./

Learning Report – Applied System Development Life Cycle and Software Testing



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be approved By** | **Remarks/Revision Details** |
| 1 |  | Name/PS No | Name/PS No | Module Owner Name | Comments |
| 2 | 22/ | Nitin N Shetty |  |  |  |
| 3 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Document History**

Contents

[1.Network Classification 5](#_Toc67589669)

[1.1 PAN 5](#_Toc67589670)

[1.2 LAN 6](#_Toc67589671)

[1.3 WAN 6](#_Toc67589672)

[1.4 MAN 6](#_Toc67589673)

[1.5 WLAN 6](#_Toc67589674)

[1.6 WIFI 7](#_Toc67589675)

[1.7 WIMAX 7](#_Toc67589676)

[2. Components of Network: - 7](#_Toc67589677)

[2.1 Work Stations 8](#_Toc67589678)

[2.2 File Servers 8](#_Toc67589679)

[2.3 Gateway 8](#_Toc67589680)

[2.4 NIU [Network Interface Unit] 8](#_Toc67589681)

[2.5 HUB 9](#_Toc67589682)

[2.6 Communication Channel / LAN Channels 9](#_Toc67589683)

[2.7 Switch 9](#_Toc67589684)

[2.8 Bridge 10](#_Toc67589685)

[2.9 Access Points 10](#_Toc67589686)

[3. OSI MODEL 10](#_Toc67589687)

[3.1 Physical Layer 11](#_Toc67589688)

[3.2 Data link layer 11](#_Toc67589689)

[3.3 Transport Layer 12](#_Toc67589690)

[3.4 Session Layer 12](#_Toc67589691)

[3.5 Presentation Layer 12](#_Toc67589692)

[3.6 Application Layer 12](#_Toc67589693)

[4. NETWORK TYPES AND TOPOLOGIES 13](#_Toc67589694)

[4.1 Bus Topology 13](#_Toc67589695)

[4.1.1 Advantages: 13](#_Toc67589696)

[4.1.2 Disadvantages: 14](#_Toc67589697)

[4.2 Mesh Topology 14](#_Toc67589698)

[4.2.1 Advantages: 14](#_Toc67589699)

[4.2.2 Disadvantages: 15](#_Toc67589700)

[4.3 Ring Topology 15](#_Toc67589701)

[4.3.1 Advantages: 15](#_Toc67589702)

[4.3.2 Disadvantages: 16](#_Toc67589703)

[4.4 Star Topology 16](#_Toc67589704)

[4.4.1 Advantages: 17](#_Toc67589705)

[4.4.2 Disadvantages: 17](#_Toc67589706)

[4.5 Tree Topology 17](#_Toc67589707)

[4.5.1 Advantages: 18](#_Toc67589708)

[4.5.2 Disadvantages: 18](#_Toc67589709)

[4.6 Hybrid Topology 18](#_Toc67589710)

[4.6.1 Advantages: 19](#_Toc67589711)

[4.6.2 Disadvantages: 19](#_Toc67589712)

[5. PROTOCOLS 19](#_Toc67589713)

[5.1 TCP Protocol 19](#_Toc67589714)

[5.2 UDP Protocol 20](#_Toc67589715)

[5.3 IP Protocol 21](#_Toc67589716)

[5.4 L2 Protocols 21](#_Toc67589717)

[5.4.1 RARP (Reverse Address Resolution Protocol) 21](#_Toc67589718)

[5.4.2 ICMP (Internet Control Message Protocol) 22](#_Toc67589719)

[5.4.3 DHCP (Dynamic Host Configuration Protocol) 23](#_Toc67589720)

[5.4.4 ARP (Address Resolution Protocol) 23](#_Toc67589721)

[5.5 L3 Protocols 24](#_Toc67589722)

[5.5.1 BGP (Border Gateway Protocol) 24](#_Toc67589723)

[5.5.2 RIP (Routing Information Protocol) 25](#_Toc67589724)

[5.5.3 EIGRP (Enhanced Interior Gateway Routing) 25](#_Toc67589725)

[5.6 Types of WLAN Protocols 26](#_Toc67589726)

[6. IP ADDRESS 26](#_Toc67589727)

[6.1 IPV4 26](#_Toc67589728)

[6.1.2 Parts of IPv4: 26](#_Toc67589729)

[6.1.3 Characteristics of IPv4: 27](#_Toc67589730)

[6.2 IPV6 27](#_Toc67589731)

[ 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. 28](#_Toc67589732)

[ 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. 28](#_Toc67589733)

[ Benefits of Subnetting divides broadcast domains, meaning that traffic is routed efficiently, improving speed and network performance. 28](#_Toc67589734)

[ 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. 28](#_Toc67589735)

[Network Security: 29](#_Toc67589736)

[Firewall: 29](#_Toc67589737)

[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. 29](#_Toc67589738)

[How Encryption Works 29](#_Toc67589739)

[Cryptography: 29](#_Toc67589740)

[Packet Tracer 32](#_Toc67589741)

[Wireshark 32](#_Toc67589742)

# 1.Network Classification

## 1.1 PAN

* 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

* 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

* 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

* 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

* 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

* 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 PC which solicitations admittance to the LAN and change administrations to reacts the solicitations by means of change to perform devoted undertaking with having upgraded highlights. In workstation, Tasks are in types of Business, designing and so forth and in this Illustrations, UI is pre-introducing in light of the fact that it's anything but a discretionary to the workstation. A workstation is a unique PC intended for specialized or logical applications. Expected principally to be utilized by each individual 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 document frameworks or if nothing else parts of a document framework to associated customers. Record workers accordingly offer clients a focal stockpiling place for documents on inside information media, which is open to all approved customers. Here, the worker director characterizes exacting principles in regards to which clients have which access rights: For example, the design or document approvals of the separate record framework empower 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 an organization hub that shapes a section between two organizations working with various transmission conventions. The most widely recognized sort of passages, the organization door works at layer 3, for example network layer of the OSI (open frameworks interconnection) model. In any case, contingent on the usefulness, an entryway can work at any of the seven layers of OSI model. It goes about as the passage – leave point for an organization since all traffic that streams across the organizations should go through the entryway. 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 correspondence between the worker and the workstations or hubs. An independent PC or a PC that isn't joined to any arrange, lives in its own reality and does its assignments with its own inbuilt assets. Be that as it may, when it turns into a Workstation then it needs an interface to help set up an association with the organization on the grounds that without this the workstation or hub won't share network assets. You can likewise say that, an Network Interface Unit(NIU) is an essentially a gadget that joined to every one of the work station and the worker, and helps workstation and the worker and assists workstation with setting up the immensely significant association with the organization

## 2.5 HUB

A hub, also called a network hub, additionally called an organization center, is a typical association point for gadgets in an organization. Center points are gadgets usually used to interface sections of a LAN. The center point contains different ports. At the point when a parcel shows up at one port, it is duplicated to different ports so that all sections of the LAN can see all bundles. In a center, a casing is communicated to all of its ports. The center point has no chance to get of recognizing which port an edge ought to be shipped off. Giving it to each port guarantees that it will arrive at its proposed objective. This spot a ton of traffic on the arrange and can prompt helpless organization reaction times An extension is an organization gadget that interfaces various LANs (Local Area Network) together to shape a bigger LAN. The way toward accumulating networks is called network bridging

An extension interfaces the various segments with the goal that they show up as parts of a solitary organization. Scaffolds work at the information interface layer of the OSI model and henceforth likewise alluded as Layer 2 switches. Since they work at information interface layer, they send information as information outlines. On getting an information outline, the scaffold counsels a data set to conclude whether to pass, communicate or dispose of the edge. On the off chance that the casing has an objective Macintosh (media access control) address in a similar organization, the scaffold passes the edge to that hub and afterward disposes of it. On the off chance that the edge has an objective Macintosh address in an associated network, it will advance the casing toward it.

## 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 basic to the adequacy of correspondence. Stations incorporate oral methods, for example, calls and introductions, and composed modes like reports, reminders, and email.

Communication channels vary along a scale from rich to lean. Consider how you would choose a steak — some have more fat than others; they are rich and brimming with flavor and body. Assuming, notwithstanding, you are on a careful nutritional plan and simply need the meat, you will choose a lean steak. Correspondence channels are the comparable: rich channels are more intuitive, give freedoms to two-way correspondence, and permit both the sender and beneficiary to peruse the nonverbal messages

## 2.7 Switch

In networks the switch is the gadget that channels and advances bundles between LAN portions. Switches work at the information interface layer(layer 2) and now and again the organization layer(layer 3) of the OSI Reference Model and consequently support any parcel convention. LANs that utilization changes to join fragments are called exchanged LANs or for Ethernet Organizations, exchanged Ethernet LANs. Switches encourage the sharing of assets by interfacing every one of the gadgets, Including PCs, printers, and workers, in a private company organization. Building an independent venture network Is beyond the realm of imagination without changes to gadget together.

## 2.8 Bridge

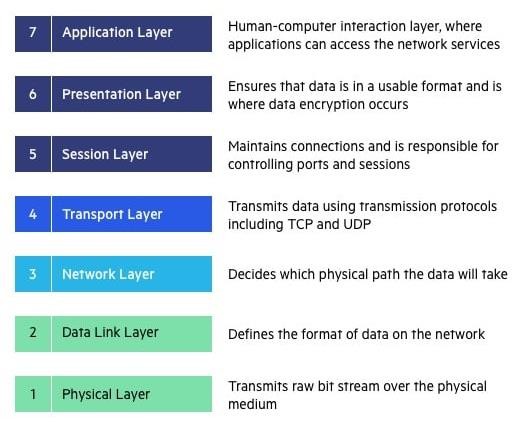
A bridge network is that associates numerous LANs (Neighborhood) together to frame a bigger LAN. The way toward collecting networks is called network crossing over. An extension associates the various segments so they show up as parts of a solitary organization. Scaffolds work at the information interface layer of the OSI model and subsequently additionally alluded as Layer 2 switches.

Since they work at information interface layer, they communicate information as information outlines. On accepting an information outline, the extension counsels a data set to conclude whether to pass, send or dispose of the edge. On the off chance that the edge has an objective Macintosh (media access control) address in a similar organization, the scaffold passes the casing to that hub and afterward disposes of it. On the off chance that the edge has an objective Macintosh address in an associated network, it will advance the casing toward it.

## 2.9 Access Points

A access-point is a gadget that wireless local area network, or WLAN, typically in an office or enormous structure. A passage associates with a wired switch, switch, or center through an Ethernet link, and tasks a Wi-Fi signal to an assigned zone.

# 3. OSI MODEL



The OSI Model (Open Systems Interconnection Model) s 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.

## 3.1 Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically communicating crude unstructured information bits across the organization from the actual layer of the sending gadget to the actual layer of the accepting gadget. It can incorporate determinations like voltages, pin format, cabling, and radio frequencies. At the actual layer, one may discover "physical" resources, for example, network centers, cabling, repeaters, network connectors or modems.

## 3.2 Data link layer

The data link layer, straightforwardly associated nodes are utilized to perform hub to-hub information move where information is bundled into outlines. The information connect layer likewise revises blunders that may have happened at the actual layer.

The information connect layer incorporates two sub-layers of its own. The first, media access control (MAC), gives stream control and multiplexing to gadget transmissions over an organization. The second, the consistent connection control (LLC), gives stream and mistake control over the actual medium just as distinguishes line conventions. **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.

## 3.3 Transport Layer

The organization layer is liable for getting outlines from the information connect layer, and conveying them to their proposed objections among dependent on the tends to contained inside the edge. The organization layer finds the objective by utilizing legitimate locations, like IP (internet protocol). At this layer, switches are an essential segment used to plainly course data where it needs to go between networks.

## 3.4 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.

## 3.5 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.

## 3.6 Application Layer

At this layer, both the end client and the application layer collaborate straightforwardly with the product application. This layer sees network administrations gave to end-client applications like an internet browser or Office 365. The application layer recognizes correspondence accomplices, asset accessibility, and synchronizes correspondence

# 4. NETWORK TYPES AND TOPOLOGIES

A network is a collection of PCs, workers, centralized computers, network gadgets, peripherals, or different gadgets associated with each other to permit the sharing of information.

There are Total 6 Topologies are there in Topology, Network topology portrays the format or presence of organization gadgets like PCs, links and different parts. Parts inside an information correspondence network are interconnected both genuinely and sensibly. The actual geography portrays the manner by which an organization genuinely spread out and intelligent geography depicts how information move through the organization.

## 4.1 Bus Topology

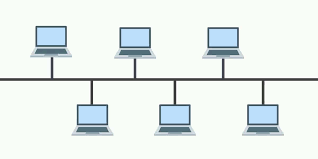
 Bus topology is a network type in which each PC and organization gadget is associated with single link. It communicates the information starting with one end then onto the next single way. Bi-directional component isn't accessible in bus topology. At the point when the PC conveys a message to the link,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

Fig1.Bus Topology

### 4.1.1 Advantages:

* The bus topology is straightforward and introduce.
* The cabling cost is low.
* The bus topology is not difficult to extend.

### 4.1.2 Disadvantages:

* Only one PC can send information at one time and others need to stand by till their turn comes.
* If the link loosens up or association then it can cut down the entire organization.
* The speed of transport geography is moderate on the grounds that just a single PC can communicate something specific at a time.

## 4.2 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

### 4.2.1 Advantages:

* it gives security and protection.
* The disappointment of a solitary PC doesn't cut down the entire organization.

### 4.2.2 Disadvantages:

* Cabling is more costly.
* The equipment cost to interface every gadget is costly
* Every framework inside interfaces with each and every other framework here and there it prompts burden

## 4.3 Ring Topology

A ring topology is an organization setup where gadget associations make a roundabout information way. Each arranged gadget is associated with two others, similar to focuses on a circle. Together, gadgets in a ring topology are alluded to as a ring organization. A Ring topology can be best depicted as gadgets associated with shut circle daisy chain. Information Transmission is unidirectional in ring topology.

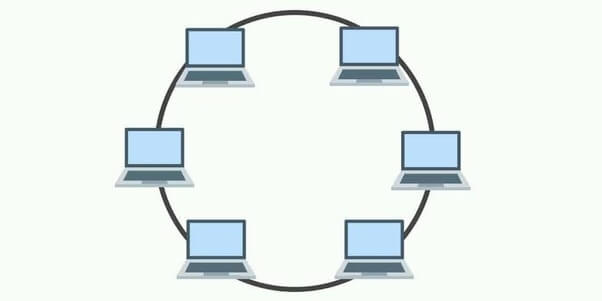


Fig 3 Ring Topology

### 4.3.1 Advantages:

* Ring networks can range over a more extended actual distance, as the hubs will recover the message as it is being passed across.
* Relatively reasonable and simple to assemble or grow a ring organization, as it is basically placing the gadgets into a shut daisy chain.
* Adding more hubs won't hinder the whole organization, as just hubs that have the token can send information.

### 4.3.2 Disadvantages:

* Depending on how the ring network is arranged, a solitary break in the organization can actually still capacity regularly. However, with 2 broken hubs, the ring organization will basically fall into 2 separate parts.
* It is an outright torment to add or eliminate a hub, as it will influence the remainder of the organization.

## 4.4 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

### 4.4.1 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.

### 4.4.2 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.

## 4.5 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.

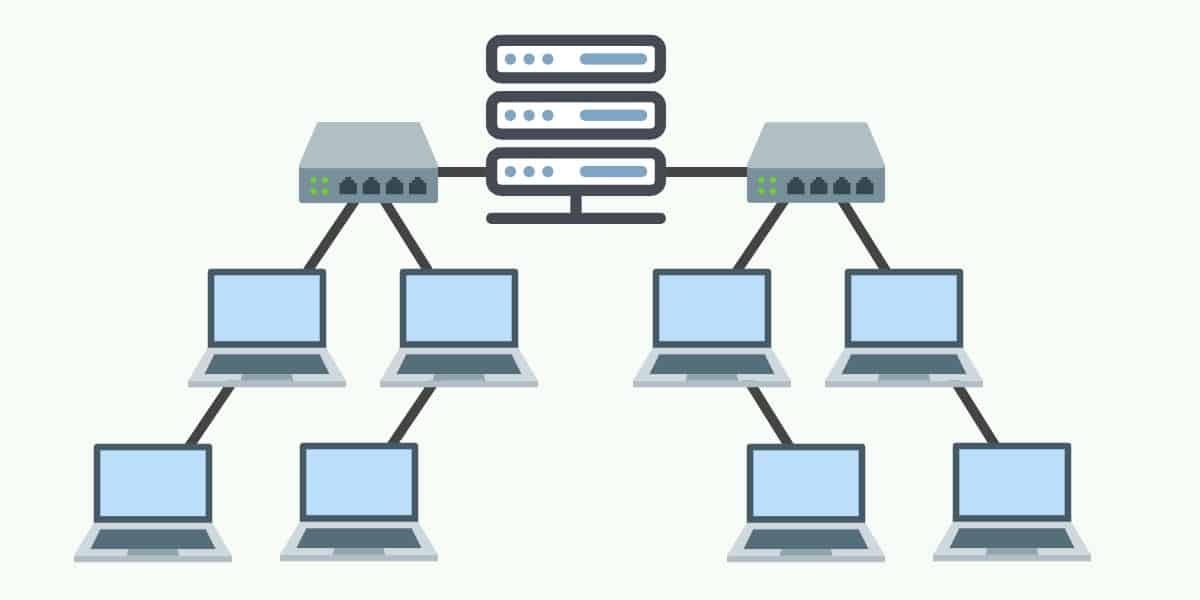


Fig 5 Tree Topology

### 4.5.1 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.

### 4.5.2 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

## 4.6 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

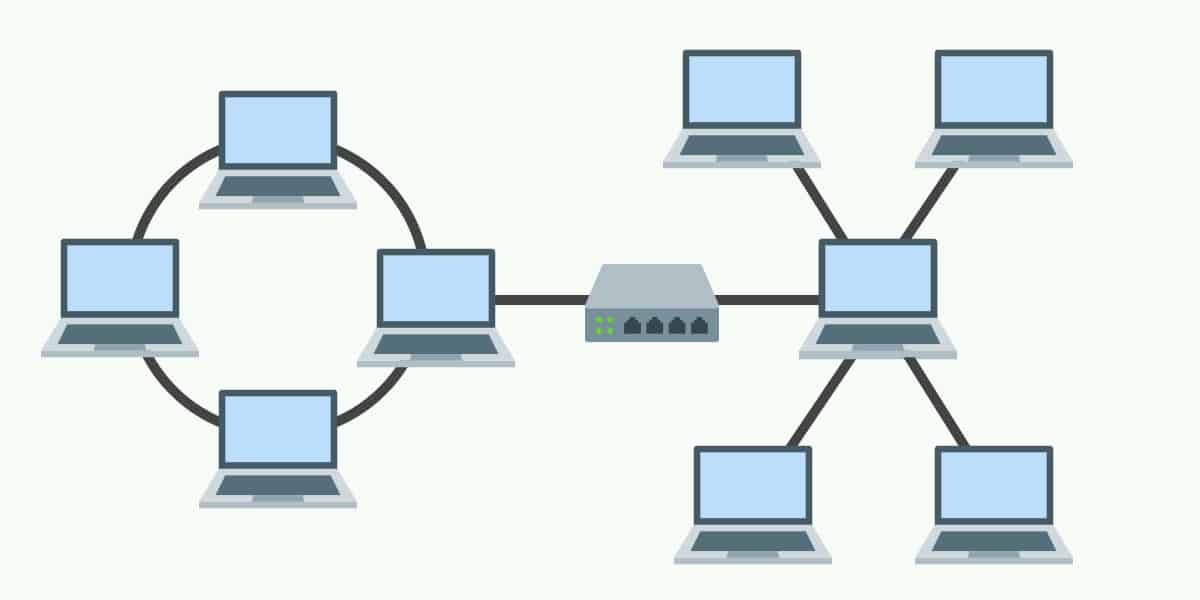


Fig 6 Hybrid Topology

### 4.6.1 Advantages:

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

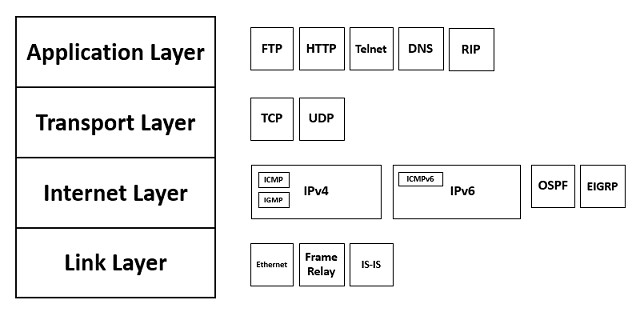
### 4.6.2 Disadvantages:

* 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.

# 5. PROTOCOLS

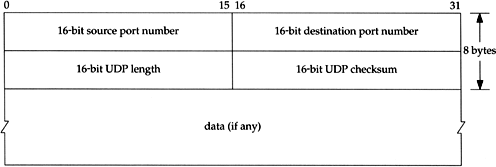
## 5.1 TCP Protocol

The Transmission Control Protocol (TCP) is a transport protocol that is utilized on top of IP to guarantee dependable transmission of bundles. TCP incorporates components to tackle a large number of the issues that emerge from packets-based informing, like lost bundles, faulty packets, copy bundles, and debased bundles. Since TCP is the convention utilized most normally on top of IP, the Web convention stack is now and again alluded to as TCP/IP.



## 5.2 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.



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.

## 5.3 IP Protocol

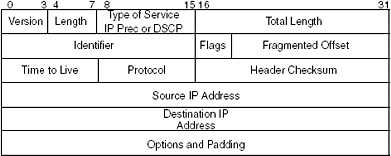


Fig IP Header

The Internet Protocol (IP) is a protocol, or set of rules, for directing and tending to parcels of information with the goal that they can traverse organizations and show up at the right objective. Information crossing the Internet is separated into more modest pieces, called bundles. IP data is joined to every bundle, and this data assists switches with sending parcels to the ideal spot. Each gadget or space that interfaces with the Internet is appointed an IP address, and as parcels are coordinated to the IP address appended to them, information shows up where it is required.

## 5.4 L2 Protocols

### 5.4.1 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 actual location, however has to know its sensible location – no enough IP delivers to dole out to each station it needs to appoint IP addresses on request.
* Another machine on the nearby organization that realizes all the IP tends to will react with a RARP reply
* It utilizes the actual location to get the consistent location by utilizing the RARP protocol.

### 5.4.2 ICMP (Internet Control Message Protocol)

* ICMP messages are separated into two general classifications: error-announcing messages and inquiry messages
* The Internet Control Message Protocol (ICMP) is an organization layer protocol utilized by network gadgets to analyze network correspondence issues..
* The error-announcing messages report issues that a switch or a host (objective) may experience when it measures an IP packet.
* ICMP is for the most part used to decide if information is arriving at its expected objective in a timely manner.
* The inquiry messages help a host or an organization chief get explicit data from a switch or another host.

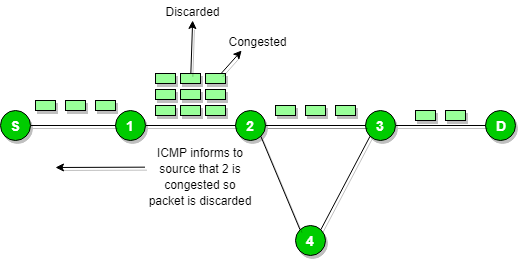
****

Fig ICMP

### 5.4.3 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 customer/worker protocol that naturally gives a Web 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 doles out an IP address for a negotiable period
* DHCP gives static and dynamic location distribution that can be manual or programmed.
* A DHCP worker has an information base that statically ties actual addresses to IP addresses known as static location.

### 5.4.4 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.

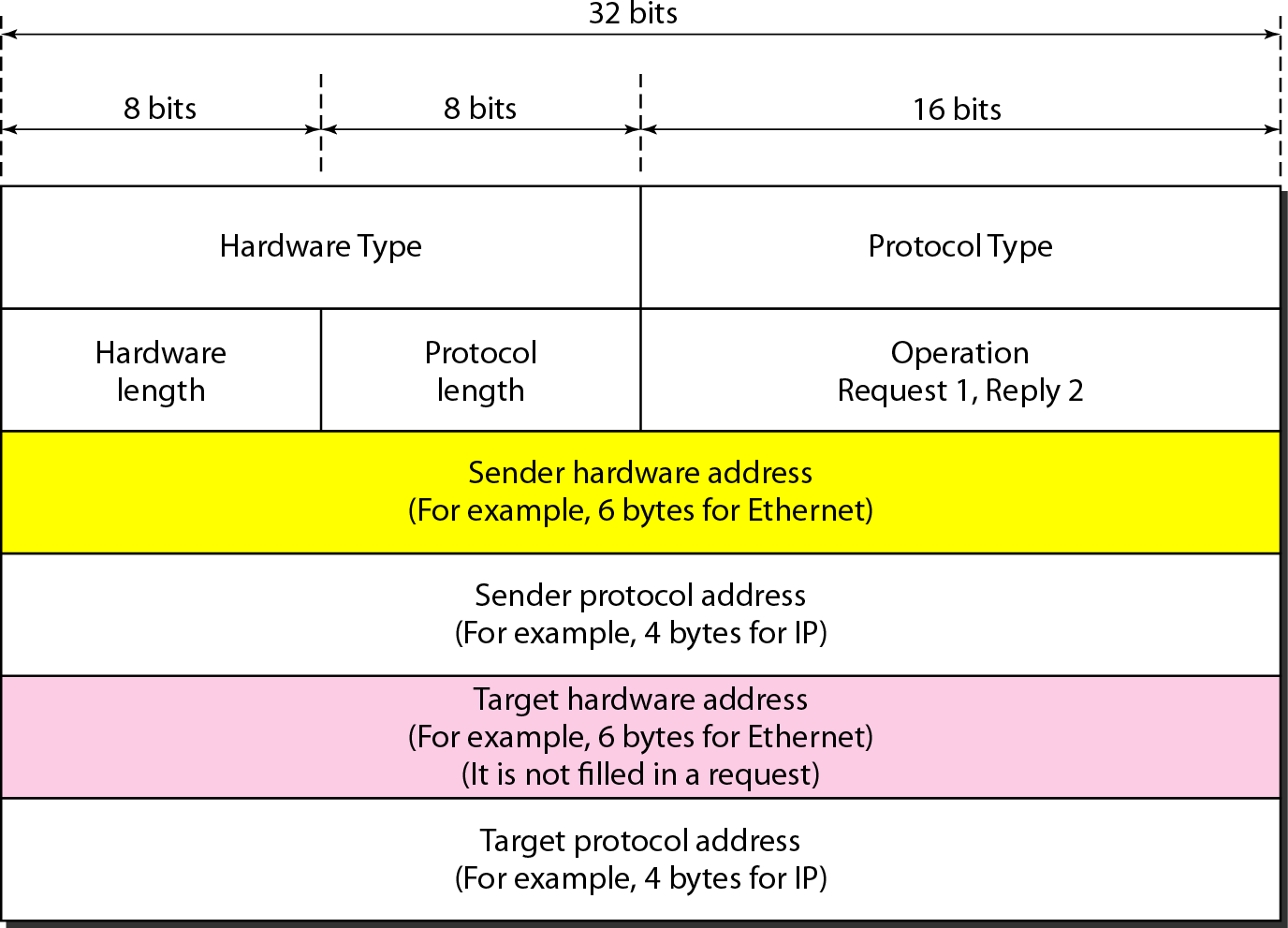


Fig ARP Packet Format

## 5.5 L3 Protocols

### 5.5.1 BGP (Border Gateway Protocol)

* + - Border Gateway Protocol (BGP) is utilized to Trade directing data for the web and is the protocol utilized between ISPs.
    - To establish a solid climate, BGP utilizes the administrations of TCP.
    - The fundamental job of BGP is to give correspondence between two self-sufficient frameworks.
    - BGP upholds Next-Bounce Worldview.
    - BGP ration network Data transmission.
    - In BGP protocol, the way among source and objective (rundown of self-ruling frameworks) is addressed as a rundown of qualities. Each property gives some data about the way.

### 5.5.2 RIP (Routing Information Protocol)

* + - Routing Information Protocol (RIP) is a dynamic routing protocol which uses bounce consider a routing metric to track down the best way between the source and the objective organization.
    - It communicates the routing updates to the whole organization that makes a great deal of traffic.
    - Infinity is characterized as 16, which implies that any course in a self-governing framework utilizing RIP can't have in excess of 15 bounces.
    - The metric utilized by RIP is characterized as the quantity of connections (organizations) to arrive at the objective. Therefore, the measurement in RIP is known as a jump check.
    - Routing Information Protocol (RIP) is a dynamic routing protocol which uses jump consider a routing metric to track down the best way between the source and the objective organization.

### 5.5.3 EIGRP (Enhanced Interior Gateway Routing)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic directing Convention which is utilized to track down the best way between any two layer-3 gadgets convey the parcel. EIGRP deals with network layer convention of OSI model and uses the convention number 88. It utilizes a few messages to speak with the neighbor gadgets that works EIGRP.

These are: -

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

## **5.6 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

# 6. IP ADDRESS

## 6.1 IPV4

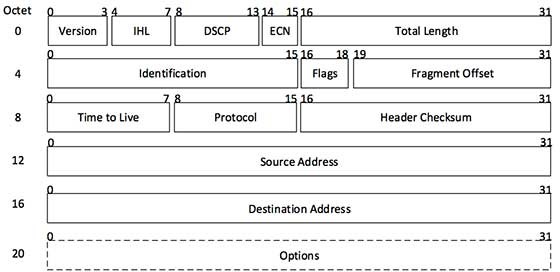
IP stands for Internet Protocol and v4 stands for version 4.I P version four addresses are 32-bit integers which will be expressed in hexadecimal notation.

### 6.1.2 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.

### 6.1.3 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.

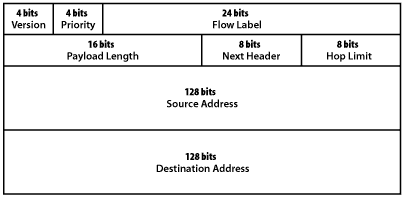


## 6.2 IPV6

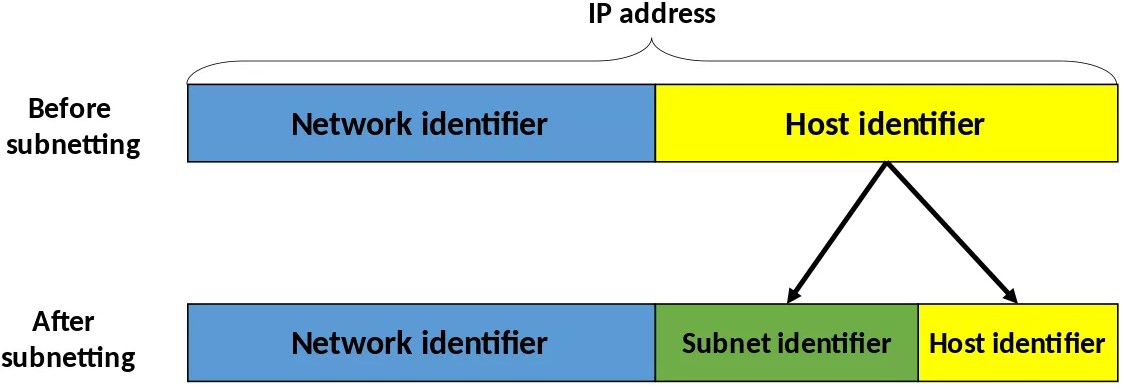
IPv6 was developed to deal with the problem of IP v4 exhaustion. IPv6 is 128-bits address having an address space of 2^128, which is bigger than IPv4. In IPv6 Colon-Hexa representation is used.

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.

****

**SUBNETTING**



# 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.

# ****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.

## **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.

**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

### ****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.

## **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.

**Classful Network**

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

Classes

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.

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.

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.

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.

Class E: -

* In Class E, an IP address is used for the future use or for the research and development purposes.
* In Class E Start Address is: - 240.0.0.0

End Address is: - 255.255.255.255

* In Class E Network id is **not defined** and Host id is **not defined**
* Total Address in Class is 2^28
* It does not possess any subnetting and higher order bits of the first octet is always set to 1111.

**NETWORK TOOLS**

## 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.

## 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.