Network Connectivity

Network connectivity Devices

Network connectivity Devices

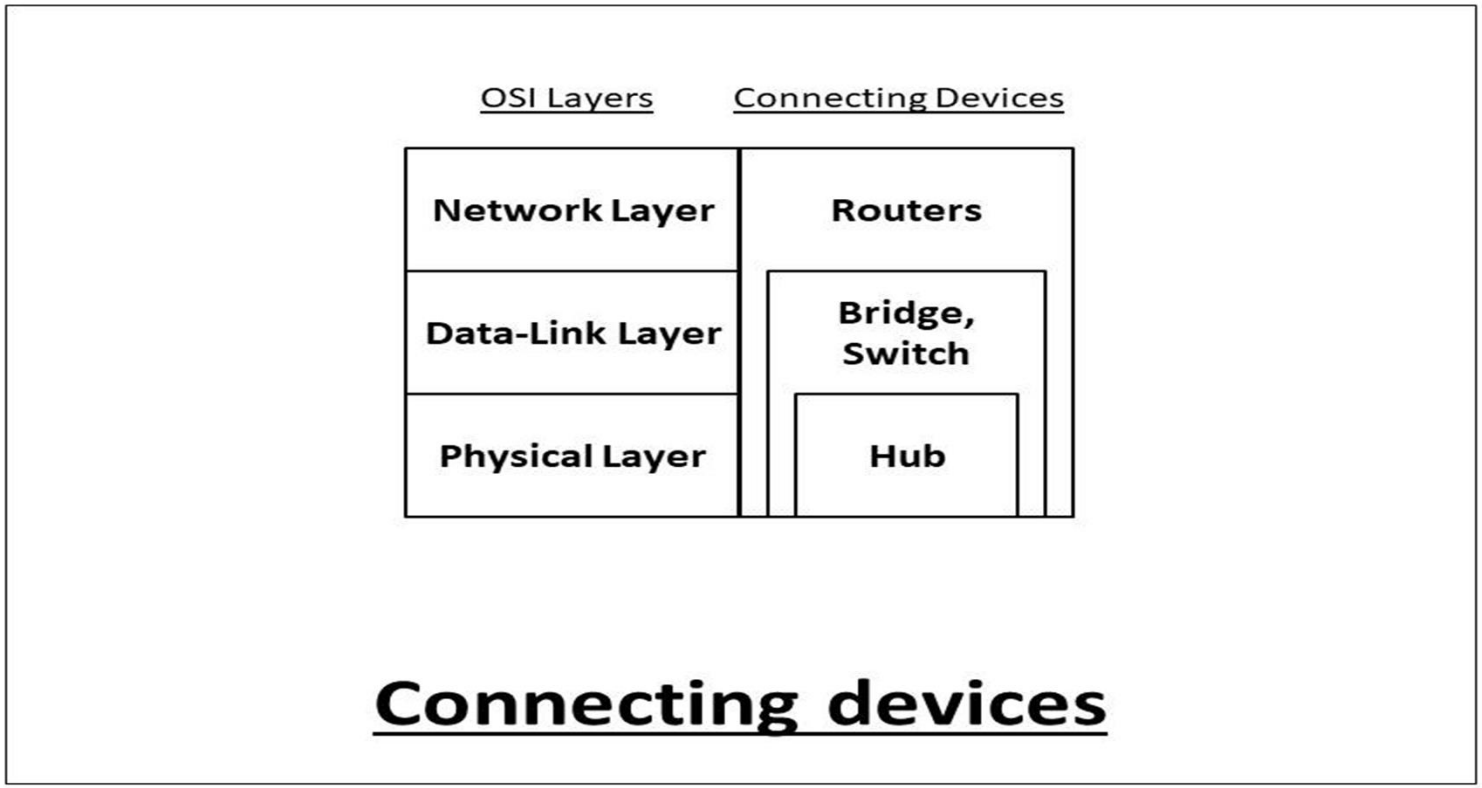
There are number of devices which are also known as data communication equipments and data terminal equipments like

- NICs
- Hubs
- Repeaters
- Switches
- Routers

NIC

- A Network Interface Card (NIC) is a computer hardware component that allows a computer to connect to a network. NICs may be used for both wired and wireless connections.
- A NIC is also known as a network interface controller (NIC), network interface controller card, expansion card, computer circuit board, network card, LAN card, network adapter or network adapter card (NAC).

- **A network connecting device is a device that connects two or more devices together that are present in the same or different networks.**
- A network connecting device can be a repeater, hub, bridge, switch, router, or gateway. But in this blog, we'll focus on hubs, switches, routers, and gateways. We'll also learn about their features, advantages, and disadvantages in networking.
- All these connecting devices operate in some specific layers of the OSI(Open System Interconnection) Model. These specifications are provided in the diagram below.



Connecting devices

1. Hub

- Hub is a very simple network connecting device. In Star/hierarchical topology, a Repeater is called Hub. A Hub in the physical network of the OSI Model. Since it works in the physical layer, it mainly deals with the data in the form of bits or electrical signals. A Hub is mainly used to create a network and connect devices on the same network only.
- A Hub is not an intelligent device; it forwards the incoming messages to other devices without checking for any errors or processing it. It does not maintain any address table for connected devices. It only knows that a device is connected to one of its ports.
- When a data packet arrives at one of the ports of a Hub, it simply copies the data to every port. In other words, a hub broadcasts the incoming data packets in the network. Due to this, there are various security issues in the hub. Broadcasting also leads to unnecessary data traffic on the channel.
- A Hub uses a half-duplex mode of communication. It shares the bandwidth of its channel with the connecting devices. It has only one collision domain, so there are more chances of collision and traffic on the channel. A hub is connected in limited network size. If the network size is increased, the speed of the network will slow down. Also, a hub can only connect the devices in the same network with the same data rates and format only.

There are two types of Hub:

- **Active Hub:** An Active hub is also known as Concentrator. It requires a power supply and can work as a repeater. Thus, it can analyze the data packets and can amplify the transmission signals, if needed.
- **Passive Hub:** A passive hub does not need any power supply to operate. It only provides communication between the networking devices and does not amplify the transmission signals. In other words, it just forwards the data as it is.

Advantages & Disadvantages of Hub

- ***Advantages of Hub:***

1. It is simple to implement.
2. The implementation cost is low.
3. It does not require any special system administration configuration.
4. We can just plug and play it.

- ***Disadvantages of Hub:***

1. It can connect devices of the same network only.
2. It uses a half-duplex mode of communication.
3. It is less secure, as it broadcasts the data packets.
4. It can be used in a limited network size only.
5. Broadcasting induces unnecessary traffic on the channel.

Bridge

- A bridge works on the physical and data-link layer of the OSI model. It interprets data in the form of data frames. In the physical layer, the bridge acts as a Repeater which regenerates the weak signals, while in the data-link layer, it checks the Media Access Control address of the data frames for its transmission.
- A bridge connects the devices which are present in the same network. It is mainly used to segment a network to allow a large network size. It has two types of port - incoming and outgoing. It uses the incoming port to receive the data frames and outgoing port to send the data frames to other devices. It has two collision domains, so there is still a chance of collision and traffic in the data transmission channel.
- A Bridge has filtering capacity. It means that it can discard the faulty data frames and will allow only the errorless data frames in the network. Also, it can check the destination MAC address of a frame and decides the port from which the frame should be sent out. For this, it maintains a table containing the physical(MAC) addresses of all the devices in the network. Whenever a data frame arrives at the incoming port of the bridge, it first checks the data frame for any kind of errors. If the frame is errorless, it directs the data frame to the specified MAC address(taking instance from the address table) using its outgoing port. It does not change the physicalof the frames during transmission. In other words, a Bridge is a Repeater with filtering capability.

Types of Bridge

- **Transparent Bridge:** Transparent bridge simply works as a transmission medium between two devices. They are actually transparent(they are present but are not functionally visible to the devices) to the networking devices.
- **Routing Bridge:** Routing bridges have their unique identity, they can be easily identified by the network devices. The source station or the sender can send the data packets through specific bridges(using the unique identity of bridges).

Advantages & disadvantages of Bridge

- ***Advantages :***
- It is not so complex to implement.
- The implementation cost is medium.
- It does not require any special system administration configuration. We can just plug and play it.
- Improves security by limiting the scope of data frames.
- It has the filtering capability.
- It can be used in a large network.
- ***Disadvantages :***
- It can connect devices of the same network only.
- There is a delay in forwarding the frames due to error checking.
- There is a need to maintain an Address table.

Switch

- A switch is a layer-2 network connecting device, i.e., it works on the physical and data-link layer of the OSI model. It interprets data in the form of data frames. A switch acts as a multiport bridge in the network. It provides the bridging functionality with greater efficiency.
- A switch maintains a Switch table which has the MAC addresses of all the devices connected to it. It is preferred more over the hub, as it reduces any kind of unnecessary traffic in the transmission channel. A switch can connect the devices only in the same network. It uses the full-duplex mode of communication and saves bandwidth. The switch table keeps on updating every few seconds for better processing.
- A Switch is an intelligent device with filtering capabilities. It can discard the faulty data frames and will allow only the errorless data frames in the network. Also, it will forward the data frames to the specific node based on the MAC address. A Switch has multiple collision domains, so it has least or no collisions in the transmission channel. In fact, every port of switch has a separate collision domain.
- When a data frame arrives at the Switch, it first checks for any kind of error in the data frame. If the frame is error-free, it will search the MAC address of the destination in the Switch table. If the address is available in the switch table, it will forward the data frame to that specific node, else switch will register the MAC address in the switch table. If the destination address is not specified, it will broadcast the data frame to each node in the network.
- A Switch can have 8/6/24/48 ports. The data transmission speed is slow in a switch (around 10-100 Mbps). Also, it has only one broadcasting domain.

Types of Switches

- **Store and Forward Switch:** It is the most widely and commonly used switch. It does not forward the data frames unless the frames are errorless and completely received in the switch buffer. It is reliable in nature.
- **Cut-through Switch:** Cut-through switches have no error checking. Also, it starts sending the data frame to the destination node when it starts receiving it. It is unreliable in nature.
- **Fragment-Free Switch:** It is a combination of store and forward, and cut-through switch. It checks only the starting 64 bytes(header information) of the data frame before transmitting the frame.
- **Adaptive Switch:** It is the most advanced kind of switch which automatically chooses any of the above three switches as per the need.

Advantages & disadvantages of Switch

- ***Advantages :***
- The implementation cost is medium.
- It does not require any special system administration configuration. We can just plug and play it.
- Improves security by limiting the scope of data frames.
- It has the filtering capability.
- It can be used in a large network.
- It uses full-duplex mode of communication
- It has multiple collision domains, so there are least or no collisions in the channel.
- ***Disadvantages :***
- It can connect devices of the same network only.
- There is a delay in forwarding the frames due to error checking.
- There is a need to maintain a Switch table.

Router

- A Router is a layer-3 network connecting device, i.e., it works on the physical, data-link and network layer of the OSI model. It interprets data in the form of data packets. It is mainly an internetworking device, which can connect devices of different networks(implementing the same architecture and protocols). In other words, it can connect two physically and logically different network devices with each other. A Router is used to connect the networks or it routes traffic between the networks. In other words, a Router is the Gateway of a network.
- Since, connecting two devices of different networks, the connecting device should implement an Internet Protocol(IP) address. So, the Router has a physical and logical(Internet Protocol) address for each of its interfaces. It routes or forwards the data packets from one network to another based on their IP addresses. It changes the physical address of the data packet(both source and destination) when it forwards the data packets.
- A router maintains a routing table using the routing algorithms. When a data packet is received at the router, it first checks the IP address. If the IP address is the same as the network's IP address, it receives the data packet, else it forwards the data packet to the destination IP address using the routing table.
- A router does not perform addressing. It can have 2/4/8 ports for connecting the devices. It can control both the collision domain(inside the network) and the broadcast domain(outside the network). It has a fast data transmission speed(up to 1 Gbps). A Router can be a Wireless Router, Core Routers, Edge Routers, Virtual Routers, etc.

Types of routing

- **Static Routing:** In Static Routing, the path for the data packets is manually set. It is generally used for small networks.
- **Dynamic Routing:** In Dynamic Routing, various routing algorithms are used to find the best and shortest path for the data packets.

Advantages & Disadvantages of Router

- ***Advantages :***
- It can connect devices and provides routing facilities over different networks implementing the same protocol and structure.
- Improves security by limiting the scope of data packets.
- It has the filtering capability.
- It can be used in a large network.
- It uses full-duplex mode of communication
- It has control over both the collision and broadcast domain.
- ***Disadvantages :***
- It is very complex to implement.
- The implementation cost is quite high.
- There is a need to maintain a Routing table.
- There is a delay in forwarding the packets due to error checking.
- It requires a special system administration configuration.

VoIP

- Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter.

- Internet telephony refers to all features of traditional telephony (phone calls, fax, voicemail etc.) where all calls and data are sent over the Internet rather than over traditional landlines. Examples of internet telephony services include the NFON cloud telephone system and Skype for Business.

Default Router Configuration

- Whenever we boot our Router first, there is always some default configuration that exists into it.
- The **show running-config** command is used to see the starting configuration of the router.

Client/Server Technology

- Client server technology means to break the application in two parts one is for client(user) and another for server(service provider).
- In such type of applications most of the controls and rights are available to server and a limited and/or exclusive access to them for end user.
- Generally there are a number of clients and a single server.
- If a client wants to communicate with another client it happens through Server.

Elements of Client/Server Technology

- Client(User) Generally do not store any data
- Server(Service Provider/Mainframe) Generally store all data
- Network

Server Management

- At its core, server management is about having control or access to a physical, virtual or application server in order to perform different types of administrative or maintenance operations. Server management also involves server monitoring and visibility into how a given server is operating to help improve and optimize performance.

- **Access.** In order to manage a server, a server management tool, server management service or server management software needs to be able to access the server it is trying to manage.
- **Updates.** Among the most basic server management functions is the ability to help start and install software or firmware updates.
- **Setup.** The ability to setup new software, add-ons or functionality is often a core feature of server management.Monitoring. Providing the capability to monitor different types of servers for status, performance and anomaly detection.
- **Optimization**. Some server management tools and services will also provide optimization capabilities to improve server efficiency and overall operations.
- **Capacity planning.** A more advanced feature is some cases is capacity planning which provides a forecast of server utilization, helping administrators to plan for when additional resources will be required.
- **Alerting.** The ability to alert an administrator, via email, SMS, slack or some other messaging system to different errors and incidents is another helpful component of server management.

Server Management Services

- Server management services help administrators to offload the direct responsibility for managing certain attributes of a given server. Depending on the type of server, there are different types of services that can be offered.
- For hardware, server management can involve a fully managed service, where the service provider is responsible for the physical and software management of the server.
- For web and application servers, server management at a hosting provider or in the cloud involves the management and maintenance of the core server software. It can often also include security as well as backup services for stability and overall resilience.
- Server management services can also help organizations to identify the best server applications and perform server software comparisons.

RAID TECHNOLOGY

- RAID – Redundant Array of Independent Disks .
- RAID is a data storage virtualization technology that combines multiple disk drive components into a logical unit for the purposes of data redundancy or performance improvement.
- MOTIVATION FOR RAID .Just as additional memory in form of cache, can improve system performance, in the same way additional disks can also improve system performance .In RAID, we use an array of disks. These disks operate independently .Since there are many disks, multiple I/O requests can be handled in parallel if the data required is on separate disks .A single I/O operation can be handled in parallel if the data required is distributed across multiple disks

RAID TECHNOLOGY

- Benefits of RAID
- Disk performance 1. Disk redundancy
- 2.Provide data security
- 3.Protects Data from disk failure

RAID TECHNOLOGY

Levels of RAID

There are 6 levels RAID schemes.

These are called RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5

The common characteristic in all these levels is:

A set of physical disk drives.

The operating system views these separate disks as a single logical disk.

Data is distributed across the physical drives of the array. Redundant disk capacity is used to store parity information.

Parity information can help in recovering data in case of disk failure

Cryptography

Encryption of data is called cryptography. To make the data secure and confidential we use it.

Cryptography

Terms related to Cryptography

- Encryption algorithm
- Codes/Keys
- Cryptanalysis

Ethical Hacking

- Ethical Hacking is used in closing the open holes in the system network. It also provides security to banking and financial establishments and prevents website defacements.

Ethical Hacking

- There are three types of hackers

1. White Hat Hackers: Who generally works with the permission of the owner of the system(software/hardware) for good cause.
2. Black Hat Hackers: Who generally works without permission of owner for their personal gain and do illegal activities.
3. Grey Hat hackers: These are the combination of both of the above

Disadvantages of ethical hacking

- All depends upon the trustworthiness of the ethical hacker
- Hiring professionals is expensive.

Wireless Networking

- WiMAX/Wireless MAN:

It is a technology of IEEE80 2.16 standard to provide a wireless broadband to the users in a large area.

It provides the internet connectivity in a city or may be in the larger area.

Wireless Networking

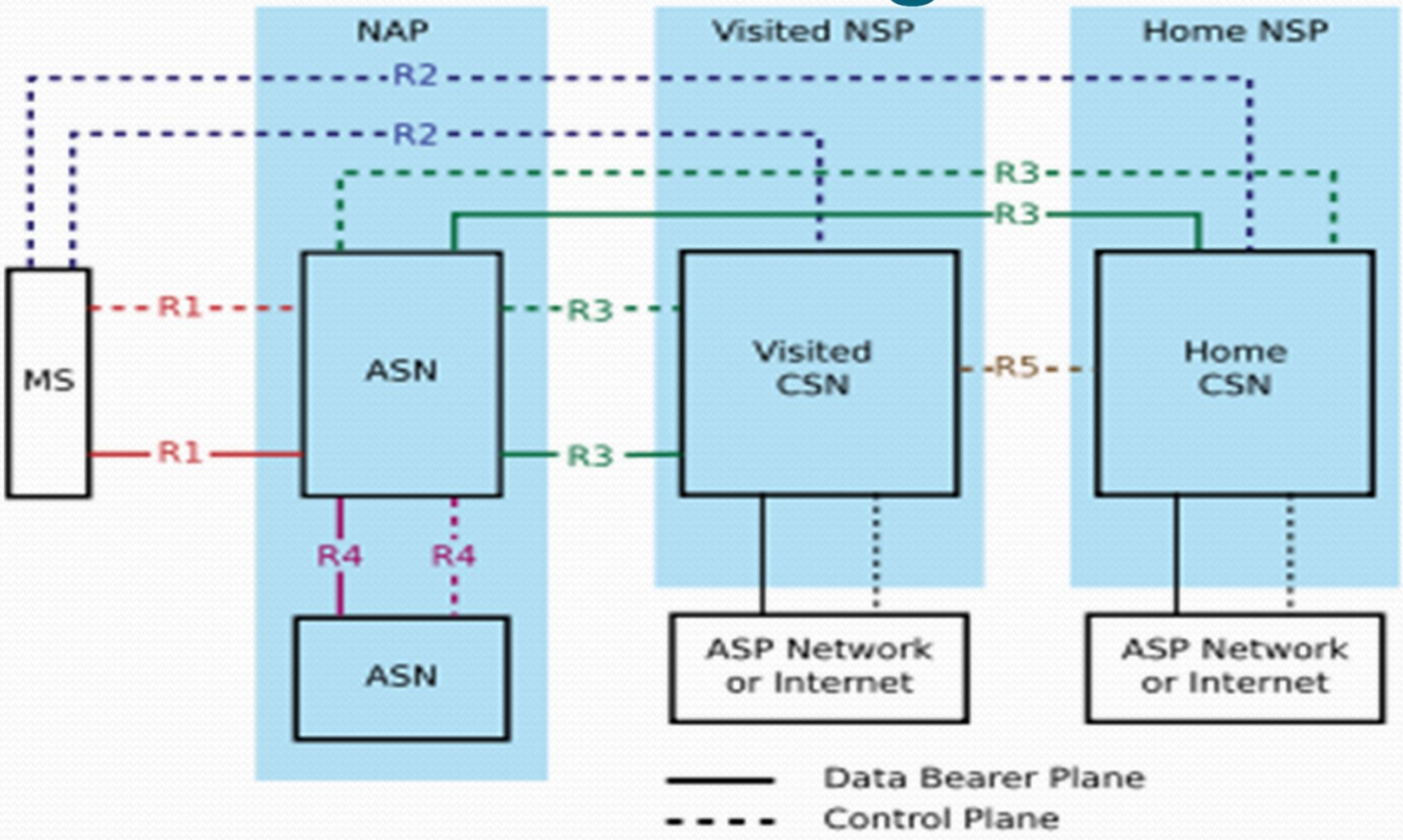
Provides portable mobile broadband connectivity across cities .

- Provides a wireless alternative to cable and digital subscribe line (DSL) for end user.
- Provides data, telecommunications (VoIP) and IPTV services.

Wireless Networking

- **Technical Details of WiMax**
- Latest version **WiMax rel 2.0** uses MIMO(Multiple Input Multiple Output) (20 MHz Time Division Duplexing) and (2x20 MHz Frequency Division Duplexing)
- Carrier spacing is constant
- Advanced antenna diversity
- Hybrid automatic repeat request
- Low density parity check

Wireless Networking



WiMax Architecture

Wireless Networking

- SS/MS: the Subscriber Station/Mobile Station
- ASN: the Access Service Network
- BS: Base station, part of the ASN
- ASN-GW: the ASN Gateway, part of the ASN
- CSN: the Connectivity Service Network
- HA: Home Agent, part of the CSN
- AAA: Authentication, Authorization & Accounting Server, part of the CSN
- NAP: Network Access Provider
- NSP: Network Service Provider

Wireless Networking

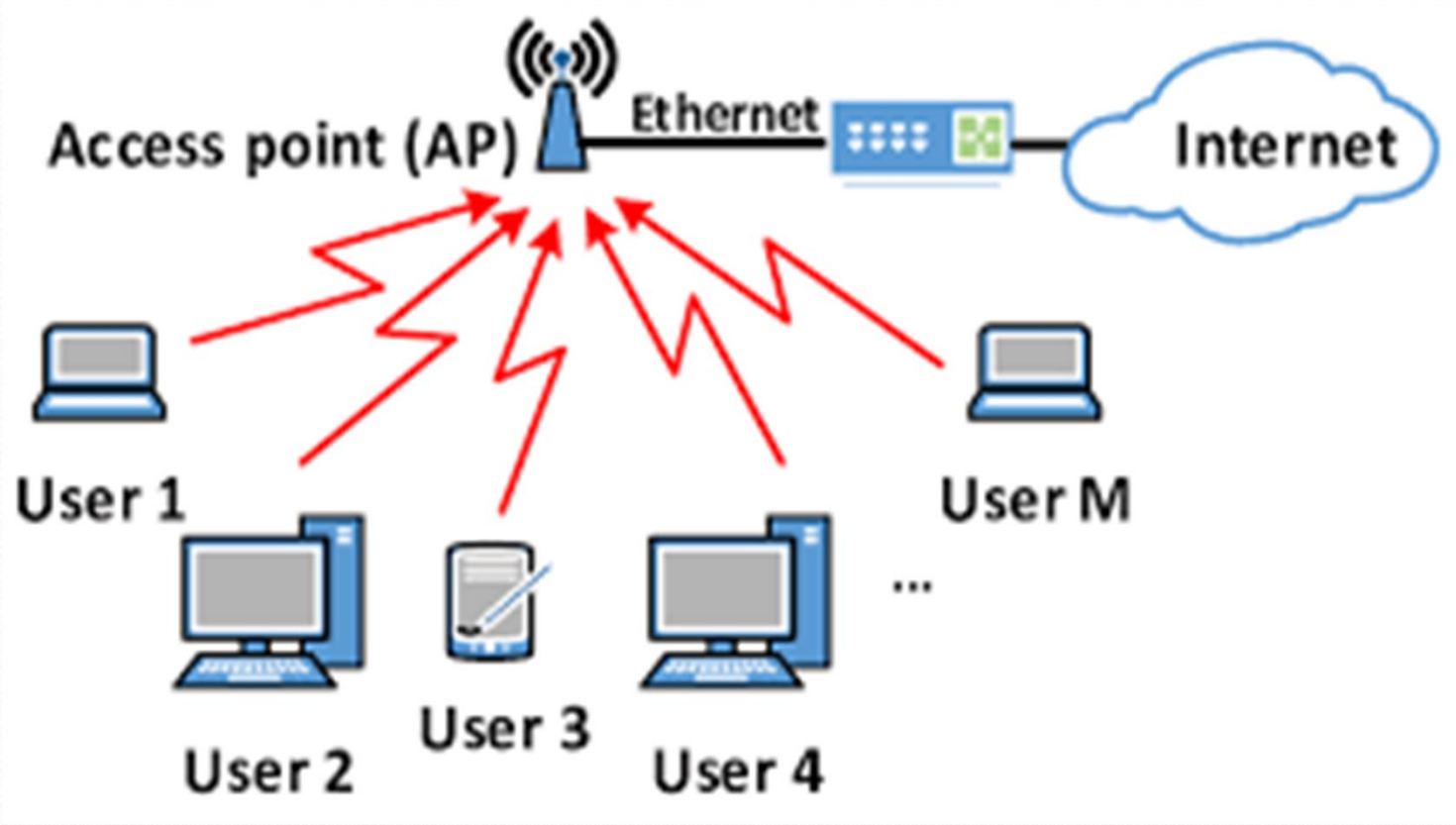
- A WiMax user with low or zero mobility may use a downstream speed of 1 Gbit/s.
- In case of mobility it depends on various factors like speed of user hand offs etc.

Wireless Networking

- **WLAN(Wireless LAN):**

Like LAN, WLAN is a method of connecting a small number of computers/devices in one premises like in a house or in an office but wirelessly.

Wireless Networking



Wireless Networking

- The main difference between LAN and WLAN is only that there is no physical connection between users and Access Point as shown in figure above.

Wireless Networking

- WiFi(Wireless Fidelity):

It is a wireless technology that is used to transmit data using RF.

It is easy and fast to install.

It is easy to manage.

It is secure.

Growth is possible as and when required.

Wireless Networking

- Disadvantages of WiFi:

Speed is less than cable network.

Affected by walls, doors and glasses.

Possibilities of unauthorized access.

Range is limited.

Interference by other signals.

Devices consume more power to use wifi.

Wireless Networking

- Li Fi(Light WiFi)

It is a technology which use light(visible, infrared or ultraviolet) to transfer the data wirelessly.

LiFi have a number of advantages over wifi like

Higher bandwidth

Can be used at sensitive places like hospitals, Aeroplanes

High Speed

Wireless Networking

LiFi

- LEDs are used to transfer the data
- LiFi works by switching the current to the LEDs off and on at a very high speed.

Limitations of LiFi:

Light cannot cross walls.

Devices should be in front of each other to communicate.

Wireless Networking

- ***Standards of LiFi***

- **PHY 1** is for outdoor applications and works from 11.67 kbit/s to 267.6 kbit/s.
- **PHY 2** layer permits reaching data rates from 1.25 Mbit/s to 96 Mbit/s.
- **PHY 3** is used for many emissions sources with a particular modulation method called color shift keying (CSK). PHY III can deliver rates from 12 Mbit/s to 96 Mbit/s.

TCP/IP

TCP/IP

It is a set of communication protocols/rules for internet and other similar networks.

It contains two things

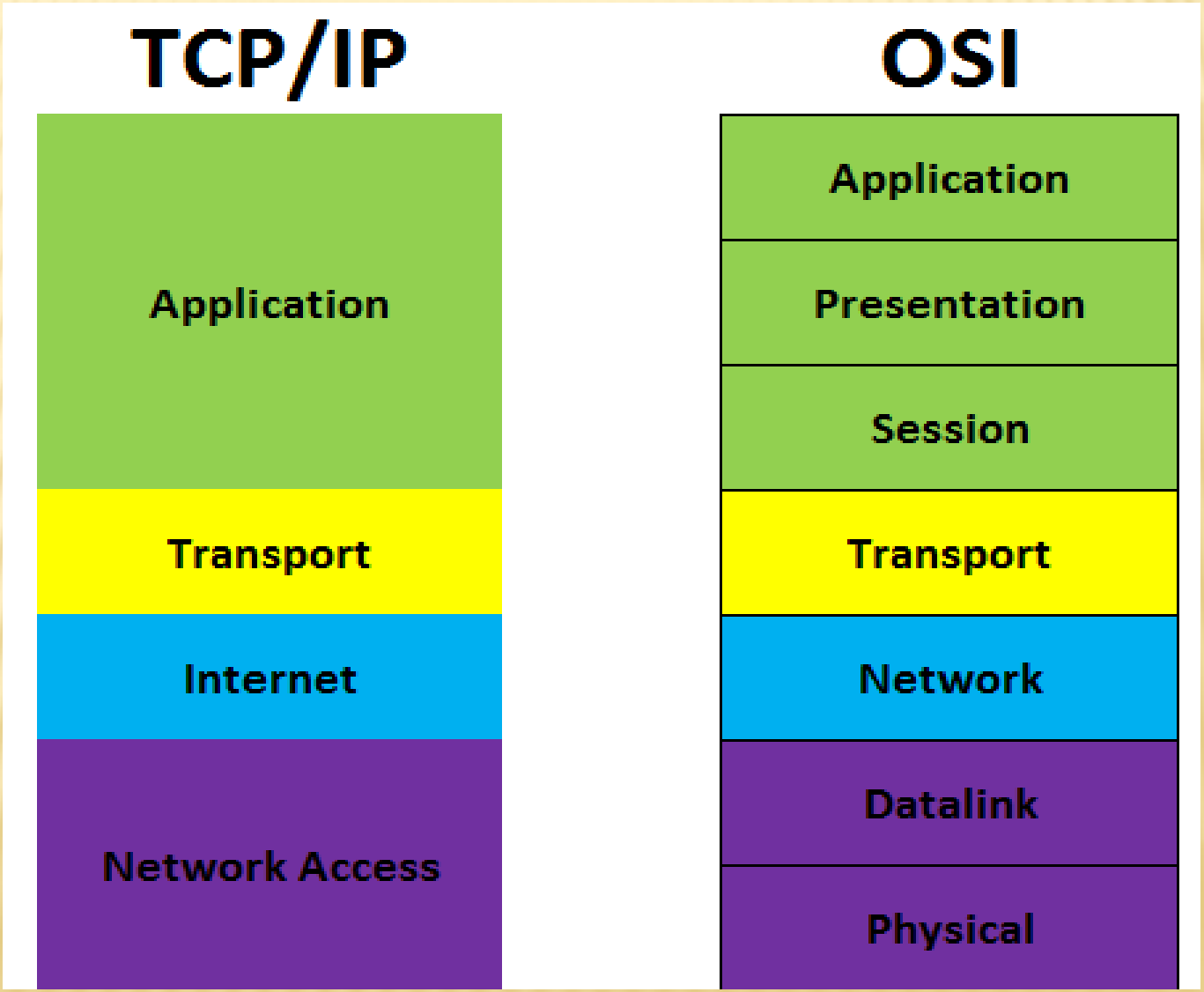
1. TCP- Transmission Control Protocol
2. IP - Internet Protocol

TCP/IP LAYERS

Application Layer
Transport Layer
Internet Layer
Network Access Layer

Application Layer	E-mail + Network Management + www & other
Transport Layer	End-to-end message integrity + Error recovery
Internet Layer	Transfer packet to appropriate layer + error detection and correction
Network Access Layer	Network Technology

OSI AND TCP/IP



APPLICATION LAYER

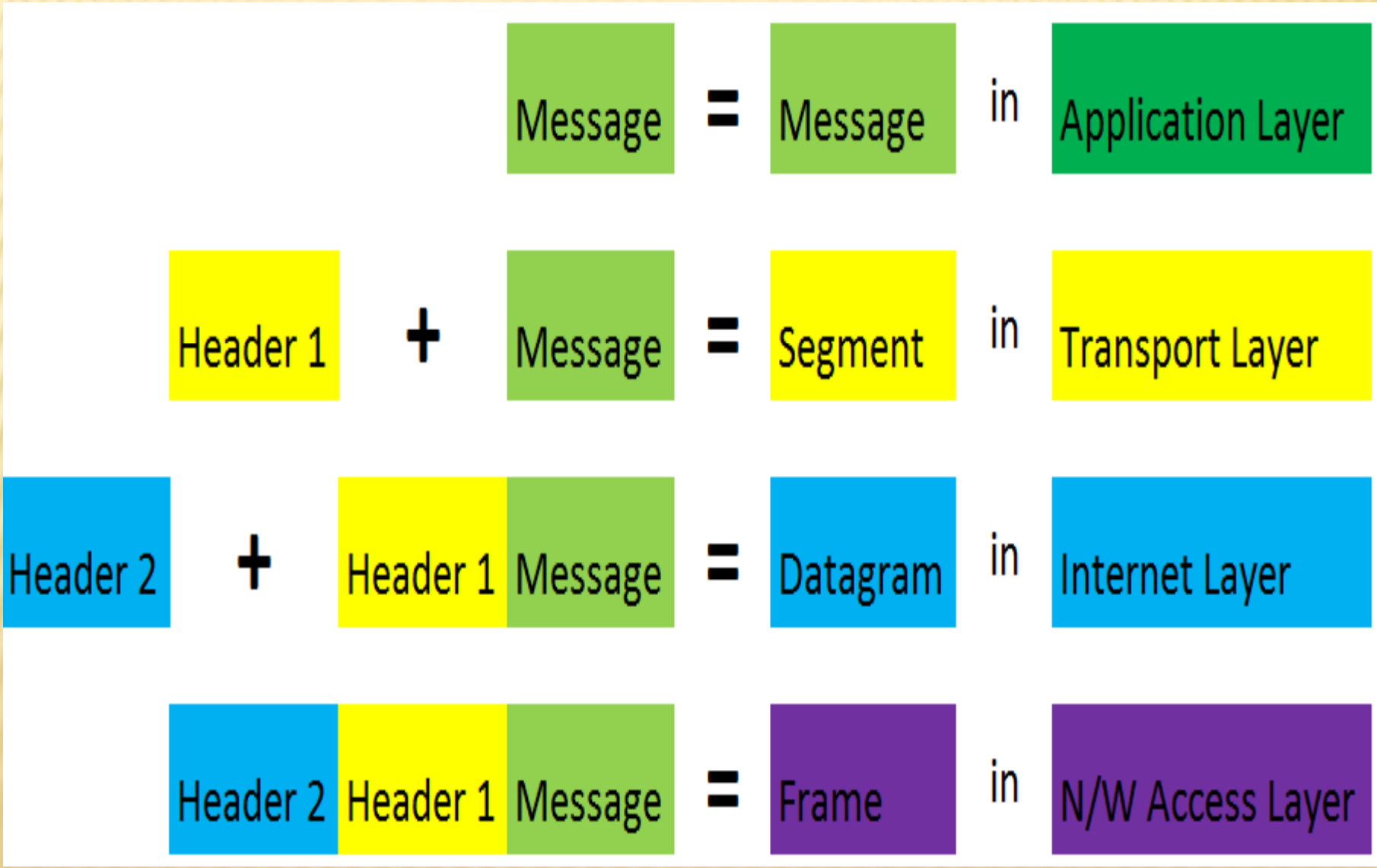
*Application layer in TCP/IP is Similar to the combination of the Session, Presentation and Application layer of the OSI Model.

*All the functions handled by these 3 layers in OSI model are handled by a single Application layer in TCP/IP/

*This layer contains higher level protocols like FTP, SMTP,HTTP etc.

*Unit of data in this layer is called a message.

FLOW OF DATA IN DIFFERENT LAYERS



FLOW OF DATA IN DIFFERENT LAYERS

*A data unit created at Application Layer is called Message.

*Transport layer add a header in message & then it is a segment.

*Internet layer add another header in it & then it becomes datagram.

* N/W Access layer encapsulates the datagram and now it becomes a frame.

TRANSPORT LAYER-UDP

*It uses two protocols

UDP(User Datagram Protocol)

TCP(Transmission Protocol)

*Both the protocols are similar but UDP is simpler and fast but lesser reliable and secure.

*Because reliability and security are important parameters so mostly we use TCP instead of UDP.

*However UDP is good for general video transmission because of its high speed.

TRANSPORT LAYER-TCP

*TCP is a reliable connection oriented protocol.

*It provides error-free transmission.

*It create short parts(messages) of the incoming byte stream and forwards them to the next layer.

*It also control the data transfer rate.

TRANSPORT LAYER-TCP

*A connection must be established between transmitter and receiver before the data transmission begins.

*TCP creates a connection between Tx and Rx for the duration of transmission.

*TCP alerts the receiver before each transmission.

*Connection terminates after each transmission.

TRANSPORT LAYER-TCP

Header Added by transport layer contains

1.Sequence or Serial no. to rearrange at receiver

2.Acknowledgement ID

3.Source Address

4.Destination Address

5.Parity or other bits for error derection

6.etc.

INTERNET/NETWORK LAYER

*It uses IP(Internet Protocol)

*IP is an unreliable and connectionless protocol.

*It doesn’t check for errors.

*It transmit the data with no guarantee.

*Datagram may be discarded due to timeout.

*Bits may be lost due to noise.

*In this layer data is in the form of datagram.

INTERNET/NETWORK LAYER

*Each datagram transported separately.

*Datagrams may be of different lengths up to 64kb.

*Datagram may travel along different routes hence may reach out of sequence.

*Header added by this layer contains source and destination address and may be some other information.

NETWORK ACCESS LAYER

*Here encapsulation of IP datagrams into the frames transmitted by the network, and mapping of IP addresses to the physical addresses used by the network is done.

*The protocols in this layer provide the means for the system to deliver data to the other devices on a directly attached network.

NETWORK ACCESS LAYER

*It defines how to use the network to transmit an IP datagram.

*Unlike higher-level protocols, Network Access Layer protocols must know the details of the underlying network (its packet structure, addressing, etc.) to correctly format the data being transmitted to comply with the network constraints.

*The TCP/IP Network Access Layer can encompass the functions of all three lower layers of the OSI reference Model (Network, Data Link, and Physical).