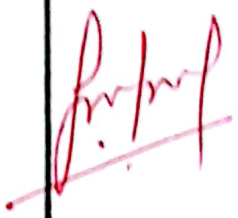
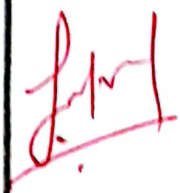
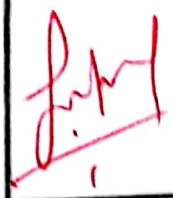
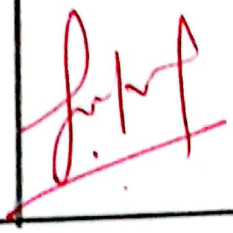
TABLE OF CONTENT

SN	Name of Project	Date	Page	Remarks
11.	Network Design with web server, switch & end devices to implement the DNS & DHCP protocol implementation.			
12.	configuration of router to connect two diff. networks having network address: 192.168.2.1 & 192.168.1.1. Also implement RIP protocol.			
13	Case study of wire shark tools with properties & result.			
14.	Network command in Linux based machine			

LABSHEET-1.

TITLE: Identify the networking cable

Objectives: To create and test Cable.

Components:
- → 2 pcs RJ45
- → cat6 cable(Wire)
- → Crimper
- → Tester

Process:

Step1: Cut the cable to desired length.

Step2: Strip the cable to expose the wires.

Step3: Untwist the wire pairs and remove the string and separator if necessary.

Step4: Organize the wires in the correct order of color code as: Half orange
Full orange
Half Green
Full Blue
Half Blue
Full Green
Half Brown
Full Brown
and trim the wires to same length.

Step5: Place the wire ends into the RJ-45 connector.

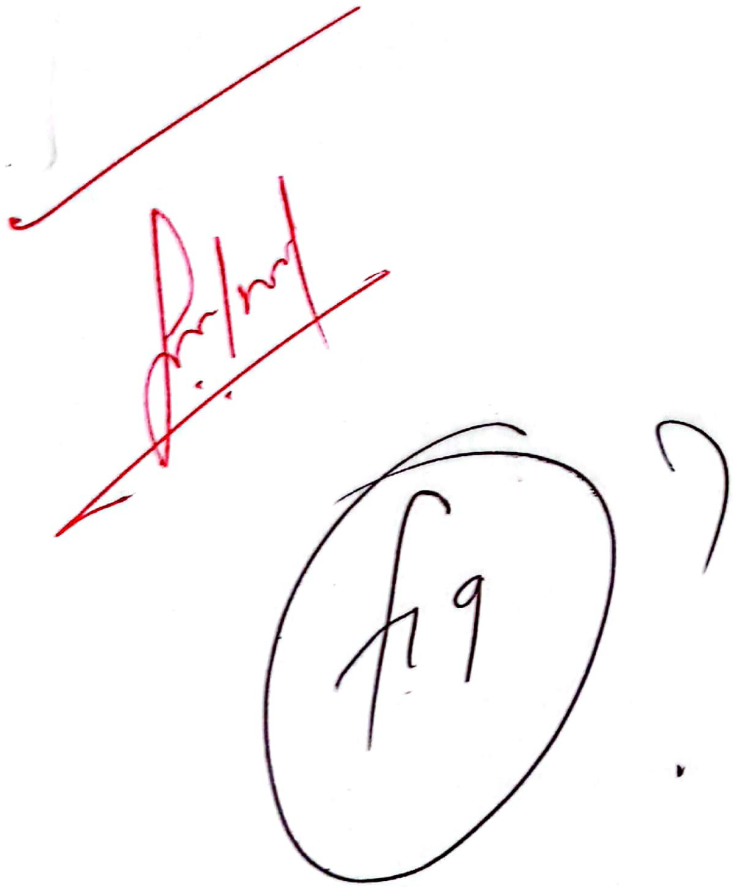
Step6: Ensure the wire ends reach to the end of the RJ-45 connector.

Step7: Crimp the RJ-45 connector to the cable.

Step8: Test the cable for continuity.

Output: When both the RJ-45 connector is inserted at the tester, all 8 signals starts to light up simultaneously, if and only if all the process has been done perfectly.

Conclusion: In this way, we can create and test cable to share data.



LAB-SHEET 2.

. Name of the experiment - To identify the networking devices with their function and uses.

) Name of the device: ROUTER

Definition: Any device, physical or virtual, that transmits data between two or more packet-switch computer networks is reffered to as a router. A router, examines the Internet Protocol (IP) address of a particular data packet's destination, determines the most effective route to take it there, and then forwards the packet in accordance with its findings. A typical kind of gateway is a router. It is situated at each point of presence on the internet where two or more networks converge. On its trip from one network to the next and to its destination, a single packet may be sent by hundreds of routers. Routers are categorized as network layer devices in the open systems Interconnection (OSI) paradigm (layer 3)

Pictorial Representation:

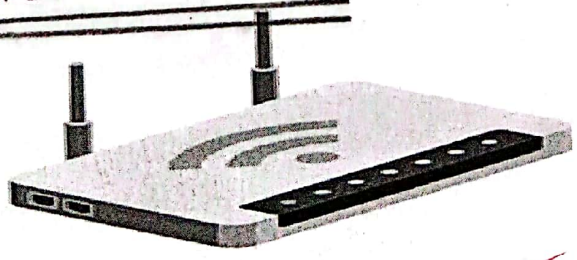


figure of Router.

Uses of Router:

- To ensure that data is flowing to the correct destination, such as when emails are sent to the correct internet provider and recipient.
- To protect against unwanted data, such as enlarge files, which are distributed to each machine over the network, and to improve network performance.

It acts as a buffer between the modem and the network, and it also allows software security to reduce the risk of viruses and other malware.

To share information with other routers connected to the network.

Function of router:

It evaluates incoming packet network address and determines which interface to forward the packet to.

It makes decisions based on its local routing table.

Routers plays a critical role in segmenting the internet network into internal network in residences or businesses.

The primary function of a router is to route web traffic dedicated for the internet outside of the internet network as a safety precaution. It also aide in ignoring data damage caused by a data packet flowing to the incorrect network.

Routers also assist many users in sharing resources such as faxes, scanners, printers, and file folders on remote ~~devices~~ drives.

Name of the device : HUB

Definition- A hub is a physical layer networking device that connects several networked devices. They are typically employed to link computers together in a LAN. A hub contains a lot of ports. A computer is inserted into one of these ports with the intention of joining the network. Data frames are broadcast to all other ports when they arrive at a port, regardless of whether they are headed there or not. Every computer or Ethernet-based device linked to a network hub receives data linked to all of these devices.

Pictorial Representation

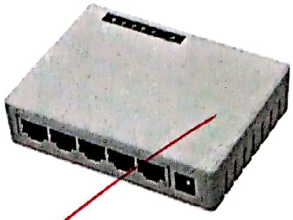


figure of HUB.

Uses of HUB:

Hubs are used to create small Home networks.
Hubs are used for monitoring the networks.
Hubs are used in organizations and computer labs for connectivity.
It makes one device or peripheral available throughout the whole network.

Functions of HUB:

A hub connects network devices in a LAN centrally and arranges them in a star pattern.
It has the ability to monitor data and select the first packet to send.
When sending packets, it can fix broken ones.
It can alert when issues like excessive collisio arise by converting weak but readable signals into stronger signals before sending them on to the ports.

2) Name of the device: SWITCH

Definition- A multiport device called a switch increases network effectiveness. The switch permits connections to hubs or routers while maintaining a minimal amount of routing information about internal network nodes. switches are typically used to link LAN strands. Switches typically have the ability to read the hardware addresses of incoming packets and send them to the correct location. Because switches have the ability to create virtual circuits, they are more efficient for networks than hubs or routers. switches also increase network security since it is more challenging to employ network monitors.

Pictorial resprosentation:

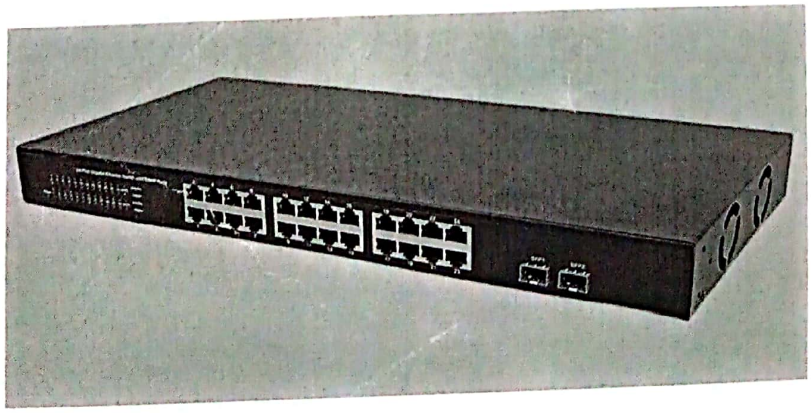


figure of switch.

Uses of SWITCH:

It connect multiple hosts as a switch provides a large number of ports for cable connections, allowing for star topology routing and it is usually used to connect multiple PCs to the network.

A switch in networking can manage traffic either coming into or exiting the network and can connect devices like computers and access points with ease.

A switch divides a LAN into multiple collision domains with independent broadband, thus greatly increasing the bandwidth of the LAN.

When a switch forwards a frame, it regenerates on undisorted square electrical signal which helps to keep the electrical signal undisorted.

Function of SWITCH:

Connects multiple hosts.
Forwards a message to a specific host.
Manage traffic.
Keep the electrical signal undistored.
Increase LAN bandwidth.

Name of the device: MODEM

Definition- MODEM full foorm is "Modulator - De modulator" that means It has ability to modulates and demodulates analog carrier signals for encoding and decoding digital data for executing. Modem is a hardware networking device that helps to make connection with computer or other hardware components like as switch or router for linking to internet. Many modems are variable-rate, permitting them to be used over a medium with less than ideal characteristics, such as a telephone line that is of poor quality or is too long.

Pictorial Representation:

Fig: Modem.

) Name of the device: MODEM

Definition- MODEM full foom is "Modulator - De modulator" that meam it hon ability to modulatos and demodulates analog carrier signals for encoding and decoding digital data for executing. Modem is a hardware networking device that helps to make connection with computer or other hardware components like an switch or router for linking to internet. Many modems are variable-rate, permitting them to be used over a medium with less than ideal characteristics, such as a telephone line that is of poor quality or is too long.

Pictorial Representation:

figure of Modem.

Uses of MODEM:

It allows computers to connect and share message photos, sound, videos, and more.

It translates the ASCII code into a format that can be sent to another location and then translates the code that comes in from other computers back into ASCII.

It is used to enable computers to communicate with each other over telephone networks.

It modulate and demodulate the network signals.

Functions of MODEM:

Modulated signals

Data compression.

Error correction.

Flow control.

Name of the device: BRIDGE

Definition- A bridge in a computer network is a device used to connect multiple LANs together with a larger local Area Network (LAN). The mechanism of network aggregation is known as bridging. The bridge is a physical or hardware device but operates at the OSI model's data link layer of two switches. The primary responsibility of a switch is to examine the incoming traffic and determine whether to filter or forward it. Basically, a bridge in computer networks is used to divide network connections into sections, now each section has separate bandwidth and a separate collision domain. Here bridge is used to improve network performance.

Pictorial Representation:

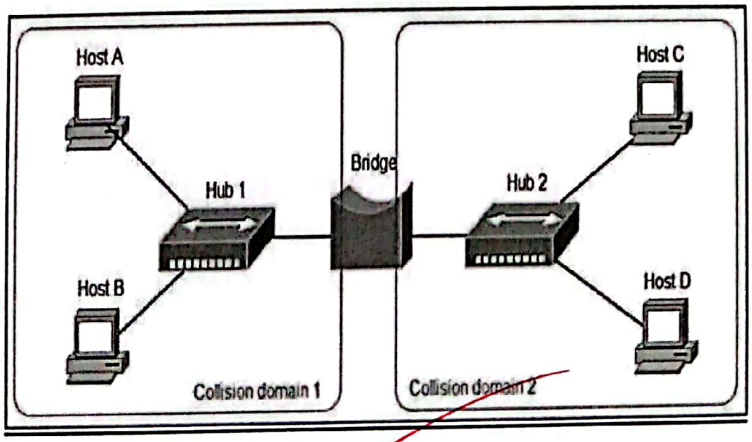


figure of Bridge.

Uses of BRIDGE:

- Bridges are used to increase the network capacity as they can integrate multiple LANs together.
- On receiving a data frame, databases use the bridge to decide whether to accept or reject the data.
- In the OSI model, it can be used to transmit the data to multiple nodes of the network.

Used to broadcast the data even if the MAC address or destination address is unavailable.

It forwards data packets despite faulty nodes.

Functions of BRIDGE:

The bridge is used to device LANs into multiple segments.

To control the traffic in the network.

It can interconnect two LANs with a similar protocol.

It can filter the data based on destinational MAC addresses.

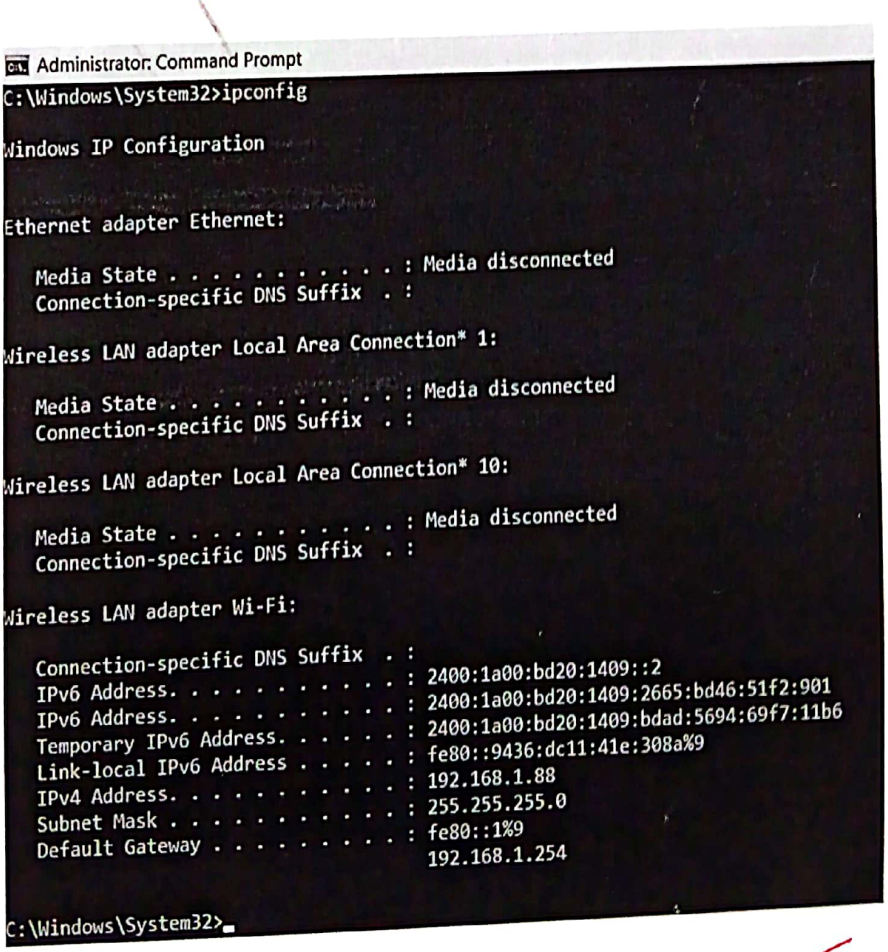
LABSHEET - 3

Name of the experiment : Basic networking command used in computer networks.

Name of the command : ipconfig

Description - Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

Screenshot :

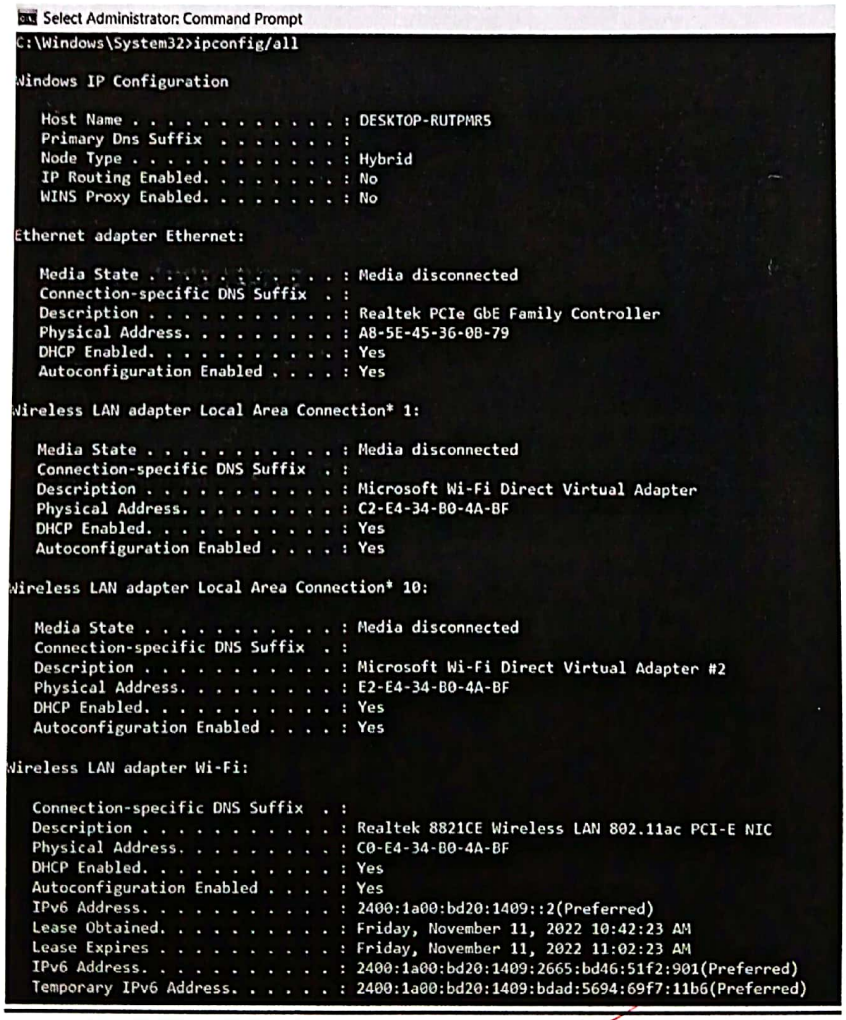


Screenshot of command ipconfig.

Name of the command: ipconfig /all

Description:- To show all the information about your network adapter. We will need to use your the network /all parameter. It is used to find out the physical Address, DHCP Enabled, IPv4 Address, Default gateway, DHCP server, DNS server, Link-local IPv6 Address as well as lease obtained.

screenshot:

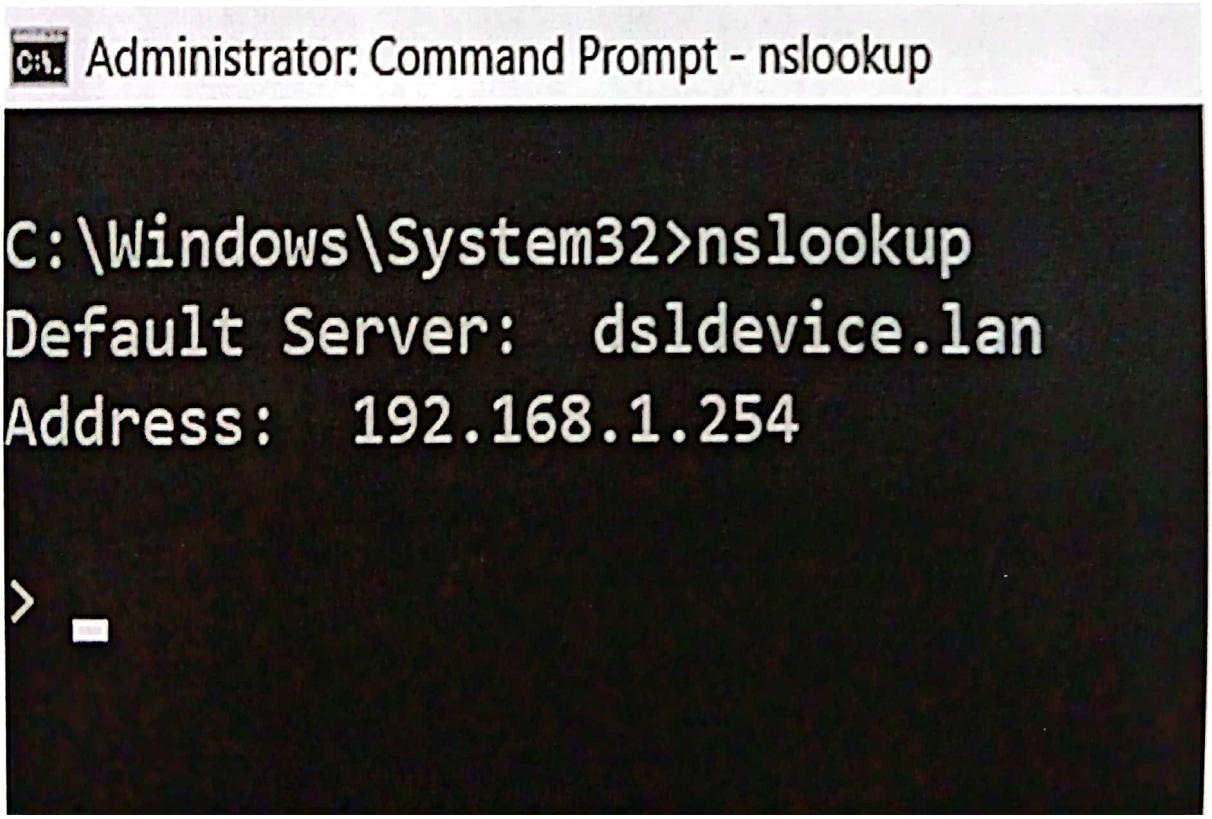


Screenshot of command ipconfig /all

Name of the command: nslookup

Description- Nslookup is typically a command-line tool, which means that it uses the command-line structure familiar to many users who have used older PC-DOS operating systems. In order to use command-line tools, users may have to shell out of a windows-based environment in order to access the command-line interface.

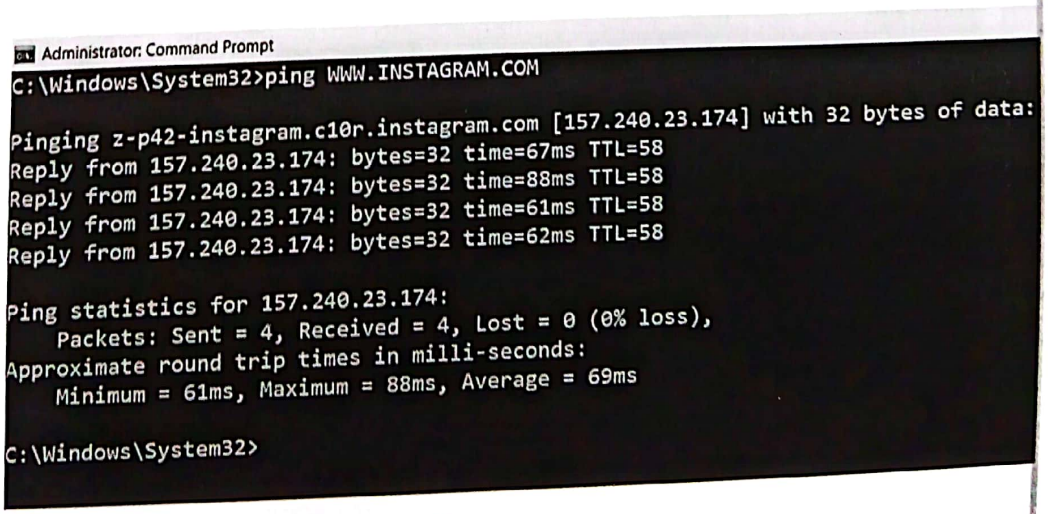
screenshot:



Name of the command : Ping.

Description- The ping utility relies on the Internet control message Protocol (ICMP) at the Internet layer of ICP/IP. Its most basic use is to confirm network connection between two hosts. Ping sends out an ICMP echo request to which it expects an ICMP echo reply response.

Screenshot:

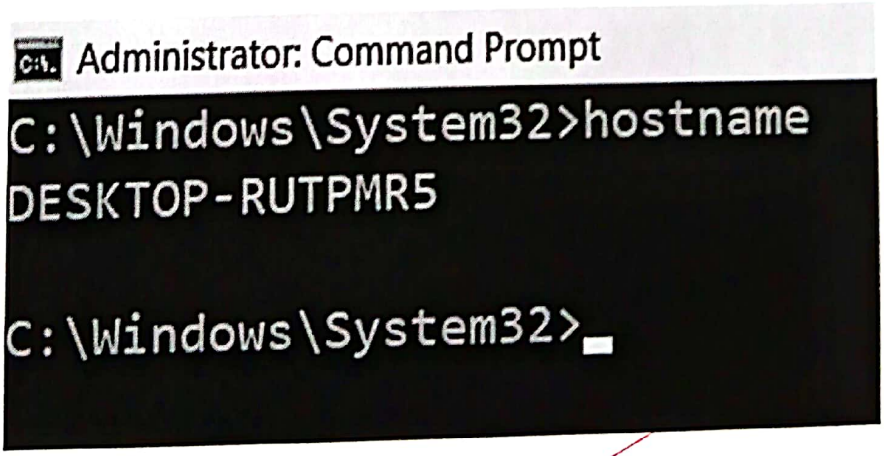


screenshot of command : ping.

Name of the command : hostname

Description- Hostname command is used to obtain the DNS (Domain Name System) name and set the system's hostname or NIS (Network Information System) domain name. A hostname is a name which is given to a computer and it attached to the network. Its main purpose is to uniquely identify over a network.

Screenshot:

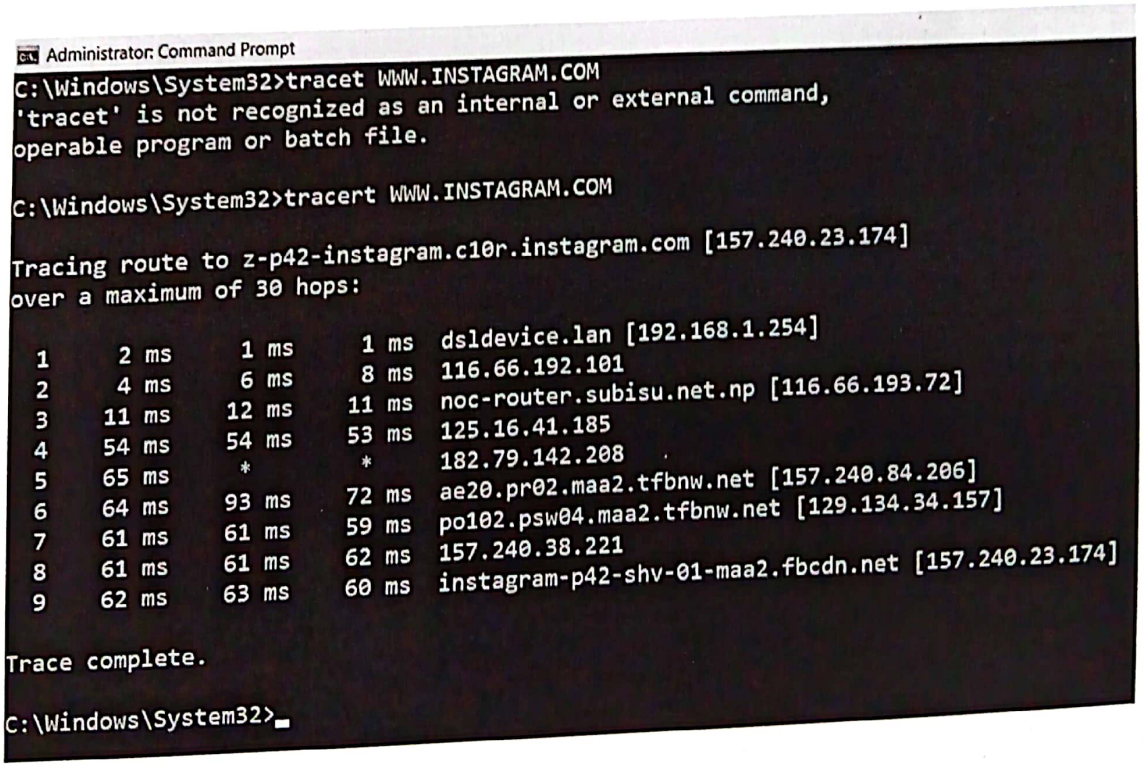


Screenshot of command : hostname

Name of the command : tracert

Description- The Trace route command (tracert) is a utility designed for displaying the time it takes for a packet of information to travel between a local computer and a destination IP address or domain. After running a trace route command, the results displayed are a list of the 'hops' that data packets take along their path to the designed IP address or domain. This command is commonly associated with the trouble shooting of connection issues.

Screenshot:

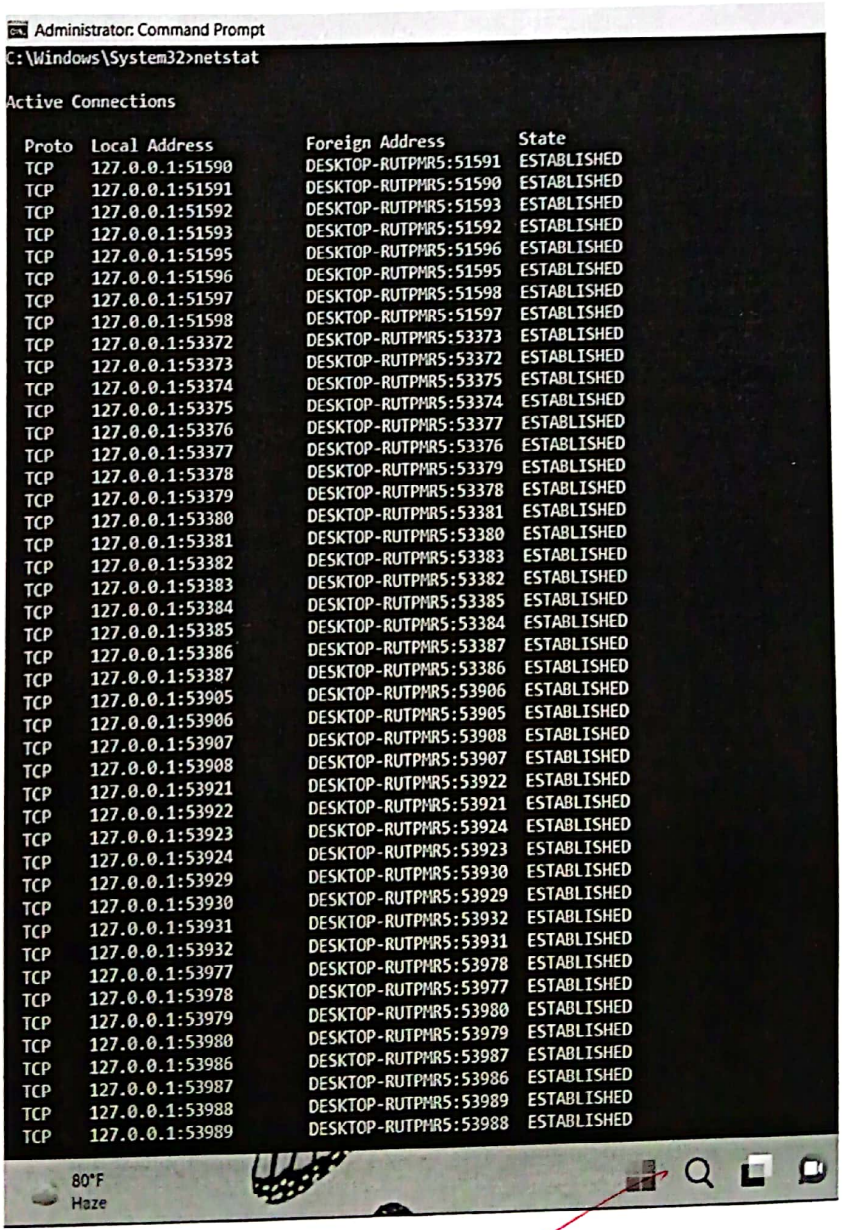


Screenshot of command : tracert.

Name of the command : netstat

Description - The network statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command let's take a look at some of the basic usage for netstat and the most used cases.

screenshot:-

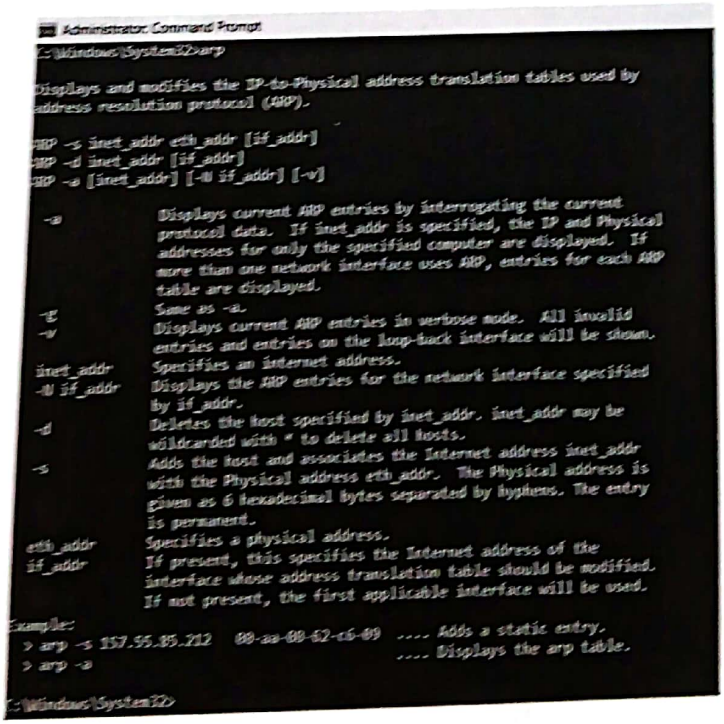


screenshot of command : netstat.

Name of the command: arp

Description - The arp command displays and modifies the Internet-to-adapter address translation tables used by the address in networks and communication management. The arp command displays the current ARP entry for the host specified by the HostName variable. The host can be specified by name or number, using Internet dotted decimal notation.

Screen shot:

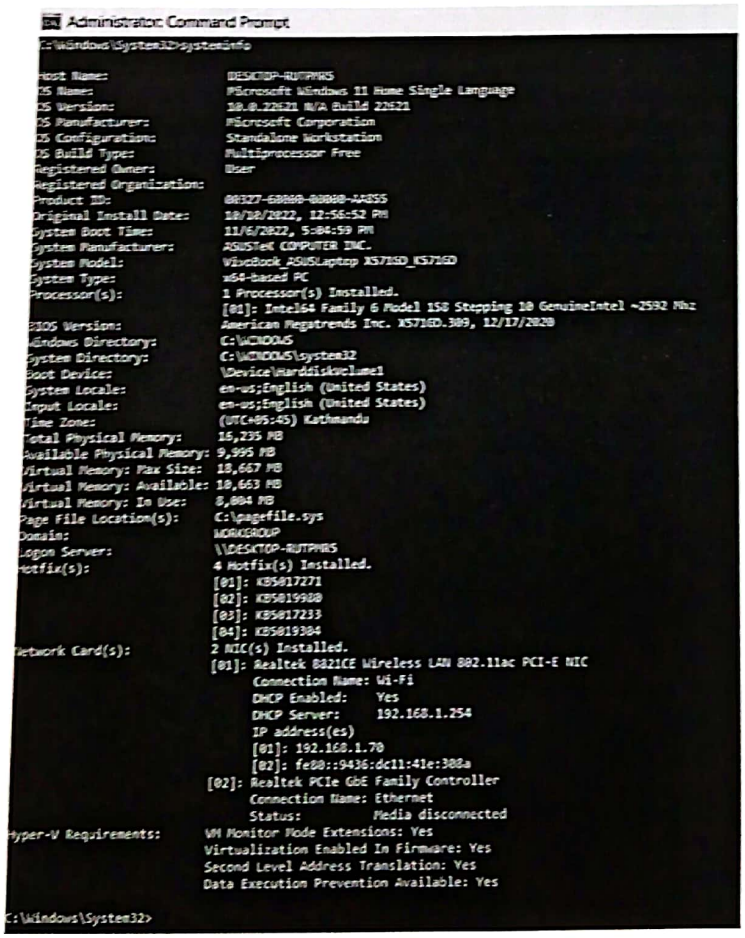


Screenshot of command: arp

Name of the command: system info

Description- It displays detailed configuration information about a computer and its operation system including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards.)

Screenshot:



Screenshot of command: systeminfo

Case Study

Tina Jha

World Wide Web

Executive Summary:

This is the case study about World Wide Web(WWW). World Wide Web (WWW) by the name the Web, the leading information retrieval service of the internet (the worldwide computer network). The World Wide Web refers to a group of web pages with a unique address hosted on a web server and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc.

It is an information system enabling documents and other web resources to be accessed over the internet. Documents and downloadable media are made available to the network through web servers and can be accessed by programs such as web browsers. Servers and resources on the World Wide Web are identified and located through character strings called uniform resource locators (URLs). The original and still very common document type is a web page formatted in Hypertext Markup Language (HTML). The invention of the World Wide Web made the internet accessible to everyone. It connects people who live in different parts of the world through social networks, websites, blogs, and much more. Development of W3 has created great positive impact on each an every sector such as business, education, entertainment etc.

This case study is being done to gain in-depth knowledge about world wide web. This case study will help to explore the history, it's importance and real life applications.

Background:

The World Wide Web (W3) was developed t be a pool of human knowledge, which would allow collaborators in remote sites to share their ideas and all aspects of a common project.

The Web was invented by English computer scientist Tim Berners-Lee at CERN, and originally conceived as a document management system. The first proposal was written in 1989, and a working system implemented by the end of 1990 including the World Wide Web browser and an HTTP server. The technology was released outside CERN to other research institutions starting in January 1991, and then to the general public on 23 August 1991. The

29/07/17

Web was a success at CERN, and began to spread to other scientific and academic institutions. Within the next two years, there were 50 websites created.

Originally, it was developed by him to fulfill the need of automated information sharing between scientists across the world, so that they could easily share the data and results of their experiments and studies with each other. CERN, where Tim Berners worked, is a community of more than 1700 scientists from more than 100 countries. These scientists spend some time on CERN site, and rest of the time they work at their universities and national laboratories in their home countries, so there was a need for reliable communication tools so that they can exchange information.

CERN made the Web protocol and code available royalty free in 1993, enabling its widespread use. After the NCSA released Mosaic later that year, the Web became very popular with thousands of websites springing up in less than a year. Mosaic was a graphical browser that could display inline images and submit forms, and HTTPd, a server that could process forms (see CGI). Marc Andreessen and Jim Clark founded Netscape the following year and released Navigator, which introduced Java and JavaScript to the Web. It quickly became the dominant browser. Netscape became a public company in 1995 which triggered a frenzy for the Web and started the dot-com bubble. Microsoft responded by developing its own browser, Internet Explorer. By bundling it with Windows, it became the dominant browser for 14 years.

Tim Berners-Lee founded the World Wide Web Consortium (W3C) which created XML in 1996 and recommended replacing HTML with stricter XHTML. In the meantime, developers began exploiting an IE feature called XMLHttpRequest to make Ajax applications and launched the Web 2.0 revolution. Mozilla, Opera, and Apple rejected XHTML and created the WHATWG which developed HTML5. In 2009, the W3C conceded and abandoned XHTML and in 2019, ceded control of the HTML specification to the WHATWG.

The World Wide Web has been central to the development of the Information Age and is the primary tool billions of people use to interact on the Internet.

Now, we have understood that WWW is a collection of websites connected to the internet so that people can search and share information. Now, let us understand how it works!

The Web works as per the Internet's basic client-server format as shown in the following image. The servers store and transfer web pages or information to user's computers on the network when requested by the users. A web server is a software program which serves the

web pages requested by web users using a browser. The computer of a user who requests documents from a server is known as a client. Browser, which is installed on the user' computer, allows users to view the retrieved documents.

All the websites are stored in web servers. Just as someone lives on rent in a house, a website occupies a space in a server and remains stored in it. The server hosts the website whenever a user requests its Web Pages, and the website owner has to pay the hosting price for the same.

The moment you open the browser and type a URL in the address bar or search something on Google, the WWW starts working. There are three main technologies involved in transferring information (web pages) from servers to clients (computers of users). These technologies include Hypertext Markup Language (HTML), Hypertext Transfer Protocol (HTTP) and Web browsers.

HTML is a standard markup language which is used for creating web pages. It describes the structure of web pages through HTML elements or tags. These tags are used to organize the pieces of content such as 'heading,' 'paragraph,' 'table,' 'Image,' and more. You don't see HTML tags when you open a web page as browsers don't display the tags and use them only to render the content of a web page. In simple words, HTML is used to display text, images, and other resources through a Web browser.

A web browser, which is commonly known as a browser, is a program that displays text, data, pictures, videos, animation, and more. It provides a software interface that allows you to click hyperlinked resources on the World Wide Web. When you double click the Browser icon installed on your computer to launch it, you get connected to the World Wide Web and can search Google or type a URL into the address bar.

Hyper Text Transfer Protocol (HTTP) is an application layer protocol which enables WWW to work smoothly and effectively. It is based on a client-server model. The client is a web browser which communicates with the web server which hosts the website. This protocol defines how messages are formatted and transmitted and what actions the Web Server and browser should take in response to different commands. When you enter a URL in the browser, an HTTP command is sent to the Web server, and it transmits the requested Web Page.

When we open a website using a browser, a connection to the web server is opened, and the browser communicates with the server through HTTP and sends a request. HTTP is carried over TCP/IP to communicate with the server. The server processes the browser's request and

sends a response, and then the connection is closed. Thus, the browser retrieves content from the server for the user.

Case Evaluation:

I imagined the web as an open platform that would allow everyone, everywhere to share information, access opportunities and collaborate across geographic and cultural boundaries.

In many ways, the web has lived up to this vision, though it has been a recurring battle to keep it open. But lately, I've become increasingly worried about negative impacts caused by W3, which I believe we must tackle in order for the web to fulfill its true potential as a tool which serves all of humanity.

We've lost control of our personal data. The current business model for many websites offers free content in exchange for personal data which are then sold or used to advertise their products by tracking our each and every move online.

It's too easy for misinformation to spread on the web. Today, most people find news and information on the web through just a handful of social media sites and search engines. These sites make more money when we click on the links they show us. And, they choose what to show us based on algorithms which learn from our personal data that they are constantly harvesting.

Nowadays people are addicted to W3 and remain socially disconnect as they decrease the time they go out and stays on the WWW for too long, which also creates the vision problems, weight gain etc. The problem of spamming and virus infections to the system has rapidly increased these days.

Similarly, there are other problems of W3 which creates inconvenience to the user such as slow search result, danger of overload and excess information, difficult to filter and prioritize information, no quality control over the available data, out-dated data and net overload due to large number of users.

Proposed solution:

In this section we will discuss about the possible solutions to before-mentioned drawbacks. They can be used to enhance user experience by pointing out the quality information and include semantic information, personalization and trust metrics.

Loss of our personal data is the great threat to humankind as there is no privacy maintained. Many business companies are trading our personal information with different motives such as advertising, earning money, blackmailing and many other to which victim is always an end-user. So to eliminate this problem development of web pages should be secure and other security measures should be implemented and also strict rules and regulation on data security should be implemented.

The problem of spreading of false information is also a huge problem which can create a conflict among people. There are laws regarding the misinformation but are not much effective. So its in our hand how and from whom and where we take information in W3. To prevent fake information we should always look for credible source, do fact check, discuss with our friends, cross check in multiple sites about the topic.

WWW has made people addicted towards social media and many other entertainment platforms making people isolated in a single room. So the user should be conscious about their physical health and valuable time being wasted on unproductive stuffs. We should promote social activities, encourage communication and dialogue in the family, encourage interests like sports, reading, etc.

Similarly, W3 should work on adding more servers, updating and managing data to eliminate the problems of slow search result, outdated and low quality data, which will hopefully reduce the user inconvenience.

Conclusion:

The WWW is an important and great informatics technology that has a significant impact on each and every sector as it offers a lot services. World Wide Web offers the availability of information from anywhere and makes friends from across the globe, World Wide Web reduces the cost of disclosure, It rapids interactive communication which can be used for different services, It offers a low cost of initial connection, It can facilitate the establishment of professional contact, It facilitates access to different sources of information, which is continuously updated, and it has become the global media. It connected the world in a way that made it much easier for people to get information, share, and communicate. It has since allowed people to share their work and thoughts through social networking sites, blogs, video sharing, and more.

So, the resulting impact depends on how we use it, using it wisely is a very much productive where as being addicted and improper use will result drastic problem physically, mentally, economically and socially.

Recommendation:

Today's, World Wide Web plays an important role in every person's life. It makes it easier to get any kind of information online. Even you can also communicate with anyone from anywhere.

I would recommend the best possible ways to use WWW as it has lot to offer. Using it the best way can result in higher productivity and profit. The ideal use of WWW is for communication, online conference call or live meeting which allow us to work remotely in an efficient manner as we ca communicate from distance and share data and information. Students may also use for online classes or learning. With the use of we can get news worldwide instantly (24X7) and we can operate online business.

Similarly, Its helpful in performing research works, professional works, publicity and advertising, entertainment, etc. To sum up there are lot of benefits and ideal ways to use the WWW for best possible outcomes.

Implementation:

A pragmatic approach for sharing manufacturing services across the Internet has been developed and shown to provide significant advantages in cost, accessibility, flexibility, and ease of use by end users. As the Web grows and its supporting infrastructure improves, delivering high-quality manufacturing services in this manner should become increasingly straightforward across the Web. Web technology and Web inter connectivity are becoming ubiquitous. Other experiments at putting engineering, design, and manufacturing services on the Web are so successful that we believe we should rethink the traditional approaches and tools for coordinating large, distributed teams. We also need to think about changes and extensions required to enable the underlying Web protocols to provide better performance, security, and reliability, as well as about the best way for Web protocols to work together with higher-level application programming interfaces and object protocols.

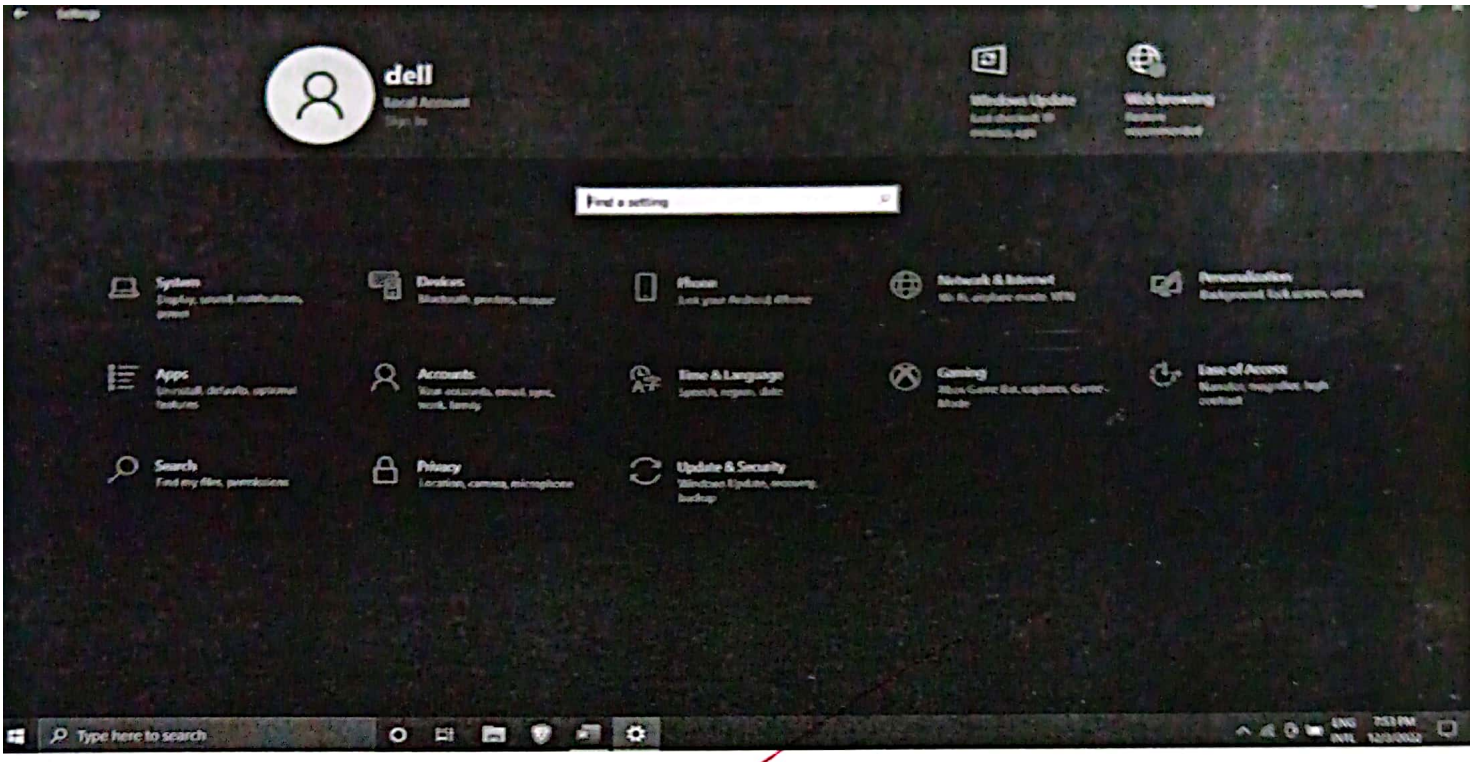
References:

https://en.wikipedia.org/wiki/World_Wide_Web

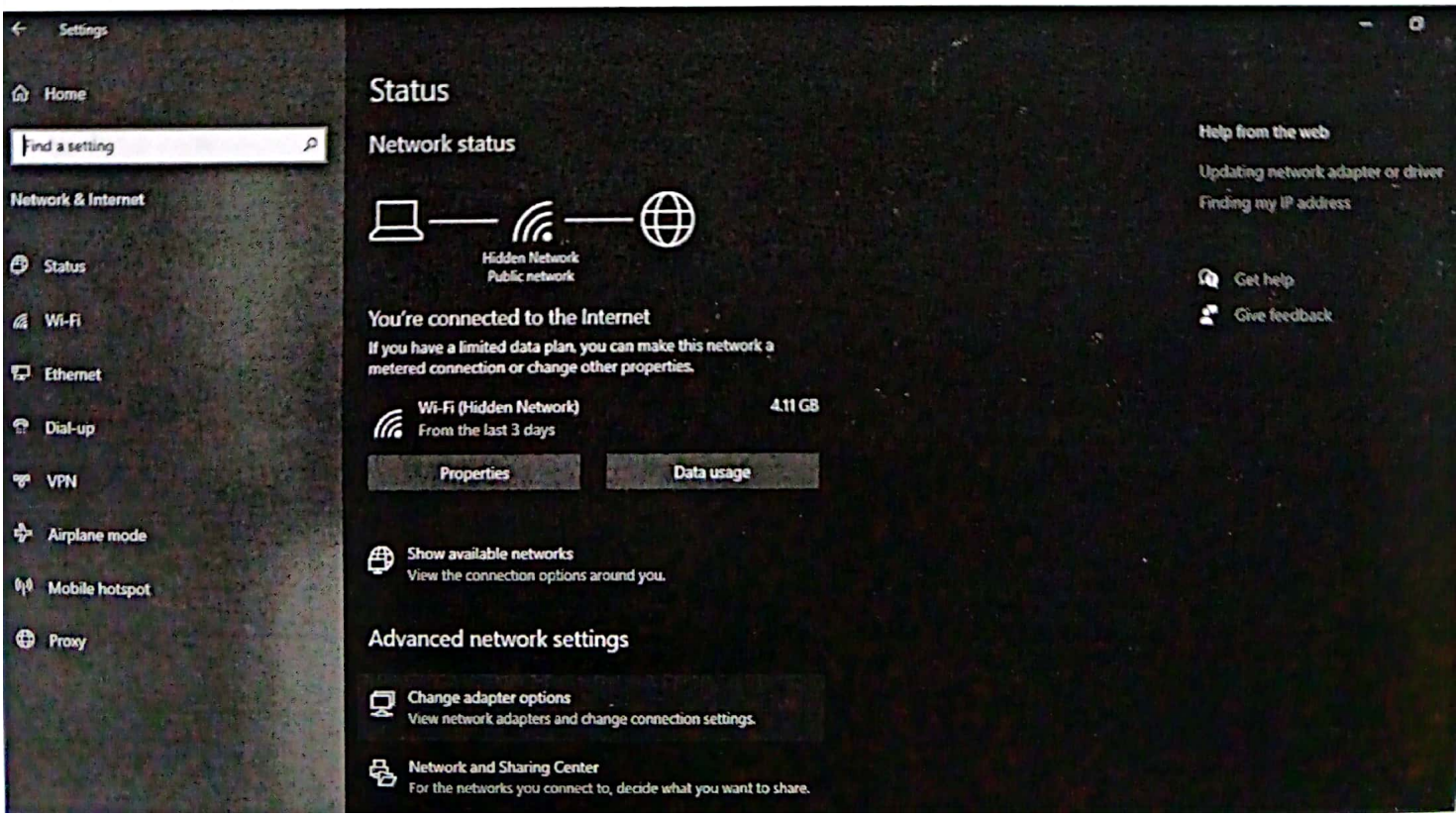
https://www.javatpoint.com/what-is-world-wide-web

https://scholar.google.com/

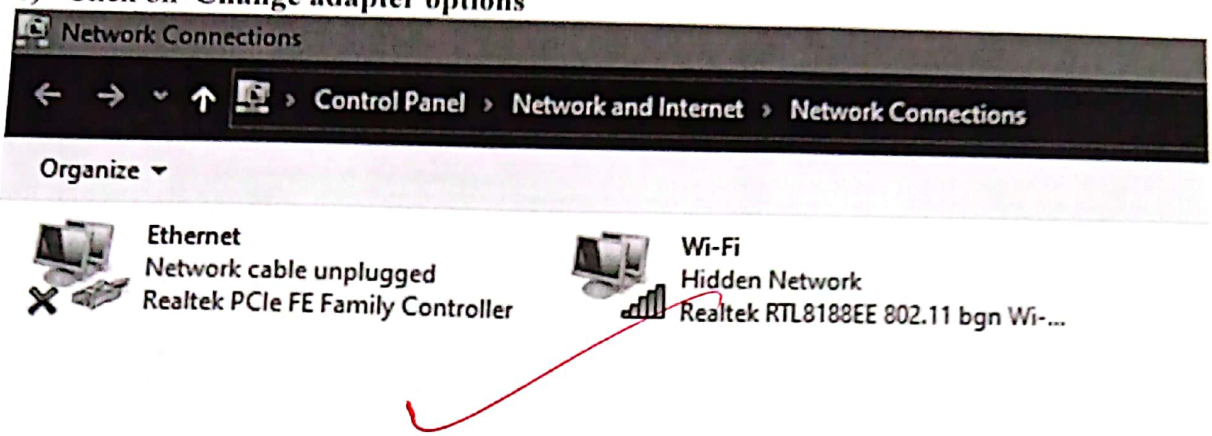
https://edifyclue.in/full-form-of-www/



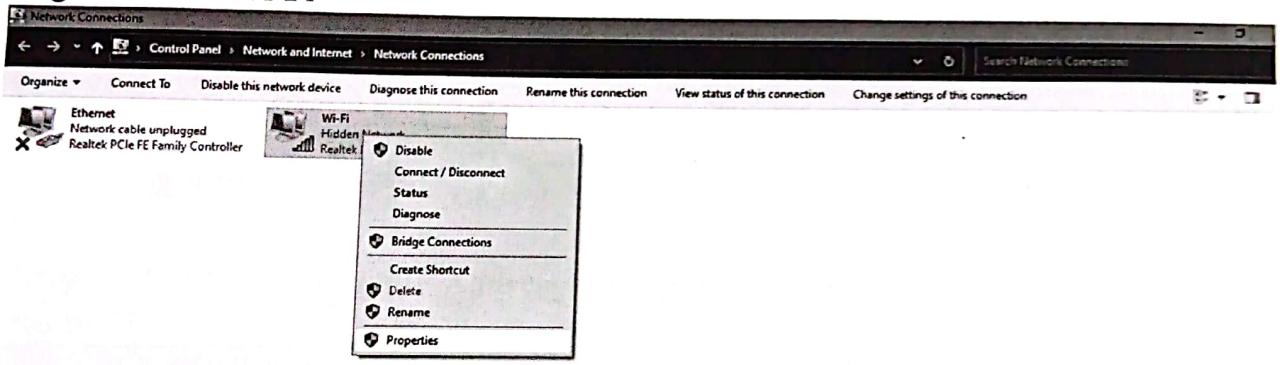
›) Click on **Network and Internet**



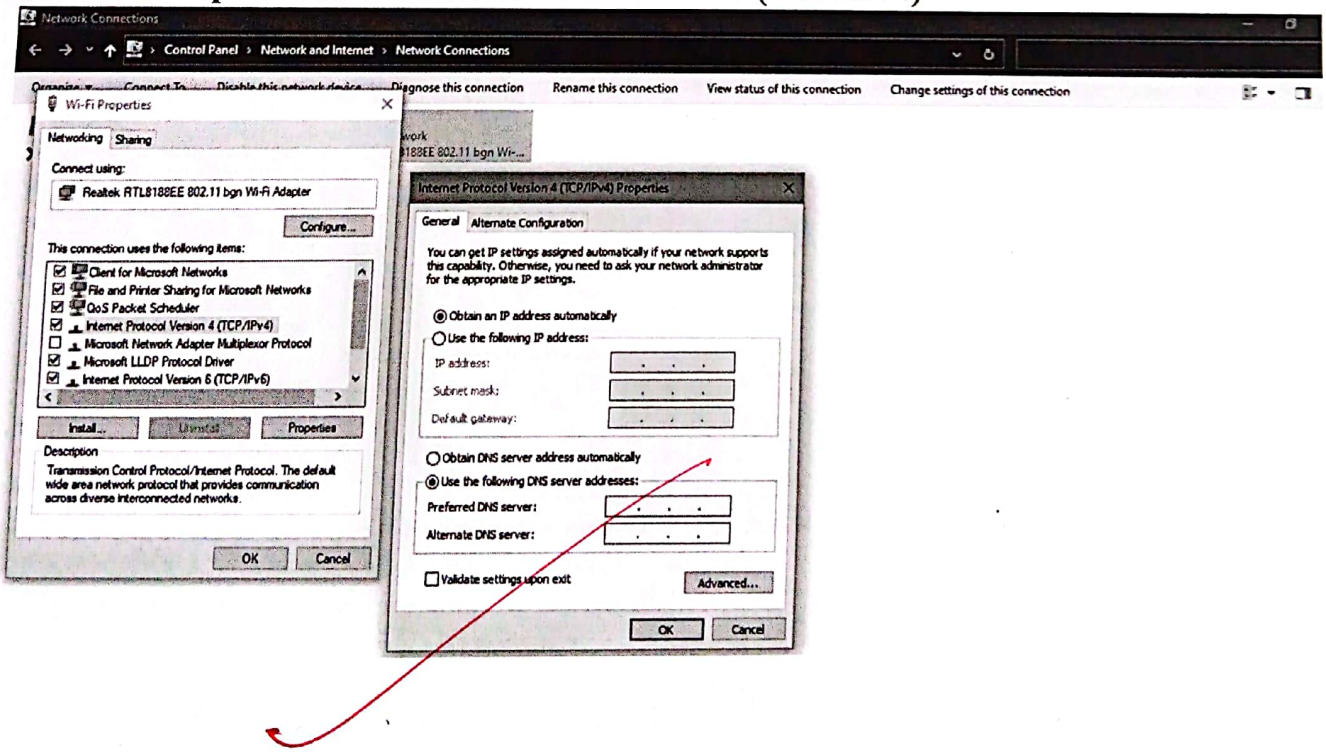
c) Click on **Change adapter options**

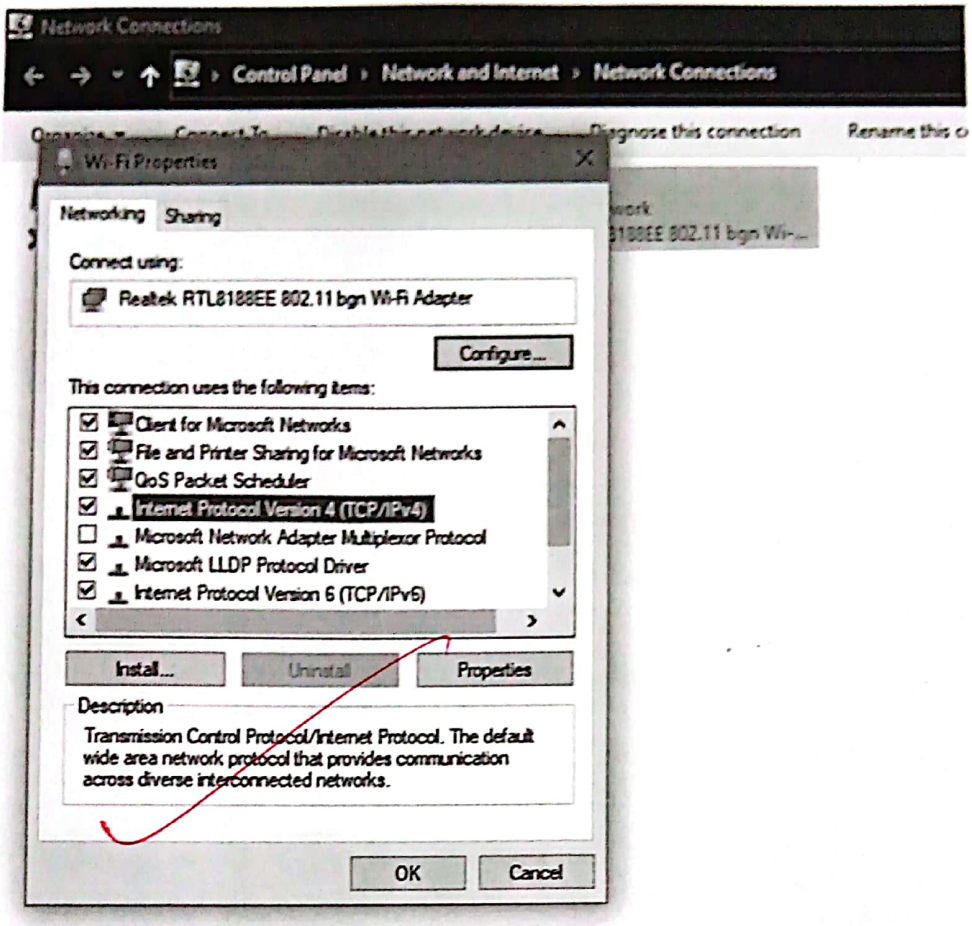


d) Right Click on **Wi-Fi**

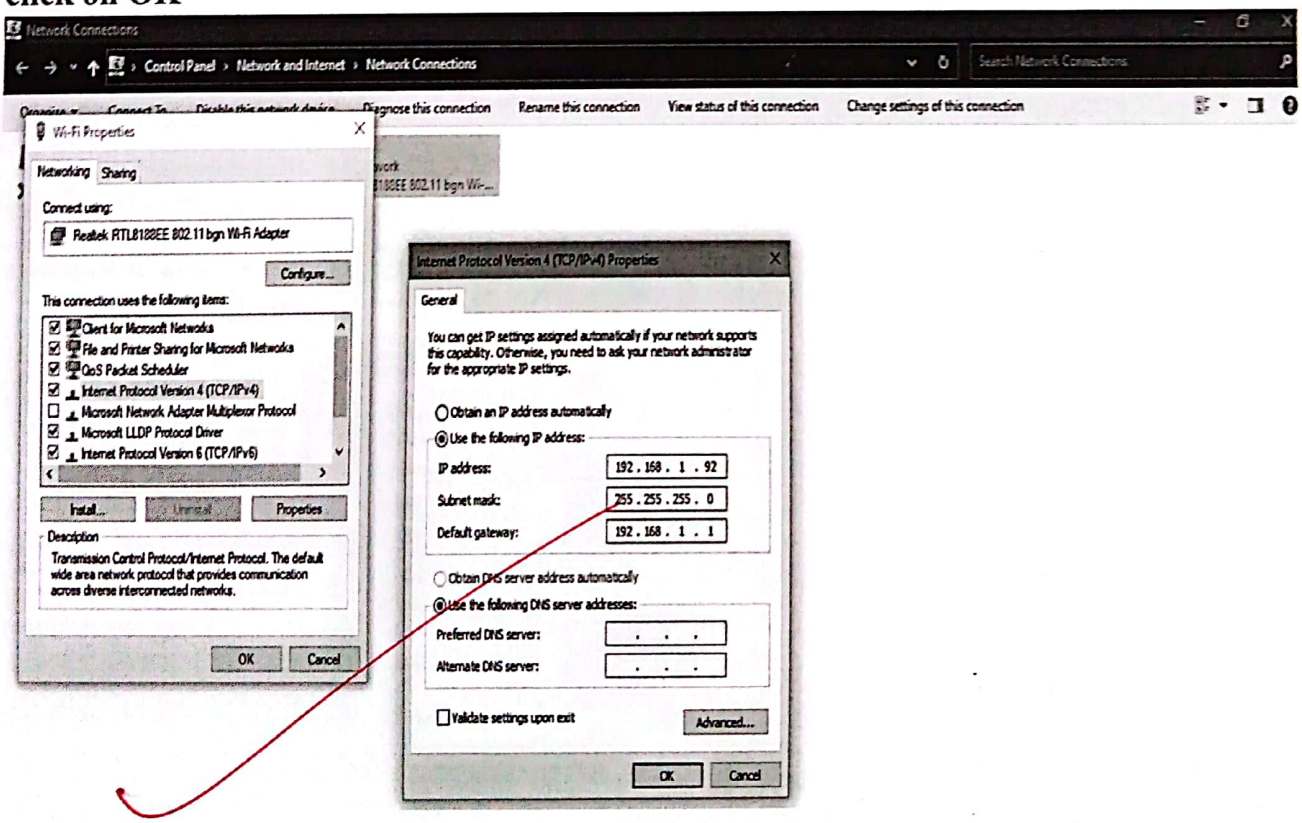


e) **Click on Properties > Internet Protocol Version 4 (TCP/IPv4)**

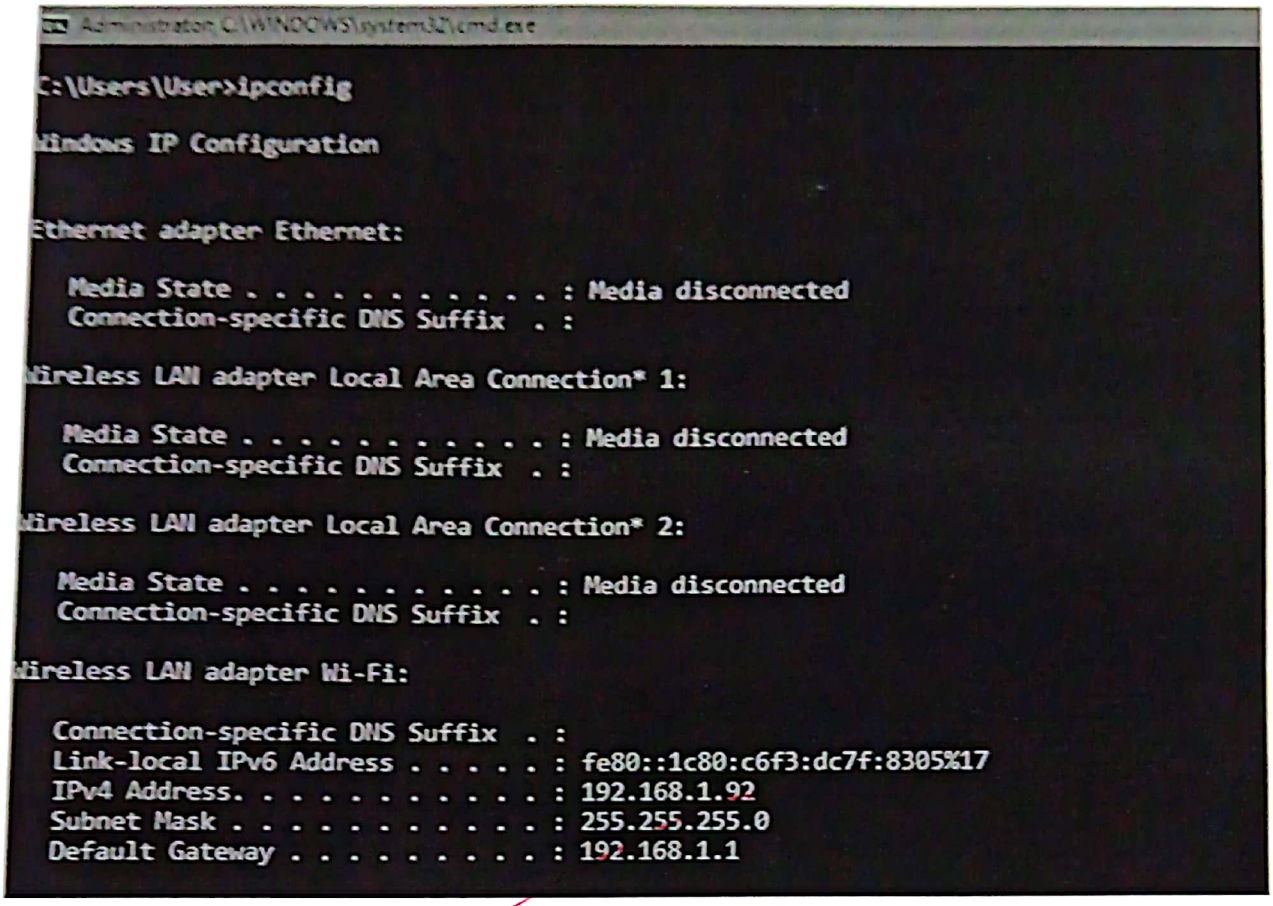




f) **Check on Use the following IP Address and input the IP address statically and click on OK**

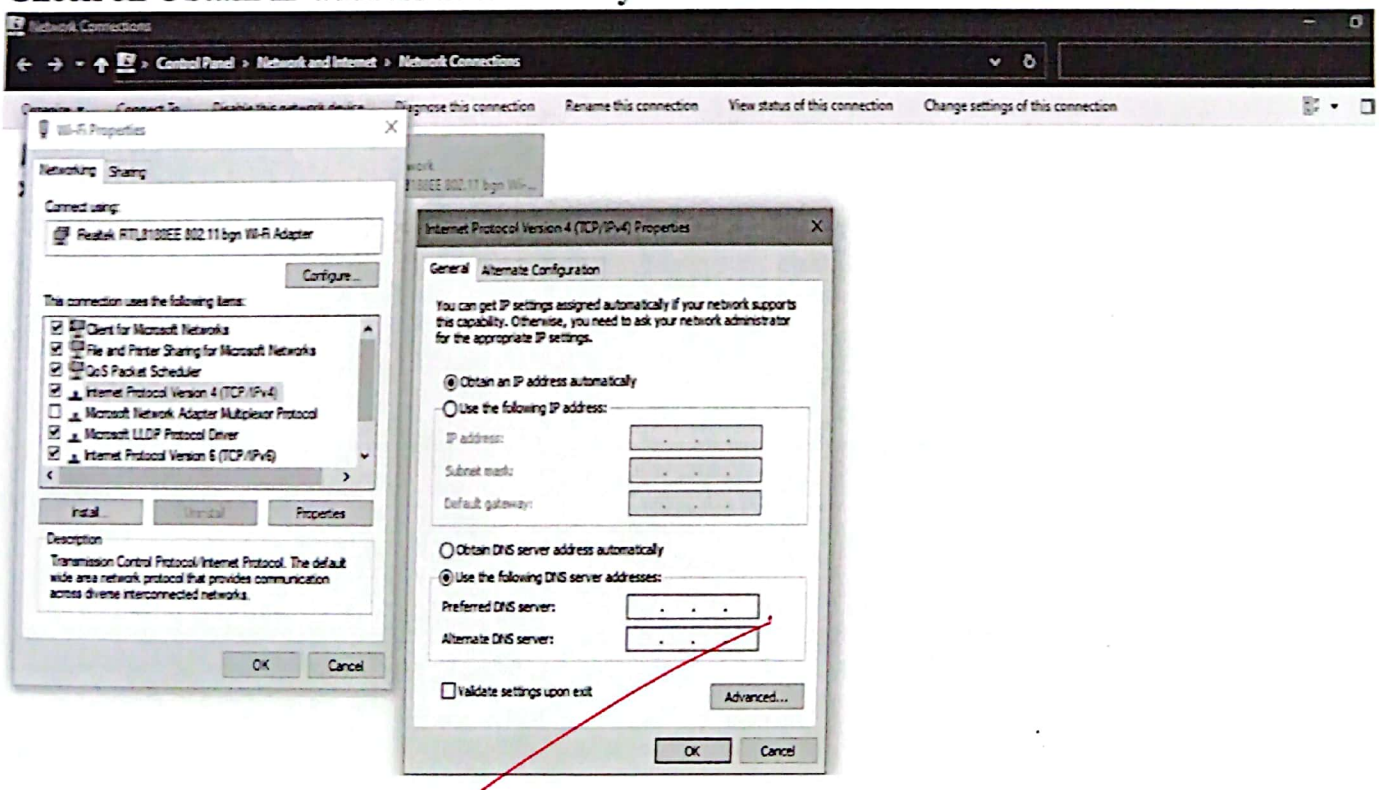


Result :

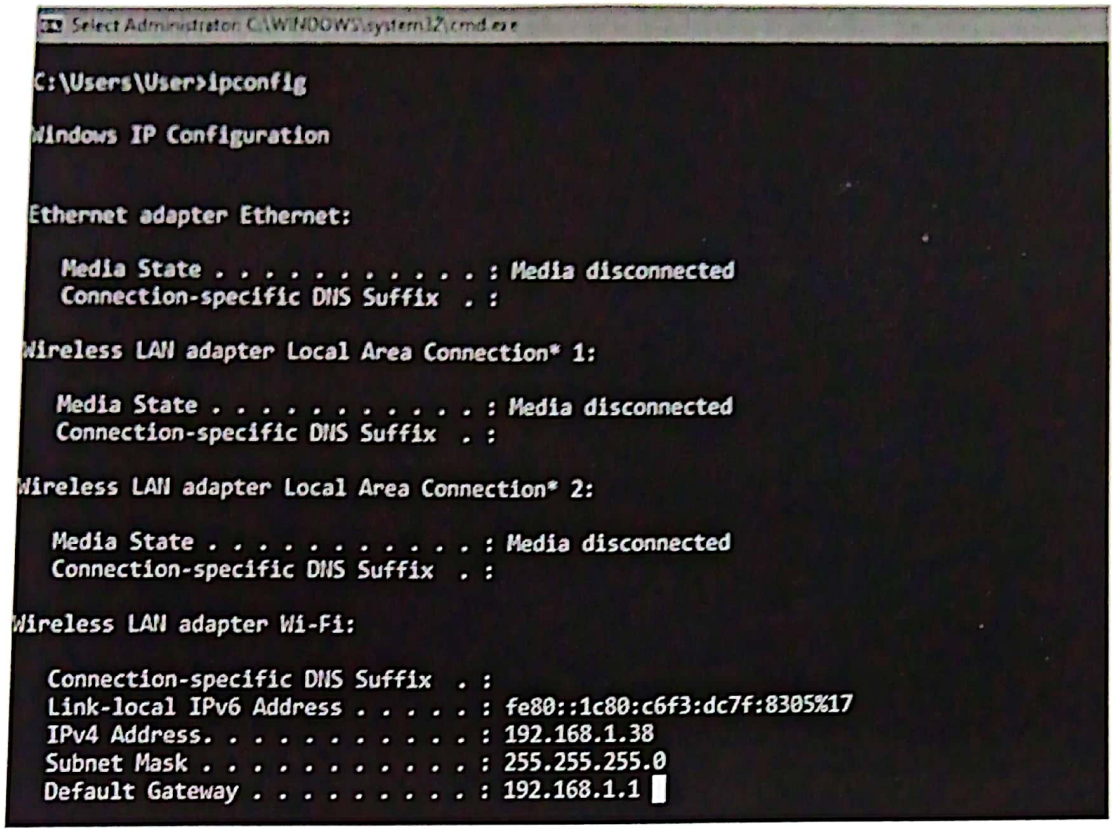


Dynamic IP addressing :

- Check on Obtain IP address automatically



Result :



LABSHEET-6

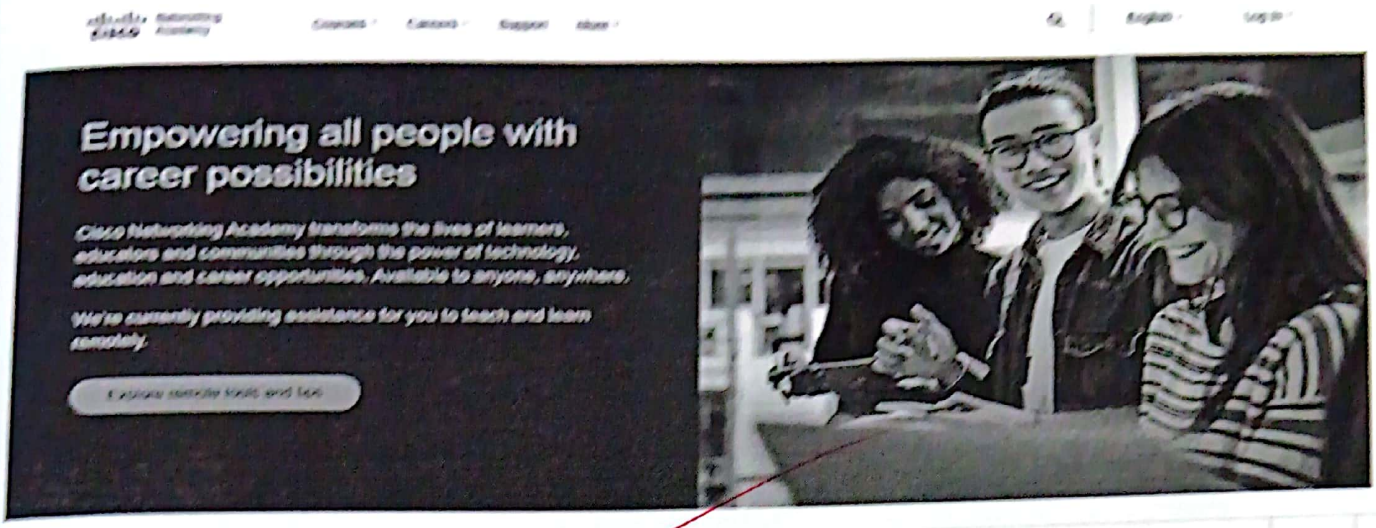
Configuration of Cisco packet Tracer and its functional uses.

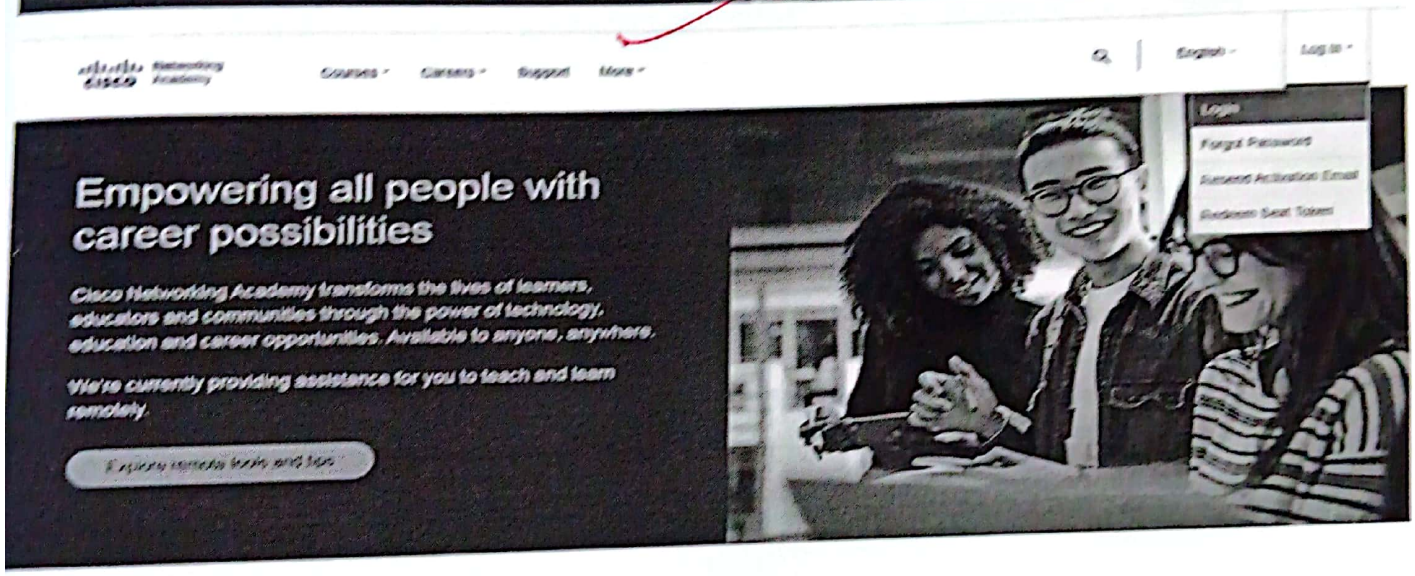
Packet tracer is computer software that is designed with the purpose of making network simulations to understand the networking and cyber security concepts in an easy way. It is built by Cisco corporation and is available for free for different OS like windows, MacOS, Linux, etc. It is easy to use with a simple interface.

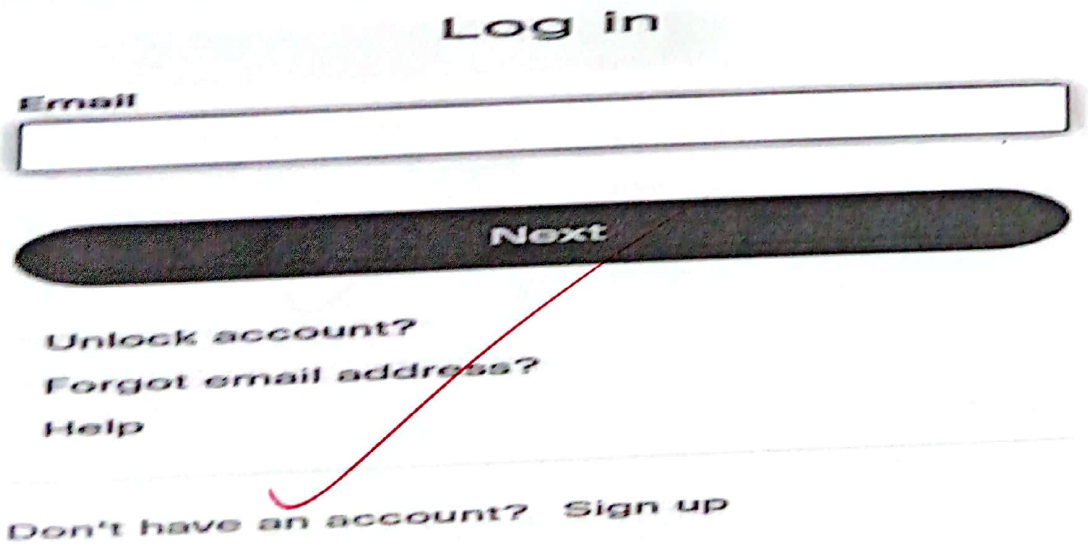
Installation steps of Cisco Packet Tracer.

Visit the official website of Netcad using any browser.
Press the login button and select log in option.
And then on other screen which appears, press sign-in option.
Enter Email, Password and other simple details and press on register.
Now the login window will apear enter your login credentials (email & password)
After loged in a dashboard will appear click on resources and choose download Packet tracer option.
choose the type of operating system you want to download the Packet Tracer.
After downloading check for the exe file in the system and run it.
They will appear a license agreement screen so click on I accept the license.
choose the installation location and press Next.
Select the start menu folder and press next.
check the box for create desktop shortcut and press next.
Press on Install button as packet tracer is ready to be installed.
The installation process will start and dont take time.
click on the finish button to complete installation.
An icon is created on desktop so run it.
Interface is initalized and the software is ready to use.

Screenshots of Steps:







Create Account

Email *

Password *

First name *

Last name *

Country or region *

Please select *

* indicates required field

By clicking Register, I confirm that I have read and agree to the Cisco Online Privacy Statement and the Cisco Web Site Terms and Conditions.

Register

US EN

cisco

Log in

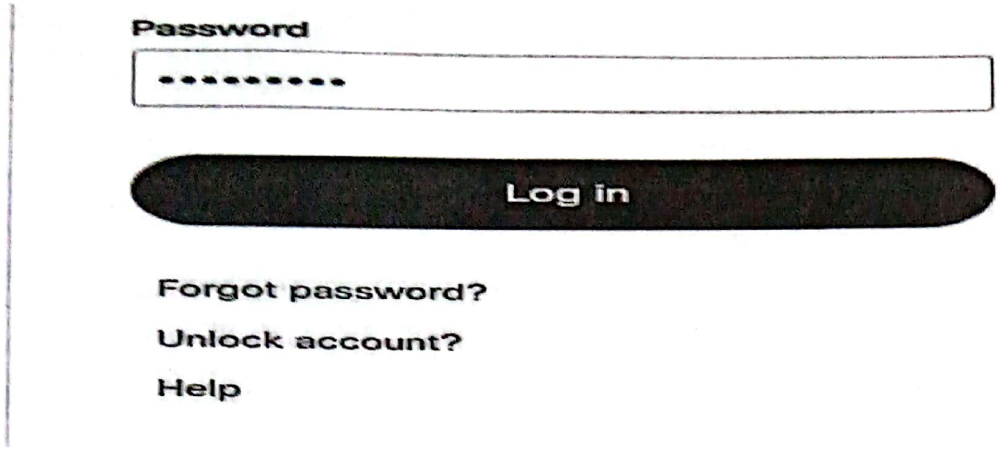
Email

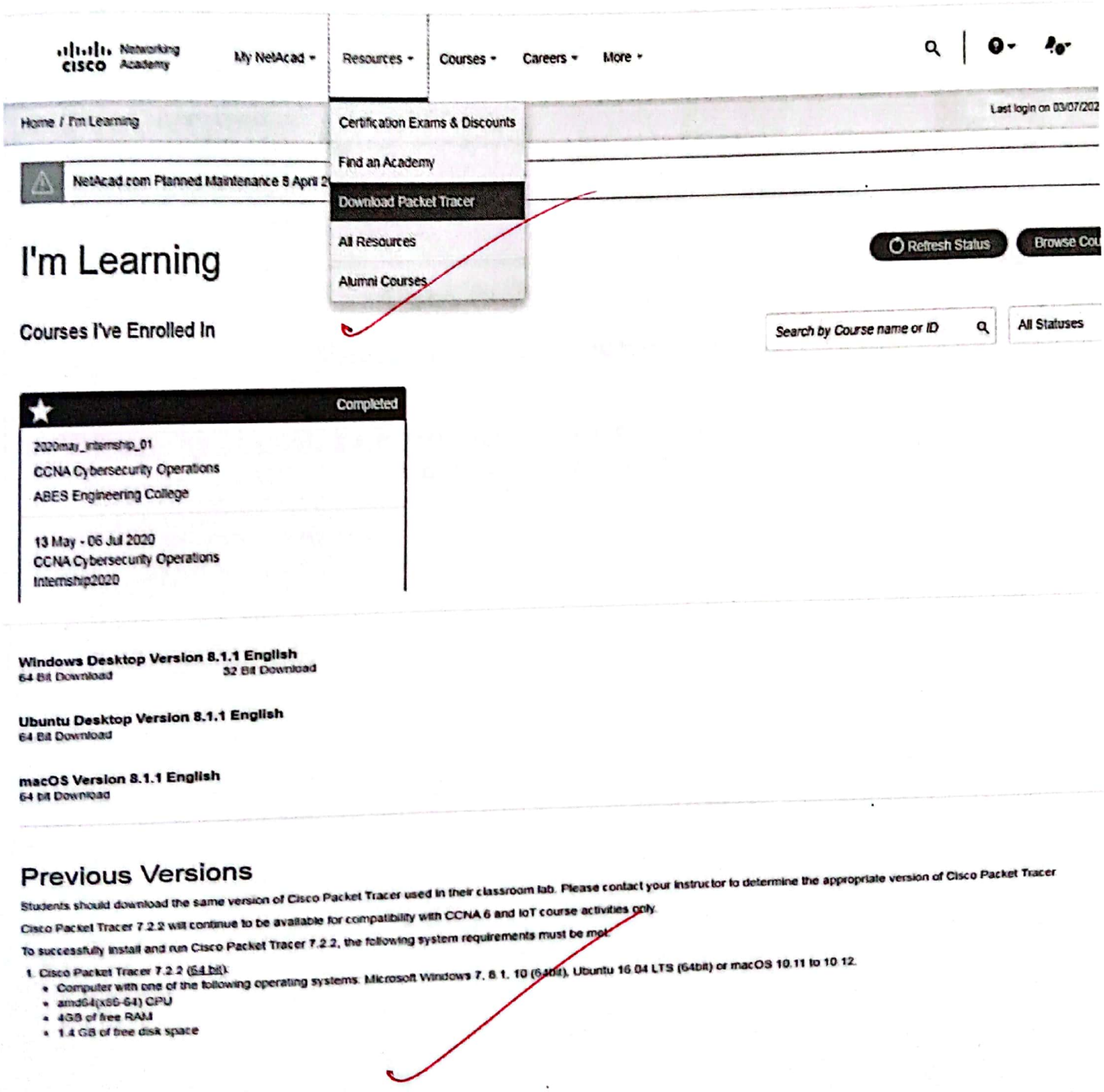
Next

Unlock account?

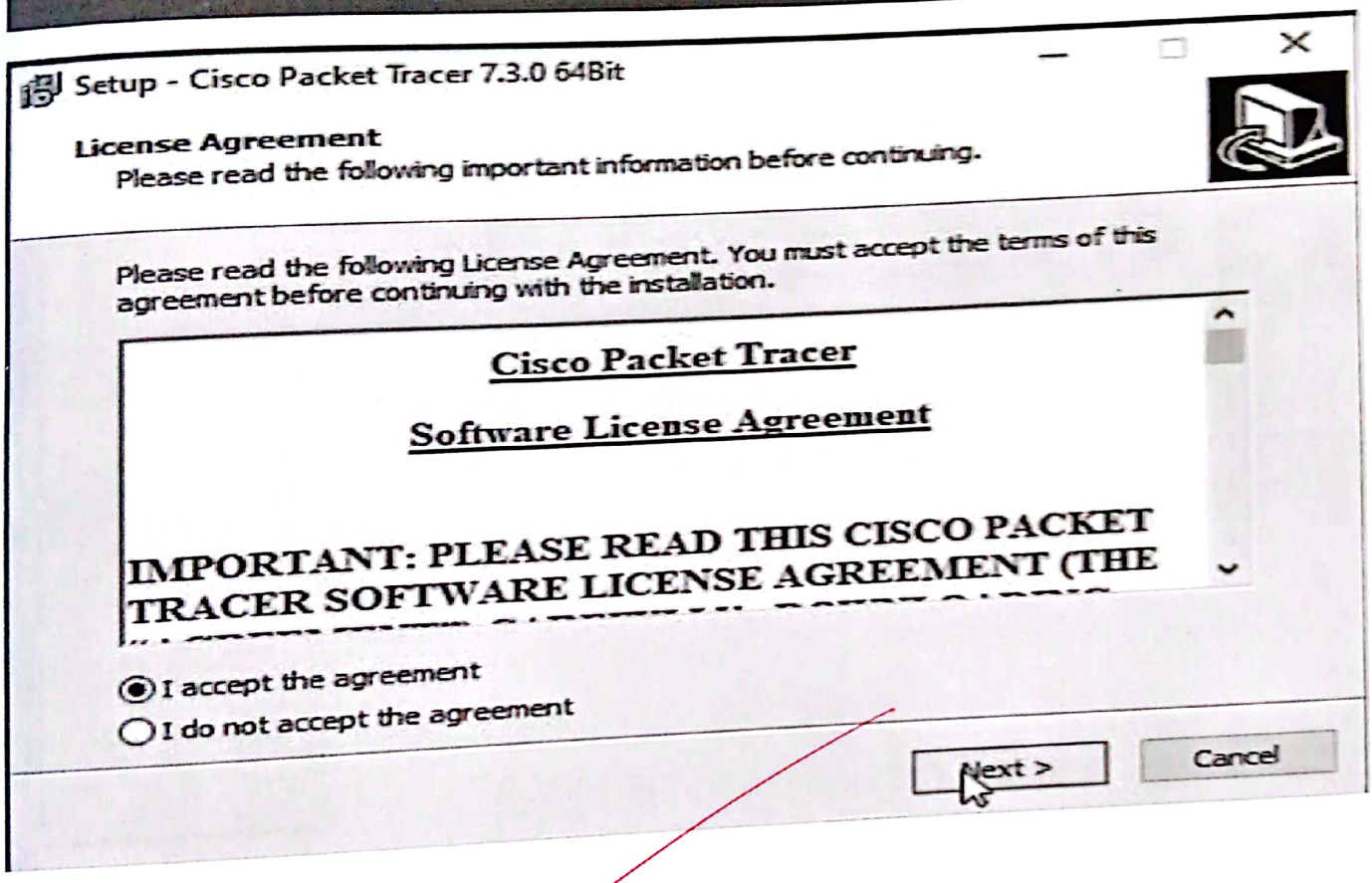
Forgot email address?

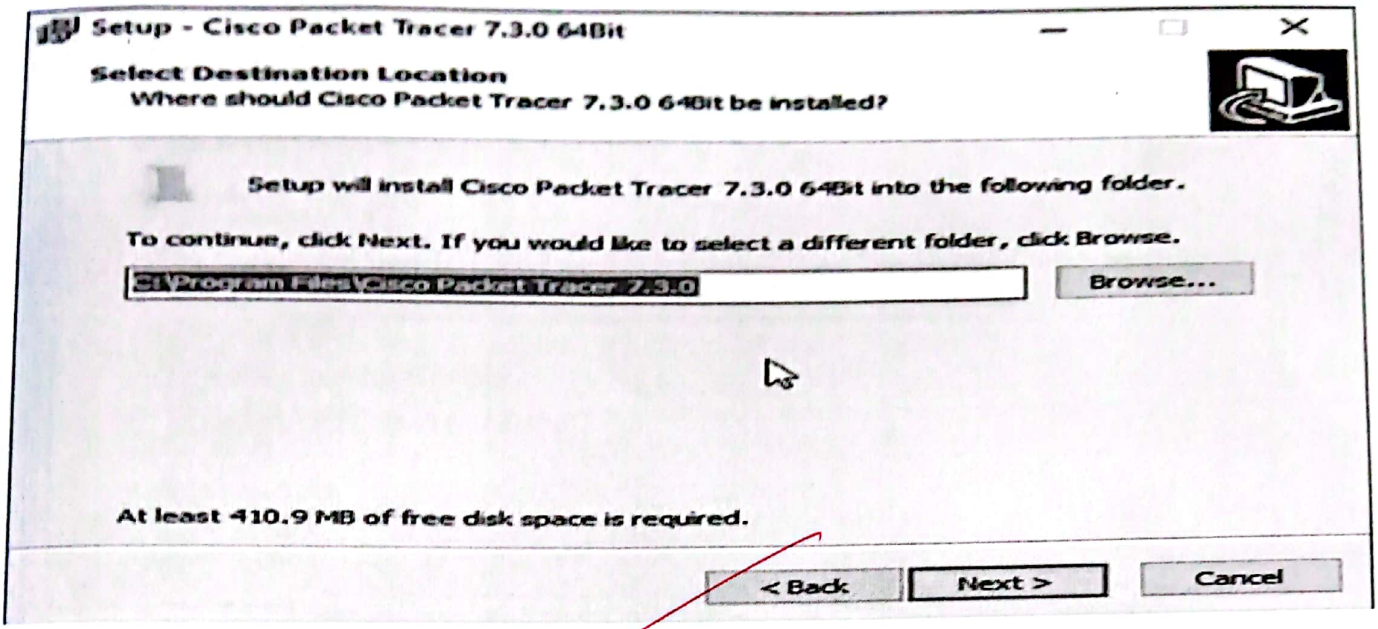
Help

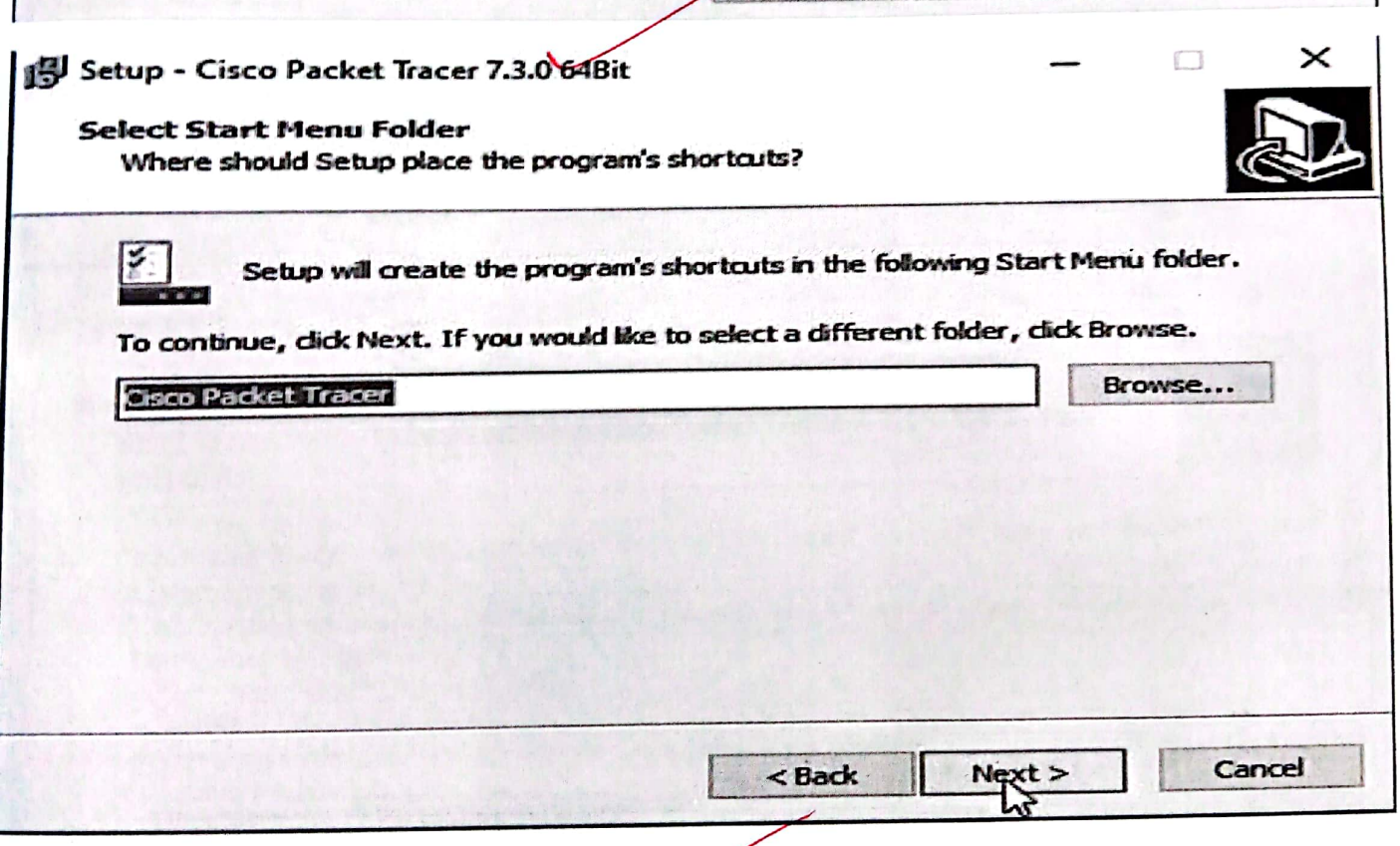

Password
Log in
Forgot password?
Unlock account?
Help

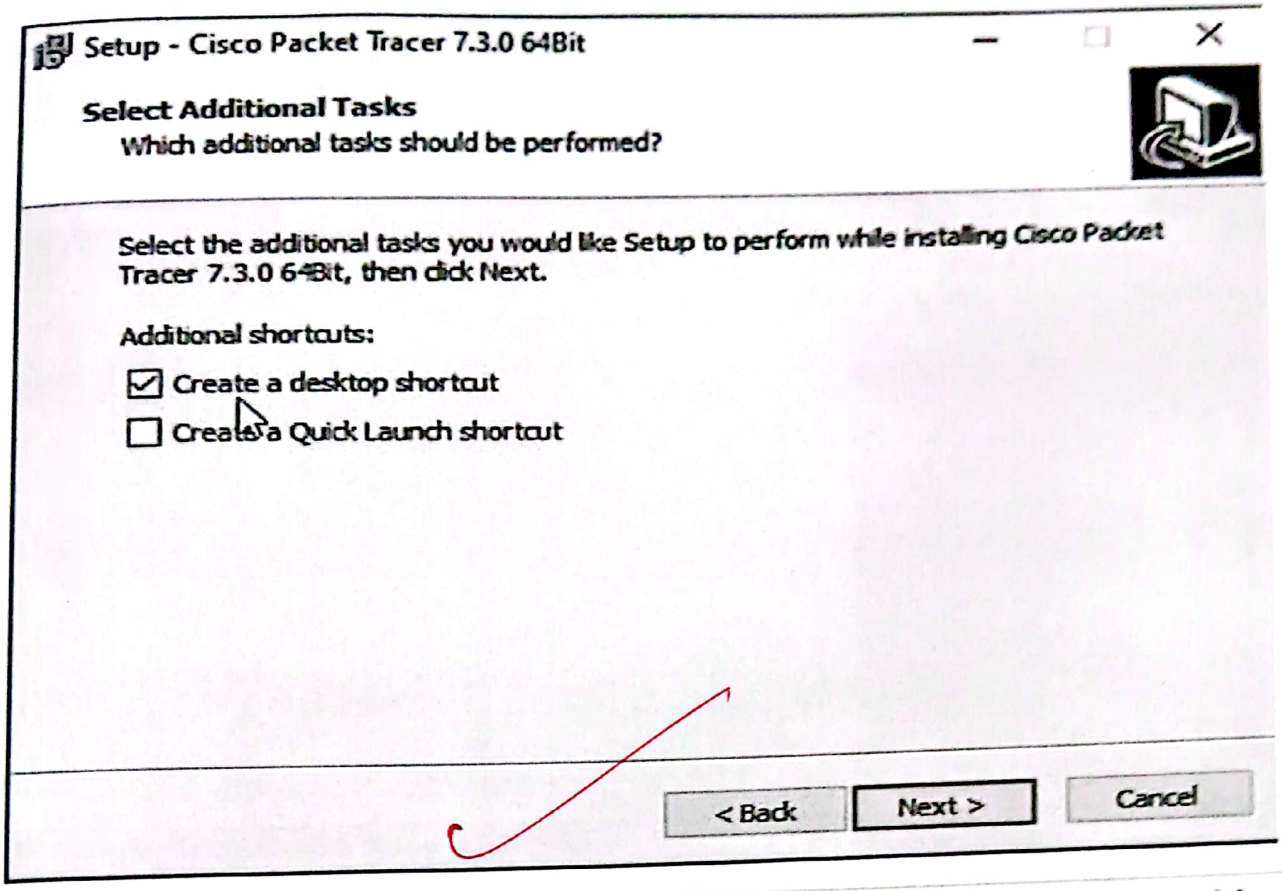

Networking Academy
My NetAcad
Resources
Courses
Careers
More
Home / I'm Learning
Last login on 03/07/202
Certification Exams & Discounts
Find an Academy
Download Packet Tracer
All Resources
Alumni Courses
NetAcad.com Planned Maintenance 8 April 2
I'm Learning
Refresh Status
Courses I've Enrolled In
Search by Course name or ID
All Statuses
Completed
2020may_internship_01
CCNA Cybersecurity Operations
ABES Engineering College
13 May - 06 Jul 2020
CCNA Cybersecurity Operations
Internship2020
Windows Desktop Version 8.1.1 English
64 Bit Download
32 Bit Download
Ubuntu Desktop Version 8.1.1 English
64 Bit Download
macOS Version 8.1.1 English
64 bit Download
Previous Versions
Students should download the same version of Cisco Packet Tracer used in their classroom lab. Please contact your instructor to determine the appropriate version of Cisco Packet Tracer
Cisco Packet Tracer 7.2.2 will continue to be available for compatibility with CCNA 6 and IoT course activities only.
To successfully install and run Cisco Packet Tracer 7.2.2, the following system requirements must be met:
1. Cisco Packet Tracer 7.2.2 (64 bit):
• Computer with one of the following operating systems: Microsoft Windows 7, 8.1, 10 (64bit), Ubuntu 16.04 LTS (64bit) or macOS 10.11 to 10.12.
• amd64(x86-64) CPU
• 4GB of free RAM
• 1.4 GB of free disk space

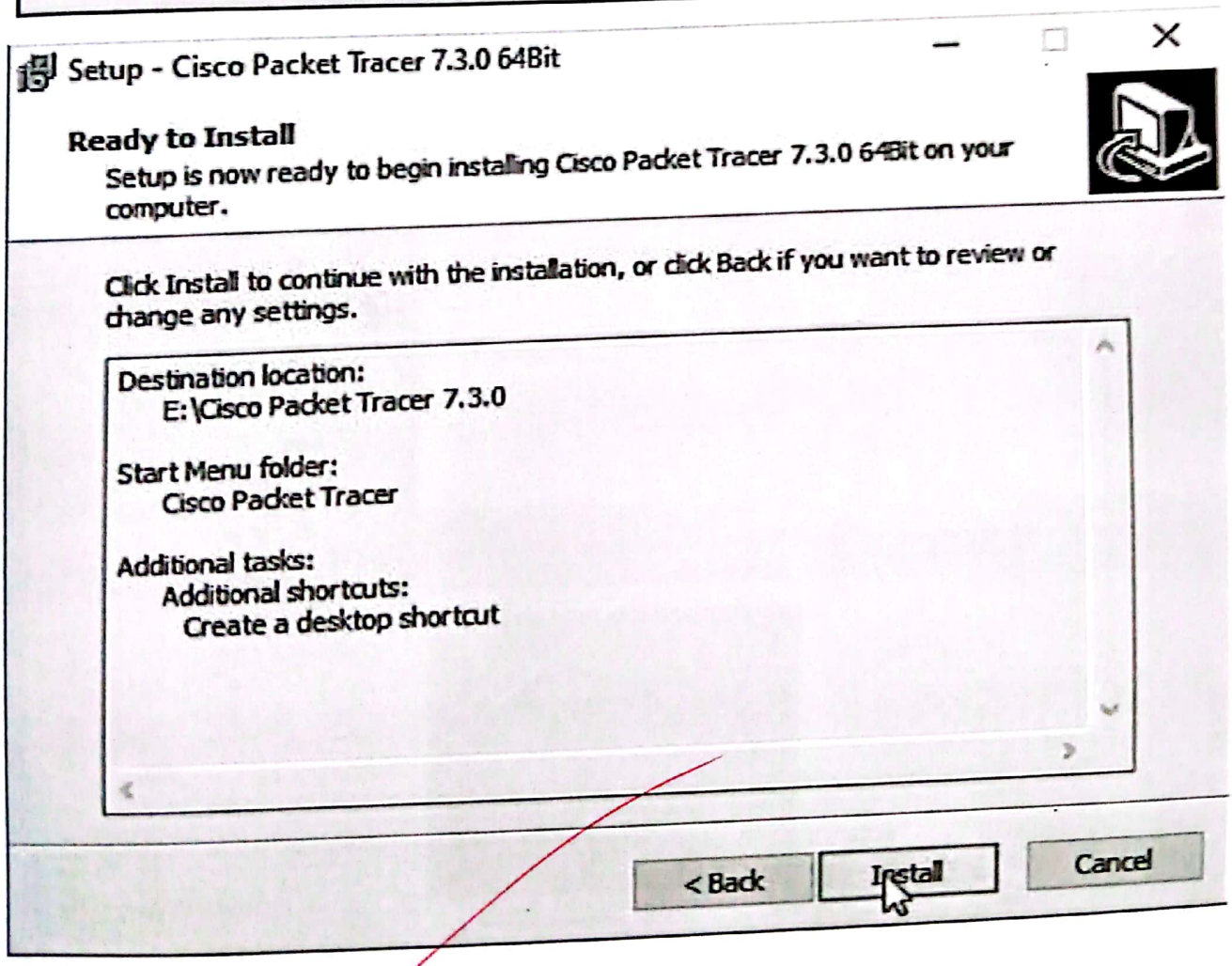

Packet Tracer
-7.3.1-win64-
setup

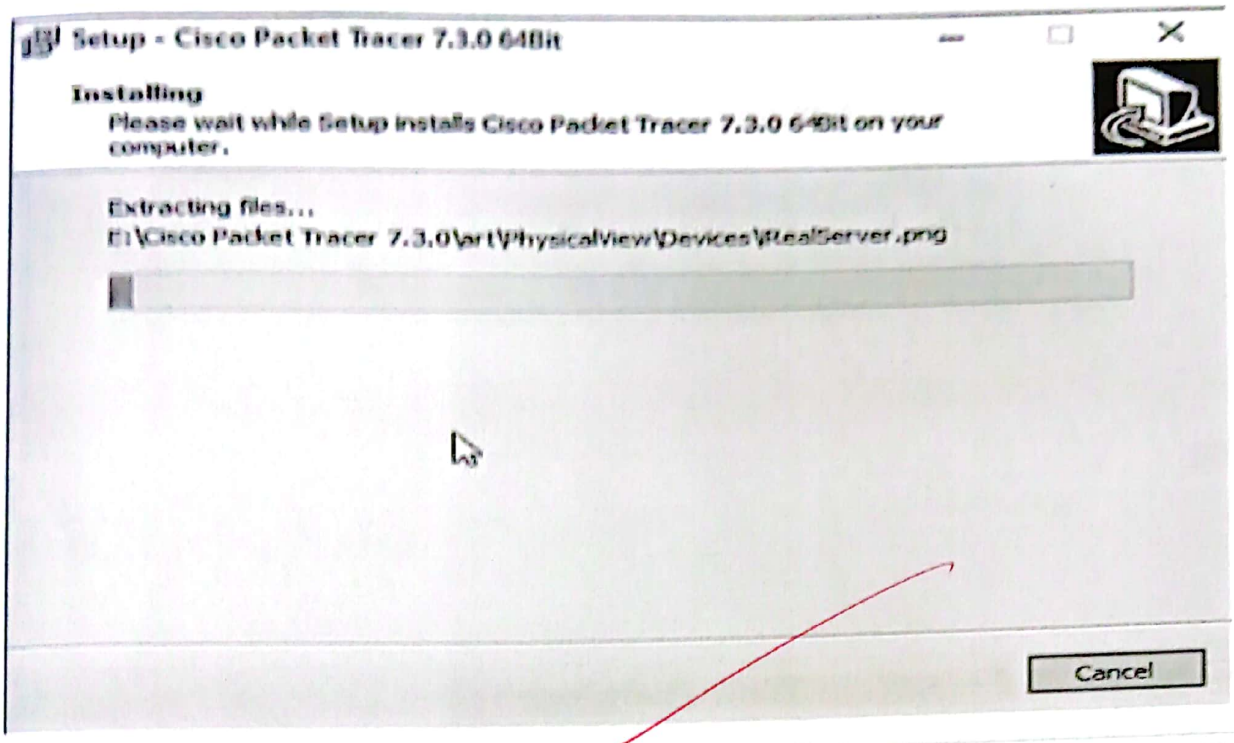

Setup - Cisco Packet Tracer 7.3.0 64Bit
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Cisco Packet Tracer
Software License Agreement
IMPORTANT: PLEASE READ THIS CISCO PACKET TRACER SOFTWARE LICENSE AGREEMENT (THE
I accept the agreement
I do not accept the agreement
Next >
Cancel

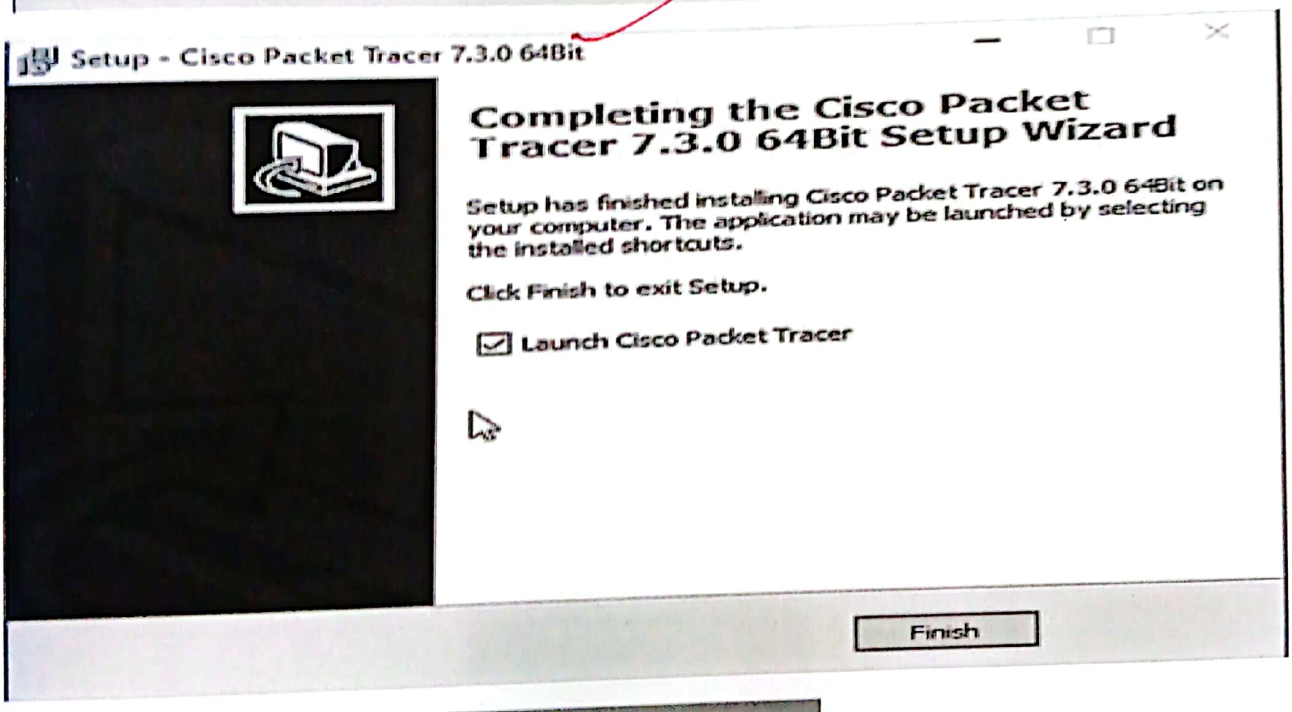

Setup - Cisco Packet Tracer 7.3.0 64Bit
Select Destination Location
Where should Cisco Packet Tracer 7.3.0 64Bit be installed?
Setup will install Cisco Packet Tracer 7.3.0 64Bit into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\Cisco Packet Tracer 7.3.0
Browse...
At least 410.9 MB of free disk space is required.
< Back
Next >
Cancel


Setup - Cisco Packet Tracer 7.3.0 64Bit
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Cisco Packet Tracer
Browse...
< Back
Next >
Cancel

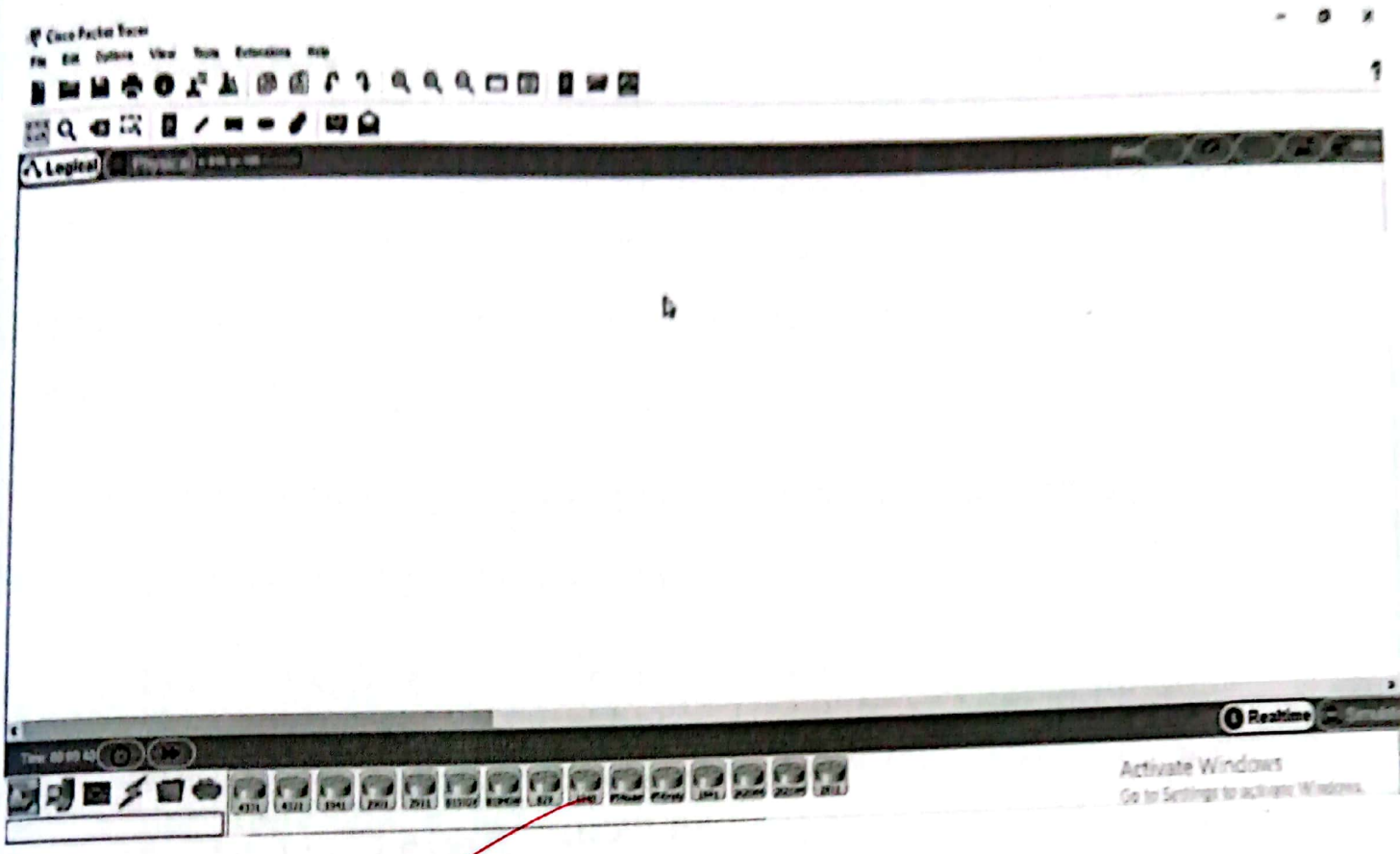

Setup - Cisco Packet Tracer 7.3.0 64Bit
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing Cisco Packet Tracer 7.3.0 64Bit, then click Next.
Additional shortcuts:
Create a desktop shortcut
Create a Quick Launch shortcut
< Back
Next >
Cancel


Setup - Cisco Packet Tracer 7.3.0 64Bit
Ready to Install
Setup is now ready to begin installing Cisco Packet Tracer 7.3.0 64Bit on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
E:\Cisco Packet Tracer 7.3.0
Start Menu folder:
Cisco Packet Tracer
Additional tasks:
Additional shortcuts:
Create a desktop shortcut
< Back
Install
Cancel


Setup - Cisco Packet Tracer 7.3.0 64Bit
Installing
Please wait while Setup installs Cisco Packet Tracer 7.3.0 64Bit on your computer.
Extracting files...
E:\Cisco Packet Tracer 7.3.0\art\PhysicalView\Devices\RealServer.png
Cancel


Setup - Cisco Packet Tracer 7.3.0 64Bit
Completing the Cisco Packet Tracer 7.3.0 64Bit Setup Wizard
Setup has finished installing Cisco Packet Tracer 7.3.0 64Bit on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch Cisco Packet Tracer
Finish


Cisco Packet Tracer



Functional uses of Cisco Packet Tracker:

a) E-learning.

b) Visualizing Networks

c) Real-time and simulation mode.

d) Compatible on various platforms.

e) support to all languages

f) Most networking protocols are supported.

g) Environment is interactive.

h) Can be used on unlimited devices

i) The main purpose of cisco Packet Tracer is to help students learn the principles of networking with hands-on experience.

j) It is used to demonstrate the technical concepts and networking systems.

k) This makes the job easier for engineers allowing them to add or remove simulated network devices, with a command line interface and a drag and drop user interface.

LAB SHEET-7

Network design with switch and end devices to implement the uses of subnet marks (static IP-design 1)

steps:

a) start

b) Take two Host (End Devices and a switch for Network connection between them.

c) connect them using connecting wire.

d) Configure IP statically of one End devices.

e) Enter the class-c IP address at IPv4 and subnet it making only 2 valid hosts (/30)

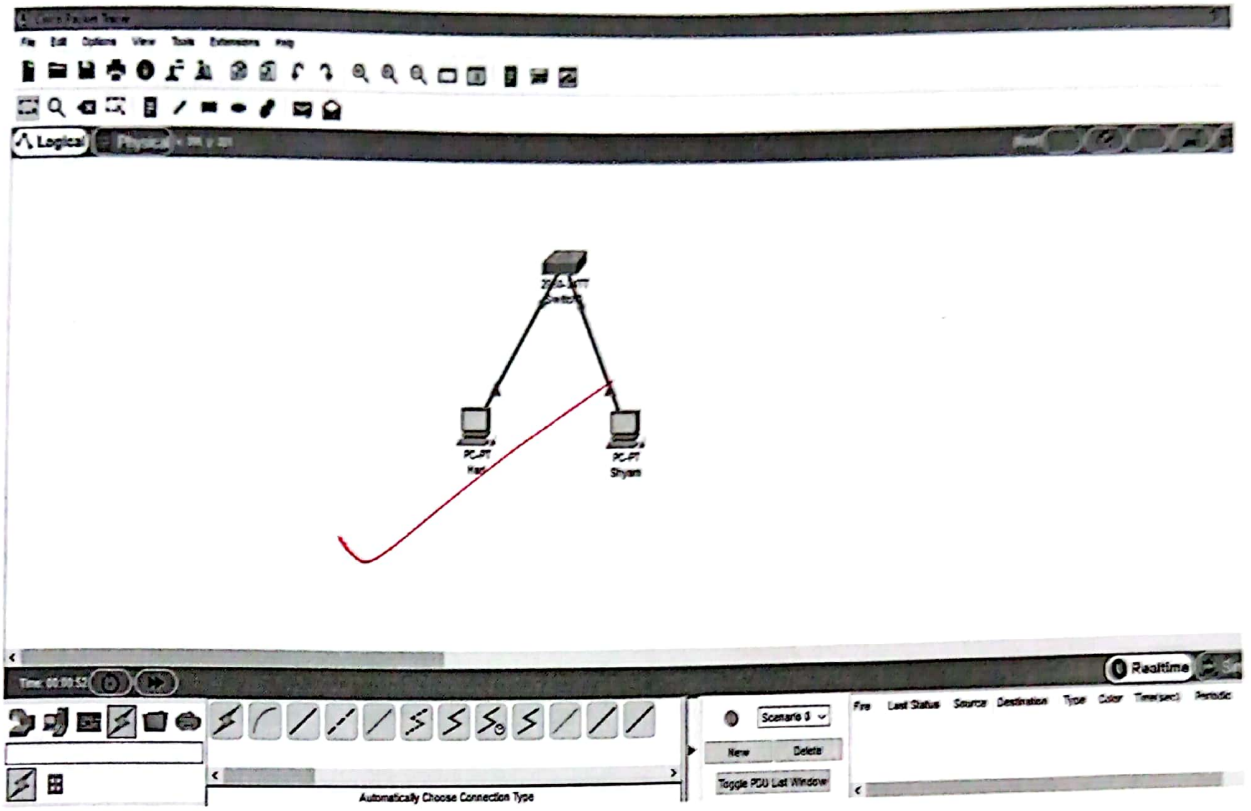
f) Repeat step (c-d) for other end devices.

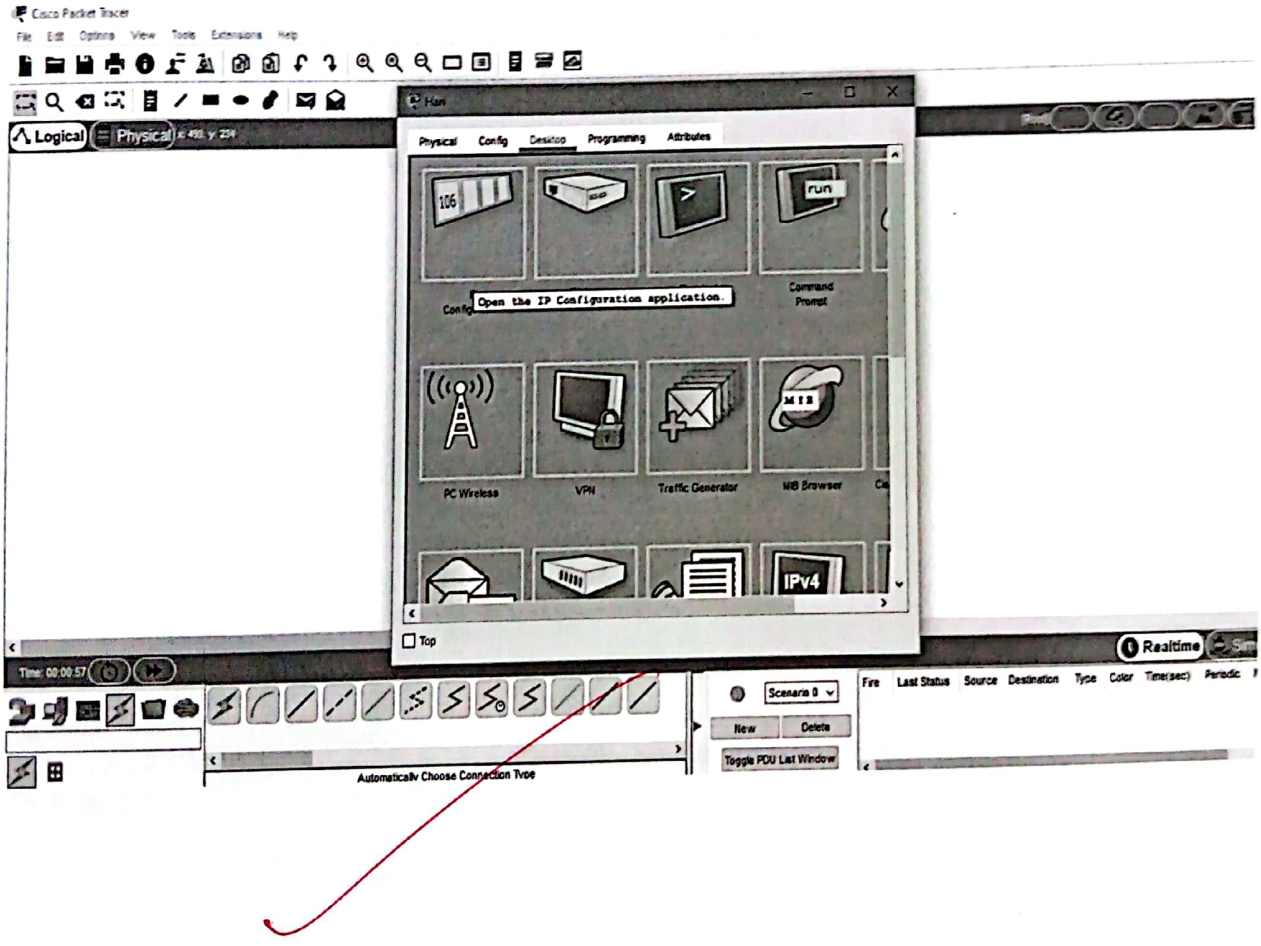
g) Pass the Message packet from one end device to other end device. (If it shows successful, the design is valid and error less).

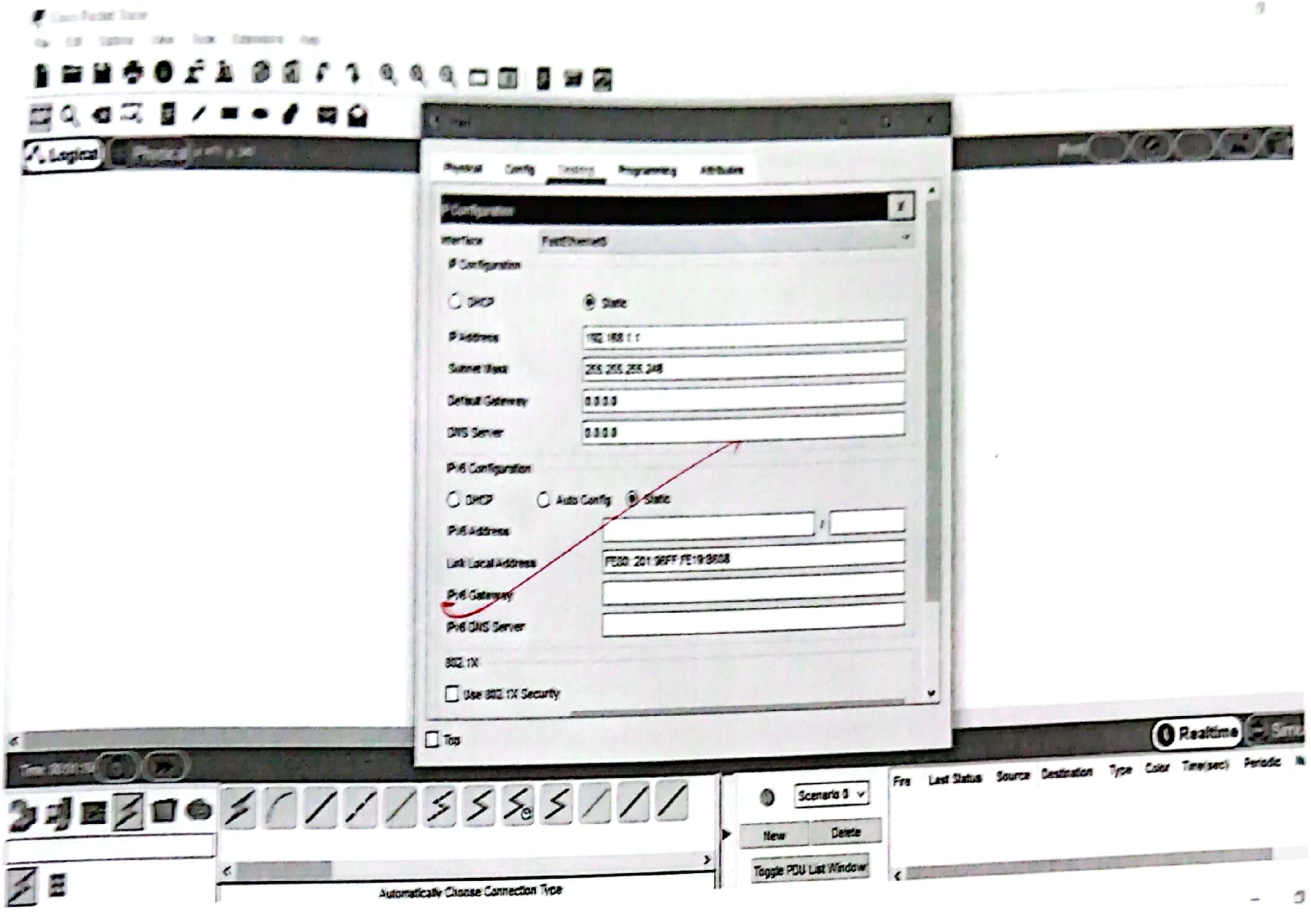
h) Ping any one device IP address using command Prompt.

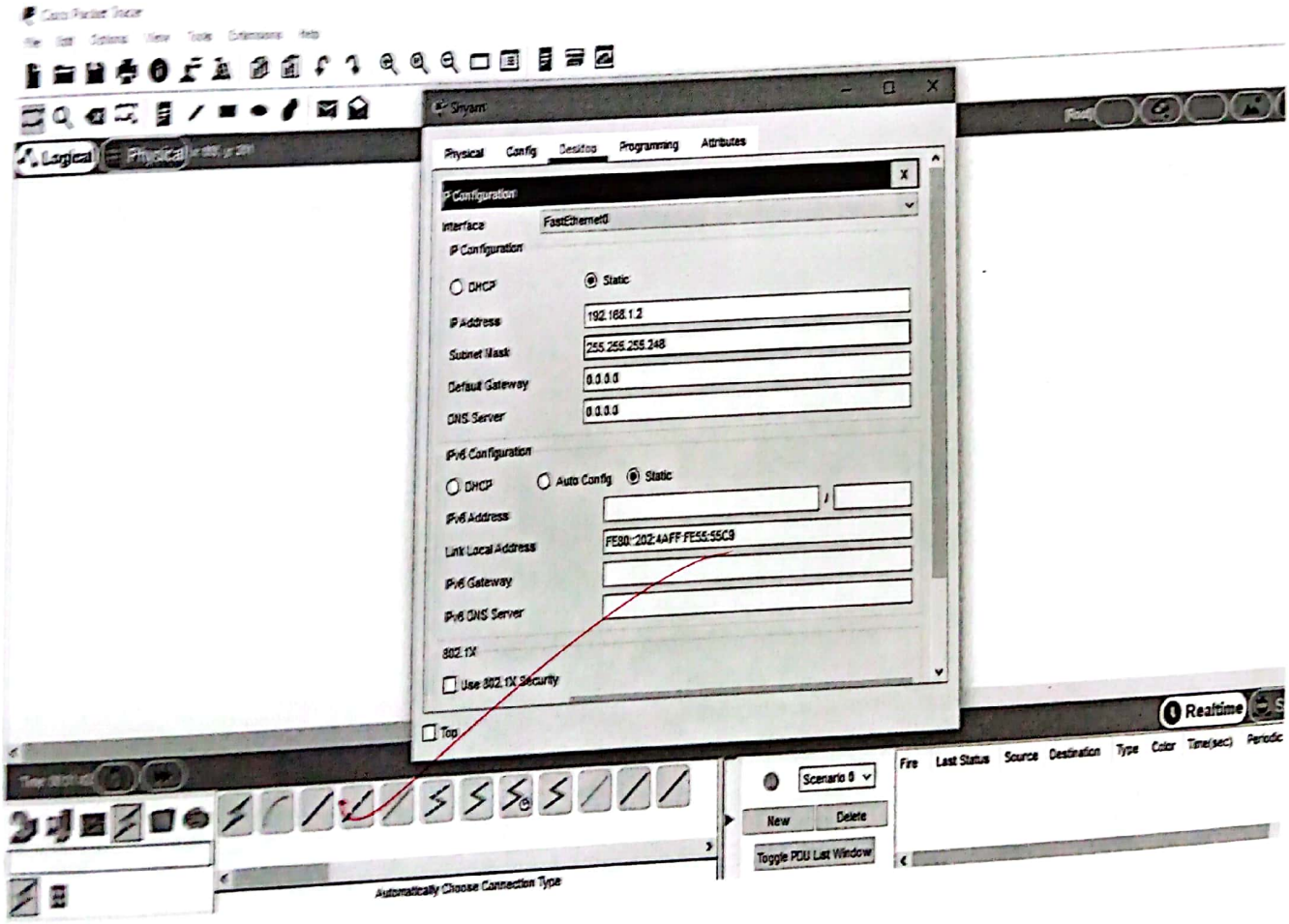
i) End.

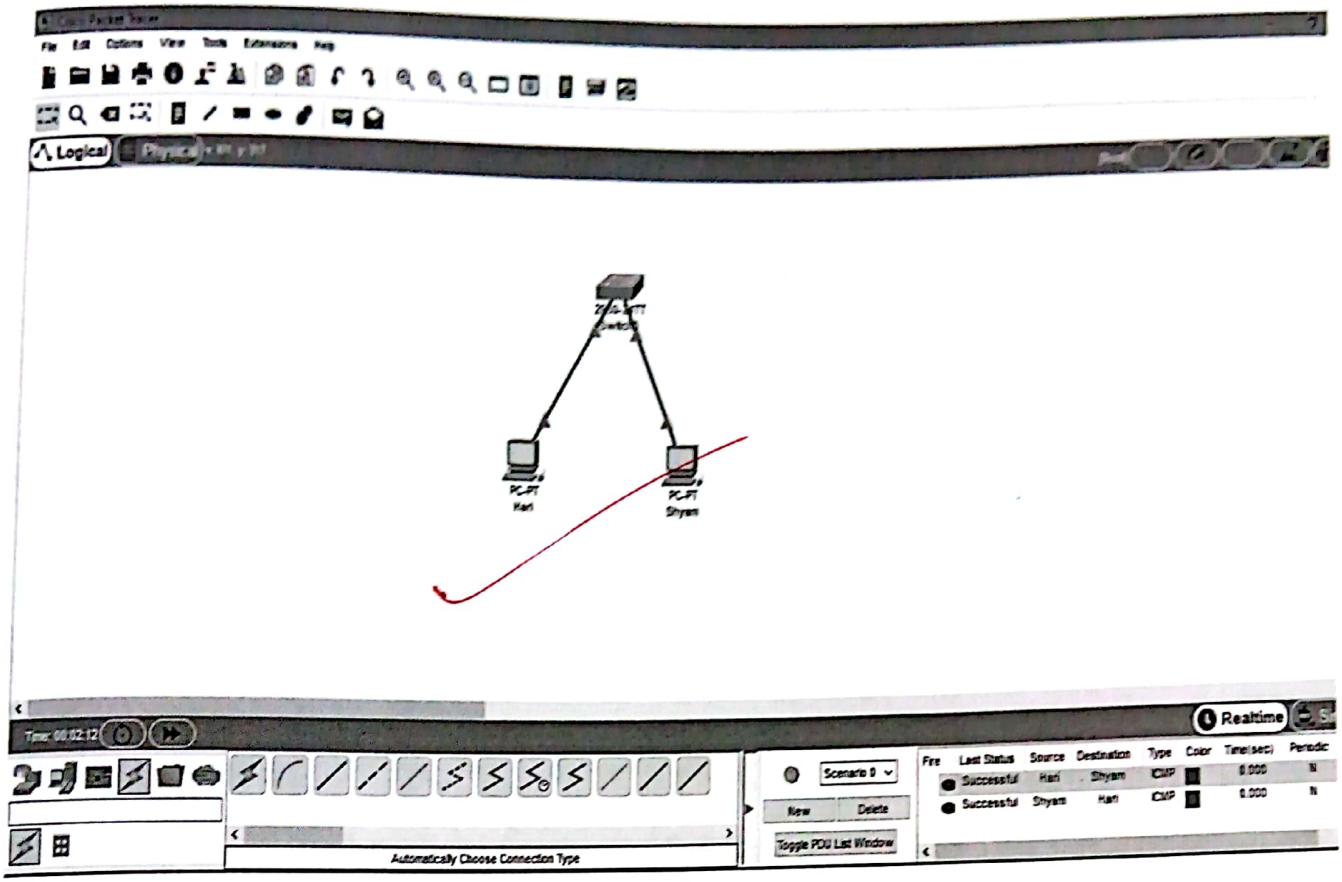
Screenshots of steps:

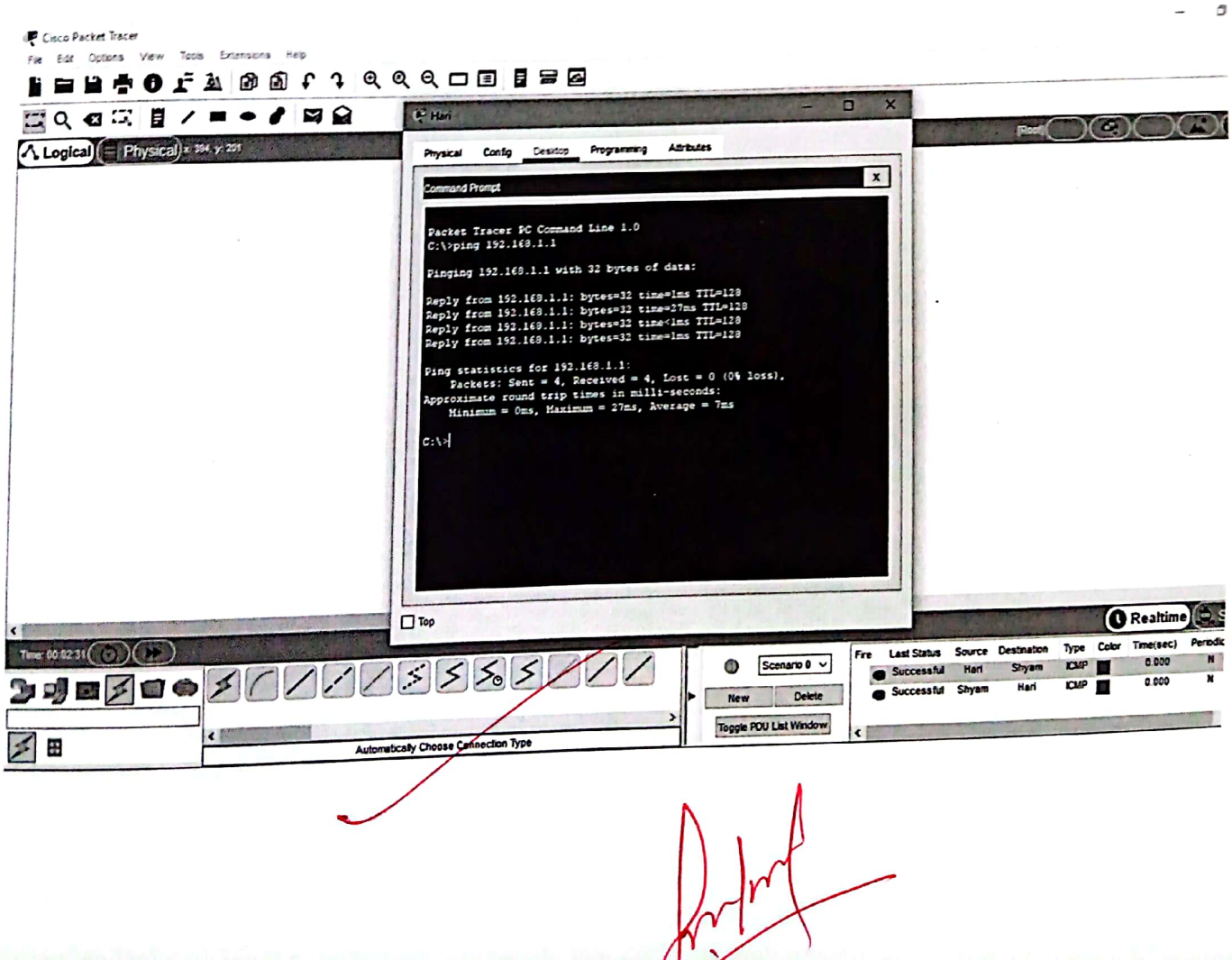





Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
Auto Config
IPv6 Address
Link Local Address
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type


Sriyam
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Auto Config
IPv6 Address
Link Local Address
FE80::202:4AFF:FE55:55C9
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type


Logical
Physical
PC-PT
Hari
PC-PT
Shyam
Realtime
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Successful
Hari
Shyam
ICMP
Successful
Shyam
Hari
ICMP


Cisco Packet Tracer
File
Edit
Options
View
Tools
Extensions
Help
Logical
Physical
Hari
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=27ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 27ms, Average = 7ms
C:\>
Top
Realtime
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Successful
Hari
Shyam
ICMP
Successful
Shyam
Hari
ICMP

LABSHEET-8

Network Design with switch and end devices to implement the uses of subnet masks (static IP design 2)

steps:

a) start

b) Take six Host/End Devices and a switch for Network connection between them.

c) Connect them using connecting wire.

d) Configure IP statically of each End devices.

e) Enter the class-C IPaddress at IPv4 and subnet it making six valid hosts (/29).

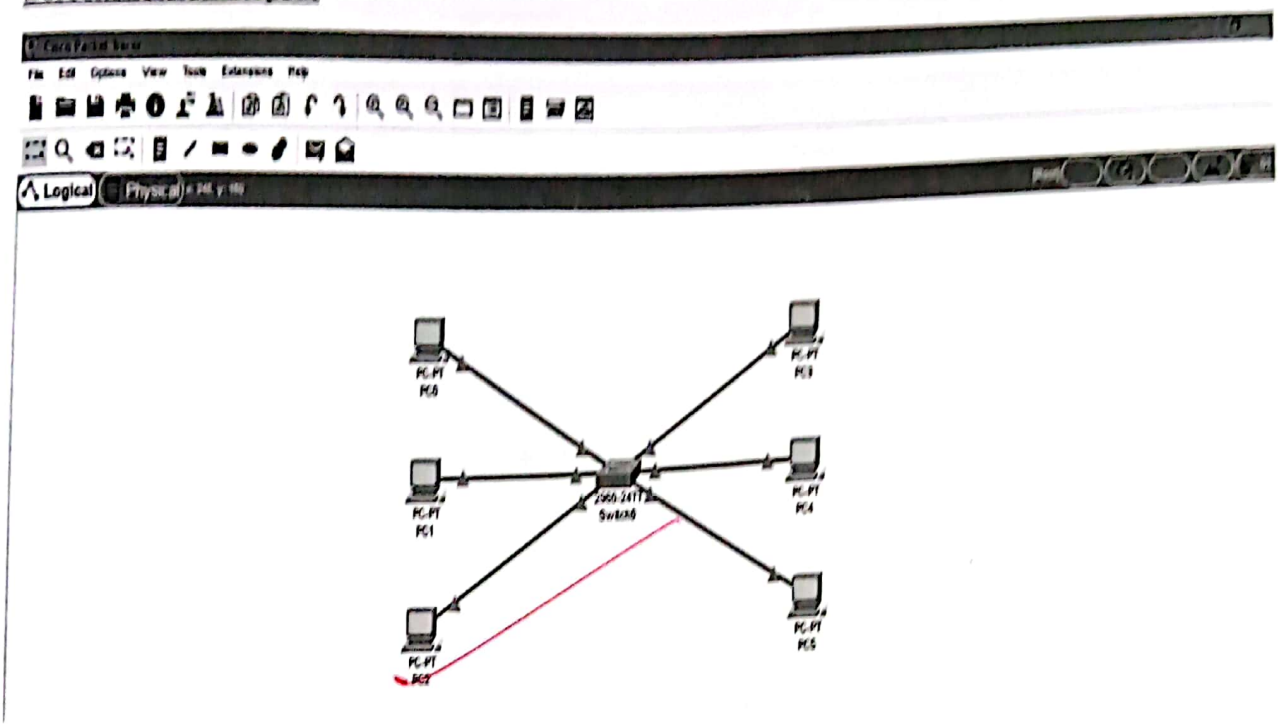
f) Repeat step (c-d) for other end devices.

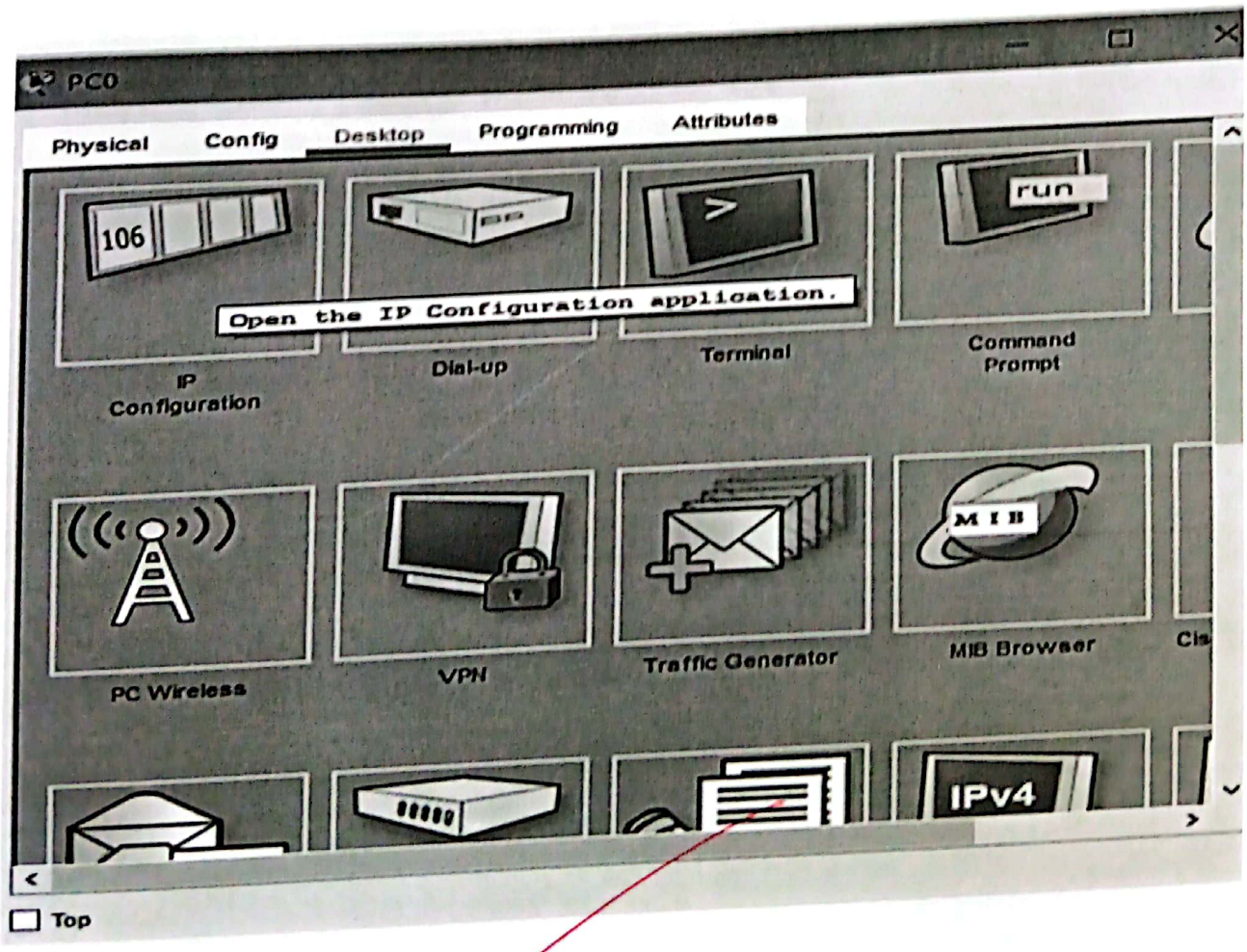
g) Pass the Message packet from one end device to other end device. (If it shows successful the design is valid and error less).

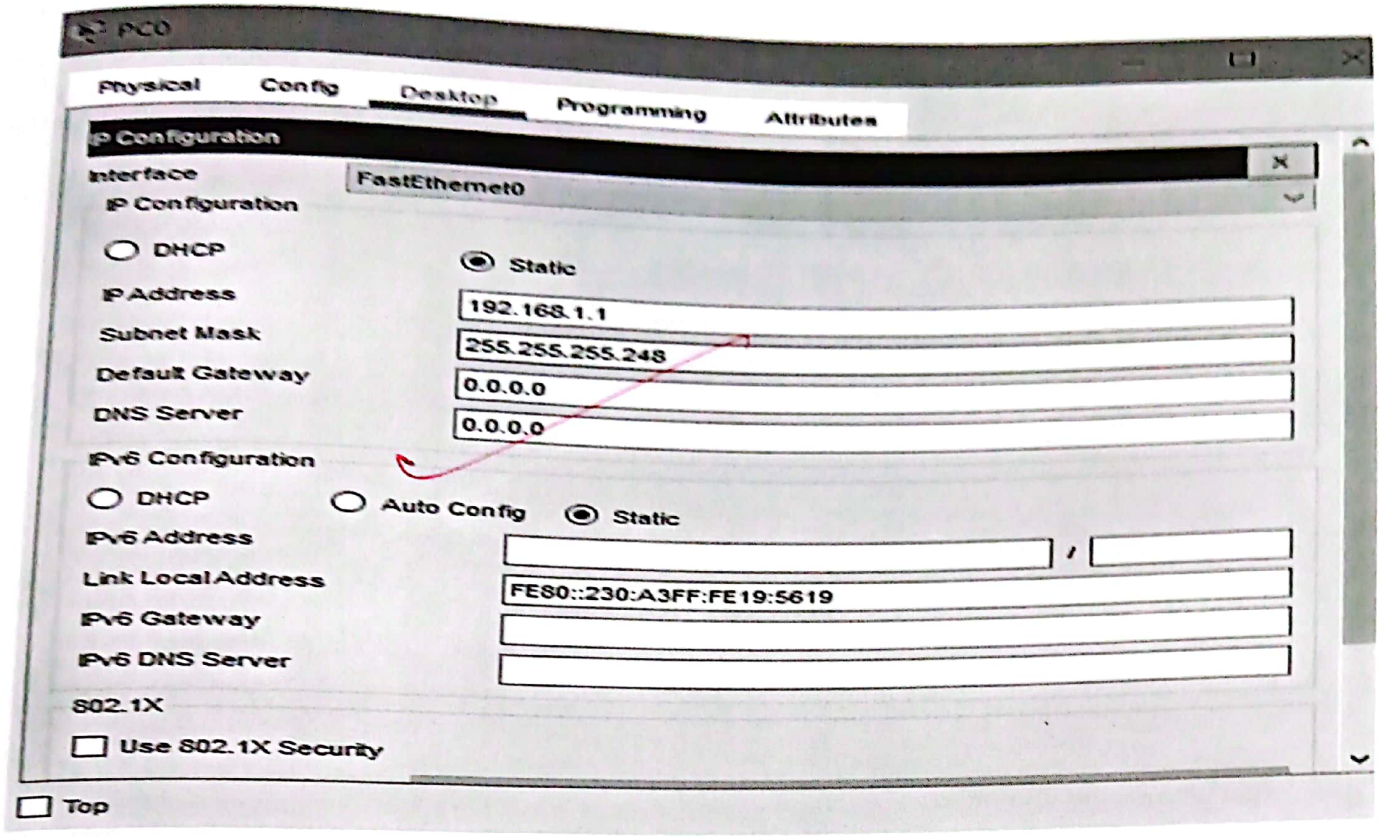
h) Ping any one device IP address using Command Prompt.

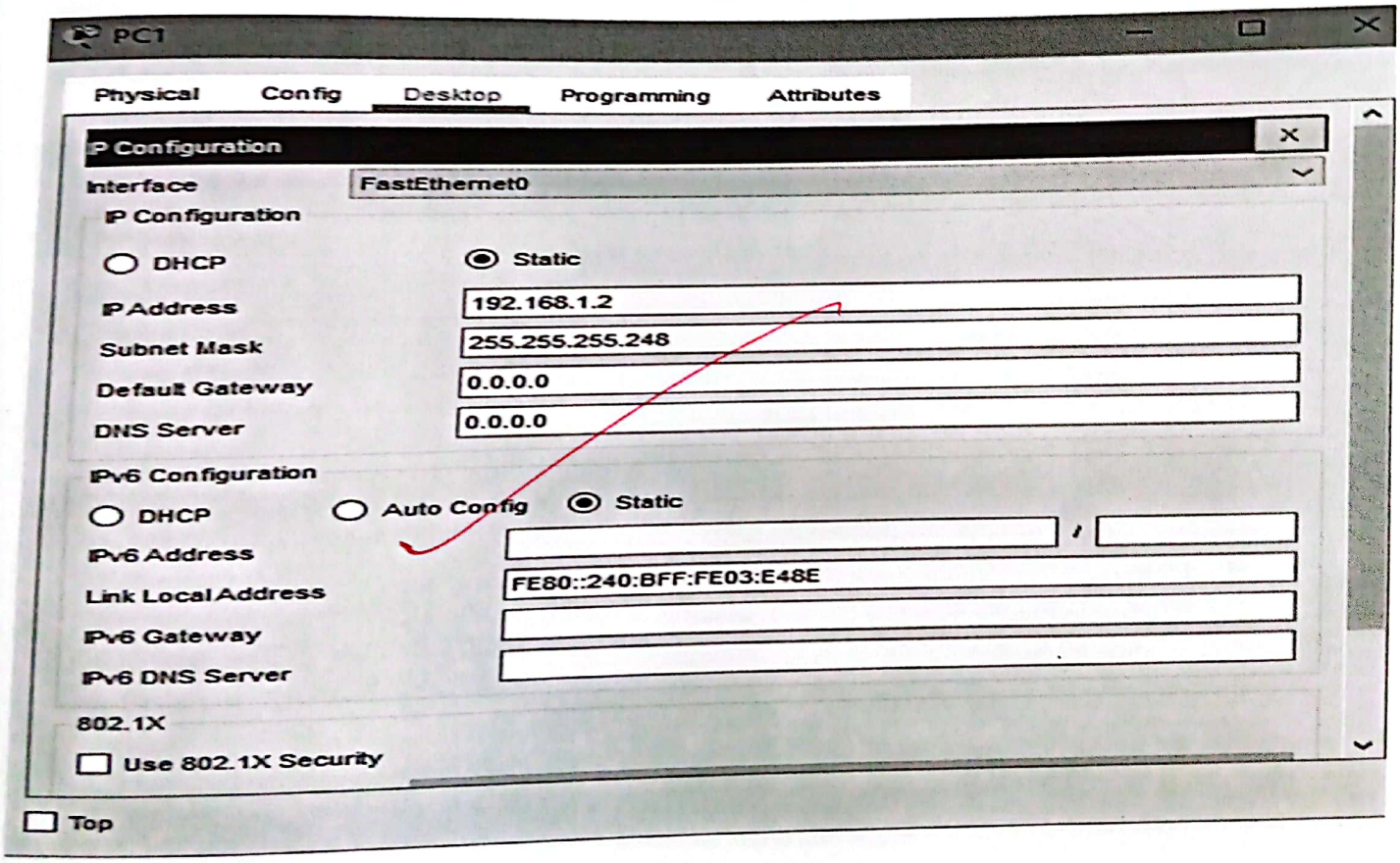
i) End.

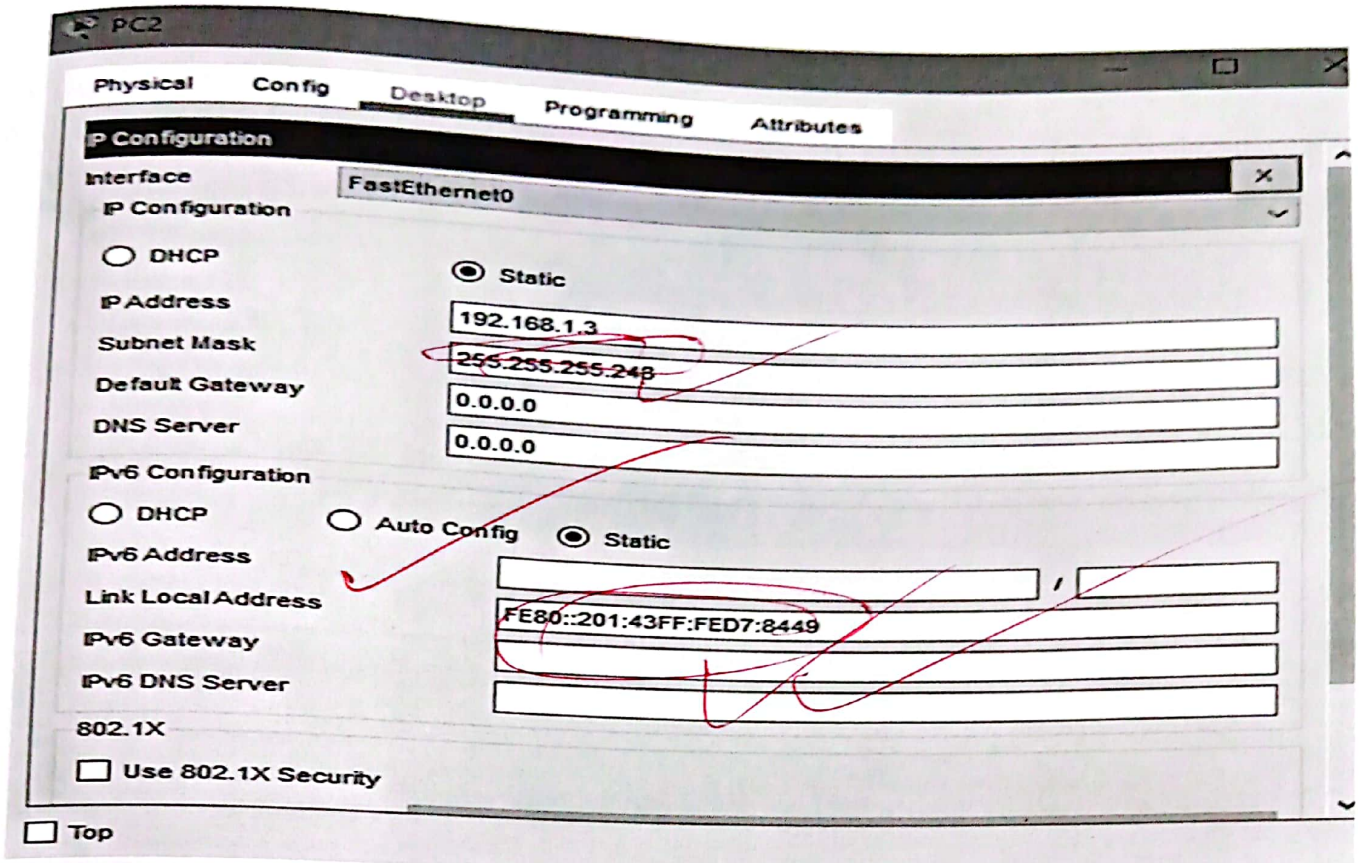
Screenshots of steps :

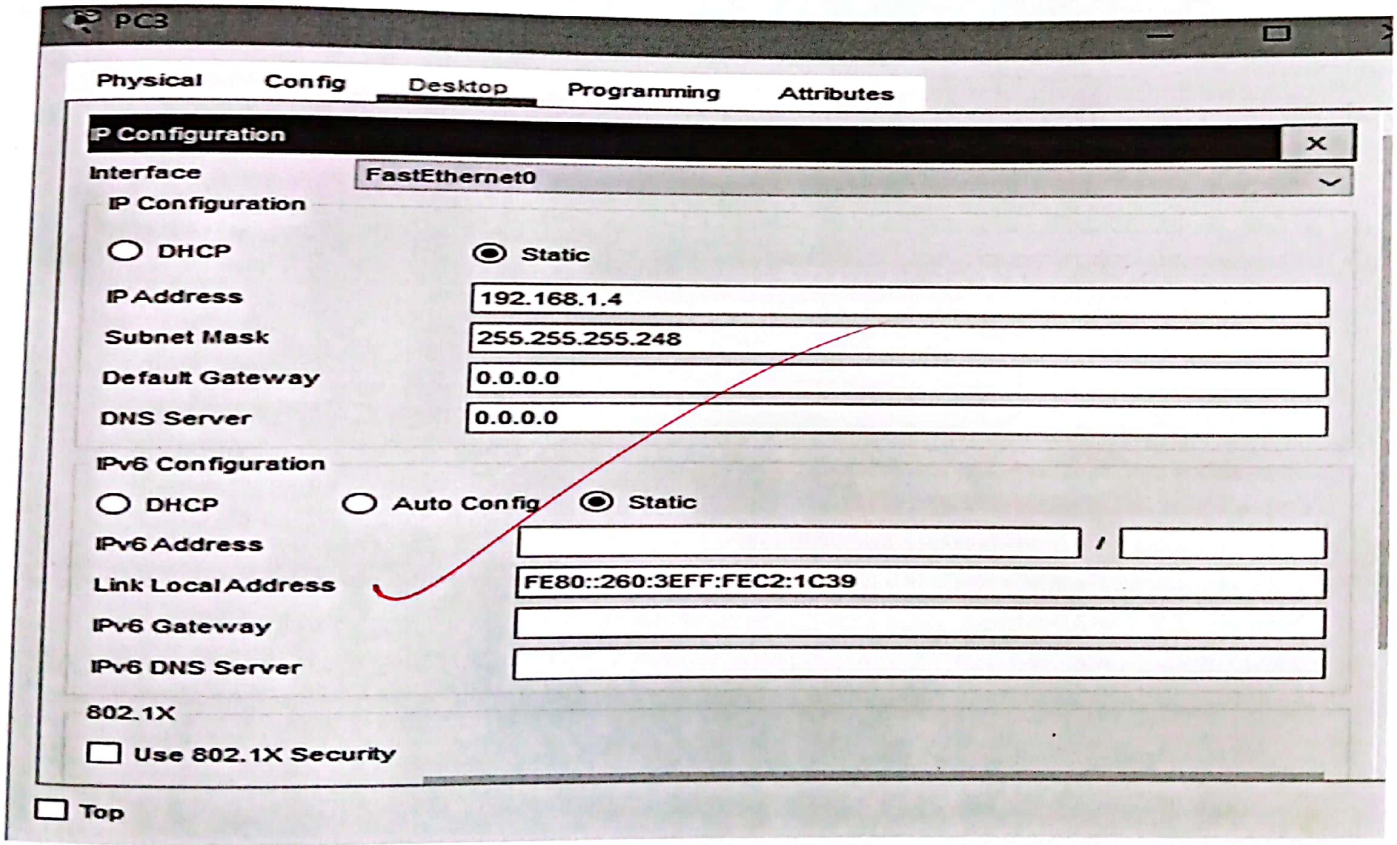


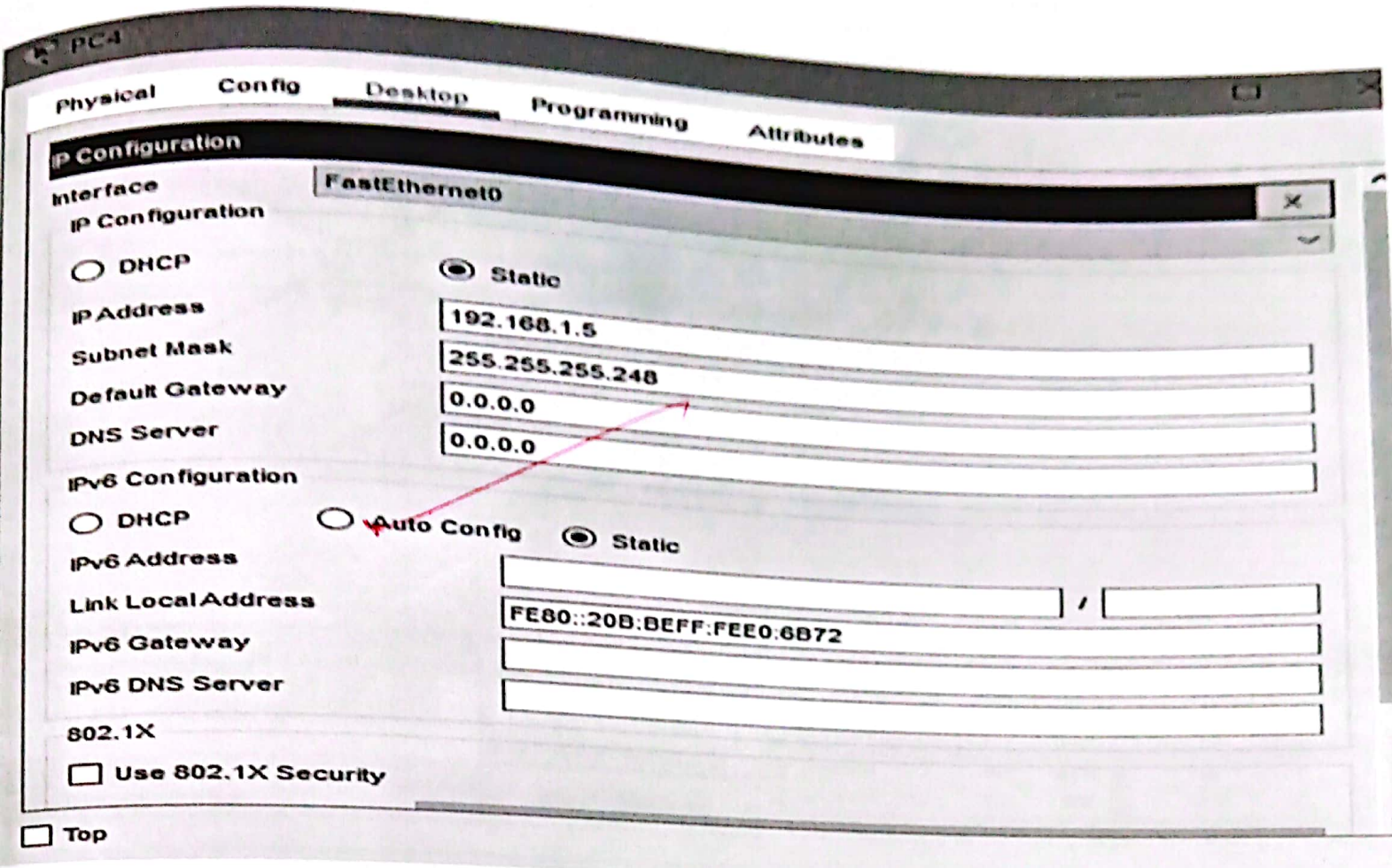


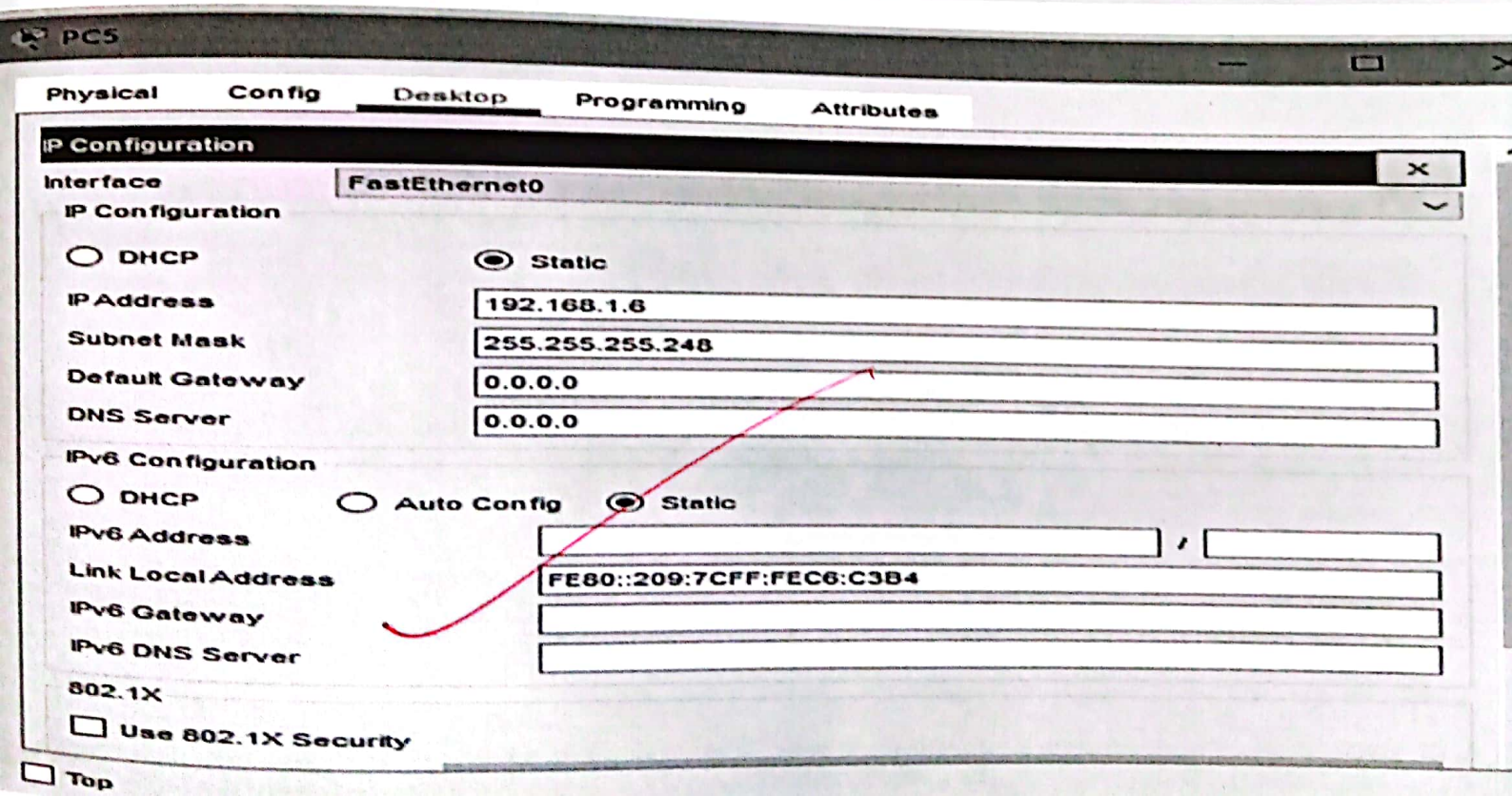

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.1
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::230:A3FF:FE19:5619
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top

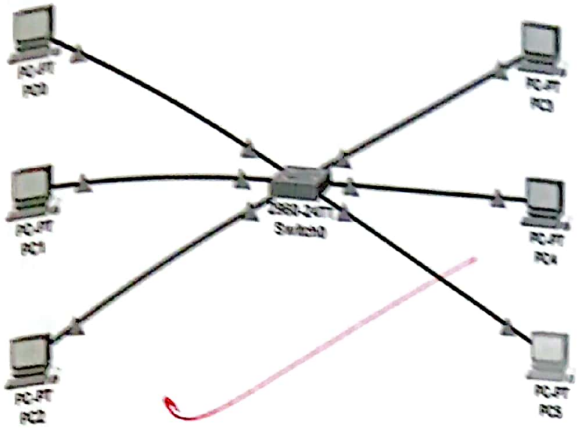

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::240:BFF:FE03:E48E
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top

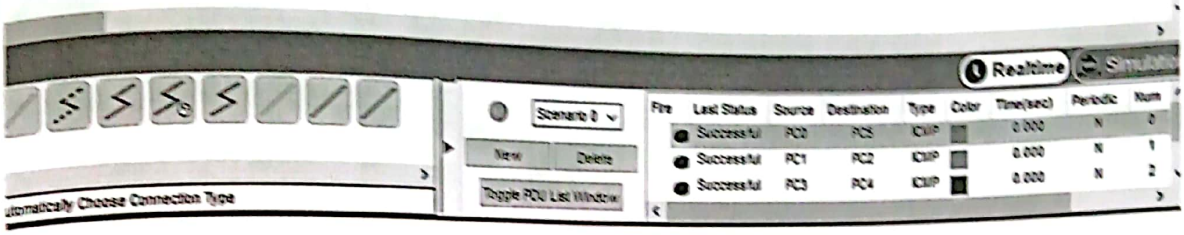

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FED7:8449
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.4
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::260:3EFF:FEC2:1C39
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.5
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20B:BEFF:FEE0:6B72
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.6
Subnet Mask
255.255.255.248
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::209:7CFF:FEC6:C3B4
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top






```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=3ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

LABSHEET-9

Network Design with switch, hub and end devices
to implement the uses of subnet marks (static
IP design s)

Steps:

a) start.

b) Take 3 Host/End Devices, a Hub and a switch
for Network connection between them.

c) connect them using connecting wire.

d) configure IP statically of each End devices.

e) Enter the class-C IP address at IPv4 and sub-
net it. (/24)

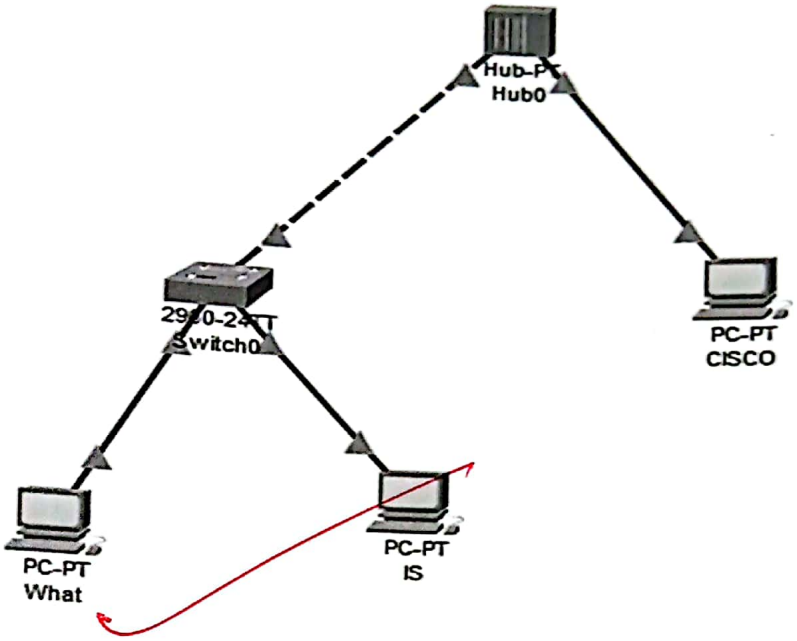
f) Repeat step (c-d) for other and devices.

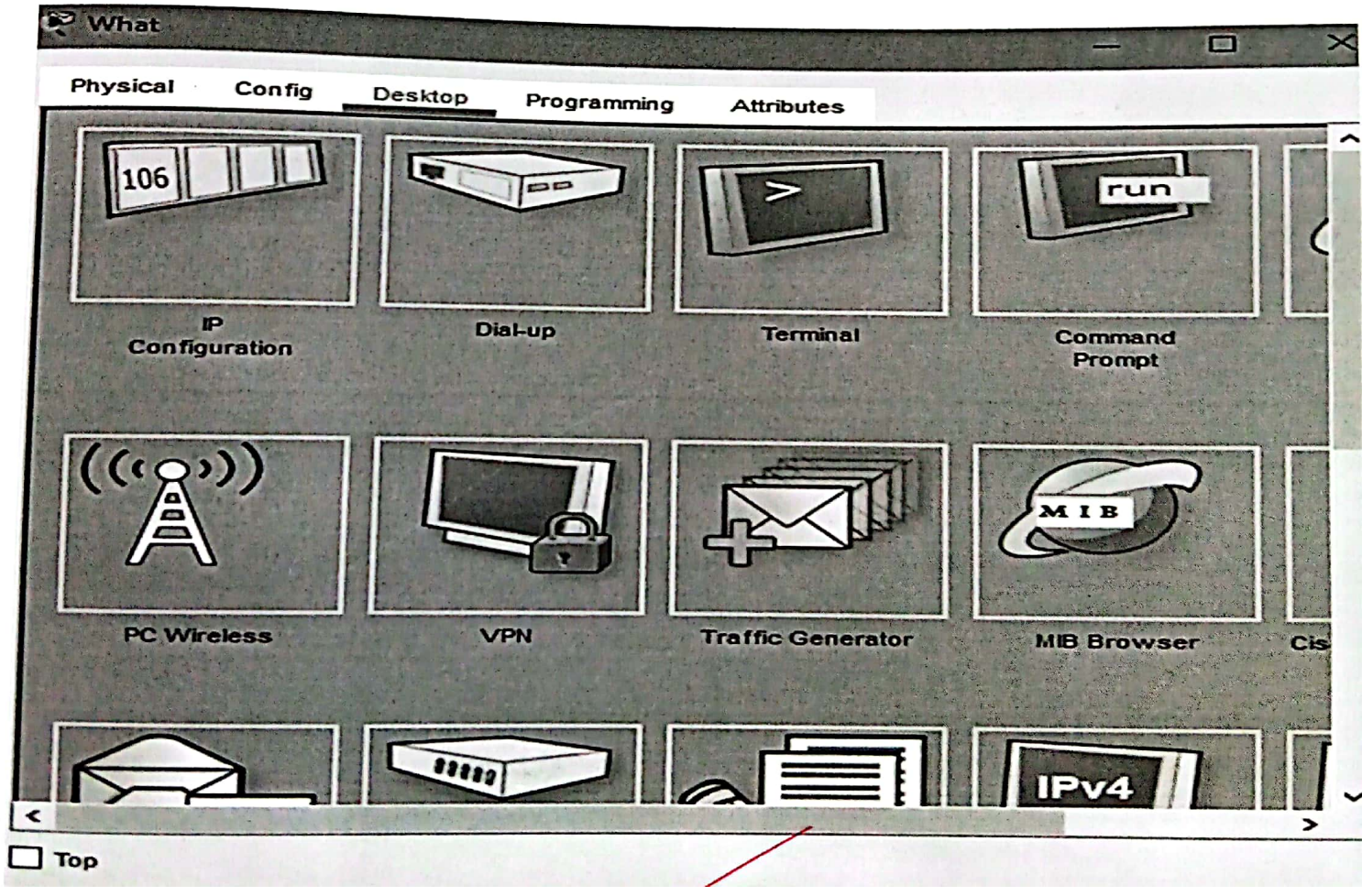
g) Pass the message packet from one end devices
to other end device. (If it shows successful the
design is valid and error less.)

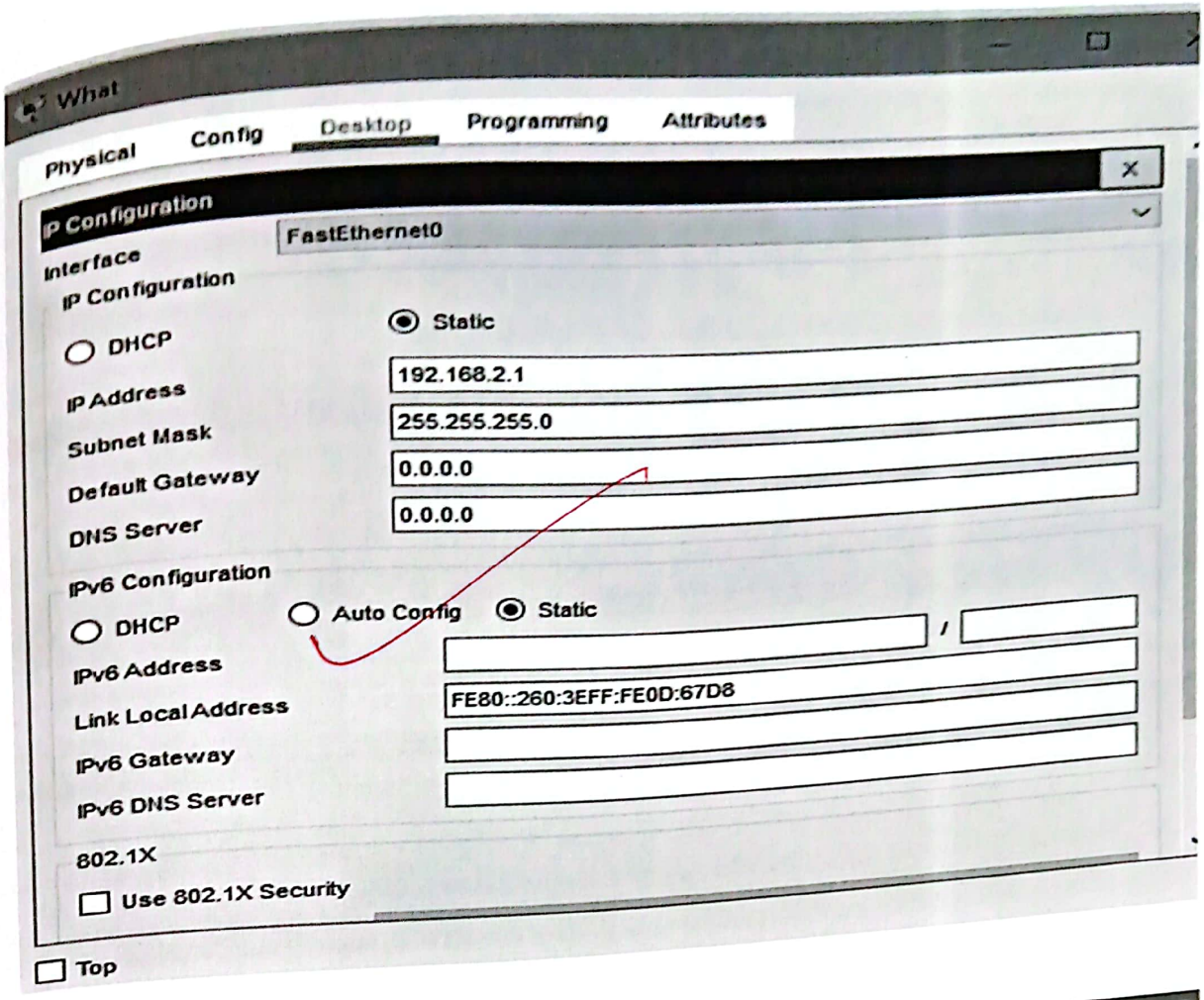
h) Ping any one device IP address using command
Prompt.

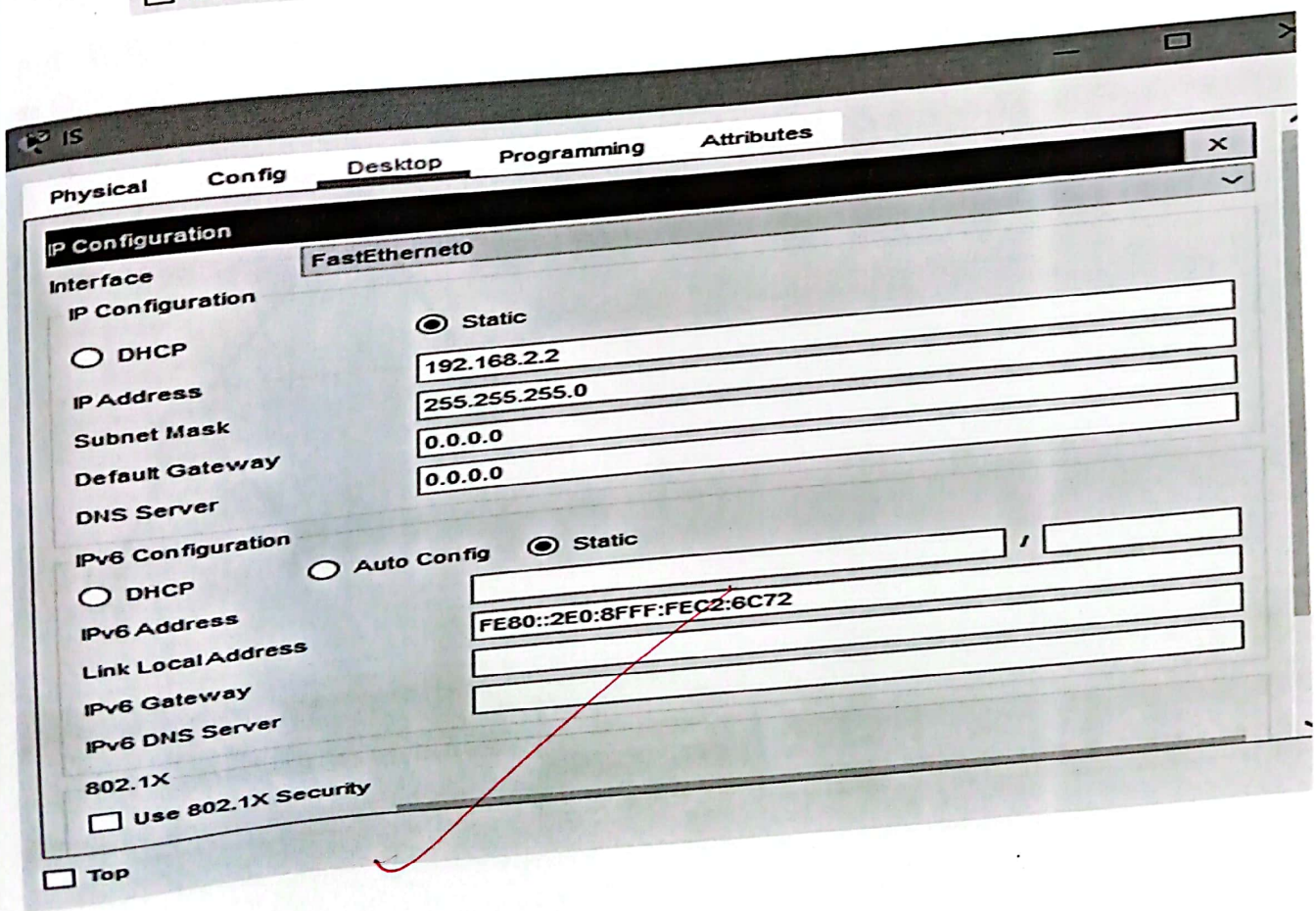
i) End.

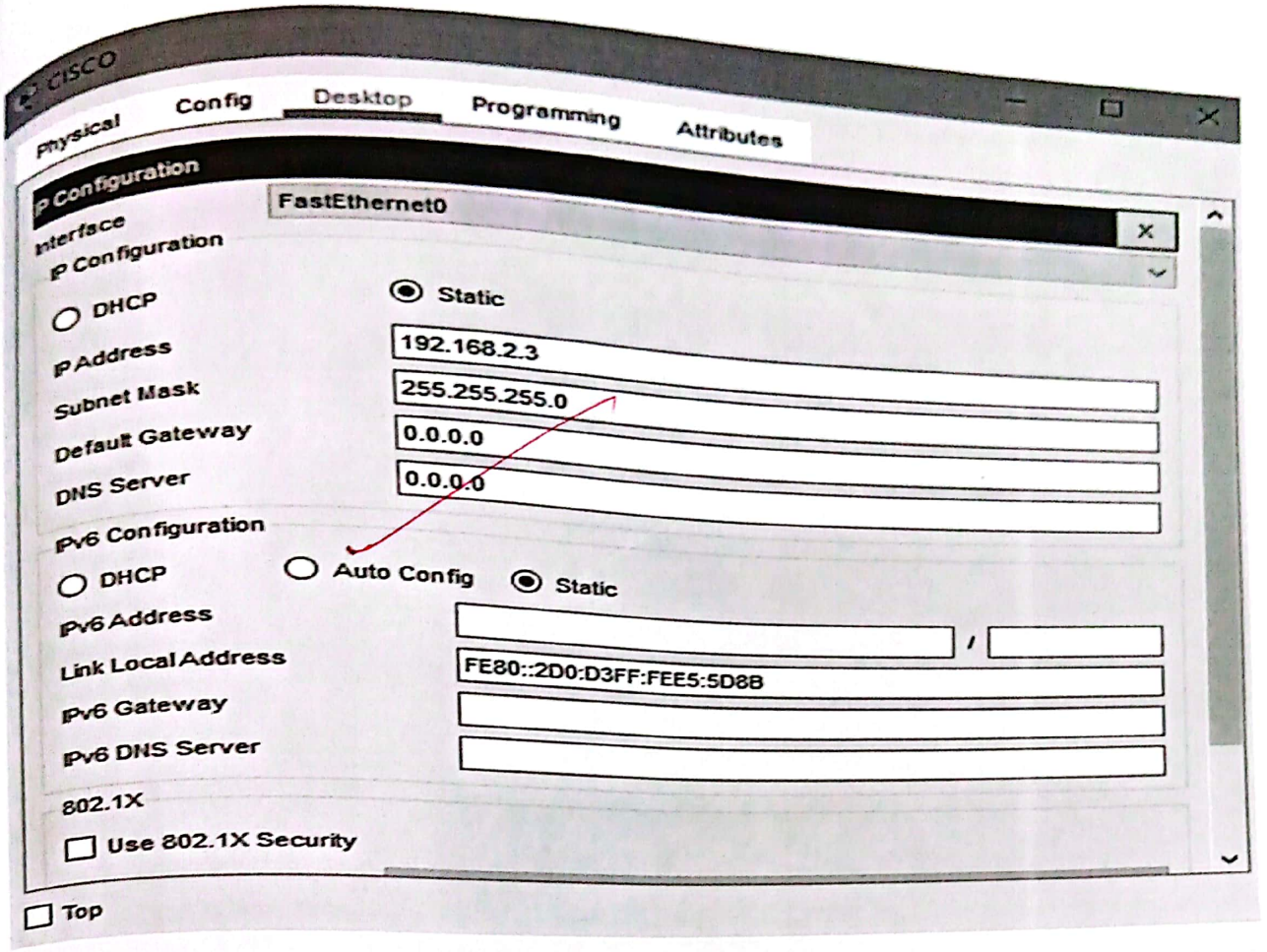
Screenshots of steps :

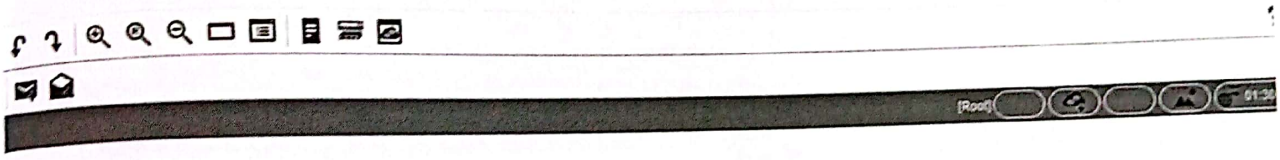


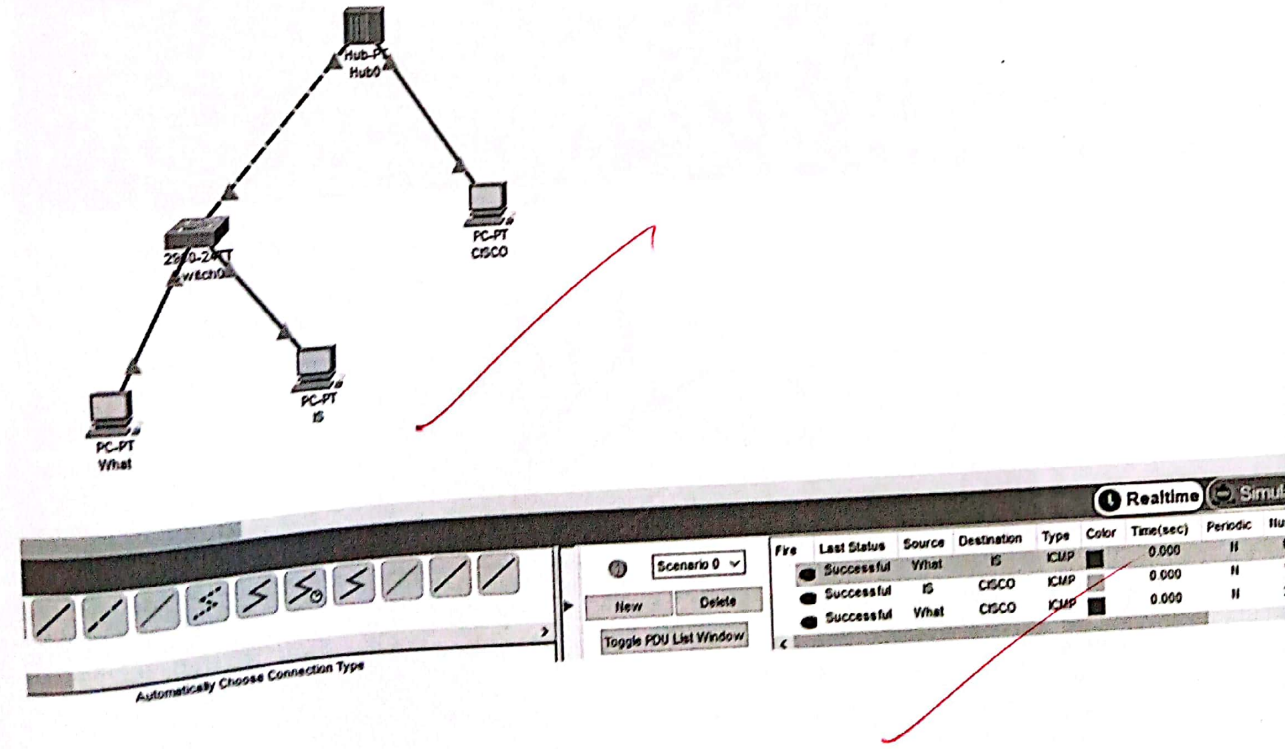



What
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::260:3EFF:FE0D:67D8
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


IS
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2E0:8FFF:FEC2:6C72
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:D3FF:FEE5:5D8B
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top




Hub-PT
Hub0
PC-PT
CISCO
PC-PT
IS
PC-PT
What

Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Successful
What
IS
ICMP
0.000
Successful
IS
CISCO
ICMP
0.000
Successful
What
CISCO
ICMP
0.000
Automatically Choose Connection Type

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

LABSHEET-10

Network Design with web server, switch, hub and end devices to implement the (dynamic IP design 4)-DHCP protocol implementation.

steps:

a) start.

b) Take 2 Host/End devices, a server & a switch for Network connection between them.

c) connect them using connection wire.

d) click on server > services > HTTP and make both http and https on.

e) click on DHCP and turn on services.

f) enter the starting IP address and its subnet mask and save it.

g) Now, Server > Desktop and configure the IPv4 addres ss in statically.

h) click on end Device > Desktop and turn on DHCP (server will automatically generate the IP address for end device follow this step.)

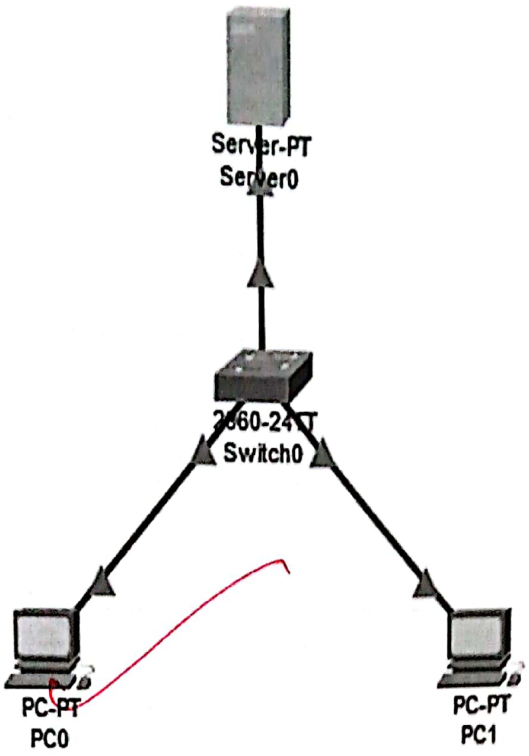
i) Repeat step h for each end device.

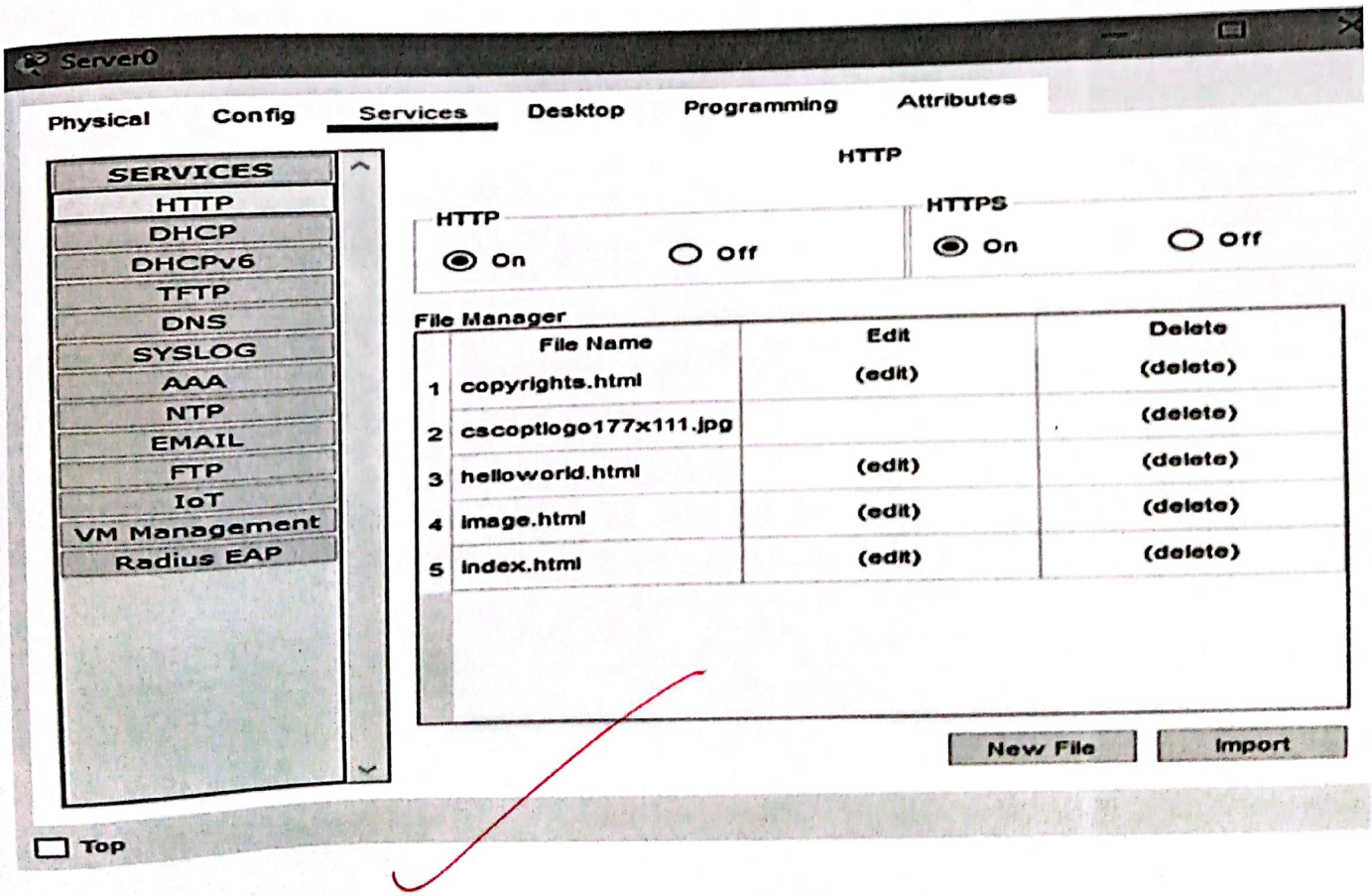
j) Pass the Message packet from one end device to other end device (If it shows successful the design is valid and error less.)

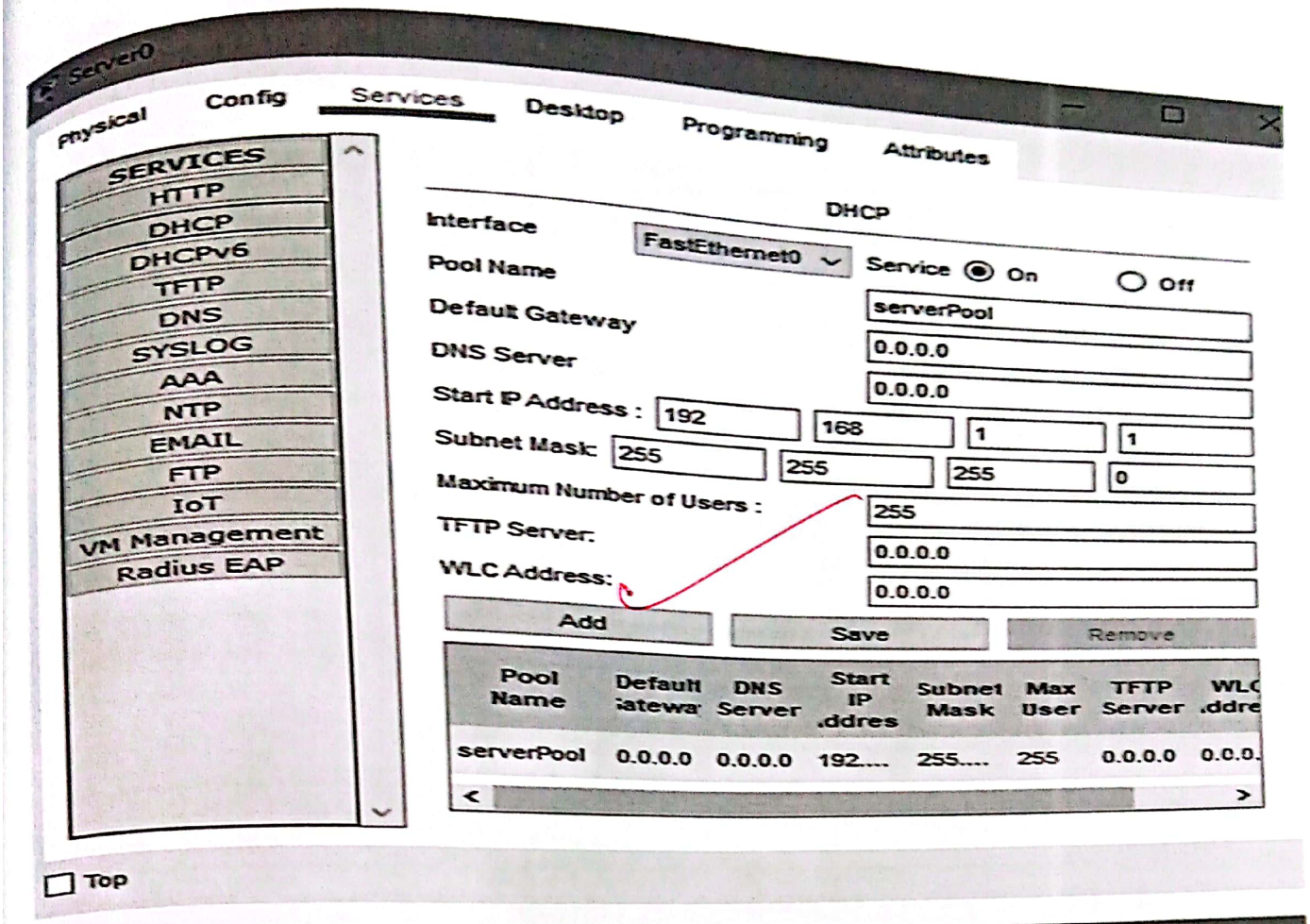
k) Ping any one device IP address using command Prompt.

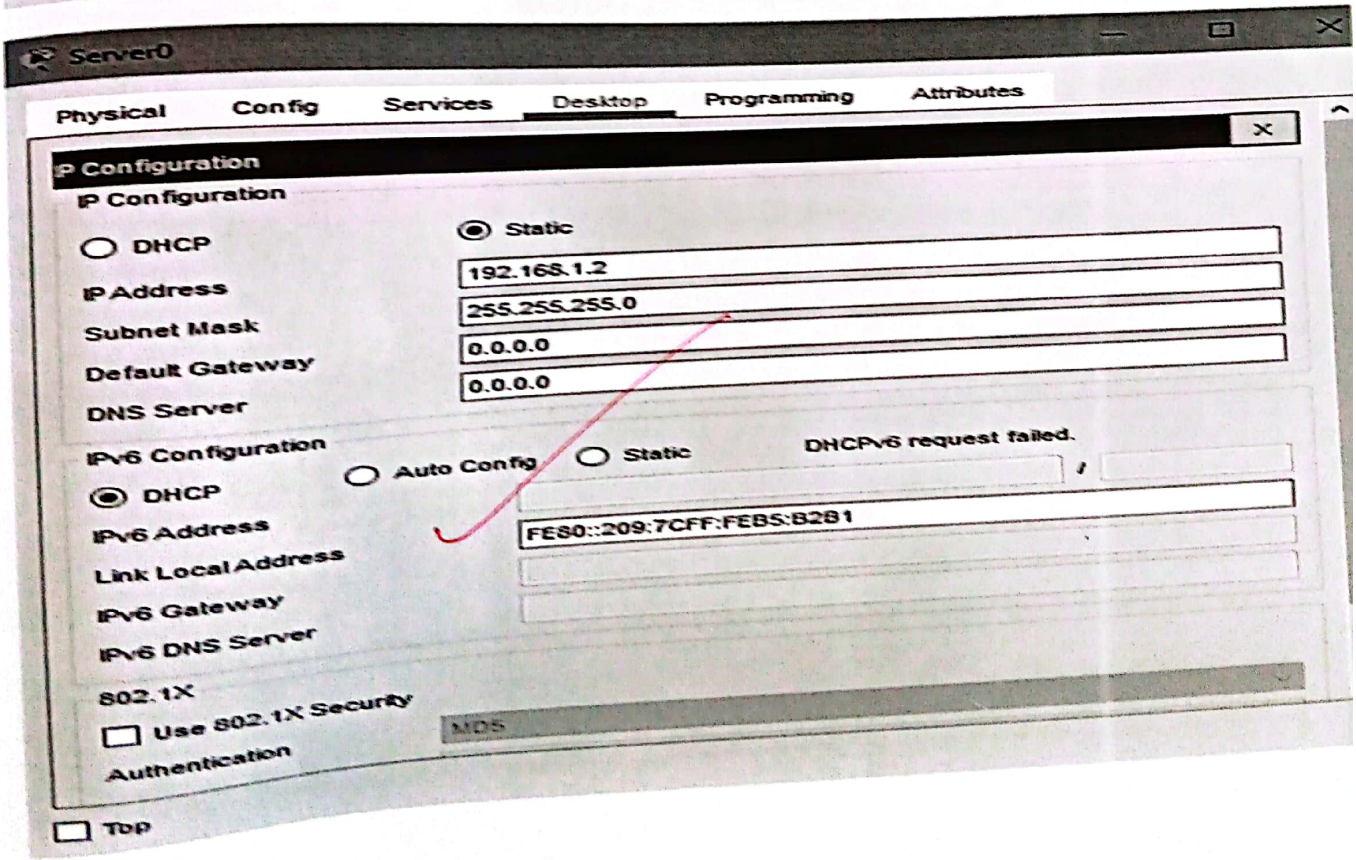
l) End.

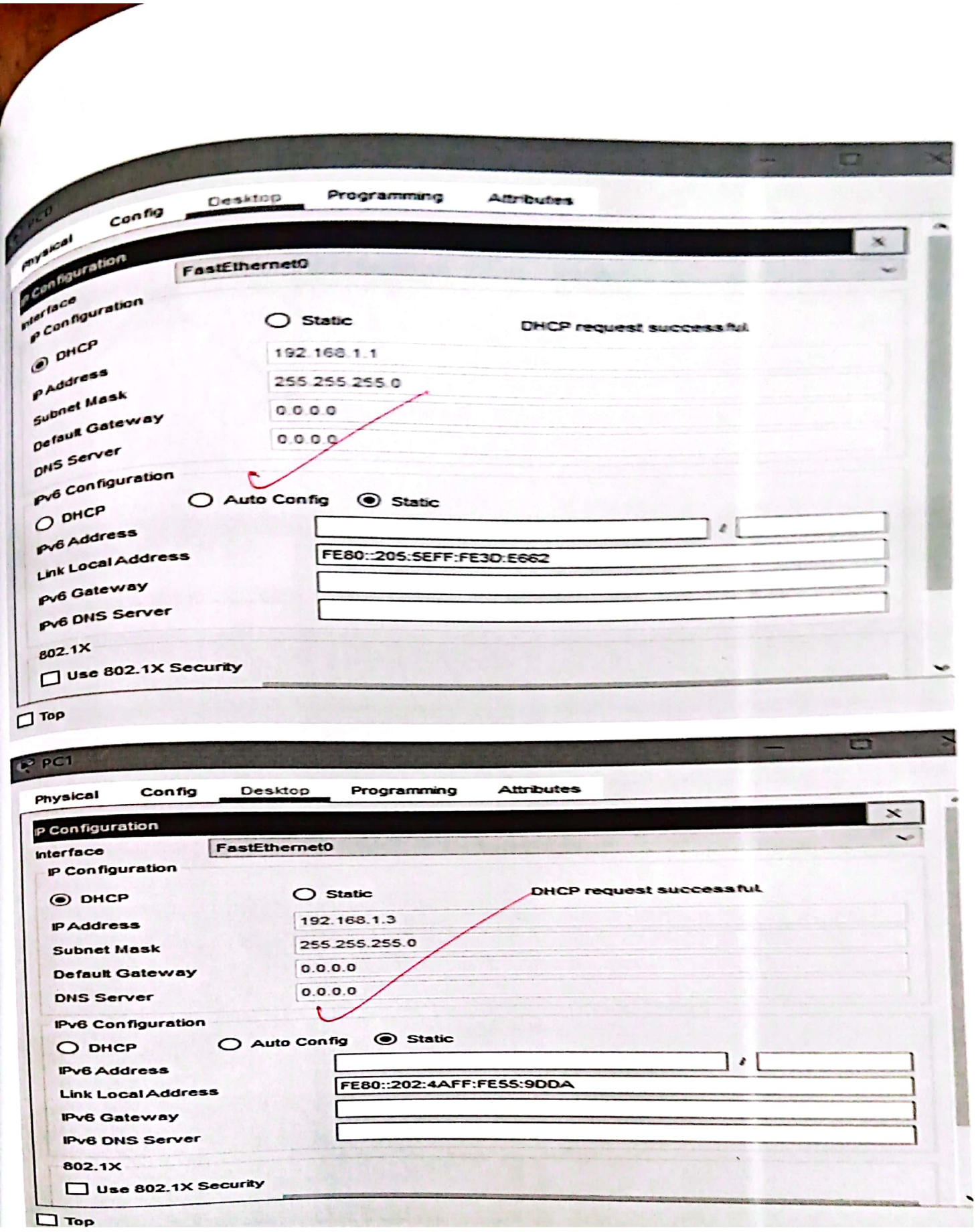
Screenshots of steps:

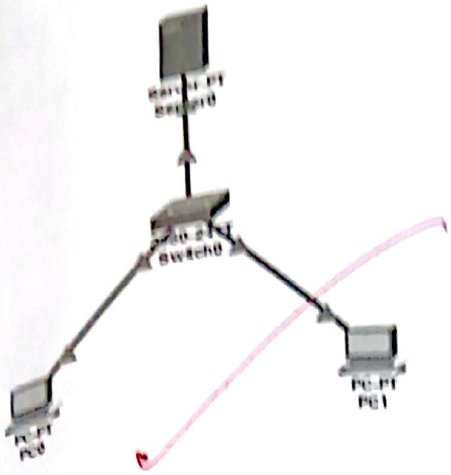


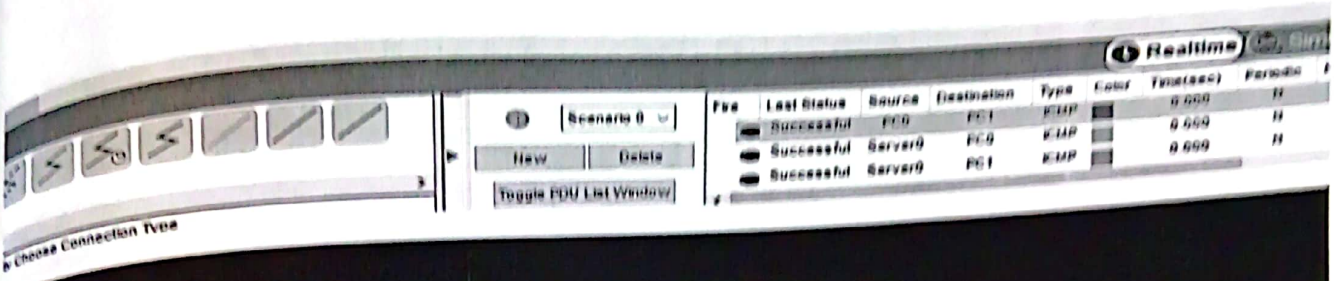



Server0
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface
FastEthernet0
Service
On
Off
Pool Name
serverPool
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
Start IP Address :
192
168
1
1
Subnet Mask:
255
255
255
0
Maximum Number of Users :
255
TFTP Server:
0.0.0.0
WLC Address:
0.0.0.0
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
WLC Address
serverPool
0.0.0.0
0.0.0.0
192....
255....
255
0.0.0.0
0.0.0.
Top


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
DHCPv6 request failed.
IPv6 Address
FE80::209:7CFF:FEB5:B281
Link Local Address
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::205:5EFF:FE3D:E662
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::202:4AFF:FE5S:9DDA
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top





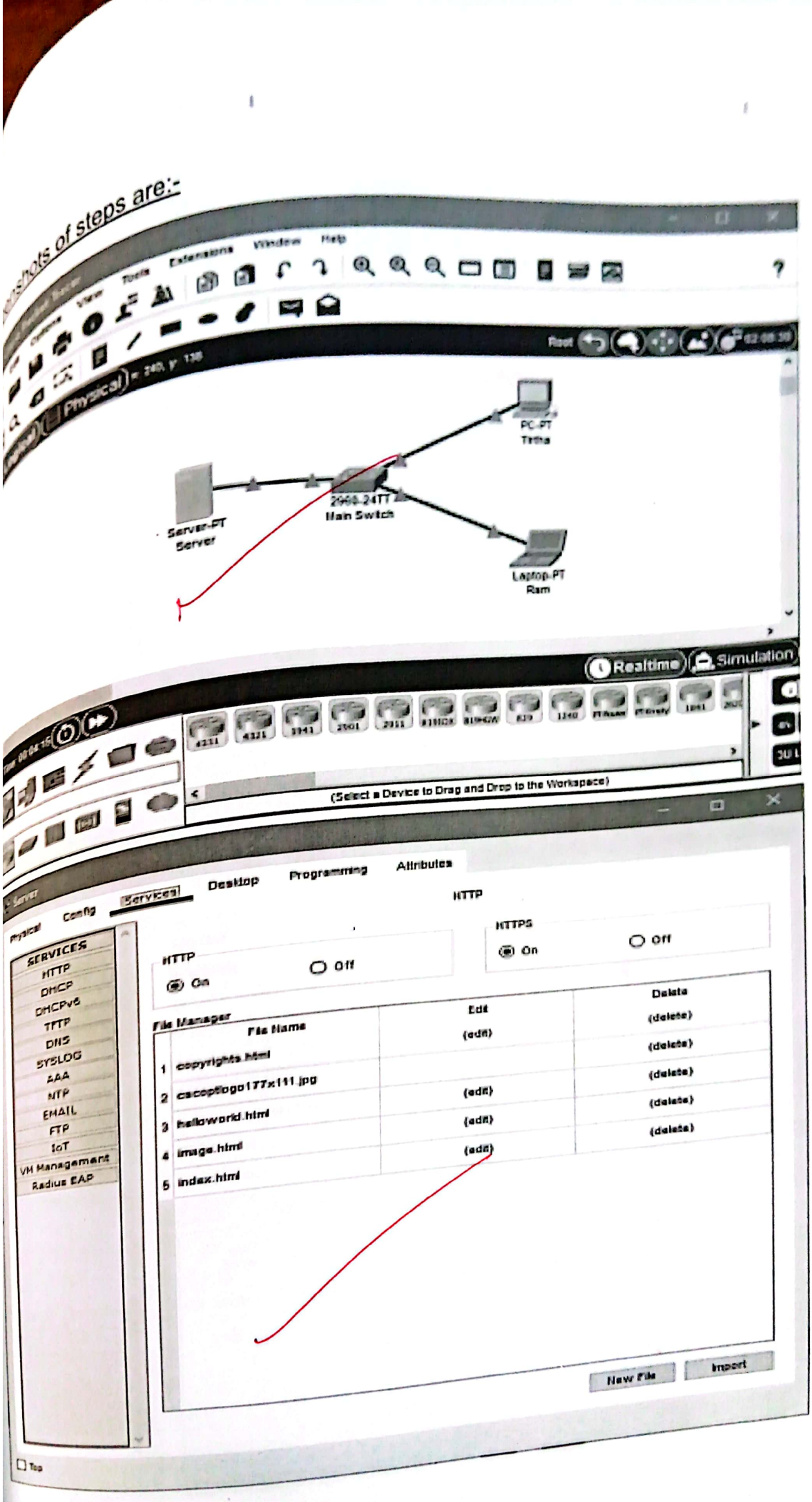

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=5ms TTL=128
Reply from 192.168.1.1: bytes=32 time=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 6ms
```

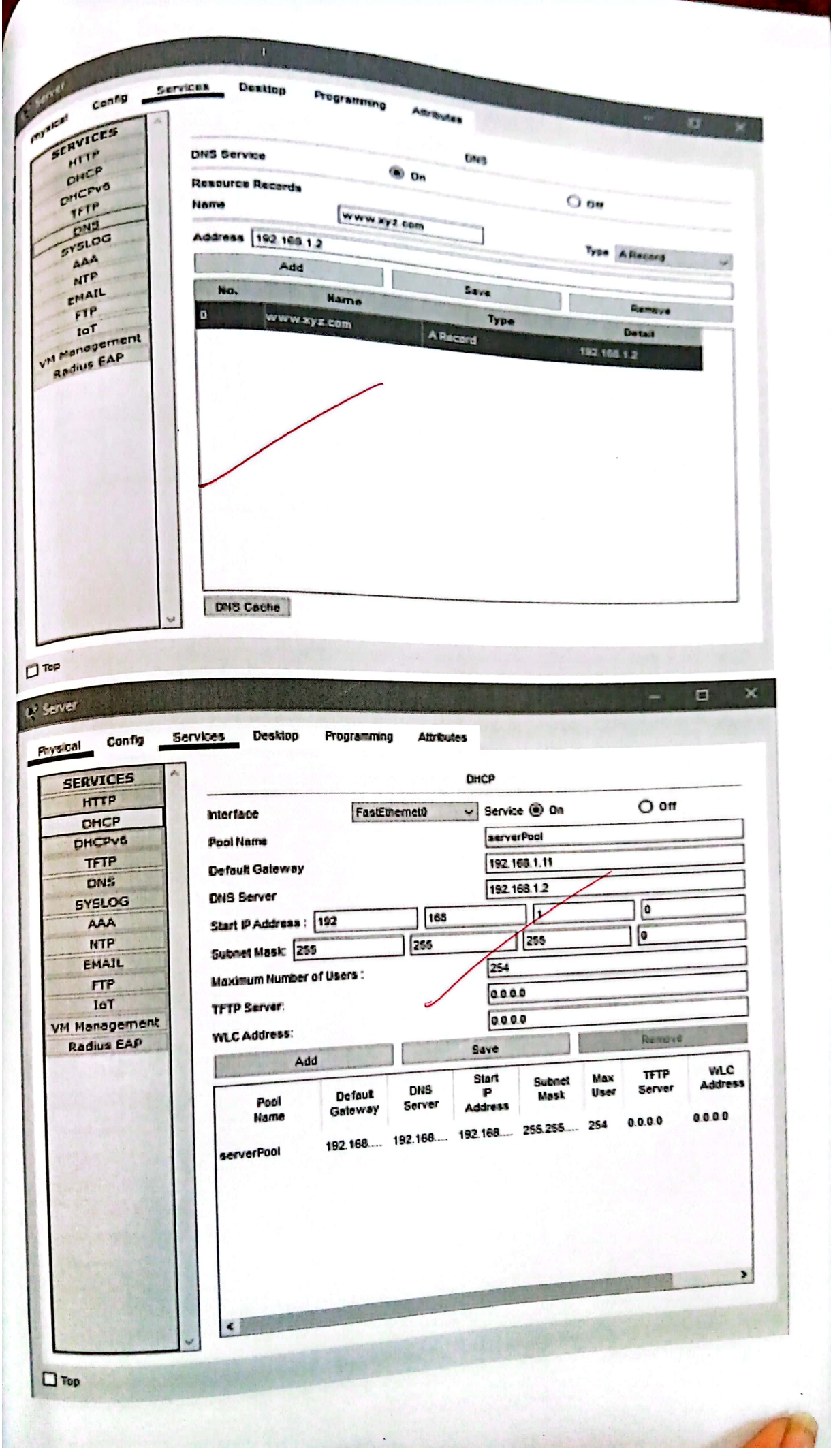
LAB-11

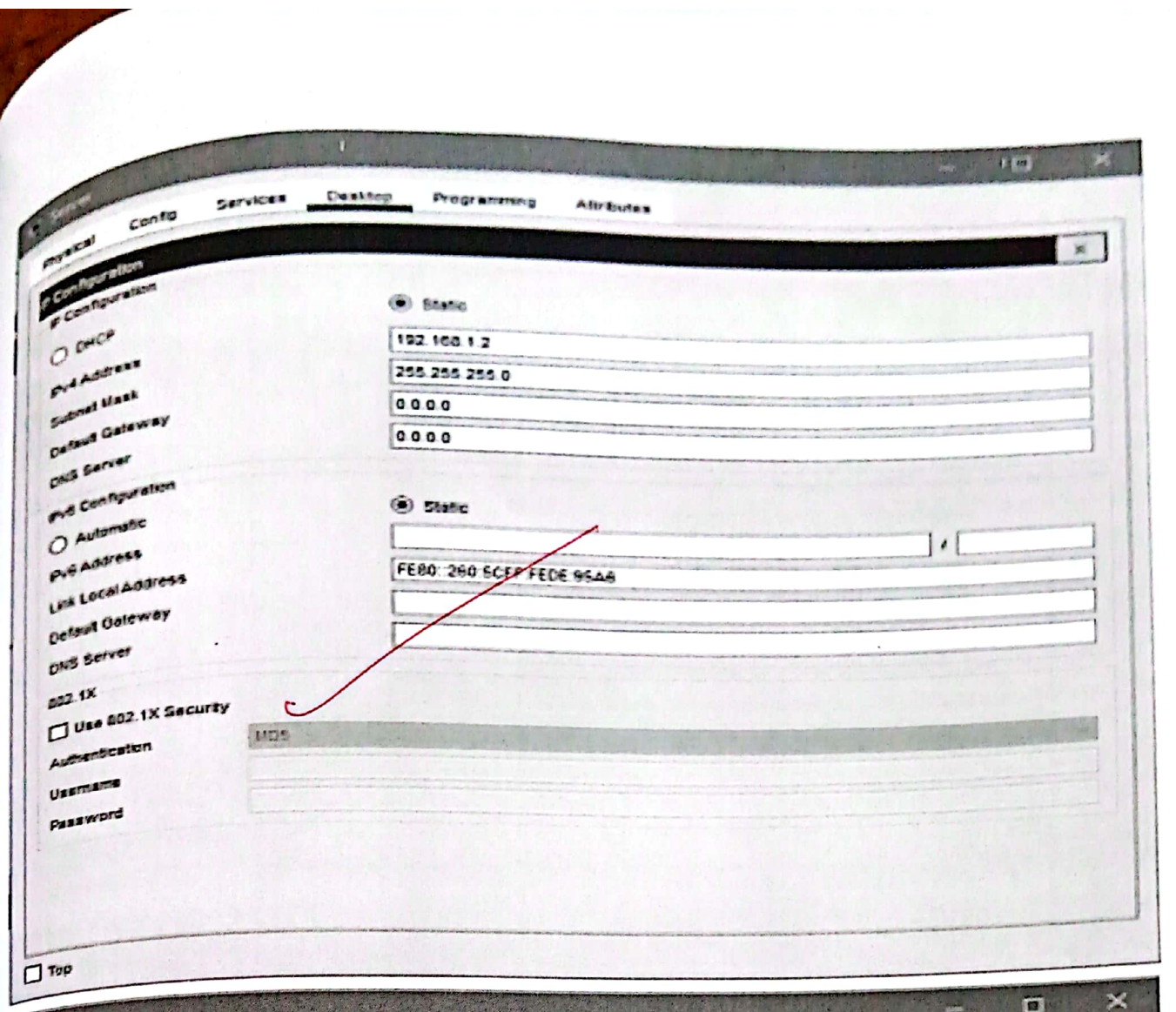
Network Design with web server, switch and end devices implement the (dynamic IP design 4). DNS and DHCP protocol implementation.

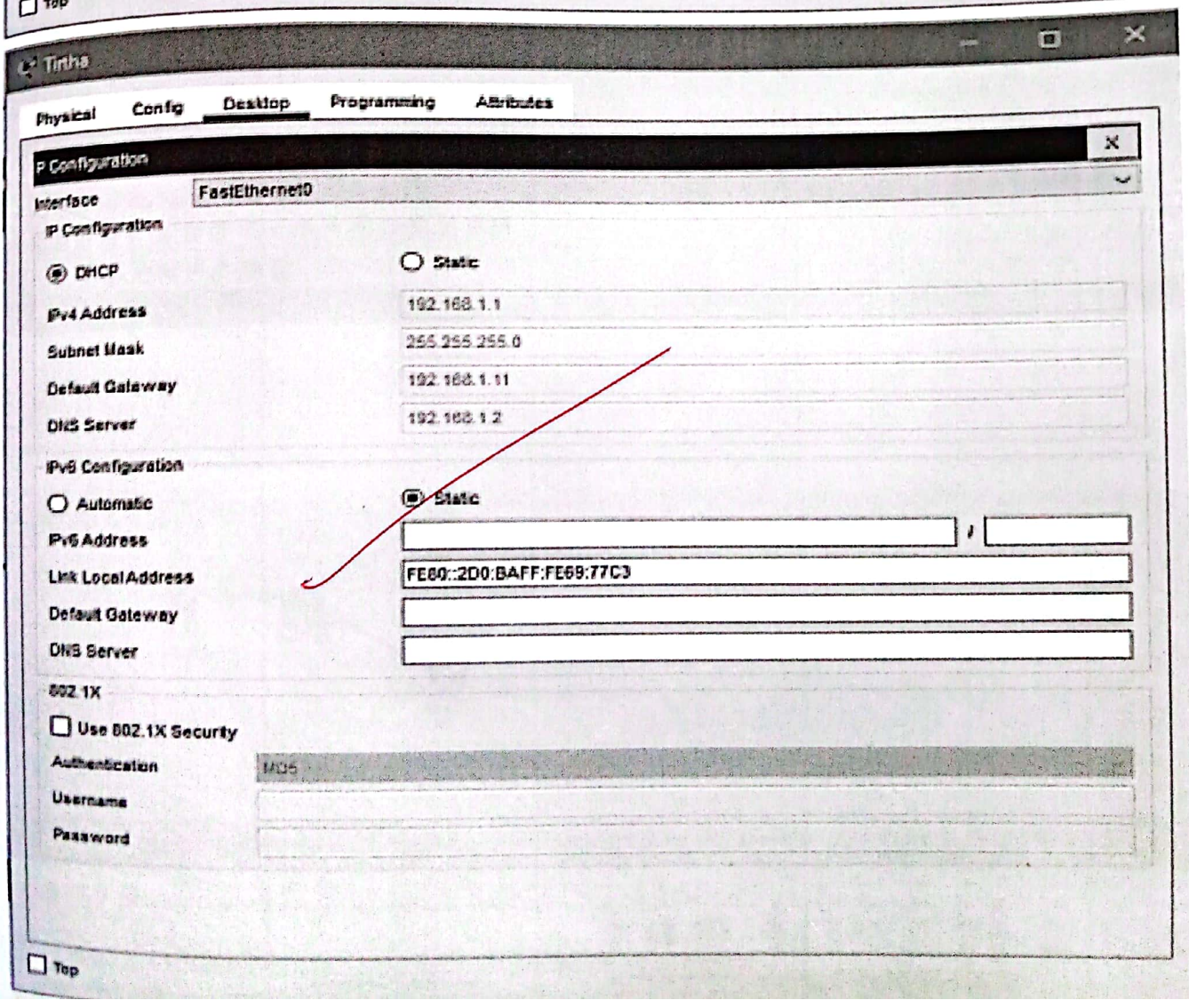
Steps:-

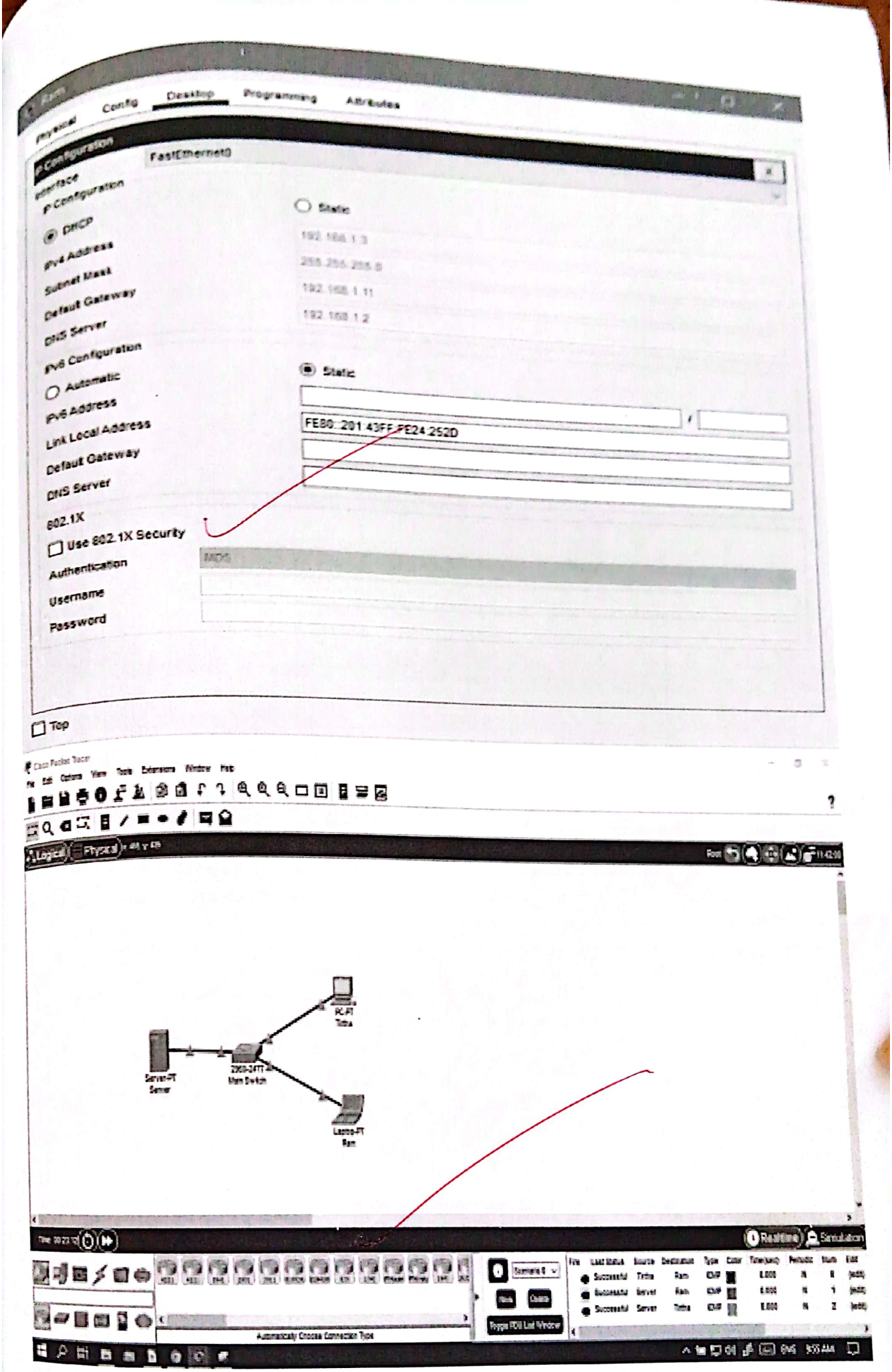
1. Start
2. Take 2 host, a server and a switch for network connection between them.
3. Connect them using connecting wire.
4. Click on server > service > HTTP and make both http and https on.
5. Click on DNS and DHCP service. Give a URL name i.e. domain name (eg. xyz.com) and IP address for domain name after that add and save.
6. Click on DHCP and turn on service.
7. Enter starting IP address, its subnet, default gateway and DNS address and save it.
8. Now, server > Desktop and configure the IPv4 address in statically.
9. Click on End device > Desktop and turn on DHCP.
10. Repeat step 9 for each end device.
11. Pass message packet from one end device to other end device (If success design is valid)
12. Ping any one device IP address using command Prompt.
13. Click on any end device > Desktop > webbrowser, type your url/domain name i.e. www.xyz.com or ip address for DNS (If web page opens than DNS is functioning good.)
14. Stop.


shots of steps are:-
PC-PT
Tirtha
2960-24TT
Main Switch
Server-PT
Server
Laptop-PT
Ram
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Physical
Config
Services
Desktop
Programming
Attributes
HTTP
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 copyrights.html (edit) (delete)
2 cscoptlogo177x111.jpg (delete)
3 helloworld.html (edit) (delete)
4 image.html (edit) (delete)
5 index.html (edit) (delete)
New File
Import

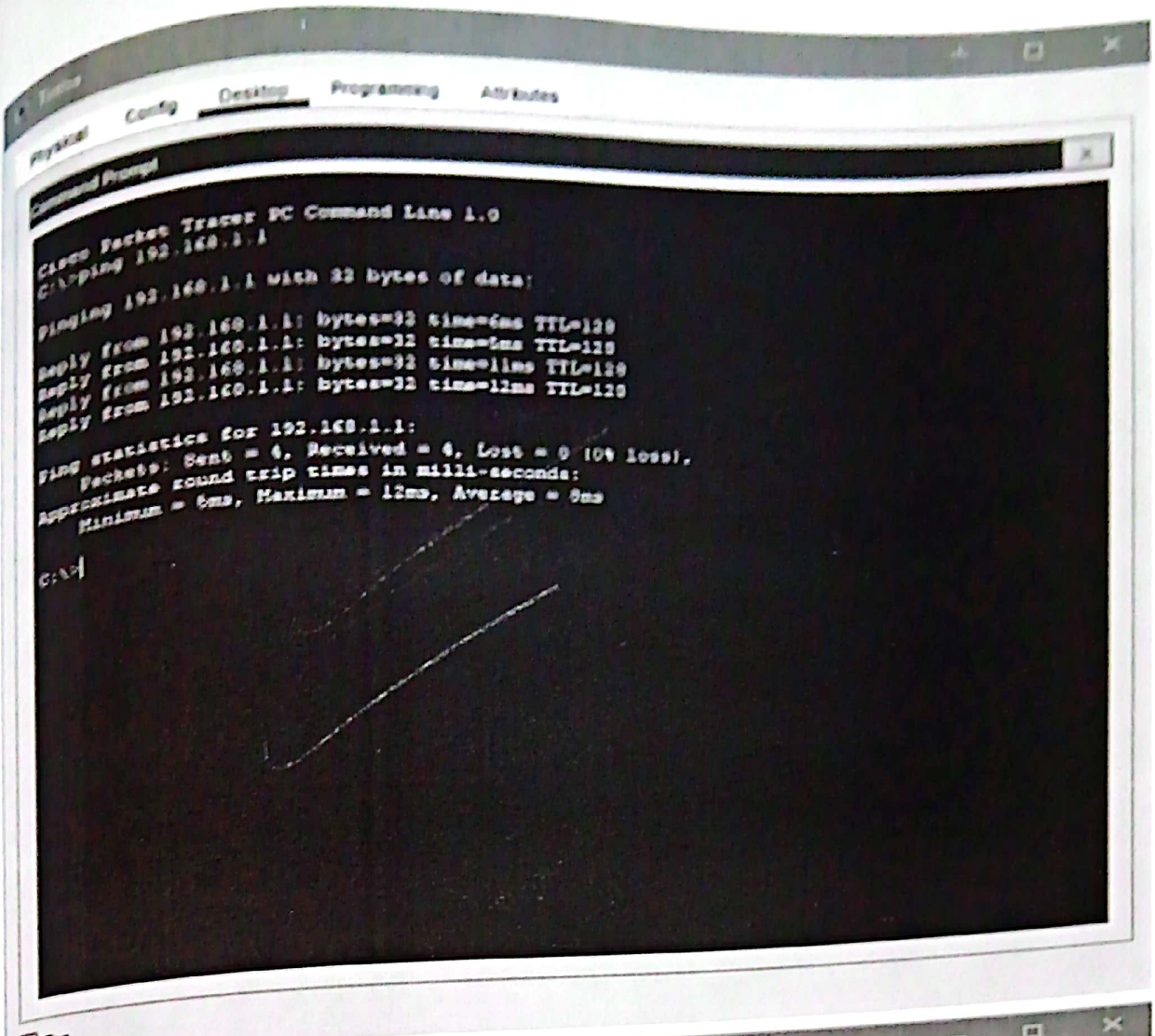

Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS Service
On
Off
Resource Records
Name
www.xyz.com
Address
192.168.1.2
Type
A Record
Add
Save
Remove
No.
Name
Type
Detail
0
www.xyz.com
A Record
192.168.1.2
DNS Cache
Top
Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface
FastEthernet0
Service
On
Off
Pool Name
serverPool
Default Gateway
192.168.1.11
DNS Server
192.168.1.2
Start IP Address :
192
168
1
0
Subnet Mask:
255
255
255
0
Maximum Number of Users :
254
TFTP Server:
0.0.0.0
WLC Address:
0.0.0.0
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
WLC Address
serverPool
192.168....
192.168....
192.168....
255.255....
254
0.0.0.0
0.0.0.0
Top

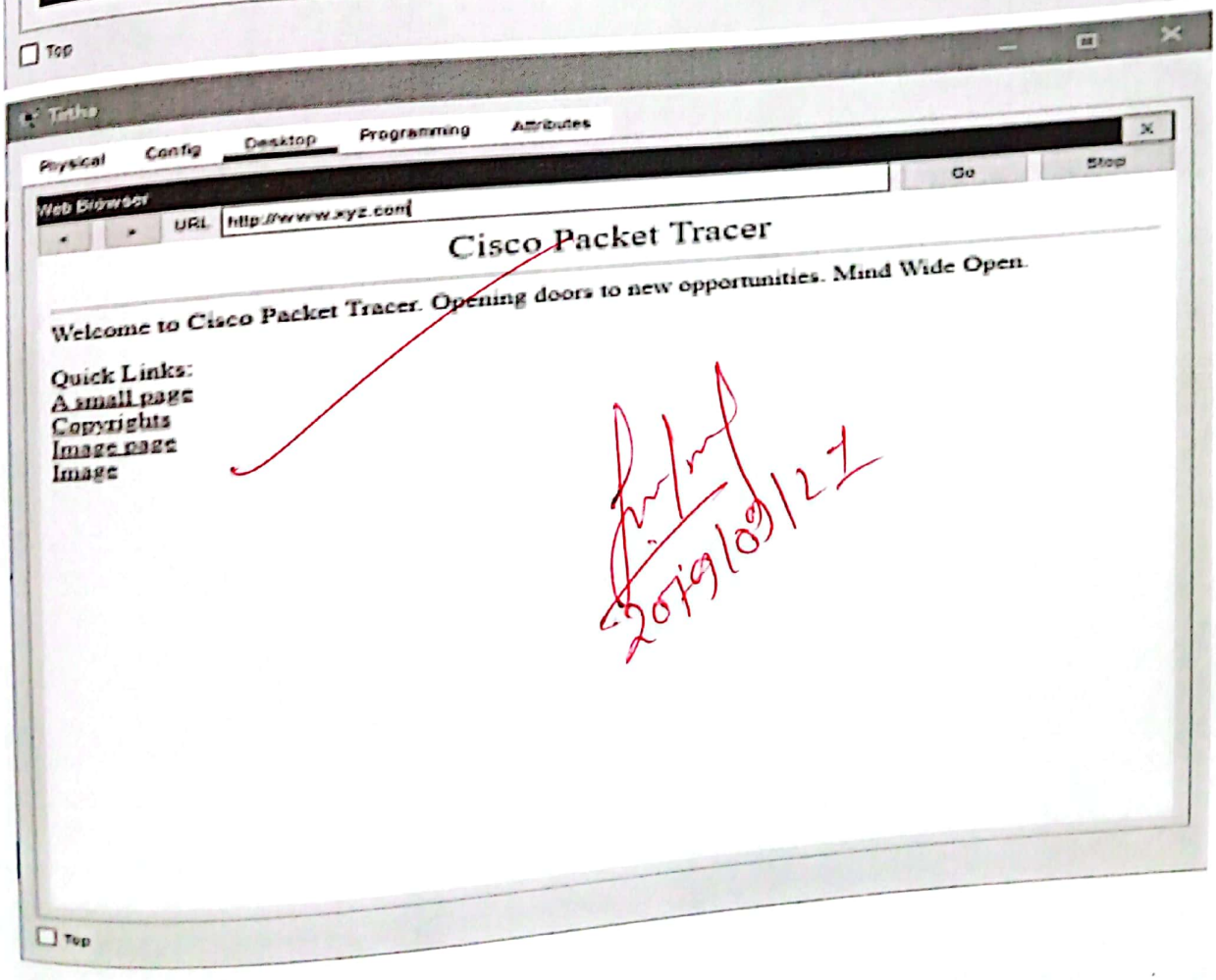

Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::260:5CEF:FEDE:9548
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Tinha
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.11
DNS Server
192.168.1.2
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:BAFF:FE69:77C3
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Physical
Config
Desktop
Programming
Attributes
IP Configuration
FastEthernet0
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.11
DNS Server
192.168.1.2
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FE24:252D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Logical
Physical
Realtime
Simulation
PC-PT
Server-PT
Server
Laptop-PT
Automatically Choose Connection Type


Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=6ms TTL=128
Reply from 192.168.1.1: bytes=32 time=5ms TTL=128
Reply from 192.168.1.1: bytes=32 time=11ms TTL=128
Reply from 192.168.1.1: bytes=32 time=12ms TTL=128
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 5ms, Maximum = 12ms, Average = 8ms
C:\>
Top


Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://www.xyz.com
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top

20/9/09/127

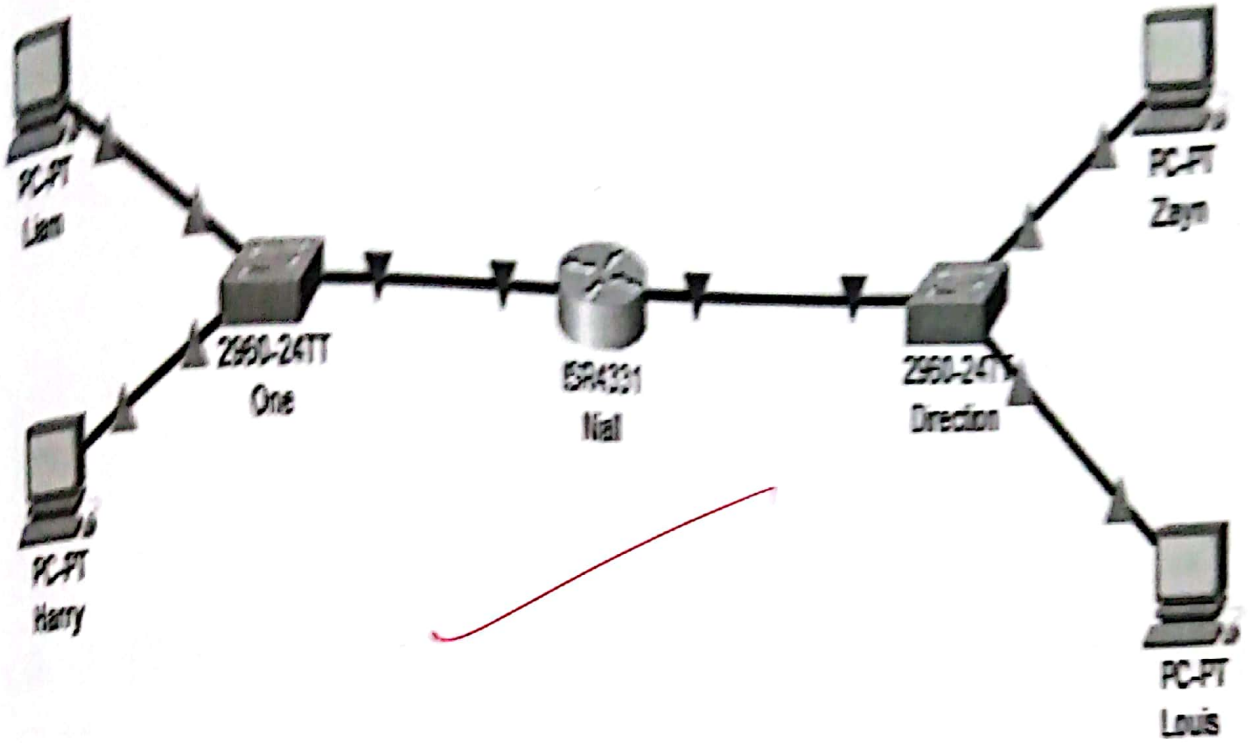
LAB-12

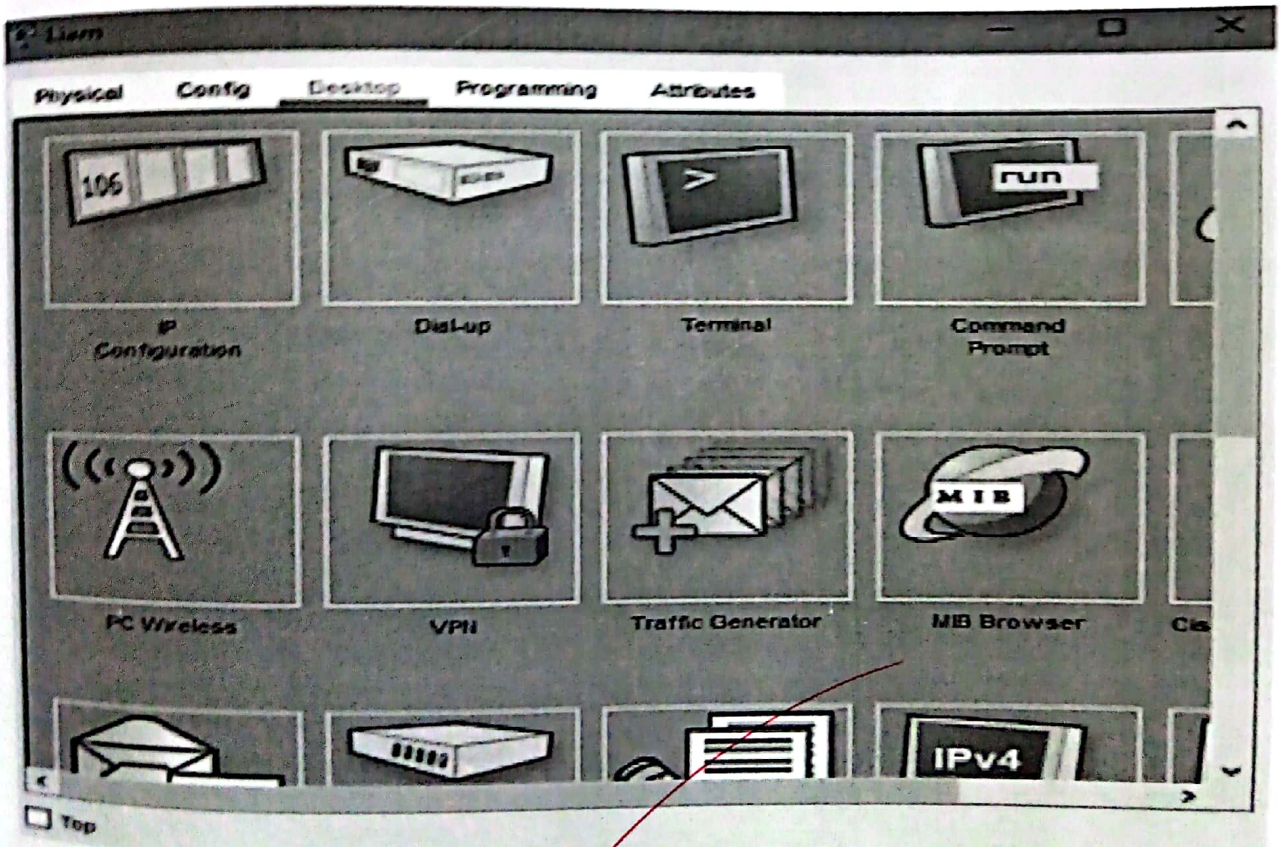
Configuration a router to connect two different networks having network address 192.168.2.1 and 192.168.1.1. Also implement RIP Protocol.

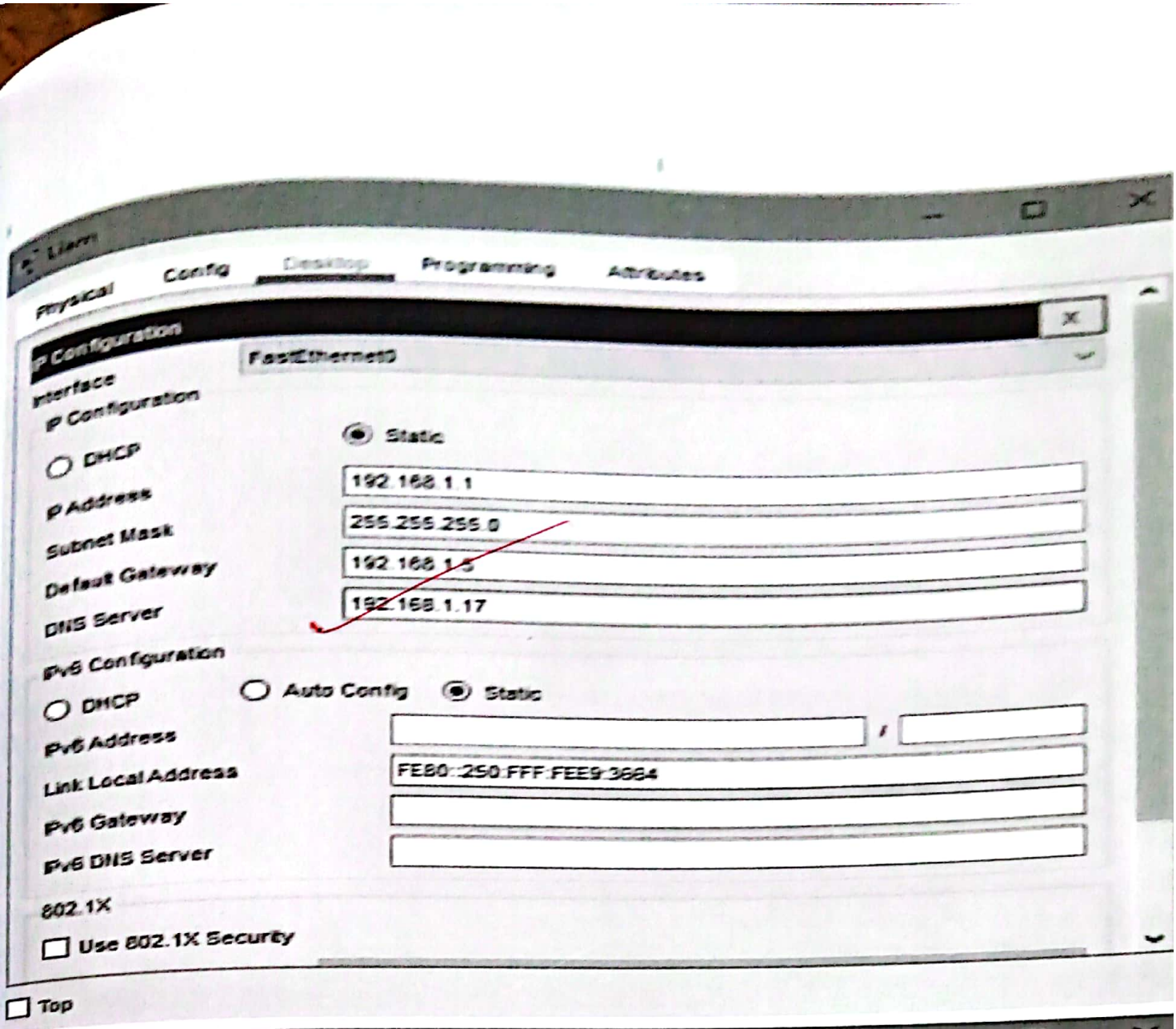
steps:

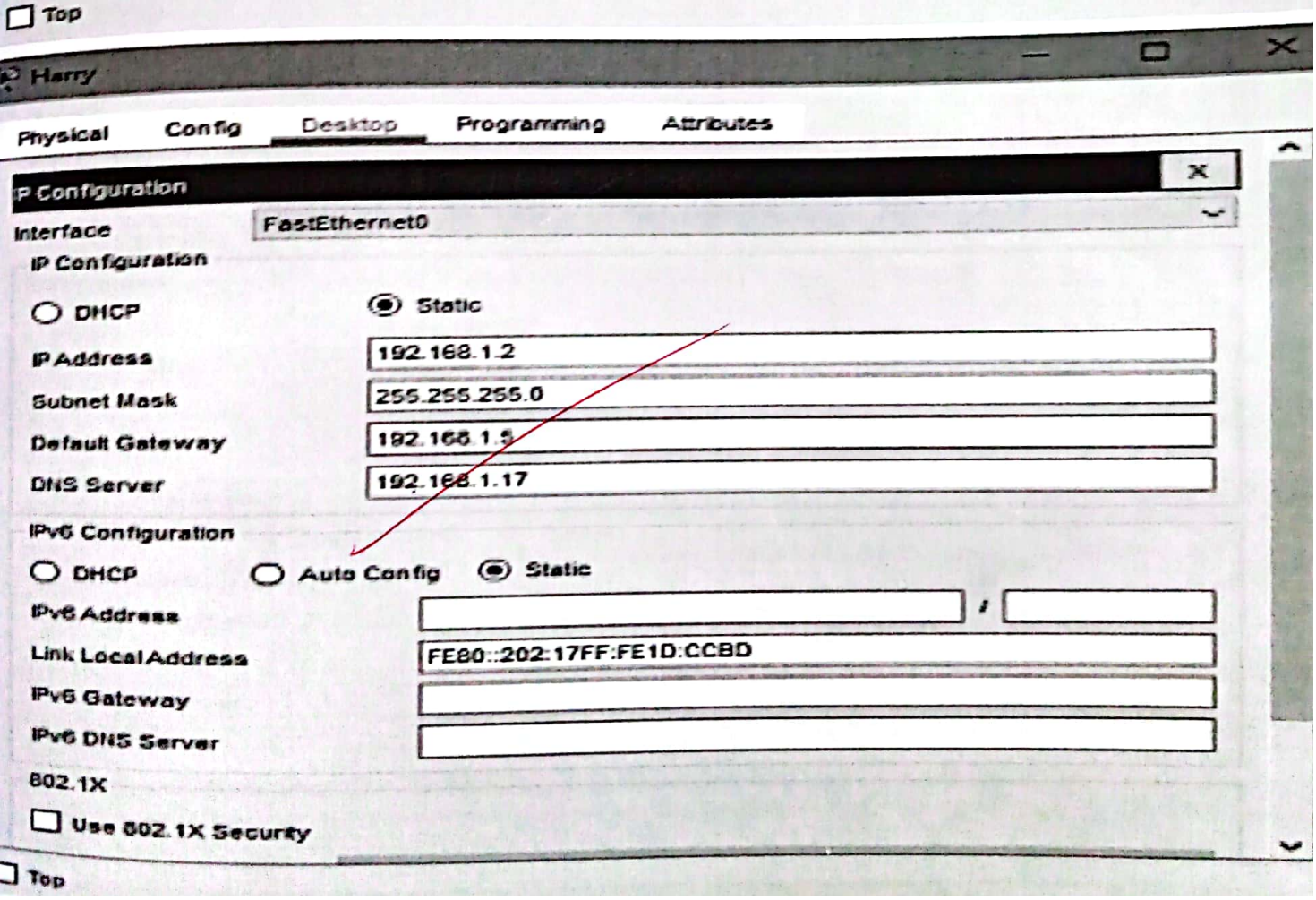
1. Start
2. Take 4 Host/End Devices, 2 switches and a Router for Network connection between them.
3. Connect them using connecting wire.
4. Configure different network IP statically of each End devices
5. Enter the class-C IP address at IPV4 and subnet it.
6. Repeat step (3-4) for other end devices.
7. Pass the message packet from one end devices to other end device (If it shows successful the design is valid and errorless.)
8. Ping any one device IP address using Command Prompt.
9. End.

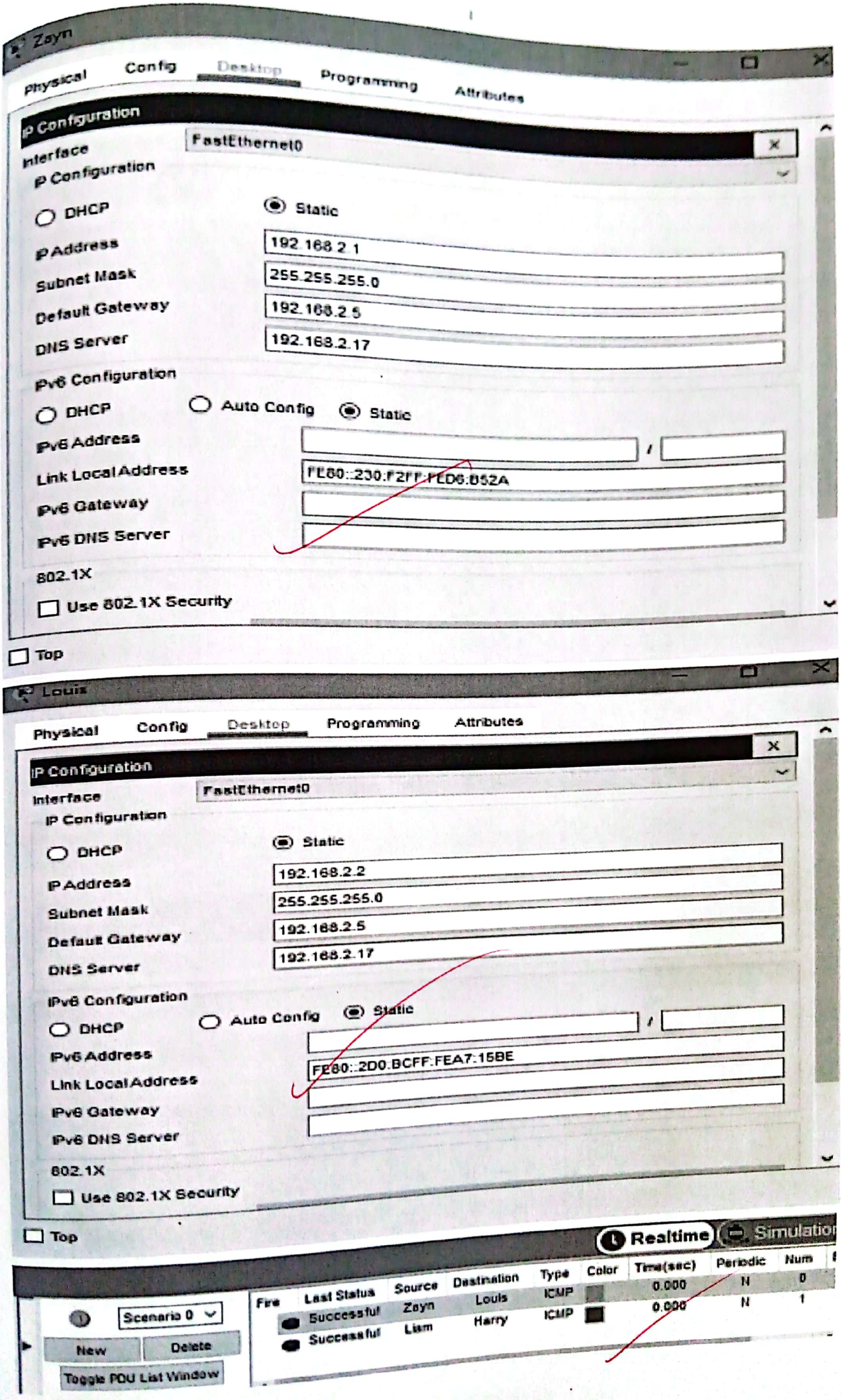
Screenshots of above steps are:

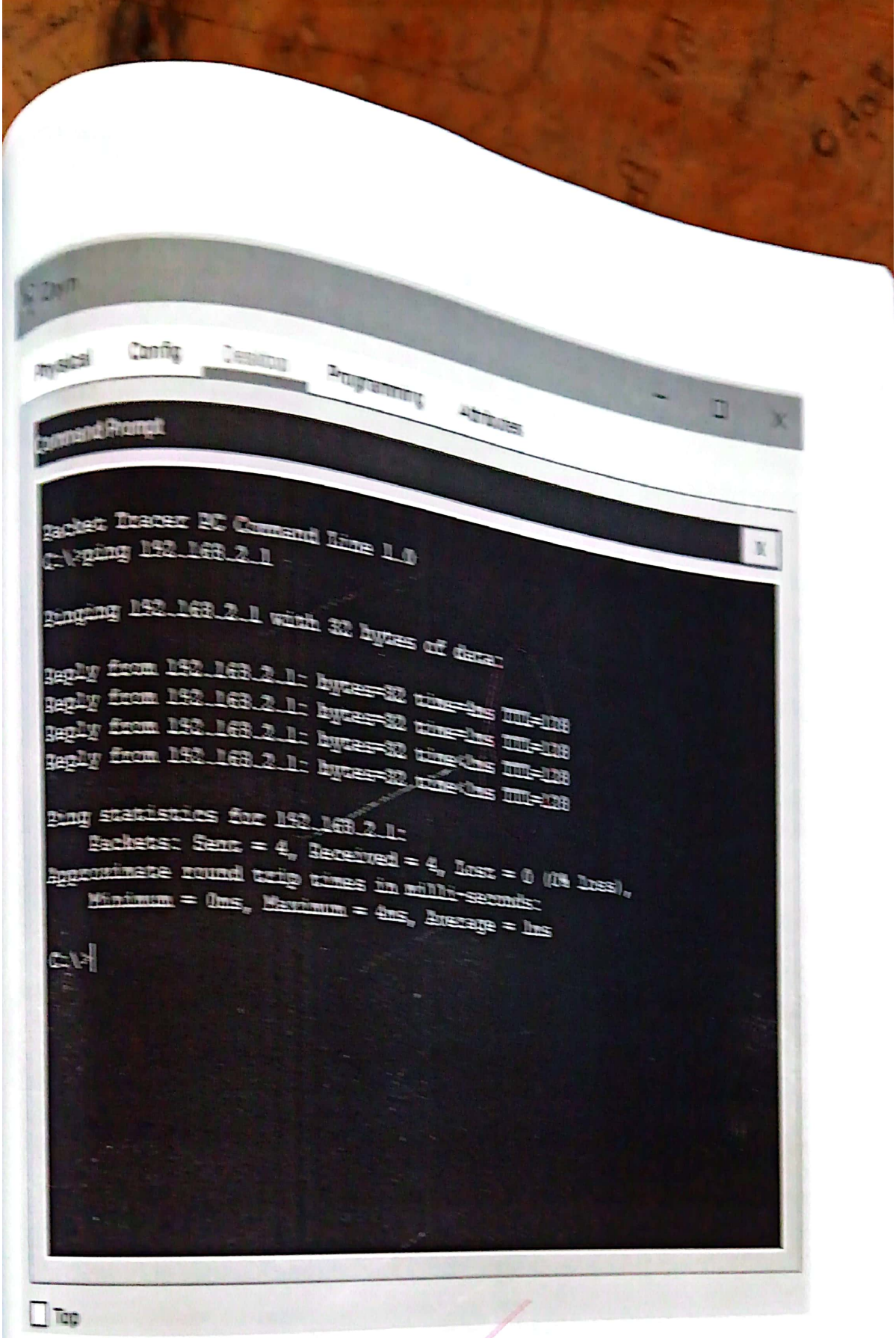





Liam
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.5
DNS Server
192.168.1.17
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::250:FFF:FEE9:3664
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


Harry
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.5
DNS Server
192.168.1.17
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::202:17FF:FE1D:CCBD
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top


Zayn
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.5
DNS Server
192.168.2.17
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::230:F2FF:FED6:852A
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Louis
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.5
DNS Server
192.168.2.17
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:BCFF:FEA7:15BE
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Realtime
Simulation
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Successful
Zayn
Louis
ICMP
0.000
N
0
Successful
Liam
Harry
ICMP
0.000
N
1
Scenario 0
New
Delete
Toggle PDU List Window



20/09/2021

1. Introduction

Wireshark is a powerful and widely used network protocol analyser tool that allows you to see what happening on you networks at a microscopic level. It is commonly used to troubleshoot network issues, as well as to secure networks by identifying and analysing network traffic.

Some key Properties of Wire Shark include.

- Capturing: Wire Shark allows you to capture live network traffic and save it for later analysis. You can choose to capture all traffic on a particular interface, or you can use a filter to only capture traffic of a specific type.
- Displaying: Wire Shark can display captured traffic in a variety of formats, including hexadecimal, ASCII, and raw data. It allows you to view the structure of individual packets and see the contents of each field in the packet.
- Filtering: Wire Shark has a power full filtering system that allows you to narrow down your captured traffic to only show what you're interested in. you can use filters based on various criteria, such as protocol, source and destination Ip address and port number.
- Decoding: Wire Shark can decode and dissect a wide variety of protocols, including Ethernet, ip, tcp and many others. This allows you to see the contents of packets at a much deeper level and understand how the protocols work.
- Analysing: Wire Shark has a number of built in tools for analysing captured traffic, including a packet reassembly tool, a sequence diagram generator, and a TCP stream graph. These tools can help you understand how the traffic on your network is behaving and identify any issues.

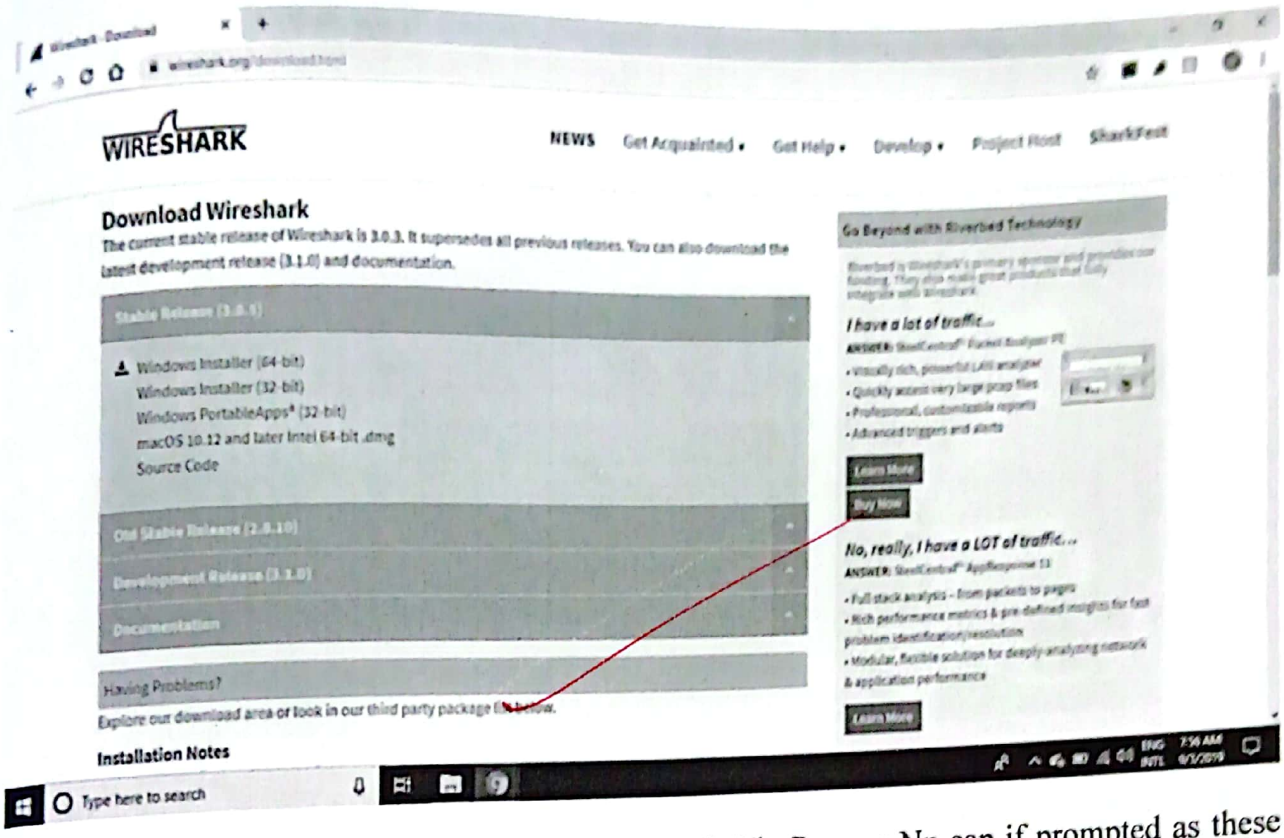
Overall, the result of using Wireshark is that you are able to gain a much deeper understanding of the traffic on your network and identify any issues that may be occurring. This can be extremely useful for troubleshooting network problems, as well as for securing your network by identifying and blocking malicious traffic.

- **Features of Wireshark**

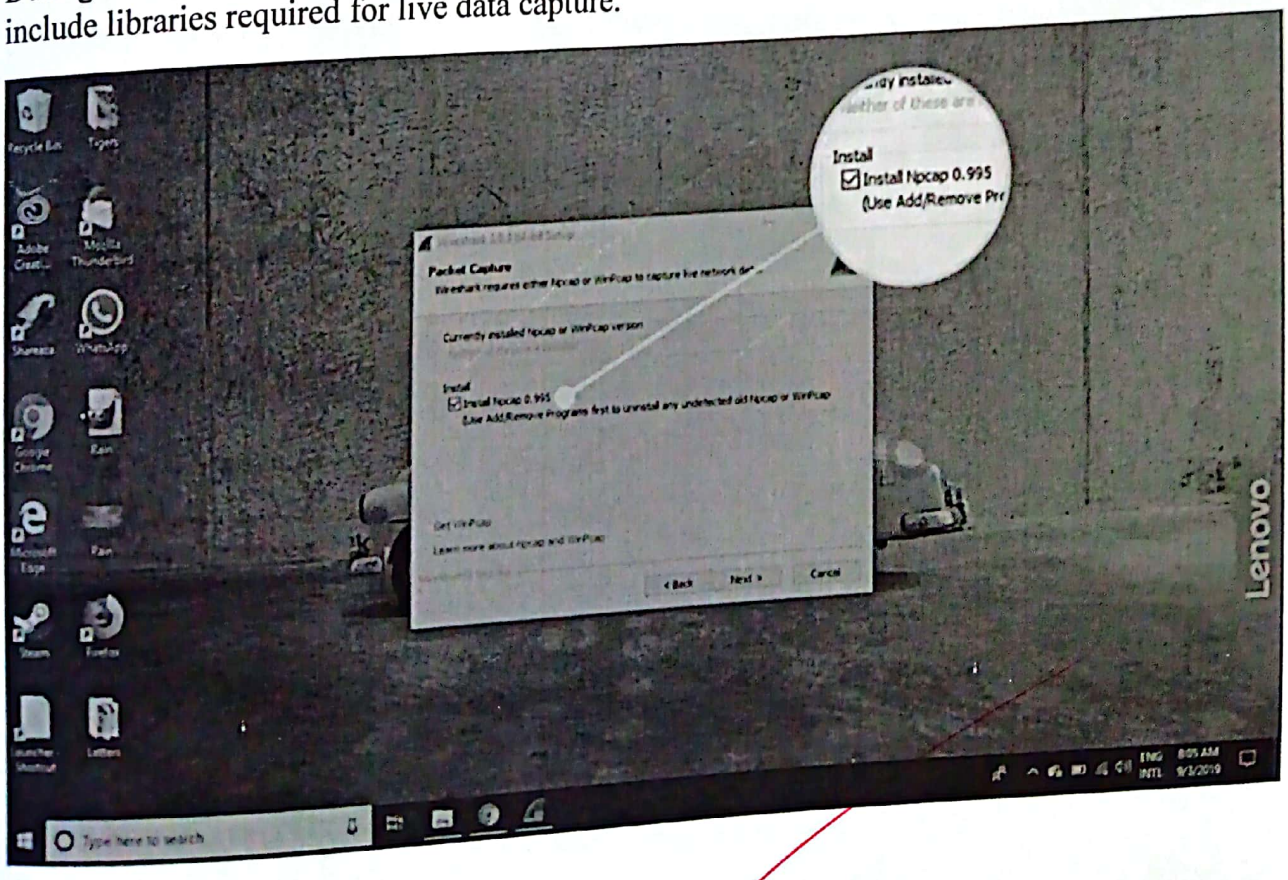
It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, Net BSD, etc.
It is a standard three-pane packet browser,
It performs deep inspection of the hundreds of protocols,
It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data,
It has sort and filter options which makes ease to the user to view the data.
It is also useful in VoIP analysis,
It can also capture raw USB traffic,
Various settings, like timers and filters, can be used to filter the output.
It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

2. HOW TO DOWNLOAD & INSTALL WIRE SHARK

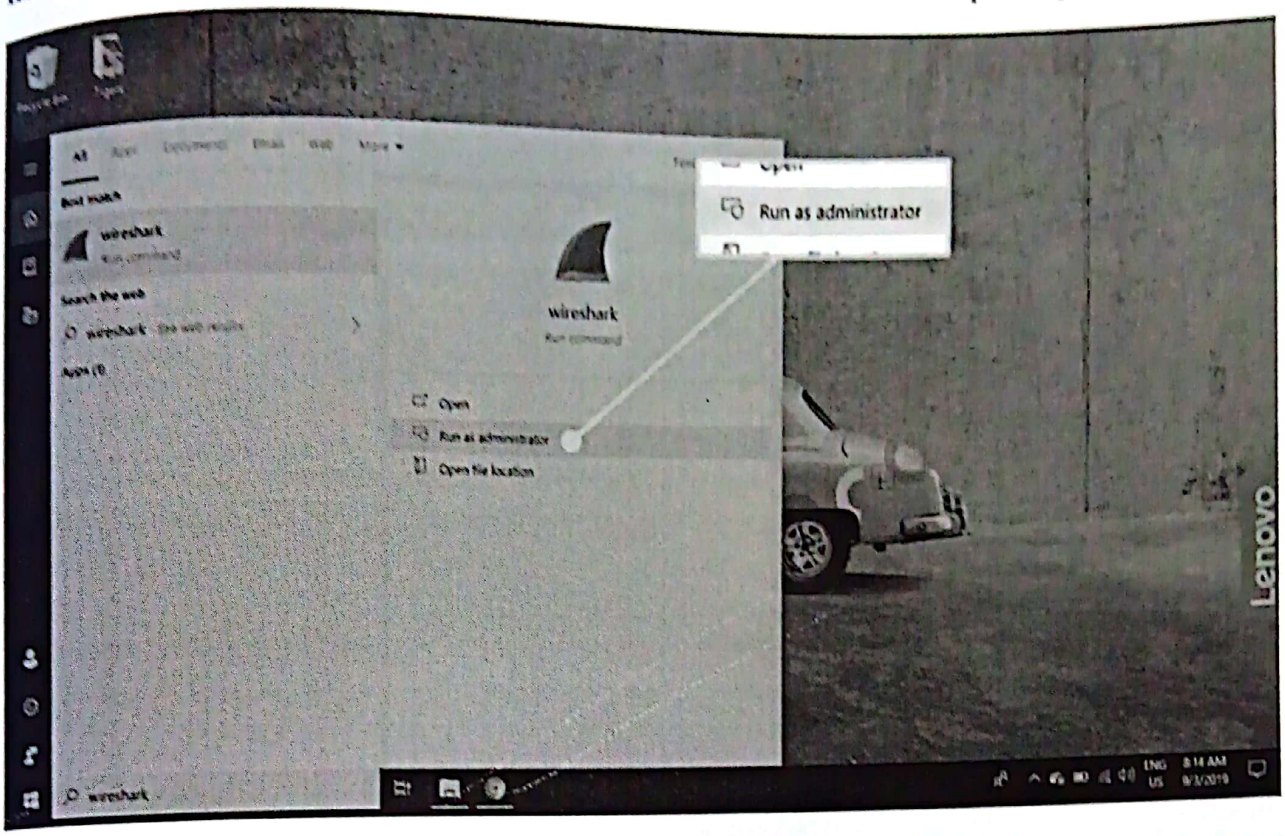
Wireshark can be downloaded at no cost from the Wireshark Foundation website for both mac OS and Windows. You'll see the latest stable release and the current developmental release. Unless you're an advanced user, download the stable version.



During the Windows setup process, choose to install Win Pcap or Np cap if prompted as these include libraries required for live data capture.



You must be logged in to the device as an administrator to use Wireshark. In Windows 10, search for Wireshark and select Run as administrator. In macOS, right-click the app icon and select Get Info. In the Sharing & Permissions settings, give the admin Read & Write privileges.



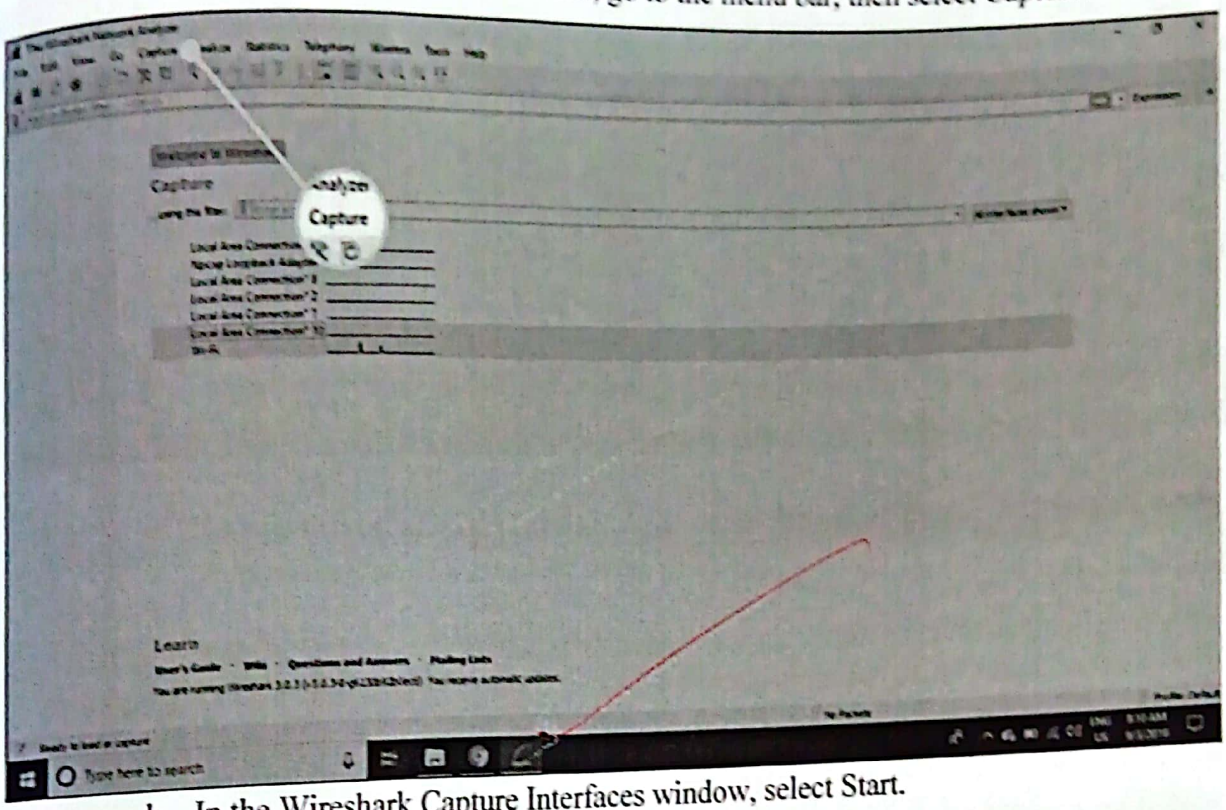
The application is also available for Linux and other UNIX-like platforms including Red Hat, Solaris, and FreeBSD. The binaries required for these operating systems can be found toward the bottom of the Wireshark download page under the Third-Party Packages section. You can also download Wireshark's source code from this page.

3. How to Capture Data Packets With Wireshark

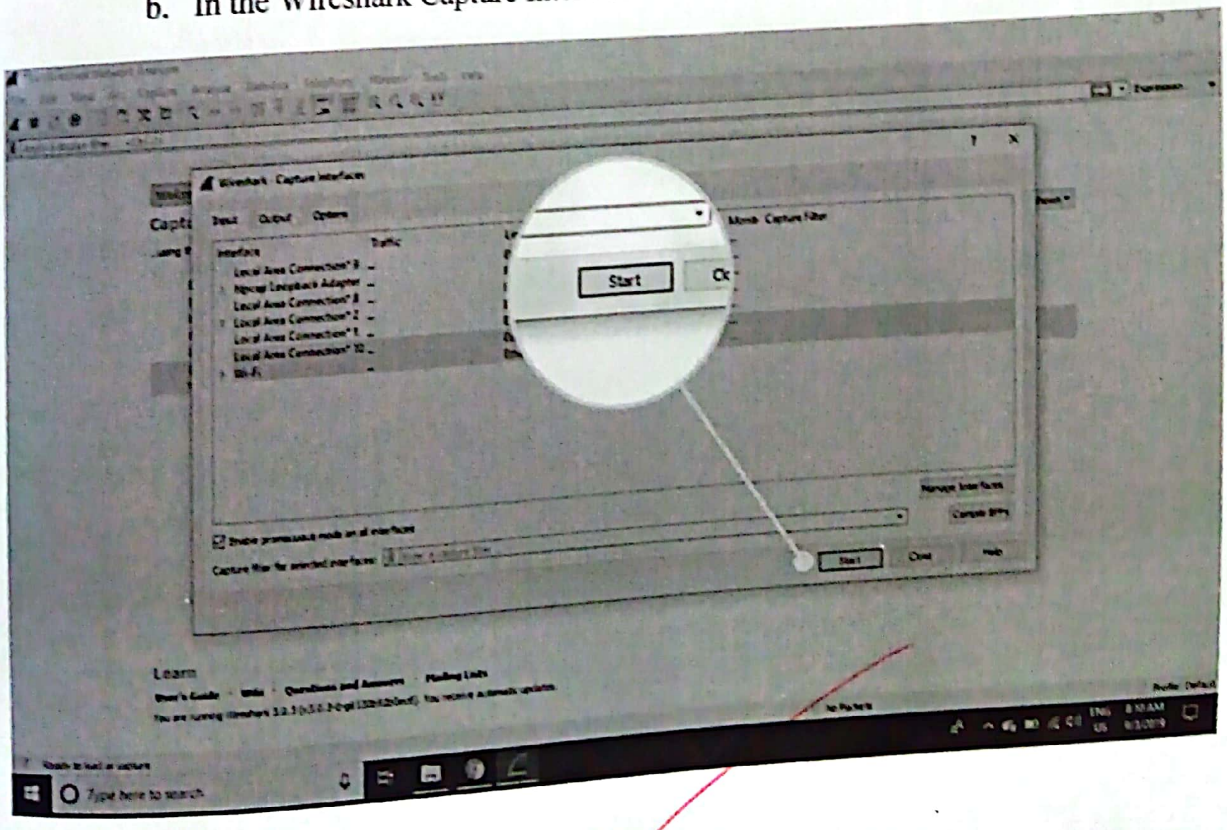
When you launch Wireshark, a welcome screen lists the available network connections on your current device. Displayed to the right of each is an EKG-style line graph that represents live traffic on that network.

To begin capturing packets with Wireshark:

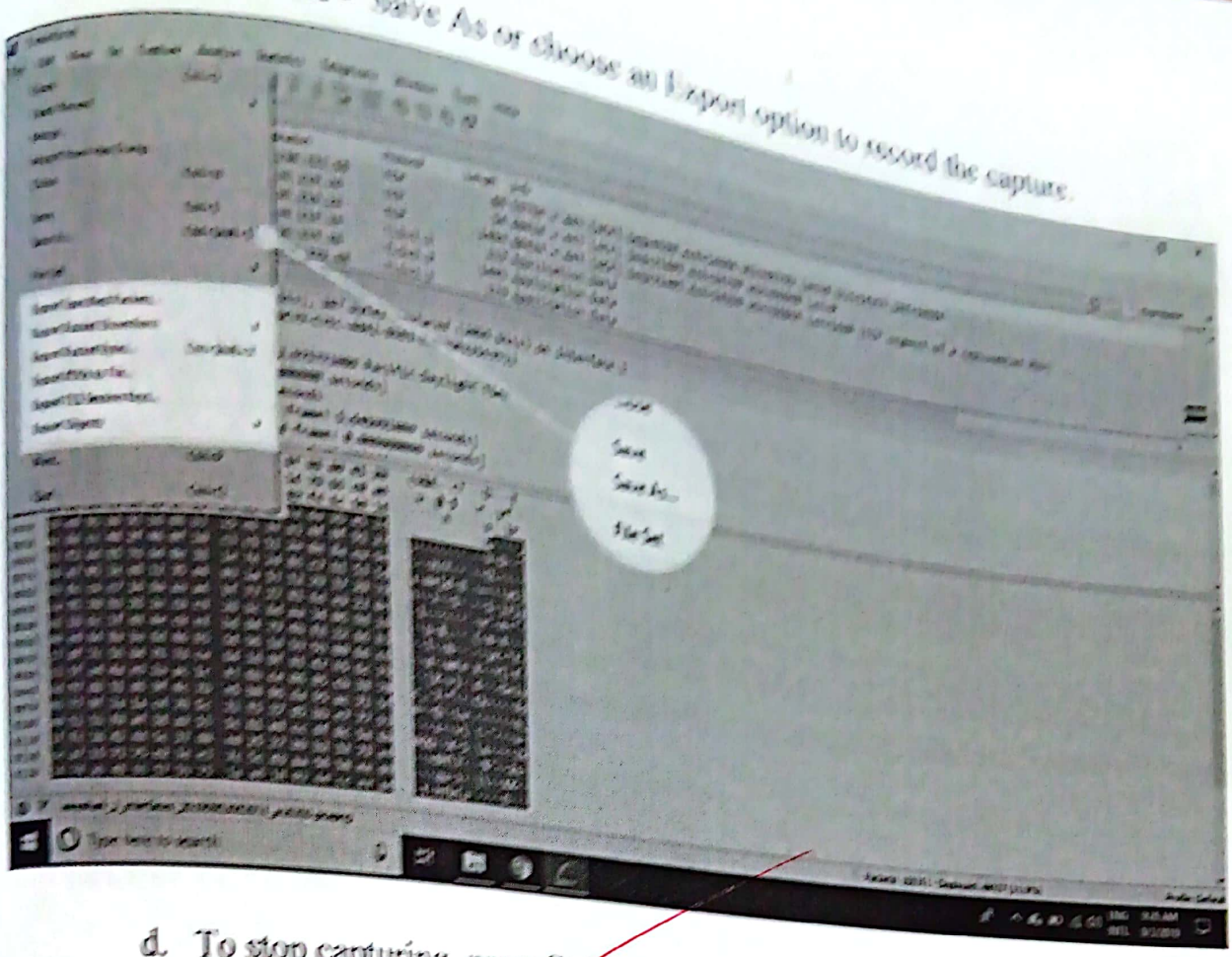
a. Select one or more of networks, go to the menu bar, then select Capture.



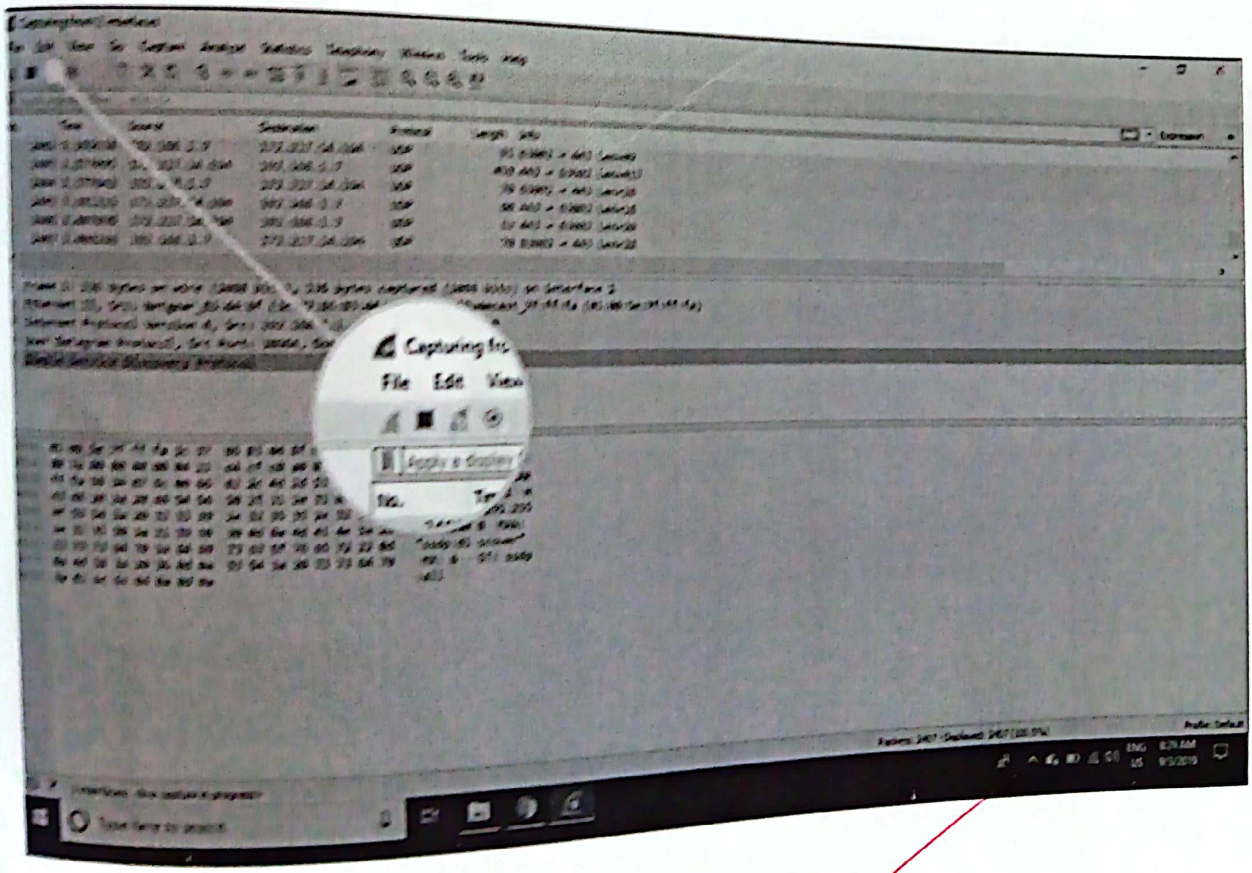
b. In the Wireshark Capture Interfaces window, select Start.



c. Select File > Save As or choose an Export option to record the capture.



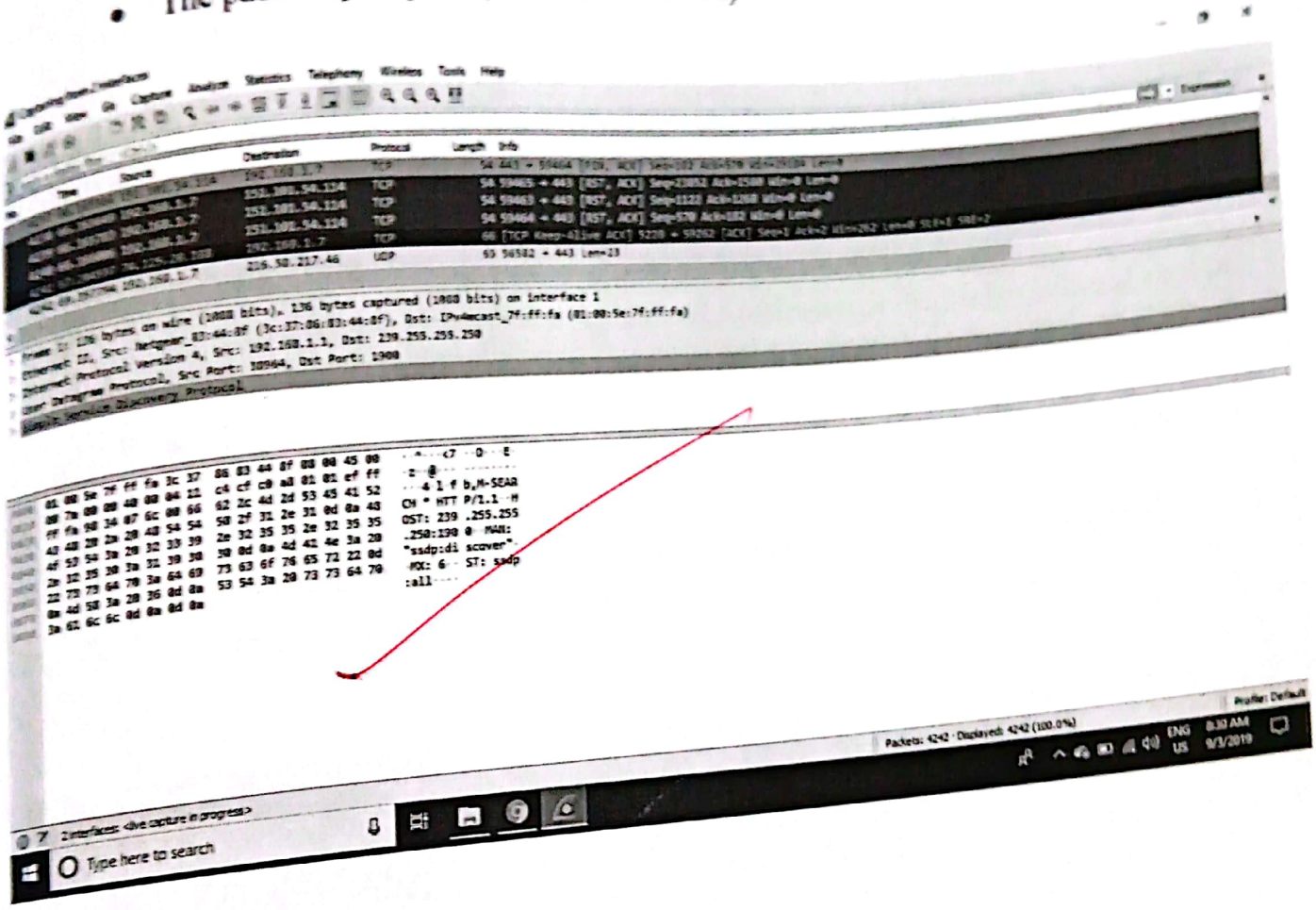
d. To stop capturing, press Ctrl+E. Or, go to the Wireshark toolbar and select the red Stop button that's located next to the shark fin.



4. How to View and Analyze Packet Contents

The captured data interface contains three main sections:

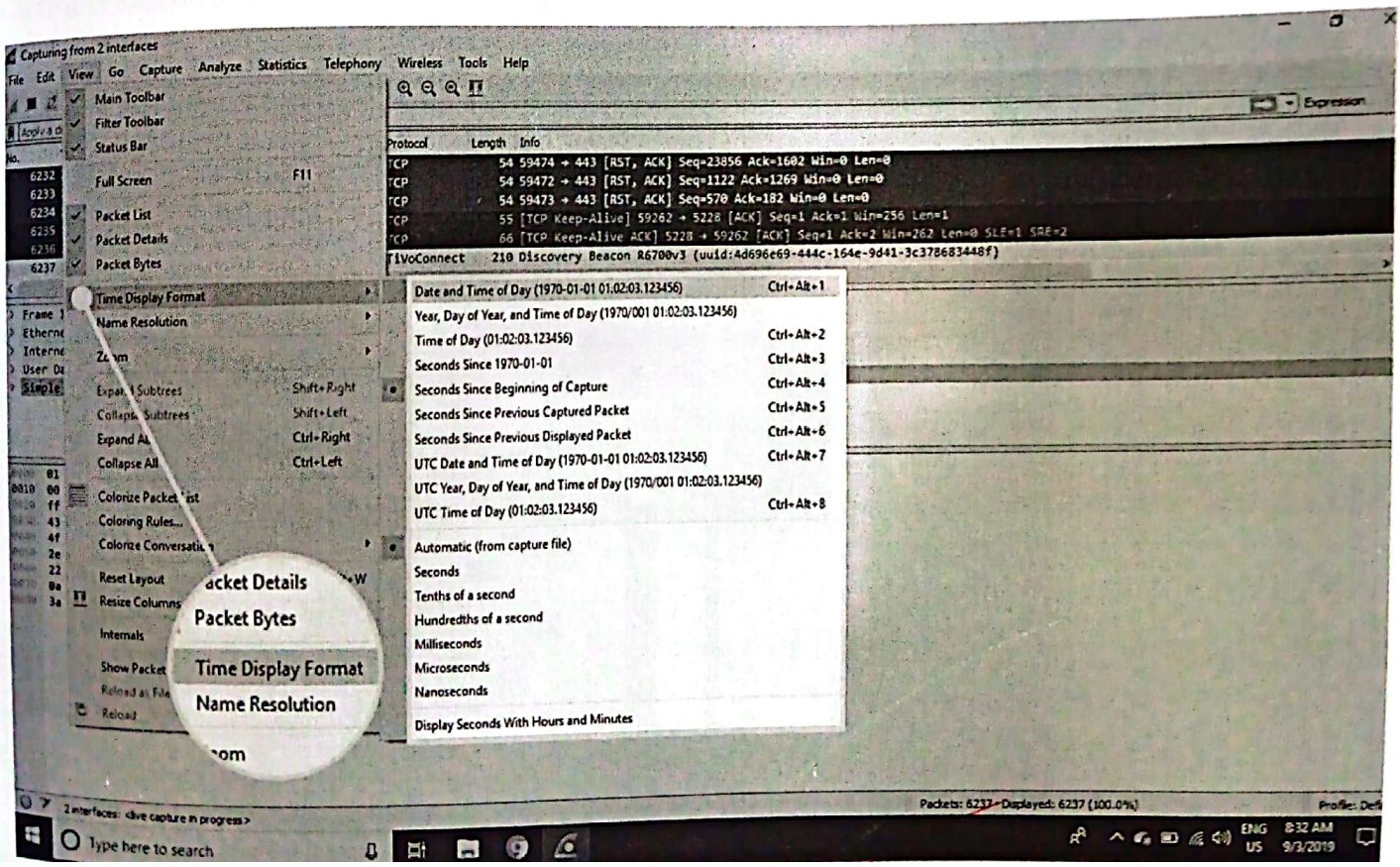
- The packet list pane (the top section)
- The packet details pane (the middle section)
- The packet bytes pane (the bottom section)



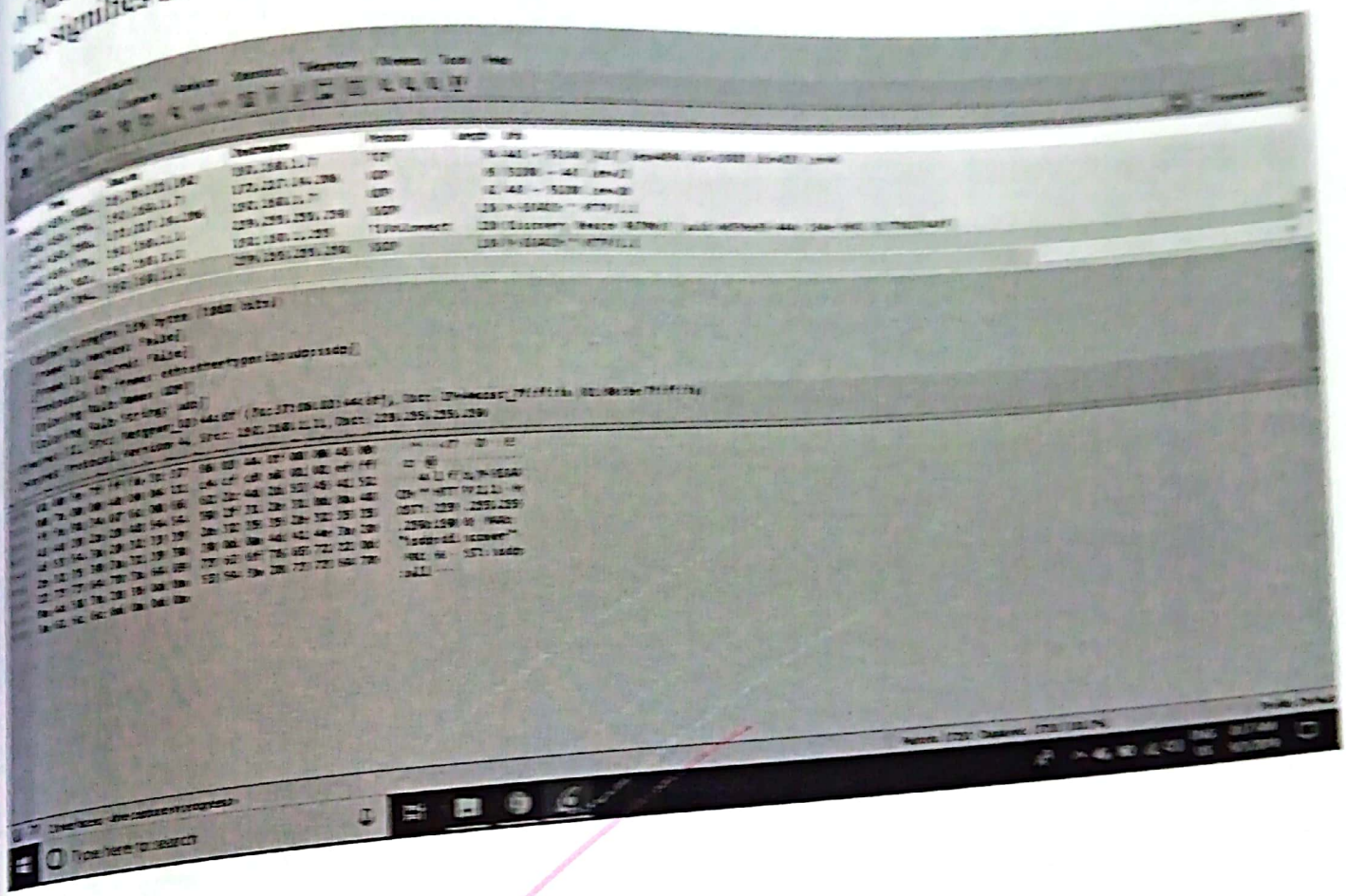
i. Packet List

The packet list pane, located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points:

- No: This field indicates which packets are part of the same conversation. It remains blank until you select a packet.
- Time: The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture file was first created.
- Source: This column contains the address (IP or other) where the packet originated.
- Destination: This column contains the address that the packet is being sent to.
- Protocol: The packet's protocol name, such as TCP, can be found in this column.
- Length: The packet length, in bytes, is displayed in this column.
- Info: Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.
- To change the time format to something more useful (such as the actual time of day), select View > Time Display Format.

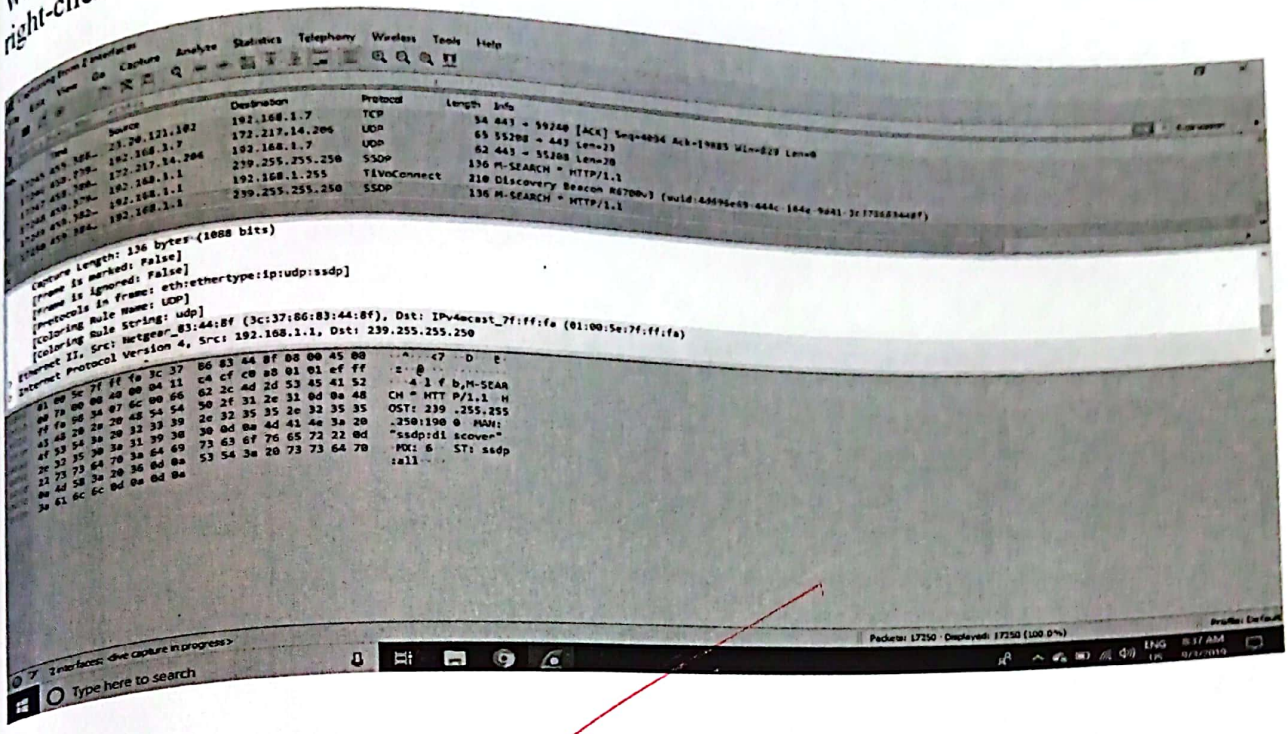


When a packet is selected in the top pane, you may notice one or more symbols appear in the No. column. Open or closed brackets and a straight horizontal line indicate whether a packet or group of packets are part of the same back-and-forth conversation on the network. A broken horizontal line signifies that a packet is not part of the conversation.



ii. Packet Details

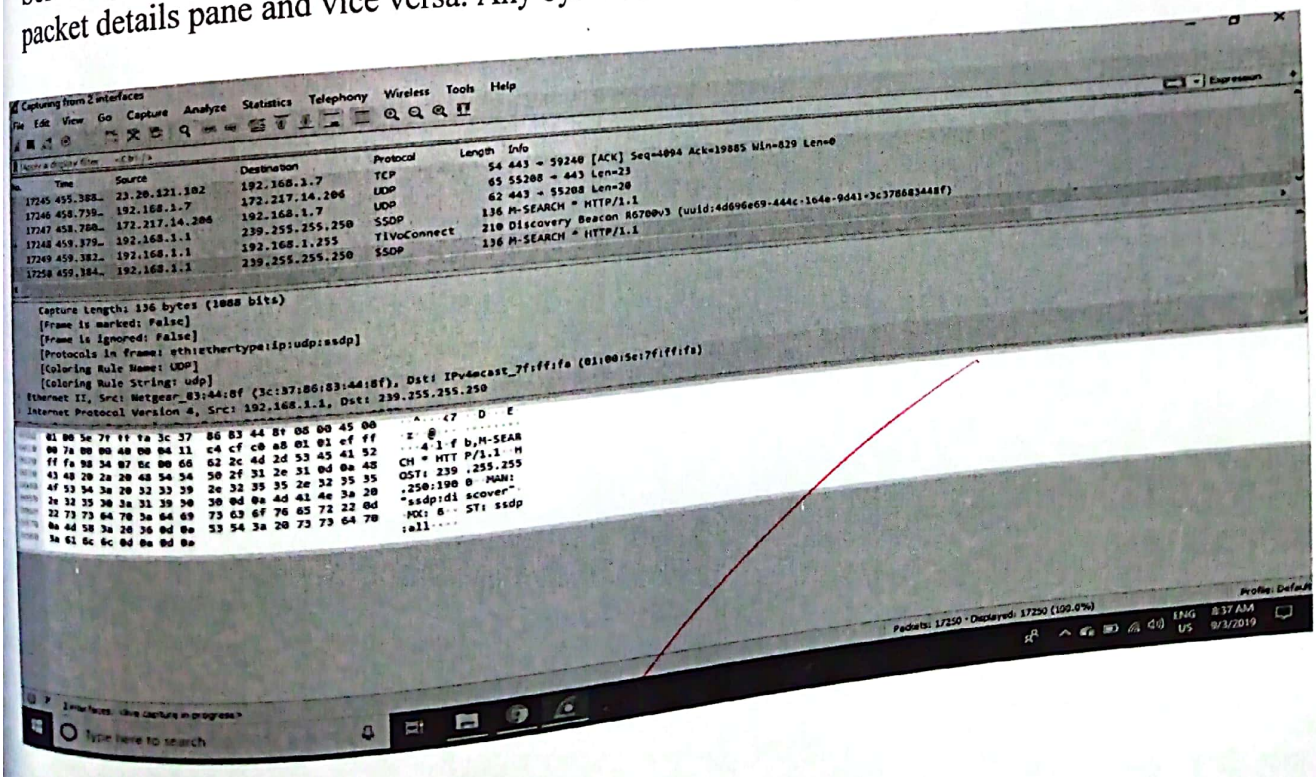
The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.



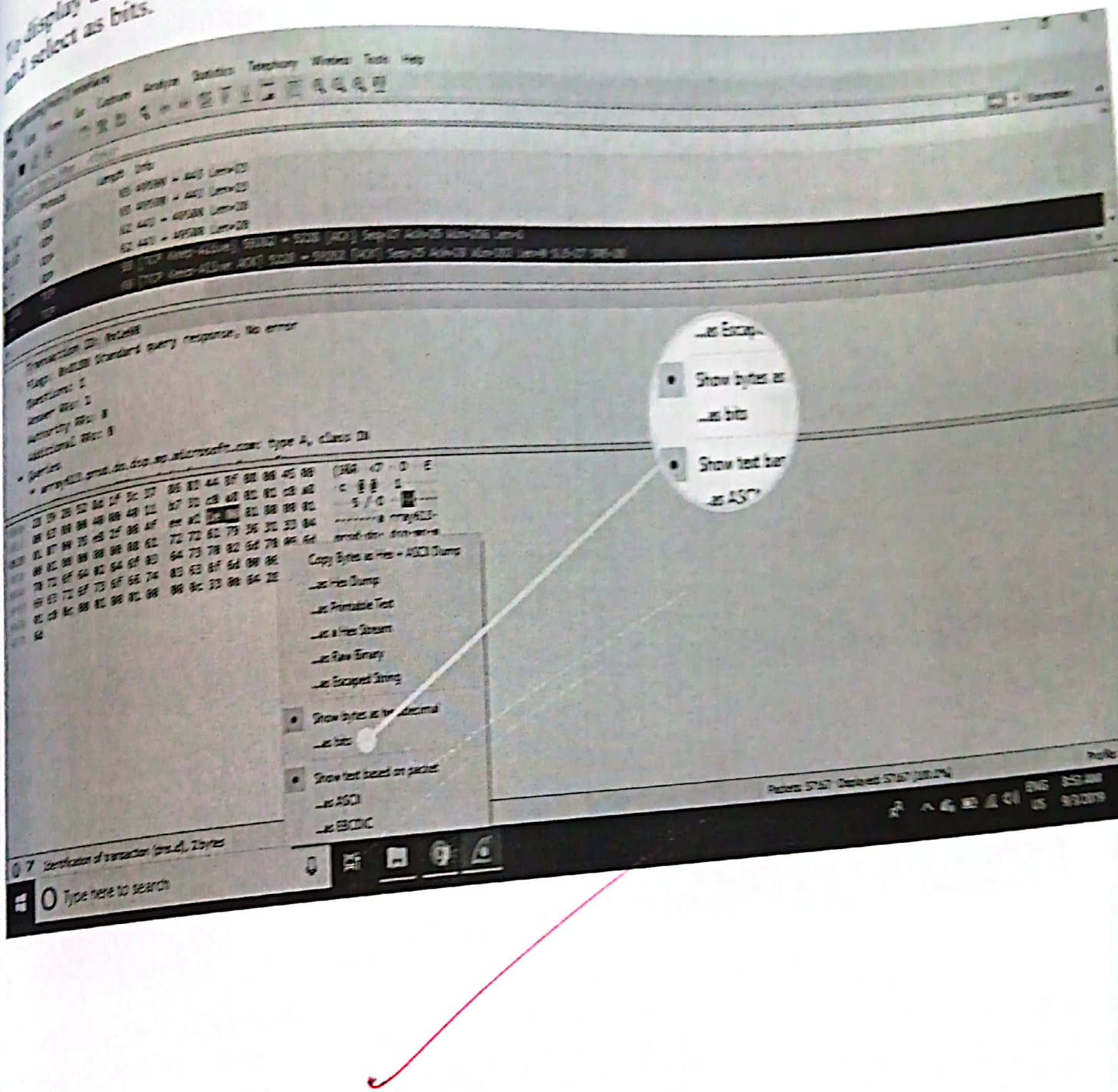
iii. Packet Bytes

At the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.

Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that cannot be printed are represented by a period.



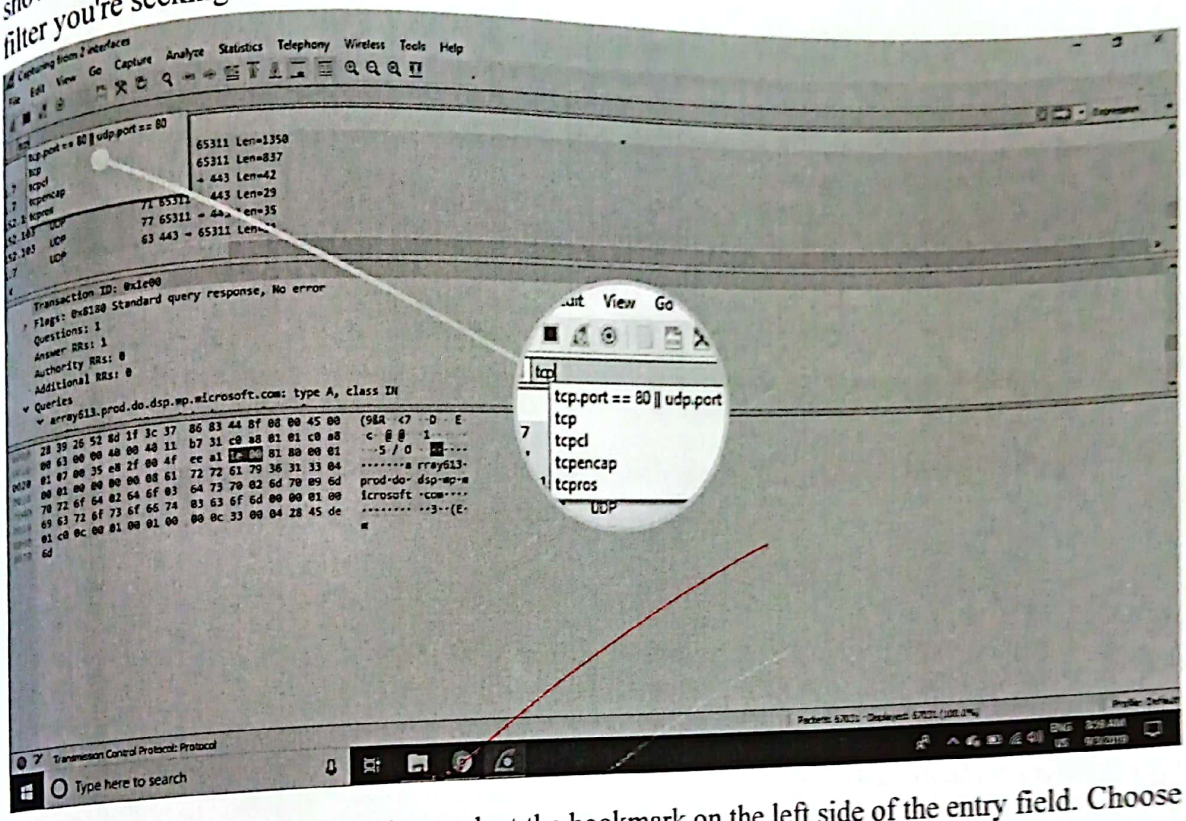
To display this data in bit format as opposed to hexadecimal, right-click anywhere within the pane and select as bits.



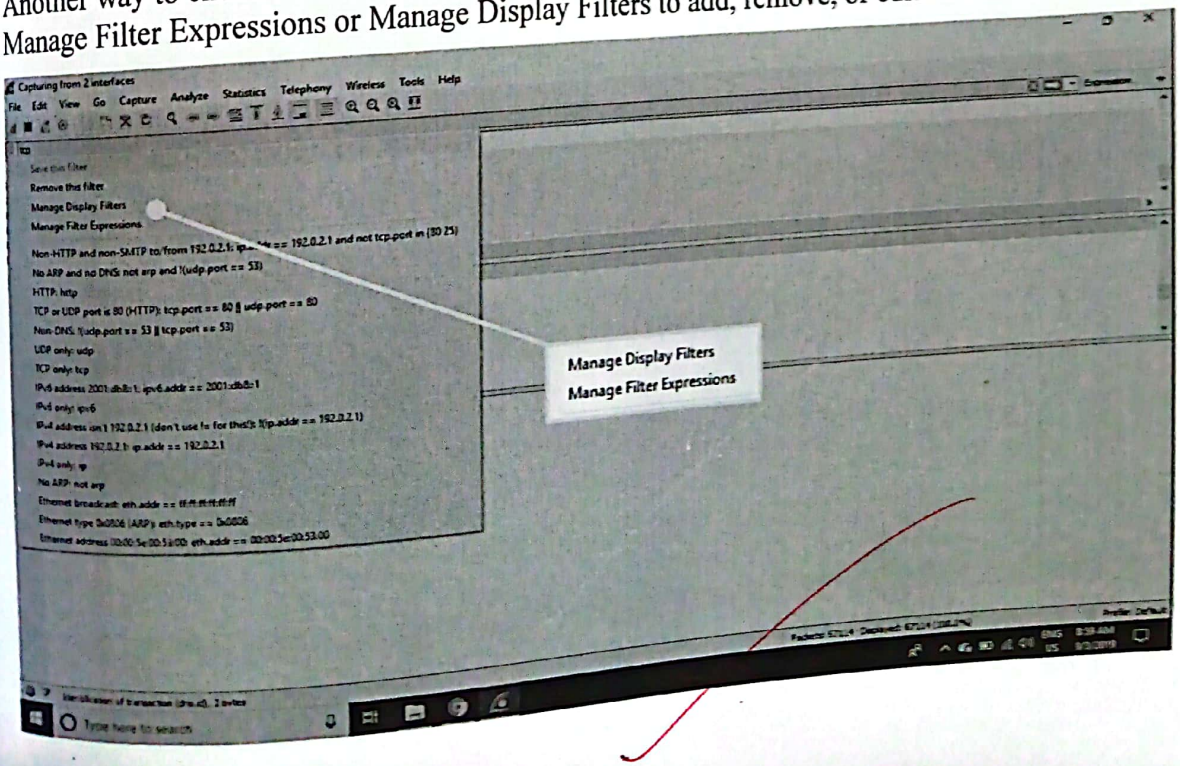
5. How to Use Wireshark Filters

Capture filters instruct Wireshark to only record packets that meet specified criteria. Filters can also be applied to a capture file that has been created so that only certain packets are shown. These are referred to as display filters .Wire shark provides a large number of predefined filters by default. To use one of these existing filters, enter its name in the Apply a display filter entry field located below the Wireshark toolbar or in the Enter a capture filter field located in the centre of the welcome screen.

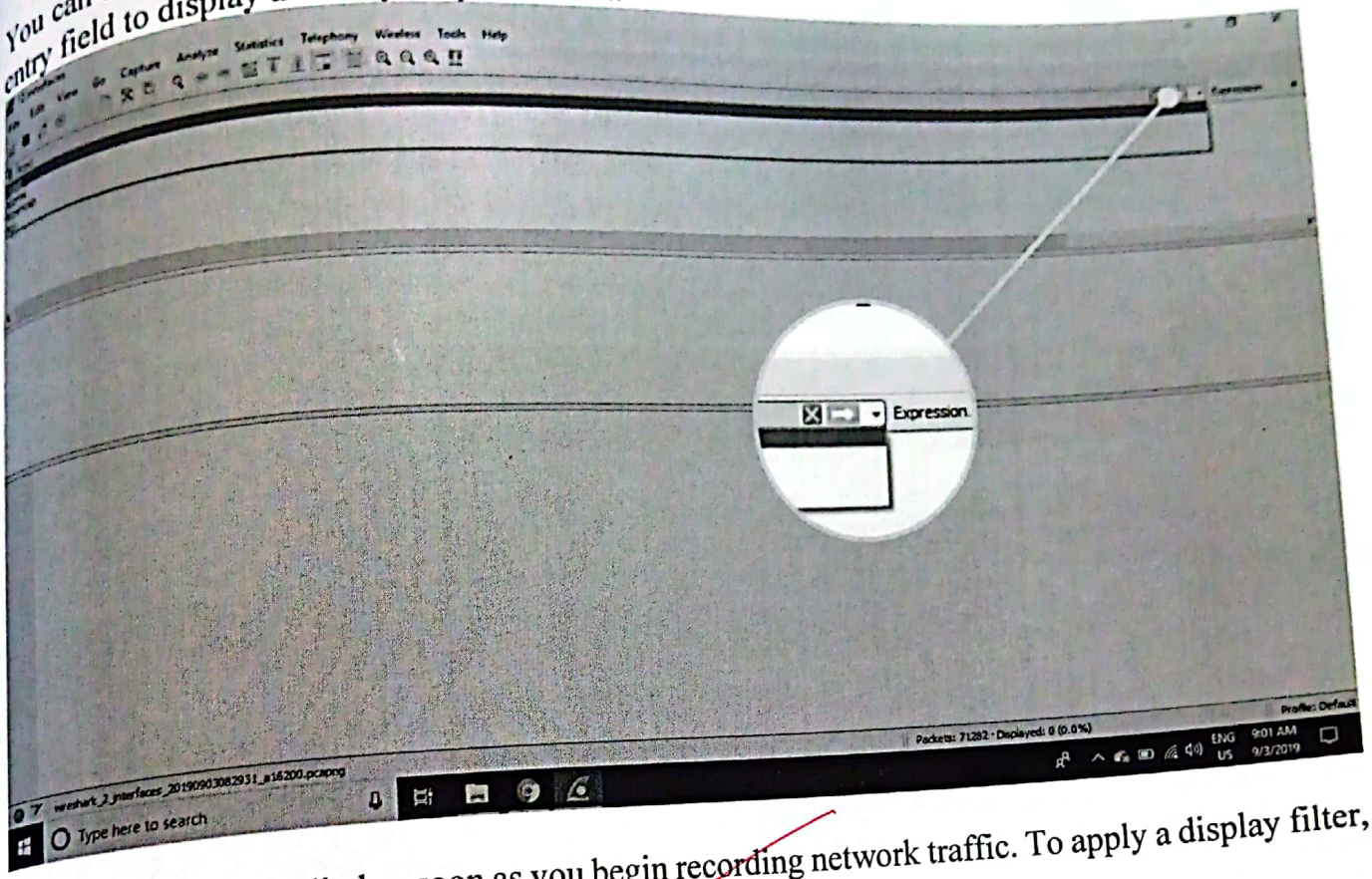
For example, if you want to display TCP packets, type tcp. The Wireshark autocomplete feature shows suggested names as you begin typing, making it easier to find the correct moniker for the filter you're seeking.



Another way to choose a filter is to select the bookmark on the left side of the entry field. Choose Manage Filter Expressions or Manage Display Filters to add, remove, or edit filters.



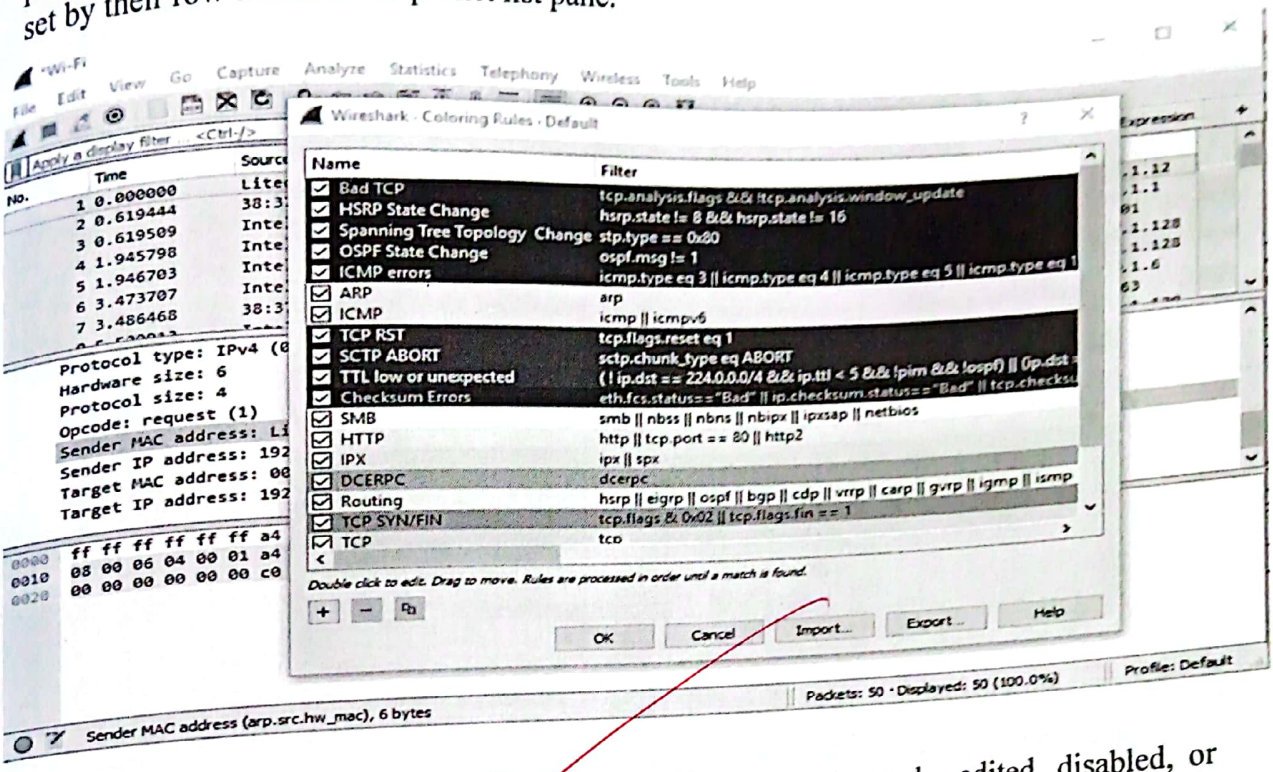
You can also access previously used filters by selecting the down arrow on the right side of the entry field to display a history drop-down list.



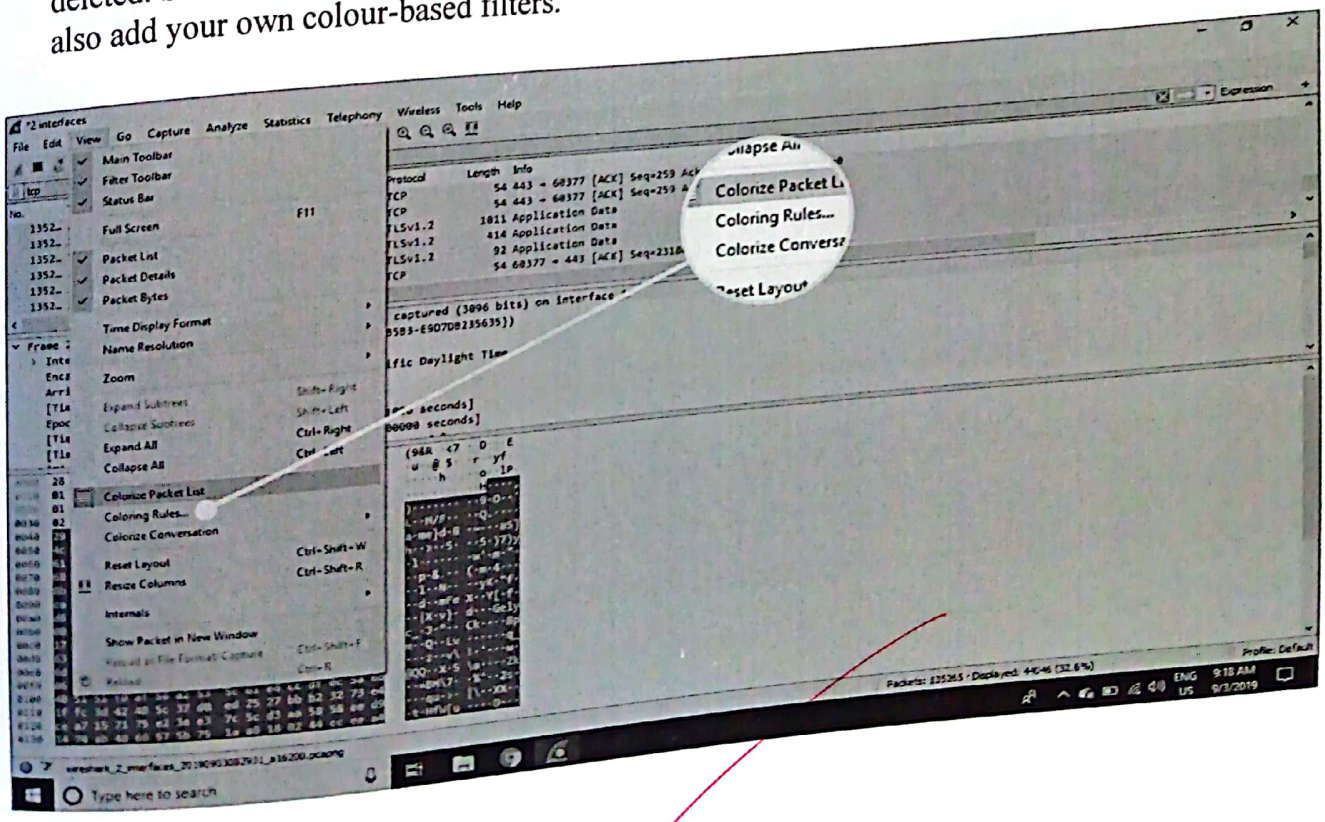
Capture filters are applied as soon as you begin recording network traffic. To apply a display filter, select the right arrow on the right side of the entry field.

6. Wireshark Colour Rules

While Wireshark's capture and display filters limit which packets are recorded or shown on the screen, its colorization function takes things a step further: It can distinguish between different packets types based on their individual hue. This quickly locates certain packets within a saved set by their row colour in the packet list pane.

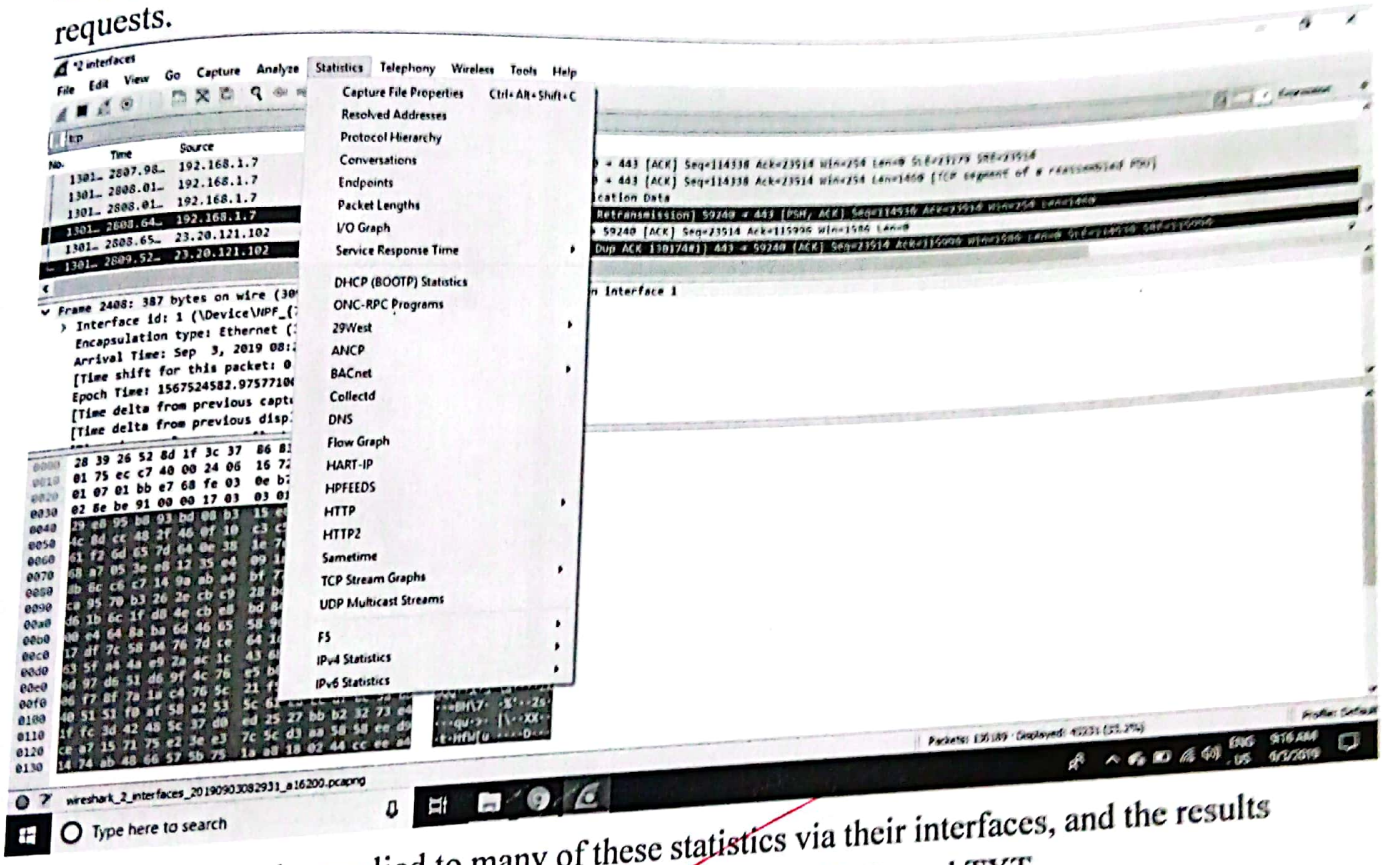


Wireshark comes with about 20 default colouring rules, each can be edited, disabled, or deleted. Select View > Colouring Rules for an overview of what each colour means. You can also add your own colour-based filters.



7. Statistics in Wireshark

Other useful metrics are available through the Statistics drop-down menu. These include size and timing information about the capture file, along with dozens of charts and graphs ranging in topic from packet conversation breakdowns to load distribution of HTTP requests.

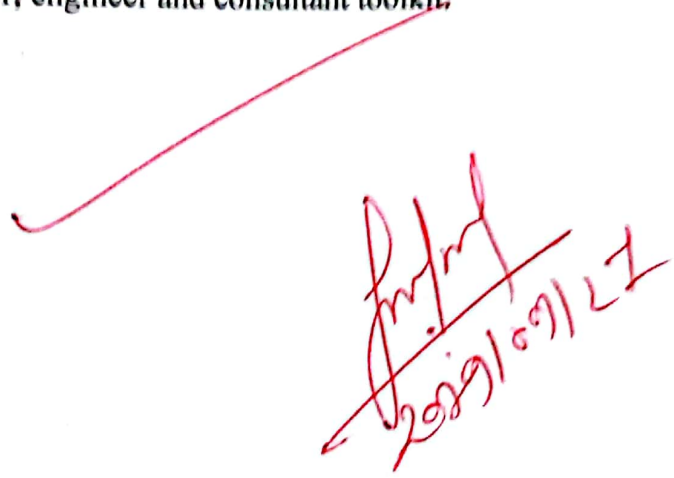


Display filters can be applied to many of these statistics via their interfaces, and the results can be exported to common file formats, including CSV, XML, and TXT.

8. Conclusion

Wire shark's wireless analysis features have grown to be a very powerful tool for troubleshooting and analysing wireless networks. With wire shark's display filters and powerful protocol dissector features, in today's era, most organizations use Wireshark for their security issues for detecting any suspicious activities on their networks and systems.

We can say that the history of Wireshark is a great journey through which security professionals made a difference. This has been possible because Wireshark was invented by a group of people who have a concern about network security, and they worked on this software in order to give some new direction to this industry. you can shift through large quantities of wireless traffic. Without a doubt, wire shark is a powerful assessment and analysis tool for wireless networks that should be a part of every auditor, engineer and consultant toolkit.



LAB-14.

Name of the experiment: Network command in Linux based machine.

ip
This is the latest and updated version of ipconfig command.

syntax:

- ip a
- ipaddr

This command gives the details of all networks like ifconfig.

This command can also be used to get the details of a specific interface.

commands to get details are:

syntax:

ip a show eth0
ip a show lo
ip a show wlan0

tracepath

Linux tracepath is similar to traceroute command. It is used to detect network delays. However, it doesn't require root privileges.

It is installed in Ubuntu by default.

It traces the route to the specified destination and identifies each hop in it. If your network is weak, it recognizes the point where the network is weak.

Syntax:
tracepath <destination>
example:
tracepath mindmajix.com

nslookup

Linux nslookup is also a command used for DNS related queries. It is the older version of dig.

syntax:
nslookup <domain Name>

Example:
nslookup mindmajix.com

Output:
As we see in the output, it displays the record information relating to mindmajix.com.

host

Linux host command displays the domain name for a given IP address and IP address for a given hostname It is also used to fetch DNS lookup for DNS related query.

example:
host mindmajix.com
host 149.77.21.18

You can combine the host command with -t, and get DNS resource like SOA, NS, A, PTR, CNAME, MX, SRV

Syntax:
host -t <resourceName>

arp

Linux arp command stands for Address Resolution Protocol. It is used to view and add content to the kernel's ARP table.

syntax:

arp

All the system maintain a table of IP addresses and their corresponding MAC addresses. This table is called the ARP lookup table. When a destination is requested to connect through IP address, your router will check for the MAC address in this table. If it is cached, the table will be not used.

By default, arp displays the hostnames. You can get the IP addresses by using:

ommand:

$arp -n

we can also delete the entries from the arp table, as shown below.

ommand:

$arp -d HWADDR

iwconfig

Linux iwconfig is used to configure the wireless network interface. It is used to set and view the basic wifi details like SSID and encryption. To know more about this command, refer to the main page.

syntax: iwconfig.

Linux whois command is used to fetch all the information related to a website. You can get all the information about a website including the registeration and the owner.

Syntax:

whois <websiteNames>

Example:

whois mindmajix.com

if plug status

Linux ifplugstatus command is used to check if a cable is plugged into the network interface. This command is not directly available on Ubuntu. You can install this using the command below.

command:

Sude apt-get install ifplugd

Syntax:

ifplugstatus

mtr

Linux mtr command is a combination of ping and the traceroute command. It continuosly displays information regarding the packets sent with the ping time of each hop. It is also used to view the network issues.

Syntax

mtr <path>

Example:

$ mtr google.com

Output:

You can use mtr with -report option. It sends 10 packets to each hop that is found on the way.

Syntax:

$ mtr --report <path>

curl & wget

Linux curl and wget commands are used in downloading files from the internet through CLI. The curl command has to be used with the option "O" to fetch the file, while the wget command is used directly.

Below are the syntax and the example for the two commands.

- curl

syntax:

curl -O <filelink>

Example:

curl -O google.com/doodles/childrens-day-2014-multiple-countries.

- wget

syntax:

wget <filelink>

Example:

wget google.com/doodles/new-years-day-2012.