./

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 | 22/03/21 | Nitin N Shetty 99003746 |  |  |  |
| 3 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Document History**

# Network Classification

## 1.PAN

A personal area network (PAN) is a computer network organized around an individual for personal use only. They typically involve a computer, phone, printer, tablet, or some other device 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.

## 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. **WAN**

* A wide area network spans a large geographic area such as a city, state, or country.
* It can be private to connect parts of a business, or it can be public to connect smaller networks.
* It ranges more than 1,00,000 kms.
* It runs on bandwidths of 20 Mbps, 50 Mbps, or 100 Mbps.

1. **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. **WLAN**

* WLAN is local area network that doesnot 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 connectio

1. **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. **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.

**Components: -**

1. **Work Stations**

Workstation is a computer which requests access to the LAN and switch services to responds the requests via switch to perform dedicated task with having enhanced features. In workstation, Operations are in forms of Business, engineering etc. and in this Graphics User Interface is pre-install because it is not an optional to the workstation.A workstation is a special computer designed for technical or scientific applications. Intended

primarily to be used by one person at a time, they are commonly connected to a local area network and run

multi-user operating systems.

1. **File Servers**

A file server is a central server in a computer network that provides file systems or at least parts of a file system to connected clients. File servers therefore offer users a central storage place for files on internal data media, which is accessible to all authorized clients. Here, the server administrator defines strict rules regarding which users have which access rights: For instance, the configuration or file authorizations of the respective file system enable the admin to set which files can be seen and opened by a certain user or user group, and whether data can only be viewed or also added, edited, or deleted.

1. **Gateway**

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

1. **NIU [Network Interface Unit]**

NIU stands for Network Interface Unit, it is basically an interpreter that is used to establish the communication between the server and the workstations or nodes. A standalone computer or a computer that is not attached to any network, lives in its own world and carries out its tasks with its own inbuilt resources. But as soon as it becomes a Workstation then it needs an interface to help establish a connection with the network because without this the workstation or node will not be able to share network resources. You can also say that, a Network Interface Unit(NIU) is a basically a device that attached to each of the work station and the server, and helps workstation and the server and helps workstation establish the all-important connection with the network

1. **HUB**

A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. In a hub, a frame is broadcasted to every one of its ports. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This place a lot of traffic on the network and can lead to poor network response times A bridge is a network device that connects multiple LANs (Local Area Networks) together to form a larger LAN. The process of aggregating networks is called network bridging

A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches. Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame. If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it. If the frame has a destination MAC address in a connected network, it will forward the frame toward it.

1. **Communication Channel / LAN Channels**

In communications, a channel is the means of passing information from a sender to a recipient. Determining the

most appropriate channel, or medium, is critical to the effectiveness of communication. Channels include oral

means such as telephone calls and presentations, and written modes such as reports, memos, and email.

Communication channels differ along a scale from rich to lean. Think about how you would select a steak

—some have more fat than others; they are rich and full of flavor and body. If, however, you are on a diet

and just want the meat, you will select a lean steak. Communication channels are the similar: rich channels

are more interactive, provide opportunities for two-way communication, and allow both the sender and

receiver to read the nonverbal messages

1. **Switch**

In networks the switch is the device that filters and forwards packets between LAN segments. Switches operate at

the data link layer(layer 2) and sometimes the network layer(layer 3) of the OSI Reference Model and therefore

support any packet protocol. LANs that use switches to join segments are called switched LANs or for Ethernet

Networks, switched Ethernet LANs. Switches facilitate the sharing of resources by connecting all the devices,

Including computers, printers, and servers, in a small business network. Building a small business network is not

Possible without switches to device together.

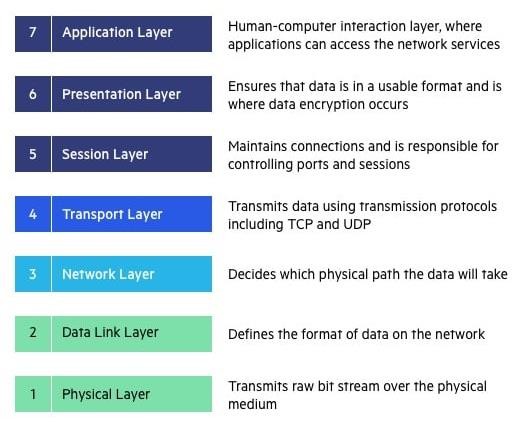
1. **Bridge**

A bridge is a network device that connects multiple LANs (Local Area Networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame. If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it. If the frame has a destination MAC address in a connected network, it will forward the frame toward it.

1. **Access Points**

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.



# OSI MODEL

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

**Physical Layer**

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

**Data link layer**

The data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

**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.

**Transport 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.

**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.

**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.

**Application Layer**

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication

**Network**

A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

## TYPES AND TOPOLOGIES:

There are Total 6 Topologies are there in Topology, Network topology describes the layout or appearance of network devices such as computers, cables and other components. Components within 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.

1. **Bus Topology**

Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. Bi-directional feature is not available in bus topology. When the computer sends a signal to the cable, all the computers receive the information but the computer whose address matches with the signal accepts the data.

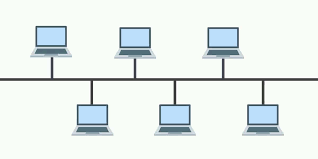


Fig1.Bus Topology

### Advantages:

* + The bus topology is easy to understand and install.
  + The cabling cost is low.
  + The bus topology is easy to expand.

### Disadvantages:

* Only one computer can transmit data at one time and others have to wait till their turn comes.
* If the cable breaks or loose connection then it can bring down the whole network.
* The speed of bus topology is slow because only one computer can send a message at a time.

1. **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

### Advantages:

* It provides security and privacy.
* The failure of a single computer does not bring down the whole network.

### Disadvantages:

* Cabling is more expensive.
* The hardware cost to connect each device is expensive
* Every system internally connects to every other system sometimes it leads to disadvantage

1. **Ring Topology**

A ringtopology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ringtopology are referred to as a ringnetwork. A Ring topology can be best described as devices connected to closed loop daisy chain. Data Transmission is unidirectional in ring topology.

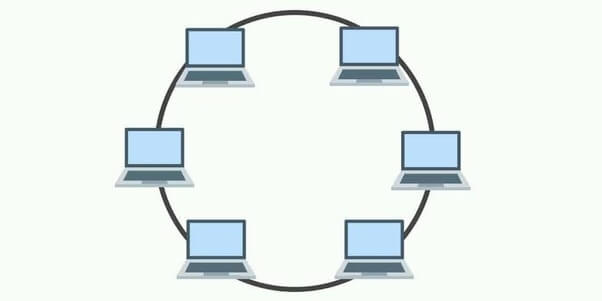


Fig 3 Ring Topology

### Advantages:

* Ring networks can span over a longer physical distance, as the nodes will regenerate the message as it is being passed across.
* Relatively affordable and easy to build or expand a ring network, as it is essentially just putting the devices into a closed daisy chain.
* Adding more nodes will not slow down the entire network, as only nodes that have the token can transmit data.

### Disadvantages:

* Depending on how the ring network is configured, a single break in the network can technically still function normally. But with 2 broken nodes, the ring network will essentially collapse into 2 separate halves.
* It is an absolute pain to add or remove a node, as it will affect the rest of the network.

1. **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

### 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.

### 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.

1. **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.

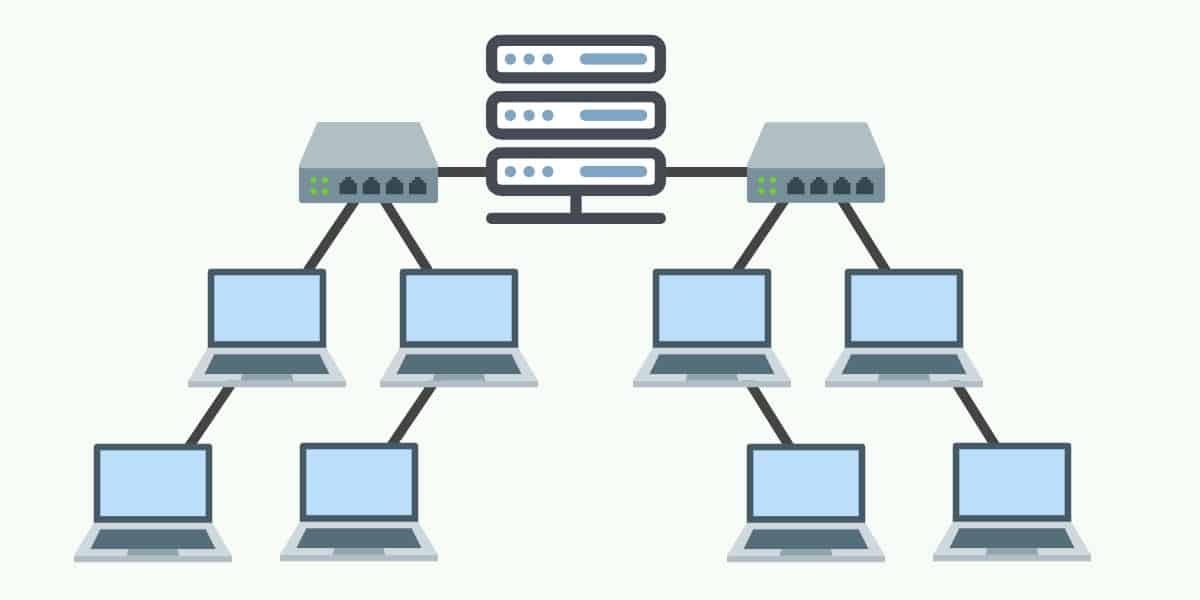


Fig 5 Tree Topology

### 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.

### 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

1. **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

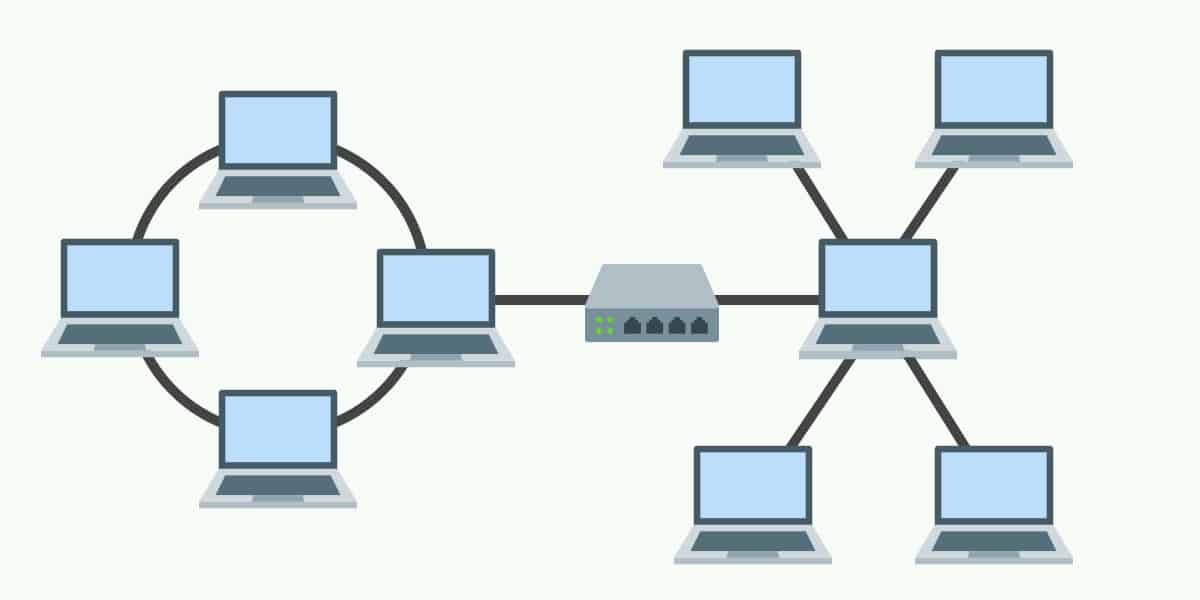


Fig 6 Hybrid Topology

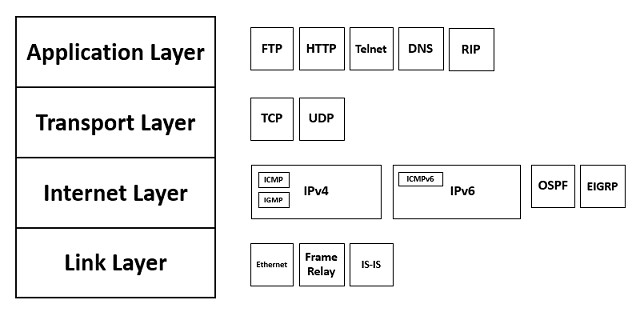
### Advantages:

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

### Disadvantages:

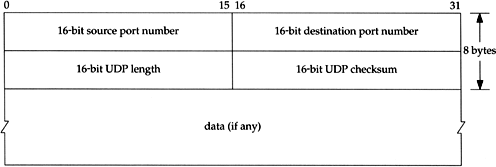
* Complex in design. The network engineer has to know various topologies and network gimmicks.
* May not be the most cost-effective, as it may involve the use of many different networking devices.

**TCP Protocol**

The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets. Since TCP is the protocol used most commonly on top of IP, the Internet protocol stack is sometimes referred to as TCP/IP.

**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.

**IP Protocol**

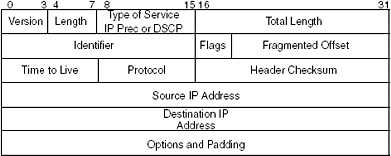


Fig IP Header

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. 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 where it is needed.

**L2 Protocols**

## **RARP** (Reverse Address Resolution Protocol)

* A RARP request is created and broadcast on the local network.
* RARP stands for Reverse Address Resolution Protocol.
* It is used when a host knows its physical address, but needs to know its logical address – no enough IP addresses to assign to each station it needs to assign IP addresses on demand.
* Another machine on the local network that knows all the IP addresses will respond with a RARP reply
* It uses the physical address to get the logical address by using the RARP protocol.

**ICMP** (Internet Control Message Protocol)

* ICMP messages are divided into two broad categories: error-reporting messages and query messages
* The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.
* The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
* ICMP is mainly used to determine whether data is reaching its intended destination in a timely manner.
* The query messages help a host or a network manager get specific information from a router or another host.

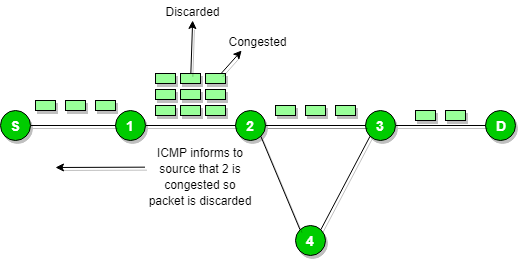
****

Fig ICMP

**DHCP** (Dynamic Host Configuration Protocol)

* DHCP has a second database with a pool of available IP addresses known as dynamic allocation.
* Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
* When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period
* DHCP provides static and dynamic address allocation that can be manual or automatic.
* A DHCP server has a database that statically binds physical addresses to IP addresses known as static allocation.

**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.

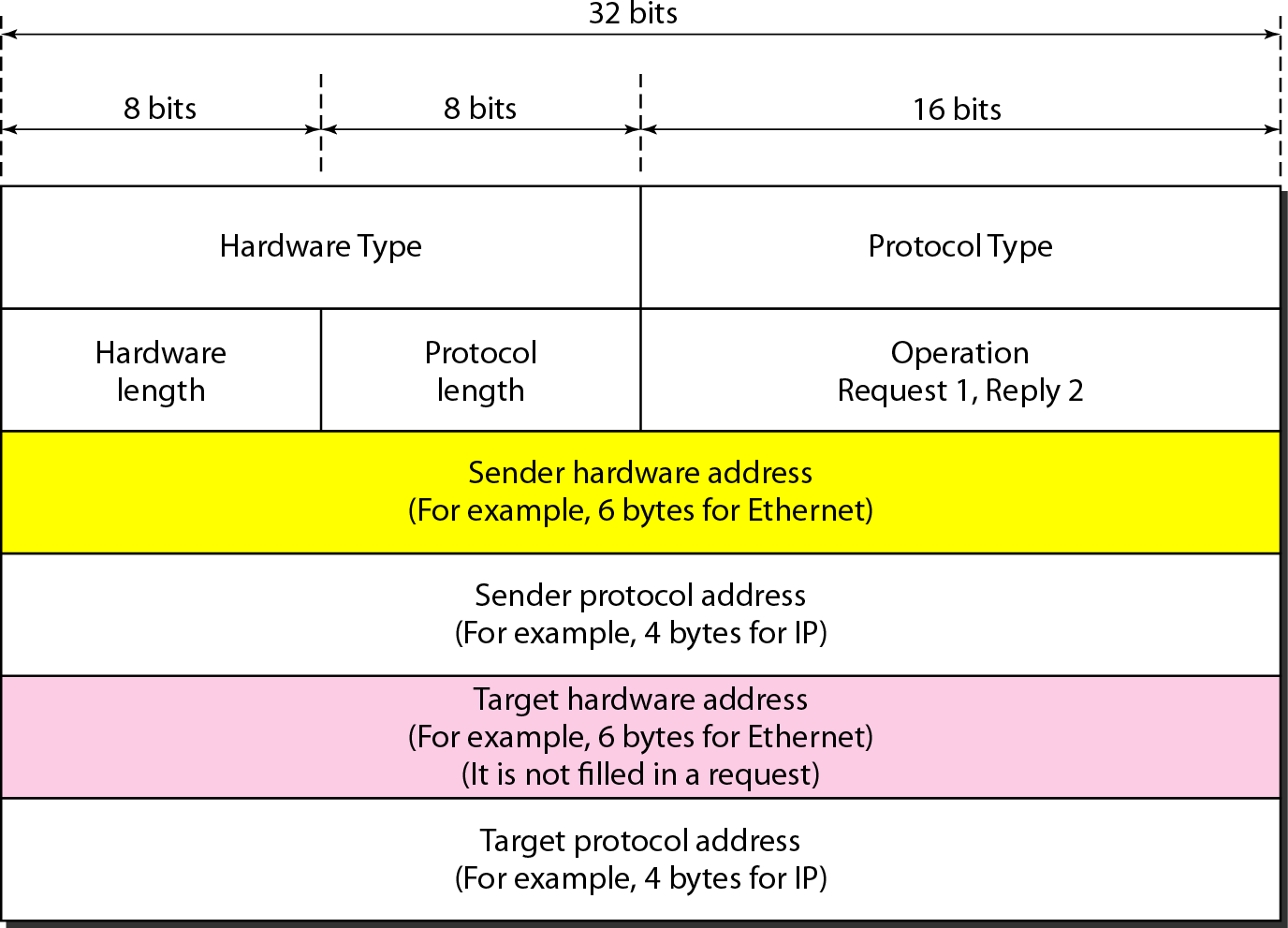


Fig ARP Packet Format

**L3 Protocols**

## **BGP** (Border Gateway Protocol)

* + - Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISPs.
    - To create a reliable environment, BGP uses the services of TCP.
    - The main role of BGP is to provide communication between two autonomous systems.
    - BGP supports Next-Hop Paradigm.
    - BGP conserve network Bandwidth.
* In BGP protocol, the path between source and destination (list of autonomous systems) is represented as a list of attributes. Each attribute gives some information about the path.

**RIP** (Routing Information Protocol)

* + - Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.
    - It broadcasts the routing updates to the entire network that creates a lot 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 as a routing metric to find the best path between the source and the destination network.

## **EIGRP** (Enhanced Interior Gateway Routing)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is used to find the best path between any two layer-3 devices deliver the packet. EIGRP works on network layer protocol of OSI model and uses the protocol number 88. It uses some messages to communicate with the neighbor devices that operates EIGRP.

These are: -

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

# ****Types of WLAN Protocols****

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

* **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

**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.

### Parts of IPv4:

* Network Part: - The network part indicates the distinctive variety that’s appointed to the

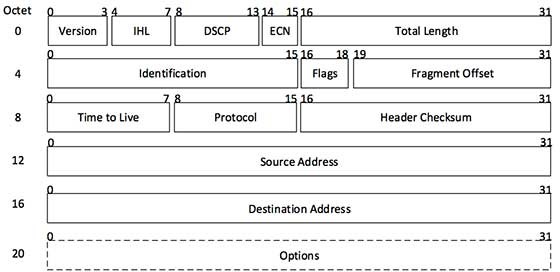
network. The network part conjointly identifies the category of the network that’s

assigned.

* Host Part: - The host part uniquely identifies the machine on your network. This a part of the IPv4 address is assigned to every host. For each host on the network, the network part is the same, however, the host half must vary.
* Subnet number: - Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

### 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.

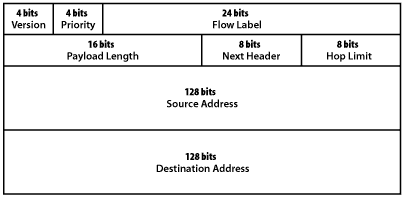


**IPV6**

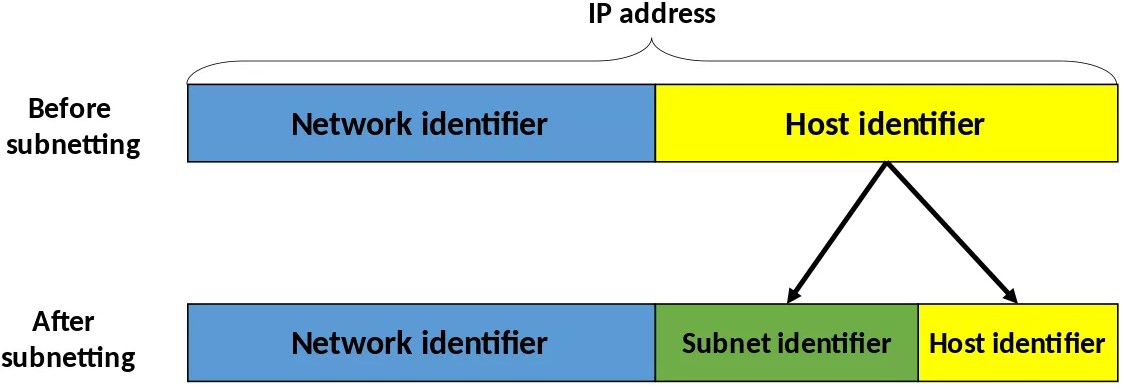
IPv6 was developed to deal with the problem of IP v4 exhaustion. IPv6 is 128-bits address having an address space of 2^128, which is bigger than IPv4. In IPv6 Colon-Hexa representation is used.

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

* + **Unicast Address:** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.
  + **Multicast Address:** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding 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

* 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 broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.

## **Firewall**:

Firewalls control incoming and outgoing traffic on networks, with predetermined security rules. Firewalls keep out unfriendly traffic and is a necessary part of daily computing. Network Security relies heavily on Firewalls, and especially next generation firewalls which focus on blocking malware and application-layer attacks.

## **Encryption**:

Encryption is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext.

### ****How Encryption Works****

Encryption uses algorithms to scramble your information. It is then transmitted to the receiving party, who can decode the message with a key. There are many types of algorithms, which all involve different ways of scrambling and then decrypting information.

## **Cryptography**:

The purpose of **cryptography** is to hide the contents of messages by encrypting them so as to make them unrecognizable except by someone who has been given a special decryption key. The purpose of **cryptanalysis** is then to defeat this by finding ways to decrypt messages without being given the key.