./

Learning Report – Networking



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel.**  **No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be Approved** | **Remarks/Revision Details** |
|  | 26/3/2021 | Nitin N Shetty  [99003746] |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Contents

[1.Network Classification 5](#_Toc67673572)

[1.1 PAN [Personal Area Network] 5](#_Toc67673573)

[1.2 LAN [Local Area Network] 5](#_Toc67673574)

[1.3 WAN [Wide Area Network] 5](#_Toc67673575)

[1.4 MAN [Metropolitan Area Network] 5](#_Toc67673576)

[1.5 WLAN [Wireless Local Area Network] 6](#_Toc67673577)

[1.6 WIFI 6](#_Toc67673578)

[1.7 WIMAX [Worldwide Interoperability for Microwave Access] 6](#_Toc67673579)

[2. Components of Network: - 7](#_Toc67673580)

[2.1 Work Stations 7](#_Toc67673581)

[2.2 File Servers 7](#_Toc67673582)

[2.3 Gateway 7](#_Toc67673583)

[2.4 NIU [Network Interface Unit] 7](#_Toc67673584)

[2.5 HUB 7](#_Toc67673585)

[2.6 Communication Channel / LAN Channels 8](#_Toc67673586)

[2.7 Switch 8](#_Toc67673587)

[2.8 Bridge 8](#_Toc67673588)

[2.9 Access Points 9](#_Toc67673589)

[3. Queuing and Scheduling 9](#_Toc67673590)

[4. OSI MODEL 10](#_Toc67673591)

[4.1 Physical Layer 11](#_Toc67673592)

[4.2 Data link layer 11](#_Toc67673593)

[4.3 Transport Layer 11](#_Toc67673594)

[4.4 Session Layer 11](#_Toc67673595)

[4.5 Presentation Layer 11](#_Toc67673596)

[4.6 Application Layer 12](#_Toc67673597)

[5. NETWORK TYPES AND TOPOLOGIES 12](#_Toc67673598)

[5.1 Bus Topology 12](#_Toc67673599)

[5.1.1 Advantages: 13](#_Toc67673600)

[5.1.2 Disadvantages: 13](#_Toc67673601)

[5.2 Mesh Topology 13](#_Toc67673602)

[5.2.1 Advantages: 14](#_Toc67673603)

[5.2.2 Disadvantages: 14](#_Toc67673604)

[5.3 Ring Topology 14](#_Toc67673605)

[5.3.1 Advantages: 15](#_Toc67673606)

[5.3.2 Disadvantages: 15](#_Toc67673607)

[5.4 Star Topology 15](#_Toc67673608)

[5.4.1 Advantages: 16](#_Toc67673609)

[5.4.2 Disadvantages: 16](#_Toc67673610)

[5.5 Tree Topology 16](#_Toc67673611)

[5.5.1 Advantages: 17](#_Toc67673612)

[5.5.2 Disadvantages: 17](#_Toc67673613)

[5.6 Hybrid Topology 17](#_Toc67673614)

[5.6.1 Advantages: 18](#_Toc67673615)

[5.6.2 Disadvantages: 18](#_Toc67673616)

[6. PROTOCOLS 18](#_Toc67673617)

[6.1 TCP Protocol 18](#_Toc67673618)

[6.2 UDP Protocol 19](#_Toc67673619)

[6.3 IP Protocol 20](#_Toc67673620)

[6.4 L2 Protocols 20](#_Toc67673621)

[6.4.1 RARP (Reverse Address Resolution Protocol) 20](#_Toc67673622)

[6.4.2 ICMP (Internet Control Message Protocol) 21](#_Toc67673623)

[6.4.3 DHCP (Dynamic Host Configuration Protocol) 21](#_Toc67673624)

[6.4.4 ARP (Address Resolution Protocol) 22](#_Toc67673625)

[5.5.1 BGP (Border Gateway Protocol) 23](#_Toc67673626)

[6.5.2 RIP (Routing Information Protocol) 23](#_Toc67673627)

[6.5.3 EIGRP (Enhanced Interior Gateway Routing) 23](#_Toc67673628)

[6.6 Types of WLAN Protocols 24](#_Toc67673629)

[7. IP ADDRESS 24](#_Toc67673630)

[6.1 IPV4 24](#_Toc67673631)

[7.1.2 Parts of IPv4: 25](#_Toc67673632)

[7.1.3 Characteristics of IPv4: 25](#_Toc67673633)

[7.2 IPV6 25](#_Toc67673634)

[7.3 SUBNETTING THEORY 26](#_Toc67673635)

[8. Network Security: 27](#_Toc67673636)

[8.1 Firewall: 27](#_Toc67673637)

[8.2 Encryption: 27](#_Toc67673638)

[8.2.1 How Encryption Works: 27](#_Toc67673639)

[8.3 Cryptography: 28](#_Toc67673640)

[8.4 Overflows: 28](#_Toc67673641)

[8.5 SSH PROTOCOL 28](#_Toc67673642)

[8.6 TLS PROTOCOL 30](#_Toc67673643)

[8.7 MTLS: 31](#_Toc67673644)

[9. Classful Network 32](#_Toc67673645)

[9.1 Class A: - 32](#_Toc67673646)

[9.2 Class B: - 32](#_Toc67673647)

[9.3 Class C: - 32](#_Toc67673648)

[9.4 Class D: - 33](#_Toc67673649)

[10 NETWORK TOOLS 33](#_Toc67673650)

[10.1 Packet Tracer 33](#_Toc67673651)

[10.2 Wireshark 33](#_Toc67673652)

[11 Activity 34](#_Toc67673653)

[11.1 IPv4 Subnetting 34](#_Toc67673654)

[11.3 Wireshark 37](#_Toc67673655)

[11.4 PACKET TRACER 40](#_Toc67673656)

[12. END -TO -END DATA FLOW 41](#_Toc67673657)

[13. REFRENCES 42](#_Toc67673658)

# 

# 1.Network Classification

## 1.1 PAN [Personal Area Network]

* A personal area network (PAN) is a PC network coordinated around a person for individual utilize as it were. They regularly include a PC, telephone, printer, tablet, or some other gadget like a PDA.
* It typically ranges within 10m and WLAN ranges from10m to 100m.
* PAN supports 250 kbps in ZigBee, from kbps to 24 Mbps in Bluetooth case.

## 1.2 LAN [Local Area Network]

* A local area network (LAN) is a collection of devices connected in one physical location, such as a building, office, or home.
* A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
* It ranges from 10 to 100m and more in case of wireless LAN.
* LAN supports 10, 100 and 1000 Mbps.
* Wired LAN devices are connected using Ethernet cables.

## 1.3 WAN [Wide Area Network]

* A wide zone network traverses a huge geographic region like a city, state, or country.
* It can be private to interface parts of a business, or it tends to be public to associate more modest organizations. It ranges more than 1,00,000 kms.
* It runs on bandwidths of 20 Mbps, 50 Mbps, or 100 Mbps.

## 1.4 MAN [Metropolitan Area Network]

* A Metropolitan Area Network it is more similar to LAN but range of the man covers entire city or campus or some university territory
* MANs are formed by connecting multiple LANs
* It serves geographical area of 5-50kms in range.
* Thus, MANs are larger than LANs, but smaller than wide area networks (WAN) that cover dispersed geographical areas, sometimes directly connecting users around the world.
* It supports a speed of 5-10 Mbps.

## 1.5 WLAN [Wireless Local Area Network]

* WLAN is local area network that does not depend on wired ethernet connection
* A Wireless Local Area Network it is concept of or distribution for more than two
* Devices.
* WLAN Supports 54Mbps or above
* WLAN use high-frequency radio waves and often include an access point to the internet
* A WLAN allows user to move around the coverage area, often a home or small office, while
* Maintaining a network connection.

## 1.6 WIFI

* Wi-Fi is a wireless networking protocol that devices use to communicate without direct cable connections. It is an industry term that represents a type of wireless local area network (LAN) protocol based on the 802.11 IEEE network standard
* The 802.11a will transmit data at a frequency level of 5GHz – transmits a maximum of 54Mbps.
* The 802.11b will transmit data at a frequency level of 2.4GHz- transmits a maximum of 11Mbps
* The 802.11g will transmit data at 2.4GHz – transmits a maximum of 54 Mbps.

## 1.7 WIMAX [Worldwide Interoperability for Microwave Access]

* WiMAX is a wireless communication standard designed for creating metropolitan area network it is like the Wi-Fi Standard, but supports a far greater range of coverage.
* A single WiMAX tower can provide coverage to a very large area big as 3,000 square miles i.e., 8,000 square km. The 802.11b will transmit data at a frequency level of 2.4GHz- transmits a maximum of 11Mbps.
* The 802.11g will transmit data at 2.4GHz – transmits a maximum of 54 Mbps.

# 2. Components of Network: -

## 2.1 Work Stations

Workstation is a computer which request to the LAN and change services to reacts the requests by means of change to perform dedicated task with having upgraded features. In workstation, Tasks are in forms of Business. A workstation is a unique PC intended for specialized or logical applications. Expected principally to be utilized by everyone in turn, they are normally associated with a neighborhood and run multi-client working frameworks.

## 2.2 File Servers

A file server is a central worker in a PC network that gives file system or if nothing else parts of a file system to associated customers. File Server offer a user’s a central storage place for documents on inside information media, which is open to all approved customers. Here, the server administrator defines strict principles in regard to which clients have which access rights: For example, the design or document approvals of the separate record framework to enable the administrator to set which records can be seen and opened by a specific client or client gathering, and whether information must be seen or additionally added, altered, or erased.

## 2.3 Gateway

Gateway is a network hub that shapes a section between two networks working with various transmission protocols. The most widely recognized gateways, the network gateway works at layer 3, for example network layer of the OSI (open system interconnection) model. In any case, depends on functionality, a gateway can work at any of the seven layers of OSI model. It acts as a entry – exit point for an network since all traffic that streams across the network should go through the gateway. Just the interior traffic between the hubs of a LAN doesn't go through gateway

## 2.4 NIU [Network Interface Unit]

NIU represents Network Interface Unit, it is fundamentally a translator that is utilized to set up the communicated a between the server and the workstations or hubs. An independent PC or a PC that isn't joined to any network, lives in its own reality and does its task with its own inbuilt asset. When it turns into a Workstation then it needs an interface to help set up an connection with the network on the grounds that without this the workstation or hub won't share network resources. You can likewise say that, an Network Interface Unit(NIU) is an essentially a device that joined to every one of the work station and the server, and helps workstation and the server and assists workstation with setting up the immensely significant association with the network

## 2.5 HUB

A hub, also called a network hub, additionally called an Network center, is a typical association point for devices in an network. HUB are devices usually used to interface sections of a LAN. The HUB contains different ports. At the point when a packets shows up at one port, it is duplicated to different ports so that all sections of the LAN can see all bundles. In a HUB, a casing is communicated to all of its ports. The HUB has no chance to get of recognizing which port a frame should be sent to. Passing it to each port guarantees that it will arrive at its proposed destination. This Place a lot of Traffic on the network and can lead to poor network response times. To connect multiple Lan [Local Area Network] together to form a larger network a bridge network device is Important. The steps to or process of aggregating network is called as Network bridging.

An bridge interfaces the various segments so that they appear as parts of a single network. It works at the data link Layer of the OSI model also referred to as Layer 2 Switches. Since they work at data link layer, they send data as data frames. On getting an data frames, the bridge consults a data set to conclude whether to pass, transmit or dispose of the frame. If the frame has a MAC (media access control) address in a similar network, the bridge passes the frame to that hub and afterward discards of it. It will forward the frame only it has a destination MAC address in a connected network.

## 2.6 Communication Channel / LAN Channels

In communication, a channel is the methods for passing data from a sender to a beneficiary. Deciding the most proper channel, or medium, is critical to the effectiveness of communication. Stations incorporate oral methods, for example, calls and presentations, and composed modes like reports, reminders, and email.

## 2.7 Switch

In networks the switch is the device that channels and that forwards packets between LAN portions. Switches work at the data link layer (layer 2) and now and again the network layer (layer 3) of the OSI Reference Model and consequently support any packet protocol LANs that use switches to join segments are called switched LANs or for Ethernet Networks, switched Ethernet LANs. Switches encourage the sharing of resources by interfacing every one of the device, Including PCs, printers, and servers, in a private company network. Building an independent small network Is beyond the realm of imagination without changes to device together.

## 2.8 Bridge

A bridge network is a device associates numerous LANs (Neighborhood) together to frame a bigger LAN. The process of aggregating network is known as network bridging. An bridge associates the various segments so they show up as parts of a single network. Bridges work at the data link layer of the OSI model and subsequently referred as Layer 2 switches.

Since they work at data link layer, they transmit data as data frames. On accepting an data frame, the bridge consults s a database set to conclude whether to pass, send or dispose of the frame. On the off chance that the frame has an destination MAC (media access control) address in a similar network, the bridge passes the frame to that hub and afterward disposes of it. On the off chance that the frame has an destination MAC in an associated network, it will forward the frame toward it.

## 2.9 Access Points

A access-point is a device that wireless local area network, or WLAN, typically in an office or enormous structure. A access point associates with a wired router, switch, or hub through an Ethernet cable, and projects a Wi-Fi signal to an assigned zone.

# 3. Queuing and Scheduling

Queuing and scheduling applied to an interface allows traffic to be split into multiple queues so that the scheduler can decide which type of treatment the traffic inside each queue receives. If the traffic mapped to each queue belongs to a specific class of service, the scheduler can apply differentiated behavior to different classes of service.

The two most important parameters associated with the queuing and scheduling mechanism are buffers and bandwidth. Buffering is the length of the queue, that is, how much memory is available to store packets. However, the entire packet does not need to be queued, as we see later; sometimes what is stored is a notification, which is a representation of the packet contents. The buffering value can be defined either as a time value during which packets are accepted on the interface on which queuing is enabled or as a physical size in terms of how many packets or packet notifications can reside in the queue at the same time. The buffering value is a quota of available memory and can be defined as milliseconds of traffic or absolute numbers of packets.

The bandwidth parameter refers to the scheduling part of the equation. A total amount of bandwidth is made available to the queuing and scheduling mechanism. Scheduling determines how much is allocated to each queue. The total amount of bandwidth can be either the interface speed or the shaping rate if a shaper is applied after the Scheduler. The queuing and scheduling discipline used determines how the resources are allocated. The requirement for the presence of queuing and scheduling is typically controlled by the presence of congestion. If resources are sufficient and there is no competition for resources, there is no need for queuing. One way to create congestion is to place more traffic on an interface than the outgoing line speed can support. Congestion can also be created artificially, by applying a shaping rate to the interface that imposes a speed limit lower than the maximum interface line speed. The leftover traffic is throttled or back- pressured into memory, which is then partitioned across the actual queues. The scheduler then services the queues and is responsible for the rate at which packets from each queue are transmitted.

Different Types of Queuing

**First in, first out (FIFO) queuing**

FIFO is a well-known acronym for First In, First Out, and is probably the most basic queuing scheduling discipline. The principle behind FIFO queuing is that all packets are treated equally, by all being placed in the same queue. So in a nutshell, there is one queue and the scheduler only serves this queue. This mechanism implies that the removal rate is directly inherited from either the interface speed or from the shaping rate if there is a shaper applied. Because with any queuing mechanism there is no overtaking within a queue, the packets are serviced in the same order in which they were placed into the queue.

Fair queuing (FQ)

The main disadvantage of FIFO queuing is that flows consisting of many packets can take up most of the bandwidth for less bandwidth-intensive applications, because FIFO does not separate flows or streams of packets. Fair queuing (FQ), also commonly called the fairness algorithm, is a scheduling algorithm that addresses the basic limitation of FIFO queuing. FQ classifies packet flows into multiple queues, offering a fair scheduling scheme for the flows to access the link. In this way, FQ separates traffic and flows, and avoids applications that consume less bandwidth being starved by applications that consume more bandwidth.

• Priority queuing (PQ)  
• Weighted fair queuing (WFQ)  
• Weighted round robin (WRR)  
• Deficit weighted round robin (DWRR)  
• Priority-based deficit weighted round robin (PB-DWRR)

# 4. OSI MODEL

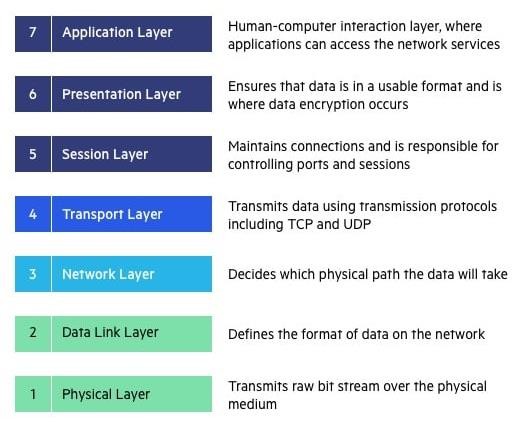


Fig OSI Model

The OSI Model (Open Systems Interconnection Model) is an applied structure used to portray the elements of a systems administration framework. The OSI model portrays registering capacities into an all-inclusive arrangement of rules and necessities to help interoperability between various items and programming. In the OSI reference model, the correspondences between a processing framework are part into seven distinctive abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

## 4.1 Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically communicating raw unstructured information bits across the network from the physical layer of the sending device

to the physical layer of the accepting device. It can incorporate determinations like voltages, pin format, cabling, and radio frequencies. At the Physical layer, one may discover "physical" resources, for example, network centers, cabling, repeaters, network connectors or modems.

## 4.2 Data link layer

The data link layer, directly associated nodes are utilized to perform node to-node data transfer where data is packaged into frames. The data link layer likewise revises errors that may occurred at the physical layer.

The data link layer incorporates two sub-layers of its own. **Network Layer** The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

## 4.3 Transport Layer

The Network layer is liable for getting frames from the data link layer, and delivering them to their proposed destinations among dependent on the tends to contained inside the frame. The network layer finds the destination by using logical addresses, like IP (internet protocol). At this layer, routers are an essential component used to plainly route information where it needs to go between networks.

## 4.4 Session Layer

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and terminal at layer 5. Session layer services also include authentication and reconnections.

## 4.5 Presentation Layer

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

## 4.6 Application Layer

At this layer, both the end client and the application layer interact directly with the software application. This layer sees network administrations gave to end-user applications like an internet browser or Office 365. The application layer recognizes communication partners, resource accessibility, and synchronizes communication

# 5. NETWORK TYPES AND TOPOLOGIES

A network is a collection of PCs, servers, mainframes, network devices, peripherals, or different devices associated with each other to permit the sharing of information.

There are Total 6 Topologies are there in Topology, Network topology describes the format or presence of network devices like PCs, links and different parts. components inside a data communication network are interconnected both physically and logically. The physical topology describes the way in which a network physically laid out and logical topology describes how data flow through the network.

.

## **5.1 Bus Topology**

Bus topology is a network type in which each PC and network devices is associated with single link. It communicates the information starting with one end then onto the next single way. Bi-directional feature isn't accessible in bus topology. At the point when the PC sends a message to the cable, every one of the computers get the data however the PC whose address matches with the signal acknowledges the data.

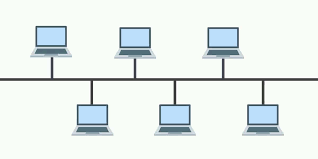


Fig1.Bus Topology

### 5.1.1 Advantages:

* The bus topology is easy to understand and install
* The cabling cost is low
* The bus topology is not difficult to extend

### 5.1.2 Disadvantages:

* Only one PC can send information at one time and others need to stand by till their turn comes.
* If the cable loose connection then it can cut down the entire network.
* The speed of bus topology is moderate because only one computer should send message at a time

## **5.2 Mesh Topology**

In mesh topology, every device is connected to another device via separate channels. These channels are known as links. If N no: of devices are connected to each other, then total number of ports required by each device is N-1 and total number of dedicated links required to connect them is NC2i.e. N(N-1)/2



Fig 2 Mesh Topology

### 5.2.1 Advantages:

* it gives security and protection.
* The failure of a single PC doesn't cut down the entire network.

### 5.2.2 Disadvantages:

* Cabling is more costly.
* The equipment cost to interface every device is costly
* Every system internally connects with each and every other system it leads to disadvantage

## **5.3 Ring Topology**

A ring topology is a network setup where device connections make a circular information way. Each arranged device is associated with two others, like focuses on a circle. Together, devices in a ring topology are referred to as a ring network. A Ring topology can be best described as devices associated with closed loop daisy chain. Information Transmission is unidirectional in ring topology.

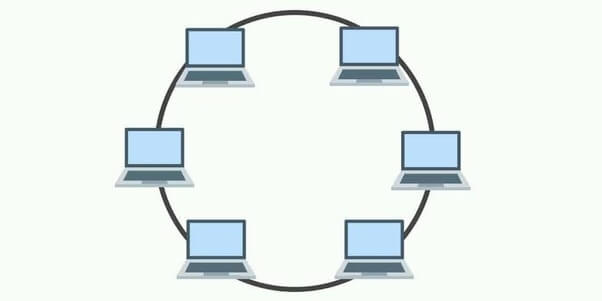


Fig 3 Ring Topology

### 5.3.1 Advantages:

* Ring networks can range over a more extended physical distance, as the nodes will recover the message as it is being passed across.
* Relatively reasonable and simple to assemble or expand a ring network, as it is basically placing the devices into a closed daisy chain.
* Adding more nodes won't slow down the whole network, as just nodes that have the token can send information.

### 5.3.2 Disadvantages:

* Depending on how the ring network is arranged, a single break in the network can actually still capacity regularly. However, with 2 broken hubs, the ring network will basically fall into 2 separate parts.
* It is an not an easy task to add or eliminate a node, as it will influence or affect the reset network.

## **5.4 Star Topology**

In a star topology, all the devices are connected to a central device known as hub This device will then control all the data traffic flow within the entire network.



Fig 4 Star Topology

### 5.4.1 Advantages:

* Relatively easy to set up and maintain – Just connect or disconnect devices from the central hub.
* A broken node will not affect the rest of the network.

### 5.4.2 Disadvantages:

* The network performance and the number of connections are limited by the central device.
* A good central hub or router can be very costly.
* Single point of failure. If the central node goes down, the entire network collapses.

## **5.5 Tree Topology**

In a tree topology, there is “top level node” followed by several “sub-level nodes” and “sub- sub-level nodes”, effectively forming a hierarchy.

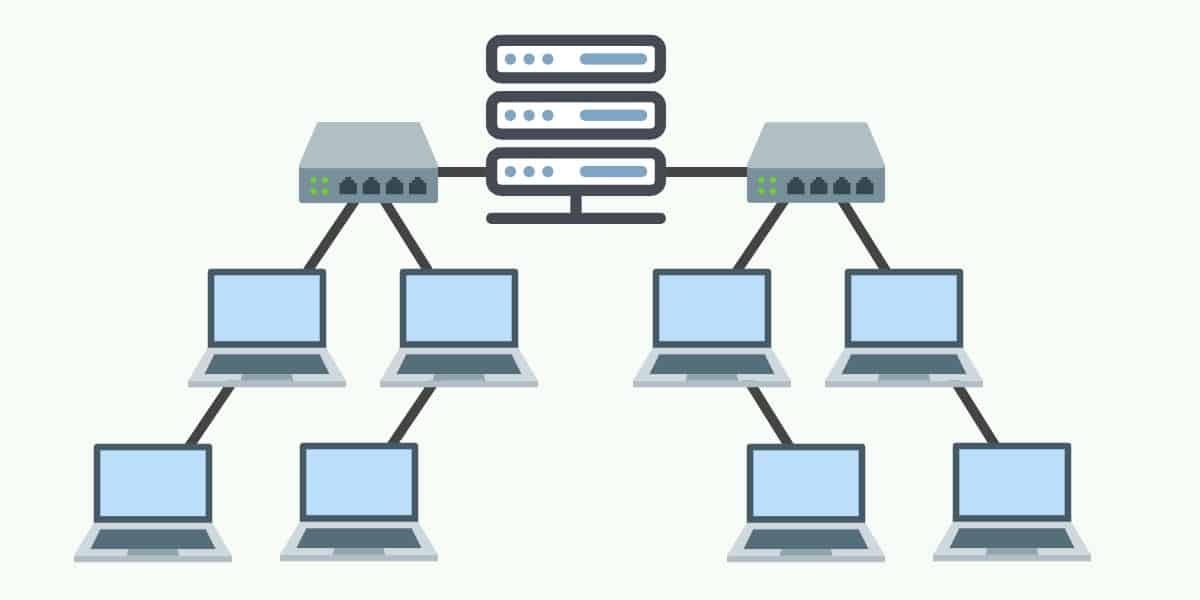


Fig 5 Tree Topology

### 5.5.1 Advantages:

* Good for large networks that are divided into groups.
* Easier to manage as the network is divided into segments.
* Quite robust when configured properly. If a break, it will not affect the rest of the network.

### 5.5.2 Disadvantages:

* Costly to build, as it involves a lot of network equipment and cables.
* Depending on how the tree network is built again – If the “top level node” or
* central hub goes down, the entire network can be cripple

## **5.6 Hybrid Topology**

A hybrid topology is a type of network topology that uses two or more differing network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology, and tree topology

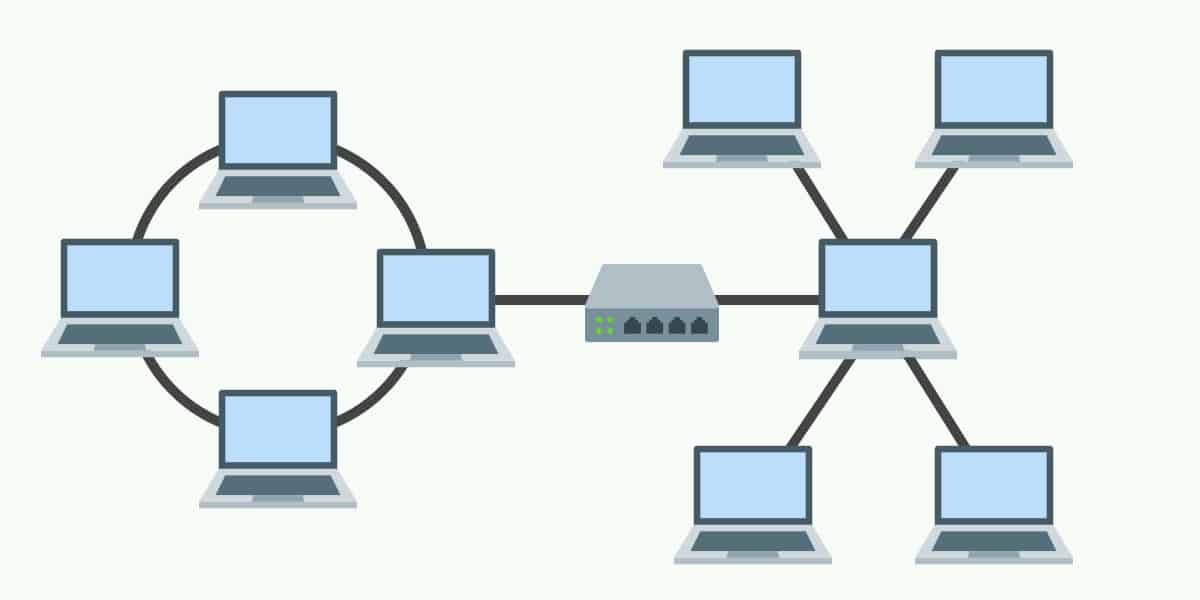


Fig 6 Hybrid Topology

### 5.6.1 Advantages:

* Flexible design.
* Scalable. Expand as the organization needs, and shrink if needed.

### 5.6.2 Disadvantages:

* Complex in design. The network engineer has to know various topologies and network gimmicks.
* May not be the most cost-effective, as it may involve the use of many different networking devices

# 6. PROTOCOLS

## **6.1 TCP Protocol**

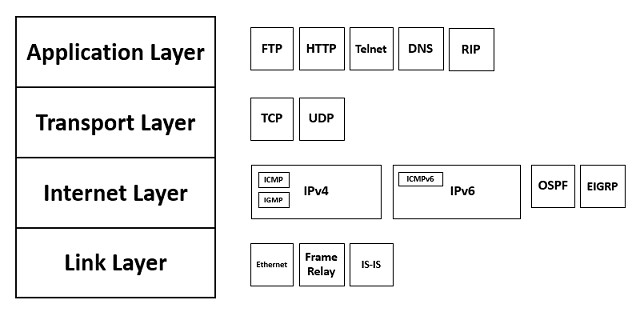
The Transmission Control Protocol (TCP) is a transport protocol that is utilized on top of IP to guarantee dependable transmission of packets. TCP includes components to solve many the issues that emerge from packets-based messaging, like lost packets, faulty packets, duplicate packets, and corrupted packets. Since TCP is the protocol utilized most normally on top of IP, the internet protocol stack is referred to as TCP/IP.

Fig TCP Header

## **6.2 UDP Protocol**

The UDP protocol allows the computer applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network. It provides an unreliable connection delivery service. It does not provide any services of IP except that it provides process-to-process communication. The UDP is a connectionless protocol as it does not create a virtual path to transfer the data. Hence it enables a faster transmission. The UDP message can be lost, delayed, duplicated, or can be out of order.

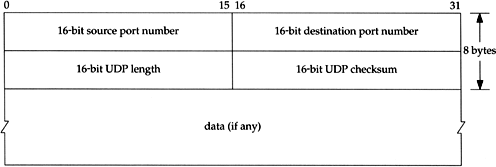


Fig UDP Header

**Difference Between TCP and UDP**

TCP is connection oriented protocol and UDP is connection less protocol

Data is Transmitted in corresponding manner in TCP which means packet arrive in order

At the receiver. But in UDP is different it is not follows any manner in data transmission

it should be managed by application layer.

## 6.3 IP Protocol

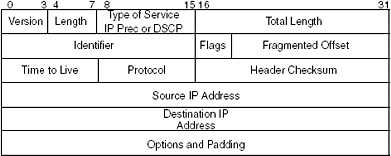


Fig IP Header

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing to packets of data that they can traverse through networks and arrive at the right destination. Data traverse the Internet is separated into more mode pieces, called packets. IP data is joined to every packet, and this data helps to routes with sending packets to the ideal packet Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives up where it is required.

## **6.4 L2 Protocols**

### 6.4.1 RARP (Reverse Address Resolution Protocol)

* A RARP demand is made and communicated on the local network.
* RARP stands for Reverse Address Resolution Protocol.
* It is utilized when a host knows its physical address, however has to know its assign IP address – no enough IP address to assign out to each station it needs to assign IP addresses on demand
* Another machine on the nearby network that realizes all the IP address to will react with a RARP reply
* It utilizes the physical address to get the logical address by using the RARP protocol.

### 6.4.2 ICMP (Internet Control Message Protocol)

* ICMP messages are separated into two general classifications: error-reporting messages and query messages
* The Internet Control Message Protocol (ICMP) is an network layer protocol utilized by network devices to analyze network communication issues.
* The error-reporting messages report issues that a router or a host (objective) may experience when it measures an IP packet.
* ICMP is used to decide if information is arriving at its expected destination in a timely manner.
* The query messages help a host or an network manager get specfic data from a router or another host.

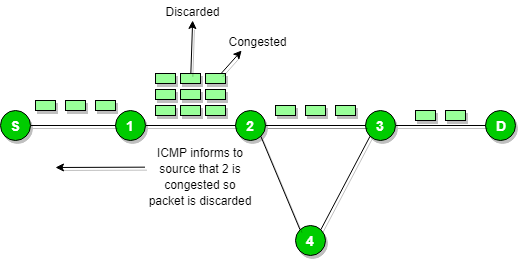
****

Fig ICM

### 6.4.3 DHCP (Dynamic Host Configuration Protocol)

* DHCP has a second information base with a pool of accessible IP addresses known as dynamic allocation.
* Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that naturally gives a Internet Protocol (IP) host with its IP address and other related configuration data, for example, the subnet cover and default gateway.
* When a DHCP customer demands a brief IP address, the DHCP worker goes to the pool of accessible (unused) IP addresses and assigns an IP address for a negotiable period
* DHCP gives static and dynamic location distribution that can be manual or automatic.
* A DHCP server has an database that statically ties actual addresses to IP addresses known as static allocation.

### 6.4.4 ARP (Address Resolution Protocol)

* ARP stands for Address Resolution Protocol.
* ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.
* The response packet contains the recipient's IP and physical addresses
* An ARP packet is encapsulated directly into a data link frame.
* The type field indicates that the data carried by the frame are an ARP packet
* The host or the router sends an ARP query packet - query is broadcast over the network
* The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
* Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.

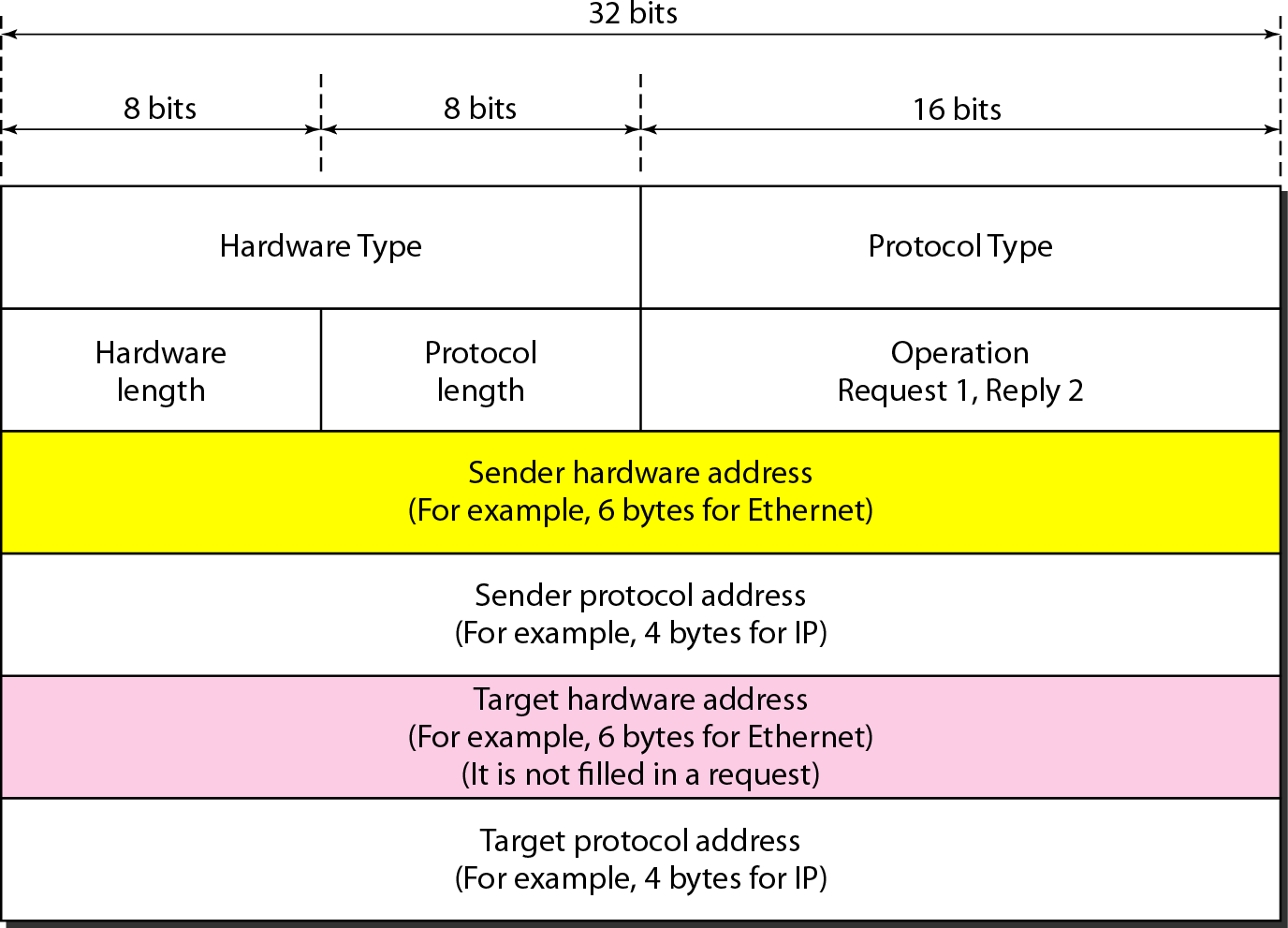


Fig ARP Packet Format

**6.5 L3 Protocols**

### 5.5.1 BGP (Border Gateway Protocol)

* + - Border Gateway Protocol (BGP) is utilized to Exchange routing data for the web and is the protocol utilized between ISPs.
    - To establish a solid climate, BGP utilizes the services of TCP.
    - The fundamental job of BGP is to give communication between two self-sufficient systems.
    - BGP supports Next-Hop Paradigm.
    - BGP converse Data transmission.
    - In BGP protocol, the way among source and destination (list of autonomous system) is addressed as list of attributes. Each property gives some data about the path.

### 6.5.2 RIP (Routing Information Protocol)

* + - Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to track down the best way between the source and the destination network.
    - It communicates the routing updates to the whole networks that makes a great deal of traffic.
    - Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
    - The metric used by RIP is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a **hop count**.
    - Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count a routing metric to track down the best way between the source and the objective organization.

### 6.5.3 EIGRP (Enhanced Interior Gateway Routing)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is utilized to track down the best way between any two layer-3 devices deliver the packet. EIGRP deals with network layer protocol of OSI model and uses the protocol number 88. It uses a few messages to communicate with the neighbor devices that works EIGRP.

These are: -

* Hello message
* Full Update
* Partial update
* Query message
* Reply message
* Acknowledgement message
* Null Update

## **6.6 Types of WLAN Protocols**

IEEE 802.11 or Wi-Fi has many variations, the main among which are −

* **5.6.1 802.11a Protocol−** This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
* **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
* **802.11g Protocol −** This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
* **802.11n Protocol −** Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive

# 7. IP ADDRESS

## 6.1 IPV4

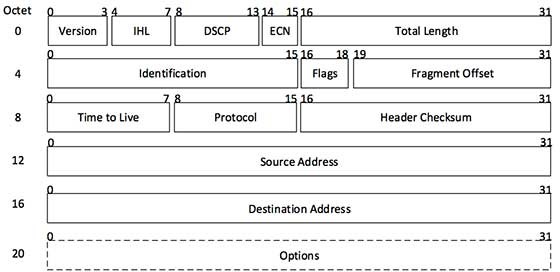
IP stands for Internet Protocol and v4 stands for version 4.I P version four addresses are 32-bit integers which will be expressed in hexadecimal notation.

### 7.1.2 Parts of IPv4:

* Network Part: - The network part demonstrates the particular assortment that is designated to the network. The network part conjointly distinguishes the category of the network that is assigned.
* Host Part: - host part remarkably recognizes the machine on your network. This a part of the IPv4 address is assigned to each host. For each host on the network, the network part is something similar, be that as it may, the host half should increase.
* Subnet number: - Local networks that have enormous quantities of hosts are separated into subnets and subnet numbers are selected to that.

### 7.1.3 Characteristics of IPv4:

* IPv4 uses 32-bit addressing which allows a total of 4,294,967,296 (2^32) addresses.
* Some addresses are reserved for public and private networks.
* An IP address consists of four octets which are separated by a period, which is also known as *dotted-decimal notation.*
* In the total no: of host IP addresses, the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

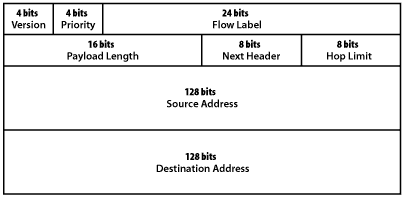


## 7.2 IPV6

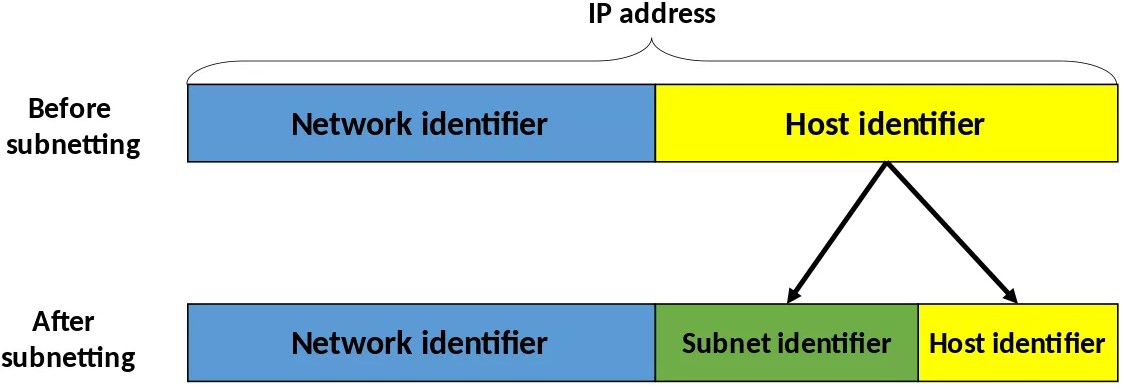
IPv6 was developed to deal with the problem of IP v4 exhaustion. IPv6 is 128-bits address having an address space of 2^128, which is bigger than IPv4. In IPv6 Colon-Hexa representation is used.

There are 8 groups and each group represents 2 Bytes. In IPv6 representation, we have three addressing methods

* + **Unicast Address:** Unicast Address recognizes a solitary organization interface. A packet sent to unicast address is conveyed to the interface recognized by that address.
  + **Multicast Address:** Multicast Address is utilized by various hosts, called as Group, secures a multicast destination address. On the off chance that any packet is sent this multicast address, it will be circulated to all interfaces relating to that multicast address.
  + **Anycast Address:** Anycast Address is assigned to a group of interfaces.

****

## 7.3 SUBNETTING THEORY



Subnetting is the practice of dividing a network into two or more smaller networks to increase the routing efficiency and the security of the network and thereby reducing the size of the broadcast domain. Applying the subnet mask to an IP address splits the address into two parts, an extended network address and a host address.

Subnetting is used for: - Organizing a network in an efficient way is crucial for large firms and those companies seeking to expand technologically. IP addresses can be kept geographically localized meaning that a subnet can be used for specific staffing structures to maintain efficiency and order.

Benefits of Subnetting divides broadcast domains, meaning that traffic is routed efficiently, improving speed and network performance.

This reduces major congestion and reduces the load imparted on the network. With sub-networks, less distance needs to be traveled by data packets, enhancing network performance.

# ****8. Network Security:****

Network security is a wide term that covers many innovations, gadgets and processes. In its most

straightforward term, it is a bunch of rules and setups intended to ensure to protect integrity, privacy and

accessibility of PC network and information utilizing both programming and hardware innovations.

## 8.1 **Firewall**:

Firewall’s control approaching and active traffic on networks, with foreordained security rules. Firewalls keep out threatening traffic and is a vital piece of day-by-day processing. Network Security depends vigorously on Firewalls, and particularly cutting-edge firewalls which center around obstructing malware and application-layer attacks.

## 8.2 **Encryption:**

Encryption is an interaction that encodes a message or document so it very well may be just be

perused by specific individuals. Encryption utilizes a calculation to scramble, or encode, information

and afterward utilizes a key for the accepting party to unscramble, or decode, the data. The

message contained in a scrambled message is alluded to as plaintext. In its encoded,

indistinguishable structure it is referred to as ciphertext

### 8.2.1 How Encryption Works:

Encryption utilizes algorithms to scramble your data. It is then sent to the getting party, who can interpret the message with a key. There are numerous sorts of algorithms, which all include various methods of scrambling and afterward unscrambling data.

## 8.3 **Cryptography**:

The motivation behind cryptography is to shroud the substance of messages by encoding them to make them unrecognizable besides by somebody who has been given an description key. The reason for cryptanalysis is then to defeat this by discovering approaches to decode messages without being given the key.

## 8.4 **Overflows**:

Overflows can be caused deliberately by hackers and then exploited to run malicious code.

There are two types of overflows: stack and heap. The stack and the heap are two areas of the memory structure that are allocated when a program is run. Function calls are stored in the stack, and dynamically allocated variables are stored in the heap. An amount of memory is allocated to the buffer. Static variable storage (variables defined within a function) is referred to as stack, because they are stored on the stack in memory. Heap data is the memory that is dynamically allocated at runtime, such as by C's malloc () function.

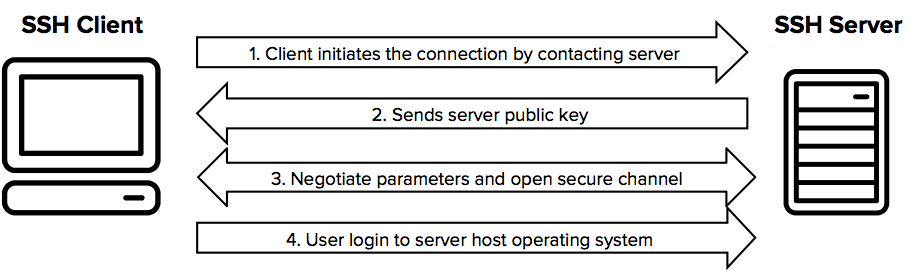
## 8.5 **SSH PROTOCOL**

SSH (also known as the Secure Shell or **Secure Socket Shell**) can be defined as a **cryptographic network protocol**. SSH aims to give the users (mostly the system administrators) a secure means to reach a computer within a network.

Although SSH is often used for applications like remote login, remote command line and remote command execution, almost all network services can be secured with the use of SSH. Secure Socket Shell employs the **public-key cryptography** methods to carry out **authentication** processes for the remote computer.

SSH offers two main functions:

* Logging on to remote systems and running terminal sessions, remote commands and such on these remote systems.
* Transferring files between remote systems on the same network.



It always comes in key pair:

* **Public key –** Everyone can see it, no need to protect it. (for encryption function)
* **Private key –** Stays in computer, must be protected. (for decryption function)

Key pairs can be of the following types:

* **User Key –** If public key and private key remain with the user.
* **Host Key –** If public key and private key are on a remote system.
* **Session key –** Used when large amount of data is to be transmitted.

**How SSH Works?**

It uses asymmetric cipher for performing encryption and decryption. There are many encryption methods:rsa, dsa, ed25519 etc.

General procedure is: -

* Public keys from the local computers (system) are passed to the server which is to be accessed.
* Server then identifies if the public key is registered. If so, the server then creates a new secret key and encrypts it with the public key which was send to it via local computer.
* This encrypted code is sent to the local computer. This data is unlocked by the private key of the system and is send to the server.
* Server after receiving this data verifies the local computer.
* SSH creates a route and all the encrypted data are transferred through it with no security issues.

SSH is key based authentication that is not prone to [brute-force attack](https://en.wikipedia.org/wiki/Brute-force_attack).  
It is more convenient and secure than login ids and passwords (which can be stolen in middle). There is no exposure of valid credentials, if a server has been compromised.

**Generating an SSH key pair:**

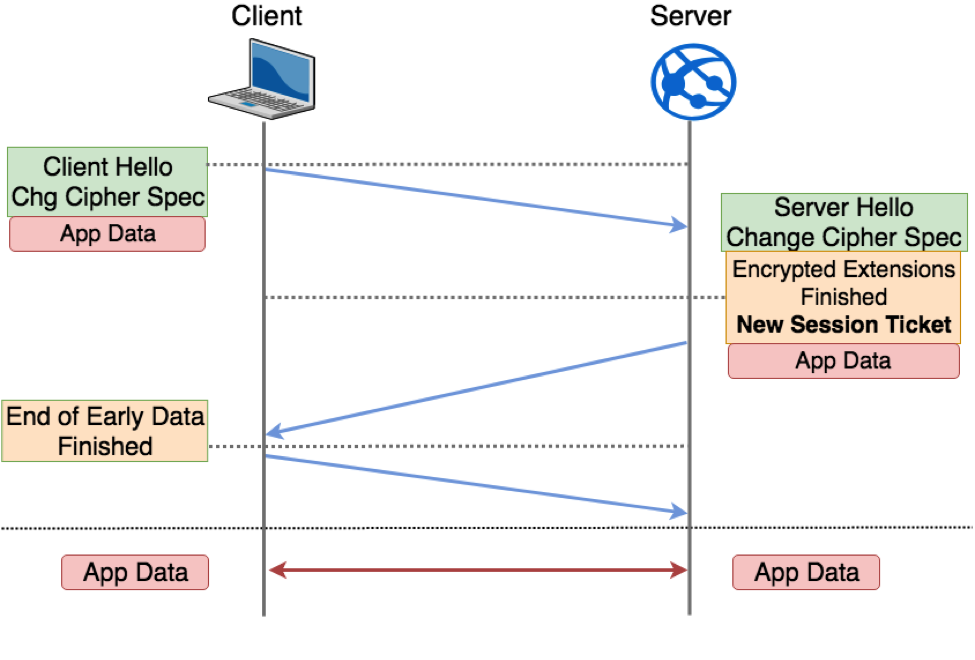
* Open your command prompt
* type: ssh-keygen
* Press enter
* It will ask you for a location. Press Enter for default location.
* If it’s already there, press 'y' to overwrite.
* You may enter passphrase as you like, press enter.
* **Generating SSH keys on Windows, Linux and Mac:**
* OMAC OsX and Linux: terminal (build in)

## 8.6 TLS PROTOCOL

TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is [an IETF standard](https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html) intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP

There are several benefits of TLS:

* **Encryption:** TLS/SSL can help to secure transmitted data using encryption.
* **Interoperability:** TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
* **Algorithm flexibility:** TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
* **Ease of Deployment:** Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
* **Ease of Use:** Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

****

## 8.7 MTLS:

Server-to-server connections rely on MTLS for mutual authentication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other. In Skype for Business Server deployments, certificates issued by the enterprise CA that are during their validity period and not revoked by the issuing CA are automatically considered valid by all internal clients and servers because all members of an Active Directory domain trust the Enterprise CA in that domain. In federated scenarios, the issuing CA must be trusted by both federated partners. Each partner can use a different CA, if desired, so long as that CA is also trusted by the other partner. This trust is most easily accomplished by the Edge Servers having the partner's root CA certificate in their trusted root CAs, or by use of a third-party CA that is trusted by both parties.

# 9. Classful Network

In Network Classful Addressing the 32 bit IPv4 address is divided into 5 Different

Classes

## **9.1 Class A: -**

* Which Network consist large no. of Hosts for that Network Class A IP Address will be assign
* In Class A Start Address is: - 0.0.0.0

End Address is: - 127.255.255.255

* In Class A Network id is 8 bit long and Host id is 24 bit long
* Total Address in Class is 2^31
* In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID.

## **9.2 Class B: -**

* Which Network has a range from small sized large sized network for that network Class B IP Address will be assign
* In Class B Start Address is: - 128.0.0.0

End Address is: - 191.255.255.255

* In Class B Network id is 16 bit long and Host id is 16 bit long
* Total Address in Class is 2^30
* In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID.

## **9.3 Class C: -**

* Which Network is very small for that network Class C IP Address will be assign
* In Class C Start Address is: - 192.0.0.0

End Address is: - 223.255.255.255

* In Class C Network id is 24 bit long and Host id is 8 bit long
* Total Address in Class is 2^29
* In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID.

## **9.4 Class D: -**

* Class D IP Address in specially assigned for Multicast Address
* In Class D Start Address is: - 224.0.0.0

End Address is: - 239.255.255.255

* In Class D Network id is **not defined** and Host id is **not defined**
* Total Address in Class is 2^28
* The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

# 10 NETWORK TOOLS

## 10.1 Packet Tracer

Packet Tracer is a cross-stage visual simulation instrument designed by Cisco Systems that permits clients to make network geographies and emulate modern PC networks. The product permits clients to simulate the setup of Cisco switches and switches utilizing a simulated command line interface. Packet Tracer utilizes a simplified UI, permitting clients to add and eliminate simulated network devices as they see fit. The product is mainly engaged towards Certified Cisco Network Associate Academy students as an instructive apparatus for assisting them with learning principal CCNA concepts. Beforehand students joined up with a CCNA Academy program could unreservedly download and utilize the tool free for instructive use.

## 10.2 Wireshark

Wireshark is a free and open-source packet analyzer. It is utilized for network investigating, examination, programming and communication protocol development, and instruction. Initially named Ethereal, the project was renamed Wireshark in May 2006 because of brand name issues. Wireshark is cross-stage, utilizing the Qt widget toolbox in current deliveries to execute its UI, and utilizing pcap to catch packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like working frameworks, and Microsoft Windows. There is additionally a terminal-based (non-GUI) variant called T Shark.

# 11 Activity

## 11.1 IPv4 Subnetting

Class A:

Design 4 Network for 20.120.30.20/22

CIDR = n+22 = 22+3 = 25

Number of Host = 2^7 -2 =126

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network 1 | Network 2 | Network 3 | Network 4 |
| Network ID | 20.120.28.0 | 20.120.29.0 | 20.120.30.0 | 20.120.31.0 |
| Host ID | 20.120.28.1  ‘  ‘  20.120.28.254 | 20.120.29.1  ‘  ‘  20.120.29.254 | 20.120.30.1  ‘  ‘  20.120.30.254 | 20.120.31.1  ‘  ‘  20.120.31.254 |
| Broadcast ID | 20.120.28.255 | 20.120.29.255 | 20.120.30.255 | 20.120.31.255 |

Class B:

Design 5 Network for 172.12.4.10/24

CIDR = n+24 = 24+3 = 27

Number of Host = 2^5 -2 =30

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Network 1 | Network 2 | Network 3 | Network 4 | Network 5 |
| Network ID | 172.12.4.0 | 172.12.4.32 | 172.12.4.64 | 172.12.4.96 | 172.12.4.128 |
| Host ID | 172.12.4.1  ‘  ‘  172.12.4.30 | 172.12.4.33  ‘  ‘  172.12.4.62 | 172.12.4.65  ‘  ‘  172.12.4.94 | 172.12.4.97  ‘  ‘  172.12.4.126 | 172.12.4.129  ‘  ‘  172.12.4.158 |
| Broadcast ID | 172.12.4.31 | 172.12.4.63 | 172.12.4.95 | 172.12.4.127 | 172.12.4.159 |

Class C:

Design 3 Network for 197.30.4.60/21

CIDR = n+24 = 21+2 = 23

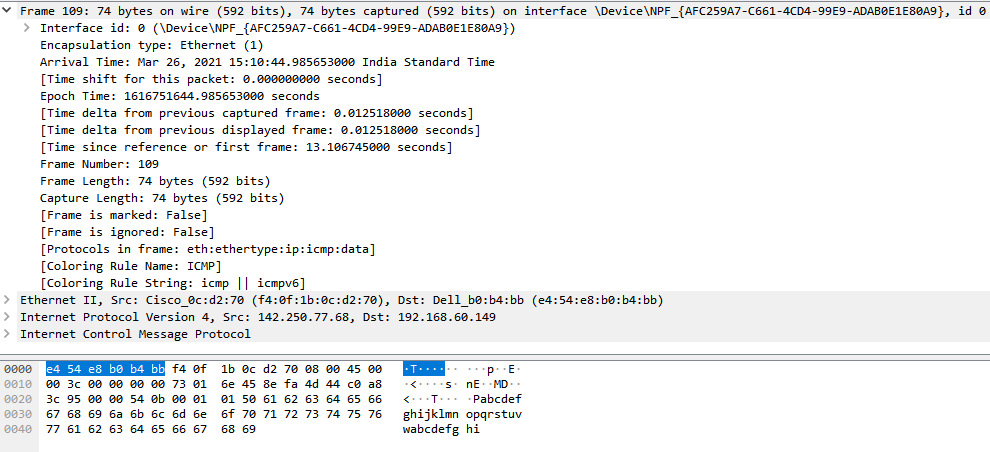
Number of Host = 2^9 -2 =510

|  |  |  |  |
| --- | --- | --- | --- |
|  | Network 1 | Network 2 | Network 3 |
| Network ID | 197.30.0.0 | 197.30.2.0 | 197.30.4.0 |
| Host ID | 197.30.0.1  ‘  ‘  197.30.1.254 | 197.30.2.1  ‘  ‘  197.30.3.254 | 197.30.4.1  ‘  ‘  197.30.5.254 |
| Broadcast ID | 197.30.1.255 | 197.30.3.255 | 197.30.5.255 |

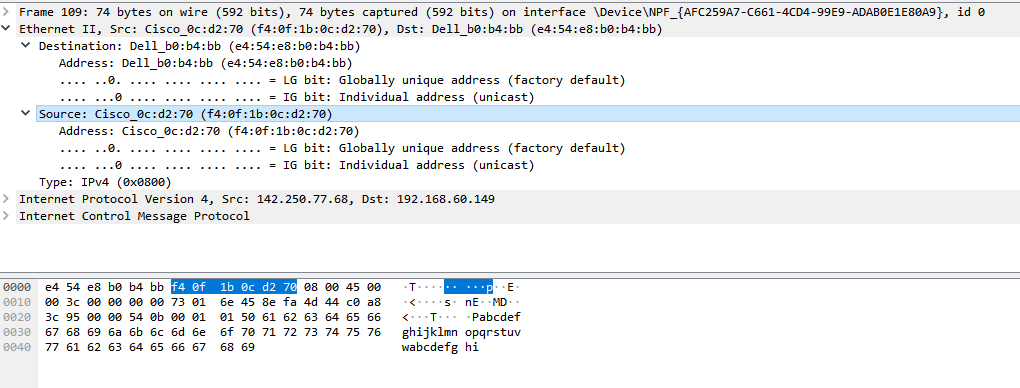
## 11.3 Wireshark

Wireshark is a free and open-source packet analyzer. It is utilized for network investigating, examination, programming and communication protocol development, and instruction. Initially named Ethereal, the project was renamed Wireshark in May 2006 because of brand name issues. Wireshark is cross-stage, utilizing the Qt widget toolbox in current deliveries to execute its UI, and utilizing pcap to catch packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like working frameworks, and Microsoft Windows. There is additionally a terminal-based (non-GUI) variant called T Shark

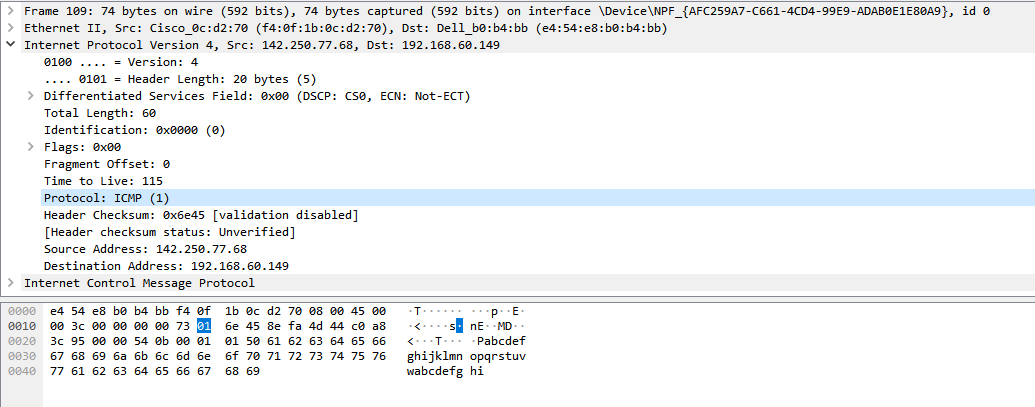
1.ping [www.google.com(frame)](http://www.google.com(frame)):



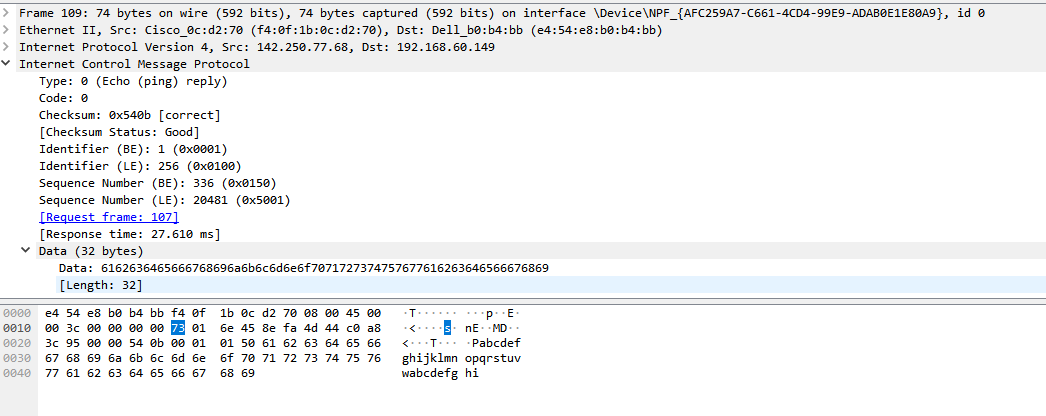
2.ping [www.google.com(Ethernet)](http://www.google.com(Ethernet)):



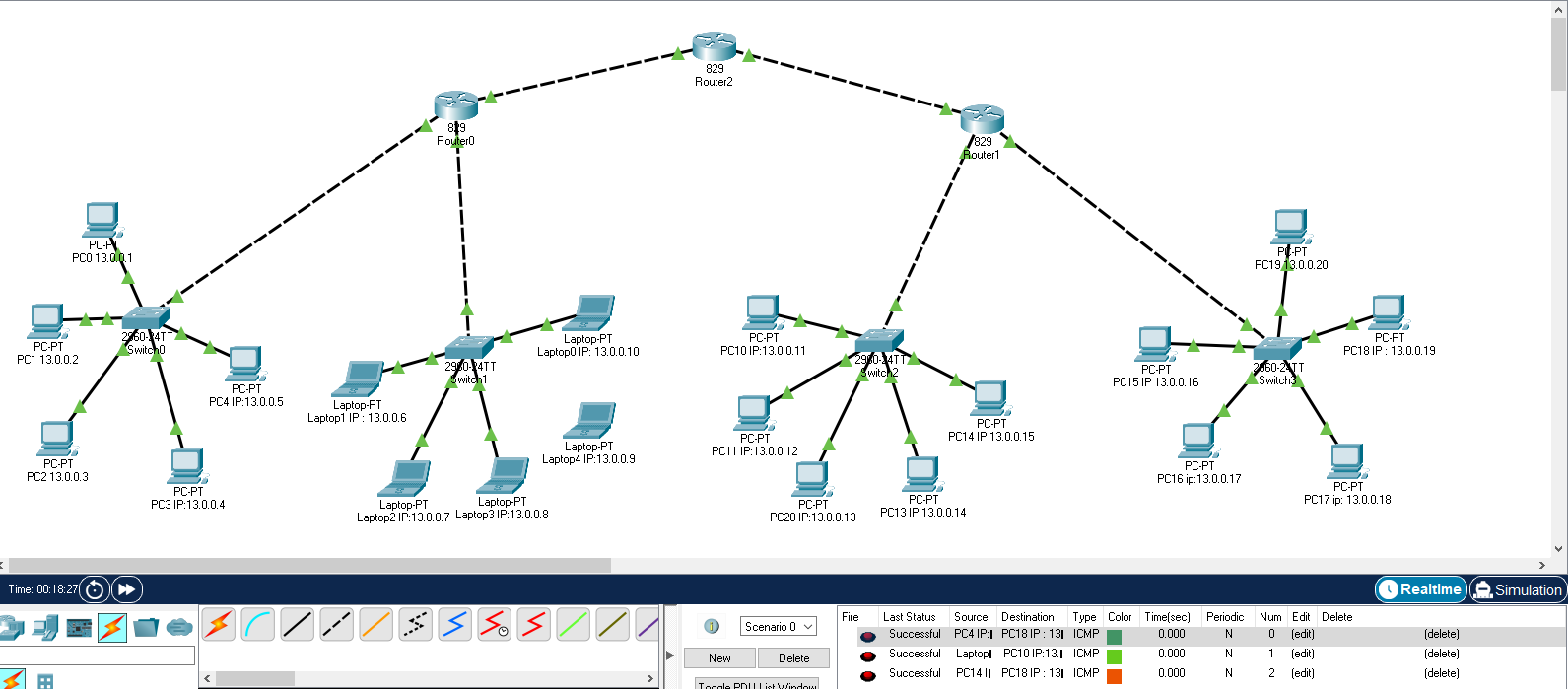
3.ping [www.google.com(IPv4)](http://www.google.com(IPv4)):

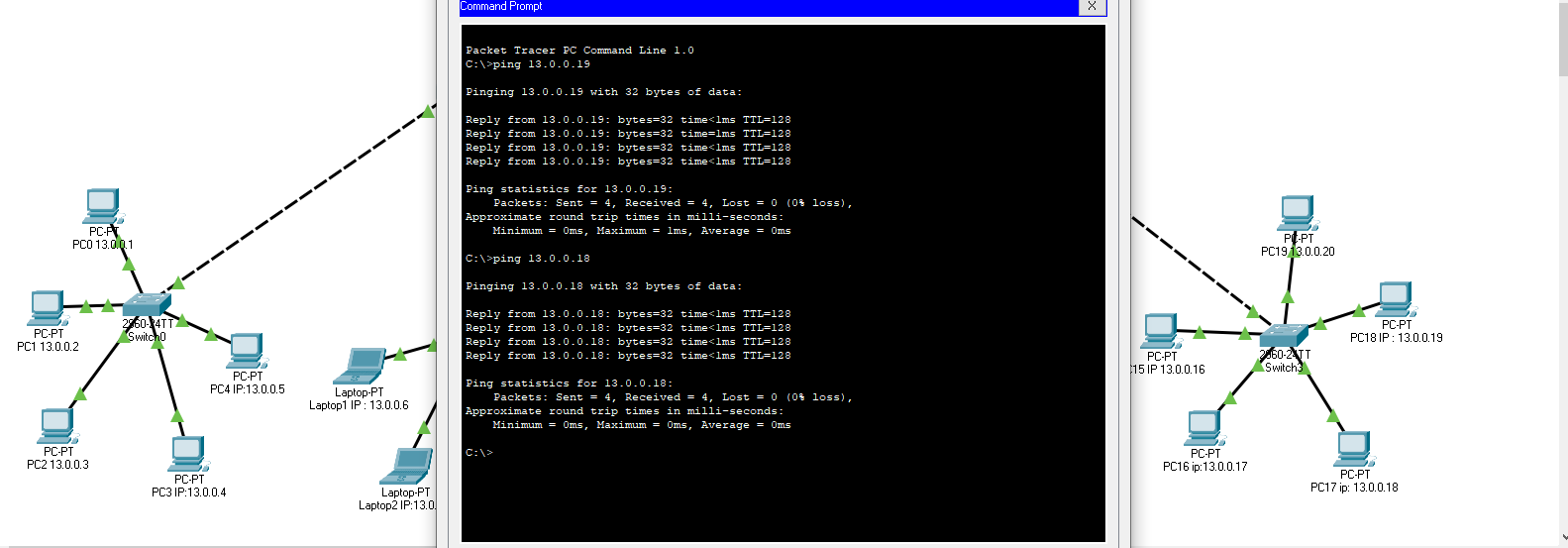


4. ping [www.google.com(ICMP)](http://www.google.com(ICMP)):



## 11.4 PACKET TRACER





# 12. END -TO -END DATA FLOW

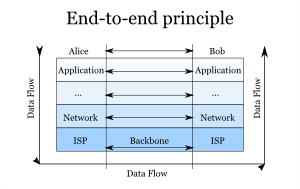


Fig End-To-End

* Application layer of both sender and receiver acts as interface between user and machine or system.
* Presentation layer present data to a uniform format to Session layer while sending and to Application Layer while receiving by encrypting and decrypting data.
* Session Layer provides orderly communication between devices by regulating the flow of data.
* Transport Layer manages end to end message delivery in a network.
* Network Layer determines how data packets is transmitted to different networks.
* Data link layer is responsible for reliable node-to-node delivery of data. It receives the data from network layer and creates frames, add physical address to these frames and pass them to physical layer. The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. Data Link layer defines the format of data on the network.

# 13. REFRENCES

<https://www.guru99.com/data-communication-computer-network-tutorial.html><https://en.wikipedia.org/wiki/IPv6>

<https://en.wikipedia.org/wiki/Wireshark>

<https://www.javatpoint.com/osi-model>

<https://en.wikipedia.org/wiki/Packet_Tracer>