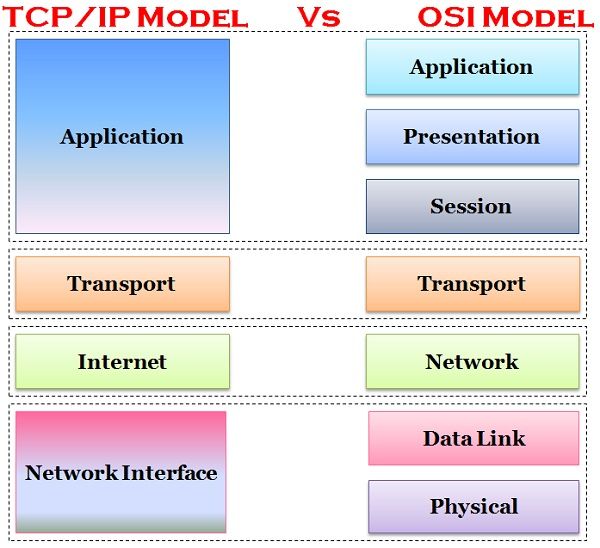
1. What are the differences between the OSI model and the TCP/IP model? (<https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html> )

Key Differences Between TCP/IP and OSI Model

* TCP/IP is a client-server model, i.e., when the client requests for service it is provided by the server. Whereas OSI is a conceptual model.
* TCP/IP is a standard protocol used for every network including the Internet, whereas OSI is not a protocol, but a reference model used for understanding and designing the system architecture.
* TCP/IP is a four-layered model, whereas, OSI has seven layers.
* TCP/IP follows Horizontal approach. On the other hand, the OSI Model supports Vertical approach.
* TCP/IP is Tangible, whereas OSI is not.
* TCP/IP follows top to bottom approach, whereas OSI Model follows a bottom-up approach.

1. How many layers do these two models have? (<https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html> )

TCP-IP: 4 layers OSI: 7 layers



1. What do the acronyms TCP and IP refer to? (<https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html> )

( <https://www.freecodecamp.org/news/what-is-tcp-ip-layers-and-protocols-explained/> )

*TCP (Transmission Control Protocol) /IP (Internet Protocol) was developed by the Department of Defence (DoD) project agency. Unlike OSI Model, it consists of four layers each having its own protocols. Internet Protocols are the set of rules defined for communication over the network.*

*TCP/IP is considered as the standard protocol model for networking. TCP handles data transmission and IP handles addresses. The TCP/IP protocol suite has a set of protocols that includes TCP, UDP, ARP, DNS, HTTP, ICMP, etc. It is a robust and flexible model. The TCP/IP model is mostly used for interconnecting computers over the internet.*

1. List the different layers of the TCP/IP model. (<https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html> )

*TCP/IP Model Layers*

*1.Network Interface Layer: This layer acts as an interface between hosts and transmission links and used for transmitting datagrams. It also specifies what operation must be performed by links like serial link and classic ethernet to fulfil the requirements of the connectionless internet layer.*

*2.Internet Layer: The purpose of this layer is to transmit an independent packet into any network which travels to the destination (might be residing in a different network). It includes the IP (Internet Protocol), ICMP (Internet Control Message Protocol) and ARP (Address Resolution Protocol) as the standard packet format for the layer.*

*3.Transport Layer: It enables a fault-free end-to-end delivery of the data between the source and destination hosts in the form of datagrams. The protocols defined by this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).*

*4.Application Layer: This layer permits users to access the services of global or private internet. The various protocols described in this layer are virtual terminal (TELNET), electronic mail (SMTP) and file transfer (FTP). Some additional protocols like DNS (Domain Name System), HTTP (Hypertext Transfer Protocol) and RTP (Real-time Transport Protocol). The working of this layer is a combination of application, presentation, and session layer of the OSI model.*

1. Give some examples of protocols and indicate which one of TCP/IP model layer they refer to.

*SMTP:*

*It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. The Port number for SMTP is 25.*

1. Explain how a connection gets established, in other words, explain the "3-way handshake" process? (<https://www.tutorialspoint.com/tcp-3-way-handshake-process> )

3 -Way Handshake Closing Connection Process

To close a 3-way handshake connection,

First, the client requests the server to terminate the established connection by sending FIN.

After receiving the client request, the server sends back the FIN and ACK request to the client.

After receiving the FIN + ACK from the server, the client confirms by sending an ACK to the server.

1. Explain how a connection is terminated, in other words, explain the "4-way disconnect" process? (<https://www.geeksforgeeks.org/tcp-connection-termination/> )

TCP supports two types of connection releases like most connection-oriented transport protocols:

Graceful connection release –

In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.

Abrupt connection release –

In an Abrupt connection release, either one TCP entity is forced to close the connection or one user closes both directions of data transfer.

How mechanism works in TCP:

Step 1 (FIN From Client) –

Suppose that the client application decides it wants to close the connection. (Note that the server could also choose to close the connection). This causes the client to send a TCP segment with the FIN bit set to 1 to the server and to enter the FIN\_WAIT\_1 state. While in the FIN\_WAIT\_1 state, the client waits for a TCP segment from the server with an acknowledgment (ACK).

Step 2 (ACK From Server) –

When the Server received the FIN bit segment from Sender (Client), Server Immediately sends acknowledgement (ACK) segment to the Sender (Client).

Step 3 (Client waiting) –

While in the FIN\_WAIT\_1 state, the client waits for a TCP segment from the server with an acknowledgment. When it receives this segment, the client enters the FIN\_WAIT\_2 state. While in the FIN\_WAIT\_2 state, the client waits for another segment from the server with the FIN bit set to 1.

Step 4 (FIN from Server) –

The server sends the FIN bit segment to the Sender (Client) after some time when the Server sends the ACK segment (because of some closing process in the Server).

Step 5 (ACK from Client) –

When the Client receives the FIN bit segment from the Server, the client acknowledges the server’s segment and enters the TIME\_WAIT state. The TIME\_WAIT state lets the client resend the final acknowledgment in case the ACK is lost. The time spent by clients in the TIME\_WAIT state depends on their implementation, but their typical values are 30 seconds, 1 minute, and 2 minutes. After the wait, the connection formally closes and all resources on the client-side (including port numbers and buffer data) are released.

1. Explain what are the "*sequence number*" and "*acknowledgment number*" in TCP. (<https://www.ibm.com/docs/en/zos-basic-skills?topic=layer-transmission-control-protocol-tcp> )

*At offset 32 into the TCP header is the sequence number. The sequence number is a counter used to keep track of every byte sent outward by a host. If a TCP packet contains 1400 bytes of data, then the sequence number will be increased by 1400 after the packet is transmitted.*

*At offset 64 is the acknowledgement number. This number is a counter to keep track of every byte that has been received. If 1000 bytes are received by a host, it increases the acknowledgement number by 1000 when it sends out a packet in response.*

*As mentioned, receiving data from a remote host causes the acknowledgement number at the local host to be increased by the number of bytes received. When the local host sends out its next packet, it will send this updated acknowledgement number, and it will also turn on the ACK flag (offset 107) to indicate to the other end that it is acknowledging the receipt of data. This is the nearest thing to a signature that TCP can do. The result is that TCP can ensure reliable delivery of data.*

1. What is the fundamental difference between TCP and UDP? (<https://www.geeksforgeeks.org/differences-between-tcp-and-udp/> )( <https://www.freecodecamp.org/news/tcp-vs-udp/> )

*TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.*

*UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.*

1. What are TCP ports? How many of them are they? What are the three main categories of TCP Ports (*with their associated range*)? (<https://www.cbtnuggets.com/blog/technology/networking/what-is-a-tcp-port-and-why-they-are-important> ) (<https://www.geeksforgeeks.org/tcp-ip-ports-and-its-applications/?ref=gcse> )

*TCP ports allow for standardized communication between devices. One device can receive information for many different processes and services, and which port the information flows on helps to keep it organized.*

*A TCP port is a 16-bit, unsigned value, so there's a finite number of TCP ports available in the world. Specifically, there are 65,535 available TCP ports.* *That said, the first 1,024 TCP ports are called well-known port numbers, and they're agreed upon among technology vendors.*

*Top firms like Google or MSN use \*well-known ports\* (0 to 10231) for their services; Certain specific functions are \*assigned registered ports\*(1024 to 49151) when requested; There are also \*private or dynamic ports\*(49152 to 65536) which can be used by anyone who wishes for private servers and temporary purposes.*

1. Provide three examples of well-known port numbers and tell which Application layer protocol they refer to. (<https://www.geeksforgeeks.org/protocols-application-layer/> )

TELNET:

Telnet stands for the TELetype NETwork. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the internet. It is used for the initial setup of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

FTP:

FTP stands for file transfer protocol. It is the protocol that lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol, but it is also a program, promotes sharing of files via remote computers with reliable and efficient data transfer. The Port number for FTP is 20 for data and 21 for control.

NFS:

It stands for a network file system. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. The Port number for NFS is 2049.

1. Explain the concept of **TCP packets** and how they are built over the layer flow.

TCP Packet contains the following fields:

Source Port and Destination Port fields (16 bits each) - Source and Destination port number

Sequence Number field (32 bits) - sequence number of the first data byte or data octet

Acknowledgment Number field (32 bits)

Data Offset field (variable length) - indicates the starting point of data

Reserved field (6 bits) - kept for future use and must be zero.

Flags field (6 bits - URG, ACK, PSH, RST, SYN, FIN) - signifies different flags

Window field (16 bits) - mention window's size of the sender

Checksum field (16 bits) - to ensure the integrity

Urgent pointer field (16 bits) - point to urgent data type

Options field (variable length) - multiple options

Data field (variable length)