The National Institute of Engineering

(Autonomous Institution)

DC Assignment Report

"CISCO PACKET TRACER"

Submitted By

SOURAV G **4NI17IS081**

Under the guidance

Dr. K. Raghuveer
Professor

Ms. B. S. Prathibha
Asst. Professor

Department of Information Science and Engineering

MYSURU – 570008

2019-2020

THE NATIONAL INSTITUTE OF ENGINEERING MYSURU-570008

Department of Information Science and Engineering

Certificate

This is to certify that the Assignment work entitled "**Cisco Packet Tracer**" is a work carried out by **SOURAVG** in partial fulfillment for the assignment prescribed by National Institute of Engineering, Autonomous Institution under Visvesvaraya Technological University, Belagavi for the Fifth Semester B.E Information Science & Engineering. It is certified that all correction/suggestions indicated for Internal Assessment have been incorporated. The report has been approved as it satisfies the academic requirements in respect of the Assignment work prescribed for the fifth Semester.

Signature of Guide	Signature of Guide	Signature of Prof. & HOD
Dr. K. Raghuveer	**Ms. B.S. Prathibha**	**Dr. P Devaki**
Professor	Assistant Professor	Dept of ISE

ACKNOWLEDGEMENT

We would like to take this opportunity to express our profound gratitude to all those people who have directly or indirectly involved in the completion of the project. We thank each and every one who encouraged us in every possible way.

We would like to thank **Dr. G. RAVI,** Principal, NIE, Mysuru for letting us to be a part of this prestigious institution and letting us to explore our abilities to the fullest.

We would like to extend our sincere gratitude to **Dr. P Devaki,** Professor & HOD, Dept of ISE, NIE, Mysuru for being a source of inspiration and instilling an enthusiastic spirit in us throughout the process of project making.

We wish to express our heartfelt gratitude towards **Dr. K Raghuveer** Professor and **Ms. B.S. Prathibha,** Dept of ISE, NIE, Mysuru for his consistent guidance and valuable knowledge.

We are extremely pleased to thank our parents, family members and friends for their continuous support, inspiration and encouragement, for their helping hand and also last but not the least. We thank all the members who supported us directly or indirectly in our academic process.

Sourav G (4NI17IS081)

ABSTRACT

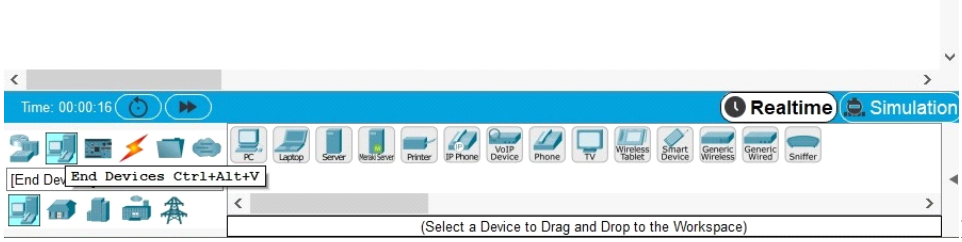
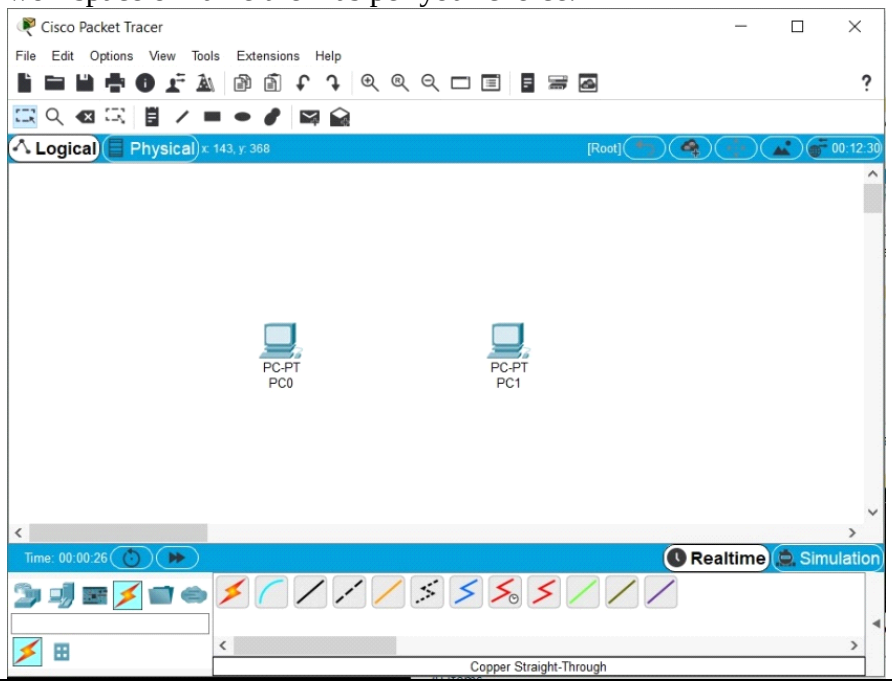
The significance of maintaining this report gives us detail study of the transmission of signals from one point to another point. This assignment helps us to update and record the data and acknowledge in step by step process about the transmission and the errors caused, the reasons for the failure of the transmission of the signal between the two computers.

Statistics are recorded for each transmission during the transmission process, and aggregated over a single transmission channel. This assignment includes all details regarding the information about the computer IP address, the wires used to connect the computers, the type of the hub, switch used. Transmission of the signal between two or more computers require lot of condition to be followed, and proper transmission channel and medium is required. These stats are used to analyze the performance each type of the transmission and also for general purposes.

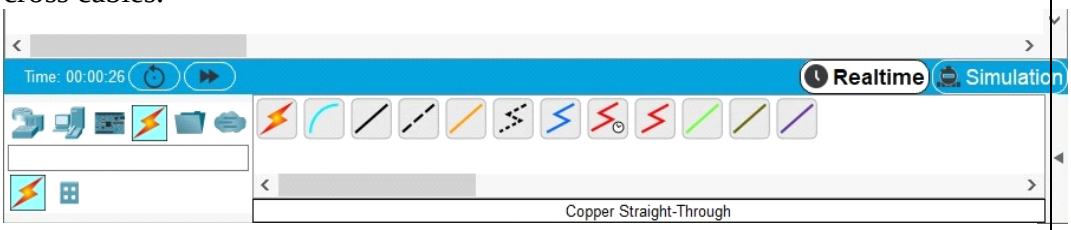
CONTENTS

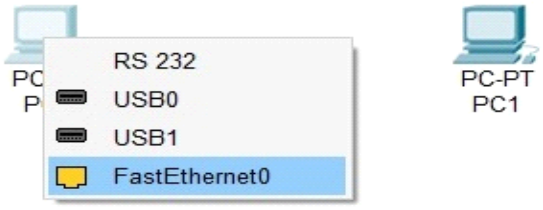
Data Communication (IS0413)

Semester: V **Experiment No:1**

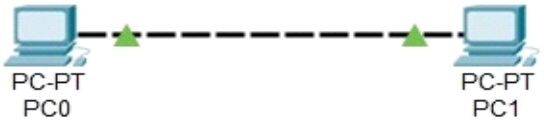
Aim of the Experiment	To establish host to host communication.
Scope of the Experiment	For communication of two network we must allow host to host communications between these two hosts or the devices
Design / Methodology	We connect two or more devices which want to communicate with the help of cable. If the two devices are like we use cross cables If the two devices are unlike we use straight pair of cables
Procedure (Steps)	 1. Select device from End Devices option and drag it on to the workspace. 2. Similarly select another device to have two devices (PC0 and PC1) on to the workspace or name them as per your choice. 

3.Select Connection option and using cross cable connect like devices and for unlike devices use straight cable, here since the two devices are like we use cross cables.





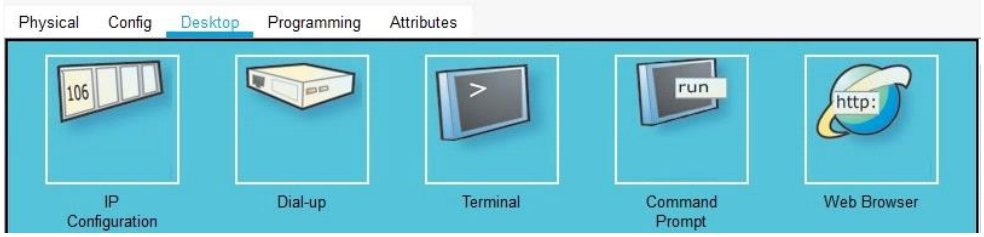
4. After selecting cable click on PC0 and select FastEthernet0 port.



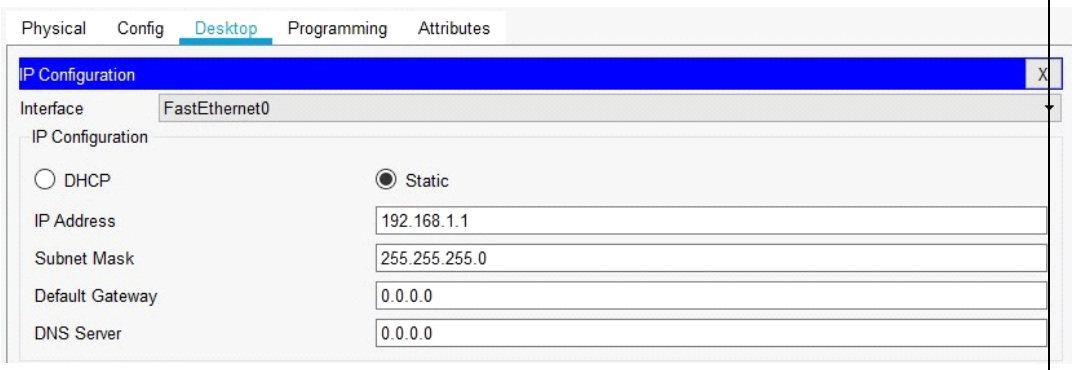
5. Then click on PC1 and select Choose FastEthernet0 to establish the connection.

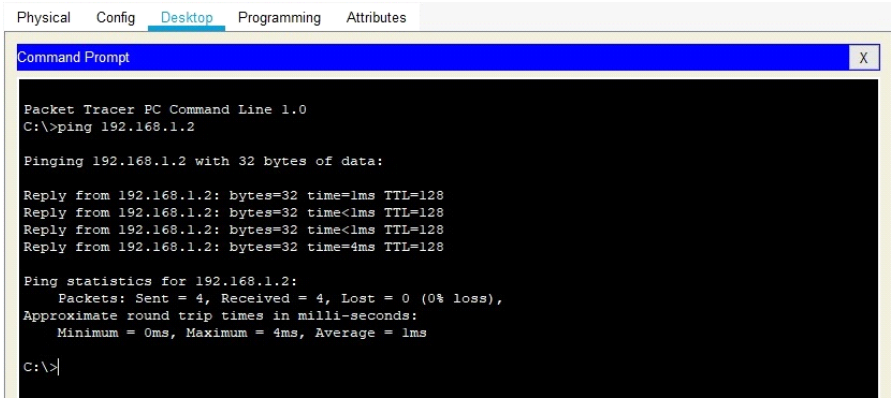
6. For unlike devices connect them using straight cable because if they are connected using cross cable connection is not established and vice versa.

7. Perform IP configuration for both the devices PC0 and PC1, by clicking on the device and then selecting Desktop and then IP Configuration.

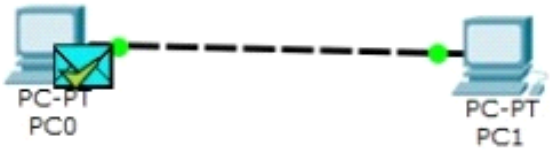


8. Then assign unique IP address to both the devices.
Here for our convenience we configure PC0 as 192.168.1.1
and PC1 as 192.168.1.2





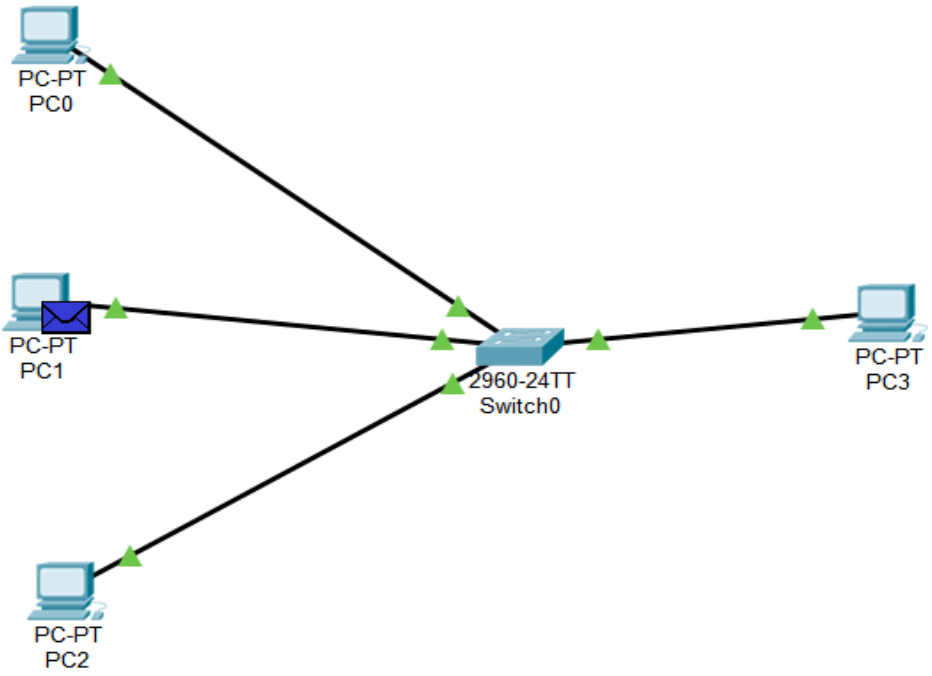
9. To check if the connection is established, open the command prompt in Desktop option, and execute ping command to the target device IP address.
to check PC1 from PC0 use the command such as ping 192.168.1.2
and to connect PC1 to PC0 use ping 192.168.1.1

	 10. Select simple PDU from PC0 to PC1 to pass a message and change to simulation mode. Packet travel from PC0 to PC1.The packet is travelled from PC0 to PC1 in simulation mode
Conclusion	Therefore we obtain a host-to-host communication between out two devices PC0 and PC1 which we confirmed in simulation mode where the packet transfers from PC0 and PC1 and the green signal in front of the devices determines that the connection is established and data can be communicated

DATA COMMUNICATION(IS0413)

Semester: V **Experiment No:2**

Aim of the Experiment	To establish a network of multiple devices with the help of switch.
Scope of the Experiment	Switches are capable of determining the destination of each individual traffic element and selectively forwarding data to the one computer that actually needs it. By generating less network traffic in delivering messages, hence a switch performs better than a hub on busy networks.
Design / Methodology	A network switch is a computer networking device that is used to connect many devices together on a computer network.Two devices can be directly connected but for more than two devices we use a switch to determine the source machine Required devices are connected to a common switch with help of straight cable and then communication can be established between the only required devices. Successful communication between PC3 to PC1

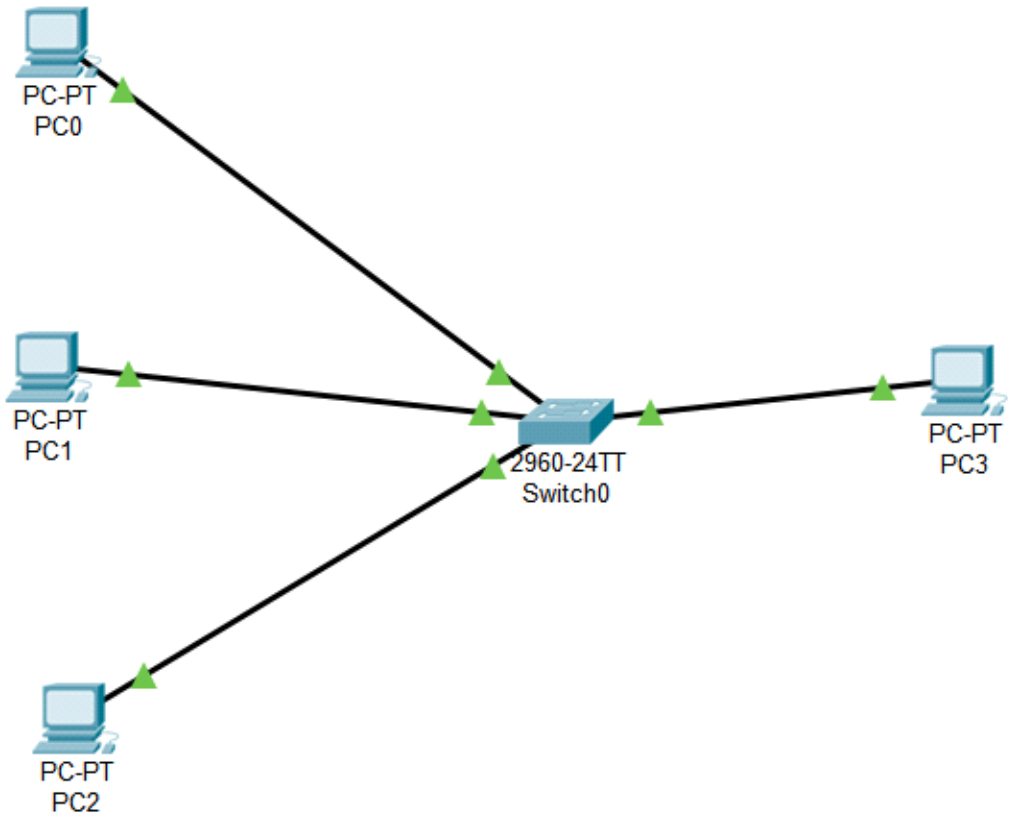


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	PC1	ICMP		0.000	N	0	(edit)	(delete

Procedure (Steps)

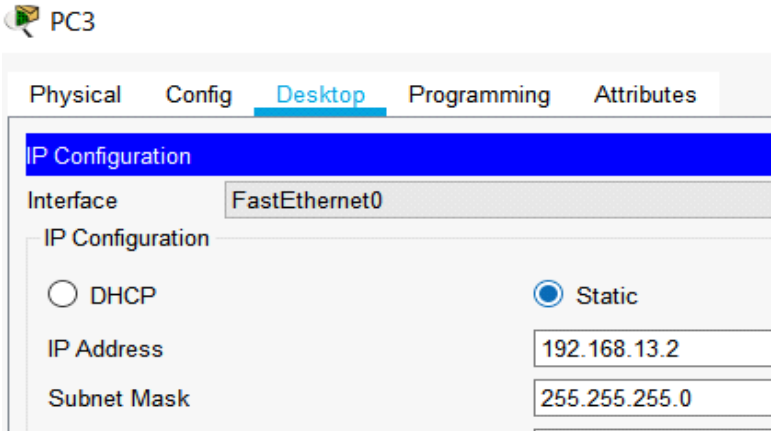
1. Open cisco packet tracer
2. Choose the end devices icon as shown on the Picture and generic PCs.

3. Add switch device to connect between the PCs. We can extract the switch device from the network devices.

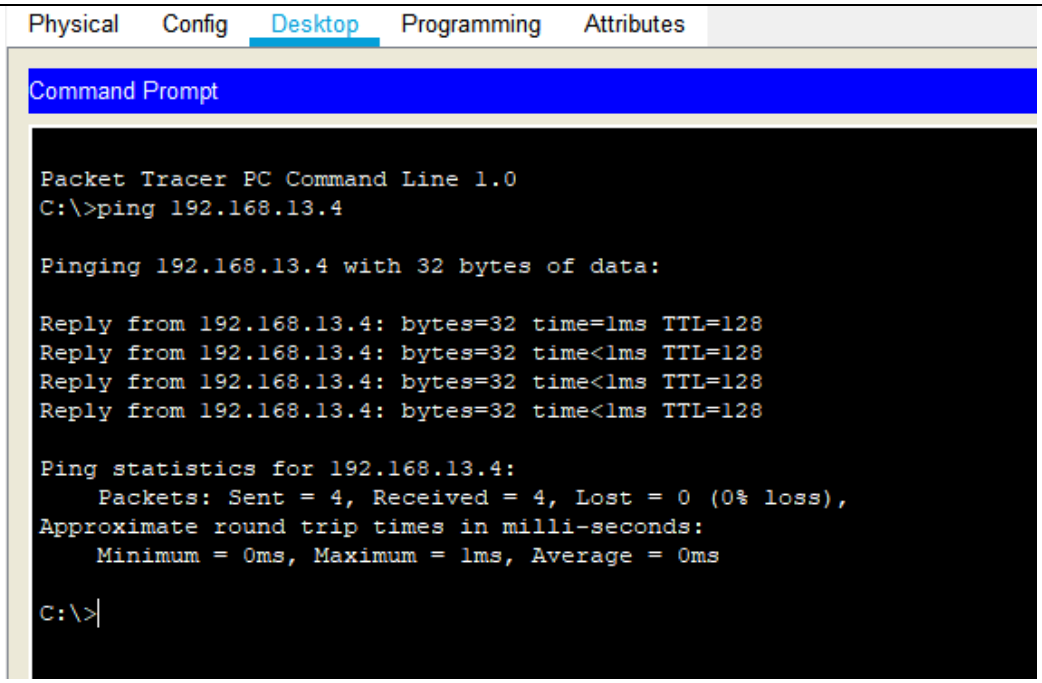


4. Select copper straight since they are two unlike device through cable from connection, then click on desktop (PC0), after that click on the switch, choose fast Ethernet port for both devices. Do this step with all PCs.

5. Use desktop tab for desktop program IP configuration give a static IP address.



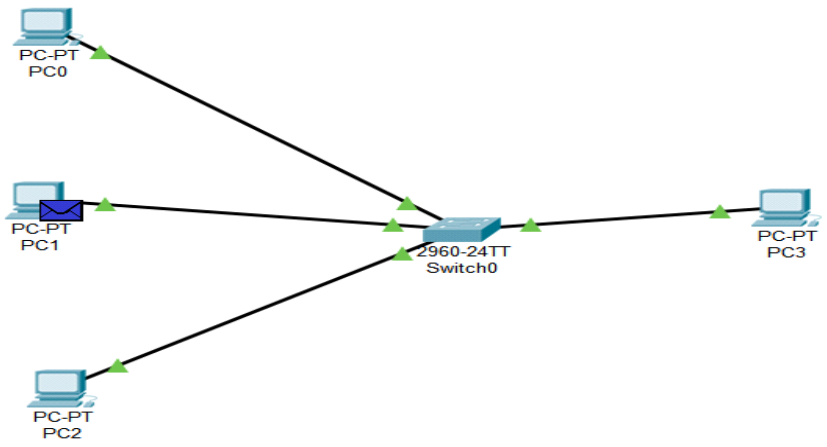
6. The IP address for (PC0) is 192.168.13.5, for (PC1) is 192.168.13.4, for (PC2) 192.168.13.3, for (PC3) is 192.168.13.2, for (PC4) is 192.168.13.5, and the subnet mask is 255.255.255.0 for all PCs.



7. To see communication from any PC to other PC through hub open desktop program command prompts and issues a ping. Suppose to send message from PC3 to PC1 click on PC1 using command prompt:-> ping 192.168.13.4.

8. Add simple PDU to pass a message then go to simulation mode from real time. Now press on auto capture/play to track the packet movements.

9. The packet travel from selected PC to the destination device through

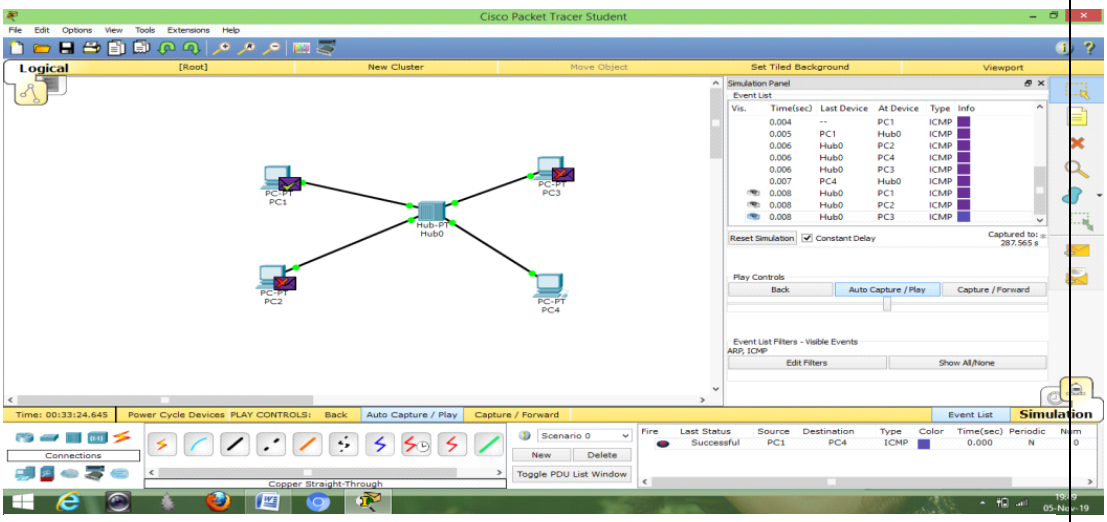


switch.

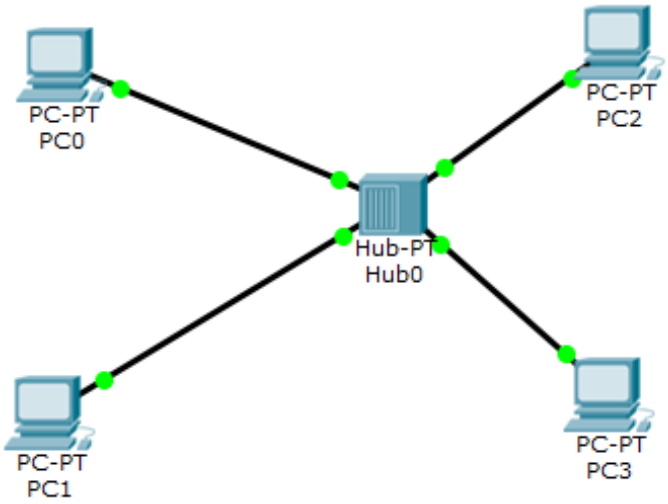
Conclusion	Hence, Switch allow to receive information from any source connected to it and dispatch that information to the appropriate destination only.

DATA COMMUNICATIONS(IS0413)

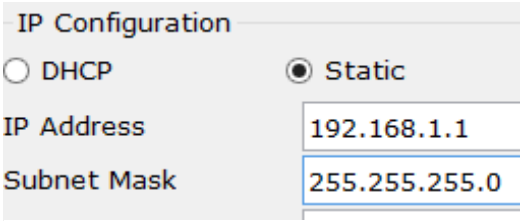
Semester: V **ExperimentNo:3**

Aim of Experiment	To establish successful communication between host to host using HUB.
Scope of the Experiment	Device communication is established using a HUB between two devices using basic tools and interface.
Design	
Procedure (Steps)	1.Open Cisco packet tracer 2. Go to end device and click on PC and drop it on the screen  3. Repeat step no 2 to add another 3 PC or click on Cltr and select on PC to add multiple Pc's at once. 4.Then drag a generic hub from hub section

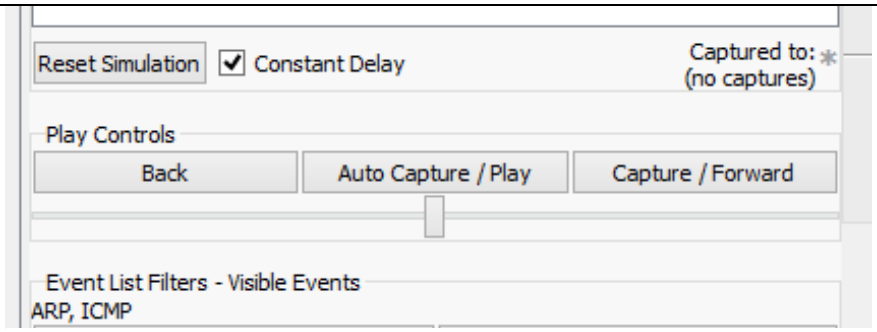
5.Connect all the devices with hub using copper straight-through cable with fastEthernet port



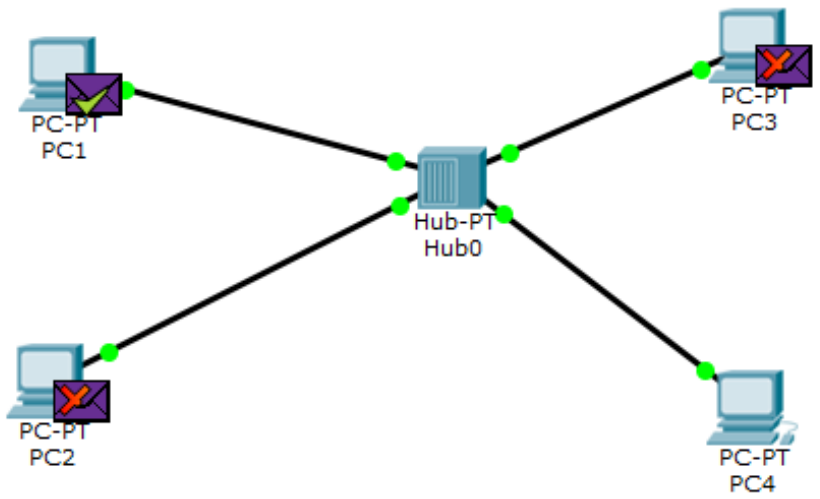
6.To communicate from one PC to another PC we need to configure then click on the PC0 use desktop tab for program IP configuration give a static IP address 192.168.1.1 for PC0, 192.168.1.2 for PC1, 192.168.1.3 for PC3, 192.168.1.4 for PC4. Put subnet mask 255.255.255.0 for each PC's.

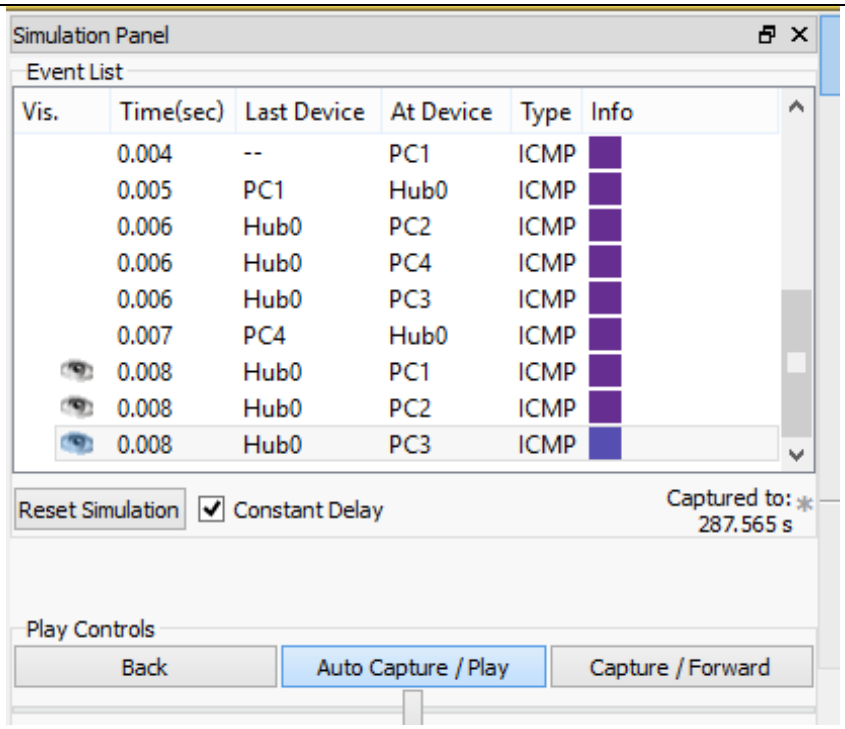


7.Now go to stimulation mode from real time. In stimulation panel under event list filter click show all/none and then click edit filter and then choose ARP (address resolution protocol) and ICMP (internet control management protocol)

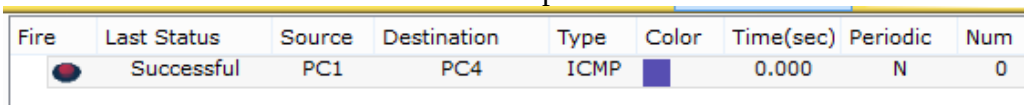


8.Then add simple PDU from right toolbar and drag it over source and then destination.
Suppose we want to send message from PC1 to PC4 then click on auto capture/play and then stimulation starts.





If communication between devices is completed then it will show successful.

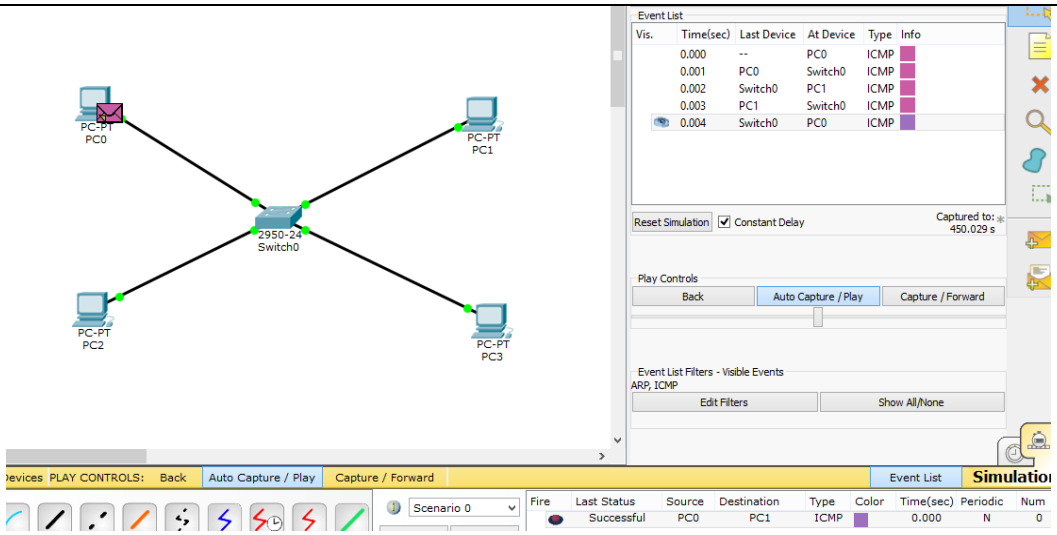


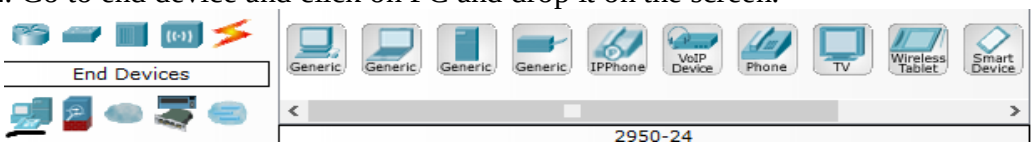
Conclusion

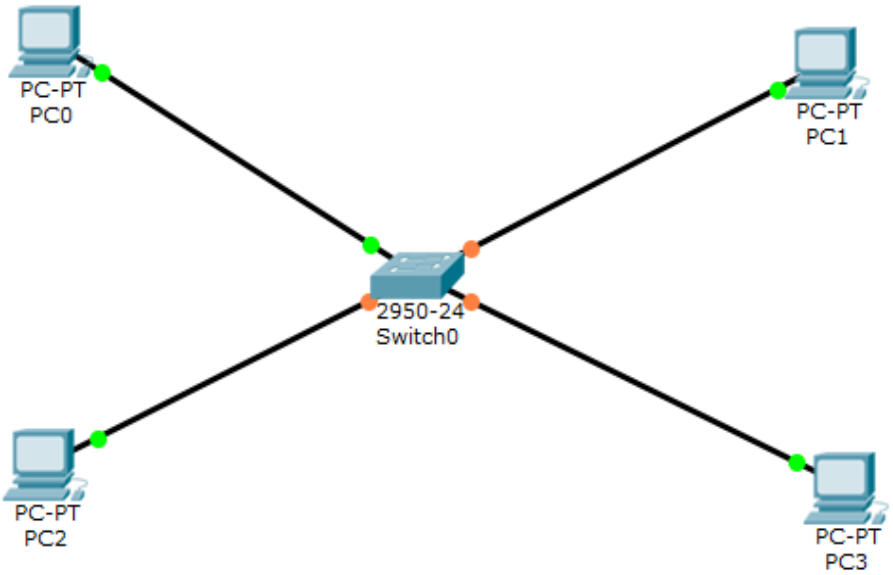
By this experiment we came know that HUB is one of the simplest devices which perform the task of connecting the multiple network ready devices. It acts as a terminal that can provide data exchange between computers in a way that multiple to single internet ready computing device or vice versa. They usually find their application in connecting multi computers to single server or single internet connection.

Data Communication (IS0413)

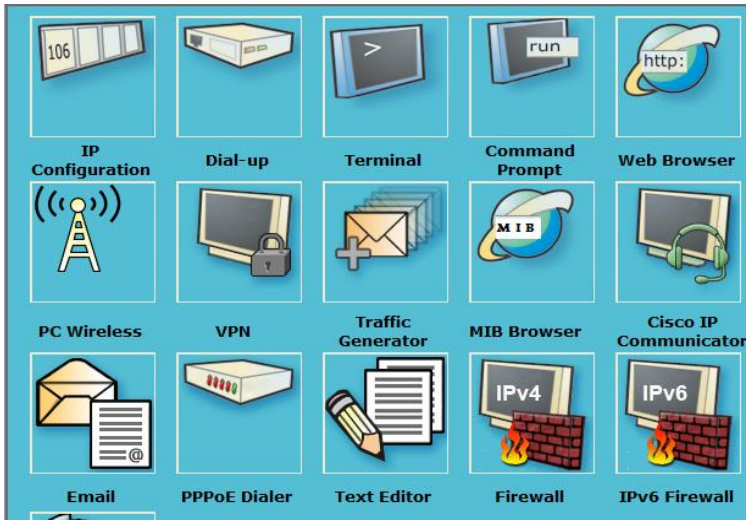
Semester: V **Experiment No:4**

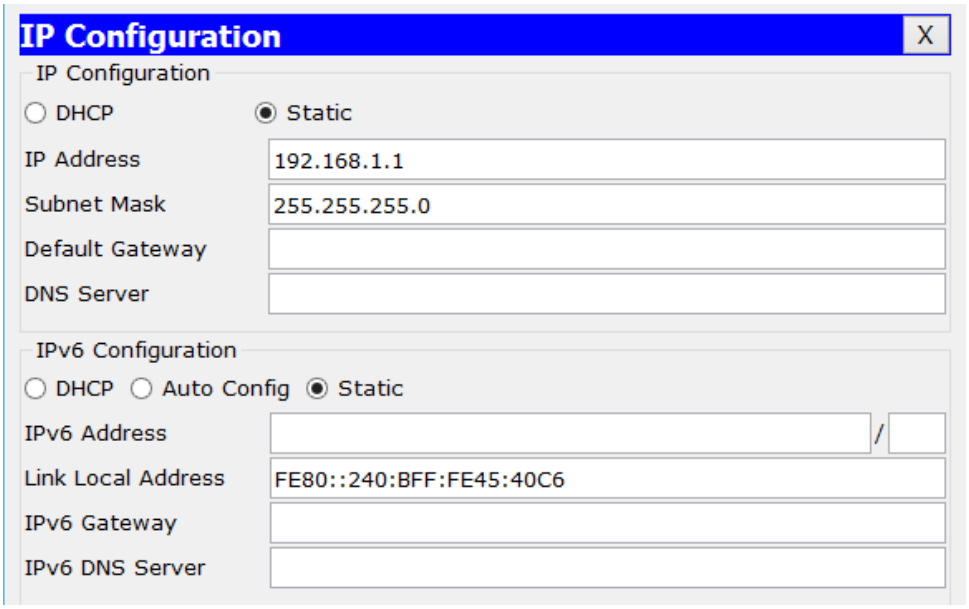
Aim of the Experiment	To analyze the working of virtual local area network (VLAN)
Scope of the Experiment	Virtual Local Area Networks (VLAN) separate an existing physical network into multiple logical networks. Thus, each VLAN creates its own broadcast domain. LAN is the abbreviation for local area network and in this context virtual refers to physical object recreated and altered by additional logic. which restricts each device communicating with every other device
Design	 Virtual local area network which is configured by software not by physical. VLAN control broadcast storm through assigning the network traffic, and data transmission between different VLAN should be with the aid of routing function. We usually use router as kind of trunk equipment in general. VLAN make it for network administration to partition network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure.

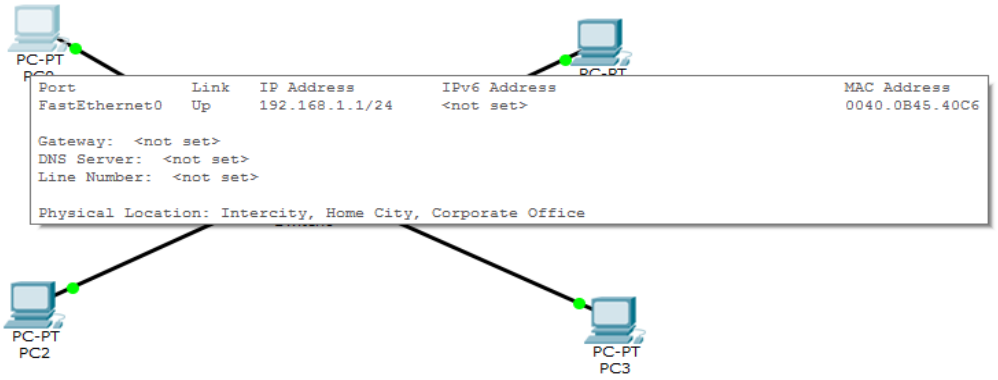
Procedure	1. Open Cisco packet tracers. 2. Go to end device and click on PC and drop it on the screen.  3. Go to switches and click on generic switch and drop it on the screen.  4. Follow step 1 and add 3 more PC's.  4. Connect these PC's to switch using a copper straight-through cable since they two different devices.



5.Click on PC0 and set the IP address by double clicking on the computer, going to desktop option in that selecting IP configuration

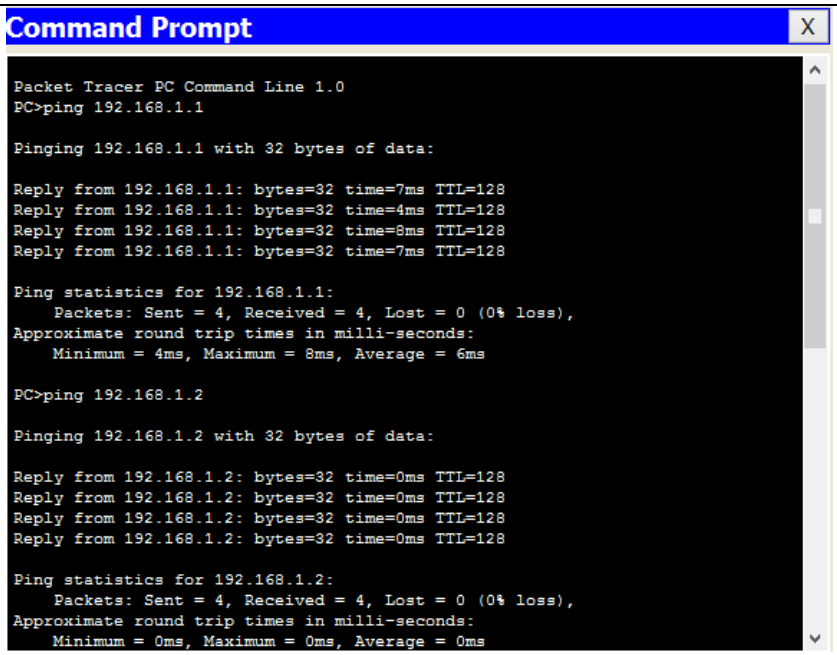






6. Repeat the step 5 for other 3 devices.

7. Click on the first device and select the command prompt from the desktop option, to check the communication between the devices. Here the command used is “ping”.



8. Repeat step 7 for other 3 devices.

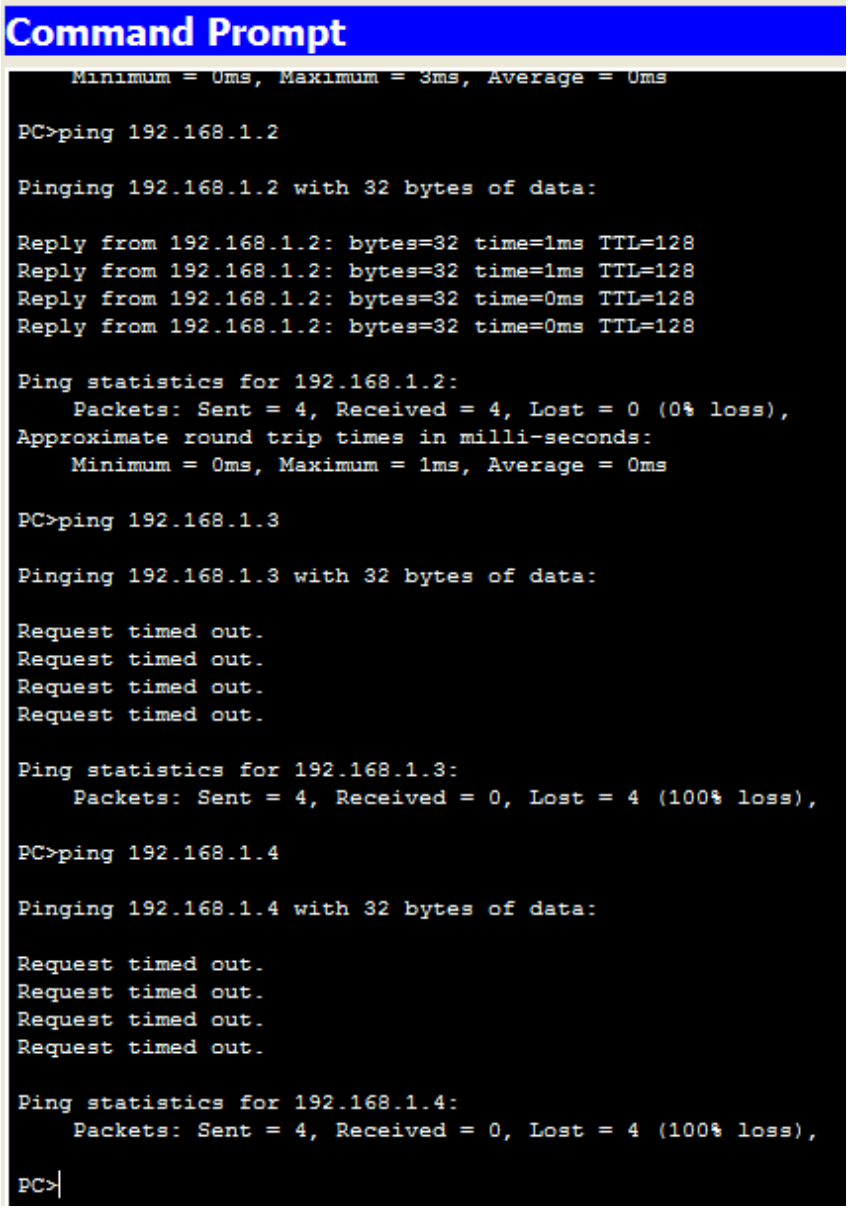
9. Double click on switch upon which we get a menu and select CLI(command line interface). Type the following command to achieve the necessary abstraction.

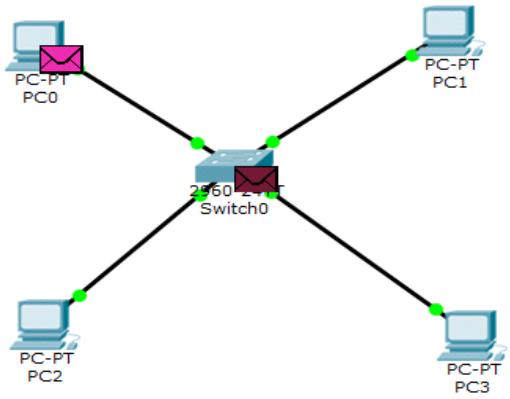
1. Switch>enable
2. Switch #config t
3. Switch(config)#VLAN 10
4. Switch(config-VLAN)#exit
5. Switch(config)#VLAN 20
6. Switch(config)#interface fastEthernet 0/1
7. Switch(config-if)#switch port access VLAN 10
8. Switch(config)#interface fastEthernet 0/2
9. Switch(config-if)#switch port access VLAN 10
10. Switch(config)#interface fastEthernet 0/3
11. Switch(config-if)#switch port access VLAN20
13. Switch(config)#interface fastEthernet 0/4
14. Switch(config)#Switch port access VLAN 20

IOS Command Line Interface

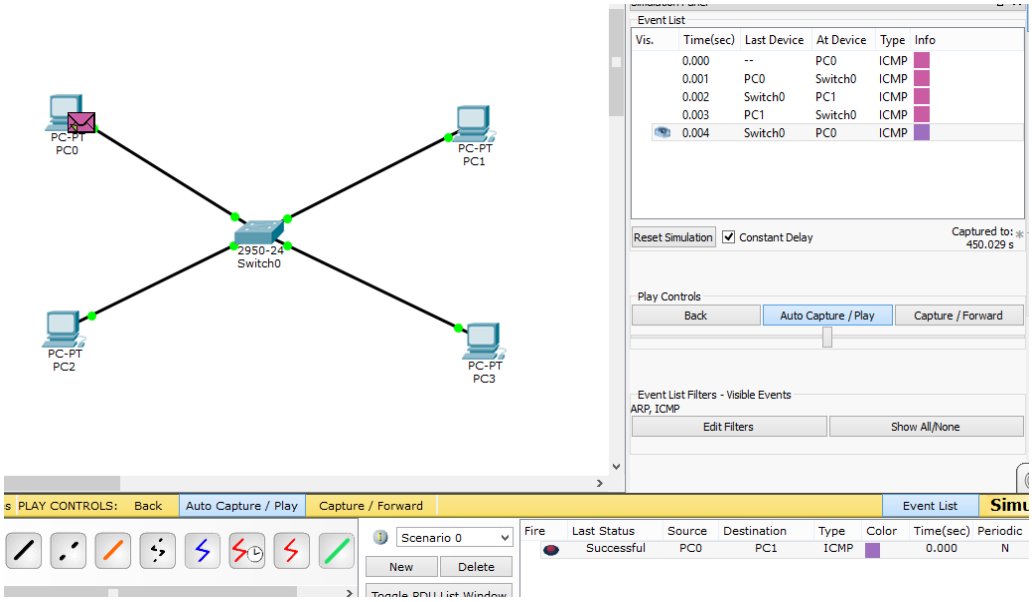
```
up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to
up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface fastEthernet 0/4
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
```

10. Now we check the communication between the device to verify our objective by using ping operation.

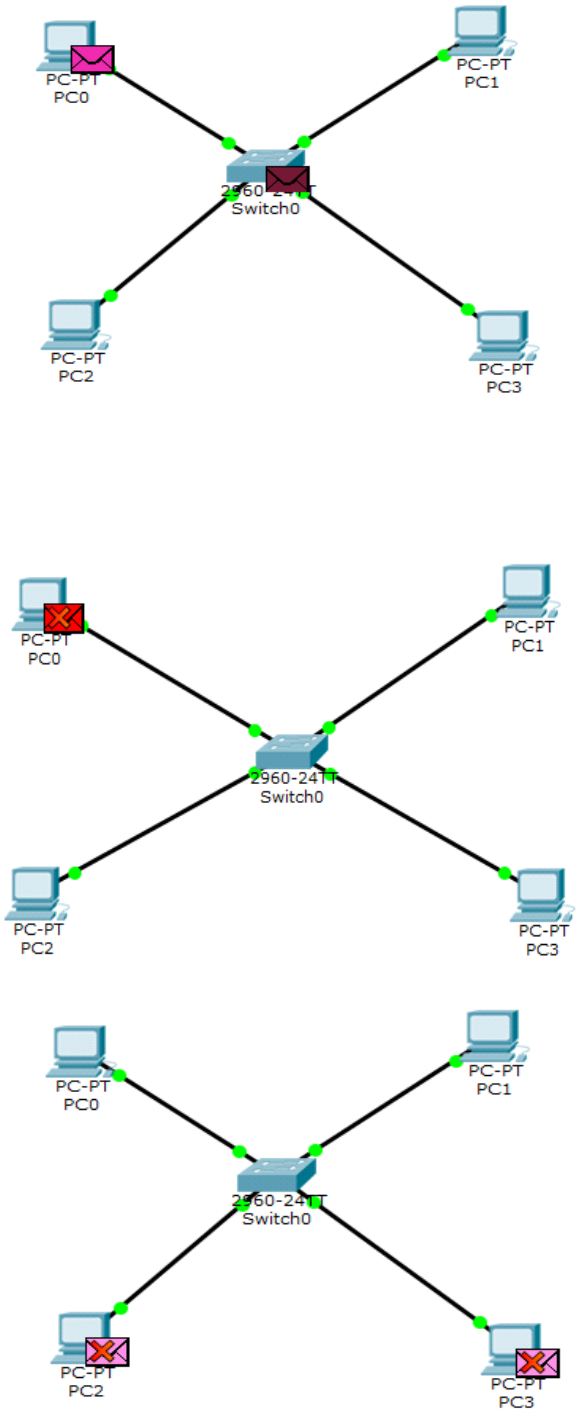

Command Prompt
Minimum = 0ms, Maximum = 3ms, Average = 0ms
PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>



11. Simulation of communication between the device PC0 and PC1 and it is successful.

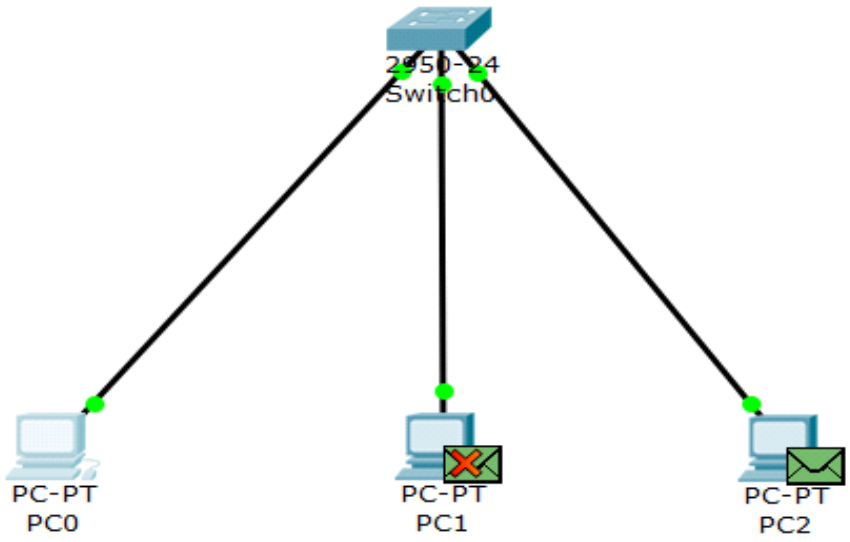


12. Simulation of communication between the device PC 0 and PC2, which is unsuccessful.

	
Conclusion	Hence by this experiment we can conclude that VLAN allows us to logically segment a LAN into different broadcast domains. where only sensitive data may be broadcast on a network. VLAN provides ease of administration, reduce broadcast traffic and enforcement of security policies.

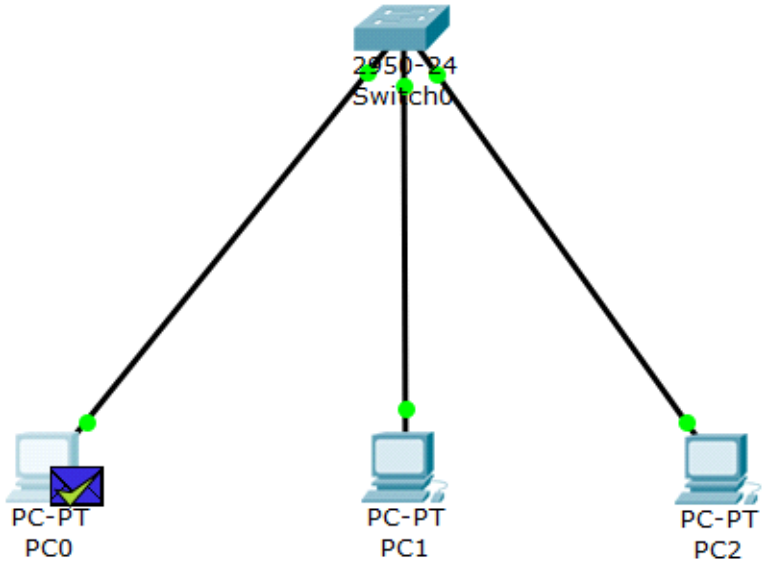
DATA COMMUNICATIONS(IS0413)

Semester: V **Experiment No: 5**

Aim of the Experiment	To analyze working of **ARP (**Address Resolution Protocol).
Scope of the Experiment	**ARP** is a function of the IP layer of the TCP/IP protocol stack. It is used to resolve 32-bit IP address to 48-bit Physical address (MAC address). While communicating one host uses ARP to determine physical address of another host. **ARP** maintains a cache (table) in which MAC addresses are mapped to IP addresses.
Design / Methodology	End devices are connected using a switch and made to communicate between them using their IP addresses. Using Address Resolution Protocol, source host will get the Physical address (MAC address) of the destination host. The IP address will be mapped to its corresponding physical address. This will be stored in ARP entries.  Successful communication between PC0 and PC3 PC1 will reject the frame.

```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           000c.8509.4b5d        dynamic
```

IP address and Physical address are mapped

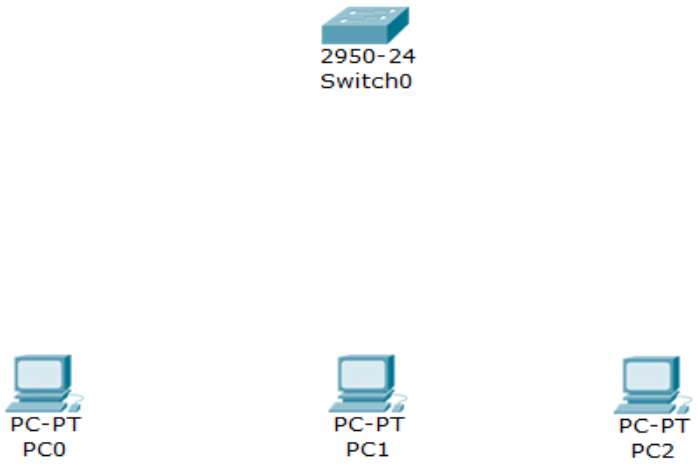


MAC address is sent to source host

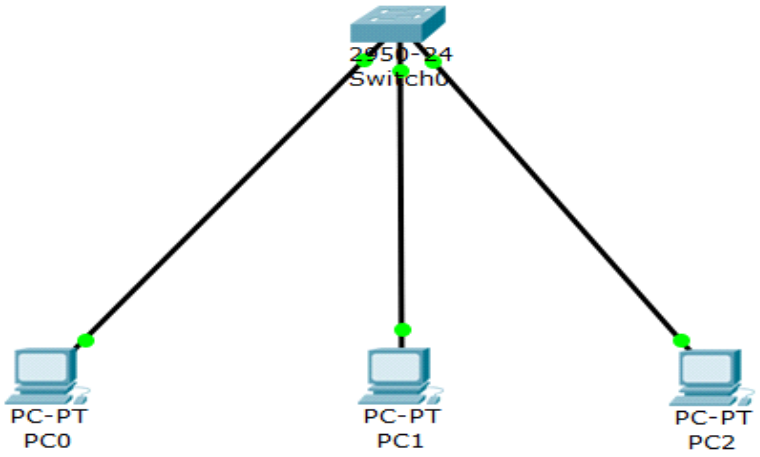
Procedure (Steps)

1.Go to switches and click on generic switch and drop it on the screen.

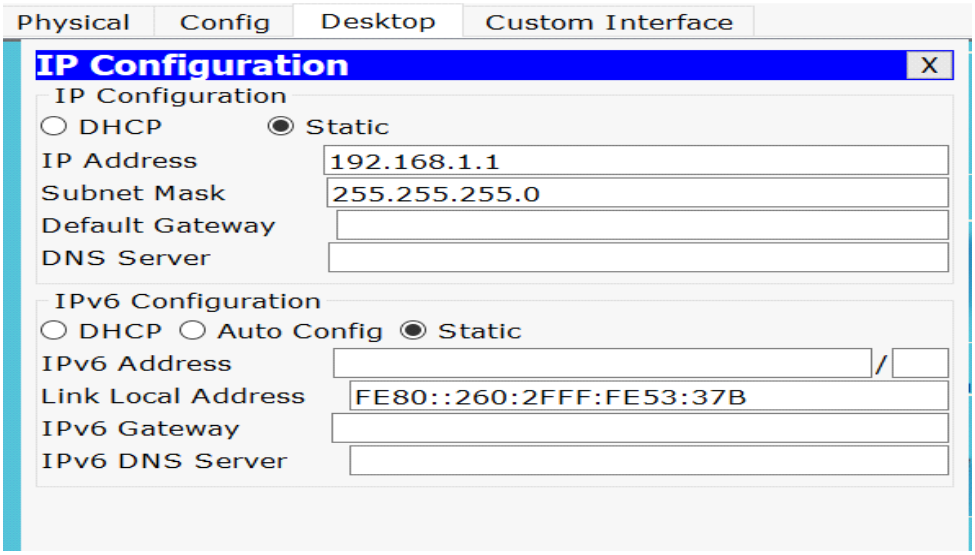
2. Go to end devices and select generic PC and drop it on the screen.



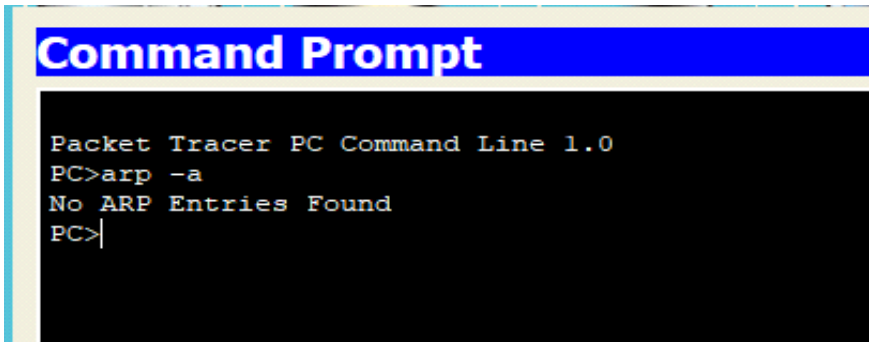
3.Select straight cable to connect since they are unlike devices.



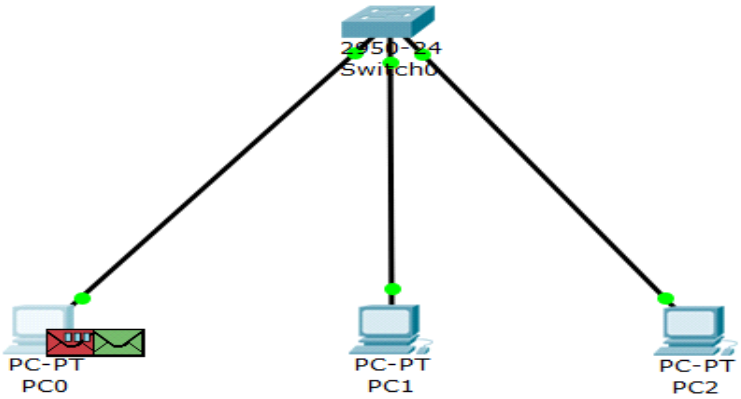
4. Select the computers and configure IP addresses for all them.



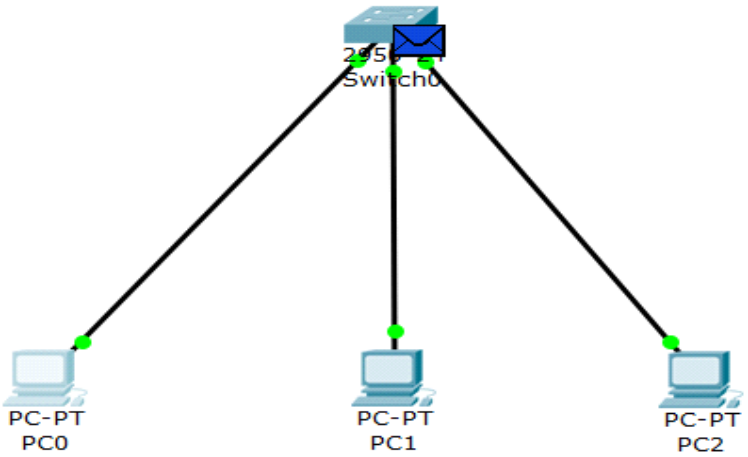
5. In command prompt Check ARP entries using the command **'arp -a'** initially it will be empty.



6. In command prompt ping from one host to another by typing its IP address.

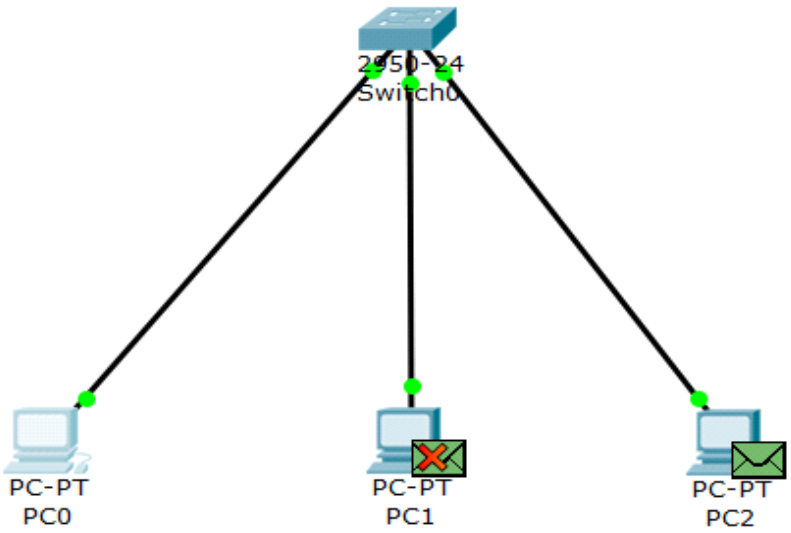


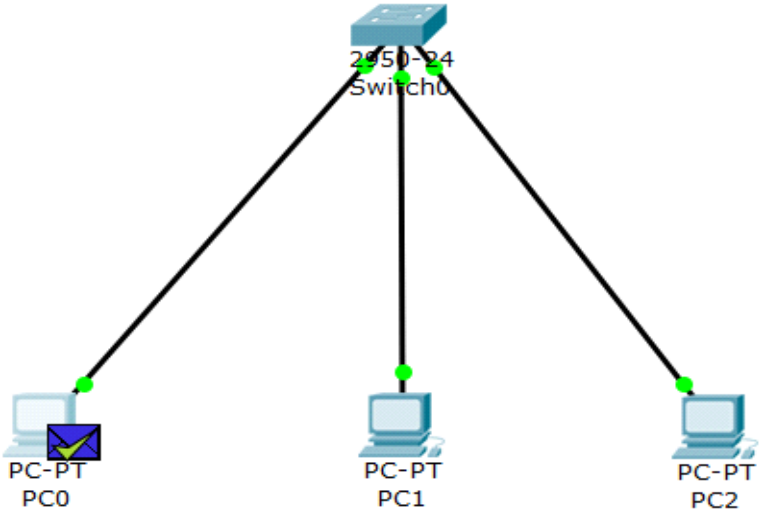

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
```



7. In simulation mode click on capture/forward option then the datagram will be transferred to the switch.

8.Then the frame is broadcasted and all other host except the destination host will reject the datagram.





9.

	Destination host will unicast the MAC address to sender through the switch.
Conclusion	Hence Address Resolution Protocol is implemented using cisco packet tracer. This protocol is used in TCP/IP model to communicate between devices by determining physical address of the host from its IP address.

DATA COMMUNICATIONS(IS0413)

Semester: V **Experiment No: 6**

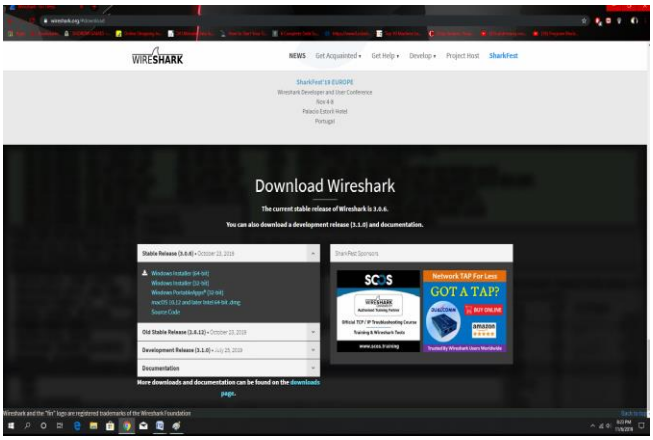
Aim of the Experiment	To discover hosts and services on a computer network with the help of Nmap (Network Mapper).
Scope of the Experiment	• Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it. • Identifying open ports on a target host in preparation for auditing. • Network inventory, network mapping, maintenance and asset management. • Finding and exploiting vulnerabilities in a network. • Used as a tool to study Ethical Hacking
Design / Methodology	Nmap (Network Mapper) is a free and open-source network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses. With Nmap we can perform: • Host discovery – Identifying hosts on a network • Port scanning – Enumerating the open ports on target hosts. • Version detection – Interrogating network services on remote devices to determine application name and version number. • OS detection – Determining the operating system and hardware characteristics of network devices. Command: nmap [<Scan Type> ...] [<Options>] {<target specification>}.

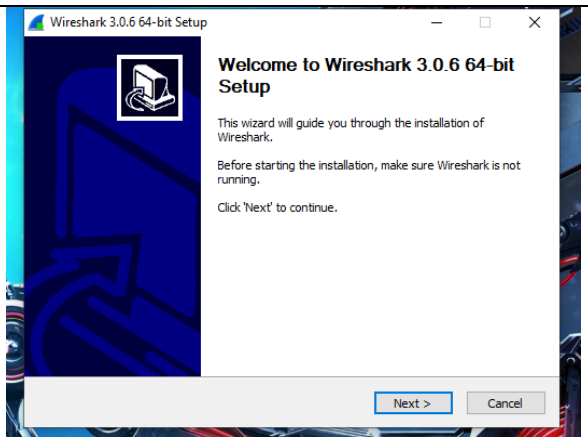
	Scan Type – A variety of scan can be performed like version scan, OS detection scan etc. Options – They may be timing or misc. options. Target specification – Can be a host name or IP addresses.
Procedure (Steps)	1. Install the Nmap in Linux using command, *sudo apt-get install nmap*. 2. Then perform scan for a host using website name or IP address as shown below. *~$ nmap <website> or <IP address>* 
Conclusion	Hence, Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features.

Data Communication (IS0413)

Semester: V **Experiment No: 7**

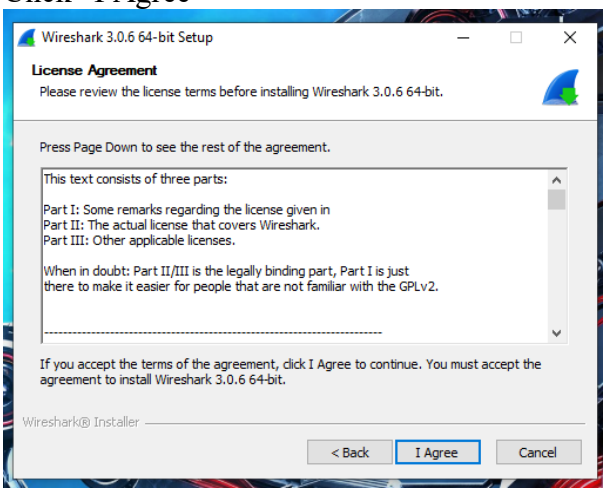
Aim of the Experiment	To Understand the basics of "Wireshark" tool and capturing the packet.
Scope of the Experiment	Wireshark is a network protocol analyzer. It's designed for network administrators so that they can see what's happening in their network and make sure that everything is working properly, and that nobody is doing anything suspicious on the network.

Design / Methodology	• The way that Wireshark works is it allows you to select an interface (through a wireless card or a wired card) and then logs all the packets, or all the traffic, that flows through that interface. • It has GUI interface that allows us to analyze this traffic, so it allows us to filter these packets based on the protocol used in them, such as HTTP or TCP. • It also allows us to look for certain things, such as cookies or POST or GET requests, and it also allows us to search through these packets.
Procedure (Steps)	• Installation of Wireshark • Go to https://www.wireshark.org/  • Choose the option for your OS and then download and Run the installer

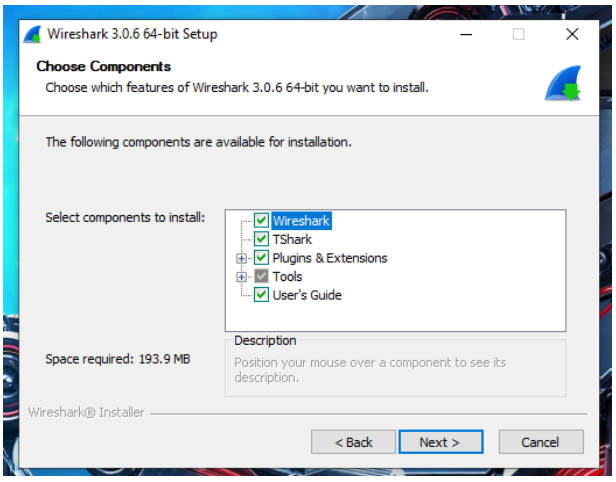


Click “Next”

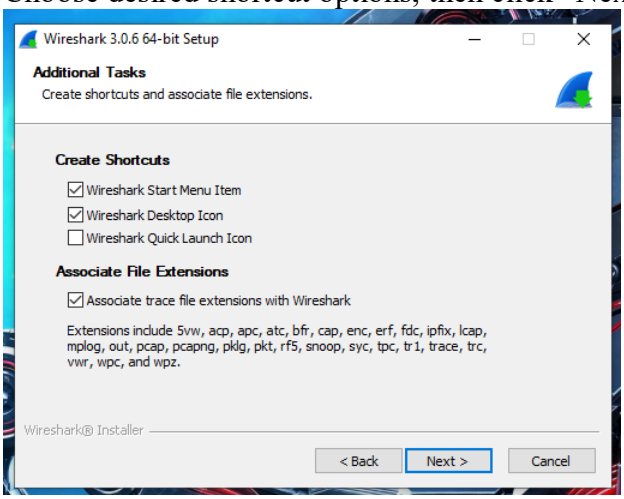
- Click “I Agree”



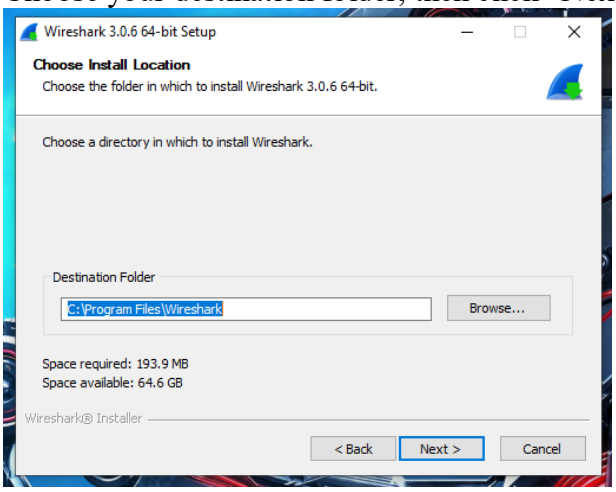
- Click “Next”



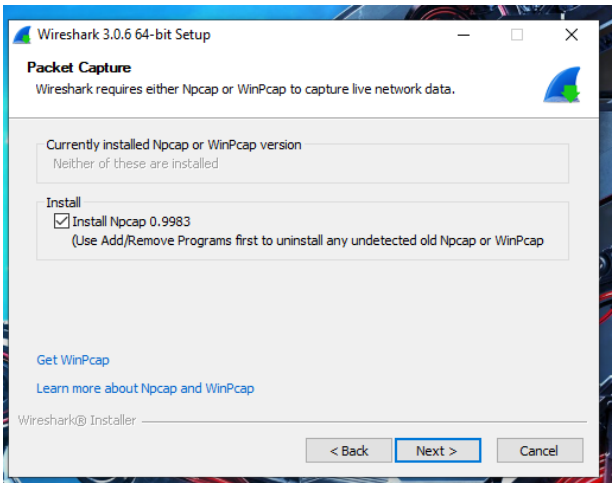
- Choose desired shortcut options, then click “Next”



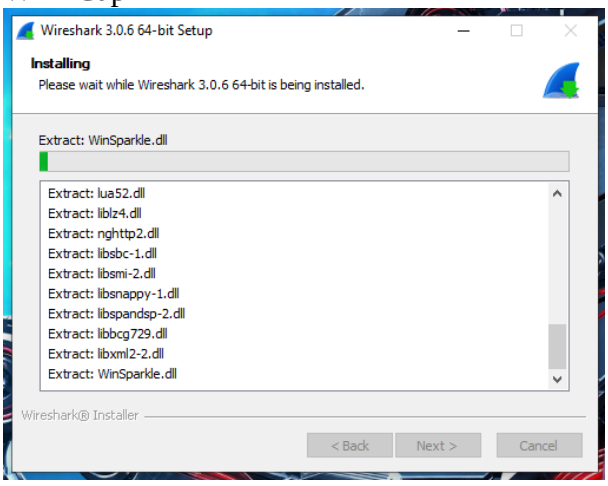
- Choose your destination folder, then click “Next”



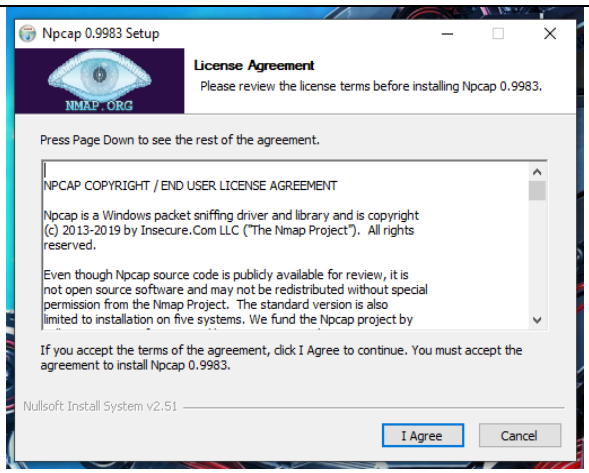
- Ensure box is selected to install WinPCap, then click “Install”



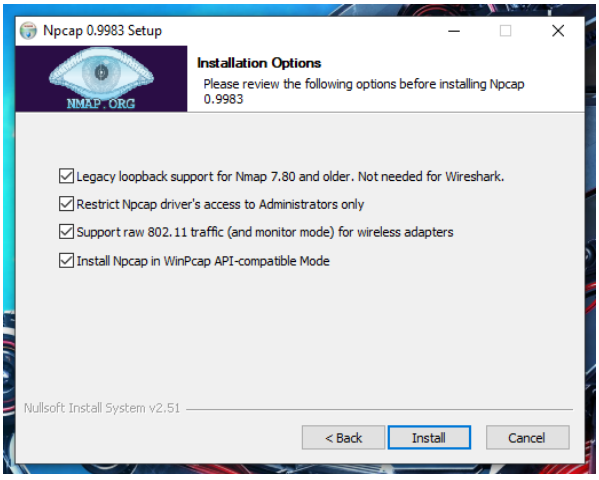
- Wireshark will begin to install, self-interrupting midway to install WinPCap



- Click “I Agree”

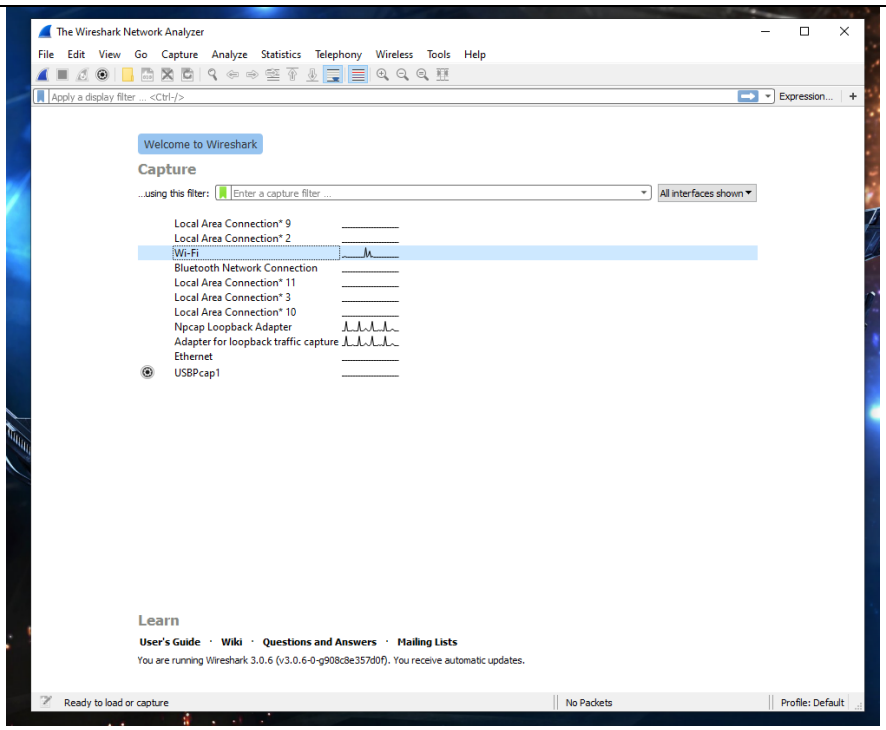


- Click “Install”

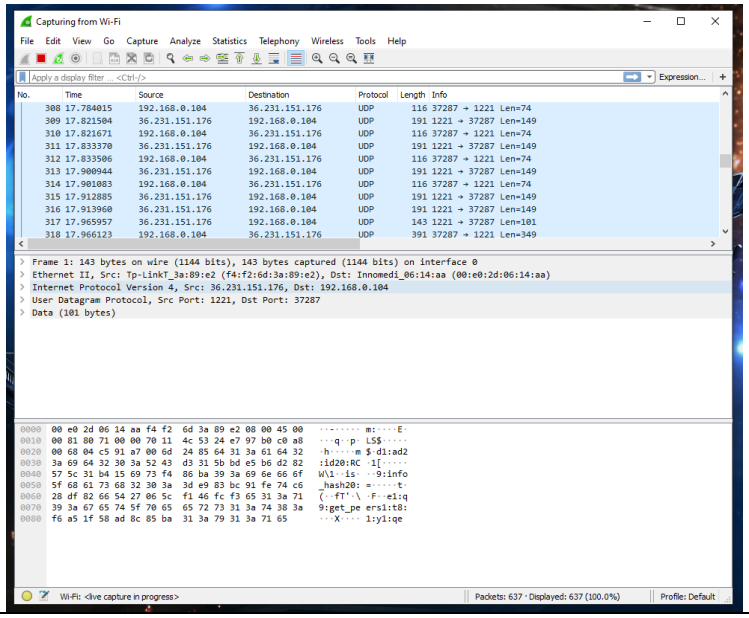


- Using Wireshark for Wireless Packet Capture:

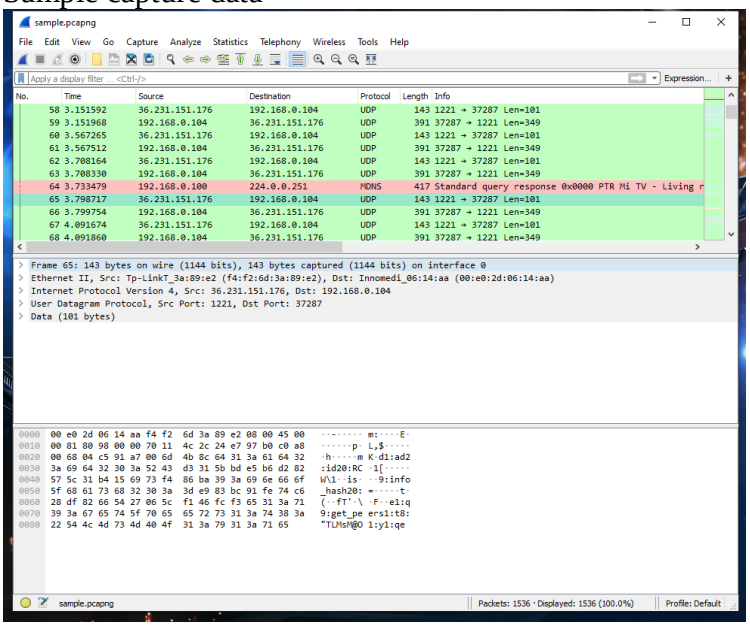
Now that the software is installed and the hardware is connected, it is time to start using Wireshark.



- Capture should begin automatically. If no packets are being displayed, you may need to minimize then maximize the window.

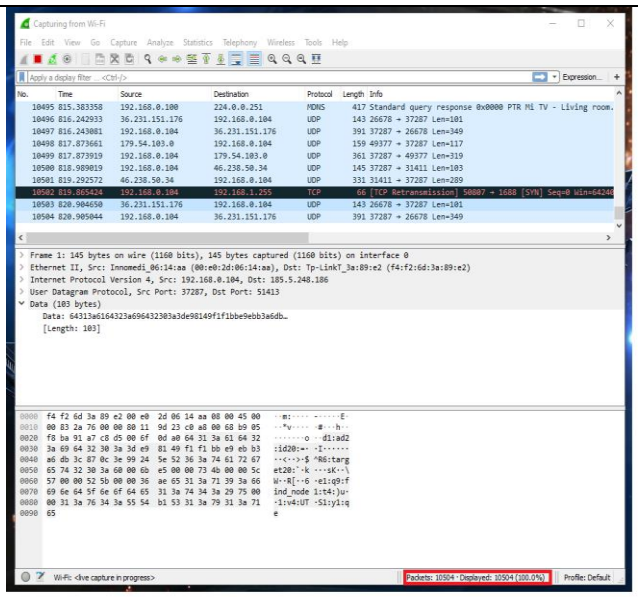


- Sample capture data



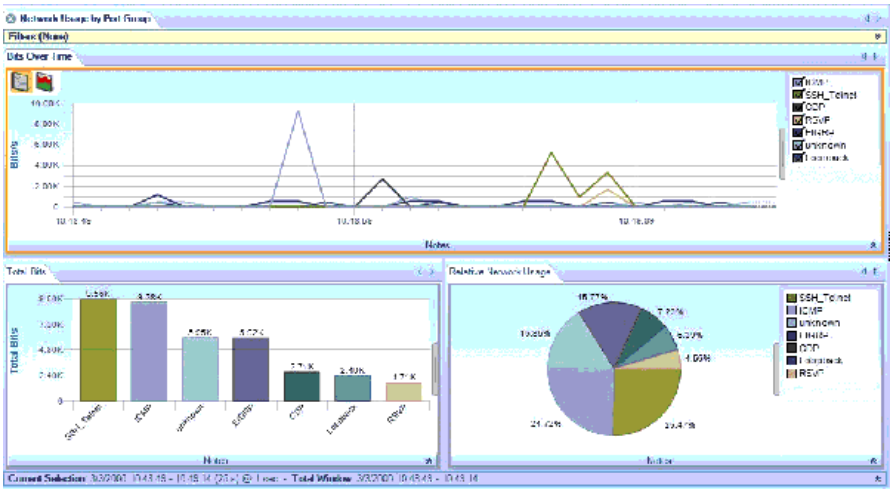
- In the capture window, several key pieces of data are available. "Time" represents the number of seconds that passed after capture was initiated until that packet was caught.
- "Source" and "Destination" provide the user with key packet information, and may include a specific IP address, a router, or a broadcast message.
- The color coding for each packet is determined by the "Protocol" type, and makes certain common protocols easier to identify.
- Packet Analysis:

To show how to perform a detailed analysis of captured packets, data from a **10-minute** capture session is used. During the course of this capture session, nearly **10504 packets** were captured, of strictly broadcast type traffic. Filters can be applied to reduce the volume of information to cover only the packets of interest.



Captured Packets

- Packet captured from **05 Nov 2019, 10:25PM to 10:35PM**



Conclusion	In conclusion, Wireshark is a very effective tool for gathering information about clients by analyzing the packets. We learned the basics of how to capture a packet.

CONCLUSION

The main focus of our Assignment is to understand how two systems communicate with each other along with the study the use of Hubs and Switches and learn how a packet of data from source to destination
In this assignment we have also used NP Zenmap UI which helps us learn how ports are connected inside a server and also tells us which ports are vulnerable to risk

The Assignment "CISCO PACKET TRACER" displays the different ways in the data signals can be transmitted from one computer to another over a transmission medium. While performing these experiments we learnt all the problems faced and errors caused during the execution of the experiments. We also have understood how the transmission occurs between two computers.

BIBLIOGRAPHY

Offline Source:

- Cisco Packet Tracer student version

Online Source:

- www.nmap.org
- www.tutorialspoint.com
- www.geeksforgeeks.com