

CERTIFICATE

*This is to certify that Mr./Ms.HEMIL...CHOVATIYA.....
with enrolment no.200303108003..... has successfully
completed his/her laboratory experiments in the COMPUTER
NETWORKS (20310525255) from the department of
.....Information Technology(4ITA1)..... during the
academic year2021-2022.....*



Date of Submission:

Staff In charge:

Head of Department:

INDEX

Sr. No	Experiment Title	Page No		Date of Performance	Date of Assessment	Marks (out of 10)	Sign
		From	To				
1	Experiments on Simulation Tools: (CISCO PACKET TRACER).						
2	Experiments of Packet capture tool: (Wireshark).						
3	To study behavior of generic devices used for networking: (CISCO PACKET TRACER).						
4	Data Link Layer (Error Correction).						
5	Virtual LAN.						
6	Wireless LAN.						
7	Internetworking with routers.						
8	Implementation of SUBNETTING.						
9	Routing at Network Layer.						
10	Experiment on Transport Layer.						

PRACTICAL:1

AIM: Experiments on Simulation Tools: (CISCO PACKET TRACER)

INTRODUCTION:

- Packet Tracer is a cross-platform visual simulation tool designed by Cisco systems that allow users to create network topologies and imitate modern computer networks
- Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.
- Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum.
- Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNA Academy students, since it is available to them for free.
- **Workspace:** workspace This is the main area where the devices are placed, designed and different information like router Name, interface names etc are seen
- **Network Component Box:** in this space you see all the devices and connections (Cables types) You can select the Device type ie router, switch etc and in the nearby box, select the specific version of router or switch e.g. 1841, 2620XM
- **Real-time Simulation Bar:** This is a toggle bar where you can move between Real time and Simulation mode. You can capture, forward, play packets using the simulation Mode
- We have dragged the devices ie Router, Switch and PC on the main workspace and then put the interfaces for connectivity. The Green dots show that the connectivity is up
- In the network scenario, click on the PC and you get a window where you can configure the IP address Click on IP Configuration Option.

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.

Types of Topology:

1. Bus Topology
2. Mesh Topology
3. Star Topology
4. Ring Topology
5. Tree Topology
6. Hybrid Topology

1. Bus Topology:

Procedure:

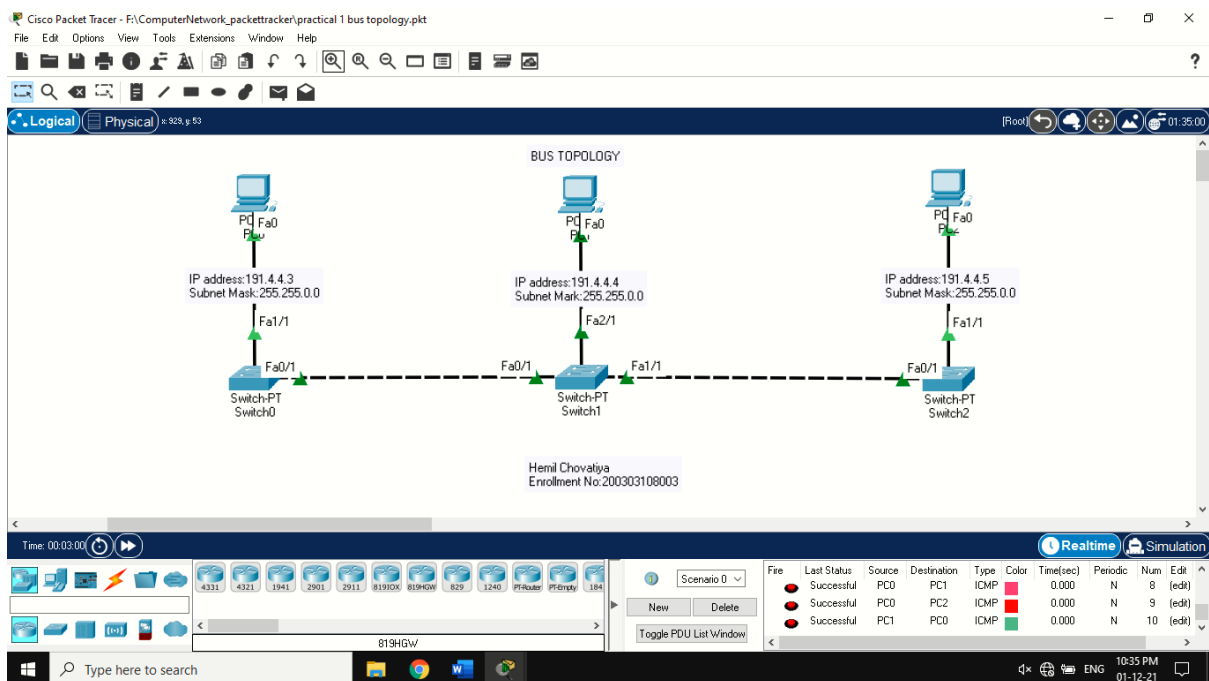
Step 1: Take 3 switches and 3 pc.

Step 2: Assign each pc to its individual switch

Step 3: Connect pc's in a vertical manner with copper straight-through wire and every switch connect with copper cross-over wire.

Step 4: Assign IP Address to every pc.

Step 5: Send the packet one pc to another pc.



2. Mesh Topology:

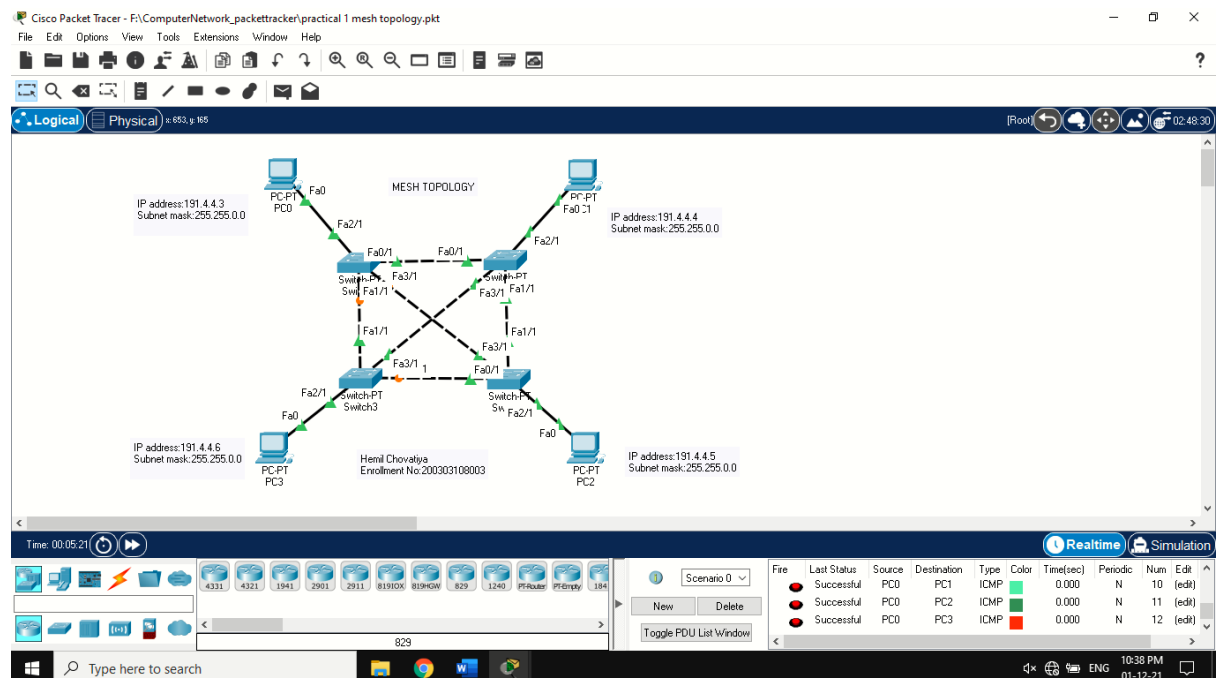
Procedure

Step 1: Take 4 switches and 4 PC.

Step 2: Connect pc's individual switch with copper straight-through wire and every switch connect with copper cross-over wire.

Step 3: Assign IP Address to every pc.

Step 4: Send the packet one pc to another pc



3. Star Topology

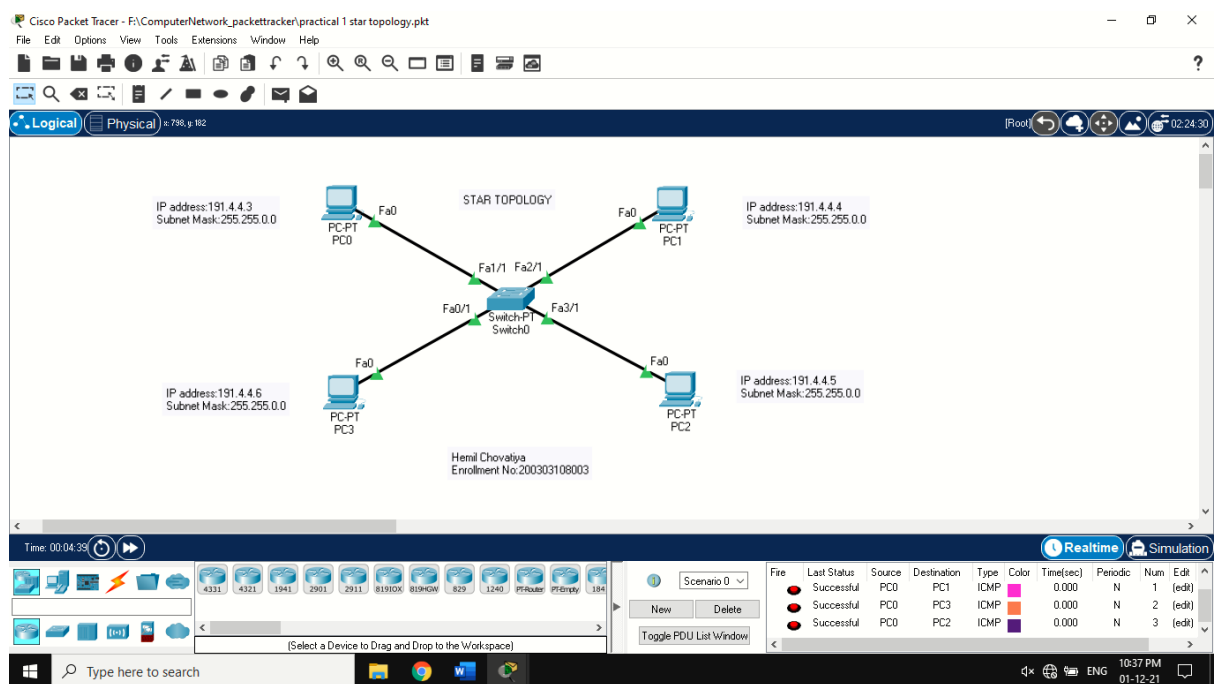
Procedure

Step 1: Take 1 switches and 4 pc.

Step 2: Connect pc's main switch with copper straight-through wire.

Step 3: Assign IP Address to every pc.

Step 4: Send the packet one pc to another pc



4. Ring Topology

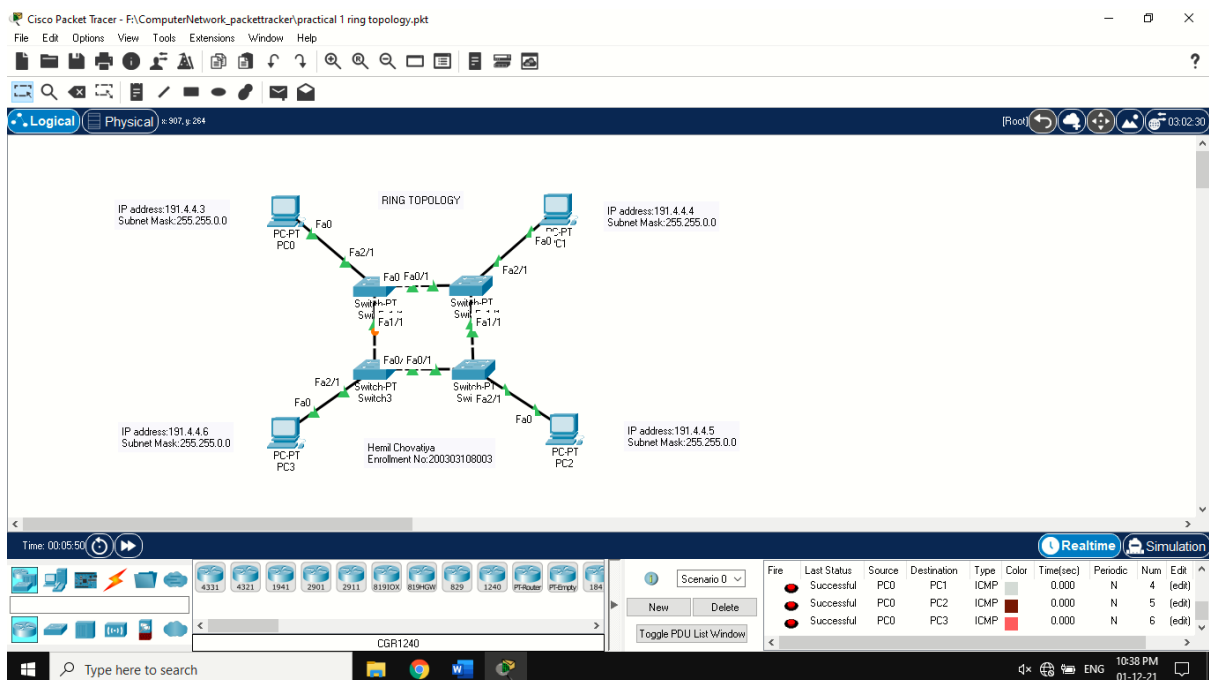
Procedure

Step 1: Take 4 switches and 4 PC.

Step 2: Connect pc's individual switch with copper straight-through wire and every switch connect with copper cross-over wire.

Step 3: Assign IP Address to every pc.

Step 4: Send the packet one pc to another pc.



5. Tree Topology

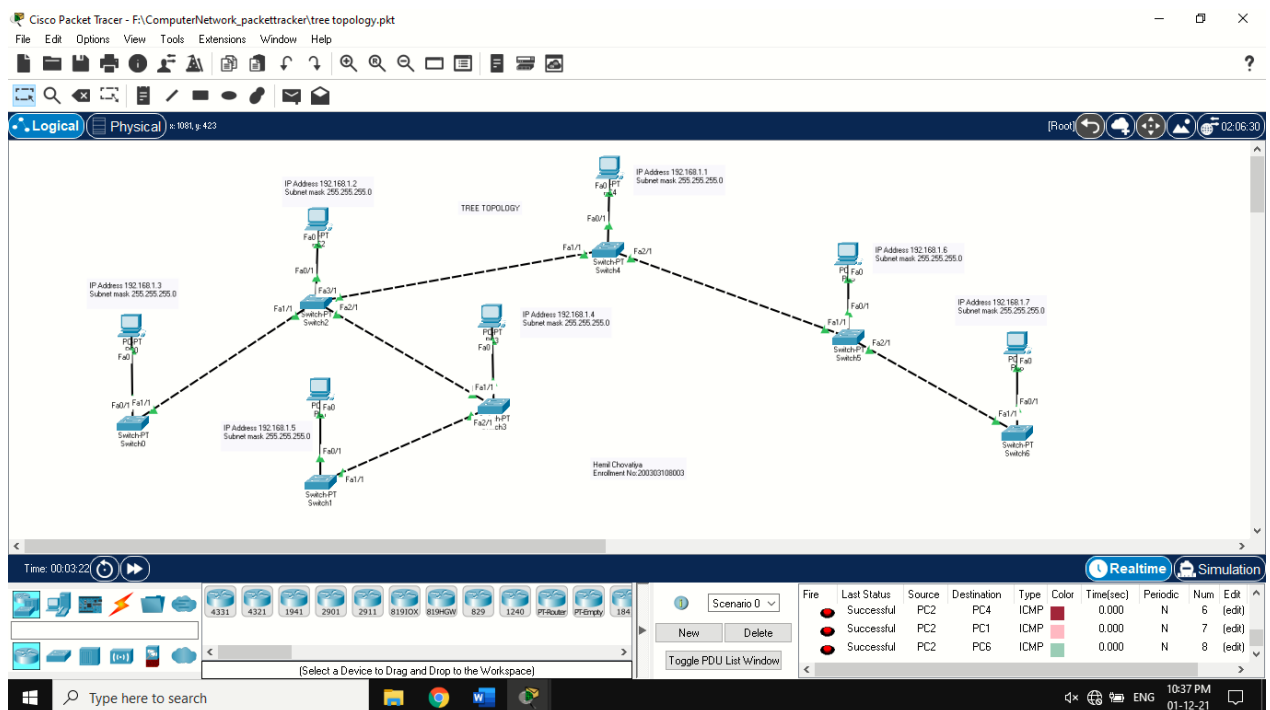
Procedure

Step 1: Take 7 switches and 7 PC.

Step 2: Connect pc's individual switch with copper straight-through wire and every switch connect with copper cross-over wire.

Step 3: Assign IP Address to every pc.

Step 4: Send the packet one pc to another pc.



6. Hybrid Topology

Procedure

- For bus topology

Step 1: Take 3 switches and 3 PC.

Step 2: Connect pc's individual switch with copper straight-through wire and every switch connect with copper cross-over wire.

Step 3: Assign IP Address to every pc.

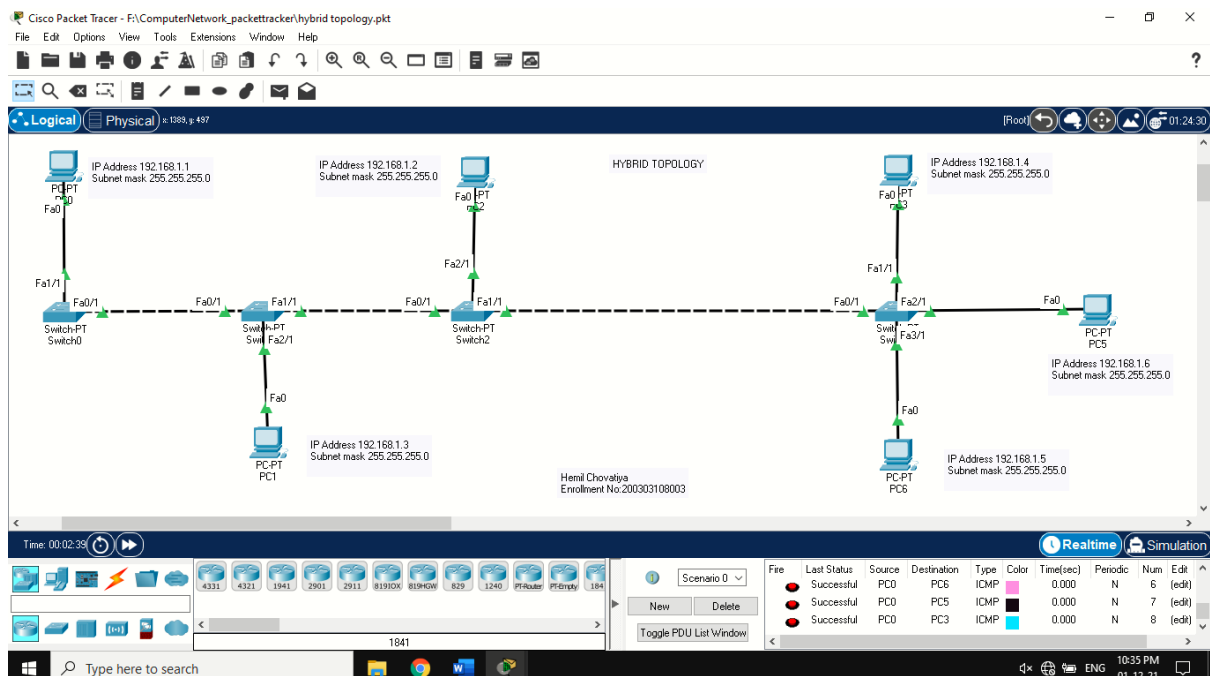
- For star topology

Step 1: Take 1 switches and 3 PC.

Step 2: Connect pc's main switch with copper straight-through wire.

Step 3: Assign IP Address to every pc.

- Combine both topology with copper-crossover wire ➤ Send the packet one topology's pc to another.



PRACTICAL:2

AIM: Make a connection using Router.

Theory:

➤ IP address Range:

1. Class A:- 0 - 127

N.H.H.H n=8, h=24

Subnet mask is 255.0.0.0

2. Class B:- 128-191

N.N.H.H n=16, h=16

Subnet mask is 255.255.0.0

3. Class C:- 192 – 223

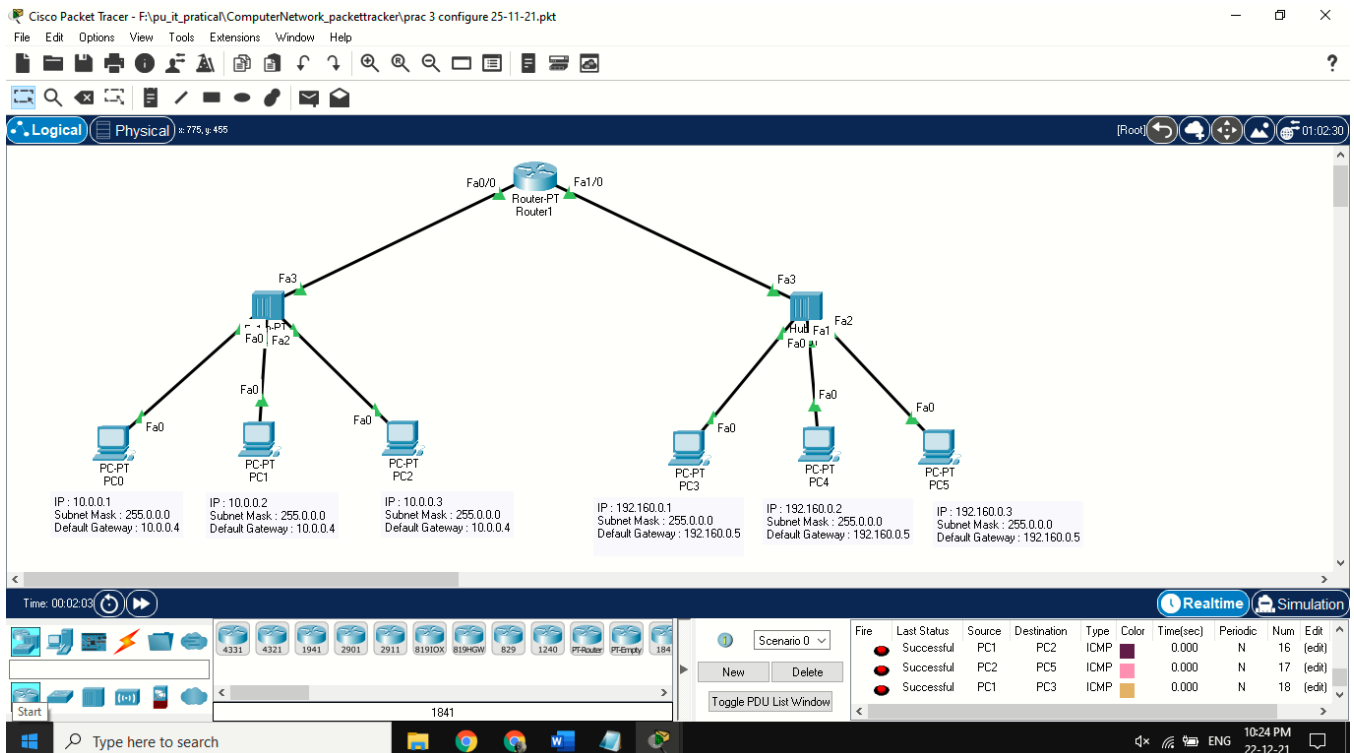
N.N.N.H n=24, h=8

Subnet mask is 255.255.255.0

4. Class D:- 224 - 239 (multicasting)

5. Class E:- 240 - 255 (experiment)

➤ Implementation:



➤ **Steps to connect router with switches.**

1. Then assign IP address to all the PC.
2. Then click on router and go to CLI(command line interface).
3. When you see “would you like to enter initial configuration dialog?” Type n and press enter key.
4. Write enable
5. Write configure
6. Write terminal
7. Write hostname Hemil
8. Write Interface giga 0/0/0
9. Write Ip address 10.0.0.9 255.255.255.0
10. Write no shut
11. Then write exit
12. Write interface giga0/0/1
13. Write ip address 192.0.0.9 255.255.255.0
14. Write no shut.
15. Now connection between two switches has been made, and now to transport data from pc0 to pc6
16. Write their side of ip address of router in the default gateway in the config.

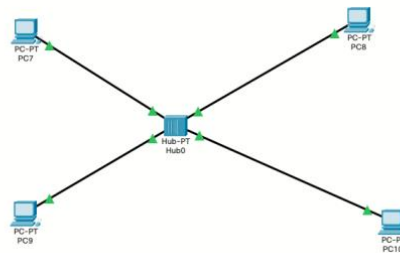
PRACTICAL:3

AIM: To study behaviour of generic devices used for networking.

Theory:

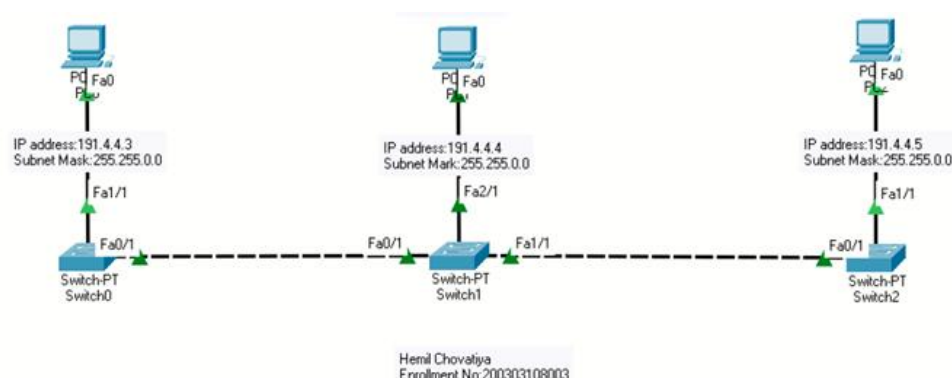
Hub: -

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.



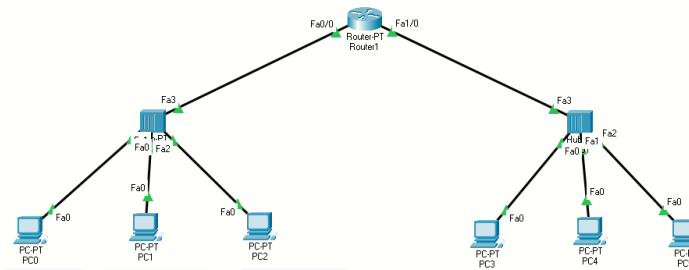
Switches:-

Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus.



Router: -

Router is a hardware which is used for sharing internet access through sharing networks within local area. These routers have designed with the potential to transfer signals from a single point to the multiple exact destinations. It is essential to get a router for sharing your application and internet within your LAN



Gate Way:

In a communications network, a network node equipped for interfacing with another network that uses different protocols.

- A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.
- A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

Bridge:

A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge. Bridges can analyse incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

Repeater:

Functioning at Physical Layer. A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports, so cannot be use to connect for more than two devices

PRACTICAL:4

AIM: To study of Hamming code.

Theory:

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. There are seven bits where 1st, 2nd and 4th bits are parity (even parity here) bits and others are data bits. Where 1st bit depends on 3rd, 5th, 7th bit. 2nd bit depends on 3rd, 6th, 7th bit. 3rd bit depends on 5th, 6th, 7th bit.

Code:

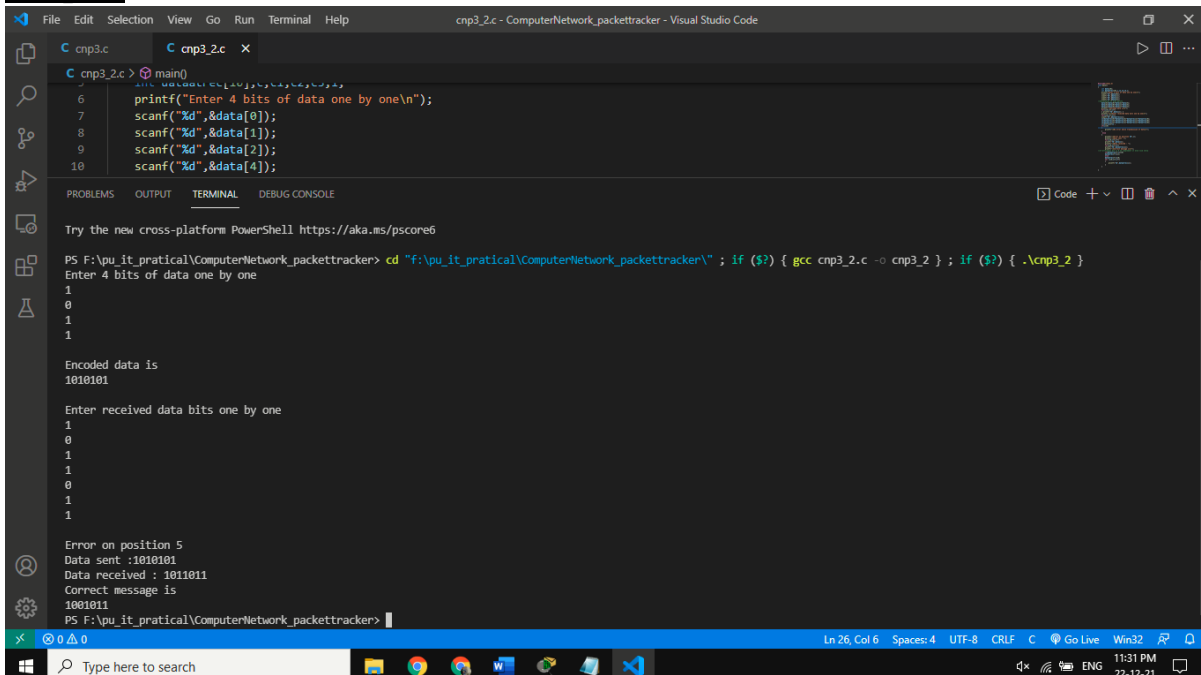
```
#include<stdio.h>
void main()
{
    int data[10];
    int dataatrec[10],c,c1,c2,c3,i;
    printf("Enter 4 bits of data one by one\n");
    scanf("%d",&data[0]);
    scanf("%d",&data[1]);
    scanf("%d",&data[2]);
    scanf("%d",&data[4]);
    //Calculation of even parity
    data[6]=data[0]^data[2]^data[4];
    data[5]=data[0]^data[1]^data[4];
    data[3]=data[0]^data[1]^data[2];
    printf("\nEncoded data is\n");
    for(i=0;i<7;i++)
    { printf("%d",data[i]); }
    printf("\n\nEnter received data bits one by one\n");
    for(i=0;i<7;i++)
    scanf("%d",&dataatrec[i]);
    c1=dataatrec[6]^dataatrec[4]^dataatrec[2]^dataatrec[0];
    c2=dataatrec[5]^dataatrec[4]^dataatrec[1]^dataatrec[0];
    c3=dataatrec[3]^dataatrec[2]^dataatrec[1]^dataatrec[0];
    c=c3*4+c2*2+c1 ;
    if(c==0)
    {
        printf("\nNo error while transmission of data\n");
    }
}
```

```

    }
    else
    {
        printf("\nError on position %d",c);
        printf("\nData sent :");
        for(i=0;i<7;i++)
            printf("%d",data[i]);
        printf("\nData received : ");
        for(i=0;i<7;i++)
            printf("%d",dataatrec[i]);
        printf("\nCorrect message is\n");
//if errorneous bit is 0 we complement it else vice versa
        if(dataatrec[7-c]==0)
            dataatrec[7-c]=1;
        else
            dataatrec[7-c]=0;
        for (i=0;i<7;i++)
        {
            printf("%d",dataatrec[i]);
        }
    }
}

```

Output:



```

cnp3_2.c
cnp3_2.c X
cnp3_2.c main()
6   printf("Enter 4 bits of data one by one\n");
7   scanf("%d",&data[0]);
8   scanf("%d",&data[1]);
9   scanf("%d",&data[2]);
10  scanf("%d",&data[4]);

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS F:\pu_it_pratical\ComputerNetwork_packettracker> cd "F:\pu_it_pratical\ComputerNetwork_packettracker\" ; if ($?) { gcc cnp3_2.c -o cnp3_2 } ; if ($?) { .\cnp3_2 }
Enter 4 bits of data one by one
1
0
1
1

Encoded data is
1010101

Enter received data bits one by one
1
0
1
1
0
1
1

Error on position 5
Data sent :1010101
Data received : 1010101
Correct message is
1001011
PS F:\pu_it_pratical\ComputerNetwork_packettracker>

```


PRACTICAL:5

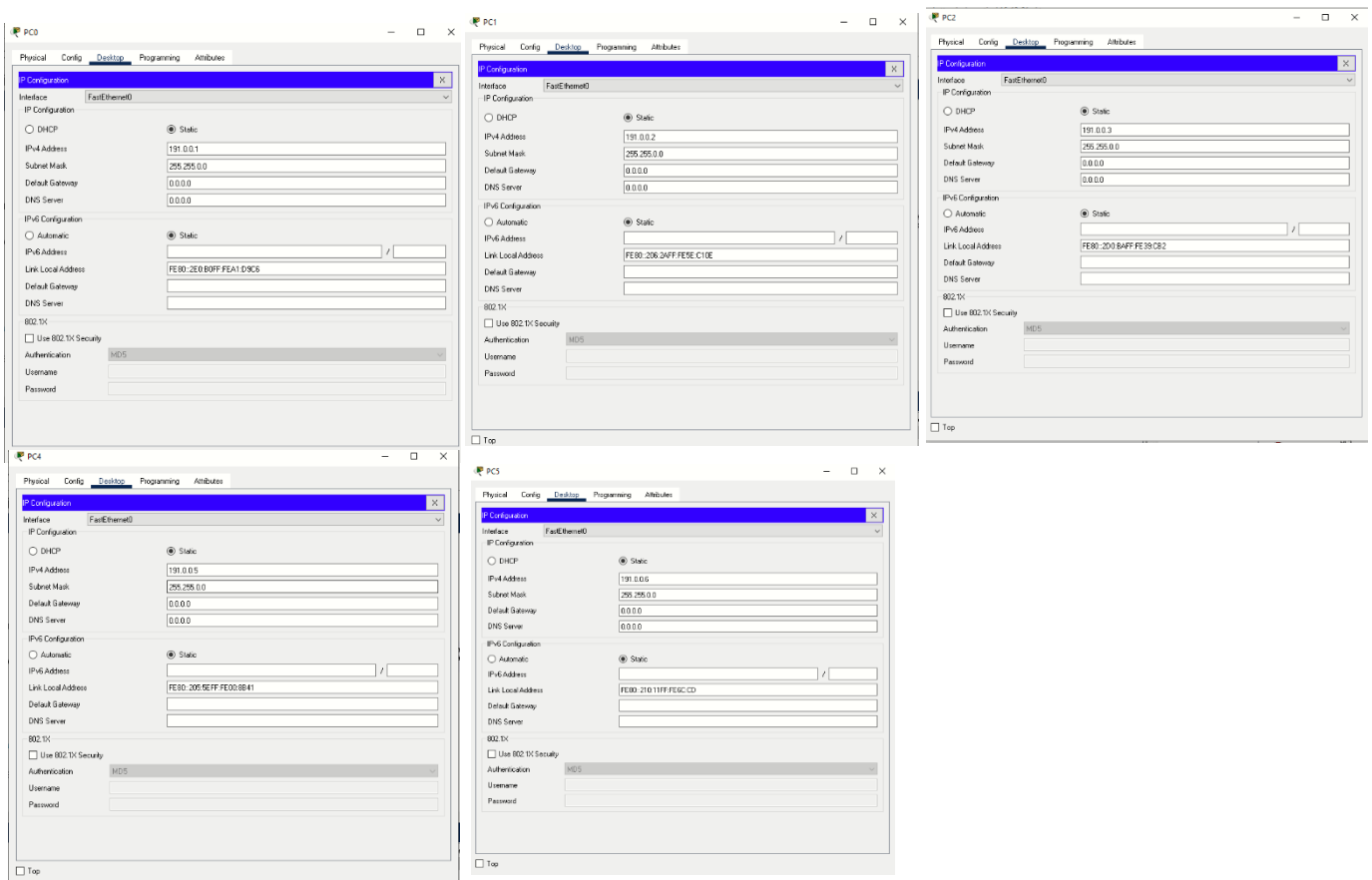
AIM : Create a VLAN on CISCO PACKET TRACER.

Theory:

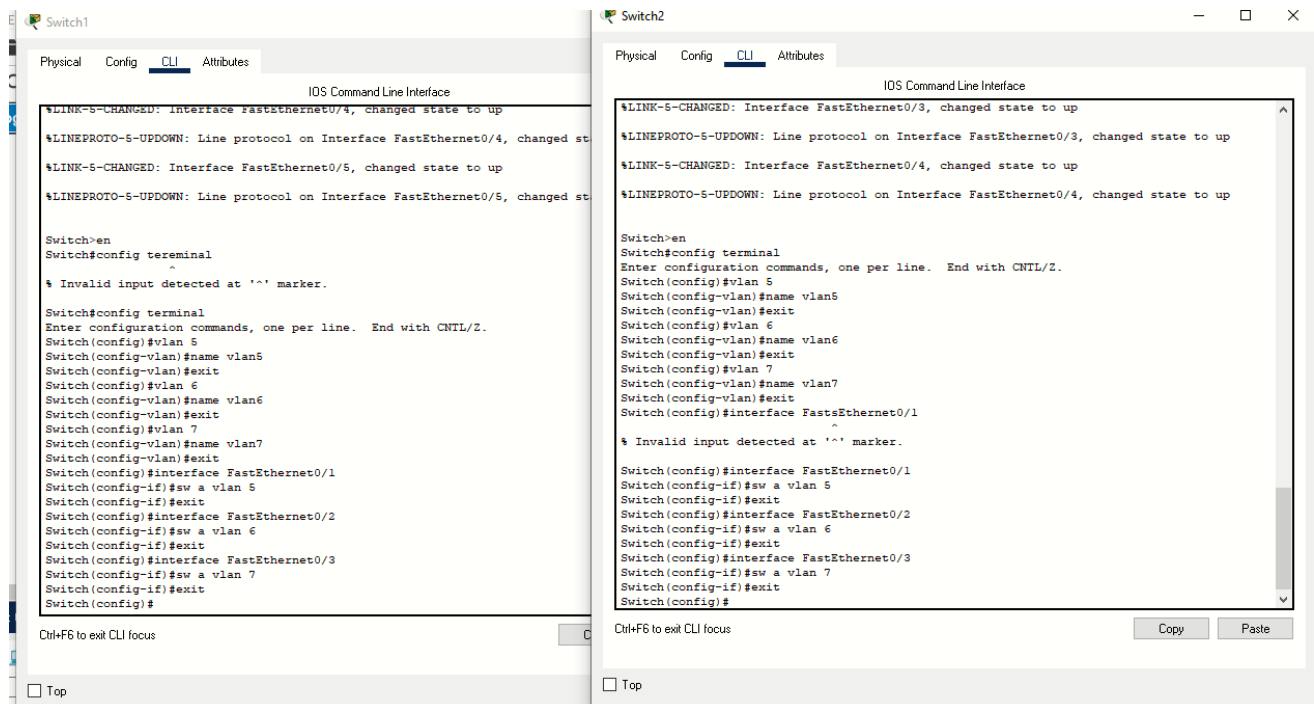
A VLAN (virtual LAN) is a subnetwork which can virtually group together collections of devices on separate physical local area networks (LANs).

Steps:

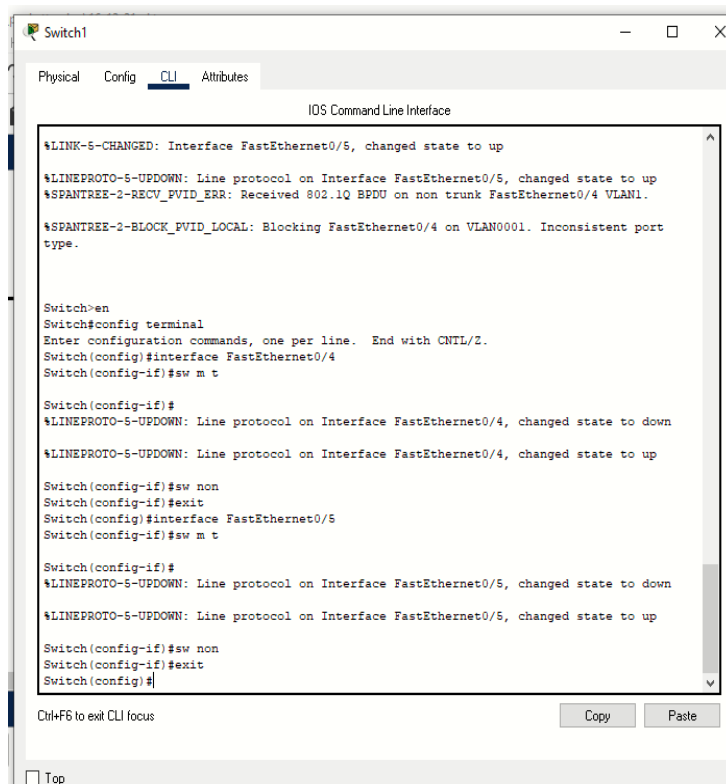
1. First make a network as in the photo, and give IP address from same class to all the PCs.

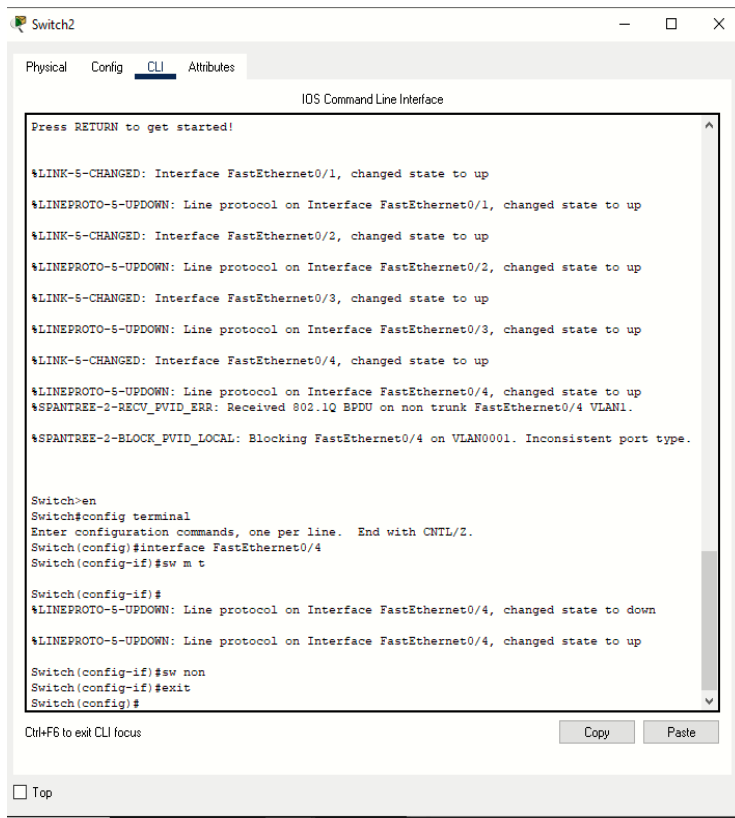


2. Then click on switch 1 and go to CLI and take following steps
enable > config > vlan 5 > name vlan5 > exit > vlan 6 > name vlan6>exit
3. Do the same for switch 2.



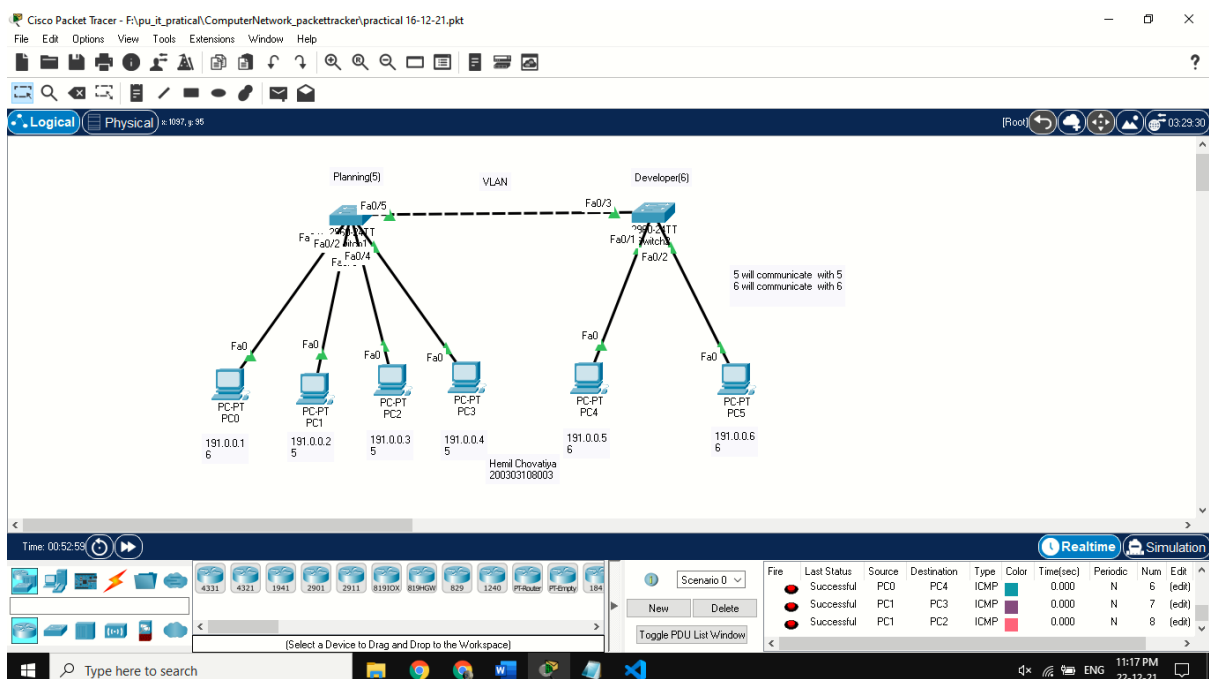
4. Click on switch 1 and go to CLI and set every PC to the VLAN from vlan 5 or vlan 6. i.e. **enable> configure terminal > interface fastethernet 0/1 > sw a vlan 6 > exit.**
5. To successfully connect two switches take following steps in CLI of both switches.i.e. **en > config terminal > interface fastethernet 0/5 > sw m t > sw non>exit.**





After this process even if PCs are in physical connection they won't be able to transfer packet.

Implementation:



PRACTICAL:6

AIM: Wireless LAN.

Theory:

Procedure

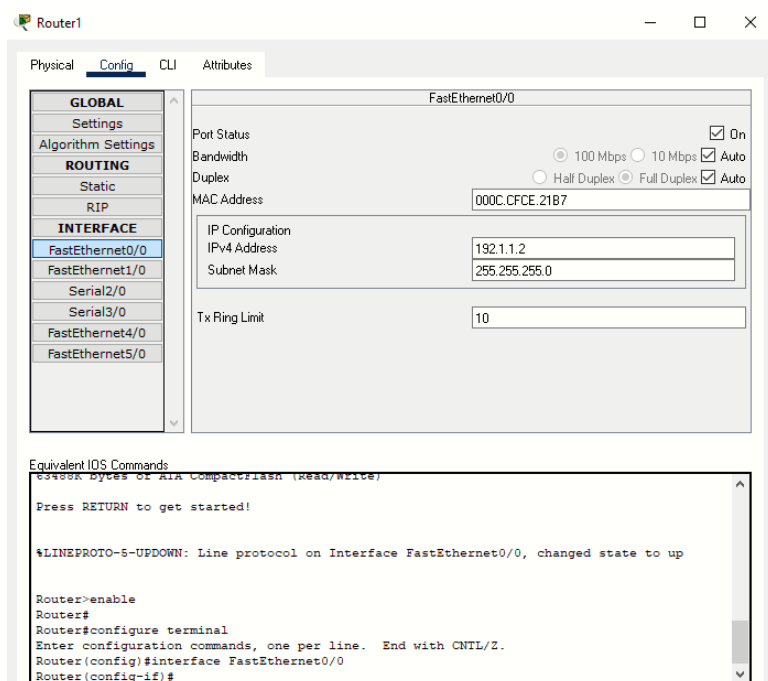
Step 1: Take 1 Switch ,1 Router, 2 Pc,1 access point.

Step 2: Connect to each other with copper straight-through wire.

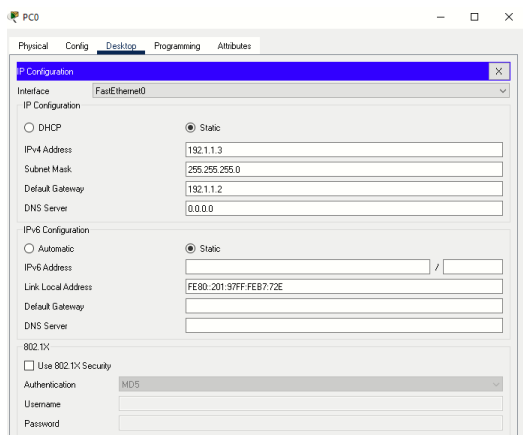
Step 3: Take 1 access point-PT and it connect with switch with straight-through wire.

Step 4: Take wireless components like 1 pc,1 laptop,1 tablet,1 smartphone,1 printer.

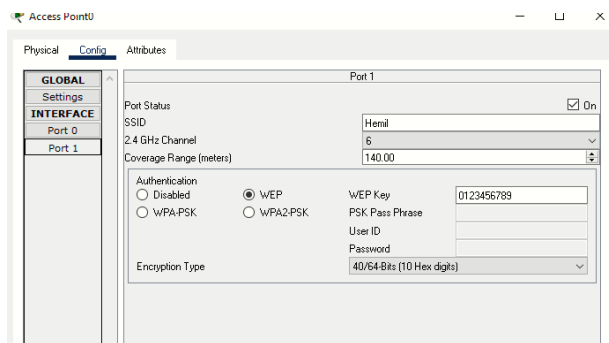
Step 5: Assign IP Address to router (192.1.1.2) and port status is on



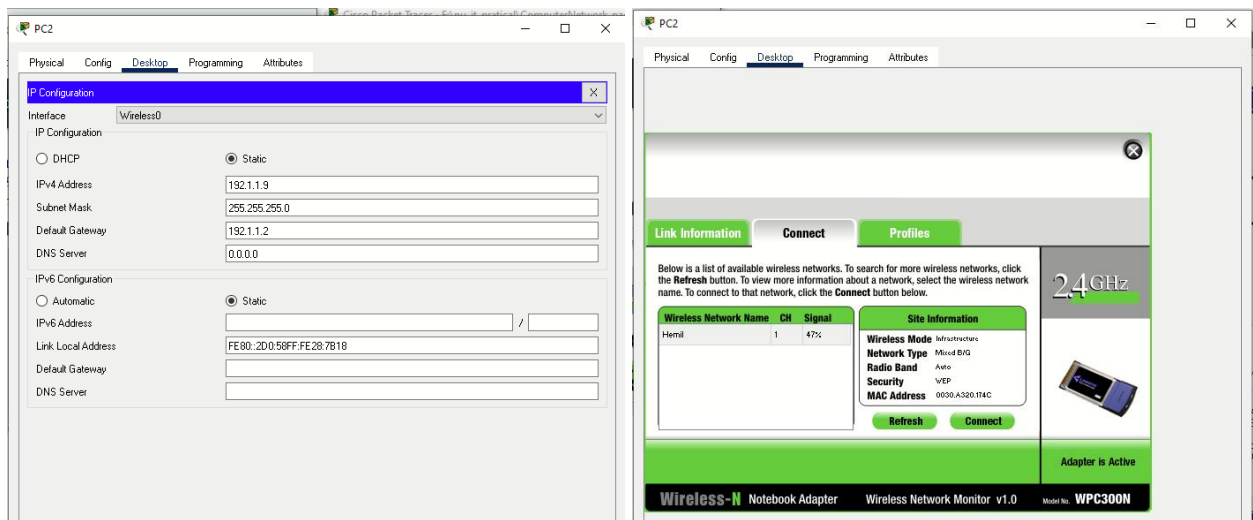
Step 6: Assign IP Address to Pc and default gateway to them.



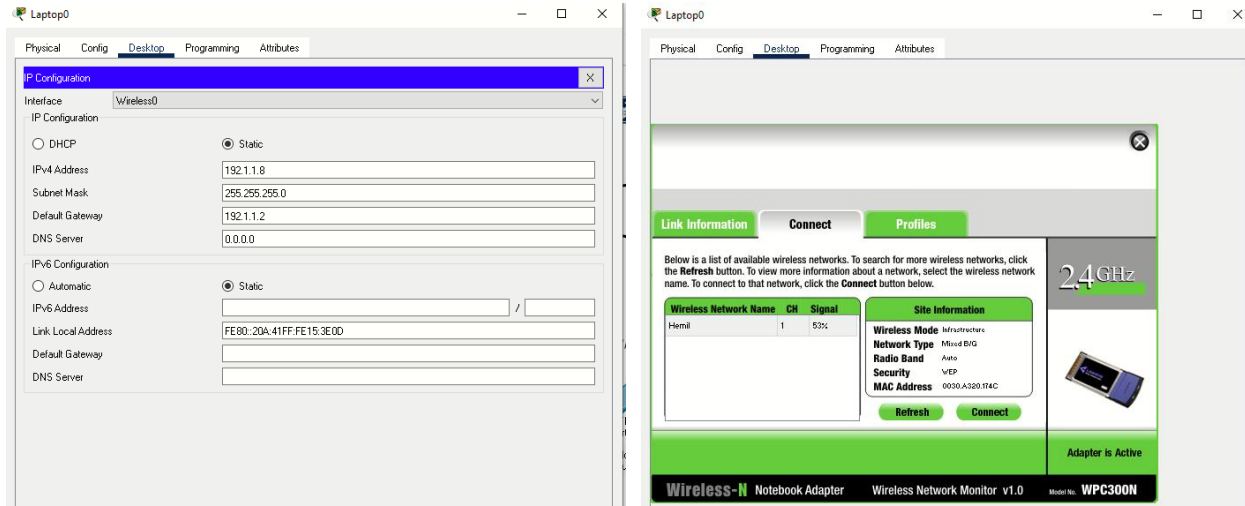
Step 7: In the access point config > port 1 select WEP, WEP Key is (0123456789) and SSID change default to name.



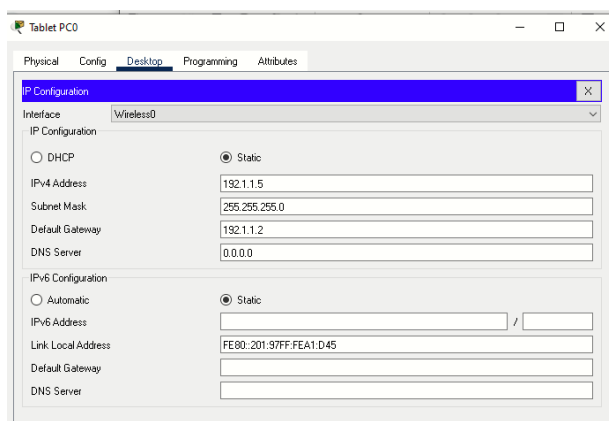
Step 8: In wireless component pc in physical section switch off and remove the port and provide WMP300N and switch on. Assign IP Address and also provide default gateway. In pc wireless section connect given wireless network.



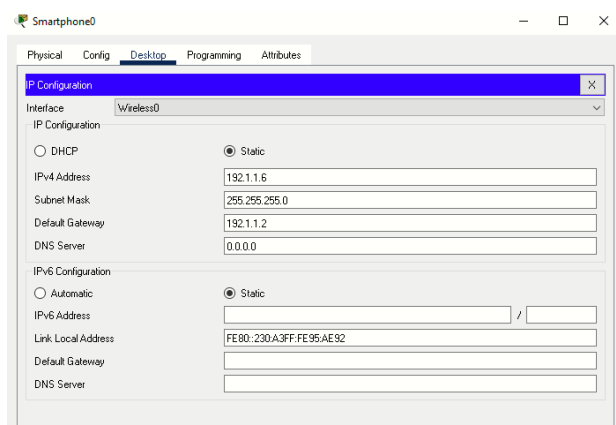
Step 9: In wireless component laptop in physical section switch off and remove the port and provide WPC300N and switch on. Assign IP Address it and also provide default gateway. In pc wireless section connect given wireless network.



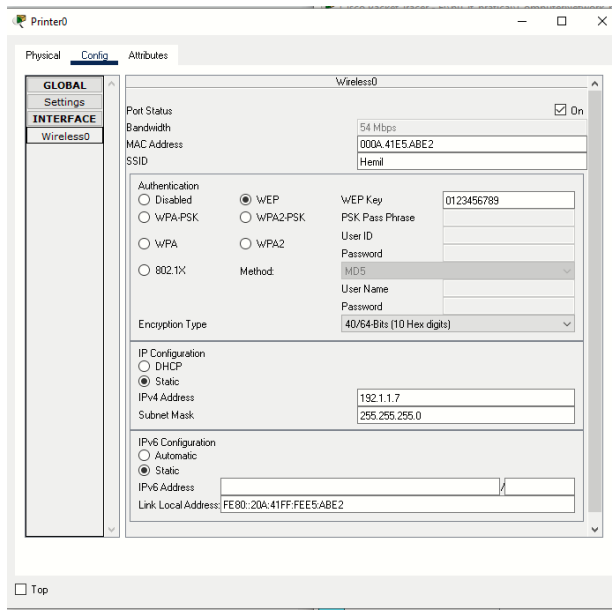
Step 10: In wireless component tablet in Assign IP Address and also provide default gateway.



Step 11: In wireless component Smartphone in Assign IP Address and also provide default gateway.

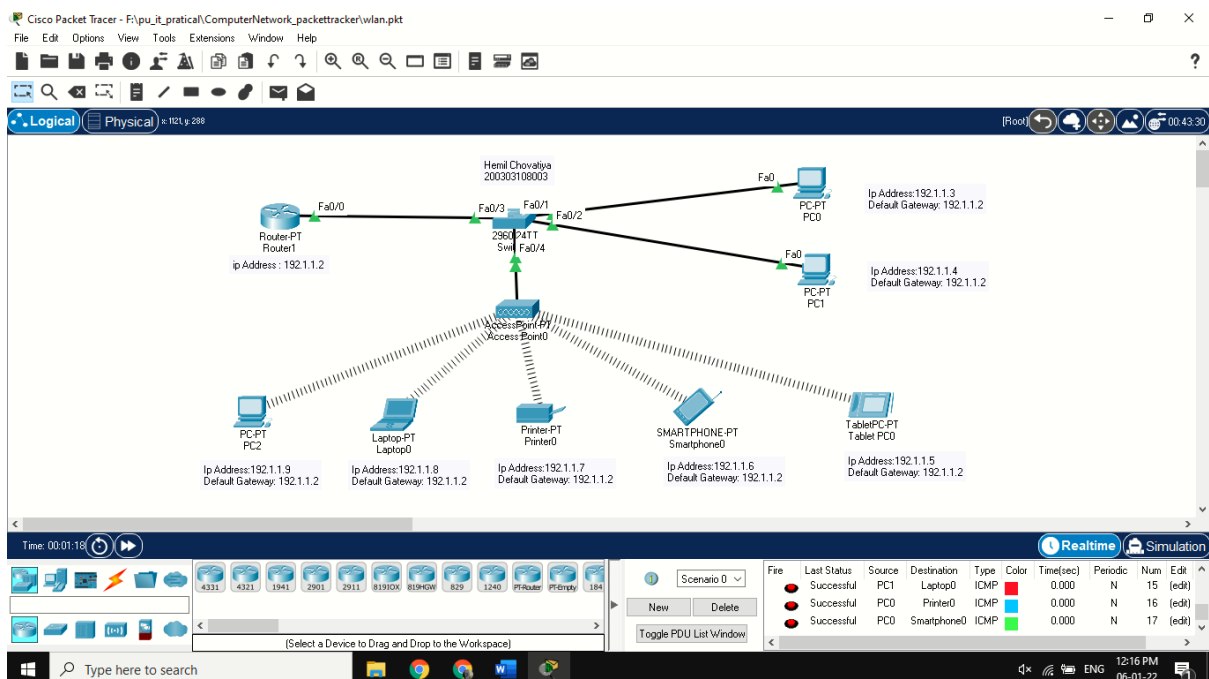


Step 12: In wireless component printer config section select WEP, write WEP Key (1234567890) and change SSID default to name. In physical section >switch off and remove the port and provide WPC300N and switch on.



Step 13: send the packet wireless devices to pc or router.

Output:



PRACTICAL:7

AIM: Internetworking with routers.

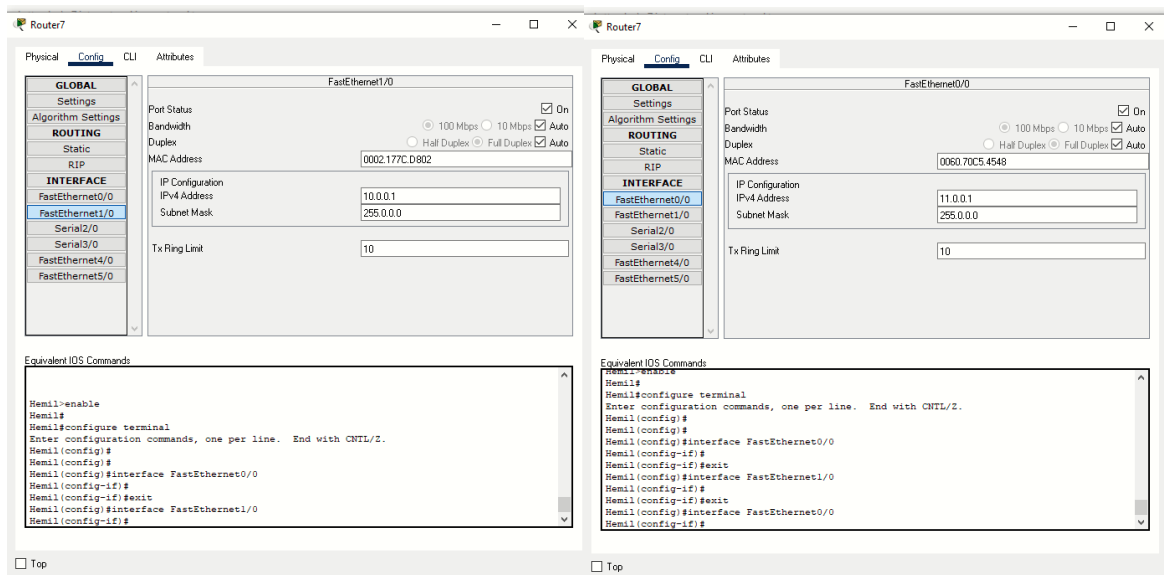
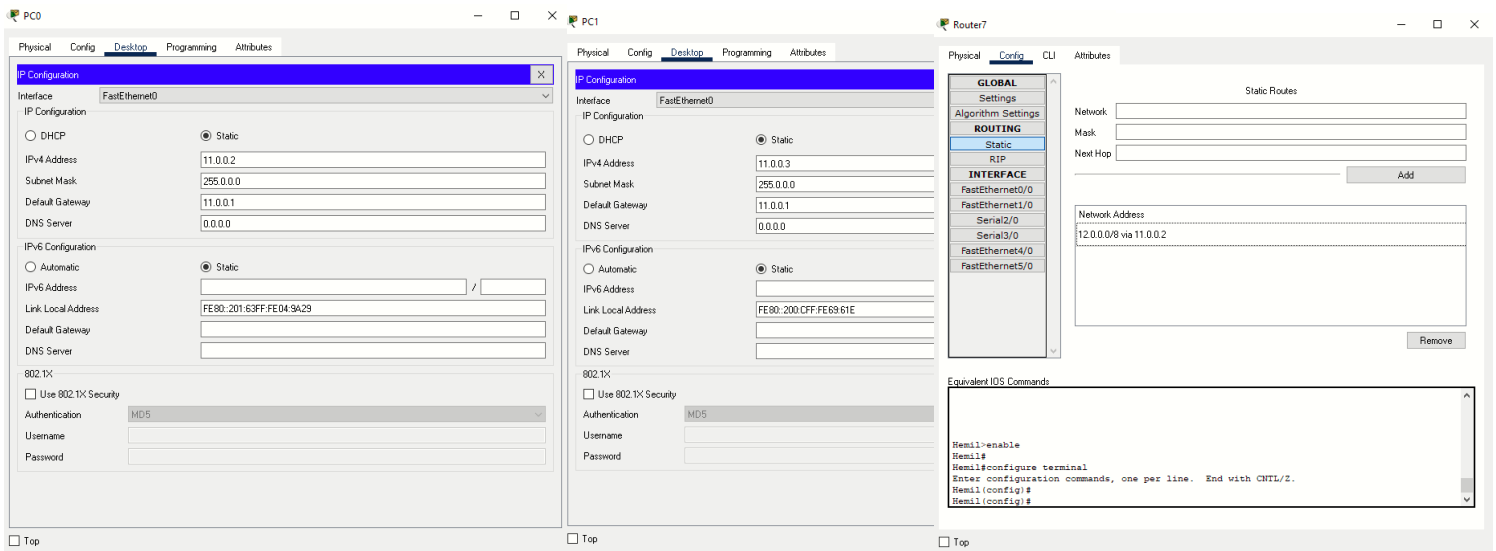
1. Experiment on same Subnet. 2. Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination.

Theory:

Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination.

Step 1: take 2 router, 2 switch, (2960-40), 4 pc and Create 3 subnet assign ip address to all pc and router.

Step 2: assign IP Address according to subnet to PC and router. also assign subnet mask and default gateway.

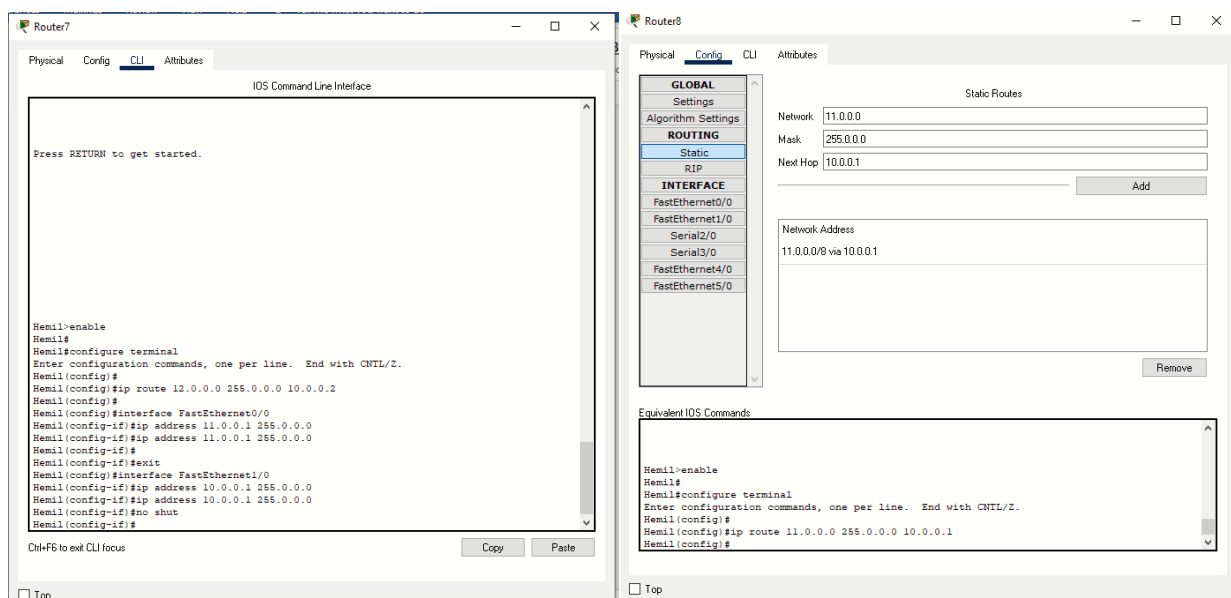


**Step 3: for router0, enable> configure terminal > interface fastethernet 0/0
> ip address 11.0.0.1 255.255.192.0 > exit.**

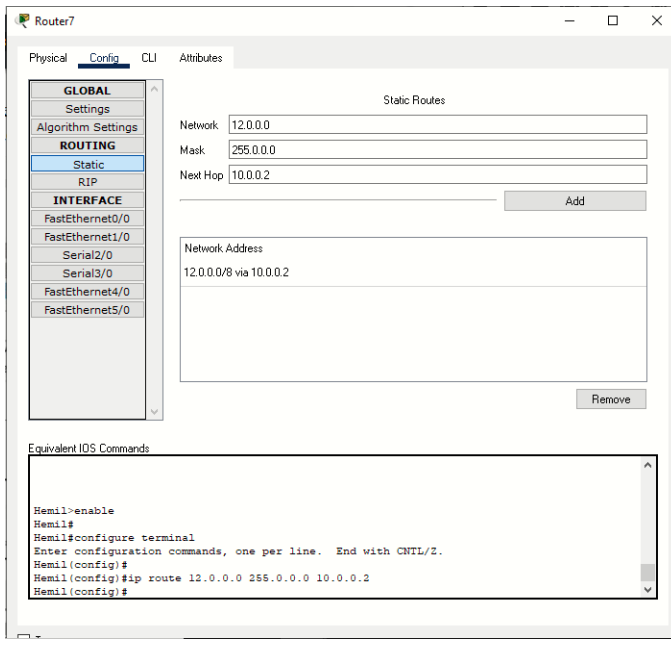
**for router0, enable> configure terminal > interface fastethernet 1/0
> ip address 10.0.0.1 255.255.192.0 > no shut>exit.**

**for router1, enable> configure terminal > interface fastethernet 1/0
> ip address 10.0.0.2 255.255.192.0 > exit.**

**for router1, enable> configure terminal > interface fastethernet 0/0
> ip address 12.0.0.1 255.255.192.0 > no shut >exit. And also ip route**



Cli command For Router 8> Hemil(config)#ip route 11.0.0.0 255.0.0.0 10.0.0.1
Cli command For Router 7 >Hemil(config)#ip route 12.0.0.0 255.0.0.0 10.0.0.2



Router7

Physical Config CLI Attributes

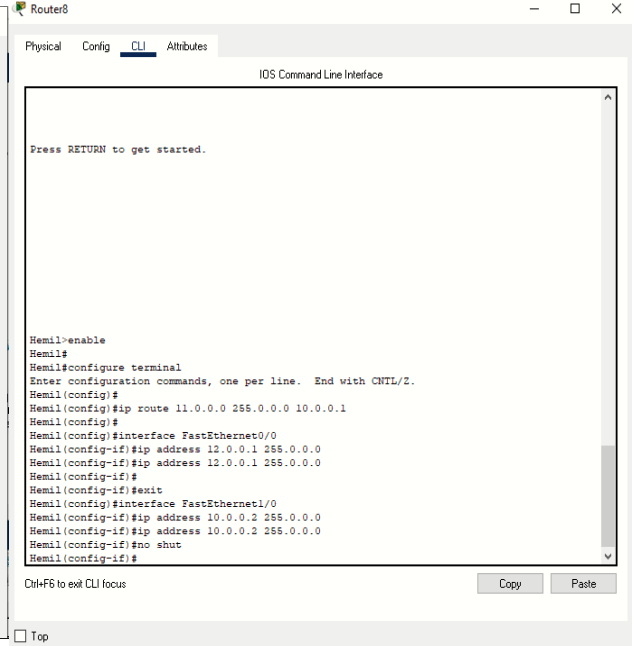
Static Routes

Network: 12.0.0.0
Mask: 255.0.0.0
Next Hop: 10.0.0.2

Network Address: 12.0.0.0/8 via 10.0.0.2

Equivalent IOS Commands:

```
Hemil>enable
Hemil#
Hemil#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hemil(config)#
Hemil(config)#ip route 12.0.0.0 255.0.0.0 10.0.0.2
Hemil(config)#
```



Router8

Physical Config CLI Attributes

IOS Command Line Interface

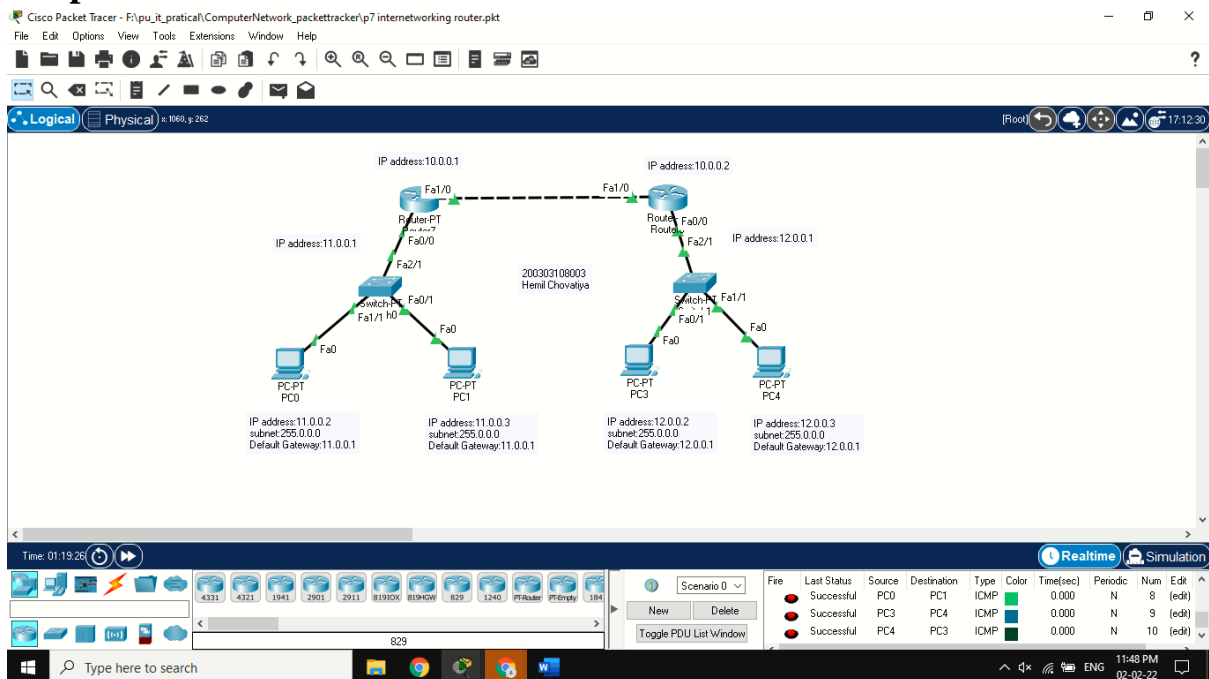
Press RETURN to get started.

```
Hemil>enable
Hemil#
Hemil#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hemil(config)#
Hemil(config)#ip route 11.0.0.0 255.0.0.0 10.0.0.1
Hemil(config)#
Hemil(config)#interface FastEthernet0/0
Hemil(config-if)#ip address 12.0.0.1 255.0.0.0
Hemil(config-if)#ip address 12.0.0.1 255.0.0.0
Hemil(config-if)#
Hemil(config-if)#exit
Hemil(config)#interface FastEthernet1/0
Hemil(config-if)#ip address 10.0.0.2 255.0.0.0
Hemil(config-if)#ip address 10.0.0.2 255.0.0.0
Hemil(config-if)#no shut
Hemil(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Output:



PRACTICAL:8

AIM: Implementation of SUBNETTING.

Theory:

SUBNETTING:

Procedure:

Step 1: Take 2 switch(2950-24TT), 2 router and 4 pc.

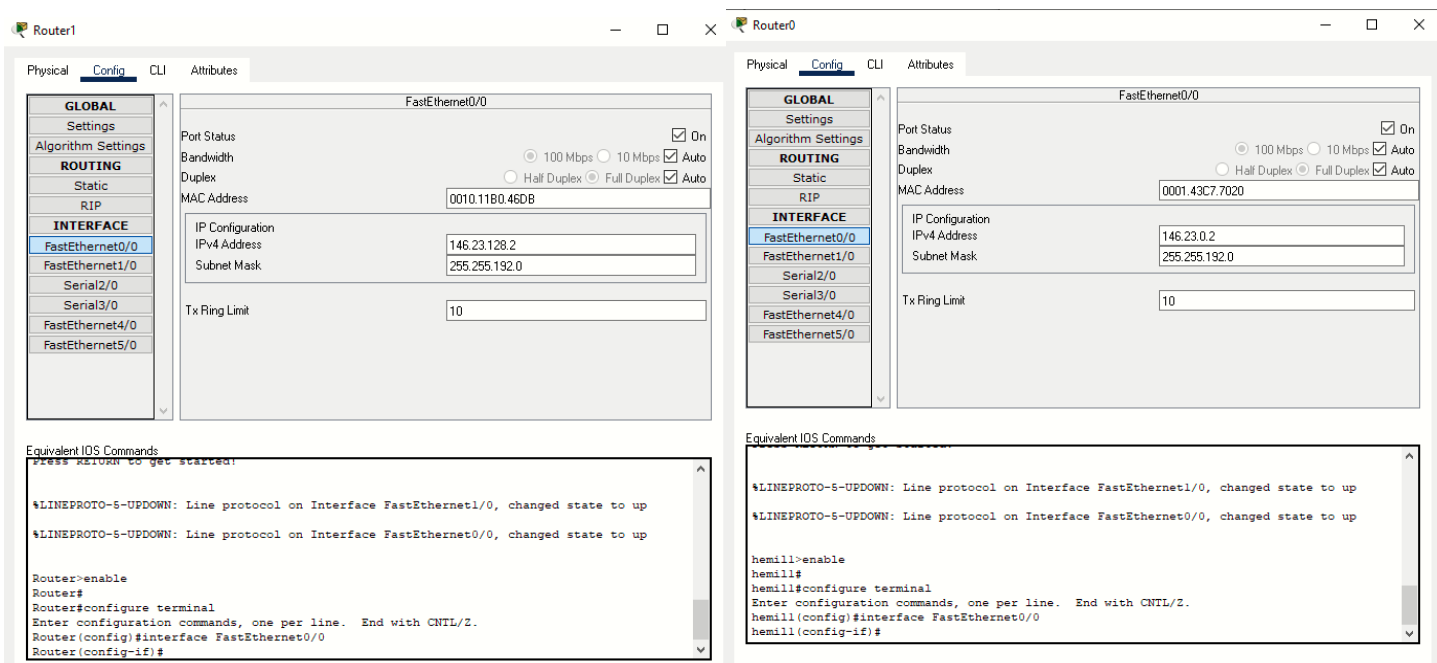
Step 2: 2 pc connected to 1st switch and remaining 2 pc connected to 2nd switch with copper straight-through wire.

Step 3: Assign ip address, default gateway and subnet mask to each pc.

Step 4: Take 2 routers and it connects with switch through copper straight wire.

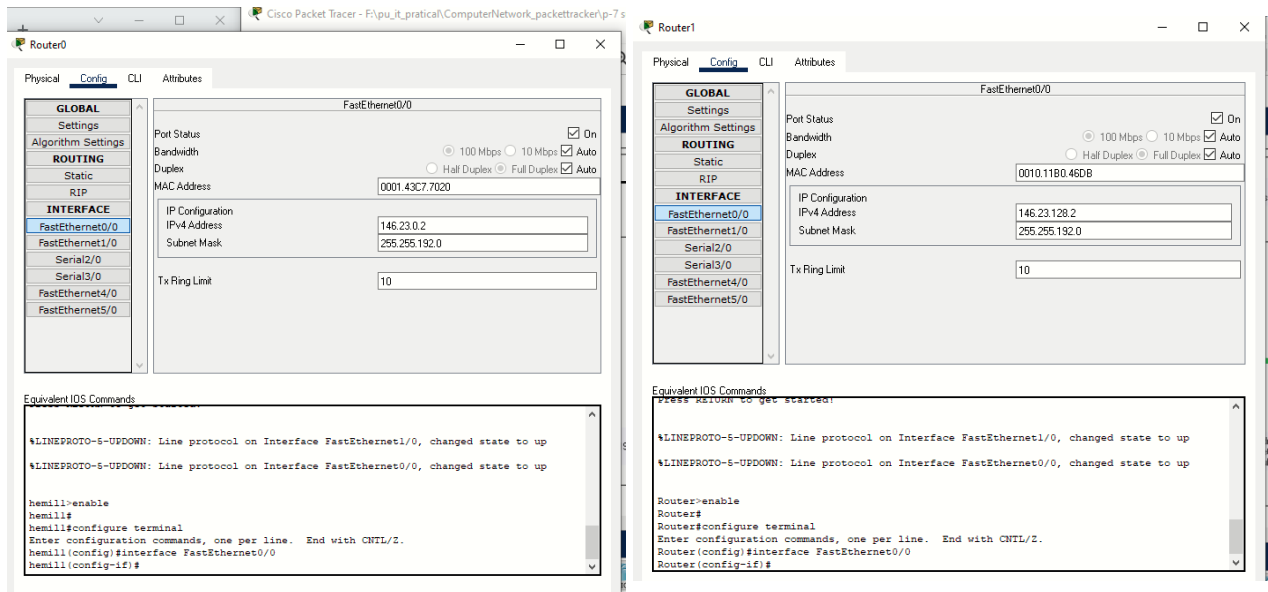
Step 5: For 1st router config section assign ip address and subnet mask of fast ethernet0/0.and port status is also on.

Step 6: For 2nd router config section assign ip address and subnet mask of fast ethernet0/0.and port status is also on.



Step 7: Connect routers with Serial DTE cable.

Step 8: In routers config section assign ip address and subnet mask of serial 0/3/0 and serial 0/3/1 and port status is also on.



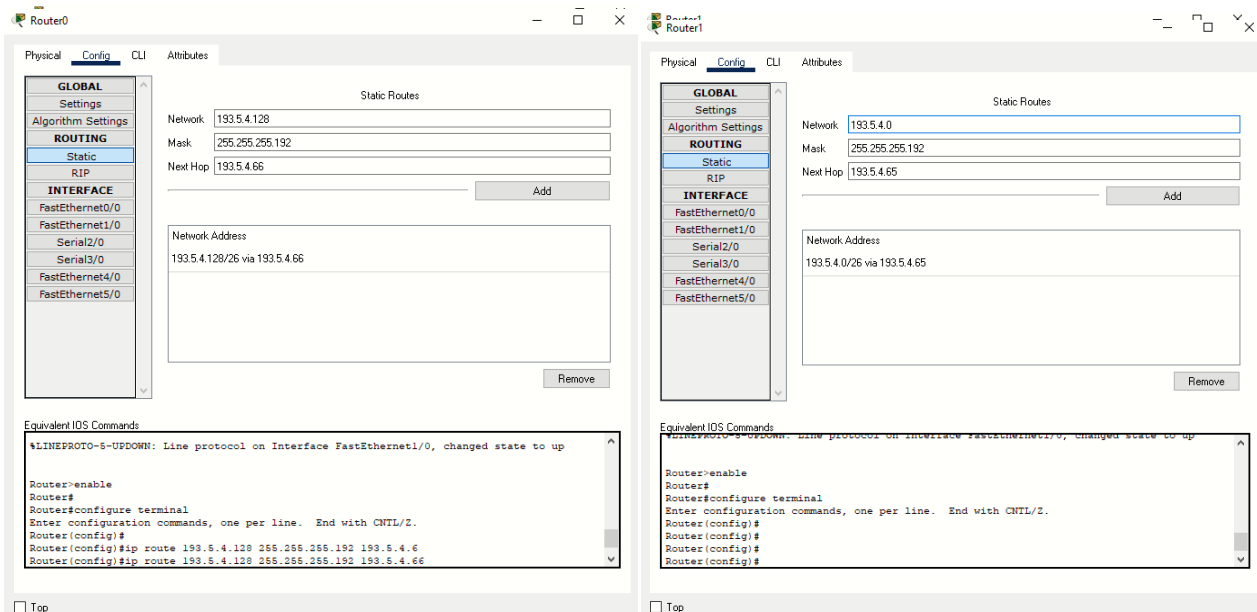
The image shows two screenshots of Cisco Packet Tracer router configuration windows. The left window is for Router0, and the right window is for Router1. Both windows show the 'Config' tab with the 'INTERFACE' section selected. In Router0, the 'FastEthernet0/0' interface is configured with IP Address 146.23.0.2 and Subnet Mask 255.255.192.0. In Router1, the 'FastEthernet0/0' interface is configured with IP Address 146.23.128.2 and Subnet Mask 255.255.192.0. Both windows also show the 'Equivalent IOS Commands' section with the following commands:

```

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
  
```

Step 9: Go to static section and add the network address.

Step 10: Go to setting and save the added network address.

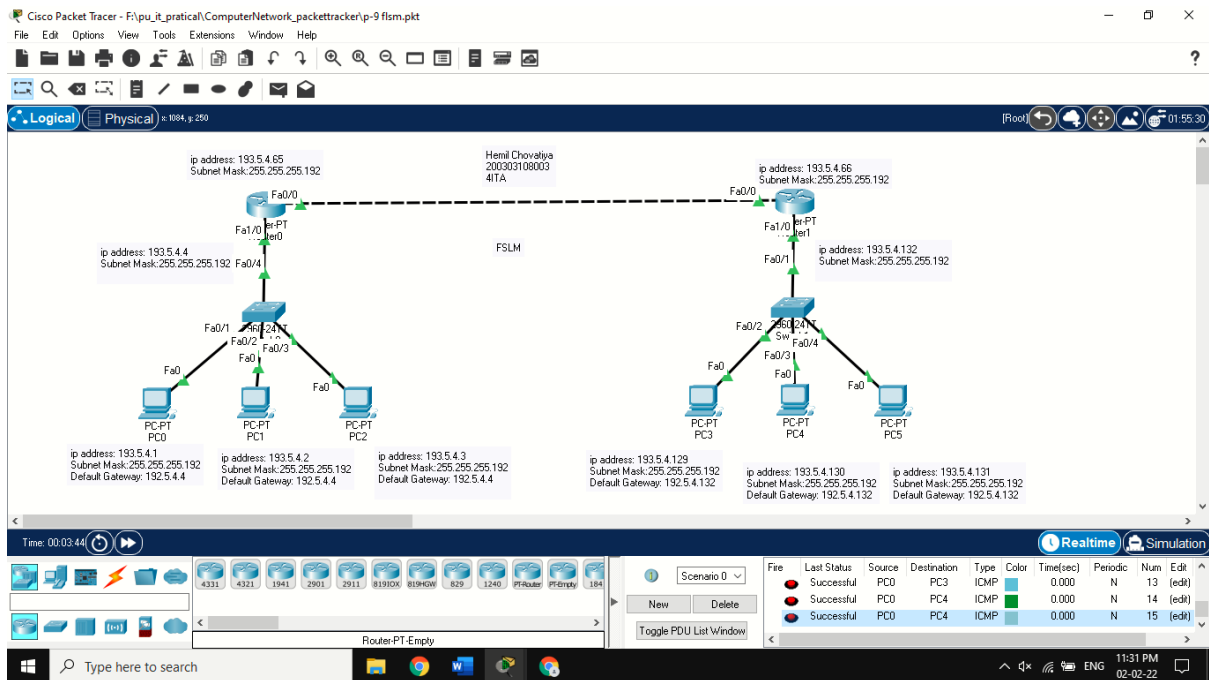


The image shows two screenshots of Cisco Packet Tracer router configuration windows. The left window is for Router0, and the right window is for Router1. Both windows show the 'Config' tab with the 'Static' section selected. In Router0, the 'Static Routes' section is configured with Network 193.5.4.128, Mask 255.255.255.192, and Next Hop 193.5.4.66. In Router1, the 'Static Routes' section is configured with Network 193.5.4.0, Mask 255.255.255.192, and Next Hop 193.5.4.65. Both windows also show the 'Equivalent IOS Commands' section with the following commands:

```

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#ip route 193.5.4.128 255.255.255.192 193.5.4.66
Router(config)#ip route 193.5.4.128 255.255.255.192 193.5.4.66
  
```

Step 11: Send the packet between different subnetting.



PRACTICAL:9

AIM: Routing at Network Layer.

Theory:

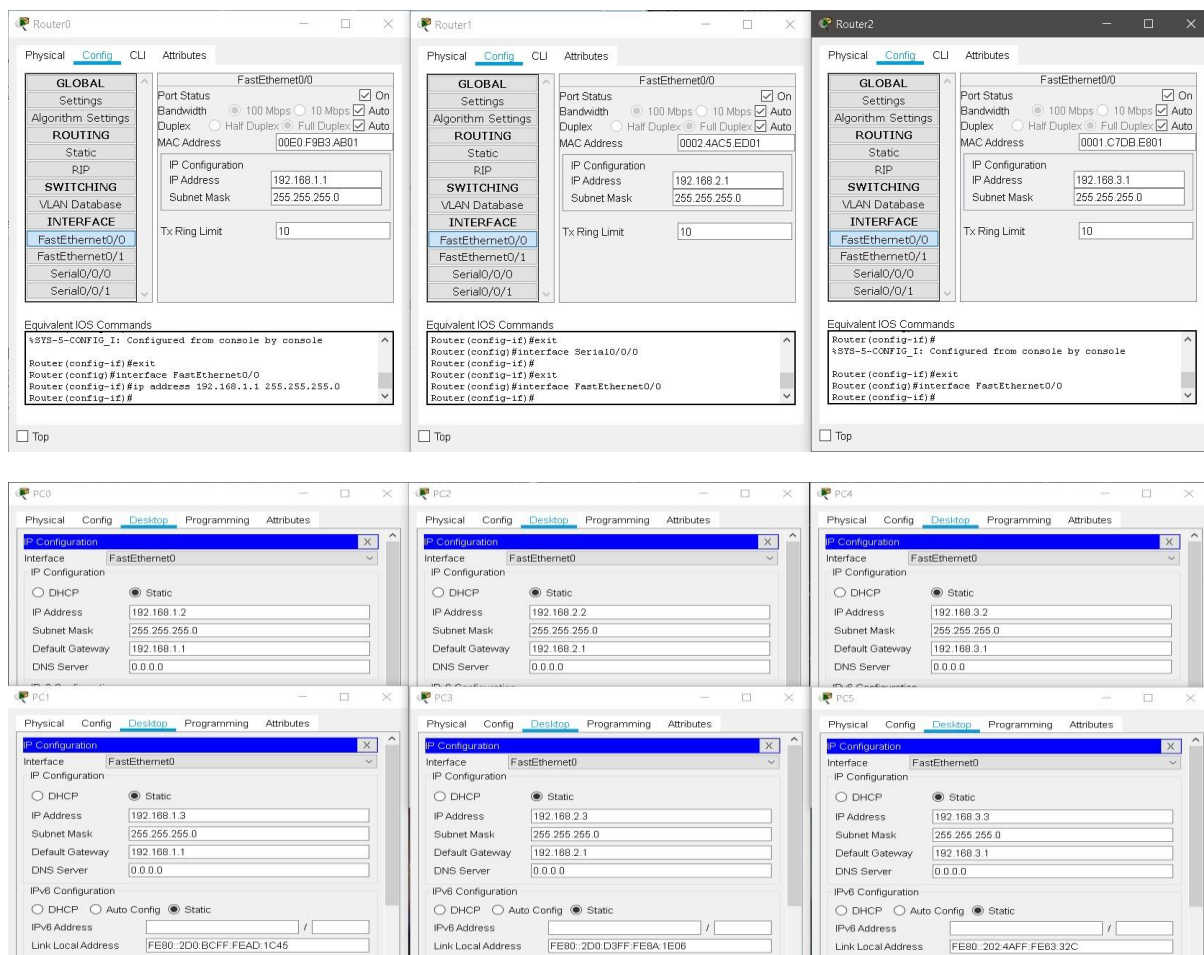
DYNAMIC ROUTING:

Step 1: Take 6 pc and 3 switch.

Step 2: Grouping the 2 pc with 1 switch connecting with copper straight-through wire.

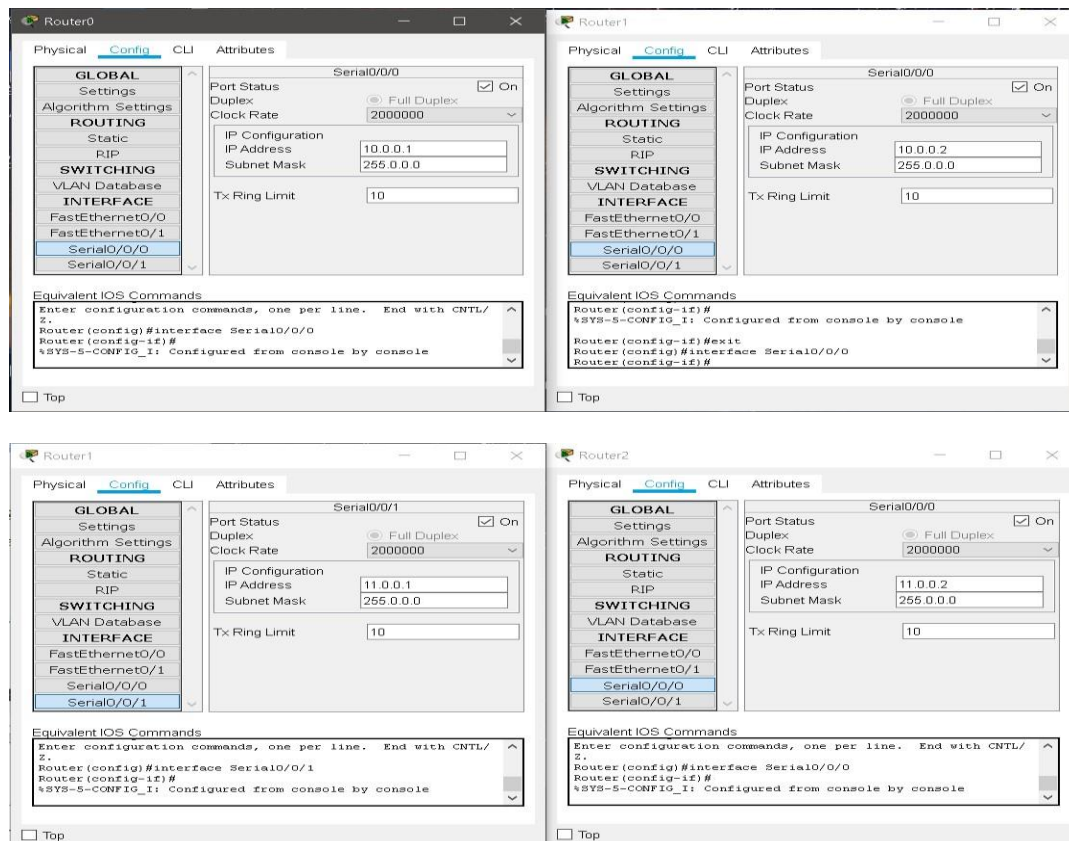
Step 3: Take 3 router and each router connect the each switch with copper straight-through wire.

Step 4: Assign ip address to router and that ip address that's pc in assign default gateway and different the ip address.



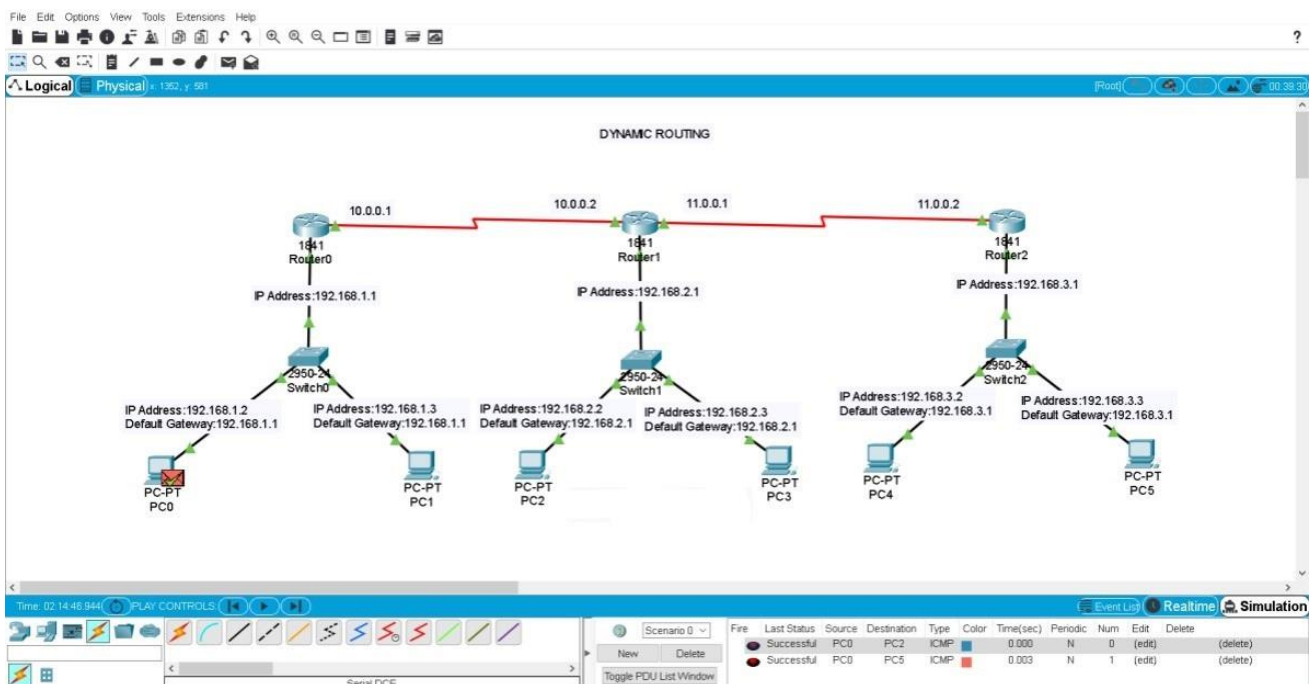
Step 5: Each routers connected with Serial DTE cable.

Step 6: Each router physical portion in change the port to WIC-2T and port status is on and serial section in assign the ip address.



Step 7: Each router in RIP section in add the network address.

Step 8: send the packet in one grouping pc to different grouping pc.



PRACTICAL:2

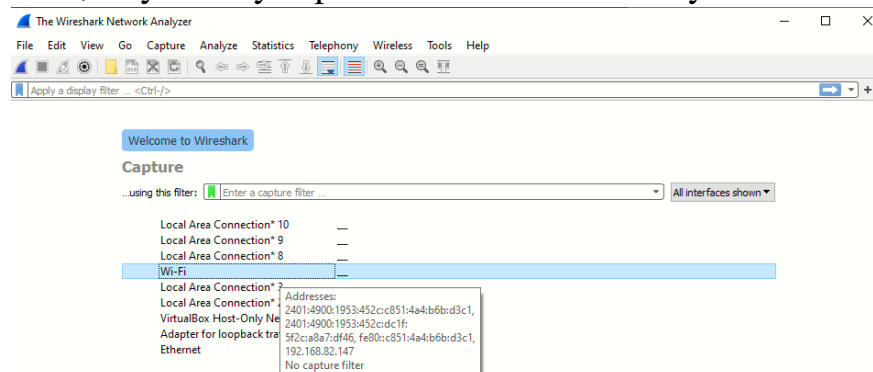
AIM: Experiments of Packet capture tool: Wireshark.

Theory:

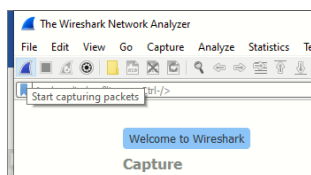
Wireshark: Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more.

Capturing Data Packets on Wireshark:

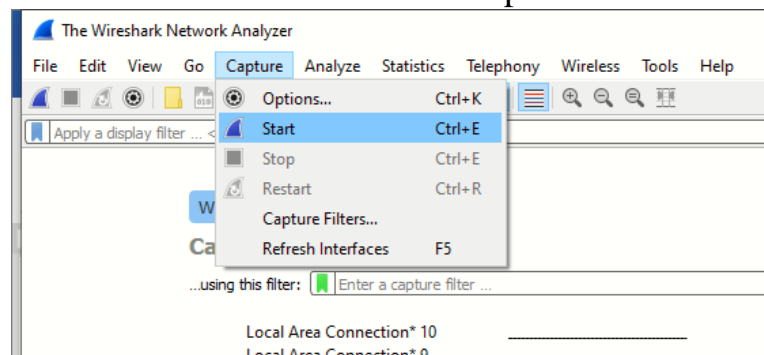
- When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.



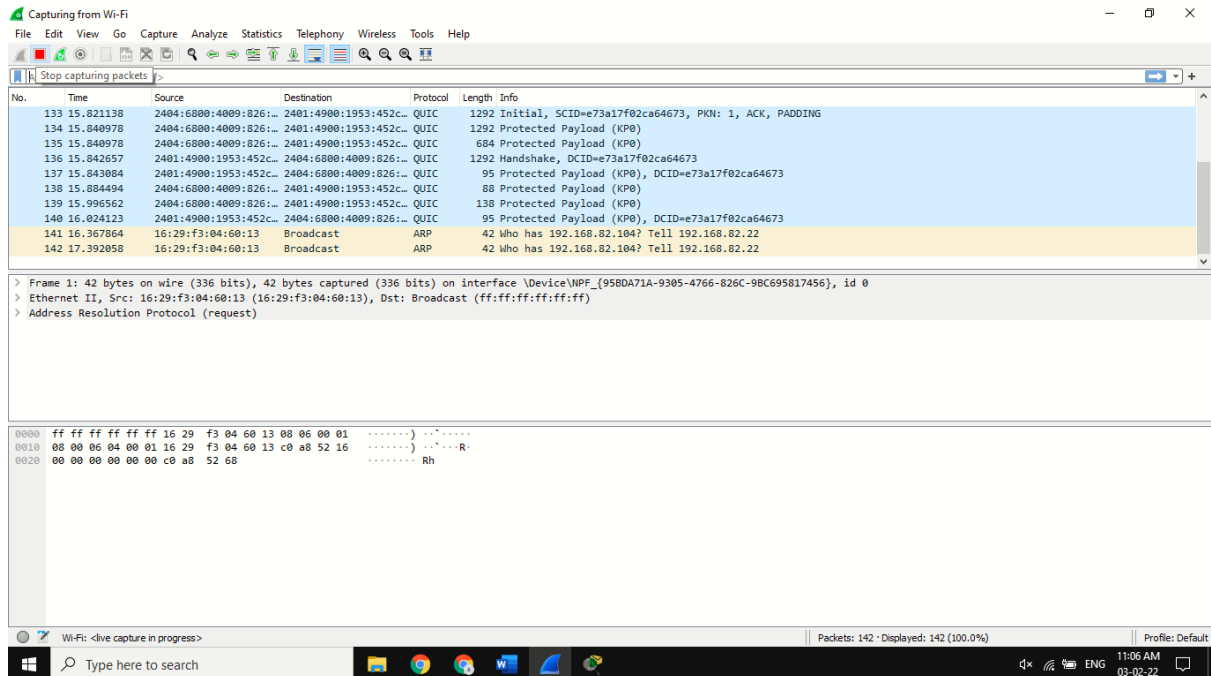
- You can select one or more of the network interfaces using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.
- Click the first button on the toolbar, titled “Start Capturing Packets.”



- You can select the menu item Capture -> Start.



- Or you could use the keystroke Control – E.
- During the capture, Wireshark will show you the packets that it captures in real-time.



- Once you have captured all the packets you need, you use the same buttons or menu options to stop the capture.
- Best practice says that you should stop Wireshark packet capture before you do analysis.

Why do we need Wireshark?

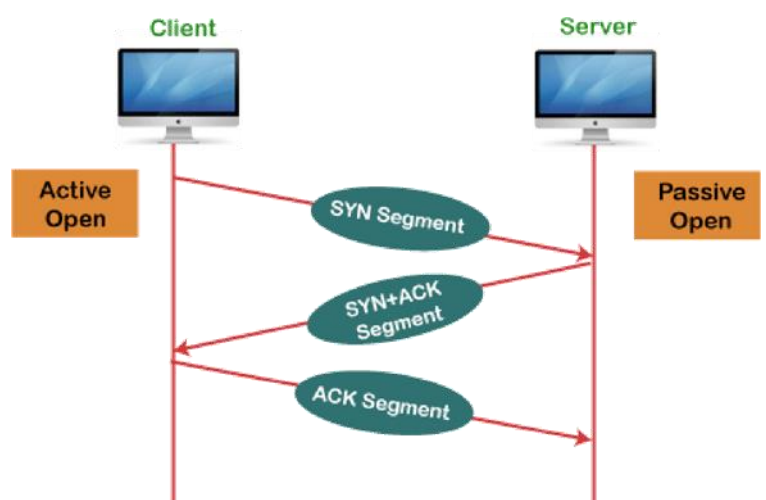
- Network administrators use it to troubleshoot network problem.
- Network security engineers use it to examine security problems.
- QA engineers use it to verify network applications.
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals.

PRACTICAL:10

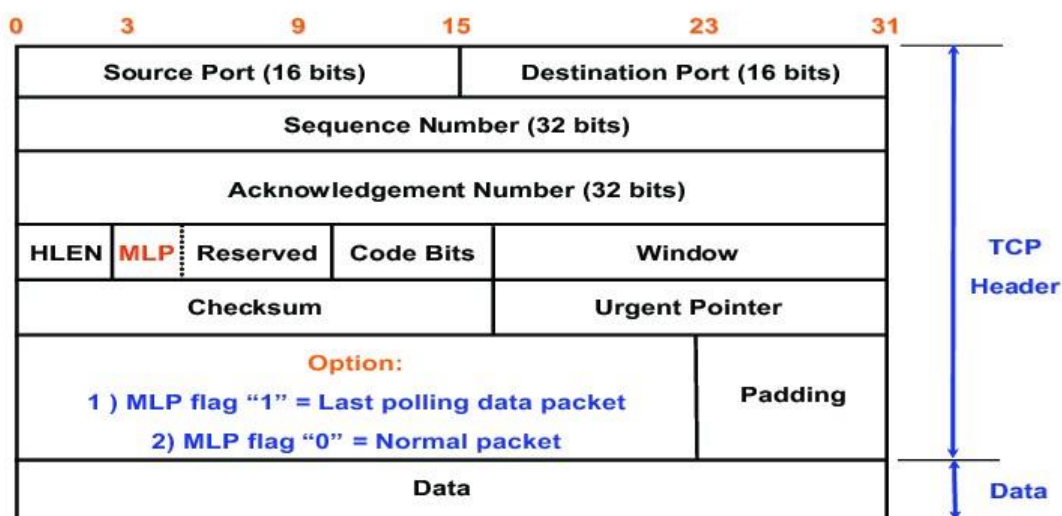
AIM: Experiment on Transport Layer.

TCP :- TCP stands for Transmission Control Protocol. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP

Working of TCP :- In TCP, the connection is established by using three-way handshaking. The client sends the segment with its sequence number. The server, in return, sends its segment with its own sequence number as well as the acknowledgement sequence, which is one more than the client sequence number. When the client receives the acknowledgment of its segment, then it sends the acknowledgment to the server. In this way, the connection is established between the client and the server.



TCP Header Format :-



UDP :- User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is apart of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

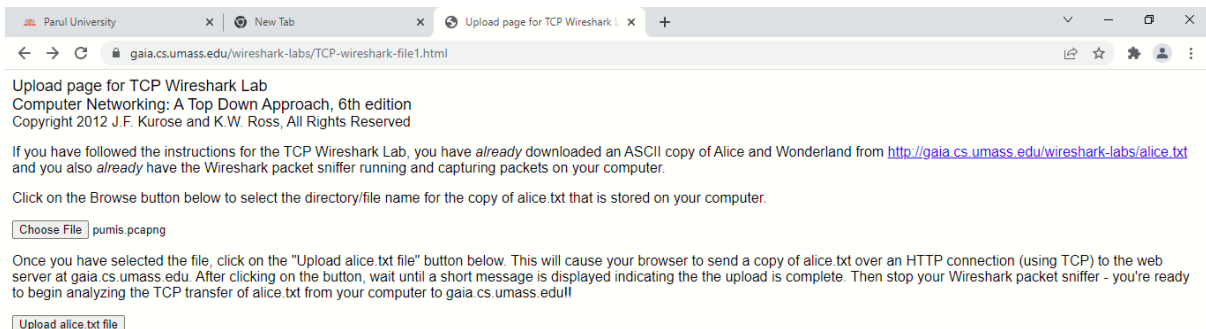
UDP Header Format :-

Source Port	Destination Port
Length	UDP Checksum
UDP data	

Analyse TCP, UDP packets using Wireshark

Step1: Run Wireshark application and start capturing packets by clicking capture, To create a traffic(Flow of incoming and outgoing packets) you can start browsing and try to do some upload/ download data or you can do the following for simple analysis of packets

- Go the <http://gaia.cs.umass.edu/wiresharklabs/alice.txt> and retrieve an ASCII copy of Alice in Wonderland. Store this file somewhere on your computer.



Parul University x New Tab x Upload page for TCP Wireshark L x +

gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html

Upload page for TCP Wireshark Lab
Computer Networking: A Top Down Approach, 6th edition
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

Choose File pumis.pcapng

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to gaia.cs.umass.edu!!

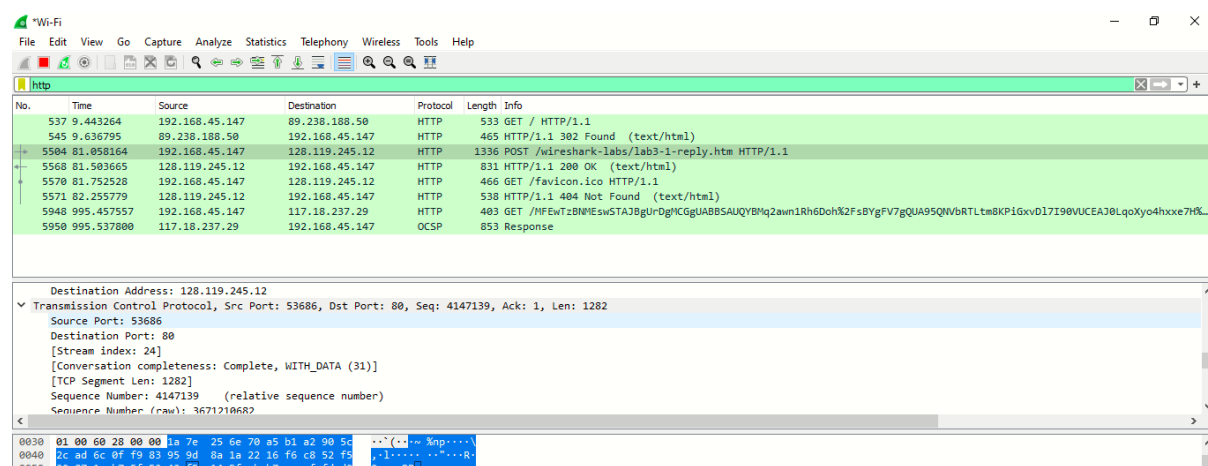
Upload alice.txt file

- Next go to <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>. And upload the saved file.
- Stop Capturing packets.

Step2: Filter TCP packets and Start Analysing TCP packets and answer following questions.

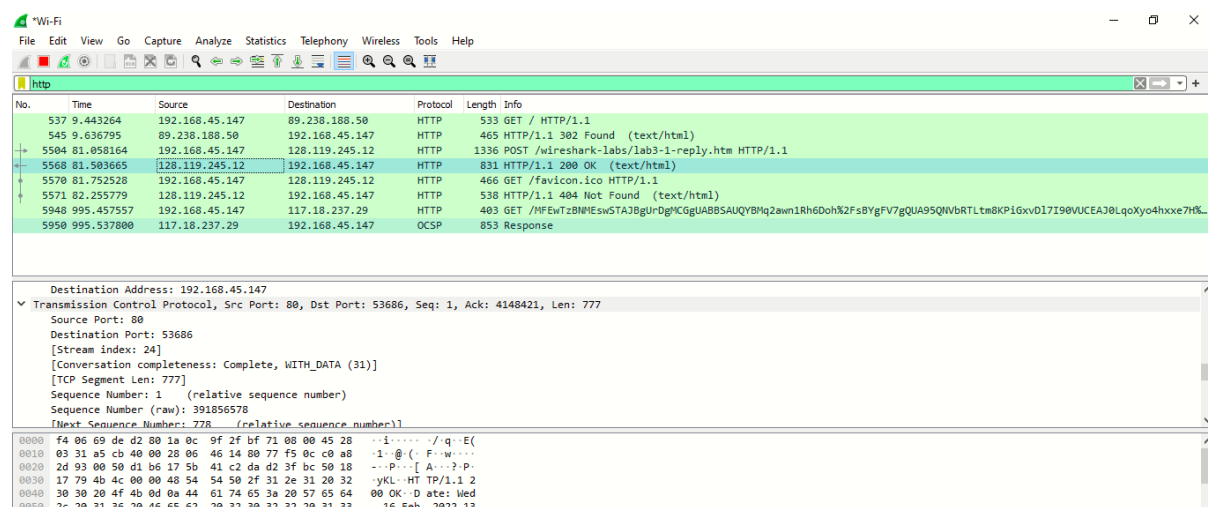
1.What is the IP address and TCP port number used by your client computer(source) to transfer the file to gaia.cs.umass.edu?

Ans :- IP address = 192.168.45.147, port number = 53686.

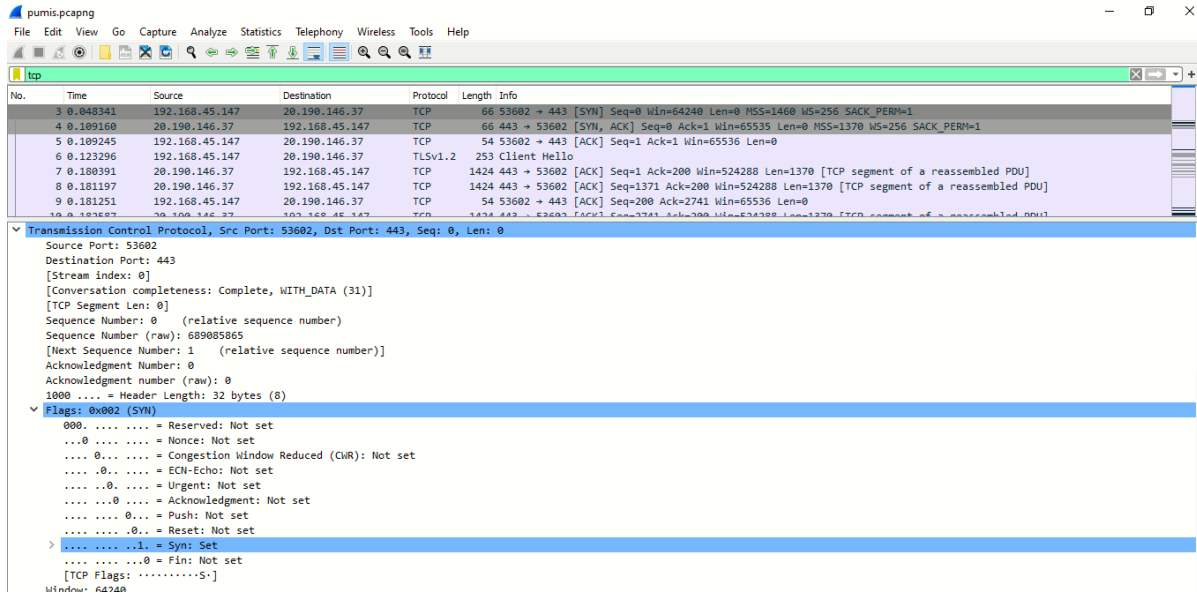


2.What is the IP address and port number used by gaia.cs.umass.edu to receive the file?

Ans :- IP address = 128.119.245.12, port number = 80.



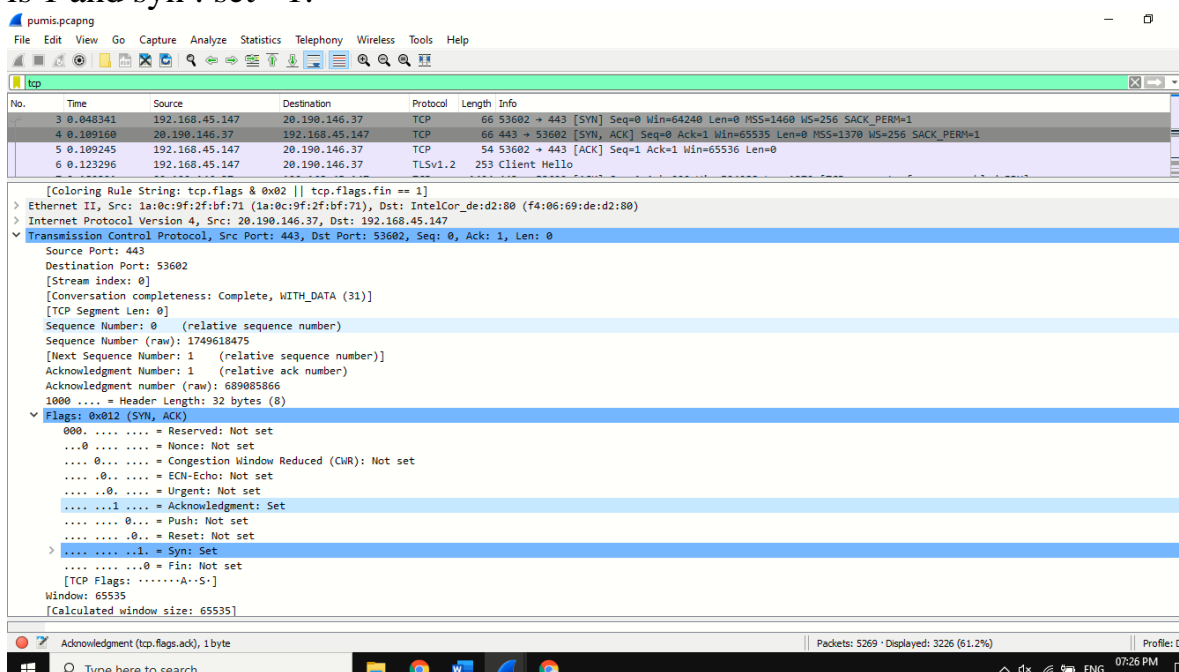
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?



Ans :- sequence number = 0, According to above figure, in the Flags section, the Syn flag is set to 1 which indicates that this segment is a SYN segment.

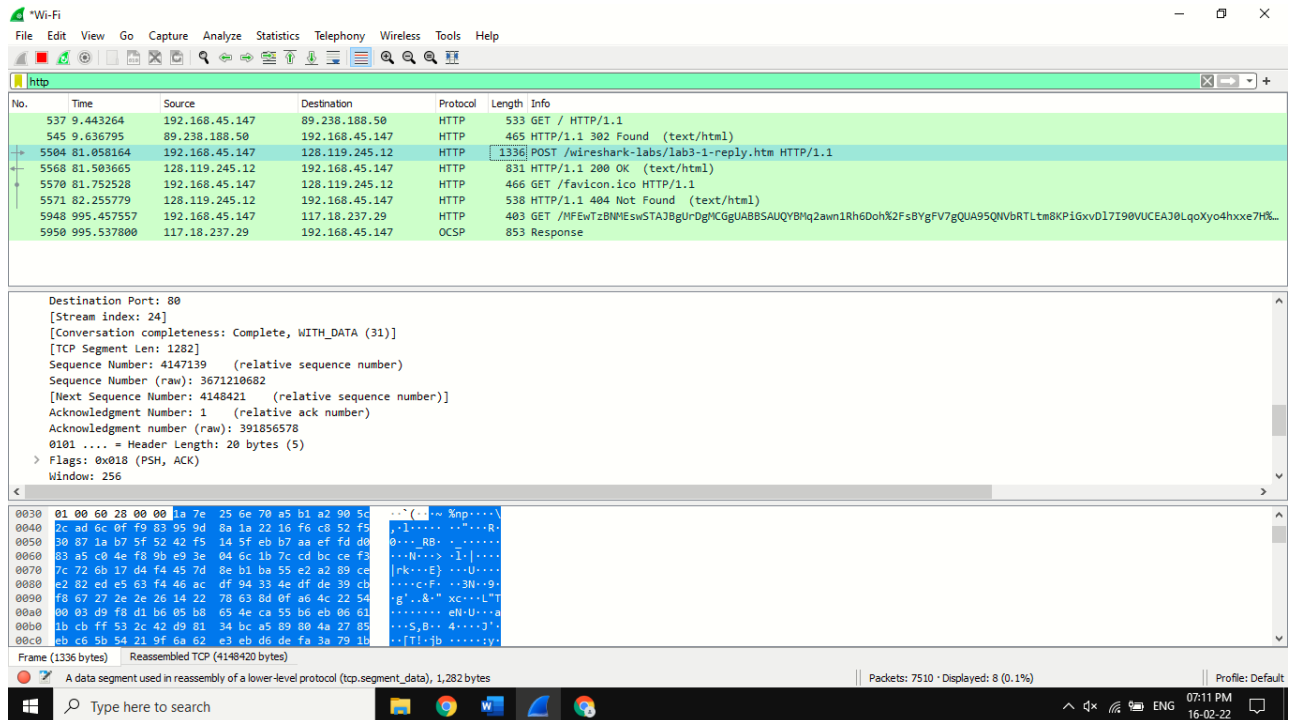
4. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Ans :- sequence number = 0, value in ACKnowledgement: set field in (SYN, ACK) is 1 and syn : set= 1.



5. What is the sequence number of the TCP segment containing the HTTP POST command?

Ans:-4147139



The screenshot shows the Wireshark Network Analyzer interface. The top pane displays a list of network packets. The middle pane shows the details of the selected packet (No. 1336), which is an HTTP POST request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
537	9.443264	192.168.45.147	89.238.188.50	HTTP	533	GET / HTTP/1.1
545	9.636795	89.238.188.50	192.168.45.147	HTTP	465	HTTP/1.1 302 Found (text/html)
5504	81.058164	192.168.45.147	128.119.245.12	HTTP	1336	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
5568	81.503665	128.119.245.12	192.168.45.147	HTTP	831	HTTP/1.1 200 OK (text/html)
5570	81.752528	192.168.45.147	128.119.245.12	HTTP	466	GET /favicon.ico HTTP/1.1
5571	82.255779	128.119.245.12	192.168.45.147	HTTP	538	HTTP/1.1 404 Not Found (text/html)
5948	995.457557	192.168.45.147	117.18.237.29	HTTP	403	GET /MFEWtzBNMEswSTA38gUrDgKCGuABBSAUQYBMq2awn1Rh6Doh%2Fs8YgFV7gQUA95QNVbRTLtm8KP1GxvD17I98VUCEA70LqoXyo4hxce7H%...
5950	995.537800	117.18.237.29	192.168.45.147	OCSP	853	Response

Destination Port: 80
[Stream index: 24]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1282]
Sequence Number: 4147139 (relative sequence number)
Sequence Number (raw): 3671210682
[Next Sequence Number: 4148421 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 391856578
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 256

Frame 1336 (bytes) | Reassembled TCP (4148420 bytes)

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1,282 bytes

Packets: 7510 · Displayed: 8 (0.1%) | Profile: Default

07:11 PM
16-02-22