Basic Concepts of Computer Networking

A computer network is a group of two or more interconnected computer systems. You can establish a network connection using either *cable* or *wireless media*.

Every network involves hardware and software that connects computers and tools

Modem

Router

Firewall

Switch

**Describe Hub, Switch and Router**

1. **Router**: Behind the modem is a router. What the router does is to allow you *separate different networks*, for instance, you can separate your network by departments, or from other users in the building from your network, to avoid hacking.

**Users / Department** **Routers Internet**

Internet

A

B

C

Here, users/departments (no matter how many computers they have on their network) can go through an assigned router to the internet, they cannot go through other routers assigned to other groups.

1. **Switch**: underneath the firewall is the switch, it splits the internet signal. All Computers, Printers and other hardware devices within your group connect through the switch, the switch will then either allow these devices on your network to communicate with each other, as well as with other networks. Switches help you share resources and reduce organizations cost.
2. **Hub**: Is a networking device that allows you to connect multiple **PC’s** to a single network. Whenever a computer requests any information from a network, it sends the request to the hub through a cable. The hub will receive the request.

**Hubs** operate as Layer 1 devices per the **OSI** model

**What is the OSI Model?**

**Open System Interconnection (OSI) Model:** Is a reference model which allows you to specify standard for communication.

**OSI** model describes 7 layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s.

Themodern internet is not based on OSI but on the Simpler **TCP/IP** Model, However, the OSI 7-layer model is still widely used as it helps visualise and communicate how networks operate and helps isolate and troubleshoot networking problems

Server

Server

**10.0.0.2 10.0.0.3  
B C port 80**

Router

**10.0.0.1  
 A**

Phone

Server

**10.0.0.5 10.0.0.4**

**D F**

**10.0.0.3** is a **web Server** having a web application and 10.0.0.5 want to visit the web page, so client phone (10.0.0.5) goes on the internet and types: <http://10.0.0.3:80>   
This **GET** request, goes through **OSI 7 layers**, and return the right data (10.0.0.3). see below how this works.

**OSI 7 Layer Model**

7. **Application Layer**: Human – computer interaction layer applications such as web browsers and email clients. It provides protocols (*Hypertext Transfer Protocol* (***HTTP)****, File Transfer Protocol (****FTP****), Post Office Protocol (****POP****), Simple Mail Transfer Protocol (****SMTP****) and Domain Name System (****DNS****)*) that allow software to send and receive information and present meaningful data to users.

6. **Presentation Layer**: The presentation Layer prepares data for the application layer. It ensures that data is in a usable format and is where data encryption occurs. The presentation Layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

5. **Session Layer**: Sessions layer creates communication channels called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them then communication ends.

4. **Transport Layer**: The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end.

3. **Network Layer**: Network layer has two main functions:

1. breaking up segments into network packets and reassembling the packets on the receiving ends
2. b. routing packets by discovering the best path across a physical network.

2. **Data link Layer**: Data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination.

1. **Physical Layer**: Physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices and is responsible for transmission of raw data, which is simply a series of 0s and 1s while taking care of bit rate control

**What do you mean by TCP/IP?**

**Transmission** **Control** **Protocol**/ **Internet Protocol** (**TCP/IP**): Is a set of standardized rules that allow computers to communicate on the network.

Just like people, it’s important for computers to have a common way to communicate with each other. Today, most computers do this through **TCP/IP**.

**IP** is the part that obtains address to which data is sent.

**TCP** is responsible for data delivery once the IP Address has been found.

By itself, an individual computer can perform any number of jobs. But, computers real power shines when they communicate with each other. But like passing a letter or package from hand to hand, the two computers need to know ahead of time, how they are expected to communicate:

* How do they start the conversation?
* Whose turn is it to communicate?
* How does each computer know its message was transmitted correctly?
* How do they end the conversation?

Computers do this through protocols. A protocol is an agreed-upon set of rules.

**TCP/IP model**

This model consists of 5 layers

1. **Application** **Layer**: to allow access to network resources
2. **Transport** **Layer**: to provide reliable process to process message delivery and error delivery
3. **Internet** **Layer**: to move packets from source to destination, to provide internetworking
4. **Network** **layer**: responsible for the transmission between two devices on the same network

**What do you mean by HTTP, TCP and UDP?**

**Hypertext Transfer Protocol (HTTP):** You've undoubtedly seen **HTTP** at the front of URLs nearly every time one shows up in your web browser.

When you type a URL into your web browser, you are sending an HTTP request to a web server. That server will then respond, again using the formatting of HTTP.

HTTP contains specific instructions on how to read and process data once it arrives. Before data is sent from one node on the Internet to another, it gets wrapped in information detailing the nature of the request being sent, or the response to said request.

The two most common examples of HTTP requests are: 1. "**POST**," denoting that this contains data to be pushed to the server 2. "**GET**," asking that a resource from the server be fetched.

**HTTP** is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server protocol, which means requests are initiated by the recipient, usually the Web browser.

**Transmission** **Control** **Protocol (TCP)**: It is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

A TCP connection is established with the help of 3-way-handshake. Once a connection is established, data transfer begins, and when the transmission process is finished, the connection is terminated by the closing of an established virtual circuit.

**User Datagram Protocol (UDP)**: is a datagram-oriented protocol. It is used for broadcast and multicast type of network transmission. (A datagram is a transfer unit associated with a packet-switched network.)

1. UDP is faster, simpler and more efficient than TCP.
2. 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 type of network transmission.
3. UDP is lightweight. And support broadcasting

**What is firewall?**

**Firewall**: Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. That is, firewall prevents internet traffic you don’t want into your network; it protects your network from hackers.

Firewalls are built into Modems, Routers, etc. If you turn on firewall either on Modems or Routers, it will block internet services for the entire network. So, if you don’t want visitors from internet to access your website for any reason, then block port 80 either on the modem or router.

**Explain DNS**

**Domain Name System (DNS)**: Enhance website performance and reduce bandwidth cost with a CDN designed for developers

So, lets assume that you want to visit <https://emtosmarket.com>

Once the request reaches the correct root server, it goes to the top-level domain( TLD) and then to the second-level domain, security has now been added.

**Define Latency**

Latency: from a general point of view is the time delay between the cause and the effect of some physical change in the system being observed. It is known within gaming circle as “lag”.

**Define Caching**

Cache: is a component – hardware or software that stores data so that future requests for that data can be served faster.

**Explain Wireless Access Point**

**Wireless Access Point (WAP)**: will allow wireless Computers, Printers, mobile phones, and other wireless devices to connect and communicate with devices on the network without cables.

**WAP** plugs into a hub or switch and is the device that joins the unwired network to the wired network.

**WAP** and **Routers Wireless Access Point** are **radio transmitters** and represent a node just like a computer, on a local area network (LAN)

From **JoyceMimi**