Practical 01
IPv4 Addressing and Subnetting

Aim:

a) Given an IP address and network mask, determine other information about the IP address such as
   i) Network address
   ii) Network broadcast address
   iii) Total number of host bits
   iv) Number of hosts

b) Given an IP address and network mask, determine other information about the IP address such as:
   i) The subnet address of this subnet
   ii) The broadcast address of this subnet
   iii) The range of host addresses for this subnet
   iv) The maximum number of subnets for this subnet mask
   v) The number of hosts for each subnet
   vi) The number of subnet bits
   vii) The number of this subnet

- Ipv4 Address Is 32 bit Long i.e 4 Bytes.
- Ipv4 Address are Unique and Universal.
- Address Space of Ipv4 is 2^{32}
- Network Address Is identifier of Network.
- Network Mask:-A Network Mask or a default mask in classful addressing is a 32-bit number with 'n' leftmost list all set to '1' and rightmost are 32-n bits all set to '0'.

Class A Subnet Mask	Netwok	Host	Host	Host
	255	0	0	0
Class B Subnet Mask	Netwok	Network	Host	Host
	255	255	0	0
Class C Subnet Mask	Netwok	Network	Network	Host
	255	255	255	0

- Subnetting:- Dividing the n number into many parts.

It means dividing a large network in 'n' parts is called Subnetting. The network mask is used when the network is subnetted.

But when we divide the network into number of parts then we need to create a subnetwork mask or subnet mask for each subnetwork.

A subnetwork has subnet id and host id.

- Subnet Mask:- A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, consider the IP address

150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

FORMULAS:-

Number Of Address(N):

$N=2^{32-n}$

Where n= net id

Number Of Sub-Network:

nsub=n+log2S

Where n=Length of Net id

nsub=Length of Each Subnet Id

S=Number Of Subnetwork

First Address Is Found By:

1st Address = (Any Address) AND (Network Mask)

Second Address Is Found By:

Last Address = (Any Address) OR (NOT (Network Mask))

Practical 02
Configuring LAN setup

Aim:

c) Planning and Setting IP networks
d) Configuring subnet
e) Study of basic network command and Network configuration commands. ipconfig, netstat, ARP, ping, trace route etc.
f) Basic network troubleshooting.
g) Configuration of TCP/IP Protocols in Windows / Linux.
h) Implementation of Drive/file sharing and printer sharing.

Part a) Planning and Setting IP networks

Planning and setting up IP networks involves several key steps and considerations to ensure a reliable, scalable, and secure infrastructure.

Following points are needed to be considered:

1) Define Network Requirements:
   We start by understanding the needs of the organization or project. Identify the number of devices to be connected, the expected network traffic, geographical locations, security requirements, and any future expansion plans.
2) Choose IP Addressing Scheme:
   Decide on the IP addressing scheme we would use, whether it's IPv4 or IPv6. For IPv4, we need to choose a private IP address range and ensure it doesn't conflict with any existing networks we might connect with.
3) Design Network Topology:
   Determine the network's physical layout and logical topology. Consider factors like the number and location of switches, routers, subnets, and how devices will connect to each other. This design should align with requirements and accommodate potential growth.
4) Subnetting:
   Divide IP address space into smaller subnets to help manage network traffic efficiently and improve security. Subnetting also enables us to isolate different departments or devices based on their functions.
5) Choose Network Equipment:
   Select routers, switches, firewalls, and other network equipment based on the network's size, expected traffic load, and the specific features and capabilities needed to meet our requirements.
6) IP Address Assignment:
   Decide how IP addresses will be assigned to devices. This can be done manually (static IP) for critical devices and servers, or dynamically (DHCP) for less critical devices. DHCP automates IP address assignment and makes it easier to manage larger networks.
7) Configure Network Devices:
   Set up the routers, switches, and firewalls based on the network design. Configure routing protocols, VLANs (if necessary), security policies, Quality of Service (QoS) settings, and any other required features.

8) Implement Network Security:
   Security is crucial in any network. Set up firewalls, intrusion prevention systems (IPS), and other security measures to protect against unauthorized access and potential threats. Regularly update firmware and keep security patches up to date.
9) Testing and Troubleshooting:
   Before deploying the network in a production environment, conduct thorough testing to identify and resolve any configuration issues or performance bottlenecks. Verify connectivity, test for any security vulnerabilities, and ensure proper functioning of all network services.
10) Documentation:
    Document the entire network setup, including IP addresses, subnet masks, network diagrams, device configurations, security settings, and any other relevant information. This documentation will be valuable for future troubleshooting, maintenance, and upgrades.
11) Monitoring and Maintenance:
    Implement network monitoring tools to keep an eye on the network's health and performance. Regularly monitor for any anomalies, assess network usage patterns, and perform necessary maintenance tasks like updating firmware, renewing SSL certificates, and checking for security updates.
12) Network Scalability:
    Plan for future growth and scalability. As the network expands, we must be ensured it can accommodate additional devices and increased traffic without major disruptions.

Part b) Configuring subnet

In order to configure a subnet, we consider the following example.
A company iSmile has 16 PCs connected in a single network, the company plans to create 4 Subnets each containing 4 PCs
To create four subnetworks, each with four PCs, we can use subnetting to divide the organization's network into smaller segments. We will use a Class C IP address range for this example, as it provides 256 IP addresses in total (ranging from 192.168.0.0 to 192.168.0.255).

First, let's find the subnet mask that allows for four subnets. Since $2^2 = 4$, we need 2 bits for subnetting (2^2 = 4). The remaining 6 bits will be used for host addresses ($2^6 = 64$ - 2 reserved for network and broadcast addresses = 62 usable host addresses).
Subnet Mask: 255.255.255.192 (/26 in CIDR notation)
(26 bits for subnet + host, with 26 bits being 1111 1111 1111 1111 1111 1111 1100 0000)

Now, let's assign the IP addresses to each subnet:
Subnet 1:
Usable IP Range: 192.168.0.1 to 192.168.0.62
Network Address: 192.168.0.0
Broadcast Address: 192.168.0.63
Assigned IP Addresses:

PC1	192.168.0.2
PC2	192.168.0.3
PC3	192.168.0.4
PC4	192.168.0.5

Remaining addresses are not assigned

Subnet 2:
Usable IP Range: 192.168.0.65 to 192.168.0.126
Network Address: 192.168.0.64
Broadcast Address: 192.168.0.127.
Assigned IP Addresses:

PC1	192.168.0.65
PC2	192.168.0.66
PC3	192.168.0.67
PC4	192.168.0.68

Remaining addresses are not assigned

Subnet 3:
Usable IP Range: 192.168.0.129 to 192.168.0.190
Network Address: 192.168.0.128
Broadcast Address: 192.168.0.191
Assigned IP Addresses:

PC1	192.168.0.129
PC2	192.168.0.130
PC3	192.168.0.131
PC4	192.168.0.132

Remaining addresses are not assigned

Subnet 4:
Usable IP Range: 192.168.0.193 to 192.168.0.254
Network Address: 192.168.0.192
Broadcast Address: 192.168.0.255
Assigned IP Addresses:

PC1	192.168.0.193
PC2	192.168.0.194
PC3	192.168.0.195
PC4	192.168.0.196

Remaining addresses are not assigned

Each subnet will have its own unique range of IP addresses, with 4 usable addresses for PCs (since there are only 4 PCs in each subnet). The remaining addresses in each subnet are reserved for the network address and broadcast address.

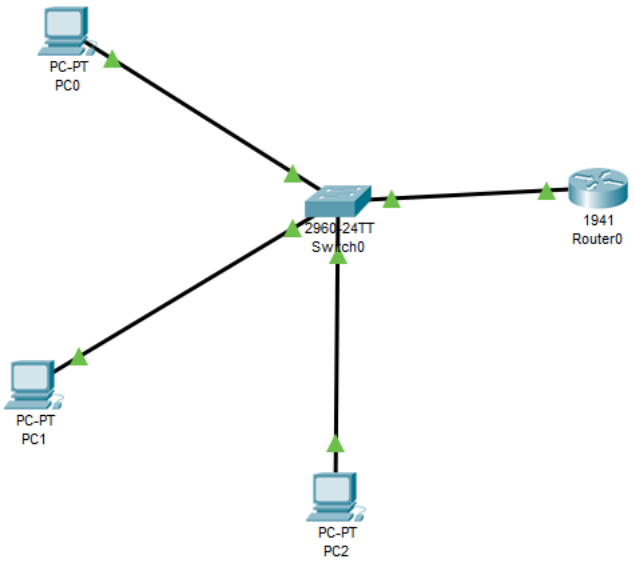
Part c) Study of basic network command and Network configuration commands

1) **arp** : This diagnostic command displays and modifies the IP-to-Ethernetor Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).
2) **ipconfig:**This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP. If you enter only ipconfig without parameters, the response is a display of all of the current TCP/IP configuration values, including IP address, subnet mask,and default gateway.

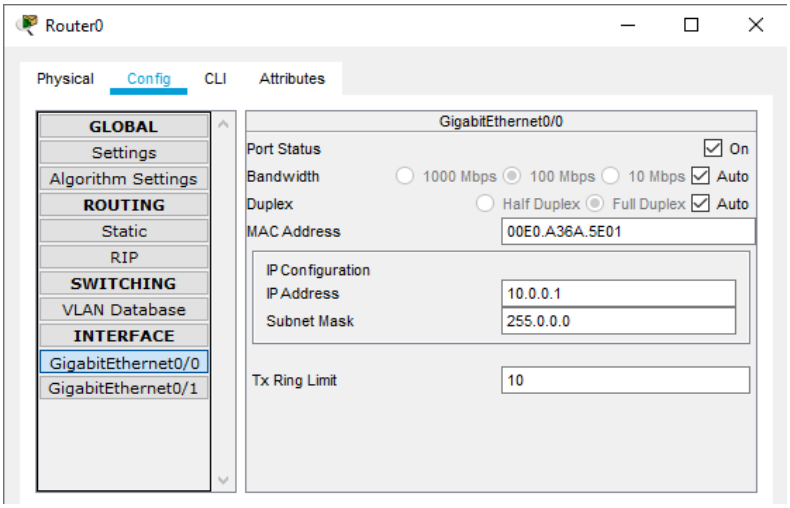
3) **ping:** This diagnostic command verifies connections to one or more remote computers.

4) **tracert:**
This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying time-to-live (TTL) values to the destination.

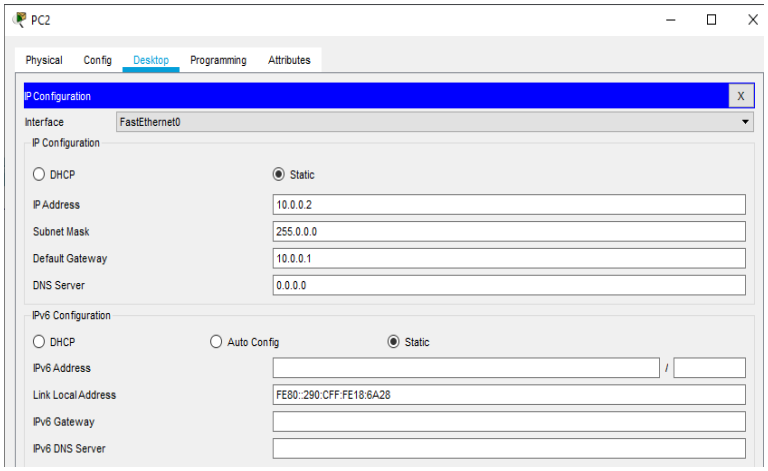
We use the following example to demonstrate the use of the commands discussed in the previous sections



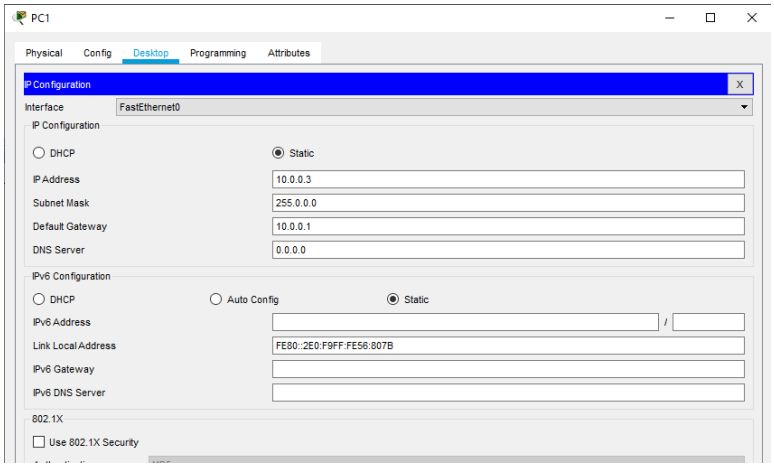
Configure the Router 0:



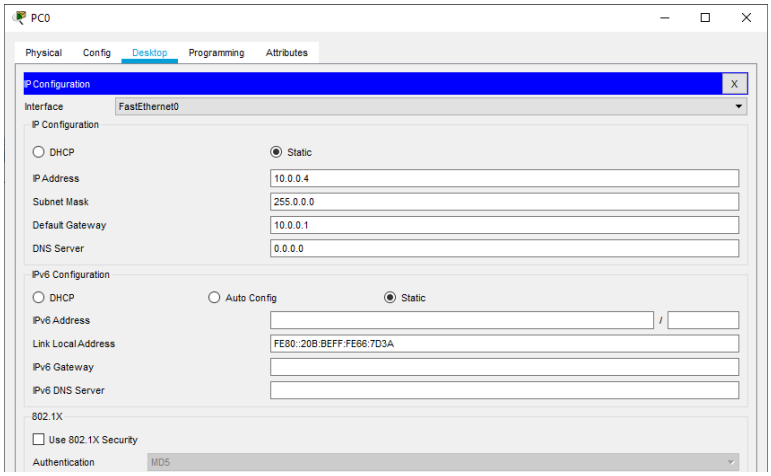
Configure PC2:



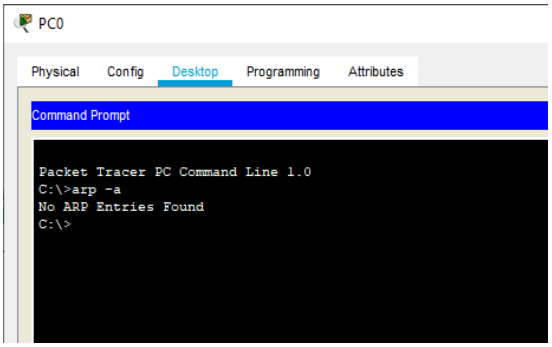
Configure PC1:

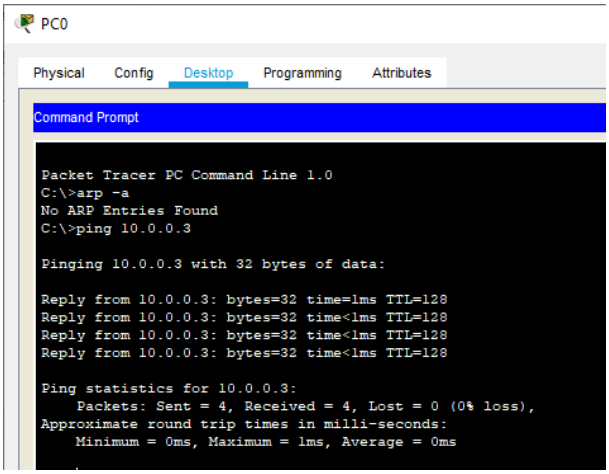


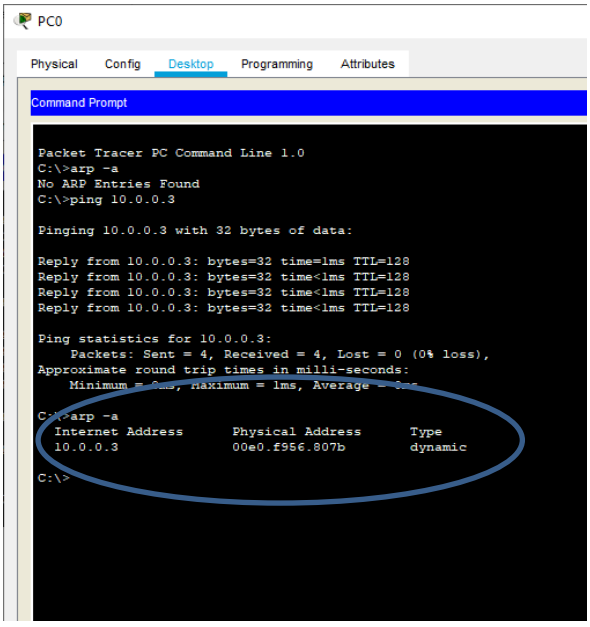
Configure PC0:

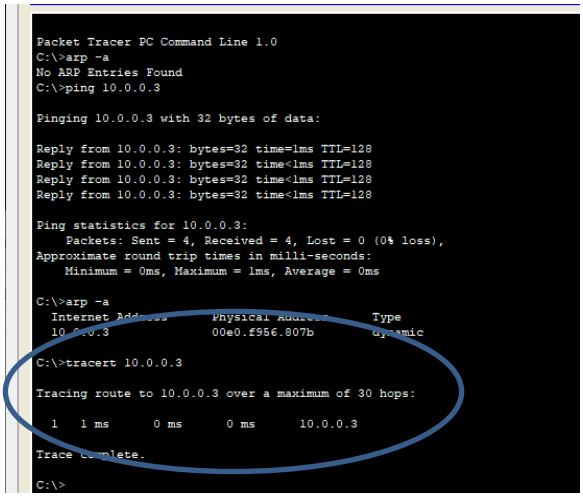


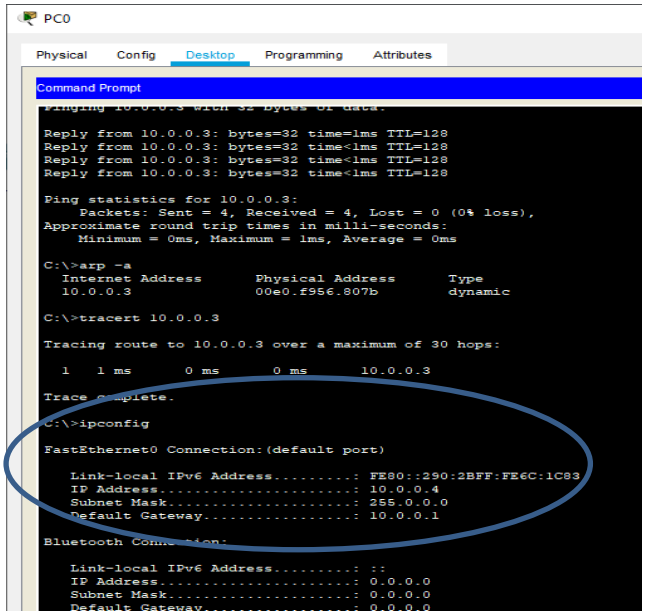
Next, we type the following commands in PC0











Part d) Basic Network Troubleshooting

Basic network troubleshooting refers to the process of identifying and resolving common issues that can arise in a computer network. Following are some essential steps and techniques for basic network troubleshooting:

a) **Identify the Problem:** Start by gathering information from the user or by observing the issue yourself. Understand what specific problem the user is facing, such as no internet access, slow connection, or inability to access certain resources.

b) **Check Physical Connections:** Ensure all network cables are securely plugged in, and network devices like routers, switches, and modems have power and functioning indicators.

c) **Restart Devices:** Sometimes, network issues can be resolved by simply restarting the network devices. Power cycle the router, modem, and any other network equipment to see if it resolves the problem.

d) **Check Network Configurations:** Verify the network settings on the computer or device experiencing the issue. Look for correct IP configurations, subnet masks, gateway addresses, and DNS server settings.

e) **Ping Test:** Use the ping command to check the connectivity between the computer and other devices on the network or the internet. For example, try pinging the router, another computer on the network, or an external website.

f) **Check for IP Conflicts**: Ensure that there are no IP address conflicts on the network. Two devices with the same IP address can cause communication problems.

g) **Firewall and Security Software**: Temporarily disable any firewall or security software to check if they are blocking network access.

h) **Update Network Drivers:** Ensure that the network interface card (NIC) drivers are up to date. Outdated drivers can lead to connectivity issues.

i) **Test Different Devices:** If possible, try connecting the problematic device to a different network or connecting a different device to the same network to see if the issue persists.

j) **Check Router and DHCP:** Verify that the router is functioning correctly and that the DHCP server is assigning IP addresses to devices on the network.

k) **Trace Route:** Use the tracert (Windows) or traceroute (macOS and Linux) command to trace the path from your computer to a remote server or website. This can help identify network hops where there might be an issue.

l) **Check for Network Outages:** Check with your Internet Service Provider (ISP) or network administrator to see if there are any known network outages or maintenance activities in your area.

m) **Use Network Troubleshooting Tools:** Network troubleshooting tools like ipconfig, ifconfig, nslookup, and netstat can provide valuable information about network configurations and connections.

n) **Check Physical Environment:** Ensure that there are no physical obstructions or interference (e.g., walls, microwave ovens) that could affect wireless network connectivity.

Part e) Networks Implementation of Drive/file sharing and printer sharing

Implementing drive/file sharing and printer sharing in a network allows multiple users to access shared files and use shared printers efficiently. These features can be set up on both small local networks (e.g., home networks) and larger corporate networks.
Implementing drive/file sharing and printer sharing in a Windows-based network as follows:

Set Up File Sharing:
File sharing allows users to access files and folders stored on a central server or on individual computers across the network.

Step 1: Share Folders:
Right-click on the folder you want to share and select "Properties."
In the Properties window, go to the "Sharing" tab.
Click on "Advanced Sharing" and check the box for "Share this folder."
Assign a Share Name (also known as a "Share Name" or "Share Path") that other users will use to access the shared folder.
You can set permissions to control who can access the folder and what level of access they have (read-only, read/write, etc.).

Step 2: Access Shared Folders:
Open File Explorer on another computer connected to the network.
In the address bar, type \\<IP address or computer name of the shared folder> and press Enter.
You should see a list of shared folders on that computer. Double-click on the folder you want to access and enter the appropriate credentials if required.

Set Up Printer Sharing:
Printer sharing allows multiple users to print to a single printer connected to a computer on the network.

Step 1: Share the Printer:
Connect the printer to the computer you want to use as a print server (the computer that will share the printer).
Open the Control Panel and go to "Devices and Printers."
Right-click on the printer you want to share and select "Printer properties."
In the properties window, go to the "Sharing" tab.
Check the box for "Share this printer" and provide a Share Name for the printer.

Step 2: Connect to the Shared Printer:
On other computers connected to the network, open the Control Panel and go to "Devices and Printers."
Click on "Add a printer" and then select "Add a network, wireless, or Bluetooth printer."
The shared printer should appear in the list. Select it and follow the on-screen instructions to install the printer driver and connect to the shared printer.

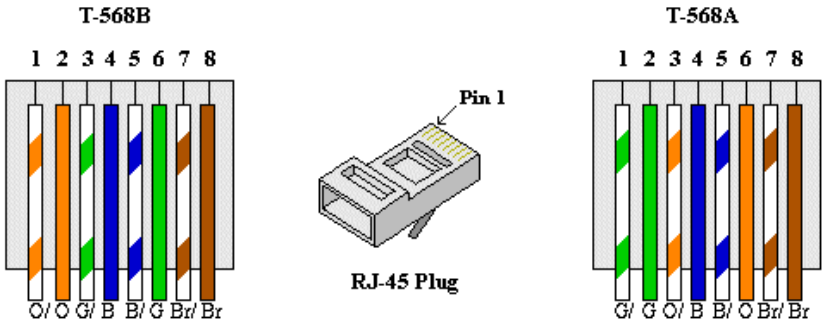
Practical 03
Colour code for crimping LAN (Cat 5/6/7) cable

Aim:

i) Study of Different colour codes
j) Study of different connecting devices and their differences
k) Crimping LAN Cable

RJ45 Pin-out Ethernet Cables and Colour codes

Ethernet LAN cables can come in two types – Crossover or Straight through. The following are the pin-outs for the RJ45 connectors



There are two different pin-out standards used worldwide, and depending on location, we determine which one to use.
T568A is used in America and Asia and
T568B is used in Britain and Europe

Different connecting devices and their differences:

There are several different connecting devices used in computer networks. Here are the most common ones and their key differences:

1) Hubs:
   a) Hubs operate at the physical layer of the network.
   b) They have a single collision domain, meaning all connected devices share the same bandwidth.
   c) They broadcast incoming data to all connected devices, regardless of the intended recipient.
   d) Hubs are considered outdated and are rarely used in modern networks.

2) Switches:
   a) Switches operate at the data link layer of the network.
   b) They create individual collision domains for each connected device, allowing for simultaneous communication.
   c) Switches use MAC addresses to direct incoming data to the appropriate device.
   d) They offer better performance, security, and scalability compared to hubs.

3) Routers:
   a) Routers operate at the network layer of the network.

b) They connect multiple networks or subnets and forward data packets between them.
c) Routers use IP addresses to route traffic based on network protocols.
d) They provide network segmentation, enable interconnectivity, and enforce security policies.

4) Bridges:
   a) Bridges operate at the data link layer of the network.
   b) They connect two network segments and filter network traffic based on MAC addresses.
   c) Bridges help to reduce network congestion and improve overall network performance.
   d) They are commonly used to extend network coverage and create smaller broadcast domains.

5) Repeaters and Extenders:
   a) Repeaters and extenders amplify or regenerate network signals to extend their reach.
   b) Repeaters operate at the physical layer, while extenders work at higher layers.
   c) Repeaters boost analog signals, while extenders can amplify both analog and digital signals.
   d) Repeaters and extenders are primarily used in long-distance or large-scale network deployments.

Crimping LAN Cable

Crimping LAN wires, also known as Ethernet cables, involves attaching RJ-45 connectors to the ends of the cable. Here are the steps to crimp LAN wires:

1) To Gather the necessary tools and materials:

a) Ethernet cable (UTP or STP)

b) RJ-45 connectors (usually 8P8C)

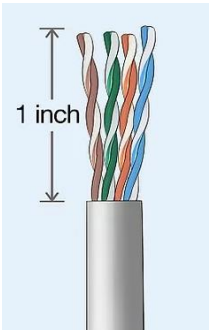
c) Crimping tool

d) Cable cutter/stripper

OR

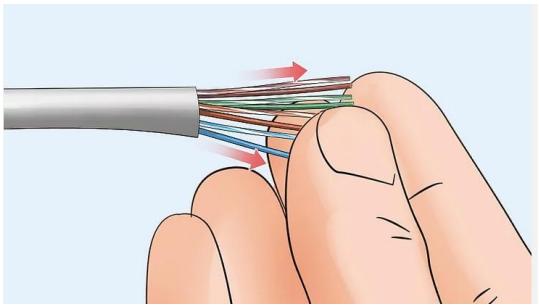
e) Cable tester (Optional)

2) Measure and cut the cable:
Determine the desired length of the LAN wire and cut the cable accordingly. Use a cable cutter to make a clean, straight cut.

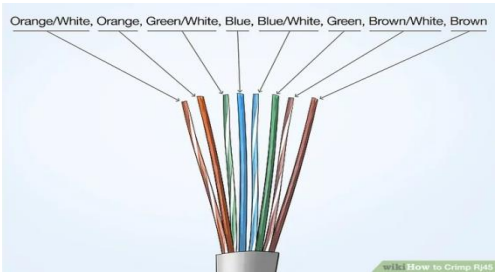


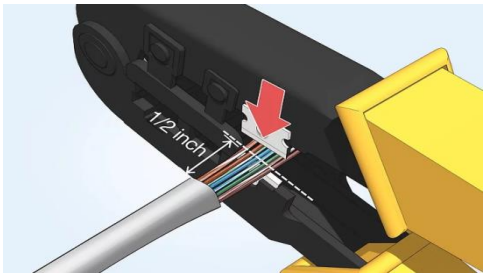
3) Strip the cable jacket:
Use a cable stripper or a sharp blade to carefully remove approximately 1-1.5 inches (2.5-3.8 cm) of the outer jacket from the cut end of the cable. Be cautious not to damage the internal wires.

4) **Untwist and arrange the wires:**
After removing the jacket, you'll find four twisted pairs of coloured wires inside.
Untwist the pairs and arrange them according to the desired wiring standard (T568A).
Make sure to maintain the same order on both ends of the cable.

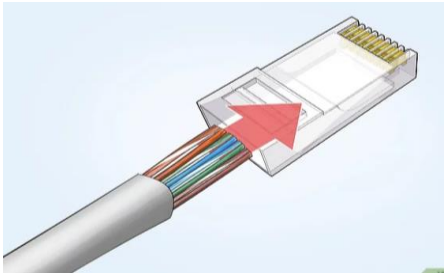


5) **Trim and straighten the wires:**
Cut the excess wire length to ensure they are even and of equal length, typically around 0.5 inches (1.3 cm).
Use your fingers or a wire straightened tool to align the wires neatly and make them easier to insert into the connector.

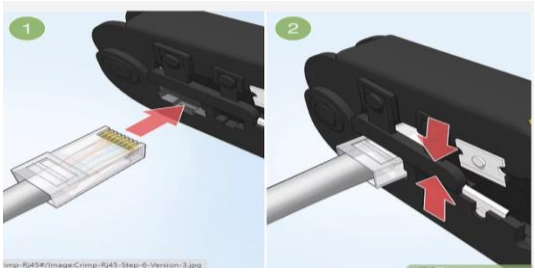




6) **Insert the wires into the connector:**
Carefully insert the arranged wires into the RJ-45 connector, ensuring they reach the end and make contact with the metal contacts inside. Check that the wire colours are in the correct order.



7) **Crimp the connector:**
   Place the connector and cable into the appropriate slot of the crimping tool, ensuring it is properly aligned.
   Squeeze the handles of the crimping tool firmly to crimp the connector. This action will secure the wires in place and create a strong connection.



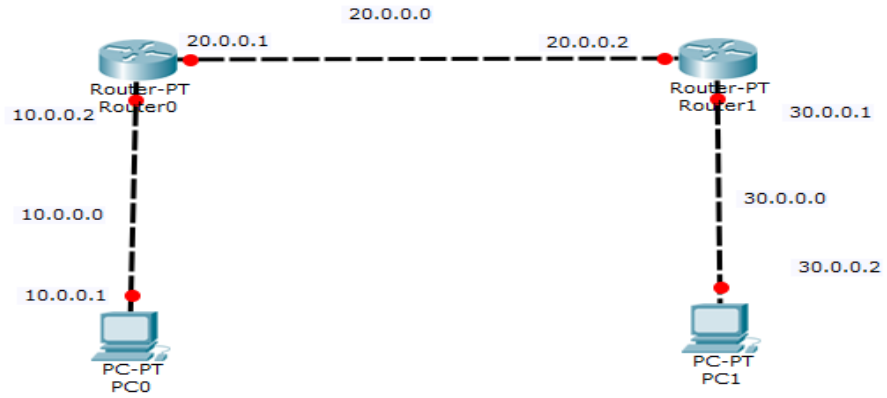
8) **Repeat for the other end:**
   Repeat steps 3 to 7 for the other end of the LAN wire, ensuring that both ends follow the same wiring standard.

9) **Test the cable (optional):**
   If available, use a cable tester to verify the connectivity and integrity of the crimped LAN wire. The tester will check for proper wire order and continuity.

By following these steps, we can crimp LAN wires and create custom Ethernet cables as per network requirements.

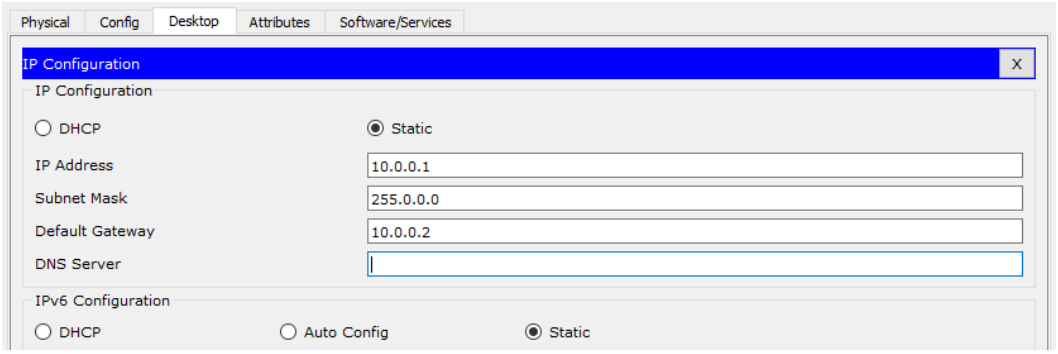
Practical 04
Designing and configuring a network topology

Aim: Configure IP static routing



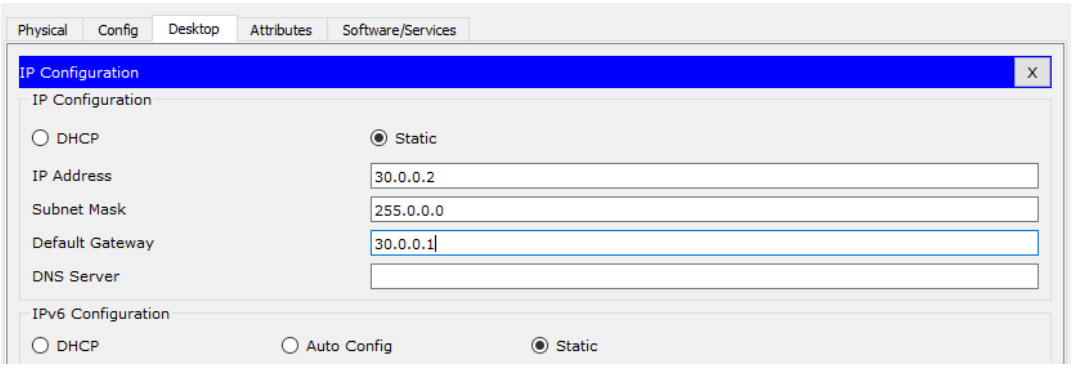
Assigning IP Address to PC0:

Open>>PC-PT-PC0>>Desktop>>IP Configuration>>IP Address>>10.0.0.1>>Default Gateway>>10.0.0.2



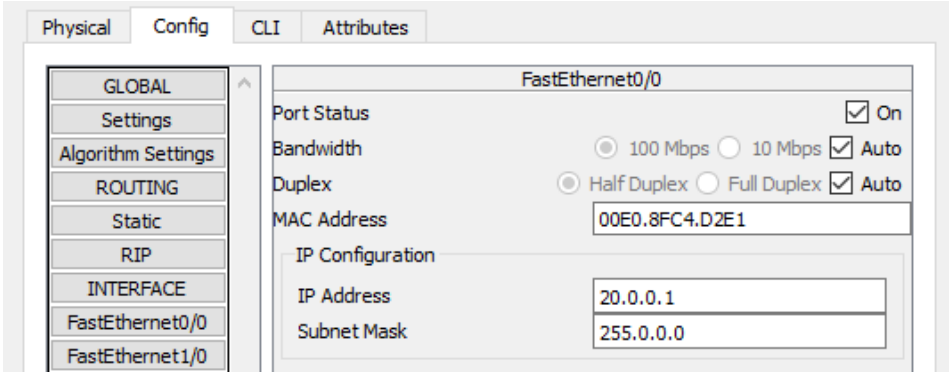
Assigning IP Address to PC1:

Open>>PC-PT-PC3>>Desktop>>IP Configuration>>IP Address>>30.0.0.1>>Default Gateway>>30.0.0.2



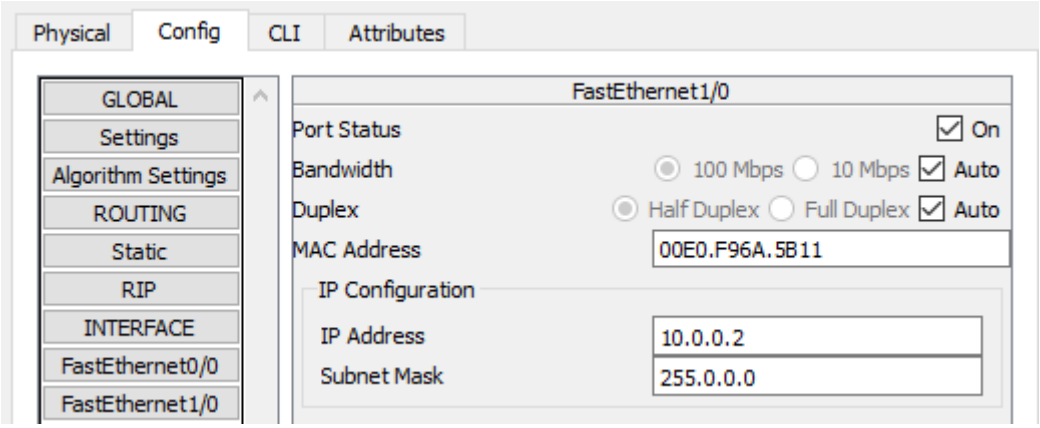
Assigning IP address to Router0>>FastEthernet0/0:

Open>>Router-PT Router0>>Config>>FastEthernet0/0>>IP Address>>20.0.0.1>>Subnet Mask>>255.0.0.0



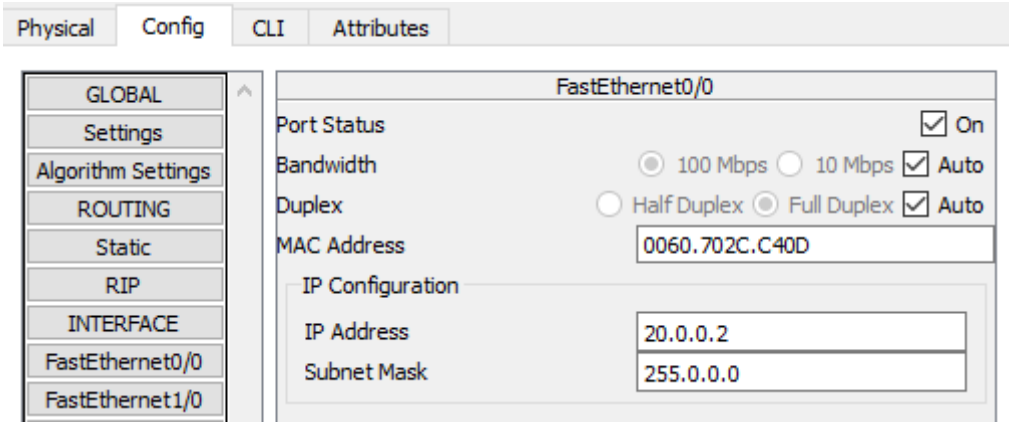
Assigning IP address to Router0>>FastEthernet1/0:

Open>>Router-PT Router0>>Config>>FastEthernet1/0>>IP Address>>10.0.0.2>>Subnet Mask>>255.0.0.0



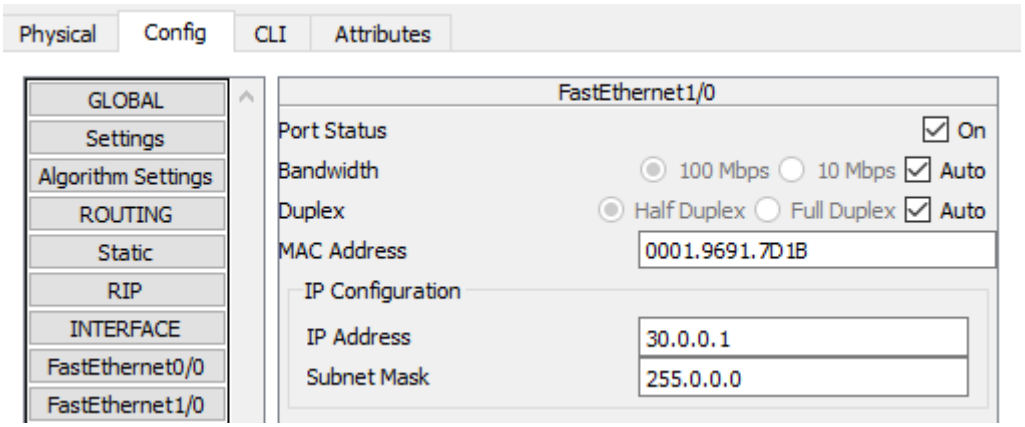
Assigning IP address to Router1>>FastEthernet0/0:

Open>>Router-PT Router1>>Config>>FastEthernet0/0>>IP Address>>20.0.0.2>>Subnet Mask>>255.0.0.0



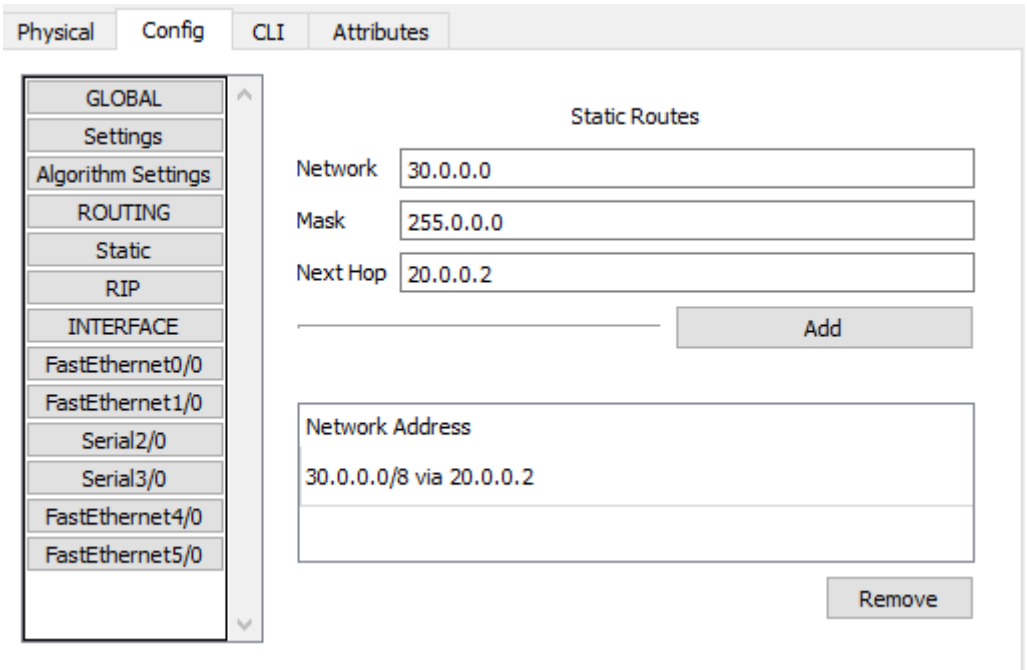
Assigning IP address to Router1>>FastEthernet1/0:

Open>>Router-PT Router1>>Config>>FastEthernet1/0>>IP Address>>30.0.0.1>>Subnet Mask>>255.0.0.0



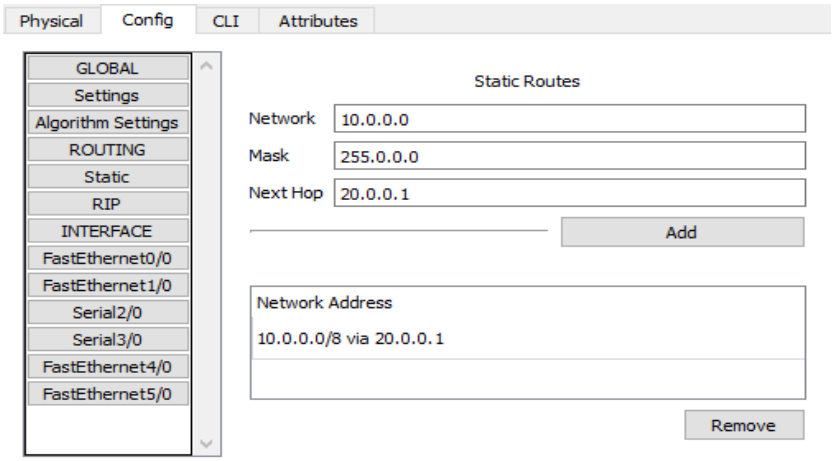
Assigning routes using static IP in router0:

Open>>Router-PT Router0>>Config>>Static>>Network>30.0.0.0>>Mask>>255.0.0.0>>Next Hop>>20.0.0.2>>Add

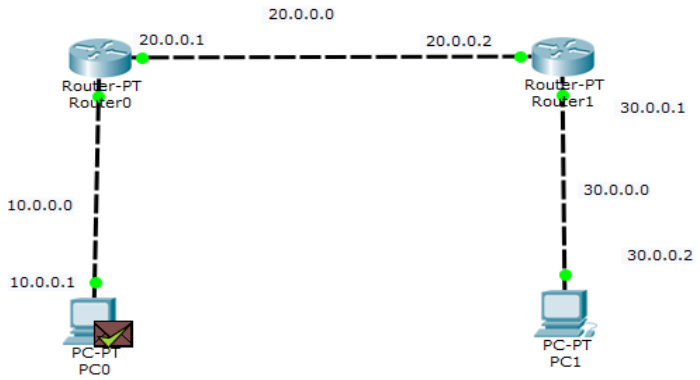


Assigning routes using static IP in router1

Open>>Router-PT Router1>>Config>>Static>>Network>10.0.0.0>>Mask>>255.0.0.0>>Next Hop>>20.0.0.1>>Add



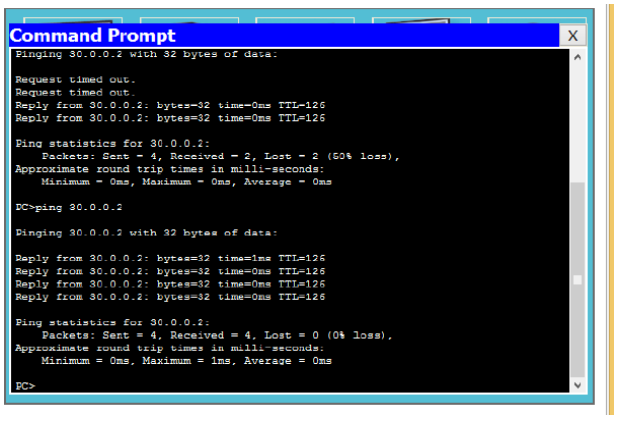
Sending Message:



Succesfull:

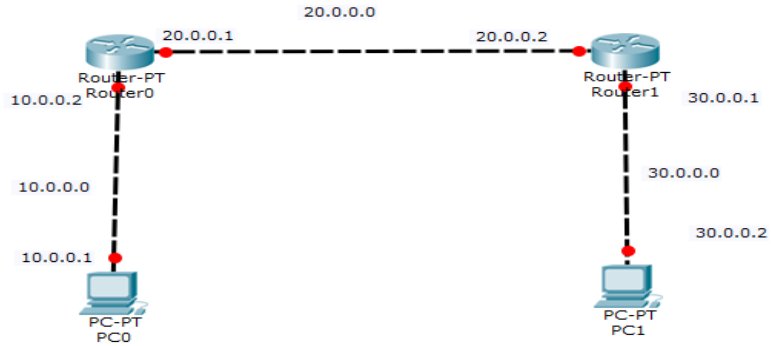
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(e...

Verifying the Connectivity using the Ping command:



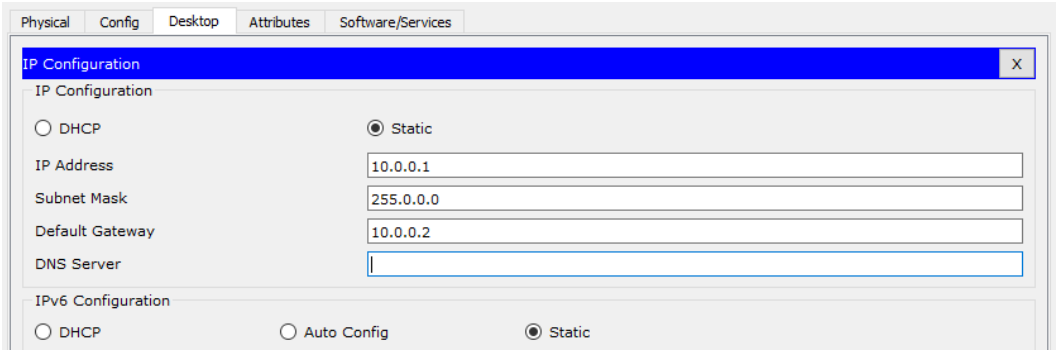
Practical 05
Configure IP routing using RIP

Aim: Configure IP routing using Routing Information Protocol (RIP)



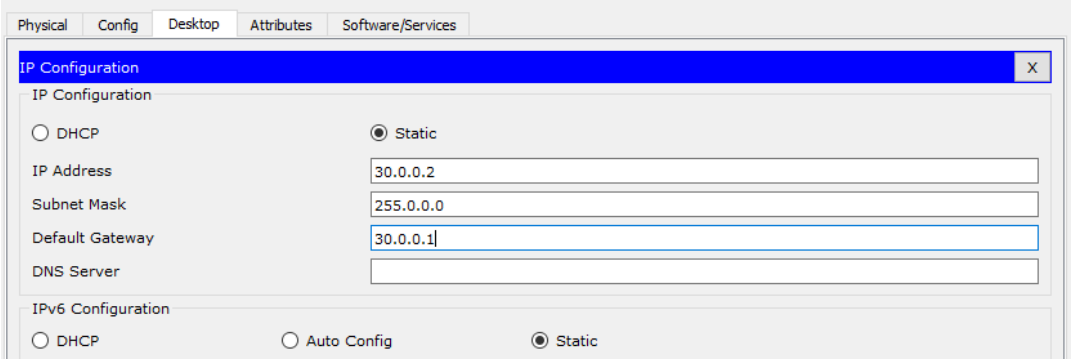
Assigning IP Address to PC0:

Open>>PC-PT-PC0>>Desktop>>IP Configuration>>IP Address>>10.0.0.1>>Default Gateway>>10.0.0.2



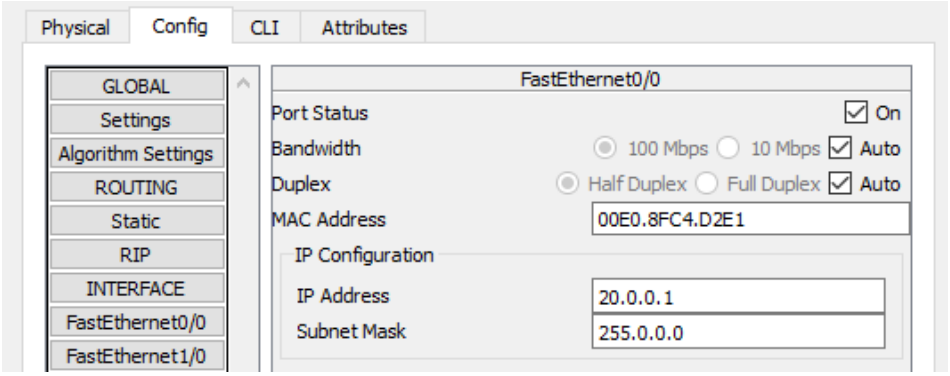
Assigning IP Address to PC1:

Open>>PC-PT-PC3>>Desktop>>IP Configuration>>IP Address>>30.0.0.1>>Default Gateway>>30.0.0.2



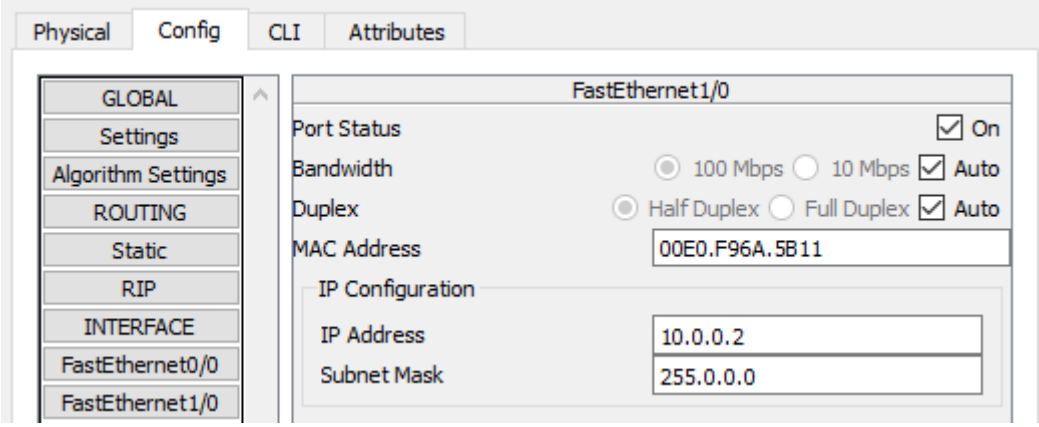
Assigning IP address to Router0>>FastEthernet0/0:

Open>>Router-PT Router0>>Config>>FastEthernet0/0>>IP Address>>20.0.0.1>>Subnet Mask>>255.0.0.0



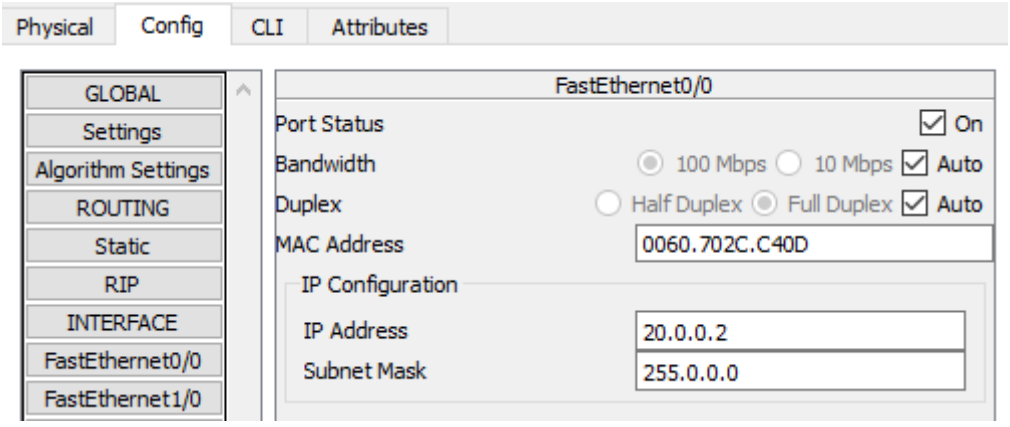
Assigning IP address to Router0>>FastEthernet1/0:

Open>>Router-PT Router0>>Config>>FastEthernet1/0>>IP Address>>10.0.0.2>>Subnet Mask>>255.0.0.0



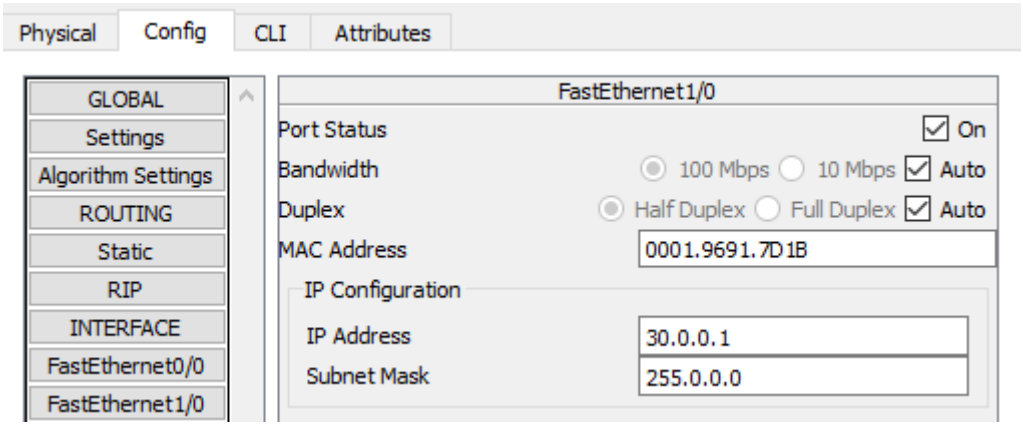
Assigning IP address to Router1>>FastEthernet0/0:

Open>>Router-PT Router1>>Config>>FastEthernet0/0>>IP Address>>20.0.0.2>>Subnet Mask>>255.0.0.0



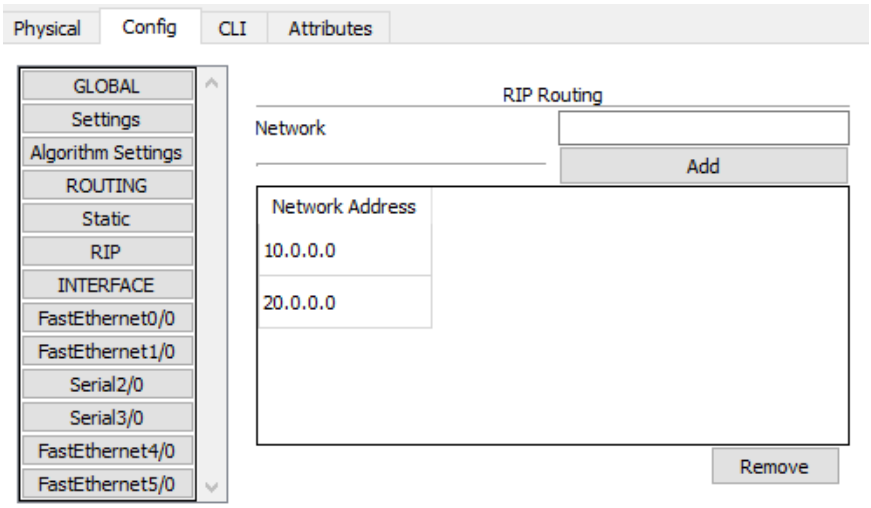
Assigning IP address to Router1>>FastEthernet1/0:

Open>>Router-PT Router1>>Config>>FastEthernet1/0>>IP Address>>30.0.0.1>>Subnet Mask>>255.0.0.0



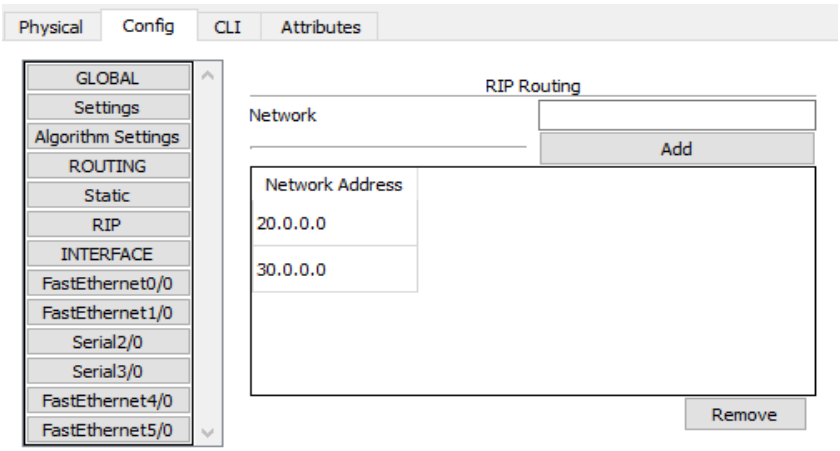
Assigning routes using RIP in Router0:

Open>>Router-PT Router0>>Config>>RIP>>Network>20.0.0.0>>Add>>10.0.0.0>>Add

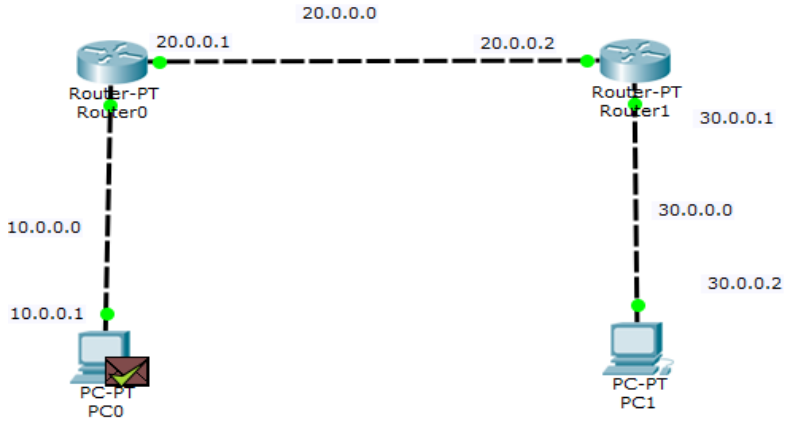


Assigning routes using RIP in Router1:

Open>>Router-PT Router1>>Config>>RIP>>Network>30.0.0.0>>Add>>20.0.0.0>>Add



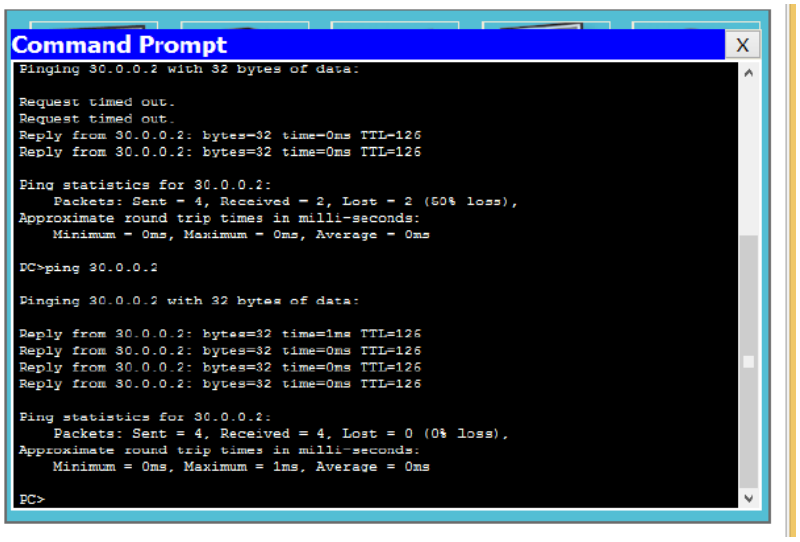
Sending Message:



Succesfull:

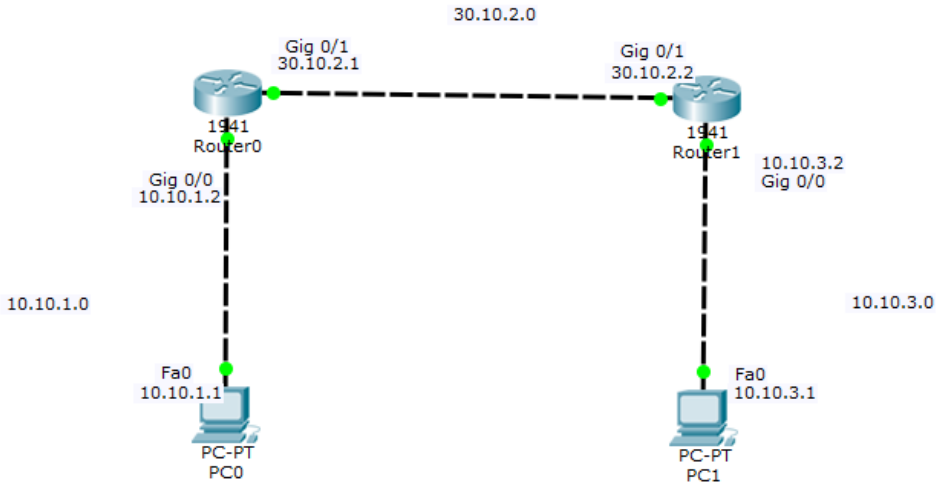
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(e...

Verifying the Connectivity using the Ping command:



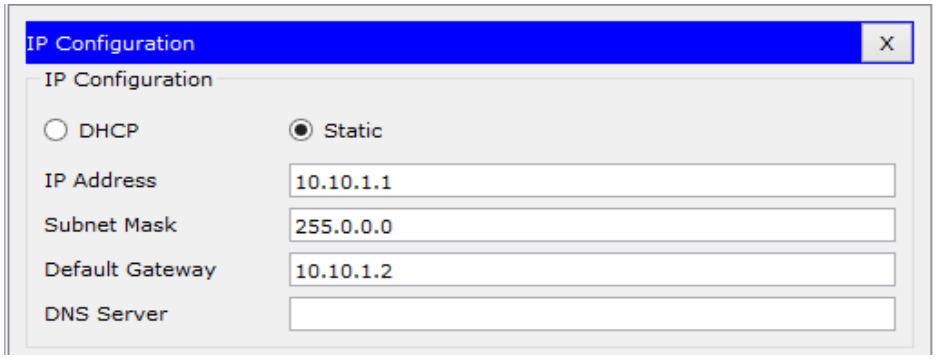
Practical 06(A)
Configuring Simple OSPF

Aim: Configuring Simple OSPF.



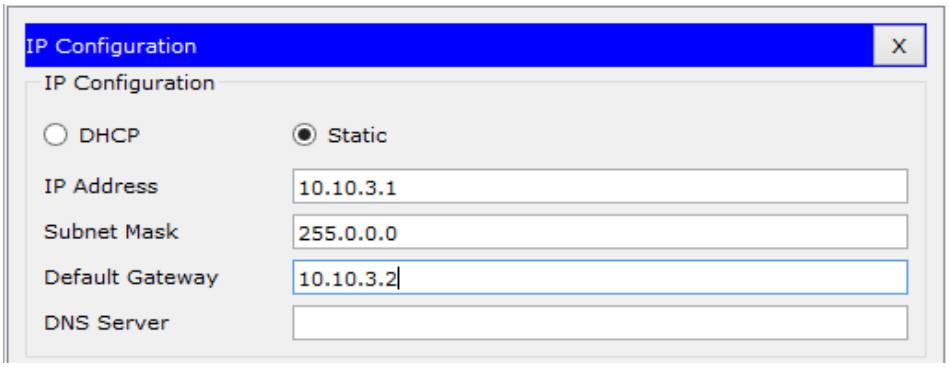
Assigning IP Address To PC 0:

Open>>PC0>>Desktop>>Ipconfiguration>> Ip Address >> 10.10.1.1 >> subnetmask >> 255.0.0.0>>default gateway>>10.10.1.2



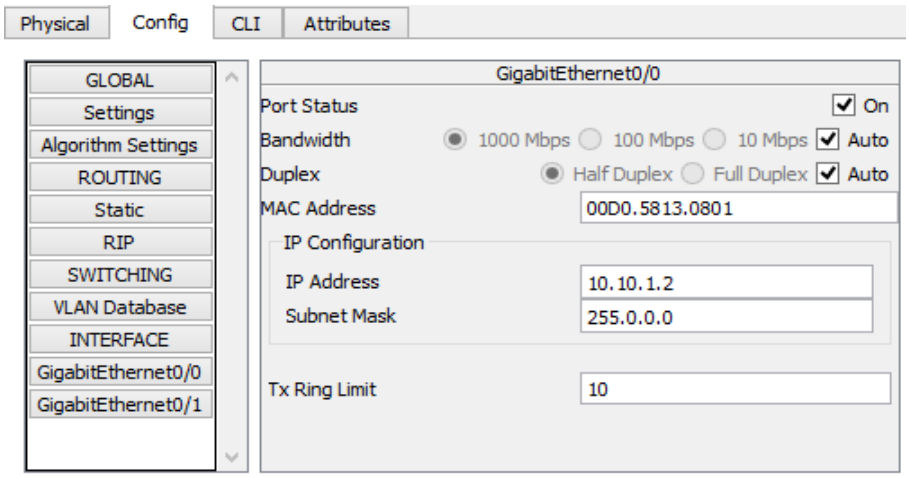
Assigning IP Address To PC 1:

Open>>PC0>>Dekstop>>Ipconfiguration>>Ipaddress>>10.10.3.1>>subnetmask>>255.0.0.0 >>default gateway>>10.10.3.2

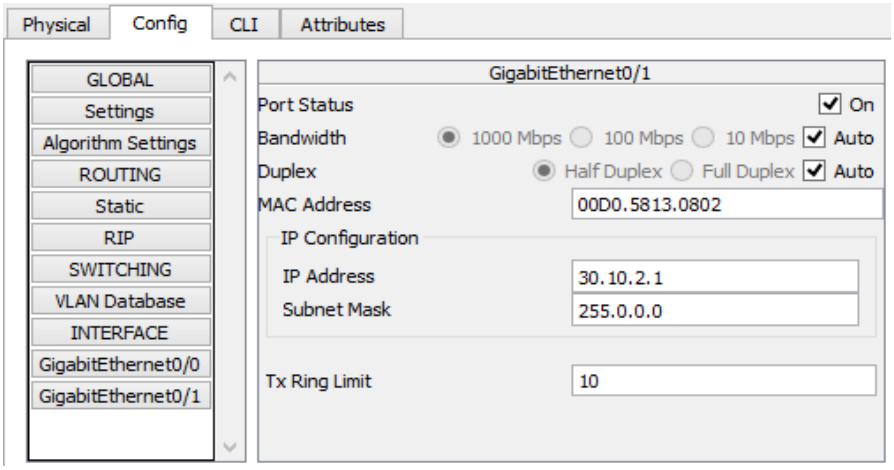


Assigning IP Address To Router 0 :

Open>>Router0>>config>>GigabitEthernet0/0>>ipconfiguration>>ipaddress>>10.10.1.2>> subnetmask>>255.0.0.0>>Port>> ON

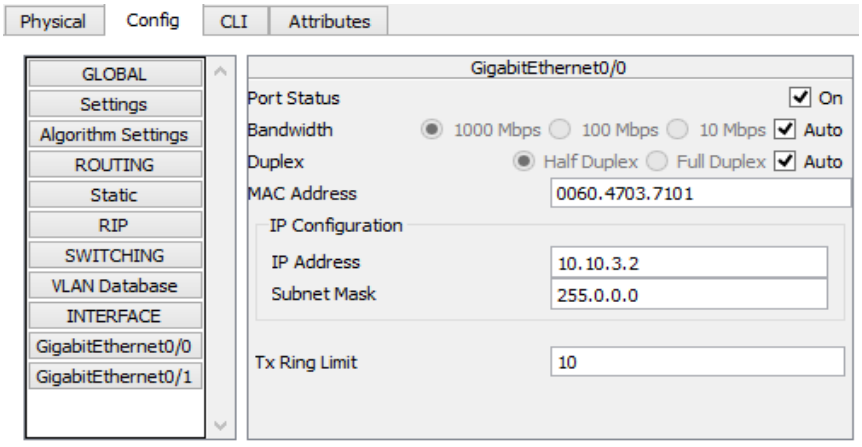


Open>>Router0>>confiig>>GigabitEthernet0/1>>ipconfiguration>>ipaddress>>30.10.2.1>> subnetmask>>255.0.0.0>>Port>> ON

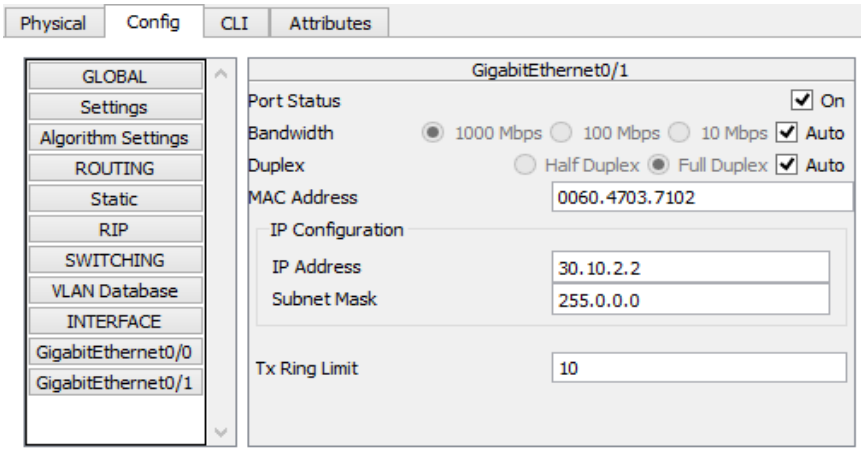


Assigning IP Address To Router 1:

Open>>Router1>>config>>GigabitEthernet0/0>>ipconfiguration>>ipaddress>>10.10.3.2>> subnetmask>>255.0.0.0>>Port>>ON



Open>>Router1>>config>>GigabitEthernet0/1>>ipconfiguration>>ipaddress>>30.10.2.2>>
subnetmask>>255.0.0.0>>Port>> ON



Configuring OSPF ON Router 0 & Router 1:-

Router 0 CLI::

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 10.10.1.0 255.0.0.0 area 0
Router(config-router)#network 30.10.2.0 255.0.0.0 area 0
Router(config-router)#exit
Router(config)#exit
Router#
```

Router 1 CLI::

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 30.10.2.0 255.0.0.0 area 0
Router(config-router)#network 10.10.3.0 255.0.0.0 area 0
Router(config-router)#exit
Router(config)#exit
Router#
```

OUTPUT:-

Goto R0:CLI

Router#sh ip ospf

```
Router#sh ip ospf
 Routing Process "ospf 1" with ID 30.10.2.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x0135a9
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Router#sh ip ospf neighbour

Router#sh ip ospf database

```
Router#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
30.10.2.2         1   FULL/BDR        00:00:31    30.10.2.2
GigabitEthernet0/1
Router#sh ip ospf database
            OSPF Router with ID (30.10.2.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
Link count
30.10.2.1       30.10.2.1       216         0x80000003 0x005338 2
30.10.2.2       30.10.2.2       164         0x80000003 0x00c9be 2

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
30.10.2.1       30.10.2.1       216         0x80000001 0x0018b3
```

Router#sh ip ospf int Gig 0/0

```
Router#sh ip ospf int Gig 0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.10.1.2/8, Area 0
  Process ID 1, Router ID 30.10.2.1, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 30.10.2.1, Interface address 10.10.1.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:02
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

To change the Hello and Dead Interval Of Interface Gig 0/0 type the following commands:-

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int Gig 0/0
Router(config-if)#ip ospf hello-interval 20
Router(config-if)#ip ospf dead-interval 30
Router(config-if)#exit
Router(config)#exit
Router#
```

Now to check weather the interval of Hello and Dead changed type:

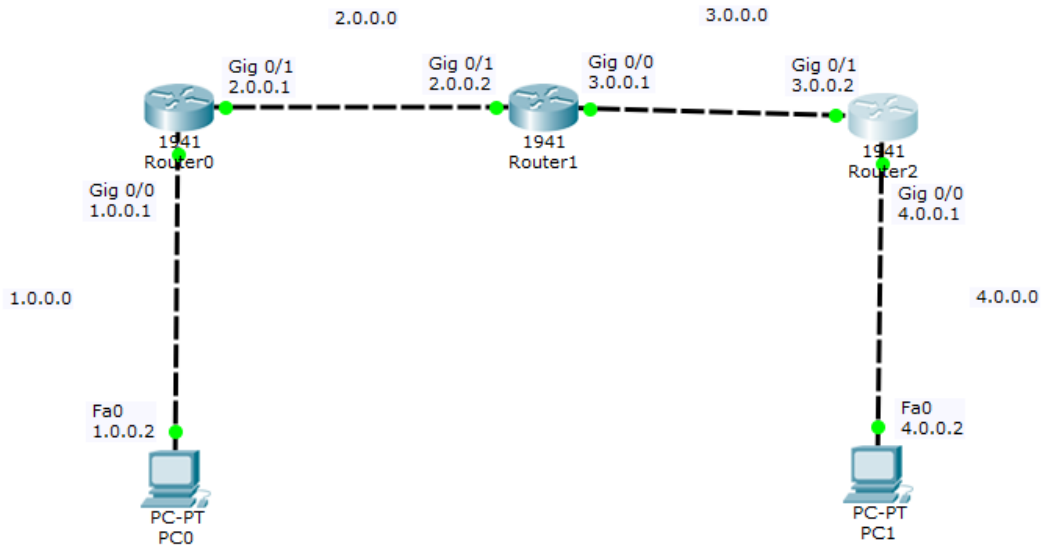
Router#sh ip ospf int Gig 0/0

```
Router#sh ip ospf int Gig 0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.10.1.2/8, Area 0
  Process ID 1, Router ID 30.10.2.1, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 30.10.2.1, Interface address 10.10.1.2
  No backup designated router on this network
  Timer intervals configured, Hello 20, Dead 30, Wait 30,
Retransmit 5
    Hello due in 00:00:15
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Perform the same for Interface Gig 0/1 to change Hello and Dead Interval.

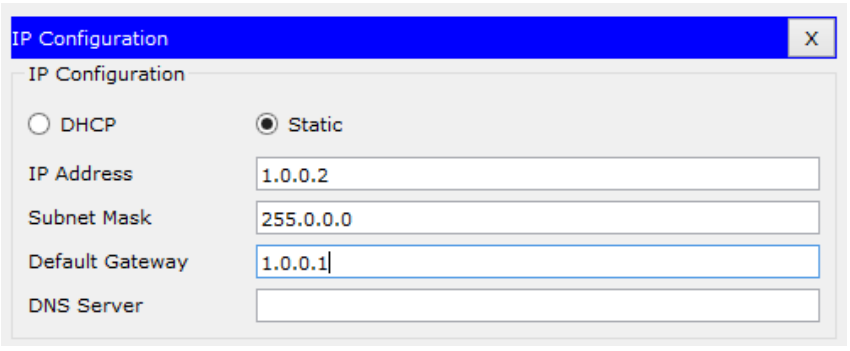
Practical 06(B)
Configuring Multiple Area OSPF

Aim: Configuring Multiple Area OSPF.



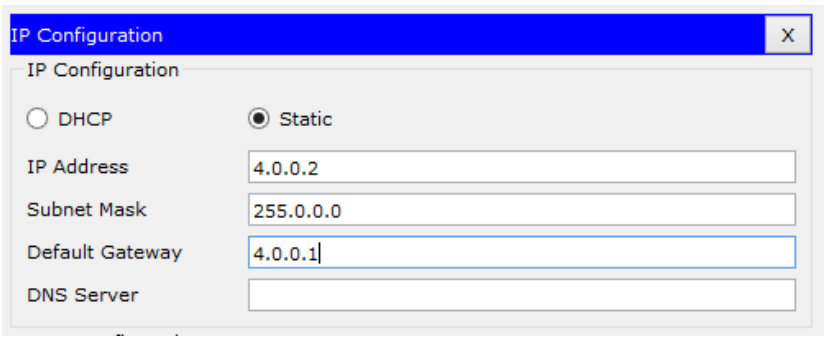
Assigning IP Address to PC0:

Open>>PC0>>Desktop>>IP Configuration>>IP Address>>1.0.0.2>>Default Gateway>>1.0.0.1



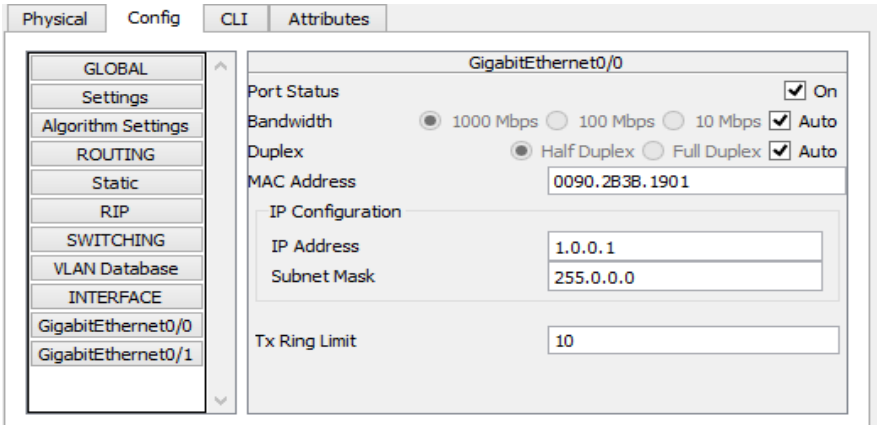
Assigning IP Address to PC1:

Open>>PC1>>Desktop>>IP Configuration>>IP Address>>4.0.0.2>>Default Gateway>>4.0.0.1

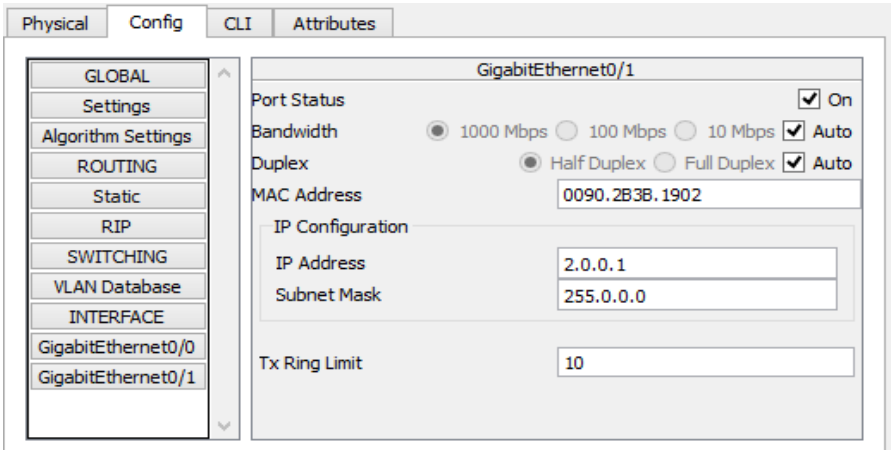


Assigning IP address to Router0:

Open>>Router0>>Config>>GigabitEthernet0/0>>IP Address>>1.0.0.1>>Subnet Mask>>255.0.0.0>>Port>>On

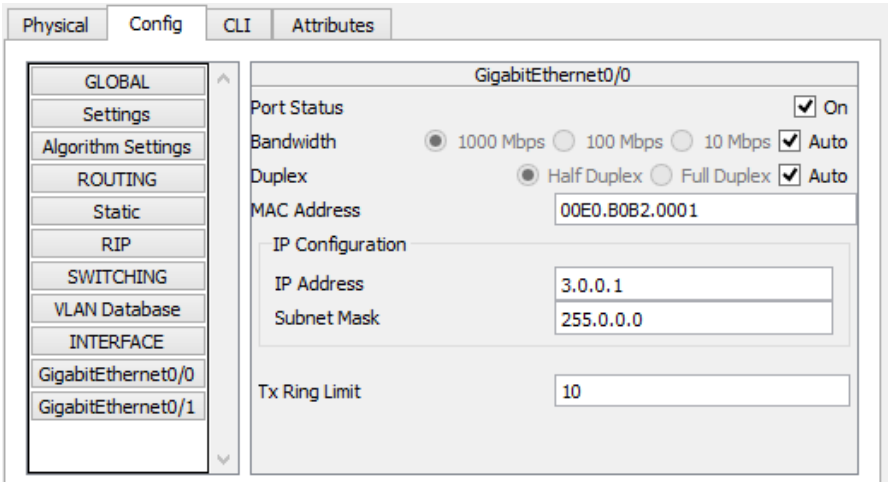


Open>> Router0>>Config>>GigabitEthernet0/1>>IP Address>>2.0.0.1>>Subnet Mask>>255.0.0.0>>Port >>On

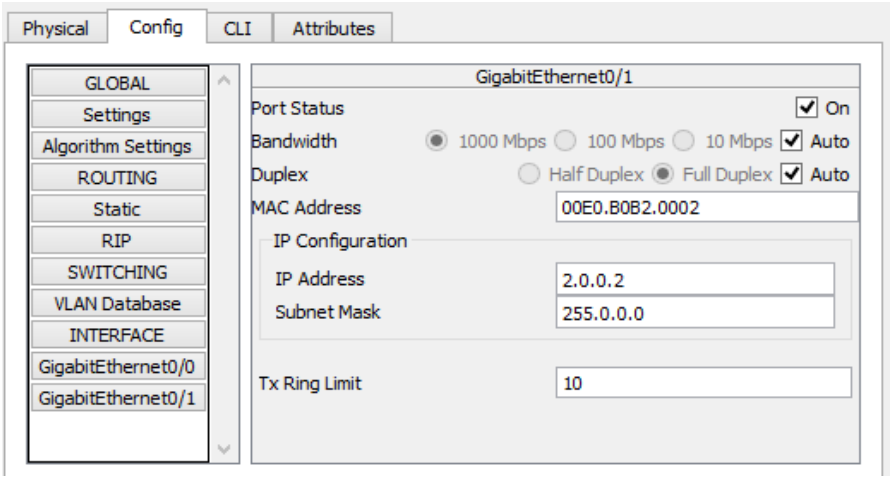


Assigning IP address to Router1:

Open>>Router1>>Config>>GigabitEthernet0/0>>IP Address>>3.0.0.1>>Subnet Mask>>255.0.0.0>>Port>>On

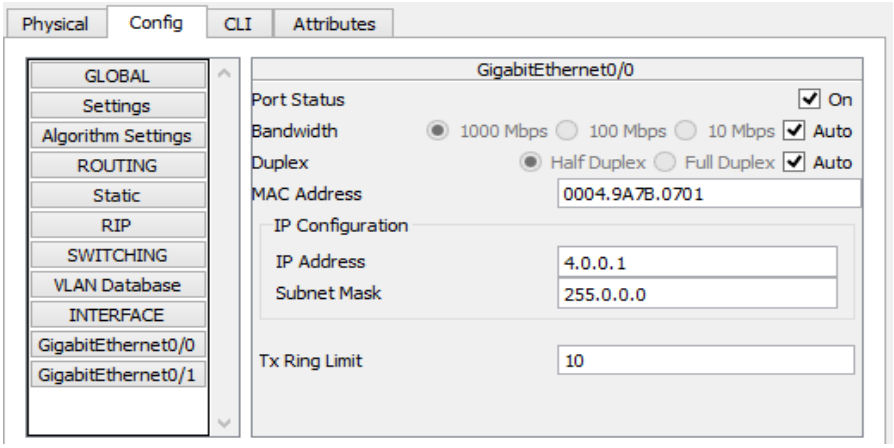


Open>> Router1>>Config>>GigabittEthernet0/1>>IP Address>>2.0.0.2>>Subnet Mask>>255.0.0.0>>Port>>On

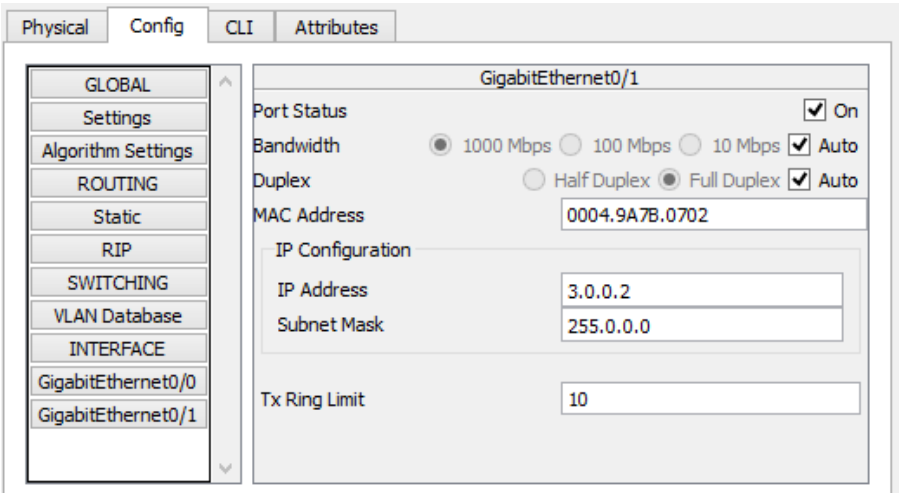


Assigning IP address to Router2:

Open>> Router2>>Config>>GigabittEthernet0/0>>IP Address>>4.0.0.1>>Subnet Mask>>255.0.0.0>>Port>>On



Open>> Router2>>Config>>GigabitEthernet0/1>>IP Address>>3.0.0.2>>Subnet Mask>>255.0.0.0>>Port>>On



Configuring OSPF on Router 0 , Router 1 & Router 2:-

Router 0 CLI::

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 1.0.0.0 255.0.0.0 area 0
Router(config-router)#network 2.0.0.0 255.0.0.0 area 0
Router(config-router)#exit
Router(config)#exit
Router#
```

Router 1 CLI::

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 2.0.0.0 255.0.0.0 area 0
Router(config-router)#network 3.0.0.0 255.0.0.0 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

Router 2 CLI::

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 3.0.0.0 255.0.0.0 area 1
Router(config-router)#network 4.0.0.0 255.0.0.0 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

OUTPUT: For router R1:

Router#sh ip ospf

```
Router#sh ip ospf
 Routing Process "ospf 1" with ID 3.0.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 5 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x02eaa3
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
 --More--
```

Router#sh ip ospf neighbor

```
Router#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
2.0.0.1           1   FULL/DR         00:00:34    2.0.0.1
GigabitEthernet0/1
4.0.0.1           1   FULL/BDR        00:00:31    3.0.0.2
GigabitEthernet0/0
```

Router#sh ip ospf database

```
Router#sh ip ospf database
            OSPF Router with ID (3.0.0.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
2.0.0.1         2.0.0.1         398         0x80000003 0x00b87c 2
3.0.0.1         3.0.0.1         364         0x80000003 0x00e260 1

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
2.0.0.1         2.0.0.1         398         0x80000001 0x00bead

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
3.0.0.0         3.0.0.1         359         0x80000001 0x004b0c
4.0.0.0         3.0.0.1         229         0x80000002 0x00460e

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
3.0.0.1         3.0.0.1         270         0x80000002 0x00e85a 1
4.0.0.1         4.0.0.1         234         0x80000003 0x00b575 2

                Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
3.0.0.1         3.0.0.1         270         0x80000001 0x004992

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
2.0.0.0         3.0.0.1         359         0x80000001 0x0058ff
 --More--
```

Router#sh ip ospf neighbor detail

```
Router#sh ip ospf neighbor detail
 Neighbor 2.0.0.1, interface address 2.0.0.1
    In the area 0 via interface GigabitEthernet0/1
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 2.0.0.1 BDR is 2.0.0.2
    Options is 0x00
    Dead timer due in 00:00:30
    Neighbor is up for 00:09:09
    Index 1/1, retransmission queue length 0, number of retransmission
0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 4.0.0.1, interface address 3.0.0.2
    In the area 1 via interface GigabitEthernet0/0
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 3.0.0.1 BDR is 3.0.0.2
    Options is 0x00
    Dead timer due in 00:00:38
    Neighbor is up for 00:07:02
    Index 2/2, retransmission queue length 0, number of retransmission
0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Router#sh ip ospf int Gig 0/0

```
Router#sh ip ospf int Gig 0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 3.0.0.1/8, Area 1
  Process ID 1, Router ID 3.0.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.0.0.1, Interface address 3.0.0.1
  Backup Designated Router (ID) 4.0.0.1, Interface address 3.0.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 4.0.0.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

To change the Hello and Dead Interval Of Interface Gig 0/0 type the following commands:-

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int Gig 0/0
Router(config-if)#ip ospf hello-interval 30
Router(config-if)#ip ospf dead-interval 20
Router(config-if)#exit
Router(config)#exit
Router#
```

Now to check weather the interval of Hello and Dead changed type:

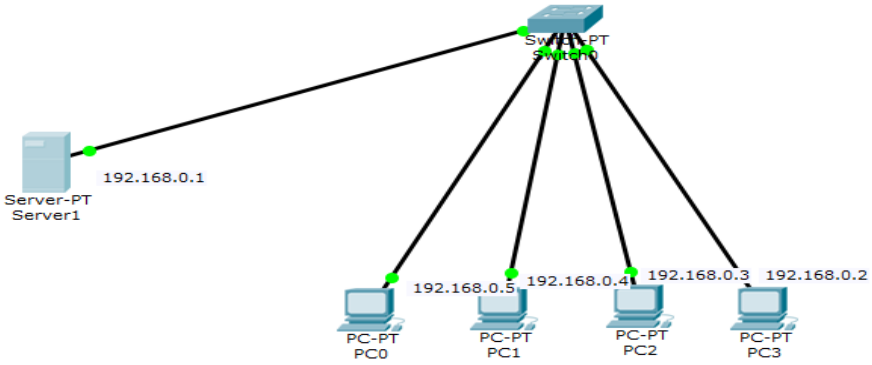
Router#sh ip ospf int Gig 0/0

```
Router#sh ip ospf int Gig 0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 3.0.0.1/8, Area 1
  Process ID 1, Router ID 3.0.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.0.0.1, Interface address 3.0.0.1
  No backup designated router on this network
  Timer intervals configured, Hello 30, Dead 20, Wait 20, Retransmit
    Hello due in 00:00:23
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Perform the same for Interface Gig 0/1 to change Hello and Dead Interval.

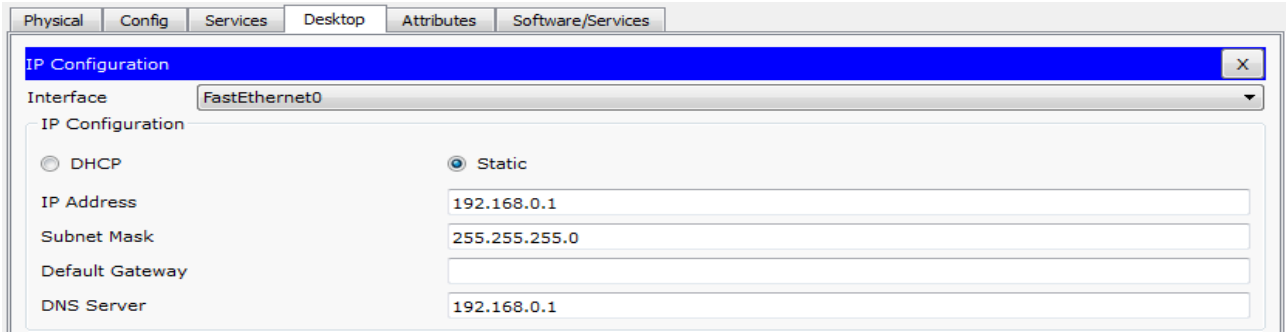
Practical 07
Configuring DNS

Aim: Configuring DNS Server and Client.



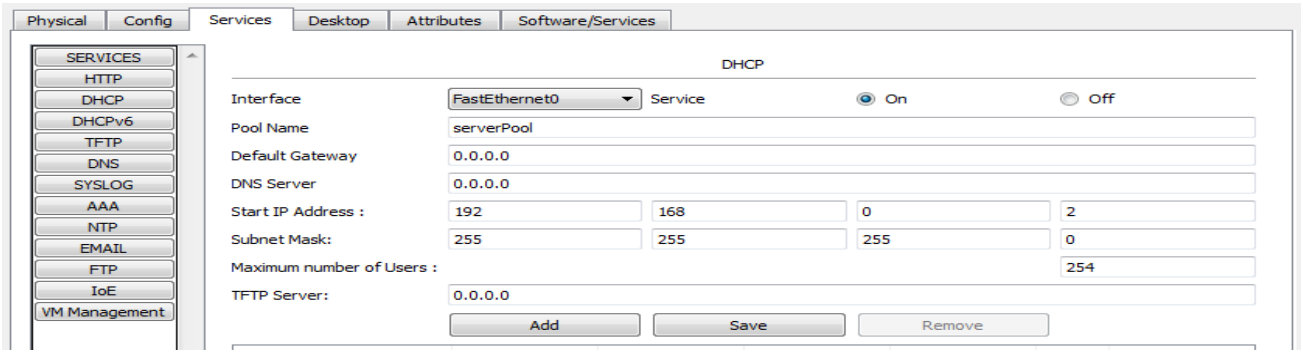
Assigning IP Address To Server-PT Server1:

Open>>Server-PT Server1>>Desktop>>IP Configure>>IP Address>>192.168.0.1>>Subnet Mask>>255.255.255.0>>DNS Server>>192.168.0.1



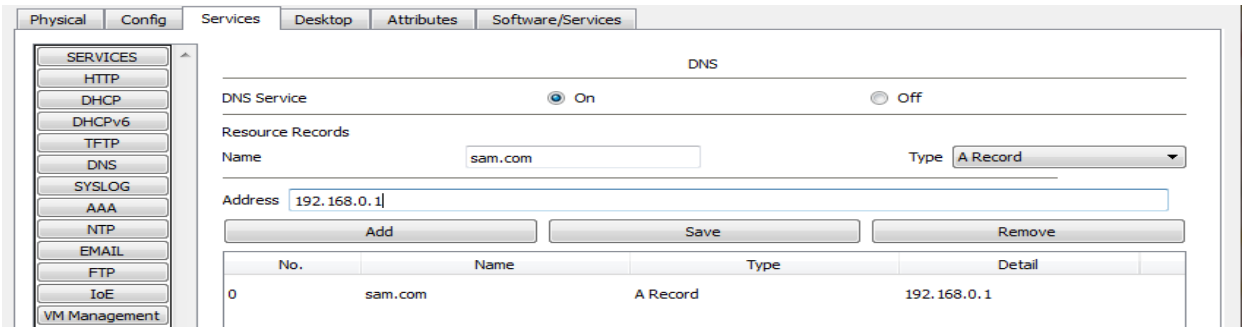
Assigning IP Address To Server-PT Server1 Through DHCP :

Open>>Server-PT Server1>>Services>>DHCP >>Start IP Address>>192.168.0.2 >>Subnet Mask>>255.255.255.0>>DHCP Service>>ON>>Save



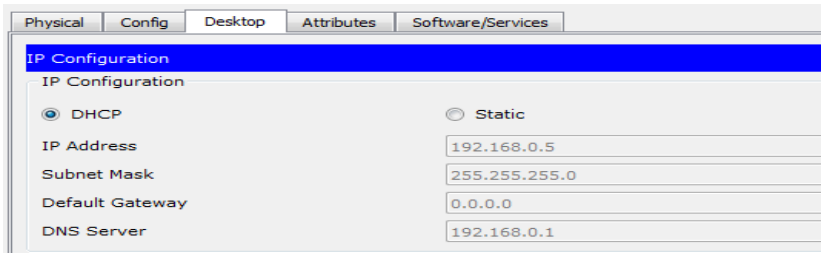
Assigning DNS NAME AND ADDRESS To Server-PT Server1 Through DNS:

Open>>ServerPTServer1>>Services>>DNS>>NAME>sam.com>>Address>>192.168.0.1>> DNS Service>>ON>>Save



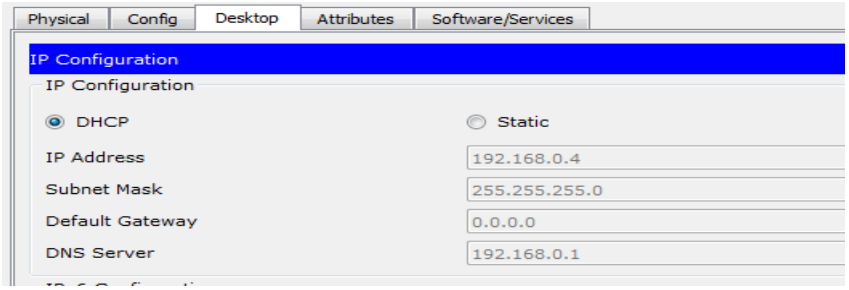
Assigning IP Address To PC0:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.5



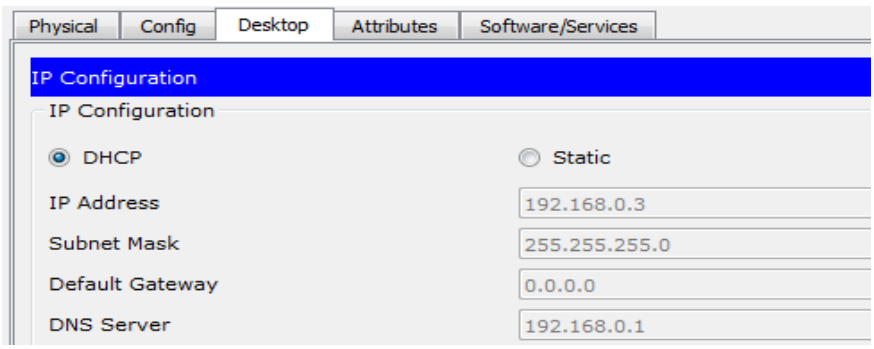
Assigning IP Address To PC1:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.4



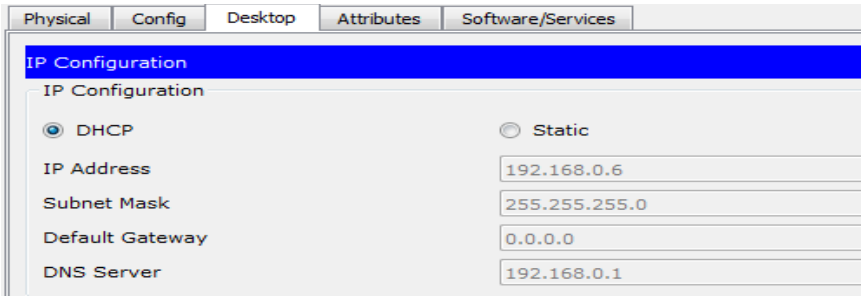
Assigning IP Address To PC2:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.3

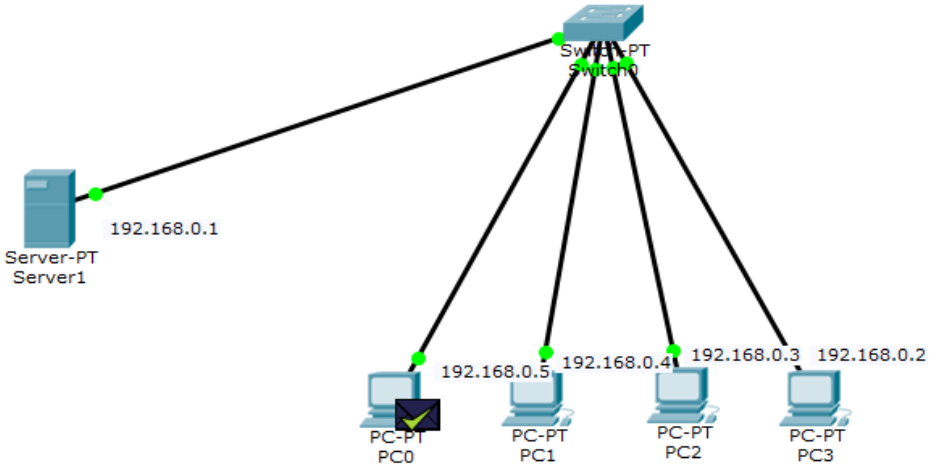


Assigning IP Address To PC4:

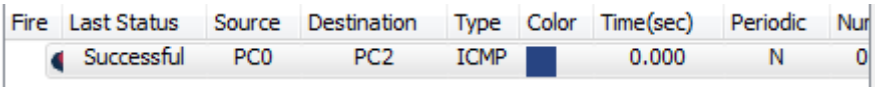
Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.2



Sending message:



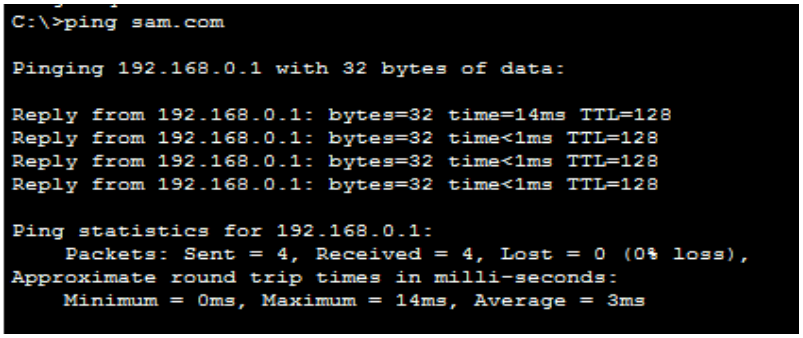
Succesfull:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Nur
	Successful	PC0	PC2	ICMP		0.000	N	0

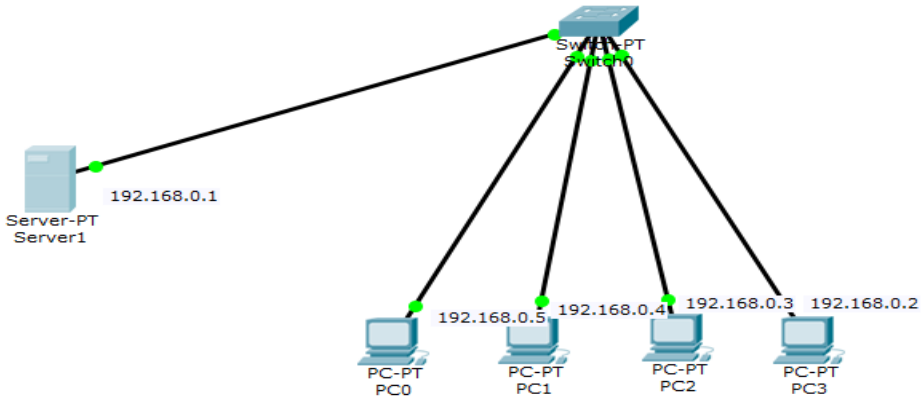
Check connection using ping command:

Open>>PC0>>Desktop>>Command Prompt>>ping sam.com >>Enter



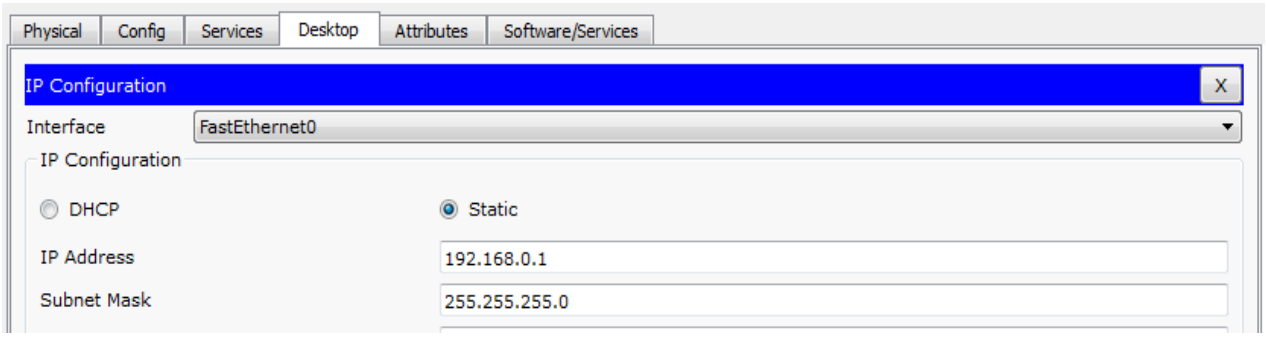
Practical 08
Configuring DHCP

Aim: Configuring DHCP Server and Client.



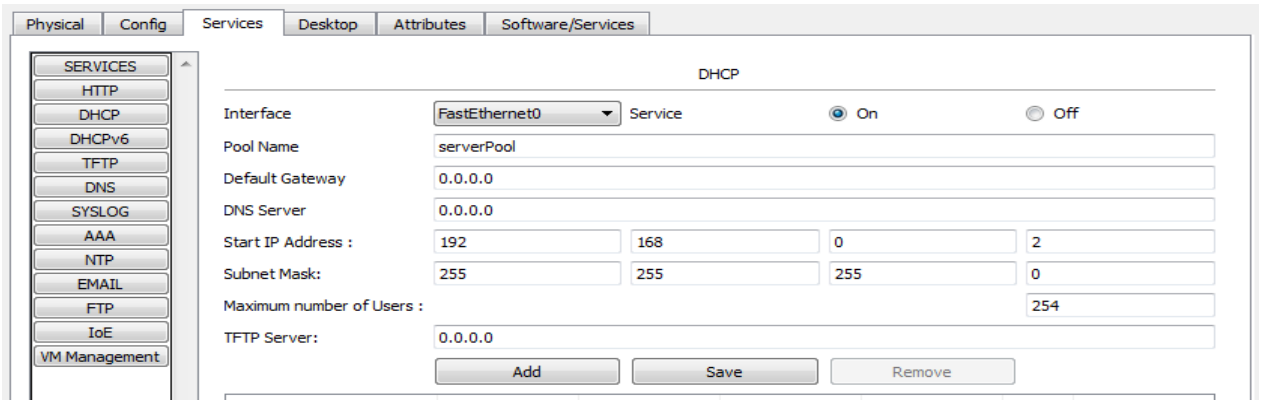
Assigning IP Address To Server-PT Server1:

Open>>Server-PT Server1>>Desktop>>IP Configure>>IP Address>>192.168.0.1>>Subnet Mask>>255.255.255.0



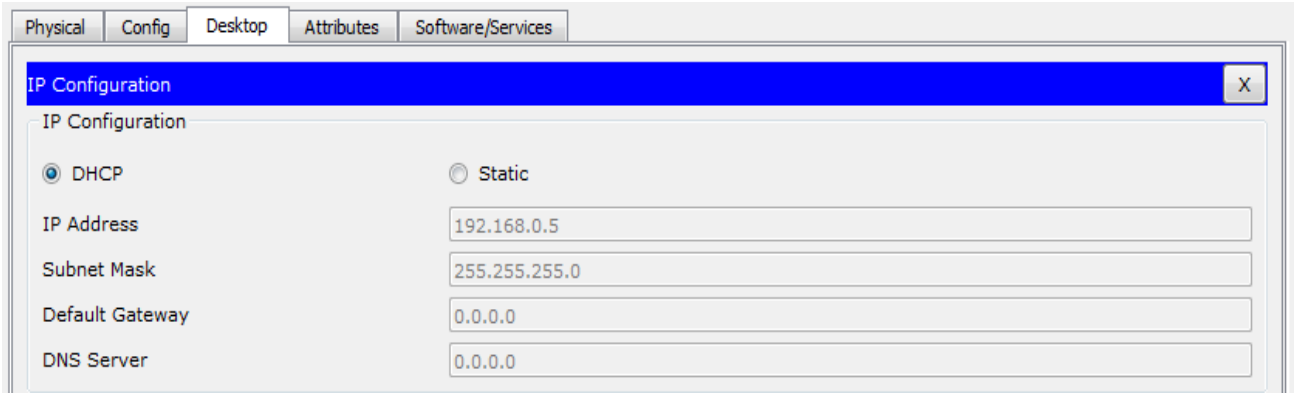
Assigning IP Address To Server-PT Server1 Through DHCP :

Open>>Server-PT Server0>>Services>>DHCP >>Start IP Address>>192.168.0.2 >>Subnet Mask>>255.255.255.0>>DHCP Service>>ON>>Save



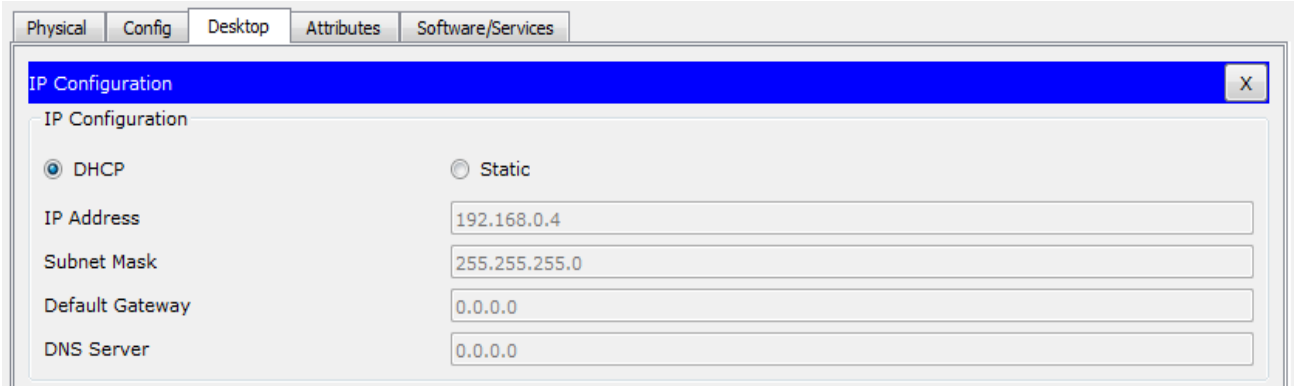
Assigning IP Address To PC0:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.5



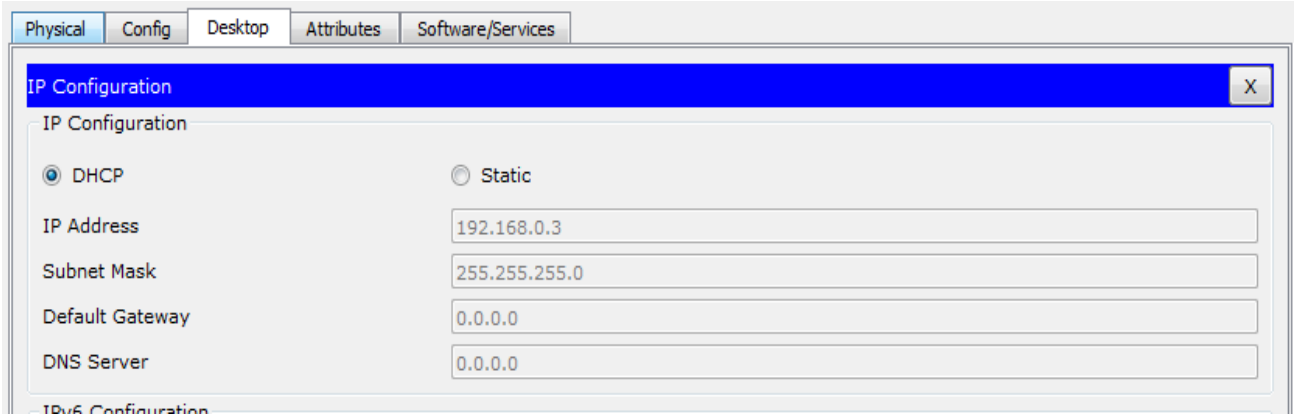
Assigning IP Address To PC1:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.4



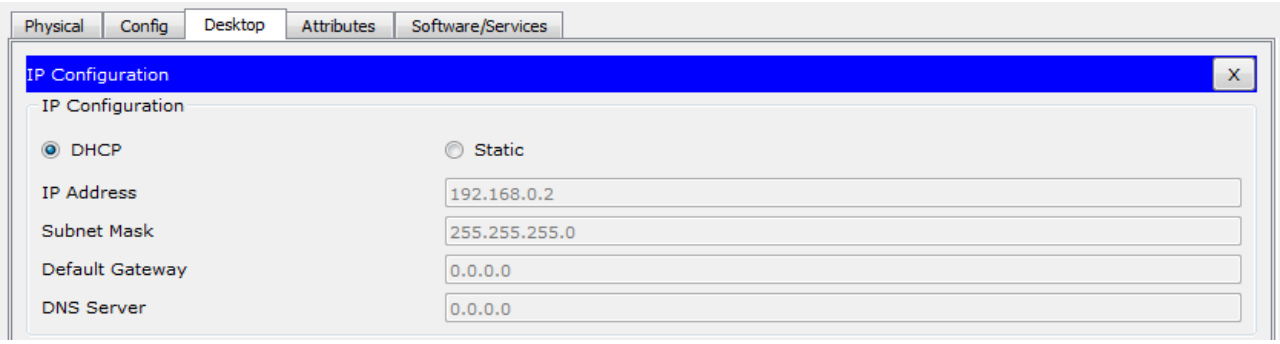
Assigning IP Address To PC2:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.3

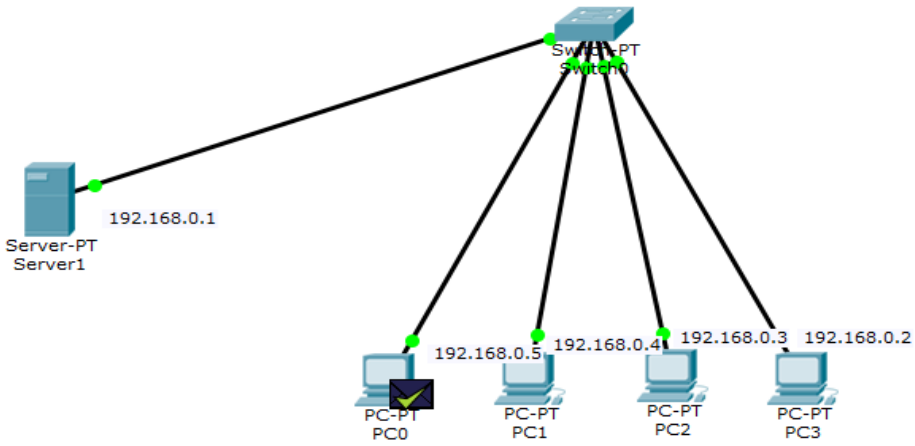


Assigning IP Address To PC4:

Open>>PC-PT PC0>> Desktop>>IP Configuration>>IP Address>>DHCP>>192.168.0.2



Sending message:



Succesfull:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Nur
	Successful	PC0	PC2	ICMP		0.000	N	0

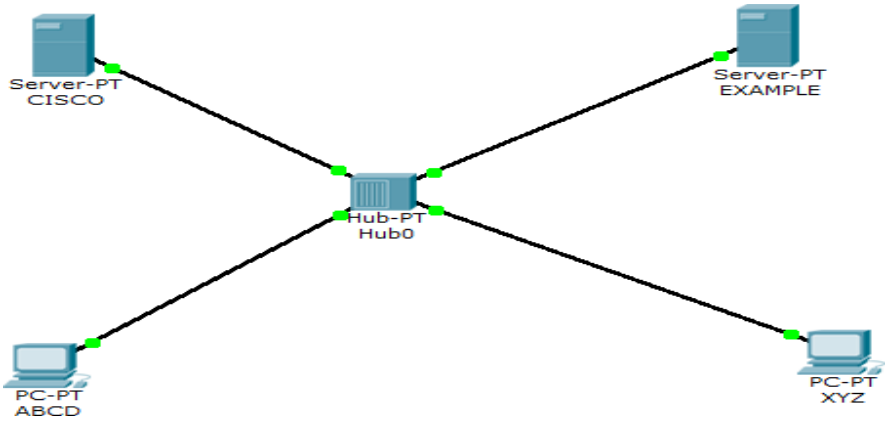
Check connection using ping command:

Open>>PC0>>Desktop>>Command Prompt>>ping 192.168.0.3>>Enter

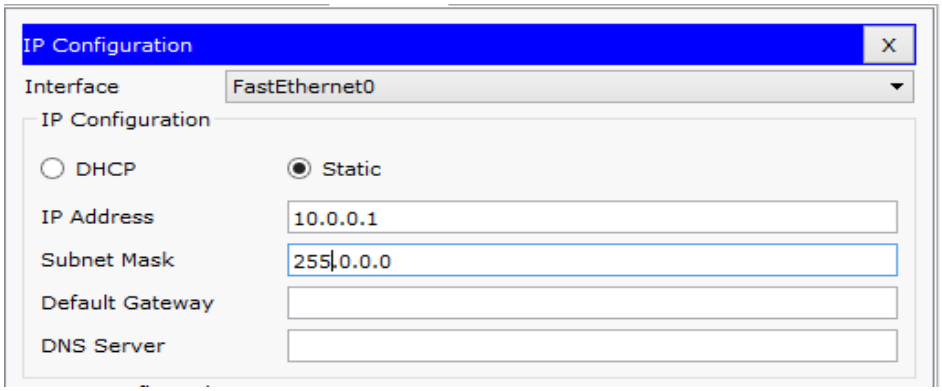
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=4ms TTL=128
Reply from 192.168.0.3: bytes=32 time=4ms TTL=128
Reply from 192.168.0.3: bytes=32 time=4ms TTL=128
Reply from 192.168.0.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms
```

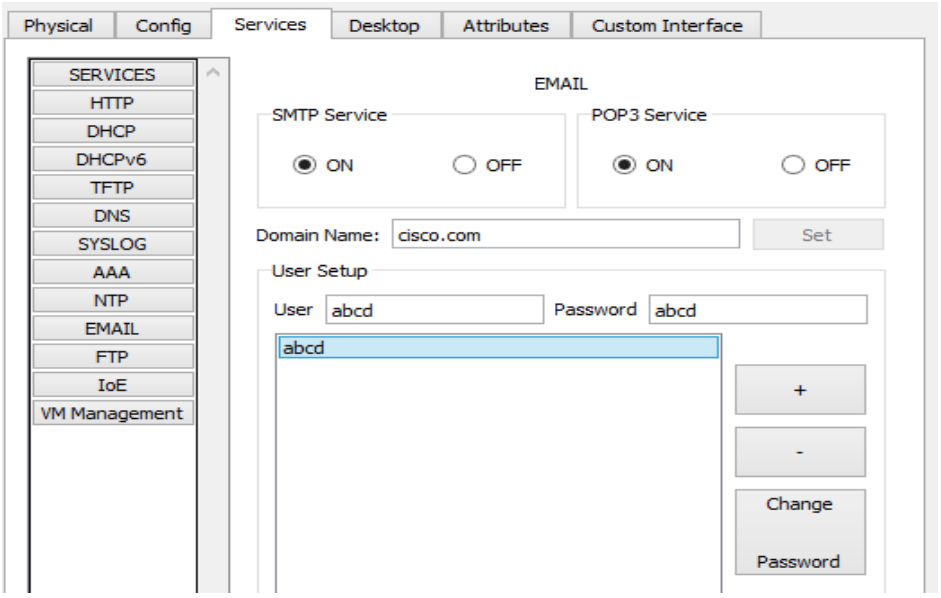
Practical 09
Configuring SMTP, POP3 & IMAP

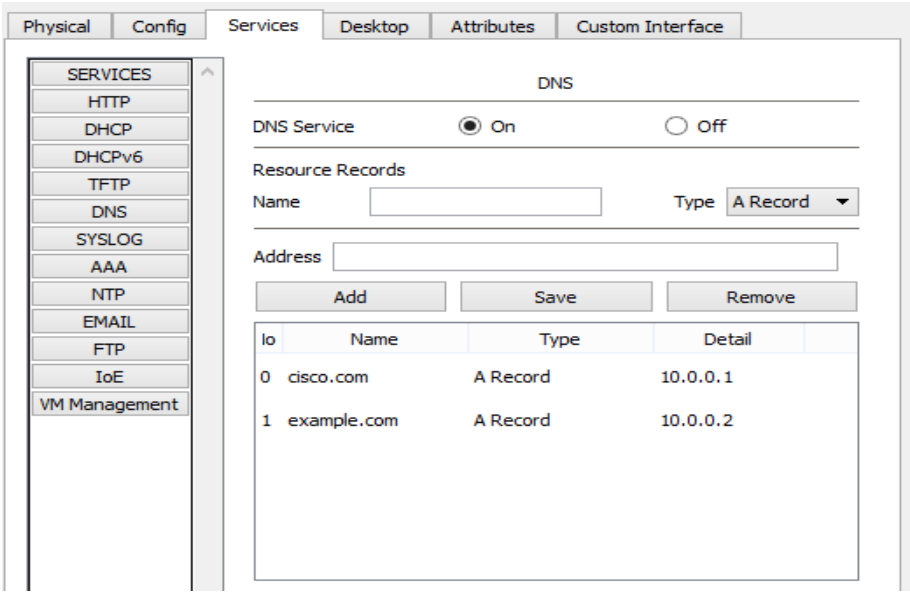
Aim: Configuring SMTP ,POP3 and IMAP



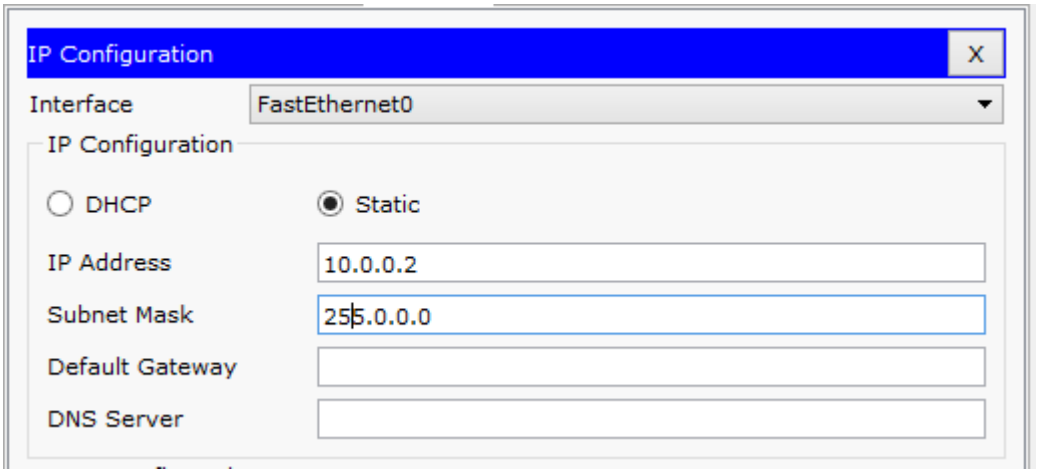
Step 1: Configuring the CISCO server

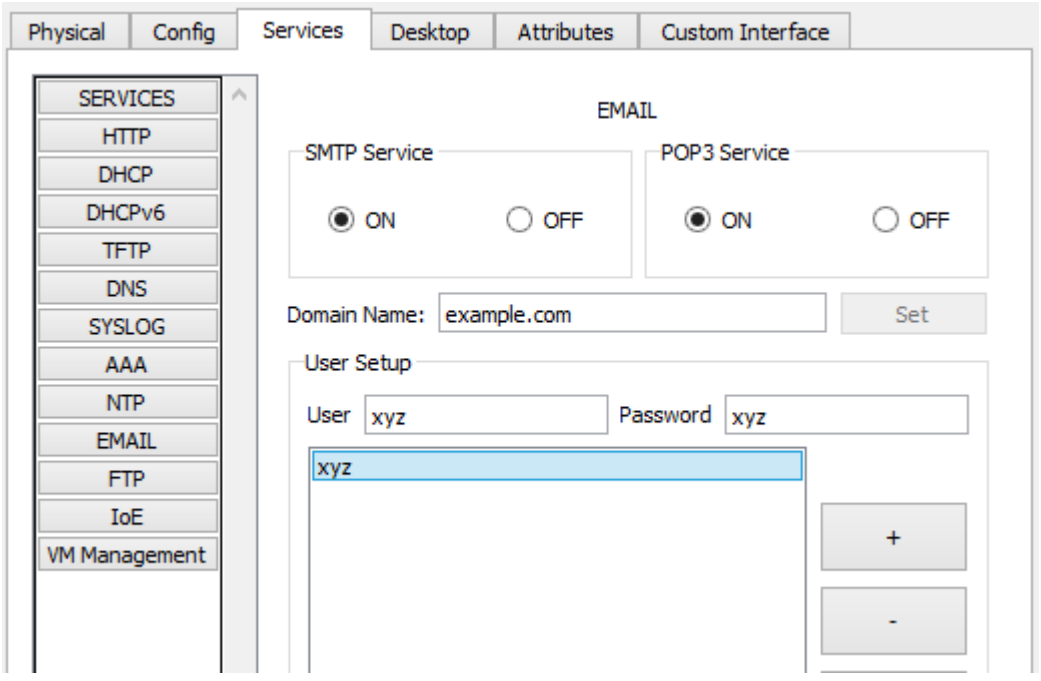


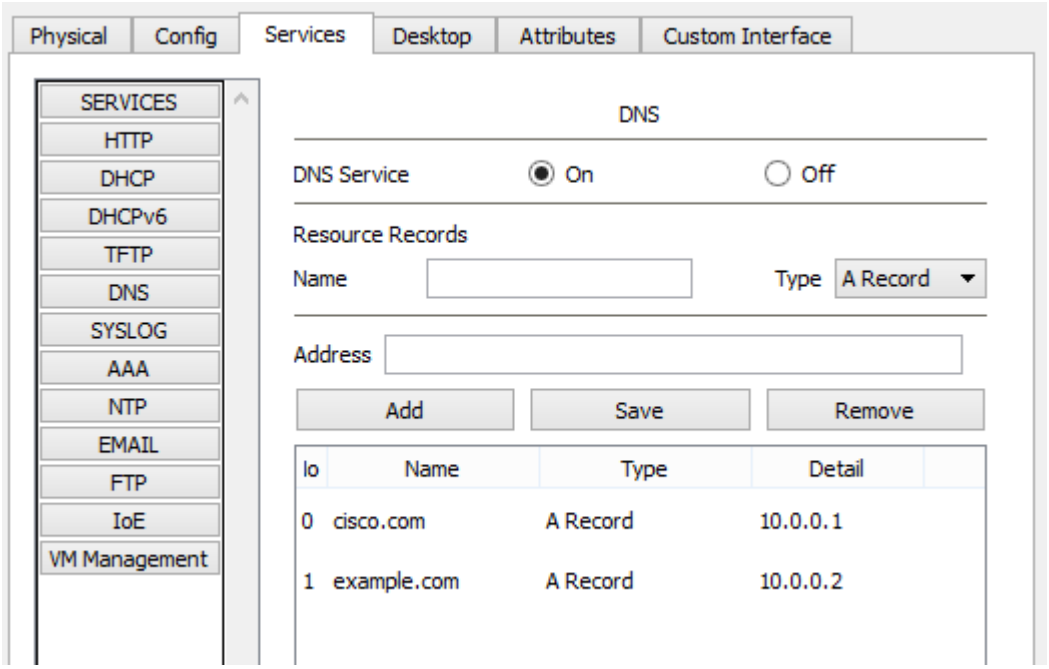


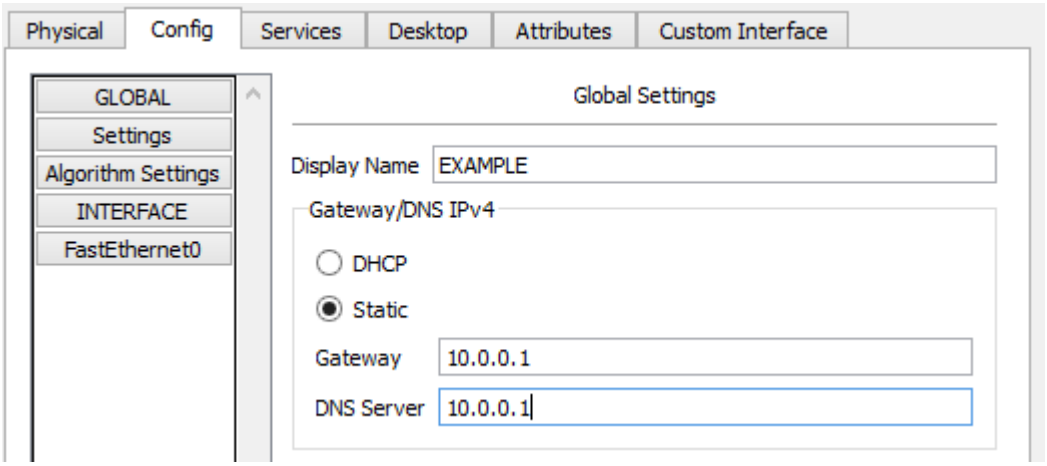


Step 2: Configuring the EXAMPLE server

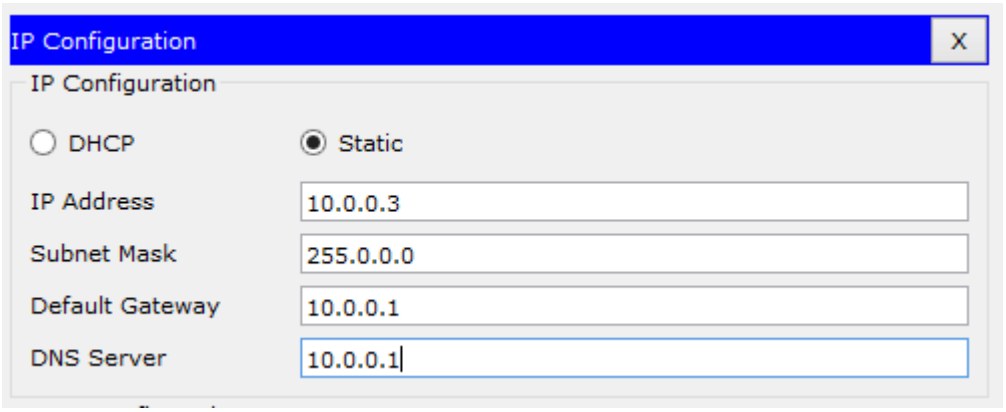


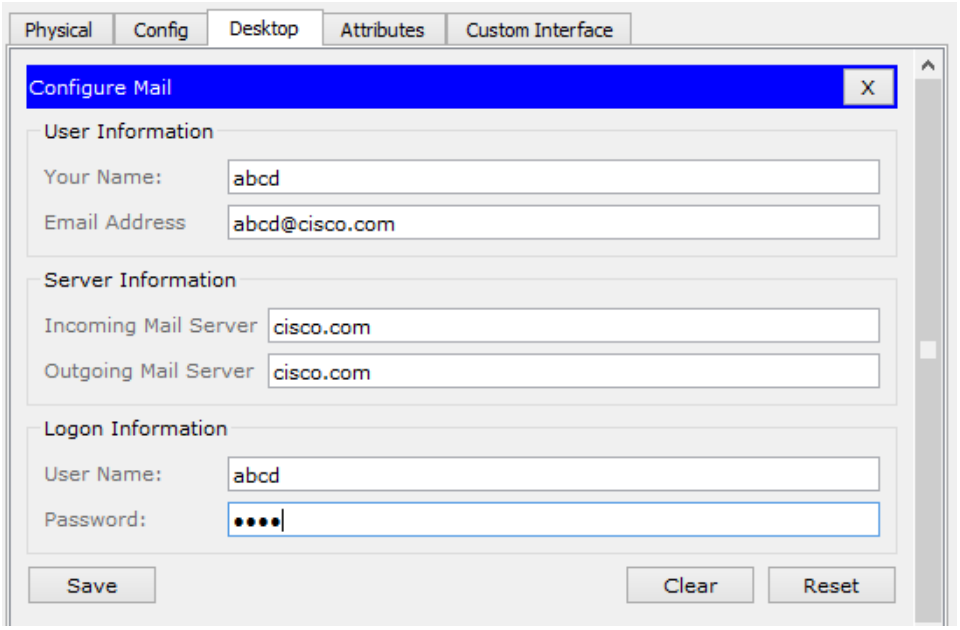




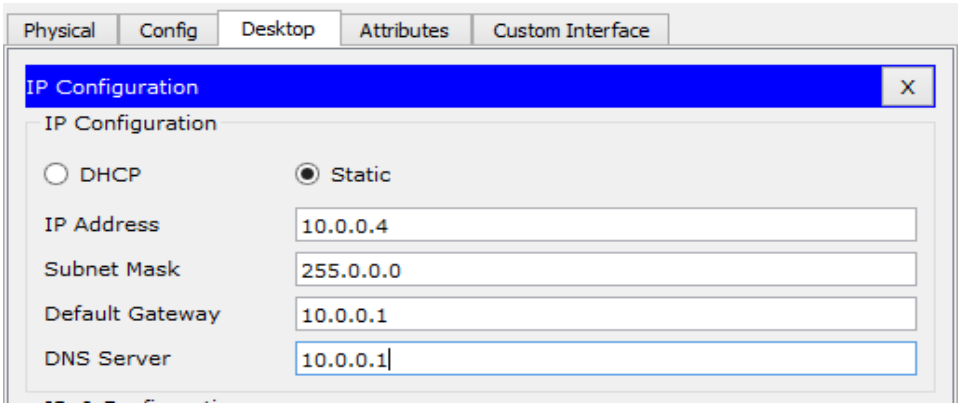


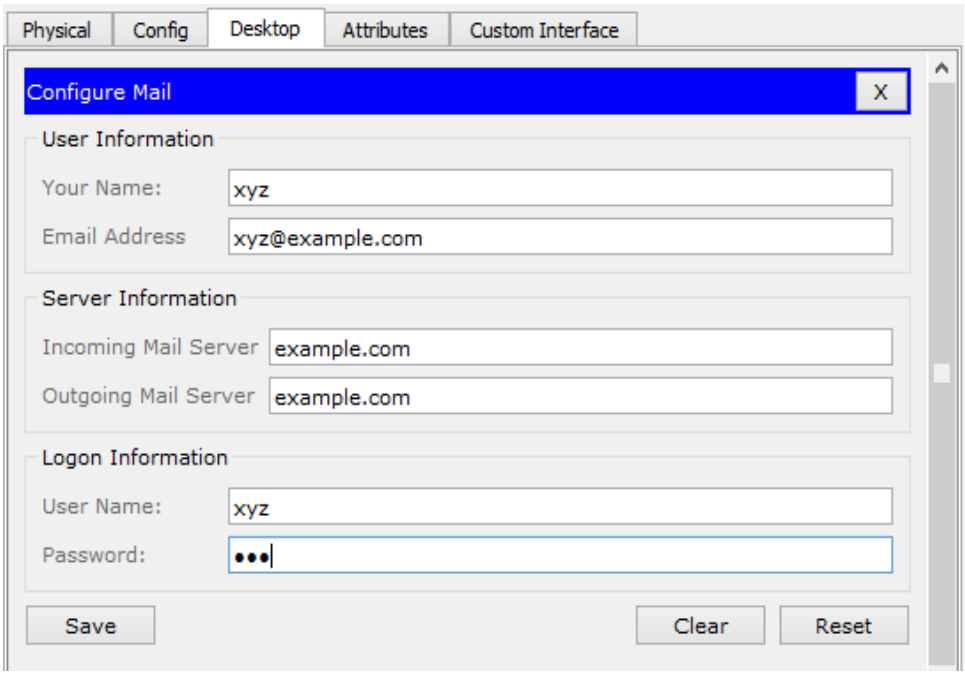
Step 3: Configuring PC0(ABCD)





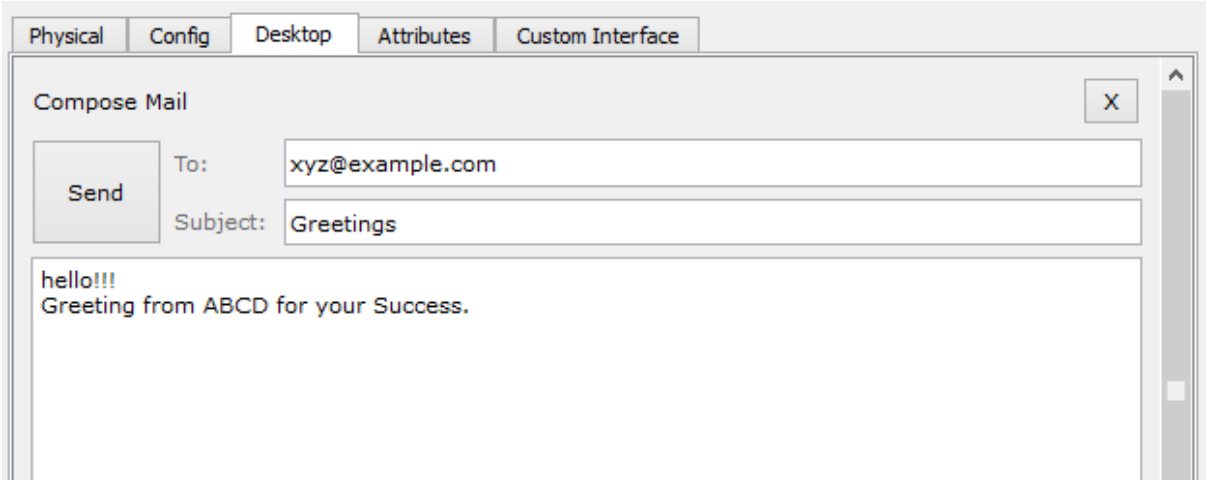
Step 3: Configuring PC1(XYZ)



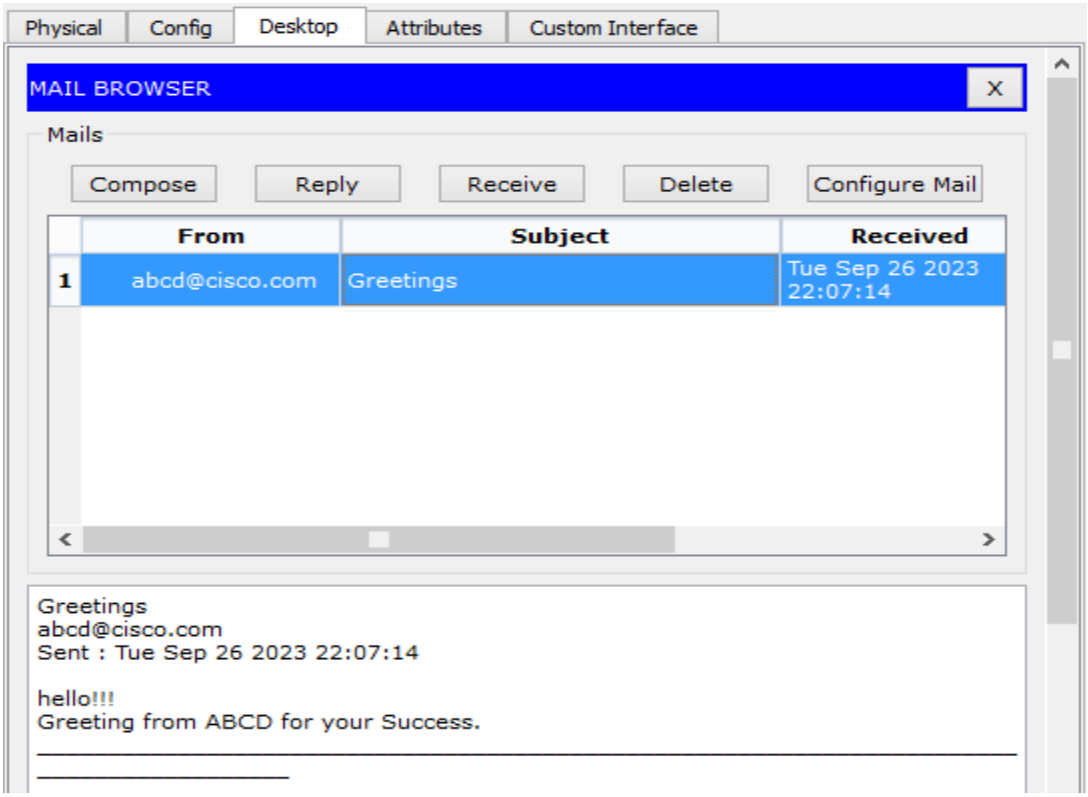


Now we check the working of the mail servers by sending mail as follows:

On PC0(ABCD) Compose a mail and click on Send Button,



Now we check the receiver mail at the PC1(xyz) by clicking on Receive Button,



Hence we have successfully created a mail server and check the working of all the protocols concerned with email.