

COMPUTER NETWORKS

LAB MANUAL

CERTIFICATE

*This is to certify that Mr./Ms.**SHUBHAM NAVGHARE**.....*
*with enrolment no.**200303108740**..... has successfully completed his/her*
*laboratory experiments in the **COMPUTER NETWORKS (20310525255)** from the*
*department of**Information Technology**..... during the academic*
*year**2020-2021**.....*



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 leasible 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 bax, 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 le Router, Switch and PC on the man 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:

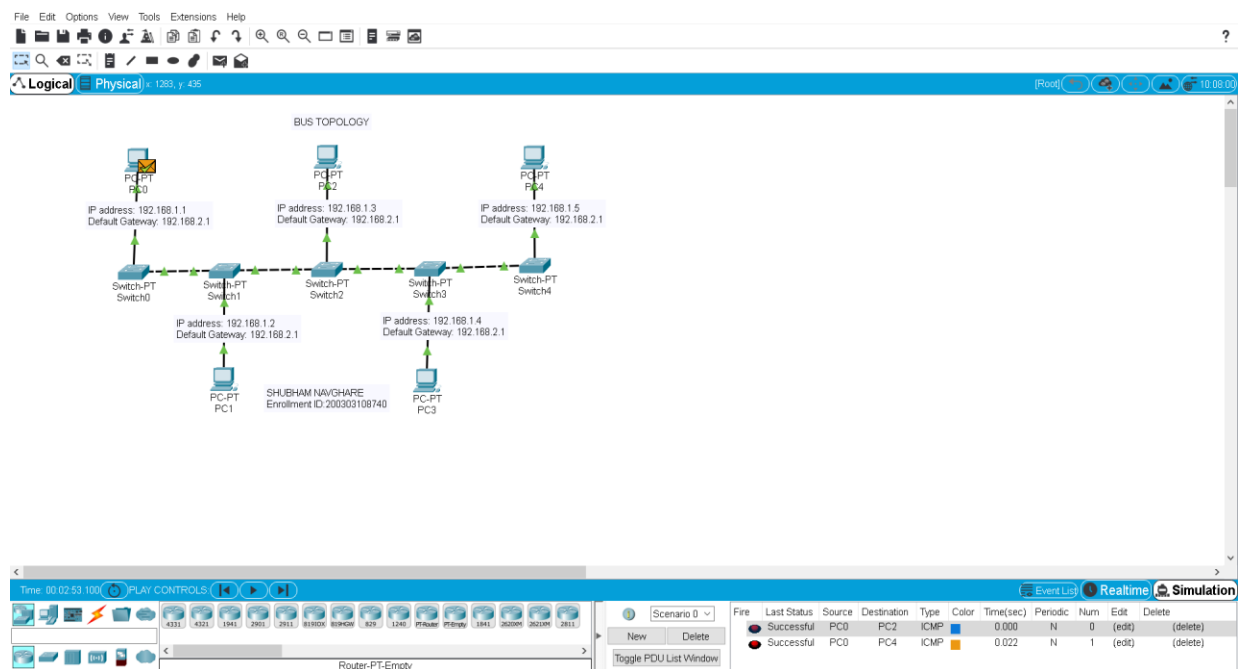
Step 1: Take 5 switches.

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:

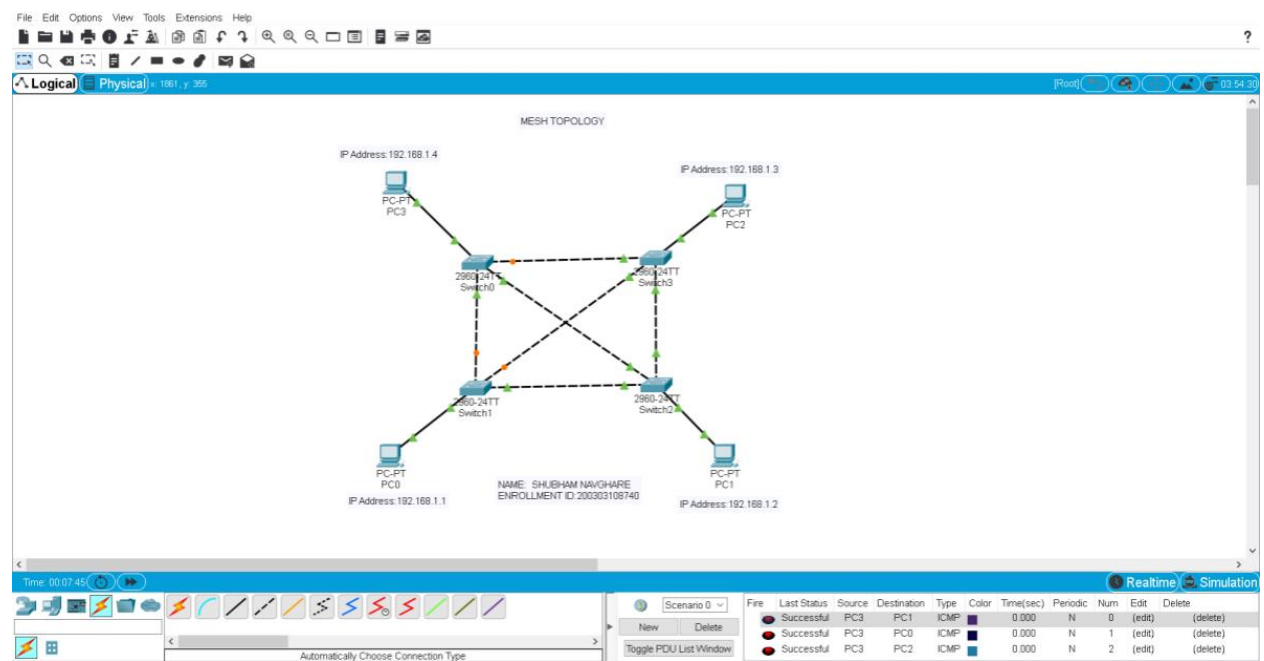
Procedure

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

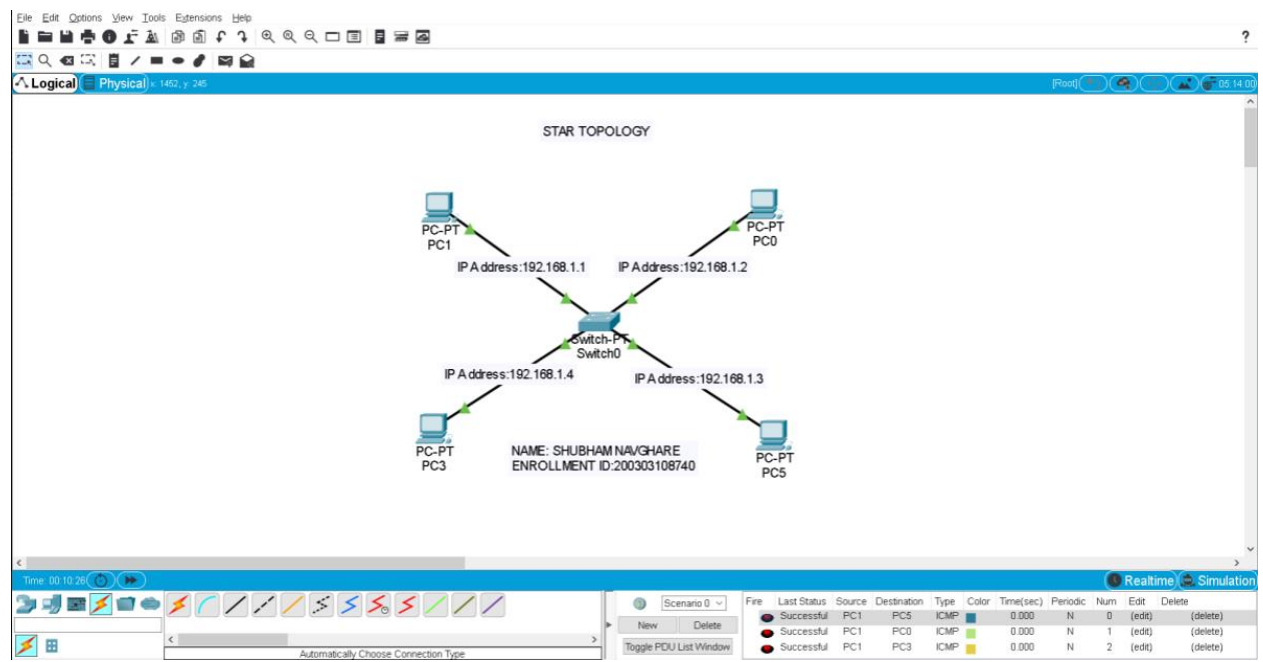
Procedure

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

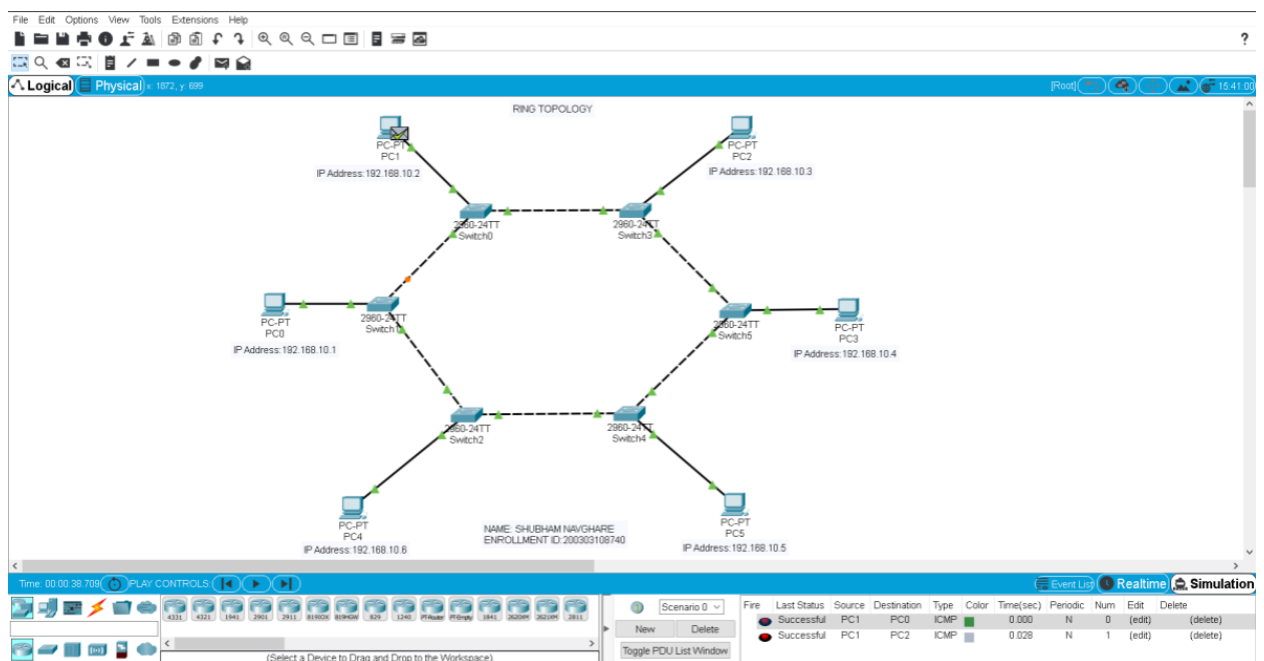
Procedure

Step 1: Take 6 switches and 6 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

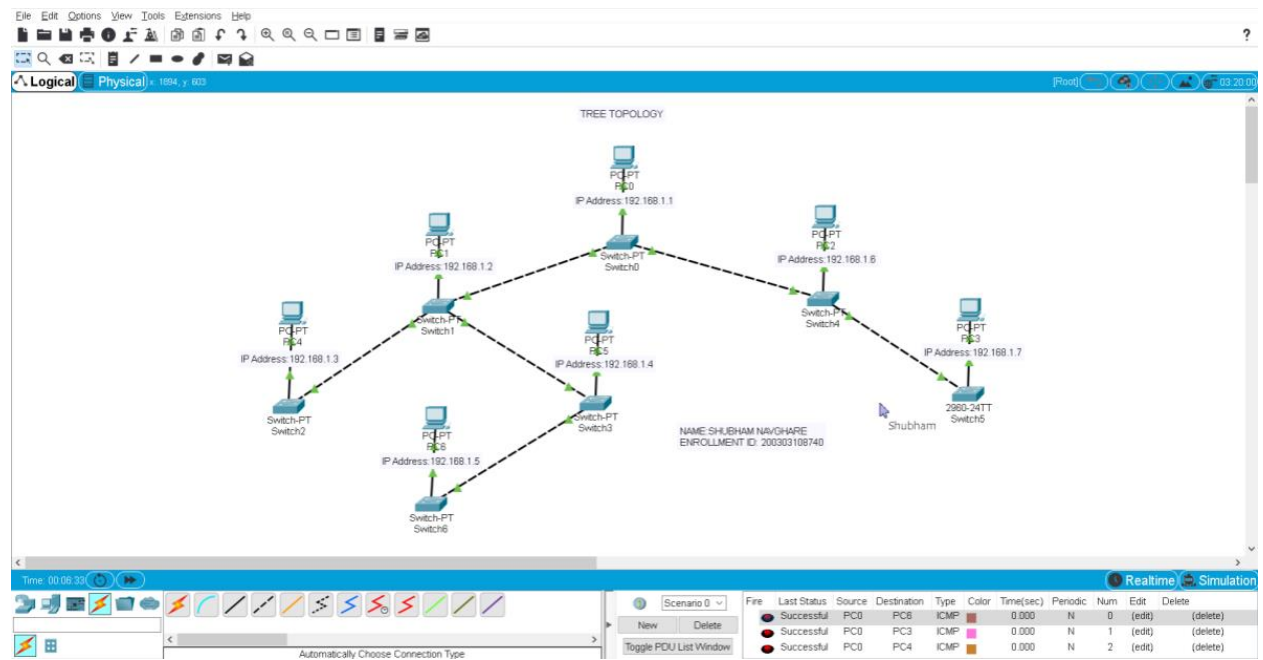
Procedure

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.

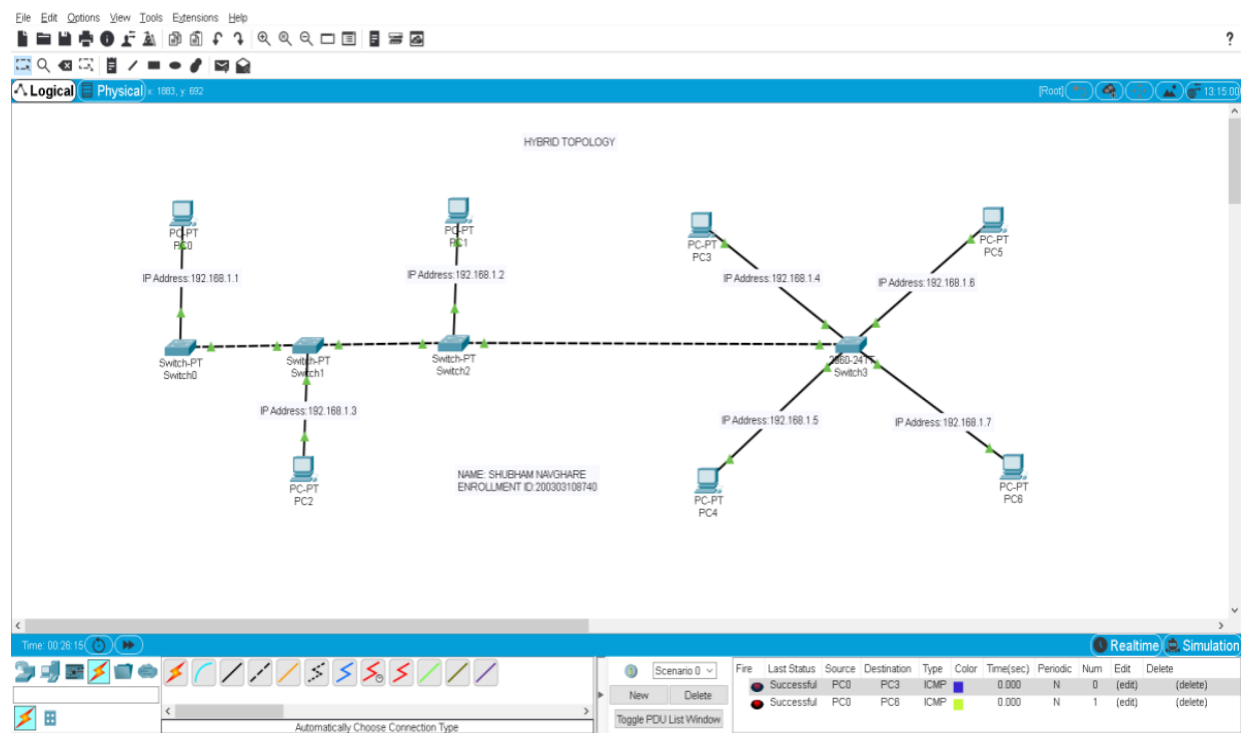
- For star topology

Step 1: Take 1 switches and 4 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

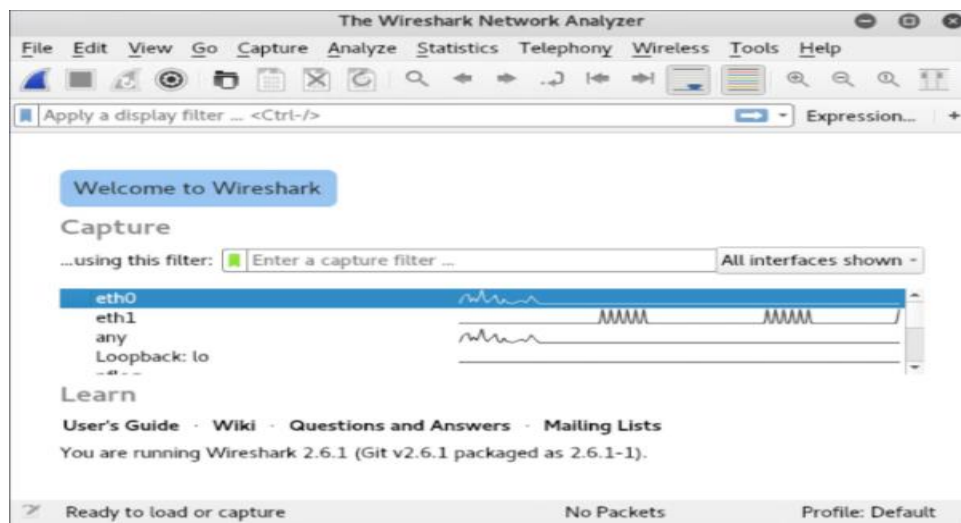
AIM: Experiments of Packet capture tool: Wireshark.

Wireshark:

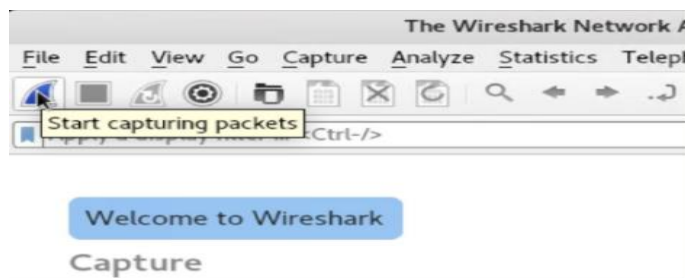
Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more.

Capturing Data Packets on Wireshark:

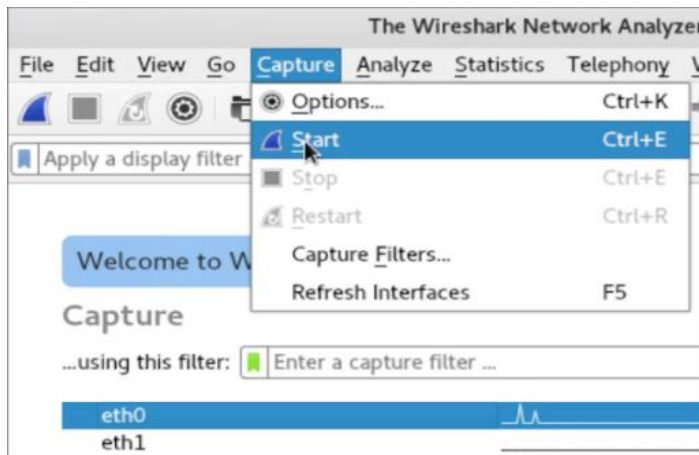
- When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.



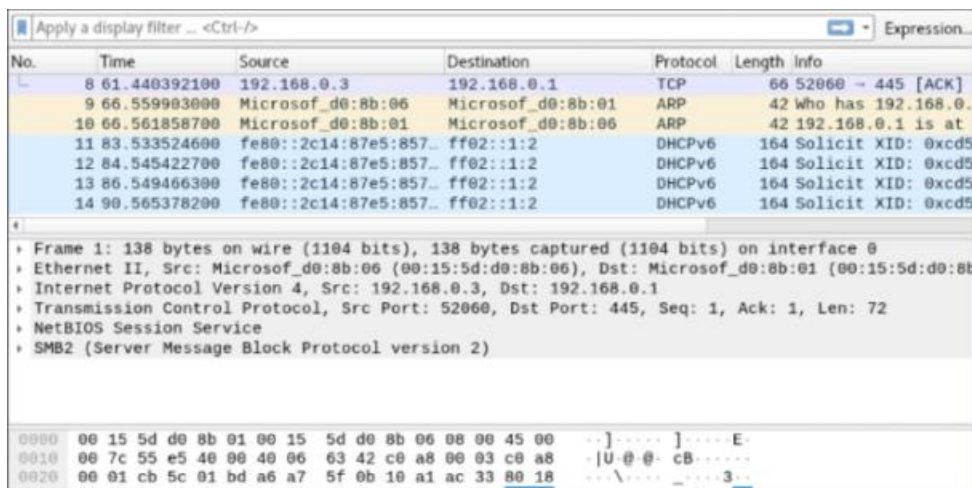
- You can select one or more of the network interfaces using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.
- Click the first button on the toolbar, titled “Start Capturing Packets.”



- 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: 3

AIM: To study behavior of generic devices used for networking: (CISCO PACKET TRACER)

1. 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 used to connect for more than two devices

2. Hub:

An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

3. Switch:

A network switch or switching hub is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

4. 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 analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

5. Router:

A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

6. 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.

PRACTICAL: 4

AIM: Data Link Layer (Error Correction)

➤ C PROGRAM FOR CRC(ERROR DETECTION)

INPUT:

```
#include <stdio.h>
#include <conio.h>
void main()
{
    int i,f[20],n[50],div[50],j,t,quo[20],z[10];
    printf("NAME: SHUBHAM NAVGHARE\n");
    printf("ENROLLMENT ID:200303108740\n");
    printf("Entre the number\n");
    for(i=0;i<8;i++)
    {
        scanf("%d",&n[i]);
    }
    printf("Enter the divisor\n");
    for(i=0;i<4;i++)
    {
        scanf("%d",&div[i]);
    }
    for(i=8;i<12;i++)
    {
        n[i]=0;
    }
    for(i=0;i<8;i++)
    {
        if(n[i]==1)
        {
            for(j=0;j<4;j++)
            {
                if(n[t]==div[j])
                {
                    n[t]=0;
                    f[j]=0;
                }
            }
            else
```



```
        {
            n[t]=1;
            f[j]=1;
        }
        t=t+1;
    }
    quo[i]=1;
}
else
    quo[i]=0;
}
printf("\nthe quotient is\n");
for(i=0;i<8;i++)
    printf("%d",quo[i]);
printf("\n the remainder is\n");
for(j=0;j<4;j++)
    printf("%d",f[j]);
getch();
}
```

OUTPUT:

```
NAME: SHUBHAM NAVGHARE
ENROLLMENT ID:200303108740
Entre the number
1
1
1
1
0
0
0
0
Enter the divisor
1
1
0
1
the quotient is
10111010
the remainder is
0001
```

PRACTICAL: 5

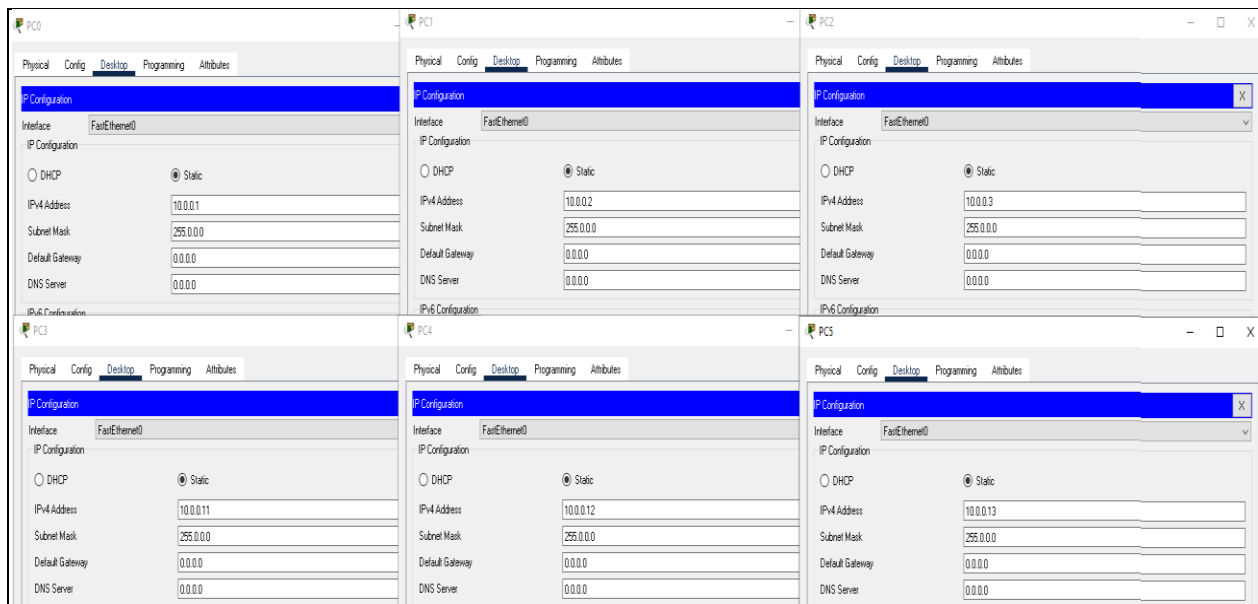
AIM: Virtual LAN

Procedure:

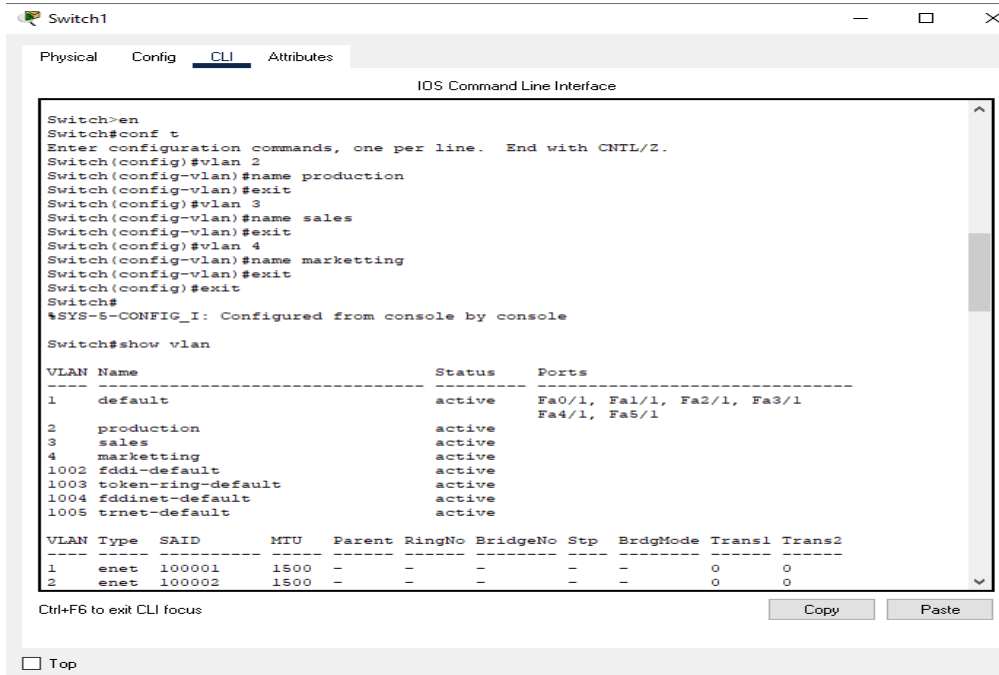
Step 1: Take 2 switches, 6 pc's.

Step 2: connect the first three pc's to switch0 with copper straight-through wire and then connect the remaining three pc's to switch 1 with copper straight-through wire.

Step 3: assign ip's to pc's accordingly pc0 (10.0.0.1), pc1 (10.0.0.2), pc2 (10.0.0.3), pc3 (10.0.0.11), pc4 (10.0.0.12), pc5 (10.0.0.13).



Step 4: now configure switch0 by assigning pc0,pc1,pc2 as vlan2,vlan3,vlan4 and naming them IT,CSE,AERO simultaneously, similarly do this with switch1 configure it by assigning pc3,pc4,pc5 as vlan2,vlan3,vlan4 and naming them IT,CSE,AERO simultaneously.



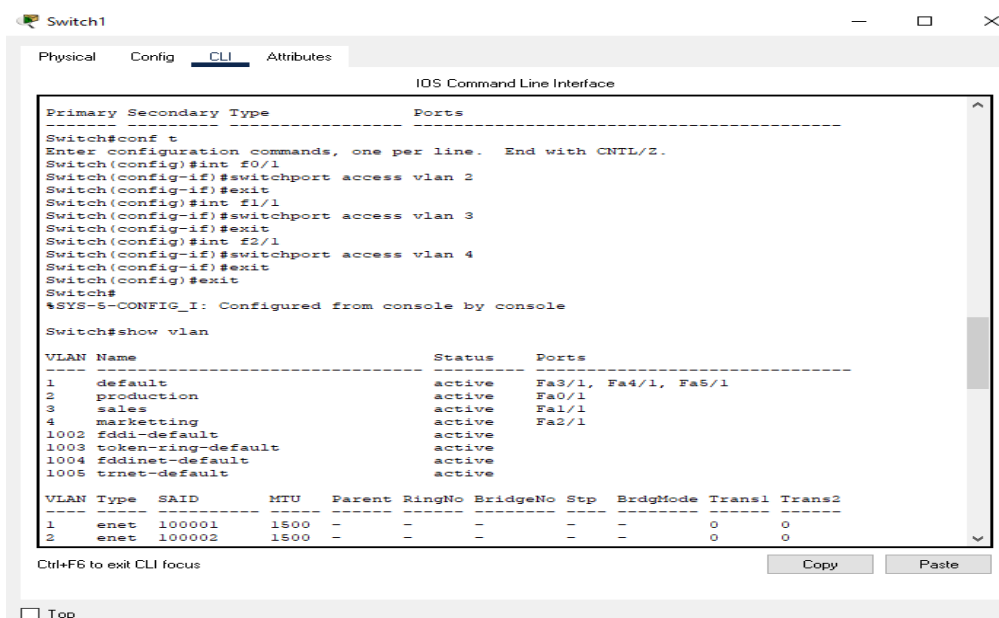
```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name production
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name marketing
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
2    production             active    Fa4/1, Fa5/1
3    sales                  active
4    marketing              active
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrgdMode Transl Trans2
-----
1    enet    100001   1500    -      -      -      -      -      0      0
2    enet    100002   1500    -      -      -      -      -      0      0
```

Step 5: then config switch0 port by giving the access and assigning them with their individual vlan connections(assign f0/1 to vlan 2...etc), similarly do this same process with switch1



```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int f1/1
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int f2/1
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console

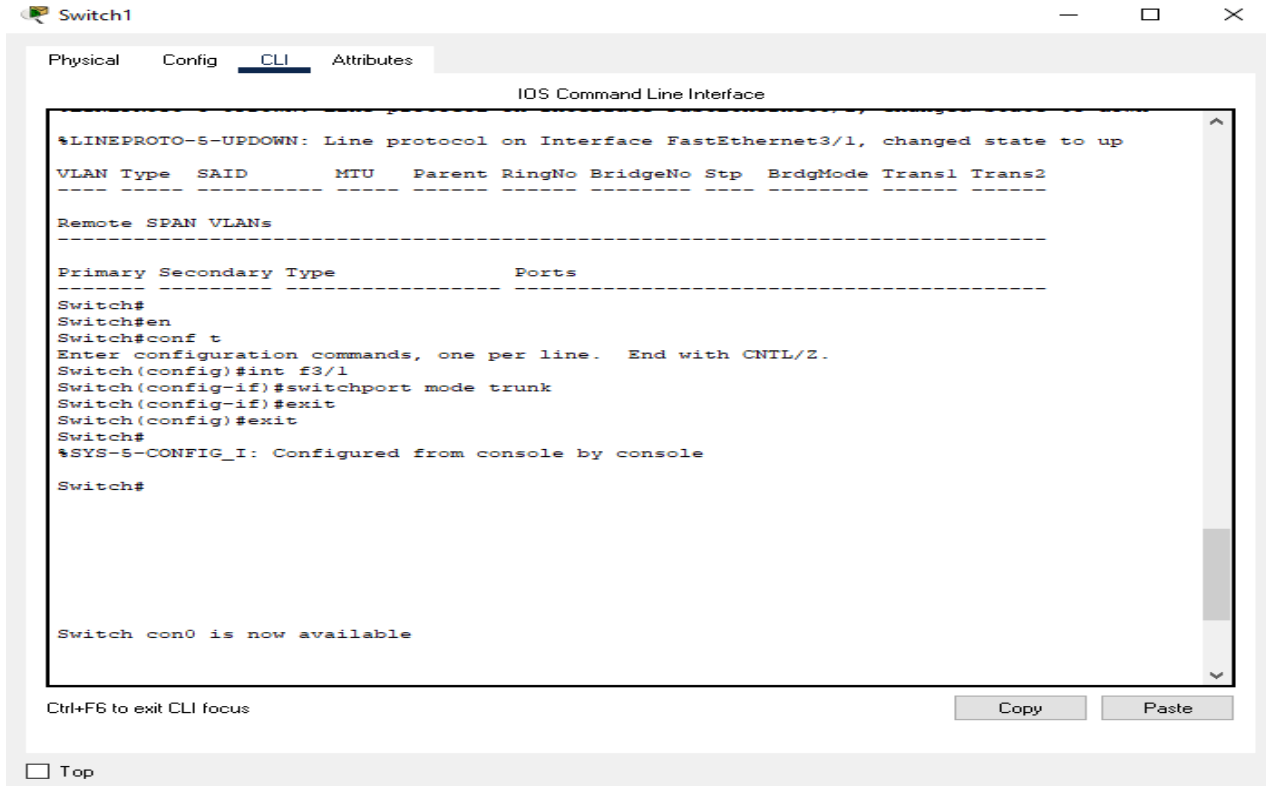
Switch#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa3/1, Fa4/1, Fa5/1
2    production             active    Fa0/1
3    sales                  active    Fa1/1
4    marketing              active    Fa2/1
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrgdMode Transl Trans2
-----
1    enet    100001   1500    -      -      -      -      -      0      0
2    enet    100002   1500    -      -      -      -      -      0      0
```

Step 6: now when all the 6 pcs have been assigned and given access to their individual switch port, now connect switch0 to switch1 using copper cross over cable make sure both the switches are connected to same ports (f3/1)

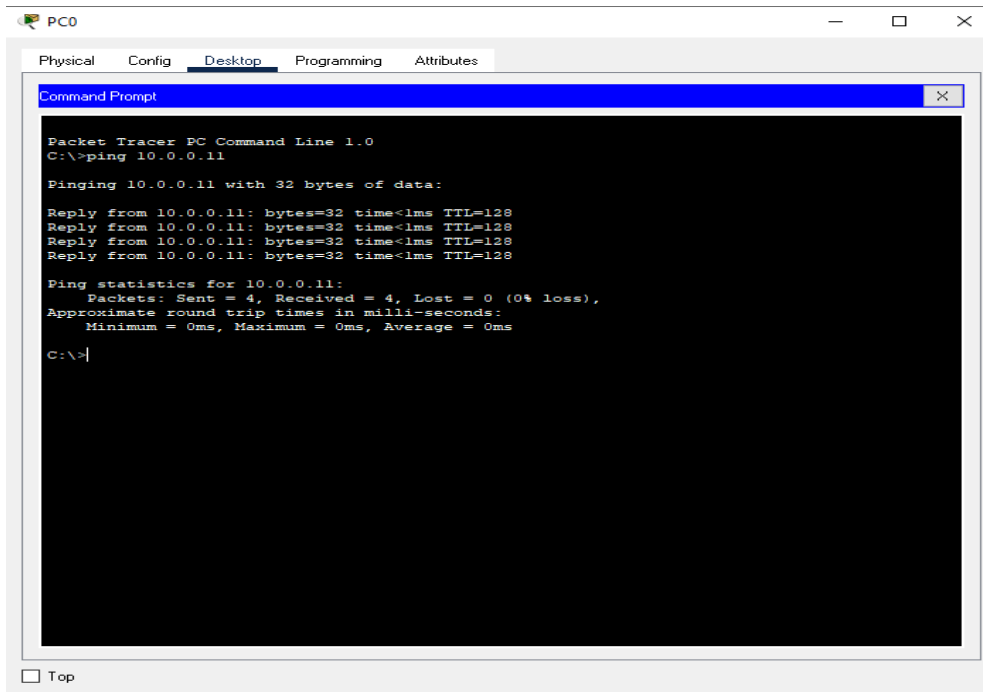
Step 7: now configure switch0 so that the same connected port(f3/0) changes it mode to trunk by using command "switchport mode trunk" when the state is changed to up follow the same instructions for switch1 by running the command.



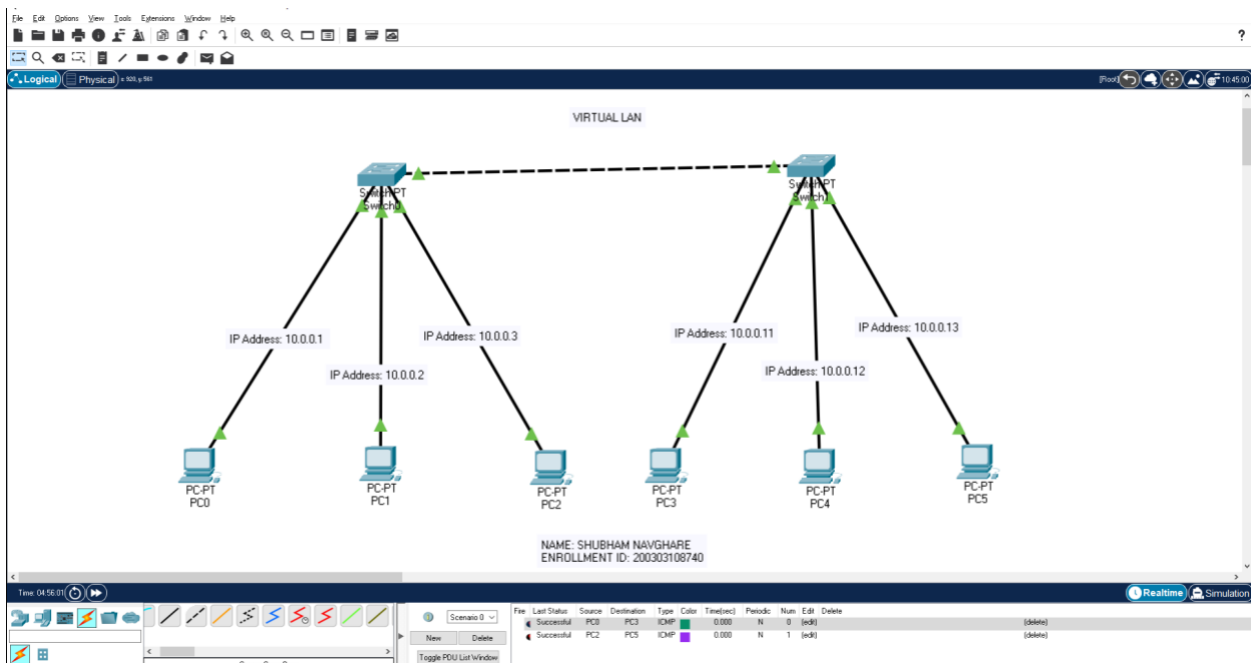
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/1, changed state to up
VLAN Type  SAID          MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
Remote SPAN VLANs
-----
Primary Secondary Type            Ports
-----
Switch#
Switch#en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f3/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#

Switch con0 is now available
```

Step 8: after this go to pc0's command prompt and ping pc3, if ping is completed you have created vlan connection



OUTPUT:



PRACTICAL: 6

AIM: Wireless LAN

Procedure:

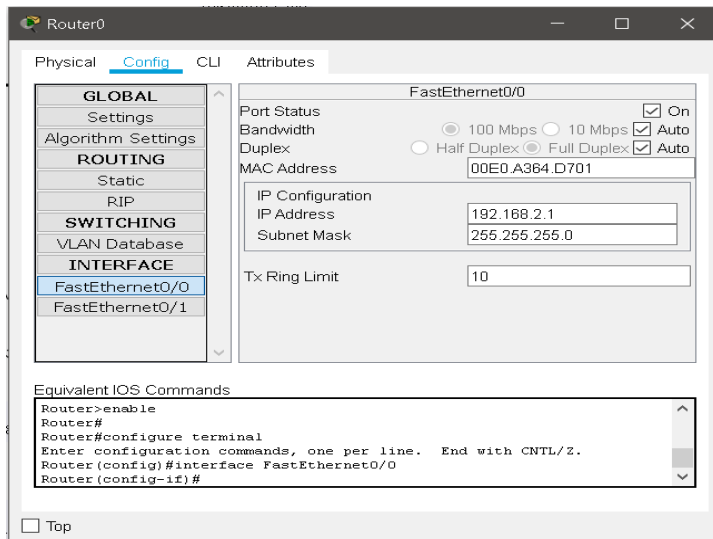
Step 1: Take 1 2950-24 switch ,1 1841 router, 1 pc.

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

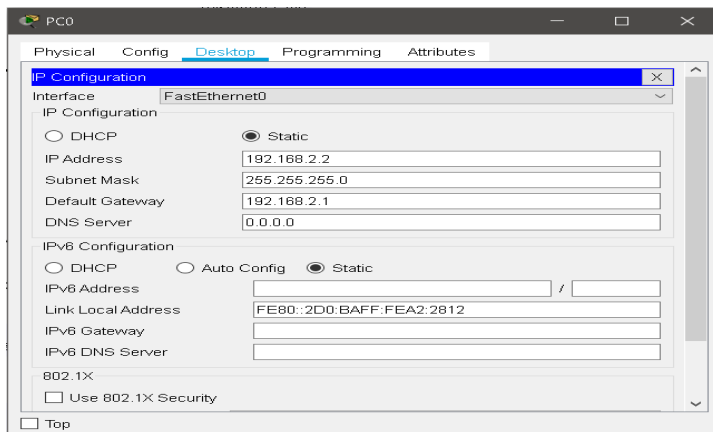
Step 3: Take 1 access point-PT and it connect with 2950-24 switch_with straight-through wire.

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

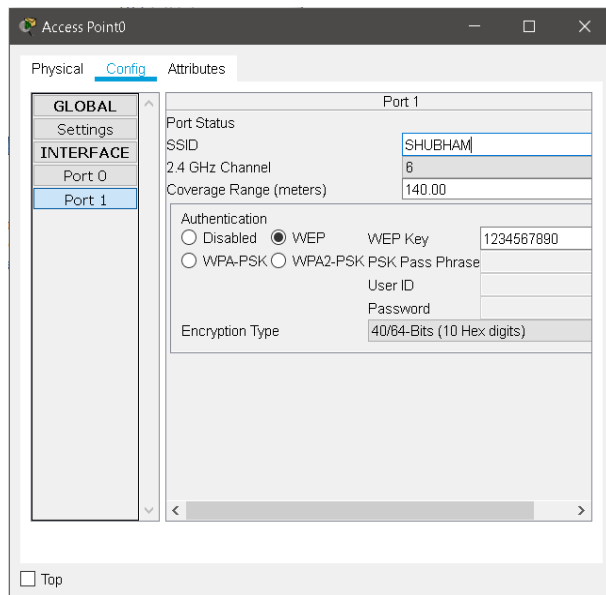
Step 5: Assign IP Address to router(192.168.2.1) and port status is on.



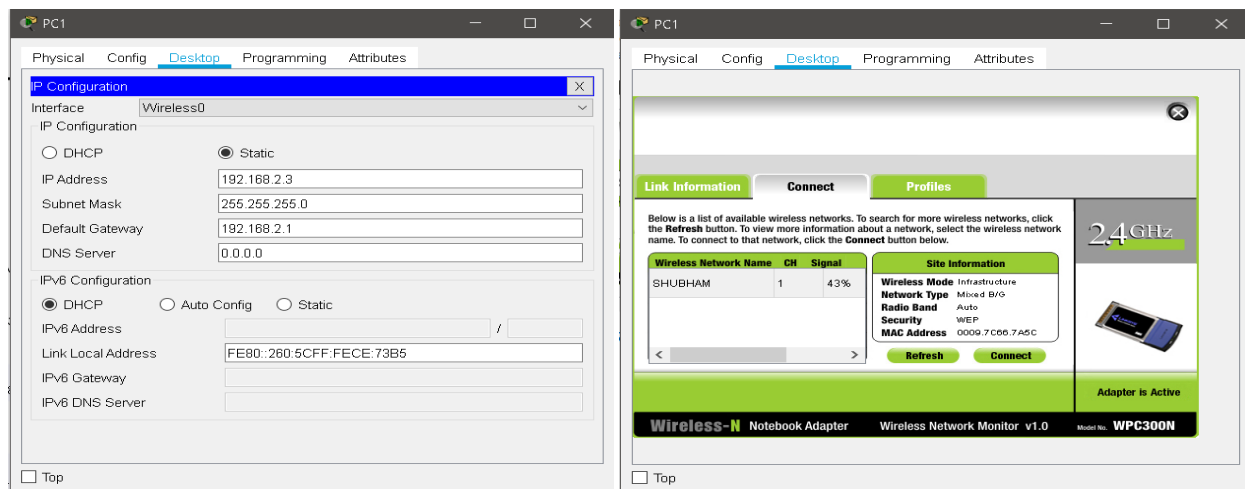
Step 6: Assign IP Address to pc(192.168.2.2) and default gateway is(192.168.2.1).



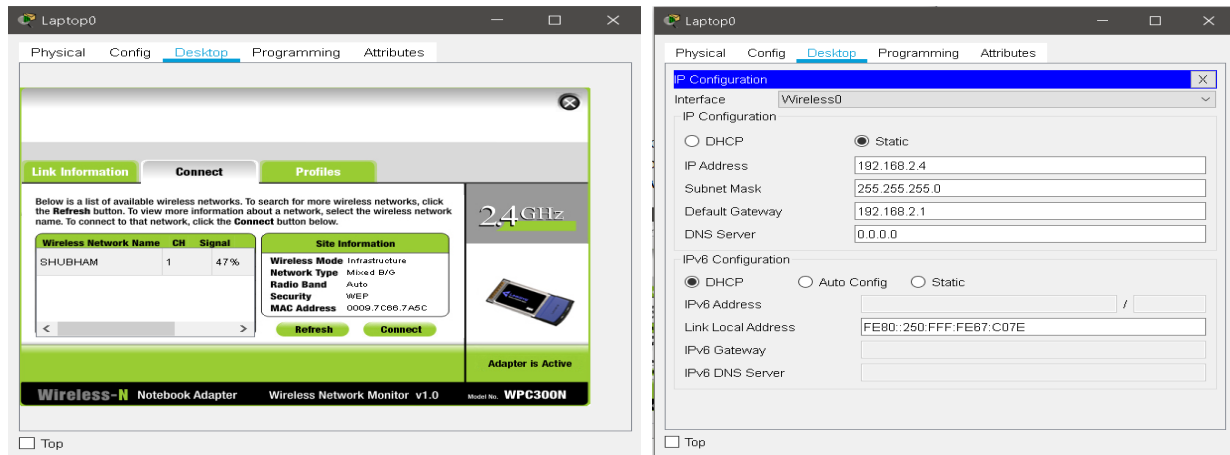
Step 7: In the access point config -> port 1 select WEP , WEP Key is (1234567890) and SSID change default to name.



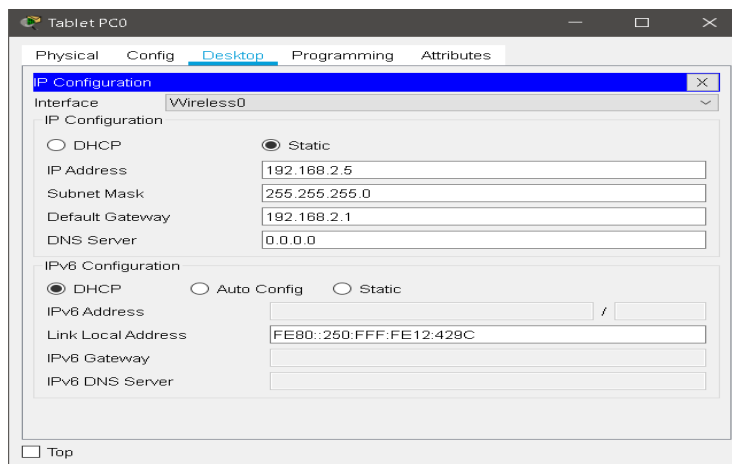
Step 8: In wireless component pc in physical section switch off and remove the port and provide WMP300N and switch on. Assign IP Address(192.168.2.3) it and also provide default gateway(192.168.2.1).In pc wireless section connect given wireless network.



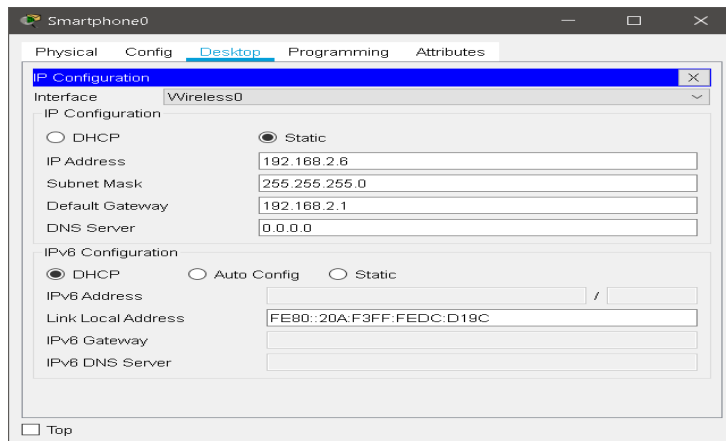
Step 9: In wireless component laptop in physical section switch off and remove the port and provide WPC300N and switch on. Assign IP Address(192.168.2.4) it and also provide default gateway(192.168.2.1).In pc wireless section connect given wireless network.



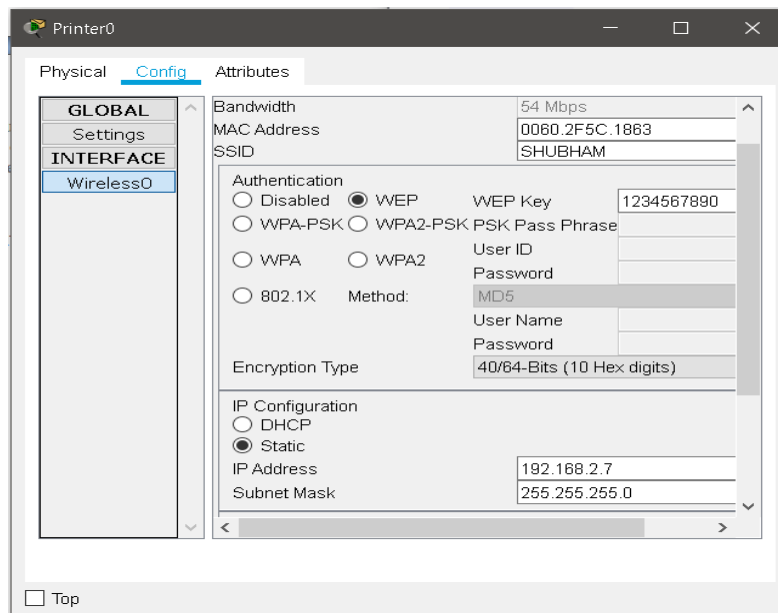
Step 10: In wireless component tablet in Assign IP Address(192.168.2.5) it and also provide default gateway(192.168.2.1).



Step 11: In wireless component Smartphone in Assign IP Address(192.168.2.6) it and also provide default gateway(192.168.2.1).

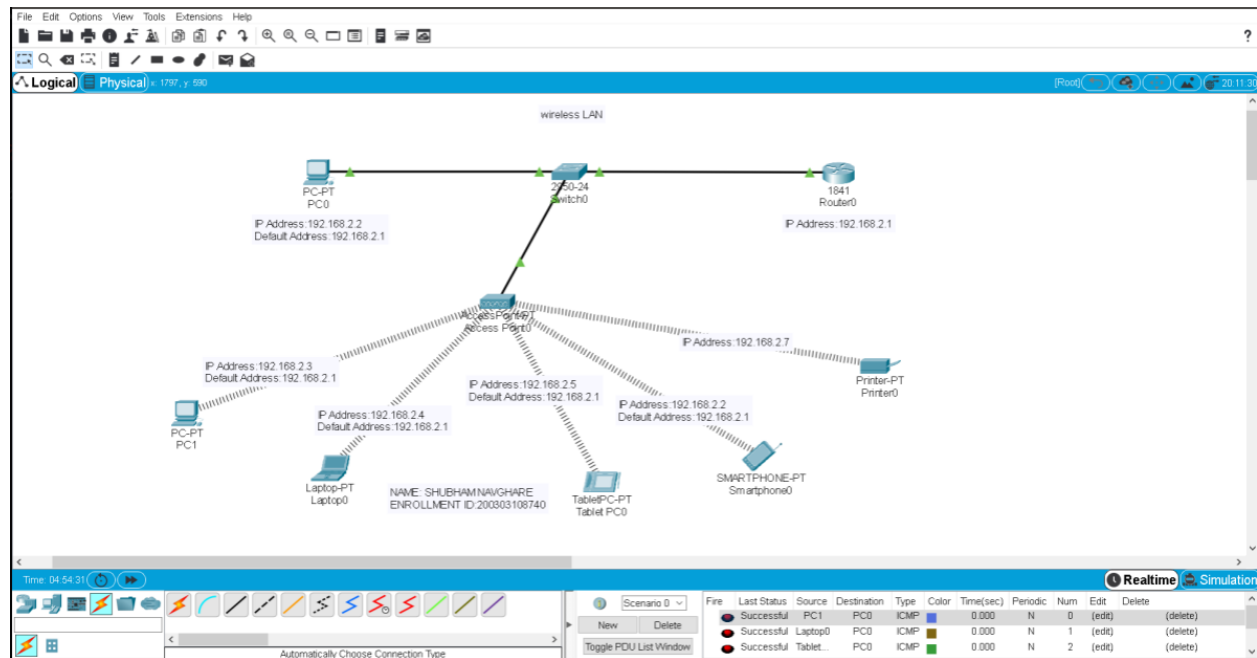


Step 12: In wireless component printer config section select WEP, write WEP Key (1234567890) and change SSID default to name. In physical section switch off and remove the port and provide WPC300N and switch on.



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

OUTPUT:



PRACTICAL:7

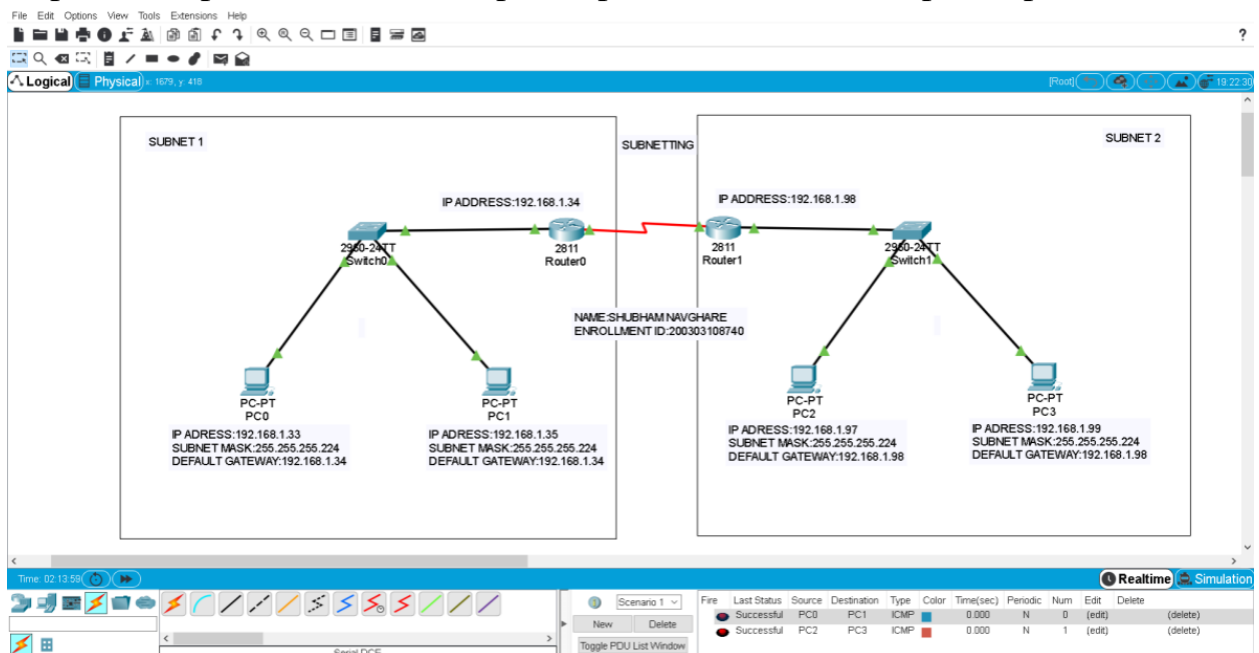
AIM: Internetworking with routers: 1: Experiment on same subnet 2:Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination.

Internetworking with routers:

1. Experiment on same subnet:

Step 1: Create 2 subnet.

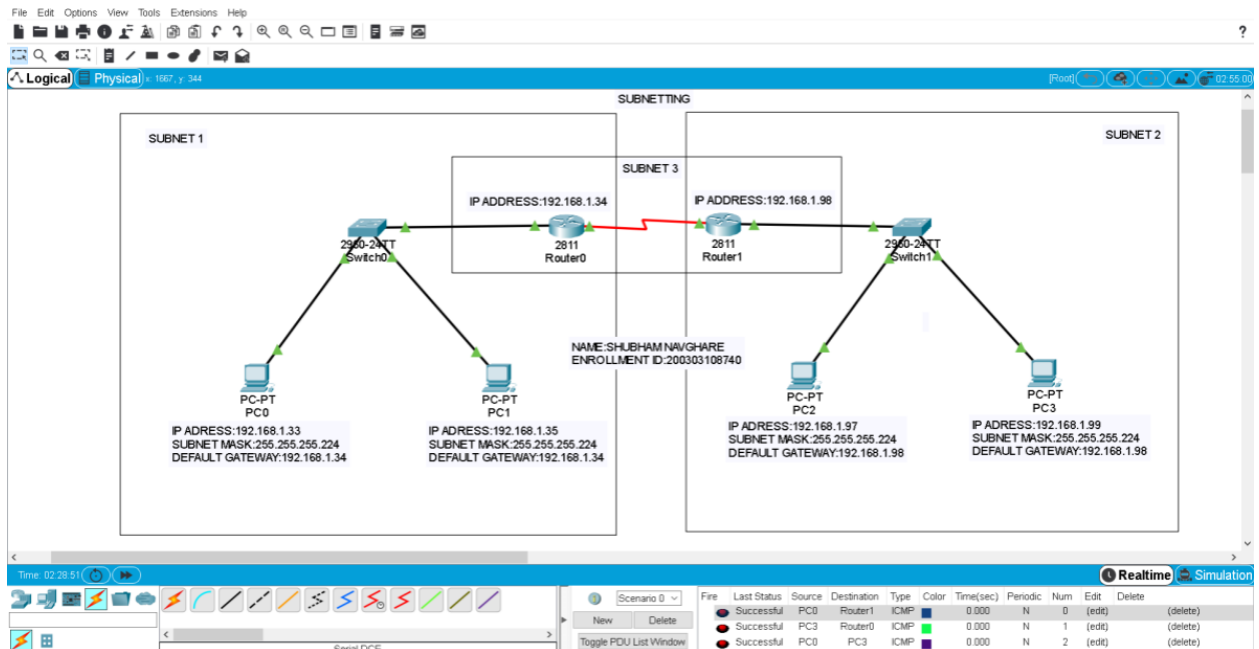
Step 2: Send packet 1st subnet in pc0 to pc1 and 2nd subnet in pc2 to pc3.



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

Step 1: Create 3 subnet.

Step 2: Send packet 1st subnet to 3rd subnet, 2nd subnet to 3rd subnet and 1st subnet to 2nd subnet.



PRACTICAL: 8

AIM: Implementation of SUBNETTING.

SUBNETTING:

Procedure:

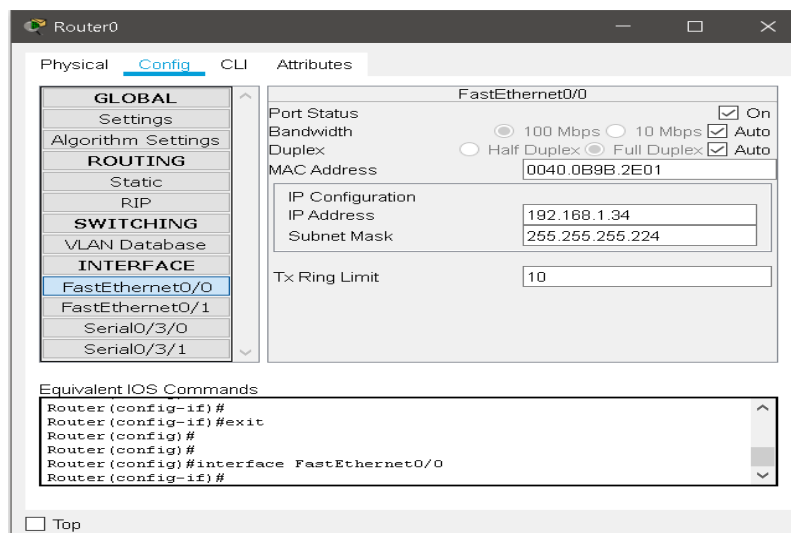
Step 1: Take 2 switch(2950-24TT) and 4 pc.

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

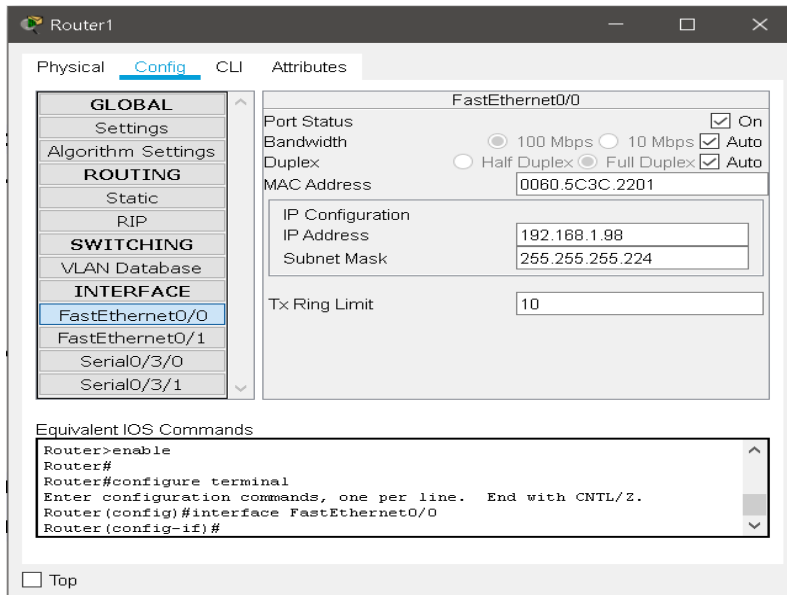
Step 3: Assign ip address to each pc.

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.



Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

FastEthernet0/0

FastEthernet0/1

Serial0/3/0

Serial0/3/1

FastEthernet0/0

Port Status ☒ On

Bandwidth ☒ Auto

Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.5C3C.2201

IP Configuration

IP Address 192.168.1.98

Subnet Mask 255.255.255.224

Tx Ring Limit 10

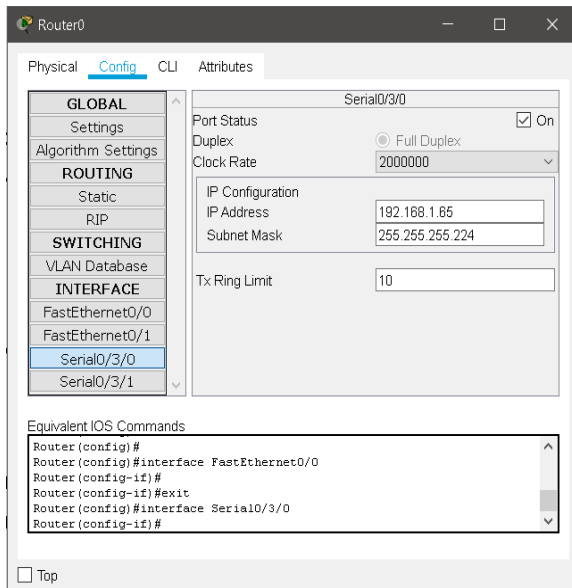
Equivalent IOS Commands

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

☐ Top

Step 7: Connect routers with Serial DTE cable.

Step 8: In routers config section assign ip address and subnet mask of serial0/3/0 and serial0/3/1 and port status is also on.



Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

FastEthernet0/0

FastEthernet0/1

Serial0/3/0

Serial0/3/1

Serial0/3/0

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 192.168.1.85

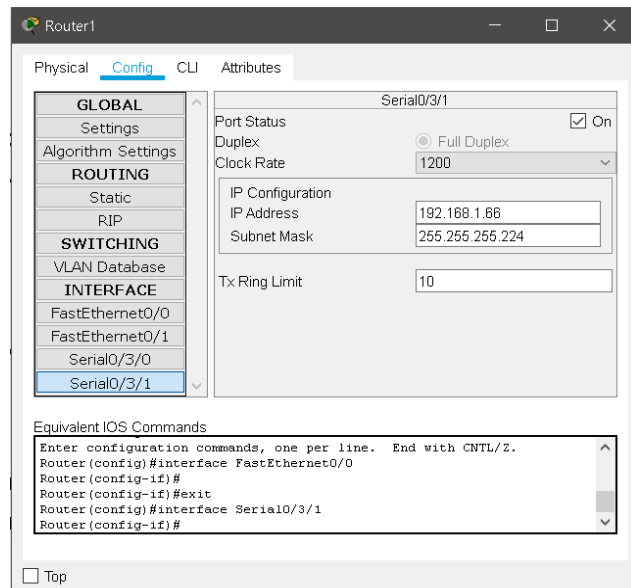
Subnet Mask 255.255.255.224

Tx Ring Limit 10

Equivalent IOS Commands

```
Router (config)#
Router (config)#interface FastEthernet0/0
Router (config-if)#
Router (config-if)#exit
Router (config)#interface Serial0/3/0
Router (config-if)#
```

☐ Top



Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

FastEthernet0/0

FastEthernet0/1

Serial0/3/0

Serial0/3/1

Serial0/3/1

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 1200

IP Configuration

IP Address 192.168.1.86

Subnet Mask 255.255.255.224

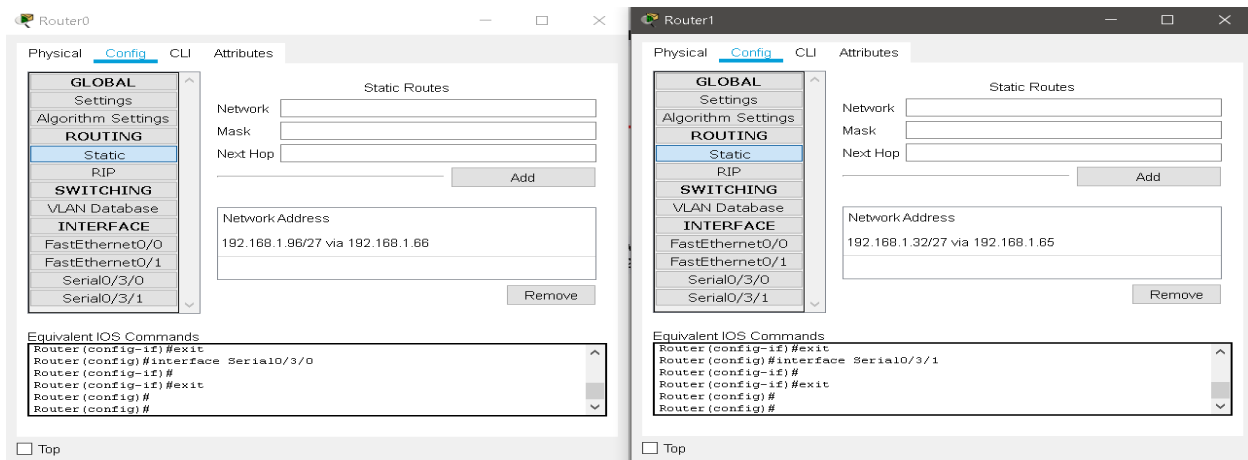
Tx Ring Limit 10

Equivalent IOS Commands

```
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#interface FastEthernet0/0
Router (config-if)#
Router (config-if)#exit
Router (config)#interface Serial0/3/1
Router (config-if)#
```

☐ Top

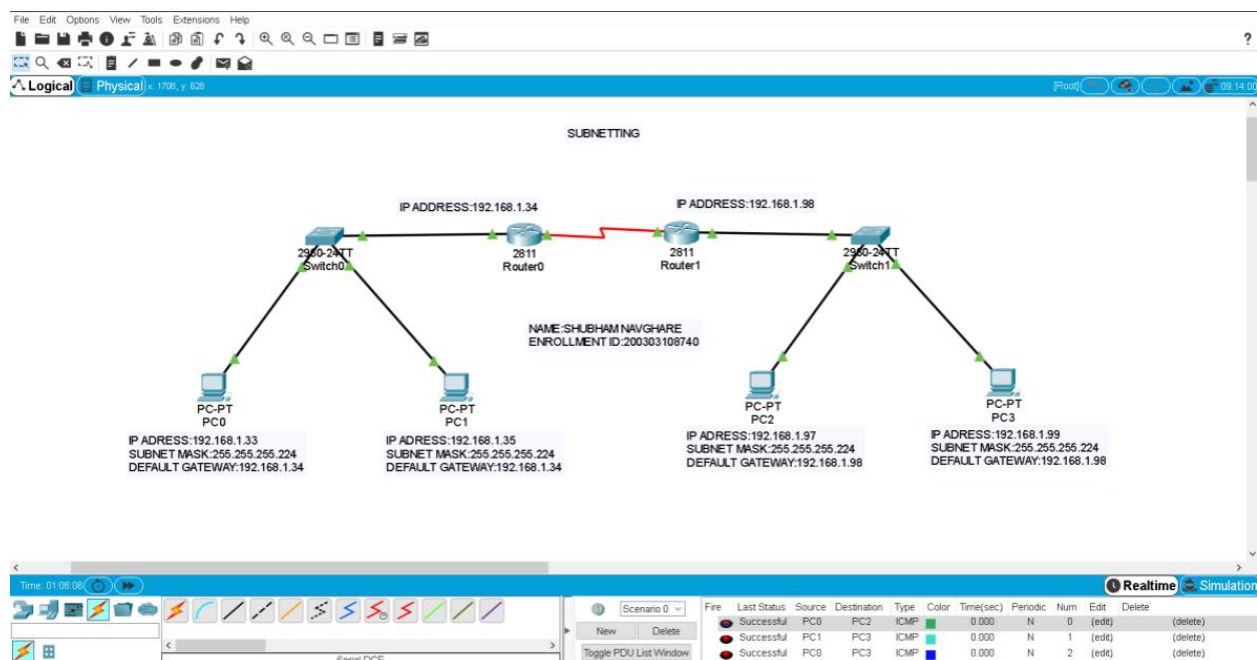
Step 9: Go to static section and add the network address.



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

Step 11: Send the packet between different subnetting.

OUTPUT:



PRACTICAL: 9

AIM: Routing at Network Layer

Procedure:

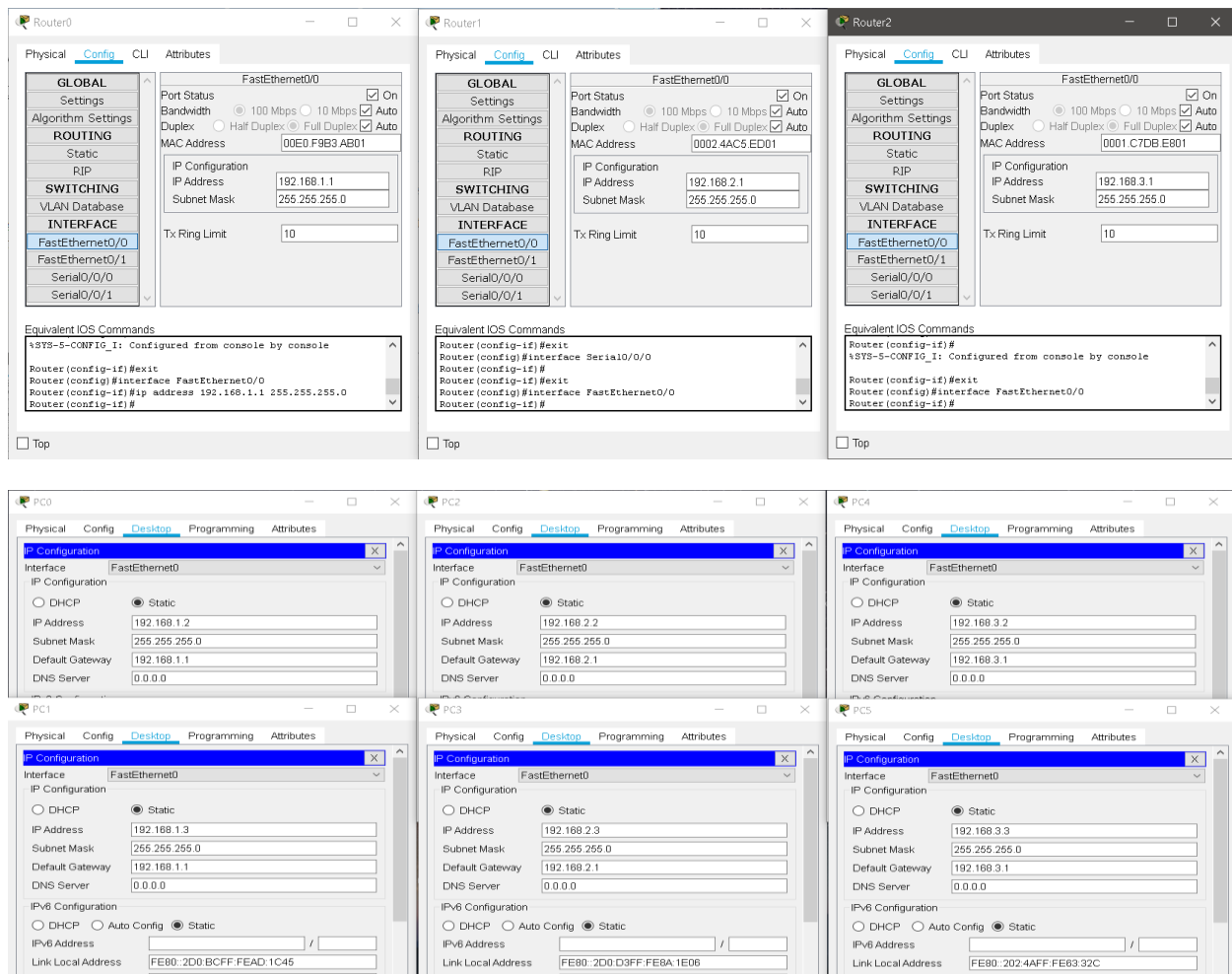
DYNAMIC ROUTING:

Step 1: Take 6 pc and 3 switch.

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

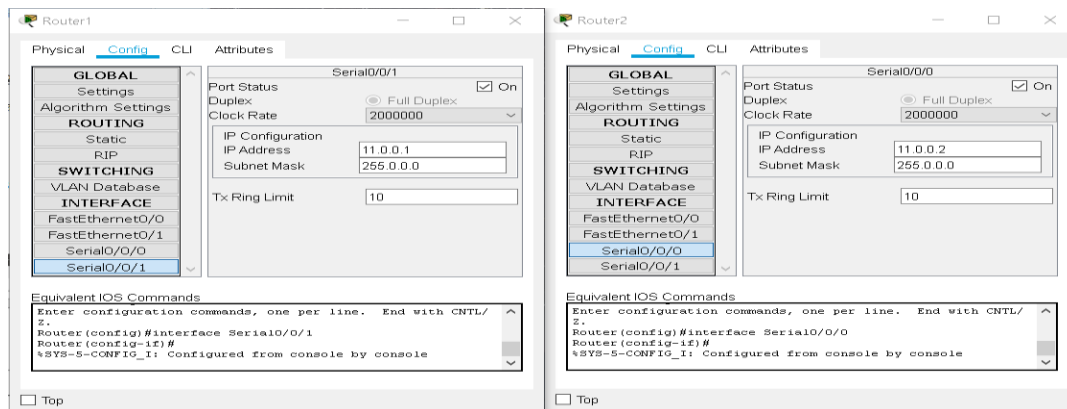
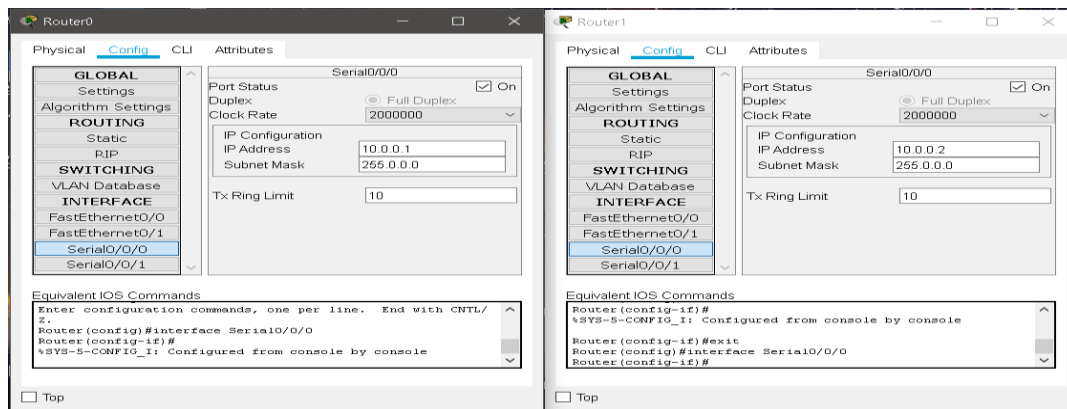
Step 3: Take 3 router and each router connect the each switch with copper straight-through wire.

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

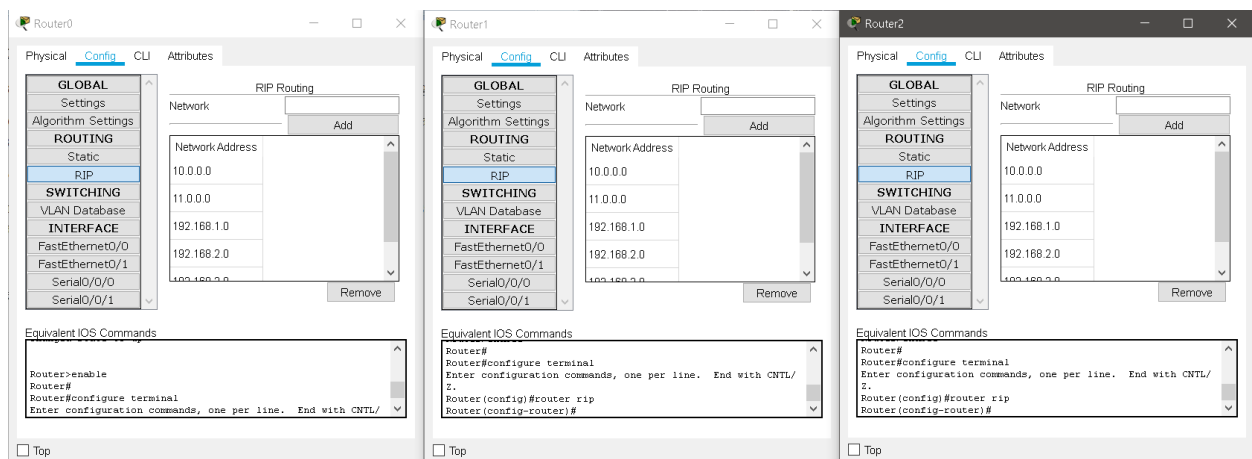


Step 5: Each routers connected with Serial DTE cable.

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.

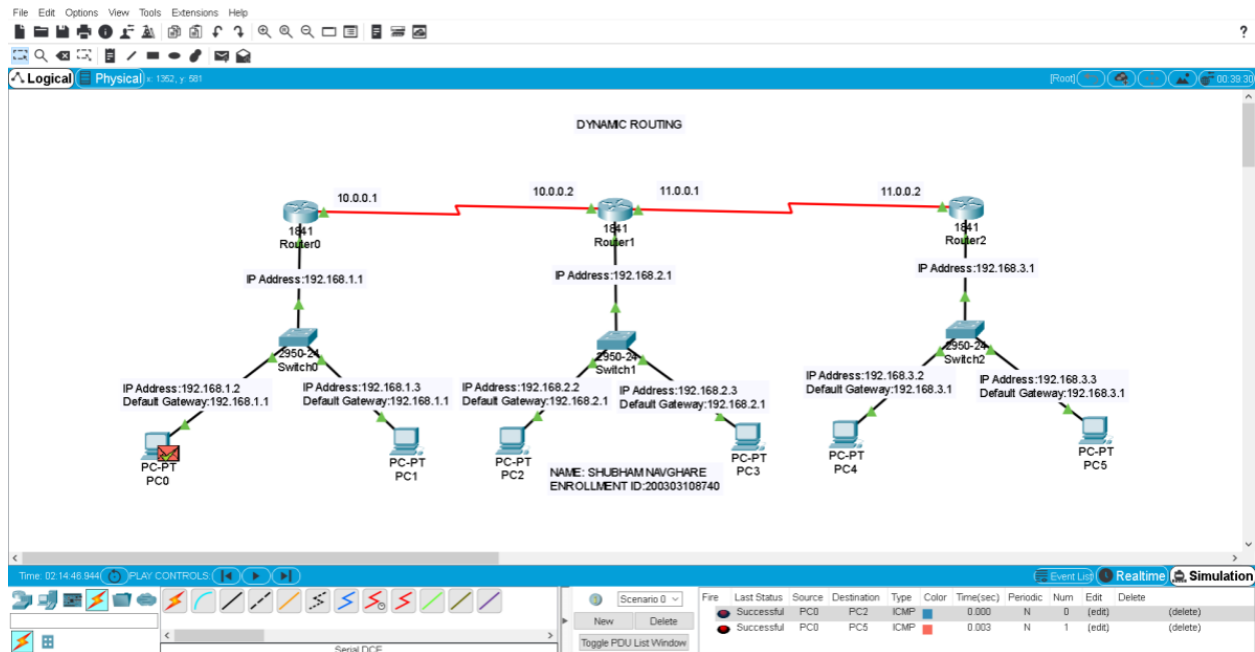


Step 7: Each router in RIP section in add the network address.



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

OUTPUT:



PRACTICAL: 10

AIM: Experiment on Transport Layer

1. Capturing a bulk TCP transfer from your computer to a remote server

- Before beginning our exploration of TCP, we'll need to use Wireshark to obtain a packet trace of the TCP transfer of a file from your computer to a remote server. You'll do so by accessing a Web page that will allow you to enter the name of a file stored on your computer (which contains the ASCII text of Alice in Wonderland), and then transfer the file to a Web server using the HTTP POST method (see section 2.2.3 in the text). We're using the POST method rather than the GET method as we'd like to transfer a large amount of data from your computer to another computer. Of course, we'll be running Wireshark during this time to obtain the trace of the TCP segments sent and received from your computer.

Do the following:

- Start up your web browser. Go the <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and retrieve an ASCII copy of Alice in Wonderland. Store this file somewhere on your computer.
- Next go to <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.
- You should see a screen that looks like:

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

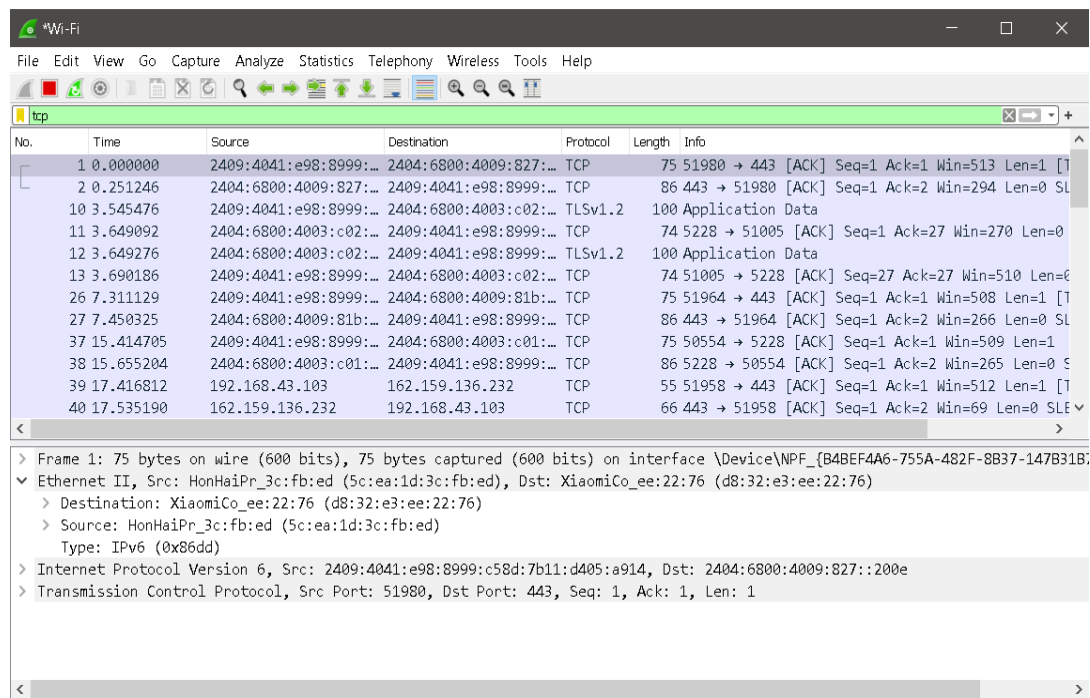
If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

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

t.bt

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!!

- Use the Browse button in this form to enter the name of the file (full path name) on your computer containing Alice in Wonderland (or do so manually). Don't yet press the "Upload alice.txt file" button.
- Now start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Returning to your browser, press the "Upload alice.txt file" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture. Your Wireshark window should look similar to the window shown below.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2409:4041:e98:8999::...	2404:6800:4009:827::...	TCP	75	51980 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [T...
2	0.251246	2404:6800:4009:827::...	2409:4041:e98:8999::...	TCP	86	443 → 51980 [ACK] Seq=1 Ack=2 Win=294 Len=0 SL...
10	3.545476	2409:4041:e98:8999::...	2404:6800:4003:c02::...	TLSv1.2	100	Application Data
11	3.649092	2404:6800:4003:c02::...	2409:4041:e98:8999::...	TCP	74	5228 → 51005 [ACK] Seq=1 Ack=27 Win=270 Len=0
12	3.649276	2404:6800:4003:c02::...	2409:4041:e98:8999::...	TLSv1.2	100	Application Data
13	3.690186	2409:4041:e98:8999::...	2404:6800:4003:c02::...	TCP	74	51005 → 5228 [ACK] Seq=27 Ack=27 Win=510 Len=0
26	7.311129	2409:4041:e98:8999::...	2404:6800:4009:81b::...	TCP	75	51964 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [T...
27	7.450325	2404:6800:4009:81b::...	2409:4041:e98:8999::...	TCP	86	443 → 51964 [ACK] Seq=1 Ack=2 Win=266 Len=0 SL...
37	15.414705	2409:4041:e98:8999::...	2404:6800:4003:c01::...	TCP	75	50554 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
38	15.655204	2404:6800:4003:c01::...	2409:4041:e98:8999::...	TCP	86	5228 → 50554 [ACK] Seq=1 Ack=2 Win=265 Len=0 S...
39	17.416812	192.168.43.103	162.159.136.232	TCP	55	51958 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [T...
40	17.535190	162.159.136.232	192.168.43.103	TCP	66	443 → 51958 [ACK] Seq=1 Ack=2 Win=69 Len=0 SLF...

> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{B4BEF4A6-755A-482F-8B37-147B31B...}

✓ Ethernet II, Src: HonHaiPr_3c:fb:ed (5c:ea:1d:3c:fb:ed), Dst: XiaomiCo_ee:22:76 (d8:32:e3:ee:22:76)

> Destination: XiaomiCo_ee:22:76 (d8:32:e3:ee:22:76)

> Source: HonHaiPr_3c:fb:ed (5c:ea:1d:3c:fb:ed)

Type: IPv6 (0x86dd)

> Internet Protocol Version 6, Src: 2409:4041:e98:8999:c58d:7b11:d405:a914, Dst: 2404:6800:4009:827::200e

> Transmission Control Protocol, Src Port: 51980, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the steps above on one of the author's computers². You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, when you explore the questions below.

2. A first look at the captured trace

Before analyzing the behavior of the TCP connection in detail, let's take a high level view of the trace.

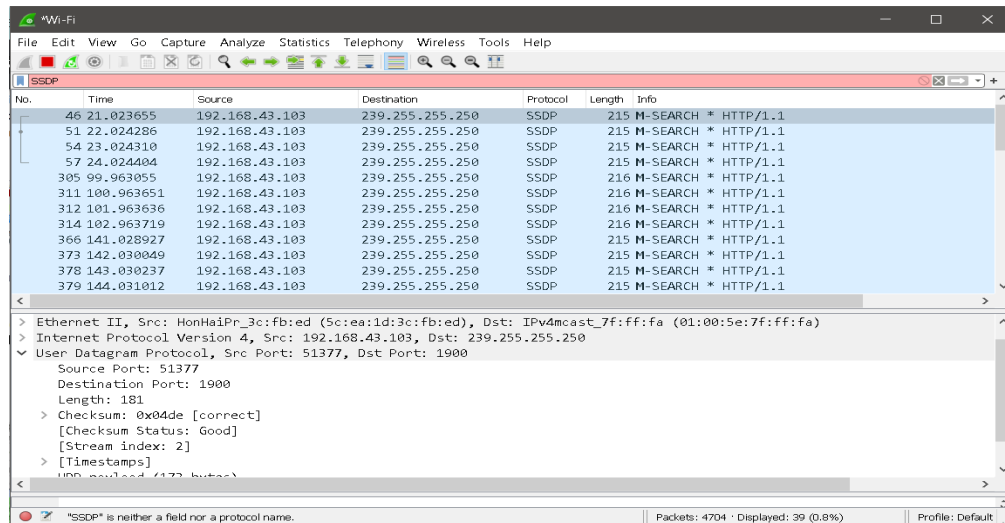
- First, filter the packets displayed in the Wireshark window by entering “tcp”(lowercase, no quotes, and don't forget to press return after entering!) into the display filter specification window towards the top of the Wireshark window.

What you should see is series of TCP and HTTP messages between your computer and gaia.cs.umass.edu. You should see the initial three-way handshake containing a SYN message. You should see an HTTP POST message. Depending on the version of

Wireshark you are using, you might see a series of “HTTP Continuation” messages being sent from your computer to gaia.cs.umass.edu. Recall from our discussion in the earlier HTTP Wireshark lab, that is no such thing as an HTTP Continuation message – this is Wireshark's way of indicating that there are multiple TCP segments being used to carry a single HTTP message. In more recent versions of Wireshark, you'll see “[TCP segment of a reassembled PDU]” in the Info column of the Wireshark display to indicate that this TCP segment contained data that belonged to an upper layer protocol message (in our case here, HTTP). You should also see TCP ACK segments being returned from gaia.cs.umass.edu to your computer.

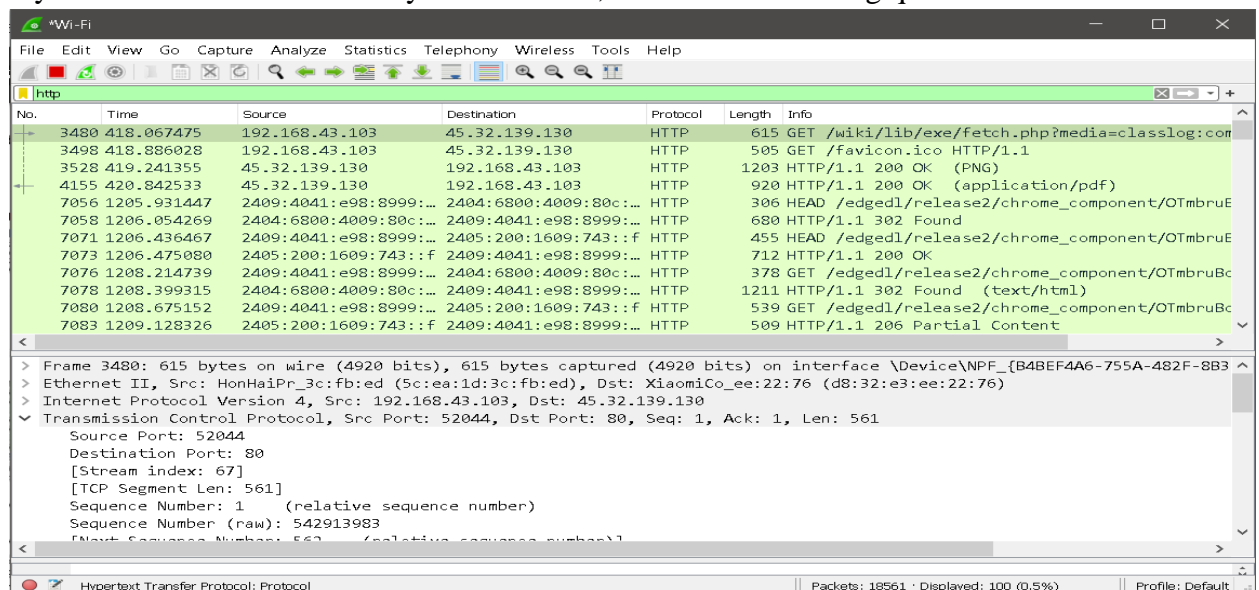
Answer the following questions, by opening the Wireshark captured packet file tcp-ethereal-trace-1 in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> (that is download the trace and open that trace in Wireshark; see footnote 2). Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout³ to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows).

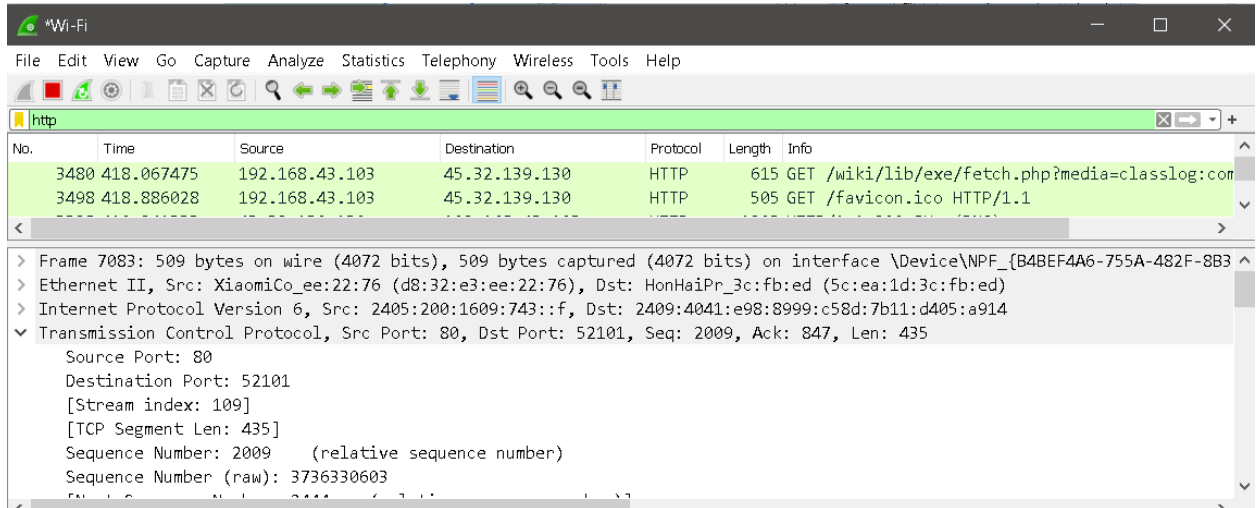


2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

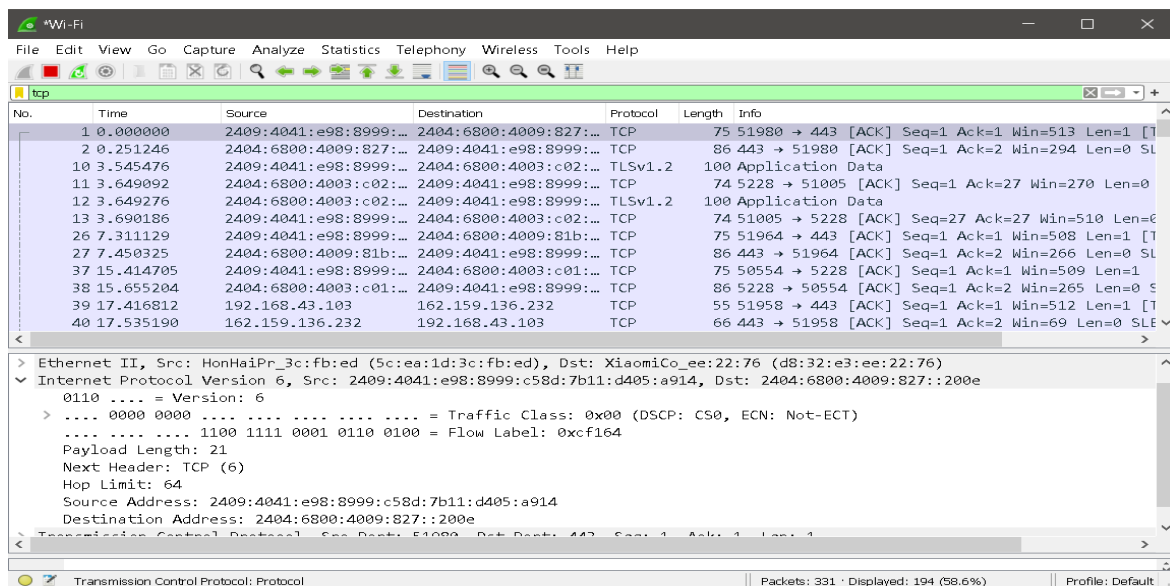
If you have been able to create your own trace, answer the following question:



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



Since this lab is about TCP rather than HTTP, let's change Wireshark's "listing of captured packets" window so that it shows information about the TCP segments containing the HTTP messages, rather than about the HTTP messages. To have Wireshark do this, select Analyze->Enabled Protocols. Then uncheck the HTTP box and select OK. You should now see a Wireshark window that looks like:



This is what we're looking for - a series of TCP segments sent between your computer and gaia.cs.umass.edu. We will use the packet trace that you have captured (and/or the packet trace tcp-ethereal-trace-1 in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>; see earlier footnote) to study TCP behavior in the rest of this lab.

3. TCP Basics

Answer the following questions for the TCP segments:

4. 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?

