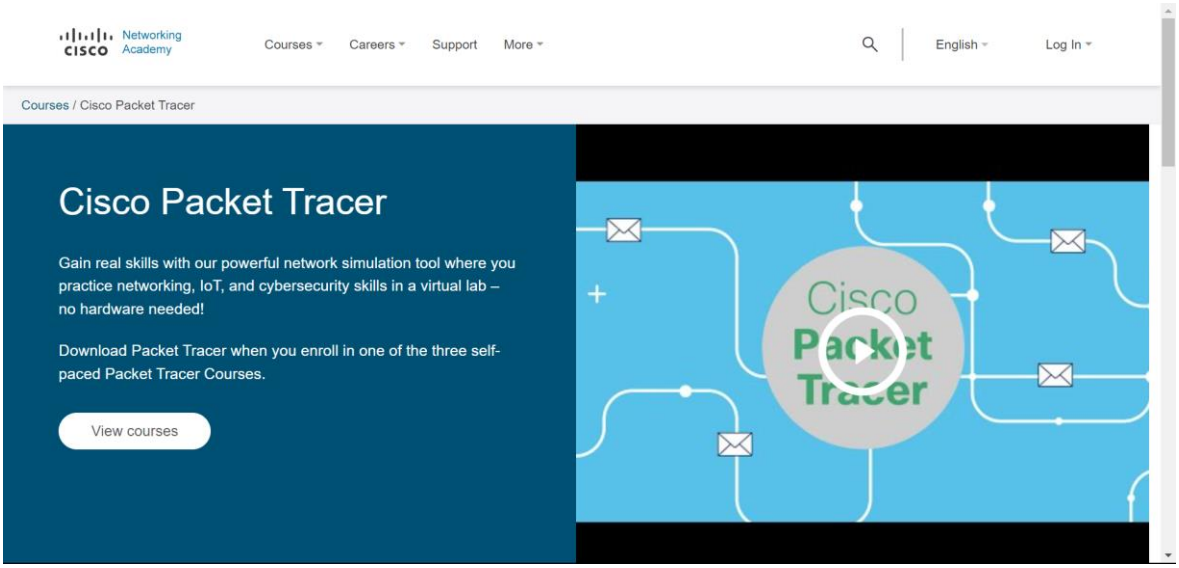
Practical No. 1

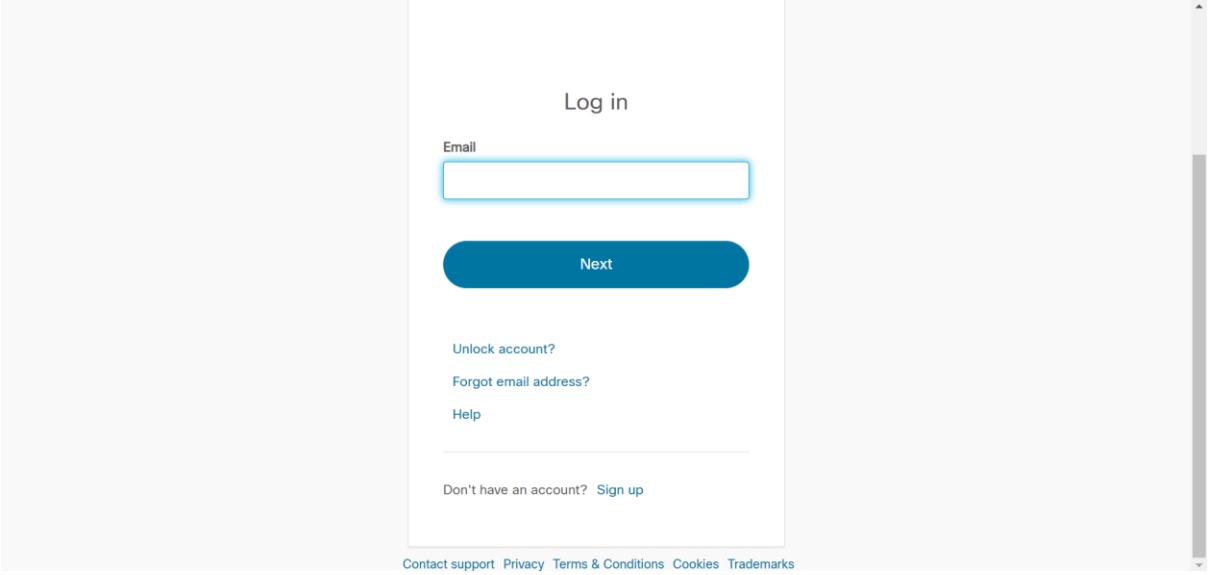
Aim: Installation and Introduction to Cisco Packet Tracer

1.1 Installation of Cisco Packet Tracer

1. Download Cisco Packet Tracer:
   Go to the Cisco Networking Academy website to download Packet Tracer.

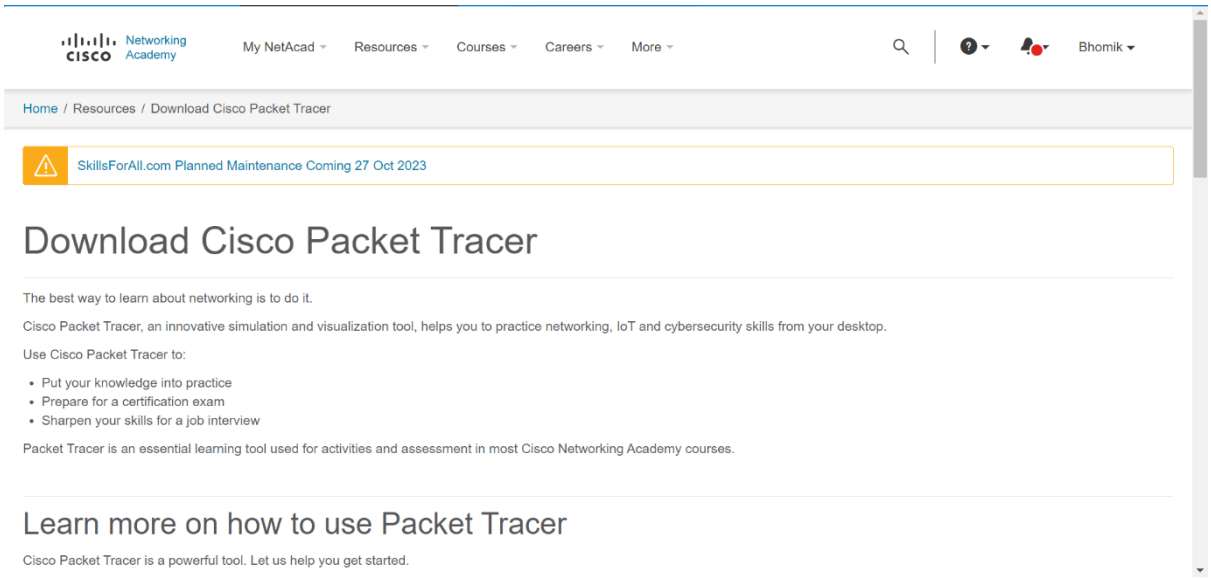


2. Login to Cisco Networking Academy:
   Log in to your Cisco Networking Academy account or create one if you don't have an account.

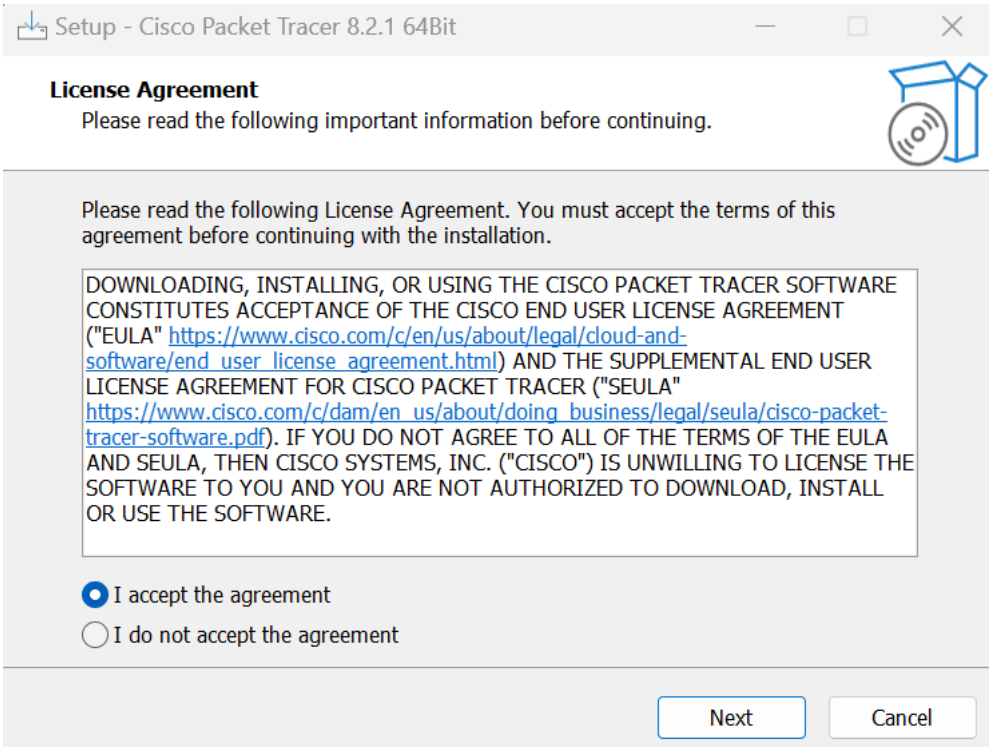


3. Download Packet Tracer:

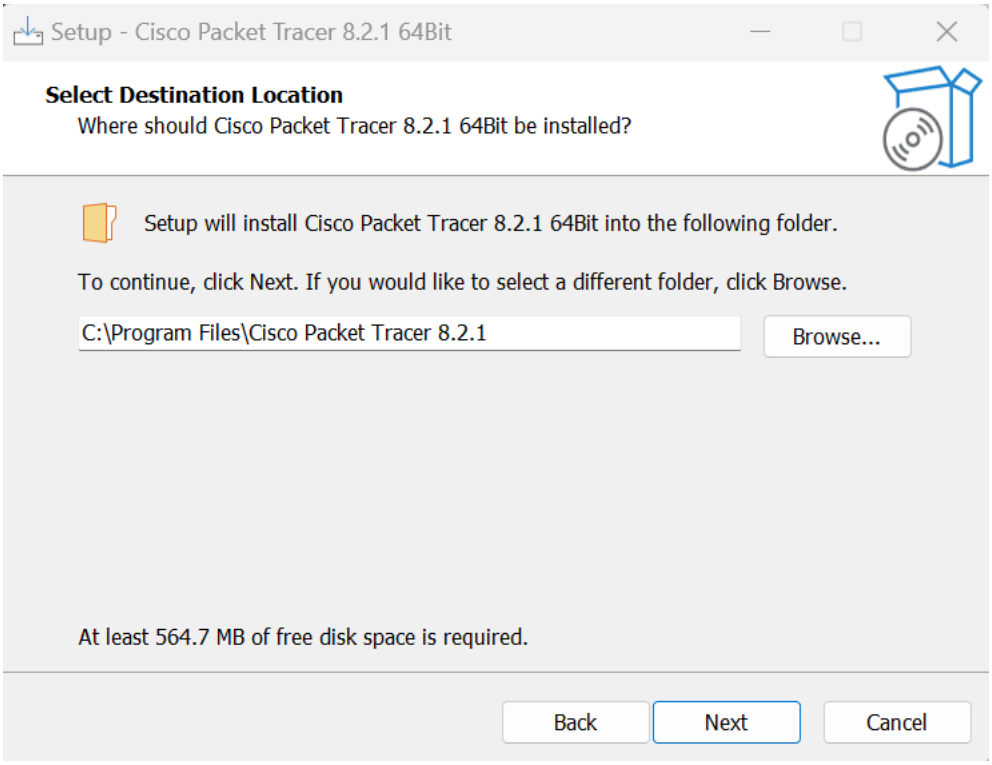
Once logged in, navigate to the Packet Tracer download page. Select the version of Packet Tracer you want to download. After selecting your version, click the download button to start downloading the Packet Tracer installer for Windows.



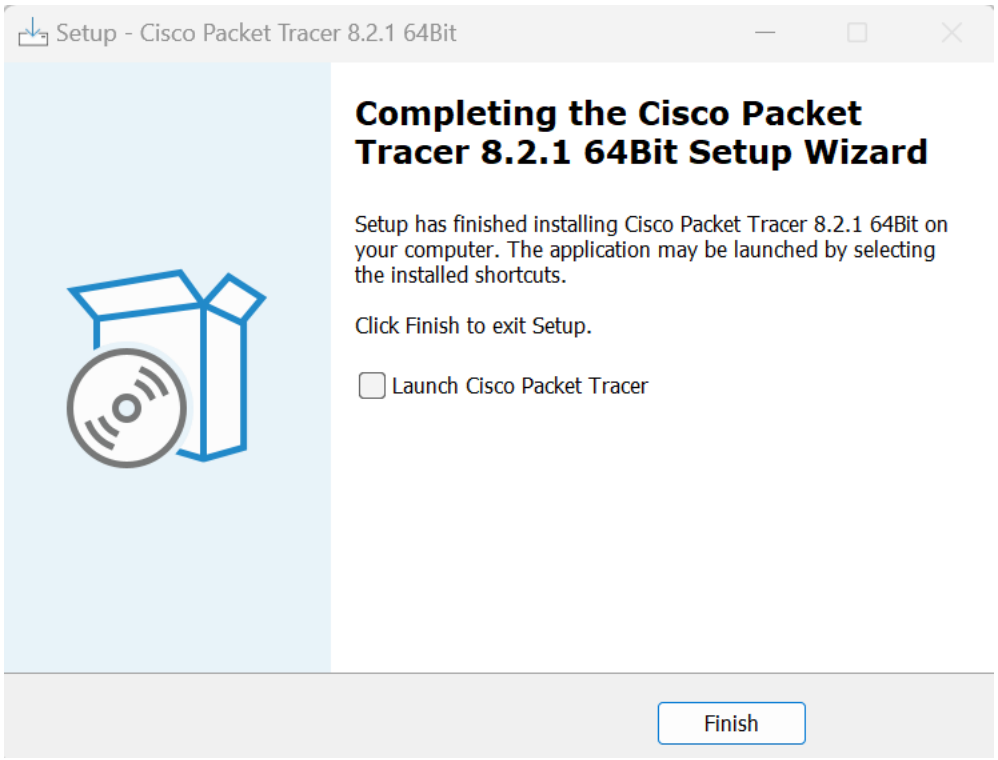
4. Install Packet Tracer:
Once the download is complete, locate the installer file (.exe file) and double-click on it to begin the installation process.



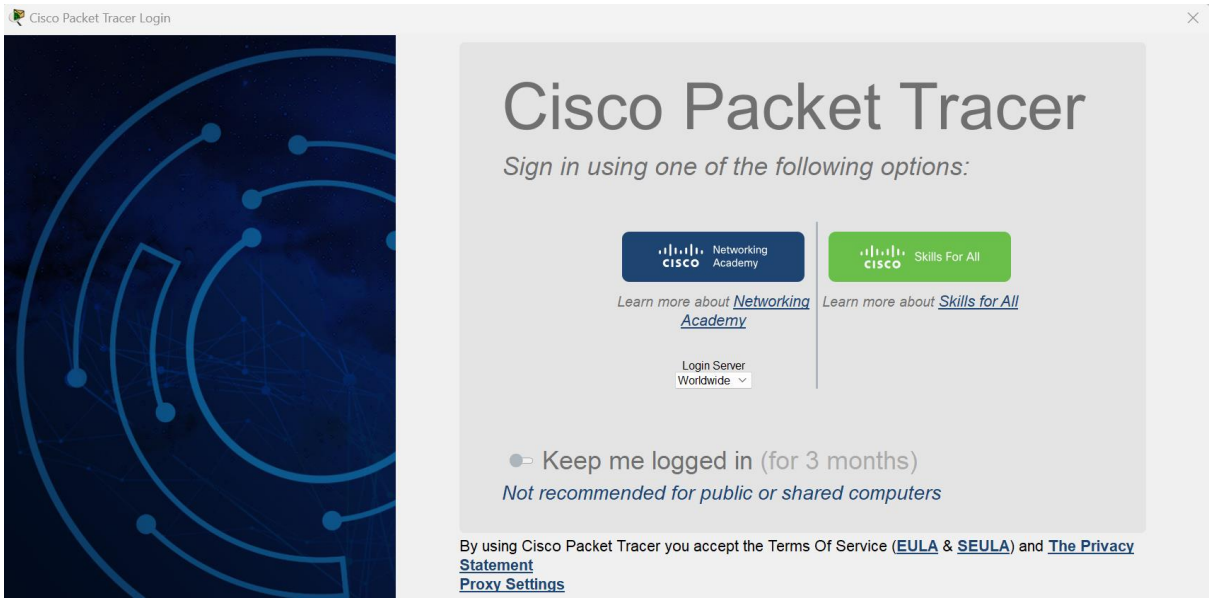
5. Follow Installation Wizard:
The installation wizard will guide you through the installation process. Follow the on-screen instructions, and make sure to select the installation location and other preferences as needed.



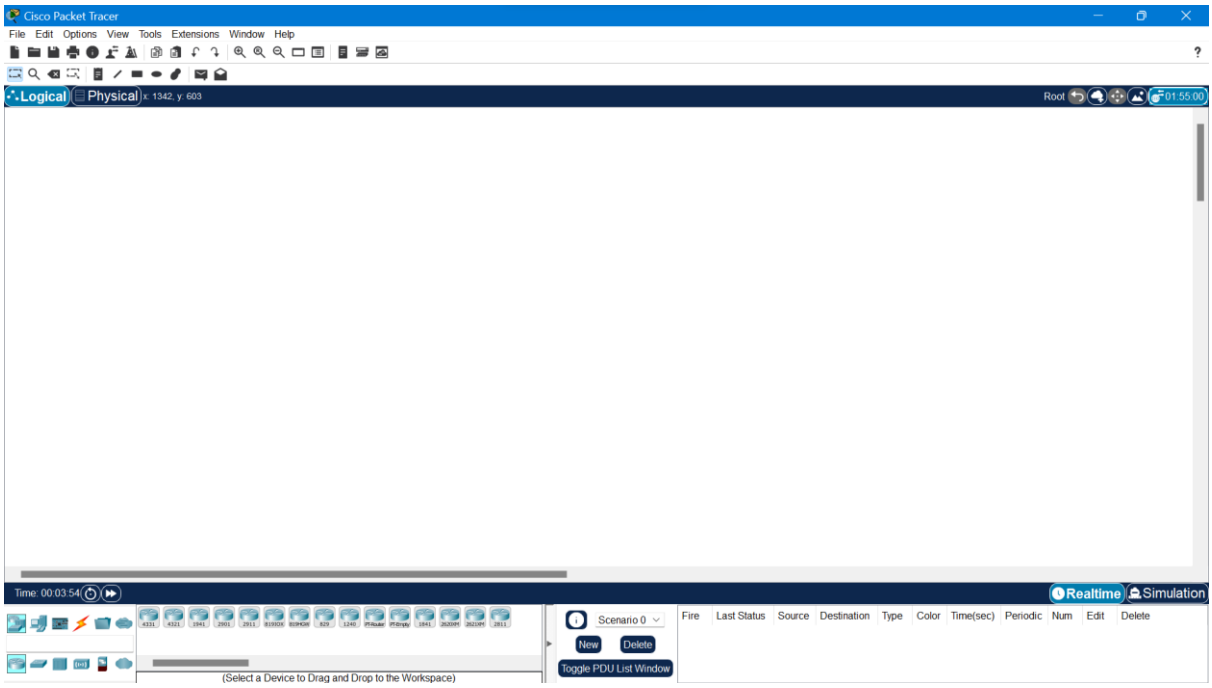
6. Complete Installation:
   After the installation is complete, you will likely see a shortcut icon for Packet Tracer on your desktop. You can launch Packet Tracer by double-clicking this icon.



7. Log In:
   When you launch Packet Tracer, you may be prompted to log in using your Cisco Networking Academy credentials. Log in to access all the features of Packet Tracer.



8. Start Using Cisco Packet Tracer:
   Once logged in, you can start using Cisco Packet Tracer to create and simulate network topologies, experiment with networking concepts, and complete various networking labs and activities.



1.2 Introduction to Cisco Packet Tracer

Introduction

Cisco Packet Tracer is Cisco's simulation software. It can be used to create complicated network typologies, as well as to test and simulate abstract networking concepts. It acts as a playground for you to explore networking and the experience is very close to what you see in computer networks.

Uses

This is primarily intended to train candidates for the CCNA certification, which professionals widely utilise. It is mostly used by Networking Curious & Aficionados, CCNA, CCNA Security and CCNP Students along with Engineers, Educators, & Trainers. Before implementing any protocol, engineers like to test it on Cisco Packet Tracer. In addition, engineers who want to deploy any modification in the production network prefer to utilise Cisco Packet Tracer to test the changes first and then deploy if everything works as planned.

Features of Cisco Packet Tracer

1. Cisco Packet Tracer supports a multi-user system that allows many users to connect various topologies across a computer network. Instructors can also build exercises for students to perform using Packet Tracer.
2. Supports feature expansion via additional programmes that use an API to improve Cisco Packet Tracer's capabilities in areas including curriculum and assessment delivery, gaming, accessibility, and interacting with real-world equipment.
3. The Enhanced Physical Mode transports you to a virtual lab where you can simulate cabling devices on a rack. Refresh key skills such as device placement (Rack & Stack), on-device power switching, device port-to-port cabling (including cable selection and management), troubleshooting, and more.
4. It can be downloaded for free through a Netacad account.
5. It enables its users to simulate the configuration relating to the Cisco routers and can be accessed anywhere anytime.
6. The Network Controller allows you a centralised dashboard to see the network's state, instantly discover and diagnose issues, and push configuration changes to all managed devices at once, whether you use its Web GUI or its APIs. You may also use real-world programmes on your computer to access the Network Controller and run your own infrastructure automation scripts.
7. It can be accessed through unlimited devices.
8. Provides an interactive and self-paced environment.

Practical No. 2

Aim: Using Cisco Packet Tracer, Connect two PCs using appropriate network wire using Static IP configuration.

Theory

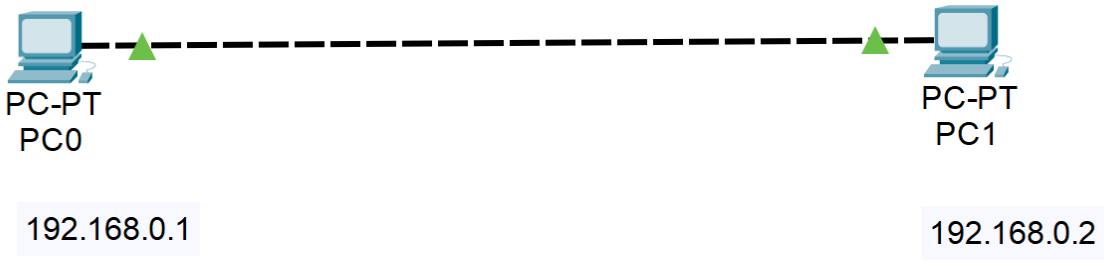
IP Address: An Internet Protocol (IP) address is a unique numerical identifier for every device or network that connects to the internet. Typically assigned by an internet service provider (ISP), an IP address is an online device address used for communicating across the internet.

Static configuration: In a static IP configuration, an onboard network device is assigned an IP address that can be accessed directly from the Internet. It does not receive an IP address from the ICM. Important! You should only assign a static IP address to a secure device, such as a firewall router.

Straight through cable: Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency.

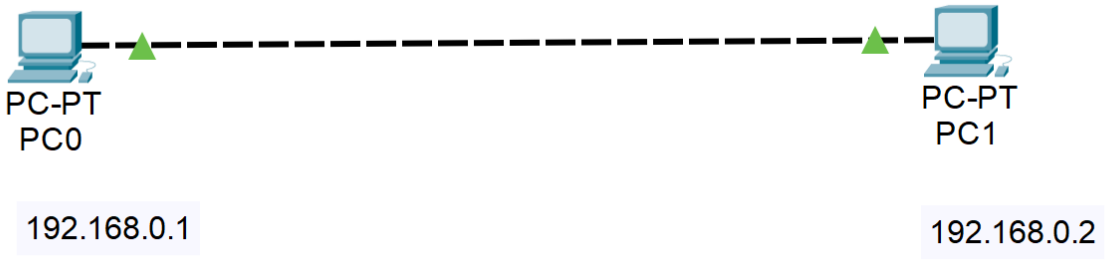
Crossover cable: Crossover cable is used to connect two or more computing devices. The internal wiring of crossover cables reverses the transmission and receive signals. It is widely used to connect two devices of the same type.

Topology



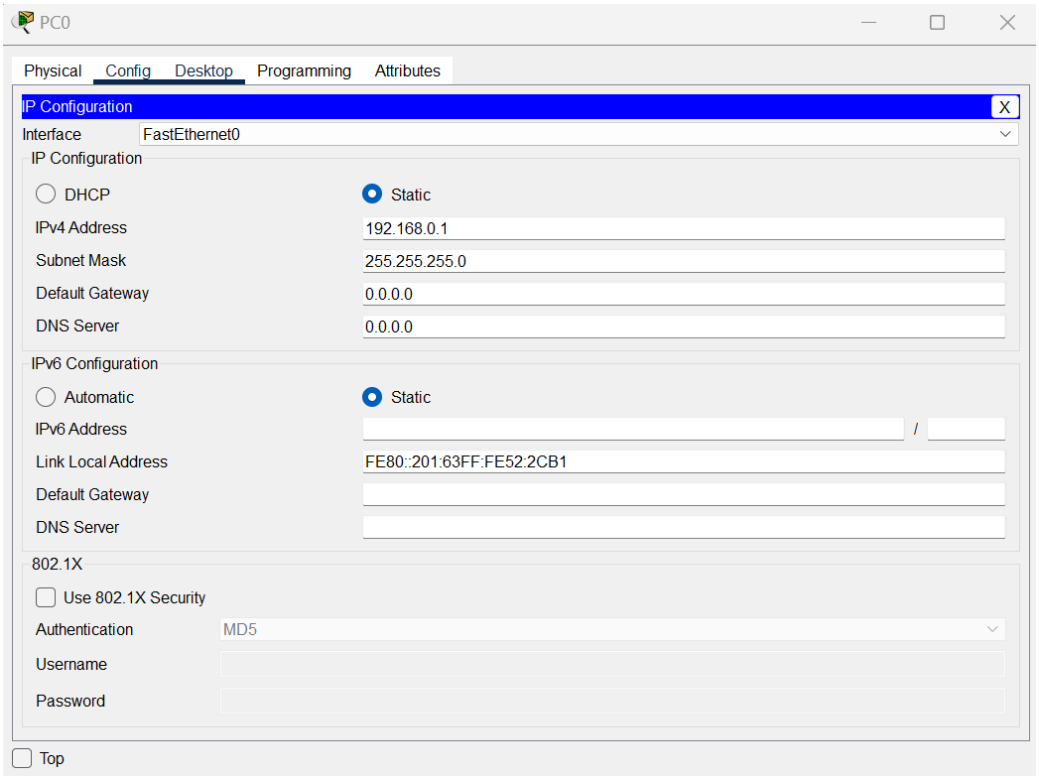
Steps to execute

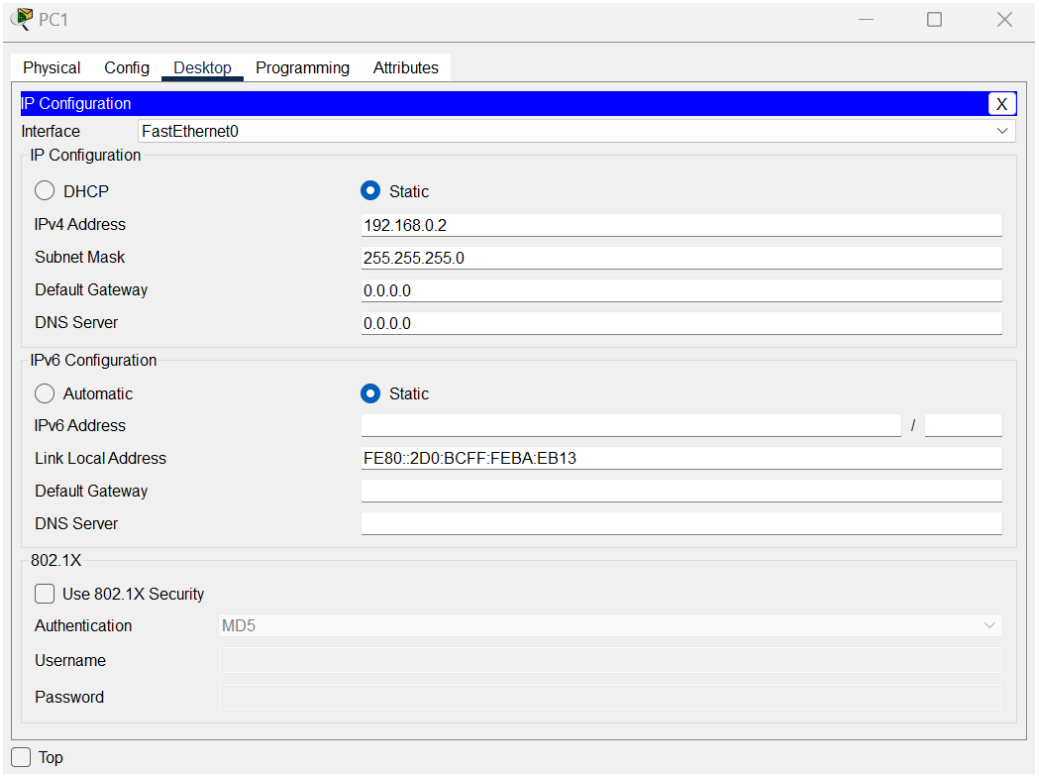
Step 1: Connect two PC's using crossover cable



Step 2: Configure the static IP addresses:

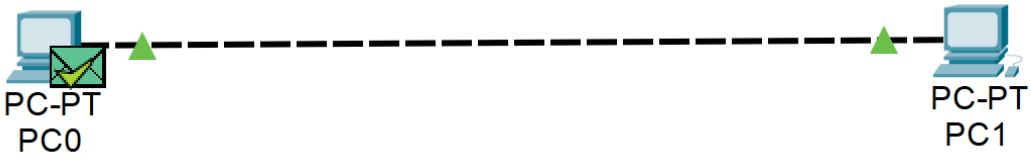
- PC0
  IPv4 Address: 192.168.0.1
- PC1
  IPv4 Address: 192.168.0.2





Step 3: Click on add simple PDU and make PC0 as source and PC1 as destination.

Step 4: Click on simulation tab to see the simulation of data.



192.168.0.1

192.168.0.2

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	PC1	ICMP
	0.002	PC1	PC0	ICMP

Reset Simulation | Constant Delay | Captured to: 3872.383 s

Command prompt

PC0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2E0:8FFF:FE8D:A94
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

```
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:5CFF:FEDD:16AE
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Practical No. 3

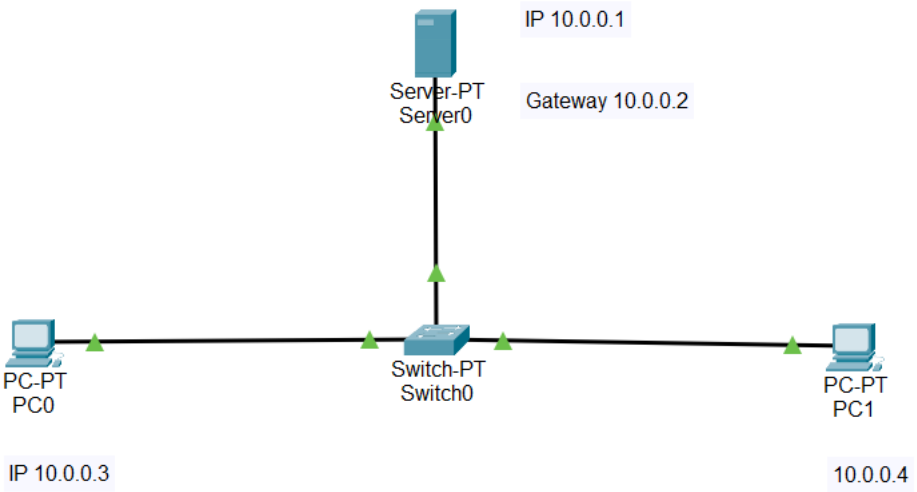
Aim: Using Cisco Packet Tracer, create a basic network of one server and two computers using appropriate network wire. Use Dynamic IP address allocation and show connectivity.

Theory

DHCP

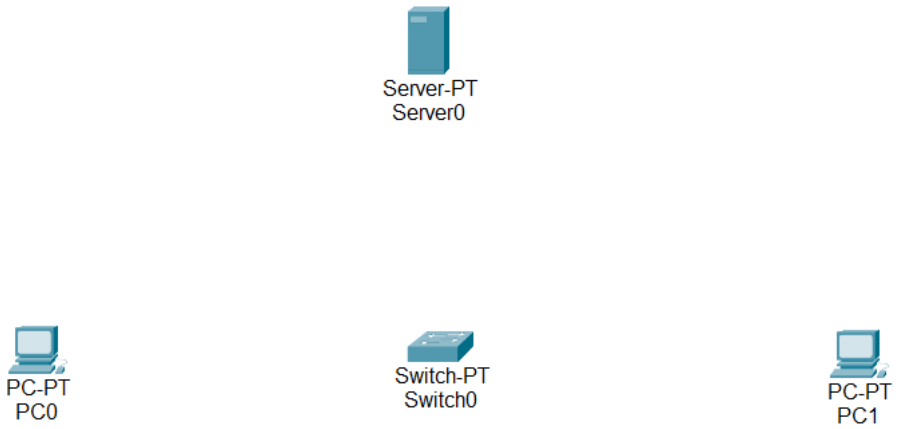
DHCP stands for Dynamic Host Configuration Protocol. It is a network protocol used to automatically assign and manage IP (Internet Protocol) addresses, as well as other network configuration parameters, to devices in a TCP/IP network. DHCP simplifies the process of IP address assignment and configuration, making it more efficient and less error-prone compared to manual configuration.

Topology

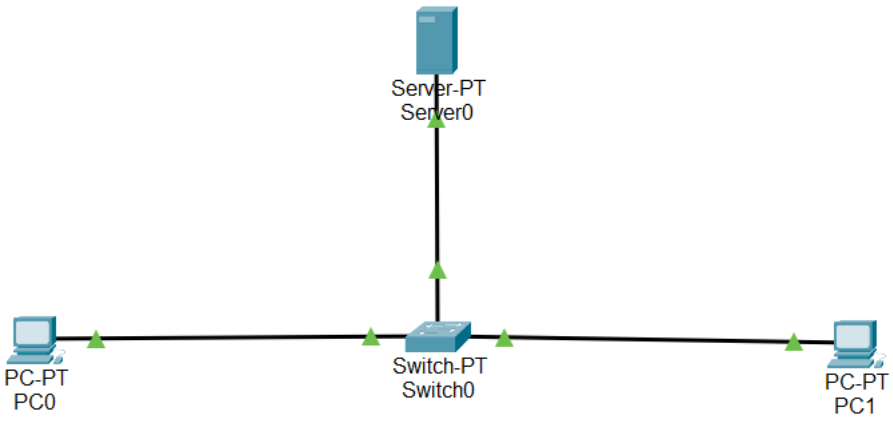


Steps to execute

Step 1: Drag and drop one server, two PCs and a switch into the workspace.

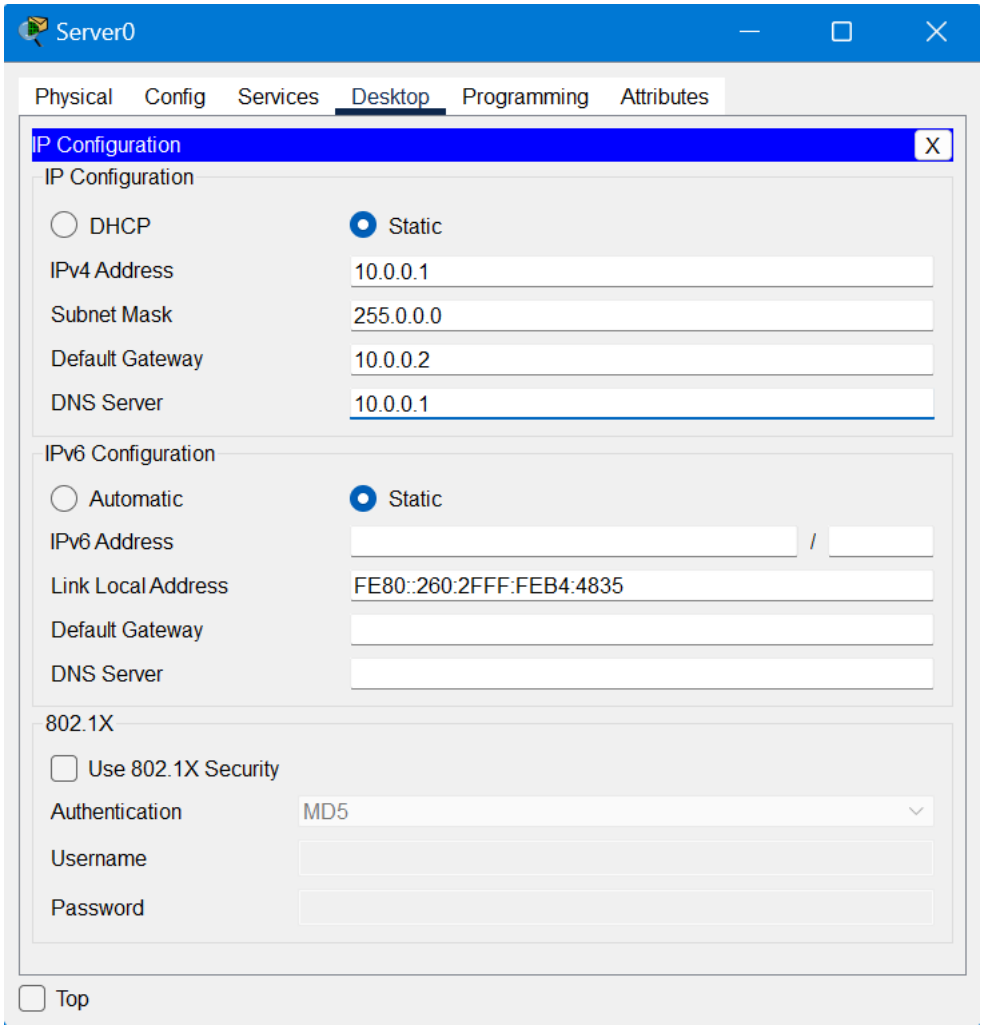


Step 2: Connect the server and PCs via switch using straight through cable.

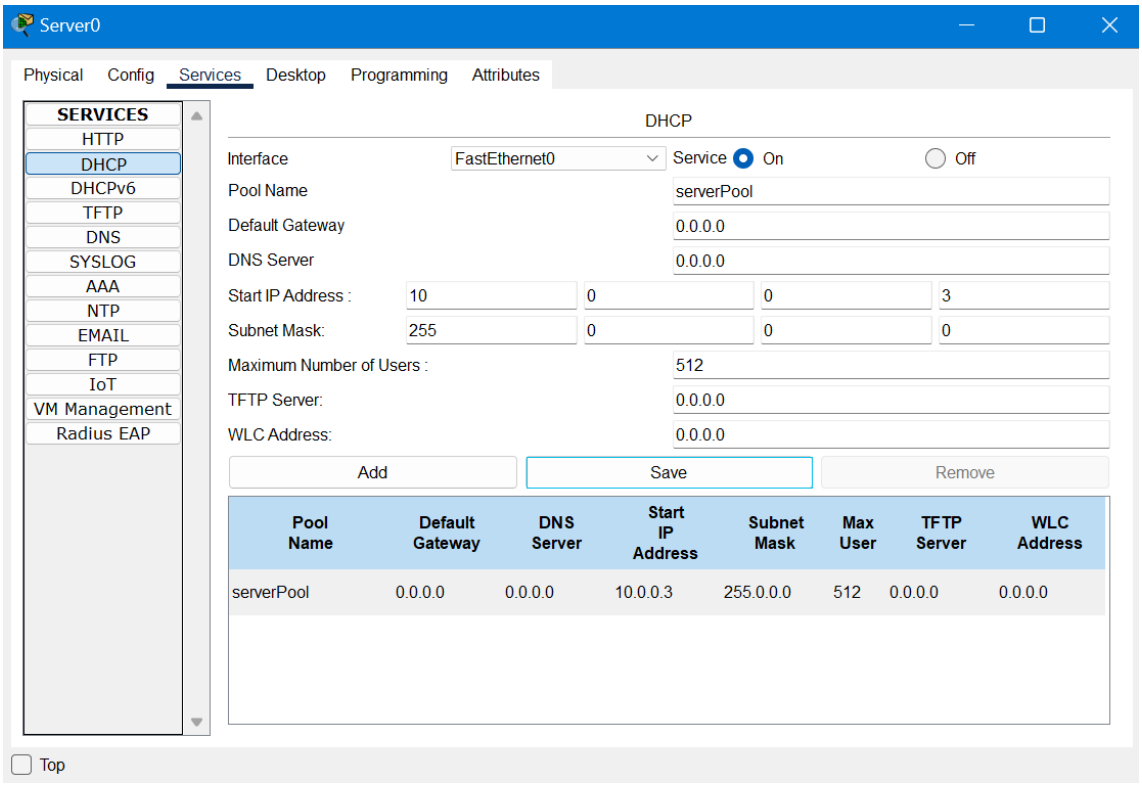


Step 3: Configure the server:

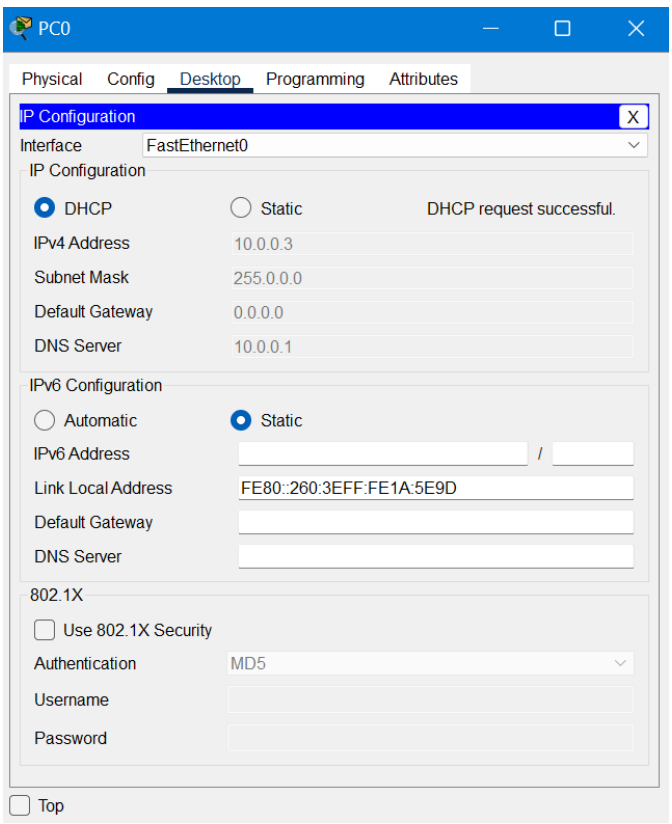
- IPv4 Address: 10.0.0.1
- Default Gateway: 10.0.0.2
- DNS Server: 10.0.0.1

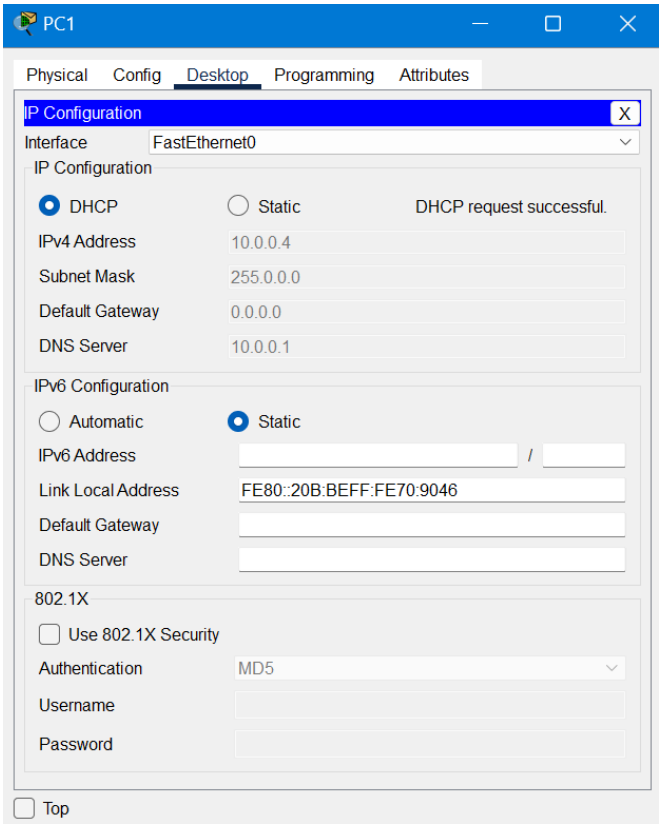


Step 4: Go to the services section and switch ON the DHCP service. Set the start IP address as 10.0.0.3.

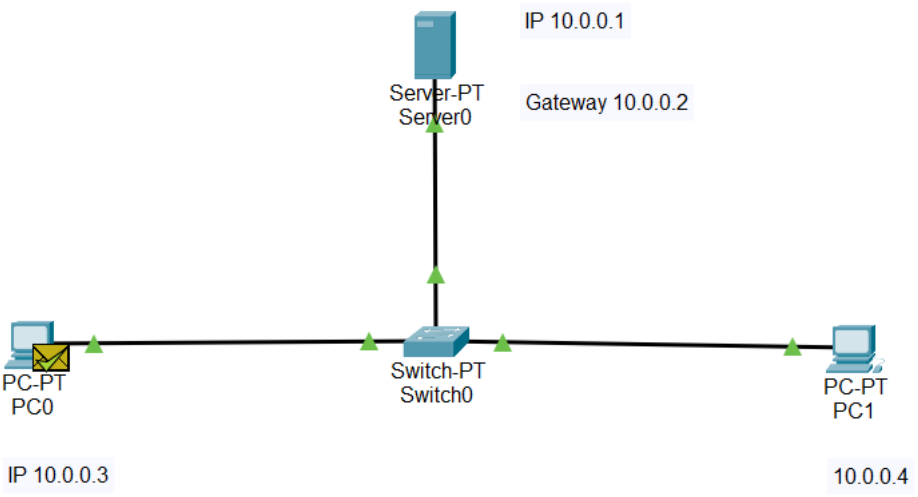


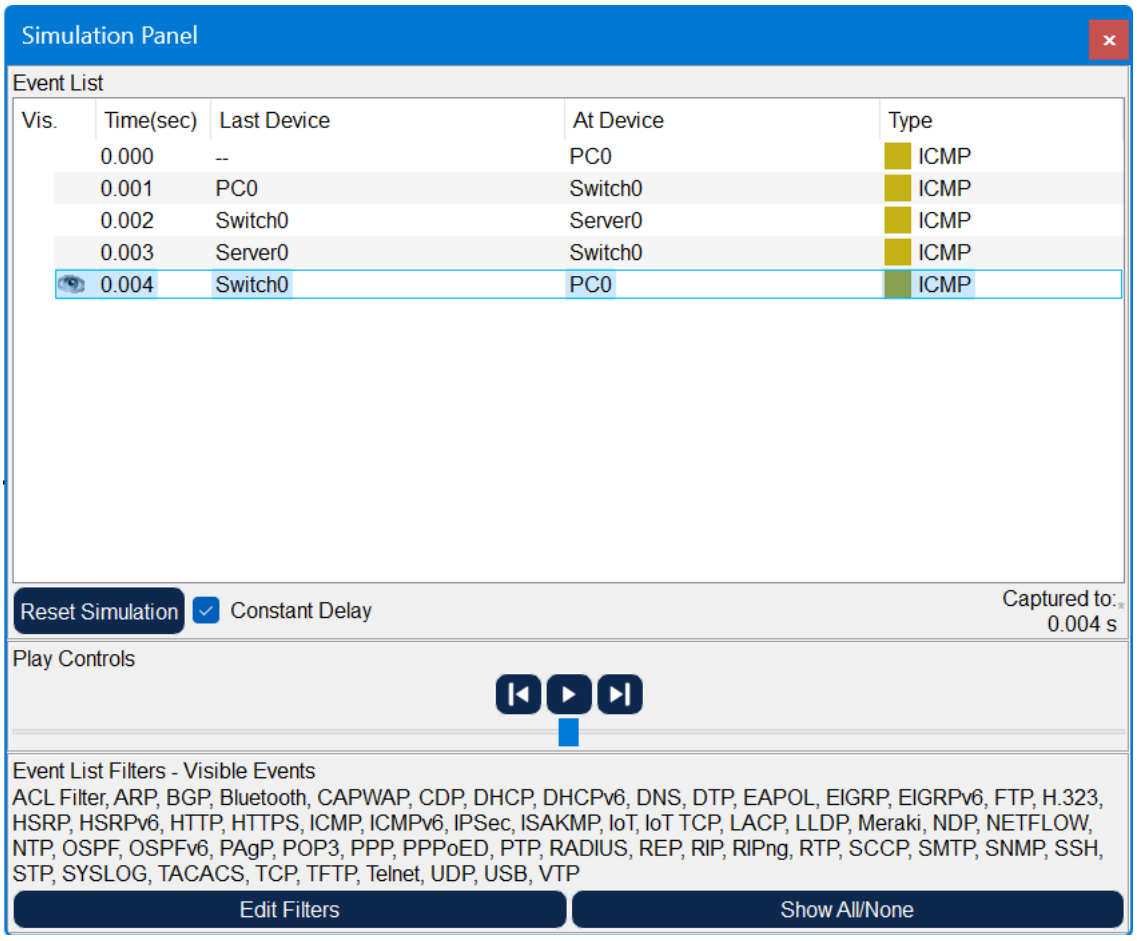
Step 5: Set IP configuration of PC0 and PC1 as DHCP.



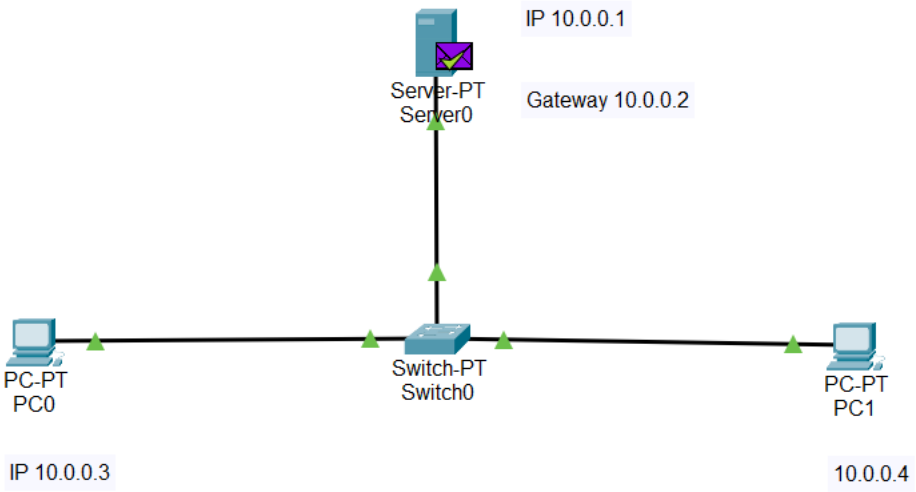


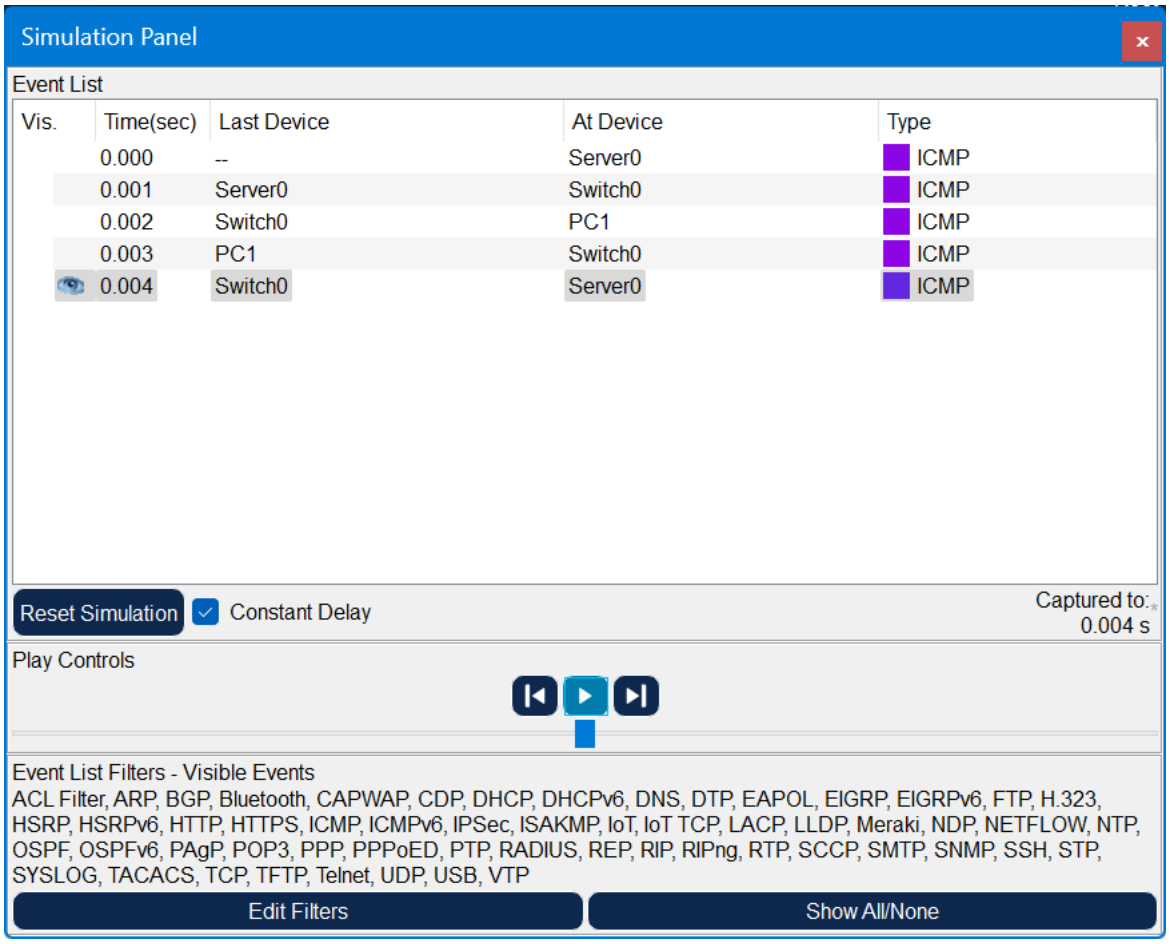
Step 6: Click on add simple PDU and make PC0 as source and server as destination. Then click on simulation tab to see the simulation of data.





Step 7: Click on add simple PDU and make server as source and PC1 as destination. Then click on simulation tab to see the simulation of data.





Command prompt

Server

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:2FFF:FEB4:4835
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.0.1
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: ::
                                 10.0.0.2

C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PC0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:3EFF:FE1A:5E9D
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.0.3
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=9ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

PC1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20B:BEFF:FE70:9046
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.0.4
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time=1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Practical No. 4

Aim: Using Cisco Packet Tracer, create a basic network of one server and two computers and two mobile/ movable devices using appropriate network cable. And verify the connectivity.

Theory

Wireless Network: A wireless network refers to a computer network that makes use of Radio Frequency (RF) connections between nodes in the network. Wireless networks are a popular solution for homes, businesses, and telecommunications networks.

Types of Wireless network connections:

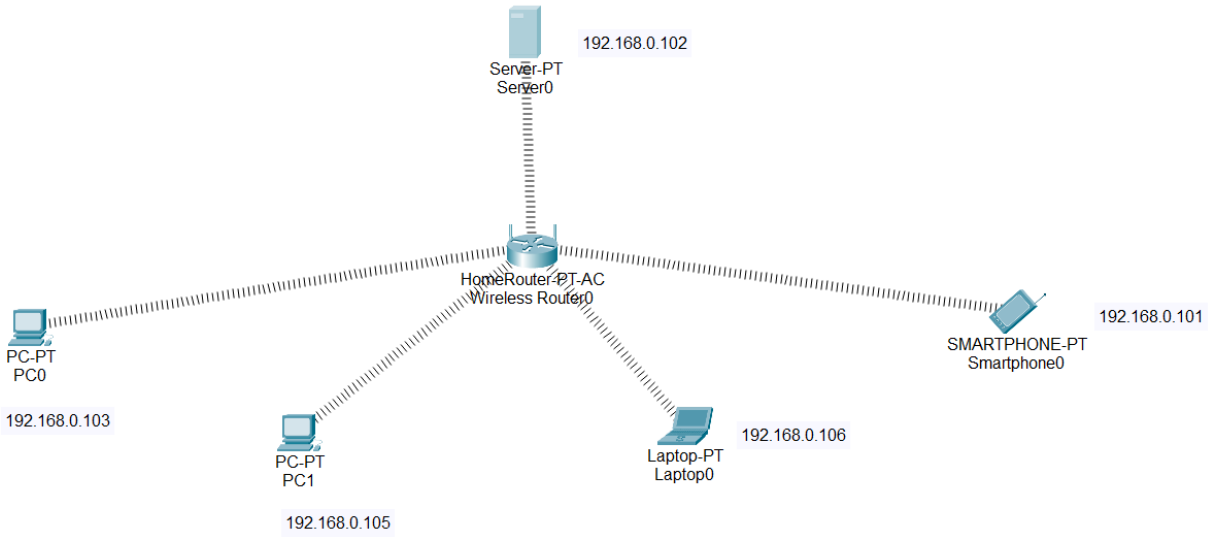
- **LAN:** A local-area network is a computer network that exists at a single site. It can be used to connect a variety of components, such as computers, printers, and data storage devices. Wi-Fi is the most known wireless LAN.
- **PAN:** A personal-area network consists of a network centralized around the devices of a single person in a single location. They are common inside homes and small office most buildings. Bluetooth is the known wireless PAN.
- **MAN:** A metropolitan-area network is a computer network that spans across a city, small geographical area, or business or college campus. A MAN can cover several square miles, depending on the needs of the organization.
- **WAN:** A wide-area network covers a very large area, like an entire city, state, or country. In fact, the internet is a WAN.

WAP (Wireless Application Protocol)

Wireless Application Protocol (WAP) is a specification for a set of communication protocols to standardize the way wireless devices, such as mobile phones and radio transceivers, can be used for internet access, including email, the web, newsgroups, and instant messaging. Benefits of WAP are as follows:

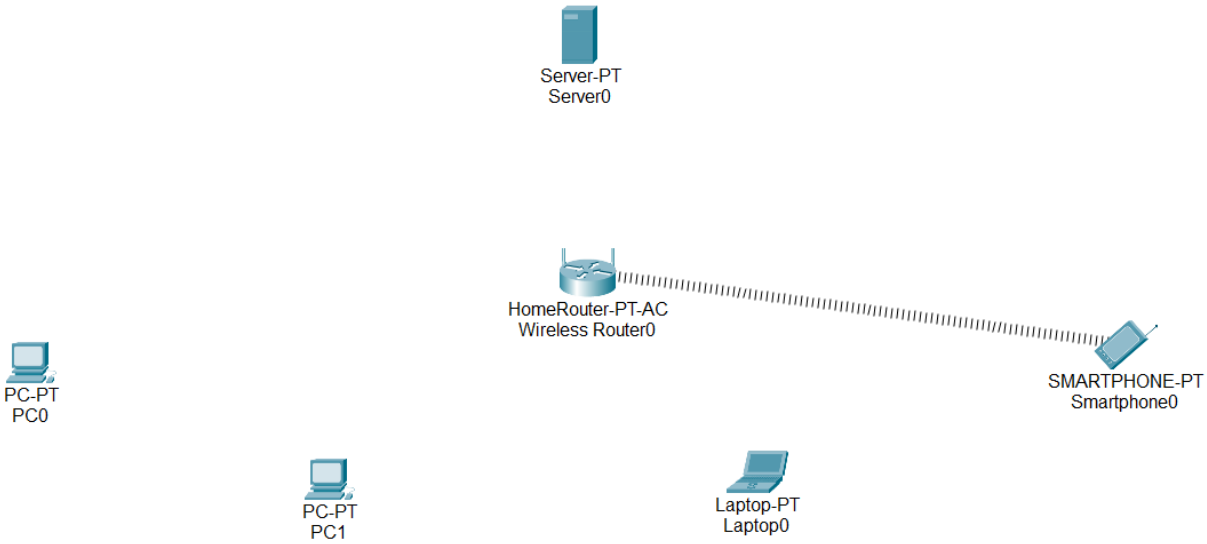
- **Wireless network and mobile phone operators**: WAP was designed to improve existing wireless data services, such as voicemail, while enabling the development of additional new mobile applications.
- **Content providers**: WAP created a market for additional applications and mobile phone functionalities for third-party application developers to exploit.
- **End users**: Mobile phone users would benefit from easy, secure access to online services, such as banking, entertainment, messaging, and other information, on mobile devices.

Topology

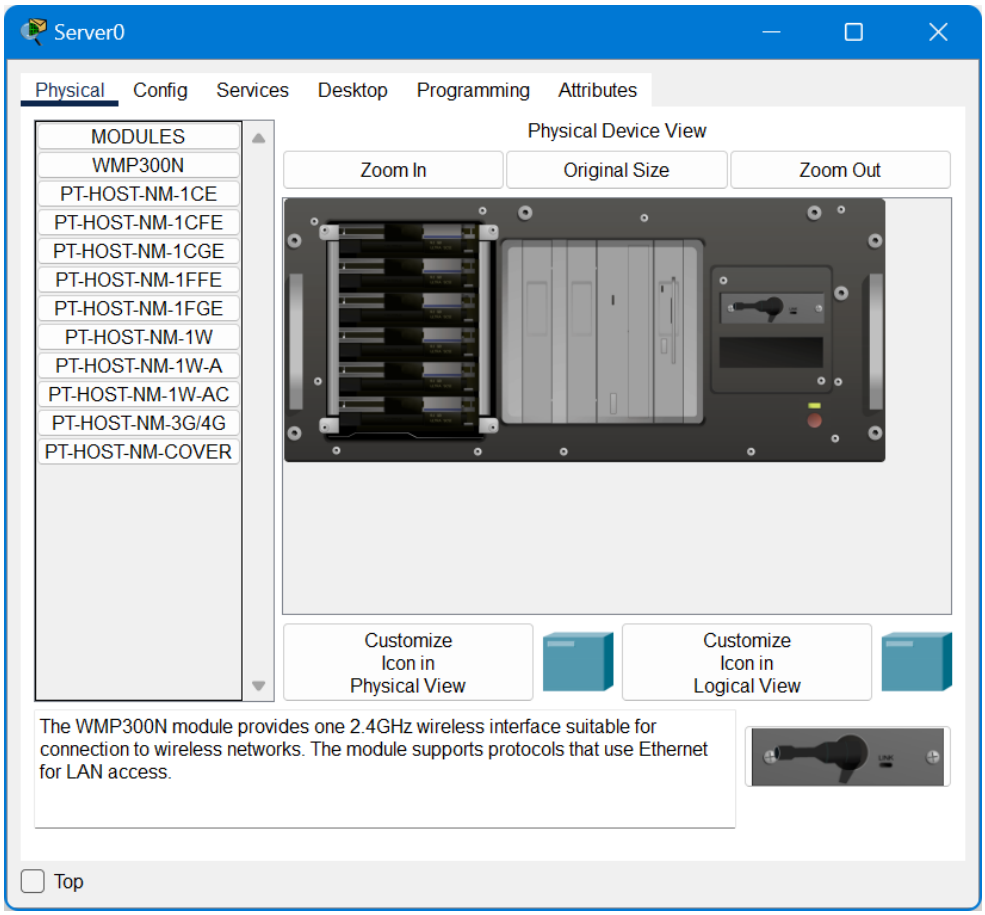


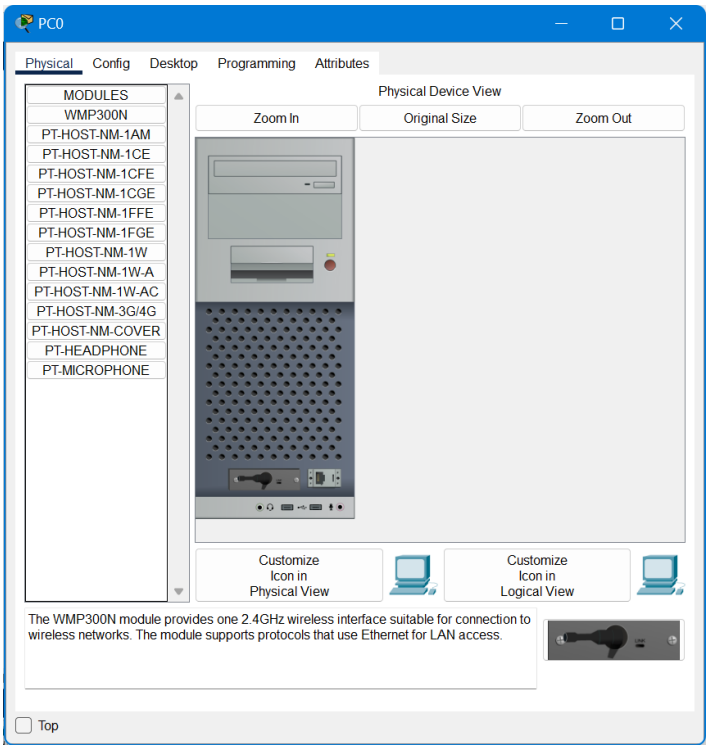
Steps to execute

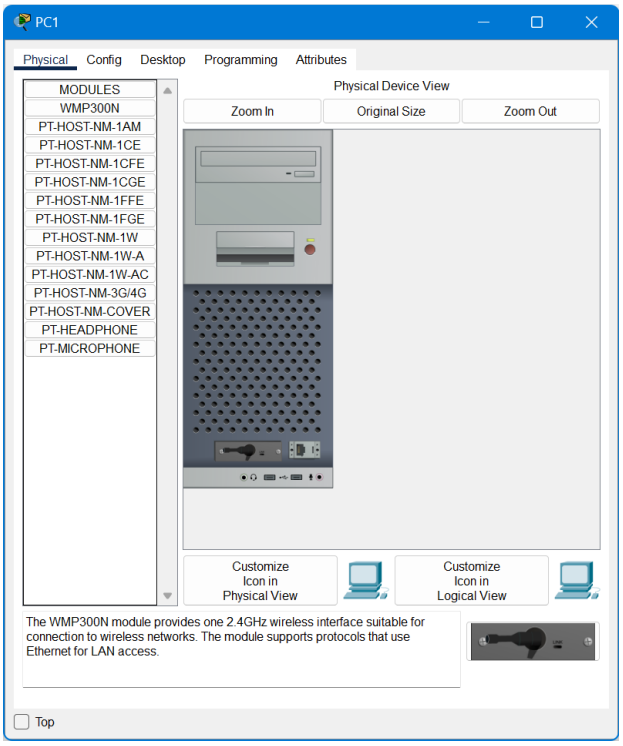
Step 1: Drag the elements required in the workplace.

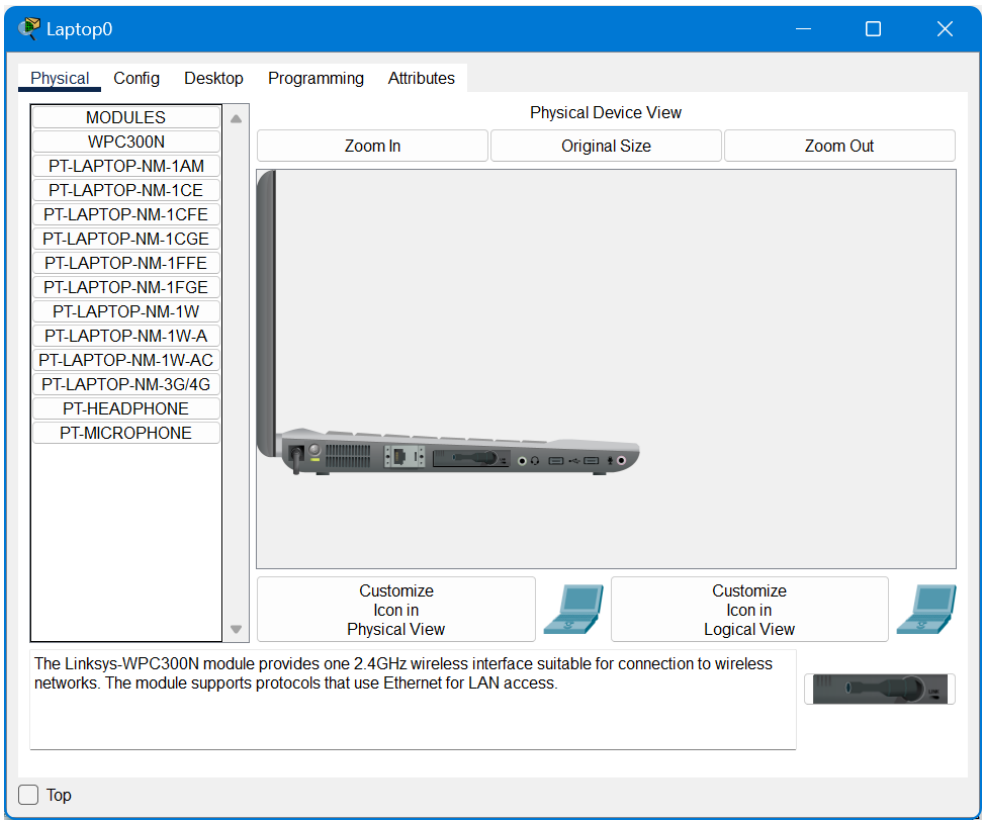


Step 2: When we drag the Smartphone, it automatically connects to the Wireless Router but we have to change the connection port in PCs, laptop and server.
Step 3: First Switch OFF the device then change the port. In case of PCs and server replace the port with WMP300N. In case of laptop replace the port with WPC300N

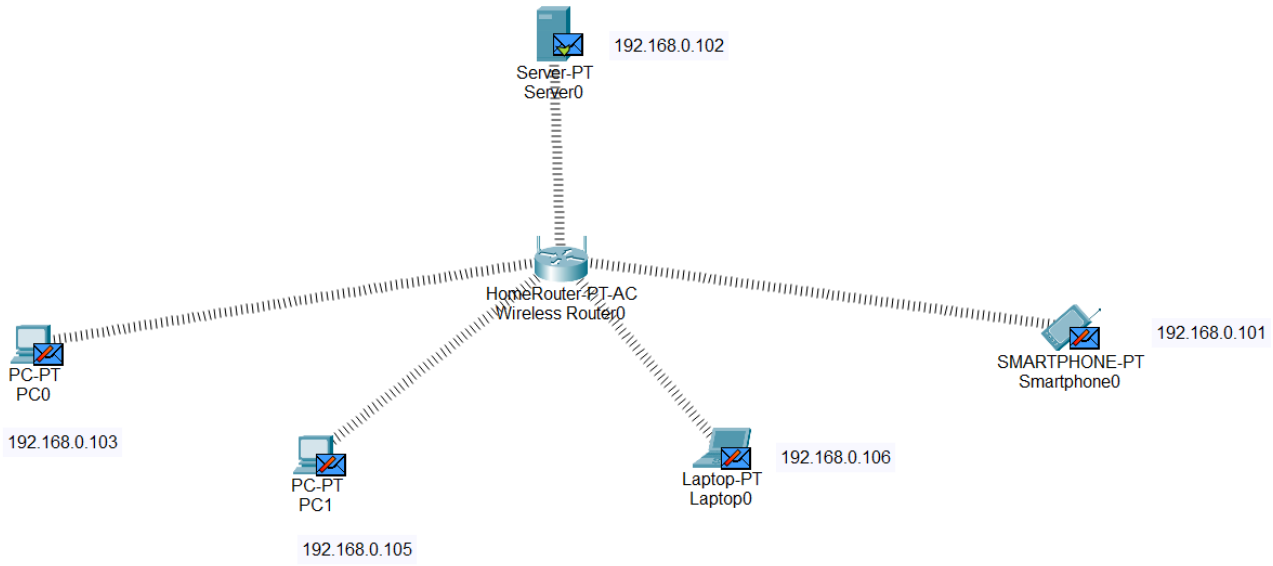








Step 4: Click on add simple PDU and make server as source and PC0 as destination. Then click on simulation tab to see the simulation of data.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Server0	ICMP
	0.001	Server0	Wireless Router0	ICMP
	0.005	--	Wireless Router0	ICMP
	0.006	Wireless Router0	PC0	ICMP
	0.006	Wireless Router0	Server0	ICMP
	0.006	Wireless Router0	Smartphone0	ICMP
	0.006	Wireless Router0	PC1	ICMP
	0.006	Wireless Router0	Laptop0	ICMP
	0.008	--	PC0	ICMP
	0.009	PC0	Wireless Router0	ICMP
	0.010	--	Wireless Router0	ICMP
	0.011	Wireless Router0	PC0	ICMP
	0.011	Wireless Router0	Server0	ICMP
	0.011	Wireless Router0	Smartphone0	ICMP
	0.011	Wireless Router0	PC1	ICMP
	0.011	Wireless Router0	Laptop0	ICMP

Reset Simulation | Constant Delay | Captured to: 0.011 s

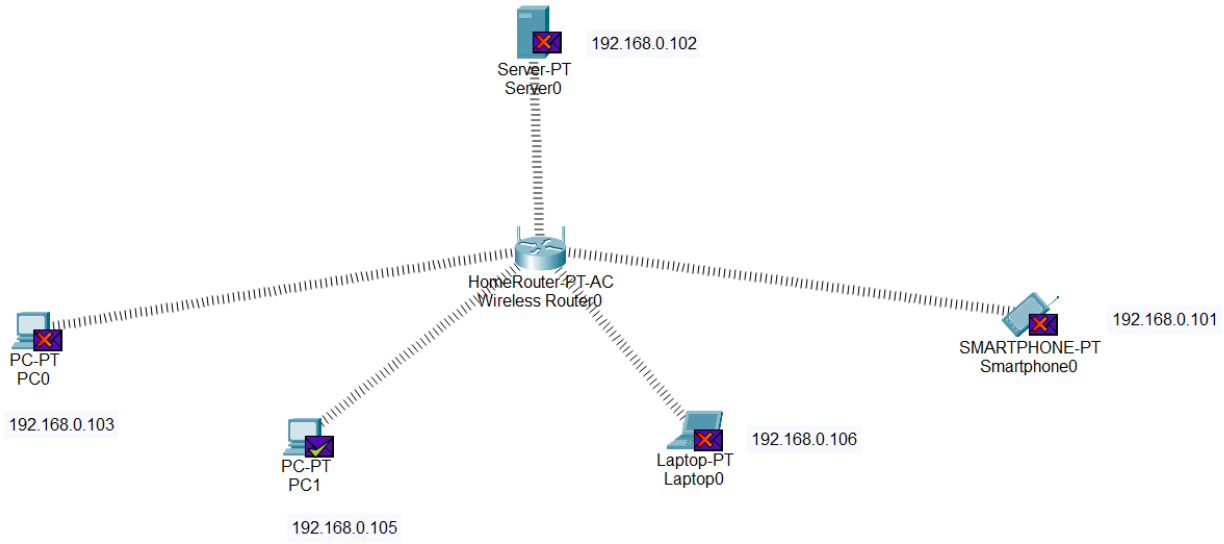
Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Step 5: Click on add simple PDU and make PC1 as source and smartphone as destination. Then click on simulation tab to see the simulation of data.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Wireless Router0	ICMP
	0.002	--	Wireless Router0	ICMP
	0.003	Wireless Router0	PC0	ICMP
	0.003	Wireless Router0	Server0	ICMP
	0.003	Wireless Router0	Smartphone0	ICMP
	0.003	Wireless Router0	PC1	ICMP
	0.003	Wireless Router0	Laptop0	ICMP
	0.007	--	Smartphone0	ICMP
	0.008	Smartphone0	Wireless Router0	ICMP
	0.013	--	Wireless Router0	ICMP
	0.014	Wireless Router0	PC0	ICMP
	0.014	Wireless Router0	Server0	ICMP
	0.014	Wireless Router0	Smartphone0	ICMP
	0.014	Wireless Router0	PC1	ICMP
	0.014	Wireless Router0	Laptop0	ICMP

Reset Simulation | Constant Delay | Captured to: 0.014 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Command prompt

Server

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>
ipconfig

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::250:FFF:FE2A:180
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.102
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

C:\>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:

Reply from 192.168.0.103: bytes=32 time=27ms TTL=128
Reply from 192.168.0.103: bytes=32 time=23ms TTL=128
Reply from 192.168.0.103: bytes=32 time=23ms TTL=128
Reply from 192.168.0.103: bytes=32 time=27ms TTL=128

Ping statistics for 192.168.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 27ms, Average = 25ms

C:\>
```

PC0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ipconfig

Bluetooth Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

Wireless0 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::250:FFF:FE2A:4A44
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.103
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

C:\>ping 192.168.0.102

Pinging 192.168.0.102 with 32 bytes of data:

Reply from 192.168.0.102: bytes=32 time=21ms TTL=128
Reply from 192.168.0.102: bytes=32 time=21ms TTL=128
Reply from 192.168.0.102: bytes=32 time=22ms TTL=128
Reply from 192.168.0.102: bytes=32 time=25ms TTL=128

Ping statistics for 192.168.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 25ms, Average = 22ms

C:\>
```

PC1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>

ipconfig

Bluetooth Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

Wireless0 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:43FF:FE3C:C34A
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.105
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

C:\>ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time=14ms TTL=128
Reply from 192.168.0.101: bytes=32 time=27ms TTL=128
Reply from 192.168.0.101: bytes=32 time=21ms TTL=128
Reply from 192.168.0.101: bytes=32 time=26ms TTL=128

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 27ms, Average = 22ms

C:\>
```

Laptop

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ipconfig

Bluetooth Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

Wireless0 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2E0:F9FF:FE5E:9533
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.106
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

C:\>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:

Reply from 192.168.0.103: bytes=32 time=41ms TTL=128
Reply from 192.168.0.103: bytes=32 time=21ms TTL=128
Reply from 192.168.0.103: bytes=32 time=21ms TTL=128
Reply from 192.168.0.103: bytes=32 time=21ms TTL=128

Ping statistics for 192.168.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 41ms, Average = 26ms

C:\>
```

Smartphone

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::250:FFF:FEED:770C
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.101
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

3G/4G Cell1 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::230:A3FF:FE38:810
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:
 --More--
   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.0.105

Pinging 192.168.0.105 with 32 bytes of data:

Reply from 192.168.0.105: bytes=32 time=22ms TTL=128
Reply from 192.168.0.105: bytes=32 time=28ms TTL=128
Reply from 192.168.0.105: bytes=32 time=22ms TTL=128
Reply from 192.168.0.105: bytes=32 time=18ms TTL=128

Ping statistics for 192.168.0.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 28ms, Average = 22ms

C:\>
```

Practical No. 5

Aim: To understand the operation of TELNET by accessing the router in a server room from a PC in IT Office.

Theory

TELNET: TELNET stands for Teletype Network. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the local computer. The computer which accepts the connection is known as the remote computer. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle. The local computer uses a telnet client program, and the remote computers use a telnet server program.

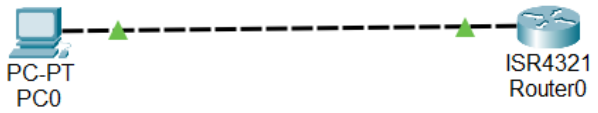
Types of Logging

1. **Local Login**: Whenever a user logs into its local system, it is known as local login.
2. **Remote Login**: Whenever a user logs into a remote computer and use services that are available on the remote computer.

Modes of Router

1. **User execution mode**: As soon as the interface up message appears and press enter, the router> prompt will pop up. This is called user execution mode. This mode is limited to some monitoring commands.
2. **Privileged mode:** As we type enable to user mode, we enter into Privileged mode where we can view and change the configuration of the router.
3. **Global configuration mode:** As we type configure terminal to the user mode, we will enter the global configuration mode. Commands entered in these modes are called global commands and they affect the running configuration of the router. In this mode, a different configuration like making a local database on the router by providing username and password can set enable and secret password, etc.
4. **Interface configuration mode:** In this mode, only the configuration of interfaces is done. Assigning an IP address to an interface, bringing up the interface are the common tasks done in this mode.
5. **ROMmon mode:** We can enter this mode when we interrupt the boot process of the router. It is like the BIOS mode of a PC.

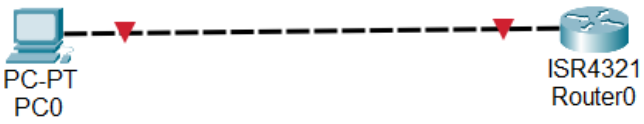
Topology



Steps to execute

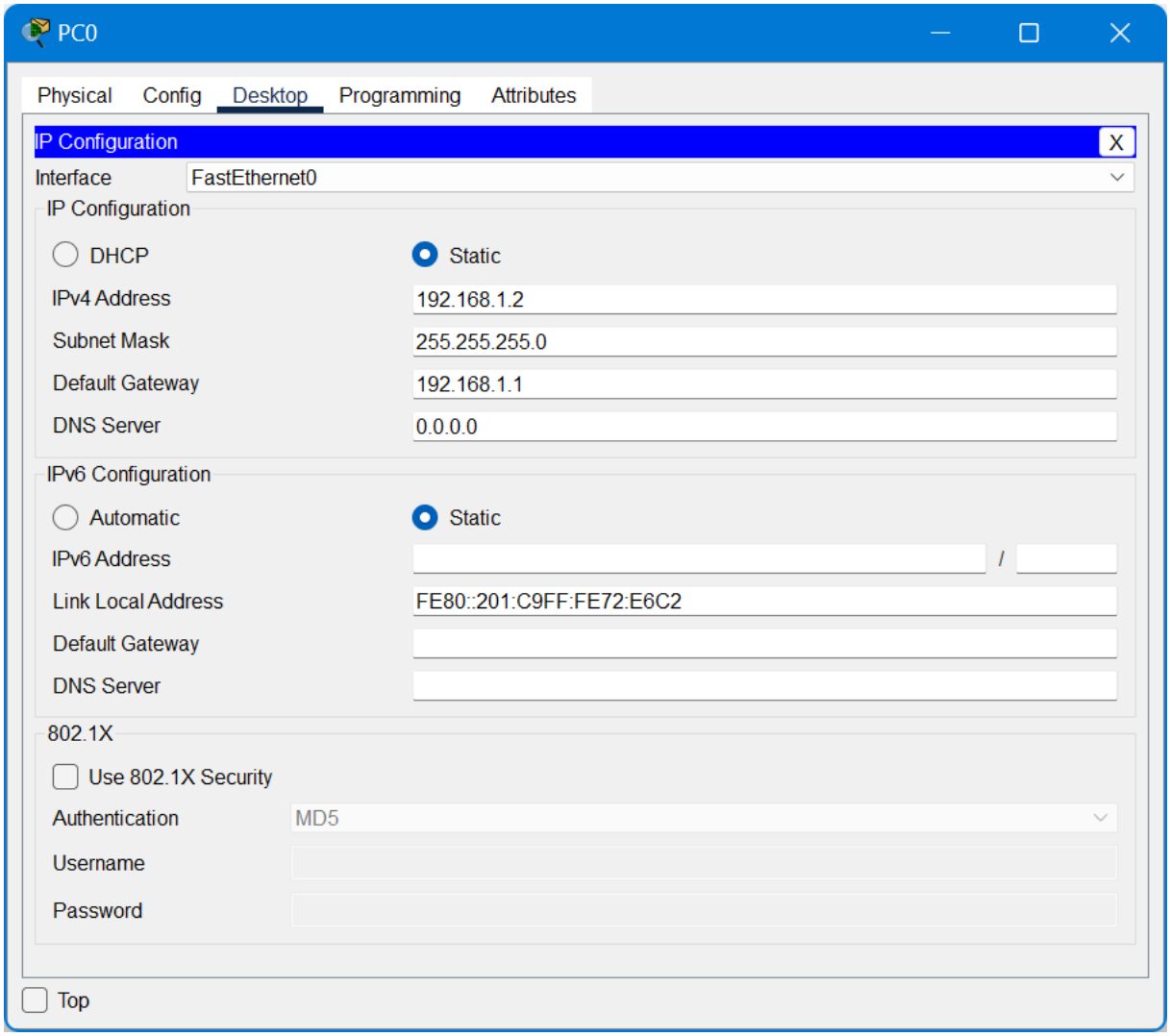
Step 1: Drag the elements required in the workplace.

Step 2: Connect the PC and router using straight through cable.

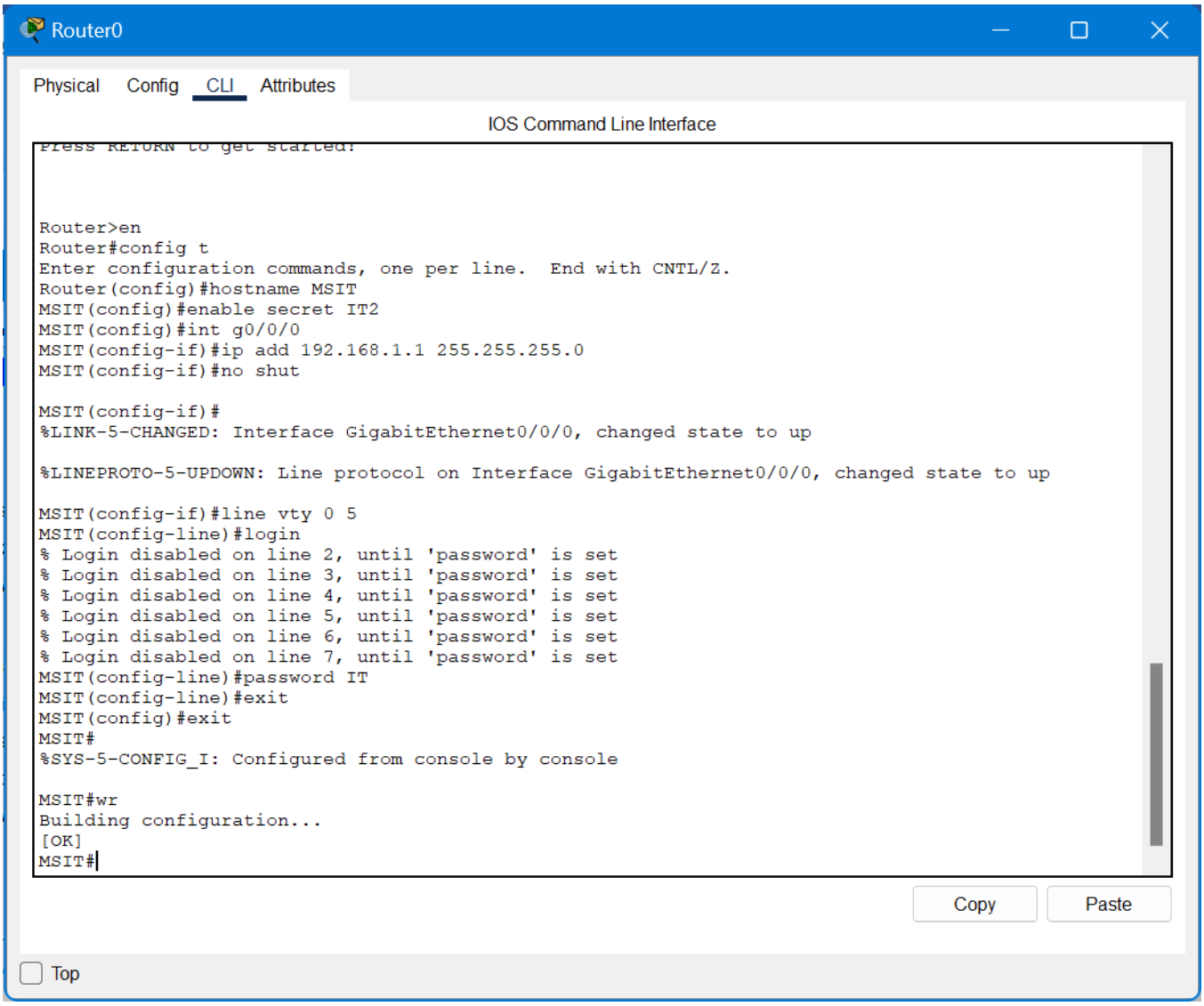


Step 3: Configure PC0:

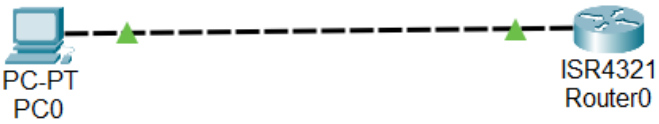
- IPv4 Address: 192.168.1.2
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.1.1



Step 4: Configure the router using CLI.



Step 5: After configuration you can access the router from PC0.



Commands to check connectivity

```
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<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

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 = 0ms, Average = 0ms

C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
MSIT>en
Password:
MSIT#config t
Enter configuration commands, one per line.  End with CNTL/Z.
MSIT(config)#hostname GGSIPU
GGSIPU(config)#exit
GGSIPU#exit

[Connection to 192.168.1.1 closed by foreign host]
C:\>
```

Practical No. 6

Aim: To implement the Static routing using CISCO packet Tracer.

Theory

Static routing: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Uses of Static routing

- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.
- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- Static routing is often used as a complement to dynamic routing to provide a failsafe backup if a dynamic route is unavailable.
- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

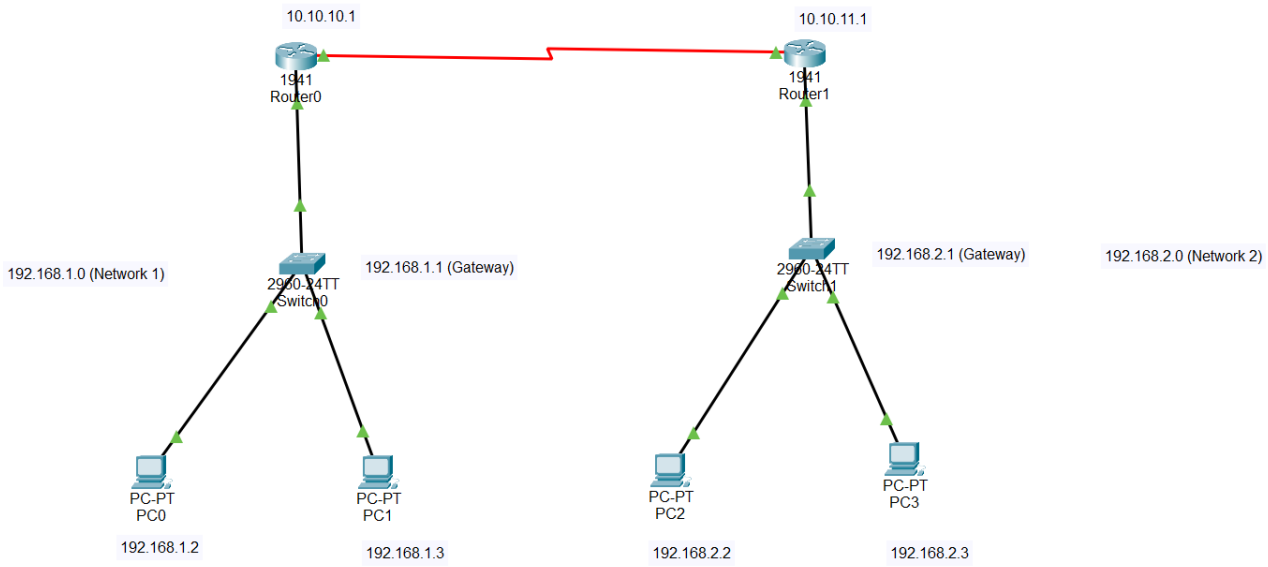
Advantages of static routing: Static routing, if used without dynamic routing, has the following advantages:

- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Static Routing is very easy to configure on small networks.

Disadvantages of static routing

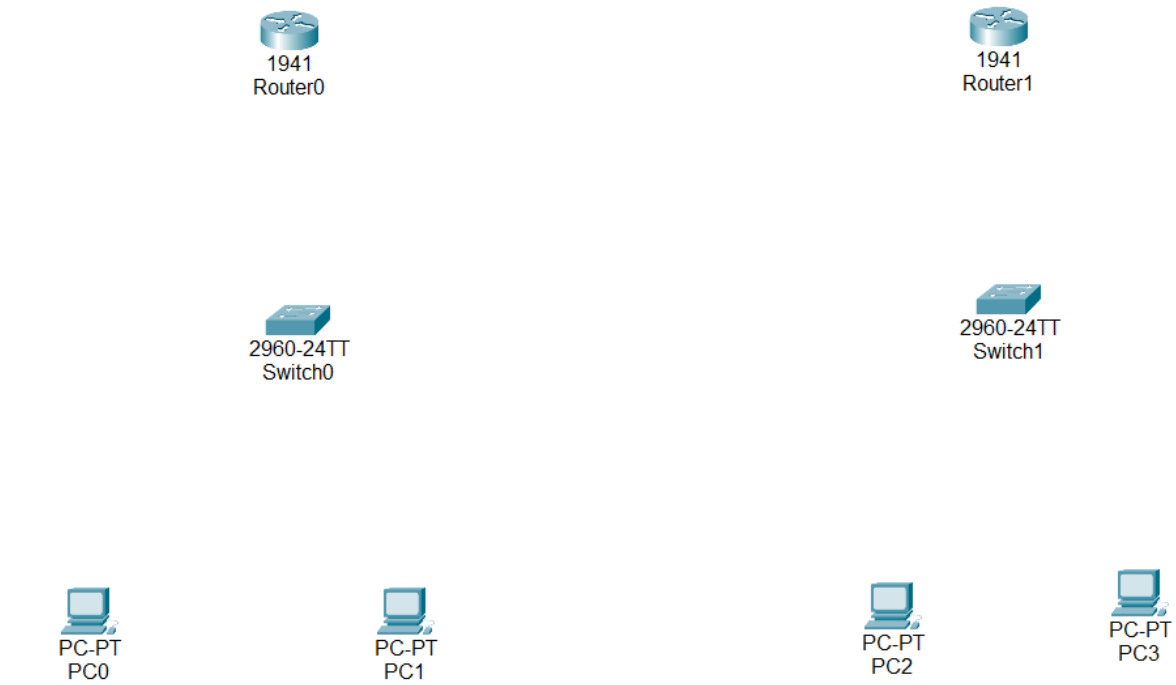
- **Human error**: In many cases, static routes are manually configured. This increases the potential for input mistakes. Administrators can make mistakes and mistype in network information, or configure incorrect routing paths by mistake.
- **Fault tolerance**: Static routing is not fault tolerant. This means that when there is a change in the network or a failure occurs between two statically defined devices, traffic will not be re-routed. As a result, the network is unusable until the failure is repaired or the static route is manually reconfigured by an administrator.
- **Administrative distance**: Static routes typically take precedence over routes configured with a dynamic routing protocol. This means that static routes may prevent routing protocols from working as intended. A solution is to manually modify the administrative distance.
- **Administrative overhead**: Static routes must be configured on each router in the network(s). This configuration can take a long time if there are many routers. It also means that reconfiguration can be slow and inefficient. Dynamic routing on the other hand automatically propagates routing changes, reducing the need for manual reconfiguration.

Topology

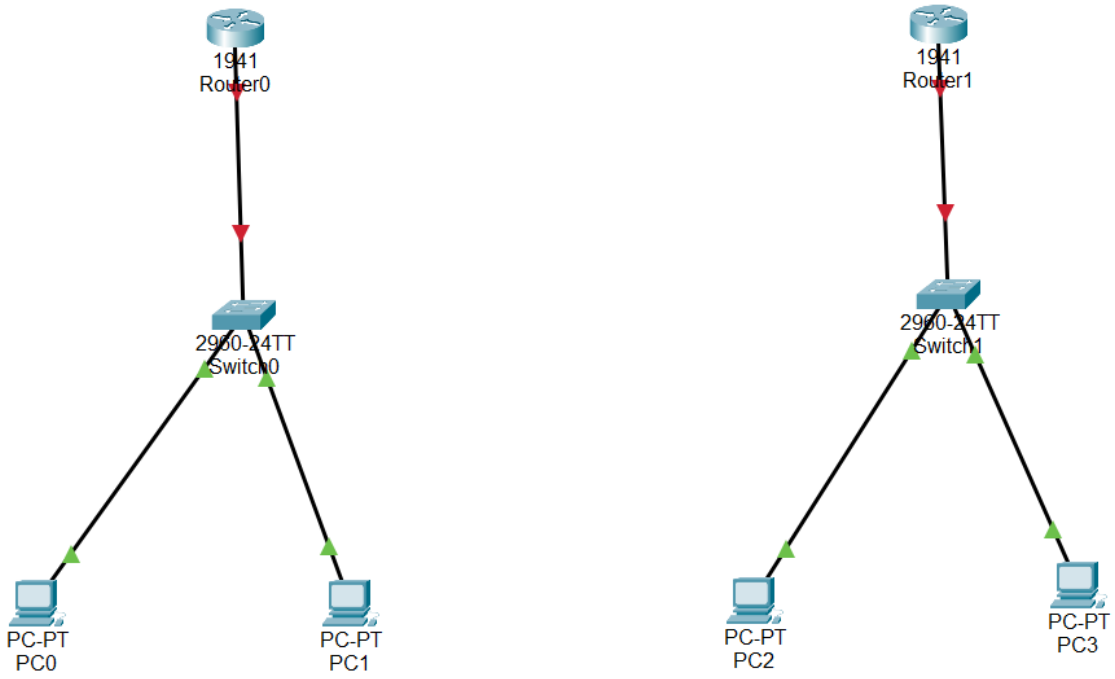


Steps to execute

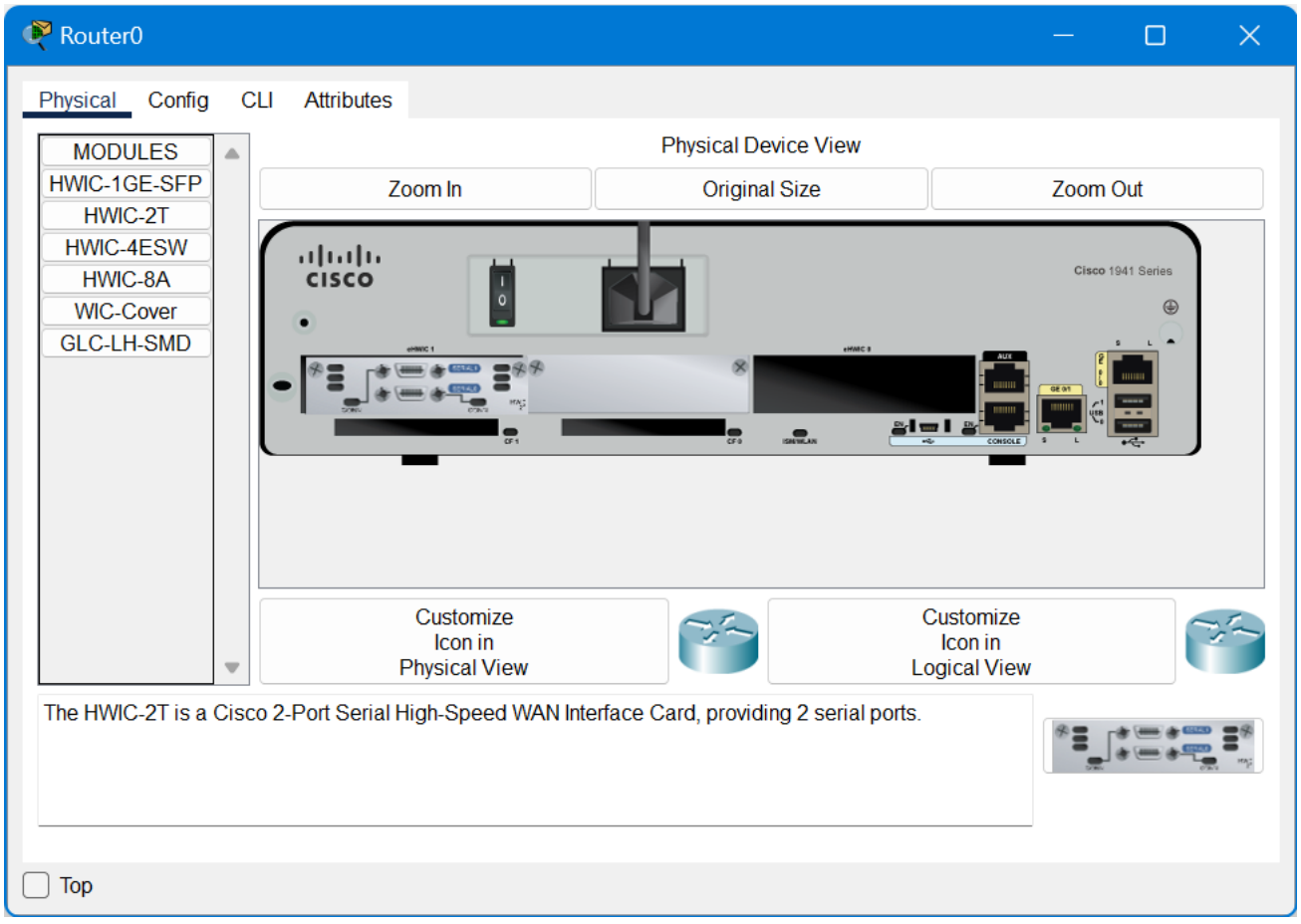
Step 1: Drag the elements required in the workplace.

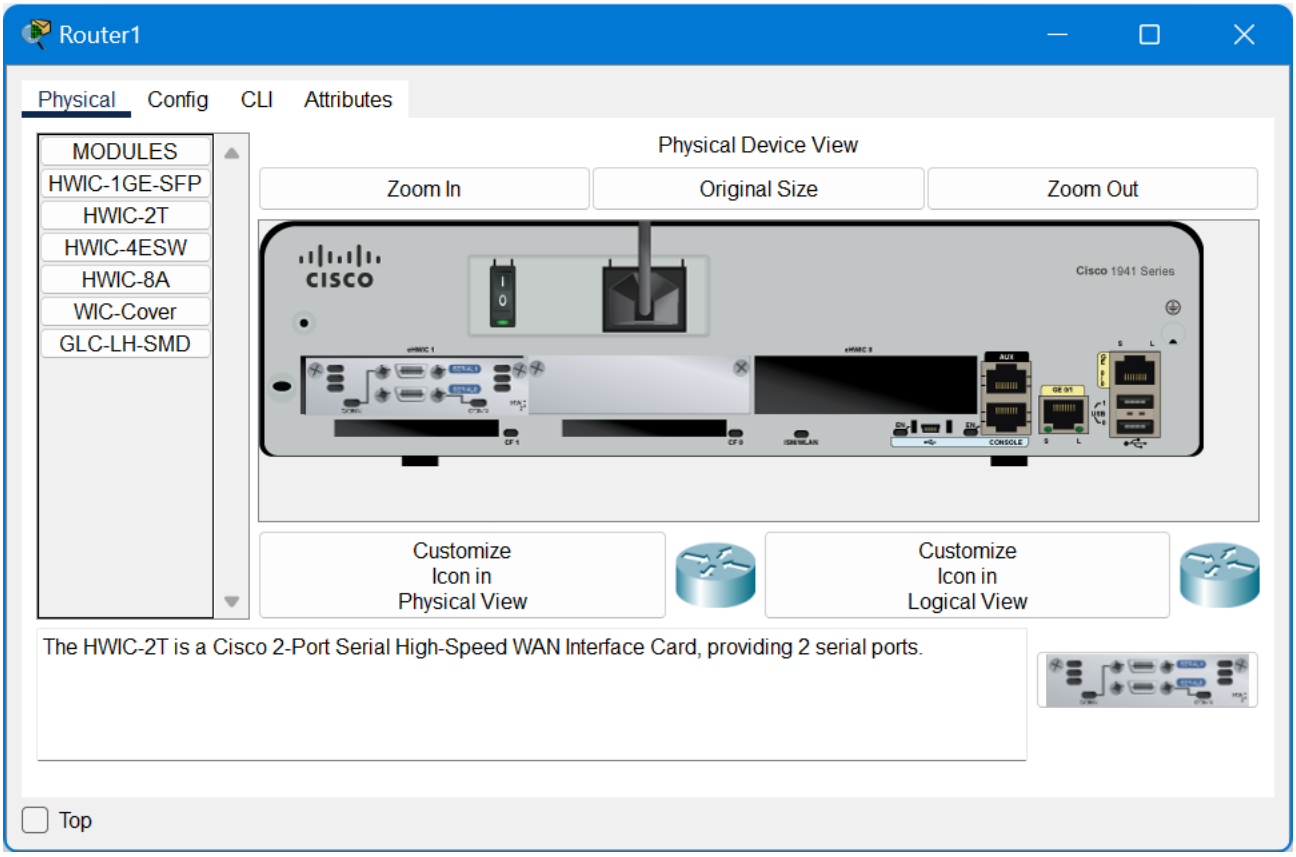


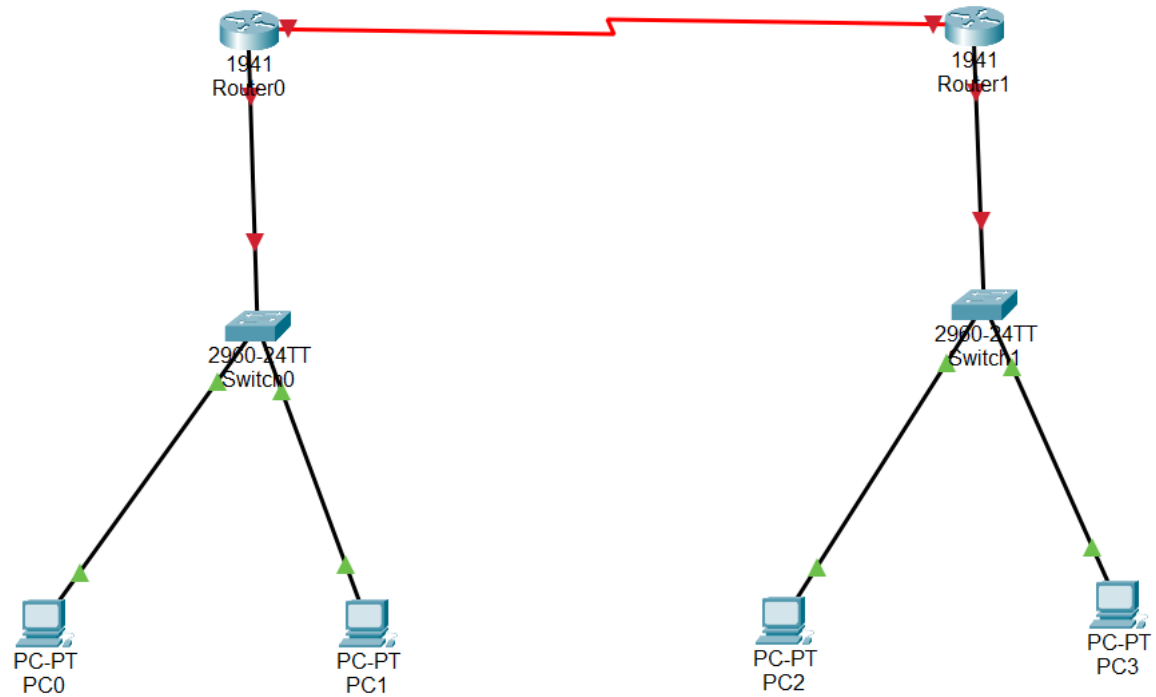
Step 2: Connect the routers and PCs via switch using straight through cable.



Step 3: Enable the routers for serial connectivity by adding HWIC-2T.

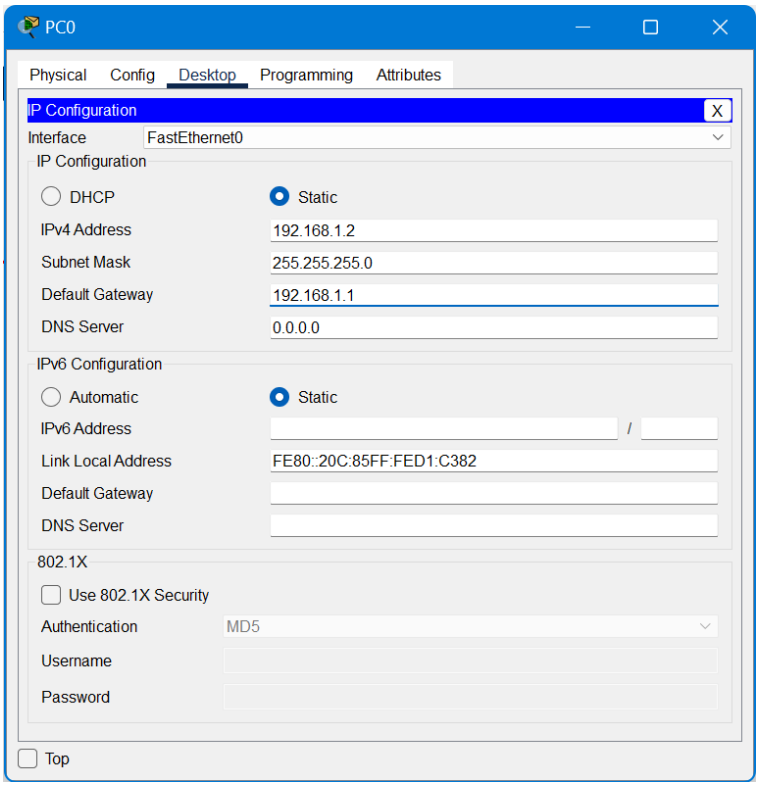






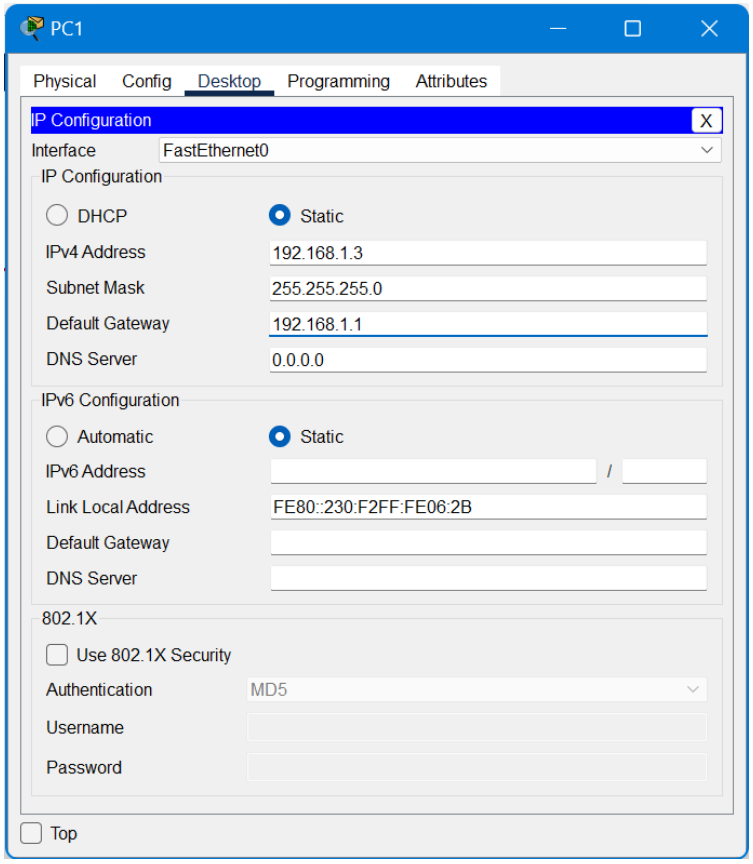
Step 4: Configure PC0:

- IPv4 Address: 192.168.1.2
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.1.1



Step 5: Configure PC1:

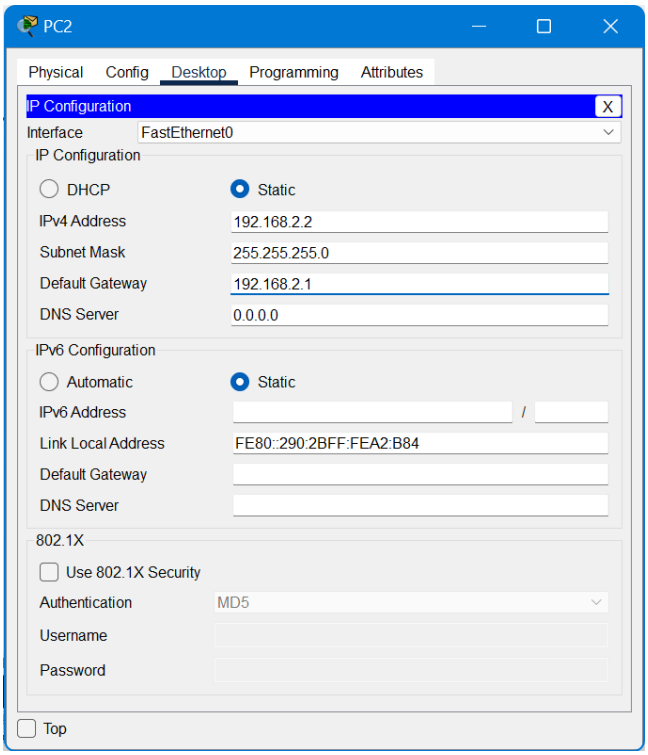
- IPv4 Address: 192.168.1.3
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.1.1



Step 6: Configure PC2:

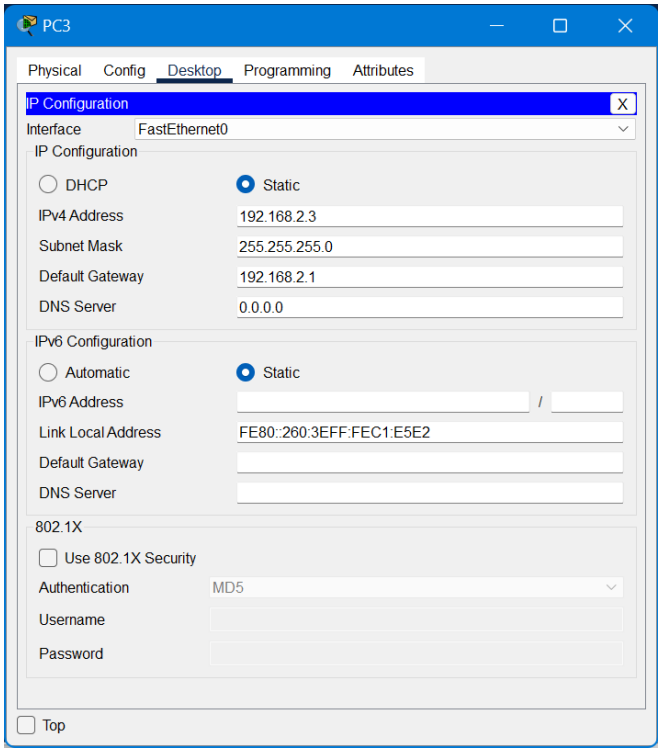
- IPv4 Address: 192.168.2.2

- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.2.1



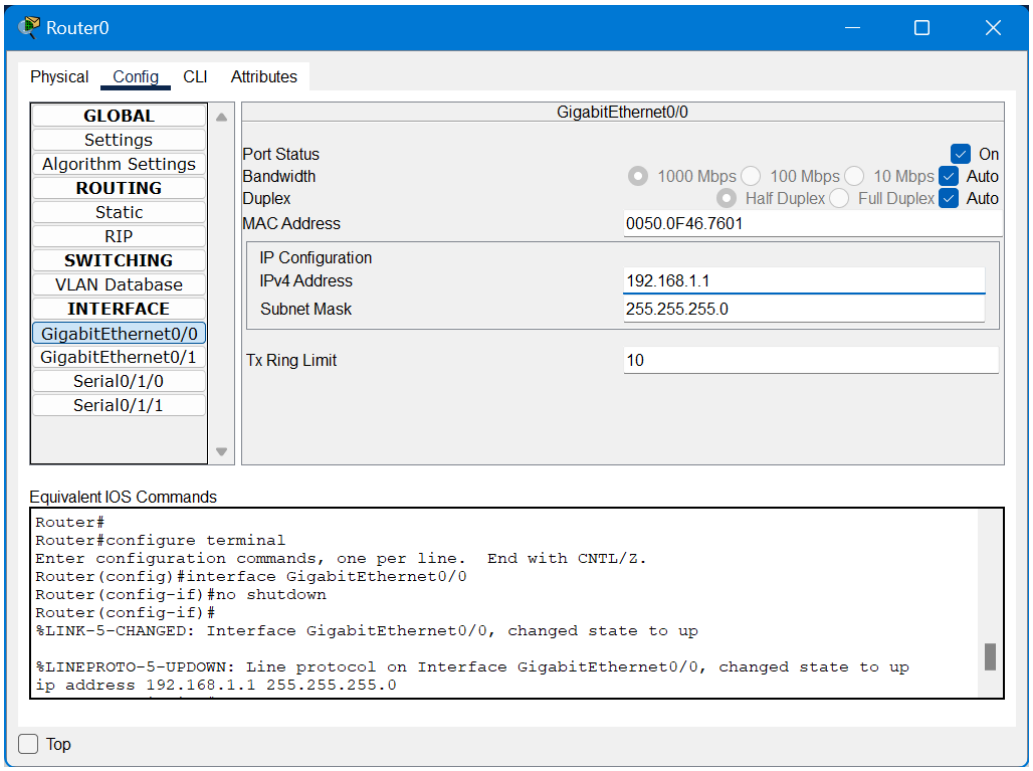
Step 7: Configure PC3:

- IPv4 Address: 192.168.2.3
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.2.1



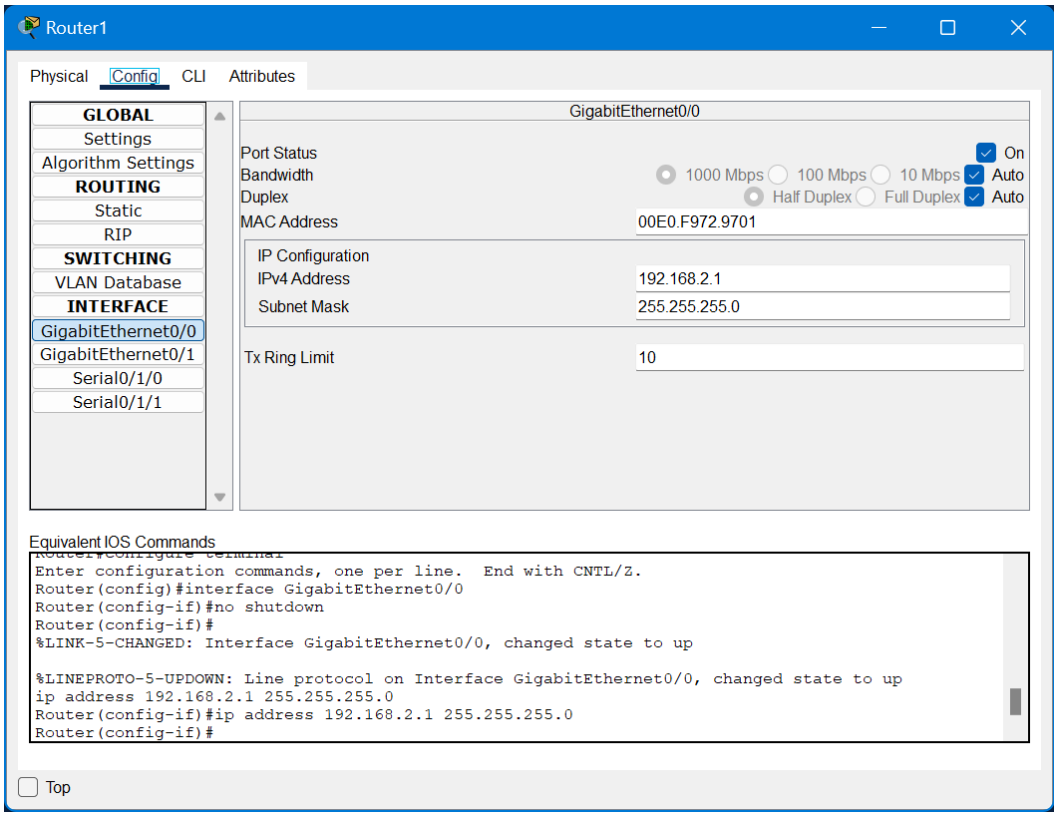
Step 8: Configure Router0 (GigabitEthernet0/0):

- IPv4 Address: 192.168.1.1
- Subnet mask: 255.255.255.0



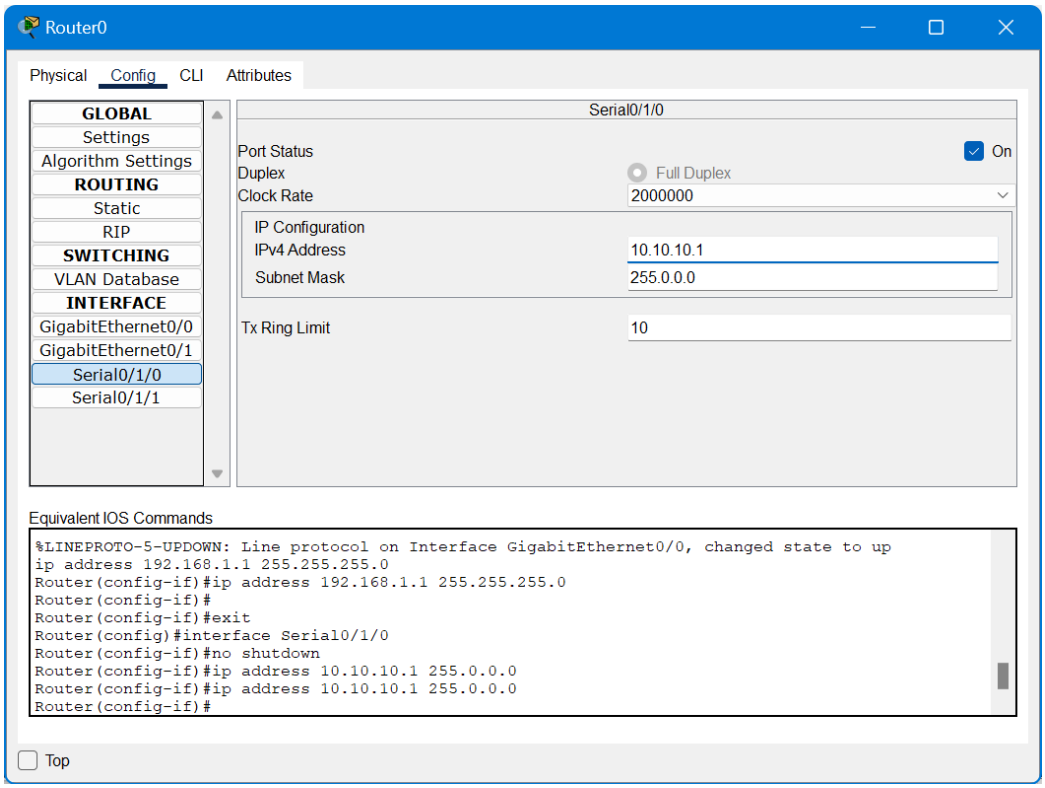
Step 9: Configure Router1 (GigabitEthernet0/0):

- IPv4 Address: 192.168.2.1
- Subnet mask: 255.255.255.0



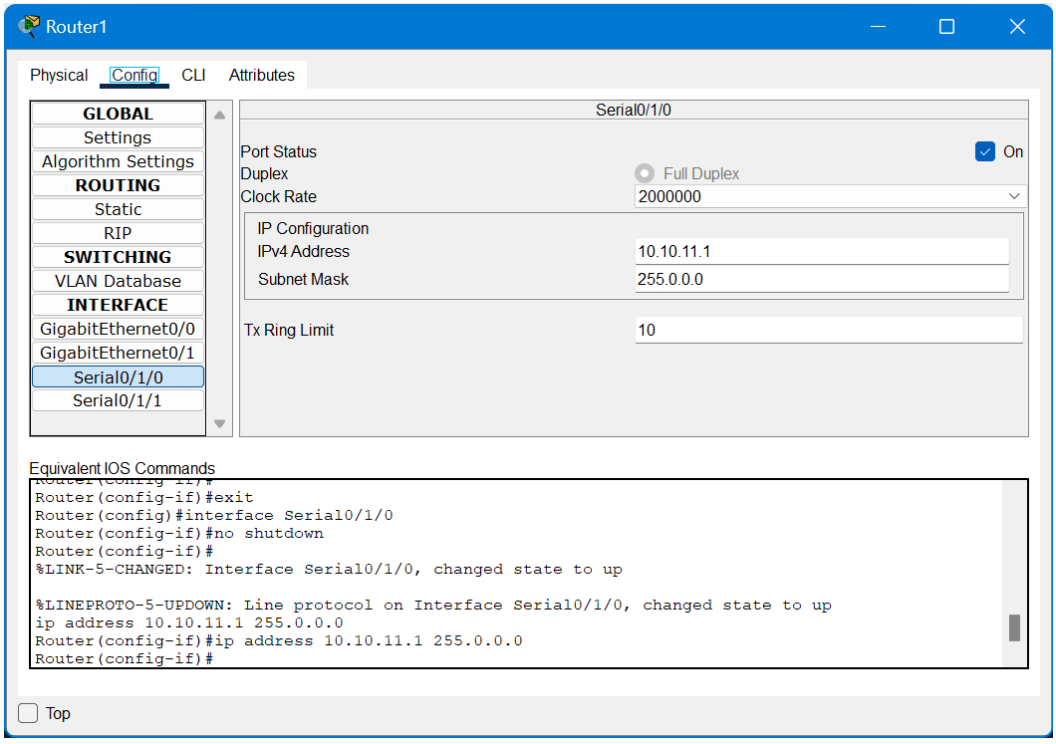
Step 10: Configure Router0 (Serial0/1/0):

- IPv4 Address: 10.10.10.1
- Subnet mask: 255.0.0.0



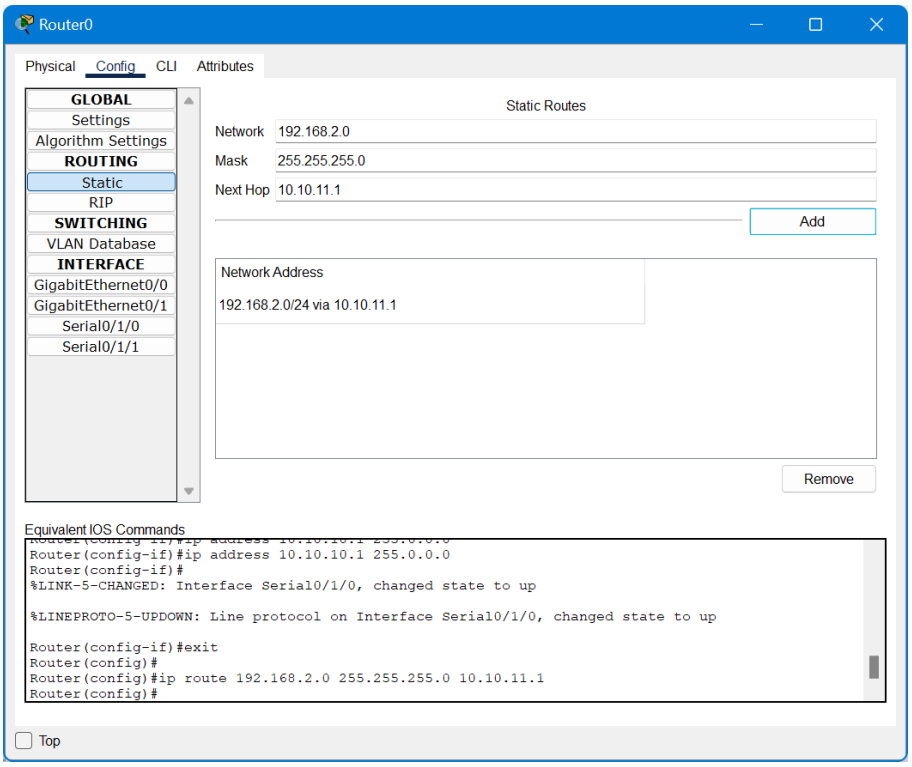
Step 11: Configure Router1 (Serial0/1/0):

- IPv4 Address: 10.10.11.1
- Subnet mask: 255.0.0.0



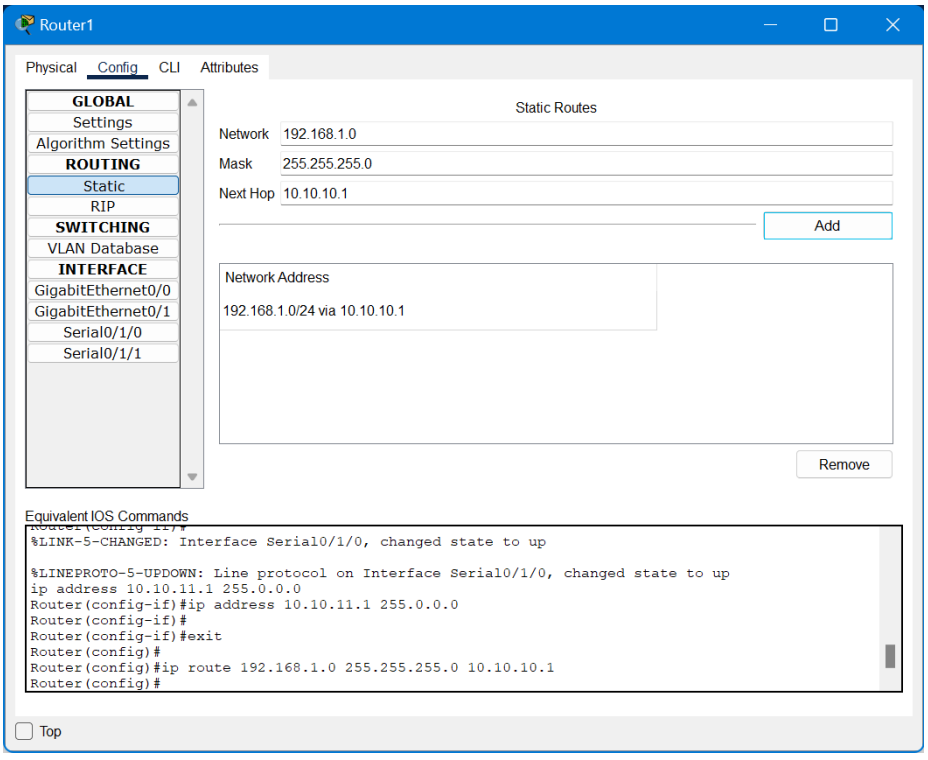
Step 12: Configure Router0 (Static routing):

- IPv4 Address: 192.168.2.0
- Mask: 255.255.255.0
- Next hop: 10.10.11.1

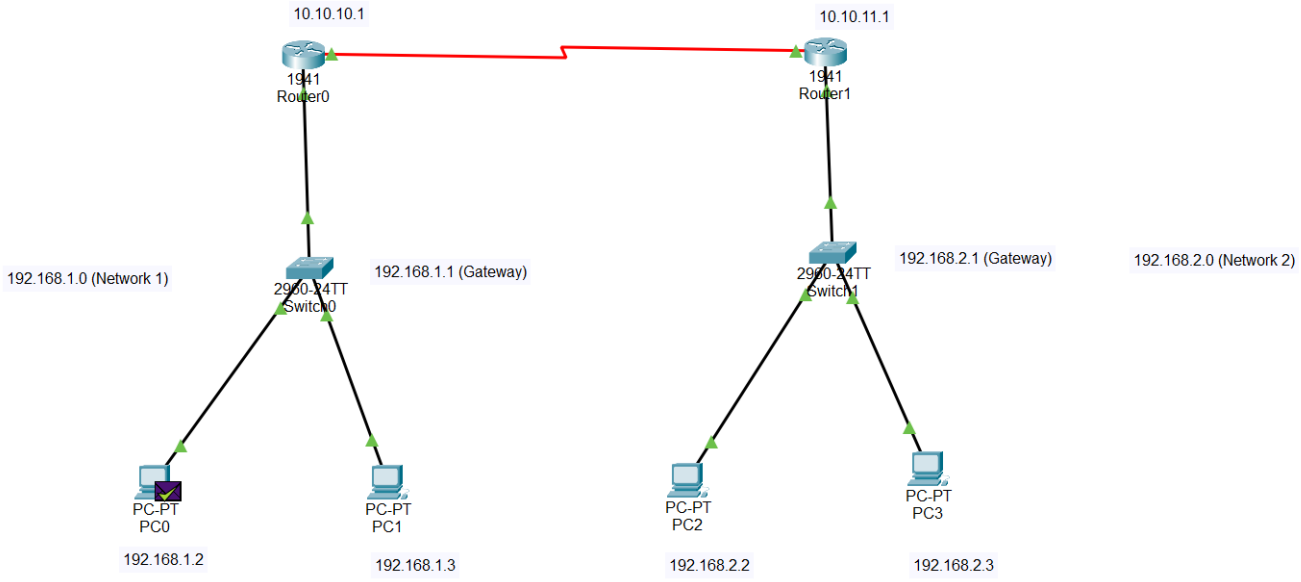


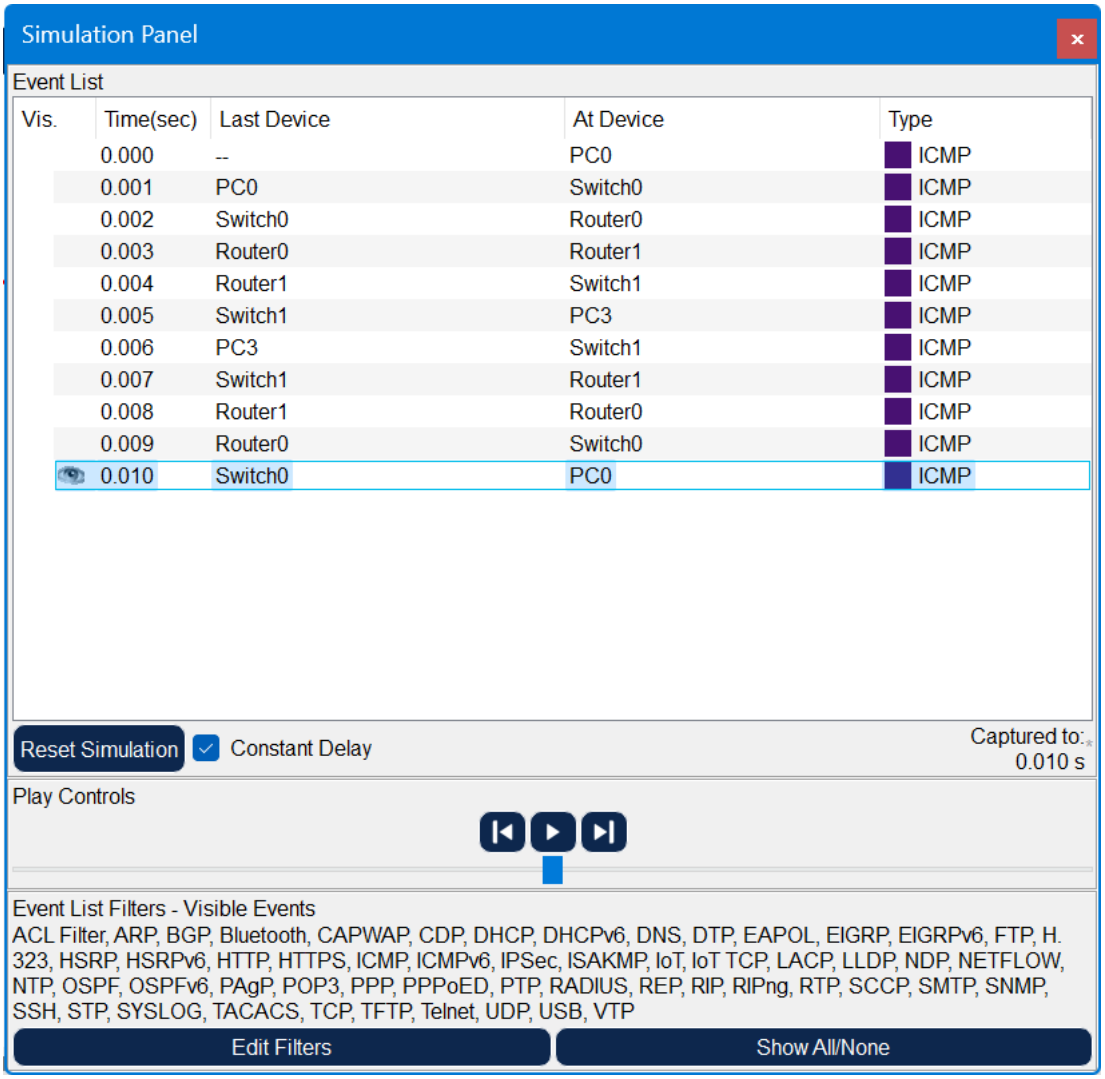
Step 13: Configure Router1 (Static routing):

- IPv4 Address: 192.168.1.0
- Mask: 255.255.255.0
- Next hop: 10.10.10.1

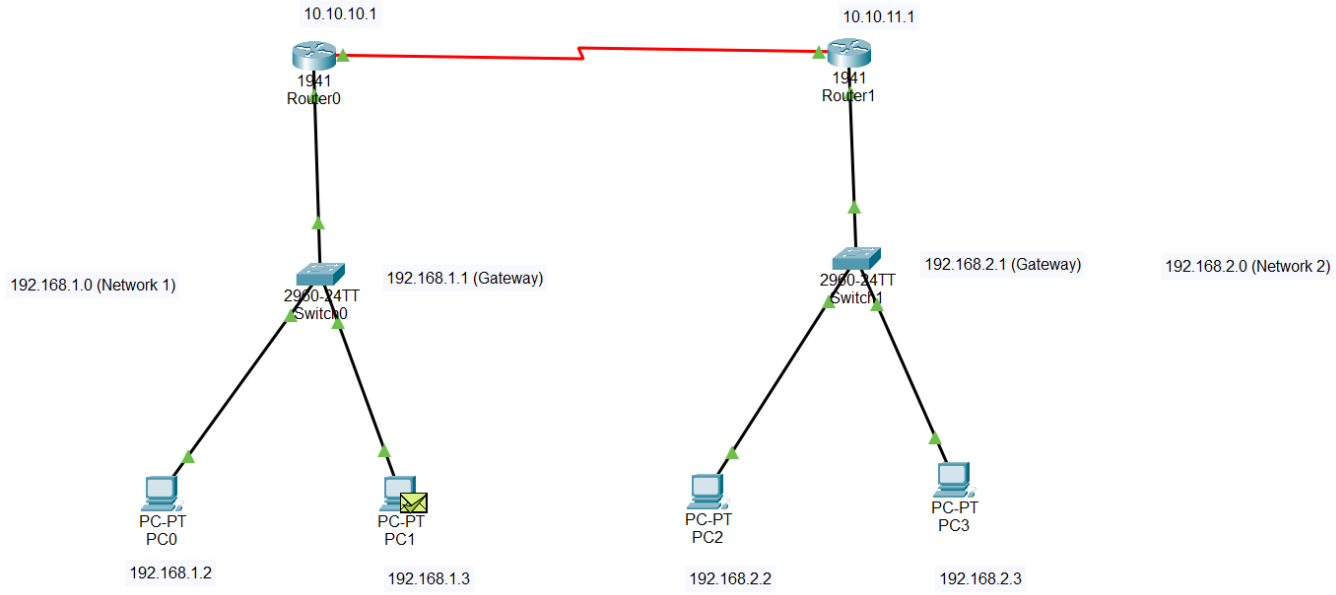


Step 14: Click on add simple PDU and make PC0 as source and PC3 as destination. Then click on simulation tab to see the simulation of data.





Step 15: Click on add simple PDU and make PC1 as source and PC2 as destination. Then click on simulation tab to see the simulation of data.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch0	ICMP
	0.002	Switch0	Router0	ICMP
	0.003	Router0	Router1	ICMP
	0.004	Router1	Switch1	ICMP
	0.005	Switch1	PC2	ICMP
	0.006	PC2	Switch1	ICMP
	0.007	Switch1	Router1	ICMP
	0.008	Router1	Router0	ICMP
	0.009	Router0	Switch0	ICMP
	0.010	Switch0	PC1	ICMP

Reset Simulation | Constant Delay | Captured to: 0.010 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Commands to check connectivity

PC1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::230:F2FF:FE06:2B
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

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=14ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 9ms

C:\>
```

PC3

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:3EFF:FEC1:E5E2
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.2.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.2.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=126
Reply from 192.168.1.2: bytes=32 time=9ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 5ms

C:\>
```

Practical No. 7

Aim: To implement the DNS, Email services, FTP and Web Server in the network using CISCO Packet Tracer.

Theory

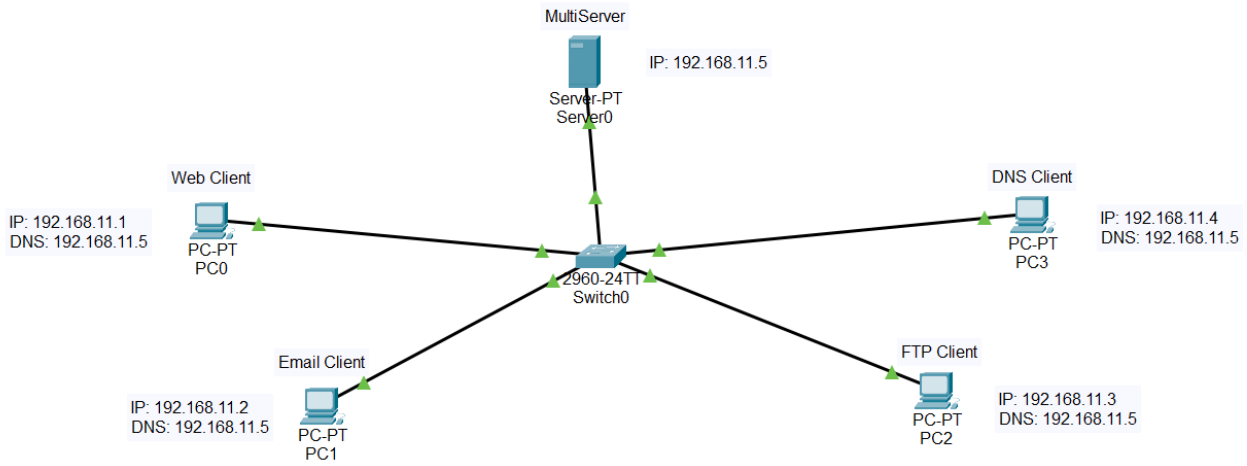
DNS Server: The DNS system is like the internet's phonebook. When you type a domain name (like www.example.com) into your browser, a DNS server translates that human-readable domain name into an IP address that computers use to locate resources on the internet. DNS servers store databases of domain names and their corresponding IP addresses. They resolve queries by mapping domain names to IP addresses, facilitating communication between devices across the internet.

Email Server: Email servers are responsible for sending, receiving, and storing emails. They use various protocols like SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), and POP3 (Post Office Protocol version 3) to handle email communication. An email server manages the flow of emails by receiving messages, determining their destinations, and delivering them to the recipient's inbox. It also authenticates users and stores emails until they are retrieved by an email client.

FTP Server: FTP servers facilitate the transfer of files between computers over a network. They use the FTP protocol to manage the uploading, downloading, and sharing of files. FTP servers host files and directories, allowing users to upload files from their devices or download files to their devices using FTP clients. It provides a way to share files securely over a network.

Web Server: Web servers deliver web content to users' browsers upon request. They use HTTP (Hypertext Transfer Protocol) or HTTPS (HTTP Secure) to communicate with clients. A web server stores and serves web pages, images, videos, and other web content to users who request them through their browsers. It processes requests, retrieves the requested data from the server's storage, and sends it to the user's device for display in the browser.

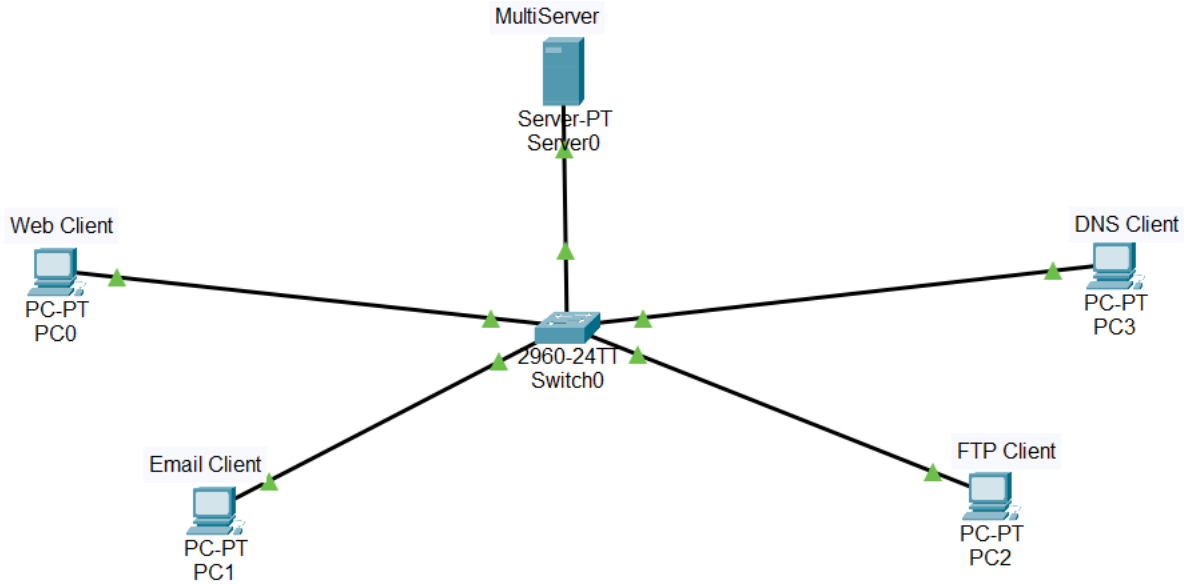
Topology



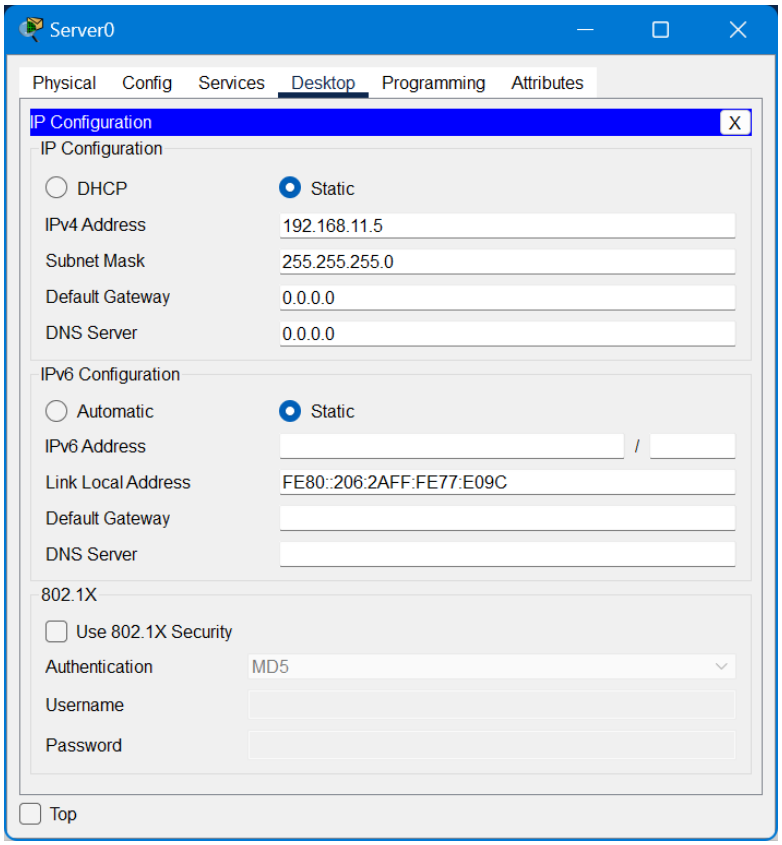
Steps to execute

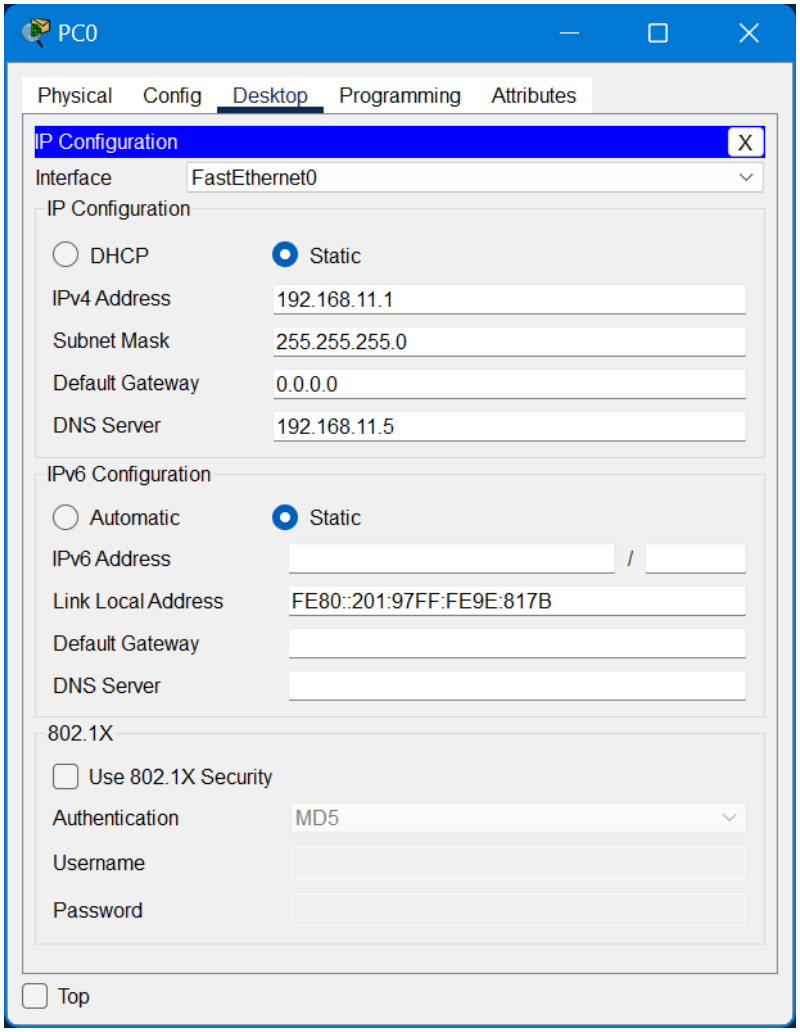
Step 1: Drag the elements required in the workplace.

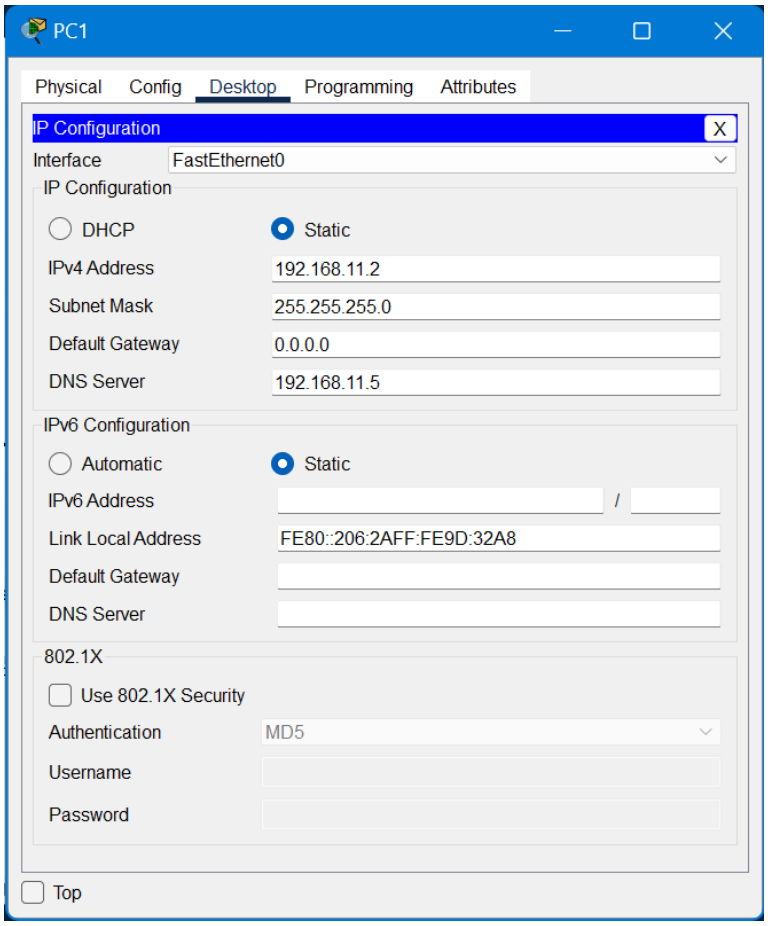
Step 2: Connect the PC's and server with the switch using straight through cable.

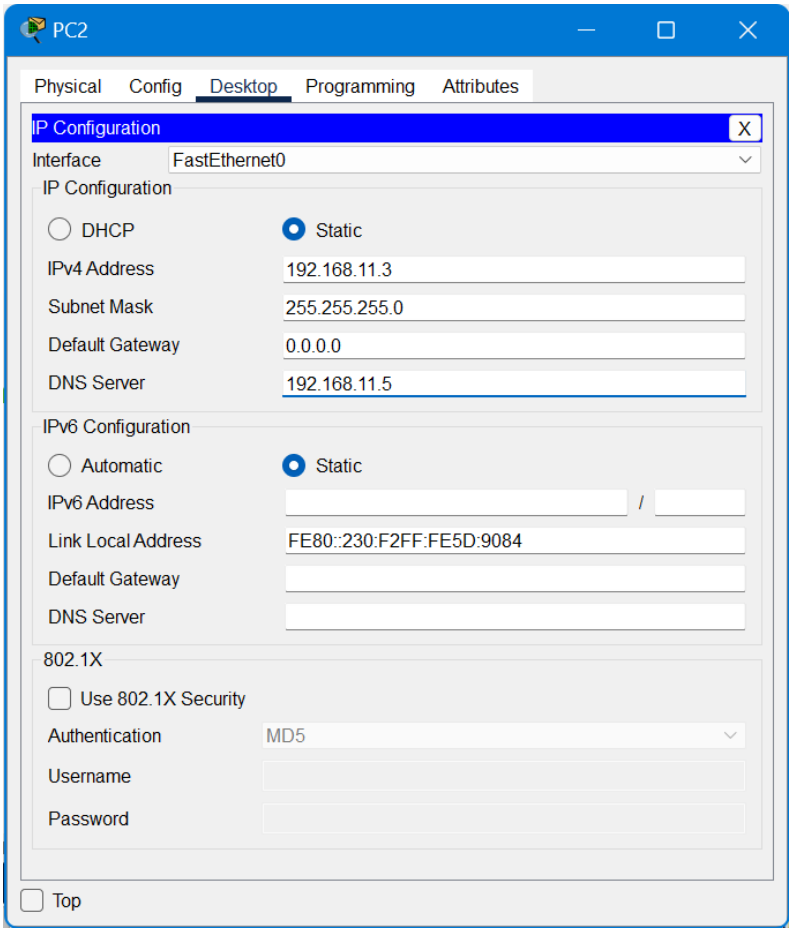


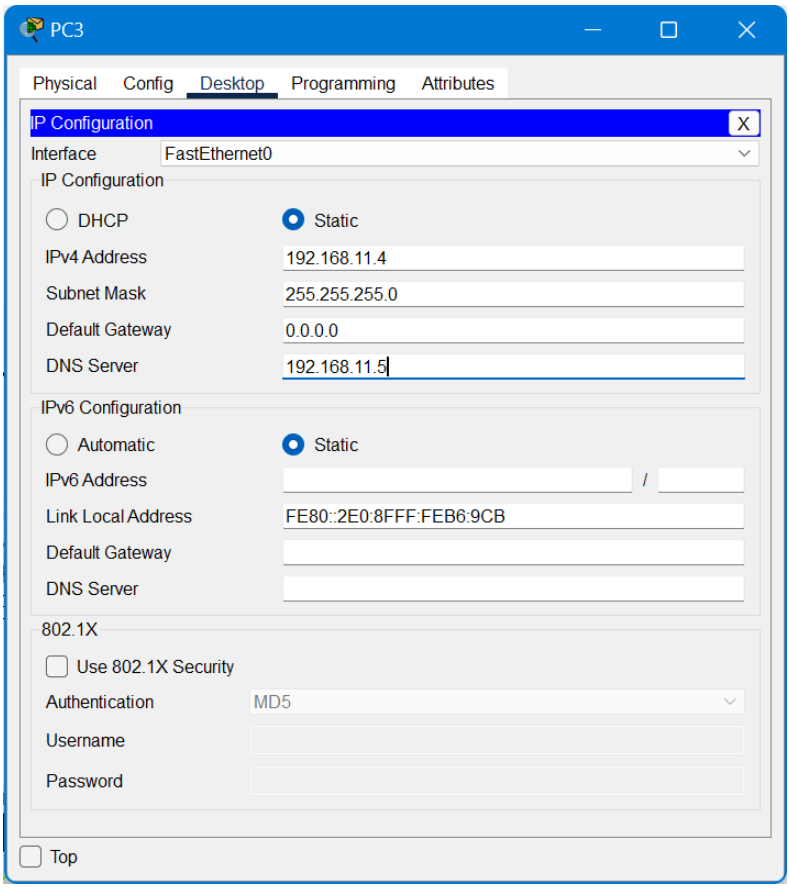
Step 3: Configure the PC's and the server.


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.11.5
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::206:2AFF:FE77:E09C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.11.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
192.168.11.5
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE9E:817B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

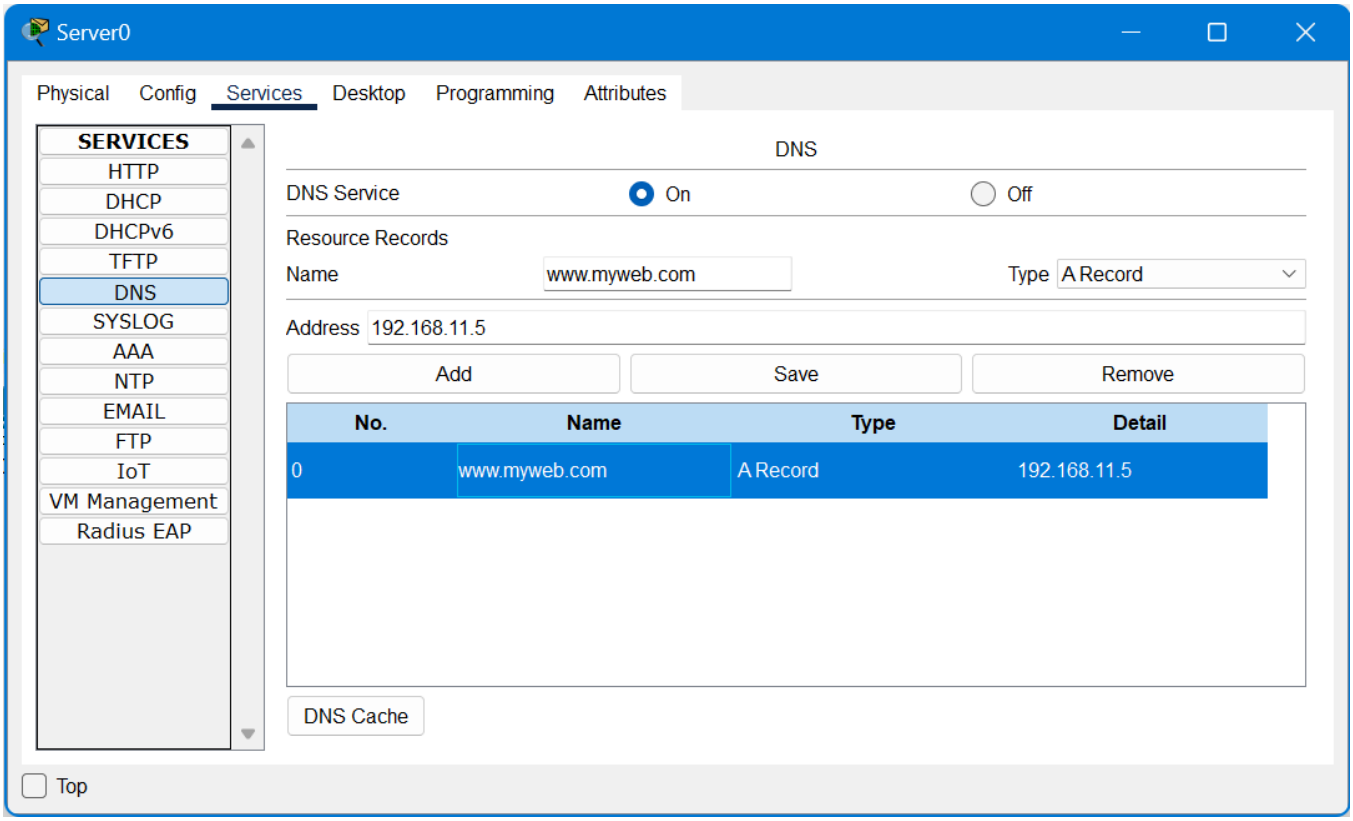

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.11.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
192.168.11.5
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::206:2AFF:FE9D:32A8
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.11.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
192.168.11.5
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::230:F2FF:FE5D:9084
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

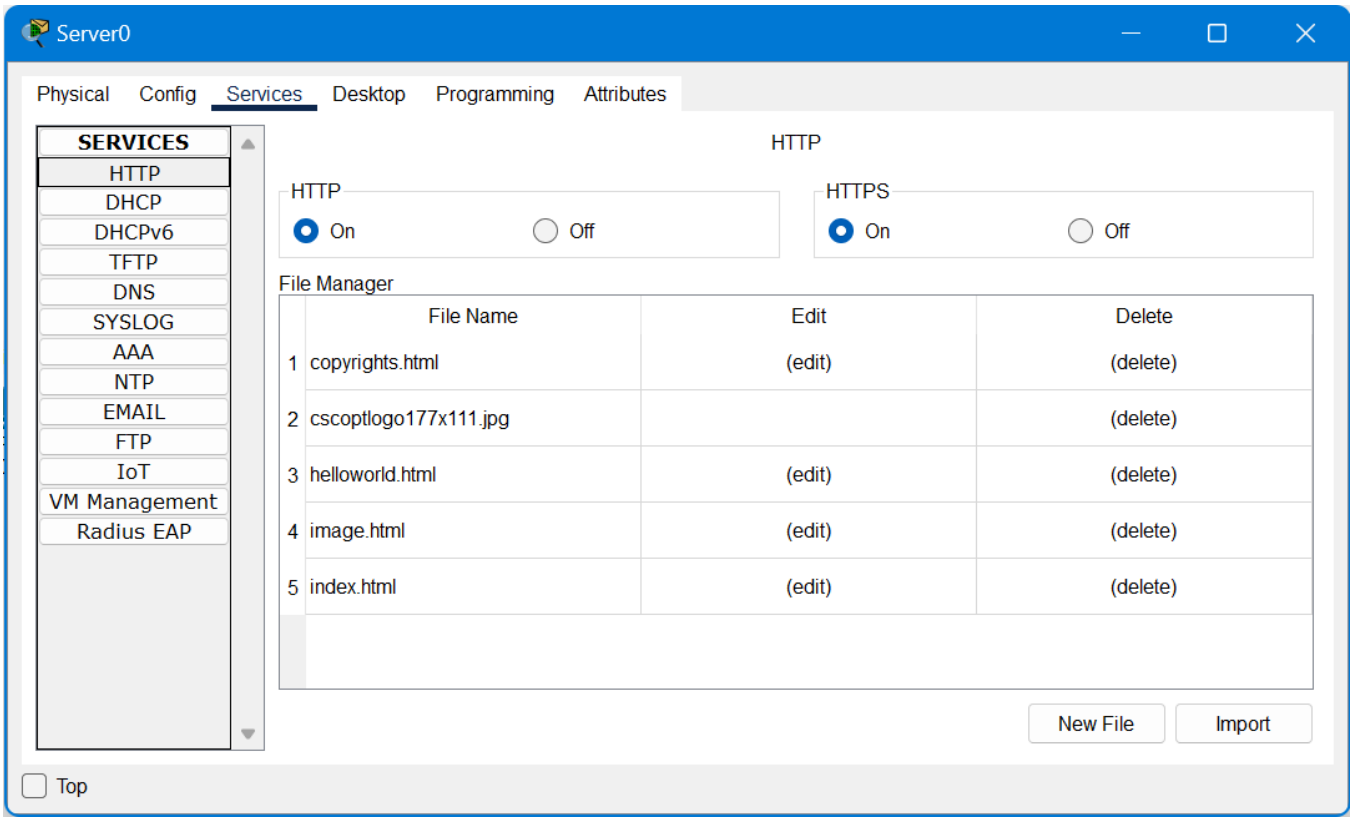


DNS and Web service

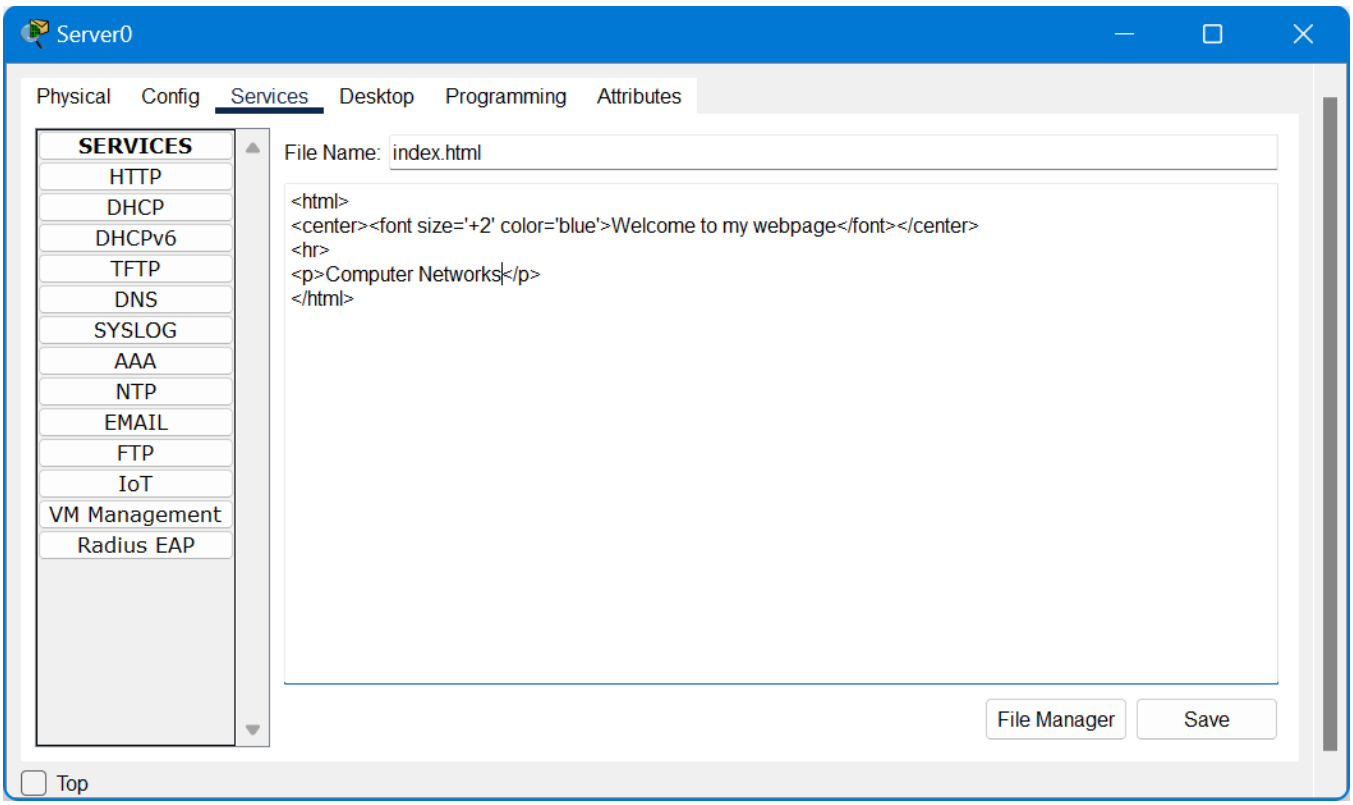
Step 4: Go to Server, then Services and choose DNS, switch it on. Add name of domain like 'www.myweb.com' and DNS address in the address field.



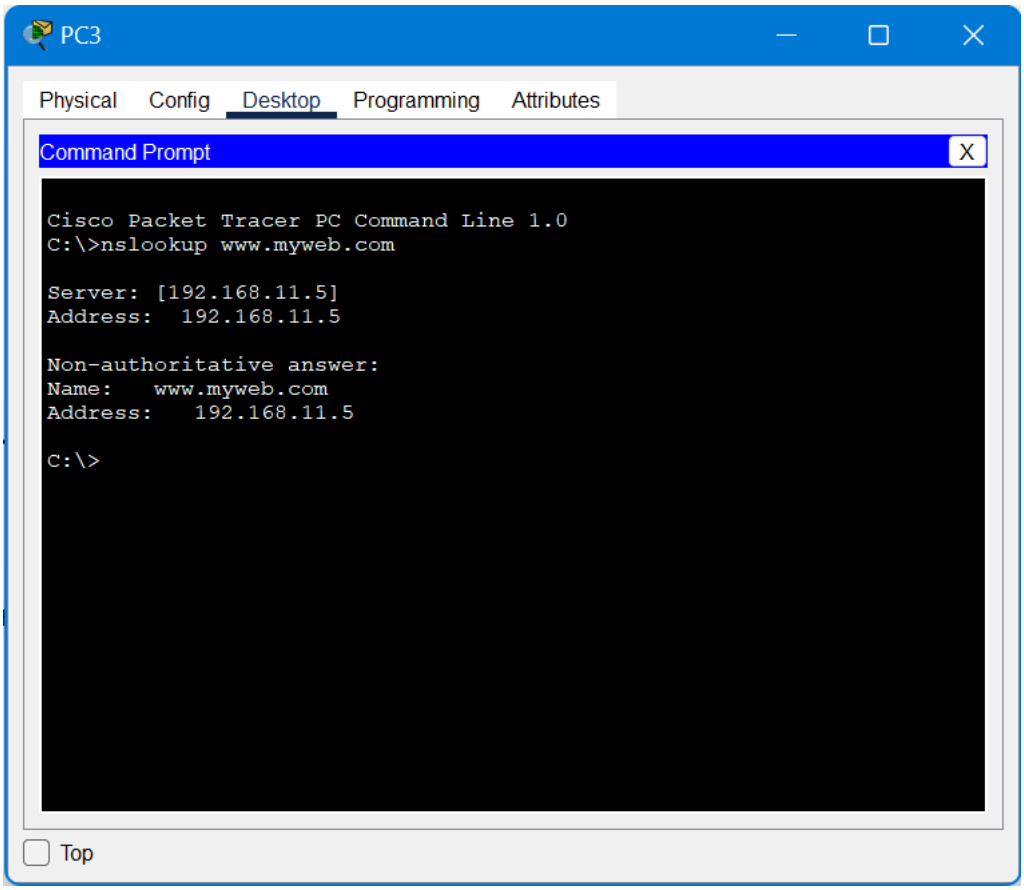
Step 5: Now for Web service, go to HTTP Service and switch on HTTP and HTTPS.



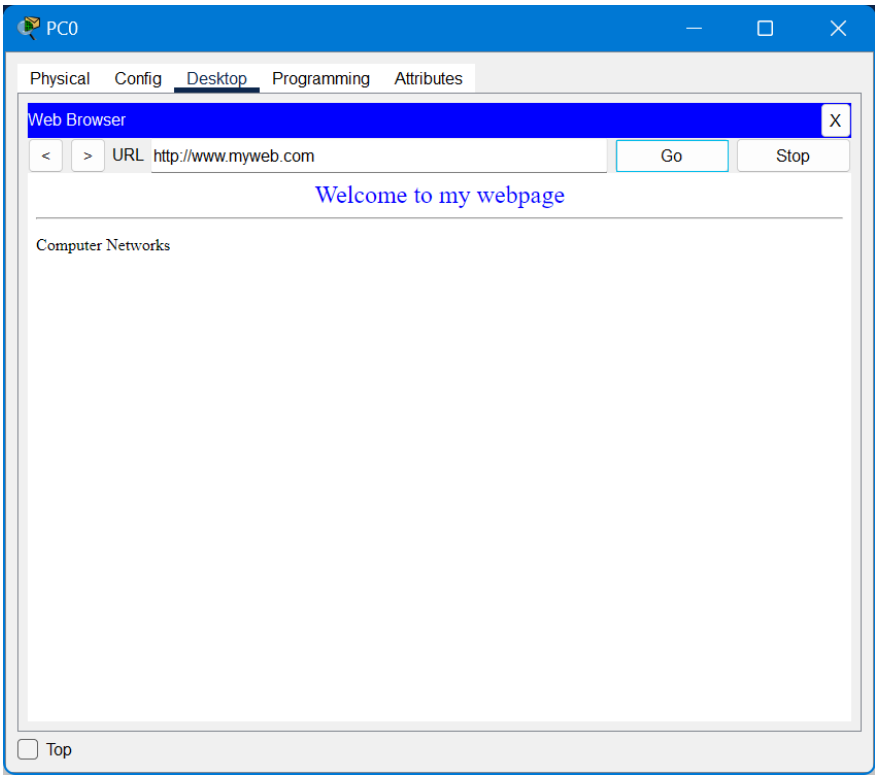
Step 6: Edit index.html only as it is the webpage i.e indexed by any browser when accessing website and save it.



Step 7: Now to check DNS service working, go to DNS Client(PC3) and open command prompt and enter given command - ‘nslookup www.myweb.com’.

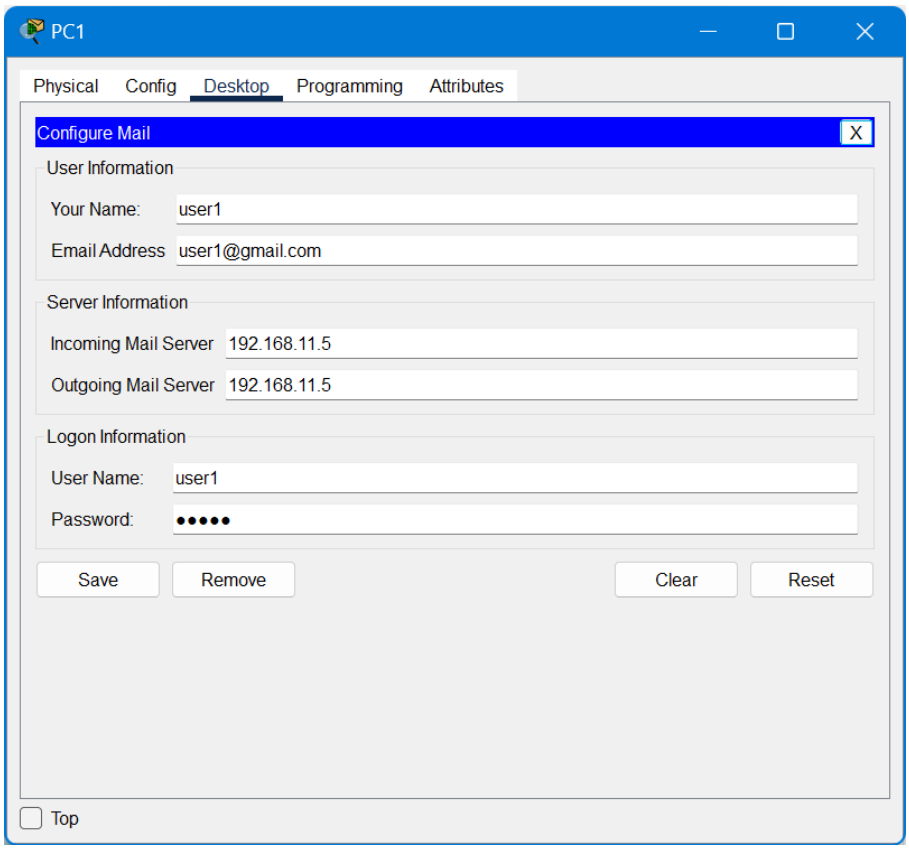


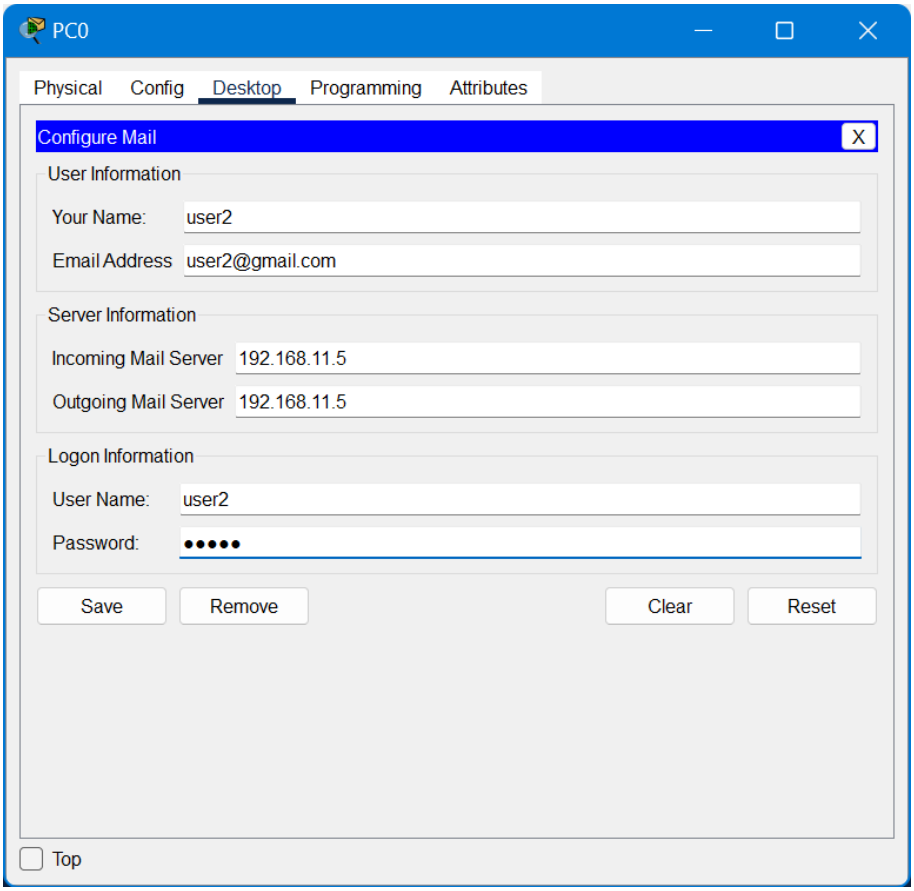
Step 8: To check web service running, go to Web Client's web browser and type 'www.myweb.com' in the URL.



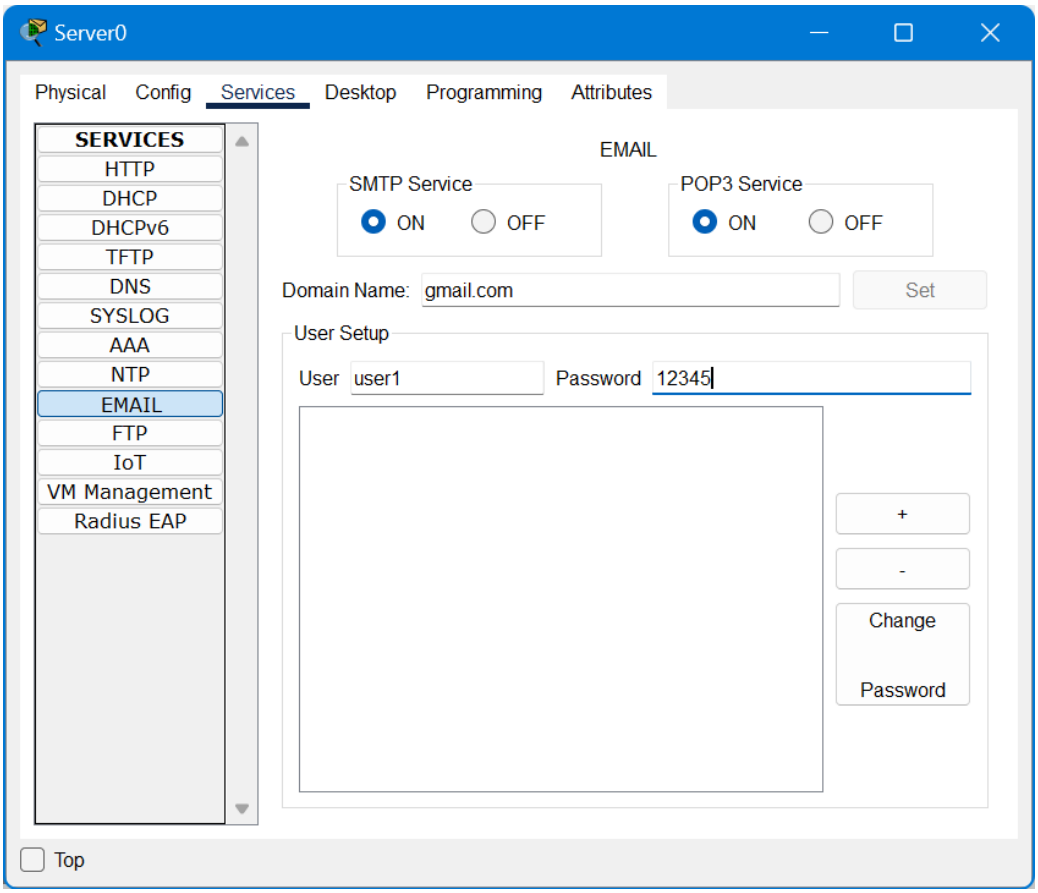
Email Service

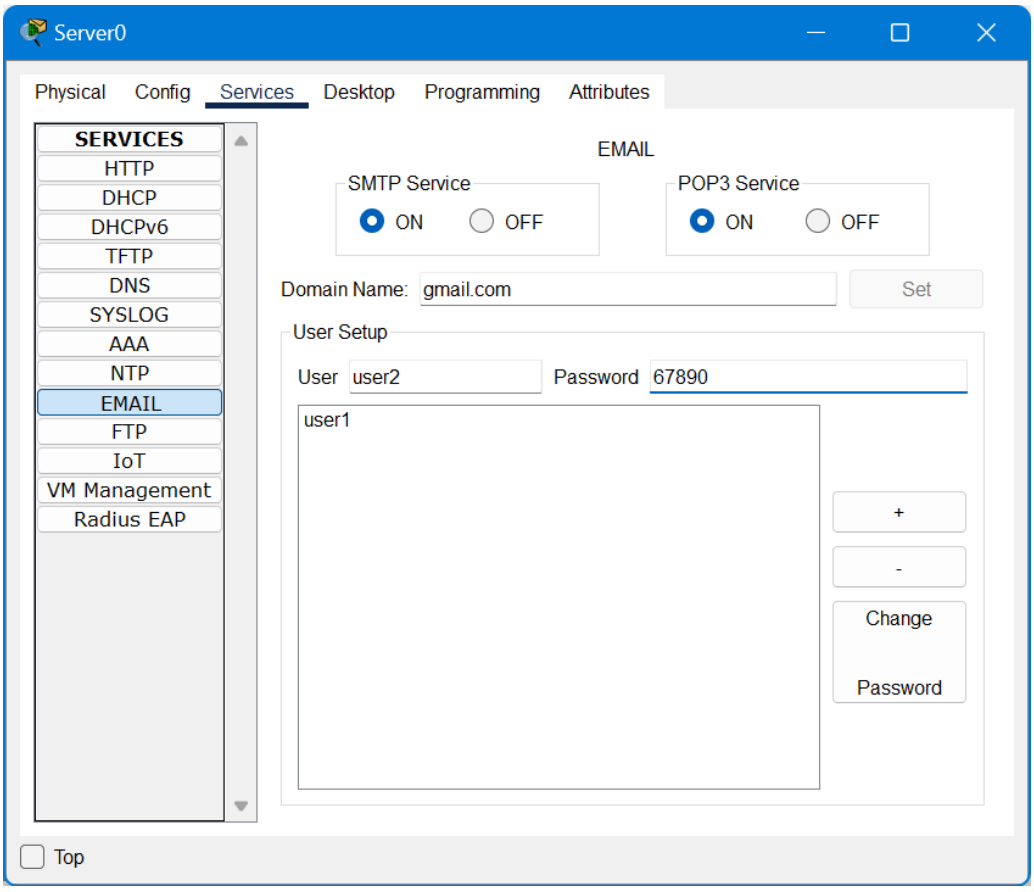
Step 9: Create 2 Email Clients with Email Client (PC1) and Web Client (PC0), go to email settings and configure new users and their passwords.

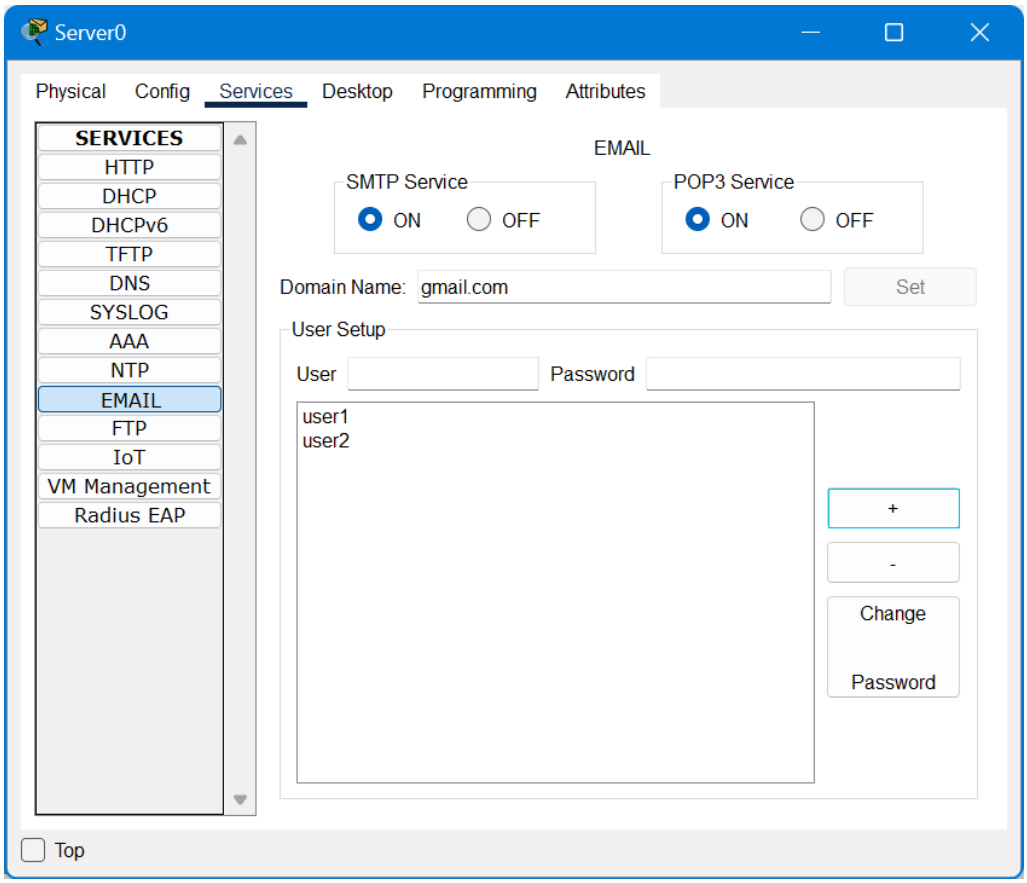




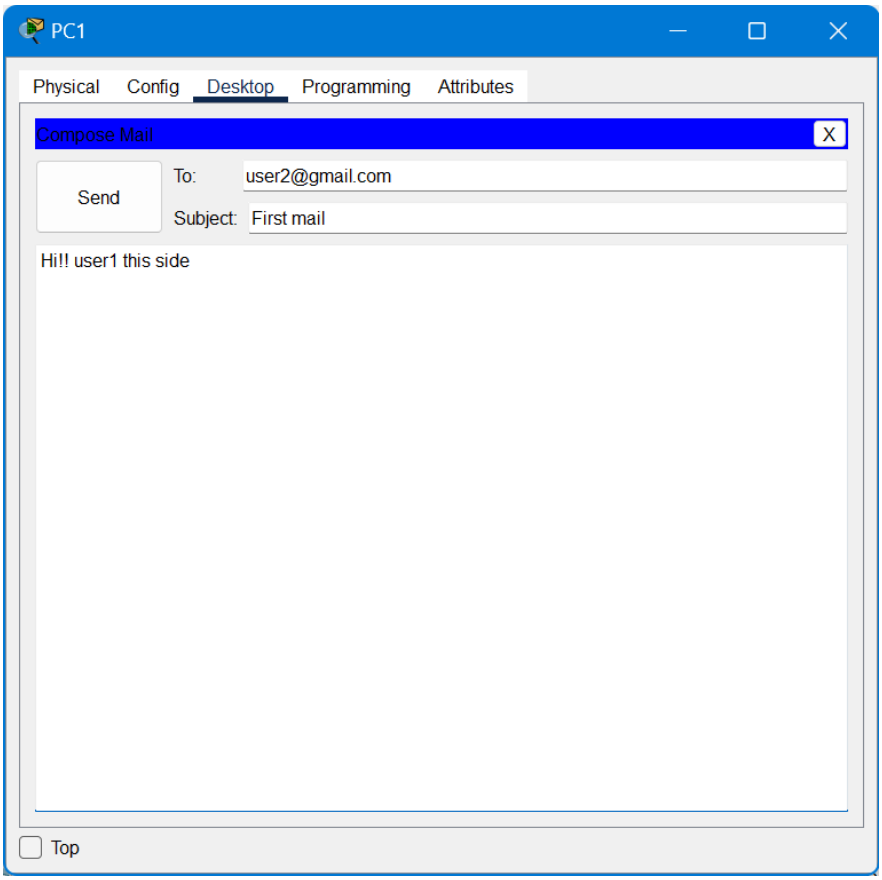
Step 10: Go to Server select EMAIL service, turn SMTP and POP3 on and set the two users credentials with domain name.

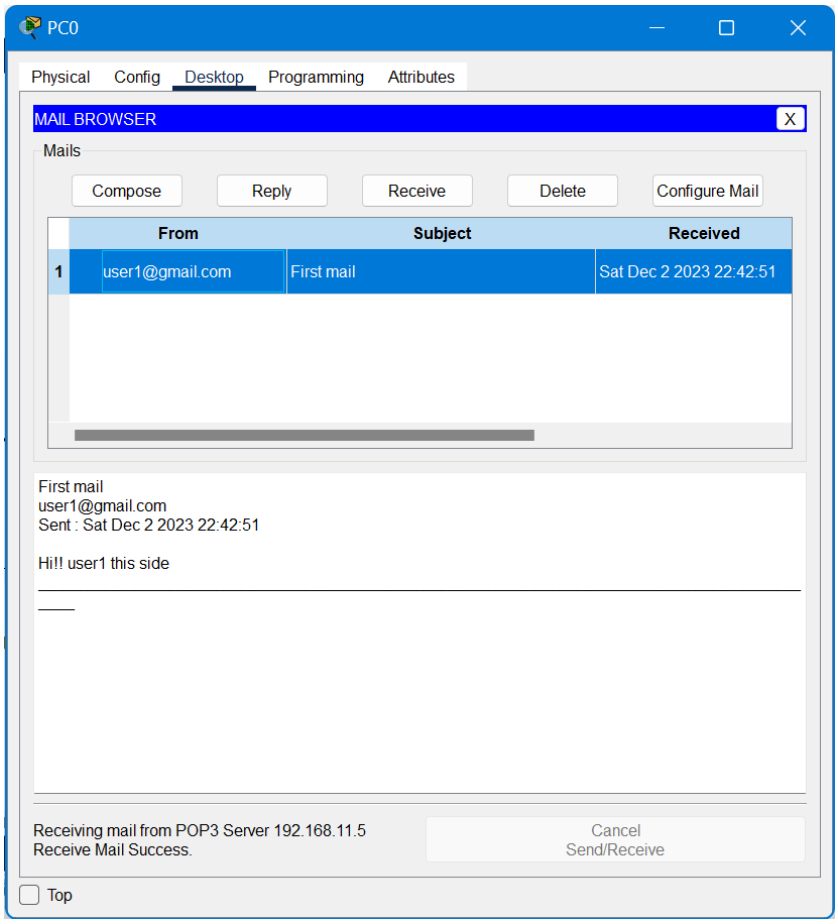

Server0
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
EMAIL
SMTP Service
ON
OFF
POP3 Service
ON
OFF
Domain Name:
gmail.com
Set
User Setup
User
user1
Password
12345
+
-
Change
Password
Top

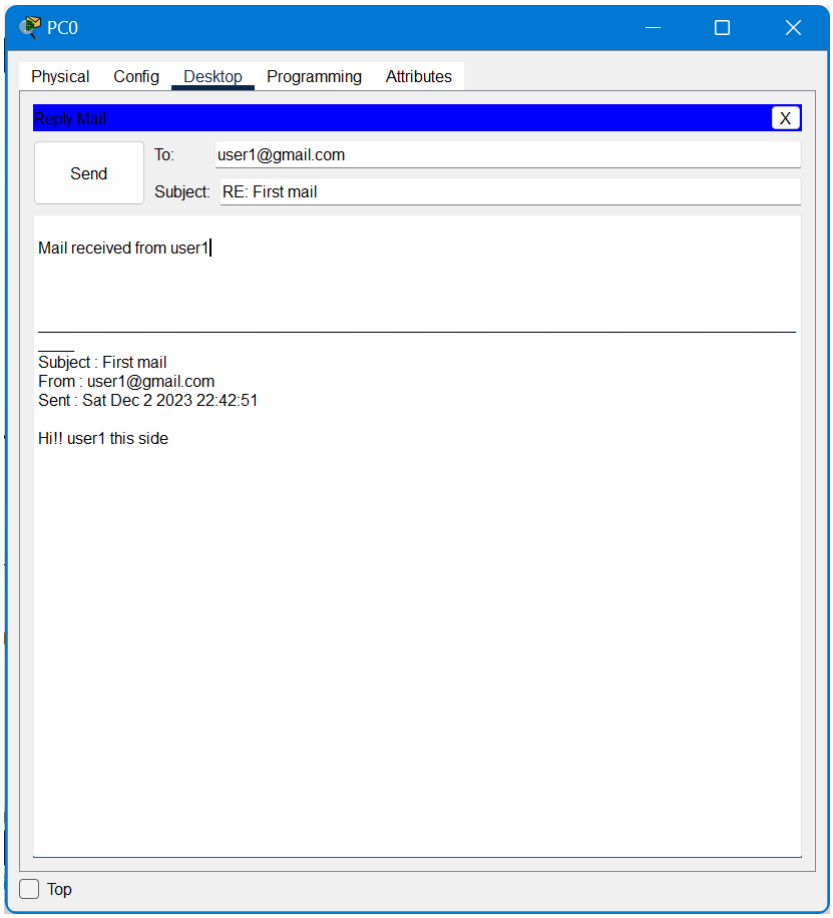

Server0
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
EMAIL
SMTP Service
ON
OFF
POP3 Service
ON
OFF
Domain Name:
gmail.com
Set
User Setup
User
user2
Password
67890
user1
+
-
Change
Password
Top

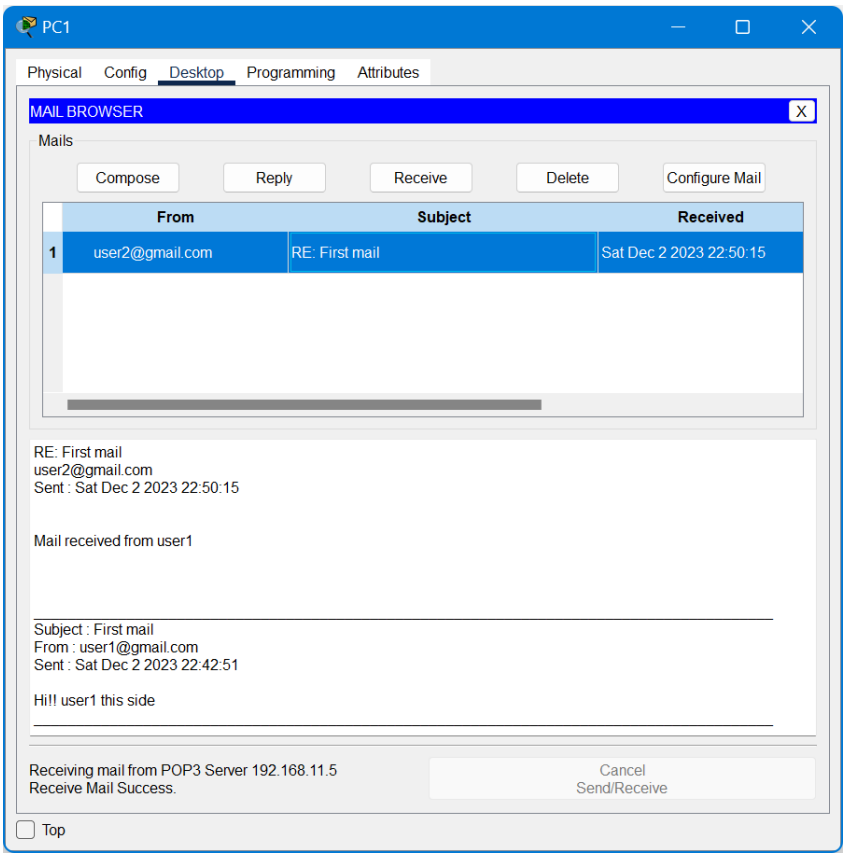


Step 11: Now to test Email service working, go to PC1 email settings and send an email to PC0 and then reply back to the PC1(Email Client) mail from the PC0(Web Client).



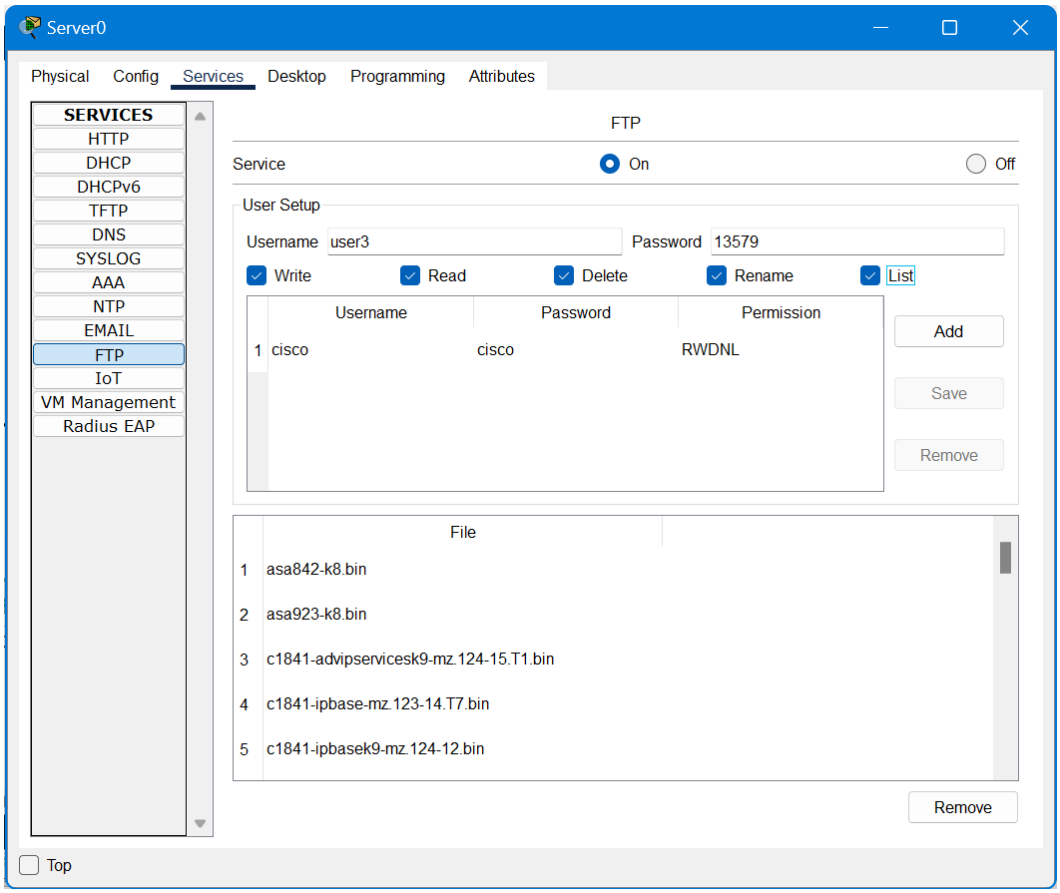

PC0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user1@gmail.com
First mail
Sat Dec 2 2023 22:42:51
First mail
user1@gmail.com
Sent : Sat Dec 2 2023 22:42:51
Hi!! user1 this side
Receiving mail from POP3 Server 192.168.11.5
Receive Mail Success.
Cancel
Send/Receive
Top

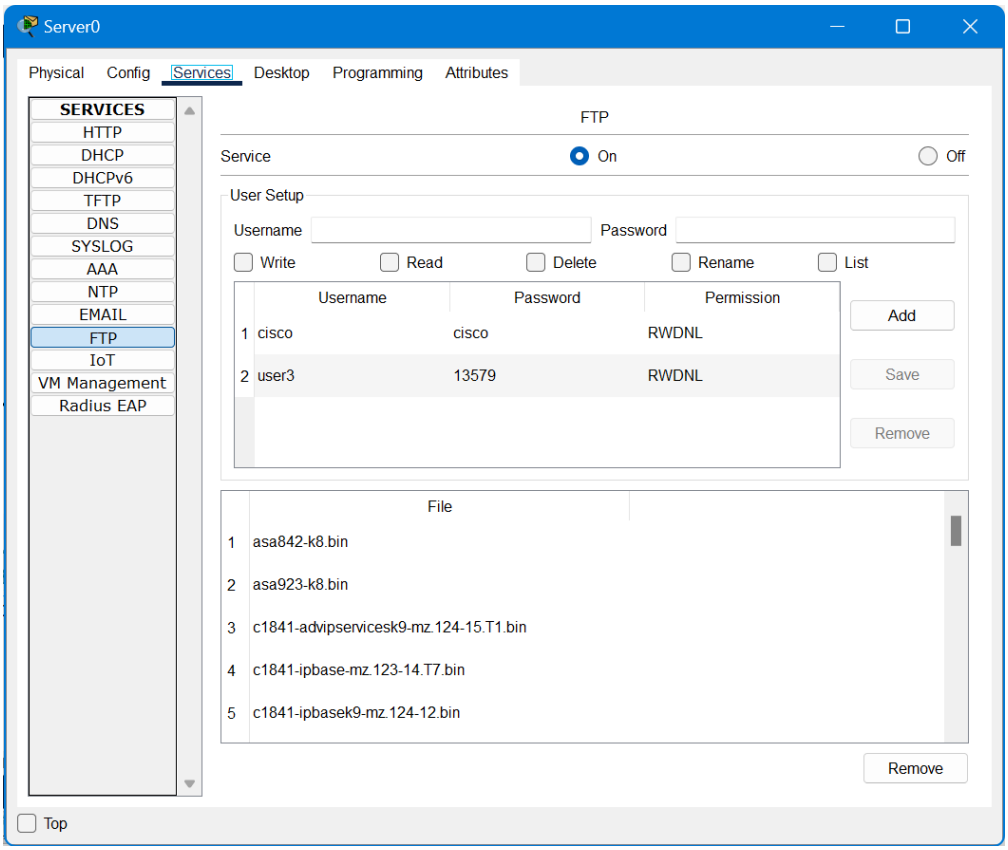

PC0
Physical
Config
Desktop
Programming
Attributes
Reply Mail
X
Send
To:
user1@gmail.com
Subject:
RE: First mail
Mail received from user1
Subject : First mail
From : user1@gmail.com
Sent : Sat Dec 2 2023 22:42:51
Hi!! user1 this side
Top



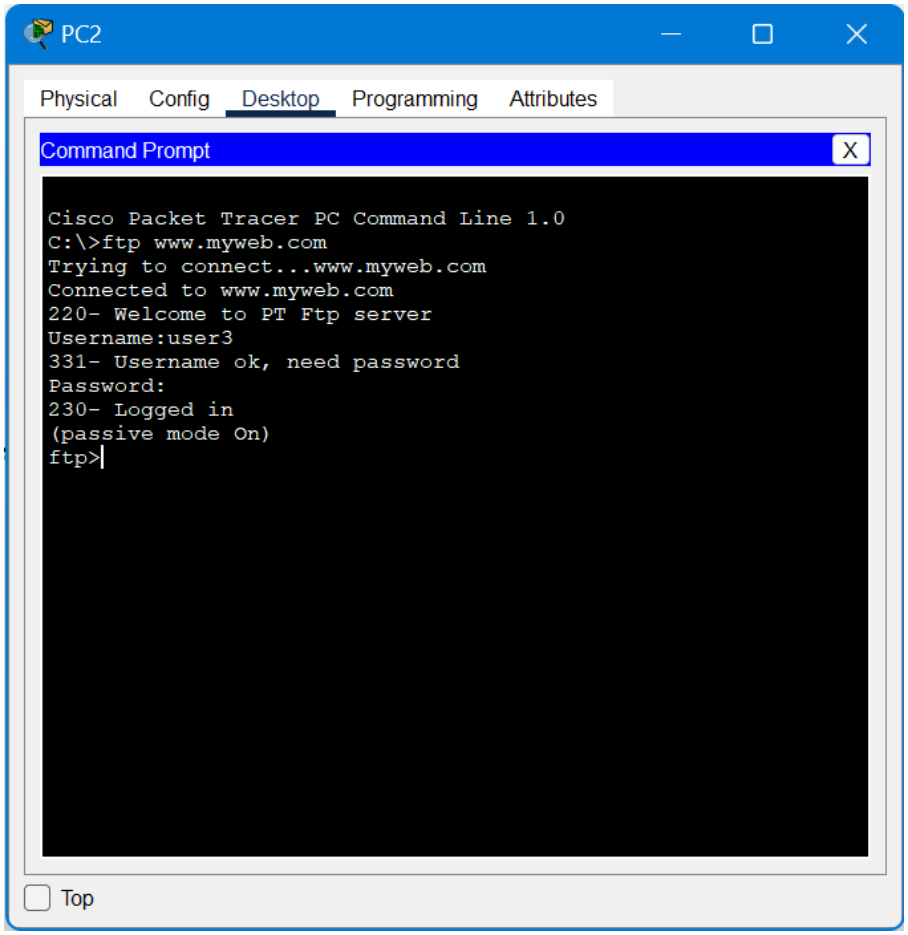
FTP Service

Step 12: Go to Server then Services, switch on the FTP service and create a user for the authorization.

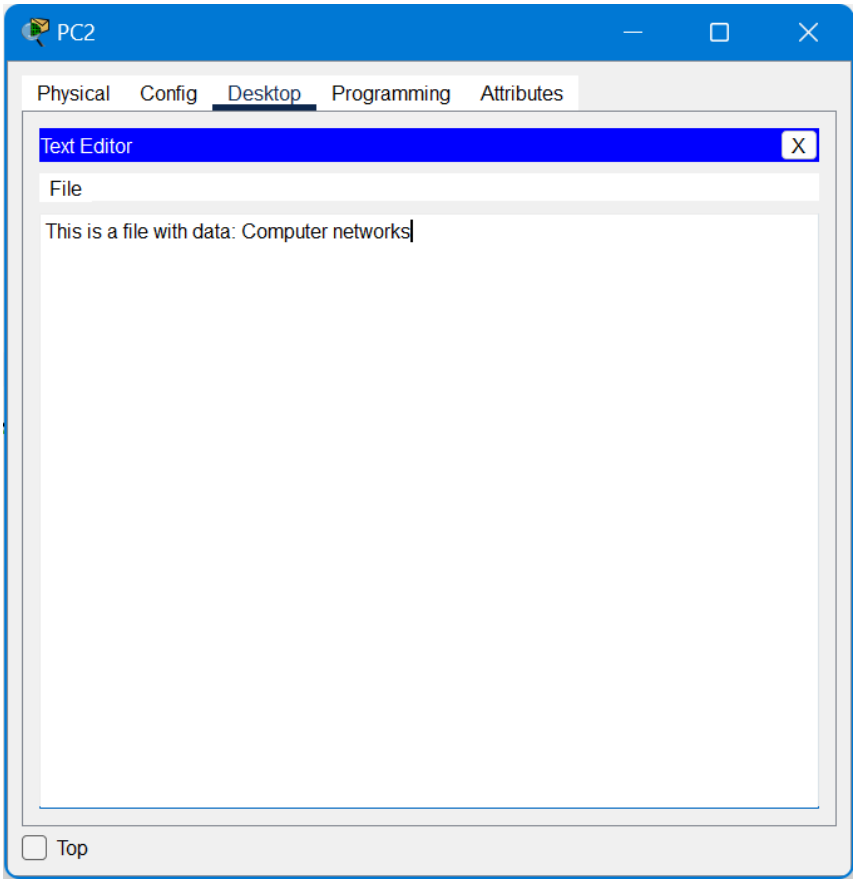


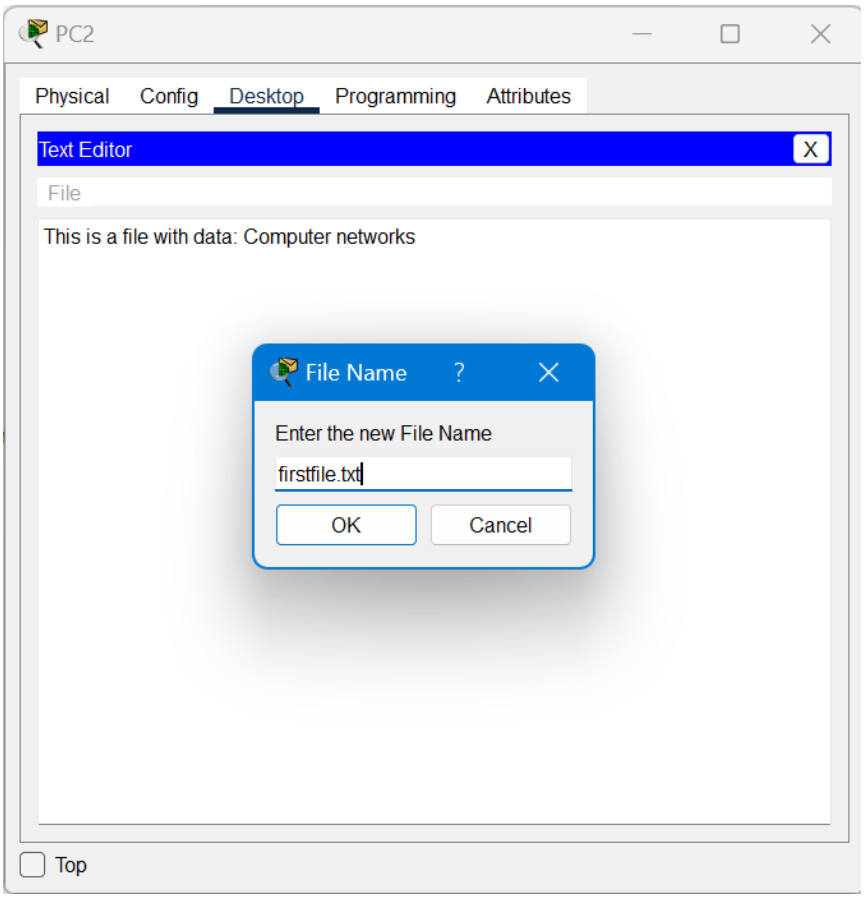


Step 13: Now, for user setup select PC2(FTP Client) and enter ‘ftp www.myweb.com’ in command prompt to get authorised to use FTP service.

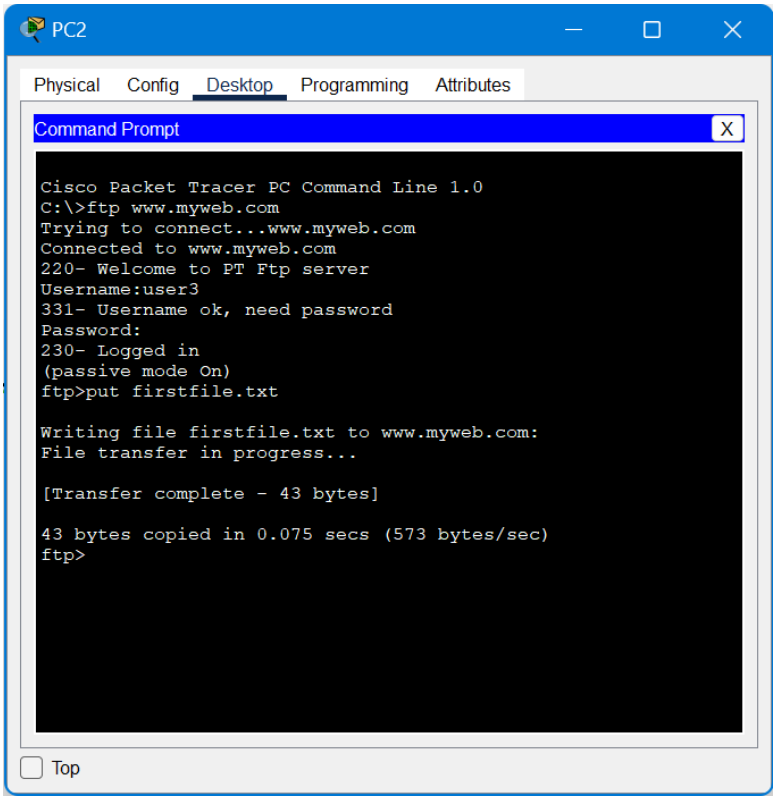


Step 14: Create a ‘firstfile.txt’ using PC2(FTP Client) text editor and then save it.

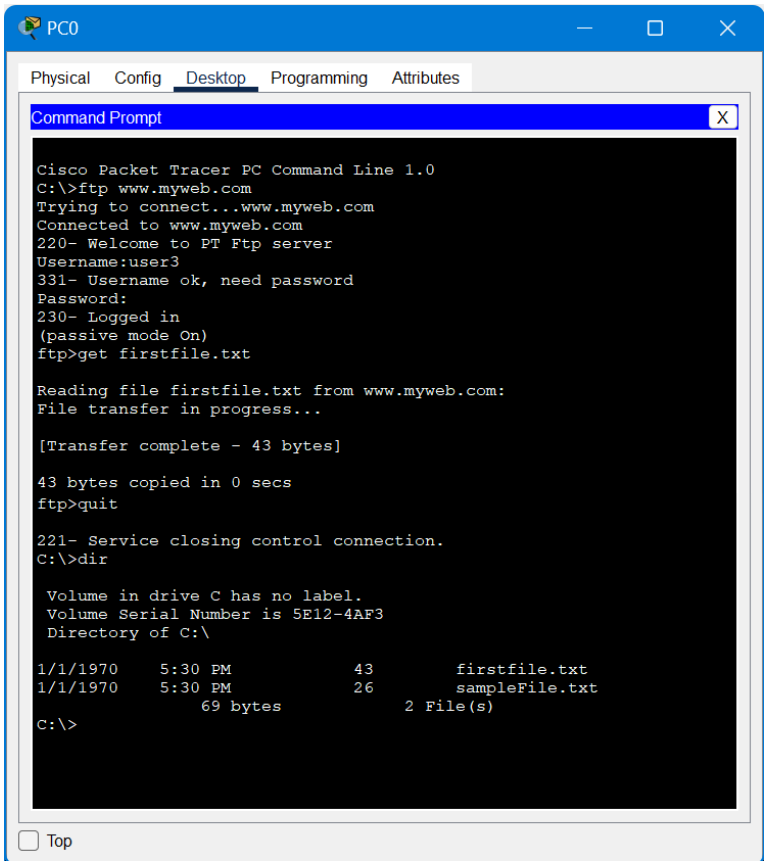




Step 15: Now go to the command prompt of PC2 (FTP Client) and use ‘put firstfile.txt’ command to put the file on the server.



Step 16: Now go to the command prompt of PC0(Web Client) and use get command to get the file from the server.



Practical No. 8

Aim: To implement the Network Address Translation (NAT) using CISCO Packet Tracer.

Theory

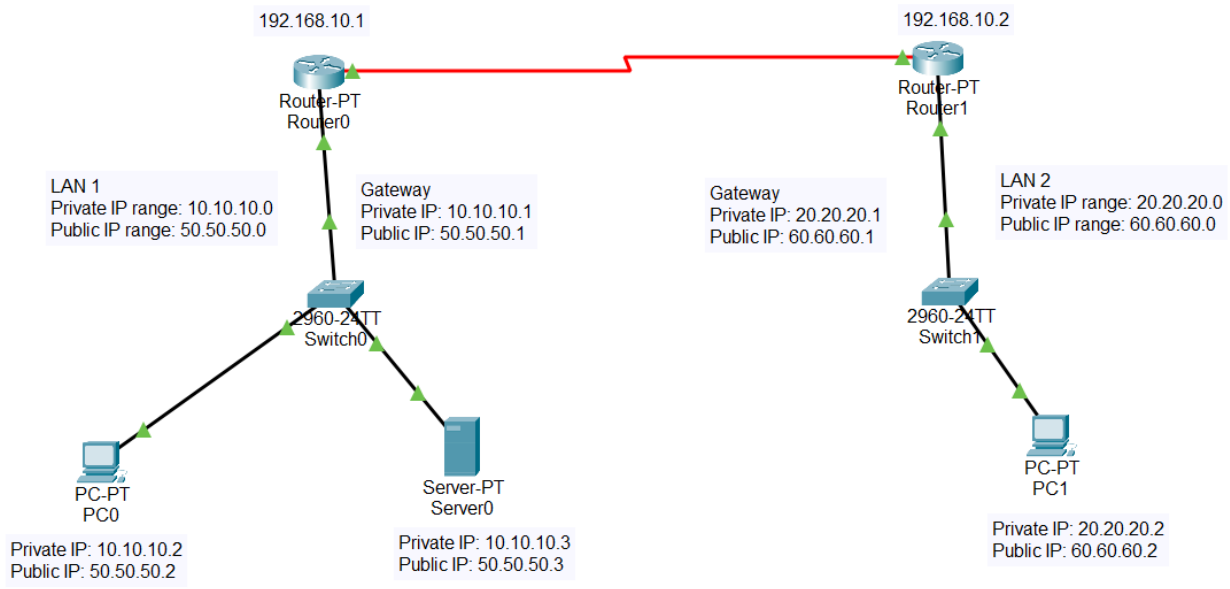
Network Address Translation: To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Working of NAT: Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address. If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Limitations of NAT

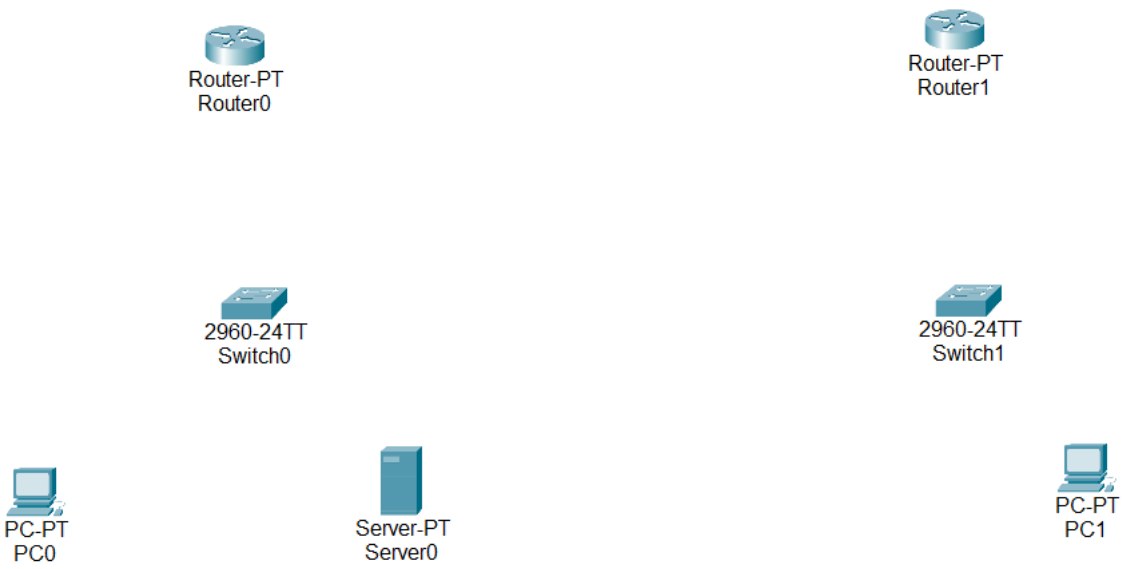
1. Translation results in switching path delays.
2. Certain applications will not function while NAT is enabled.
3. Complicates tunneling protocols such as IPsec.
4. Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

Topology

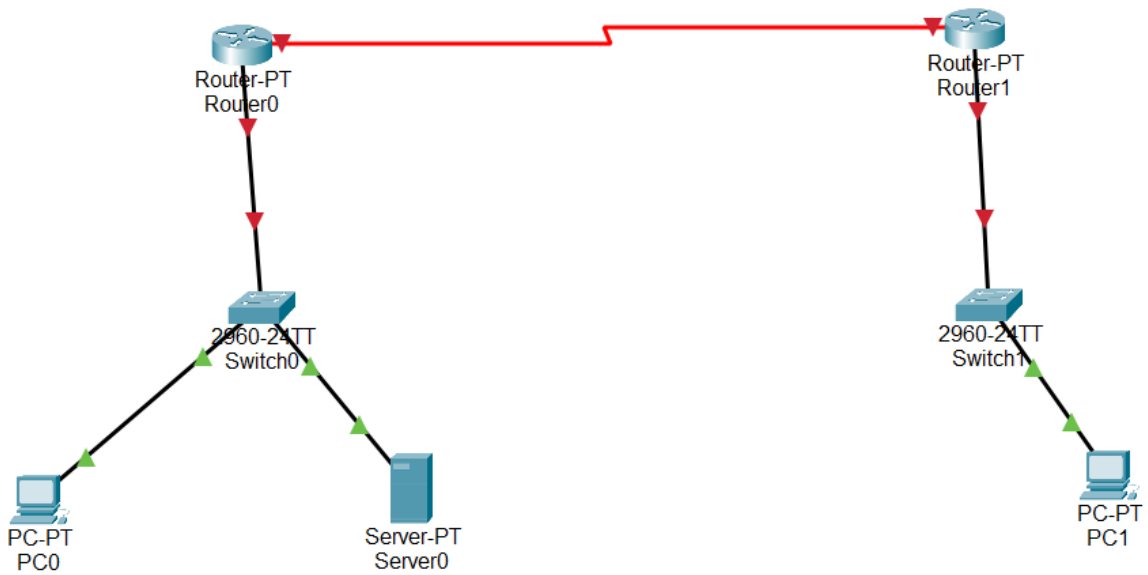


Steps to execute

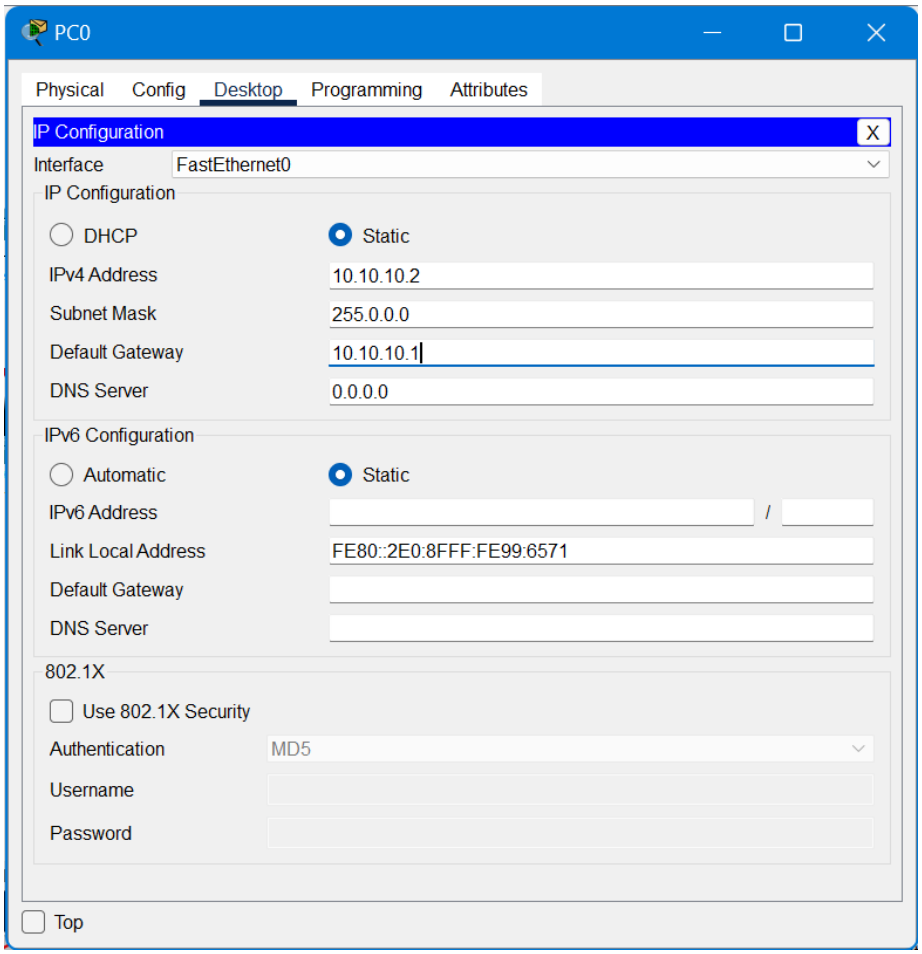
Step 1: Drag the elements required in the workplace.

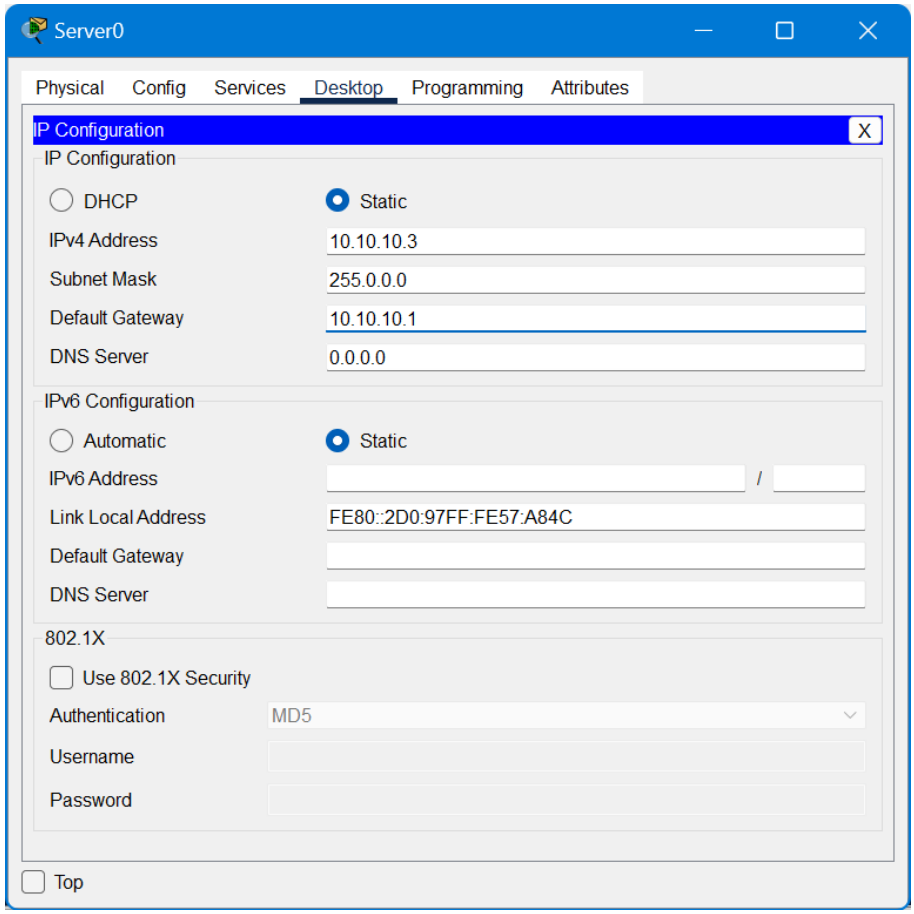


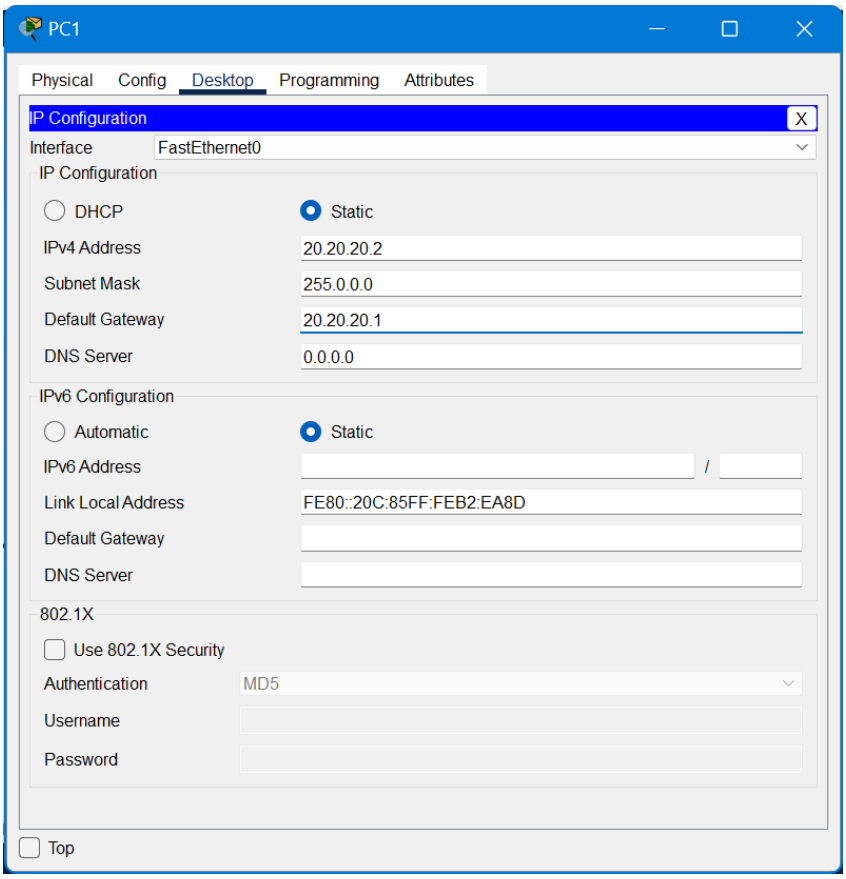
Step 2: Connect all devices using suitable wires.



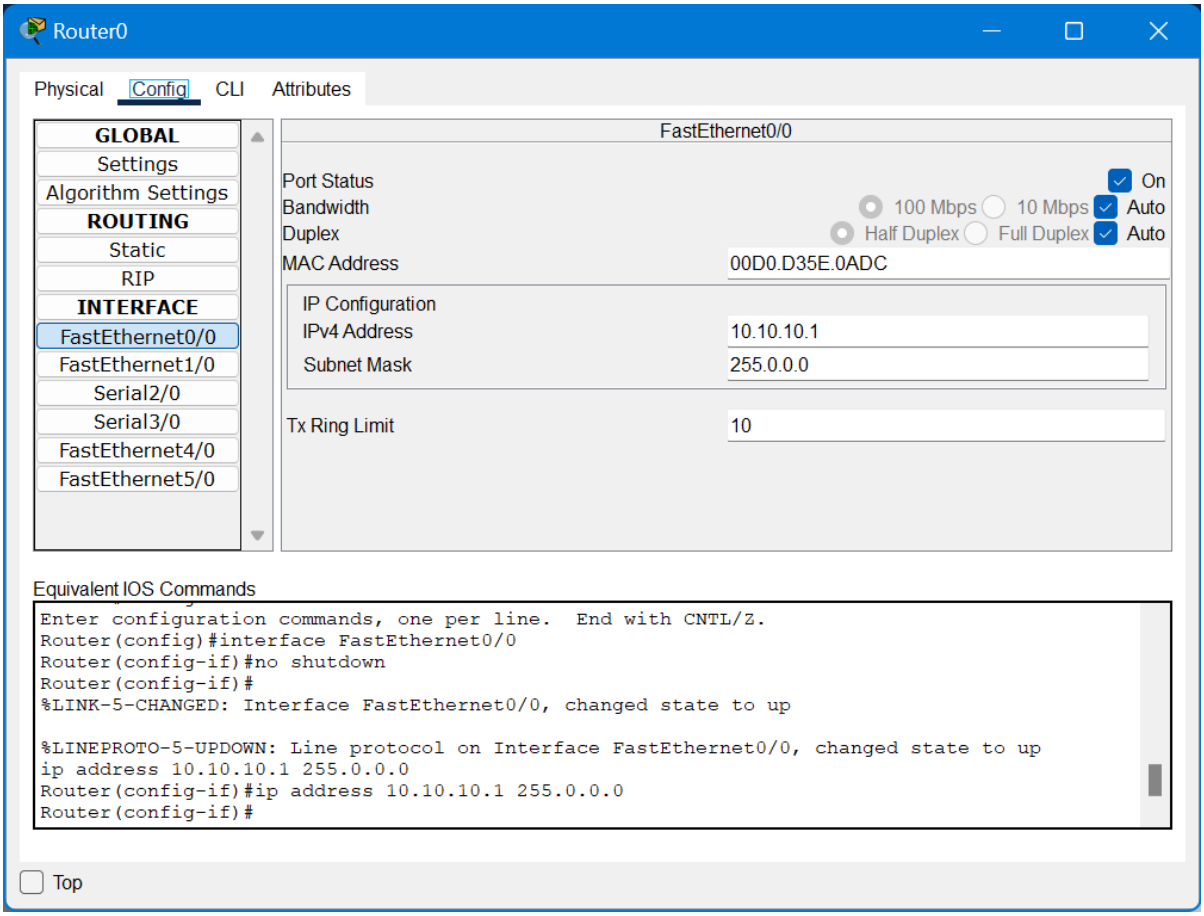
Step 3: Configure PC0, Server0 and PC1.

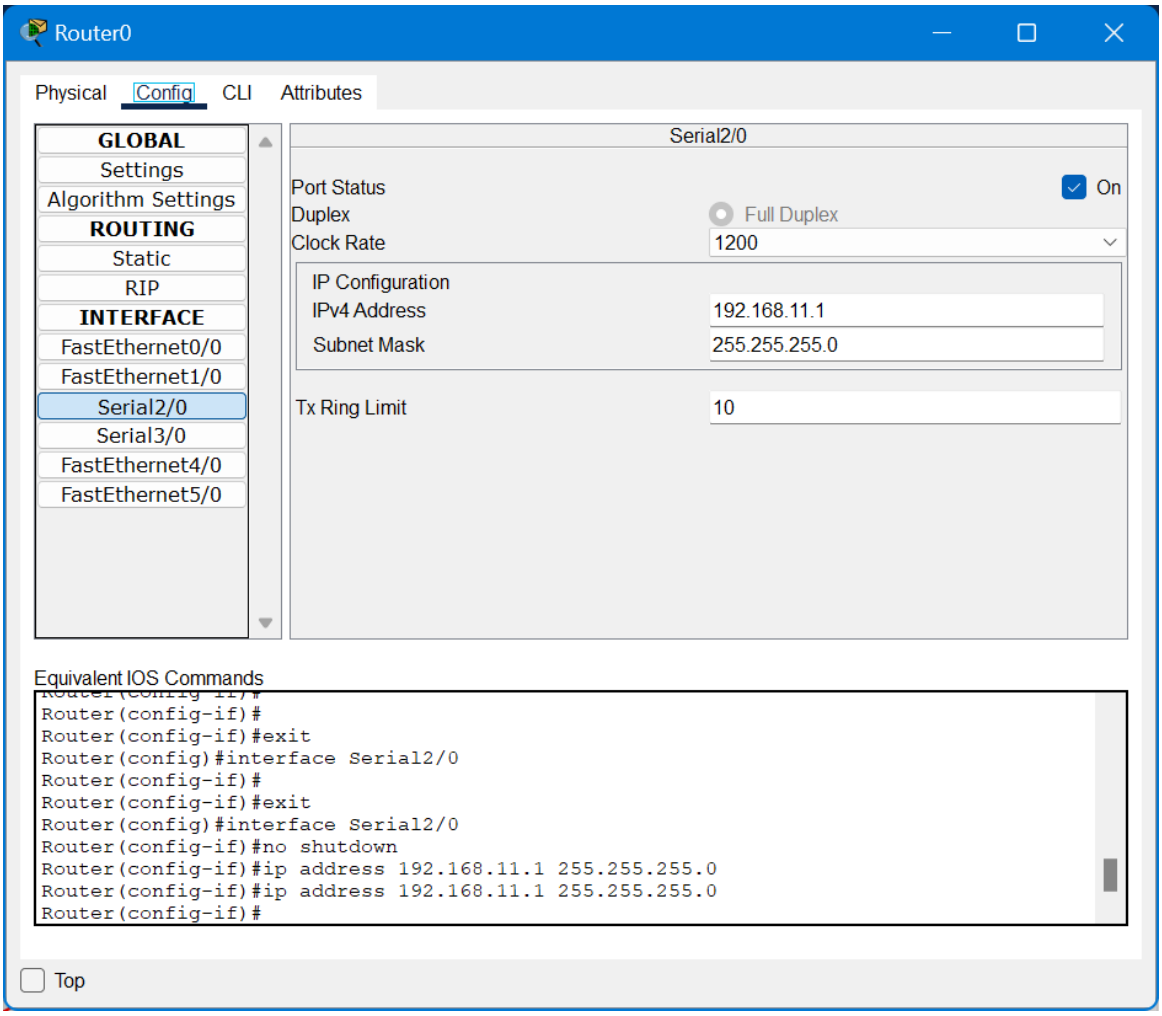

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
10.10.10.2
Subnet Mask
255.0.0.0
Default Gateway
10.10.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2E0:8FFF:FE99:6571
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

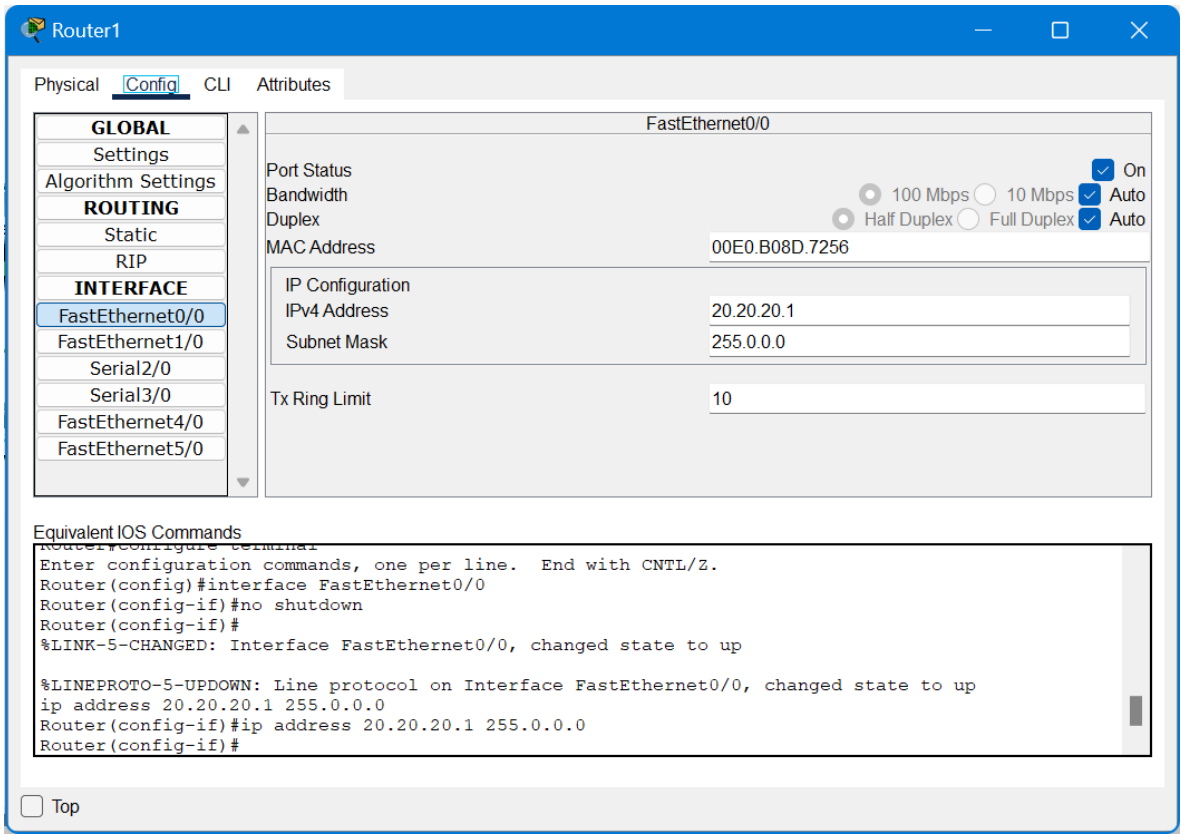

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
10.10.10.3
Subnet Mask
255.0.0.0
Default Gateway
10.10.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:97FF:FE57:A84C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

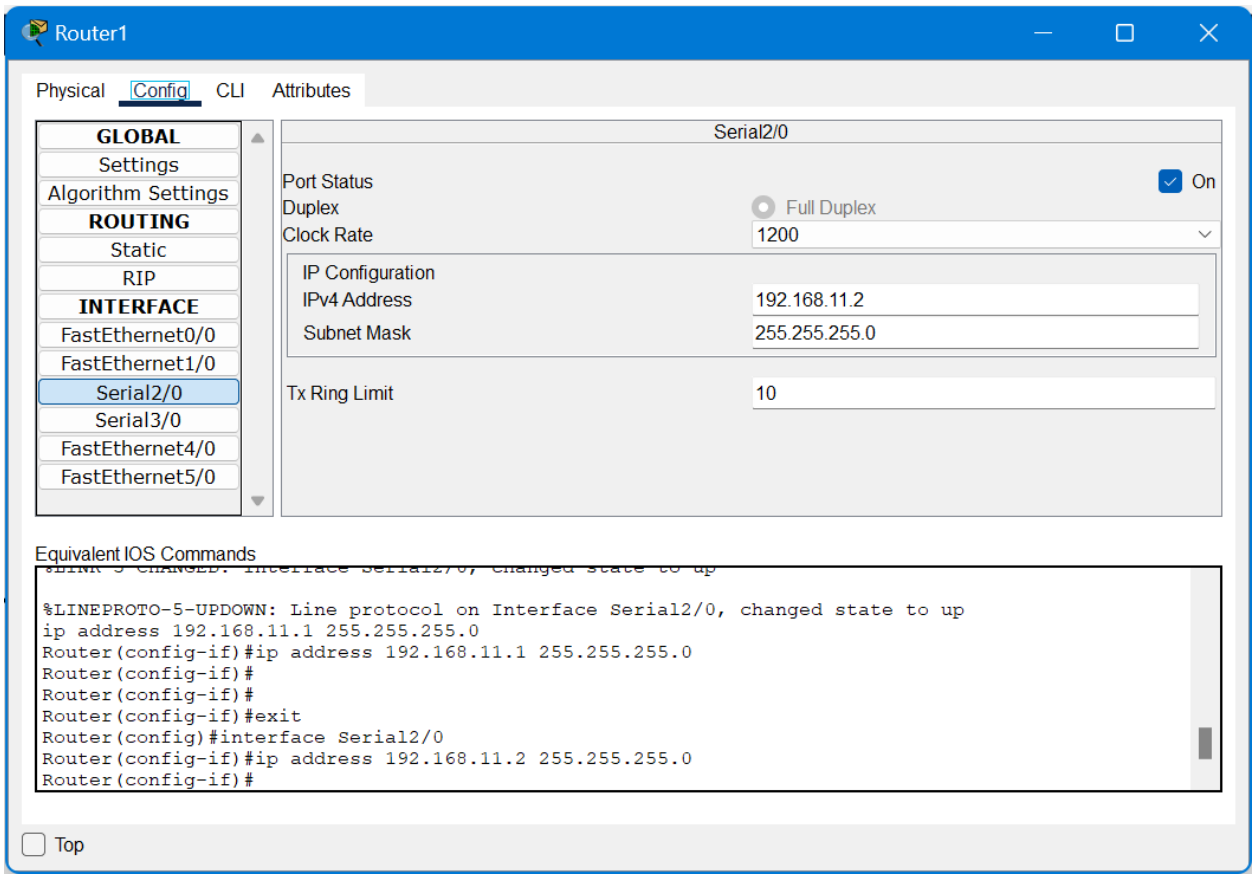


Step 4: Configure FastEthernet0/0 and Serial2/0 in both routers.

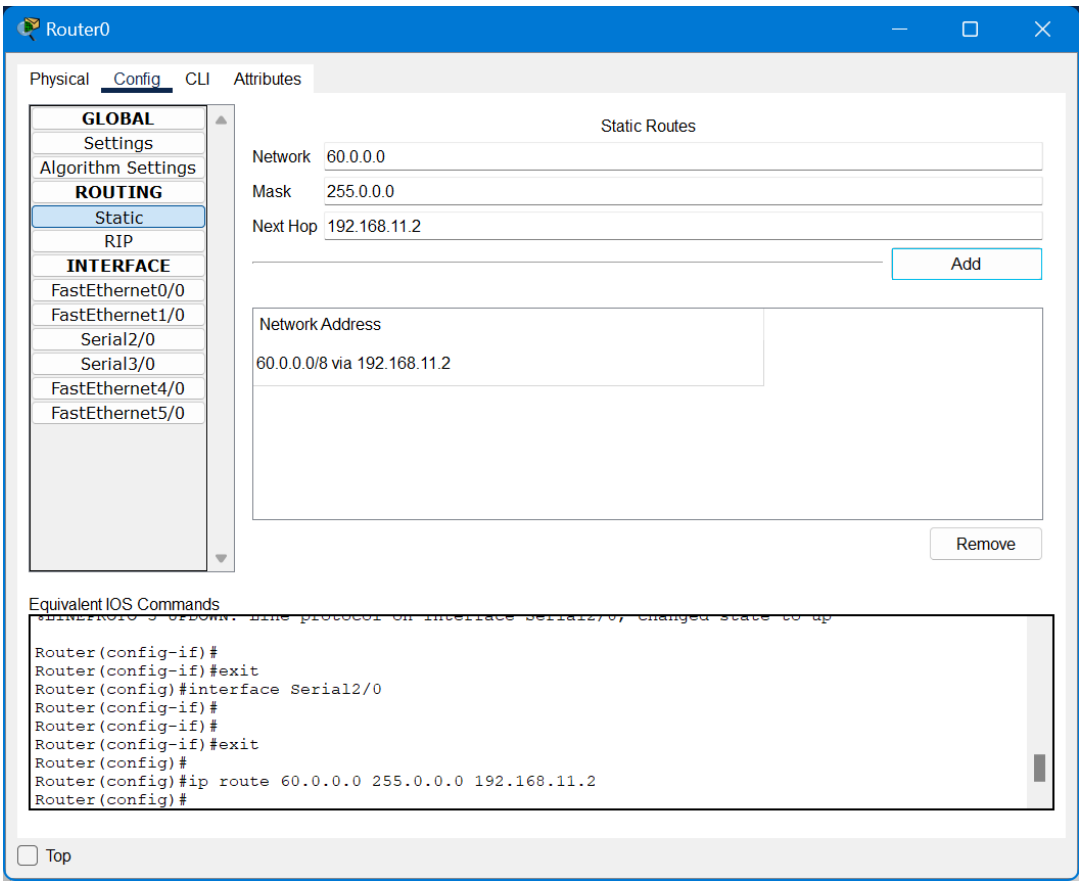


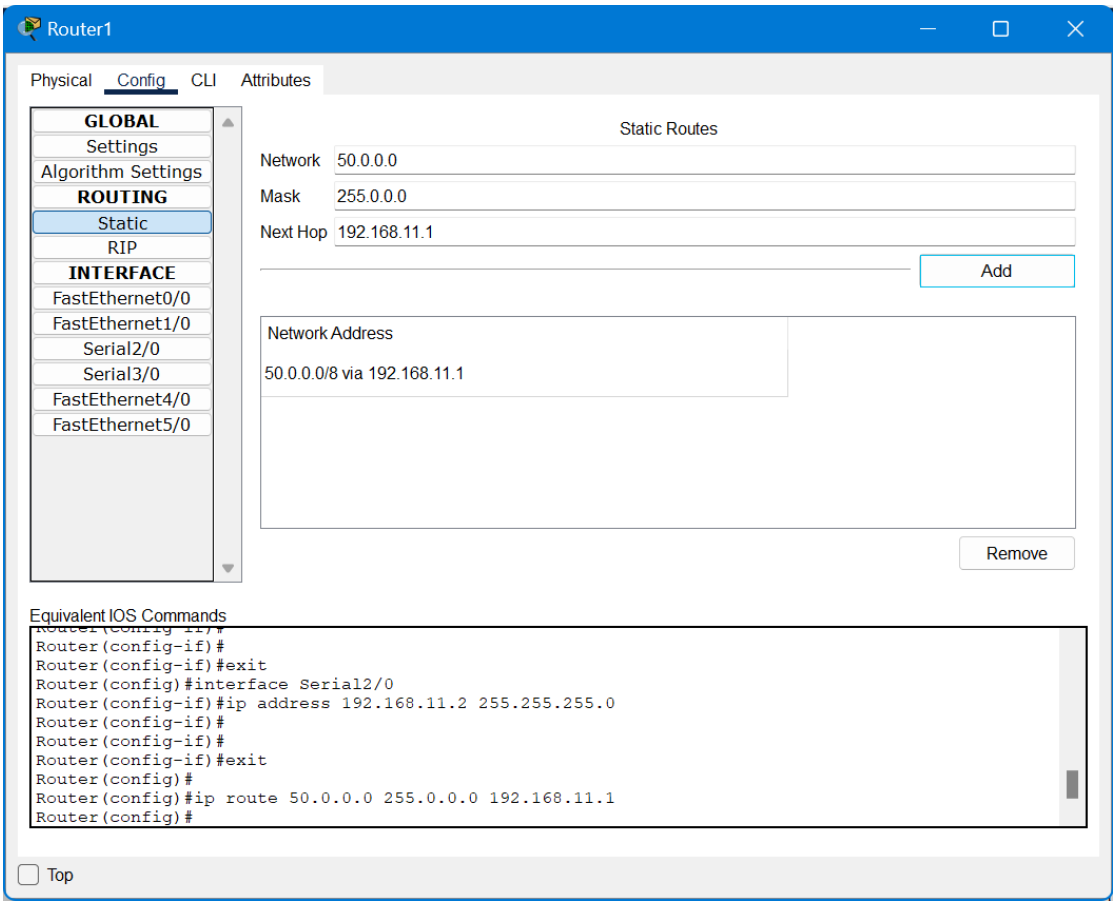

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
192.168.11.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.11.1 255.255.255.0
Router(config-if)#ip address 192.168.11.1 255.255.255.0
Router(config-if)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.B08D.7256
IP Configuration
IPv4 Address
20.20.20.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
ip address 20.20.20.1 255.0.0.0
Router(config-if)#ip address 20.20.20.1 255.0.0.0
Router(config-if)#
Top

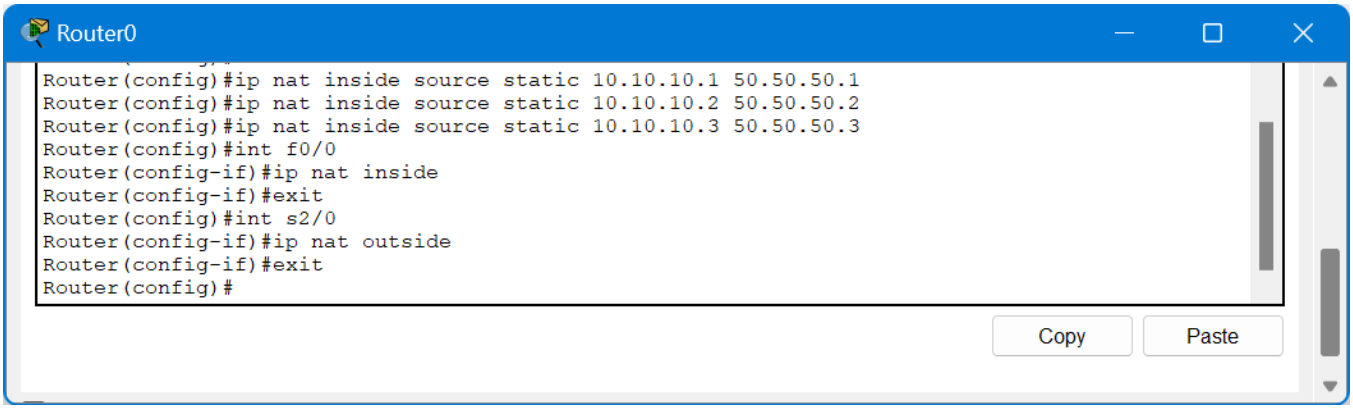


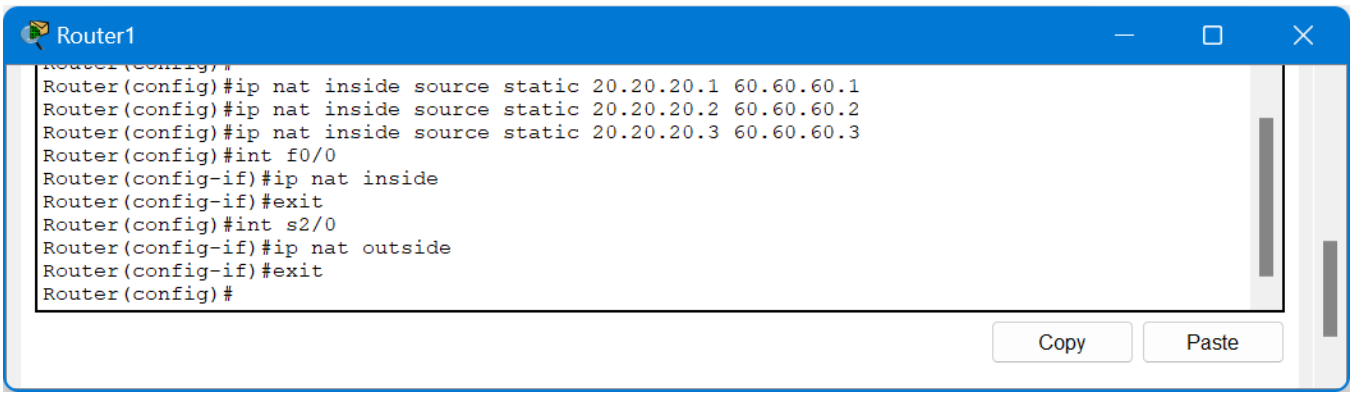
Step 5: Now, assign static routes for both routers by allocating network, mask and their next hop address in Static Routing.



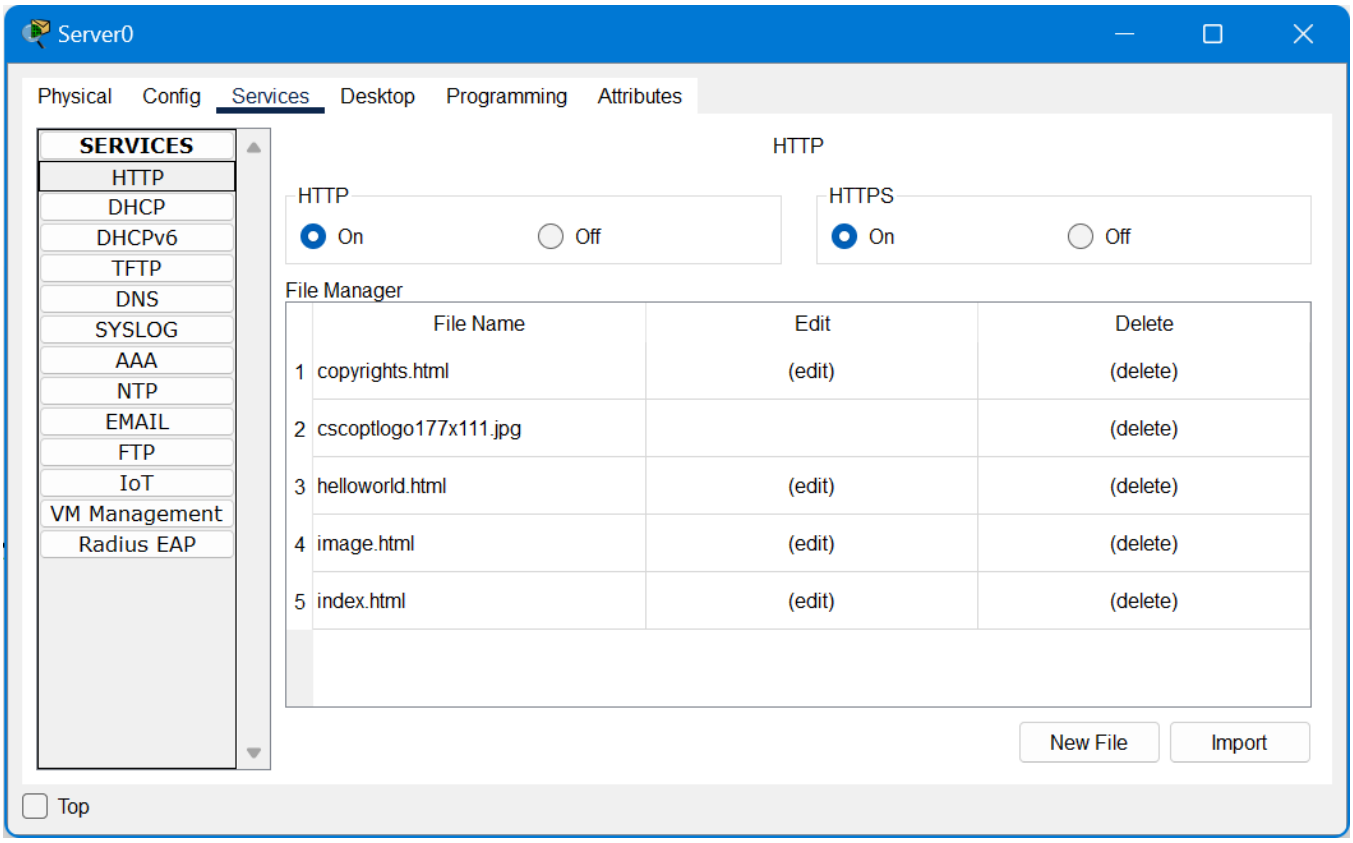


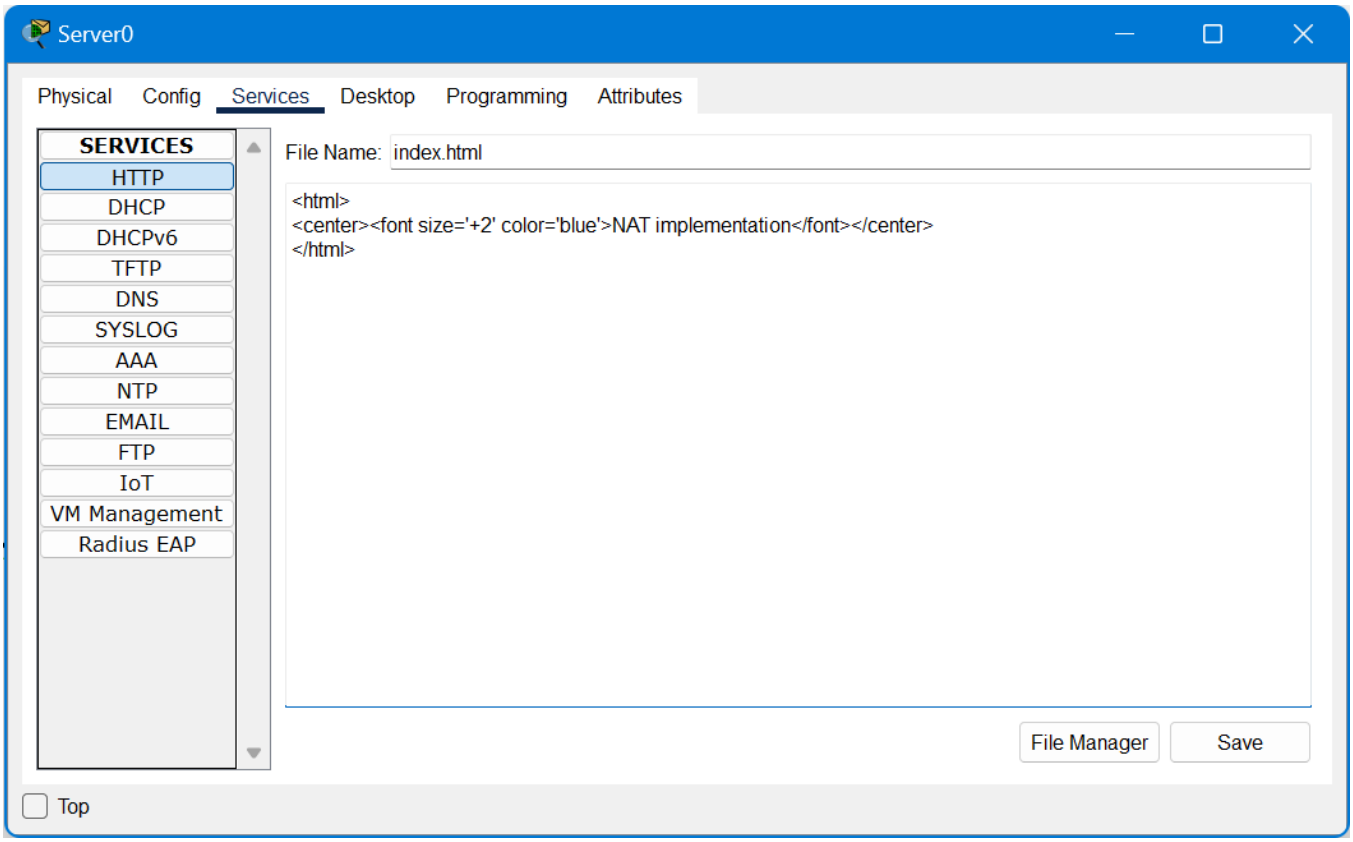
Step 6: To implement NAT, go to router's Command Line Interface (CLI) and assign all the given commands to set public and private IP addresses.



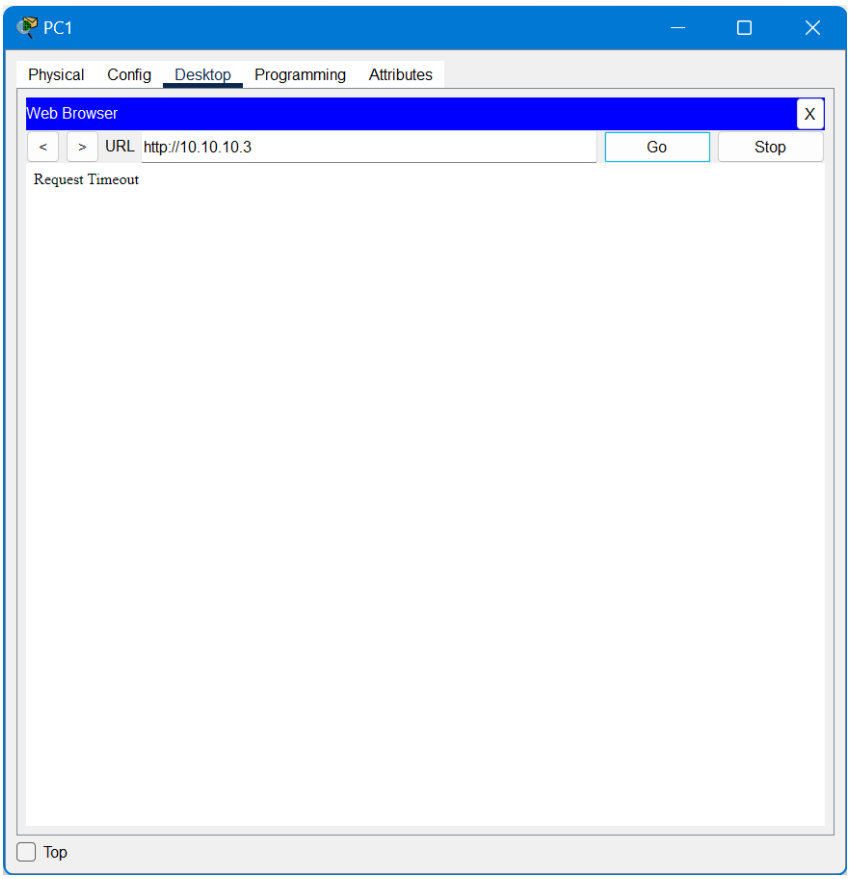


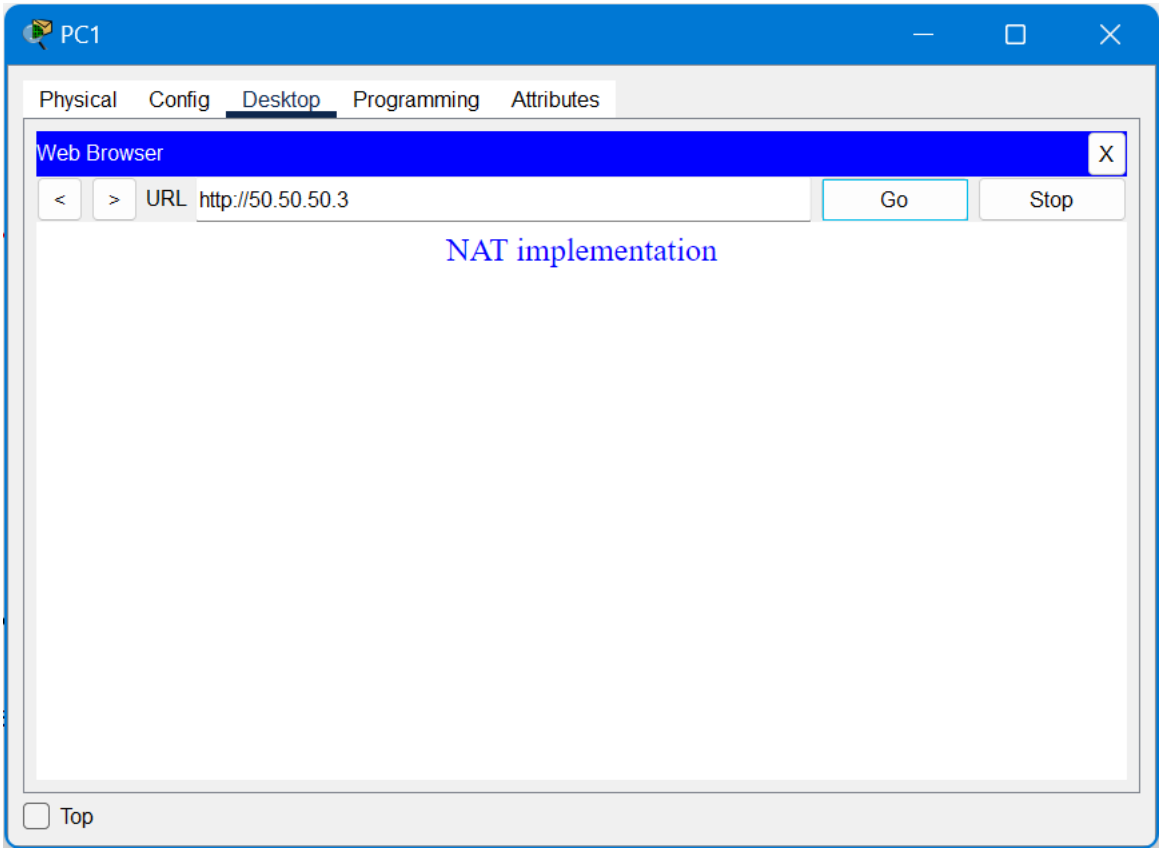
Step 7: To test the NAT working, go to Server's services, then edit the index.html file in the HTTP service.





Step 8: Go to PC1, open it's web browser and search for private IP of the server '10.10.10.3'. It will show Request Timeout as Server0 is present outside the network 2. But if you try to search for public IP of the Server0, then it will work.





Commands to check connectivity

PC0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 60.60.60.2

Pinging 60.60.60.2 with 32 bytes of data:

Reply from 60.60.60.2: bytes=32 time=1ms TTL=126
Reply from 60.60.60.2: bytes=32 time=1ms TTL=126
Reply from 60.60.60.2: bytes=32 time=1ms TTL=126
Reply from 60.60.60.2: bytes=32 time=1ms TTL=126

Ping statistics for 60.60.60.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

PC1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 50.50.50.2

Pinging 50.50.50.2 with 32 bytes of data:

Reply from 50.50.50.2: bytes=32 time=1ms TTL=126
Reply from 50.50.50.2: bytes=32 time=1ms TTL=126
Reply from 50.50.50.2: bytes=32 time=1ms TTL=126
Reply from 50.50.50.2: bytes=32 time=1ms TTL=126

Ping statistics for 50.50.50.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Practical No. 9

Aim: To implement subnetting in small networks using CISCO Packet Tracer.

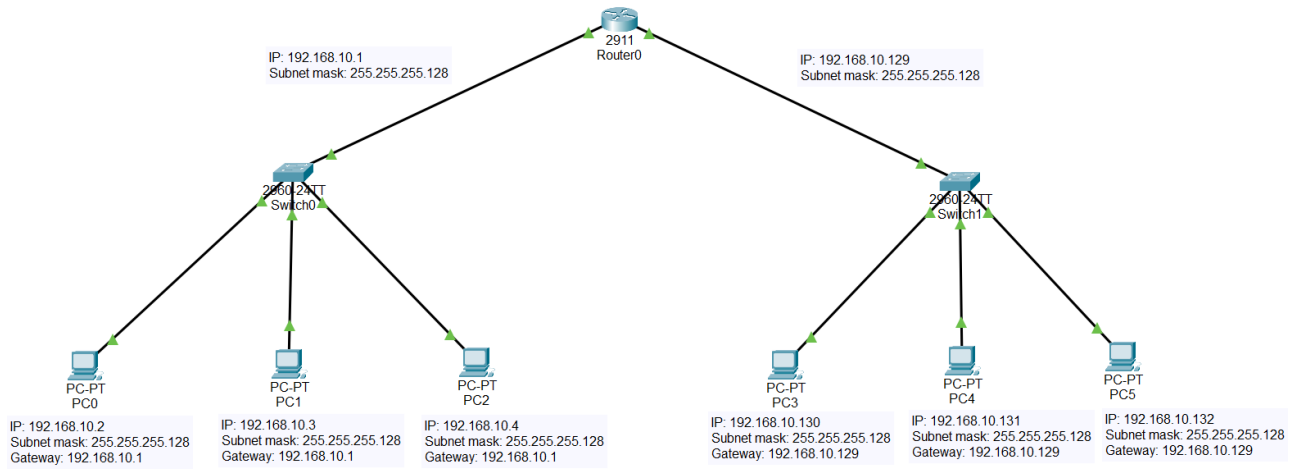
Theory

Subnetting: Subnetting is a combination of two words i.e. Sub and Netting. Here Sub word means Substitute and netting word means Network. The Substitute Network created for a function to happen is known as Subnetting. Here, Substitute Network does not mean a new network is created. A full piece of network is broken into small pieces and each piece a different is assigned. Subnet is the name given to piece of the broken network or can also be called as the Substitute network is known as Subnet. Subnets are the legal small parts of IP (Internet Protocol) Addressing process Subnetting should be done in such a way that network does not gets affected. This means that we can divide the network into different parts but all when put together should perform the same task when done before splitting in to small parts. Subnets reduce the need for traffic to use unnecessary routes, which speeds up the network. To help with the lack of IP addresses on the internet, subnets were developed. The way IP addresses are constructed makes it relatively simple for Internet routers to find the right network to route data into. However, in a Class A network (for instance), there could be millions of connected devices, and it could take some time for the data to find the right device. This is why subnetting comes in handy: subnetting narrows down the IP address to usage within a range of devices. Because an IP address is limited to indicating the network and the device address, IP addresses cannot be used to indicate which subnet an IP packet should go to. Routers within a network use something called a subnet mask to sort data into subnetworks.

Calculation

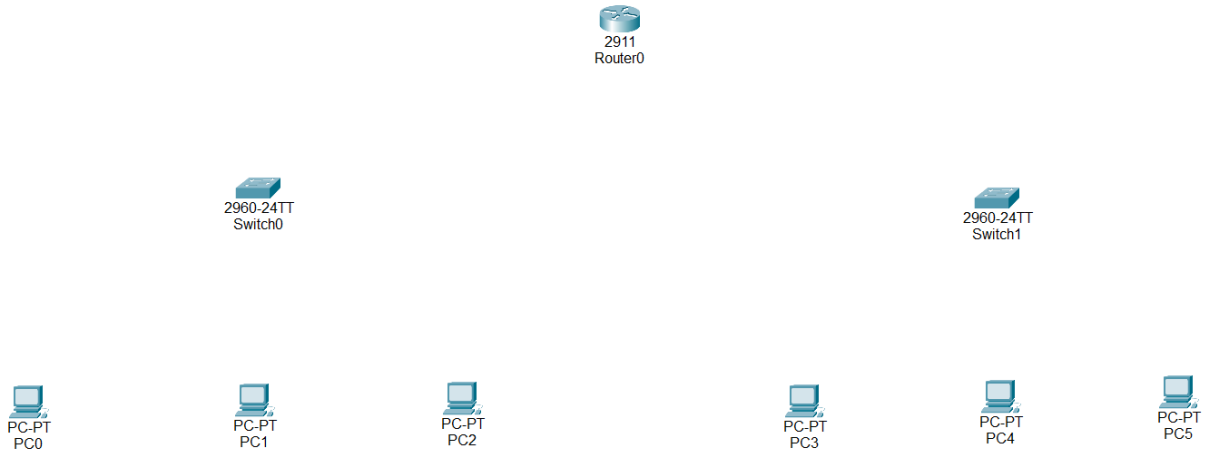
Network Address is 192.168.10.0
And mask is /25
As the network represent that the current network address lie in C class so the default subnet is 255.255.255.0 but the given mask is /25.
The binary form of subnet mask is 11111111.11111111.11111111.0000000 but as the mask is /25.
One extra one will also there and now the current subnet mask will be 11111111.11111111.11111111.1000000 = 255.255.255.128
No of subnets is equal to $2^1 = 2$
So, the network will consist of two subnet 0 and 1.
Total no hosts is equal to $2^7 = 128$
The valid subnets are 0 - 127 = Subnet 0 (255.255.255.0)
128 - 255 = Subnet 1 (255.255.255.128)
The 0,128 is used for the network id and 127, 255 is used for the Broadcasting.

Topology

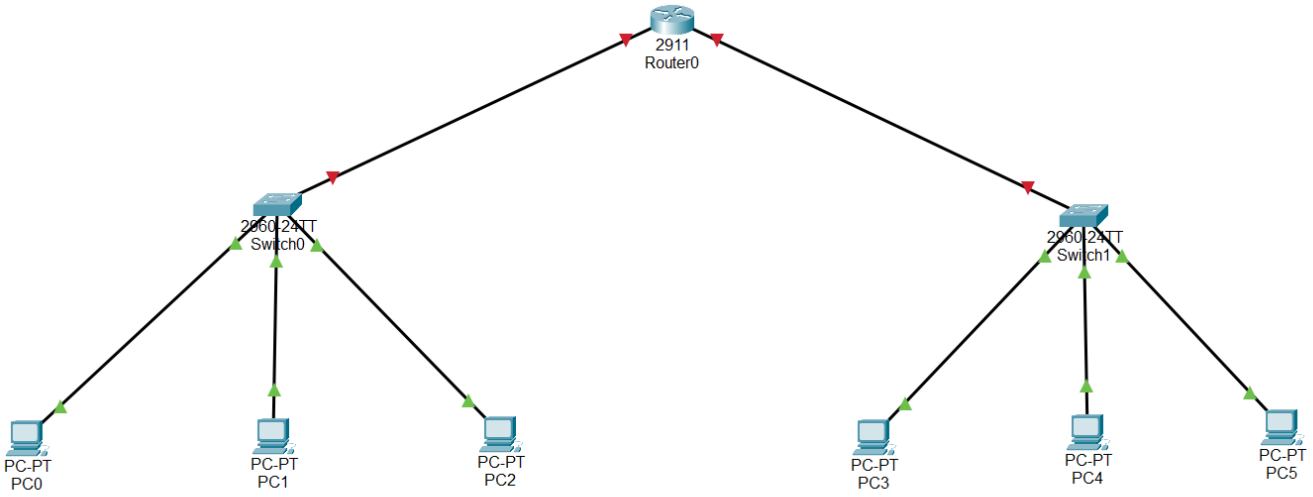


Steps to execute

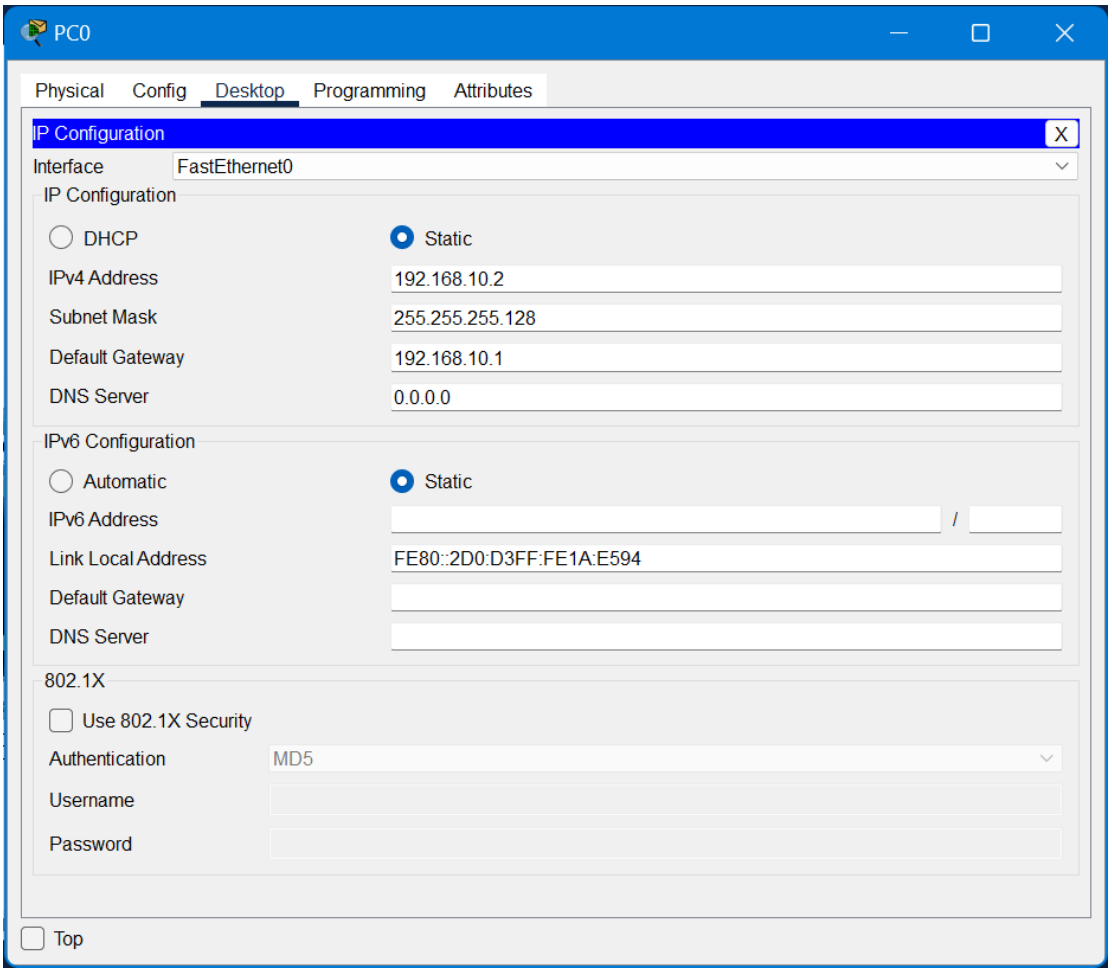
Step 1: Drag the elements required in the workplace.

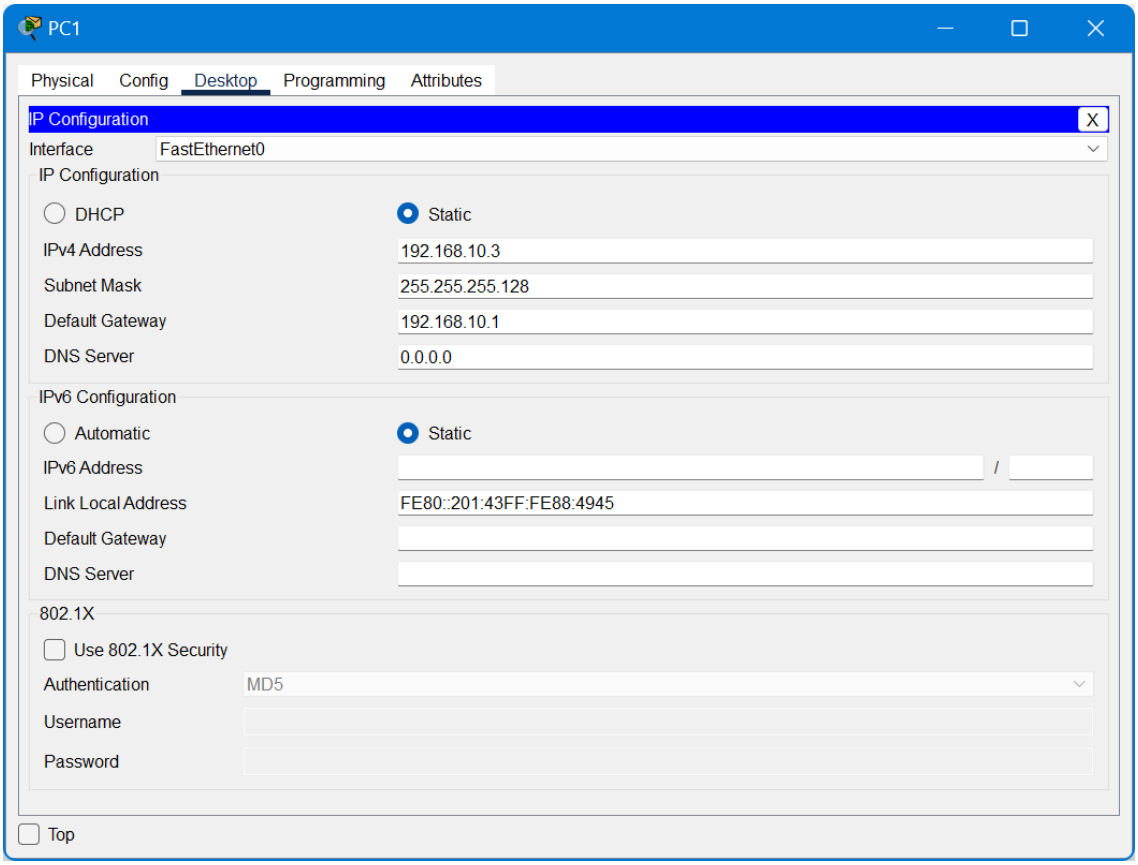


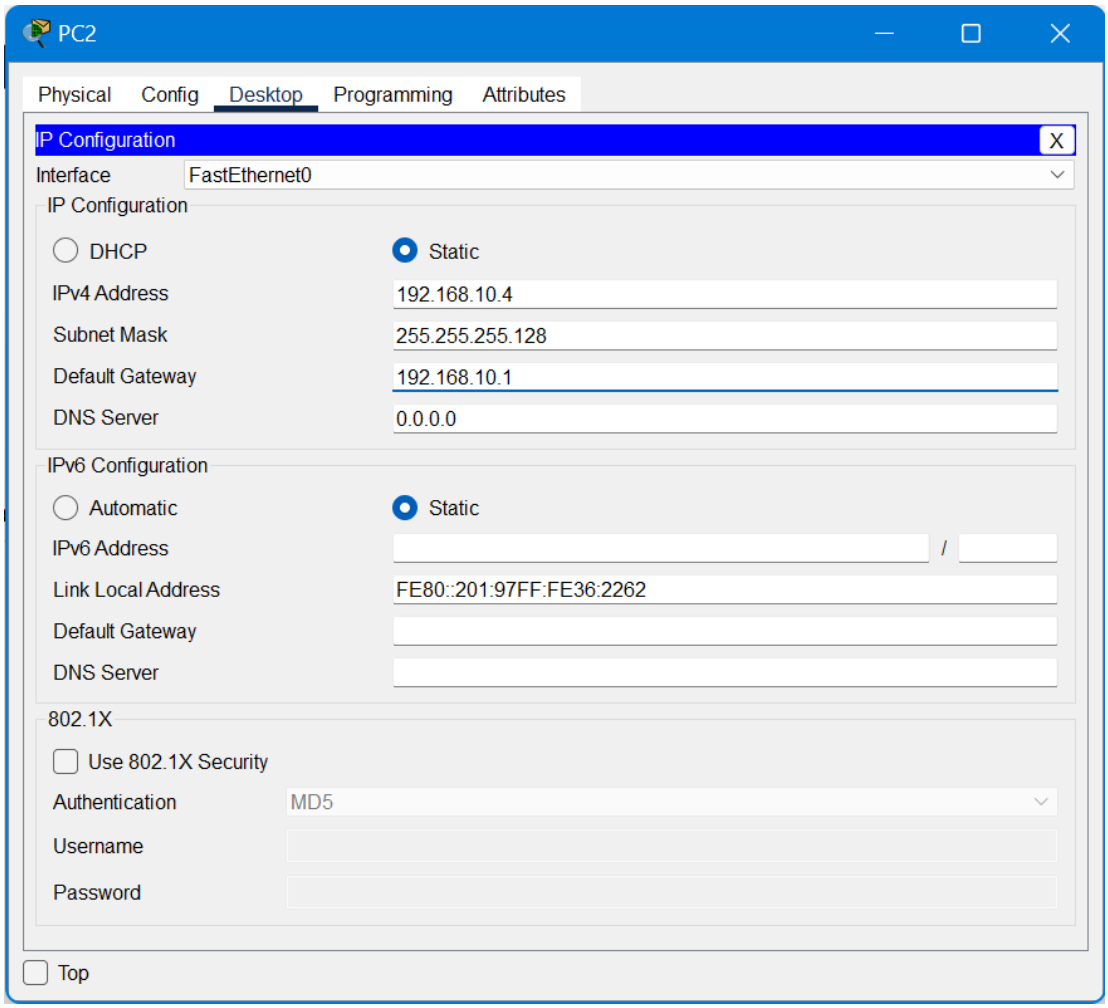
Step 2: Connect the devices with straight through wire.

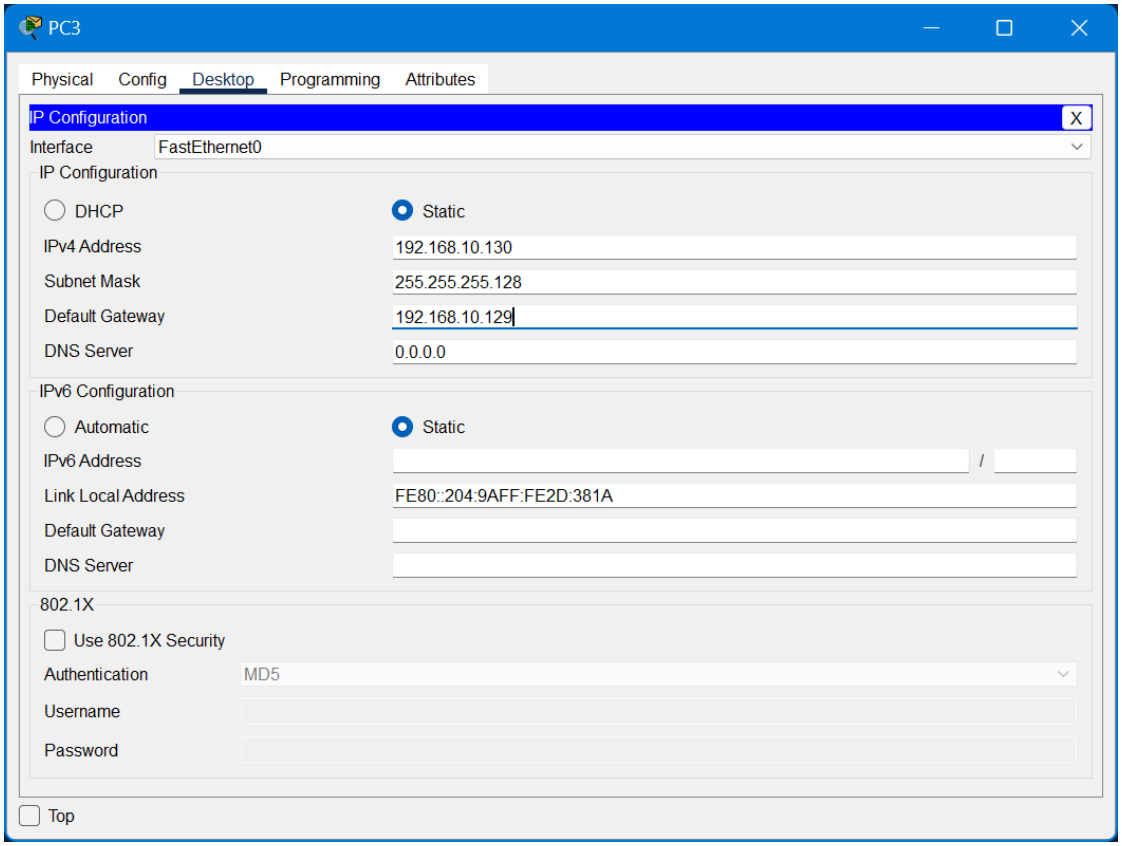


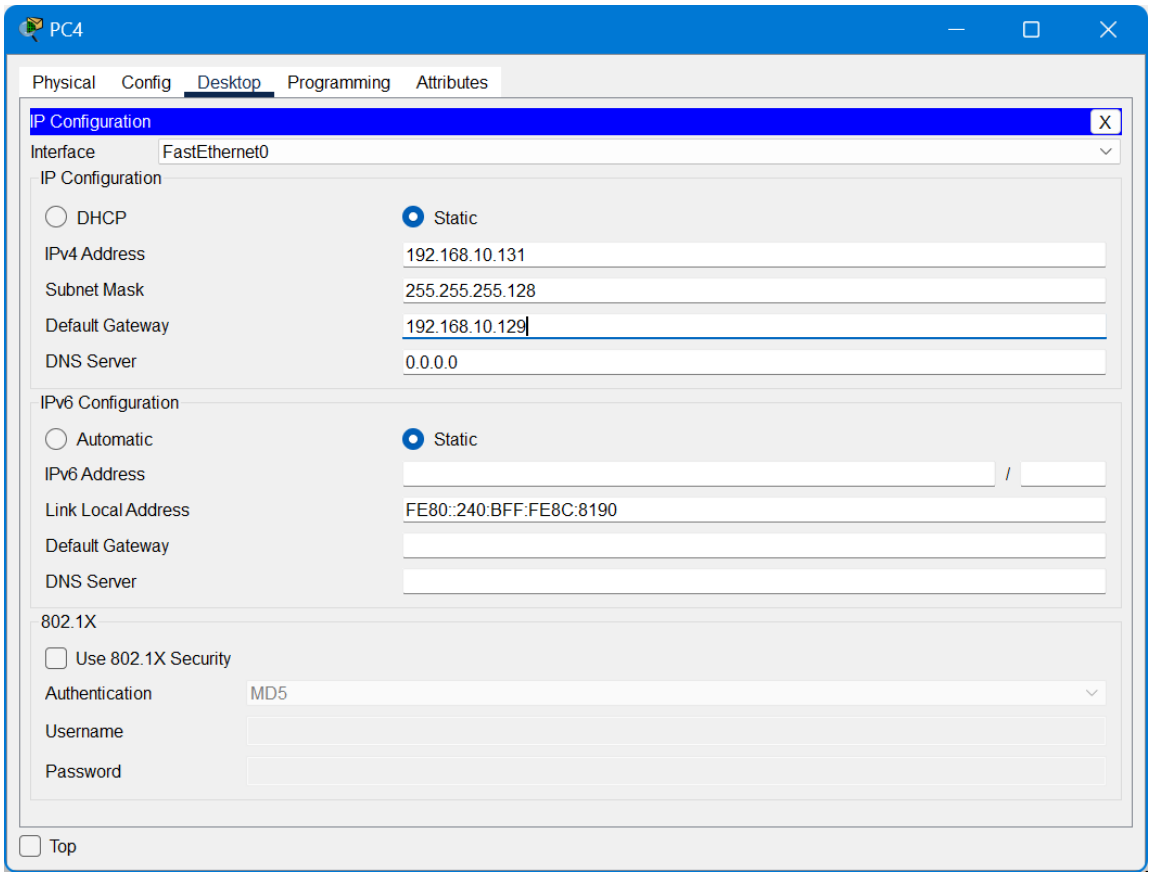
Step 3: Now assign the IP address, subnet mask and gateway address of all the PC's.

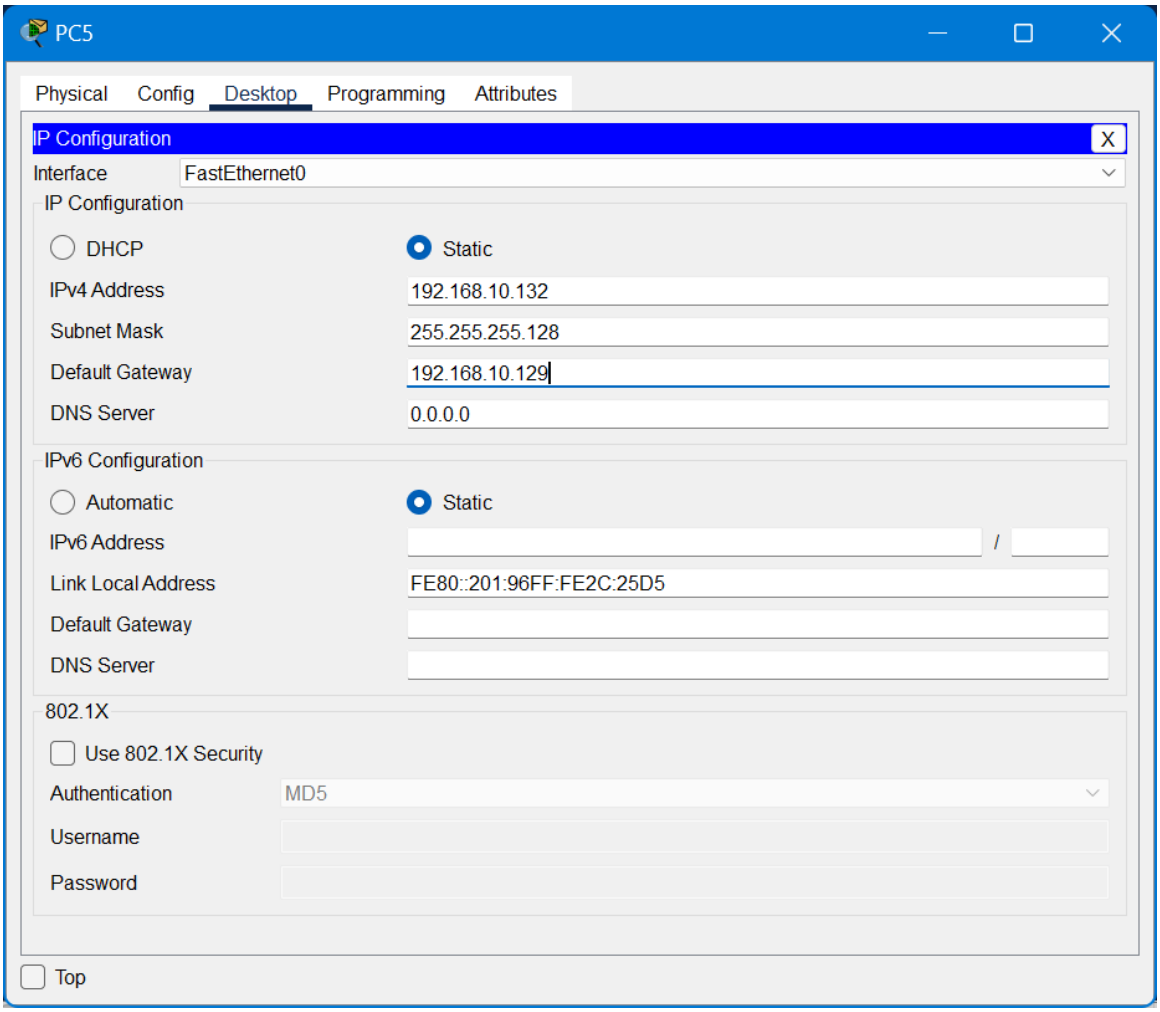

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.2
Subnet Mask
255.255.255.128
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:D3FF:FE1A:E594
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.3
Subnet Mask
255.255.255.128
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:43FF:FE88:4945
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

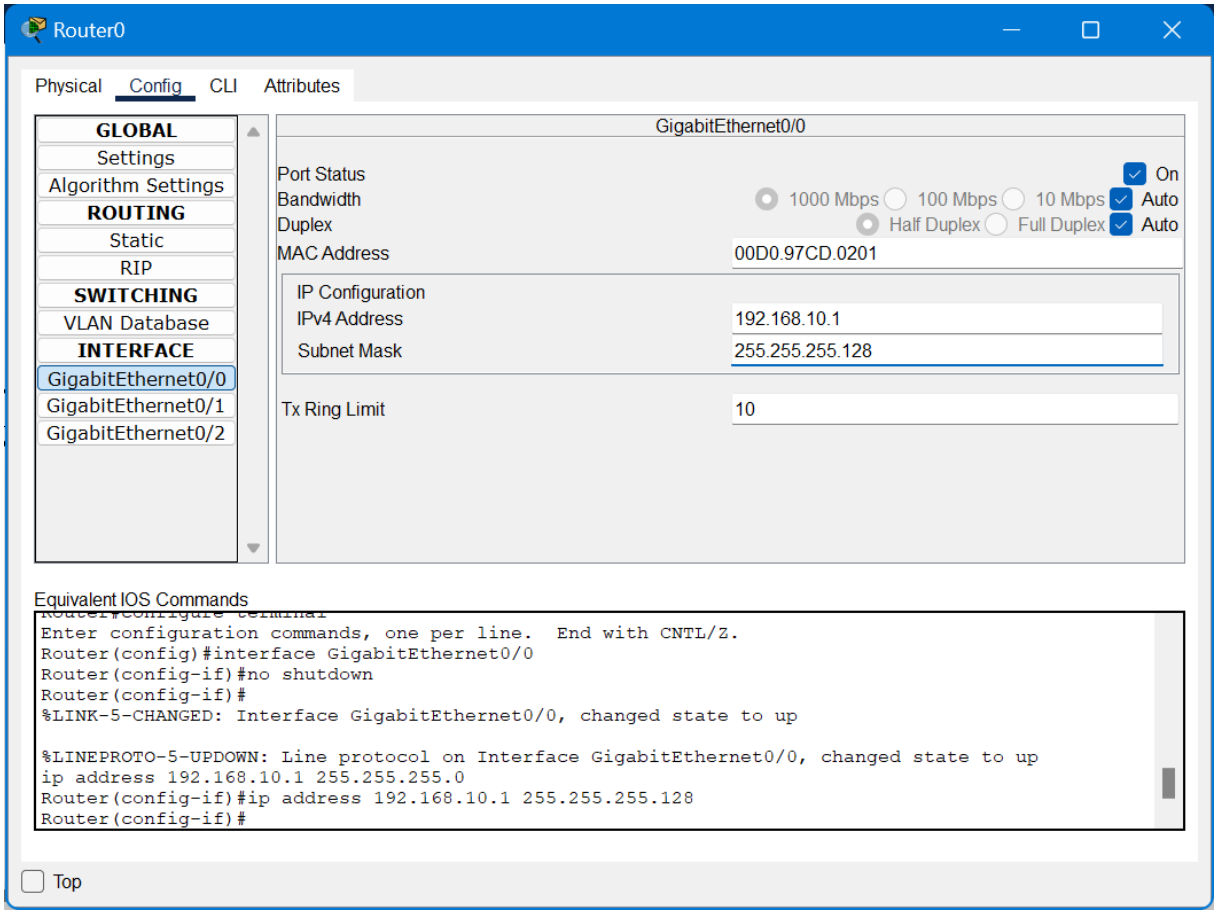

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.4
Subnet Mask
255.255.255.128
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE36:2262
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

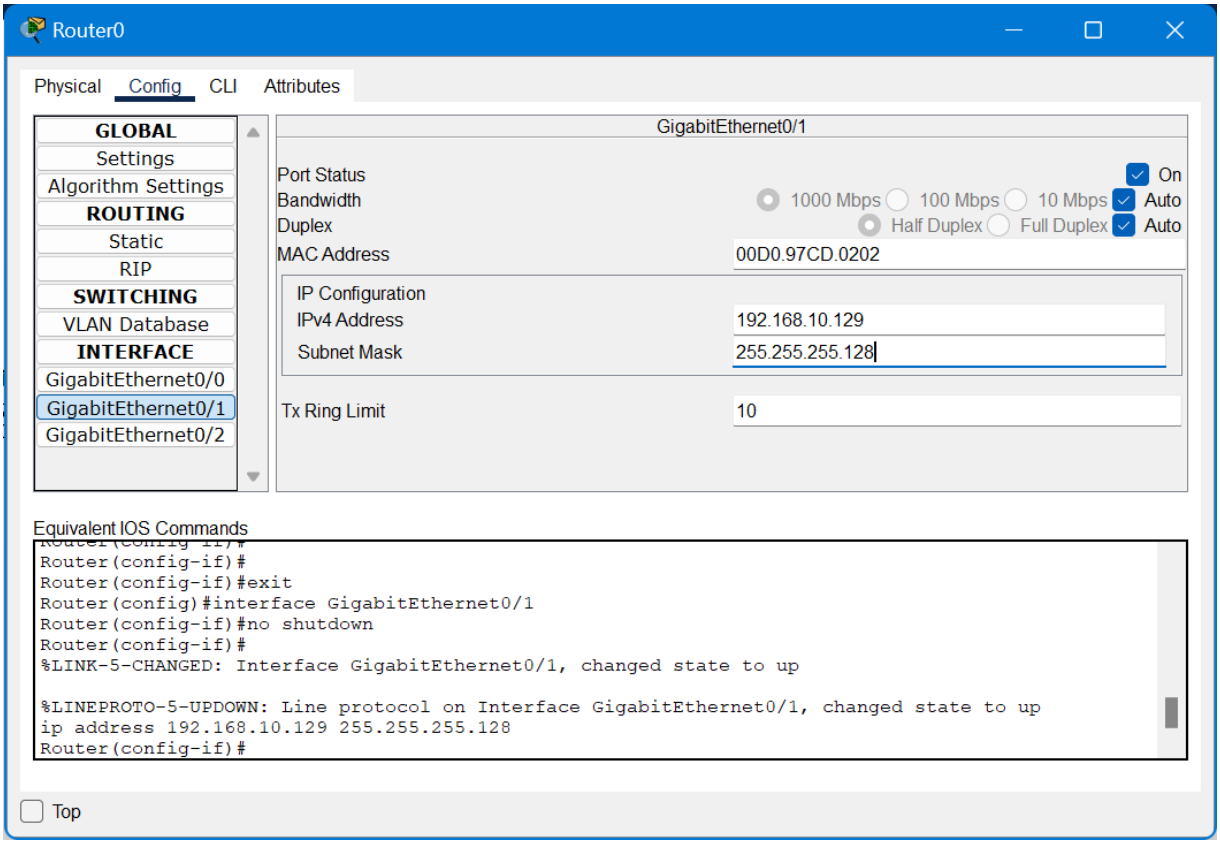

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.130
Subnet Mask
255.255.255.128
Default Gateway
192.168.10.129
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::204:9AFF:FE2D:381A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top





Step 4: Now assign the IP address and the subnet mask to GigabitEthernet0/0 and GigabitEthernet0/1 of Router0.





Commands to check connectivity

PC0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.130

Pinging 192.168.10.130 with 32 bytes of data:

Reply from 192.168.10.130: bytes=32 time<1ms TTL=127
Reply from 192.168.10.130: bytes=32 time<1ms TTL=127
Reply from 192.168.10.130: bytes=32 time=3ms TTL=127
Reply from 192.168.10.130: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>
```

PC5

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Practical No. 10

Aim: Conducting a Network Capture and Monitoring with Wireshark Simulation Tool.

Theory

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course). In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

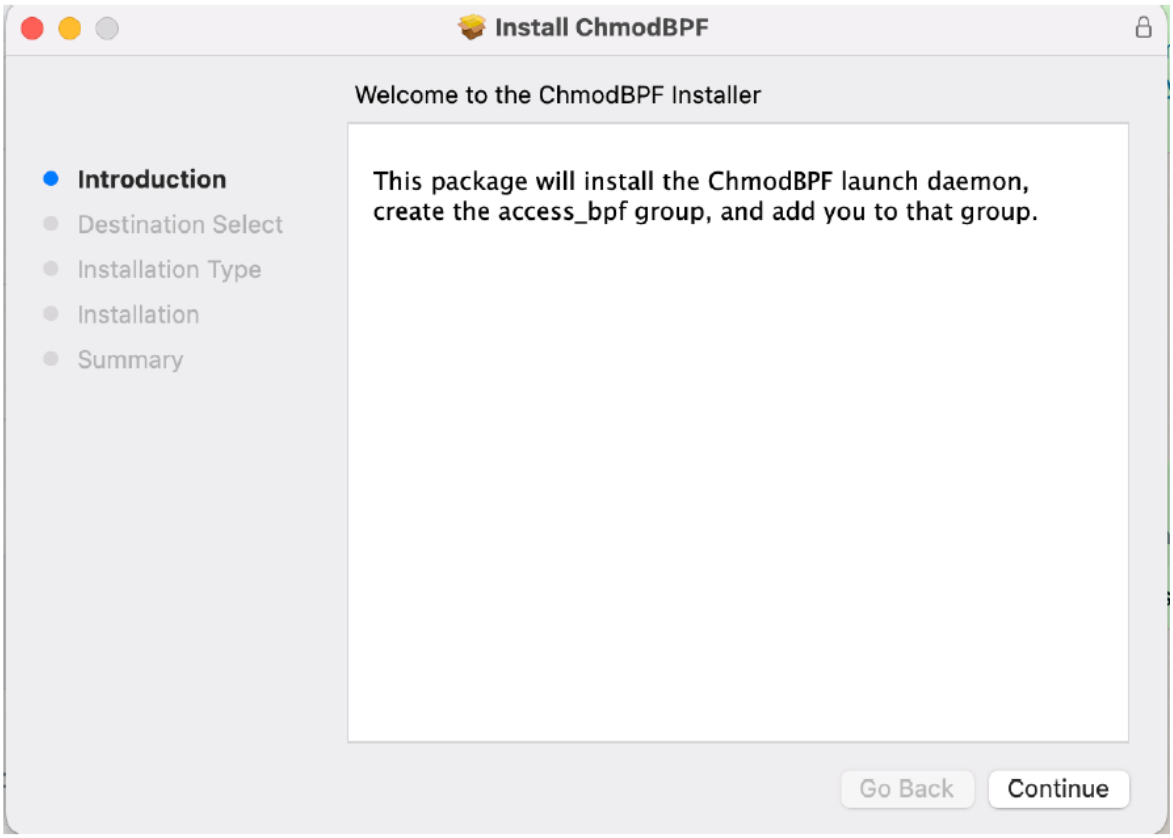
Here are some reasons people use Wireshark:

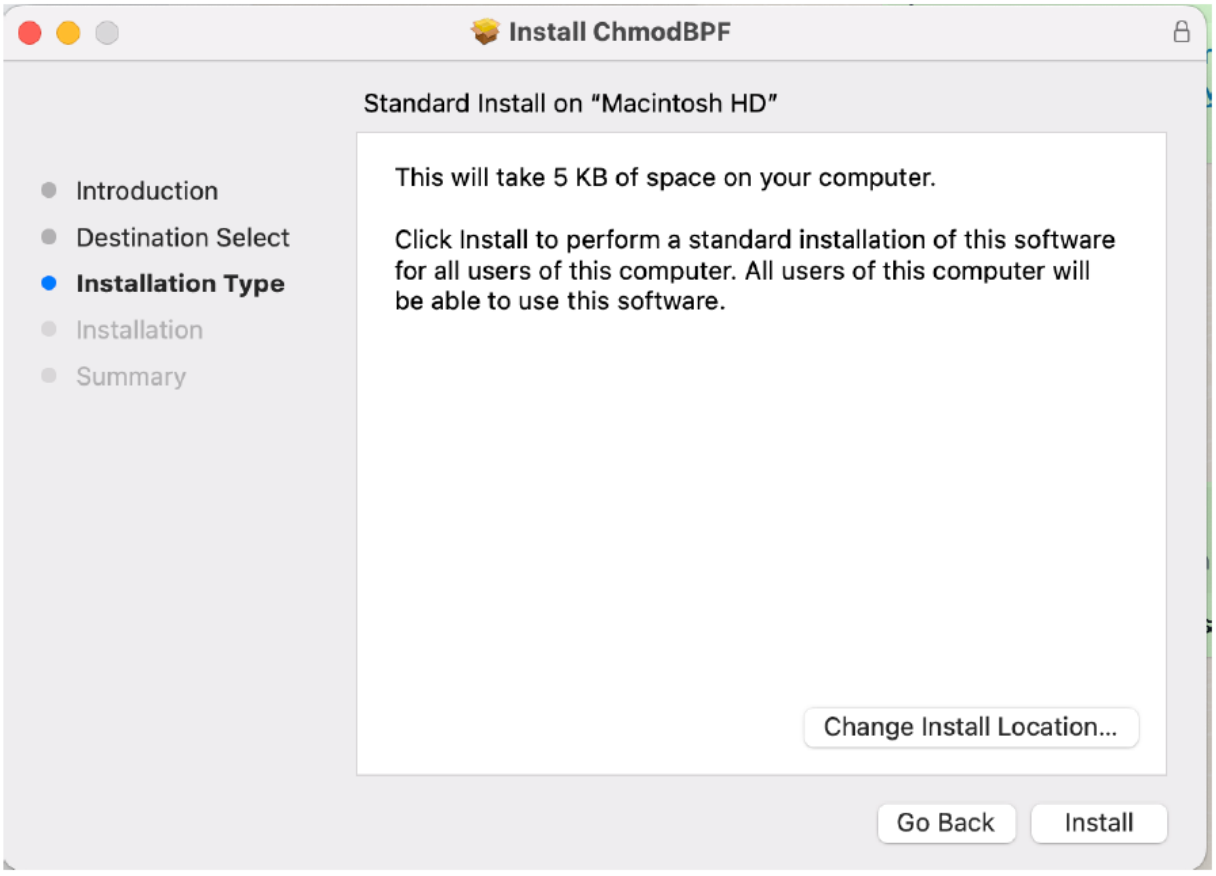
- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- QA engineers use it to verify network applications.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.

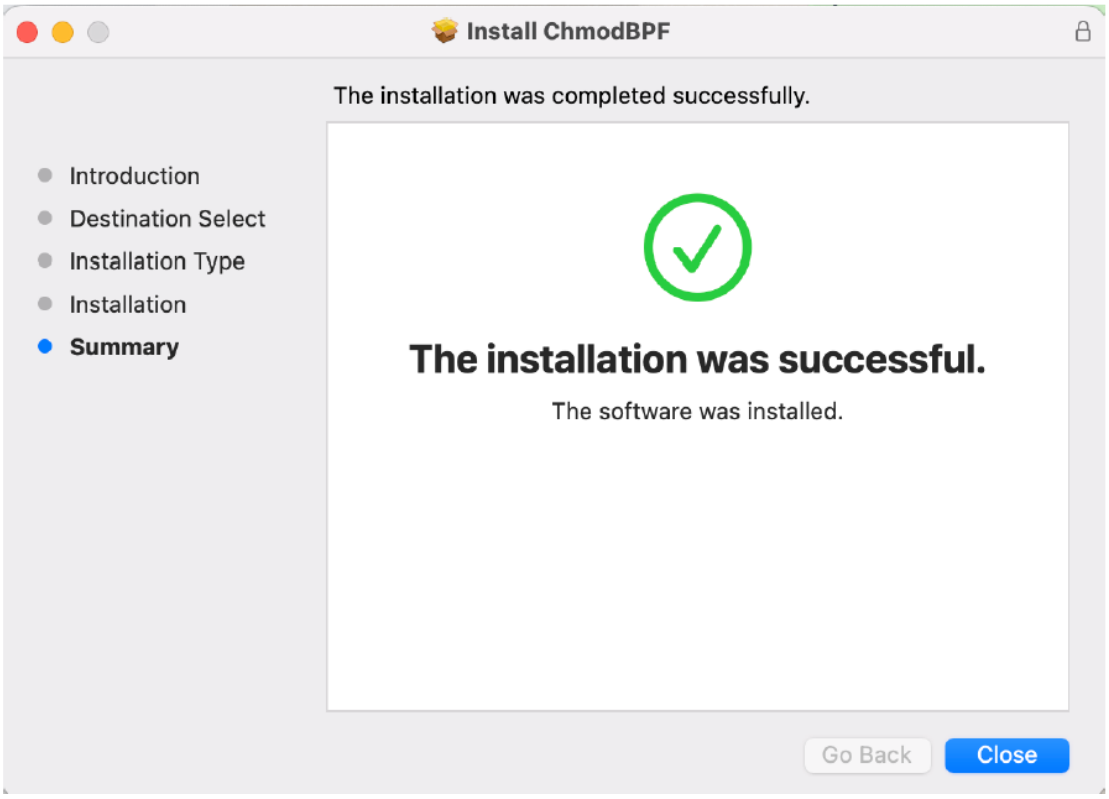
Installation

Step 1: Download the arm macOS dmg file from the Wireshark Site. And just drag the Wireshark icon to Application folder.

Step 2: If we have to capture the packets the we have to download the ChmodBPF.pkg. and install the package in various stage.

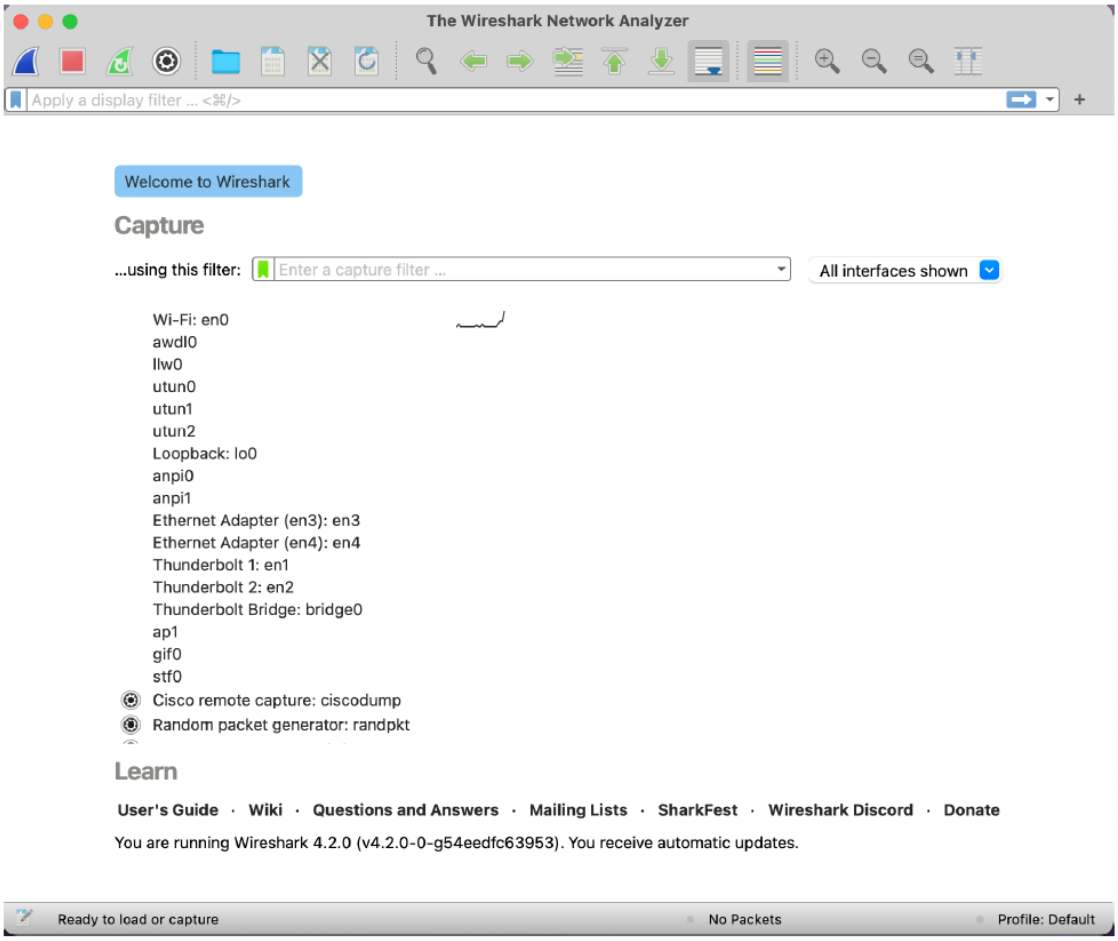

Install ChmodBPF
Welcome to the ChmodBPF Installer
Introduction
Destination Select
Installation Type
Installation
Summary
This package will install the ChmodBPF launch daemon, create the access_bpf group, and add you to that group.
Go Back
Continue


Install ChmodBPF
Standard Install on "Macintosh HD"
Introduction
Destination Select
Installation Type
Installation
Summary
This will take 5 KB of space on your computer.
Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.
Change Install Location...
Go Back
Install

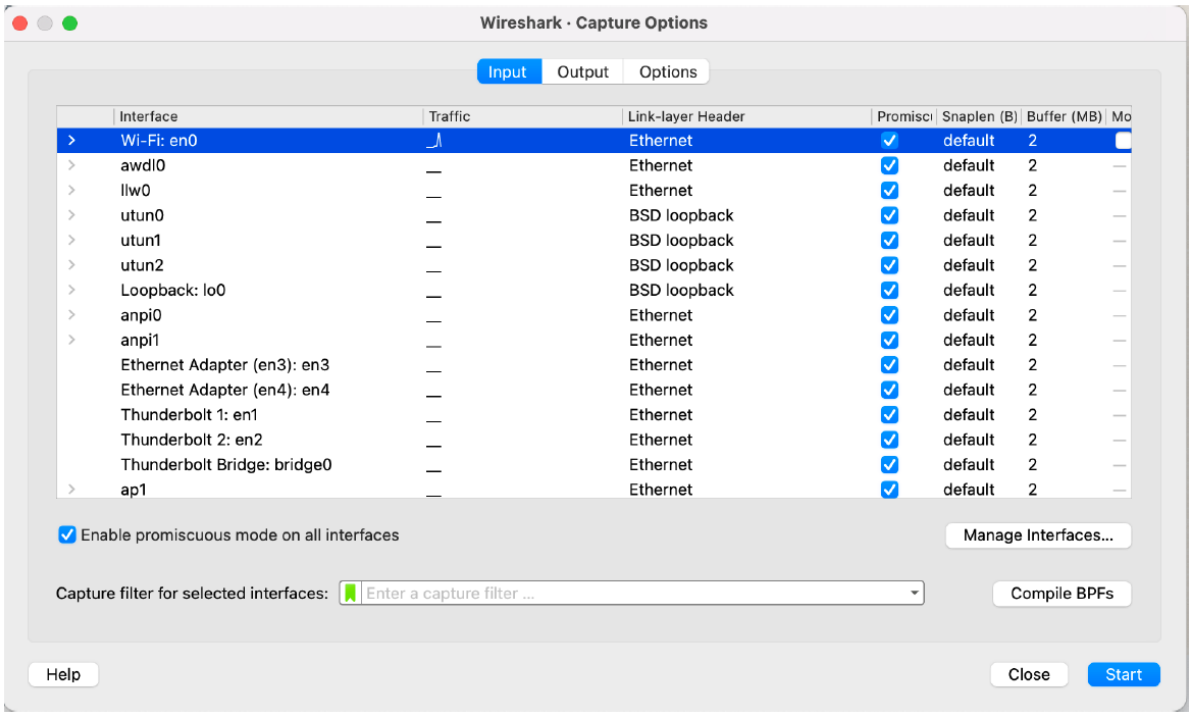


Steps to execute

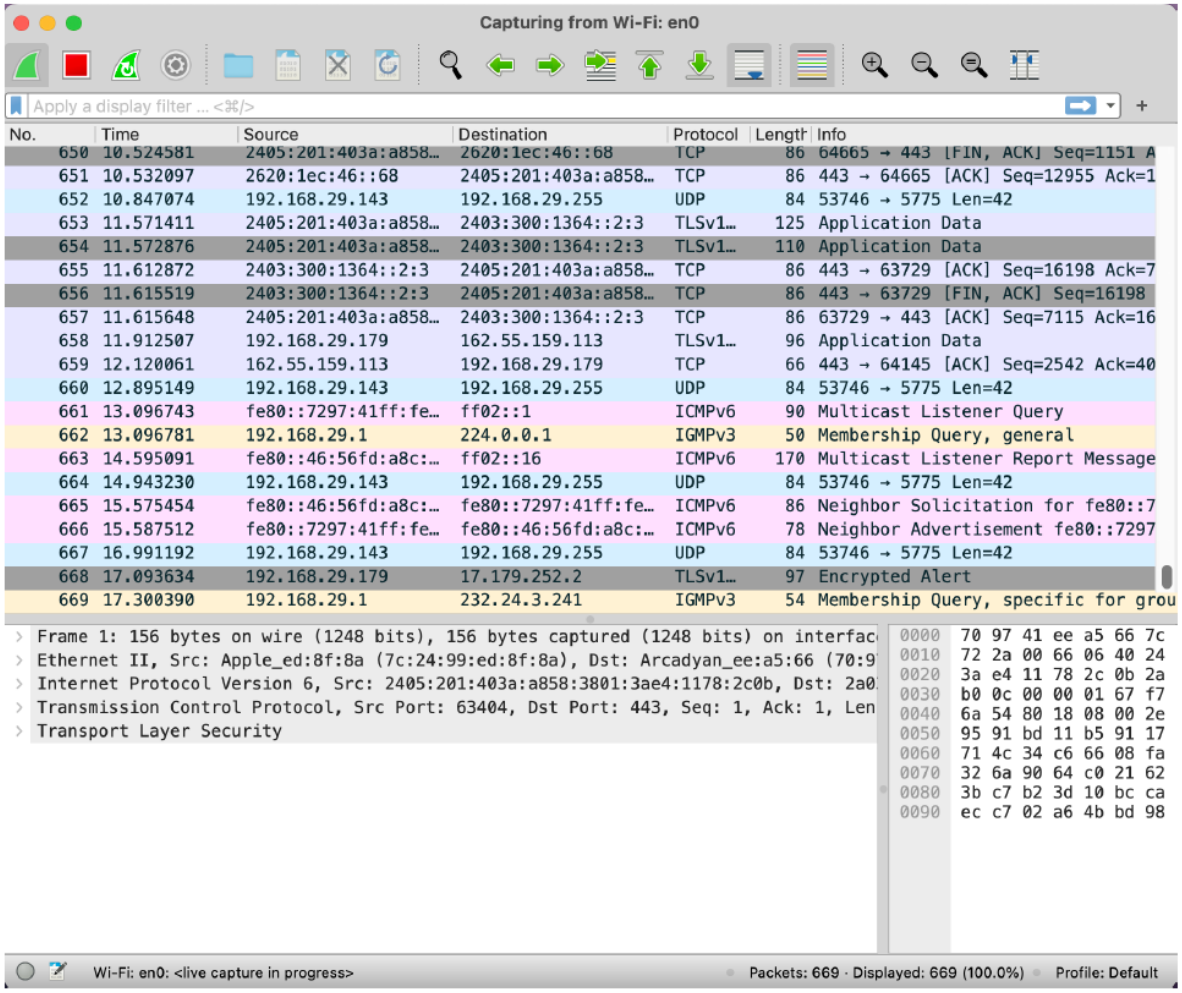
Step 1: Open wire shark Application and click on the Capture button.



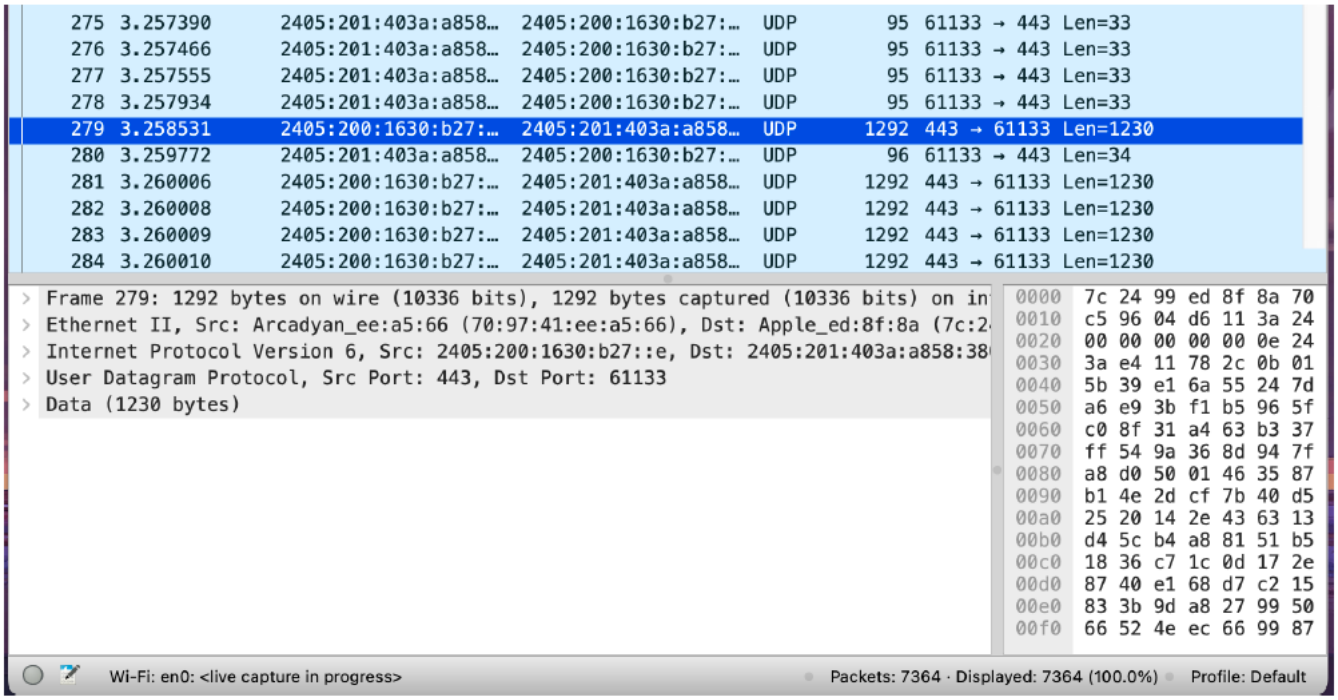
Step 2: After that there will many interfaces. Click on the the wifi interfaces and click on the start button.



Step 3: There will be simulation of capturing the Packets from wifi interface.



Step 4: Now monitor the specific Packets by clicking on that packet. The information will be provided on the lower section. Left most will show all the header information and right most will show about the data.


275 3.257390 2405:201:403a:a858… 2405:200:1630:b27:… UDP 95 61133 → 443 Len=33
276 3.257466 2405:201:403a:a858… 2405:200:1630:b27:… UDP 95 61133 → 443 Len=33
277 3.257555 2405:201:403a:a858… 2405:200:1630:b27:… UDP 95 61133 → 443 Len=33
278 3.257934 2405:201:403a:a858… 2405:200:1630:b27:… UDP 95 61133 → 443 Len=33
279 3.258531 2405:200:1630:b27:… 2405:201:403a:a858… UDP 1292 443 → 61133 Len=1230
280 3.259772 2405:201:403a:a858… 2405:200:1630:b27:… UDP 96 61133 → 443 Len=34
281 3.260006 2405:200:1630:b27:… 2405:201:403a:a858… UDP 1292 443 → 61133 Len=1230
282 3.260008 2405:200:1630:b27:… 2405:201:403a:a858… UDP 1292 443 → 61133 Len=1230
283 3.260009 2405:200:1630:b27:… 2405:201:403a:a858… UDP 1292 443 → 61133 Len=1230
284 3.260010 2405:200:1630:b27:… 2405:201:403a:a858… UDP 1292 443 → 61133 Len=1230
Frame 279: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on in
Ethernet II, Src: Arcadyan_ee:a5:66 (70:97:41:ee:a5:66), Dst: Apple_ed:8f:8a (7c:2
Internet Protocol Version 6, Src: 2405:200:1630:b27::e, Dst: 2405:201:403a:a858:38
User Datagram Protocol, Src Port: 443, Dst Port: 61133
Data (1230 bytes)
0000 7c 24 99 ed 8f 8a 70
0010 c5 96 04 d6 11 3a 24
0020 00 00 00 00 00 0e 24
0030 3a e4 11 78 2c 0b 01
0040 5b 39 e1 6a 55 24 7d
0050 a6 e9 3b f1 b5 96 5f
0060 c0 8f 31 a4 63 b3 37
0070 ff 54 9a 36 8d 94 7f
0080 a8 d0 50 01 46 35 87
0090 b1 4e 2d cf 7b 40 d5
00a0 25 20 14 2e 43 63 13
00b0 d4 5c b4 a8 81 51 b5
00c0 18 36 c7 1c 0d 17 2e
00d0 87 40 e1 68 d7 c2 15
00e0 83 3b 9d a8 27 99 50
00f0 66 52 4e ec 66 99 87
Wi-Fi: en0: <live capture in progress>
Packets: 7364 · Displayed: 7364 (100.0%)
Profile: Default