

Learning Report – Networking



L&T Technology Services



GLOBAL
ENGINEERING
ACADEMY

Genesis



Document History

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	26/03/21	99003779			

Table of Contents

NETWORKING CONCEPTS.....	5
NETWORK TYPES AND TOPOLOGIES	
WIRED AND WIRELESS NETWORKS	
QUEUEING AND SCHEDULING	
NETWORKING SECURITY.....	16
STACK OVERFLOW AND HEAP OVERFLOW	
CRYPTOGRAPHY, ENCRYPTION(FIREWALL)	
SSH,TLS,MTLS	
COMPONENTS.....	19
ROUTERS	
HUB	
SWITCHES	
BRIDGES	
GATEWAYS	
PROTOCOLS.....	21
OSI LAYERS	
TCP/UDP & IP	
L2 PROTOCOLS	
L3 PROTOCOLS	
WLAN PROTOCOLS	
BGP PROTOCOLS	
IP ADDRESS.....	37
IPv4 & IPv6 ADDRESSES	
IPv4 SUBNETTING	
SUBNETTING EXAMPLES	
NETWORK TOOLS.....	47
PACKET TRACER	
WIRESHARK	
END-TO-END DATA FLOW.....	58
TABLE OF FIGURES	
TABLE OF TABLES	
REFERENCES	

Table of Figures

FIG 1: TYPES OF NETWORKS
FIG 2: LOCAL AREA NETWORK
FIG 3: METROPOLITAN AREA NETWORK
FIG 4: WIDE AREA NETWORK
FIG 5: NETWORK TOPOLOGIES
FIG 6: COMPONENTS OF DATA COMMUNICATION
FIG 7: TWISTED PAIR CABLE
FIG 8: COAXIAL CABLE
FIG 9: FIBER OPTICS CABLE
FIG 10: WIRED AND WIRELESS NETWORKS
FIG 11: QUEUEING DIAGRAM FOR SCHEDULING
FIG 12: OSI MODEL SINGLE SIDED AND BOTH SIDED

FIG 13: TCP HEADER
FIG 14: UDP HEADER
FIG 15: IP HEADER
FIG 16: ADDRESS RESOLUTION PROTOCOL
FIG 17: WIRELESS LAN
FIG 18: NODE HOPPING OR INTERCONNECTIVITY FOR BGP ROUTING PROTOCOL
FIG 19: NETWORK OF DNS AND DHCP ON PACKET TRACER SOFTWARE.
FIG 20: CONFIGURATION OF DNS
FIG 21: WEBSITE (GOOGLE.COM) IS ACCESSED.
FIG 22: NETWORK ADDRESS TRANSLATION (NAT)
FIG 23: REPRESENTATION OF IPV6 ADDRESS
FIG 24: CLASSFUL ADDRESSING
FIG 25: SERIAL CONNECTION OF ROUTERS AND NETWORK
FIG 26: TRANSFER OF PACKETS
FIG 27: IPV4 ROUTES ON ROUTER 0 (SHOW IP ROUTE)
FIG 28: IPV6 ROUTES ON ROUTER 0 (SHOW IPV6 ROUTE)
FIG 29: IPV4 ROUTES ON ROUTER 1 (SHOW IP ROUTE)
FIG 30: IPV6 ROUTES ON ROUTER 1 (SHOW IPV6 ROUTE)
FIG 31: IPV4 ROUTES ON ROUTER 2 (SHOW IP ROUTE)
FIG 32: IPV6 ROUTES ON ROUTER 2 (SHOW IPV6 ROUTE)
FIG 33: PINGING FROM IPV4 TO IPV4 IN THE SAME NETWORK
FIG 34: PINGING FROM IPV4 TO IPV4 IN DIFFERENT NETWORK
FIG 35: CAPTURING TRAFFIC FROM ETHERNET
FIG 36: CAPTURE FILTER
FIG 37: DATA TRAFFIC FLOW
FIG 38: END-TO-END DATA FLOW OF OSI MODEL

Table of Tables

TABLE 1: ADVANTAGES AND DISADVANTAGES OF BUS TOPOLOGY
TABLE 2: ADVANTAGES AND DISADVANTAGES OF RING TOPOLOGY
TABLE 3: ADVANTAGES AND DISADVANTAGES OF MESH TOPOLOGY
TABLE 4: ADVANTAGES AND DISADVANTAGES OF STAR TOPOLOGY
TABLE 5: ADVANTAGES AND DISADVANTAGES OF HYBRID TOPOLOGY
TABLE 6: STANDARD CABLES
TABLE 7: WIRELESS STANDARDS
TABLE 8: ETHERNET STANDARDS
TABLE 9: SUBNETS WITH NO. OF IP ADDRESSES
TABLE 10: LIST OF HOSTS

DATA NETWORKING

NETWORKING CONCEPTS:

Data is basically any information which is in binary form. A system that transfers data between different nodes through data switching, system control and interconnection transmission lines is what we called as data network. The exchange of data between 2 devices via a transmission medium and following some kind of a protocol is known as data communication. Data networking and communication is used to transfer data to one or more points called as multipoint. It is of two types namely: Broadcast and Point-to-Point.

Broadcast: when data is transmitted from one point to multipoint then that is known as broadcasting of data. Data broadcasting is again of two types i.e. Independent data broadcasting and linked data broadcasting. Independent data broadcasting is the one which transmits supplementary information directly onto the main television such as news, weather forecast etc. Linked data broadcasting is the one which provides information about the characters of the television drama. For example, in a sports program one can check about the athletes, their information and their progress.

ISDB- T (Integrated Services Digital Broadcasting- Terrestrial) is able to send much more and detailed data through a communication line in order to complement broadcasting of data which has only limited Bandwidth.

Network Types and Topologies:

There are basically 4 types of Networks namely PAN, LAN, MAN, WAN. The figure shown below shows the basic types of data networks:

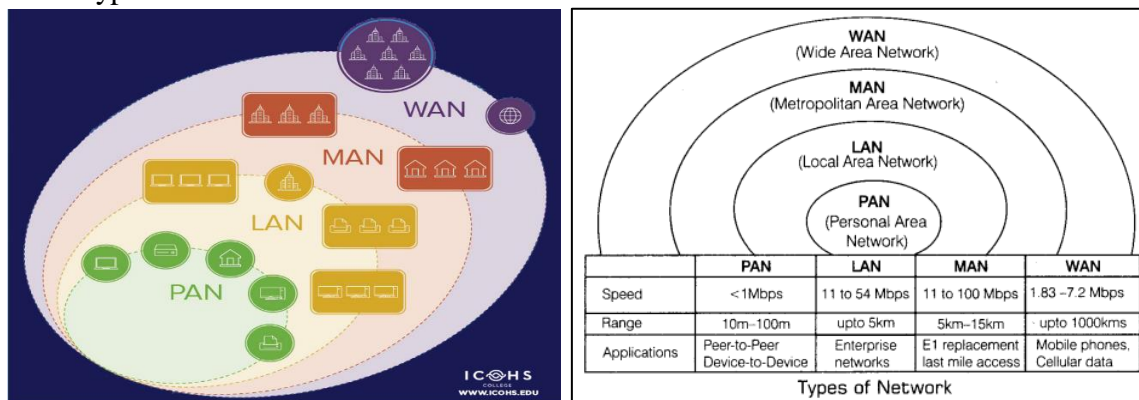


Fig 1: Types of Networks

- PAN (Personal Area Network) :-** It is the smallest network which is personal to the users. It is basically involved with the personal usage of the person that's why named as personal area network. Its range is around 10 meters. It includes Bluetooth, Zigbee, Smartphones, TV Remotes etc. It ranges generally from 10m to 100m with a speed of upto 250 Kbps in zigbee and 24Mbps in Bluetooth.

Some Standards are shown below;

Bluetooth:- Bluetooth was standardized by the IEEE with a standards 802.15.01

802.15.01B

802.15.1.1 Ratified as IEEE Standard 802.15.1–2002

802.15.1.2 Ratified as IEEE Standard 802.15.1–2005

And so on

2. **LAN (Local Area Network):-** It is a network which is local to an area like school, college, office, building etc. It is a privately owned network which can be directly accessed by using an ethernet or a central device like switch or a hub. With Ethernet cables, the speed of data transfer can reach upto 54Mbps and with Gigabit Ethernet, it can reach upto 1Gbps. It ranges from basically 100m to 5km

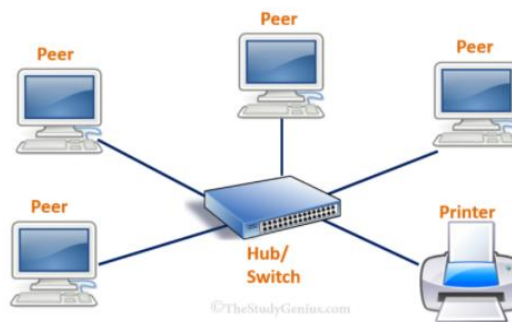


Fig 2: Local Area Network

3. **MAN (Metropolitan Area Network) :-** When two or more LAN are interconnected then a MAN network is formed. It is bigger than LAN but smaller than WAN. For example, an organization has many branches at numerous locations which uses LAN network. So the organization can connect a telephone line over the LAN network to create a MAN network. Its speed is around 100Mbps with a range of upto 15Km.

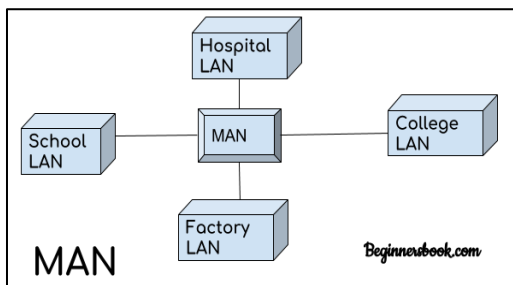


Fig 3: Metropolitan Area Network

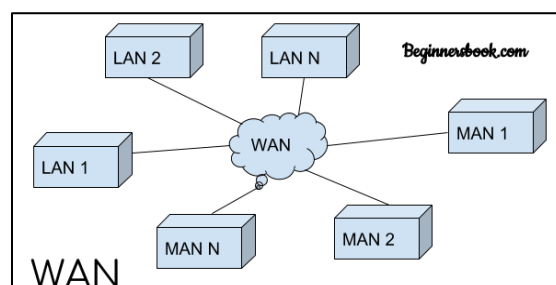


Fig 4: Wide Area Network

4. **WAN (Wide Area Network) :-** It includes a large geographical area like a country or a continent and uses a carrier such as a telephone line or a satellite system etc. It is basically when multiple MANs and LANs are interconnected to form a network then a WAN network is formed. Its Speed speed varies from 1.83 to 7.2 Mbps with a range of upto 1000km

The effectiveness of data communication system depends on 5 fundamental characteristics which includes:

Accuracy:- The accuracy of data transfer should be high i.e whatever data is transmitted must be received at the receiver site. The data that has been changed while transmission and useless.

Delivery:- The data must be delivered to the correct destination. The data transmitted, if received by some other receiver other than the intended one is useless.

Jitter:- Any abrupt change in the delay is what is known as jitter. It is basically defined as the variation in the arrival time of the packet.

Timeliness:- It indicates that the system must deliver the data timely. Any data delivered after the allotted time is useless. Such kind of D=delivery is known as real-time transmission.

Latency:- It is the delay between the transmission time and the reception time. It is less than 10ms in 4G.

Network Topologies:

The way a network has been arranged to transfer the data is known as topology. Network topology is basically defines how a connection, device and nodes are interconnected in a network with respect to each other. There are two approaches to the network topology i.e physical and logical.

Physical:- It refers to the actual wired connections of how the networks are arranged.

Logical:- The logical topology refers to the high level idea of the interconnection of nodes and devices on the network. It also determines how the data is transmitted over the network.

Types of Topologies: -

- 1. Bus Topology:** It is responsible for the orientation of all the devices on a single cable from one end to another in a single direction. It is also known as line topology or the backbone topology.

Table 1: Advantages and disadvantages of Bus topology

Advantages	Disadvantages
1. Bus topologies are a good, cost-effective choice for smaller networks	1. It uses a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.
2. As the layout is simple, so it allows all the devices to be connected via a single coaxial cable or RJ45.	2. Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.
3. More nodes can be easily added to the network by joining additional cables.	3. Data is "half-duplex", which means it can't be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

- 2. Ring Topology:** It is a topology where nodes are arranged in rings. The data can travel in one or both direction through a ring network.

Table 2: Advantages and disadvantages of Ring topology

Advantages	Disadvantages
1. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.	1. A ring topology is vulnerable to failure without proper network management.
2. It reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.	2. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays.
3. Ring topologies are cost-effective and inexpensive to install	3. The entire network must be taken offline to reconfigure, add, or remove nodes.

3. **Mesh Topology:** It is an integrated structure of point to point network. Here each node is connected to all the other nodes.

Table 3: Advantages and disadvantages of Mesh topology

Advantages	Disadvantages
1. Mesh topologies are reliable and stable,	1. Mesh topologies are incredibly labor-intensive.
2. the complex degree of interconnectivity between nodes makes the network resistant to failure.	2. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up.
3. no single device going down can bring the network offline.	3. the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

4. **Star Topology:** It is one of the most common topology in which every node is connected to a central hub via a fiber optic, twisted pair, or coaxial cable. The central hub is responsible for managing data transmission and hence functions as a repeater.

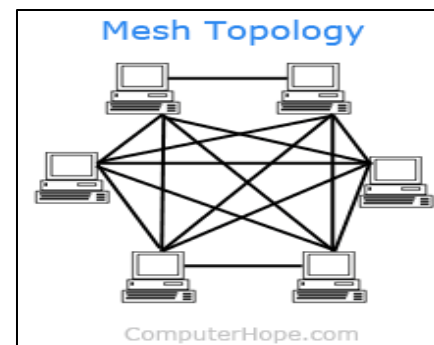
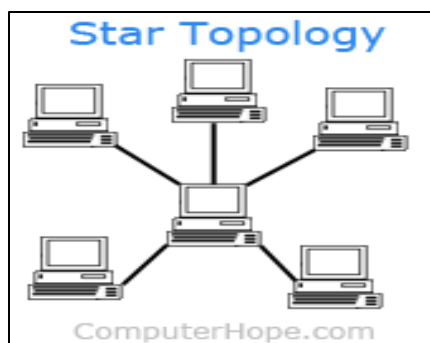
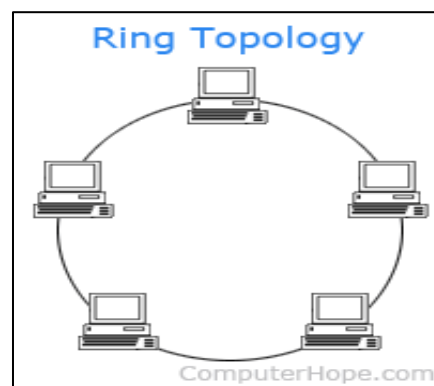
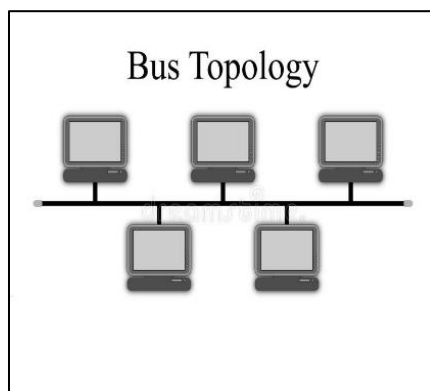
Table 4: Advantages and disadvantages of Star topology

Advantages	Disadvantages
1. Each of the nodes is independently connected to the central hub, if one goes down, the rest of the network will continue functioning unaffected.	1. If the central hub goes down, the rest of the network can't function.
2. Devices can be added, removed, and modified without taking the entire network offline.	2. The overall bandwidth and performance of the network are also limited by the central node's configurations
3. The structure of the star topology uses relatively little cabling	3. Star topologies expensive to set up and operate.

5. Hybrid Topology: It combines two or more different topologies. It is mostly used in larger companies where each department is having a personalized network topology as per their need.

Table 5: Advantages and disadvantages of Hybrid topology

Advantages	Disadvantages
1. Can be modified as per requirement.	1. Design of a hybrid network is very complex.
2. It is extremely flexible and reliable.	2. There is change hardware to connect topology with another topology.
3. Error detecting and troubleshooting is easy	3. Usually hybrid architectures are usually larger in scales so they require a lot of cables in installation process.



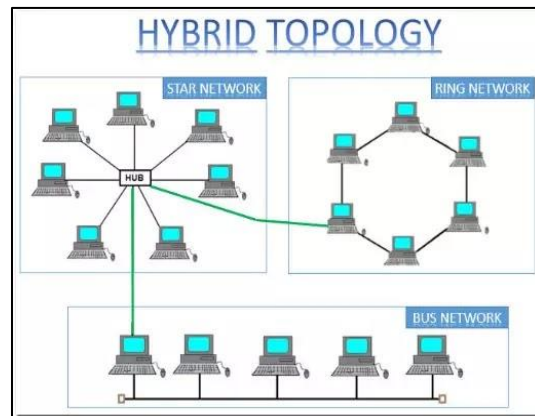


Fig 5: Network Topologies

Data Communication system has five components namely:

1. **Message:** Any piece of data which needs to be communicated is a message. It is the most useful asset of a communication system.
2. **Sender:** Any device which is responsible for sending the data from transmitter is known as sender.
3. **Receiver:** It is the destination which receives the data send by the transmitter.
4. **Transmission medium:** The bridge between transmitter and receiver is known as medium. It could be through twisted pair cable, microwaves, fibre optic cable, radio waves, etc. . It can be simplex, half duplex or full duplex. Transmission medium in detail on wired and wireless is explained later.
5. **Protocols:** These are the set of rules which governs the transmission of data from transmitter to receiver.

Lets take an example of data communication system in sending an email. Here the user who sends an email acts as a sender, the receiver of email is the reciver and message is the data. Email is an example of application layer where SMTP protocol is used. However there are many protocols involved in the whole process. Below is the explanationof whole OSI action in sending an email.

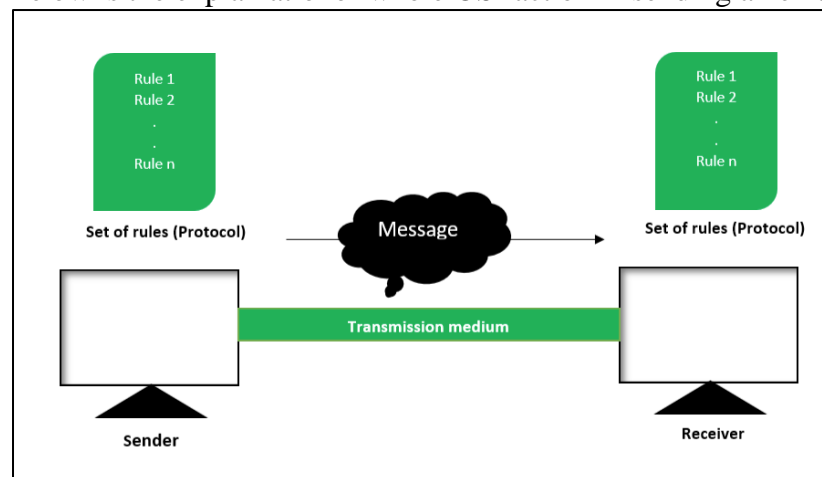


Fig 6: Components of data communication

Wired and Wireless Networks:

1. Wired Networks: It is also known as guided media. It provides a channel from one device to another, using dual-twisted cable, coaxial cable, and fiber-optic cable. Signal movement for any of these devices is governed by medium.

- **Twisted Pair Cable:** The twisted cable has two drivers (usually copper), each with its own plastic to divide, to twist together. One of the cables is used to carry signals to the receiver, while the other is only used as a ground reference. The recipient uses the difference between the two.

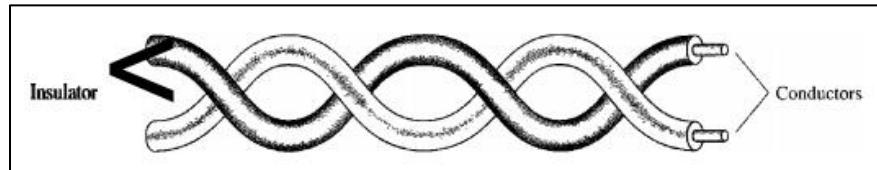


Fig 7: Twisted Pair Cable

In addition to the signal sent by the sender on one of the cables, interference (sound) and the crosstalk can touch both wires and create unwanted signals. These are of two types:

Shielded twisted pair & Unshielded twisted pair:

The commonly used twisted cable that is widely used in communication is called UTP. IBM has also produced a twisted type of cord for its use called shielded twisted-pair (STP). The STP cable consists of a metal foil or mesh cover that encloses two of the inserted conductors. Even metal wrapping improves cable quality by preventing sound intrusion or crosstalk, of course bulkier and more expensive.

- **Co-axial cable:** These cables carry a relatively higher signal frequency than those of twisted-pair cable. This is because the medium of two wires are different.

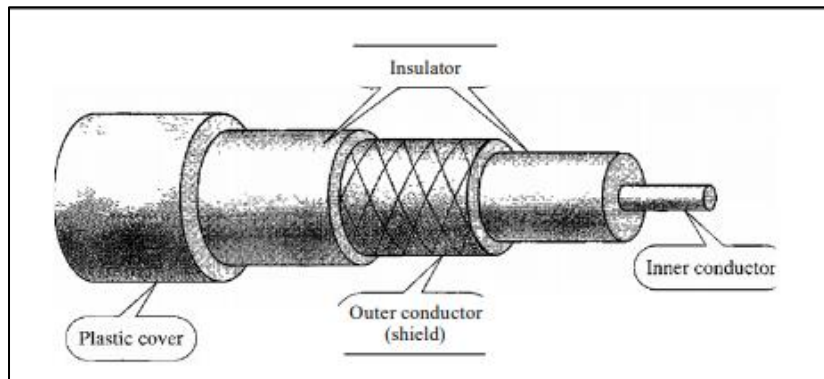
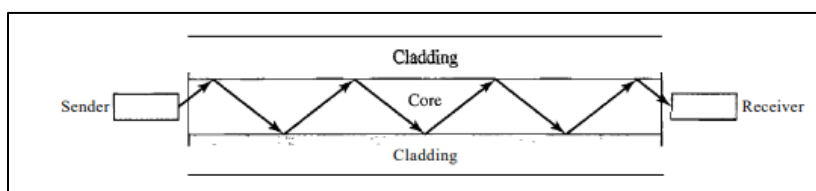


Fig 8: Coaxial Cable

- **Fiber optic cable:** These are made of plastic or glass and transmits signal in the form of light.

**Fig 9: Fiber Optics cable**

Most commonly used cable is UTP. Following are the list of standard cables including RJ45. RJ 45 is an 8 pin cable which is used for computers, Ethernet network adapters etc.

Table 6: Standard Cables

RJ = Registered Jack						
Nomenclature example	Connector Series	Capability	Number of Positions	Pins installed	Typical Uses	Twisted pair wire
	RJ10		4	4	telephone, data	UTP
6P2C	RJ11	1 phone line	6	2	standard telephone connection	UTP
	RJ12		6	6	telephone, data	UTP
6P4C	RJ14 same connector as RJ11	2 phone lines	6	4	connection for two analog phone lines	UTP
	RJ22		n/a	n/a	n/a	UTP
6P6C	RJ25	3 phone lines	6	6	telephone, data	UTP
8P8C	RJ45		8	8	ISDN, LAN, data	UTP
	RJ48X		10	8,10	data	

2. Wireless Networks are those which are made of wireless medium or unguided medium like radio waves, microwaves or infrared.

- **Radiowaves:-** These are the EM Radiations in which wavelength are in the EM Spectrum which is longer than those of Infrared Radiations.
- **Microwaves:-** It is a widely used radiations in the field of tool synthesis and chemical application of coordination compounds. It is used for point to point communication of data from one point to another. It is involved in long distance communication.
- **Infrared Waves:-** These are the waves which falls in the EM spectrum. These are basically used in TV etc. These radations are popularly known as heat radiations.

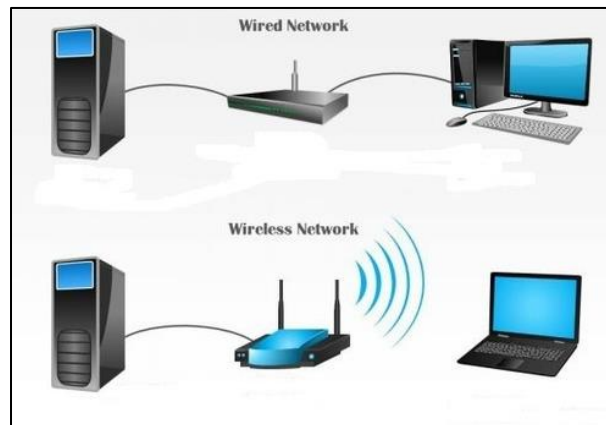


Fig 10: Wired and Wireless Networks

Some wireless standards are shown below:

Table 7: Wireless Standards

S. No	Transmission Standard	Description
1.	802.11a	1. Very high transmission speeds of 54Mbps. 2. It has a high frequency of 5GHz range 3. It employs Orthogonal Frequency Division Multiplexing (OFDM).
2.	802.11b	1. Supports 11Mbps speed. 2. Operates within the frequency range of 2.4GHz 3. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
3.	802.11g	1. Supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). 2. Provides high speeds, varying signal range, and resilience to obstruction. 3. It is more expensive for implementation.
4.	802.11n	1. Popularly known as Wireless N, this is an upgraded version of 802.11g. 2. It provides very high bandwidth up to 600Mbps 3. It uses Multiple Input/Multiple Output (MIMO) 4. The implementation is highly expensive.

Queuing and Scheduling:

The queuing and scheduling included in the interface allows the traffic to be divided into multiple lines so that the schedule can determine what type of action the traffic within each queue it receives. If the traffic placed on each queue is for a particular category of service, the scheduler may apply a separate code for different categories of service

Buffer and bandwidth are the two most important parameters which is associated with queuing and scheduling. Buffer is basically the queue length, that is, how much memory is available for storing packets. However, the whole package does not need to be lined up, sometimes stored as a notification,

which is an indication of the content of the package. The buffer value can be defined either as the amount of time the packets are received on the interface when the queue is enabled or as a portable size depending on how many packets or notifications of the packs remain on the line at a time. The buffer value is the amount of memory available and can be defined as milliseconds of traffic or the total number of packets.

Bandwidth parameter means the scheduling component of the equation. The total amount of bandwidth is made available to scheduling and queuing process. Scheduling determines how much is shared on each line. The total amount of bandwidth can be the speed of the interface or the size of the shaper if I is applied post scheduler.

The queue and schedule used, determine how resources are distributed. The need for queue and schedule is usually determined by the presence of traffic congestion. If resources are available and there is no resource competition, there is no need to line up. Another way to build traffic is to put more traffic on a connector than an outgoing line speed that can support it. Congestion can also be created incorrectly, by using a rate on the connector that sets the speed limit lower than the visible line speed. The remaining traffic was crashed or pressed back into memory, then separated from the actual lines. The scheduler also uses the queue and monitors the rate at which packets from each line are sent.

The packet enters the line at the tail, stays in line until it reaches the head, and then leaves the line. In the line system, packets may be discarded from the tail or head of the line, and both may be discarded at the same time. Usually, the packets are discarded at the tail. When the filling rate is much faster than the subtraction level, the buffer fills up completely. The result is that no packets can be placed in the buffer, and any newly arrived package should be discarded.

But the queue can throw packets from the head. The data at the head of the line are the ones that go from the tail to the head, so they are the ones that stay in line the longest. In overcrowding and resource starvation, the line does not find editing spaces. To avoid queuing up, and to have a long and hopeless period of traffic jams, it is often forced on all data in the queue how long they are allowed to stay in queue, waiting to be scheduled. The name of this is the aging of the packets, which means that the old packets are out of line because there is no point in trying to deliver them.

Tail drops and data aging are not associated. If, to remove the line, the rate at which the packets fall on the head of the queue cannot match the level at which the data enter the line at the tail, the drop of the packet may occur on both the tail and the head due to the wear of the packet.

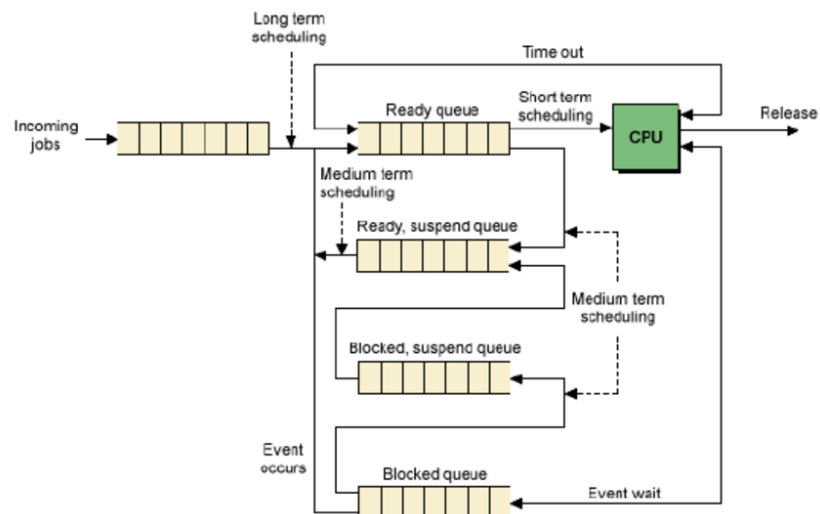


Fig 11: Queueing diagram for scheduling

NETWORK SECURITY

In order to send the data over the internet, security is one of the major concerns now-a-days. So, firewall is used for this purpose.

Stack and Heap overflow:

There are two types of overload: stack and heap. Stack and heap are two areas of memory structure shared when the system is running. Calling functions are stored in the stack, and dynamic variables are stored in a heap. A certain amount of memory is given to the buffer. Static variable storage (variables defined within a function) is called a stack, because it is actually stored in a stack in memory. The Heap data is a memory that is strongly distributed during operation. This data is actually not stored in a stack, but somewhere in the middle of a large "mass" of temporary, discarded memory used for this purpose. In fact, exploitation is a major factor, as there are no simple framework indicators (as there are stacks) that you can write over.

Attackers can use buffer overload to override a password, file name, or other data. When the file name is rewritten, a separate file will be opened. If this is a usable file, the code that was intended to be valid will apply.

The overflow of the buffer is based on how the editing languages work. Most calling functions do not check to ensure that the buffer will be large enough to hold the copied data in it. System planners can use phones that perform these tests to prevent overcrowding, but many do not.

Creating a massive buffer attack requires the intruder to understand the assembly language and technical details about the OS in order to be able to write code that will fit into the stack. However, the code for this attack is usually published so that others, with little technical knowledge, can use it. Some types of fire extinguishers, called experimental firefighters, allow for buffer overflow attacks, while application gates (if properly configured) can filter out excessive buffer attacks.

Buffer overload occurs when a task / function writes more data to a variable (actually just a memory location) rather than a variable designed to capture. The result is that data starts to overwrite other memory areas without computer experts to make things worse, most hardware structures (like Intel and Sparc) they use a stack (a storage repository) to store recovery addresses. So, the problem is that overloading the buffer will overwrite these recovery addresses, and the computer — not knowing anything better — will still try

to use them. If the attacker has enough skills to accurately control which values were used to overwrite recovery returns, the attacker can control the next (computer) operation of the computer.

Firewall:- It is a security system of the network which is used to monitors and controls all the outgoing and incoming network traffic depending upon the defined and advanced set of protocols. It is basically a software program which prevents illegal access to and from a private network.

A firewall usually performs the following task :

- Defend resources
- Manage and control network traffic
- Validate access
- Acts as an intermediary
- Record and report on events

Another way that allows a secure connection to another network over the internet is by establishing a VPN connection.

VPN (Virtual Private Network) :

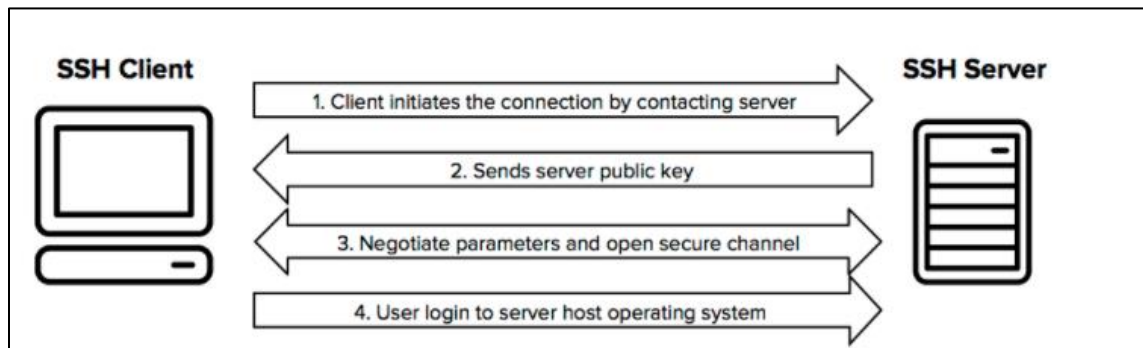
It is an encrypted connection over the internet . VPN connects a laptop, PC or smartphone to another computer, somewhere over the internet and allows to browse the internet using that computer's internet connection [8]. A VPN is formed by joining two or more VRF (Virtual Router Forwarding). So that they can share the routing table and can communicate with each other.

- **Tunneling** is one of the most important process in VPN. In this data is send privately over the internet. In a tunnel connection , every packet is placed under another packet before sending over to the internet. This is known as encapsulation.
- **Cryptography:** It is the process by which data is protected and communicated over the internet with specific codes, so that the message will be read by the one for whom it is written. Cryptography is the basically the study encryption and decryption
- **Encryption:** It is the process of coding the message for a secure communication over the internet.

SSH, TTL, and MTLS:

Tunneling process occurs with the help of different protocols which includes SSH (Secure Shell), TTL(Time To Live) and MTLS (Mutual Transport Layer Security)

- **SSH:** The SSH protocol uses encryption to protect the connection between the client and the server. All user authentication, commands, output, and file transfers are encrypted to protect against network attacks.



- **TTL:** Life time (TTL) determines how long the query or content is stored. TTL's core business is focused on managing information packets regarding DNS requests. When one of these packages is created and transmitted online, there is a chance that it will pass, continuously, from a permanent route to a permanent route. To prevent this from happening, each packet has a specific TTL or hop limit. It is also possible to check the TTL data packet for details of how it went online during its journey.

Within each packet, there is a specified location where the TTL value is stored. This is the tag, and it shows how long the package should go over the internet. When the router receives the data packet, it removes one unit from the TTL number before sending it to the next location within the network. This continues to occur until the TTL inside the packet is dropped to zero.

At that point, the router removes the data packet and transmits the Internet Control Message Protocol (ICMP) message to the host where the package originates. ICMP is a protocol that allows devices to communicate and transmit errors regarding data packets.

- **MTLS:** MTLS Agreements provide encrypted communications and authentication of final points on the Internet. The server-server connection depends on MTLS authentication. In an MTLS connection, the server from the message and server receives the exchange certificates from a trusted CA. Certificates prove the identity of each server.

COMPONENTS OR THE CONNECTING DEVICES:

Devices which operates at different layers are known as connecting devices or the components. It includes routers, hub, switches, bridge, gateways.

- 1) The device which works below physical layer are known as passive hub. These are the repeaters which slows down the signal propagation.
- 2) The device which works at the physical layer are known as Active Hub. These are multiport repeaters which is used in star topology.
- 3) The device that works at physical and data link layer is known as bridge or a layer 2 switch
- 4) The device that operates at physical layer and network layer are called as router or a layer 3 switch.
- 5) The device that works at all the layers are known as gateway.

Following are the functions of each Components:-

Functions of Hub:

1. It amplifies signal
2. It do not filter data packets based on destination.
3. There is no path determination or switching.
4. It do not buffer incoming traffic.
5. It propagates signal through the network.

Functions of bridge:

1. It connects and passes packets between two ne segments.
2. It is intelligent than hub.

Functions of Switch:

1. It is a multiport bridge.
2. It isolates traffic in various domains.

Functions of Router:

1. It routes the packet based on their logical address.
2. It is software oriented as router configurations are needed. It is faster than others.

PROTOCOLS

OSI Model:- Data (Packet) transmission over the internet

When data is sent from one server to another, it goes through all the 7 layers of the transmission model from top to bottom and bottom to top. At one side these layers talk to its upper layer and at the other side they talk to their lower layers. There is also side to side communication i.e each layer talks to their corresponding layer in the other side eg. application layer of one side communicates with only the application layer of the other side, it cannot talk to the presentation layer of the other side.

The communication between different layers for passing of the data and the network information is made possible by interfaces existing between each pair of adjacent layers. Layered functions and well defined interfaces provides modularity to the network. The OSI model is a layered framework for the designing of a network system that is establishes connection between all types of computer system.

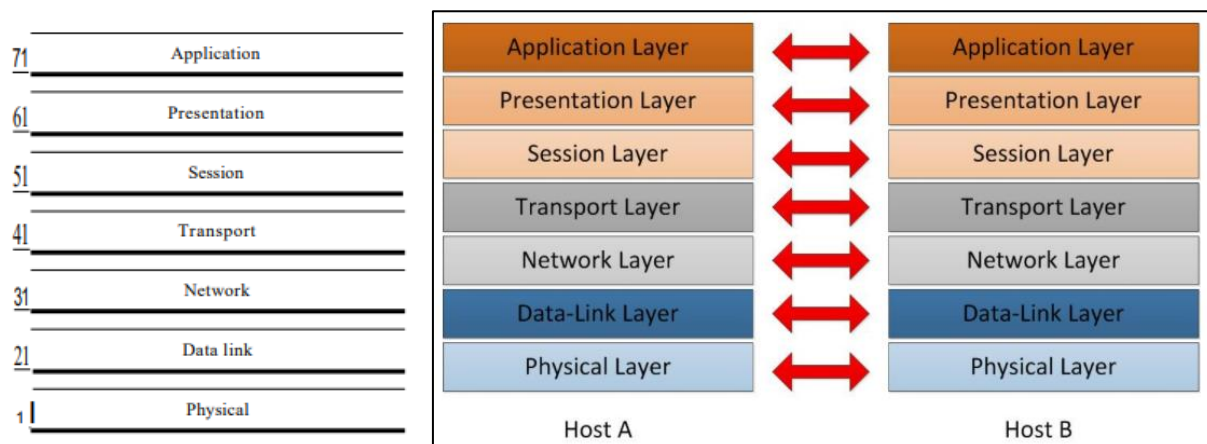


Fig 12: OSI Model Single sided and both sided

Data is transmitted over the internet not in its actual form but rather they are subdivided into smaller packets and the transmission between computers (or server) across the internet is featured by different protocols [7]. It is a seven layered model consisting of physical, data link, internet (network), transport, session, presentation and application layer. When an email is sent from one server to another, it goes to the application layer of the OSI model. It provides interface to the user in order to tell the computer how to handle the data. Gradually, the data and information moves to different layers using different protocols and reaches to its destination. The protocols has been discussed in the latter sections.

Physical layer :-

- It coordinates function required to carry a bit stream over physical layer.
- It is a peer-to-peer communication.
- It provides physical and electrical specification for device and medium.
- It is responsible for representation of bits and synchronization of sender and receivers clock.

Data link layer:-

- It makes the unliable physical layer to a reliable link.
- It converts bit streams into manageable units called frames.
- It provides physical addressing to the frames and responsible for node-to-node delivery.
- It is also responsible for error control and detection of damaged, duplicate or lost frames.
- Protocols at this layer includes:

1. **Ethernet:-** Ethernet is not a single thing, it refers to a family of standards. The main purpose of Ethernet is to act as a single LAN technology even if the data can pass through different types of connections (visible and copper cables, wireless connectors) at different speeds (from 10Mbps trough 100Gbps), because it uses the same data- various media and technologies. However, the network engineer should be aware of the names of at least the most commonly used Ethernet standards such as FastEthernet and GigabitEthernet.

Table 8: Ethernet Standards

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name
10 Mbps	Ethernet	10BASE-T	802.3
100 Mbps	FastEthernet	100BASE-T	802.3u
1 Gbps	GigabitEthernet	1000BASE-T	802.3ab
10 Gbps	10 GE	10GBASE-T	802.3an
40 Gbps	40 GE	40GBASE-T	

IEEE standards include:

Logic Link Layer (LLC): 802.2

Wired Network or ethernet: 802.3

Wifi: 802.11

Bluetooth: 802.15

WiMax: 802.16

2. **Token Ring :-** It is a protocol used in communication of LAN Network. This topology is used to define the order in which the stations send. The connections of stations are shown below. Token is a three byte single frame. It travels around the ring. Token passing is the mechanism which is used here. Data packets are also transmitted in the same direction as that of the token. The station that carries the token is the one which transmits the data packets.
3. **RS 232:-** RS 232 is the communication protocol used for serial communication. It allows the connected servers to and its peripheral devices to allow serial exchange of data between them. RS 232 is used for connecting DTE i.e. data transmission equipment and DCE i.e data communication equipment.
4. **FDDI/ FTTH :-** It is Fiber distributed data interface/ Fiber to the home which is a set of ANSI and ISO standards for data transmission over LAN via fiber optics cable. It is applicable only to the LAN which is over the range of 200 km in diameters.

Network layer:-

- It is responsible for host to host delivery i.e source to destination delivery of the packets across multiple networks.
- It is responsible for providing logical address and also performs the function of routing.
- It is L3 Layer consisting of various routing protocols, discussed further.

Transport Layer:-

- It is responsible for process to process delivery of the packets.
- It is also responsible for segmentation, sequencing and service-point addressing known as port address which is used to achieve multiplexing.

- It is L4 Layer including protocols like TCP/UDP and IP, discussed further.

Application Layer:-

- It is the top most layer of the OSI model through which the user interacts. It is responsible for the services provided to the users. For example :- E-mail services, file transfer etc.
- This layer contains many protocols which includes,
 1. **TELNET (TELEcommunication NETwork):** It allows the client to access the resources of the server. It is responsible for file management and set up devices like switches. Port number is 23.

Command is:

```
telnet [\\RemoteServer]
\\RemoteServer : Specifies the name of the server to which you want to connect
```

2. **FTP (File Transfer Protocol):** It is actually responsible for transfer of files. It promotes reliable and efficient data transfer via remote computers. Port number is 20 for data and 21 for control.

Command

```
ftp machinename
```

3. **TFTP (Trivial File Transfer):** It is a simplified version of FTP. If we know exactly what to find and where to find then TFTP is the protocol.

Command

```
tftp [ options... ] [host [port]] [-c command]
```

4. **NFS (Network File Transfer):** It allows the remote host to mount the file systems over the network and interact with those file systems as though they are mounted locally.

Command

```
service nfs start
```

5. **SMTP (Simple Mail Transfer Protocol):** It is responsible for the movement of the emails on and across the networks. It works closely with MTA (Mail Transfer Protocol) to send data to the right email box. SMTP port number is 25.

Command

```
MAIL FROM:<mail@abc.com>
```

6. **LPD (Line Printer Daemon):** It is responsible for printer sharing. Daemon is an agent or a server.

Command

```
lpd [ -d ] [ -l ] [ -D DebugOutputFile]
```

7. **X-Windows:** It is responsible for writing the GUI based applications. It allows a program(client) to run on one server.
8. **POP3 (Post Office Protocol version 3):** It is a mailing protocol which is used to receive emails to local email client from remote server. It works on two ports i.e.

Port 995 – It is used to connect using POP3 securely.

Port 110 – It is default non-encrypted port of POP3.

9. IMAP (Internet Message Access Protocol): It is a mailing protocol which is used to receive emails to remote server from local client. It has two ports:

Port 993 – It is responsible for secure connection using IMAP securely.

Port 143 – It is default non-encrypted IMAP port.

TCP/UDP and IP protocols - L4 Layer protocols:

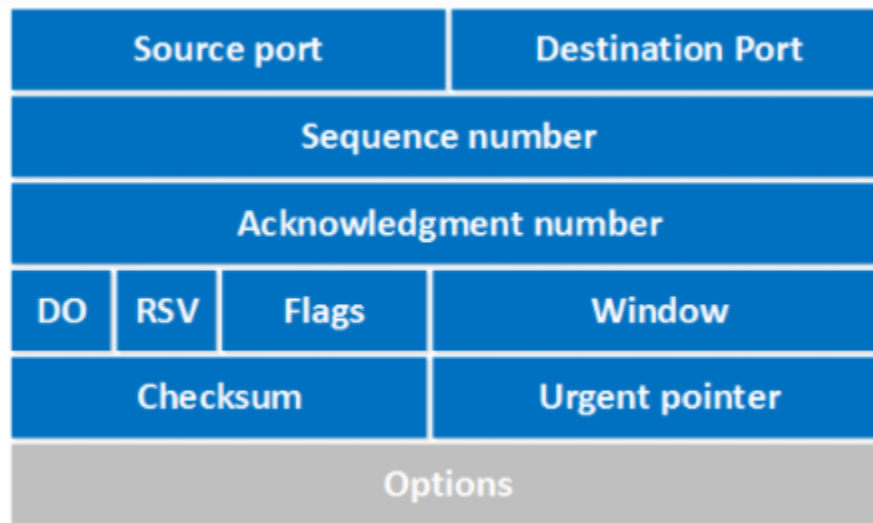
L4 layer is basically responsible for process to process communication. Process delivery requires two identifiers, an IP address and a port number, to each end to make a connection. The combination of IP address and port number is called a socket address. The client socket address describes the client process separately as the server socket address describes the server process. Transport layer protocol requires two socket addresses:

client socket address and

server socket address. These four pieces of information are part of the IP title and the headline of the transport layer protocol. L4 Protocols include TCP, UDP and IP. Following are their headers with explanation.

TCP(Transmission control protocol) Header:

TCP is a reliable protocol of transport layer. It establishes the path before sending the packet and each packet is acknowledged by the receiver.

**Fig 13: TCP Header**

- **Source port:** This is the 16th field that specifies the number in the sender port.
- **Destination port:** This is a 16-point field that specifies the port number of recipients.
- **Sequence number:** the sequence number is a 32 bit indicating how much data is sent during the TCP period. If you set up a new TCP connection (3-way handshake) then the first sequence number is a random 32 bit number. The recipient will use this sequence number and send back to approve. Protocol analysts like the wireshark often use the same number sequence 0 because it is easier to read than a certain random higher number.
- **Notification number:** This 32 bit field is used by the recipient to request the next part of TCP. This number will be the sequence number added by 1.
- **DO:** This is a 4 bit data offset field, also known as title length. Indicates the length of the TCP title so we know where the actual data starts.
- **RSV:** These are 3 bits of specified field. They are not used and are always set to 0.
- **Flags:** There are 9 bits of flags, and we call them bits bits. We use them to establish connections, send data and end connections. Window: A 16 bit window field specifies how many bytes the recipient is willing to receive. It is used so that the recipient can tell the sender that they would like to receive more data than they currently receive. It does this by specifying the number of bytes beyond the serial number in the consent field.
- **Checksum:** 16 pieces are used in the checksum to check whether the TCP title is correct or not.

- **Emergency identifier:** These 16 pieces are used when the URG bit is set, the emergency identifier is used to indicate where the emergency data ends.
- **Options:** This field can be selected and can be between 0 and 320 bits. These fields can be seen in the wireshark platform.

UDP (User Datagram Protocol) Header:

1. It is a connectionless and unreliable protocol.
2. It is same as that of IP and responsible for process to process communication.
3. In UDP, real time data sending is not possible.
4. There is no error and flow control except checksum. Here datagram is discarded if any error occurs.
5. It is a simple protocol with a faster delivery of data packets.



Fig 14: UDP Header

Source port:

- 1) It identifies the port of the sending application.
- 2) Source port 16 bit field.

Destination port:

- 1) It identifies the port of the received application.
- 2) Destination port 16 bit area.

Length:

- 1) It identifies the overall length of the UDP header and the covered data.
- 2) Length 16 bit area.

Length = UDP header length + encapsulated data length

Checksum:

- 1) It counts on UDP headers, encapsulated data and IP pseudo-headers.
- 2) Checksum counting is not mandatory in UDP.
- 3) The checksum is a 16 bit field used for error control.

IP(Internet Protocol) Header:

Version (4 bits)	IHL (4 bits)	Type of Service (8 bits)	Total Length (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragment Offset (13 bits)
Time to Live (8 bits)		Protocol (8 bits)	Header Checksum (16 bits)	
Source Address (32 bits)				
Destination Address (32 bits)				
Options and Padding (multiples of 32 bits)				

Fig 15: IP Header

- **Version:** This is the version of the Internet Protocol used. As one can imagine, the two possible values for this area are 4 or 6. Mostly, used IPv4 and IPv6 are growing rapidly. The length of this field is 4 bits.
- **Header Length (IHL):** This field is used to indicate the length of the IP header. This field indicates the length of the IP header as a number of words. Also, this field usually has a value of 5.

Header length = 5

words = 5 * 32

bits = 160 bits = 20 bytes.

The minimum and maximum length of the IP header are 20 bytes and 24 bytes, respectively.

Service type: This field is 8 bits long. From those 8 bits, the first 3 bits are not used. The next four bits indicate the type of service. This can reduce delays, increase output, increase reliability and reduce monetary costs. The last bit has not been used.

- **Total Length:** This is a 16-bit long field used to express the total length of the IP packet PDU. Since the IP header contains the header length in a different field, the difference between the total length field and the header field gives the length of the data. This 16-bit field has a maximum value of 65535 (from 216). Thus, the maximum length of an IP packet datagram is 65535 bits.
- **Identity:** This field is commonly used to identify datagrams. This area is really important when re-displaying segmented datagrams. This field is 16 bits wide.
- **Flags:** This field is 3 bits long. From those 3 bits, the first bit is still reserved. The second bit is called "Do not fragment". When this bit is set to 1, the datagram should never be broken and if there is any need for fragmentation, the datagram will be discarded. The third bit is called the "More Bit". When this bit is 1, the current datagram is broken and there are more fragments.
- **Fragments Offset:** 13 bits are allocated for this field and the IP datagram contains offsets from the beginning. This field is important when reconnecting broken datagrams.
- **Time to live:** TTL 8 bits wide field and used to indicate the hop count before the packet falls. In other words, it can be described as an effective lifetime for IP packets in the network.
- **Protocol:** This refers to the transport layer protocol that assigns the payload to the network layer. This is useful when multiplexing data at a destination in DE to assign data to the appropriate protocol. This field is 8 bits wide.
- **Header checksum:** This is a 16 length field. The value of this field is generated by a complex algorithm using the contents of the IP header. Its purpose is to verify the integrity of the datagram and to ensure that the source and destination are not damaged in any way.
- **Source IP:** The 32-bit-wide IP address of the packet sender.
- **Destination IP:** The 32 bit wide IP address of the packet receiver.
- **Options and Padding:** This includes the optional field and the variable length. This field indicates a list of options available for a given datagram. If it exists, the first byte has the following order. Copy the flag (1 bit), option class (2 and 3 bits) and option number (4 to 8 bits).

L2 Protocols and L3 Protocols:

L2 Protocol :

Layer 2, also known as Data Link Layer, is the second-level OSI reference model with seven layers of internet protocol design. Layer 2 consists of two sublayers:

Logical link control (LLC) sublayer, responsible for managing link links and managing frame traffic.

A MAC or medium access controller, controls access to the protocol between virtual networks. By using the MAC addresses assigned to all ports on the switch, multiple devices on the same physical link can be identified separately. IP address are converted to MAC address sing ARP Protocol i.e. address resolution protocol. L2 layer has MAC Address but L3 layer has IP Address. So, mapping of IP address with MAC Address is achieved by ARP Protocol.

Address Resolution Protocol (ARP):

It is basically involved in address mapping. Internet is a network of networks connected through routers. Datagram passes through different networks. The router and the host across the networks are identified using logical address. Datagram Passes through physical network and at this network, hosts and routers are identified by physical address.

Therefore, there is a need for one to one mapping or association of logical and MAC address. Mapping is of two types:

- 1. Dynamic Mapping:** It is based on other protocols in which if machine knows one of the addresses then the address can be identified by protocols.
- 2. Static Mapping:** It involves a table in which the IP addresses are mapped to MAC addresses. Each time mapping is required, look u table is needed.

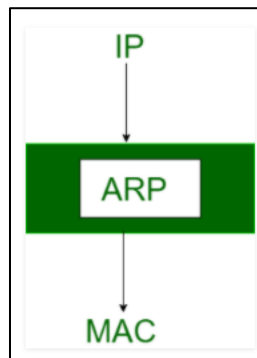


Fig 16: Address Resolution Protocol

Keywords associated with ARP Protocol:

ARP Cache Timeout: This refers to the time the MAC address can live in the ARP cache

ARP cache: After resolving the MAC address, ARP sends it to the source stored in the table for future reference. The MAC address can be used from the next communication table

ARP Request: This is nothing more than transmitting the packet over the network to verify that we have reached the destination MAC address.

- The physical address of the sender.
- Recipient's ip address
- The physical address of the receiver is FF: FF: FF: FF: FF: FF or 1's.
- Sender IP address.

ARP Response / Answer: This is a MAC address response that receives a source from a destination that facilitates further communication of data.

L3 Protocol:

L3 is basically the network layer which supports node to node delivery or the source to destination across multiple networks. Protocol involved at this layer are the routing protocols which are as follows:

- OSPF (Open Shortest Path First) :-** This protocol will listen to the neighbors and gather all the link to develop a topology map of all the available path and save it to its database. Now from the information gathered and the topology in its database, it will calculate the shortest path to reach the subnet/network. It is basically based on the Link State Routing (LSR) Protocol.
- RIP (Routing Information Protocol) :-** It counts the number of hops to find the best path between the destination and the source network.
- IS-IS (Intermediate System to Intermediate System) :-** It is very much similar to OSPF but it supports dual IP and supports IPv6. It is basically an L2 protocol whereas OSPF is L3 protocol.
- EIGRP (Enhanced Interior Gateway Routing Protocol) :-** It allows the router to exchange information in a more efficient manner. In this, the router keeps a copy of its neighbor's routing table. If a router cannot find a route to the destination in its table then it queries it's neighbor's table and then their neighbor's and so on until it finds a route. It is basically a network protocol.

- e) **BGP (Border Gateway Protocol) :-** It is responsible for looking at all the available path that the data can travel and then pick up the best route, which usually means hopping between individual smaller network (autonomous system)

While sending the packets there exist a dialogue between the protocol of receiver and sender. If any packet goes missing then the protocol of the receiver side ask to resend the packet. Once all the packets reaches the destination, it is reassemble by the protocol of receiver to form the original data.

WLAN (Wireless LAN) Protocol:

Wireless LANs refer to LANs (local area networks) that use high frequency radio waves instead of cables to connect devices. It can be perceived as a set of laptops and other wireless devices that transmit radio signals. Users connected to the WLAN can move within network coverage. Most WLAN standards are based on IEEE 802.11 or WiFi.

Wireless LAN configuration

Every station on a wireless LAN has a wireless network interface controller. The station is divided into two categories -

Customers - Customers include smart phones, printers, offices, computers, laptops, , etc. These are ten meters within the AP range.

Wireless Access Point (WAP) - WAP or bus access points (AP) are usually wireless routers that are the base station or access point. APs are wired together using fiber or copper wires through a distribution system.

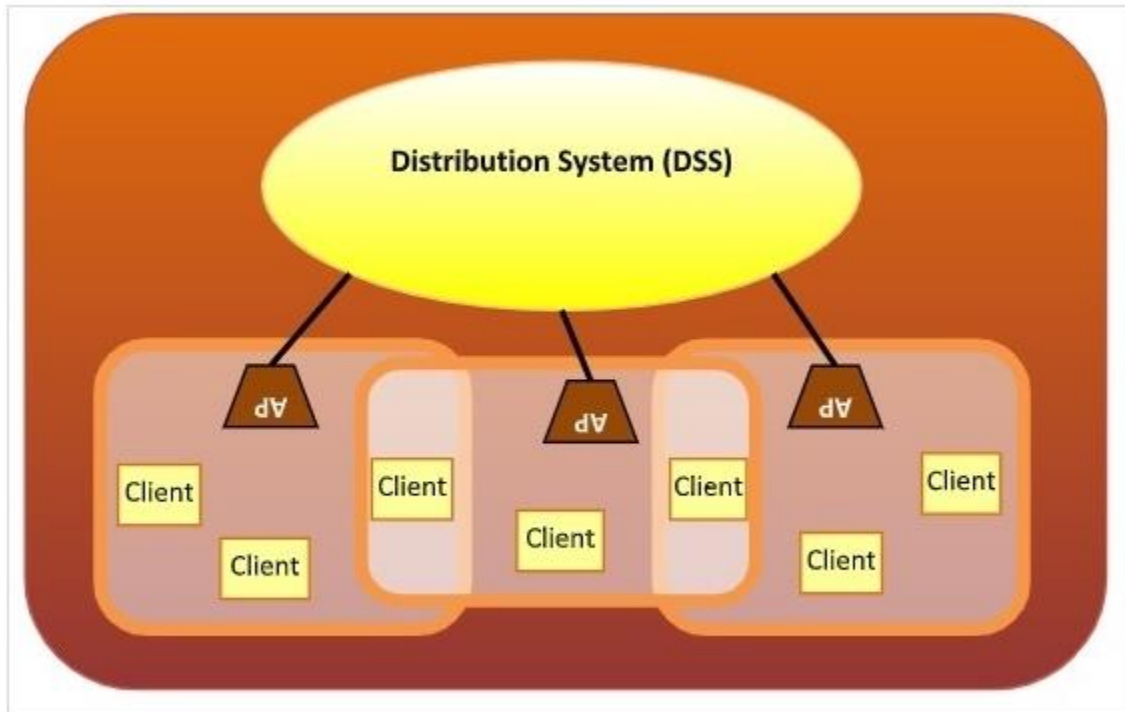


Fig 17: Wireless LAN

Types of WLAN protocols:

There are many variations on IEEE 802.11 or WiFi, the main ones being –

- **802.11n protocol:** Popularly known as wireless n, which is an improved version of 802.11g. It offers very high bandwidth up to 600Mbps and provides signal coverage. It uses multiple input / multiple outputs (MIMO) with multiple antennas at both the transmitter end and the receiver end. In the case of signal interruptions, alternative routes are used. However, implementation is very expensive.
- **802.11g Protocol:** This protocol combines the features of the 802.11a and 802.11b protocols. It supports both frequency 5GHz (802.11a standard) and 2.4GHz (802.11b standard). Due to its dual characteristics, the 802.11g lags behind the 802.11b devices. 802.11g provides high speed, different signal range and flexibility for interruption. However, it is more expensive to implement.

- **802.11a Protocol:** This protocol supports high transmission speeds of 54Mbps. It has a high frequency frequency frequency of 5GHz, which makes it difficult for signal walls and other barriers to penetrate. It uses orthogonal frequency division multiplexing (OFDM).
- **802.11b Protocol:** This protocol operates in the 2.4GHz frequency range and supports speeds of up to 11Mbps. This facilitates route sharing and is less sensitive to interruptions. It uses Carrier Sense Multiple Access with Ethernet Protocol Conflict Prevention (CSMA / CA).

BGP Protocol:

The Border Gateway Protocol (BGP) is the Internet's postal service. When someone leaves a letter in the mailbox, the postal service processes the piece and chooses the fastest and most efficient way to deliver the letter to its recipient. Similarly, when an individual accumulates data on the Internet, the BGP is responsible for looking at all the ways in which data can travel and choosing the best route, usually by jumping between autonomous systems.

BGP is an Internet protocol. It does this by enabling data routing over the Internet. When a user in Singapore loads a website with a local server in Argentina, BGP is the protocol that allows the communication to take place quickly and efficiently.

What is an autonomous system?

The Internet is a network of networks; It is divided into thousands of smaller networks called Autonomous Systems (AS). Each of these networks is a large pool of routers run by a single company.

If we consider BGP as the postal service of the Internet, AS is like personal post offices. There may be hundreds of mailboxes in one city, but mail from those boxes must go through the local postal branch before heading to another destination. Internal routers in AS, such as mailboxes, send their outbound transmissions to AS, which then uses BGP routing to transmit these transmissions to their destination.

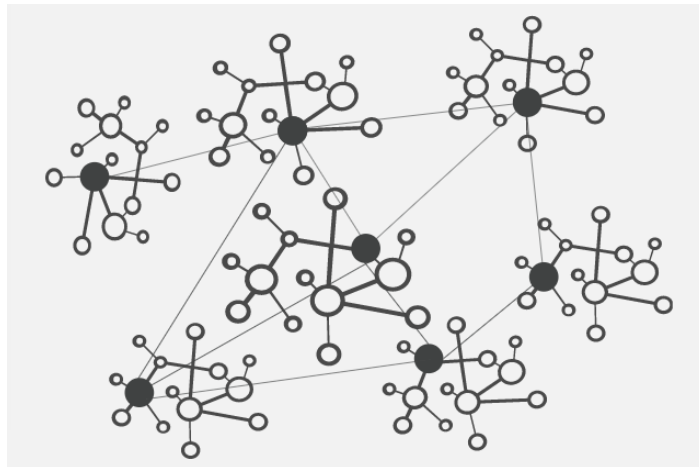


Fig 18: Node hopping or interconnectivity for BGP routing protocol

IP ADDRESSES

IPv4 and IPv6 Addressing:

Allocation of IP addresses can be done manually or dynamically. So for dynamic allocation of IP addresses DHCP server is used. DHCP servers uses a pool of IP addresses and give it uniquely to the host. It also provides subnet mask, DNS servers and default gateway.

Eg.:- IP address : 192.168.1.5

Subnet mask : 255.255.255.252

Default gateway : 192.168.1.1

DNS server : 8.8.8.8

DNS :-

DNS stands for Domain Name System. It is a function of application layer and is used to give domain name to the IP addresses. It is used by/for programs like emails, websites etc. So, basically it is used for the mapping of IP addresses to the domain name which can be easily memorize by the users. Eg :- www.xyz.com, www.abc.co.in etc. A full domain name has labels separated by dots.

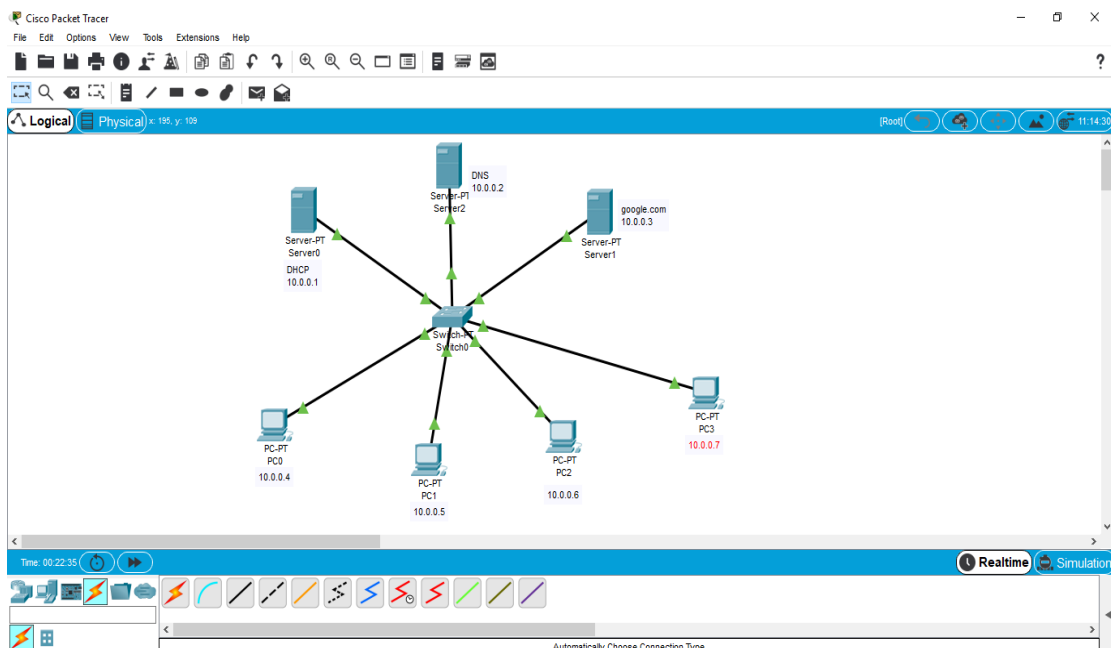
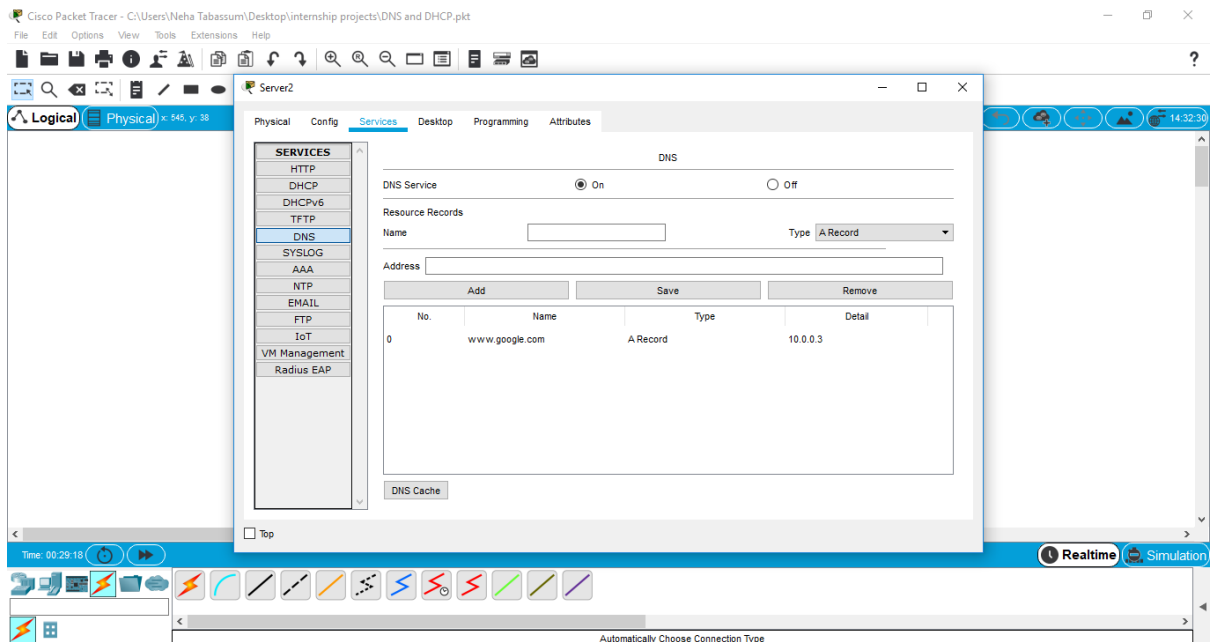
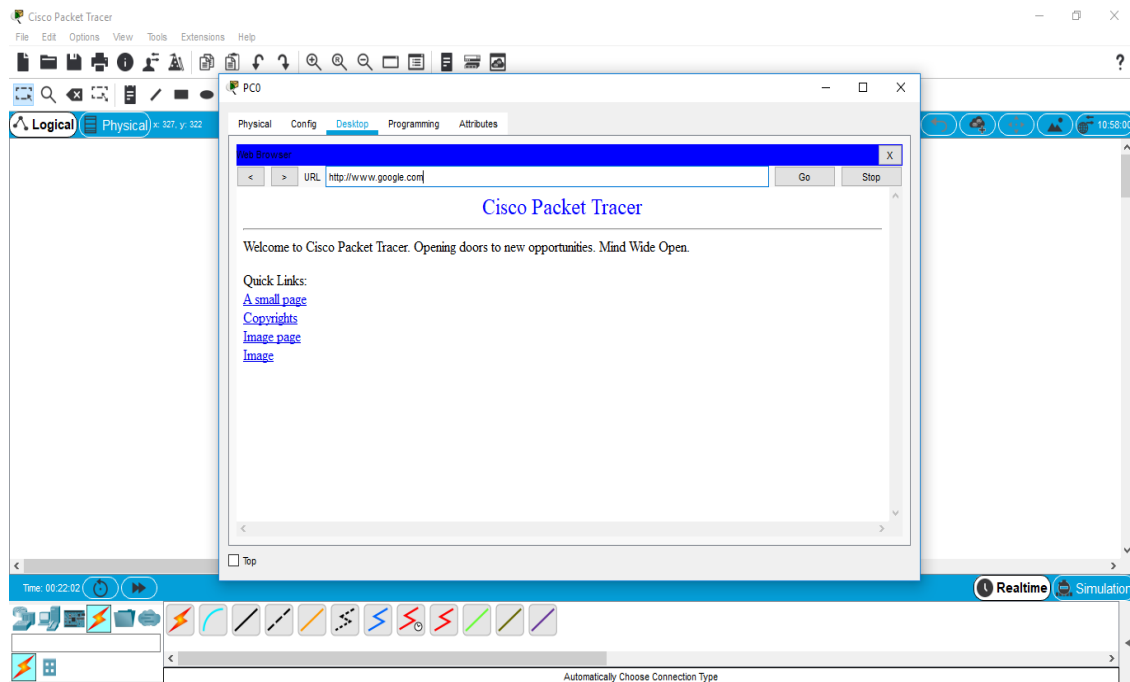


Fig 19: Network of DNS and DHCP on packet tracer software.

**Fig 20: Configuration of DNS****Fig 21: Website (google.com) is accessed.**

Reserved Addresses :-

There are also some reserved IPv4 addresses for special purpose. These addresses cannot be used to serve the internet and are known as private addresses [6]. Below is list of private addresses:-

10.0.0.0 to 10.255.255.255.....class A

172.16.0.0 to 172.31.255.255.....class B

192.168.0.0 to 192.168.255.255.....class C

Also the pool of 127.0.0.0 is booked for loopback IP addressing.

In order to communicate over different networks, these addresses must be converted to the public address and the process of converting is known as NAT (Network Address Translation).

NETWORK ADDRESS TRANSLATION :-

With the increasing demand for IP addresses in organizations, address space of IPv4 i.e 2^{32} , (nearly equal to 4 billion) is not sufficient for them. So, NAT was introduced which translates the private address to public address and allow the user to communicate over the internet [6]. The organization were given private addresses and a single global address with a NAT router. NAT has a translation table with private IP address in one of the columns and a pool of global (public) IP Address in another column. Whenever a server (eg. Server A) having a private address wants to send data to the internet, it passes it to the NAT router. The router makes a note of its source address and destination address in the table and provide a global address to the packet to access the internet. When the packet returns from destination address, the router again checks its table for the source address and send the packet to the server (i.e server A).

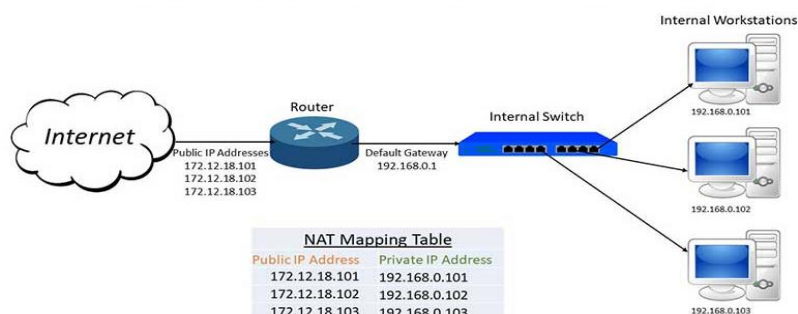


Fig 22: Network Address Translation (NAT)

IPv6 :-

In spite of the short term solutions like classless addressing, DHCP NAT, there is still a problem of depletion of addresses. So, IPv6 came into effect. IPv6 is a 128 bit address with an address space of 2^{128} .

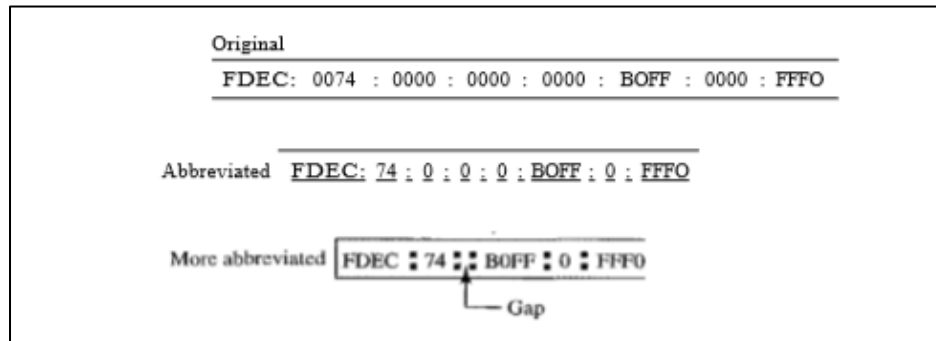


Fig 23: Representation of IPv6 address

There are 3 addressing methods in IPv6 representation :-

- 1) **Unicast address :-** When a packet is send to unicast address then that packet is delivered only to that interface which is recognized by the unicast address.
- 2) **Multicast address :-** When a packet is send to multicast address then it will be delivered to all the interfaces recognized by that address. This type of address is generally used by multiple host known as group.
- 3) **Anycast address :-** When a packet is send to anycast address then it will be delivered to only one member interface mostly the nearest one.

IPv4 Subnetting:

Allocation of IP addresses can be done manually or dynamically. So for dynamic allocation of IP addresses DHCP server is used. DHCP servers uses a pool of IP addresses and give it uniquely to the host. It also provides subnet mask, DNS servers and default gateway.

Eg.:- IP address : 192.168.1.5

Subnet mask : 255.255.255.252

Default gateway : 192.168.1.1

DNS server : 8.8.8.8

Internet Assigned Numbers Authority (IANA) is accountable for the allocation of physical (MAC) as well as Logical (IP) address to the users.

Physical address :- It is also known as Media access control address or MAC address, which is handed over to the users as well as the manufacturers of device. It is 48 bit hexadecimal address present on the NIC (Network Interface Controller) card which is a Layer 2 device.

Logical Address :- It's a 32 bit IP address (IPv4) with an address space of 2^{32} and is not present in the NIC card but is assigned for the purpose of routing between the networks. In order to connect over the internet IP address is required. It is generally given by Internet Service Providers (ISP). But these IP addresses are very much costly. So APNIC (Asia Pacific Network Information Centre) has divided the IP address into classes according to size.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

Fig 24: Classful addressing

Class D and E are reserved classes. Addresses in IPv4 have two parts :-

1. Host ID
2. Network ID

Class A has network ID of 8 bits and host ID of 24 bits. Class B has network ID of 16 bits and host ID of 16 bits. Class C has network ID of 24 bits and host ID of 8 bits. So class A address is given to those which have a large no. of hosts. However, classful addresses have many demerits so they are replaced with classless addressing which provides more flexibility [5].

Demerits of classful addressing:-

- Millions of class A addresses remained unused.
- So many class B addresses are also wasted
- Class C addresses are not enough to fulfil the need of organization
- Multicast routing is done by class D addresses.
- For experimental purposes, class E addresses are booked.

In classful address class A,B and C has fixed subnet mask which does not provide flexibility of using less number of host in a network.

Class A → /8

Class B → /16

Class C → /24

5.1 Classless Addressing :-

Classless Inter Domain Routing (CIDR) provides the flexibility of reducing the number of host per network. In order to reduce the wastage of addresses, concept of subnetting is used. Subnetting is defined as a practice to divide a larger network into smaller networks or subgroups.

Table 9 : Subnets with no. of IP addresses

S.No.	Subnets	No. of IP addresses
1	/25	$2^{(32-25)}=128$
2	/26	$2^{(32-26)}=64$
3	/27	32
4	/28	16
5	/29	8
6	/30	4
7	/31	2 (Used in new routers with tech. 0 known as IP-subnet-zero)
8	/32	

From the total IP provided, First and the last IP address are useless and cannot be used as Host IDs. E.g: 10.0.0.0 and 10.0.0.255 are useless (i.e 256-2=254 are used).

So, below are the usable Hosts IDs.

Table 10: List of hosts

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Rules of addressing in CIDR:-

- 1) The address used should be contiguous i.e one after the other.
- 2) No. of address in a block must be a power of two (i.e 0,2,4,8...)
- 3) The least significant bit of the first IP address should always start with zero.

Example problems:

1. You have been given a class C address i.e 192.168.8.0/24 (classful addressing). Create 3 subnet addresses for different departments of an organization.

Answer: creating a network of 3 subnets require a total of 4 subnets because subnetting occurs in power of 2 i.e $2^2 = 4$

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/8	/9	/10	/11	/12	/13	/14	/15	/16
	/16	/17	/18	/19	/20	/21	/22	/23	/24
	/24	/25	/26	/27	/28	/29	/30	/31	/32

Network ID	Subnet mask	Host ID Range	No. of Host	Last ID/Broadcast ID
192.168.8.0	/26	192.168.8.1– 192.168.4.62	64	192.168.8.63
192.168.8.64	/26	192.168.8.65– 192.168.4.126	64	192.168.8.127
192.168.8.128	/26	192.168.8.129– 192.168.4.190	64	192.168.8.191
192.168.8.192	/26	192.168.8.193– 192.168.4.254	64	192.168.8.255

2. You have been given a class B address i.e 172.16.1.0/16 (classful addressing). Create 6 subnet addresses for different departments of an organization.

Answer: creating a network of 6 subnets requires a total of 8 subnets because subnetting occurs in power of 2 i.e $2^4 = 8$

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/8	/9	/10	/11	/12	/13	/14	/15	/16
	/16	/17	/18	/19	/20	/21	/22	/23	/24
	/24	/25	/26	/27	/28	/29	/30	/31	/32

Network ID	Subnet mask	Host ID Range	No. of Host	Last ID/Broadcast ID
172.16.1.0	/19	172.16.1.1-172.16.1.30	32	172.16.1.31
172.16.1.32	/19	172.16.1.33-172.16.1.62	32	172.16.1.63
172.16.1.64	/19	172.16.1.65-172.16.1.94	32	172.16.1.95
172.16.1.96	/19	172.16.1.97-172.16.1.126	32	172.16.1.127
172.16.1.128	/19	172.16.1.129-172.16.1.158	32	172.16.1.159
172.16.1.160	/19	172.16.1.161-172.16.1.190	32	172.16.1.191
172.16.1.192	/19	172.16.1.193-172.16.1.222	32	172.16.1.223
172.16.1.224	/19	172.16.1.225-172.16.1.254	32	172.16.1.255

3. You have been given a class A address i.e 10.16.2.0/8 (classful addressing). Create 2 subnet addresses for different departments of an organization.

Answer: creating a network of 2 subnets requires a total of 2 subnets because subnetting occurs in power of 2 i.e $2^1 = 2$

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/8	/9	/10	/11	/12	/13	/14	/15	/16
	/16	/17	/18	/19	/20	/21	/22	/23	/24
	/24	/25	/26	/27	/28	/29	/30	/31	/32

Network ID	Subnet mask	Host ID Range	No. of Host	Last ID/Broadcast ID
10.16.2.0	/9	10.16.2.1- 10.16.2.126	128	10.16.2.127
10.16.2.128	/9	10.16.2.129- 10.16.2.254	128	10.16.2.255

NETWORK TOOLS

1. Cisco Packet Tracer:

It is a strong network simulation program or the software that allows many researchers, scholars and students across the globe to experiment with the behavior of network. It supplements physical equipments so that students will be able to create networks immense number of devices. Following is a small network demonstrating many networks interconnected by routers and switch.

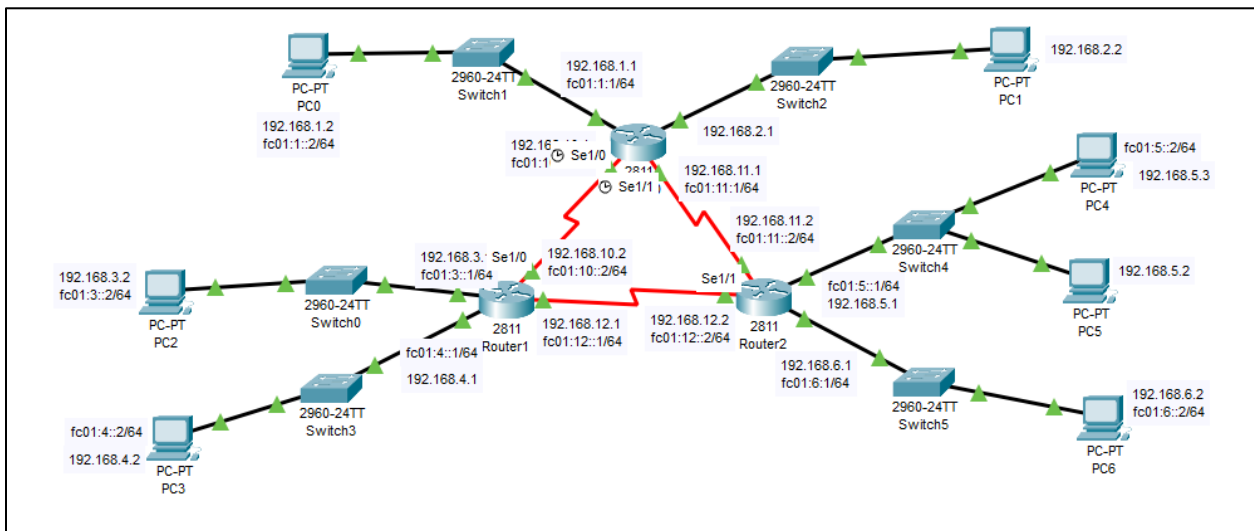


Fig 25: Serial Connection of routers for packet transmission from one server to the other







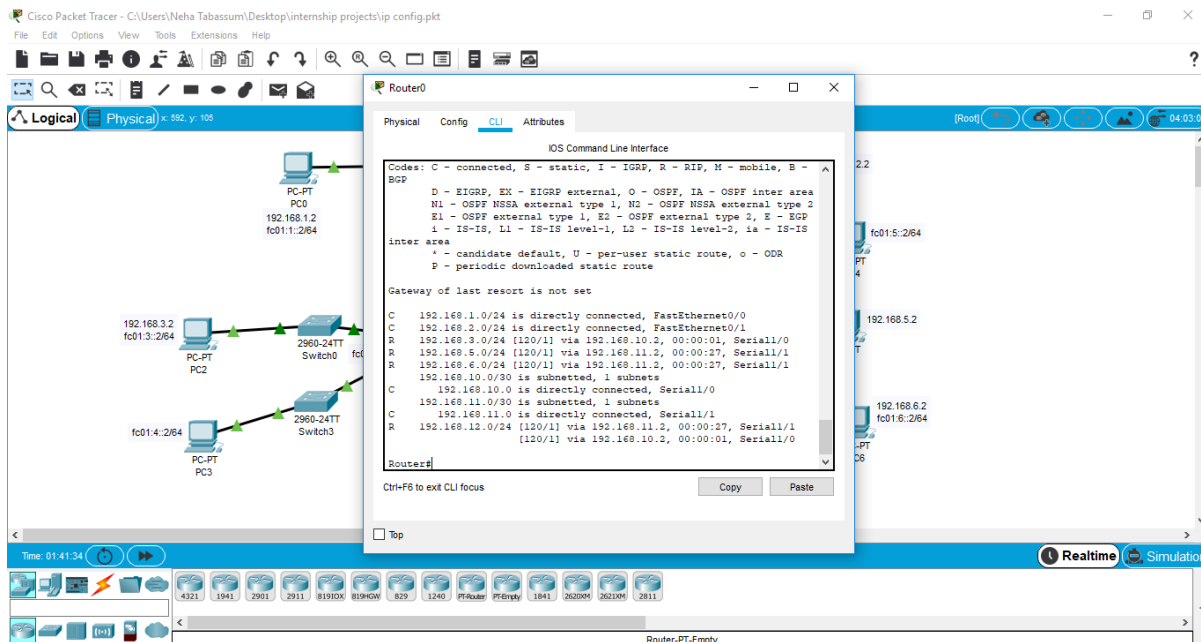
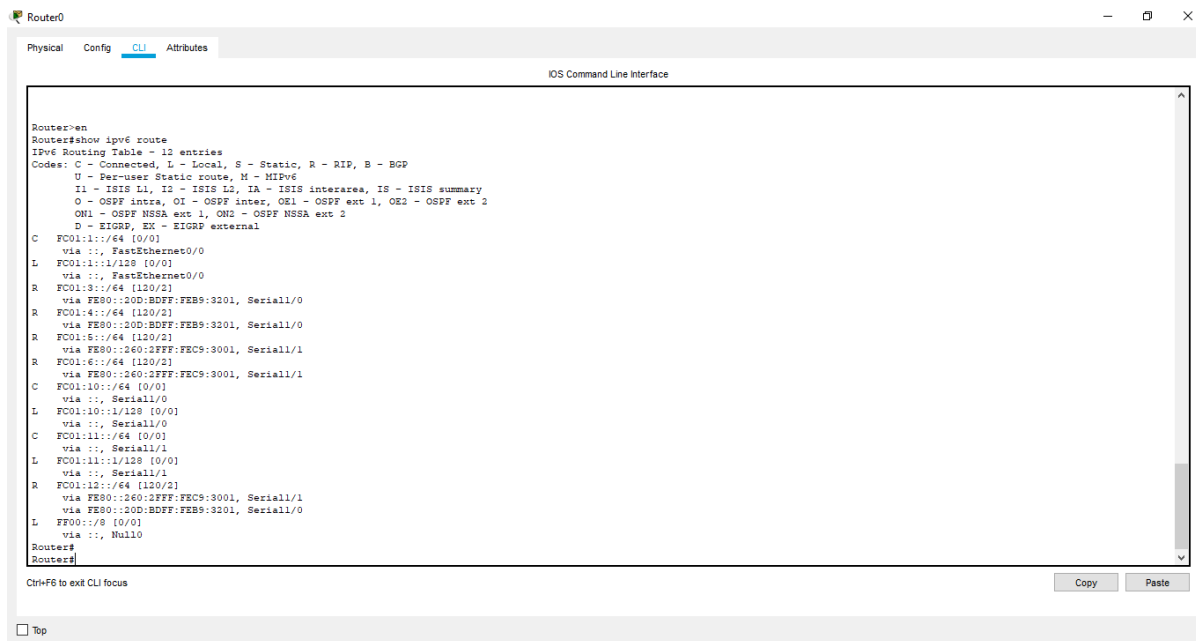
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	De
	Successful	PC0	PC6	ICMP		0.000	N	0	(edit)	(de
	Successful	PC1	PC5	ICMP		0.000	N	1	(edit)	(de
	Successful	PC6	PC2	ICMP		0.000	N	2	(edit)	(de

Fig 26: Transfer of Packets from different sources to different destination

**Fig 27: IPv4 routes on router 0 (show ip route)****Fig 28: IPv6 routes on router 0 (show ipv6 route)**

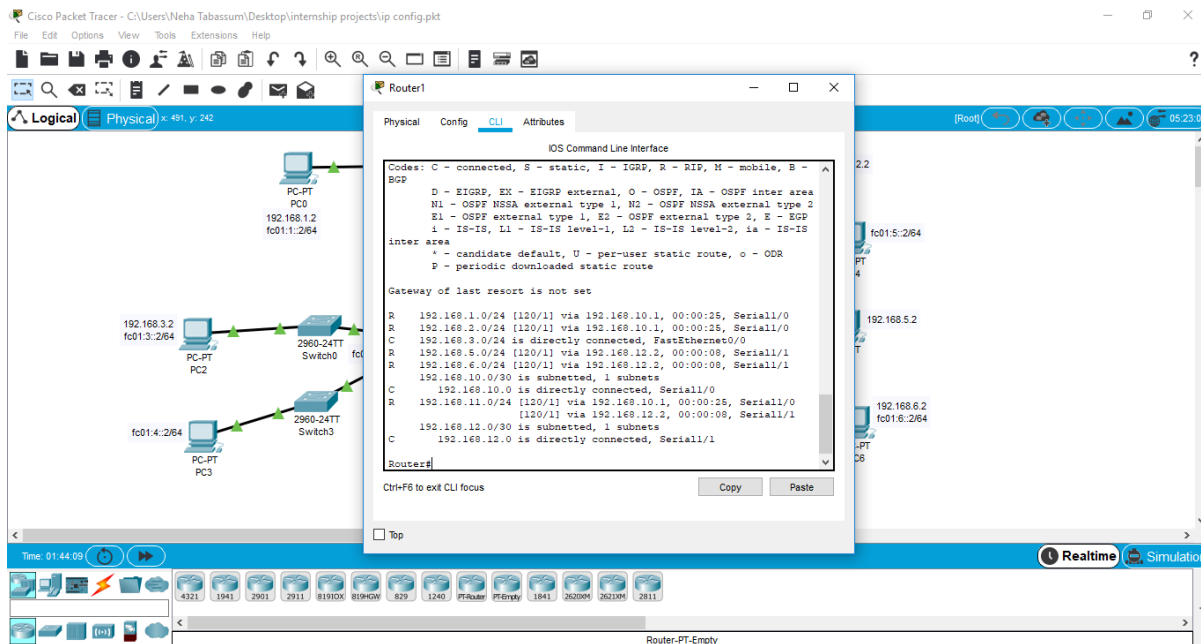


Fig 29: IPv4 routes on router 1 (show ip route)

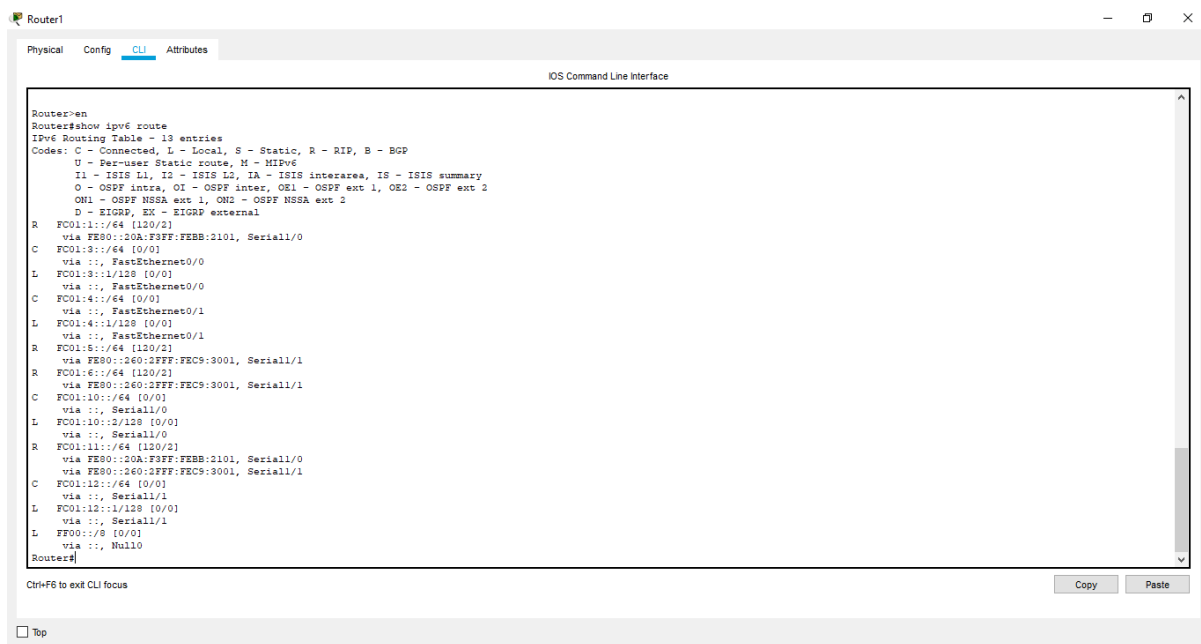


Fig 30: IPv6 routes on router 1 (show ipv6 route)

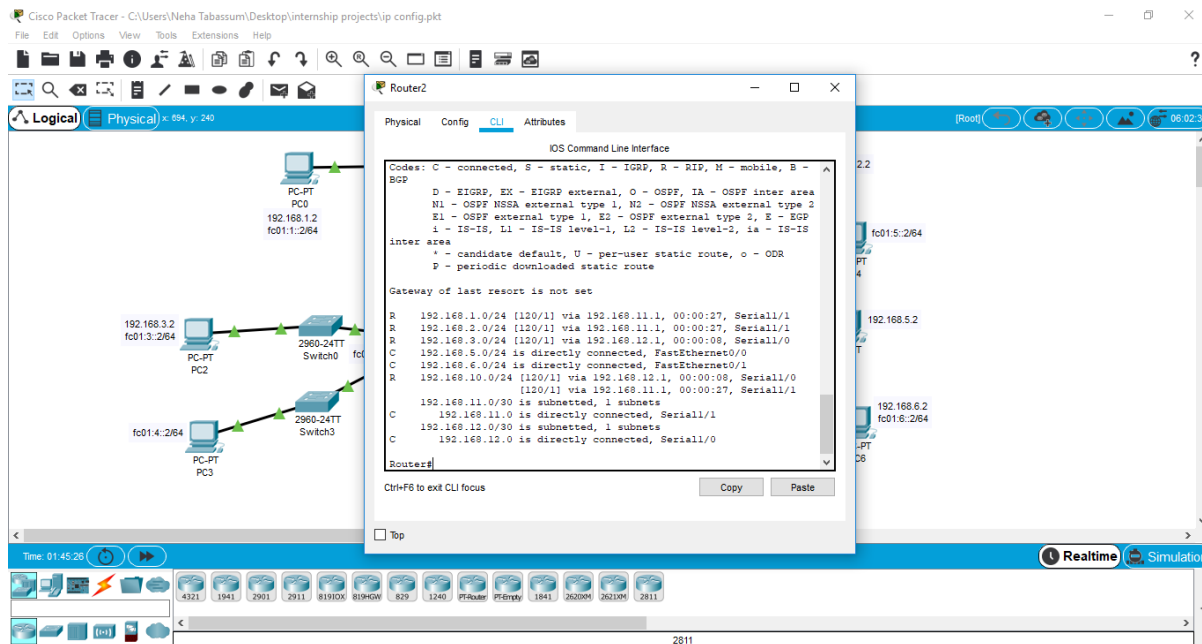


Fig 31: IPv4 routes on router 2 (show ip route)

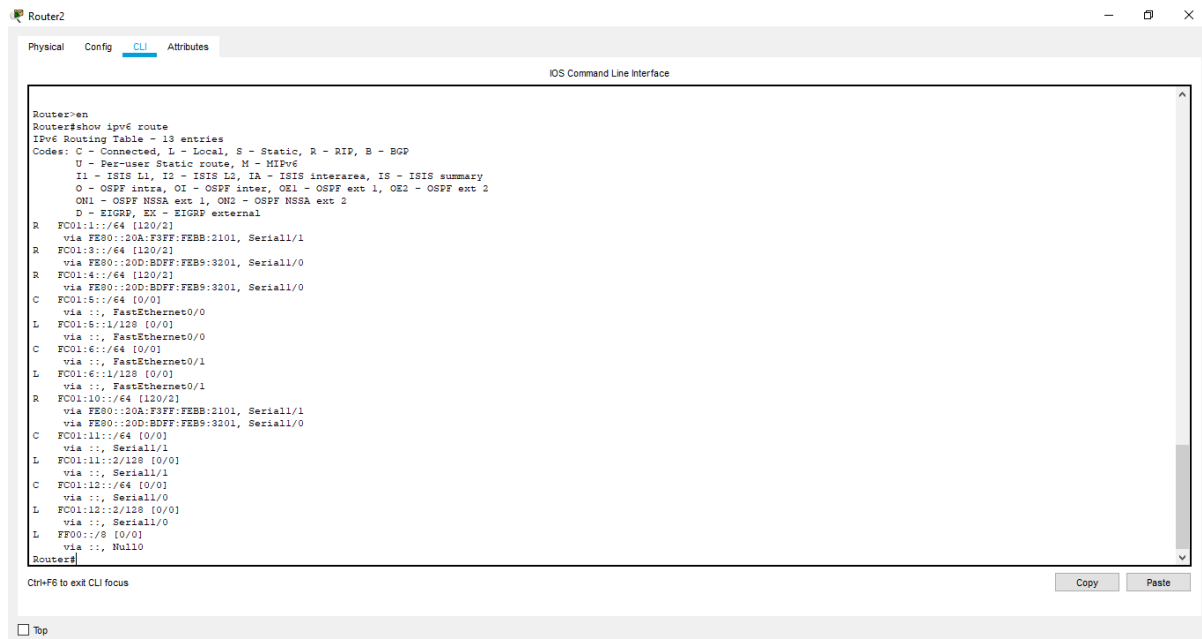


Fig 32: IPv6 routes on router 2 (show ipv6 route)

Testing results :-

To test whether a network is working properly or not, a ping command is used. Ping is a tool or a network utility program which allows you to check whether a particular host is reachable or not. Loop back address is another IP address which is used to check the working of the self server. Example of loop back IP address is 127.0.0.1 and it will always return a reply unless a network security system prevents it. Eg firewall.

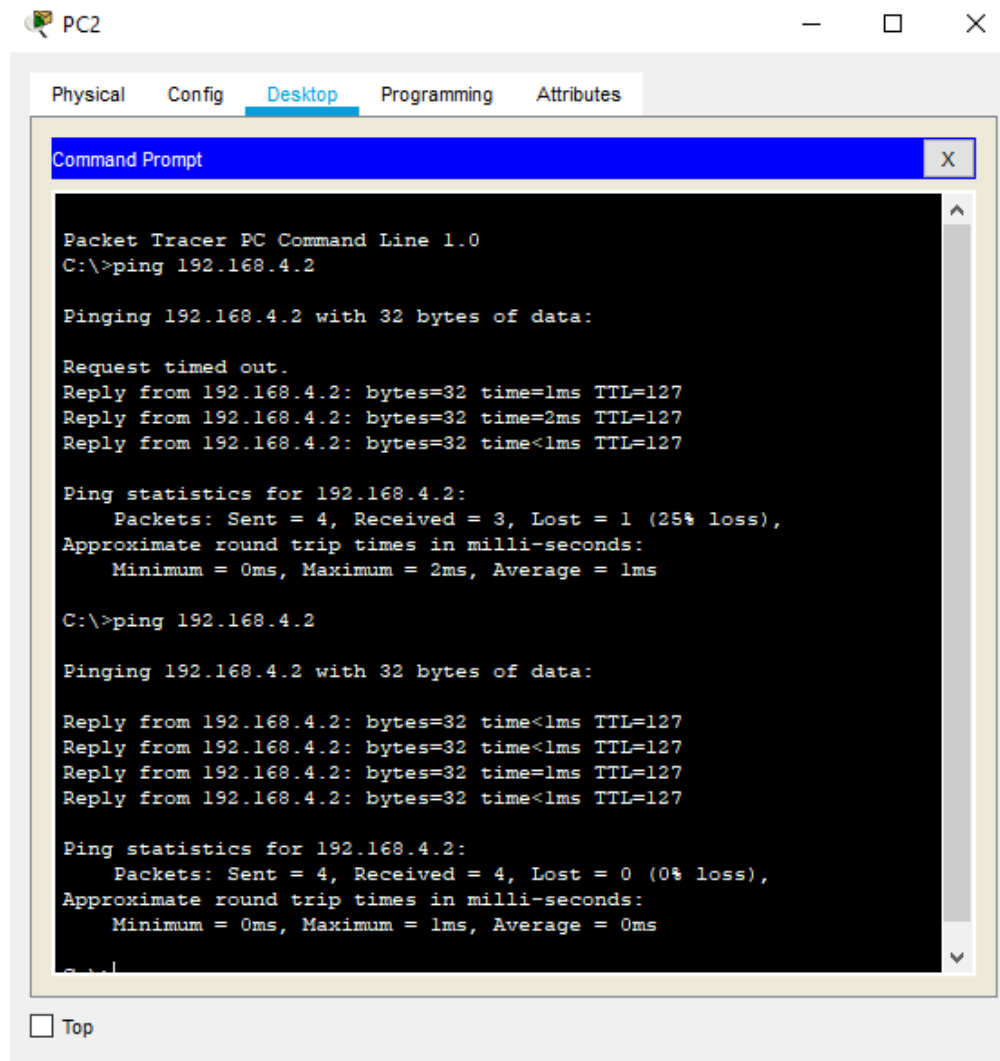
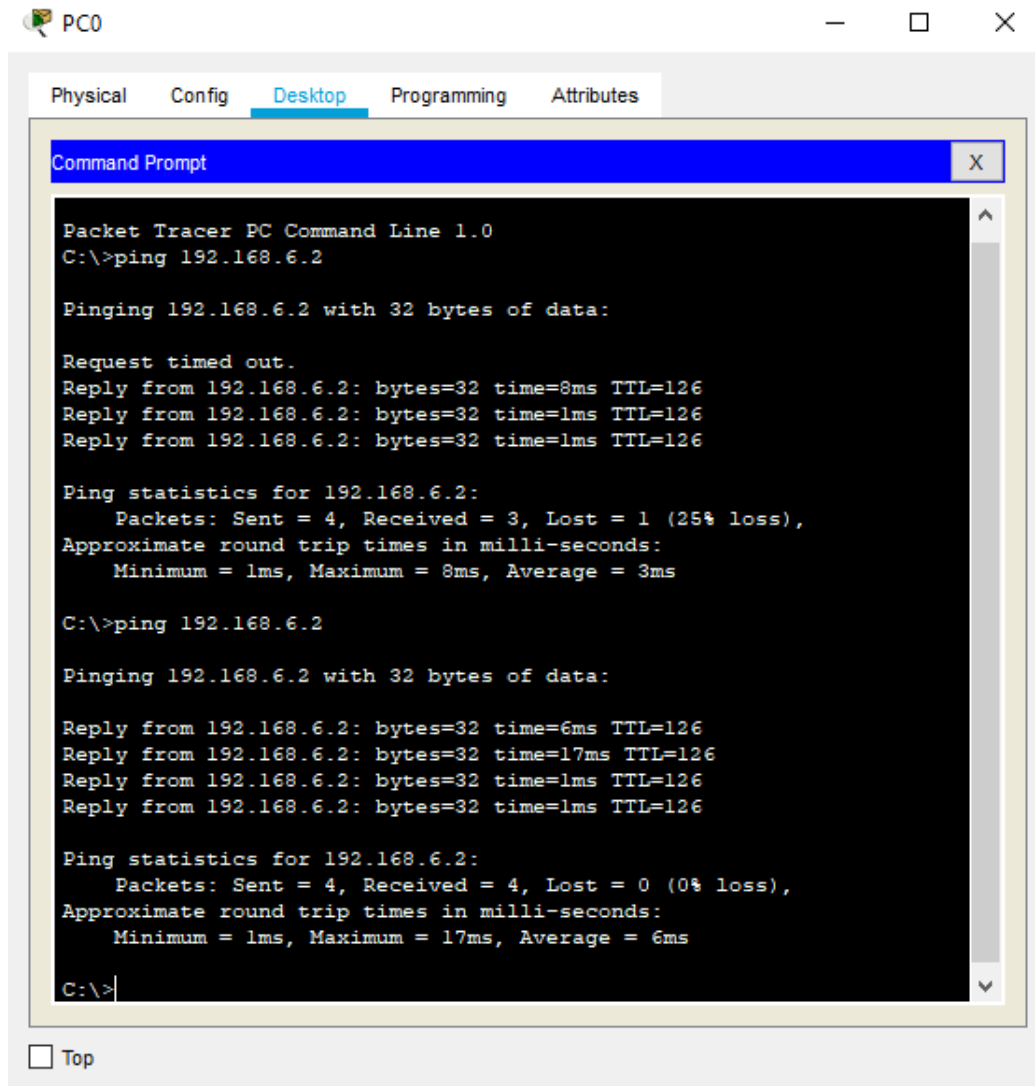


Fig 33: Pinging from IPv4 to IPv4 in the same network



PC0

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.6.2: bytes=32 time=8ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 3ms

C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.6.2: bytes=32 time=6ms TTL=126
Reply from 192.168.6.2: bytes=32 time=17ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 6ms

C:\>
```

☐ Top

Fig 34: Pinging from IPv4 to IPv4 in different network

2. Wireshark:

Wireshark is a network protocol analyzer. This software let us know what is happening in the network at a microscopic level.

The screenshot shown below represents the traffic. The traffic is being captured from ethernet.

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
28966	818.267021	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x731f800f
28967	818.362000	fe80::2558:bbed:d72...	ff02::1:2	DHCPv6	164	Solicit XID: 0x124920 CID: 0001000127a05e0e454e8b6229c
28968	818.673749	192.168.60.10	224.0.0.252	LLMNR	75	Standard query 0xc3ad ANY INFENSER-BA-001
28969	818.850278	Cisco:53:61:19a	Spanning-tree-for...	STP	60	Conf. Root = 0/85/78:ba:f9:c4:9a:41 Cost = 1 Port = 0x8132
28970	818.905903	192.168.60.149	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
28971	818.912624	fe80::ea10:6f26:f06...	ff02::2	ICMPv6	62	Router Solicitation
28972	818.905610	192.168.60.144	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
28973	819.088057	192.168.60.10	224.0.0.252	LLMNR	75	Standard query 0xc3ad ANY INFENSER-BA-001
28974	819.512000	192.168.60.10	224.0.0.252	LLMNR	75	Standard query 0xc7bf ANY INFENSER-BA-001
28975	819.650787	192.168.60.77	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
28976	819.932515	192.168.60.10	224.0.0.252	LLMNR	75	Standard query 0xc7bf ANY INFENSER-BA-001
28977	819.909044	192.168.60.144	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
28978	820.400235	192.168.60.141	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

[Checksum Status: Unverified]
[Stream index: 1620]
> [Timestamps]
UDP payload (173 bytes)
▼ Simple Service Discovery Protocol
> M-SEARCH * HTTP/1.1\r\n\r\nHOST: 239.255.255.250:1900\r\nMAN: "ssdp:discover"\r\nMX: 1\r\nST: urn:dial-multiscreen-org:service:dial:1\r\nUSER-AGENT: Microsoft Edge/89.0.774.57 Windows\r\n\r\n\r\n[Full request URI: http://239.255.255.250:1900*]
[HTTP request 2/4]
[Prev request in frame: 27205]
[Next request in frame: 27222]

0010 00 c9 7b 31 00 00 01 11 50 c4 c0 a8 3c 8c ef ff ...1...P...<...
0020 ff fa c9 b0 07 6c 00 b5 ee af 4d 2d 53 45 41 52 ...1...H-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1-H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 :250:190 0:MAN:
0060 22 73 73 64 10 3a 64 69 73 6f 6f 76 65 72 22 0d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a MX: 1: ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:service:dial:
00a0 6c 3a 31 0d 0a 53 54 3a 20 75 72 6e 3a 64 69 61 l:1: USER-AGENT:
00b0 20 4d 69 63 72 6f 73 6f 66 74 20 45 64 67 65 2f Microsoft Edge/
00c0 38 39 2e 30 2e 37 37 34 2e 35 37 20 57 69 6e 64 89.0.774.57 Wind
00d0 2f 77 73 6d 6d 6d 0a oss:...

242	14.743510	192.168.60.157	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
243	14.764449	142.250.77.78	192.168.60.84	TCP	66	443 → 54351 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2

> Frame 243: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{FA4B2910-6D29-403A-8552-5C6D1B2F4213}, id 0
> Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:87:71 (e4:54:e8:b1:87:71)
> Internet Protocol Version 4, Src: 142.250.77.78, Dst: 192.168.60.84
▼ Transmission Control Protocol, Src Port: 443, Dst Port: 54351, Seq: 1, Ack: 2, Len: 0
Source Port: 443
Destination Port: 54351
[Stream index: 7]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2616602508
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 4080745332
1000 = Header Length: 32 bytes (8)
> Flags: 0x010 (ACK)
Window: 261
[Calculated window size: 261]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x71d6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK
> [SEQ/ACK analysis]
> [Timestamps]

0000 e4 54 e8 b1 87 71 f4 0f 1b 0c d2 70 08 00 45 00 -T...q...p...E
0010 00 34 d0 50 00 00 39 06 d8 2e 8e fa 4d 4e c0 a8 -4-P...9...MN..
0020 3c 54 01 bb d4 4f 9b f6 2f 8c f3 3b 3b 74 80 10 <T...O.../...;t..
0030 01 05 71 d6 00 00 01 01 05 0a f3 3b 3b 73 f3 3b -q.....;...;..
0040 3b 74 ;t

242	14.743510	192.168.60.157	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1
243	14.764449	142.250.77.78	192.168.60.84	TCP	66 443 → 54351 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2

>	Frame 243: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{FA4B2910-6D29-403A-8552-5C6D1B2F4213}, id 0
>	Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:87:71 (e4:54:e8:b1:87:71)
>	Internet Protocol Version 4, Src: 142.250.77.78, Dst: 192.168.60.84
>	0100 = Version: 4
> 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	0000 00.. = Differentiated Services Codepoint: Default (0)
>00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
>	Total Length: 52
>	Identification: 0xd050 (53328)
>	Flags: 0x00
>	0... = Reserved bit: Not set
>	.0.. = Don't fragment: Not set
>	..0. = More fragments: Not set
>	Fragment Offset: 0
>	Time to Live: 57
>	Protocol: TCP (6)
>	Header Checksum: 0xd82e [validation disabled]
>	[Header checksum status: Unverified]
>	Source Address: 142.250.77.78
>	Destination Address: 192.168.60.84
>	Transmission Control Protocol, Src Port: 443, Dst Port: 54351, Seq: 1, Ack: 2, Len: 0

0000	e4 54 e8 b1 87 71 f4 0f	1b 0c d2 70 08 00 45 00	·T···q·····p··E·
0010	00 34 d0 50 00 00 39 06	d8 2e 8e fa 4d 4e c0 a8	·4·P··9····MN··
0020	3c 54 01 bb d4 4f 9b f6	2f 8c f3 3b 3b 74 80 10	<T···O···/··;;t··
0030	01 05 71 d6 00 00 01 01	05 0a f3 3b 3b 73 f3 3b	··q·····[··;;s·;
0040	3b 74		·t

242	14.743510	192.168.60.157	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1
243	14.764449	142.250.77.78	192.168.60.84	TCP	66 443 → 54351 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2

>	Frame 243: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{FA4B2910-6D29-403A-8552-5C6D1B2F4213}, id 0
>	Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:87:71 (e4:54:e8:b1:87:71)
>	Destination: Dell_b1:87:71 (e4:54:e8:b1:87:71)
>	Address: Dell_b1:87:71 (e4:54:e8:b1:87:71)
>0. = LG bit: Globally unique address (factory default)
>0. = IG bit: Individual address (unicast)
>	Source: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70)
>	Address: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70)
>0. = LG bit: Globally unique address (factory default)
>0. = IG bit: Individual address (unicast)
>	Type: IPv4 (0x0800)
>	Internet Protocol Version 4, Src: 142.250.77.78, Dst: 192.168.60.84
>	Transmission Control Protocol, Src Port: 443, Dst Port: 54351, Seq: 1, Ack: 2, Len: 0

0000	e4 54 e8 b1 87 71 f4 0f	1b 0c d2 70 08 00 45 00	·T···q·····p··E·
0010	00 34 d0 50 00 00 39 06	d8 2e 8e fa 4d 4e c0 a8	·4·P··9····MN··
0020	3c 54 01 bb d4 4f 9b f6	2f 8c f3 3b 3b 74 80 10	<T···O···/··;;t··
0030	01 05 71 d6 00 00 01 01	05 0a f3 3b 3b 73 f3 3b	··q·····[··;;s·;
0040	3b 74		·t

242	14.743510	192.168.60.157	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1
243	14.764449	142.250.77.78	192.168.60.84	TCP	66 443 → 54351 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2

▼

Frame 243: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{FA4B2910-6D29-403A-8552-5C6D1B2F4213}, id 0

▼

Interface id: 0 (\Device\NPF_{FA4B2910-6D29-403A-8552-5C6D1B2F4213})

Interface name: \Device\NPF_{FA4B2910-6D29-403A-8552-5C6D1B2F4213}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Mar 26, 2021 16:33:43.507457000 India Standard Time

[Time shift for this packet: 0.00000000 seconds]

Epoch Time: 1616756623.507457000 seconds

[Time delta from previous captured frame: 0.020939000 seconds]

[Time delta from previous displayed frame: 0.020939000 seconds]

[Time since reference or first frame: 14.764449000 seconds]

Frame Number: 243

Frame Length: 66 bytes (528 bits)

Capture Length: 66 bytes (528 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

>

Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:87:71 (e4:54:e8:b1:87:71)

>

Internet Protocol Version 4, Src: 142.250.77.78, Dst: 192.168.60.84

```

0000  e4 54 e8 b1 87 71 f4 0f 1b 0c d2 70 08 00 45 00  .T...g...p..E.
0010  00 34 d0 50 00 00 39 06 d8 2e 8e fa 4d 4e c0 a8  .4.P..9...MN..
0020  3c 54 01 bb d4 4f 9b f6 2f 8c f3 3b 3b 74 80 10  <T...O.../...;t..
0030  01 05 71 d6 00 00 01 01 05 0a f3 3b 3b 73 f3 3b  ..q.....;s;
0040  3b 74                                     ;t

```

Fig 35: Capturing traffic from Ethernet

Following is the filter of the traffic captured:

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

Fig 36: Capture Filter

When a computer wants to interact over the network it goes through a lots of steps. Following is the step by step walkthrough of a traffic example.

L&T Technology Services

CONFIDENTIAL

Page 55 of 59

1. When a computer wants to send traffic, it first configure a default gateway, IP address, DNS server and subnet mask. Default gateway and DNS server start pointing to the LAN IP address of the home network.
2. After this role of DNS comes into effect. The Operating System check out its DNS cache to check if it is already having the IP address. If there is no history available then it send the query for IP Address.
3. DNS uses User Datagram Protocol as a L4 protocol.
4. The server will now check for its ARP table to get the MAC address corresponding to the IP address.
5. If the ARP table is empty then an ARP request will be made to the network.
6. When reply has been received then the OS enter the detail to the ARP Table.
7. The DNS query is now send from computer to the DNS server.
8. Now the home router will check for the DNS cache.
9. The home router prepares and sends away its DNS query.
10. Now the DNS query will be routed over the internet and the DNS server responds.
11. A DNS reply from the home router to the computer will be send.
12. Now the computer sets up the session to the website and a TCP sync message will also be send.
13. The web server replies back with an acknowledge i.e sync-ack.
14. Now the computer sends a TCP Acknowledge.
15. Finally the web server will be able to communicate with the web browser.

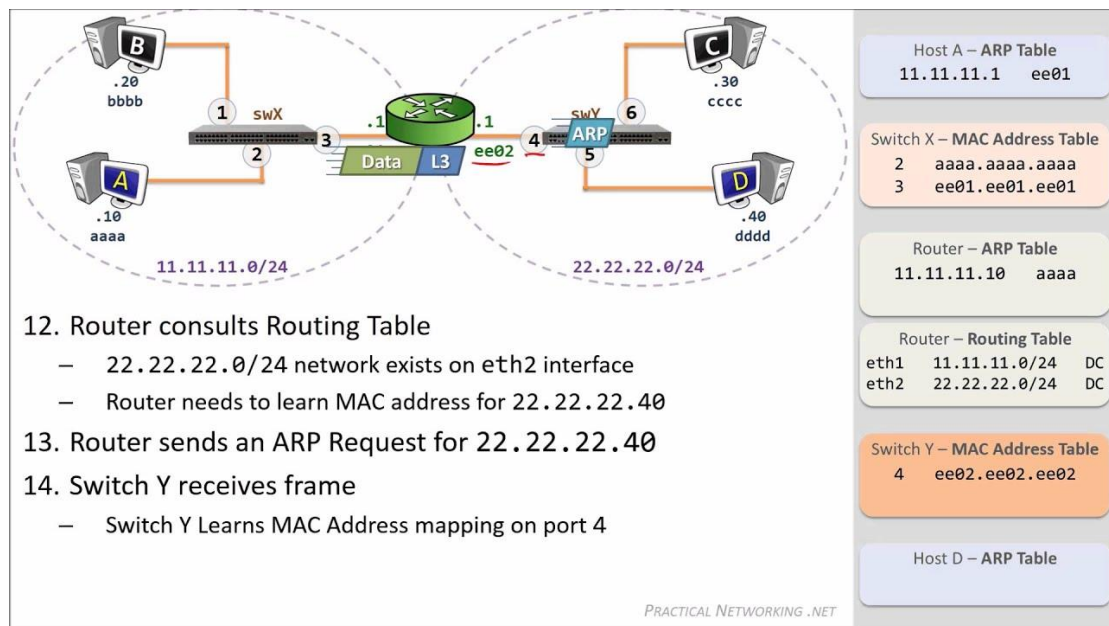


Fig 37: Data traffic Flow

END TO END DATA FLOW

The figure below provides a complete overview of OSI layers, D7 refers to the data unit in layer 7, D6 means unit data in layer 6, and so on. The process begins with a L7 (application layer), and then from layer to layer descending, sequentially. In each layer, the header, or perhaps a trailer, can be added to the data unit.

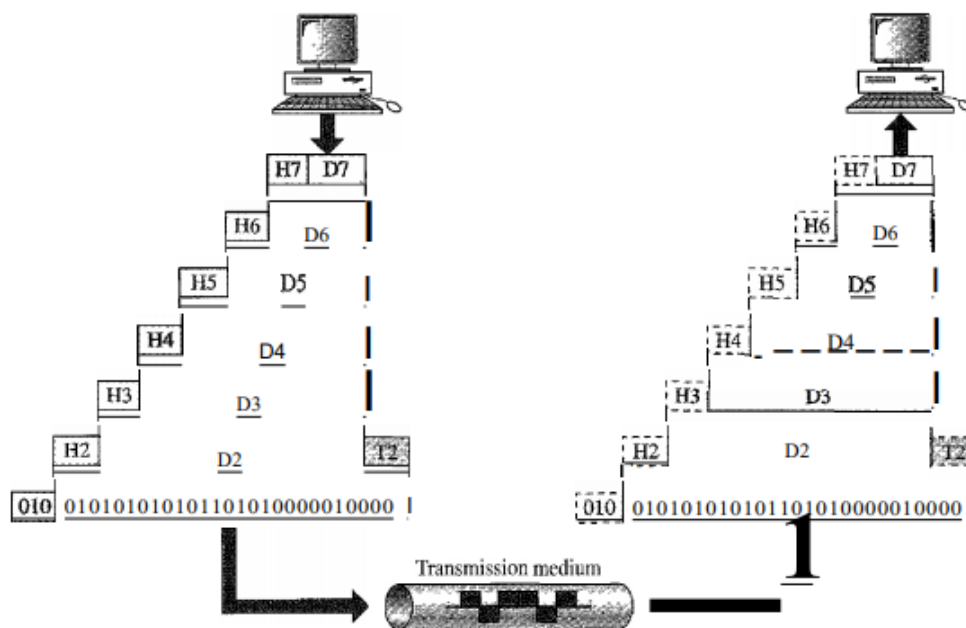


Fig 38: End-to-end data flow of OSI Model

Normally, a trailer can only be added in L2. When a formatted data unit passes with the L1, it is converted into an electric signal again and transmitted by physical link. When we reach our destination, the signal passes through layer 1 and is converted back to digital form. The data units then go back through the OSI layers. As each data block reaches the next higher layer, the headers and trailers attached to it the corresponding post layer is removed, and the appropriate actions for that layer are removed taken. After reaching layer 7, the message is in the appropriate form, the request is also made available to the recipient. The concept also reveals the feature of encapsulation i.e the packet (header and data) at level 7 is packaged at level 6, the entire package at level 6 is packaged in level 5, and so on.

REFERENCES:

- [1] Thiagarajan Viswanathan, Manav Bhatnagar. n.d. Telecommunication Switching Systems and Networks, Second Edition.
- [2] LTE technology overview, prepared by samsung, approved by RJIL,
<https://www.slideshare.net/maheshsavita/day-1-lte-technology-overview>
- [3] <http://www.techplayon.com/rrh-remote-radio-head-connected-bbu-base-band-unit/>
- [4] Reliance Jio Telecom, LTE System Overview for Reliance Jio Installation Project, 2 January,2017,<http://reliance-jio-telecom.blogspot.com/2017/01/lte-system-overview-for-reliance-jio.html>
- [5] Andrew S. Tanenbaum, David Wetherall. n.d. Computer Networks.Pearson, 23-Jul-2013.
- [6] Behrouz A. Forouzan, Sophia Chung Fegan. n.d. *Data Communications and Networking, Fourth Edition*. mcgraw hill education.
- [7] Internet and Networks, http://www.cellbiol.com/bioinformatics_web_development/chapter-1-internet-networks-and-tcp-ip/data-transmission-on-the-internet/
- [8] Express VPN, <https://www.expressvpn.com/internet-privacy/guides/vpn-security-work/>
- [9] https://serc.carleton.edu/introgeo/google_earth/what.html
- [10] ADVANCED GEOGRAPHIC INFORMATION SYSTEMS – Vol. II - GIS Project Planning and Implementation – Somers R.M., Somers-St. Claire, Fairfax, Virginia, USA