॥ सिद्धिः भूषयते विद्याम् ॥

avantika
UNIVERSITY

Discipline

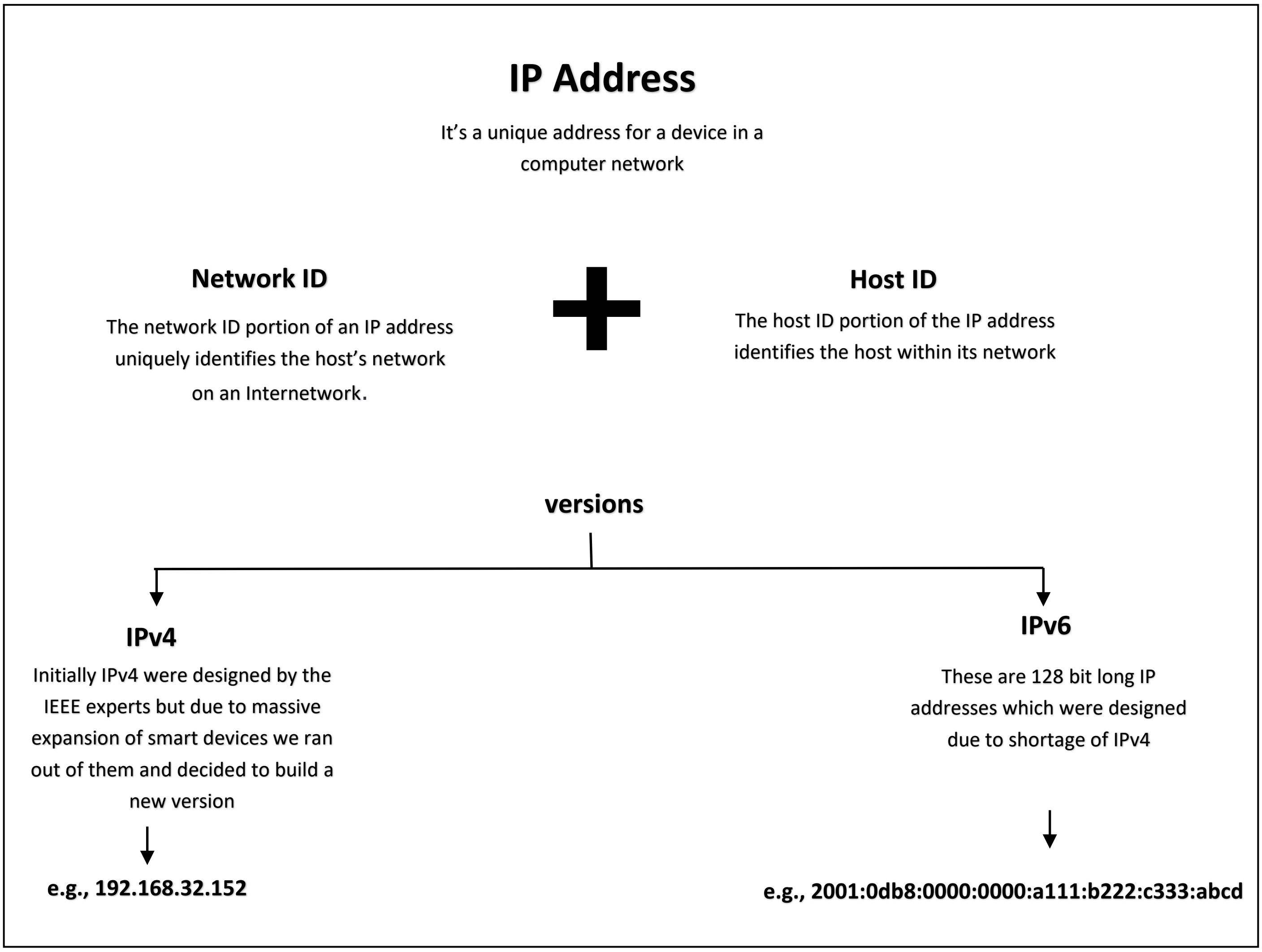
IPv4 Addressing and Data Flow with OSI Model

CS5001

Assignment 1

Sheikh Muhammed Tadeeb (AU19B1014)

❖ Brief:



IP Address

It's a unique address for a device in a computer network

Network ID

The network ID portion of an IP address uniquely identifies the host's network on an Internetwork.

Host ID

The host ID portion of the IP address identifies the host within its network

versions

IPv4

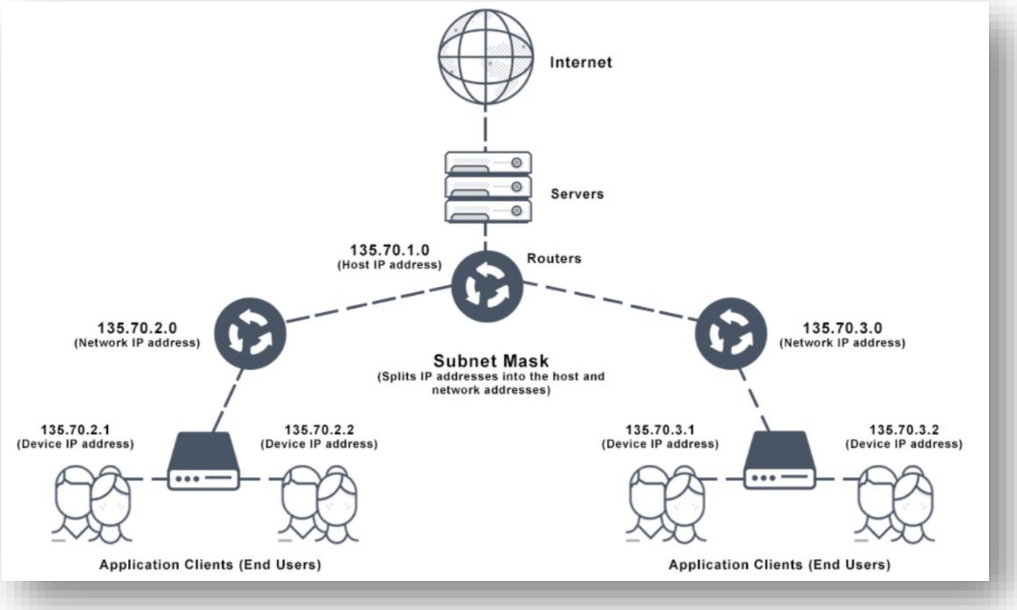
Initially IPv4 were designed by the IEEE experts but due to massive expansion of smart devices we ran out of them and decided to build a new version

e.g., 192.168.32.152

IPv6

These are 128 bit long IP addresses which were designed due to shortage of IPv4

e.g., 2001:0db8:0000:0000:a111:b222:c333:abcd



❖ IPv4 addressing and subnetting with examples:

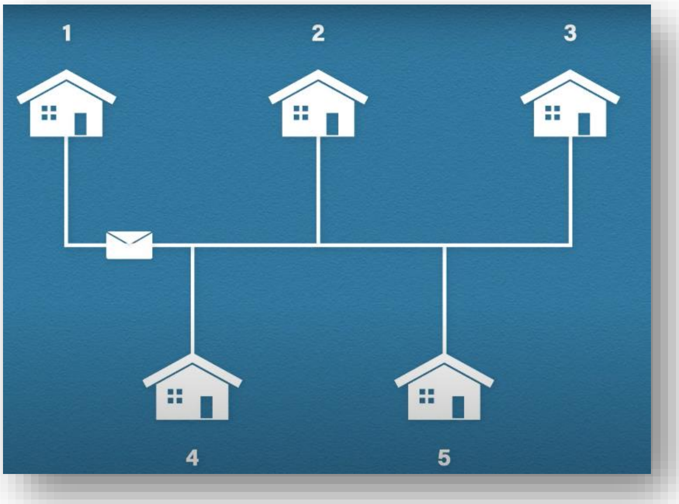
Q1) What is IPv4?

Ans: -

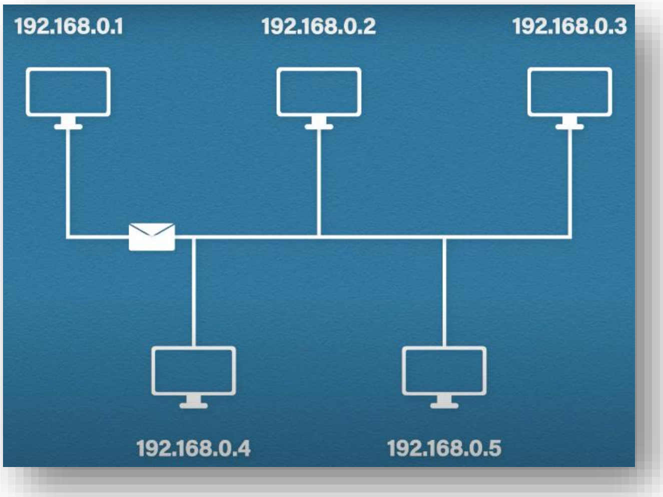
An IPv4 address is the 1st version of IP address used to identify each device uniquely connected in a computer network.

- *Example:*

The most common analogy for an IP address is the postal service. For the postal service to work, every house needs to have its own, unique address. If you need to send a letter, you'll need to write the destination address on the envelope. That way, when you send your letter, the postman knows exactly where to deliver it. Computers work in the same way. Each computer in a network needs to have a unique address, called an IP address. and when sending data to a computer, just like letters, we need to add the destination address. We also need to include a return address, so they know where to reply.



Computers work in the same way. Each computer in a network needs to have a unique address, called an IP address. and when sending data to a computer, just like letters, we need to add the destination address. We also need to include a return address, so they know where to reply.



Q2) What is IPV4 Addressing and Subnetting?

Ans: -

- ✓ *IPv4 Addressing:*

  An IPv4 address is 32-bits in length. A 32-bit IP address uniquely identifies a single device on an IP network. The 32 binary bits are divided into the host and network sections by the subnet mask but they are also broken into four 8-bit octets.

  Because binary is challenging, we convert each octet so they are expressed in dot decimal. This results in the characteristic dotted decimal format for IP addresses—for example, 172.16.254.1. The range of values in decimal is 0 to 255 because that represents 00000000 to 11111111 in binary.

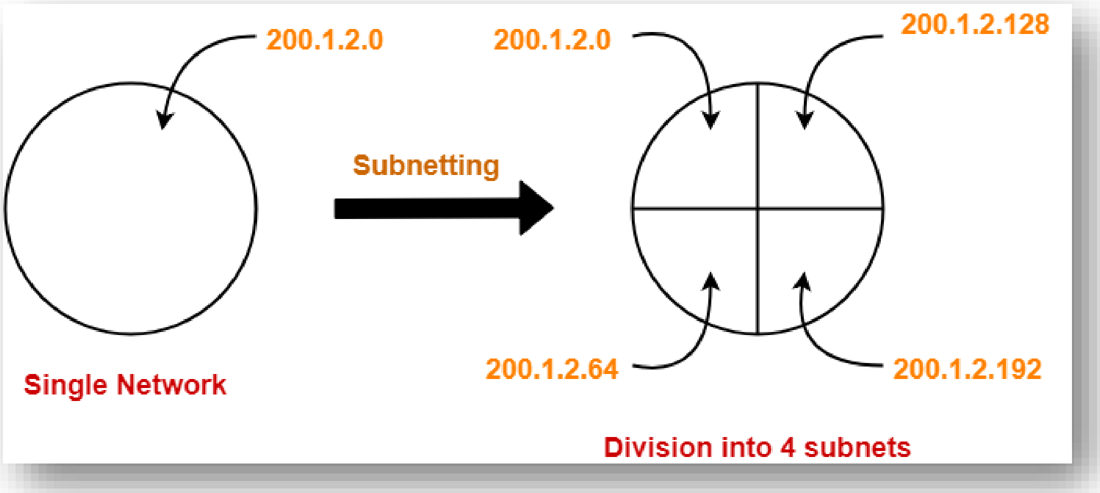
- ✓ *Subnet Mask:*

  A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses.

  The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address. Neither can be assigned to hosts, as they are reserved for these special purposes.

  When organizations need additional sub networking, subnetting divides the host element of the IP address further into a subnet. The goal of subnet masks is simply to enable the subnetting process. The phrase “mask” is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.

  Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.



- *Example:*

In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

204.17.5.0 - 11001100.00010001.00000101.00000000

255.255.255.224 - 11111111.11111111.11111111.11100000

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of all zeros or all ones are not allowed (it is very important to remember this). So, with this in mind, these subnets have been created.

Subnet Address	204.17.5.0	204.17.5.32	204.17.5.64	204.17.5.96
Host per Subnet	1 to 30 hosts	33 to 62 hosts	65 to 94 hosts	97 to 126 hosts

Subnet Address	204.17.5.128	204.17.5.160	204.17.5.192	204.17.5.224
Host per Subnet	129 to 158 hosts	161 to 190 hosts	193 to 222 hosts	225 to 254 hosts

Note: New Subnet = 255.255.255.224, CIDR = /27

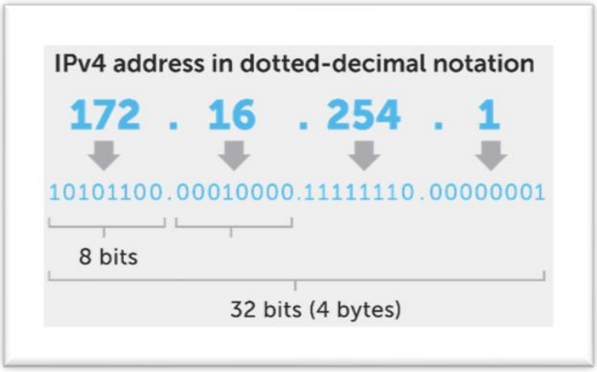
Q3) How IPv4 addresses look and its class?

Ans: -

✓ *IP Address look:*

An IPv4 address is written in decimal digits, divided into four 8-bit fields that are separated by periods or dots. Each 8-bit field represents a byte of the IPv4 address. This form of representing the bytes of an IPv4 address is often referred to as the dotted-decimal format. E.g. 172.16.50.56.

The following figure shows the component parts of an IPv4 address: -



IPv4 still routes most of today’s internet traffic. A 32-bit address space limits the number of unique hosts to 232, which is nearly 4.3 billion IPv4 addresses for the world to use (4,294,967,296, to be exact).

➢ But due to massive explosion of internet and coming up of so many smart devices we ran out of IPv4 address space.

✓ *IPv4 Classes:*

IP Address classes concept was decided to split all of the available addresses into groups called classes. The idea was to make address allocation scalable. We have class A, class B, and class C. Class D and E are reserved.

➢ *Example:*

Class A addresses would be used by large organisations (e.g., IBM) which had lots of computers (nodes) and so would require a large number of node addresses.

Class B network addresses were for medium sized organisations and used 2 bytes (16 bits) for the Network and 2 bytes for node addresses.

Class C network addresses were for small organisations and used 3bytes for the Network and 1 byte for node addresses.

Class	Networking size	Start address	End address
Class A	Very Large	0.0.0.0	127.255.255.255
Class B	Large	128.0.0.0	191.255.255.255
Class C	Small	192.0.0.0	223.255.255.255
Class D (multicast)	Special Purpose	224.0.0.0	239.255.255.255
Class E (reserved)	Special Purpose	240.0.0.0	255.255.255.255

❖ Data flow with reference to OSI Model:

Q1) DNS resolution with URL request and response on the Browser

Ans: -

- **Layer Seven Application Layer:**

Network Process to Application

As the top layer of the OSI model, application layer is the layer that we (users) interact directly with. Application-layer functions typically include identifying communication partners (where to transmit the data), determining resource availability (is the destination available), and synchronizing communication (send the data).

In our URL-clicking case, the application is the browser. The browser selects which web server it is sending data to, contacts the server and send the request. When a response is returned, the browser displays the desired content on the web page.

- **Layer Six Presentation Layer:**

  Data Encapsulation and Encryption

  Sometimes called the syntax layer, the presentation layer provides a mapping of different syntaxes to a unified data representation. It translates between application and network format, and transform data into the format that the application accepts. Other functions of this layer include data encryption and data compression.

  Usually, a web page contains different formats of data: HTML files, JavaScript files, image files, etc. In the presentation layer these files are transformed by Abstract Syntax Notation One into XML format to be displayed on the browser.

- **Layer five Session layer:**

  Interhost Communication

  The session layer controls the connections between two computers by establishing, managing, and terminating sessions. Whenever we visit any website, our computer is creating a session with the web server. In applications that uses Remote Procedure Calls, the session layer is commonly implemented explicitly.

  When we request a web page, the web browser opens a TCP/UDP connection (explained below) to the web server. The web server sends back the web page and closes the connection. Each TCP/UDP connection is a session.

- **Layer four Transport Layer:**

  End-to-End Communication and Reliability

  This layer provides host-to-host communication services for applications. That is, it is responsible for delivering data to the appropriate application process on the host computers. It also coordinates the data transfer process: how much data to send, at what rate, with what behaviours, and so on. Two important protocols for this layer are the TCP (Transmission Control Protocol) and the UDP (User Datagram Protocol). They each describes a very different approach to this transfer process.

- *Transmission Control Protocol (TCP):*

We (well if you don't, I) often hear the term "TCP/IP" in the context of computer networking. TCP is the original implementation which provides a delivery of data between hosts, or end systems, running via an IP network. Later, the term "TCP/IP" commonly refers to the entire network model (like the OSI model that we are walking through). We will go into that in the next post. Now, some characteristics of TCP:

1. It is a connection-oriented protocol. It requires handshaking (that is, acknowledging each side is there and ready) to set up communications.
2. It is reliable. TCP makes sure of the right order, and the integrity of data. It manages message acknowledgment, retransmission and timeout. If a message is lost along the way, the server will re-request the lost parts.
3. It is heavyweight. TCP's handshaking mechanism requires three packets to set up a socket connection, before any user data can be sent. Also, it has a fat overhead so that it could provide the functionalities mentioned above.
4. A brief TCP connection walk-through: new socket → bind → listen (handshakes begin) → (connection established) → accept

- *User Datagram Protocol (UDP):*

Like TCP, UDP is a protocol that instructs how the data-transporting process in the Transport layer should go about. Yet UDP's principle is quite different from TCP. TCP gets things done in a slower but throughout manner. UDP, on the other hand, values speed over reliability.

Some characteristics:

1. UDP uses a simple connectionless communication model. It has no hand-shaking dialogues, so a message can be sent from one end point to another without prior arrangement.
2. UDP does not keep track of lost packets, nor does it care about packet arrival order.
3. As a result, UDP requires less computer resources.

4. UDP is suitable for purposes where error checking and correction are either not necessary or are performed in the application, like streaming media applications and real-time applications.

Since it is transaction-oriented, UDP is suitable for simple query-response protocols such as the Domain Name System (where queries must be fast and only consist of a single request followed by a single reply packet.

It provides datagrams, basic transfer units associated with a packet-switch network, suitable for modelling other protocols such as IP tunnelling or Remote Procedure Call.

Q2) Data Packet flow from Host A (Sender) and Host B (Receiver) on the LAN?

Ans: -

- **Layer Three Network layer:**

  Path Determination and Logical Addressing

  This is the layer responsible for transferring variable-length network packets from a source to a destination, possibly through several proxies (networks). The router here plays an important part. It connects networks formed by switches. An important protocol for this layer is Internet Protocol (IP).

  - *IP: Internet Protocol:*

    An IP is a piece of software that operates at the Network Layer of the OSI model. It provides unique addresses (IP addresses), connectionless communication, routing, and unicast/broadcast/multicast.

    The IP address is for anything connected to an internet. These addresses can change, but they are guaranteed to be unique. For example, “104.27.187.82” would be a valid IP address for website jennycodes.me.

  - *Router/Gateway:*

    A router/gateway is a specialized host responsible for forwarding packets between networks. The reason why it exists is that many networks are partitioned into subnetworks and connect to other networks for wide-area communication.

- *Sending a packet to the router:*

  If we know both the IP address and MAC address (explained below) of our destination, we can send the data. In the case that the source and destination are not from the same IP domain, the source will be sending the data to the router first for transmission.

- **Layer Two Data Link layer:**

  Physical Addressing

  At the layer, data are decoded into frames of bits. It manages and handles errors in the physical layer, flow control and frame synchronization. Data link layer has two sub-layers: the Medium Access Control (MAC) layer and the Logical Link Control (LLC) layer. The implementation widely adopted now is a network switch.

  - MAC (Medium Access Control):

    This sub-layer controls how the computer hardware gains access to the data and permission to transmit them. A MAC address (Media Access Control address) is a unique identifier for a device in communications within a network segment. It is used as a network address for technologies including Wi-Fi, Bluetooth and Ethernet.

    MAC address is assigned by the manufacturer of network interface cards, so they are sometimes referred to as burned-in address. A MAC address looks like this: ‘3A-34–52-C4–69-B8’.

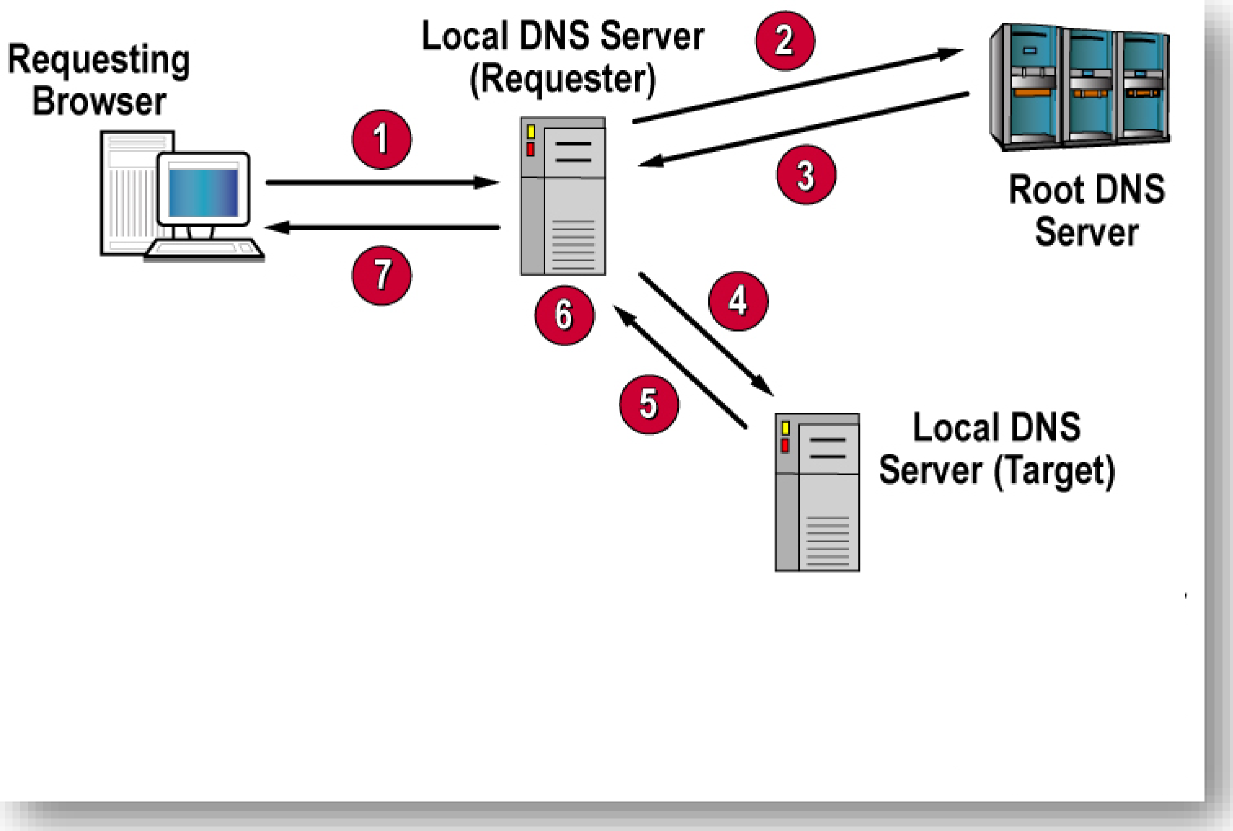
  - Network Switch

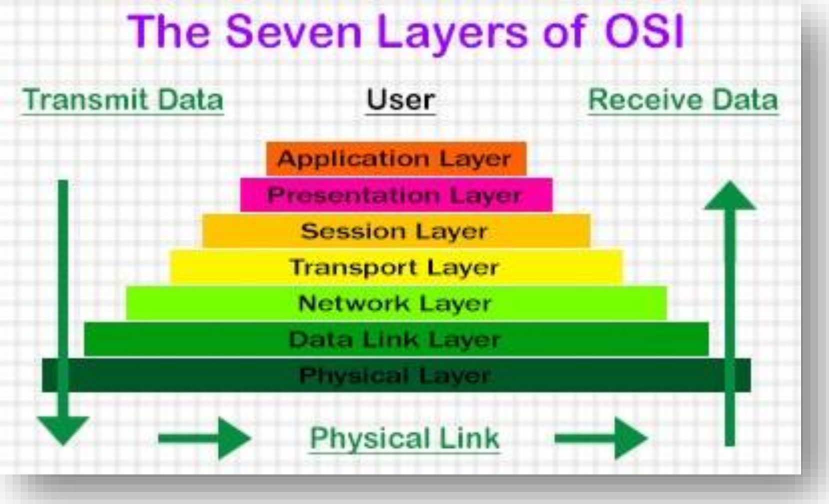
    A switch is a computer networking device which connects devices on a network. It uses hardware addresses (physical addresses or MAC Addresses) to process and forward data in the data link layer. Also, it offers port-to-port support–data are only sent between concerning devices as well as buffering service.

- **Layer One Physical layer:**

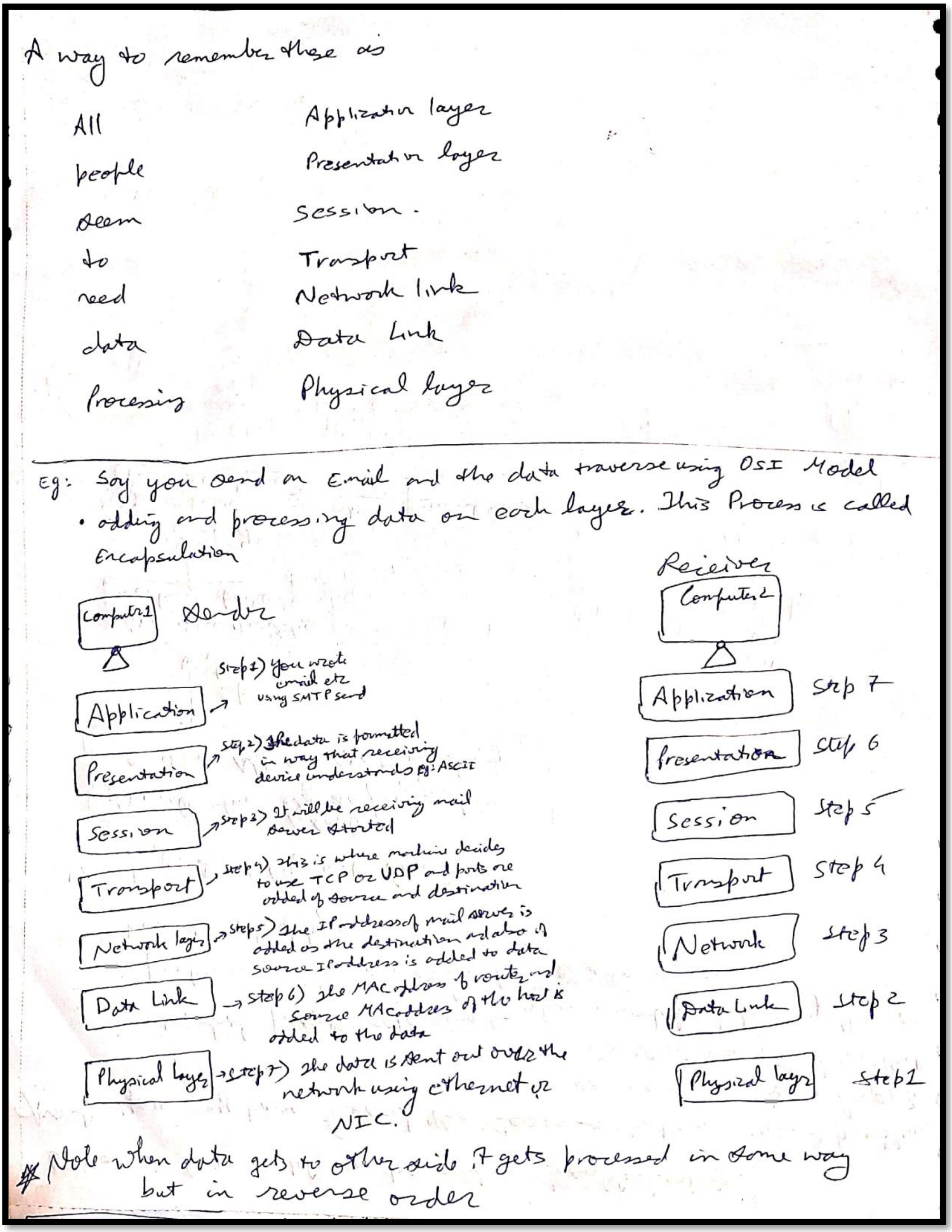
Media, Signal and Binary Transmission

The physical layer is where the raw data are transported in the form of bits–0 and 1–across the network (i.e., where the magic happens). The form can be either electrical, mechanical or radio waves.





❖ Paper Work:



A way to remember these as

All	Application layer
people	Presentation layer
seem	Session.
to	Transport
need	Network link
data	Data Link
Processing	Physical layer

Eg: Say you send an Email and the data traverse using OSI Model

• adding and processing data on each layer. This Process is called Encapsulation

Computer1 Sender

Application → step1) You wrote email etc using SMTP send

Presentation → step2) The data is formatted in way that receiving device understands Eg: ASCII

Session → step3) It will be receiving mail server started

Transport → step4) this is where machine decides to use TCP or UDP and ports are added of source and destination

Network layer → step5) the IP address of mail server is added as the destination and also it source IP address is added to data

Data Link → step6) the MAC address of router and source MAC address of the host is added to the data

Physical layer → step7) the data is sent out over the network using ethernet or NIC.

Receiver

Computer2

Application Step 7

Presentation Step 6

Session Step 5

Transport Step 4

Network Step 3

Data Link Step 2

Physical layer Step1

* Note when data gets to other side it gets processed in same way but in reverse order