

Networking Learning Report

# Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel.**  **No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be Approved** | **Remarks/Revision Details** |
| 1.0 |  | Akshansh Mishra |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Table of Contents**

1. [NETWORK 5](#_bookmark0)
   1. [TYPES AND TOPOLOGIES 5](#_bookmark1)
      1. [BUS TOPOLOGY 5](#_bookmark2)
      2. [MESH TOPOLOGY 6](#_bookmark3)
      3. [STAR TOPOLOGY 6](#_bookmark4)
      4. [RING TOPOLOGY 7](#_bookmark5)
      5. [HYBRID TOPOLOGY 8](#_bookmark6)
      6. [TREE TOPOLOGY 9](#_bookmark7)
2. [WIRED AND WIRELESS NETWORKS 10](#_bookmark8)
   1. [PAN 10](#_bookmark9)
   2. [LAN 10](#_bookmark10)
   3. [WLAN 10](#_bookmark11)
   4. [WAN 10](#_bookmark12)
   5. [MAN 10](#_bookmark13)
   6. [WIFI 11](#_bookmark14)
   7. [WIMAX 11](#_bookmark15)
3. [COMPONENTS 11](#_bookmark16)
   1. [ROUTER 12](#_bookmark17)
   2. [SWITCH 12](#_bookmark18)
   3. [HUB 12](#_bookmark19)
   4. [BRIDGE 12](#_bookmark20)
   5. [GATEWAY 13](#_bookmark21)
   6. [ACCESS POINTS 13](#_bookmark22)
4. [OSI MODEL 14](#_bookmark23)
5. [TCP PROTOCOL 14](#_bookmark24)
6. [UDP PROTOCOL 15](#_bookmark25)
7. [IP PROTOCOL 16](#_bookmark26)
8. [L2 PROTOCOLS 17](#_bookmark27)
   1. [ARP 17](#_bookmark28)
   2. [RARP 17](#_bookmark29)
   3. [DHCP 18](#_bookmark30)
   4. [ICMP 18](#_bookmark31)
9. [L3 PROTOCOLS 19](#_bookmark32)
   1. [BGP 19](#_bookmark33)
   2. [EIGRP 19](#_bookmark34)
   3. [RIP PROTOCOL 19](#_bookmark35)
   4. [OSPF 20](#_bookmark36)

[10 IPV4 20](#_bookmark37)

* 1. [CLASSFUL ADDRESSING 21](#_bookmark38)
  2. [SUBNETTING 23](#_bookmark39)

[11 IPV6 24](#_bookmark40)

1. [CISCO PACKET TRACER OUTPUT 25](#_bookmark41)

[12.1 PING OUTPUT FROM PC0 (132.10.10.1) TO PC4 (192.168.10.2) 25](#_bookmark42)

[12.2 PING OUTPUT FROM PC4 (192.168.10.2) TO PC6 (132.10.10.4) 26](#_bookmark43)

[12.3 PING OUTPUT FROM LAPTOP0 (192.168.10.4) TO SERVER (10.10.10.2) 26](#_bookmark44)

[12.4 PING OUTPUT FROM PC2 (132.10.10.3) TO SERVER (10.10.10.2) 27](#_bookmark45)

[12.5 PING OUTPUT FROM PC1 (132.10.10.2) TO PRINTER0 (128.12.12.1) 27](#_bookmark46)

[12.6 PING OUTPUT FROM PC2 (132.10.10.3) TO PRINTER1 (132.10.10.6) 28](#_bookmark47)

1. [REFERENCES 29](#_bookmark48)

# List of Figures

Figure 1: Bus Topology 5

Figure 2: Mesh Topology 6

Figure 3: Star Topology 7

Figure 4: Ring Topology 8

Figure 5: Hybrid Topology 8

Figure 6: Tree Topology 9

Figure 7: OSI Model 14

Figure 8: TCP Protocol 15

Figure 9: TCP Header 15

Figure 10: UDP Header 16

Figure 11: IP Header 16

Figure 12: ARP Packet Format 17

Figure 13: ICMP Message Format 18

Figure 14: IP Header 21

Figure 15: Classful Addressing 22

Figure 16: Subnetting 23

Figure 17: IPv6 Header 24

Figure 18: Network in Cisco Packet Tracer 25

Figure 19: Ping Output - 1 25

Figure 20: Ping Output - 2 26

Figure 21: Ping Output - 3 26

Figure 22: Ping Output - 4 27

Figure 23: Ping Output - 5 27

Figure 24: Ping output - 6 28

# **Computer Network:**

* A computer network is a group of two or more interconnected computer systems. You can establish a network connection using either cable or wireless media.
* Every network involves hardware and software that connects computers and tools.
* Computer networks help you to connect with multiple computers together to send and receive information.
* The purpose of having computer network is to send and receive data stored in other devices over the network. These devices are often referred as nodes.

There are **five basic components** of a computer network

**Message**: It is the data or information which needs to be transferred from one device to another device over a computer network.

**Sender**: Sender is the device that has the data and needs to send the data to other device connected to the network.

**Receiver**: A receiver is the device which is expecting the data from other device on the network.  
Transmission media: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

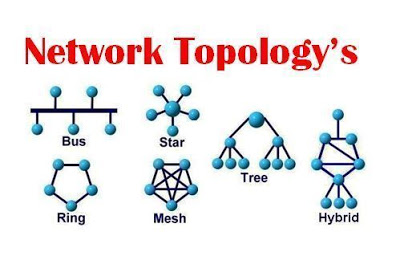
**Protocol**: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol. For example, http and https are the two protocols used by web browsers to get and post the data to internet, similarly smtp protocol is used by email services connected to the internet.

A list Of Computer network features is given below

* + - Communication speed
    - File sharing
    - Back up and Roll back is easy
    - Software and Hardware sharing
    - Security
    - Scalability
    - Reliability

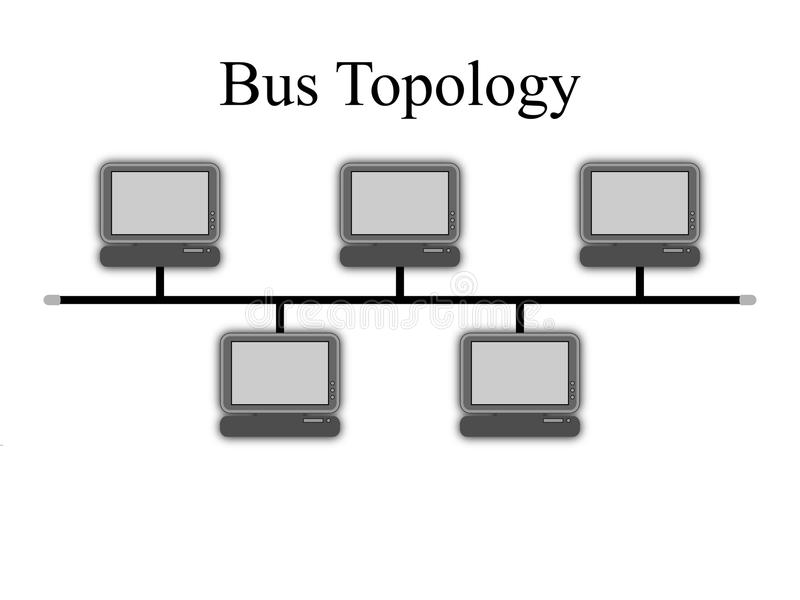
What is Topology?

* Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.
* Physical topology is the geometric representation of all the nodes in a network.



1. BUS Topology –

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



1. RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Advantages of Ring Topology :

* Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
* Cheap to install and expand

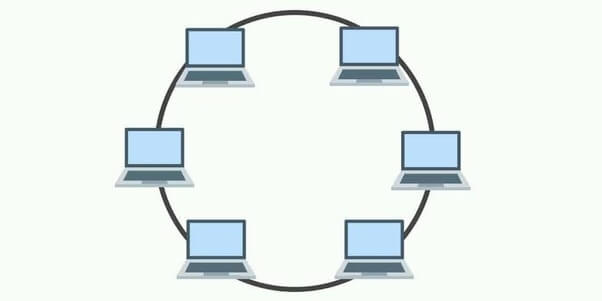
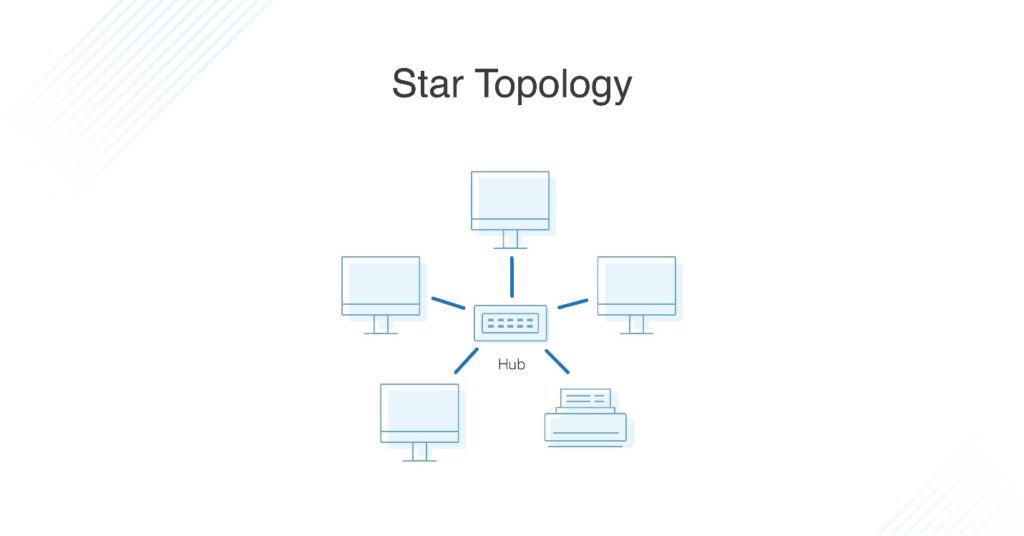


Figure: Bus Topology

1. STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.



1. MESH Topology

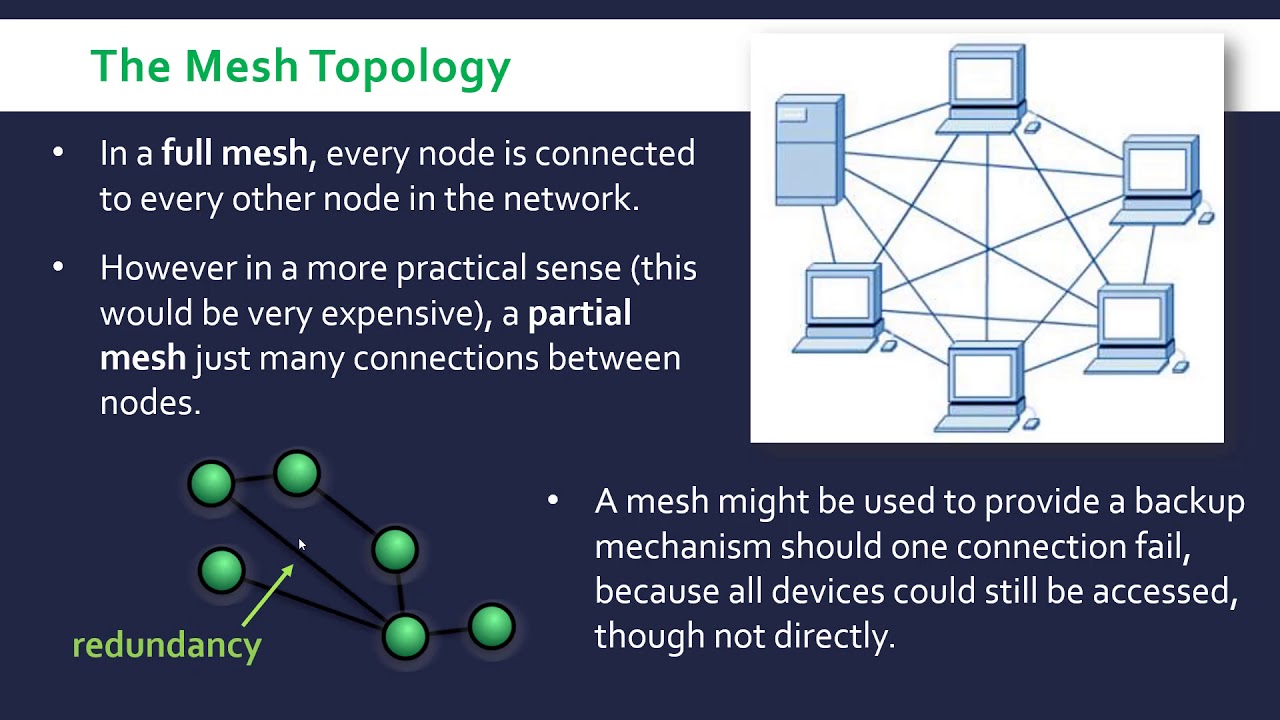
It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are

* Routing
* Flooding

Types of Mesh Topology

1. Partial Mesh Topology : In this topology, some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. Full Mesh Topology : Each and every nodes or devices are connected to each other.



1. TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology –

* Ideal if workstations are located in groups.
* Used in Wide Area Network

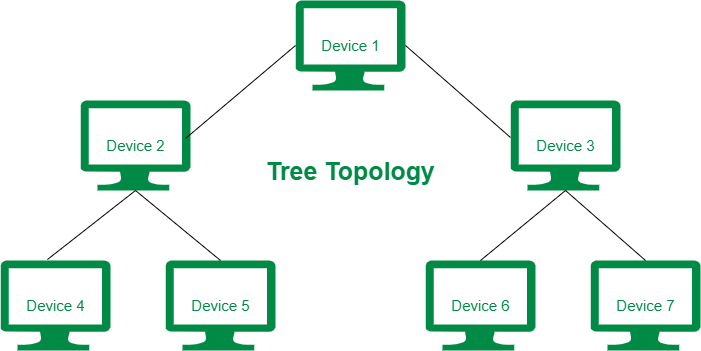
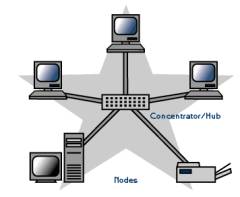


Figure – Tree topology

**Wired Networks**

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today



The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which computer gets what signal.

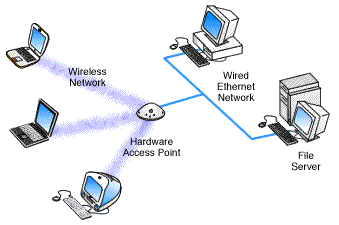
The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently.

Wireless Networks

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range.

There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure.

An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.



Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal. Interference can be caused by other devices operating on the same radio frequency and it is very hard to control the addition of new devices on the same frequency.

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

* LAN(local area network)

A local area network (LAN) consists of a series of computers linked together to form a network in a circumscribed location. The computers in a LAN connect to each other via TCP/IP ethernet or Wi-Fi. A LAN is normally exclusive to an organization, such as a school, office, association or church.

A LAN comprises **at least two end devices**, but it can also link several thousand devices to one another. If larger distances need to be bridged, however, this is normally achieved using MANs and WANs. A Local Area Network can connect computers, smartphones, printers, scanners, storage devices, servers and other network devices with each other and to the internet. If a printer is only connected to a computer via a USB cable, for example, usually only this PC will be able to access the device. But connecting the printer to the network allows multiple devices in the area to use the printer.

The distinguishing features of LAN are

* Network size is limited to a small geographical area, presently to a few kilometers.
* Data transfer rate is generally high. They range from 100 Mbps to 1000 Mbps.
* In general, a LAN uses only one type of transmission medium, commonly category 5 coaxial cables.
* WAN (Wide Area Network)

WAN is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

A wide-area network (or WAN) is a computer network that connects smaller networks. Since

WANs are not tied to a specific location, they allow localized networks to communicate with

one another across great distances. They also facilitate communication and the sharing of information between devices from anywhere in the world.

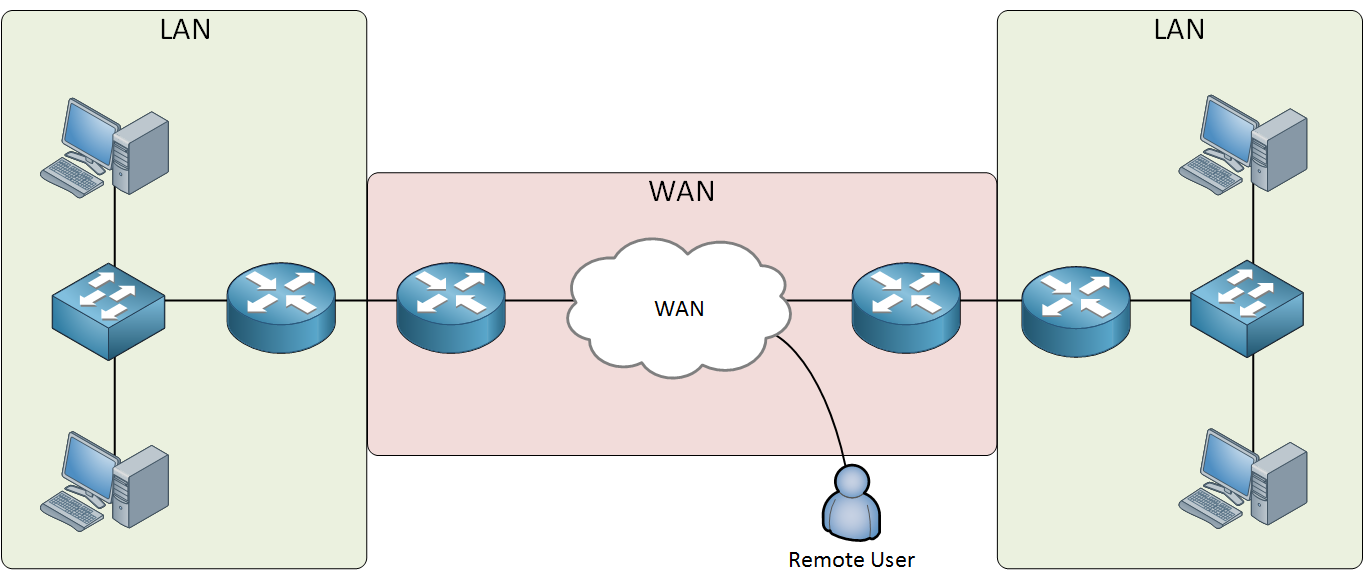


Figure : Wide area Network

* Metropolitan area network (MAN)

A metropolitan area network (MAN) is a network with a size greater than LAN but smaller than a WAN. It normally comprises networked interconnections within a city that also offers a connection to the Internet. A metropolitan area network (MAN) is similar to a local area network (LAN) but spans an entire city or campus, or some other municipal or organizational territory. MANs are formed by connecting multiple LANs. 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.

**Advantages**

* 1. **Less expensive**
  2. **Sending local emails**
  3. **High speed than WAN**
  4. **High Security**

**Disadvantages**

* 1. **Difficult to manage**
  2. **Internet speed difference**
  3. **Hackers attack**
  4. **More wires required**

**Personal area network (PAN)**

**Personal Area Network (PAN)** is a the computer network that connects computers/devices within the range of an individual person. As PAN provides a network range within a person’s range typically within a range of 10 meters(33 feet) it is called as Personal Area Network. A Personal Area Network typically involves a computer, phone, tablet, printer, PDA (Personal Digital Assistant) and other and other entertainment devices like speakers, video game consoles etc

**Types of Personal Area Network (PAN) :**  
Personal Area Network can be of 2 types depending upon its connection i.e., Wireless PAN, and Wired PAN.

**These are explained as following below –**

1. **Wireless PAN –**

Wireless Personal Area Network (WPAN) is connected through signals such as infrared, ZigBee, Bluetooth and ultrawideband etc.

1. **Wired PAN –**

Wired PAN is connected through cables/wires such as Firewire or USB.

**Examples of PAN** :

* **Body Area Network** –  
  It is a mobile network that moves with a persona range for example when person connects his smart phone to the Bluetooth headphone and moves in the market that refers to a body area network.
* **Offline Network** –  
  In this multiple devices are connected through Bluetooth or Wi-Fi. The devices attached to your computer including printers, mouse, speakers, and other appliances are integrated using a Personal Area Network (PAN) and do not use internet. So a communication network is formed between the devices used in a small single space for example home.
* **Home Office** –  
  In Home Office setup a separate smaller network is setup for work purpose which is separate from the network used by other home appliances. This network works as a separate body with multiple other devices connected for office work purpose.

# WIFI Technology

Wi-Fi is a popular wireless networking technology. Wi-Fi stands for “wireless fidelity”. Wi-Fi was invented by NCR Corporation/AT&T in the Netherlands in 1991. By using this technology we can exchange information between two or more devices. Wi-Fi has been developed for mobile computing devices, such as laptops, but it is now extensively using for mobile applications and consumer electronics like televisions, DVD players, and digital cameras. There should be two possibilities in communicating with the Wi-Fi connection that may be through an access point to the client connection or client to client connection. Wi-Fi is one type of [wireless technology](https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/). It is commonly called a wireless [LAN](https://www.elprocus.com/what-is-virtual-lan-architecture-types-of-links-differences/) (local area network). WiFi technology allows local area networks to operate without cable and wiring. It is making a popular choice for home and business networks. A computer’s wireless adaptor transfers the data into a radio signal and transfers the data into an antenna for users.

**Types of WIFI Technologies**

Currently, they are the four major types of WIFI technologies.

* + - Wi-Fi-802.11a
    - Wi-Fi-802.11b
    - Wi-Fi-802.11g
    - Wi-Fi-802.11n

The advantages of Wi-Fi technology include the following.

* A wireless laptop can be moved from one place to another place
* Wi-Fi network communication devices without wire can reduce the cost of wires.
* Wi-Fi setup and configuration is easy than the cabling process
* It is completely safe and it will not interfere with any network

The disadvantages of Wi-Fi technology include the following.

* + - Wi-Fi generates radiations which can harm the human health
    - We must disconnect the Wi-Fi connection whenever we are not using the server
    - There are some limits to transfer the data, we can’t able to transfer the data for long-distance
    - Wi-Fi implementation is very expensive when compared to the wired connection

**WiMAX Network Architecture**

# 

WiMAX technology is a wireless broadband communications technology based around the IEE 802.16 standard providing high speed data over a wide area.

The letters of WiMAX stand for Worldwide Interoperability for Microwave Access (Access), and it is a technology for point to multipoint wireless networking.

WiMAX technology is able to meet the needs of a large variety of users from those in developed nations wanting to install a new high speed data network very cheaply without the cost and time required to install a wired network, to those in rural areas needing fast access where wired solutions may not be viable because of the distances and costs involved - effectively providing WiMAX broadband. Additionally it is being used for mobile applications, providing high speed data to users on the move.

**Competition**

The competition with WiMAX, 802.16 depends upon the type or version being used. Although initially it was thought that there could be significant competition with Wi-Fi, there are other areas to which WiMAX is posing a threat.

* **DSL cable lines**     WiMAX is able to provide high speed data links to users and in this way it can pose a threat to DSL cable operators.
* **Cell phone operators**     As LTE was being developed and the initial roll-outs were taking place, cell phone operators saw the mobile version of WiMAX as a significant threat. It was even considered for adoption as the IMT 4G standard, but LTE was adopted as the standard, leaving WiMAX for fixed WiMAX broadband, last mile links and a variety of other point to point applications.

WiMAX technology has been deployed in many areas. Although initially seen as a candidate for 4G, its use is decreasing, although it is used as WiMAX broadband and also for last mile links.

**Components of Computer Network :**

**Router**

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are Cisco, 3Com, HP, Juniper, D-Link, Nortel, etc. Some important points of routers are given below:

* It shares information with other routers in networking.
* It uses the routing protocol to transfer the data across a network.
* Furthermore, it is more expensive than other networking devices like switches and hubs.

**Features of Router**

* A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
* A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
* It allows the users to configure the port as per their requirements in the network.
* Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card

**Switches**

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

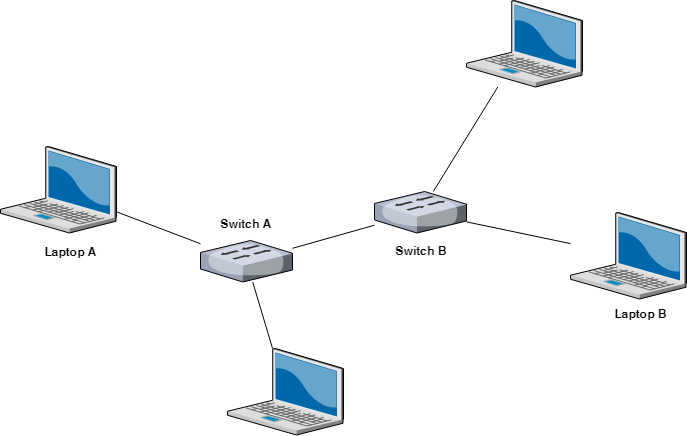


Figure : Switch connected with computer

**Features of Switches**

* A switch operates in the layer 2, i.e. data link layer of the OSI model.
* It is an intelligent network device that can be conceived as a multiport network bridge.
* It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
* It uses packet switching technique to receive and forward data packets from the source to the destination device.

### Hubs

Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.

## Features of Hubs

* + A hub operates in the physical layer of the OSI model.
  + A hub cannot filter data. It is a non-intelligent network device that sends message to all ports.
  + It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.
  + Transmission mode is half duplex.

## Types of Hubs

* **Passive Hubs** − Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.
* **Active Hubs** − Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting center. Due to their regenerating capabilities, they can extend the maximum

distance between nodes, thus increasing the size of LAN.

* **Intelligent Hubs** − Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

**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.

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

* **Transparent Bridges:-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-**In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The host can discover frame by sending a

special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

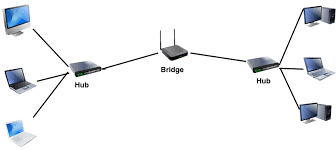


Figure : Bridge

**Gateway**

In computer networking and telecommunications, a gateway is a component that is part of two networks, which use different protocols. The gateway will translate one protocol into the other. A router is a special case of a gateway.

Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of the router or switch as it communicates using more than one protocol.

Both the computers of internet users that serve pages to users are *host nodes*. The nodes that connect the networks in between are *gateways*. These are gateway nodes:

* the computers that control traffic between company networks
* the computers used by Internet Services Provider (ISPs) to connect users to the internet.

**Types of Gateways in Networking**

There are two types of gateways that perform as the nodes specifically to connect the servers and other business systems in a comprehensive business association.

The two prototypes of gateway subsuming:

1. Bidirectional Gateway
2. Unidirectional Gateway

**Advantages of Gateway**

* Gateways are being used to expand the network.
* It is a server that provides major security.
* We can effortlessly connect two different types of network.
* Gateways are so easier to access, that one can quickly access the device from one to another.

**Disadvantages of Gateway**

* Gateways are so slower than the other devices network.
* More expensive than the other valuable devices.
* Never filter out the information/data.
* The transmission rate is slower.
* Gateways are quite hard to handle.

**OSI Model**

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

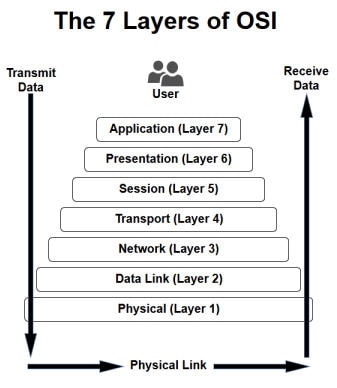


Figure : Open System Interconnection (OSI)

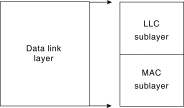
Physical Layer(1)

The lowest layer of the OSI model is concerned with data communication in the form of electrical, optic, or electromagnetic signals physically transmitting information between networking devices and infrastructure. The physical layer is responsible for the communication of unstructured raw data streams over a physical medium. It defines a range of aspects, including:

* Electrical, mechanical, and physical systems and networking devices that include specifications such as cable size, signal frequency, voltages, etc.
* Topologies such as Bus, Star, Ring, and Mesh
* Communication nodes such as Simplex, Half Duplex, and Full Duplex.

Data Link Layer(2)

The second layer of the OSI model concerns data transmission between the nodes within a network and manages the connections between physically connected devices such as switches. The raw data received from the physical layer is synchronized and packaged into data frames that contain the necessary protocols to route information between appropriate nodes. The protocols used in Data link layer are SLIP, PPP, MTU, and CSLP.



**Consists of two sub layers**:

* Logical Link Control (LLC) defines how data is transferred over the cable and provides data link service to the higher layers.
* Medium Access Control (MAC) defines who can use the network when multiple computers are trying to access it simultaneously (i.e. Token passing, Ethernet [CSMA/CD]).

Network layer(3)

Responsible for the routing of data (packets) through the network; handles the addressing and delivery of data. This layer provides for congestion control, accounting information for the network, routing, addressing, and several other functions. IP (Internet Protocol) is a good example of a network layer protocol. Network layer does not deal with lost messages. The network layer is responsible for routing the data via the best physical path based on a range of factors including network characteristics, best available path, traffic controls, congestion of data packets, and priority of service, among others. The network layer implements logical addressing for data packets to distinguish between the source and destination networks.

# Important features of Network layer protocols:

* Concerned with the transmission of packets.
* Choose the best path to send a packet (routing).
* The routing may be complex in a large network (e.g. Internet).
* Routing packets through a network may be accomplished by using simple static routes or by using complex dynamic routing algorithms.

 Transport Layer(4)

The fourth layer of the OSI model ensures complete and reliable delivery of data packets.

Responsible for reliable transmission of data and service specification between hosts. The major responsibility of this layer is data integrity--that data transmitted between hosts is reliable and timely. Upper layer data grams are broken down into network-sized data grams if needed and then implemented using appropriate transmission control. The transport layer creates one or more than one network connection, depending on conditions. This layer also handles what type of connection will be created. Two major transport protocols are the TCP (Transmission Control Protocol) and the UDP (User Data gram Protocol).

Important features of Transport layer:

* Transport layer ensures reliable service.
* Breaks the message (from sessions layer) into smaller packets, assigns sequence number and sends them.

**Important features of TCP/UDP:**

* TCP/IP Widely used for network/transport layer (UNIX).
* TCP (Transport Control Protocol): This is a connection oriented protocol.
* UDP (Universal Data Gram Protocol): This is a connectionless transport layer protocol.
* Application programs that do not need connection-oriented protocol generally use UDP.

Session Layer(5)

The session layer (layer 5) is responsible for establishing, managing, synchronizing and terminating sessions between end-user application processes.

The main functions of the session layer are as follows −

* It works as a dialog controller. It allows the systems to communicate in either half-duplex or full-duplex mode of communication.
* It is responsible for token management. Through this, it prevents the two users to simultaneously attempt the same critical operation.

It defines how to start, control and end a session, including the control and management of multiple bidirectional messages so that applications can be notified when only a portion of a continuous message has been completed, so that the data seen by the presentation layer is contiguous, In some cases, if the presentation layer has received all of the data, the data represents the presentation layer.

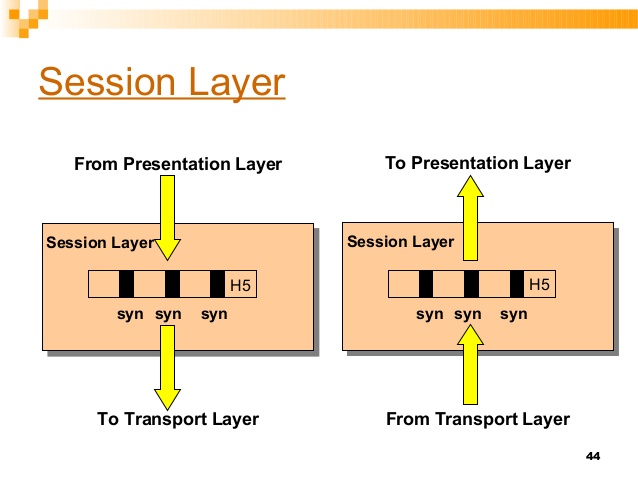


Figure : Session Layer

Presentation Layer(6)

The sixth layer of the OSI model converts data formats between applications and the networks. Responsibilities of the [presentation layer](https://en.wikipedia.org/wiki/Presentation_layer) include:

* [Data conversion](https://en.wikipedia.org/wiki/Data_conversion)
* [Character code translation](https://en.wikipedia.org/wiki/Character_encoding#Character_encoding_translation)
* [Data compression](https://en.wikipedia.org/wiki/Data_compression)
* [Encryption and decryption](https://en.wikipedia.org/wiki/Encryption)

The presentation layer mainly translates data between the application layer and the network format. Data can be communicated in different formats via different sources. Thus, the presentation layer is responsible for integrating all formats into a standard format for efficient and effective communication. Network devices or components used by the presentation layer include redirectors and gateways.

The presentation layer follows data programming structure schemes developed for different languages and provides the real-time syntax required for communication between two objects such as layers, systems or networks. The data format should be acceptable by the next layers; otherwise, the presentation layer may not perform correctly.

Application layer(7)

Provides a means for the user to access information on the network through an application. This layer is the main interface for the user to interact with the application and therefore the network.

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist.

In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

Some examples of application layer implementations include Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

**Common  Application Layer include**:

* File Transfer Protocol (FTP)
* Simple Mail Transfer Protocol (SMTP)
* Domain Name System (DNS)

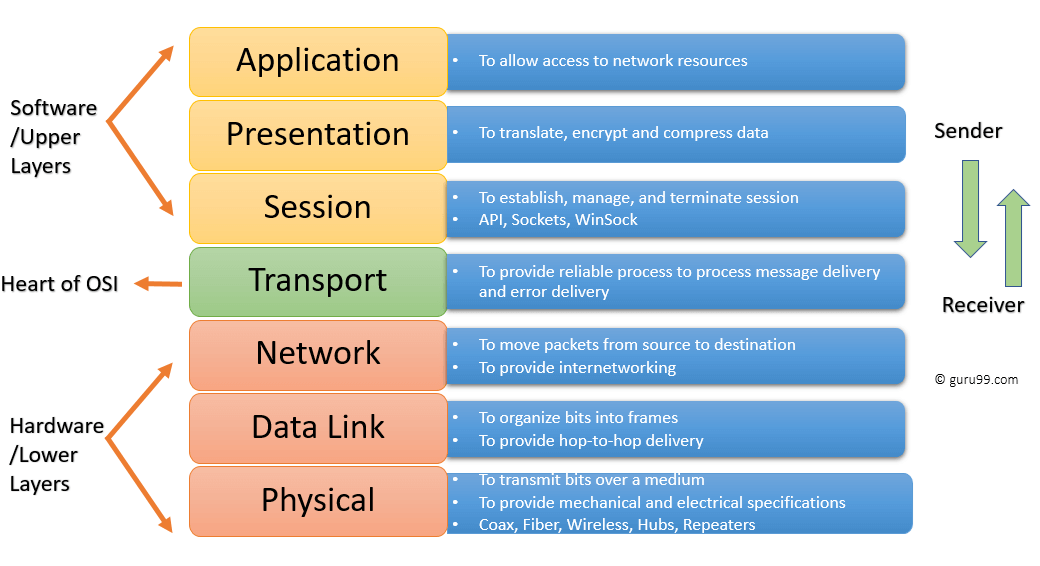


Figure : OSI Layers Diagram

**Transmission Control Protocol (TCP)**

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

**Features**

* + TCP provides error-checking and recovery mechanism.
  + TCP provides end-to-end communication.
  + TCP provides flow control and quality of service.
  + TCP operates in Client/Server point-to-point mode.
  + TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

**The four layers of the TCP/IP model are as follows:**

* Datalink layer: The datalink layer defines how data should be sent, handles the physical act of sending and receiving data, and is responsible for transmitting data between applications or devices on a network. This includes defining how data should be signaled by hardware and other transmission devices on a network, such as a computer’s device driver, an Ethernet cable, a network interface card (NIC), or a wireless network. It is also referred to as the link layer, network access layer, network interface layer, or physical layer and is the combination of the physical and data link layers of the [Open Systems Interconnection (OSI) model](https://www.fortinet.com/resources/cyberglossary/osi-model), which standardizes communications functions on computing and telecommunications systems.
* Internet layer: The internet layer is responsible for sending packets from a network and controlling their movement across a network to ensure they reach their destination. It provides the functions and procedures for transferring data sequences between applications and devices across networks.
* Transport layer: The transport layer is responsible for providing a solid and reliable data connection between the original application or device and its intended destination. This is the level where data is divided into packets and numbered to create a sequence. The transport layer then determines how much data must be sent, where it should be sent to, and at what rate. It ensures that data packets are sent without errors and in sequence and obtains the acknowledgment that the destination device has received the data packets.
* Application layer: The application layer refers to programs that need TCP/IP to help them communicate with each other. This is the level that users typically interact with, such as email systems and messaging platforms. It combines the session, presentation, and application layers of the OSI model.

**User Datagram Protocol (UDP)**

In [computer networking](https://en.wikipedia.org/wiki/Computer_network), the User Datagram Protocol (UDP) is one of the core members of the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite). With UDP, computer applications can send messages, in this case referred to as [datagrams](https://en.wikipedia.org/wiki/Datagram), to other hosts on an [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) network. Prior communications are not required in order to set up [communication channels](https://en.wikipedia.org/wiki/Communication_channel) or data paths.

UDP uses a simple [connectionless communication](https://en.wikipedia.org/wiki/Connectionless_communication) model with a minimum of protocol mechanisms. UDP provides [checksums](https://en.wikipedia.org/wiki/Checksum) for data integrity, and [port numbers](https://en.wikipedia.org/wiki/Port_numbers) for addressing different functions at the source and destination of the datagram. It has no [handshaking](https://en.wikipedia.org/wiki/Handshaking) dialogues, and thus exposes the user's program to any [unreliability](https://en.wikipedia.org/wiki/Reliability_(computer_networking)) of the underlying network; there is no guarantee of delivery, ordering, or duplicate protection. If error-correction facilities are needed at the network interface level, an application may use [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) or [Stream Control Transmission Protocol](https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) (SCTP) which are designed for this purpose.

**Features**

* + UDP is used when acknowledgement of data does not hold any significance.
  + UDP is good protocol for data flowing in one direction.
  + UDP is simple and suitable for query based communications.
  + UDP is not connection oriented.
  + UDP does not provide congestion control mechanism.
  + UDP does not guarantee ordered delivery of data.
  + UDP is stateless.
  + UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

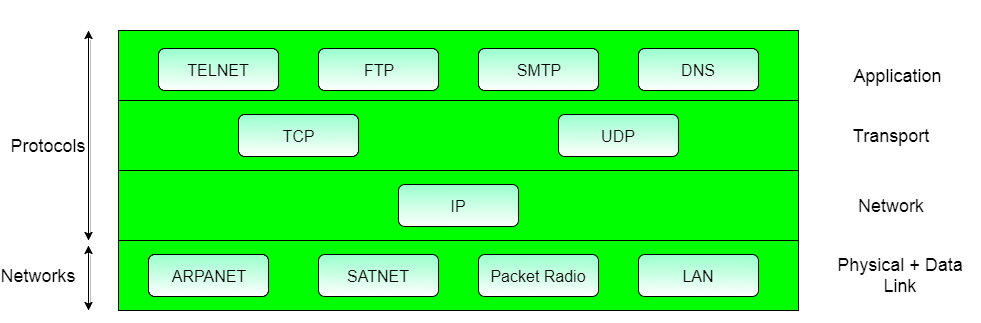
****

Figure : TCP/UDP

**Internet Protocols(IP)**

Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

**Function**

The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more [IP](https://www.javatpoint.com/ip-full-form) networks. In order to achieve these functionalities, [internet](https://www.javatpoint.com/internet) protocol provides two major things which are given below.

**An internet protocol defines two things:**

* Format of IP packet
* IP Addressing system

**L2 protocols**

Layer 2 protocols are a list of communication protocols used by Layer 2 devices (such as network interface cards (NIC), switches, multiport bridges, etc.) to transfer data in a wide area network, or between one node to another in a local area network.

**Layer 2 contains two sublayers:**

* **Logical link control** (LLC) sublayer, which is responsible for managing communications links and handling frame traffic.
* **Media access control** (MAC) sublayer, which governs protocol access to the physical network medium. By using the MAC addresses that are assigned to all ports on a switch, multiple devices on the same physical link can uniquely identify one another.

**Layer 2 Protocols**

There are several L2 protocols used during the engine scan. These include:

* **SNMP**: Simple Network Management Protocol is used for collecting information from devices and configuring them.
* **CDP**: Cisco Discovery Protocol is used to share information about directly-connected Cisco equipment
* **LLDP**: Link Layer Discovery Protocol is used to advertise the identity, capabilities, and neighbors on a wired LAN Ethernet. It gathers the sys name, description, port name, VLAN, etc.
* **STP**: Spanning Tree Protocol works on the switch of a bridged Ethernet LAN, ensuring you do not create loops when you have a redundant path in your network.
* **ARP**: Address Resolution Protocol is used to map an IP address to a physical address (MAC) that is recognized on the local device.
* **FDB**: Forwarding Database is used by Layer 2 devices to store which ports the mac was learned on. When an Ethernet frame arrives at a Layer 2 device, the Layer 2 device will inspect the destination MAC address of the frame and look to its FDB table for information on where to send that specific Ethernet frame

**L3 protocols**

**Queue**

A queue, in computer networking, is a collection of data packets collectively waiting to be transmitted by a network device using a per-defined structure methodology.

You are familiar with queues as lines of people waiting to buy tickets or to talk to a service representative on the phone. A queue is also a collection of objects waiting to be processed, one at a time. In the networking environment, packets are queued up into the memory buffers of network devices like routers and switches. Packets in a queue are usually arranged in first-in, first-out order, but various techniques may be used to prioritize packets or ensure that all packets are handled fairly, rather than allowing one source to grab more than its share of resources.

* + - **FIFO queuing**    This is the basic first-in, first-out queuing technique in which the first packet in the queue is the first packet that is processed. When queues become full, congestion occurs and incoming packets are dropped. FIFO relies on end systems to control congestion via congestion control mechanisms.
    - **Priority queuing**    This technique uses multiple queues, but queues are serviced with different levels of priority, with the highest priority queues being serviced first. Figure Q-2 illustrates Cisco's priority queuing scheme. When congestion occurs, packets are dropped from lower-priority queues. The only problem with this method is that lower-priority queues may not get serviced at all if high-priority traffic is excessive.
    - **Fair queuing**    This method helps solve the problem where some queues may not get serviced because high-priority queues are being serviced. A round-robin approach is used to service all queues in a fair way. This prevents any one source from overusing its share of network capacity. Problems can occur when packets are variable in length and each queue is allowed to release one packet at a time.
    - **WFQ (weighted fair queuing)**    This can be seen as a combination of priority queuing and fair queuing. All queues are serviced so that none are starved, but some queues are serviced more than others. A weight is applied to queues to give some queues higher priority. For example, one queue may get half the available bandwidth and other queues will get an allocation of the remaining bandwidth.

**Scheduling**

In computing, scheduling is the method by which work is assigned to resources that complete the work. The work may be virtual computation elements such as threads, processes or data flows, which are in turn scheduled onto hardware resources such as processors, network links or expansion cards.

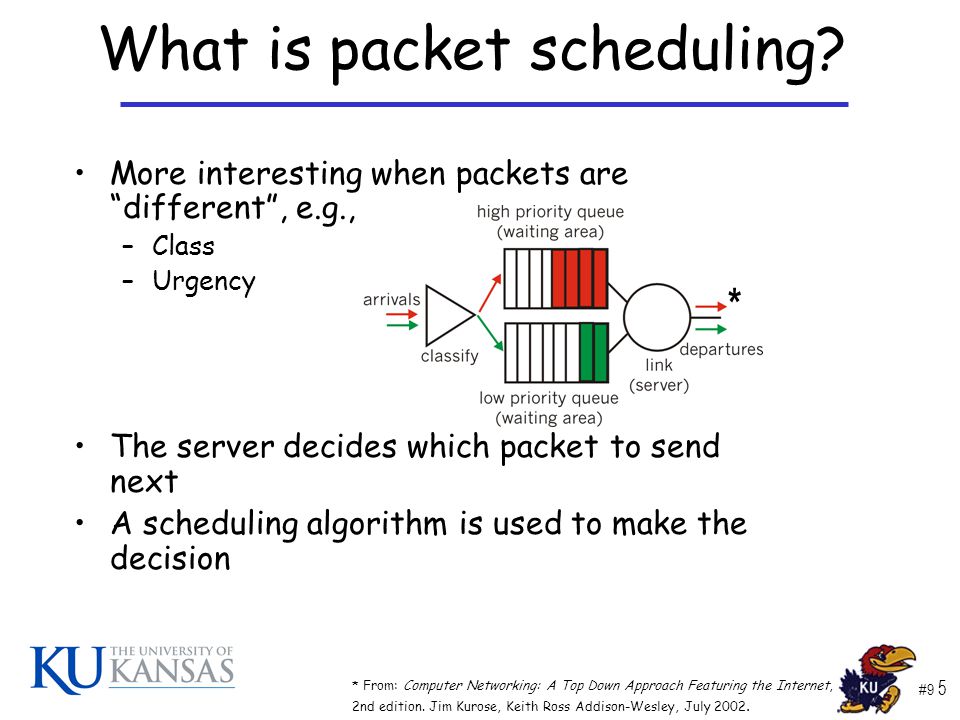


Figure : Working of Scheduling

**The main contributions of the paper are summarized as follows**:

(1)The packet scheduling issue is identified with the SDN controller in edge computing environment. The FCFS-PO and FCFS-PO-P scheduling scheme are proposed for coping with this issue

(2)Analytical model of the proposed scheduling scheme is developed using queueing theory, which can be applied to the evaluation of priority-based scheduling scheme

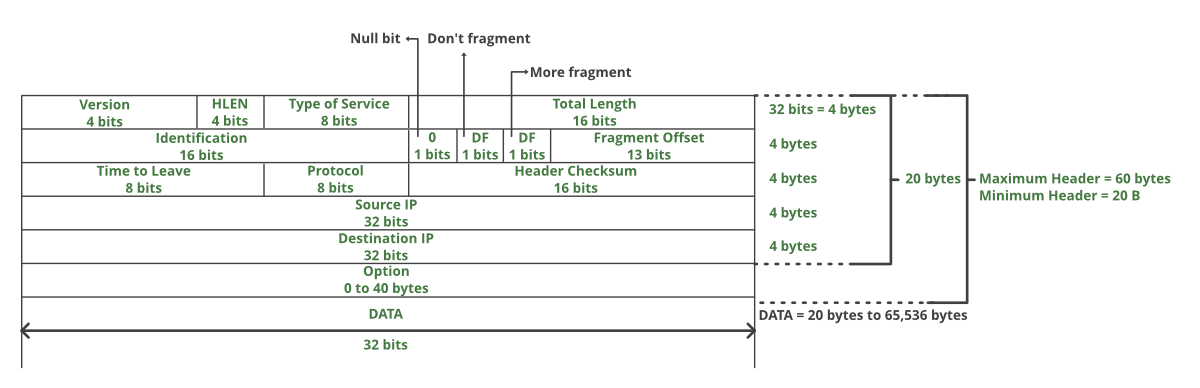
(3)The scheduling for solving the packet scheduling problem of SDN controller in edge computing environment is revealed by comparing the proposed method with existing methods

**Internet Protocol version 4 (IPv4)**

IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

**IPv4 Datagram Header**

Size of the header is 20 to 60 bytes.



**Drawback of IPv4**

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet.

**Internet Protocol version 6 (IPv6)**

IP v6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion. IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes.

**In IPv6 representation, we have three addressing methods :**

* + - Unicast
    - Multicast
    - Anycast

**(1) --Unicast Address:** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.

**(2)--Multicast Address:** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.

**(3)--Anycast Address:** Anycast Address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible).

IPv6 provides several improvements over its predecessor. The advantages of IPv6 are detailed in many other books on IPv6. However, the following list summarizes the characteristics of IPv6 and the improvements it can deliver:

* + - **Larger address space:** Increased address size from 32 bits to 128 bits
    - **Streamlined protocol header:** Improves packet-forwarding efficiency
    - **Stateless autoconfiguration:** The ability for nodes to determine their own address
    - **Multicast:** Increased use of efficient one-to-many communications
    - **Jumbograms:** The ability to have very large packet payloads for greater efficiency
    - **Network layer security:** Encryption and authentication of communications
    - **Anycast:** Redundant services using nonunique addresses
    - **Mobility:** Simpler handling of mobile or roaming nodes

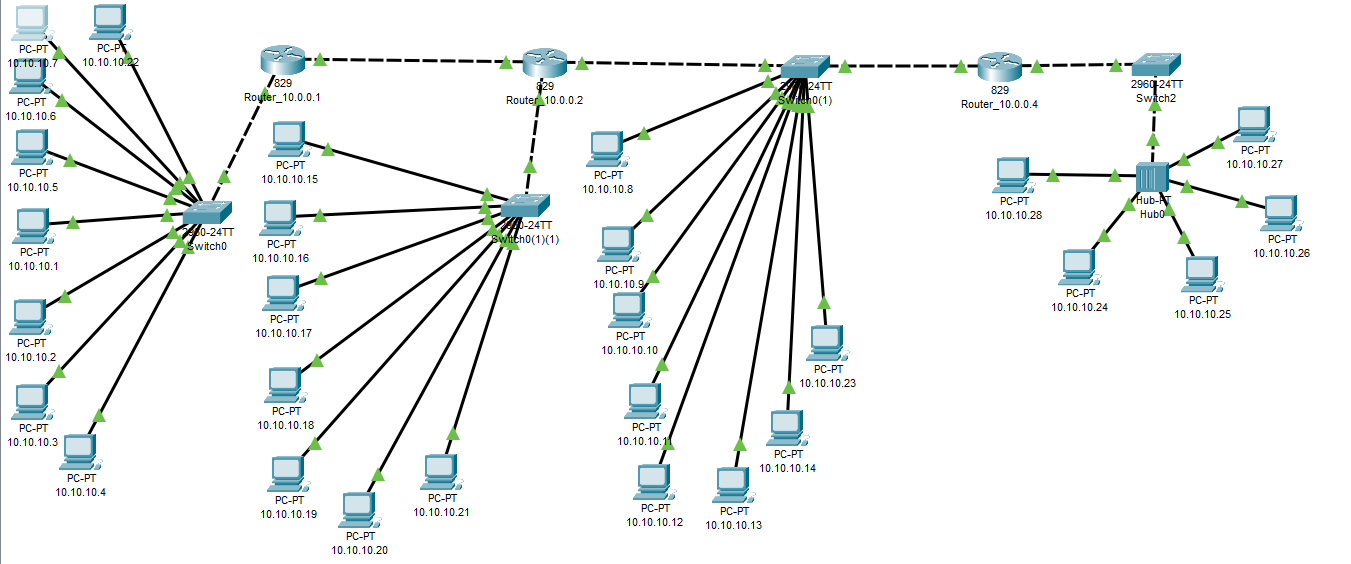
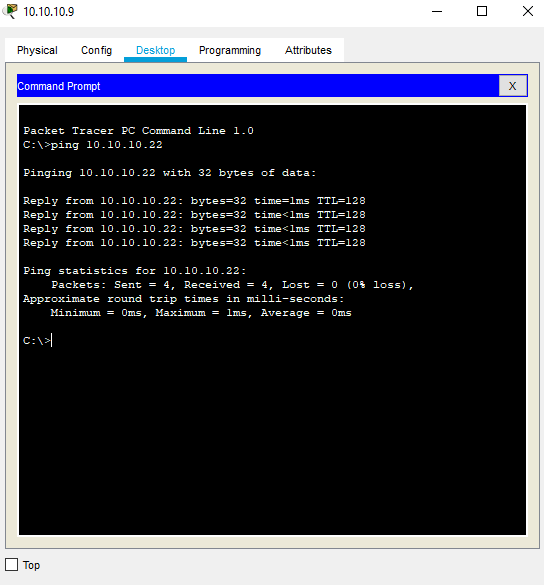


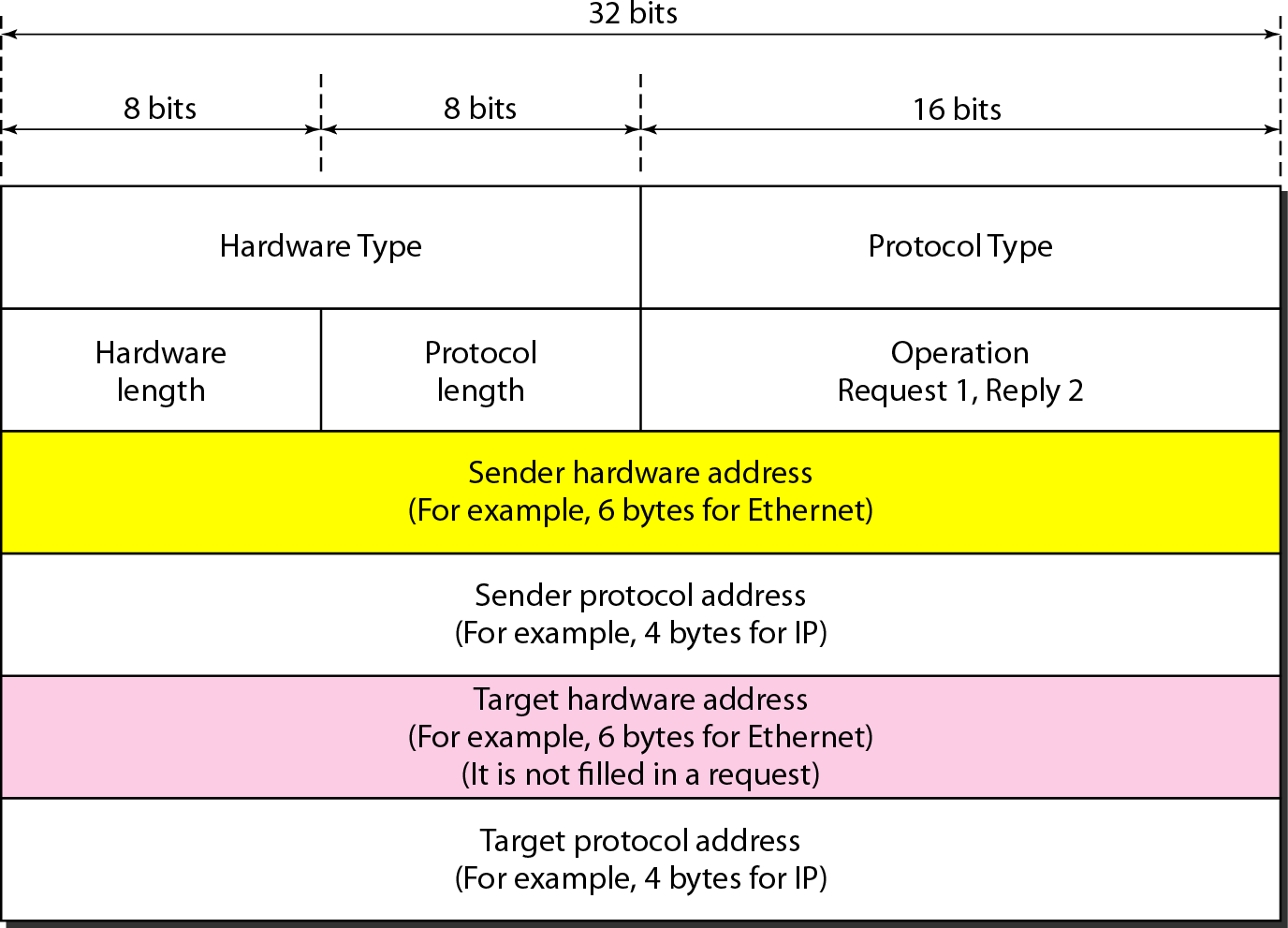
Figure:



# L2 PROTOCOLS

## ARP

* + - 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 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.
    - 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.



**Figure 12: ARP Packet Format**

## RARP

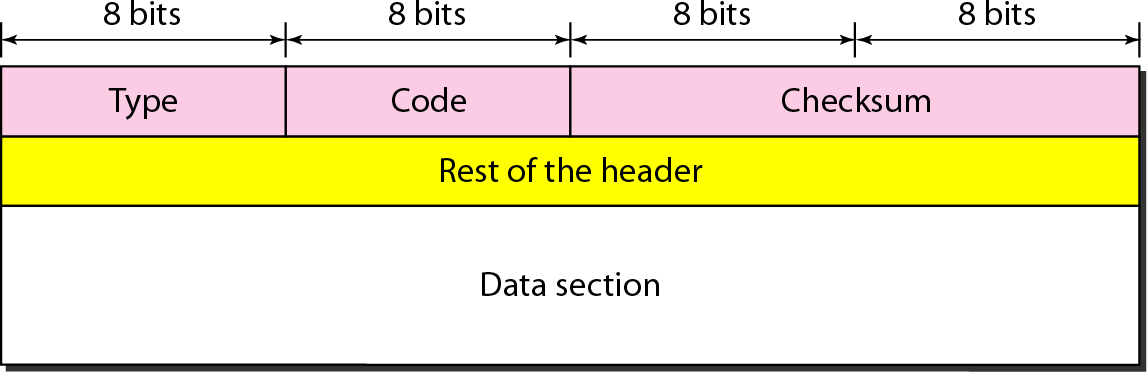
* + - RARP stands for Reverse Address Resolution Protocol.
    - It is used when a host knows its physical address, but needs to know its logical address – no enough IP addresses to assign to each station it needs to assign IP addresses on demand.
    - It uses the physical address to get the logical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

## DHCP

* + - 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.
    - 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.
    - DHCP has a second database with a pool of available IP addresses known as dynamic allocation.
    - 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 of time.

## ICMP

* + - The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.
    - ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.
    - ICMP messages are divided into two broad categories: error-reporting messages and query messages.
    - The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
    - The query messages help a host or a network manager get specific information from a router or another host.



**Figure 13: ICMP Message Format**

# L3 PROTOCOLS

# IPv4

* + IP stands for Internet Protocol and v4 stands for version 4.
  + IP 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:

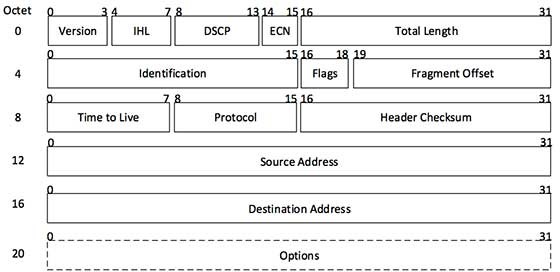
The host part uniquely identifies the machine on your network. This a part of the IPv4 address is assigned to every host. For each host on the network, the network part is the same, however, the host half must vary.

* + - 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.



**Figure 14: IP Header**

## CLASSFUL ADDRESSING

* + - The 32 bit IP address is divided into five sub-classes.

### Class A:

* + - * In Class A, an IP address is assigned to those networks that contain a large number of hosts.
      * The network ID is 8 bits long and the host ID is 24 bits long.
      * 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:

* + - * In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.
      * The Network ID is 16 bits long.
      * The Host ID is 16 bits long**.**
      * 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:

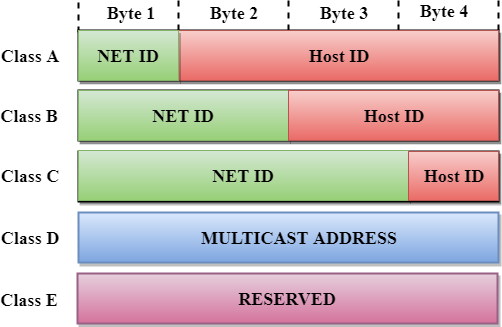
* + - * In Class C, an IP address is assigned to only small-sized networks.
      * The Network ID is 24 bits long.
      * The host ID is 8 bits long.
      * In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID.

### Class D:

* + - * In Class D, an IP address is reserved for multicast addresses.
      * It does not possess subnetting.
      * 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:

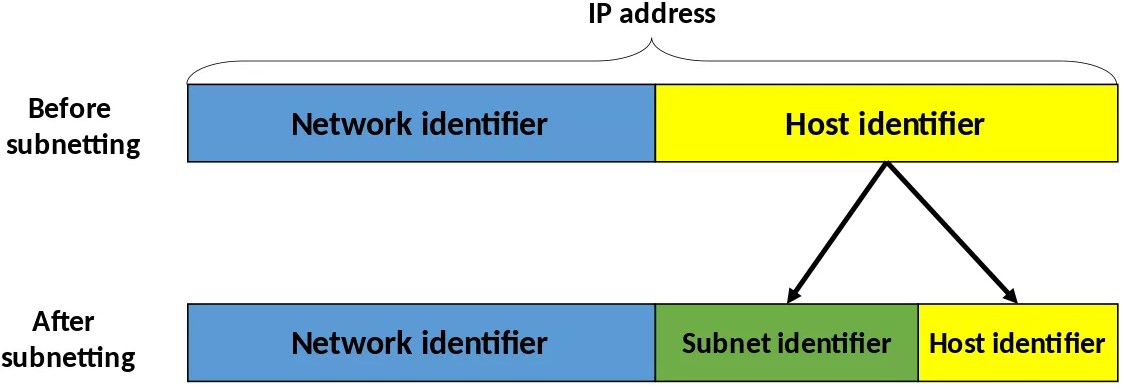
* + - * In Class E, an IP address is used for the future use or for the research and development purposes.
      * It does not possess any subnetting and higher order bits of the first octet is always set to 1111.



**Figure 15: Classful Addressing**

## 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.



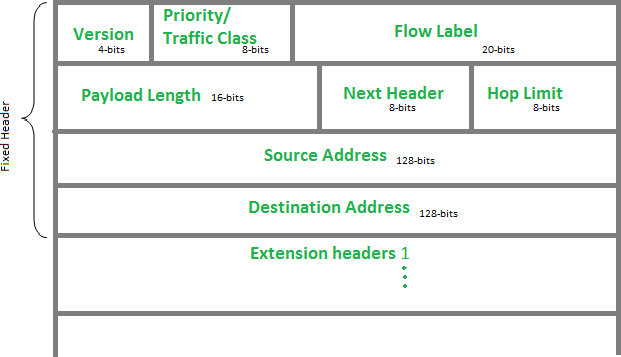
**Figure 16: Subnetting**

### Example: Designing of 3 networks in class B using subnetting.

* + - * IP Address: 132.108.6.0/16
      * 2^2 = 4 networks can be generated by borrowing 2 bits from the host field.
      * Therefore, the no: of host bits are reduced to 16-2 =14 bits.
      * Network has now 16+2=18 bits.
      * The total no: of network addresses become 2^18 and total host addresses become 2^14.

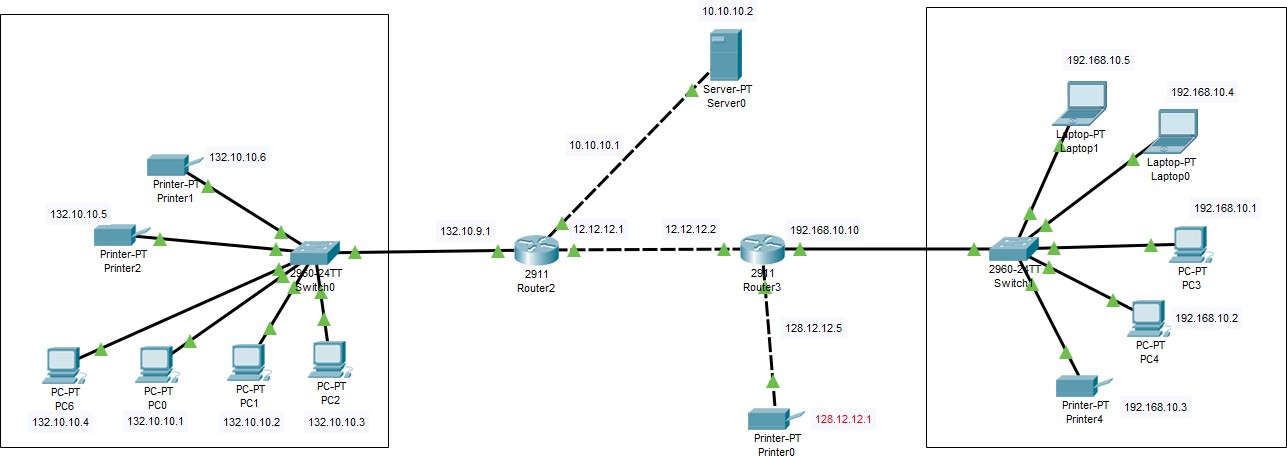
# IPv6

* + 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
    - Multicast
    - Anycast
  + **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.



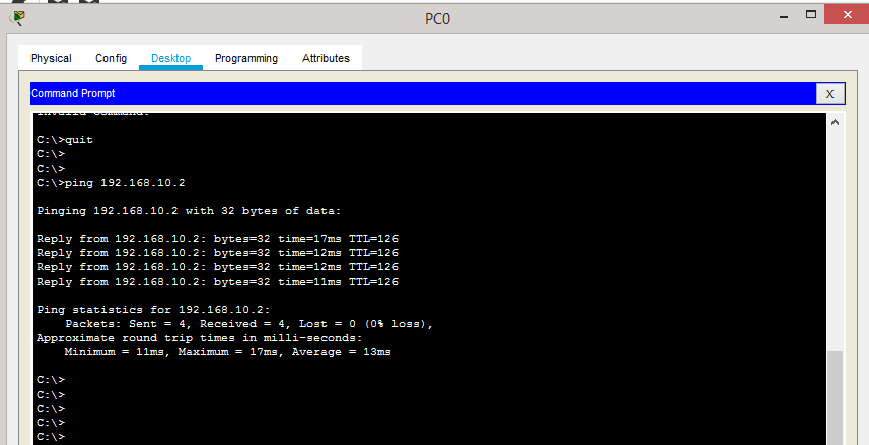
**Figure 17: IPv6 Header**

# CISCO PACKET TRACER OUTPUT



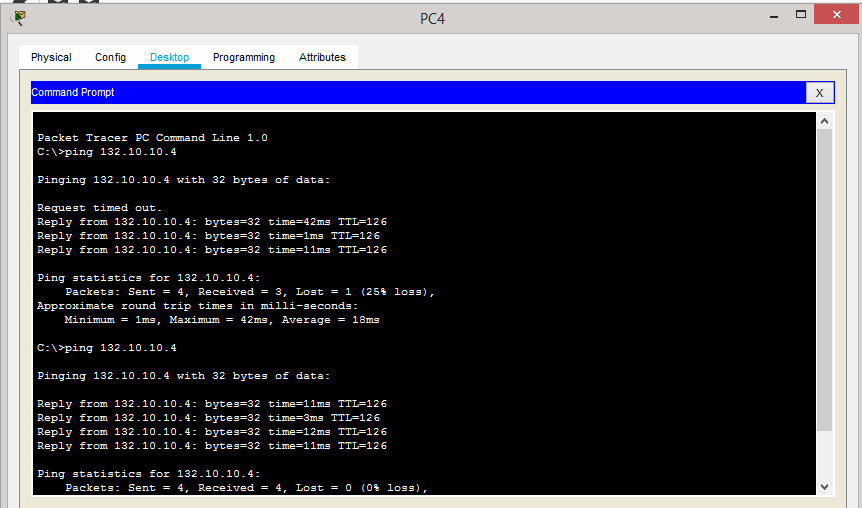
**Figure 18: Network in Cisco Packet Tracer**

## 12.1 Ping output from PC0 (132.10.10.1) to PC4 (192.168.10.2)



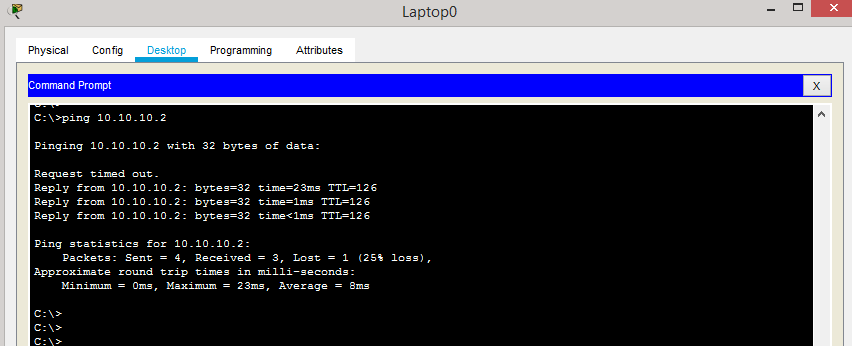
**Figure 19: Ping Output - 1**

## 12.2 Ping output from PC4 (192.168.10.2) to PC6 (132.10.10.4)



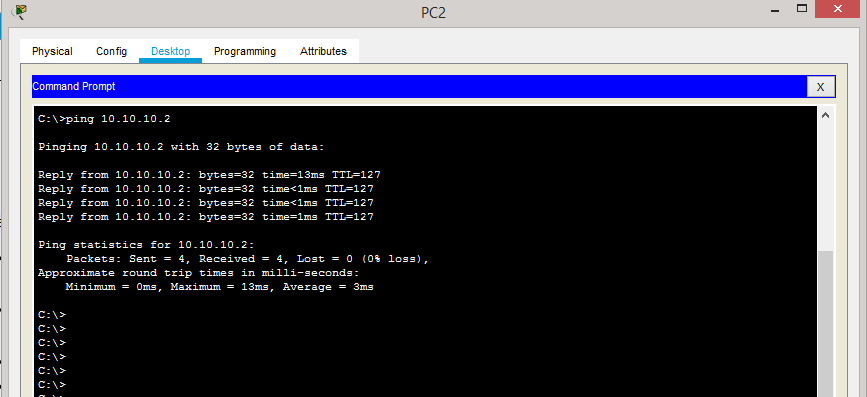
**Figure 20: Ping Output – 2**

## 12.3 Ping output from Laptop0 (192.168.10.4) to server (10.10.10.2)



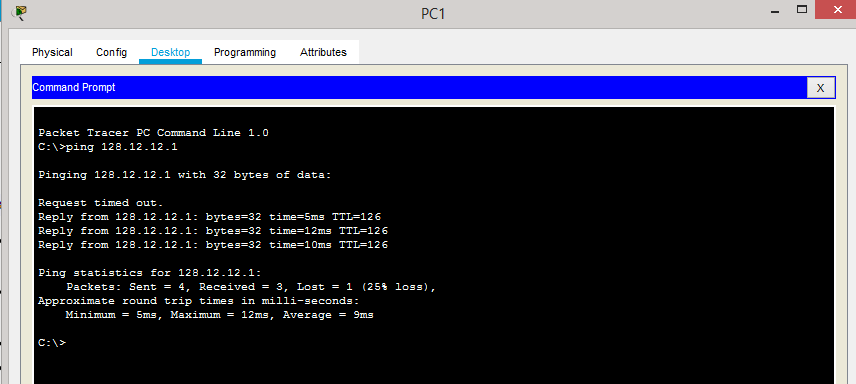
**Figure 21: Ping Output - 3**

## 12.4 Ping output from PC2 (132.10.10.3) to server (10.10.10.2)



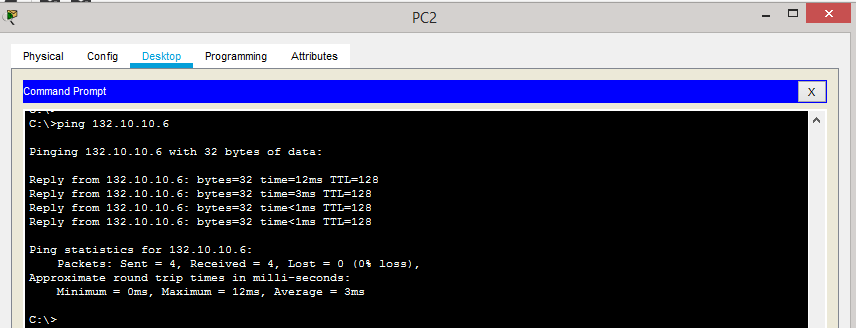
**Figure 22: Ping Output - 4**

## 12.5 Ping output from PC1 (132.10.10.2) to Printer0 (128.12.12.1)



**Figure 23: Ping Output - 5**

## 12.6 Ping output from PC2 (132.10.10.3) to Printer1 (132.10.10.6)



**Figure 24: Ping output - 6**

# REFERENCES

1. Types of Network Topology - GeeksforGeeks
2. 7 Types of Computer Network Topology (With Diagrams) (red-dot-geek.com)
3. Uses of Bridges in Computer Network (tutorialspoint.com)
4. IPv4 Address: Structure, Classes and Types - Video & Lesson Transcript | Study.com
5. https://[www.javatpoint.com/rip-protocol](http://www.javatpoint.com/rip-protocol)
6. https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp- top
7. https://[www.cbtnuggets.com/blog/technology/networking/networking-basics-](http://www.cbtnuggets.com/blog/technology/networking/networking-basics-) what-is- ipv4-subnettingrg/how-address-resolution-protocol-arp-works
8. https://[www.geeksforgeeks.org/how-address-resolution-protocol-arp-works](http://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works)