



*Thakur Educational Trust's (Regd.)*  
**THAKUR COLLEGE OF SCIENCE & COMMERCE**  
AUTONOMOUS COLLEGE, PERMANENTLY AFFILIATED TO UNIVERSITY OF MUMBAI  
NAAC Accredited Grade 'A' (3<sup>rd</sup> Cycle) & ISO 9001: 2015 (Certified)  
**Best College Award by University of Mumbai for the Year 2018-2019**



Thakur College of  
Science & Commerce

**COMPUTER NETWORKING  
MANUAL**  
3<sup>rd</sup> SEMESTER ( B.Sc. I.T. )



## **LIST OF EXPERIMENTS**

### **( Using CISCO Packet tracer )**

**1. (A) IPv4 addressing and sub-netting.**

**(B) Find the first and the last address of :**

**i. 180.8.17.9**

**ii. 25.34.12.56/16**

**2. Use the basic commands of TCP/IP in Cisco packet tracer.**

**3. Configuring IP static routing.**

**4. Configuring IP RIP routing.**

**5. Configuring IP OSPF routing.**

**6. Configuring IP DHCP routing.**

**7. (A) Study of different color codes.**

**(B) Study of different connecting devices and their differences.**

**(C) Crimping LAN cable.**

**8. Configuring DNS server.**

**9. Configure basic security features.**

**10. To construct wireless LAN and make PC wireless using DHCP server.**

## **Practical - 1**

### **Practical - 1(A)**

#### **AIM :**

IPv4 addressing and sub-netting.

#### **THEORY :**

Given an IP address and network mask determine other information about IP address such as :-

#### **IP address :**

- IP stands for internet protocol and describes a set of standards and requirements for creating and transforming data packets of data-gram across networks.

#### **Classes of IP address :**

- TCP/IP defines five classes of IP addresses i.e. Class A, B, C, D and E .
- Each class has a range of valid IP address.
- The value of first octet determines the class of the IP addresses.
- IP addresses from first 3 classes A, B, C can be used for addressing.
- The other two classes are used for other purpose.

<b>Class</b>	<b>First octet value(Range)</b>	<b>Sub net mask</b>
A	0 - 127	8
B	128 - 191	16
C	192 - 223	24
D	224 - 239	-
E	240 - 255	-

- Any IP address is divided into two parts :
  - i. Network id - The number of networks.
  - ii. Host id - The number of hosts.

#### **Network address (First address) :**

- A network address is an identifier for a node or host on a telecommunication network.
- The first part of an IP address is used as a network address

### Network broadcast address (Last address) :

- An IP broadcast address is the highest number in this class.
- For e.g. - the broadcast address of class C 192.168.16.0 network is 192.168.16.255
- The broadcast address for a sub-net must account for the part of the address that is reserved for the sub-net.

### Total number of host bits :

- Host bits are the position of an IP address that identify a specific host in a sub-net.

### Number of hosts :

- A host is only a hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack or any other means.
- Table :

Class	Leading bits	Net ID bits	Host bits	No. Of networks	Address per network	Start address	End address
A	0	8	24	$2^7 = 128$	$2^{24} = 16,777,216$	0.0.0.0	127.255.255.255
B	10	16	16	$2^{14} = 16,384$	$2^{16} = 65,536$	128.0.0.0	191.255.255.255
C	110	24	8	$2^{21} = 2,097,152$	$2^8 = 256$	192.0.0.0	223.255.255.255
D	1110	-	-	-	-	224.0.0.0	239.255.255.255
E	1111	-	-	-	-	240.0.0.0	255.255.255.255

## Practical - 1(B)

### AIM :

Find the first address and the last address of :

- i. 180.8.17. 9
- ii. 25.34.12.56/16

### THEORY :

i. 180.8.17. 9 :-

- The given address is class B, therefore  $n=16$
- Number of address (N) -

$$N = 2^{32-n}$$

$$N = 2^{32-16}$$

$$N = 2^{16}$$

$$N = 65,536$$

- First address :

- For class B address, the network ID will be 16.
- Therefore the network mask is 255.255.0.0 .
- To find the first address we logically AND the given address with the network mask.

<b>Given address</b>	180	8	17	9
<b>Network mask</b>	255	255	0	0
<b>AND Operation (First address)</b>	180	8	0	0

- Last address :

- The network Mask is 255.255.0.0 .
- To find the last address we logically OR the given address with the complement of the network mask i.e. 0.0.255.255 .

<b>Given address</b>	180	8	17	9
<b>Network address (complement)</b>	0	0	255	255
<b>OR Operation (Last address)</b>	0	0	255	255

- First address :- 180.8.0.0
- Last address :- 180.8.255.255

ii. 25.34.12.56/16

- The given address is of Class A, therefore  $n = 8$ .

- Number of address (N) -

$$N = 2^{32-n}$$

$$N = 2^{32-8}$$

$$N = 2^{24}$$

$$N = 16,777,216$$

- The number of addresses are 16,777,216

- Network mask - 11111111.0.0.0

255.0.0.0

- First address :

- For class B address, the network ID will be 8.

- Therefore the network mask is 255.0.0.0 .

- To find the first address we logically AND the given address with the network mask.

<b>Given address</b>	25	34	12	36
<b>Network mask</b>	255	0	0	0
<b>AND Operation (First address)</b>	25	0	0	0

- Last address :

- The network Mask is 255.0.0.0 .

- To find the last address we logically OR the given address with the complement of the network mask i.e. 0.255.255.255 .

<b>Given address</b>	25	34	12	36
<b>Network address (complement)</b>	0	255	255	255
<b>OR Operation (Last address)</b>	25	255	255	255

- First address :- 25.0.0.0

- Last address :- 25.255.255.255

## **Practical - 2**

### ● **AIM :**

Use of basic commands of TCP/IP in Cisco packet tracer.

### ● **THEORY :**

- Diagnostic commands helps you to detect TCP/IP networking problem.
- Some of the diagnostic commands are ARP, Host name, IP config, netstat, ping, route, tracert.

#### 1. ARP (Address resolution protocol) :

- This diagnostic command displays and modifies the IP to the Ethernet or token ring, physical address translatable used by ARP.
- It is used to map the IP address to the mac address needed for communication on a local network.
- Basic usage of ARP commands :-
  - i. arp-a : It displays all the entries in the ARP table.
  - ii. arp-s : Adds an ARP (arp-s ip-address mac-address).
  - iii. arp-d : Detects an arp entry (arp-d ip-address).

#### 2. Host name :

- The host name prints the name of the host of which the command is used.

#### 3. IP config :

- The ip config command in windows is used to display and manage the IP configuration of a computer.
- It provides detailed information about the network interface, such as ip address, default gateway and DNS servers.
- Basic usage of ip config command :-
  - i. ip config : This command displays the ip address.
  - ii. ip config/all : This command displays detailed information including mac address, DHCP status, lease information.
  - iii. ip config/release : This command releases current ip address obtained from DHCP server, making the ip address available for reassignment.
  - iv. ip config/renew : This command requests a new ip address from the DHCP server for all the network adapters.
  - v. ip config/flushdns : This command clears the DNS resolver cache which can help to resolve DNS related issue.
  - vi. ip config/displaydns : It displays the DNS cache.

#### 4. Netstat :

- This diagnostic command displays protocol and statistics and current TCP/IP network connection.
- It is very powerful network utility tool used to display network connection, routing tables, interface, statistics and multicast membership.
- It is available on various OS including Windows, Linux and Mac OS.
- Basic usage of netstat command :-
  - i. netstat-a : This command displays all the active connections on the listening port.
  - ii. netstat-an : This command displays only the ports that are listening for the incoming connections.
  - iii. netstat-r : This command displays the kernel routing table.
  - iv. netstat-e : This command displays statistics for each command interface.
  - v. netstat-s : This command displays statistics for each network protocol.
  - vi. netstat-u : This command displays connections by protocols.

#### 5. Ping Command :

- This command is used to test the reachability of host on an internet protocol.

#### 6. Route Command :

- The route command manipulates the network routing table.
- The routing table determines the path data packet take to take their destination.

#### 7. Tracert Command :

- It is used to to determine the path data packets takes to reach a specific destination.
- It works by spending a series of ICMP(Internet Control Message Protocol).
- Eco request message with incrementally increases TTL (Time To Leave) value, which explicitly ICMP time exceeded message from intermediate routers along the path to the destination.
- This allows you to each hop the packet, take along with the round trip for each hop.



## Practical - 3

### ● AIM :

Configure IP Static Routing.

### ● THEORY :

#### Static Routing :

- Static routing method is most trusted by the routers.
- Static routing is not really a routing protocol.
- It do not dynamically adapt to network changes, are not particularly scalable, requires manual updating to reflect changes.

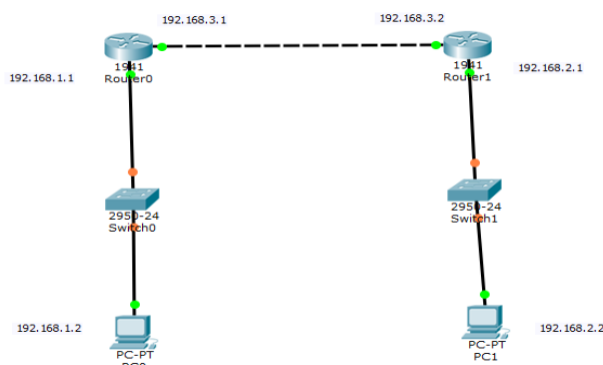
#### Advantages of Static Routing :

- There is no bandwidth usage between routers, which means you could possibly save money on WAN links.
- There is no overhead on the router CPU, which means you could possibly by a cheaper route than you would use if you were using dynamic routing.
- It adds security because the administrator can choose to allow routing access to certain network only.

#### Disadvantages of Static routing :

- Static routing don't dynamically adapt to network changes.
- If a network is added to a inter-network, the administrator has to add a route it on all routers by hand.
- It's not feasible in large network grows, it can be difficult just to keep adding static routes to make sure everybody can still get everything.
- The administrator must really understand the inter-network and how each router is connected in order to configure routers correctly.

#### Topology :

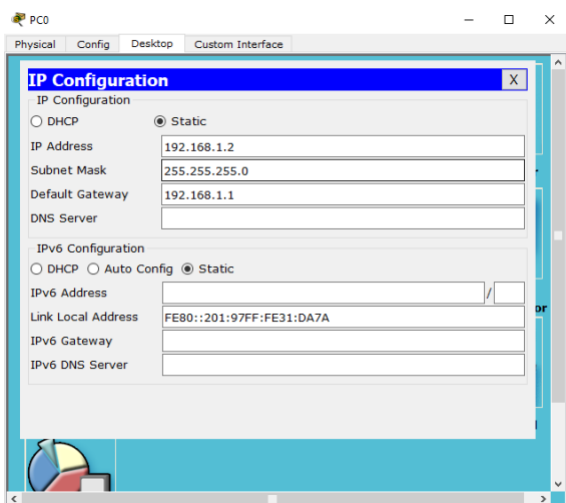


## Routing Table :

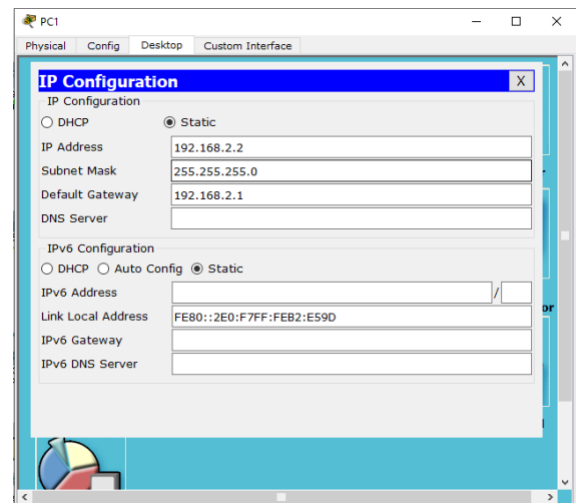
Devices	IP addresses
PC 0	192.168.1.2
PC 1	192.168.2.2
Router 0 (GigabitEthernet 0/0)	192.168.1.1
Router 0 (GigabitEthernet 0/1)	192.168.3.1
Router 1 (GigabitEthernet 0/0)	192.168.2.1
Router 1 (GigabitEthernet 0/1)	192.168.3.2

We configure it as follows :

Step 1 : Configure all PC's with respect to their IP addresses.



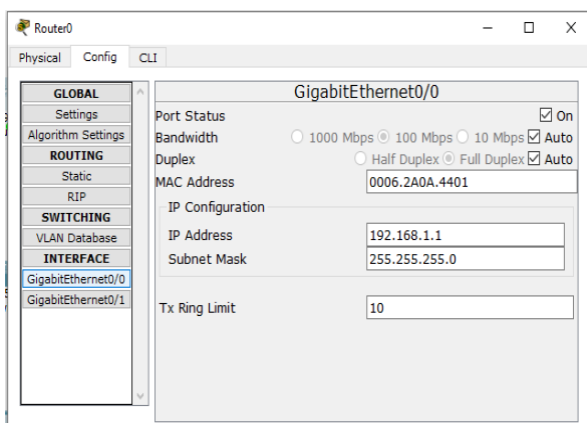
PC 0



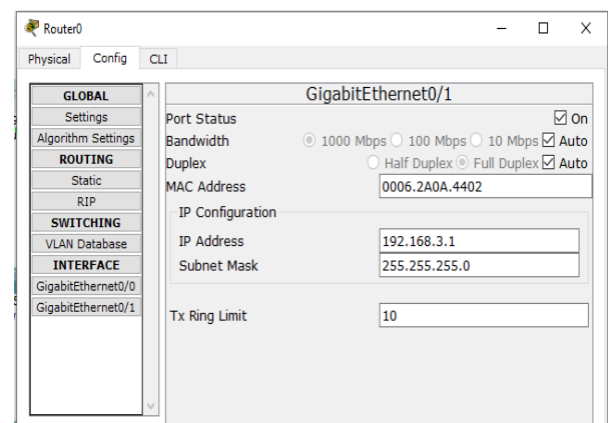
PC 1

Step 2 : Configure all Routers with respect to their IP addresses.

## Router 0

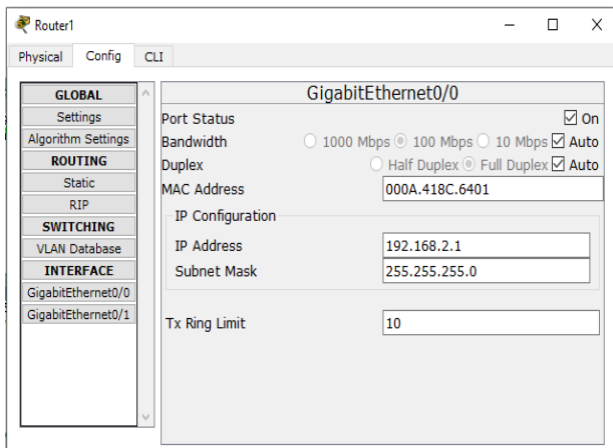


GigabitEthernet 0/0



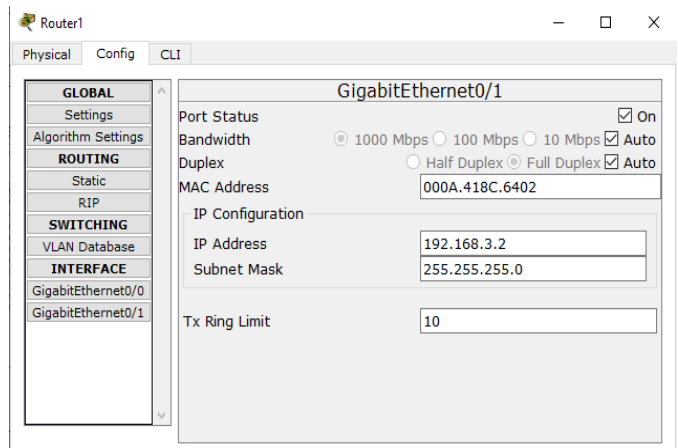
GigabitEthernet 0/1

## Router 1



Router1 configuration window for GigabitEthernet0/0. The left sidebar shows the configuration tree with 'GigabitEthernet0/0' selected. The main panel shows the configuration for this interface. The 'Port Status' is 'On'. 'Bandwidth' is set to '100 Mbps' and 'Auto'. 'Duplex' is set to 'Full Duplex' and 'Auto'. 'MAC Address' is '000A.418C.6401'. 'IP Configuration' shows 'IP Address' as '192.168.2.1' and 'Subnet Mask' as '255.255.255.0'. 'Tx Ring Limit' is '10'.

GigabitEthernet 0/0

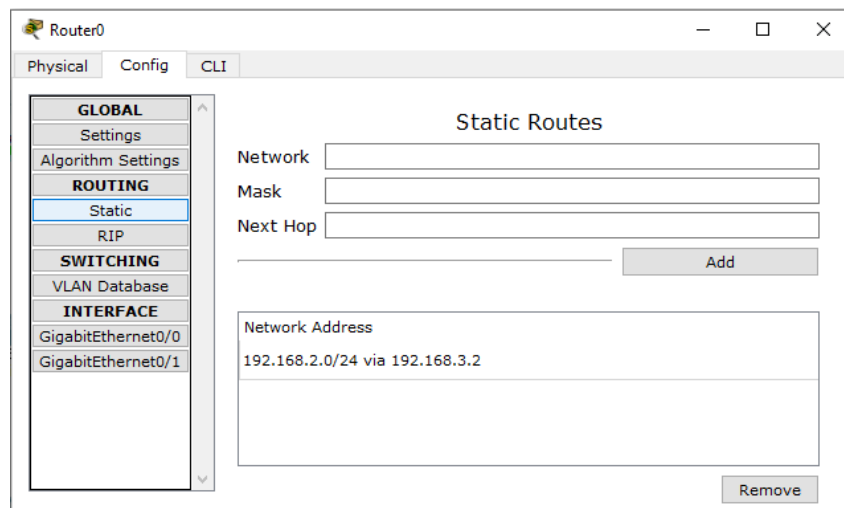


Router1 configuration window for GigabitEthernet0/1. The left sidebar shows the configuration tree with 'GigabitEthernet0/1' selected. The main panel shows the configuration for this interface. The 'Port Status' is 'On'. 'Bandwidth' is set to '100 Mbps' and 'Auto'. 'Duplex' is set to 'Full Duplex' and 'Auto'. 'MAC Address' is '000A.418C.6402'. 'IP Configuration' shows 'IP Address' as '192.168.3.2' and 'Subnet Mask' as '255.255.255.0'. 'Tx Ring Limit' is '10'.

GigabitEthernet 0/1

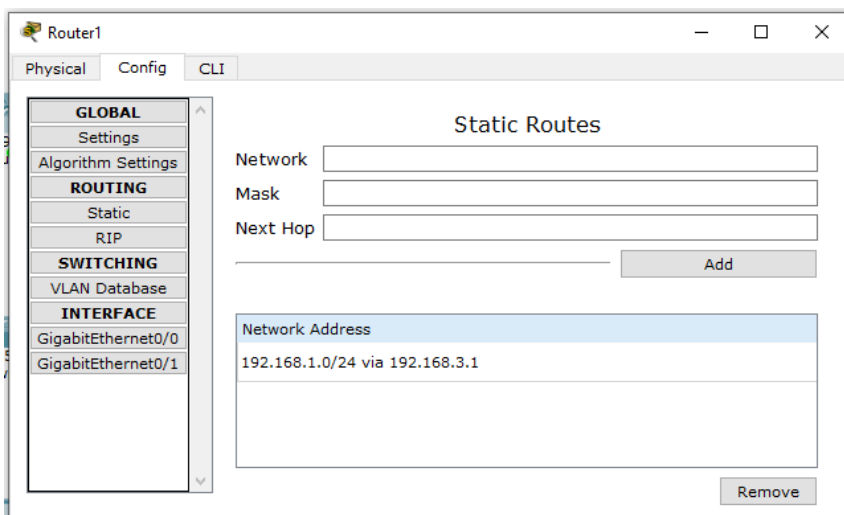
The routing table is configured in the following way :

## Router 0



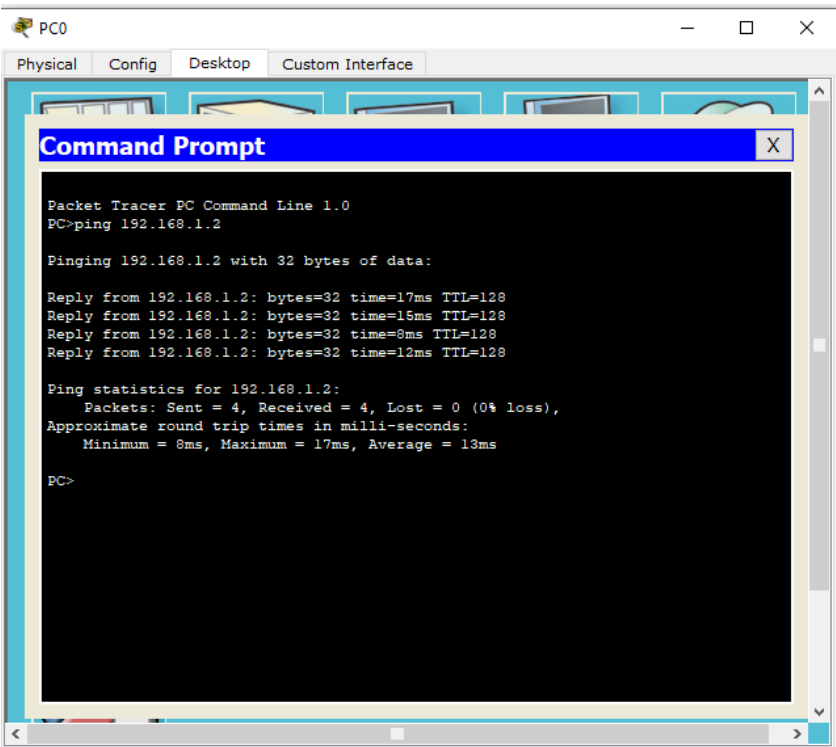
Router0 configuration window for Static Routes. The left sidebar shows the configuration tree with 'Static' selected. The main panel shows the 'Static Routes' configuration. The 'Network' field is empty. The 'Mask' field is empty. The 'Next Hop' field is empty. The 'Add' button is visible. Below the input fields, the 'Network Address' is listed as '192.168.2.0/24 via 192.168.3.2'. The 'Remove' button is visible.

## Router 1



Router1 configuration window for Static Routes. The left sidebar shows the configuration tree with 'Static' selected. The main panel shows the 'Static Routes' configuration. The 'Network' field is empty. The 'Mask' field is empty. The 'Next Hop' field is empty. The 'Add' button is visible. Below the input fields, the 'Network Address' is listed as '192.168.1.0/24 via 192.168.3.1'. The 'Remove' button is visible.

Now we can give the ping command as shown to check the connectivity :



We can also send packets through PC's :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC1	ICMP		0.000	N	8
	Successful	PC1	PC0	ICMP		0.000	N	9
	Successful	PC0	PC1	ICMP		0.000	N	10

Packets Sent Successfully

## Practical - 4

### ● AIM :

Configure IP RIP Routing.

### ● THEORY :

#### RIP Routing :

- It uses hop count as the matrix, with a maximum of 15 hops.
- Routers share their entire routing table with neighbour in every 30 seconds.
- Lists routes and matrices based on information received from the neighbouring routers.

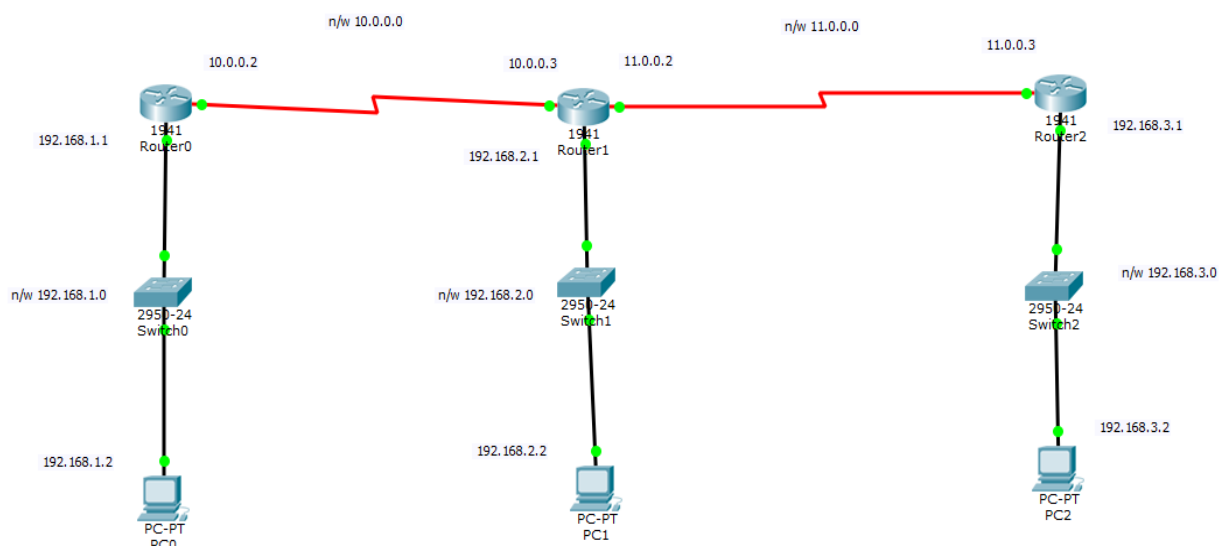
#### Advantages of RIP Routing :

- Easy to configure and understand.
- Minimal computational and memory requirements.
- Periodic updates reduce manual management.
- Supported by many devices.

#### Disadvantages of RIP Routing :

- Limited to 15 hops, unsuitable for large networks.
- Takes time to adapt the network changes.
- Frequent full table broadcast can consume bandwidth.
- Uses simple methods that may not handle complex loops as effectively.
- Lacks advanced capabilities found in modern protocols.

#### Topology :

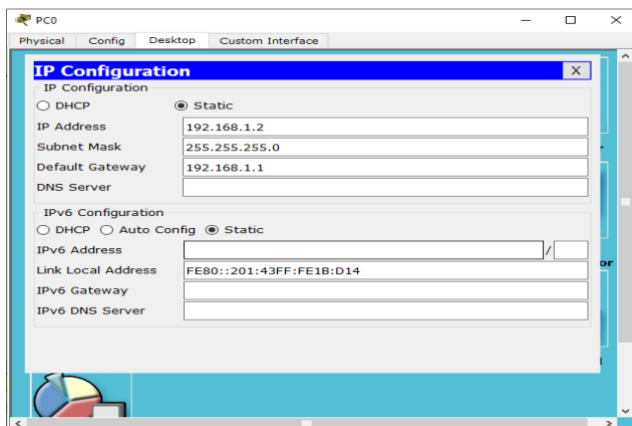


## Routing Table :

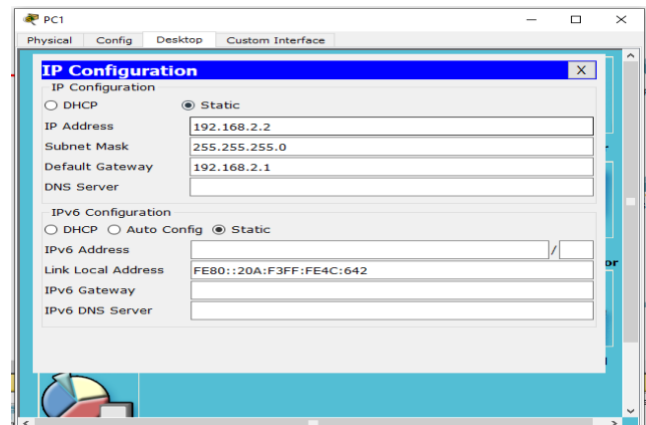
Devices	IP Addresses
PC 0	192.168.1.2
PC 1	192.168.2.2
PC 2	192.168.3.2
Router 0 (GigabitEthernet 0/0)	192.168.1.1
Router 0 (Serial 0/1/0)	10.0.0.2
Router 1 (GigabitEthernet 0/0)	192.168.2.1
Router 1 (Serial 0/1/0)	10.0.0.3
Router 1 (Serial 0/1/1)	11.0.0.2
Router 2 (GigabitEthernet 0/0)	192.168.3.1
Router 2 (Serial 0/1/0)	11.0.0.3

We configure it as follows :

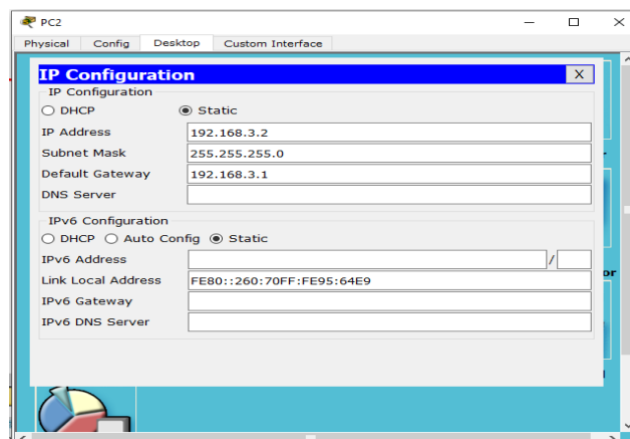
Step 1 : Configure all PC's with respect to their IP addresses.



PC 0



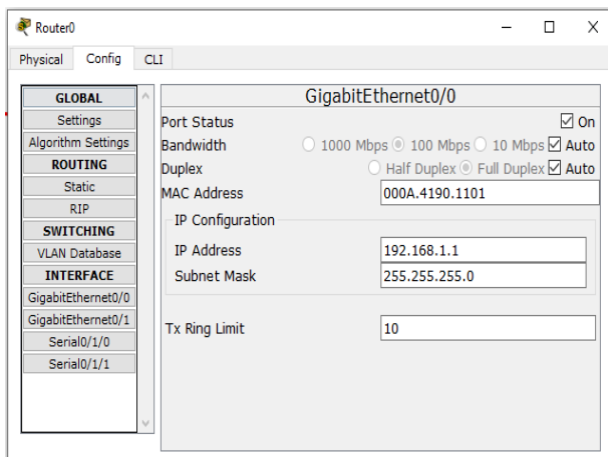
PC 1



PC 2

Step 2 : Configure all Routers with respect to their IP addresses.

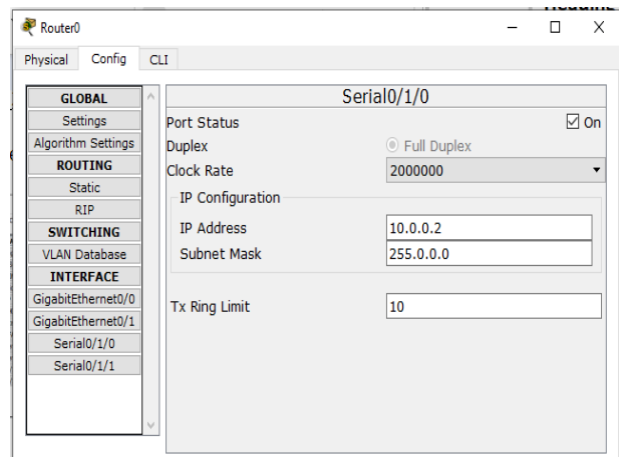
## Router 0



Router0 configuration window for GigabitEthernet0/0. The left sidebar shows the configuration tree with 'GigabitEthernet0/0' selected. The main panel shows the following settings:

- Port Status: ☒ On
- Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address: 000A.4190.1101
- IP Configuration:
  - IP Address: 192.168.1.1
  - Subnet Mask: 255.255.255.0
- Tx Ring Limit: 10

GigabitEthernet 0/0

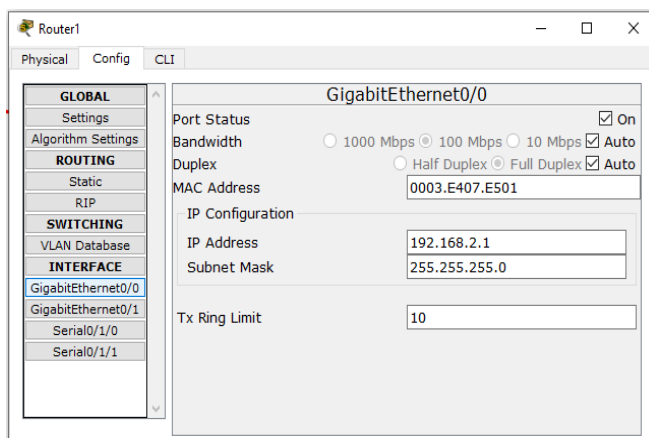


Router0 configuration window for Serial0/1/0. The left sidebar shows the configuration tree with 'Serial0/1/0' selected. The main panel shows the following settings:

- Port Status: ☒ On
- Duplex: ☒ Full Duplex
- Clock Rate: 2000000
- IP Configuration:
  - IP Address: 10.0.0.2
  - Subnet Mask: 255.0.0.0
- Tx Ring Limit: 10

Serial 0/1/0

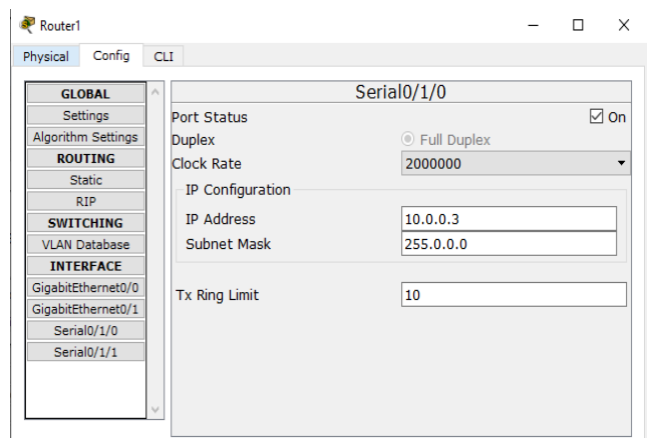
## Router 1



Router1 configuration window for GigabitEthernet0/0. The left sidebar shows the configuration tree with 'GigabitEthernet0/0' selected. The main panel shows the following settings:

- Port Status: ☒ On
- Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address: 0003.E407.E501
- IP Configuration:
  - IP Address: 192.168.2.1
  - Subnet Mask: 255.255.255.0
- Tx Ring Limit: 10

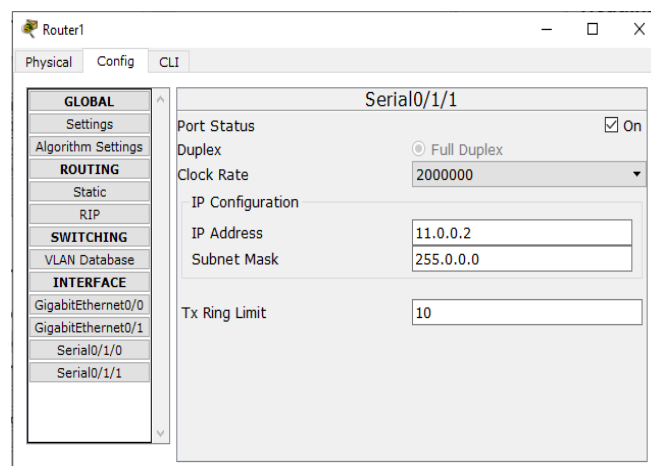
GigabitEthernet 0/0



Router1 configuration window for Serial0/1/0. The left sidebar shows the configuration tree with 'Serial0/1/0' selected. The main panel shows the following settings:

- Port Status: ☒ On
- Duplex: ☒ Full Duplex
- Clock Rate: 2000000
- IP Configuration:
  - IP Address: 10.0.0.3
  - Subnet Mask: 255.0.0.0
- Tx Ring Limit: 10

Serial 0/1/0

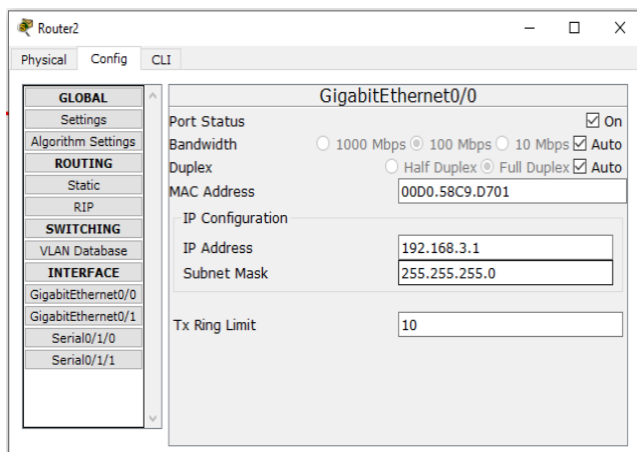


Router1 configuration window for Serial0/1/1. The left sidebar shows the configuration tree with 'Serial0/1/1' selected. The main panel shows the following settings:

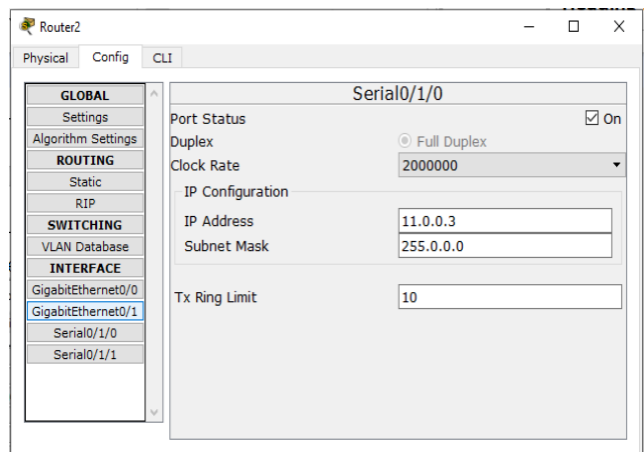
- Port Status: ☒ On
- Duplex: ☒ Full Duplex
- Clock Rate: 2000000
- IP Configuration:
  - IP Address: 11.0.0.2
  - Subnet Mask: 255.0.0.0
- Tx Ring Limit: 10

Serial 0/1/1

## Router 2



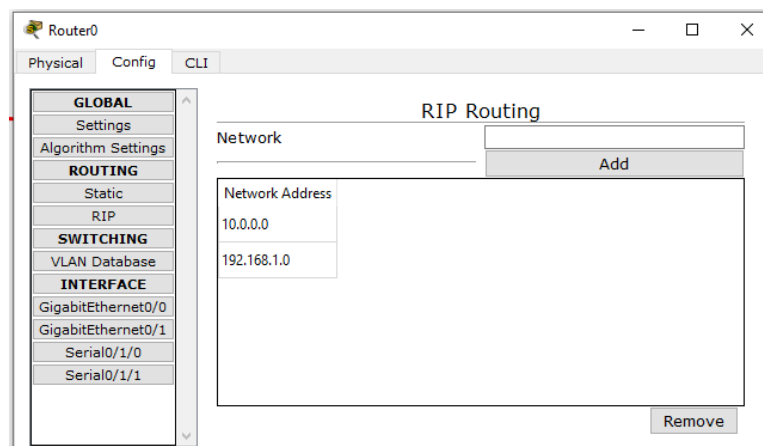
GigabitEthernet 0/0



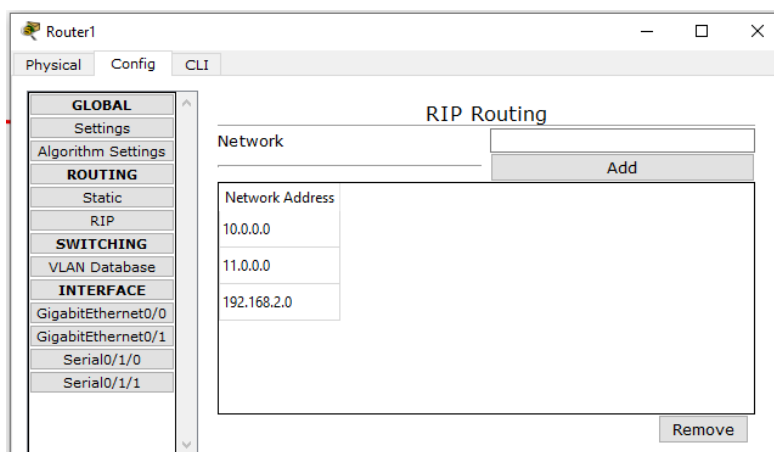
Serial 0/1/0

The routing table is configured in the following way :

## Router 0

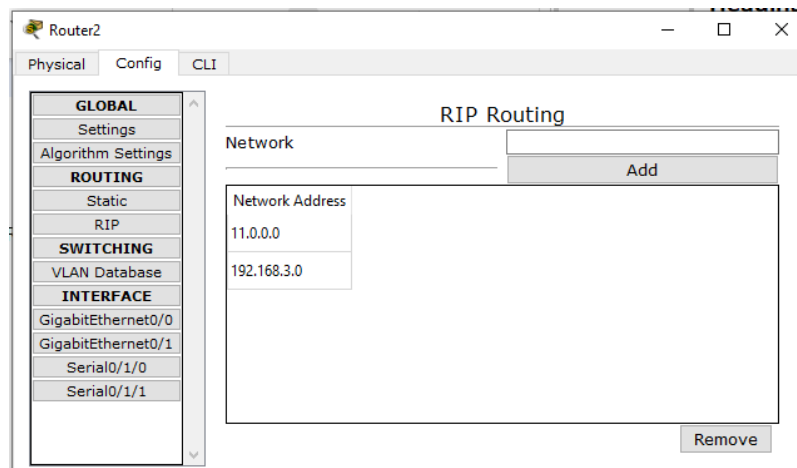


## Router 1

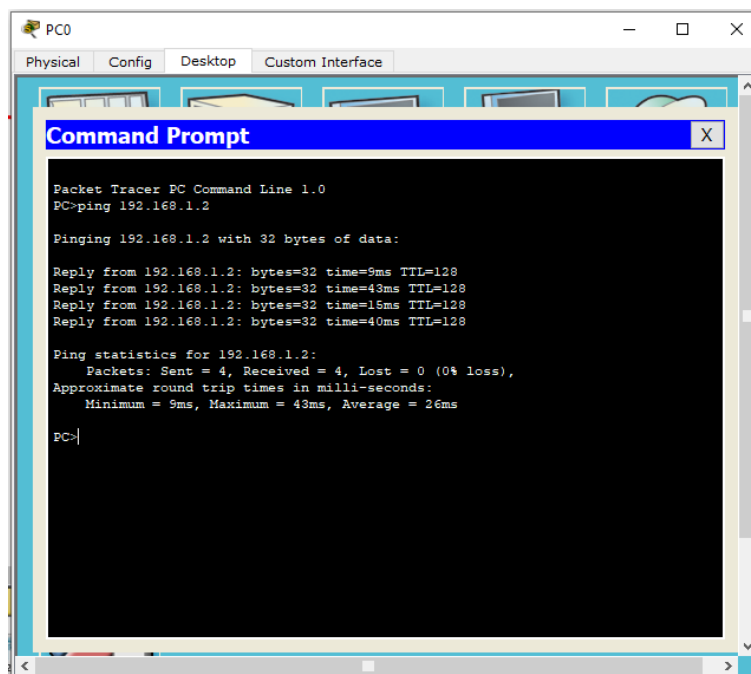










## Router 2



Now we can give the ping command as shown to check the connectivity :



We can also send packets through PC's :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC2	ICMP		0.000	N	13
	Successful	PC0	PC2	ICMP		0.000	N	14
	Successful	PC1	PC2	ICMP		0.000	N	15

Packets sent successfully

## Practical - 5

- **AIM :**

Configure IP OSPF Routing.

- **THEORY :**

OSPF(Open Shortest Path First) :

- OSPF (Open Shortest Path First) is a widely used routing protocol in computer networks, particularly in large enterprise networks.
- It helps routers determine the most efficient path for data to travel across the network.

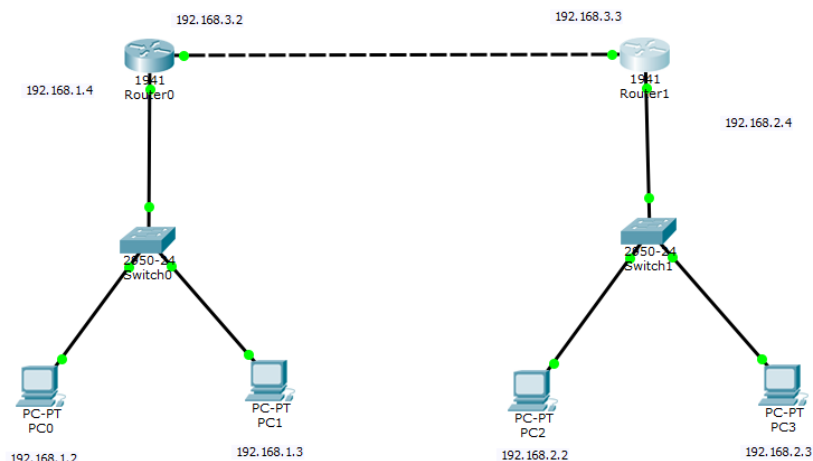
Advantages of OSPF Routing :

- Scalable: Handles large and complex networks with hierarchical areas.
- Fast Convergence: Quickly recalculates routes after topology changes.
- Efficient: Minimizes bandwidth usage by updating only on changes.
- Authentication: Supports security features for trusted routing information.

Disadvantages of OSPF Routing :

- Complex: Configuration and management can be intricate, especially in large networks.
- Resource Intensive: Requires significant memory and CPU for large-scale deployments.
- Initial Overhead: Initial synchronization can be resource-heavy.
- Hierarchical Complexity: Proper design is needed to avoid issues in large, multi-area setups.

Topology :

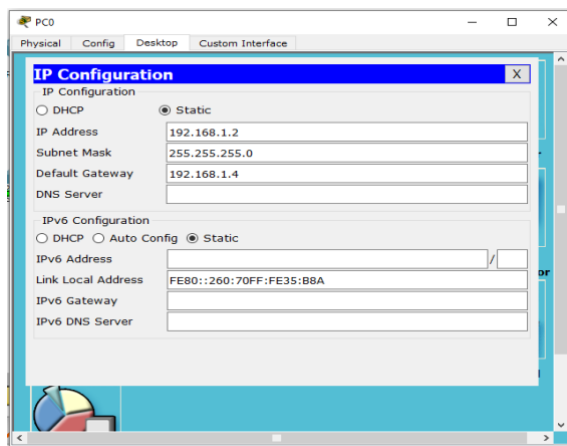


## Routing Table :

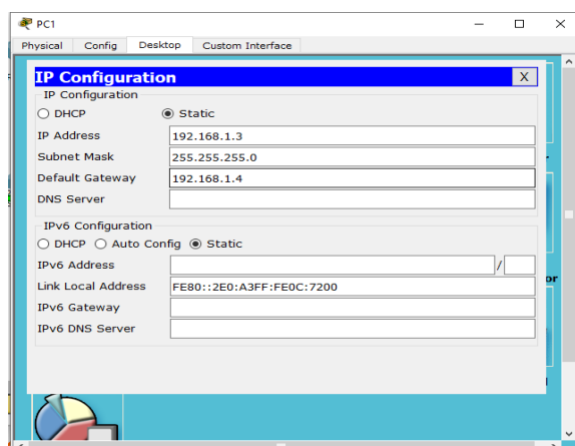
Devices	IP Addresses
PC 0	192.168.1.2
PC 1	192.168.1.3
PC 2	192.168.2.2
PC 3	192.168.2.3
Router 0 (GigabitEthernet 0/0)	192.168.1.4
Router 0 (GigabitEthernet 0/1)	192.168.3.2
Router 1 (GigabitEthernet 0/0)	192.168.2.4
Router 1 (GigabitEthernet 0/1)	192.168.3.3

We configure it as follows :

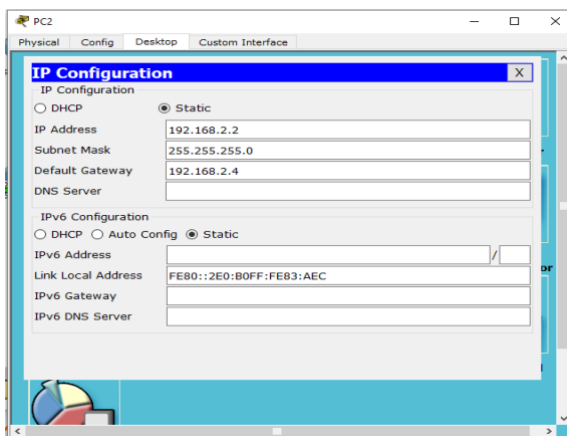
Step 1 : Configure all PC's with respect to their IP addresses.



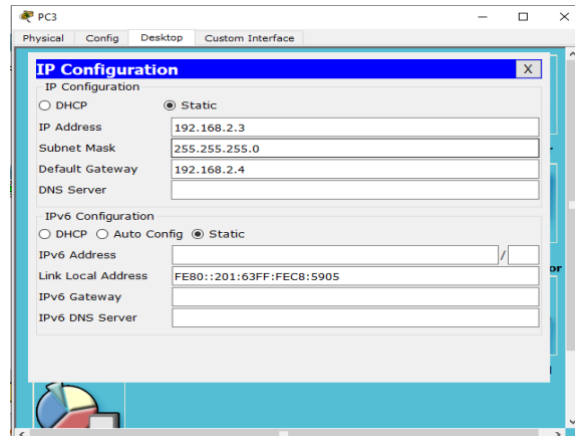
PC 0



PC 1



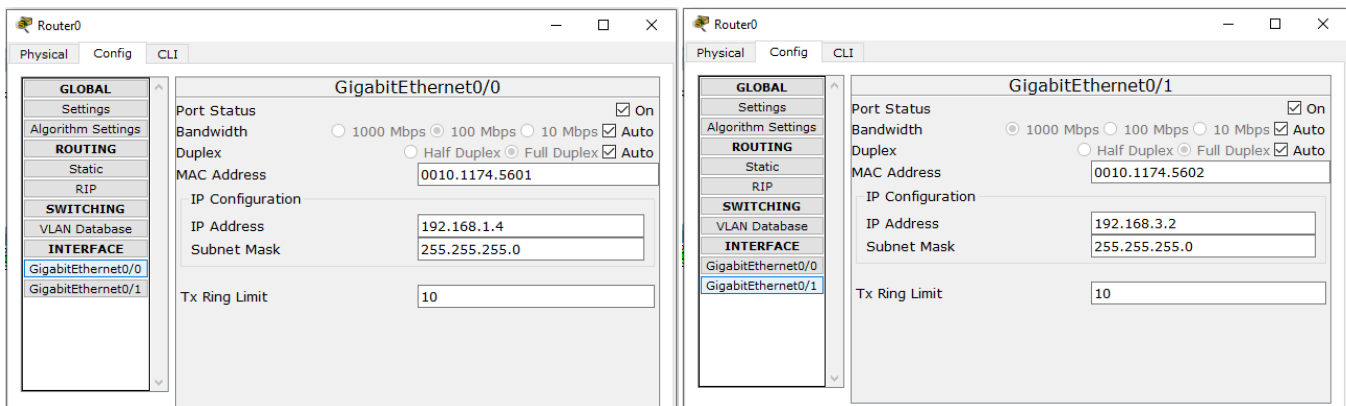
PC 2



PC 3

Step 2 : Configure all Routers with respect to their IP addresses.

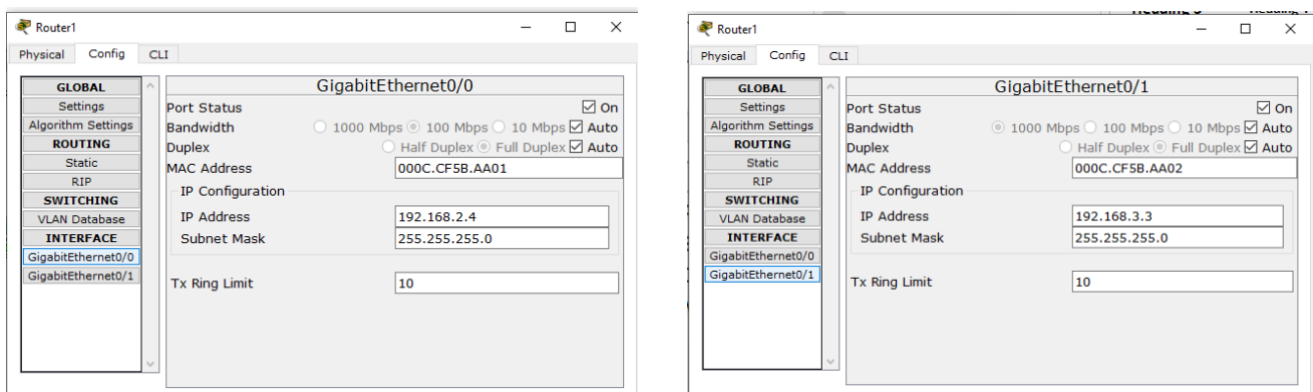
## Router 0



GigabitEthernet 0/0

GigabitEthernet 0/1

## Router 1

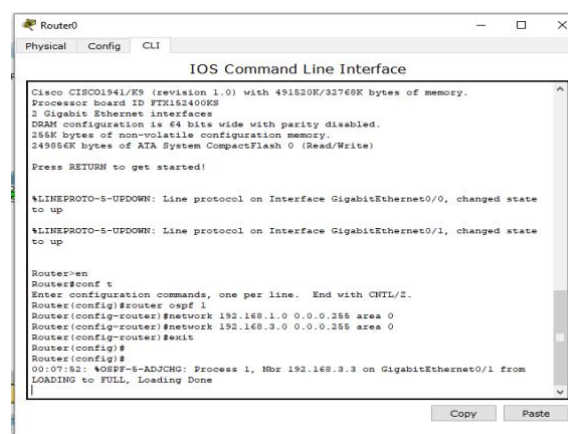


GigabitEthernet 0/0

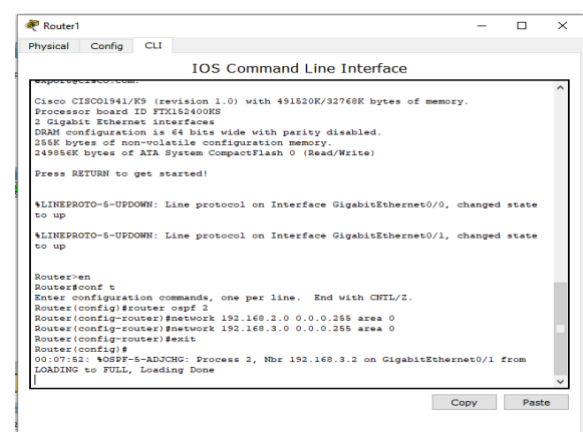
GigabitEthernet 0/1

The routing table is configured in the following way :

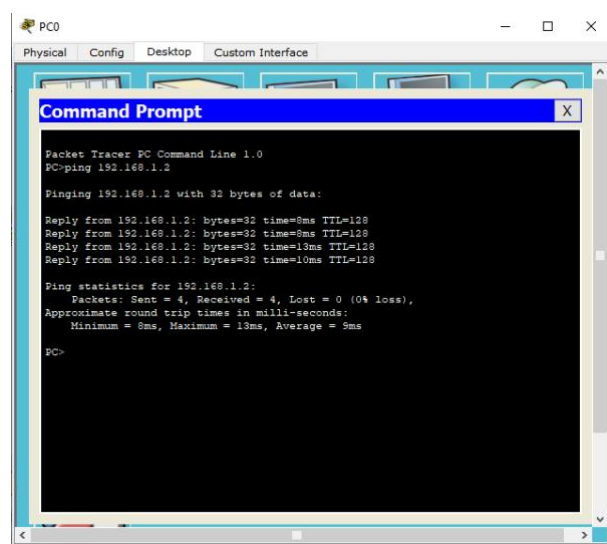
## Router 0









Router 1



Now we can give the ping command as shown to check the connectivity :



We can also send packets through PC's :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC3	ICMP		0.000	N	4
	Successful	PC1	PC2	ICMP		0.000	N	5
	Successful	PC3	PC1	ICMP		0.000	N	6

Packets Sent Successfully

## Practical - 6

- **AIM :**

Configuring IP DHCP Routing.

- **THEORY :**

### DHCP (Dynamic Host Configuration Protocol) :

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used in computer networks.
- It automates the process of assigning IP addresses to devices (like computers, smartphones, or printers) on a network.
- Instead of manually configuring each device with a unique IP address, DHCP automatically provides this information when the device connects to the network.

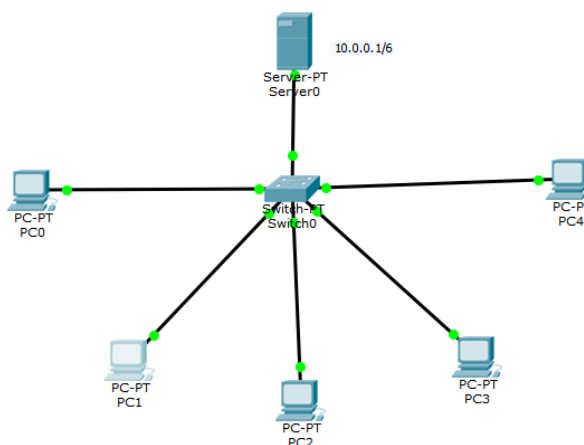
### Advantages of DHCP Routing :

- Automatic Configuration: Devices get IP addresses and settings automatically.
- Simplified Management: Centralized control reduces manual work.
- Efficient IP Use: Optimizes address allocation from a pool.
- Flexibility: Supports both dynamic and static IP assignments.

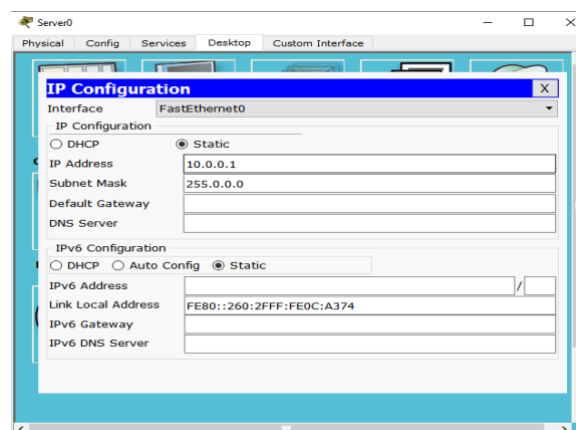
### Disadvantages of DHCP Routing :

- Server Dependency: Network access can be disrupted if the DHCP server fails.
- Security Risks: Rogue DHCP servers can cause issues.
- IP Conflicts: Potential for address conflicts due to misconfigurations.
- Limited Control: Less precise control over static IP assignments.

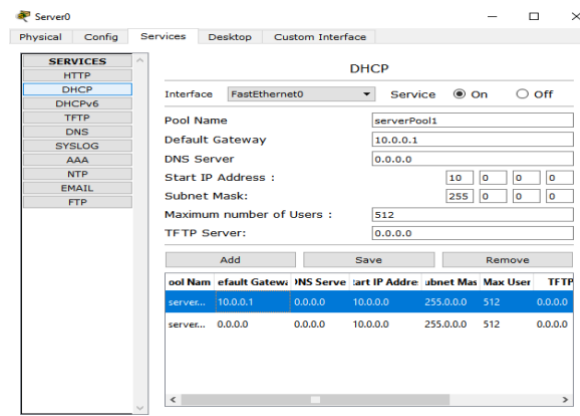
### Topology :



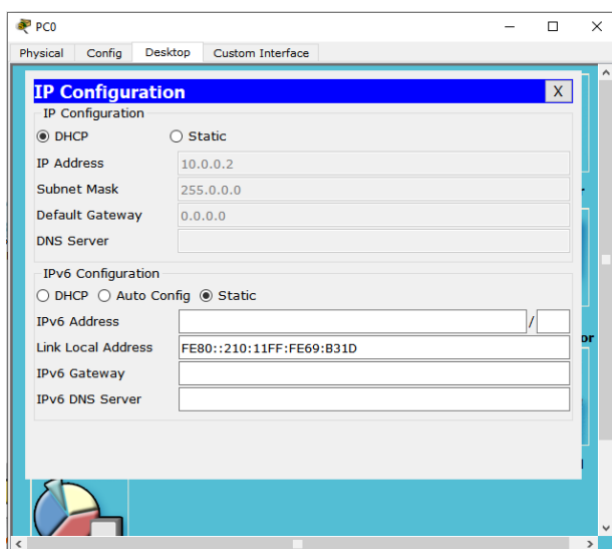
We will configure the server :



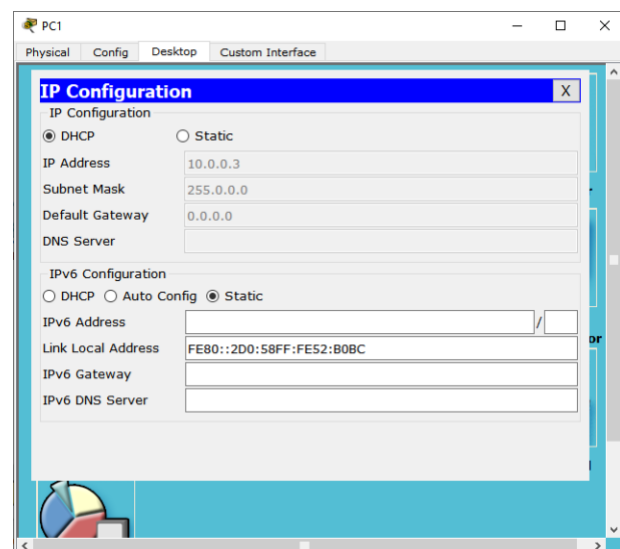
We will turn on the services of the DHCP server to provide IP addresses to the end devices :



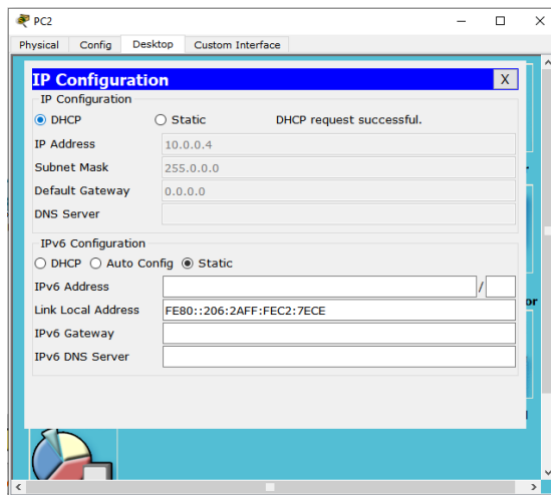
Now we can check the end devices :



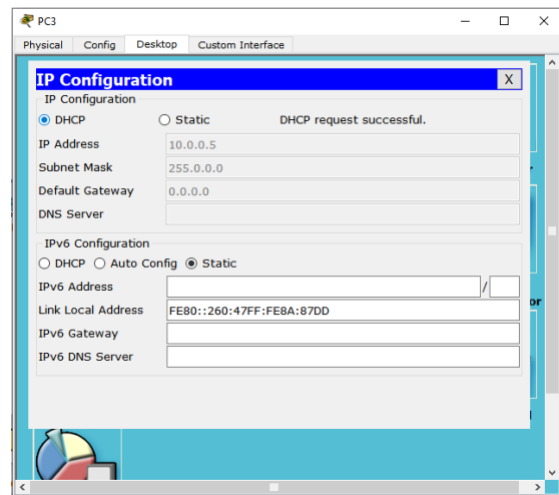
PC 0



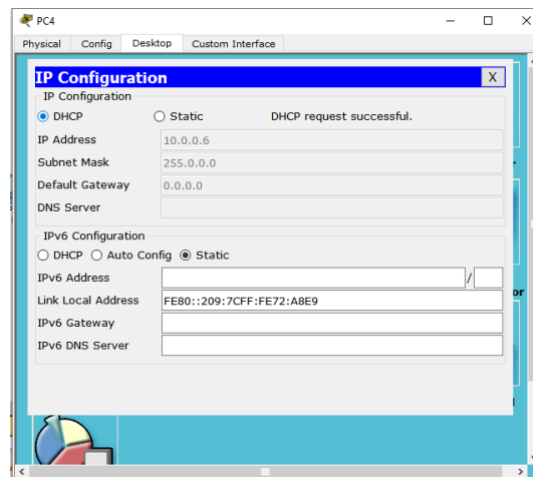
PC 1



PC 2

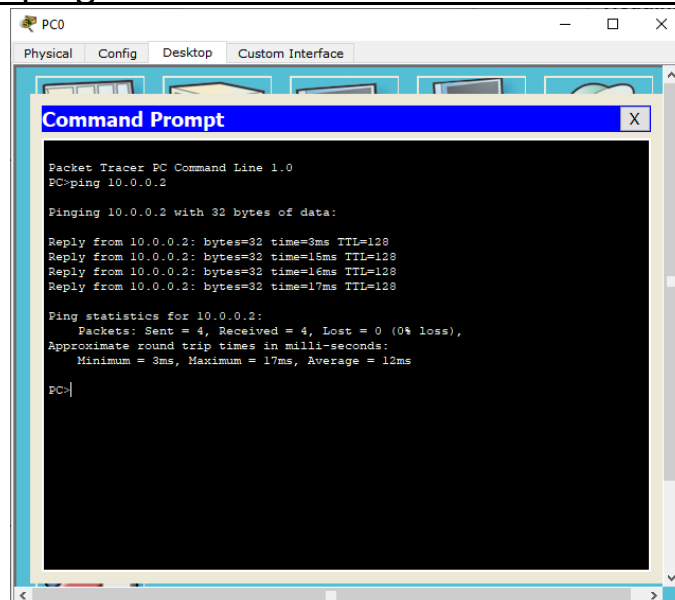


PC 3



PC 4

Now we can give the ping command as shown to check the connectivity :



We can also send packets through PC's :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC1	ICMP		0.000	N	0
	Successful	PC2	PC3	ICMP		0.000	N	1
	Successful	PC4	PC0	ICMP		0.000	N	2

Packets sent successfully



## Practical - 7

- **AIM :**

- (a) Study of different colour codes.
- (b) Study of different connecting devices and their differences.
- (c) Crimping LAN cable.

- **THEORY :**

### **CAT 5, CAT 6, and CAT 7**

CAT 5, CAT 6, and CAT 7 are different generations of Ethernet cables, each with varying characteristics. Following are the key differences between them:

1) **Speed and Bandwidth:**

CAT 5: It supports data transfer speeds up to 100 Mbps (Megabits per second) with a maximum bandwidth of 100 MHz. CAT 5 cables are considered outdated and are rarely used for new installations.

CAT 6: It supports data transfer speeds up to 10 Gbps (Gigabits per second) with a maximum bandwidth of 250 MHz. CAT 6 cables are commonly used for home and small office networks.

CAT 7: It offers higher performance with data transfer speeds up to 10 Gbps and beyond, reaching up to 40 Gbps. It has a higher bandwidth capacity of 600 MHz.

CAT 7 is designed for more demanding applications and larger network infrastructures.

2) **Shielding:**

CAT 5: It is typically an unshielded twisted pair (UTP) cable, meaning it does not have any shielding to protect against electromagnetic interference (EMI) or crosstalk.

CAT 6: It can be either unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Shielded variants have additional shielding to reduce EMI and crosstalk.

CAT 7: It features additional shielding known as individually shielded pairs (S/FTP or S/STP). This shielding provides better protection against EMI and crosstalk, leading to improved signal quality and reduced interference.

3) **Connectors and Backward Compatibility:**

CAT 5: It commonly uses RJ-45 connectors, which are the standard connectors for Ethernet cables. CAT 5 cables are backward compatible with newer Ethernet standards like CAT 5e, CAT 6, and CAT 7.

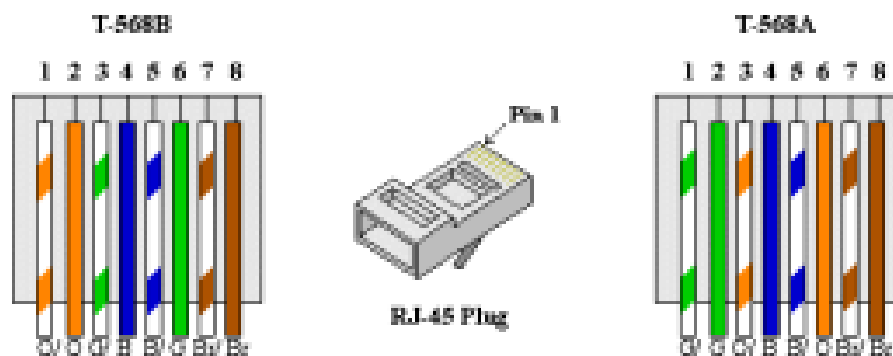
CAT 6: It also uses RJ-45 connectors, and CAT 6 cables are backward compatible with CAT 5 and CAT 5e.

CAT 7: It uses specialized RJ-45 connectors with stricter specifications to ensure better signal integrity at higher frequencies. CAT 7 cables are backward compatible with older Ethernet standards as well.

- 4) Distance:
- CAT 5: It is suitable for shorter distances within a network, typically up to 100 meters (328 feet).
  - CAT 6: It can also reach up to 100 meters for 10 Gbps speeds but may have reduced performance at longer distances.
  - CAT 7: It can achieve 10 Gbps speeds at longer distances, typically up to 100 meters (328 feet).

## 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.



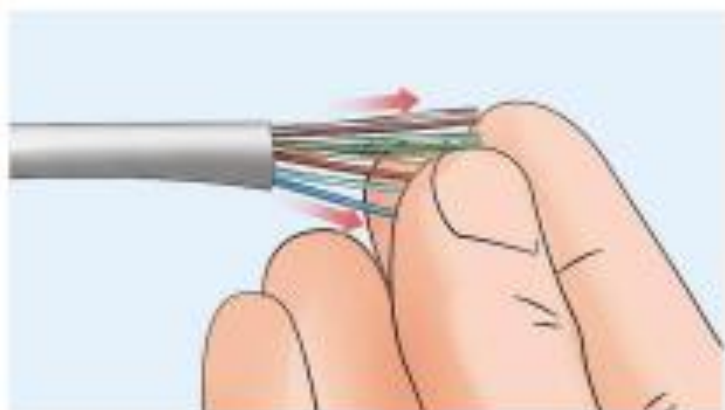
3) Strip the cable jacket:

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:

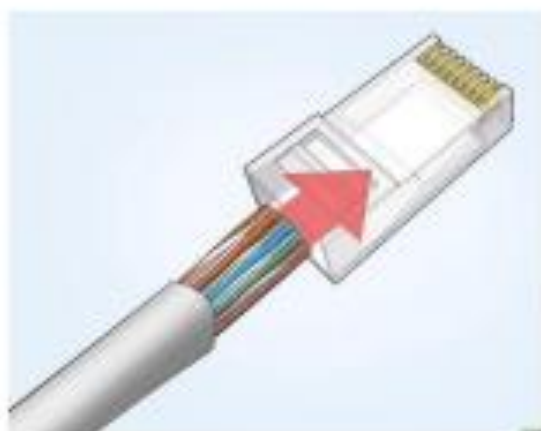
Cut the excess wire length to ensure they are even and of equal length, typically around 0.5 inches (1.3 cm).

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:

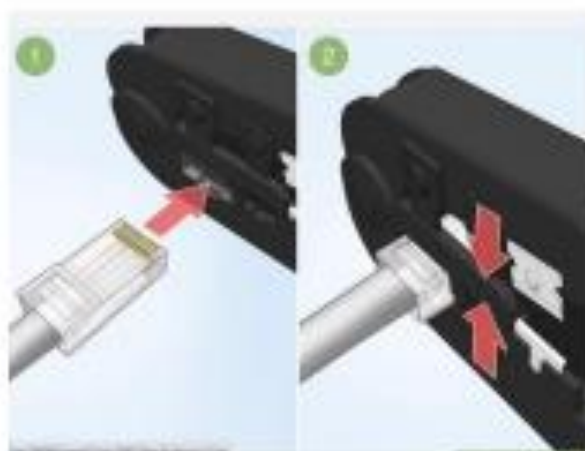
Carefully insert the arranged wires into the RJ-45 connector, ensuring they reach the end and make contact with the metal contacts inside. Check that the wire colours are in the correct order.



- 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 - 8

### ● AIM :

Configuring DNS server and client.

### ● THEORY :

#### DNS (Domain Name Server) :

- DNS, or Domain Name System, is a crucial component of the internet that translates human-readable domain names (like `www.example.com`) into IP addresses (like `192.0.2.1`), which computers use to identify each other on the network.
- When you type a domain name into your web browser, a DNS query is sent to a DNS server, which then looks up the IP address associated with that domain name and returns it to your browser.
- This process enables users to access websites using easy-to-remember names instead of numerical IP addresses.

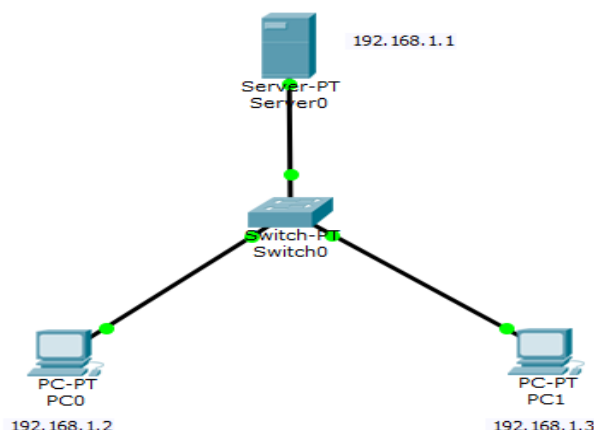
#### Advantages of DNS Server :

- Human-Friendly: Translates domain names into IP addresses for easier access.
- Distributed: Enhances reliability and fault tolerance.
- Caching: Speeds up access by storing frequently requested data.
- Scalable: Handles a vast number of domain names and queries.

#### Disadvantages of DNS Server :

- Security Risks: Vulnerable to attacks like spoofing and DDoS.
- Single Point of Failure: Individual servers can still fail.
- Latency: Adds minor delays to web requests.
- Complexity: Management can be intricate and error-prone.

#### Topology :

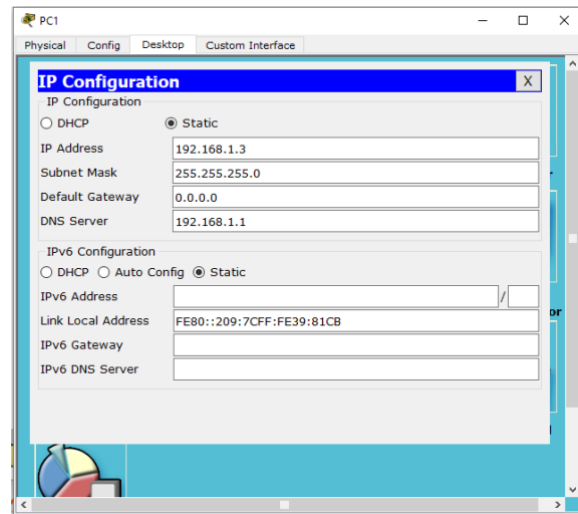
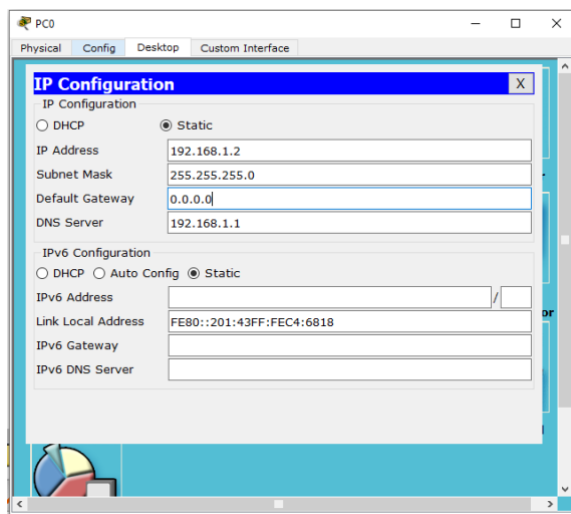


## Routing table :

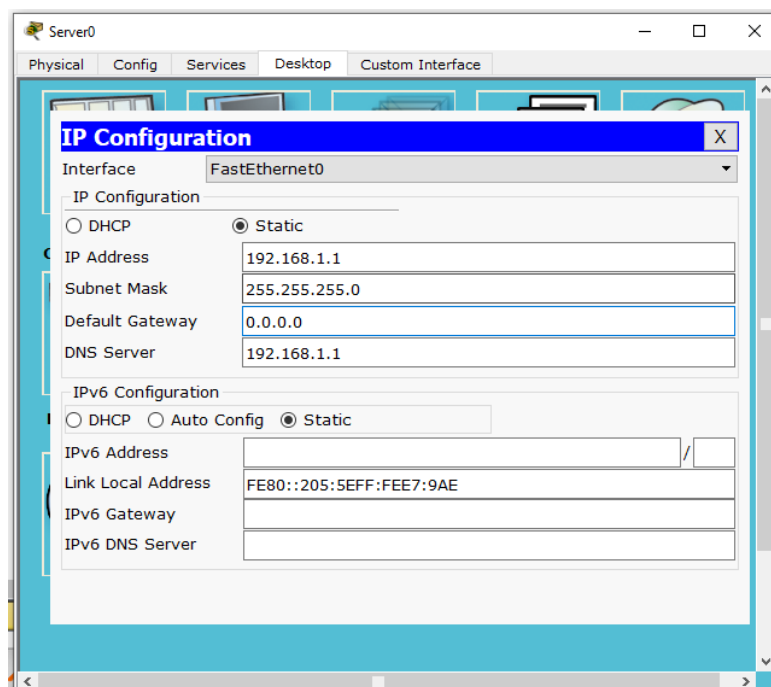
Devices	IP Addresses
Server	192.168.1.1
PC 0	192.168.1.2
PC 1	192.168.1.3

We configure it as follows :

Step 1 : Configure all PC's with respect to their IP addresses.

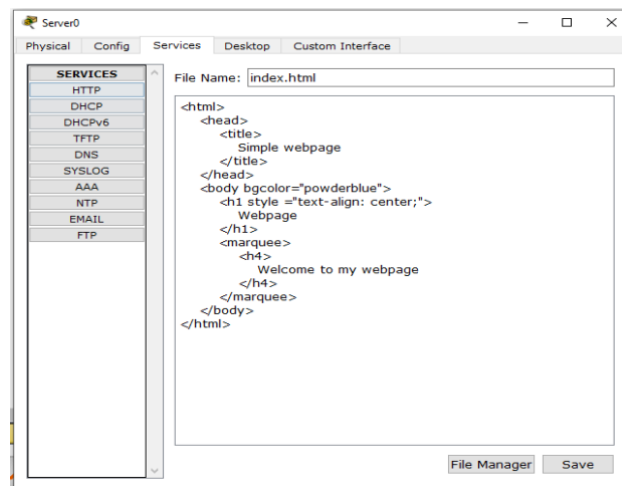


Step 2 : Configure the DNS server.

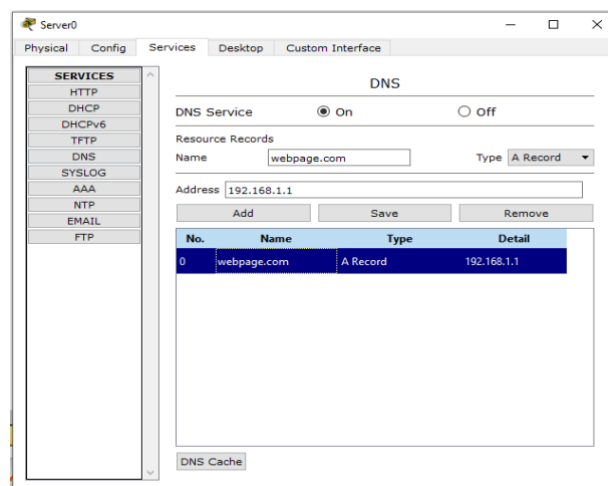




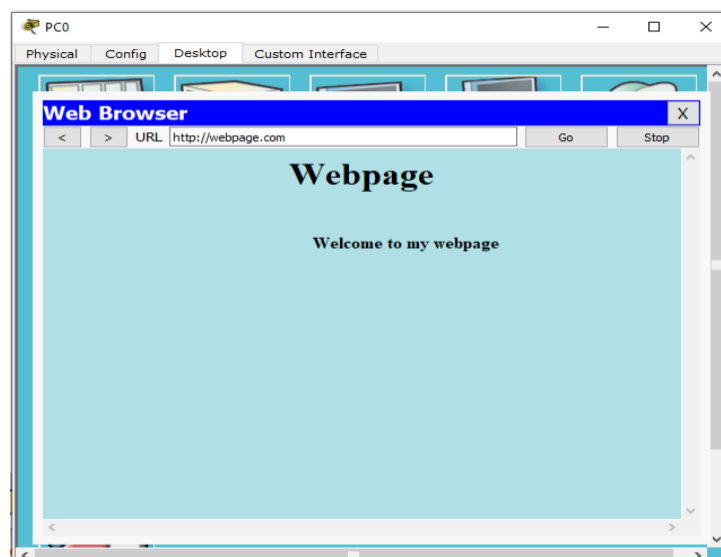
We will edit the HTML file to get the web page in our end devices :



We will turn on the DNS Services :



Finally, we made a webpage which is present in our PC's :



## Practical - 9

- **AIM :**

Configuring basic security routers for network.

- **THEORY :**

Basic security features for networks are foundational measures that are essential for securing a network and its data. These features help protect against common threats and vulnerabilities.

Here are some key basic security features for networks:

1. **Firewalls:** Firewalls act as a barrier between a trusted internal network and untrusted external networks (like the internet). They control incoming and outgoing network traffic based on an organization's previously established security policies. Firewalls can be hardware-based or software-based.
2. **Network Segmentation:** Divide the network into segments or VLANs (Virtual LANs) to isolate different parts of the network from each other. This prevents lateral movement of threats within the network.
3. **Strong Authentication:** Require strong and unique passwords or passphrases for all devices and user accounts. Implement multi-factor authentication (MFA) whenever possible to add an extra layer of security.
4. **Encryption:** Use encryption protocols like HTTPS, SSL/TLS, and VPNs to protect data in transit. Also, encrypt sensitive data at rest to safeguard it from unauthorized access.
5. **Intrusion Detection and Prevention Systems (IDPS):** Deploy IDPS to monitor network traffic for signs of suspicious or malicious activity and take action to prevent or mitigate threats.
6. **Patch Management:** Regularly update and patch network devices, operating systems, and software to address known vulnerabilities. Vulnerability management is a critical component of network security.
7. **Security Policies:** Establish and enforce security policies and procedures. These policies should cover access control, data handling, incident response, and more.
8. **Network Monitoring and Logging:** Continuously monitor network traffic and maintain logs of network activities. Analyze logs to detect and respond to security incidents.
9. **User Education and Awareness:** Educate users about security best practices, including how to recognize phishing attempts, avoid downloading malicious attachments, and report suspicious activity.
10. **Backup and Recovery:** Regularly back up critical data and test the restoration process. Having reliable backups is crucial for recovering from data breaches or system failures.
11. **Access Control:** Implement role-based access control (RBAC) to ensure that users have the minimum necessary privileges to perform their tasks. Restrict access to sensitive data and systems.

12. Security Updates: Stay informed about security threats and vulnerabilities by subscribing to security bulletins and alerts. Promptly apply security updates and patches to address new threats.

13. Denial of Service (DoS) Protection: Implement DoS protection mechanisms to mitigate or prevent attacks that can overwhelm network resources.

14. Perimeter Security: Secure the network perimeter by configuring routers and switches to filter traffic and block unauthorized access attempts.

These basic security features provide a strong foundation for network security. Organizations often build upon these foundational measures with more advanced security technologies and practices to address specific threats and risks relevant to their environment.

### Topology:

For the present case we use the Access Control Lists, to demonstrate one of the basic security features  
Consider the following topology

	Interface	IP address	Subnet Mask	Gateway	Wildcard Mask
PC0	FastEthernet0	192.168.1.2	255.255.255.0	192.168.1.1	0.0.0.255
PC1	FastEthernet0	192.168.1.3			
PC2	FastEthernet0	192.168.1.4			
PC3	FastEthernet0	192.168.2.2		192.168.2.1	
PC4	FastEthernet0	192.168.2.3			
PC5	FastEthernet0	192.168.2.4			
Router0	FastEthernet0/0	192.168.1.1			
	FastEthernet0/1	192.168.2.1			
	Ethernet0/1/0	192.168.3.1			
Server	FastEthernet0	192.168.3.2		192.168.3.1	

Note:

We use Router 1840; by default it has 2 interfaces

- FastEthernet0/0 and
- FastEthernet0/1

And we need to add an extra interface Ethernet0/1/0.

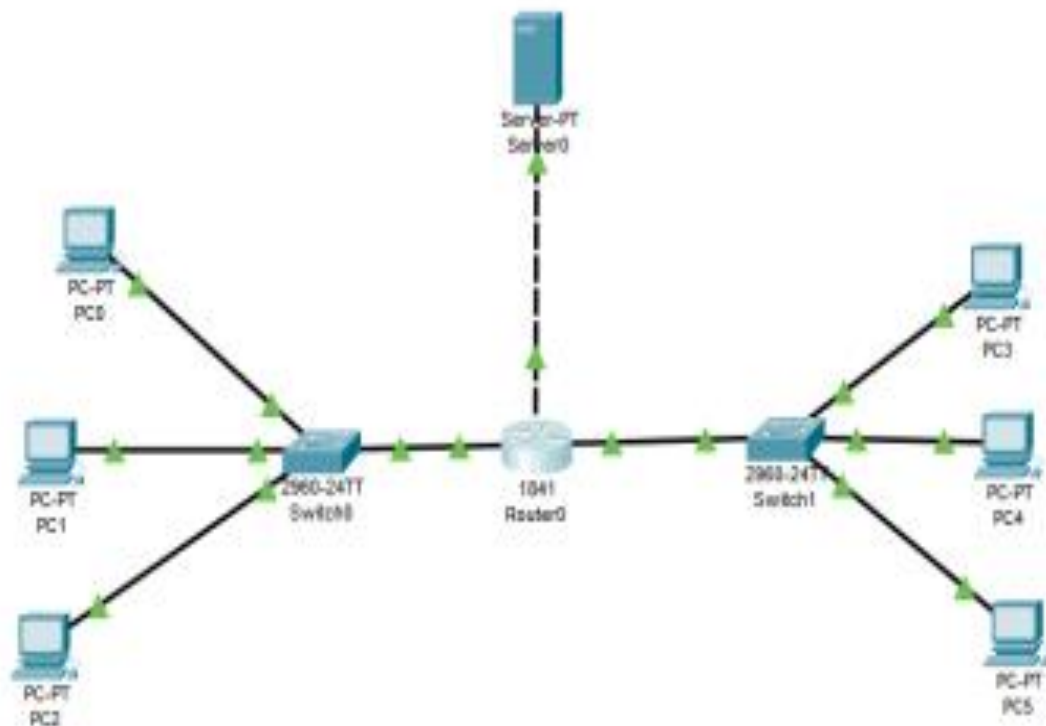
It is done as follows,

- Click on Router0
- Turn it OFF
- Select WC-1ENET interface
- Drag and drop in the slot and
- Turn ON the Router

This is how insert the WC-1ENET interface in Router0

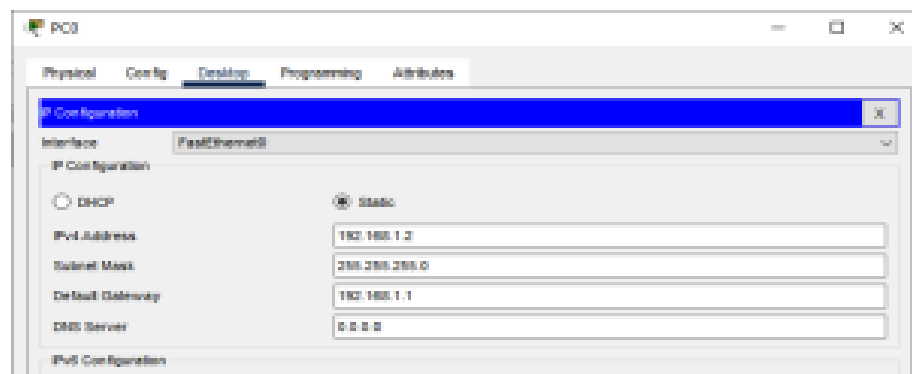


We implement the given topology in Cisco Packet Tracer



Now we configure the components

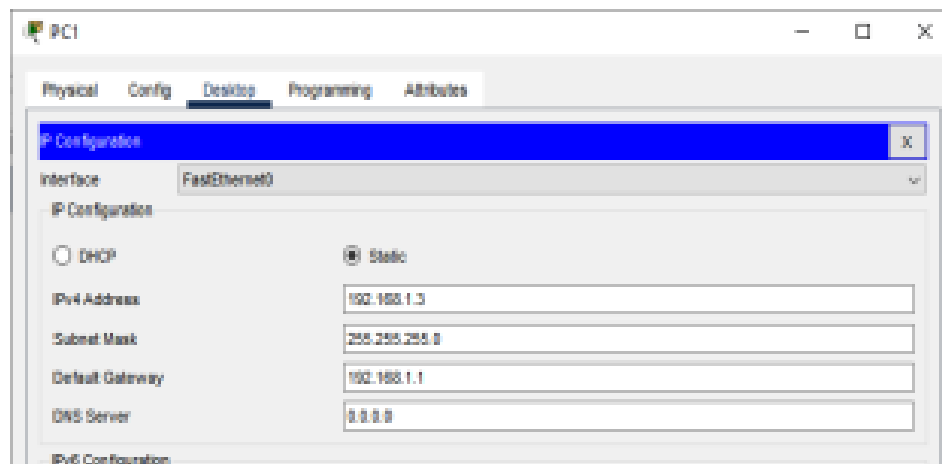
**PC0:**



The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

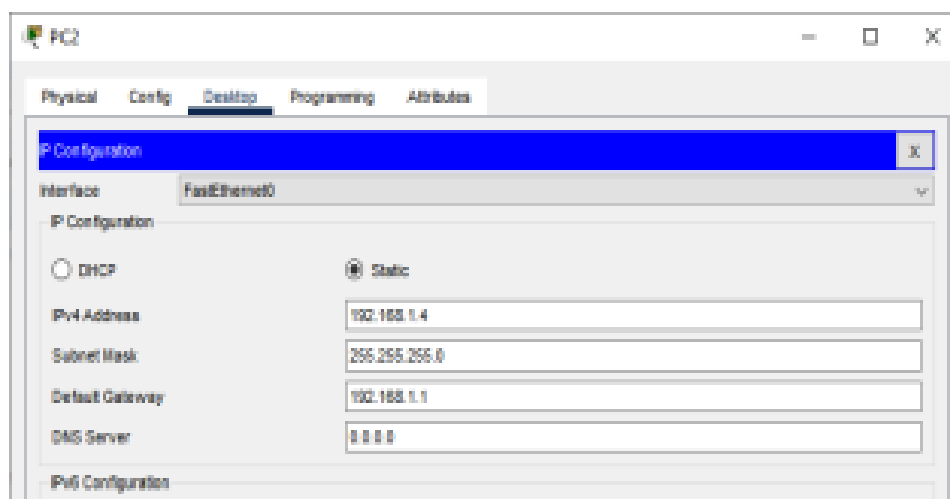
**PC1:**



The screenshot shows the configuration window for PC1. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

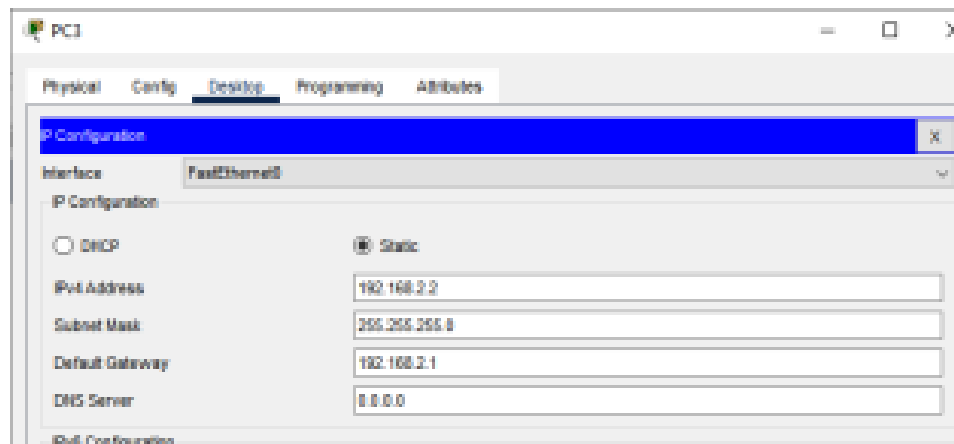
**PC2:**



The screenshot shows the configuration window for PC2. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

PC3:



PC3

Physical Config Desktop Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

PC4:



PC4

Physical Config Desktop Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

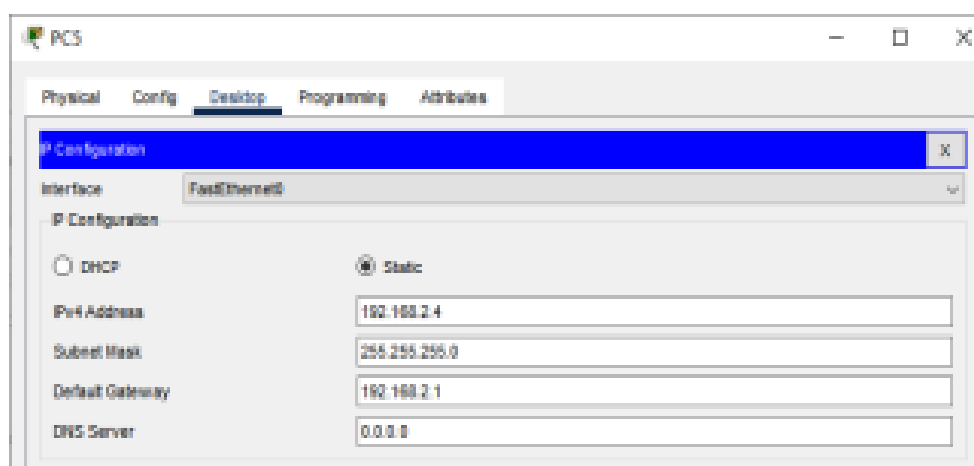
IPv4 Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

PC5:



PC5

Physical Config Desktop Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

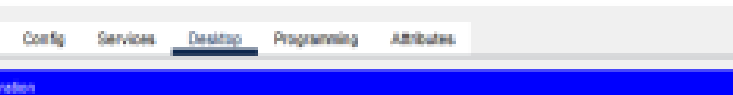
IPv4 Address: 192.168.2.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

## Server 10:



Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.3.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

**Router0: Interface FastEthernet0/0**

The screenshot displays the Cisco Packet Tracer configuration window for a Cisco 2950 switch. The 'Config' tab is active, and the 'FastEthernet0/0' interface is selected. The configuration parameters are as follows:

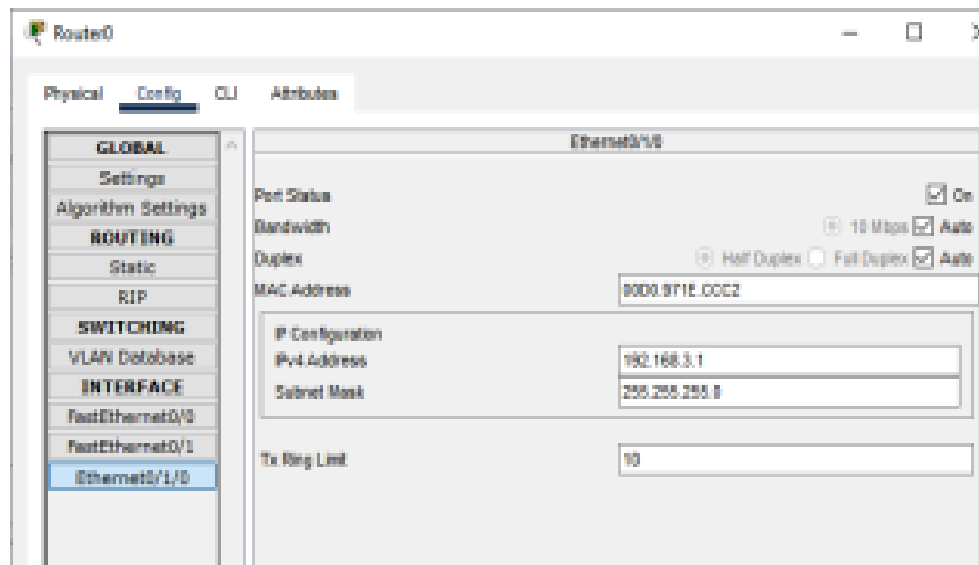
- Port Status:** On (checked)
- Bandwidth:** 100 Mbps (selected)
- Duplex:** Half Duplex (selected)
- Flow Control:** Auto (checked)
- MAC Address:** 0830.F2A6.7C81
- IP Configuration:**
  - IPv4 Address:** 192.168.1.1
  - Subnet Mask:** 255.255.255.0
- Tx Ring Limit:** 18

### Router0: Interface FastEthernet0/1

The screenshot displays the Cisco Packet Tracer configuration window for a router. The 'Config' tab is active, and the 'FastEthernet0/1' interface is selected. The configuration parameters are as follows:

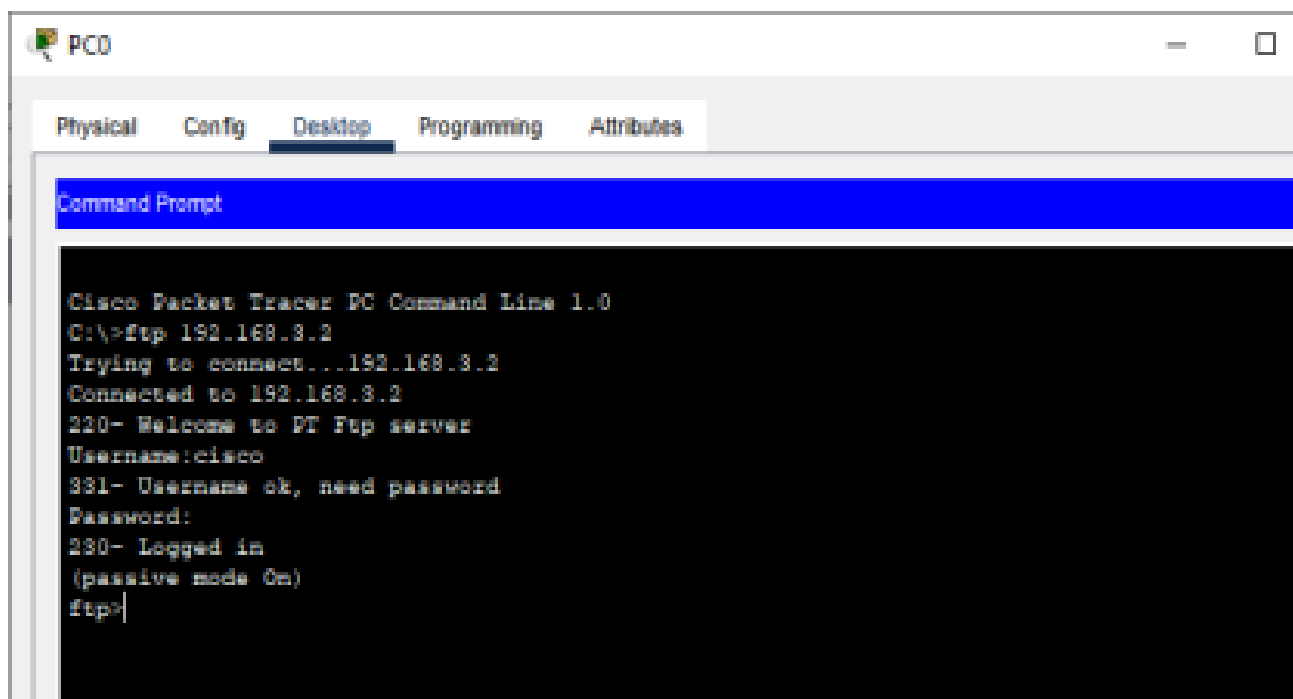
- Port Status:** On (checked)
- Speed:** 100 Mbps (selected)
- Duplex:** Half Duplex (selected)
- Auto Negotiation:** Auto (checked)
- MAC Address:** 0830.F248.7C82
- IP Configuration:**
  - IPv4 Address: 192.168.2.1
  - Subnet Mask: 255.255.255.0
- To Ring Limit:** 10

### Router0: Interface Ethernet0/1/0



### Checking the ftp Service:

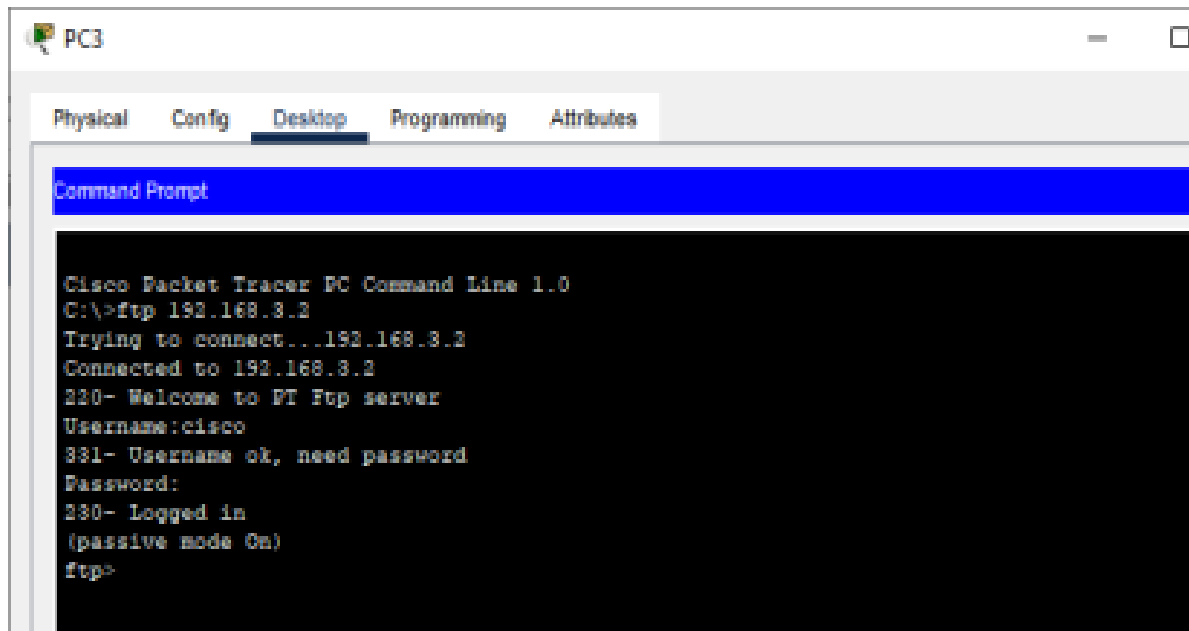
From PC0: (Username: cisco Password: cisco)



We see that ftp service is accessible to PC0 and all the PCs in its network



From PC3: (Username: cisco: Password: cisco)



We see that ftp service is accessible to PC3 and all the PCs in its network

**Configuring ACLs:** Now we configure the ACLs so that ftp service is available to all PCs in one network and is not available to the PCs in the other network

We configure so that PC0 – PC2 get the ftp Service while PC3-PC5 do not get the service

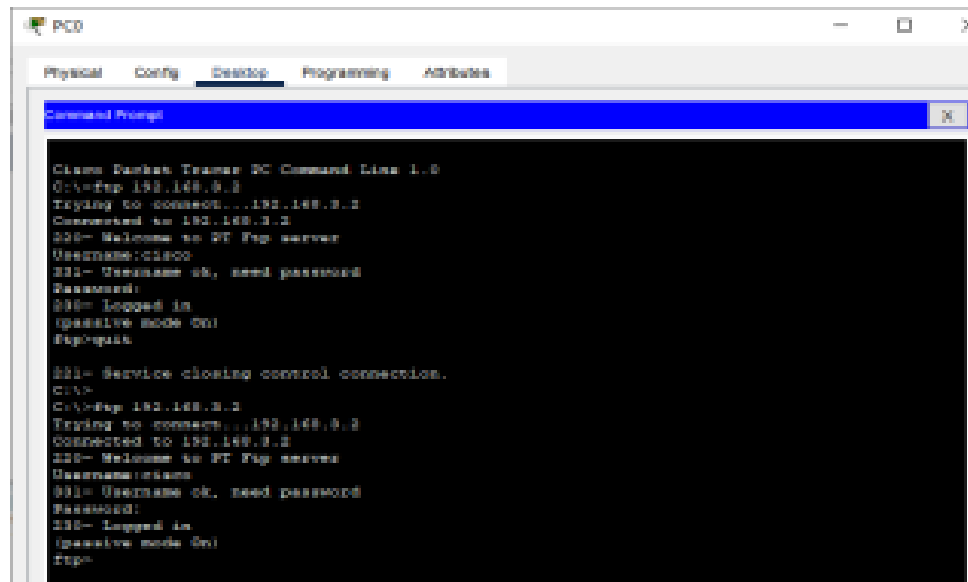
### Configuring Router0 for ACLs:

We enter the following commands in the CLI mode of Router0

```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq ftp
Router(config)#access-list 100 deny tcp 192.168.2.0 0.0.0.255 any eq ftp
Router(config)#interface ethernet 0/1/0
Router(config-if)#
Router(config-if)#ip access-group 100 out
Router(config-if)#
```

After configuring the Router0 for ACL, we check the ftp service on PC0 (network 1) and PC3(network 2)

PC0:



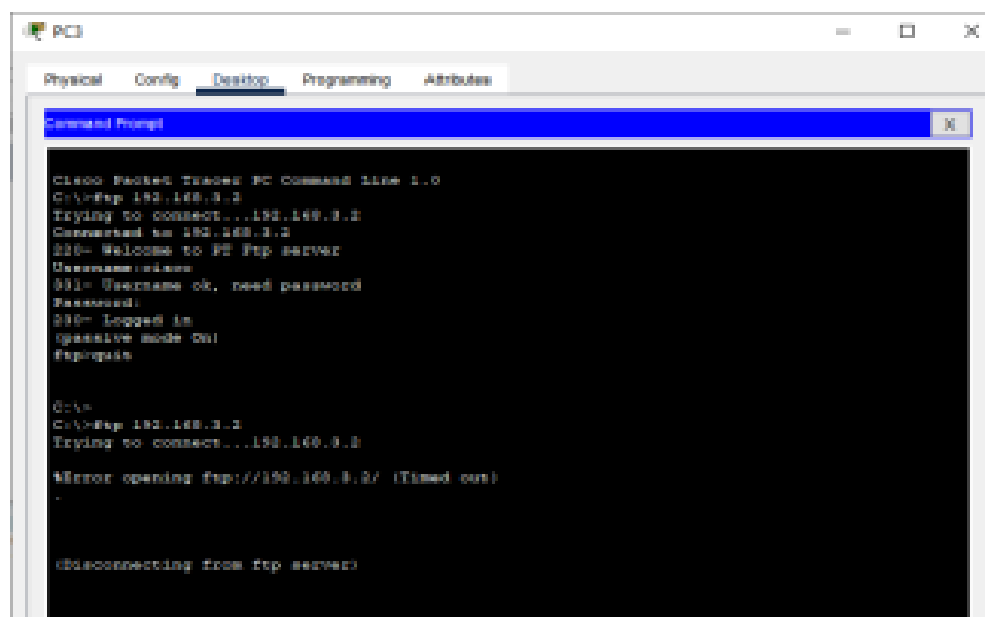
```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

C:\>cd C:\Users\Trainer\PC Command Line 1.0
C:\>ftp 192.168.0.2
Trying to connect...192.168.0.2
Connected to 192.168.0.2
220- Welcome to FT Ftp server
Username:claco
231- Username ok, need password
Password:
230- logged in
passive mode On
ftp>quit

221- Service closing control connection.
C:\>
C:\>ftp 192.168.0.2
Trying to connect...192.168.0.2
Connected to 192.168.0.2
220- Welcome to FT Ftp server
Username:claco
231- Username ok, need password
Password:
230- logged in
passive mode On
ftp>
```

As expected PC0 and all PCs in the network will be ALLOWED access to ftp service

PC3:



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt

C:\>cd C:\Users\Trainer\PC Command Line 1.0
C:\>ftp 192.168.0.2
Trying to connect...192.168.0.2
Connected to 192.168.0.2
220- Welcome to FT Ftp server
Username:claco
231- Username ok, need password
Password:
230- logged in
passive mode On
ftp>quit

C:\>
C:\>ftp 192.168.0.2
Trying to connect...192.168.0.2
Error opening ftp://192.168.0.2/ (Timed out)
-

(Disconnecting from ftp server)
```

As expected PC3 and all PCs in the network will be DENIED access to ftp service

## Practical - 10

- **AIM :**

To construct wireless LAN and make PC wireless using DHCP Server.

- **REQUIREMENT :**

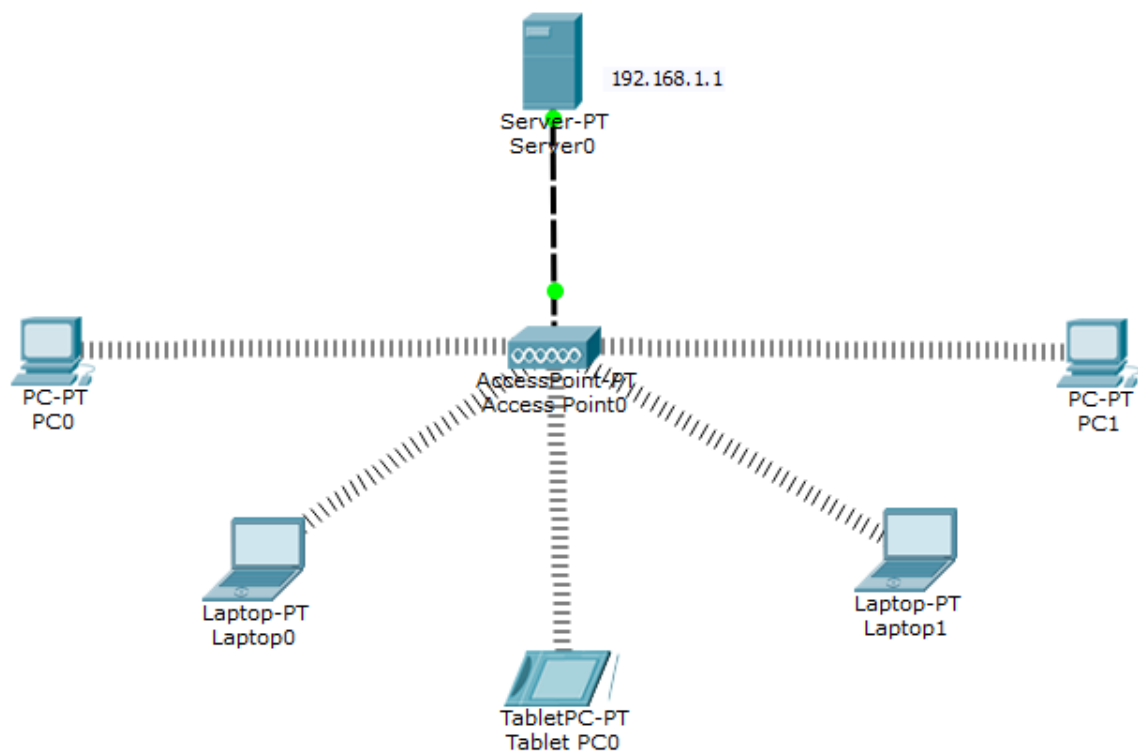
1. Windows PC (Minimum 2)
2. Access point Switch (1)
3. Server (1)
4. Wireless Tab (1)

- **THEORY :**

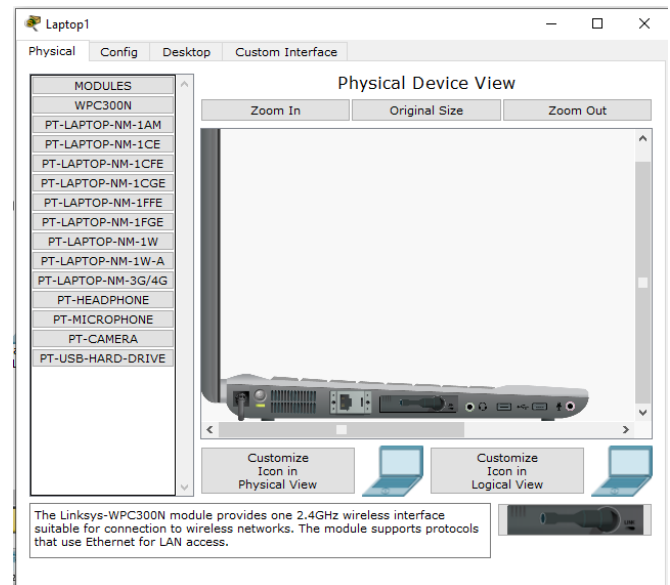
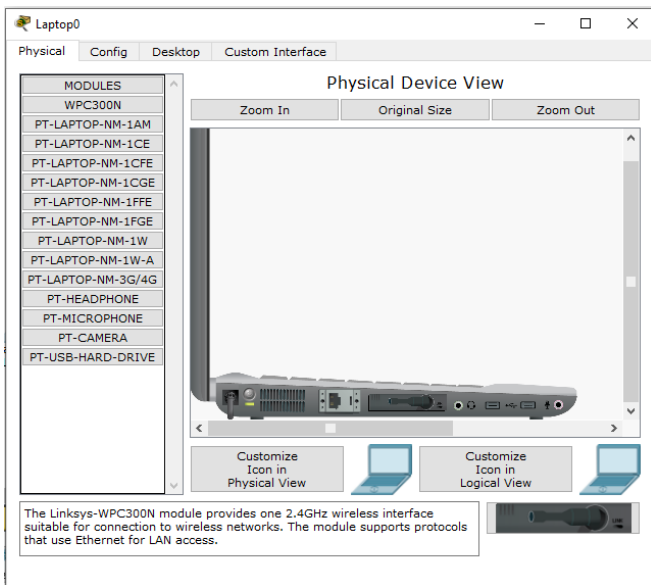
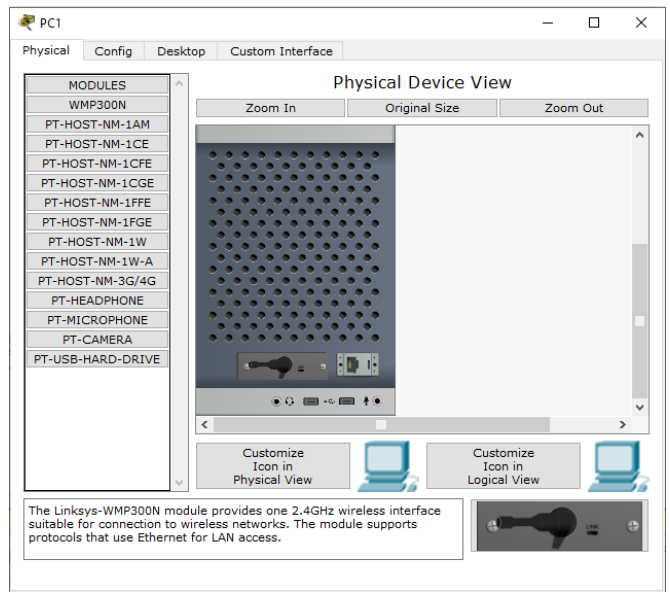
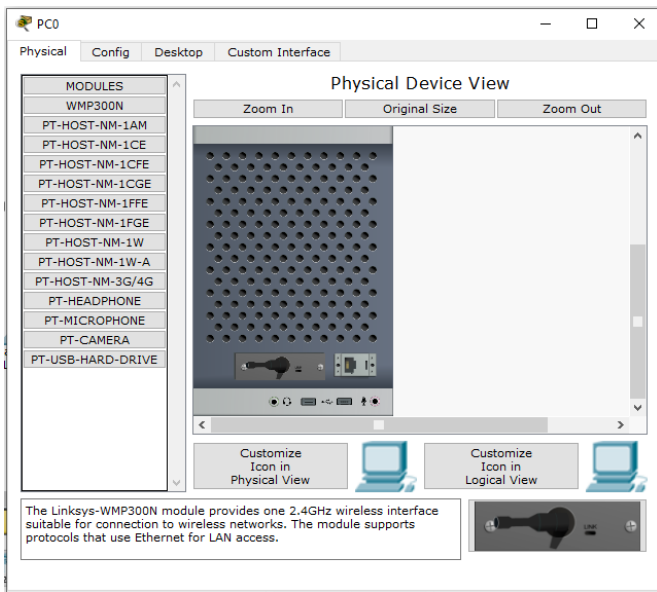
### WLAN(Wireless Local Area Network) :

A wireless local area network implements a flexible data communication system, frequently augmenting rather than replacing a wired LAN within a building or campus WLAN uses radio frequency to transmit and receive data over the air minimizing the need for wired communication.

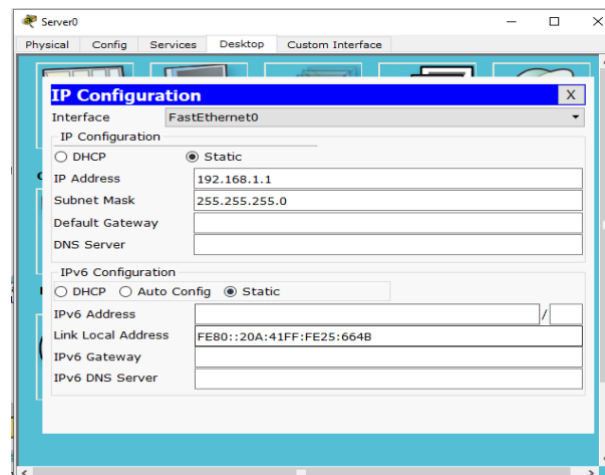
### Topology :



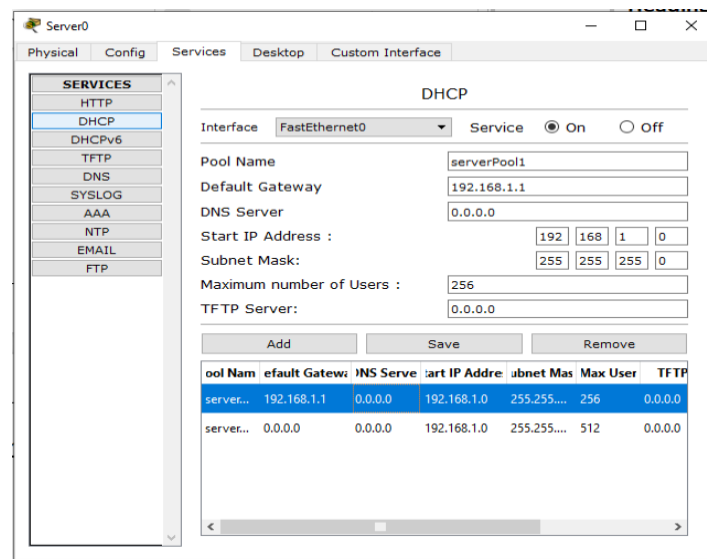
## Adding wireless port to PC's and Laptops :



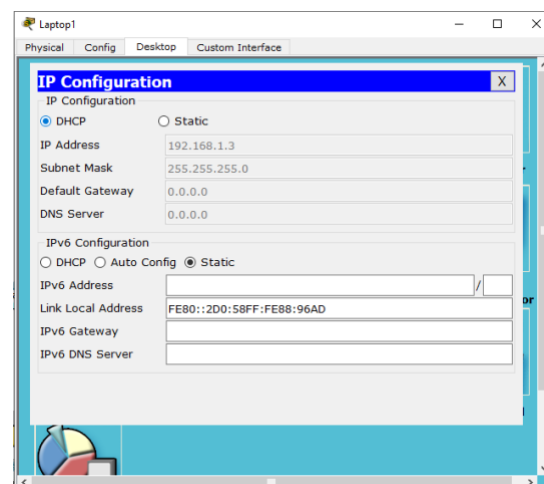
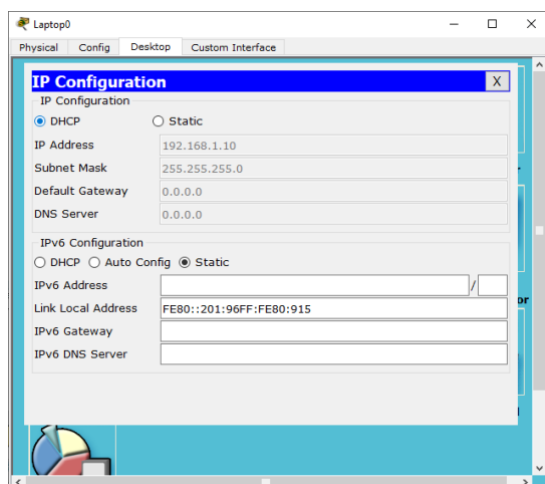
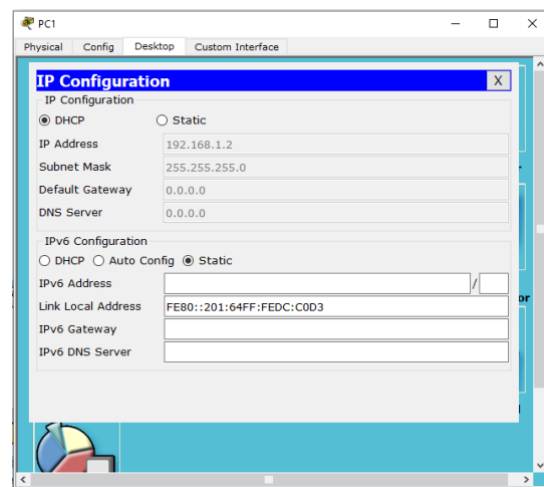
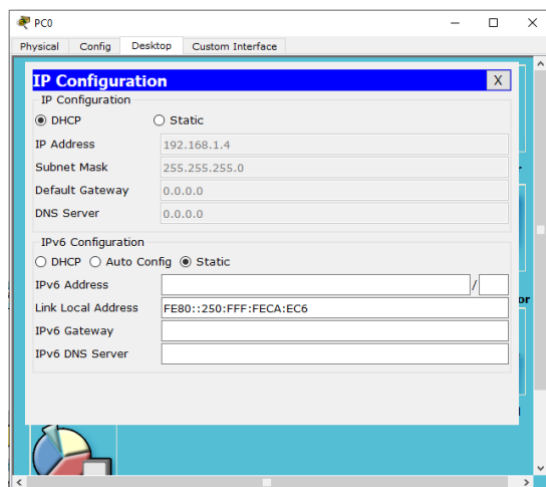
## We will configure the server :

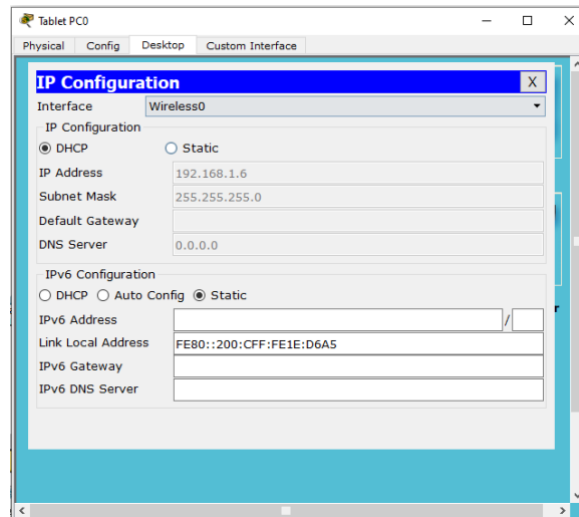


We will turn on the services of DHCP server to provide IP addresses to the end devices :

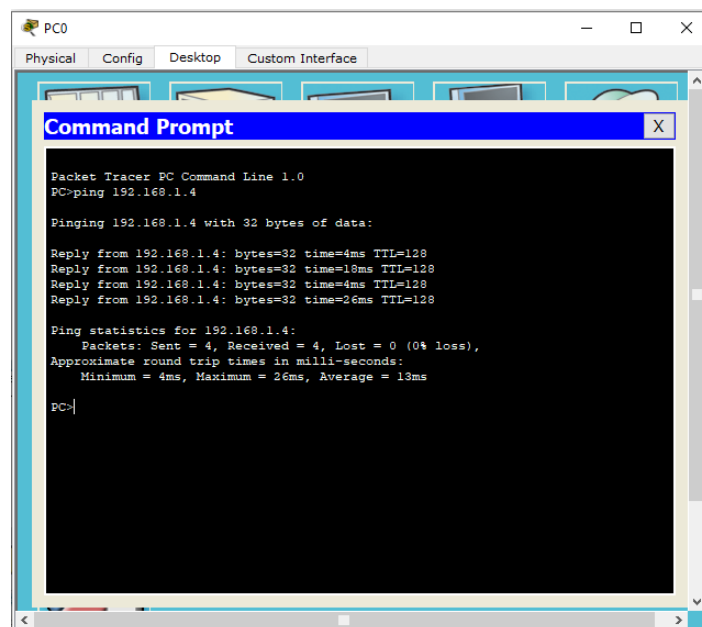


All the end devices are wirelessly connected and got their IP addresses through DHCP Server :





Now we can give the ping command as shown to check the connectivity :



We can also send packets through PC's :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	Tablet PC0	ICMP		0.000	N	0
	Successful	Laptop0	Laptop1	ICMP		0.000	N	1
	Successful	Tablet ...	PC1	ICMP		0.000	N	2

Packets Sent Successfully