Q. What is open system?

A. A system which is connected to the network and ready for communication is called open system.

A ------ (Internet)

A is open system as it is connected to the network.

Q. What is closed system?

A. A system which is not connected to the network and can’t communicate with others is called closed system.

A (internet)

Here A is called closed system as it is not connected to the network.

Q. What is computer network?

A. A computer network is a digital telecommunications network which allows network to share resources. In computer network, computing devices exchange data among them using connections (data links) between nodes. These data links are established over cable media such as wires cable, wireless media such as WIFI.

A computer network is a set of computers connected together for the purpose of sharing resources. The most common resources shared today is connection to the internet. Other shared resources can be printer or file server. The internet itself can be considered a computer network.

Q. What is OSI model?

A. OSI Model stands for Open Systems Interconnection. Actually it is a reference model that specifies standards for communication protocol and also the functionalities of each layer.

There are 7 layers of OSI Model.

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

Q. What is protocol?

A. Protocol is just nothing but a set of rules or algorithms which defines the way how two entities can communicate with each other across the network. There exist different protocols in each layer of OSI model. Some protocols are – TCP/IP, UDP, ARP, DHCP, FTP and so on.

Q. What is socket?

A. The unique combination of IP address and port number together are termed as socket.

Q. What is DNS server?

A. DNS is basically a server which translate web addresses into corresponding IP addresses. Actually every server has an IP address. But we don’t need to remember this address. We just need to remember the web address. And DNS translate this web address into corresponding IP address.

Q. What is ARP?

A. ARP stands for Address Resolution Protocol.

ARP is used to convert the IP address into its corresponding physical address (MAC address).

ARP is used by the data link layer to identify the MAC address of the Receiver’s machine.

Q. What is RARP?

A. As the name suggest, it is reverse of ARP. It is used to convert the machine’s mac address into corresponding IP address.

Q. What is TCP?

A. TCP stands for Transmission Control Protocol. As the name indicates, there are two layers in TCP/IP. The top layer, TCP, is responsible to take large amount of data, compiles them into packets and then sending them on their way to be received by a fellow TCP layer, which turns the packets into information/data.

Q. What is IP?

A. IP stands for internet protocol. It is the bottom layer of TCP/IP layer. The data which are sent by TCP need to be delivered into destination. IP contains the information about the destination. If we think IP in term of map, the IP layer serves as the packet GPS to find the correct location. If we think about a car driving on a highway, each packets passes through a gateway computer (sings on the map), which serve to forward the packets to their right destination.

Q. What is the difference between TCP and UDP?

A.

TCP:

It is connection oriented – once a connection is established, data can be sent bidirectional.

When you load a web page, your computer sends TCP packets to the web server’s address, asking it to send the web page to you. The web server responds by sending a stream of TCP packets, which your web browser stitches together to form the web page and display it to you.

TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender doesn’t get a correct response, it will resend the packets to ensure the recipient received them.

UDP:

UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

Let’s say you’re watching a live video stream. Live streams are often broadcast using UDP instead of TCP. The server just sends a constant stream of UDP packets to computers watching. If you lose your connection for a few seconds, the video will freeze for a moment and then jump to the current bit of the broadcast, skipping the bits you missed. If you experience minor packet-loss, the video or audio may be distorted for a moment as the video continues to play without the missing data.

When using UDP, packets are just sent to the recipient. The sender won’t wait to make sure the recipient received the packet — it will just continue sending the next packets. If you’re the recipient and you miss some UDP packets, too bad — you can’t ask for those packets again. There’s no guarantee you’re getting all the packets and there’s no way to ask for a packet again if you miss it.

Q. How TCP/IP works?

A. <https://www.youtube.com/watch?v=OXUzJb6AeGk&t=3s>