Network Basics

by Durgesh Thakare

Network

A network is a collection of devices that are interconnected and can communicate with each other. These devices can include computers, servers, routers, switches, and other network equipment. Networks can be local, connecting devices within a small area like a home or office, or they can be wide, connecting devices across multiple locations or even across the globe.

or

It is a connection of devices connected together with peripheral devices to share information is known as a network

Packet

- Packets are envelopes of information used to transmit data over a network.
- They break data into smaller pieces to transmit efficiently.

Network Interface

- A network interface is a point of connection, like a Wi-Fi card or an Ethernet cable, that allows devices to connect to a network.

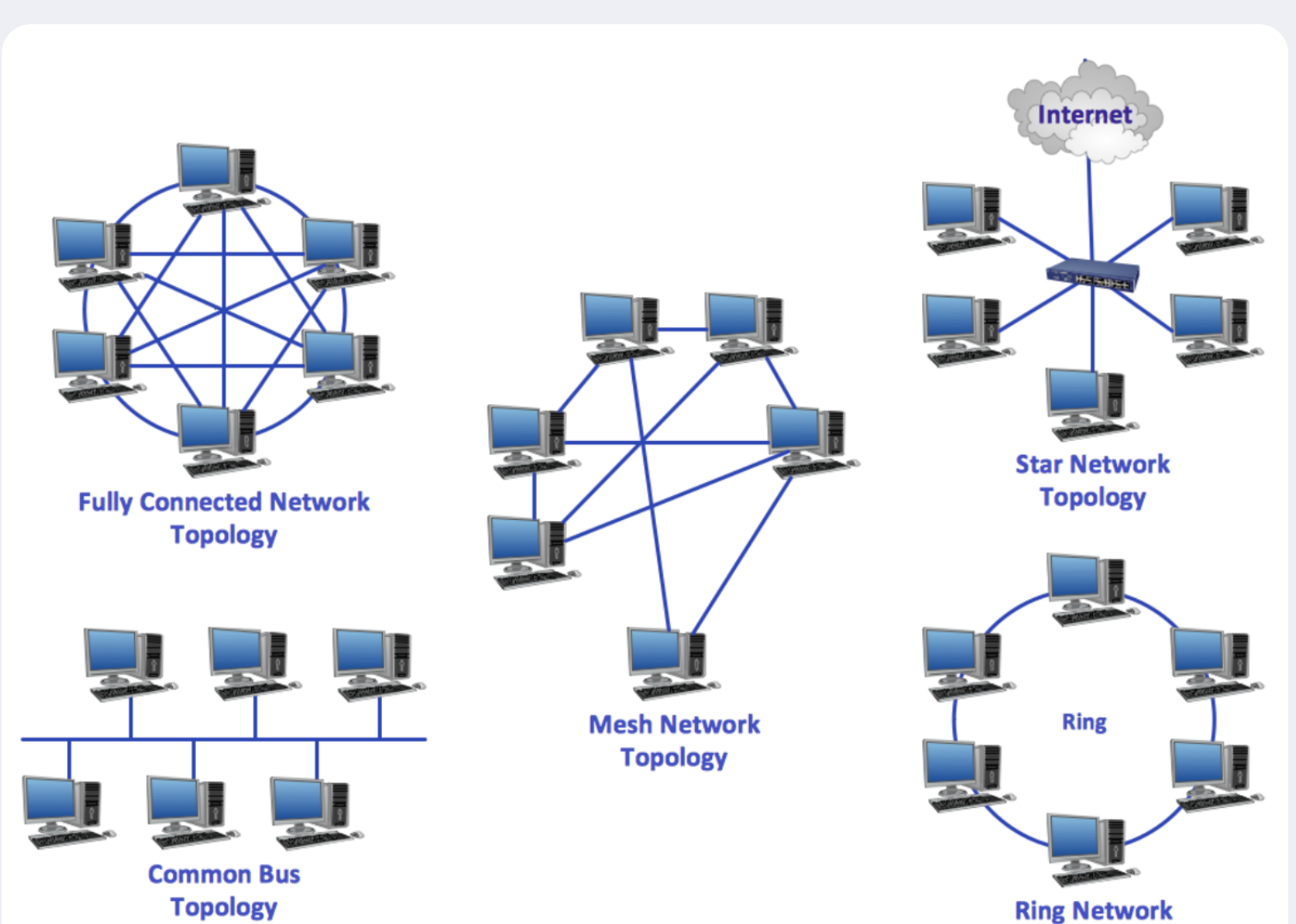
Types of Networks

- LAN (Local Area Network): Covers a small area like a home, office, or campus.
- WAN (Wide Area Network): Spans larger geographical areas, often connecting LANs.
- MAN (Metropolitan Area Network): Covers a city or a metropolitan area.
- PAN (Personal Area Network): A small network typically for personal devices.
- SAN (Storage Area Network): Used for high-speed data storage.

Network Topologies

- Topologies define how devices or nodes are connected in a network.

1. Bus Topology: Nodes are serially connected.
2. Ring Topology: Circular, serial connection.
3. Star Topology: All nodes connect to a central hub.
4. Mesh or Hybrid Topology: Interconnected nodes without a parent node.



Network protocols

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

- internet Protocol Suite/TCP/IP: Set of data transfer protocols used by modern networks.
- Key Protocols:

```
TCP-----transmission control protocol-------connection to connect internet[81]
UDP----user datagram protocol--------------graphical format---------video streaming[81]
VOIP---voice over internet protocol----------audio streaming[5060]
HTTP---hyper text transfer protocol----------send data over browser[80]
HTTPS--hyper text transfer protocol secure-------HTTP+SSL(Secure Socket Layer)[443]
FTP------file transfer protocol-------file sharing over intranet connection(local connection)[21]
SSH-----secure shell protocol-------terminal security(Linux)[22]
SMTP---simple mail transfer protocol-------Sending mail over communication channel[465/25/578]
TELNET--- telicom services[23]
POP3-----post office protocol 3-------Recieving + Storing mail into the server[110]
DHCP---- dynamically host configuration protocol-------Get the ip address from the router[67]
```

PORTS

Ports are the doors from where data comes and goes out of any device connected to a network can be LAN MAN or WAN.

Types of Ports

Physical Ports : They are tangible in nature. i.e we can see touch and feel the ports, and as its nature data comes and goes out from these ports.

For Example: USB Ports, LAN, HDMI, VGA etc etc.

Virtual Ports : There are total 65535 ports avialable as it clear from the virtual they non tangible ports which you can see and feel but cant touch. For Example: Ports 80,8080 for HTTP : data comes and goes from client to server. Some well known ports:

```
Port     |     Name
 21      | File Transfer Protocol (FTP)
 22      | Secured shell (Ssh)
 23      | Telnet
 25      | SMTP
 80      | HyperText Transfer Protocol (http)
```

Registered Ports: The registered port numbers are the port numbers that companies and other users register with the Internet Corporation for Assigned Names and Numbers (ICANN) for use by the applications that communicate using the Internet's Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).

The registered port numbers are in the range from 1024 through 49151.

Dynamic Ports: Besides the well-known port numbers and the registered port numbers, the remaining ports in the port number spectrum are referred to as dynamic ports or private ports and are numbered from 49152 through 65535.

Proxy or Proxy Servers:

A proxy server is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer sends your requests to the server which then processes your request and returns what you were wanting.

A proxy server is a computer that acts as a gateway between a local network and a larger-scale network such as the Internet

Proxy servers provide increased performance and security.

Example: www.hidemyass.com

https://www.proxysite.com

VPN(Virtual Private Network)

A virtual private network, or VPN, extends across a public or shared network, and acts like a tunnel so you can exchange data securely and anonymously across the internet as if you were connected directly to a private network.

Once you connect through a VPN, all your traffic becomes encrypted and your IP (Internet Protocol) address gets replaced with the address of the VPN server.

Services:

Online Services : hidemyass

extension based : hoxx vpn, Anonymox

Stand Alone Services : Psiphon

DNS (Domain Name System)

The Domain Name System (DNS) is the phonebook of the Internet. google.com--> 121.123.23.212

Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

WHAT IS AN IP ADDRESS ?

- An IP address is a 32-bit unique address assigned to a computer on the internet for communication.
- IPv4: 32-bit (4.29 billion unique addresses).
- IPv6: 128-bit (340 undecillion unique addresses

example 192.168.1.1 -> an ip address

8bit.8bit.8bit.8bit

A bit can either have value of 0 or 1

8 bits = 1 byte

1 killobyte = 1000 bytes

192 = 11000000 in binary

```
1×2^7 + 1×2^6 + 0x2^5 + 0x2^4 + 0x2^3 + 0x2^2 + 0x2^1 + 0x2^0 = 192
11000000
```

OR

```
92.168.32.1

(Binary form)so we have 192=128+64 = 11000000
            168=128+32+8=     = 10101000
                    32=        = 00100000
                     1=        = 00000001
so we have
                  11000000.10101000.00100000.00000001

128 64   32   16   8    4    2    1
--------------------------------------------------------------
1    1    0    0    0    0    0    0
1    0    1    0    1    0    0    0
0    0    1    0    0    0    0    0
0    0    0    0    0    0    0    0
```

Now the question is -> How 4 billion ip address are enough or were enough for today's world and how did we even we make it so far with only 4 billion ip address and That is with help of NAT or NETWORK ADDRESS TRANSLATION

NAT (Network Address Translation)

- Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses(common personal computers) to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

Private vs. Public IP Addresses

An ip address is of two types 1 Private 2 Public

Private Ip address -> Internal IP address valid on LAN but not on the internet for example All the devices connected to your wifi network have recieved a private ip address

There are three Different blocks of ipv4 addresses

```
Class A -> 10.0.0.0/8
(10.0.0.0 to 10.255.255.255)

Class B -> 172.16.0.0/12
(172.16.0.0 to 172.31.255.255)

Class C ->192.168.0.0/16
(192.168.0.0 to 192.168.255.255)
```

Public Ip address ->

Public ip address on the other-hand are globally unique and valid on the internet Example the ip address assigned to my WAN interface wireless router by ISP eg 42.111.108.97

www.whatismyip.com ---will show global ip

IP Subnets

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called sub-netting

One network into many networks so that it can be easily managed and be secured

DHCP Server

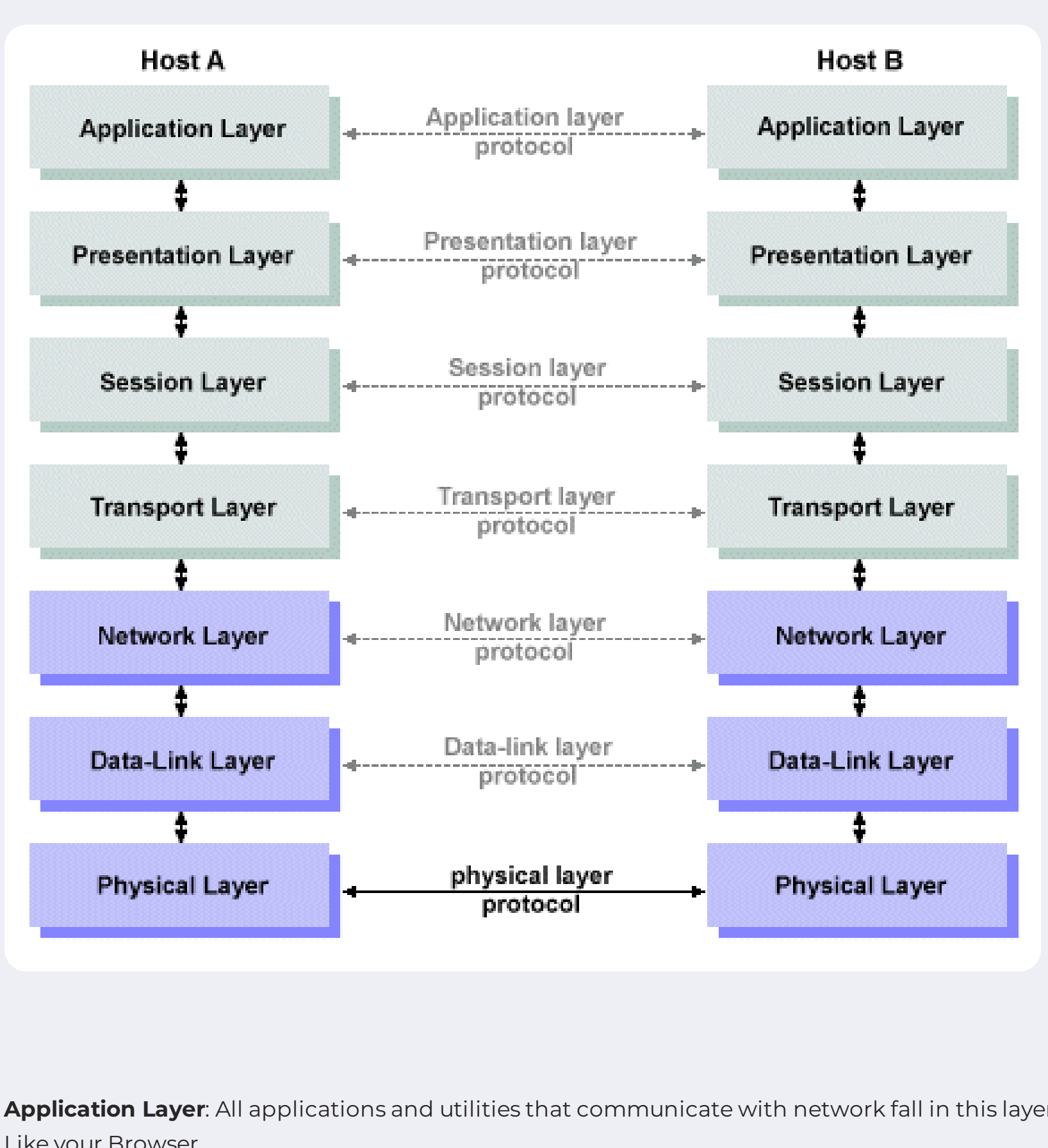
- Dynamic Host Configuration Protocol Server assigns IP addresses to devices on a network.
- DHCP server assigns IP addresses with lease durations.
- IP address assignment is done when devices connect to the network.
- every time some device is connected to wifi router an ip address is assigned to the device and that assigning of the task is done by dhcp server in wifi router

The ip address is assigned with a lease (Time limit) to which the ip address will remain functional for a device

Example Router Ip address =192.168.15.1

so The router can assign ip address to the devices from 192.168.15.2 to 192.168.15.255
And This Assigning is done with the help of dhcp server

OSI Layer



Application Layer: All applications and utilities that communicate with network fall in this layer. Like your Browser...

Presentation Layer: This layer is usually part of an operating system (OS) and converts incoming and outgoing data from one presentation format to another -- for example, from clear text to encrypted text at one end and back to clear text at the other.

Session Layer: This layer sets up, coordinates and terminates conversations. Its services include authentication and reconnection after an interruption.

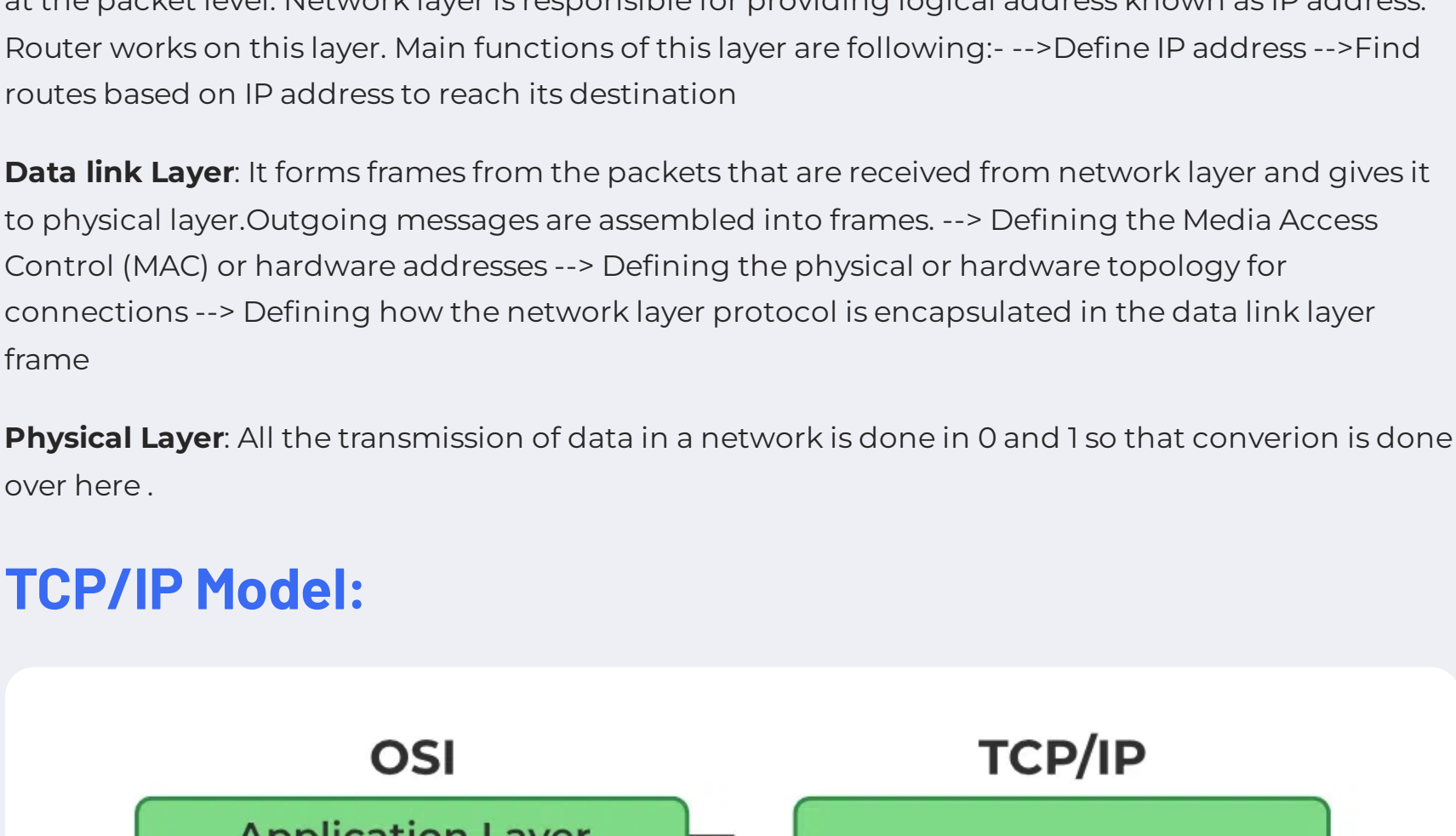
Transport Layer: This layer manages packetization of data, then the delivery of the packets, including checking for errors in the data once it arrives. (TCP AND UDP) -->Segmentation -->Connection management -->Reliable and unreliable data delivery

Network Layer: This layer handles addressing and routing the data -- sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level. Network layer is responsible for providing logical address known as IP address. Router works on this layer. Main functions of this layer are following:- -->Define IP address -->Find routes based on IP address to reach its destination

Data link Layer: It forms frames from the packets that are received from network layer and gives it to physical layer.Outgoing messages are assembled into frames. --> Defining the Media Access Control (MAC) or hardware addresses --> Defining the physical or hardware topology for connections --> Defining how the network layer protocol is encapsulated in the data link layer frame

Physical Layer: All the transmission of data in a network is done in 0 and 1 so that converion is done over here .

TCP/IP Model:



1. **Network Interface Layer (Link Layer):**
   - This layer deals with the physical and data link aspects of network communication.
   - It encompasses the actual hardware devices and their drivers that transmit data on a physical network medium.
   - It is responsible for addressing on the local network (e.g., MAC addresses for Ethernet) and handles error detection and correction.
2. **Internet Layer:**
   - The Internet layer primarily deals with the logical addressing and routing of data packets between different networks.
   - The Internet Protocol (IP), such as IPv4 and IPv6, operates at this layer and provides a unique IP address for devices on the network.
   - It is responsible for routing packets across different networks to reach their destination.
3. **Transport Layer:**
   - The transport layer is responsible for end-to-end communication between devices across different networks.
   - It ensures the reliable and error-checked delivery of data.
   - The two most common transport layer protocols are:
     - **Transmission Control Protocol (TCP):** Ensures reliable and connection-oriented communication. It provides features such as error checking, data sequencing, and flow control.
     - **User Datagram Protocol (UDP):** Provides connectionless and low-overhead communication. It is used when a lower level of reliability is acceptable, as in real-time applications like VoIP or streaming.
4. **Application Layer:**
   - The top layer is where applications and network services that the end-users interact with reside.
   - It includes various protocols and services that enable user applications to communicate over the network, such as HTTP (web), SMTP (email), FTP (file transfer), and many others.

OSI - protocol independent,TL guarantees delivery of packets

TCP/IP - based on standard protocol,TL does not