Table of contents

Lab-1

Overview of Network and basic Router Configuration.

Objectives:

- Understand basic commands for router configuration.
- Understand to connect the router, switch.

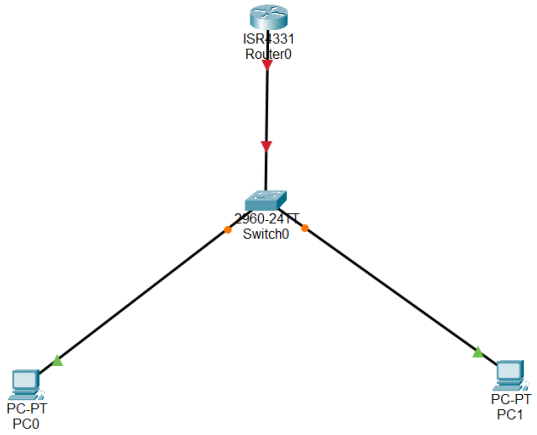
Background:

Routers: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the internet. Data sent through the internet, such as a webpage or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node. A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the networks address information in the packet header to determine the ultimate destination. Then, using the information in its routing table or routing policy, it directs the packet to the next network on its journey.

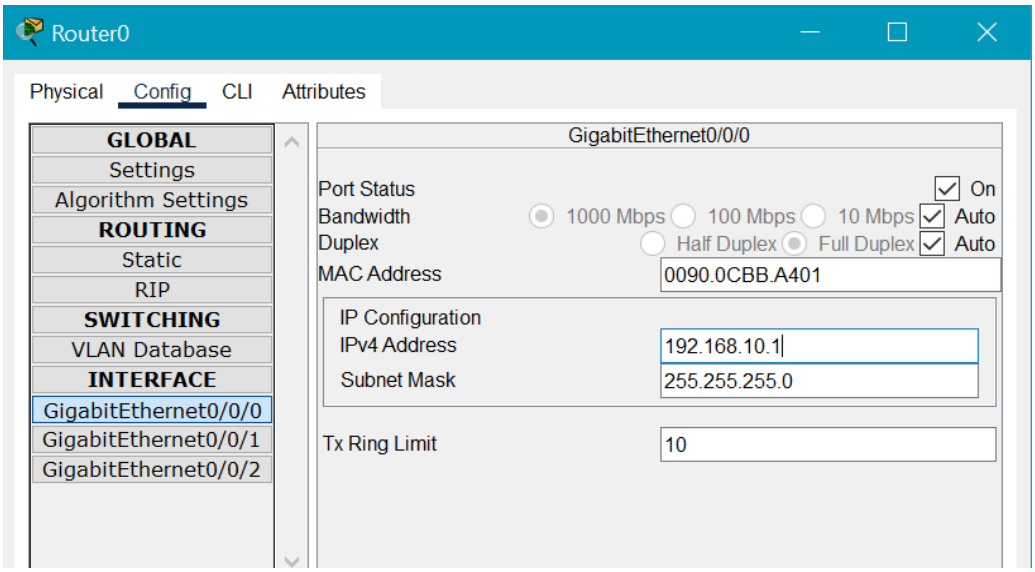
Switch: A switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

Procedure:

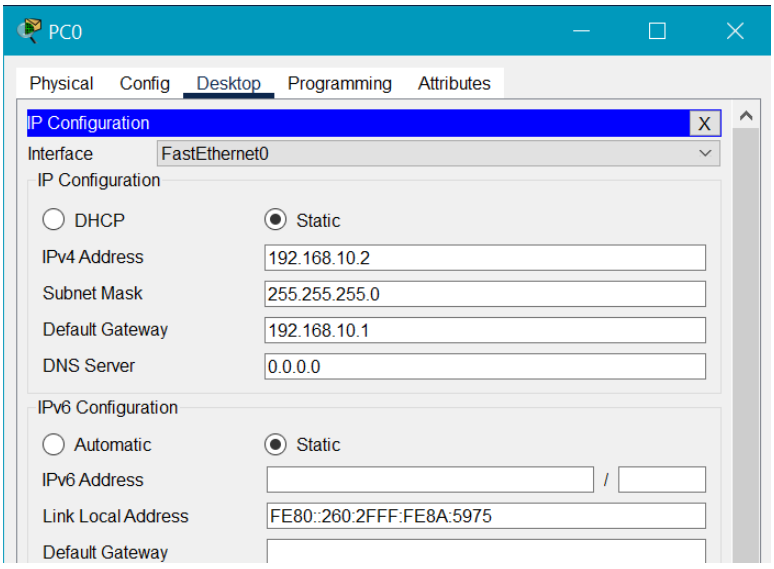
- Configure router and switch with two pc as follow:



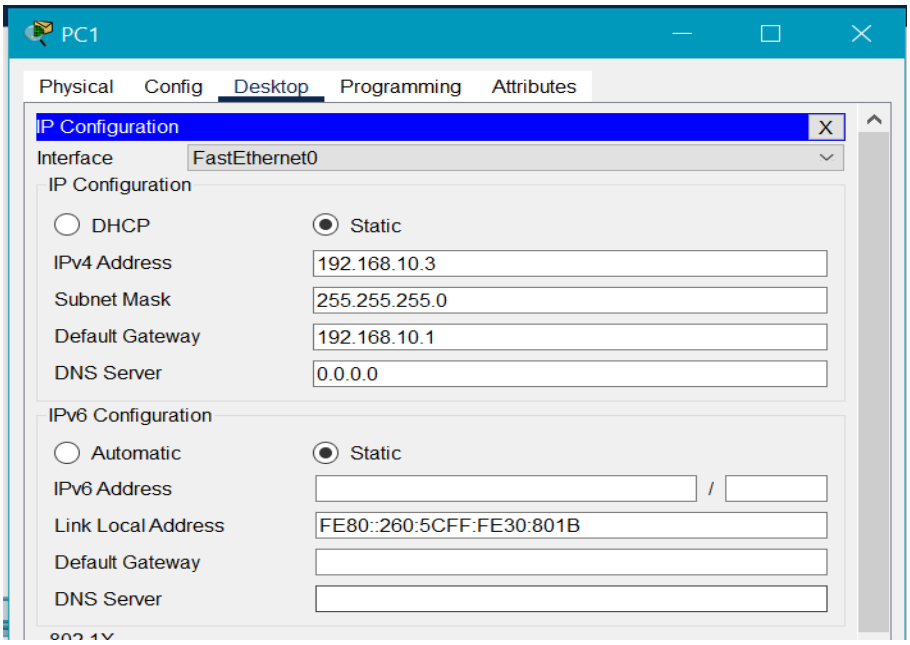
- Configuration of the router:



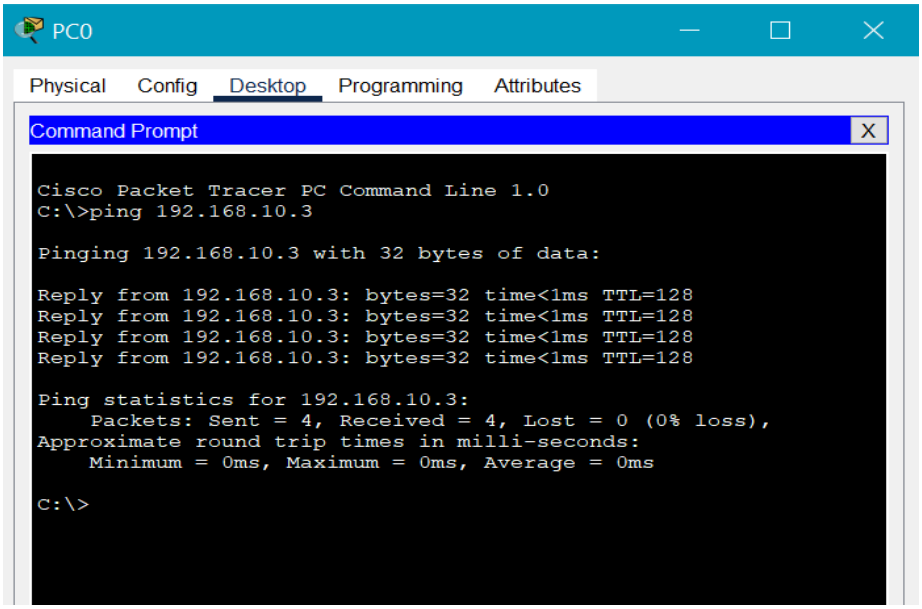
- Configuration of pc0:



- Configuration of pc1:



- To check whether PC0 is connected with PC1:



Conclusion: In this way, we can connect two pcs with the help of router and switch.

Lab-2

CAT6 UTP EIA/TIA 568A/B straight and cross-over wiring, testing

Objectives:

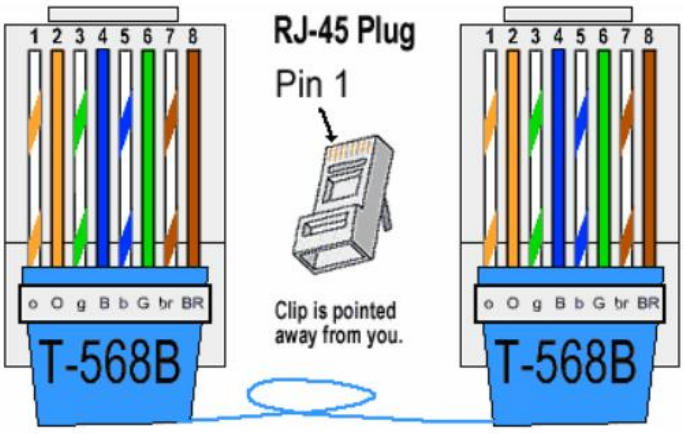
- To understand the color coding standard of UTP cable.
- To create straight and crossover cable and test/verify its connectivity.

Apparatus: UTP CAT6 cable (1M), Crimper, LAN tester.

Background: RJ-45 connectors intended for use with CAT-6 cable are larger than their CAT-5 counter-parts. Begin by stripping the outer covering from the end of the cable. Remove about an inch of covering. Eventually we'll have to cut down the amount of exposed cable, but the process of installing the RJ-45 connector will be easier if we have plenty of exposed cable to work with (but not too much). Once we remove the router cover, we'll see that some of the pairs of wire are twisted together (hence the name twisted-pair cable). Untwist these wires. Once all the wires have been separated, pull them backward so we can cut off the exposed plastic core, as shown below. Remove as much of this core as you can. Be careful not to accidentally cut the wires in the process.

Now that the core has been removed, our next task is to straighten the wires that were previously twisted. The easiest way to do this is by using two pairs of tweezers. Use one set of tweezers to firmly hold the wire just beneath a bend, and the other pair to straighten the bend. The wires don't have to be perfectly straight, but the straighter they are, the easier our job will be. Once you've straightened the wires, our next task is to arrange them in the order they'll be placed into the RJ-45 connector.

Working from left to right, the order of the wires shall be set with EIA 568 A or B standard as follows:



Let's start wiring by B standard. Since the leftmost wire is the orange with the white stripe, there's a natural tendency to start with this wire on the left. Although it's possible to get the wires in the correct order using this technique, getting the wires to stay in order when you insert the RJ-45 connector becomes very difficult. Rather than starting with the orange and white wire, lining up the wires is a lot easier if you start with the green wire with the white stripe, and then work on lining up the blue, partial blue, and green wires. When all is said and done, the wires will still have to be in the correct order, but starting with the partial green wire forces us to turn the cable a different direction than if we were initially working with the partial orange. This seems to make all the difference in the world for getting the wires lined up in a way that facilitates easy installation of the RJ-45 connector.

Now that the wires are in the correct order, hold the RJ-45 connector next to the cable to determine how much wire needs to be cut off. We'll want to make the cut so that the ends of the wires line up evenly. The proper length can be determined by looking at the cable's outer insulation. The insulation should stop just inside of the RJ-45 connector. It's better to make a series of small cuts to determine the appropriate cable length than to try to get it exactly right on the first cut. Test-fit the RJ-45 connector between each cut. If we try to get the length exactly right on the first cut, we risk cutting the wires too short.

The easiest way to slide the RJ-45 connector onto the cable is to use our thumb to apply pressure to the cable in the spot where the wires are first exposed from beneath the insulation. This will help keep the wires in order. When the cable is finally cut to the correct length, we should check a few things before crimping the cable. First, make sure the wires go all the way to the end of the RJ-45 connector.

The easiest way to do this is to look at the end of the connector and make sure we see copper in each wire slot. We should also verify that the wires are still in the correct order. It's easy for the wires to get out of order when installing the cable end. A quick check at this point will keep us from having to cut the cable end off and starting over later.

Assuming the wires are in order, we can go ahead and crimp the cable. When we've finished crimping both cable ends, we can use a cable tester to verify that the ends were installed correctly.

Lab-3

Overview of Static Router Configuration

Objective:

- Understand how to configure static routing.
- Understand how to enable, configure, manage and delete static routes in the Cisco router.

Background:

Static routing: It is the most secure way of routing. It reduces overhead from network resources. In this type of routing, we manually add routes to the routing table. It is useful where the numbers of routers are limited.

Advantages:

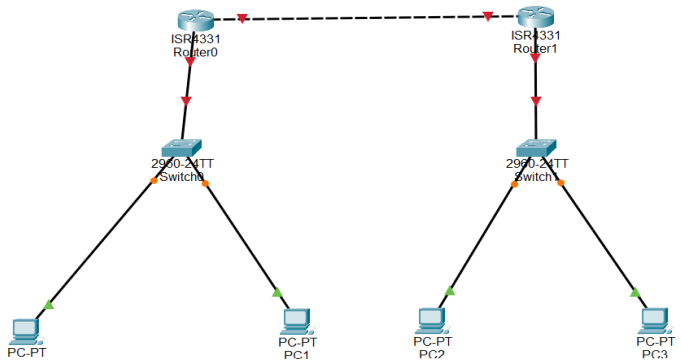
- It is easy to implement.
- It is the most secure way of routing since no information is shared with other routers.
- It puts no overhead on resources such as CPU or memory.

Disadvantage:

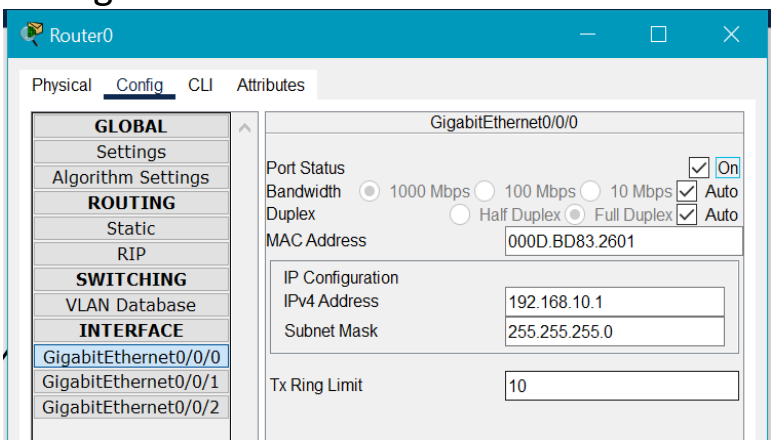
- It is suitable only for a small network.
- If a link fails it cannot reroute the traffic.

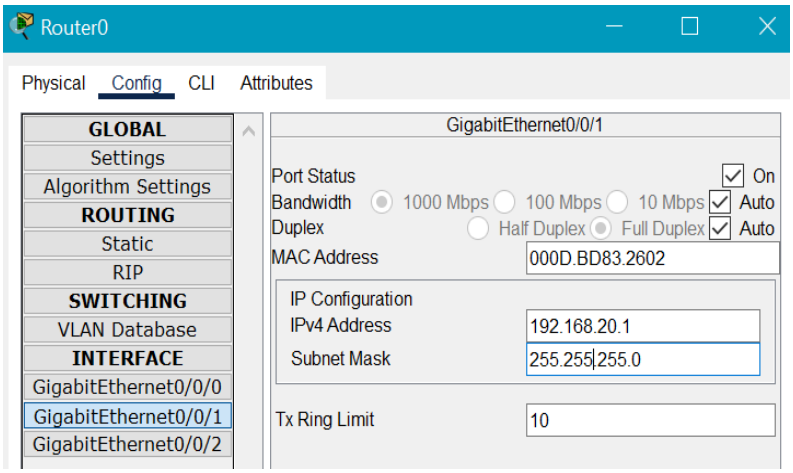
Procedure:

- Configure the two routers by static and two pc each:

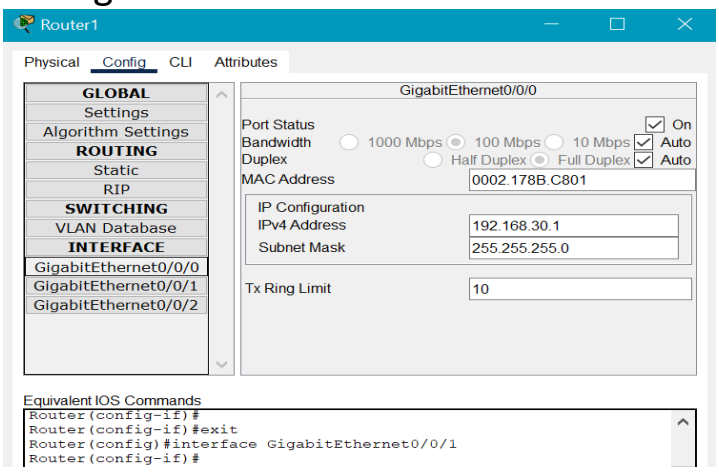


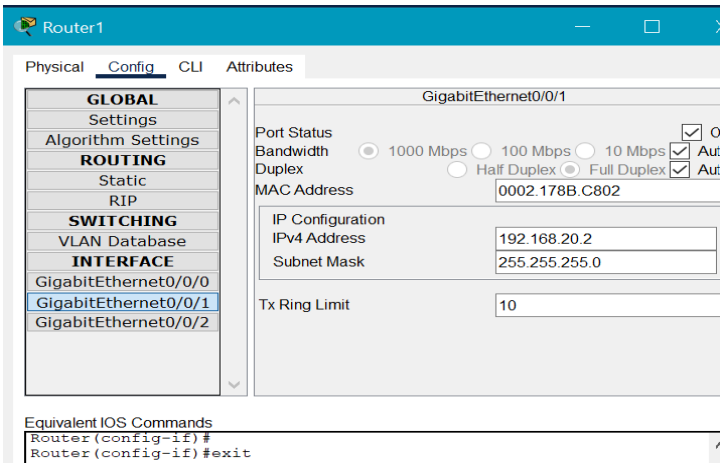
- Configuration of router0:



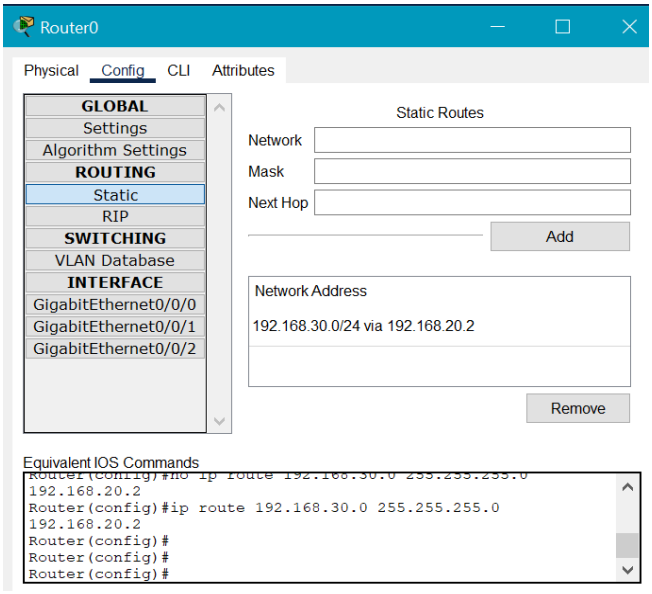


- Configuration of router1:

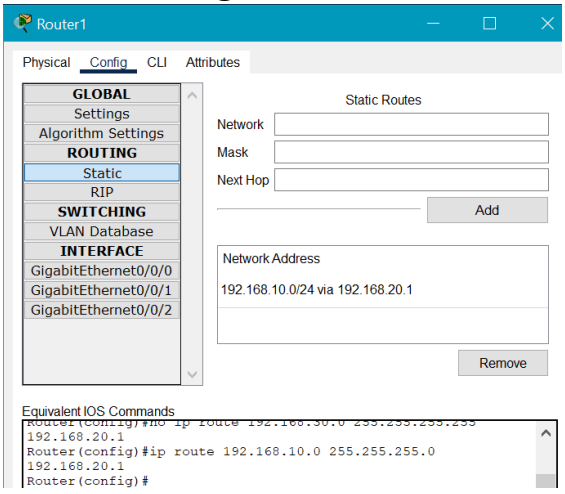




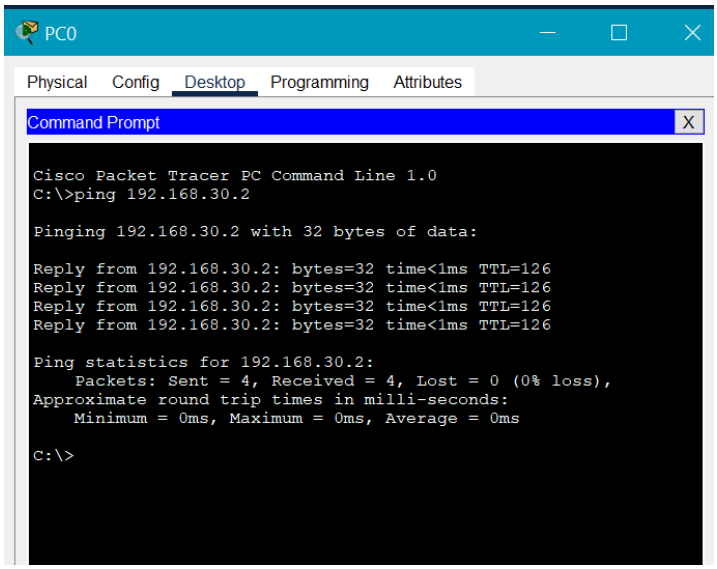
- Static routing of router0:



- Static routing of router1:



- To check whether pc0 is connected with pc2 with the help of router and switch:



Conclusion: In this way, we can configure static routing with the help of routers and switches.

Lab-4

Overview of Email Server Configuration

Objective:

- Understand basic configuration of Email Server.
- Understand to connect the router, switch and server.

Background:

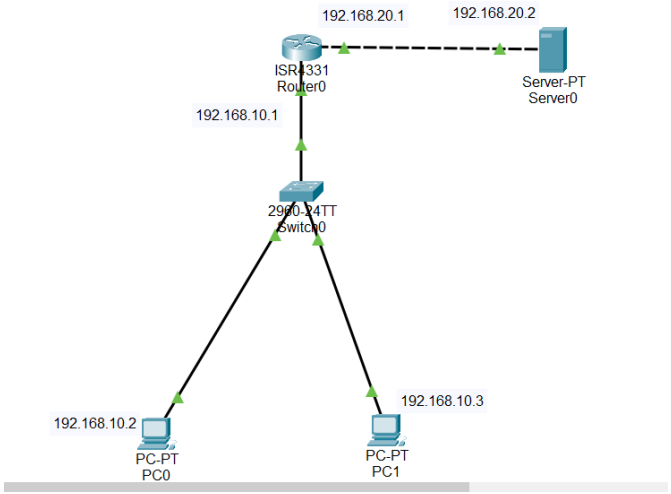
Email Server: A mail server is a server that handles and delivers e-mail over a network, usually over the internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver emails to client computer. A client computer is normally the computer where you read your e-mails.

Router: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the internet. Data sent through the internet, such as a webpage or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node. A router is connected to two or more data lines from different IP networks.

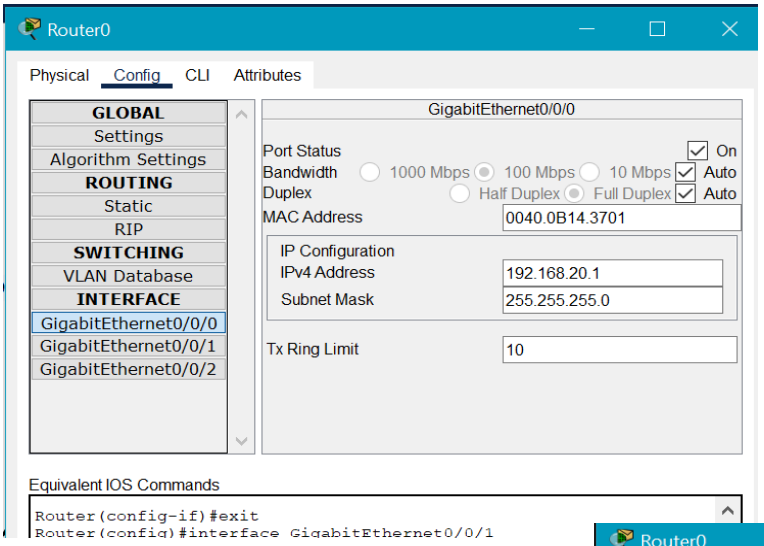
Switch: A switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

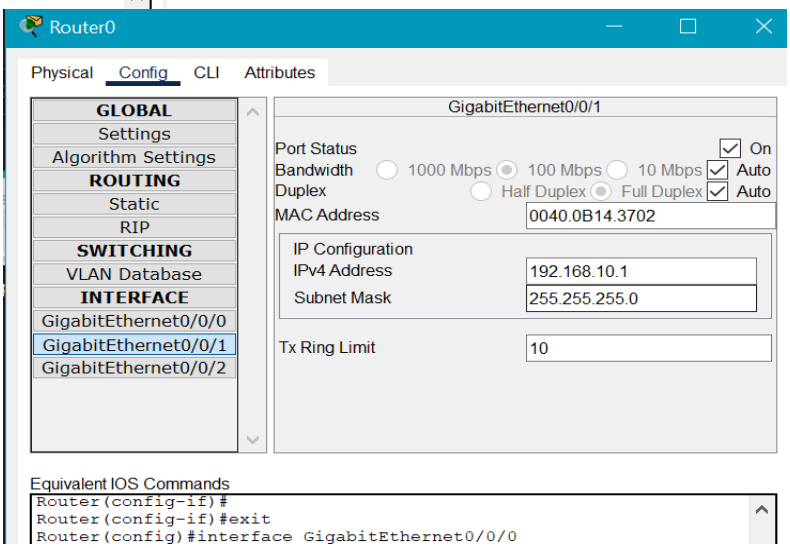
Procedure:

- Configure mail server, router and switch with two pcs as follows:

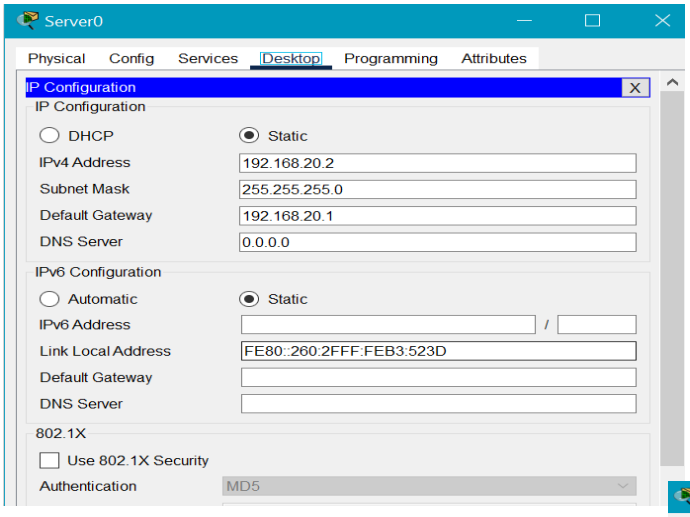


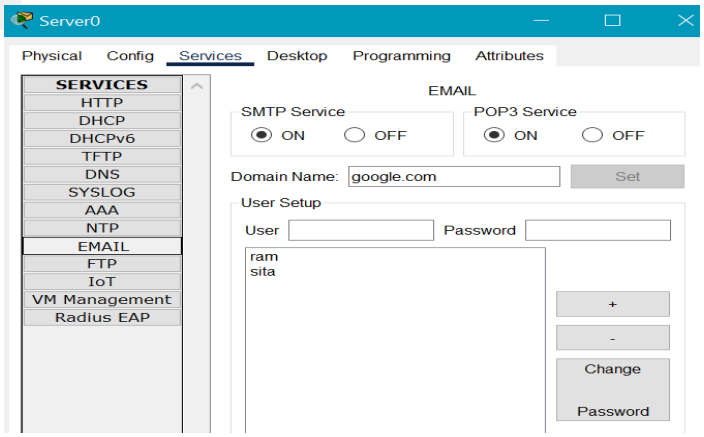
- Configuration of router:



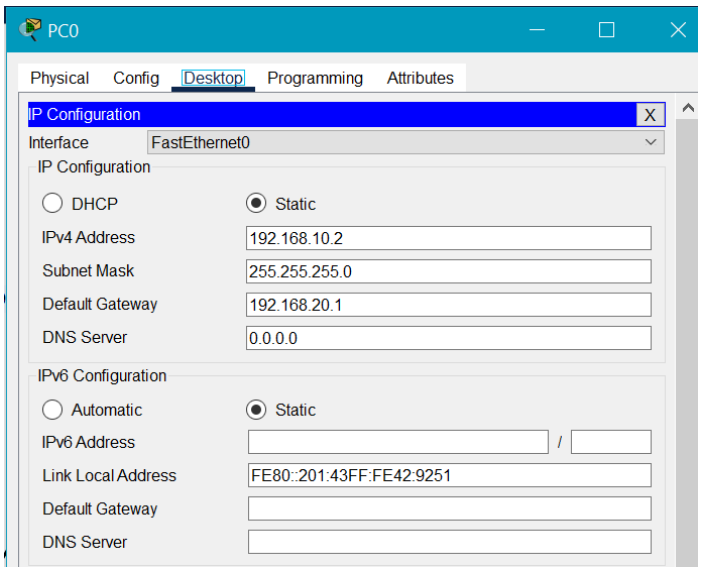


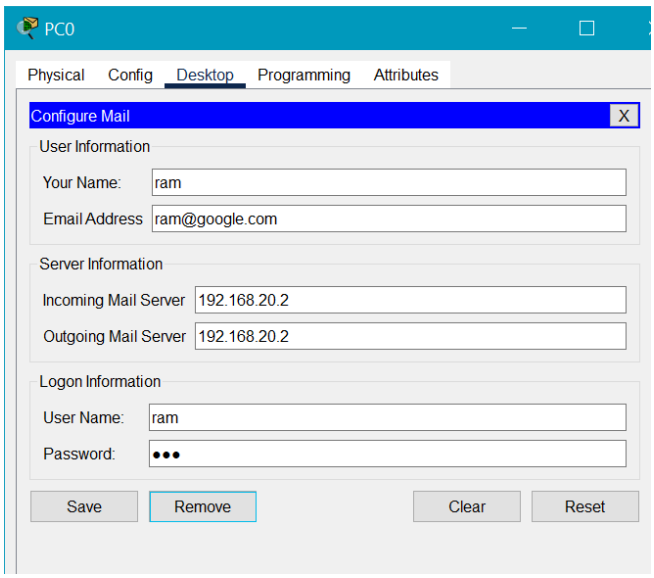
- Configuration of server:



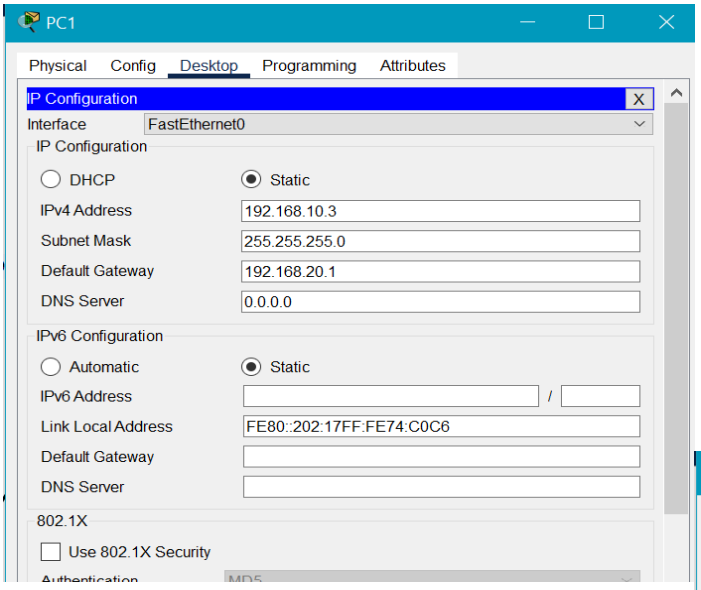


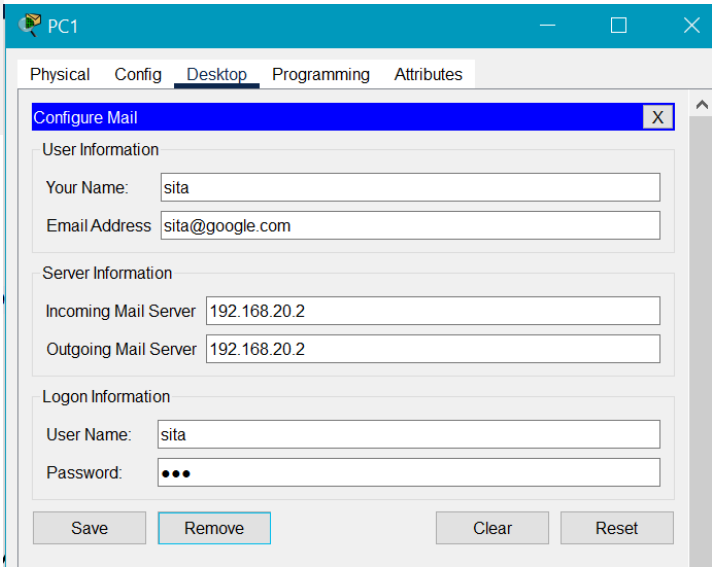
- Configuration of PC0:



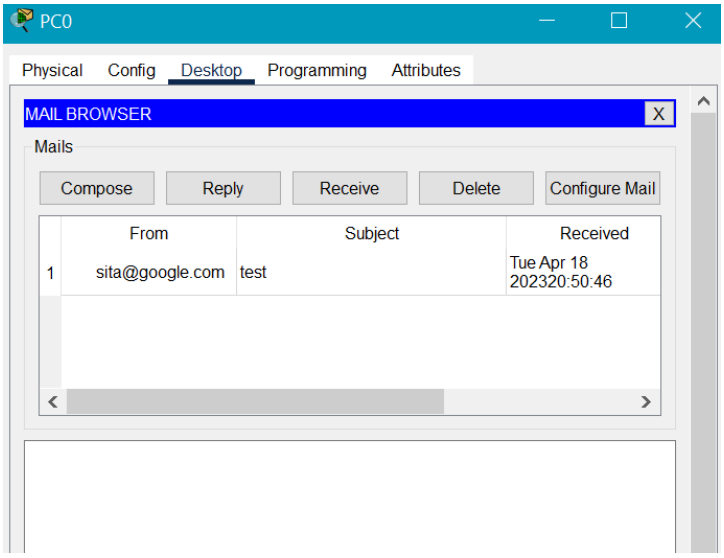


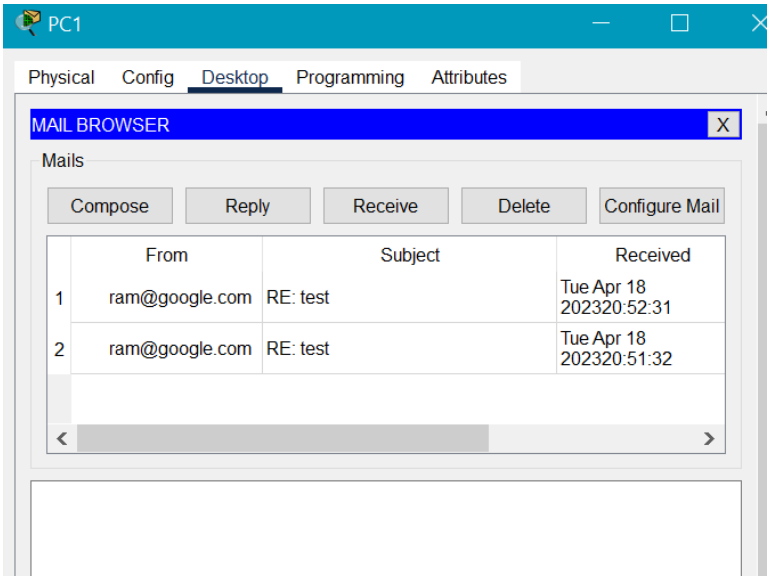
- Configuration of PC1:





- Check emails from composing in pc0 and receiving in pc1:





Conclusion: In this way, we can configure the mail server and can communicate between different pcs in the network.

Lab-5

Overview of FTP server configuration

Objective:

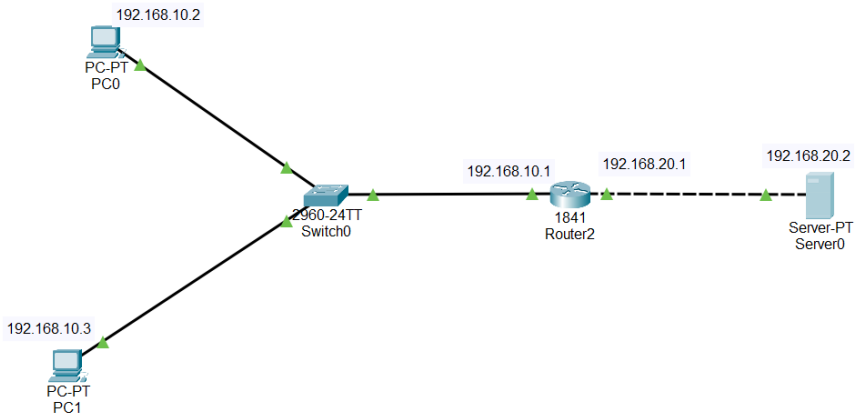
- Understand how to configure the server.
- Understand how to upload file and download file from server.

Background:

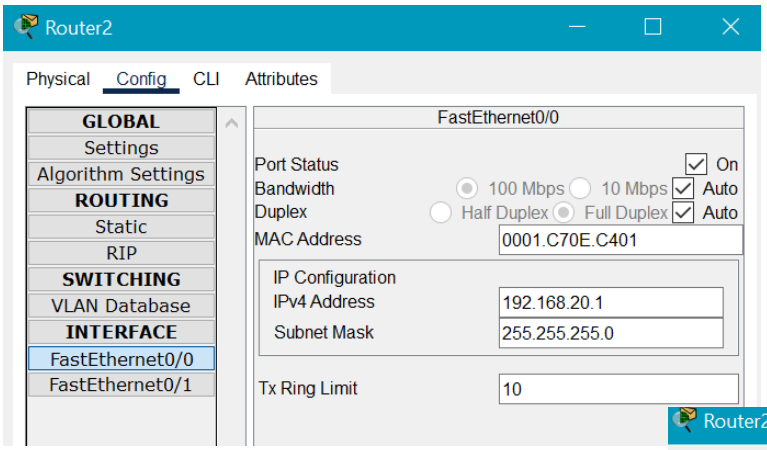
FTP server: The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to client on a computer network. FTP is build on a client-server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS or replaced with SSH File Transfer Protocol (SFTP).

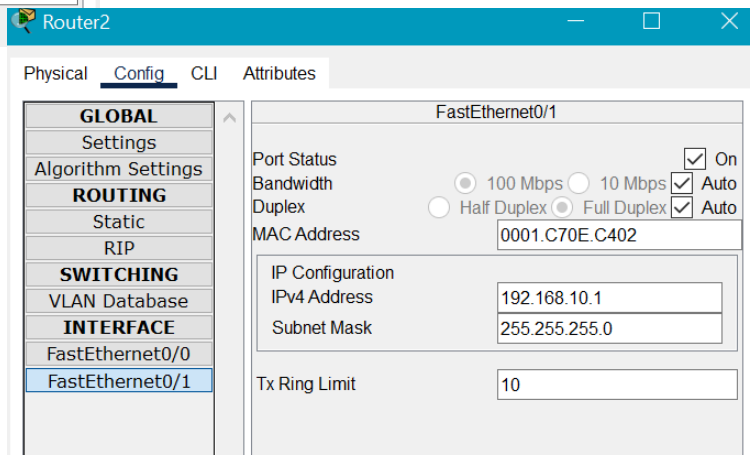
Procedure:

- Configure FTP server, router and switch with two pcs as follows:

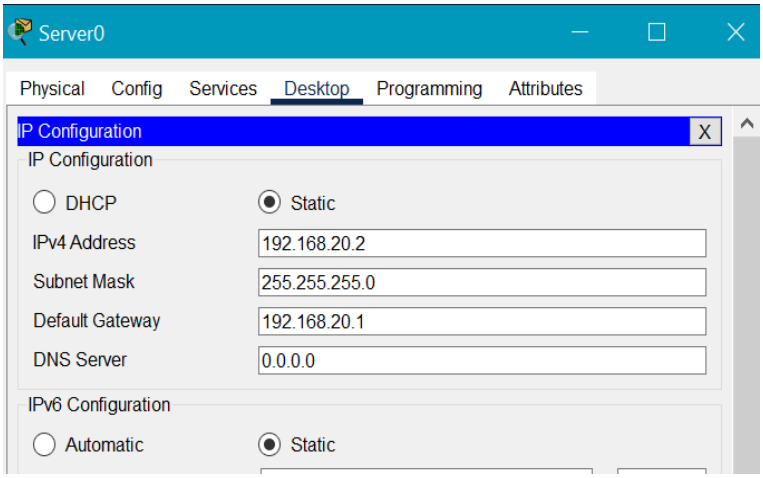


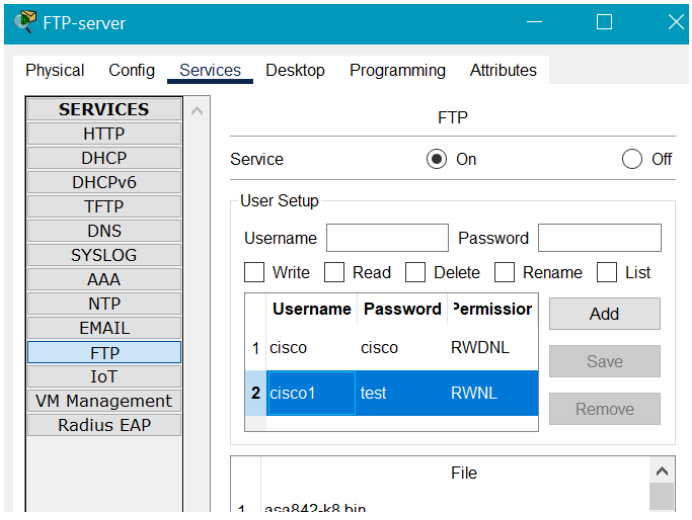
- Configuration of router:



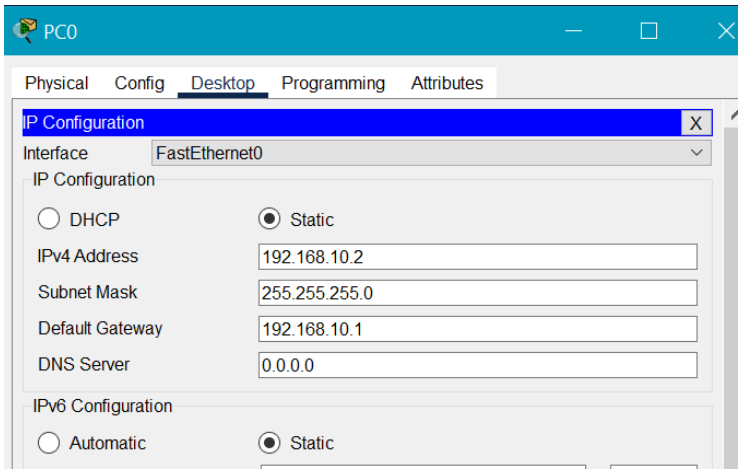


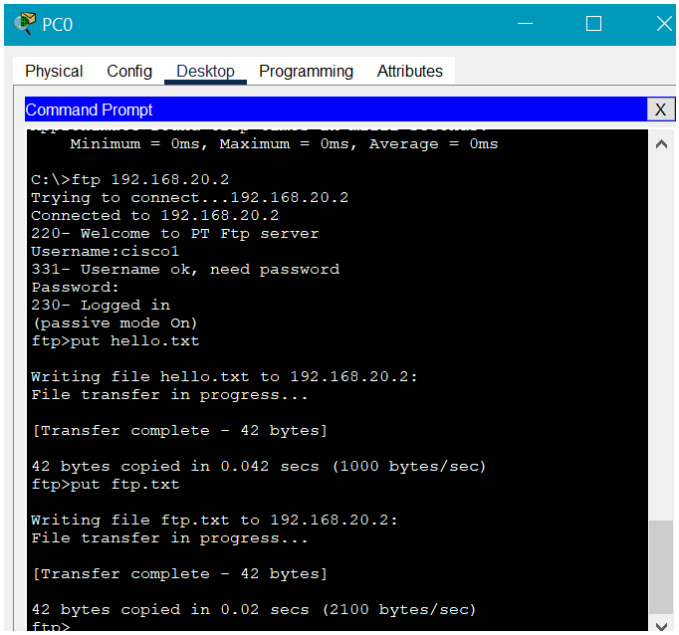
- Configuration of FTP server:



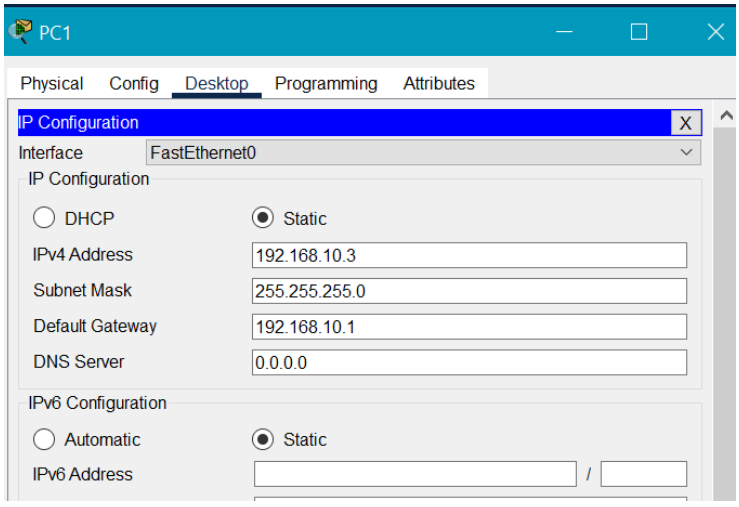


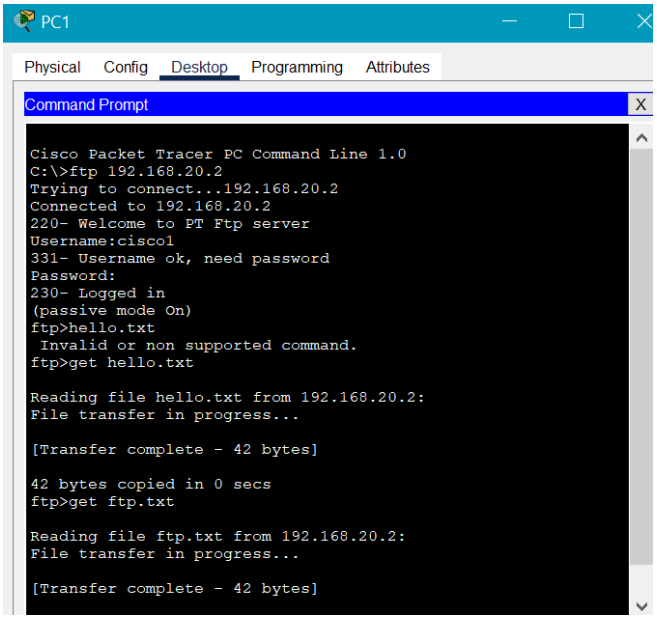
- Configuration and file upload from pc0:





- Configuration and file download from pc1:





Conclusion: In this way, we can upload and download files in the server.

Lab-6

Overview of Web server configuration.

Objective:

- Understand the configuration of web server, DNS server and DHCP server.
- Understand the connectivity of the router and switch.

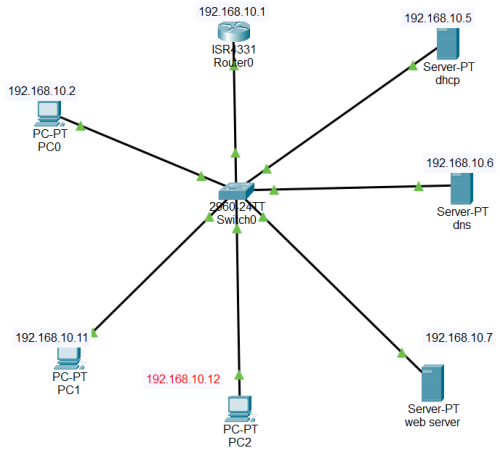
Background:

Web server: A web server is computer software and the underlying hardware that accepts requests via HTTP, the network protocol created to distribute web content, or its secure variant HTTPS. A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP, and the web server responds with the content of that resource or an error message. The web server can also accept and store resources sent from the user agent that is configured to do so.

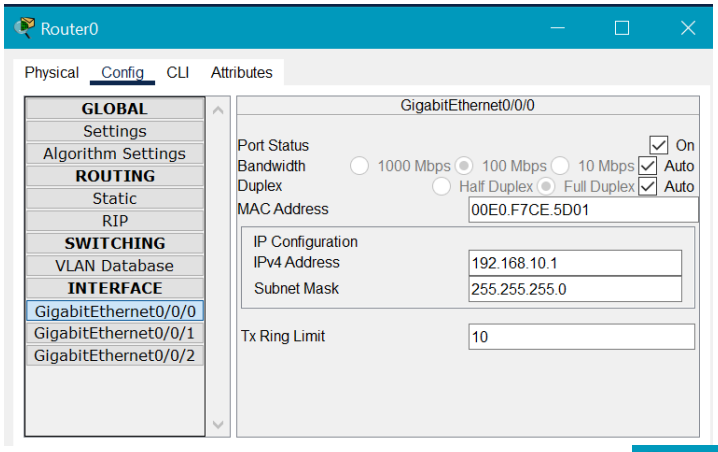
DNS server: A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases servers to resolve, or translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols.

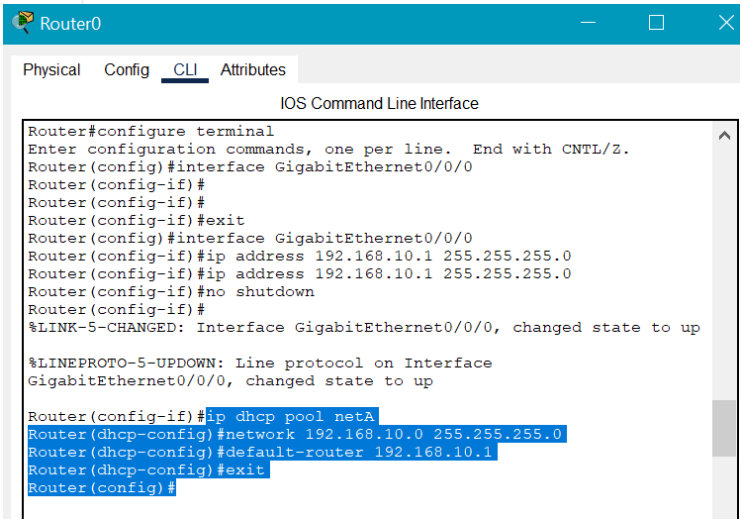
Procedure:

- Configure the webserver, DNS server, DHCP server, router and switch as follows:

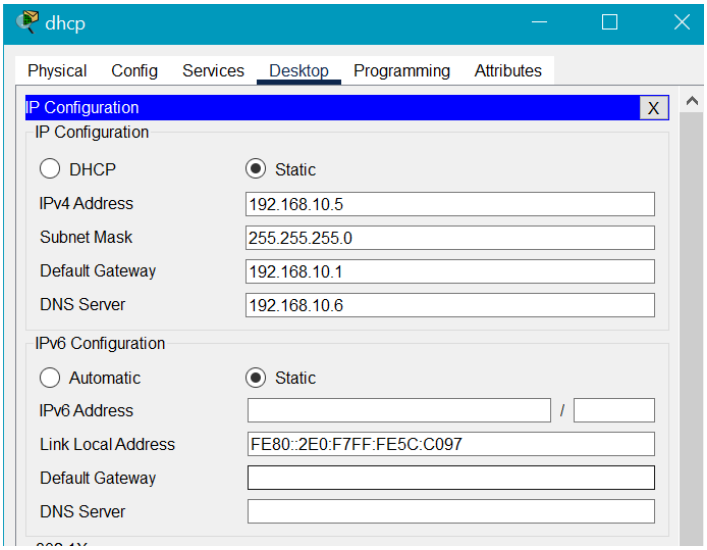


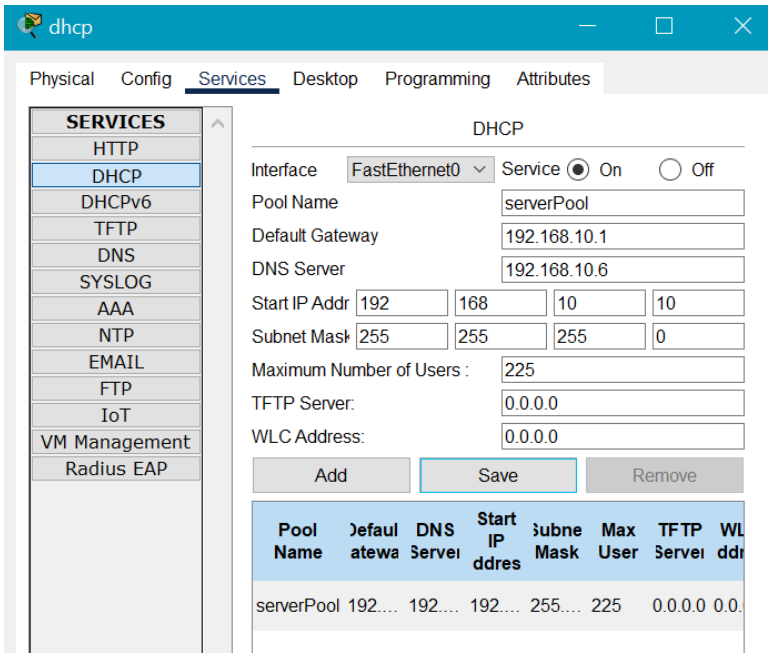
- Configuration of router:



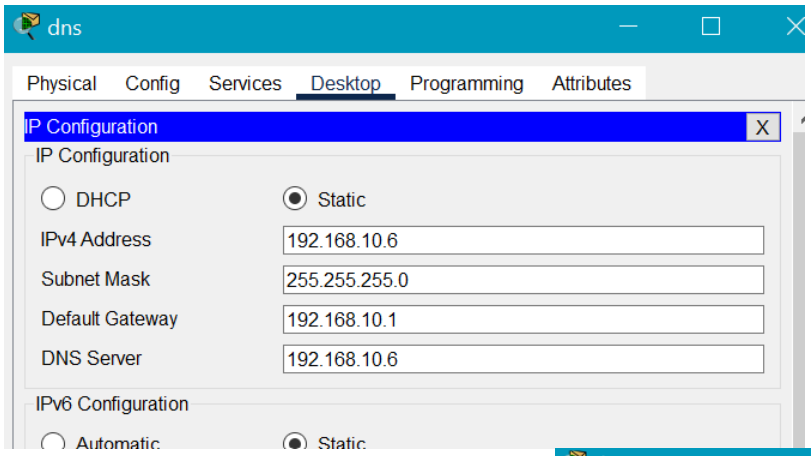


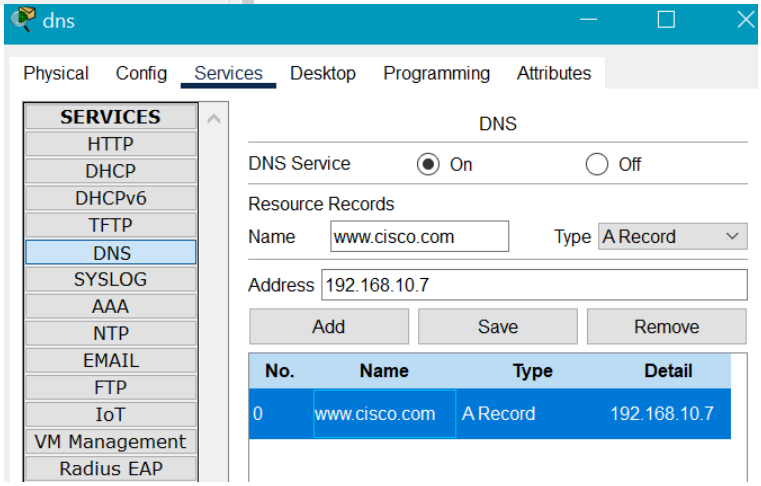
- Configuration of DHCP server:



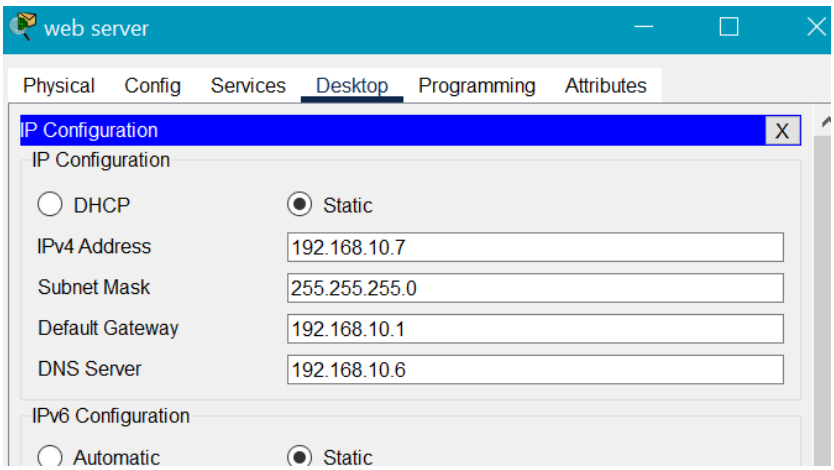


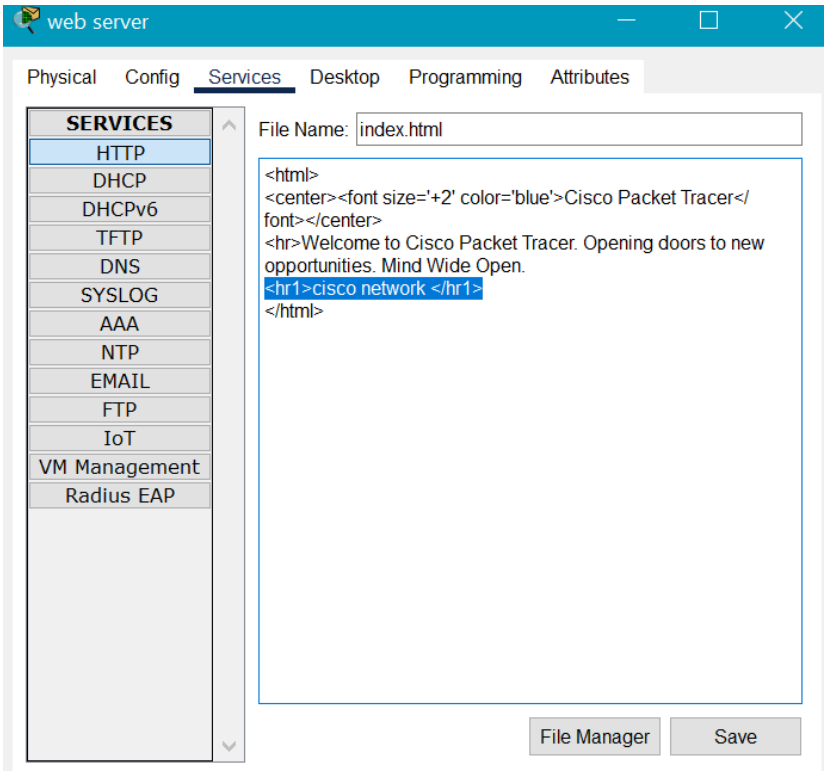
- Configuration of DNS server:



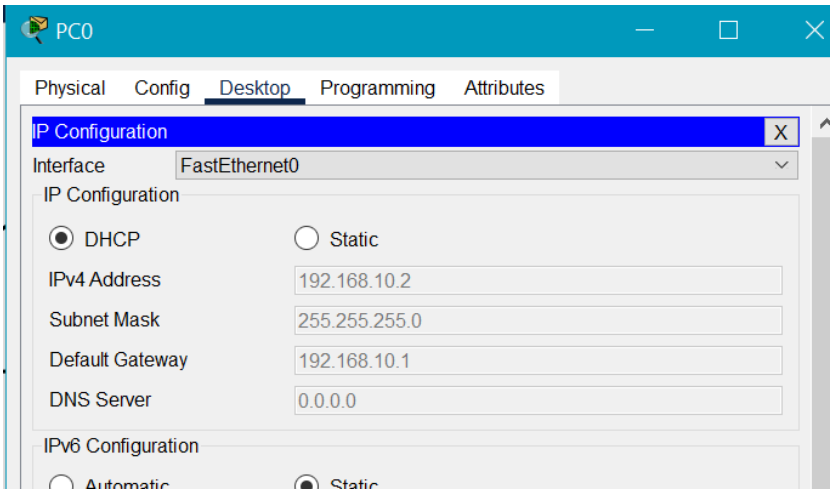


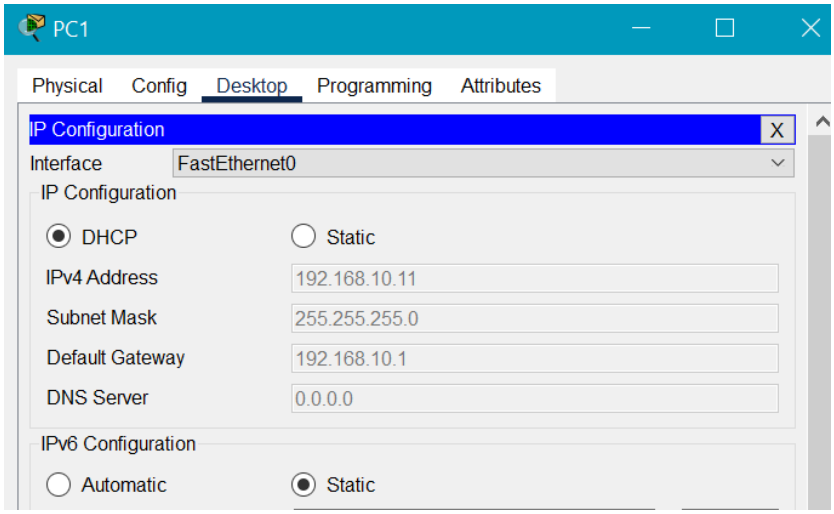
- Configuration of Web server:

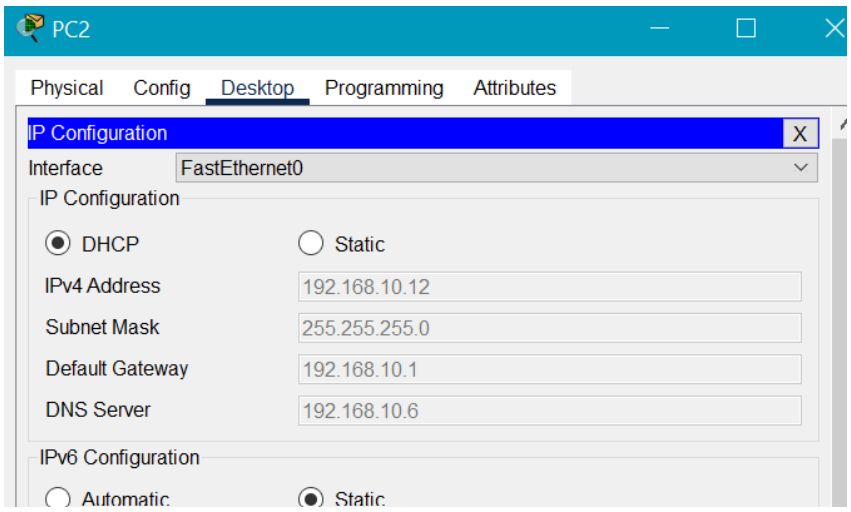




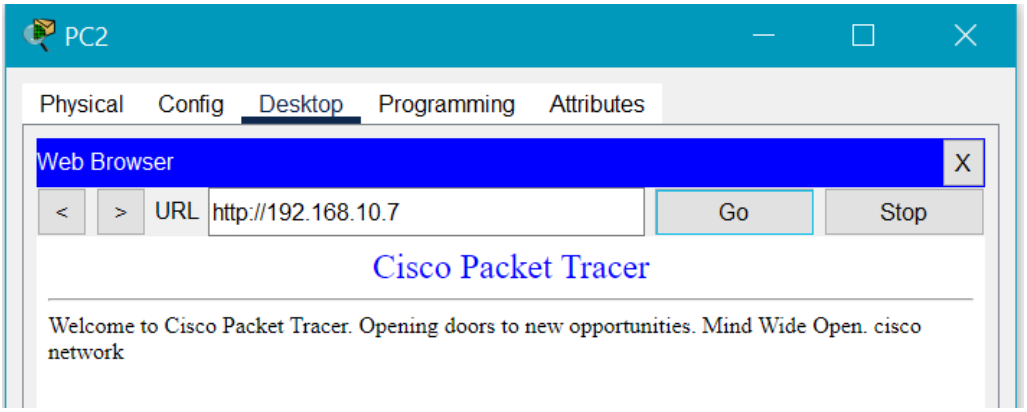
- Configuration of pc0, pc1 and pc2:







- Checking if pc2 can open the URL or not:



Conclusion: In this way, we can configure the webserver from different pcs by using the DHCP server.

Lab-7

Overview of DNS server configuration

Objective:

- Understand the configuration of the DNS server.
- Understand how the switch and pcs are connected to the DNS server.

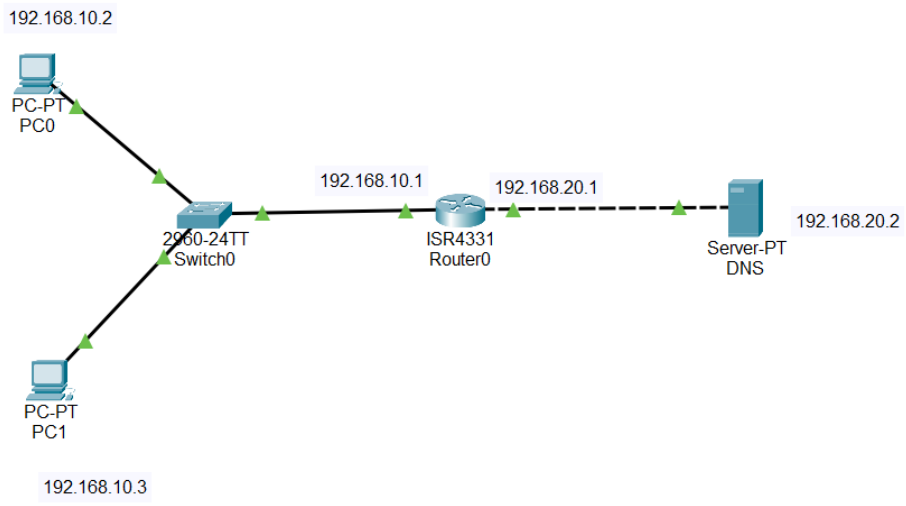
Background:

DNS Server: A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases servers to resolve, or translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols.

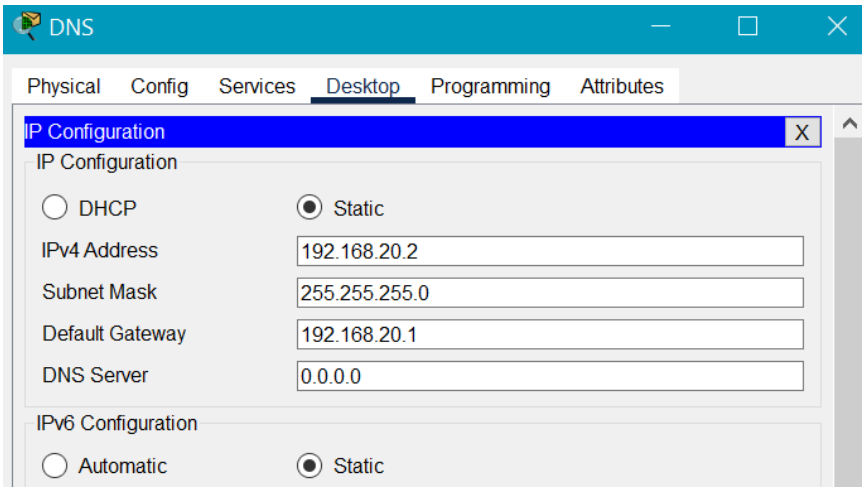
Switch: A switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

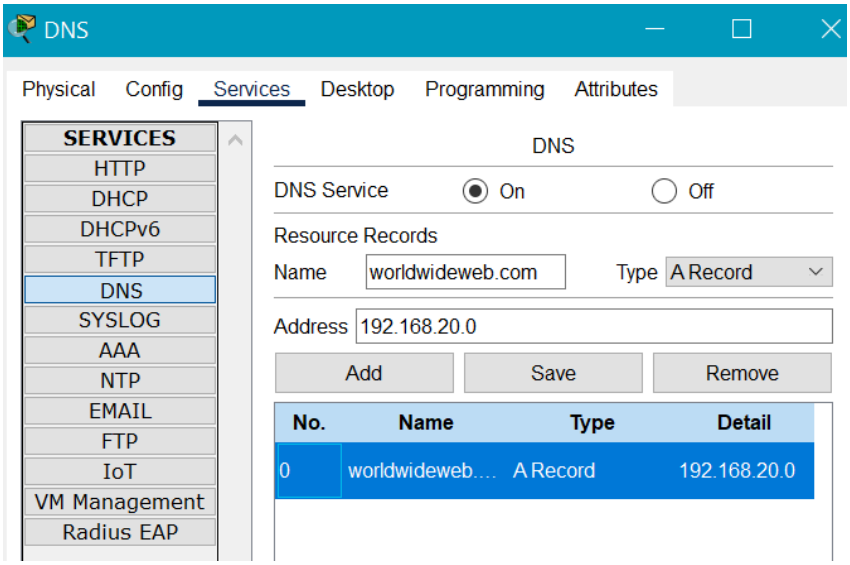
Procedure:

- Configure the DNS server and switch as follows:

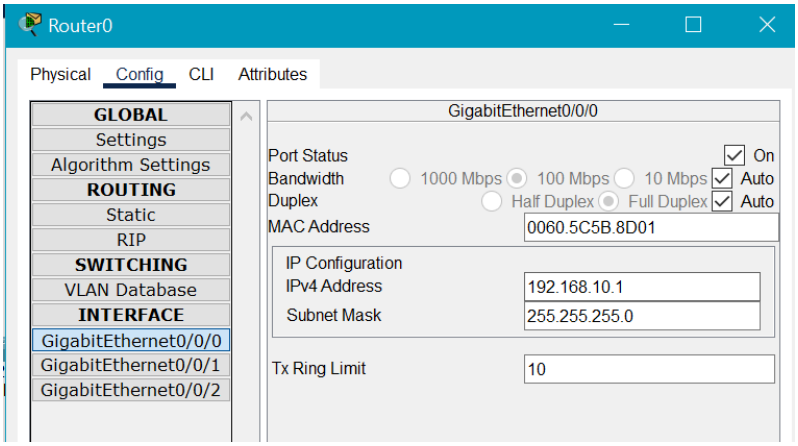


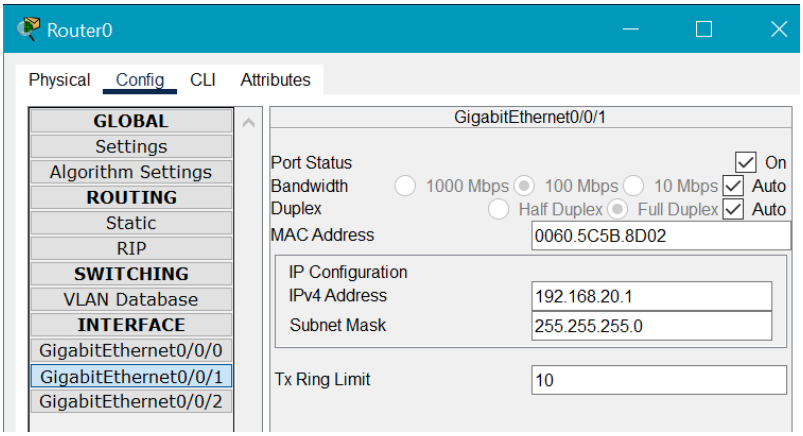
- Configuration of DNS Server:



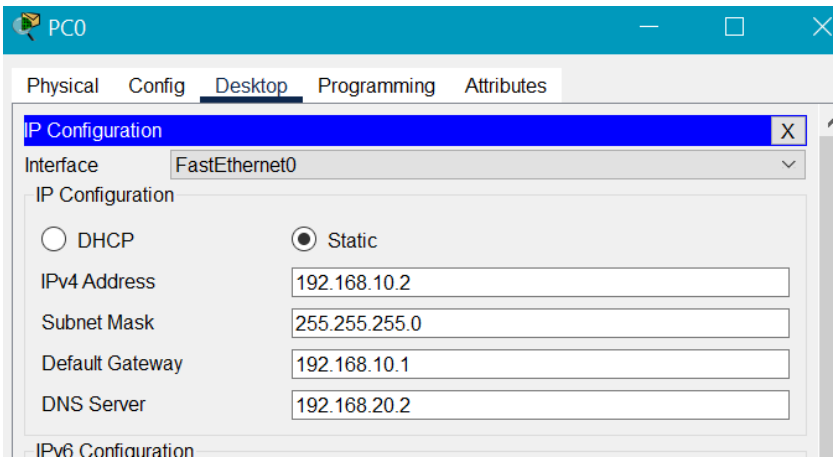


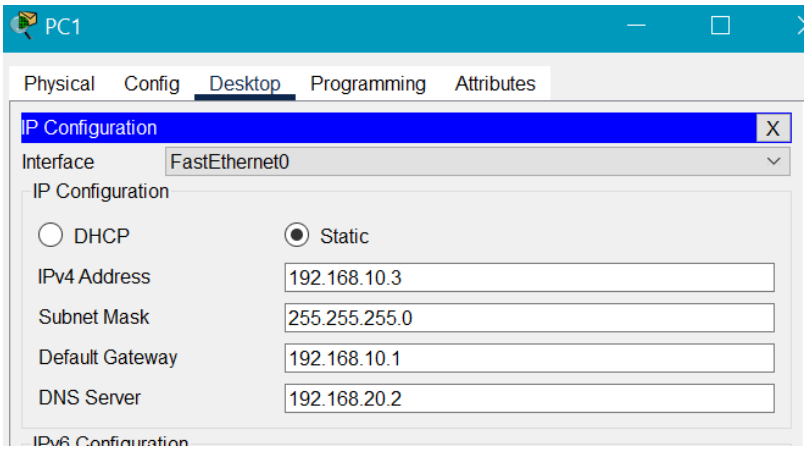
- Configuration of router:



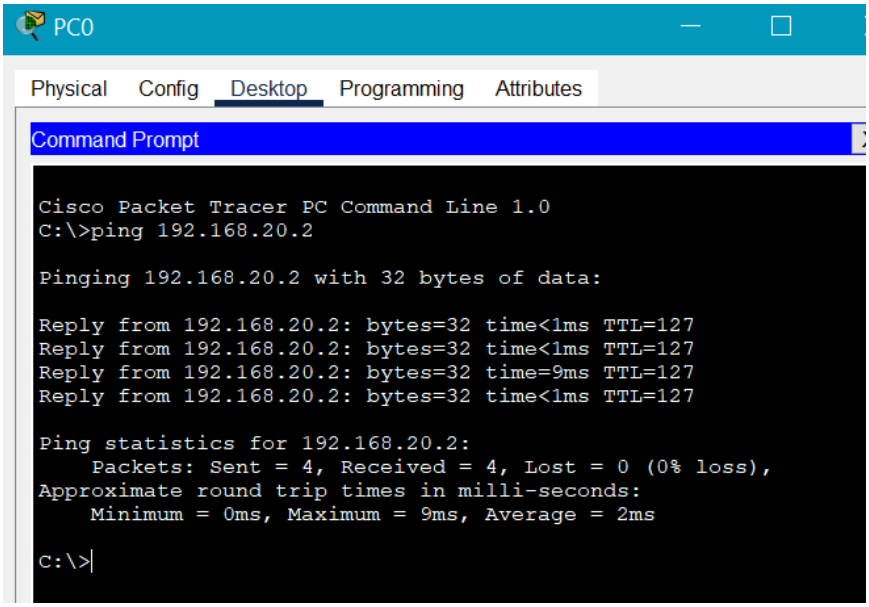


- Configuration of pc0 and pc1:





- To check whether pcs are connected with DNS server, example of pc0:



Conclusion: In this way, we can connect the DNS server with pcs with the help of a switch.

Lab-8

Overview of firewall configuration on server

Objective:

- Understand the configuration of the firewall server.
- Understand how to block the packet or give access to the user.

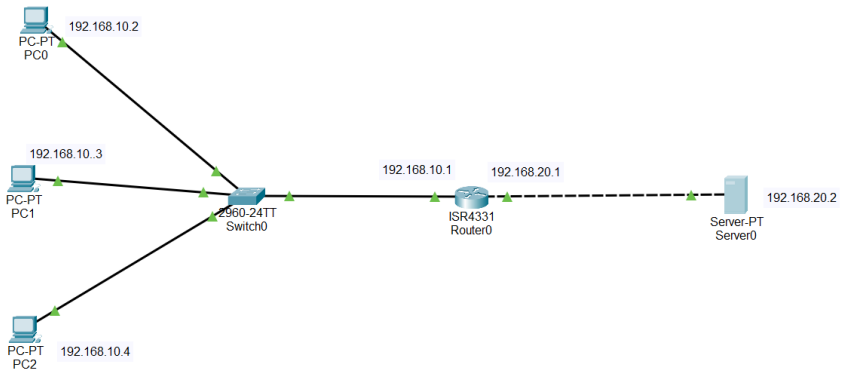
Background:

Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been the first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the internet. A firewall can be hardware, software or both.

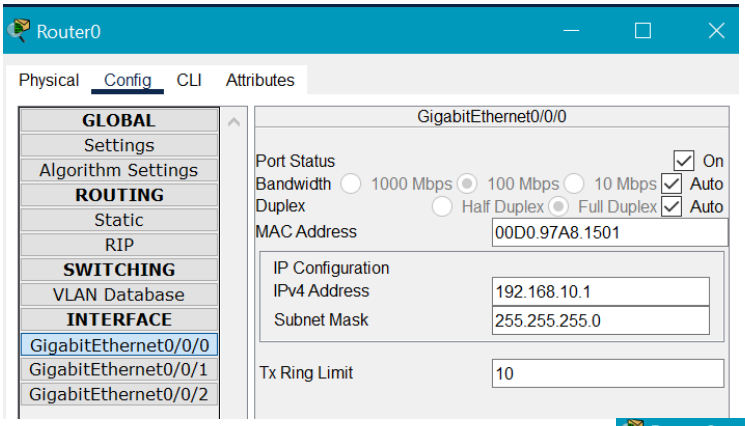
Hub: A hub is a physical layer networking device that is used to connect multiple devices in a network. They are generally used to connect computers to a LAN. A hub has many ports in it. A computer that intends to be connected to the network is plugged into one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

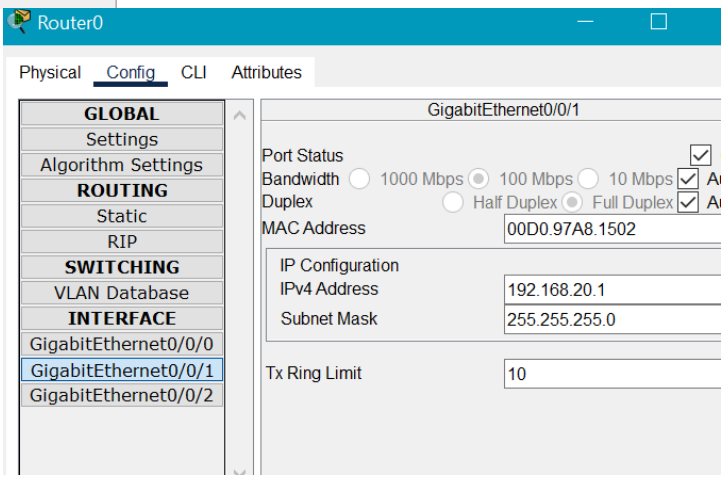
Procedure:

- Configure firewall and hub as follows:

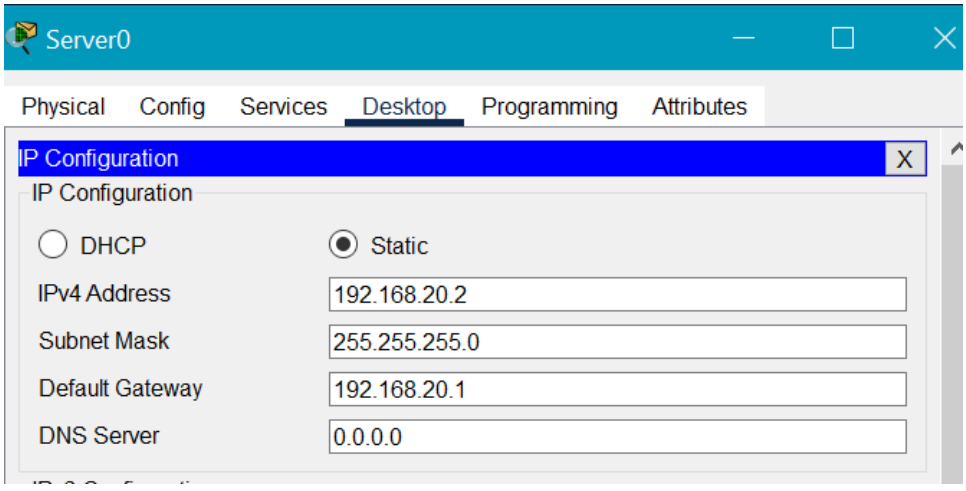


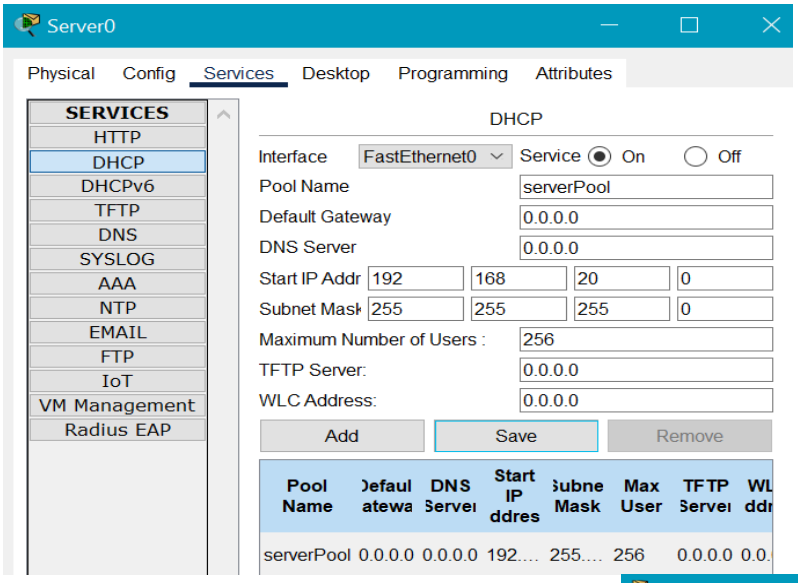
- Configuration of router:

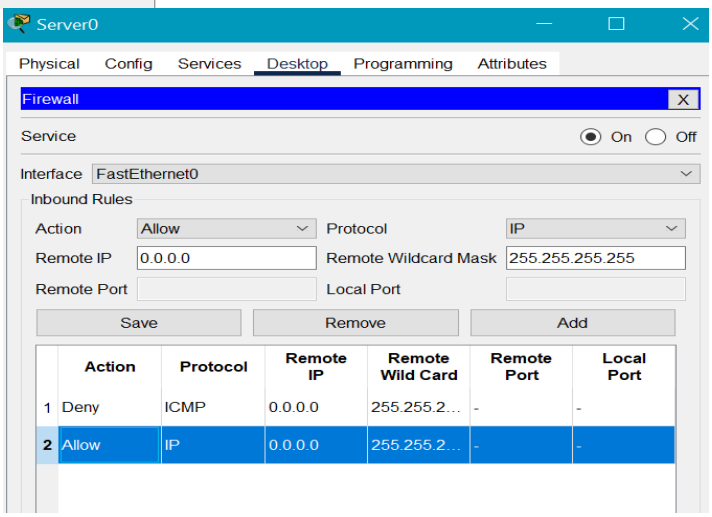




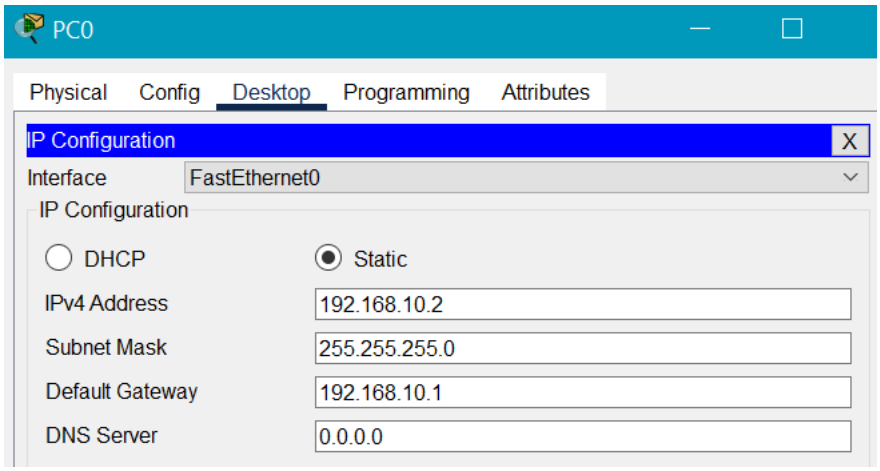
- Configuration of server:

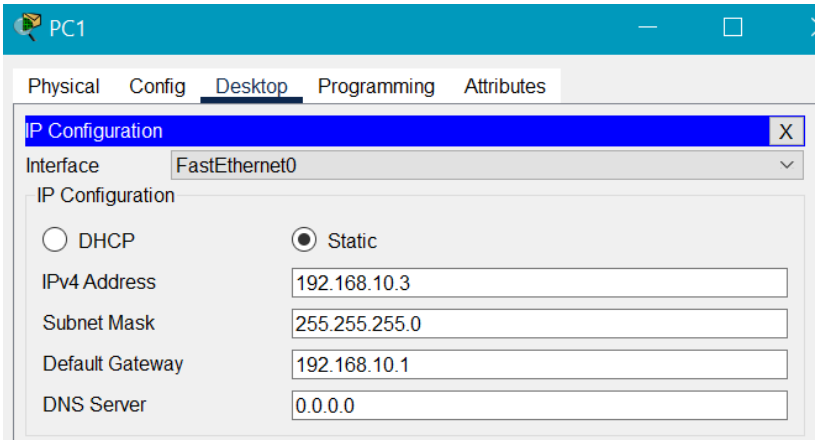


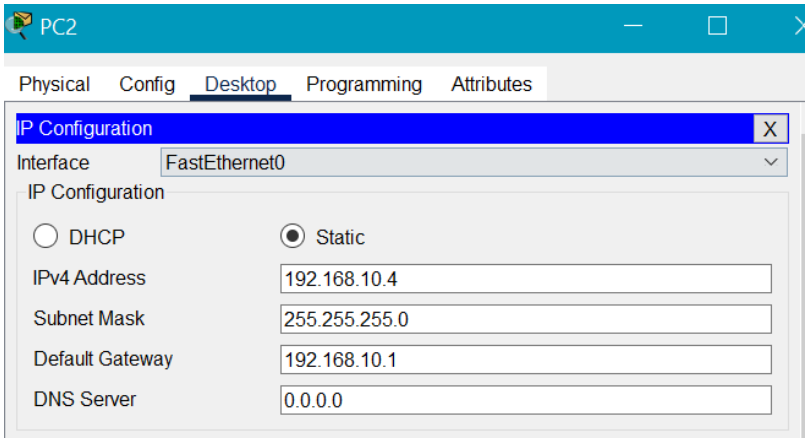




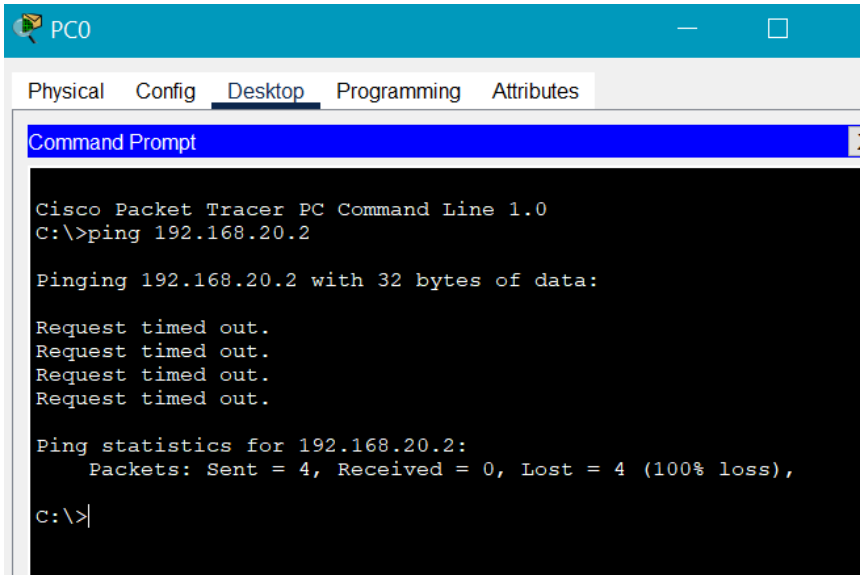
- Configuration of pc0, pc1 and pc2:

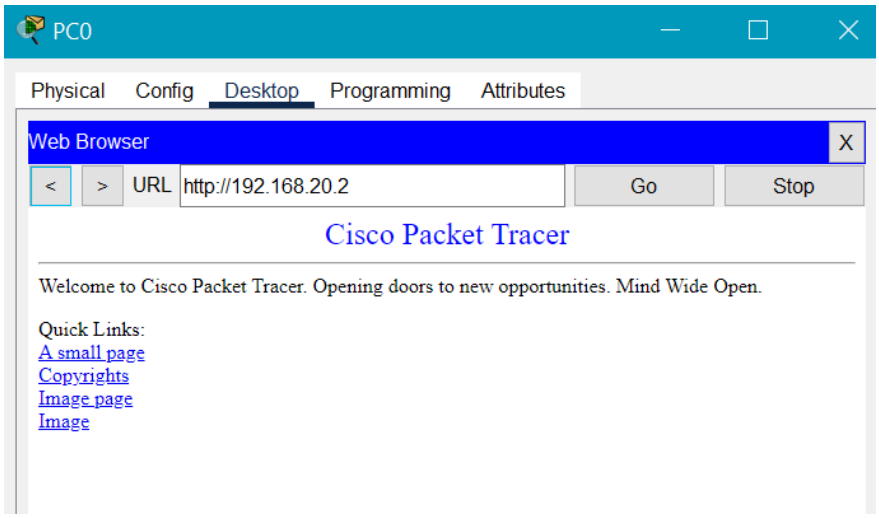






- To check whether ICMP is blocked and IP is allowed or not:





Conclusion: In this way, we can connect the Firewall server with the help of a hub and pcs.

Lab-9

Overview of RIP configuration

Objective:

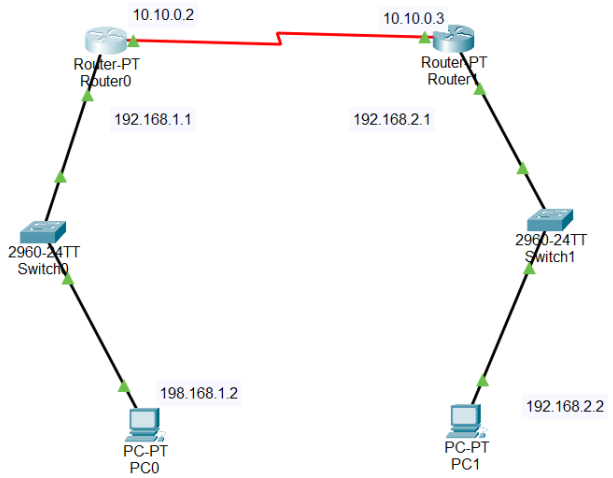
- Understand the RIP configuration.
- Understand how to connect the switch and router.

Background:

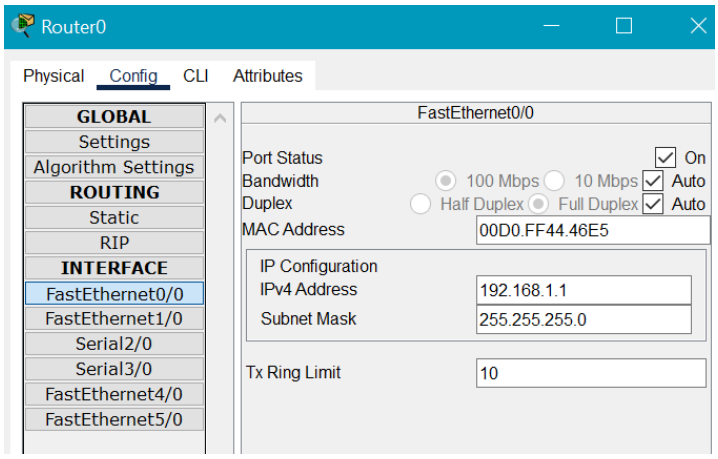
RIP configuration: Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the application layer of the OSI model. Cisco software sends routing information updates every 30 seconds, which is termed advertising. If a device does not receive an update from another device for 180 seconds or more, the receiving device marks the routes served by the non-updating device as unusable.

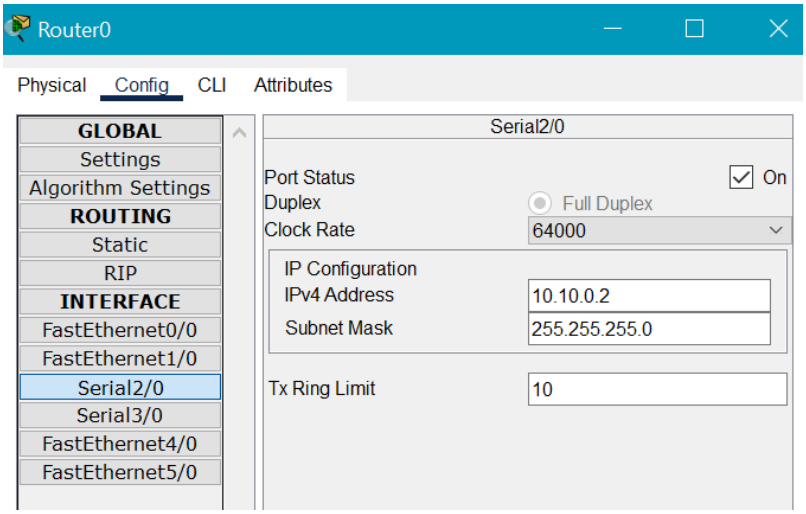
Procedure:

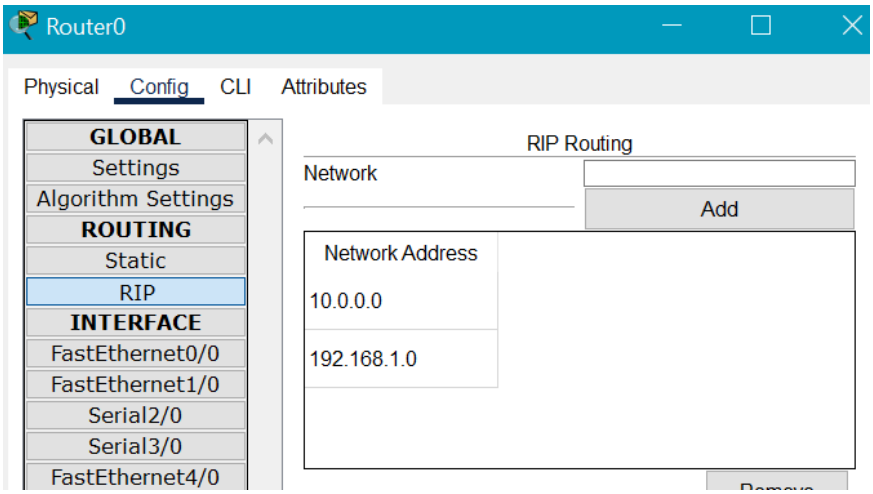
- Configure RIP, router, switch with pcs as follows:



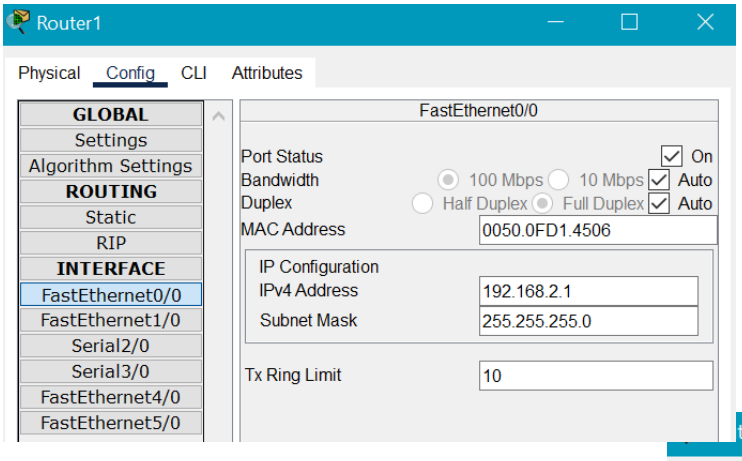
- Configuration of router0:

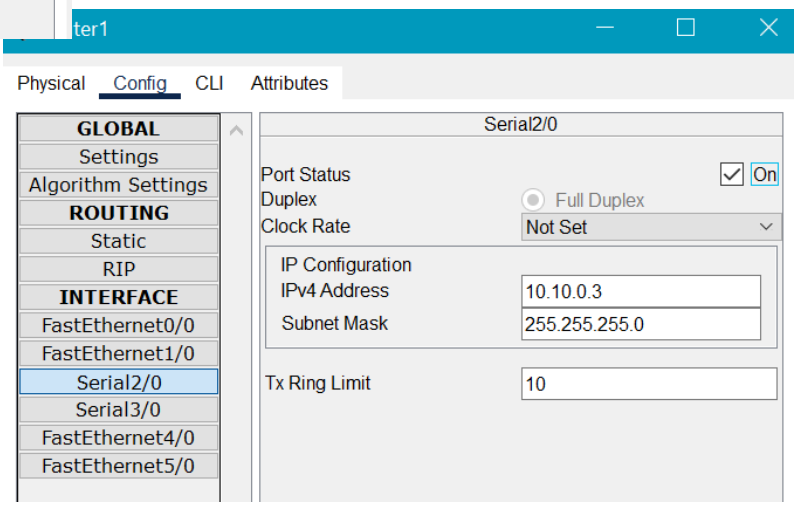


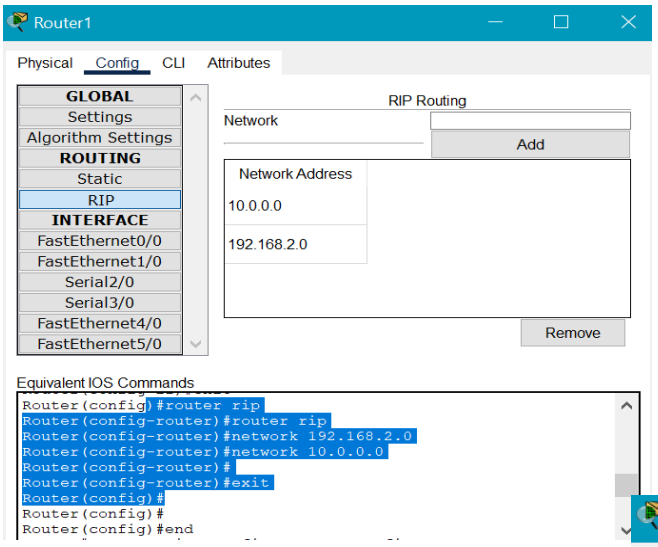


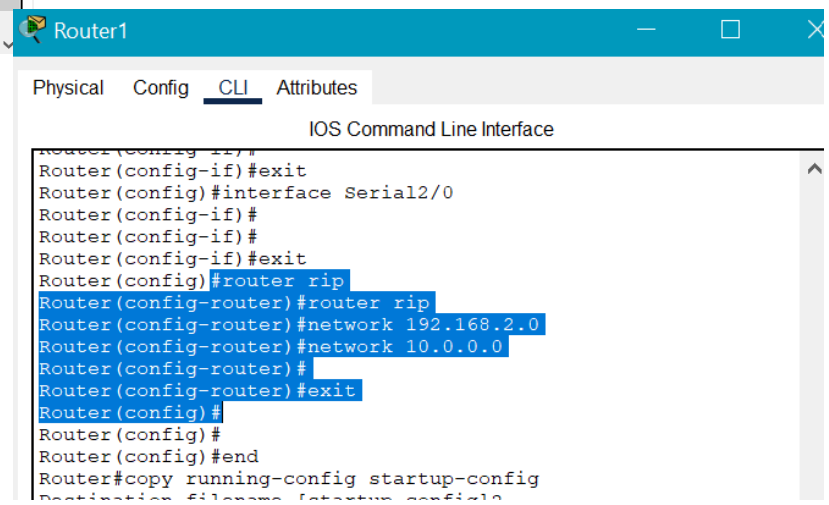


- Configuration of router1:

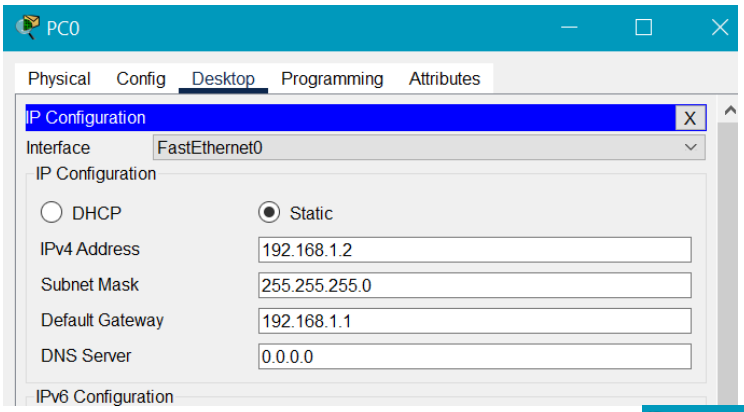


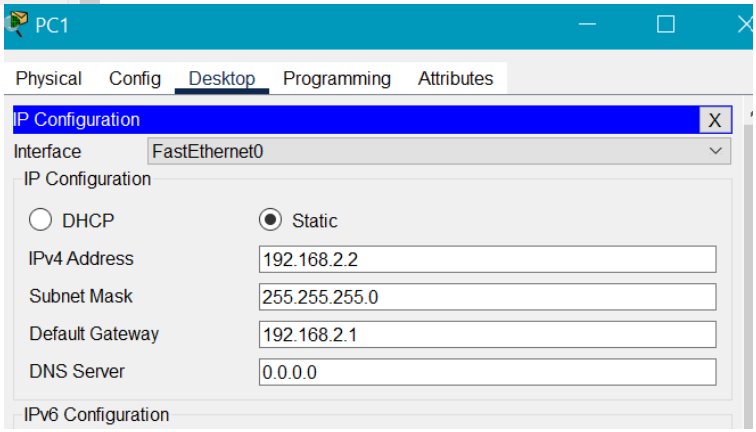




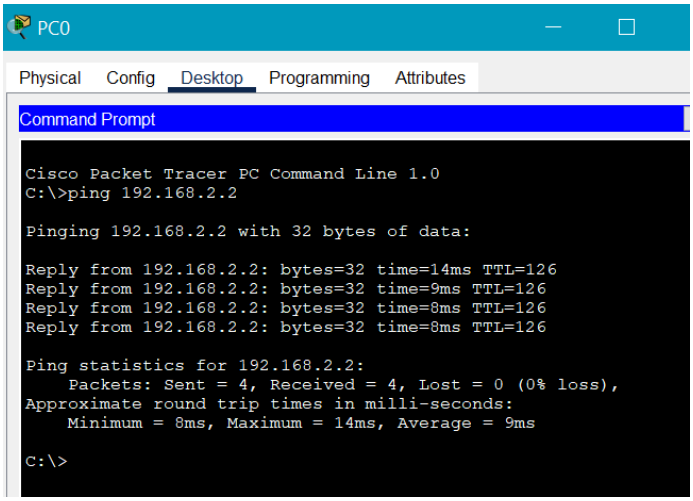


- Configuration of pc0 and pc1:





- To check whether pc0 ping pc1 or not:



Conclusion: In this way, we can configure the Routing Information Protocol (RIP) of router0 and router1.

Lab-10

Overview of BGP

Objective:

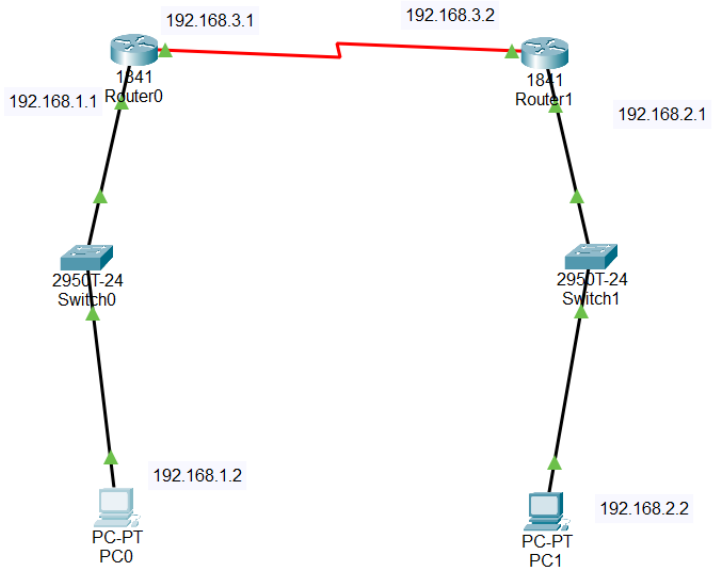
- Understand the RIP configuration.
- Understand how to connect the switch and router.

Background:

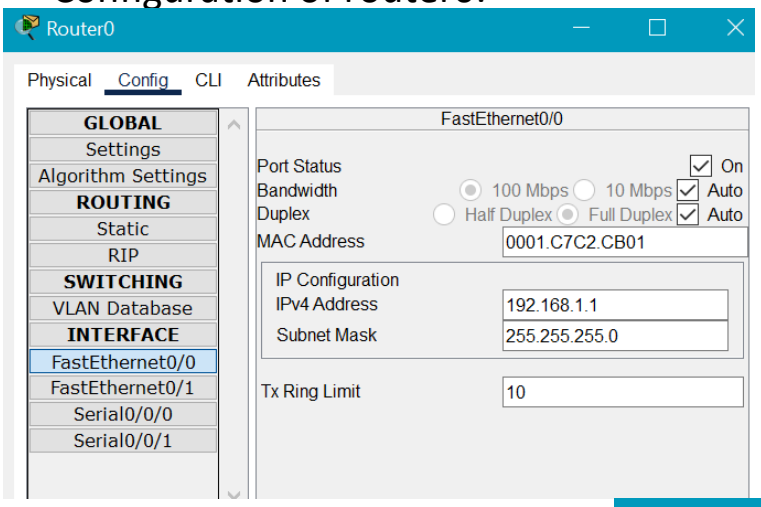
BGP configuration: Border Gateway Protocol (BGP) refers to a gateway protocol that enables the internet to exchange routing information between autonomous systems (AS). As networks interact with each other, they need a way to communicate. This is accomplished through peering. BGP makes peering possible. Without it, networks would not be able to send and receive information with each other.

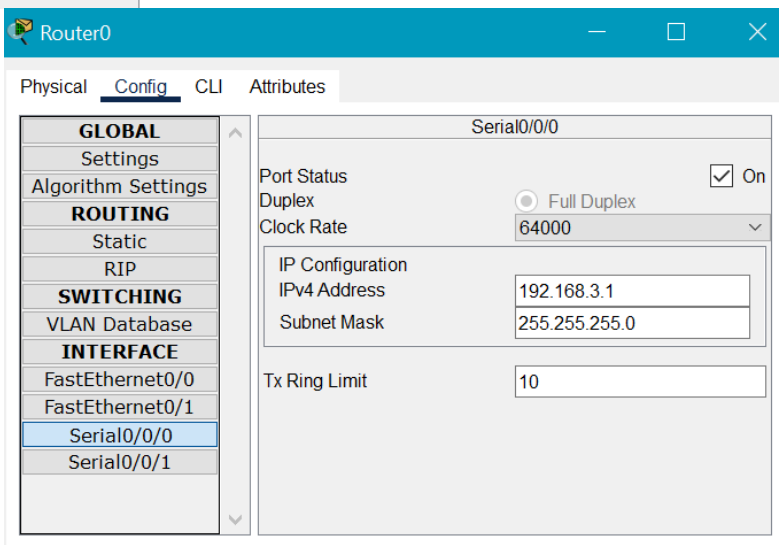
Procedure:

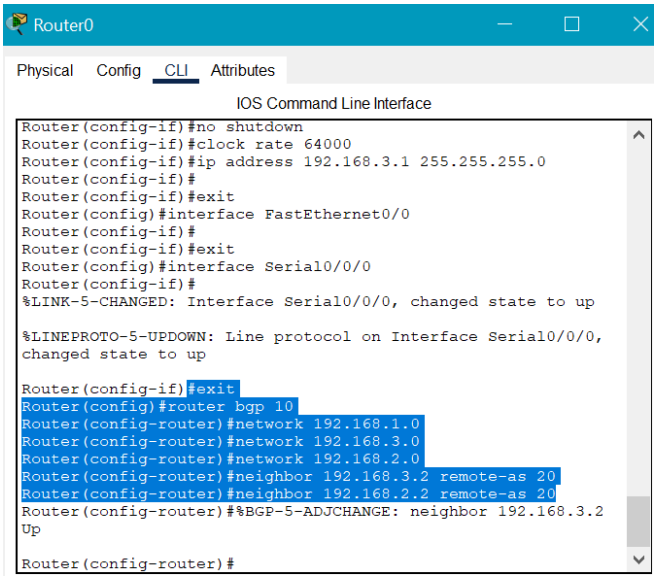
- Configure the BGP router, switches with pcs as follows:



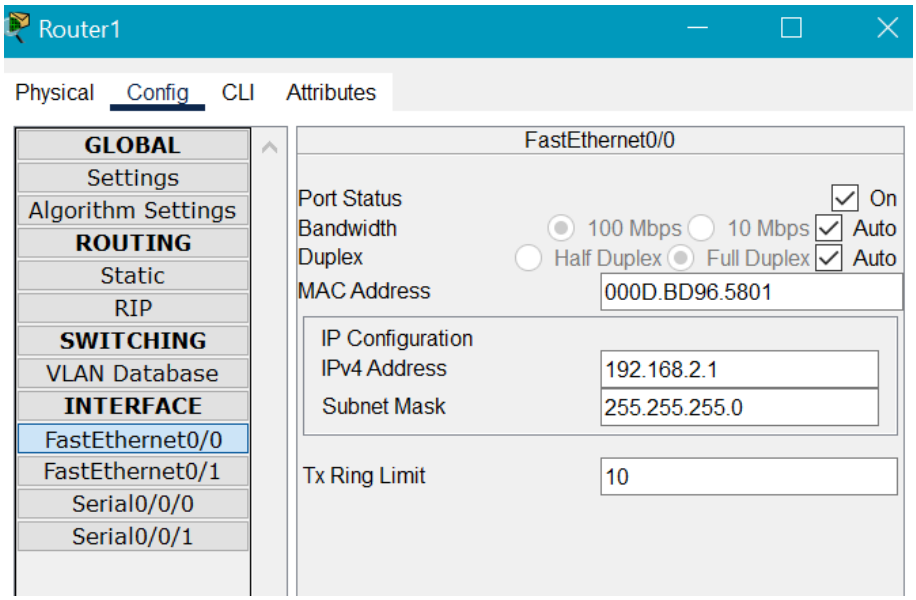
- Configuration of router0:

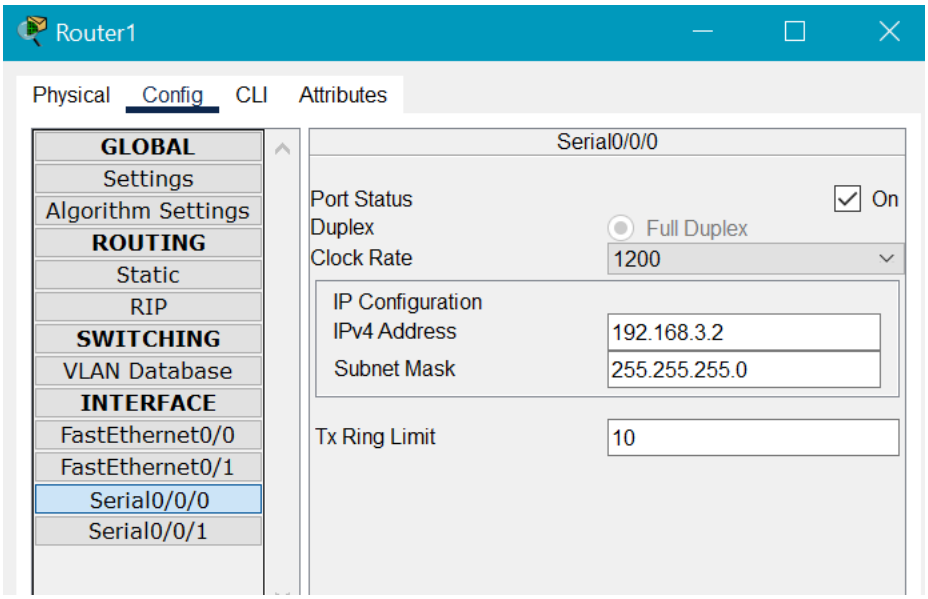


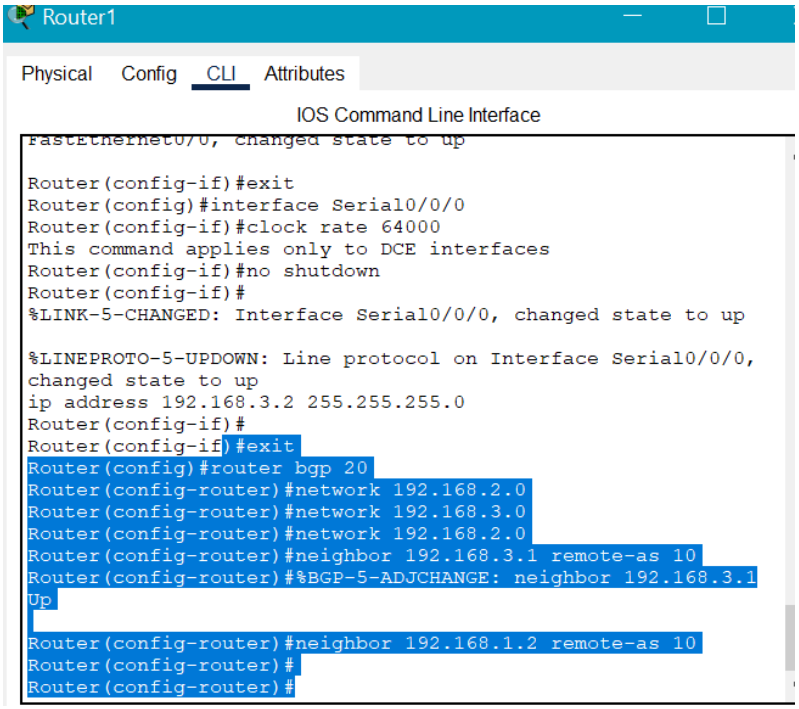




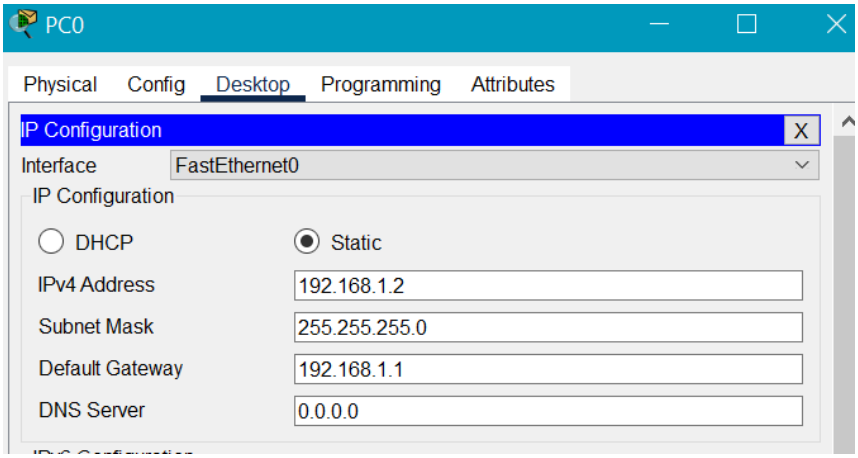
- Configuration of router1:

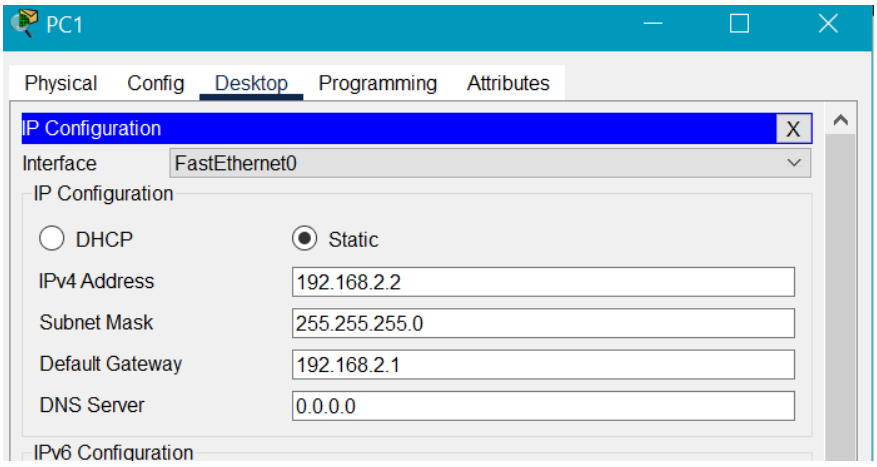




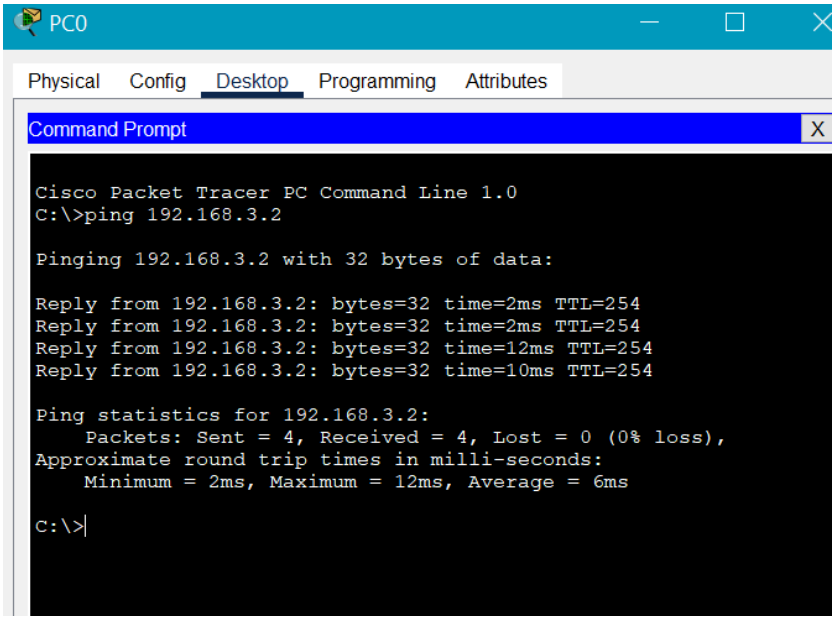


- Configuration of pc0 and pc1:





- To check whether pc0 ping pc1 or not:



Conclusion: In this way, we can configure the Border Gateway Protocol (BGP) of router 0 and router 1.

Lab-11

Overview of OSPF configuration.

Objective:

- Understand the OSPF configuration.
- Understand how to connect the pc and router with OSPF.

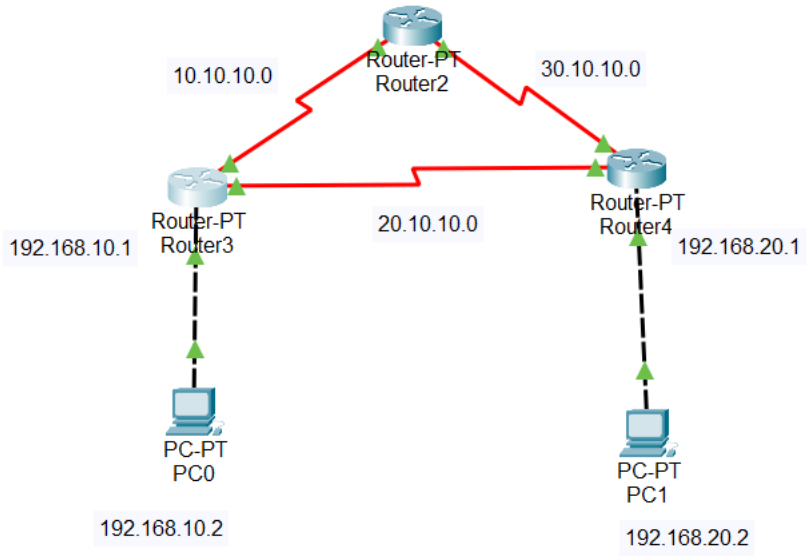
Background:

OSPF configuration: The Open Shortest Path First (OSPF) protocol, developed by the Internet Engineering Task Force (IETF), is a link-state Interior Gateway Protocol (IGP).

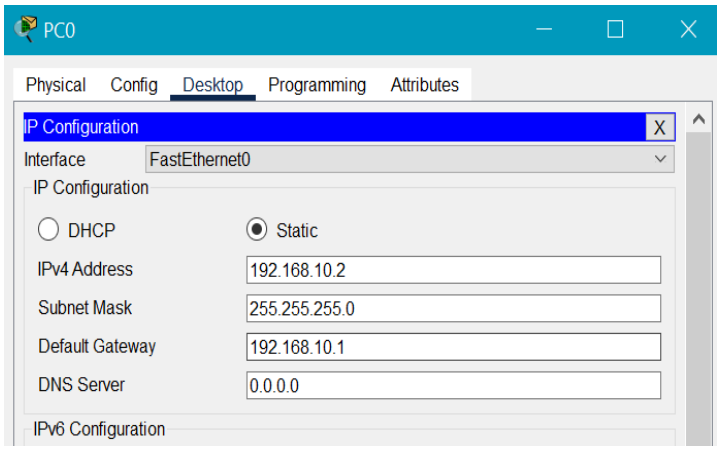
At present, OSPF Version 2, defined in RFC 2328, is intended for IPv4, and OSPF Version 3, defined in RFC 2740, is intended for IPv6. Unless otherwise stated, OSPF stated in this document refers to OSPF Version 2.

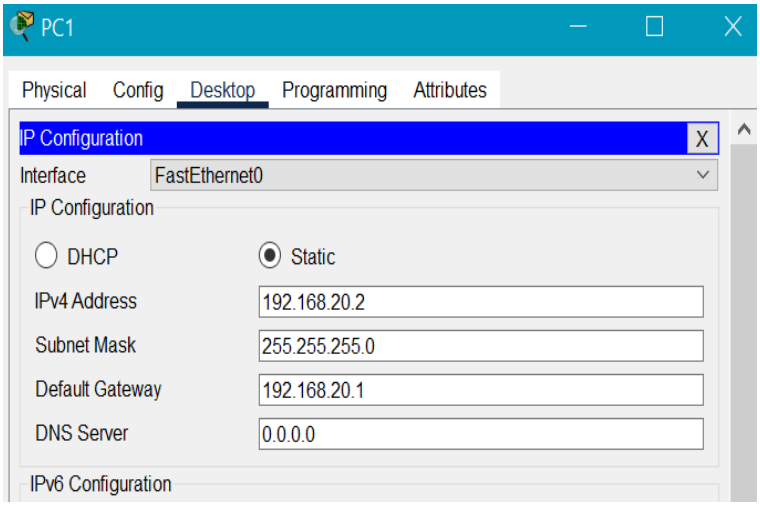
Procedure:

- Configure OSPF, router with pcs as follows:

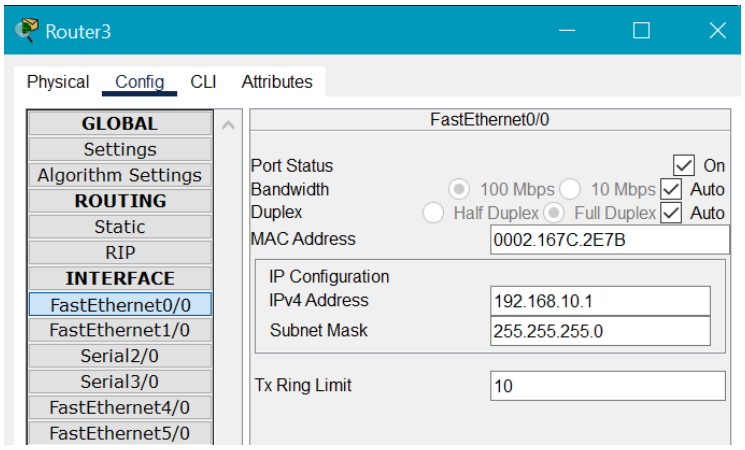


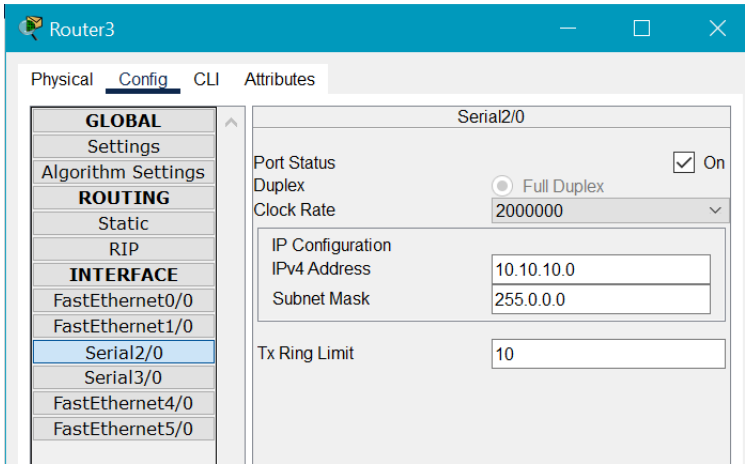
- Configuration of pc0 and pc1:

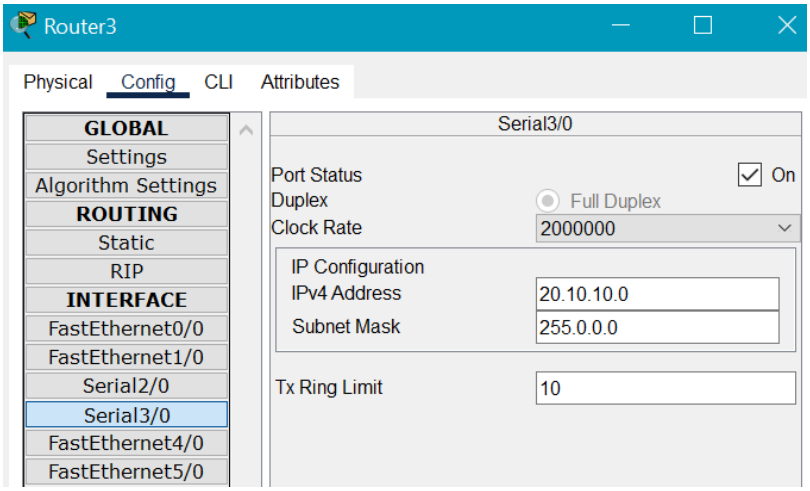


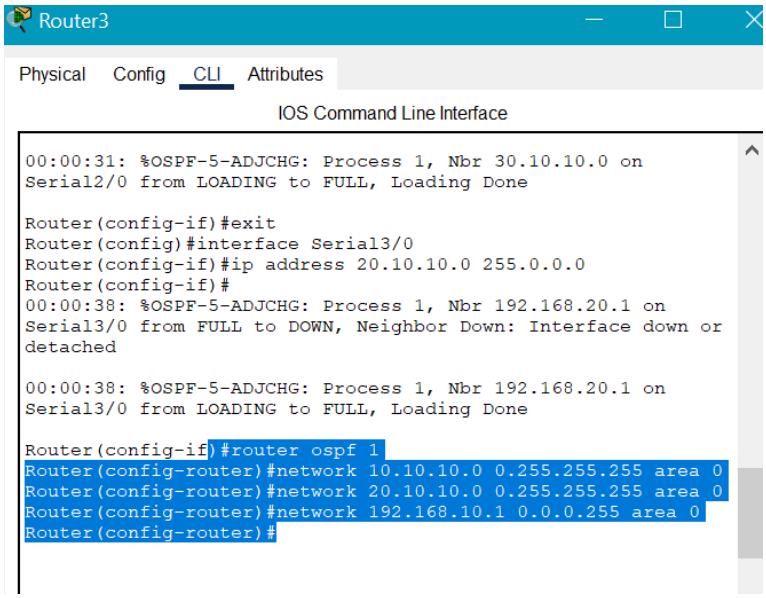


- Configuration of router3:

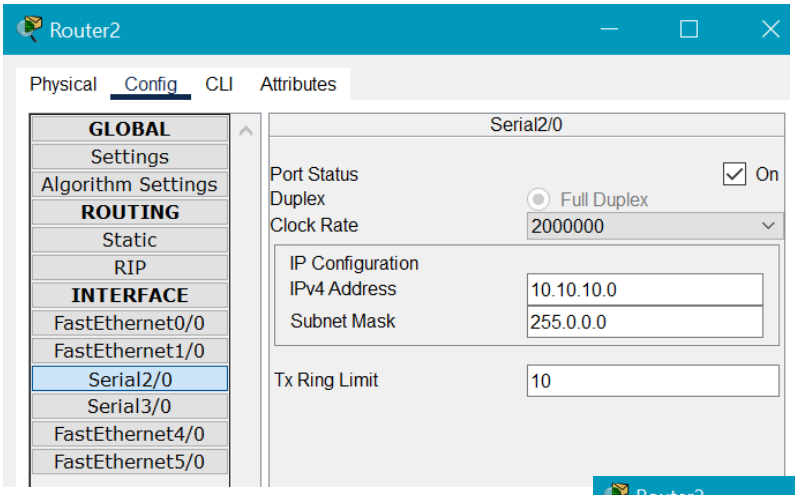


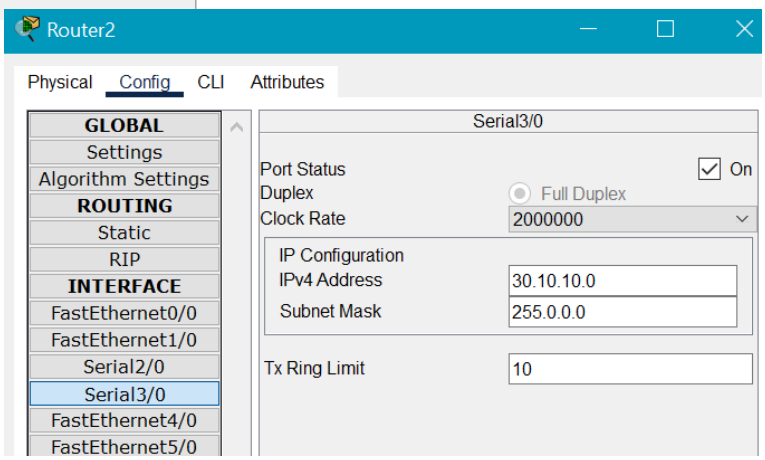

Router3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.10.10.0
Subnet Mask
255.0.0.0
Tx Ring Limit
10

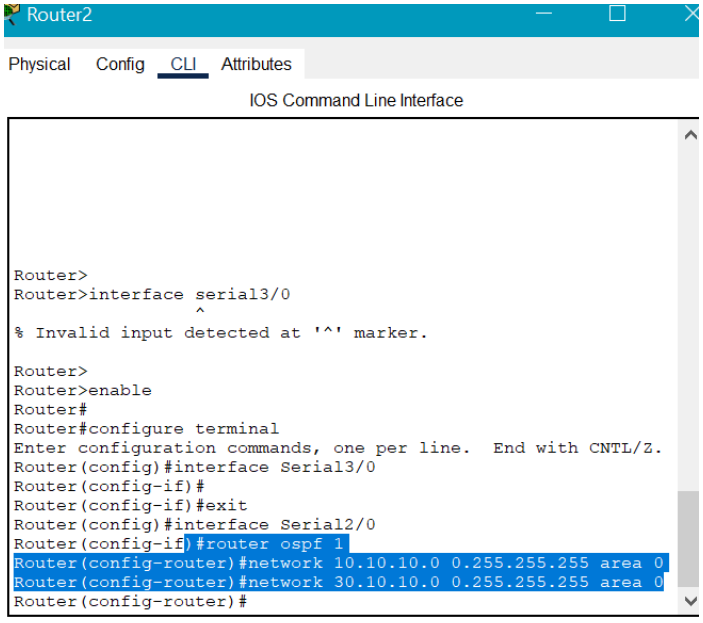

Router3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial3/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
20.10.10.0
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router3
Physical
Config
CLI
Attributes
IOS Command Line Interface
00:00:31: %OSPF-5-ADJCHG: Process 1, Nbr 30.10.10.0 on Serial2/0 from LOADING to FULL, Loading Done
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#ip address 20.10.10.0 255.0.0.0
Router(config-if)#
00:00:38: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial3/0 from FULL to DOWN, Neighbor Down: Interface down or detached
00:00:38: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial3/0 from LOADING to FULL, Loading Done
Router(config-if)#router ospf 1
Router(config-router)#network 10.10.10.0 0.255.255.255 area 0
Router(config-router)#network 20.10.10.0 0.255.255.255 area 0
Router(config-router)#network 192.168.10.1 0.0.0.255 area 0
Router(config-router)#

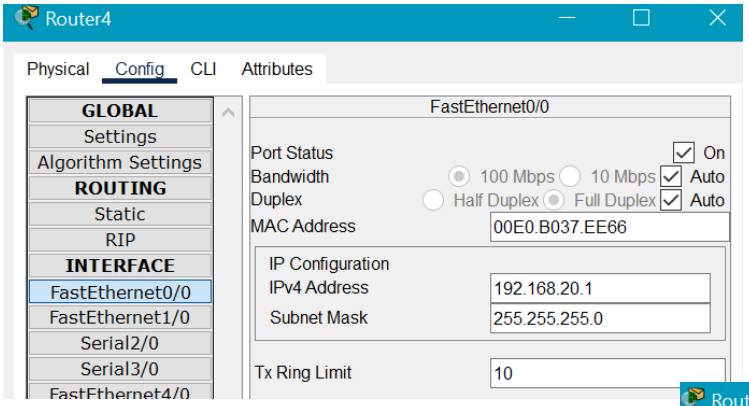
- Configuration of router2:

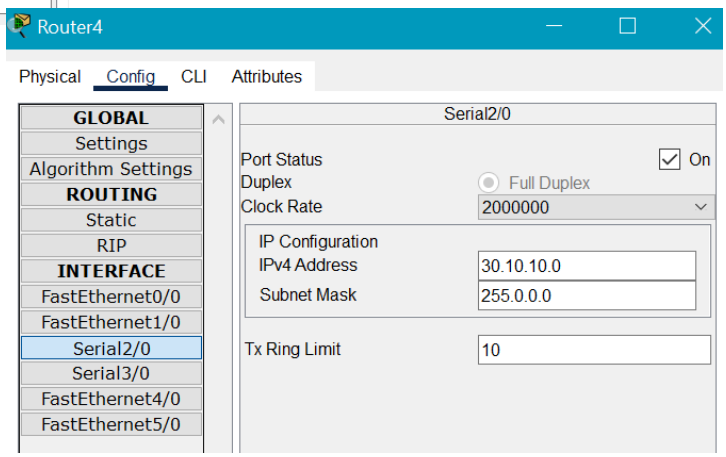


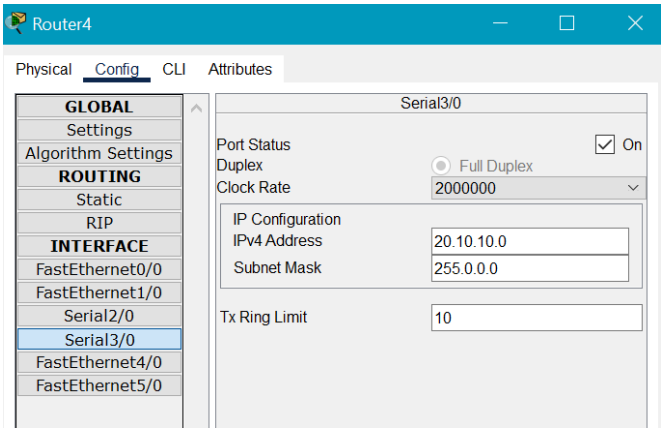


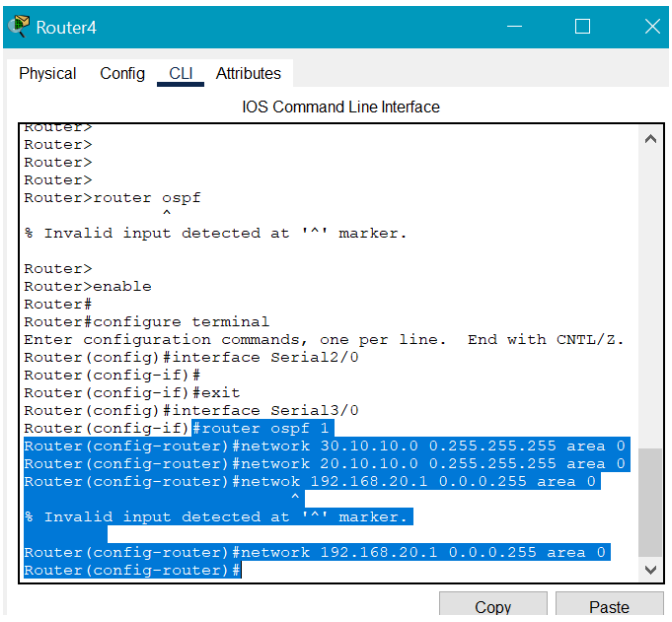


- Configuration of router4:

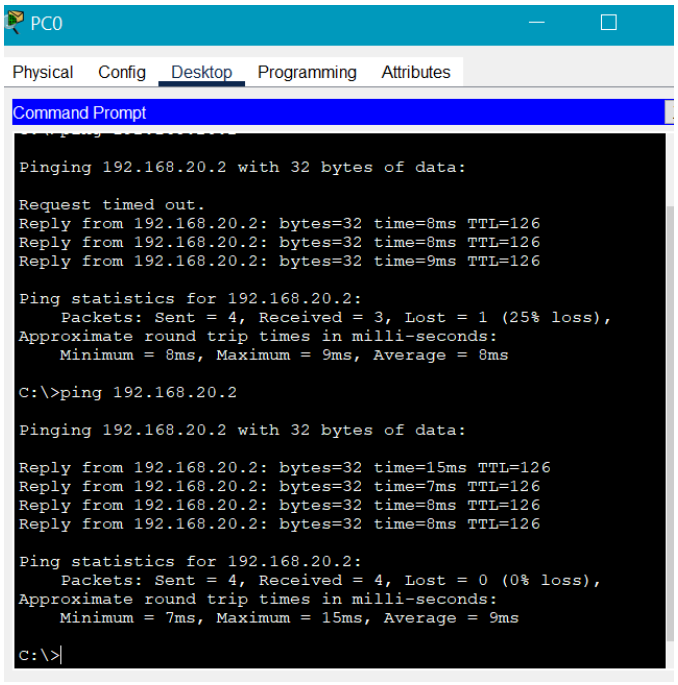








- To check whether pc0 ping pc1 or not:



Conclusion: In this way, we can configure the Open Shortest Path First (OSPF) of routers.

Lab-12

Overview of IP, ICMP, TCP, UDP using wireshark

Objective:

- We can easily know about wireshark.
- Can easily understand on IP, ICMP, TCP, UDP on wireshark.

Background:

IP: IP for Internet Protocol is 32 bit address assigned to network devices (laptop/IP camera/IP phones/Router/Switch/Firewall etc. IP has two parts; Header and Actual data.

Header- Source IP address and Destination IP address.

Actual Data- Payload

ICMP: ICMP stands for Internet Control Message Protocol is used to test reachability to a remote network device. Example; PING is a tool used to check if one network device can reach another network device.

TCP: TCP stands for Transmission Control Protocol is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

TCP is one of the basic standards that define the rules of the internet and is included within the standards defined by the Internet Engineering Task Force (IETF). It is one of the most commonly used protocols within digital network communications and ensures end-to-end data delivery.

UDP: UDP stands for User Datagram Protocol is part of the Internet Protocol suite used by programs running on different computers on a network. UDP is used to send short messages called datagrams but overall, it is an unreliable, connectionless protocol. UDP is officially defined in RFC 768 and was formulated by David P. Reed.

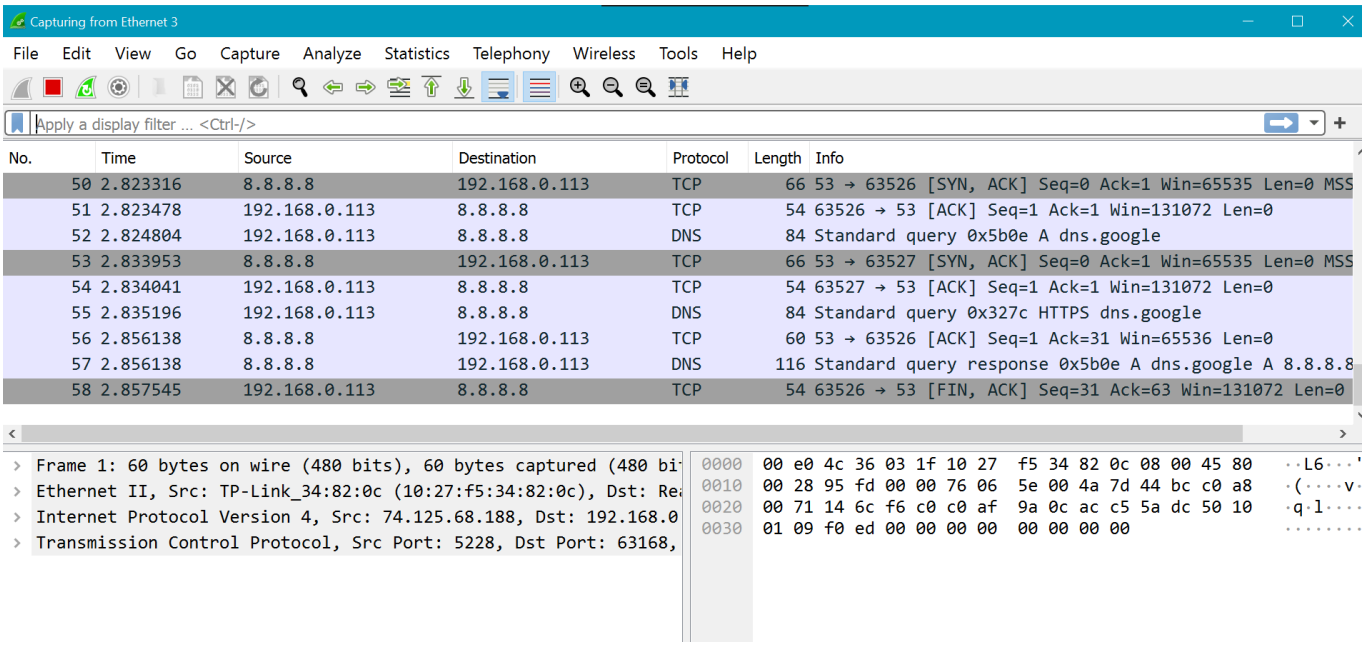
Wireshark: Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.



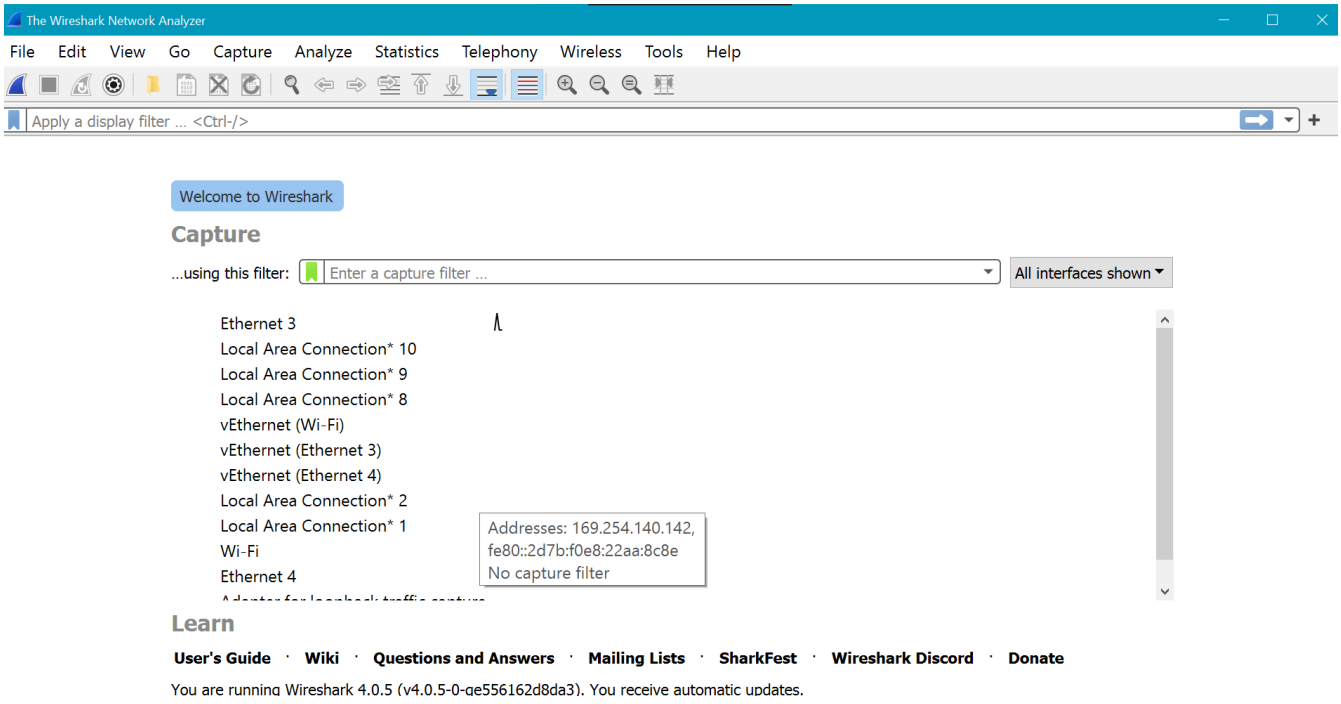
Qn. How to Capture Packets Using Wireshark?

We can start grabbing network traffic. But remember: To capture any packets, we need to have proper permissions on our computer to put Wireshark into promiscuous mode.

->In a Windows system, this usually means we have administrator access.

->In a Linux system, it usually means that we have root access.

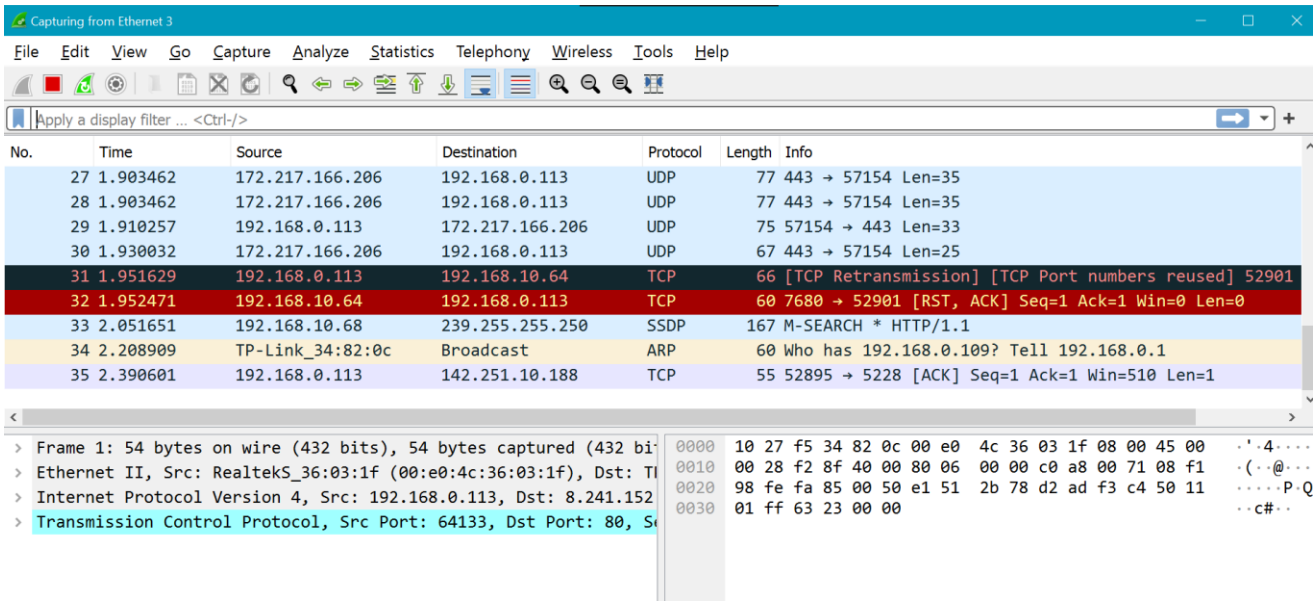
As long as we have the right permissions, we have several options to actually start the capture. Perhaps the best is to select Capture >> Options from the main window. This will bring up the Capture Interfaces window, as shown below in Figure below;



This window will list all available interfaces. In this case, Wireshark provides several to choose from.

For this example, we'll select the Ethernet 3 interface, which is the most active interface. Wireshark visualizes the traffic by showing a moving line, which represents the packets on the network.

Once the network interface is selected, we simply click the Start button to begin our capture. As the capture begins, it's possible to view the packets that appear on the screen, as shown in figure below;



Conclusion: From above procedure, we can easily understand and get information on IP address and many more of source by capturing in wireshark.