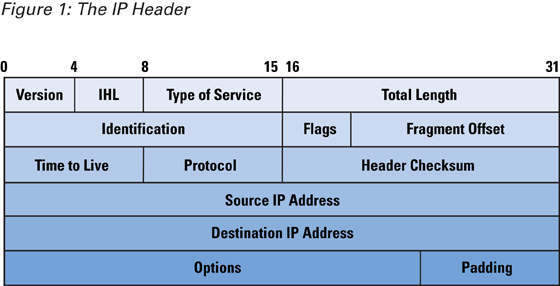
* Internet protocol is a part of tcp/ip model which allows the packets to be transferred from source machine to destination over the internet.
* Every machine in the network has its own unique mac and ip address.
* When a packet is transmitted from point A to point B the packet is appended with both the source and destination ip address.
* There Exists two versions of internet protocol i.e. IPv4 and IPv6. For the purpose of transmission of packets.
* Routing is also one of the major functions that the internet protocol performs apart from the addressing function.

**INTERNET PROTOCOL**



(Fig. Reference: https://www.thegeekstuff.com/2012/03/ip-protocol-header/)

* Frame header & Frame footer: the header and footer are appended in the data link layer of the ip protocol onto the frame data that has to be sent.
* Ip header: it contains the information about the destination and source ip addresses of the machines over the network and is appended to ip data on the internet layer of the protocol.



(Fig. Reference: <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html>)

IHL: gives the size of the header

Type of service: there are two types of services i.e. explicit congestion notification and differentiated services code point.

Total length: provides with the entire length of the packet.

Identification: useful for the identification of the group of fragments of the datagram uniquely.

Flags: Fragmentation option states.

Fragment offset: gives the position of the fragment.

Time to live: indicates the amount of time that the fragment can make hops.

Protocol: defines the protocol to be used for the data section in the datagram

Header Checksum: method used for the checking error.

Source IP address: gives the ip address of the source machine

Destination IP address: gives the ip address of the destination machine.

Options: padding is done in this field to ensure whether the header has 32 bit word.

* Payload/Data: it is the original message that has to be sent over the network and the headers allow the message to be sent in secure and ordered manner.
* TCP/UDP header : it is the header which is used to order the packets upon reception and check for error or drop in packet. It is appended onto the tcp/udp data in the transport layer.

IP addressing:

* The ip address is 32 bit in size
* The address is represented in dot decimal format.
* It is also divided into 5 classes as well

There are 5 types of class in ip addresses

Class A:

* There is a possibility of 127 networks
* The network number ranges from 1.0.0.0-126.0.0.0
* The address is used by multinational companies mostly.

Class B:

* There is a possibility of 16,348 networks.
* The network number ranges from 128.0.0.0-191.255.0.0
* It is used by educational institutes and the internet service provider.

Class C:

* Has a possibility of 2,097,152 networks
* The network number ranges from 192.0.0.0-233.255.255.0
* It is used by small versions.

Class D:

* The network number ranges from 224.0.0.0-239.255.255.255
* Data from the server is sent to multicast ip

Class E:

* The network number range from 240.0.0.0-247.255.255.255
* It is reserved for internet engineering task force.

**4. Different protocols used in different models:**

* UDP : the user datagram protocol is connectionless model, it does not guarantees the delivery of the packets and provides checksum.
* It is mostly used for video streaming and live gaming scenarios. where no handshaking protocol is followed.
* It is a part of TCP/IP model.
* ARP: the address resolution protocol is mainly used for finding the address of a machine in a network that Is it identifies the unique ip address of the computer in a network.
* There are main 4 messages that a ARP protocol uses i.e. ARP-request, ARP-reply, RARP- request & RARP- reply.
* SMTP: simple mail transfer protocol is used for sending and receiving emails through the network. It communicates with the server using the Tcp port number 25.
* The mail servers in the SMTP protocol often use the port 587 for out going emails.
* HTTP: Hypertext transfer protocol is application protocol.
* It uses various request methods to communicate such as GET,HEAD,POST,PUT,DELETE, TRACE, OPTIONS,CONNECT & PATCH.
* The HTTP protocol is a stateless protocol which enables the HTTP server to not store/retain the status of each user.
* PPP: Point to Point protocol, as the name suggests the protocol establishes the connection between two nodes. It connects two machines without the need of any networking device.
* Normally used as data link layer protocol for the connections on the synchronous and asynchronous circuits.
* Provides authentication, compression & encryption as well.