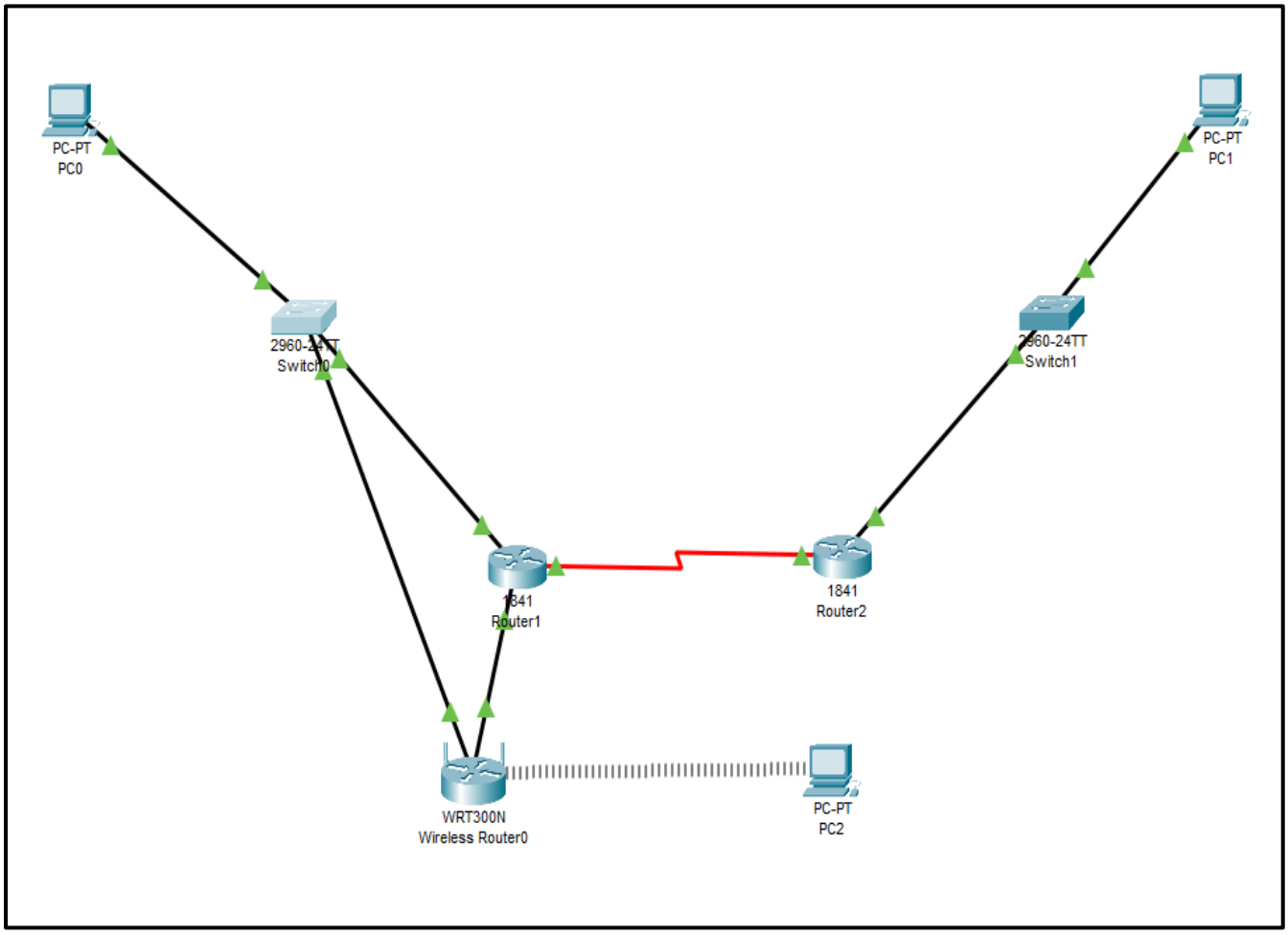
Practical No: 01

Aim: Configuring WEP on a Wireless Router

Components: Wireless Router, Router, Switch, Device (PC)

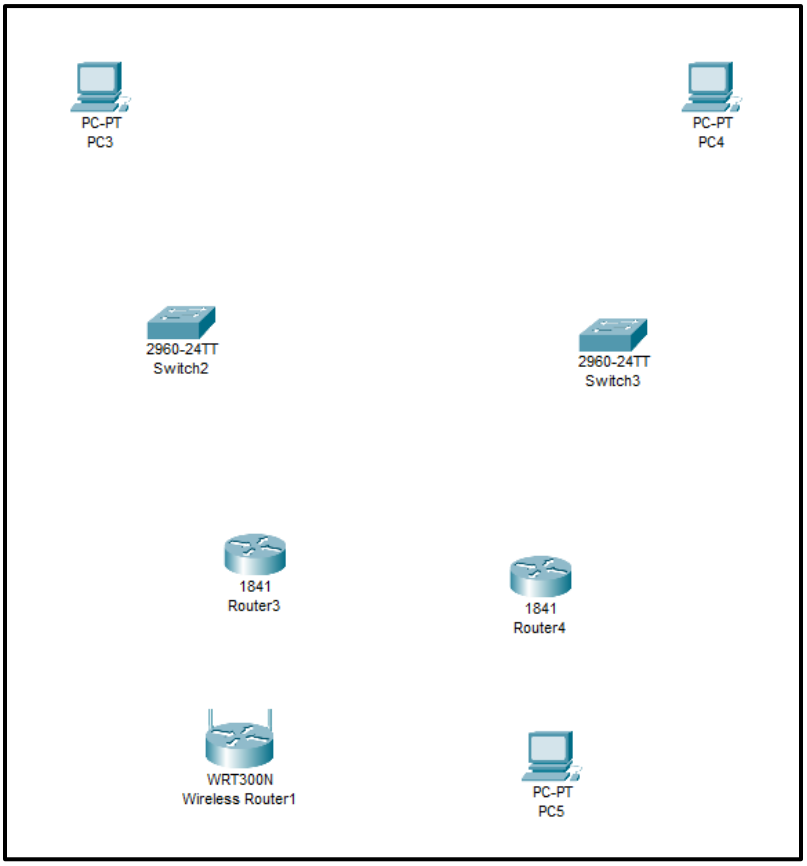
Theory: Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

Cisco Packet Tracer Setup:-

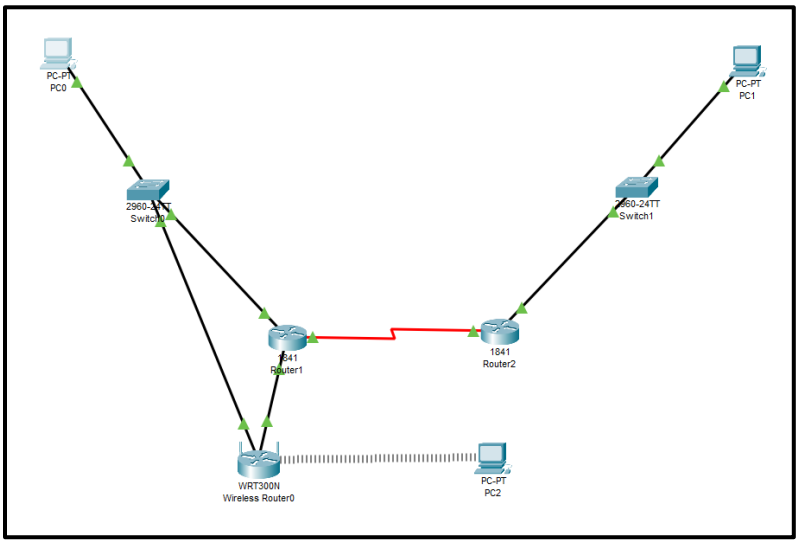


Implementation:

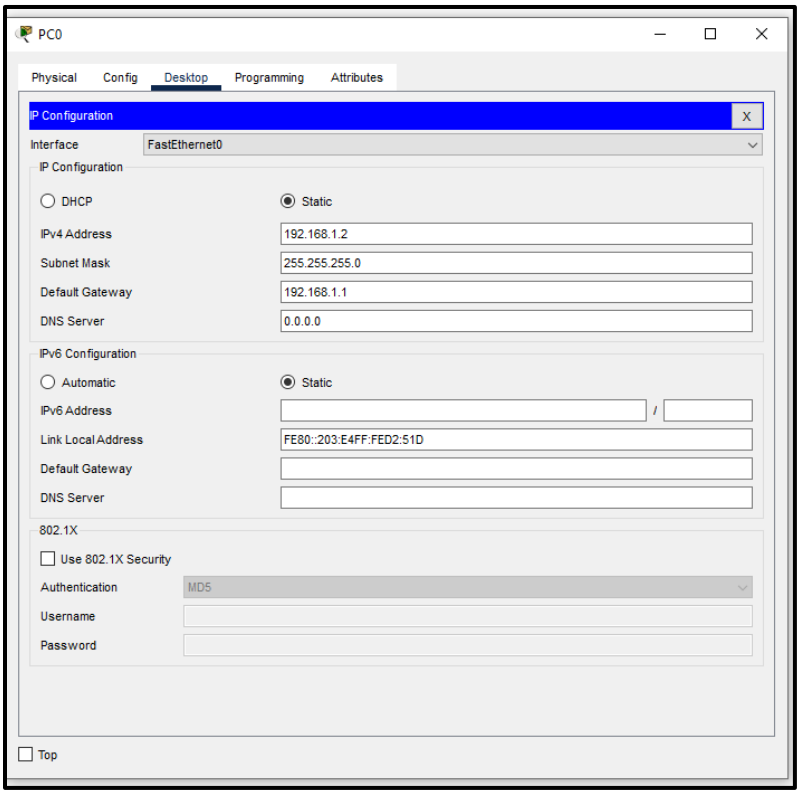
Step 1: Arranging devices

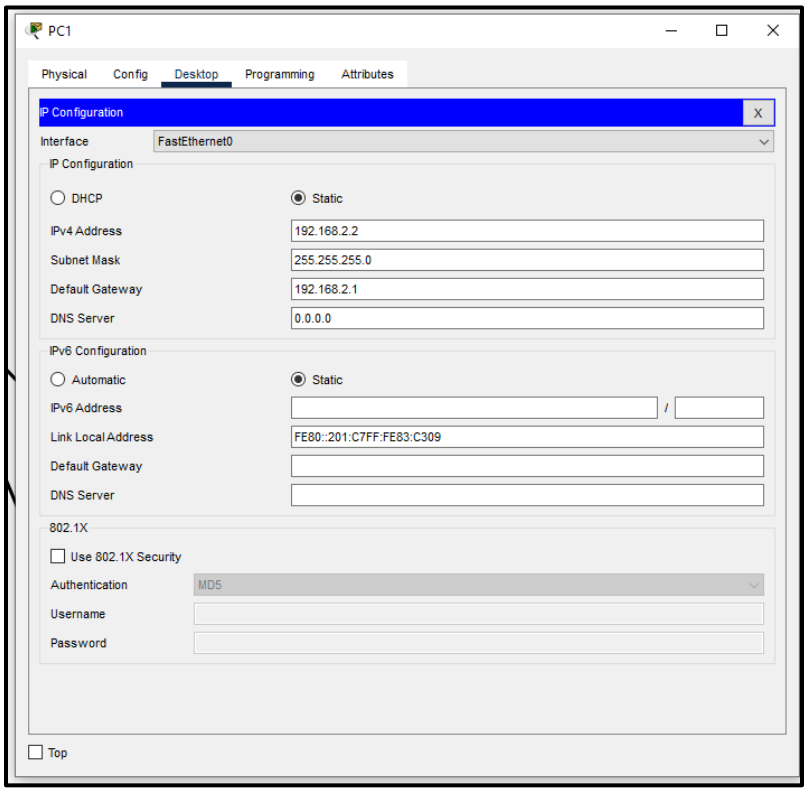


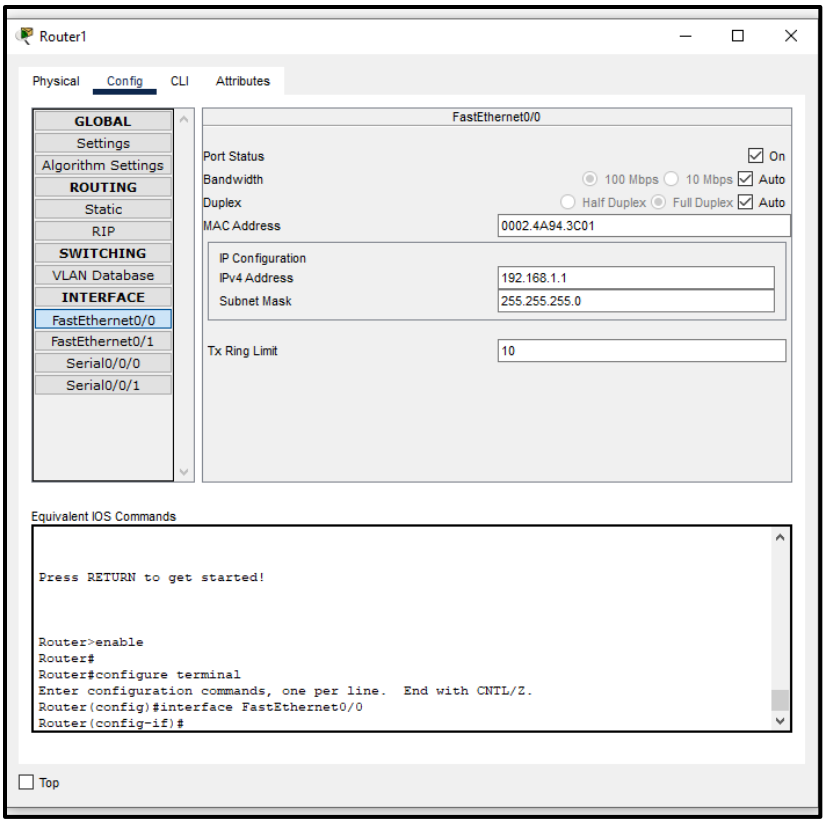
Step 2: Creating connections using Ethernet and serial cable between devices

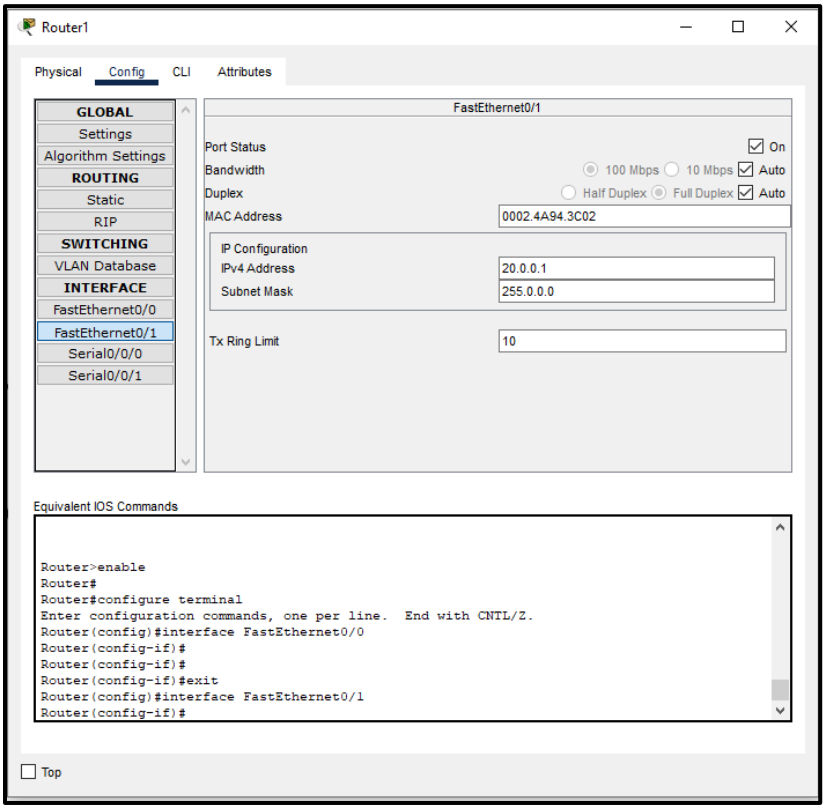


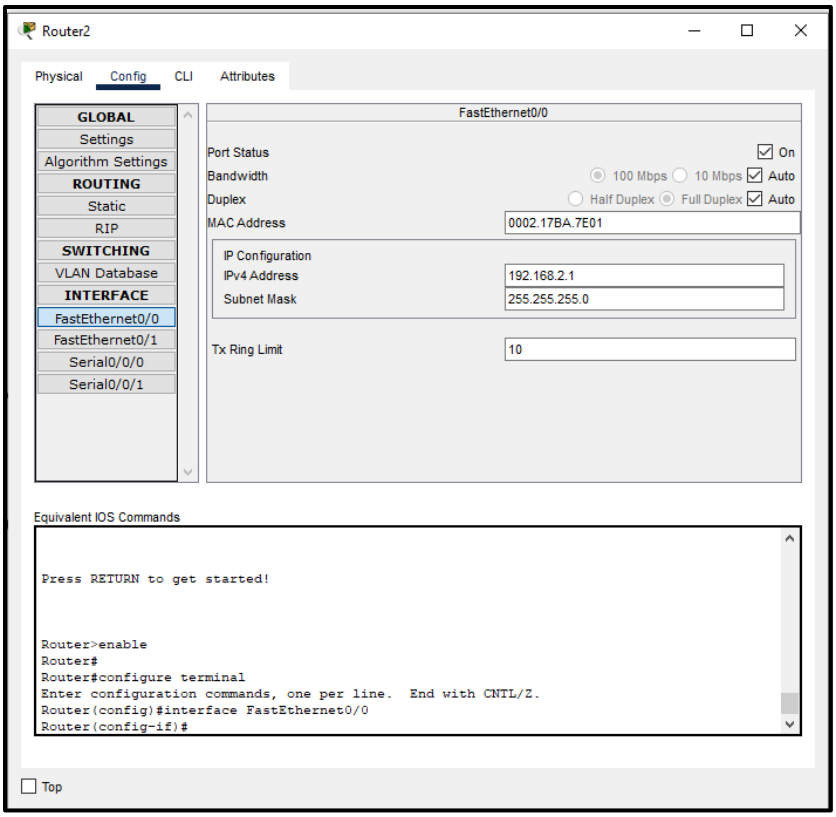
Step 3: Configuring all devices

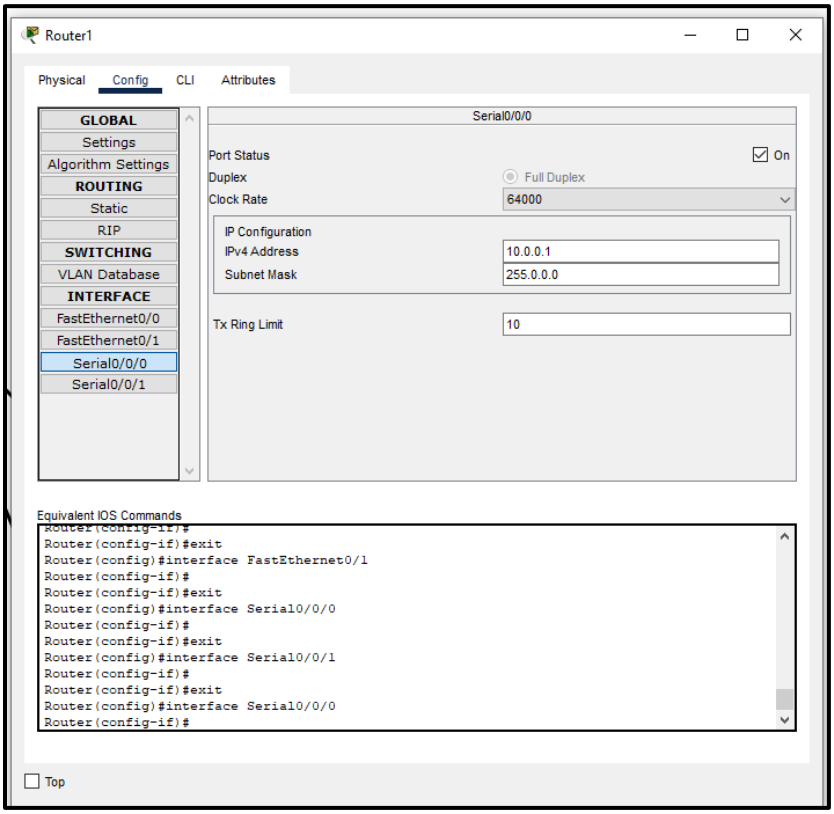


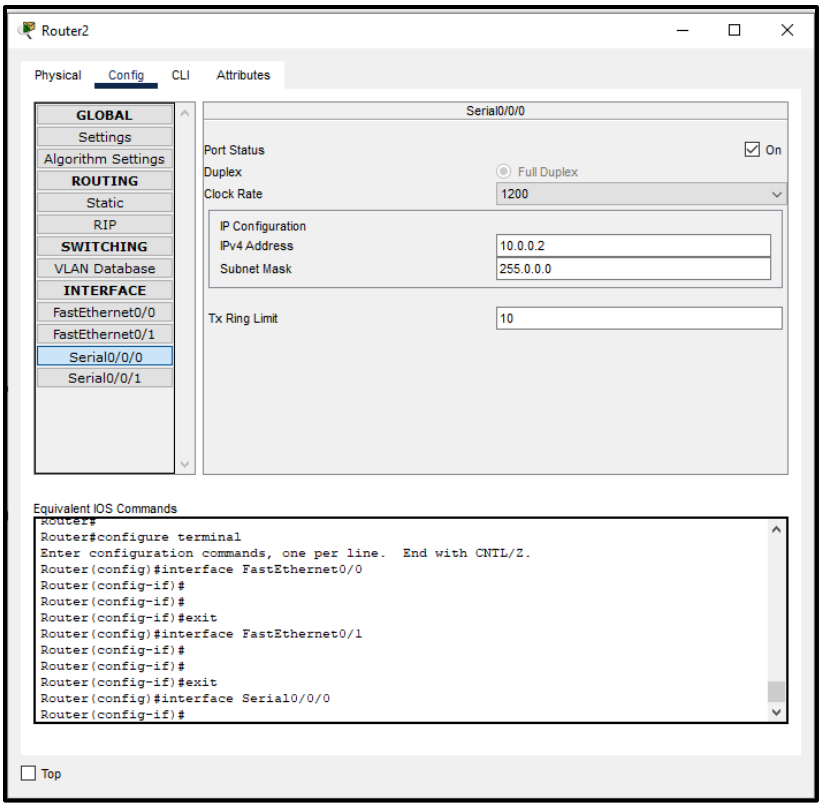


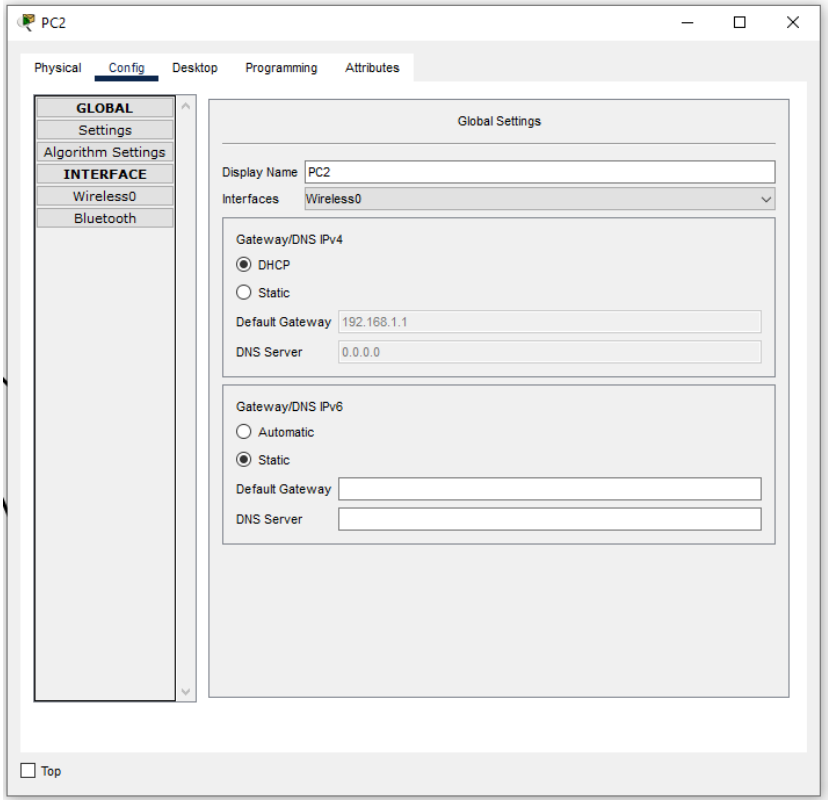

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.4A94.3C01
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Press RETURN to get started!
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.4A94.3C02
IP Configuration
IPv4 Address
20.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Top

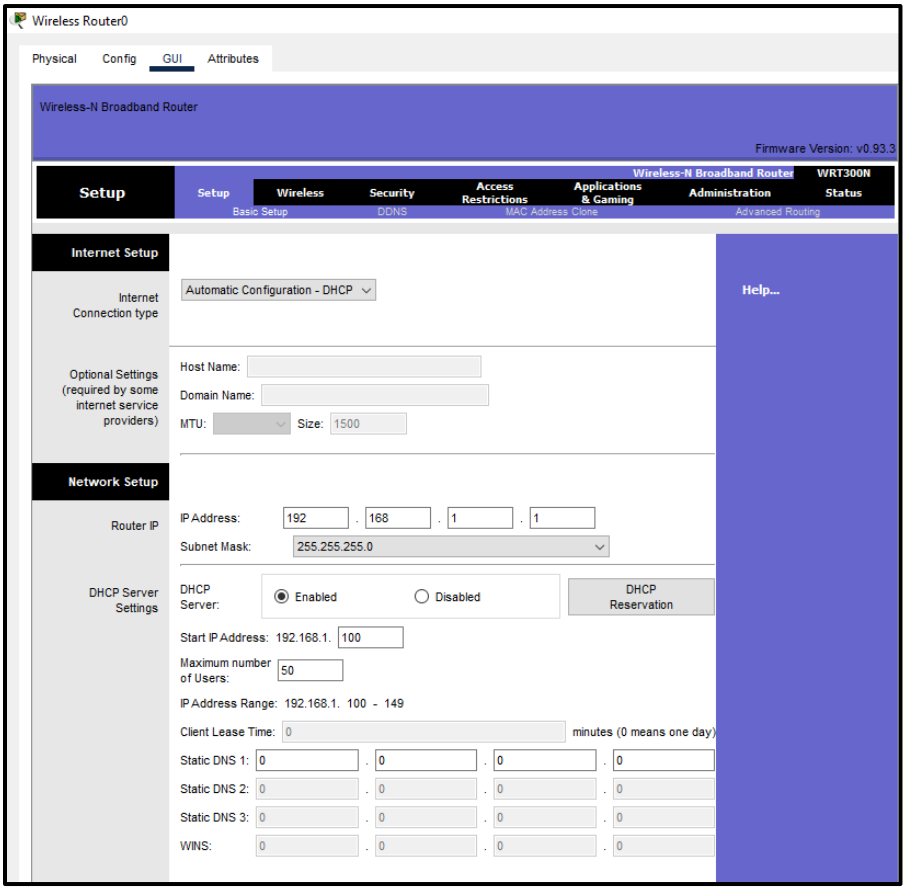

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.17BA.7E01
IP Configuration
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Press RETURN to get started!
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
64000
IP Configuration
IPv4 Address
10.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Top

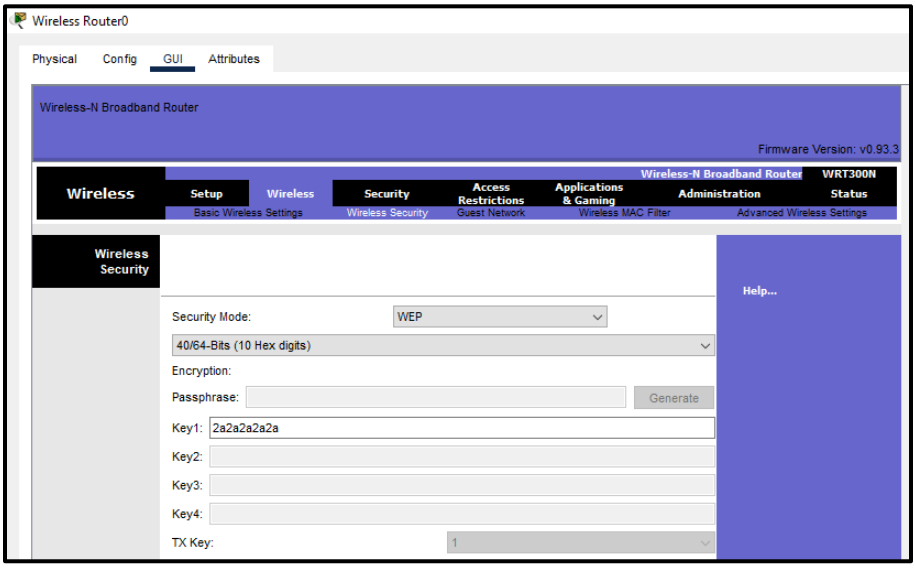

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
10.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Top


PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Bluetooth
Global Settings
Display Name
PC2
Interfaces
Wireless0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

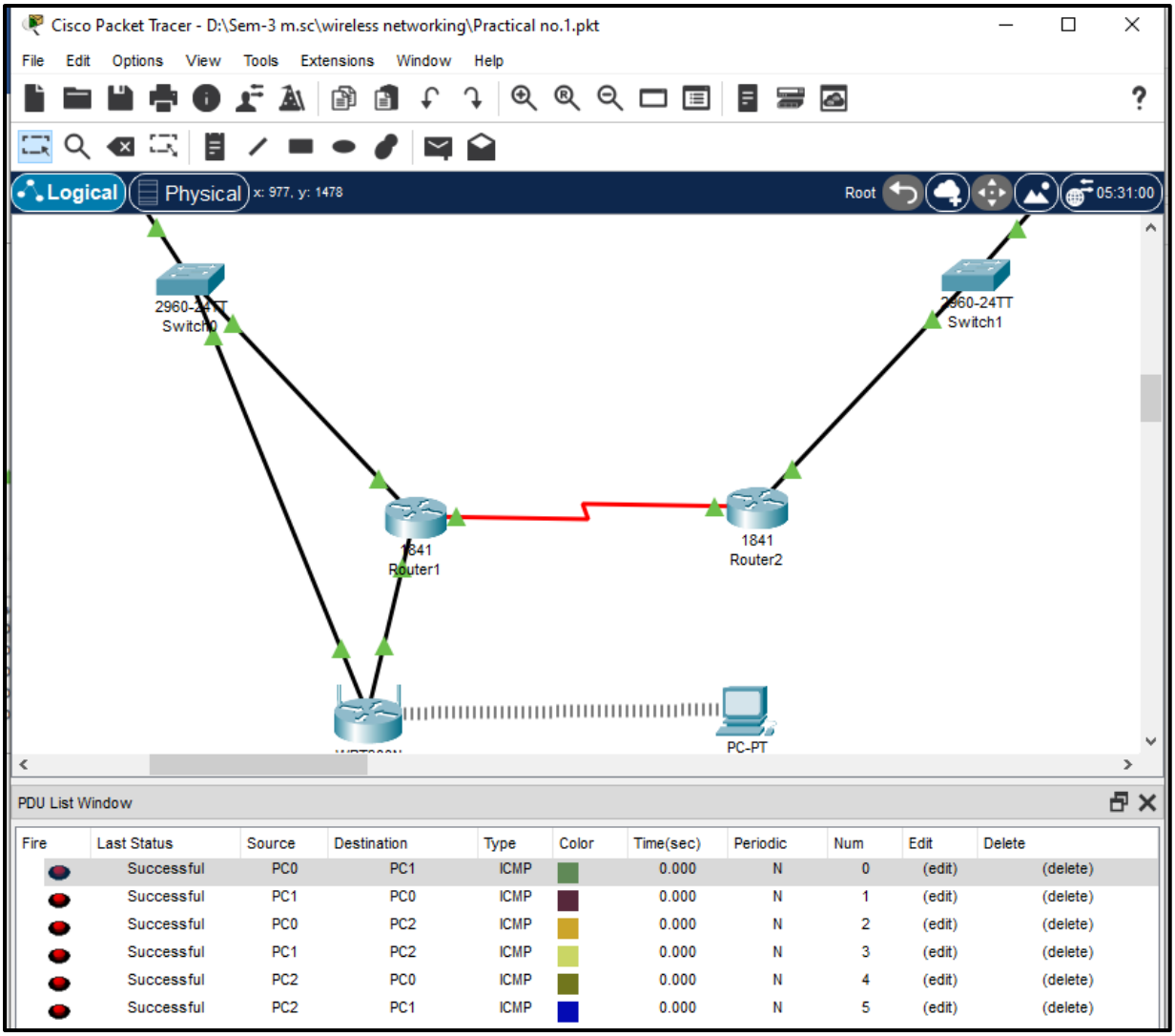
Step 4: Configuring wireless router



Step 5: Adding security mode as **WEP** and setting up key as **2a2a2a2a2a**



Checking connection:



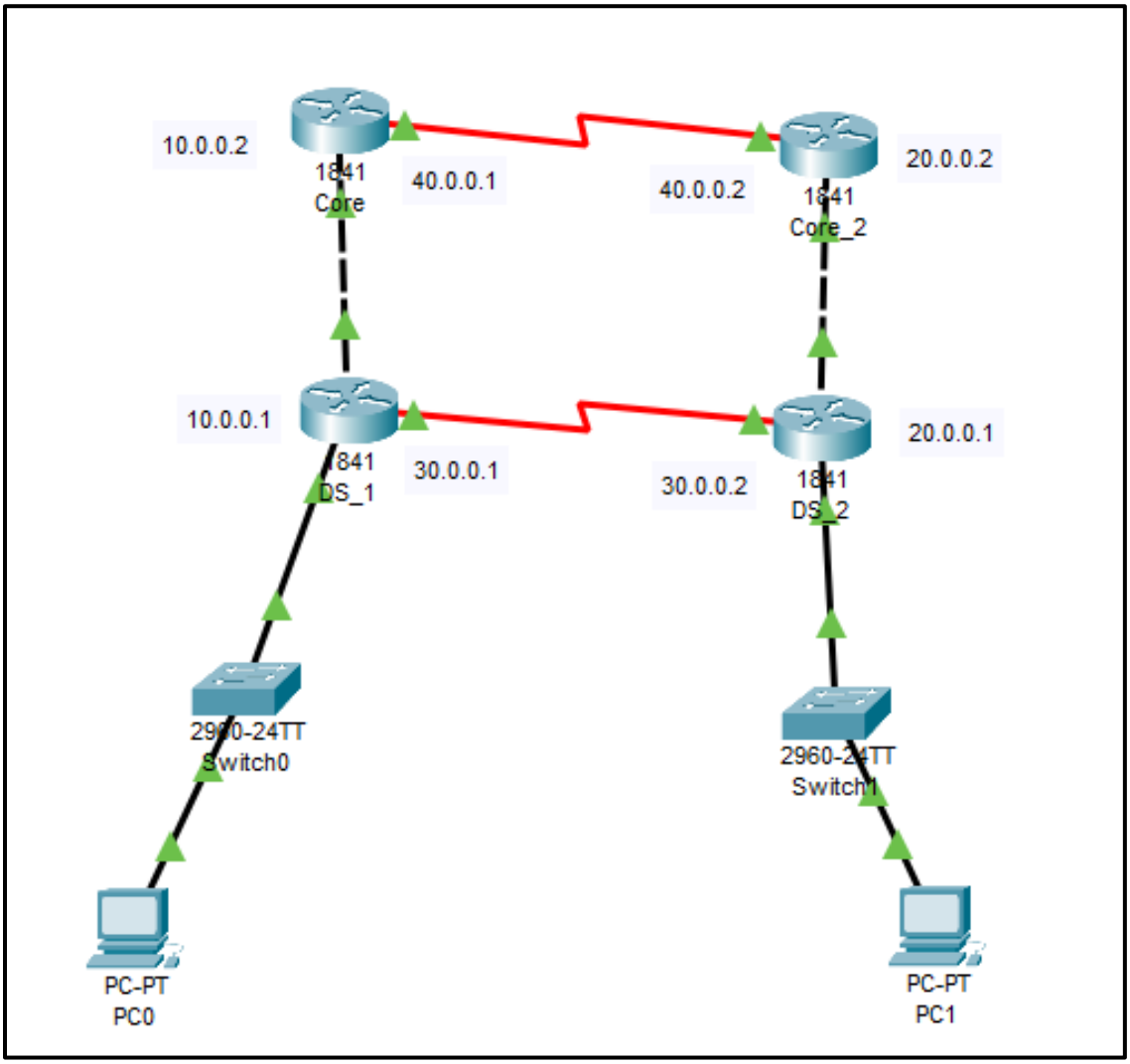
Practical No: 02

Aim: Demonstrating Distribution Layer Functions

Components: Router, Switch, Device (PC)

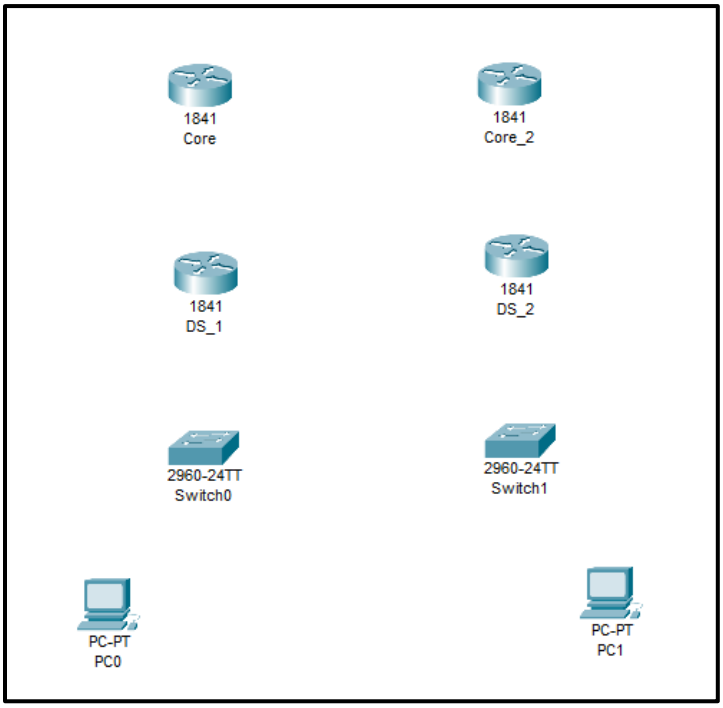
Theory: The distribution layer is the smart layer in the three-layer model. Routing, filtering, and QoS policies are managed at the distribution layer. Distribution layer devices also often manage individual branch-office WAN connections. This layer is also called the Workgroup layer.

Cisco Packet Tracer Setup:-

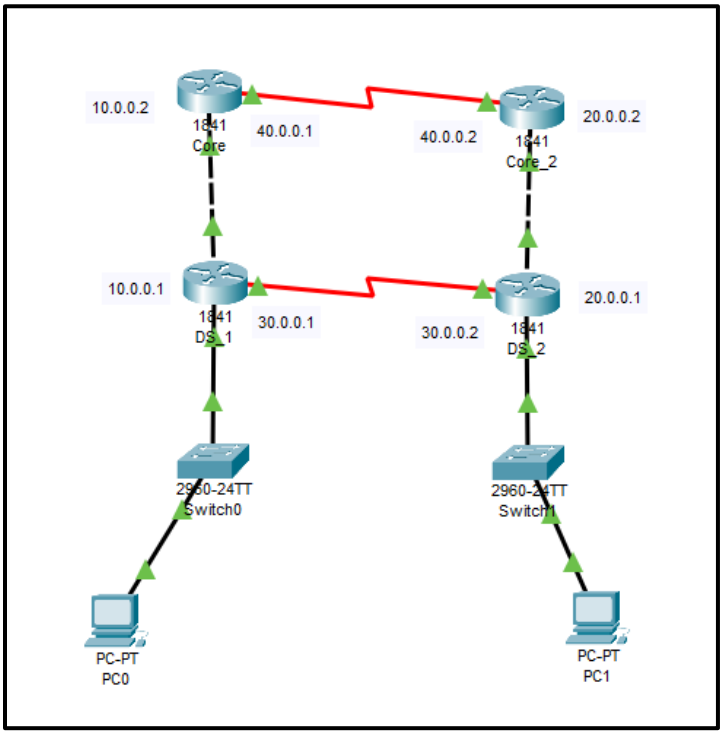


Implementation:

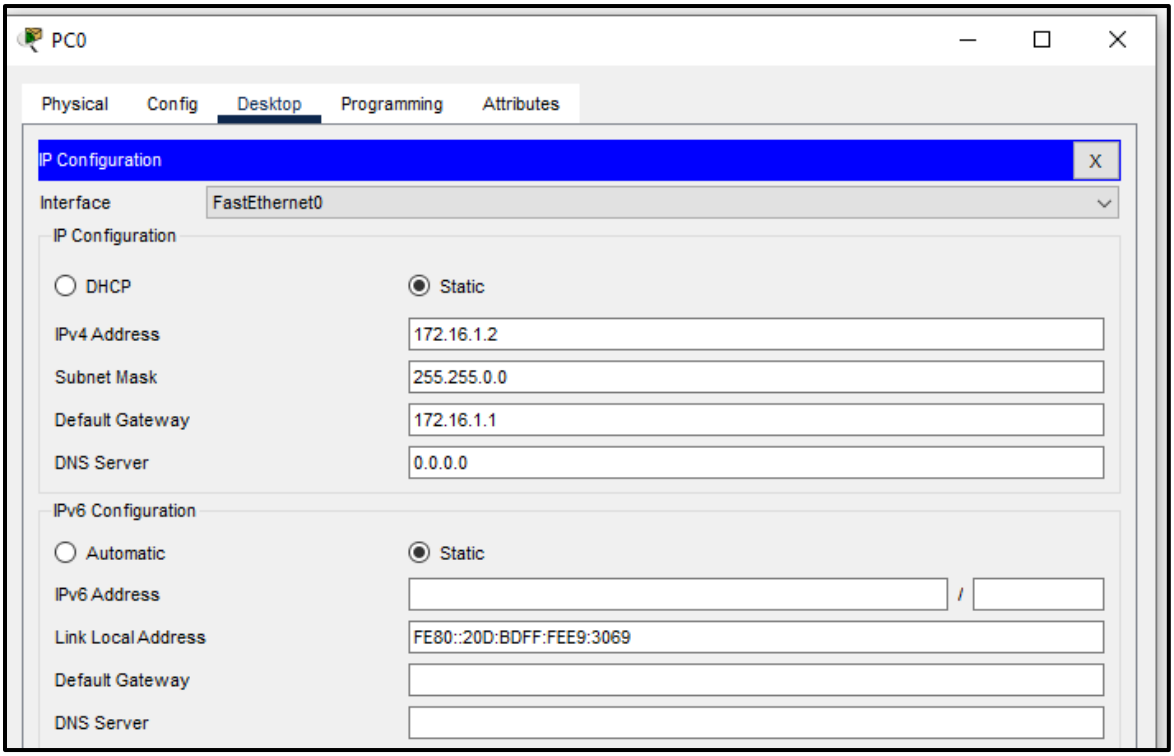
Step 1: Arranging devices



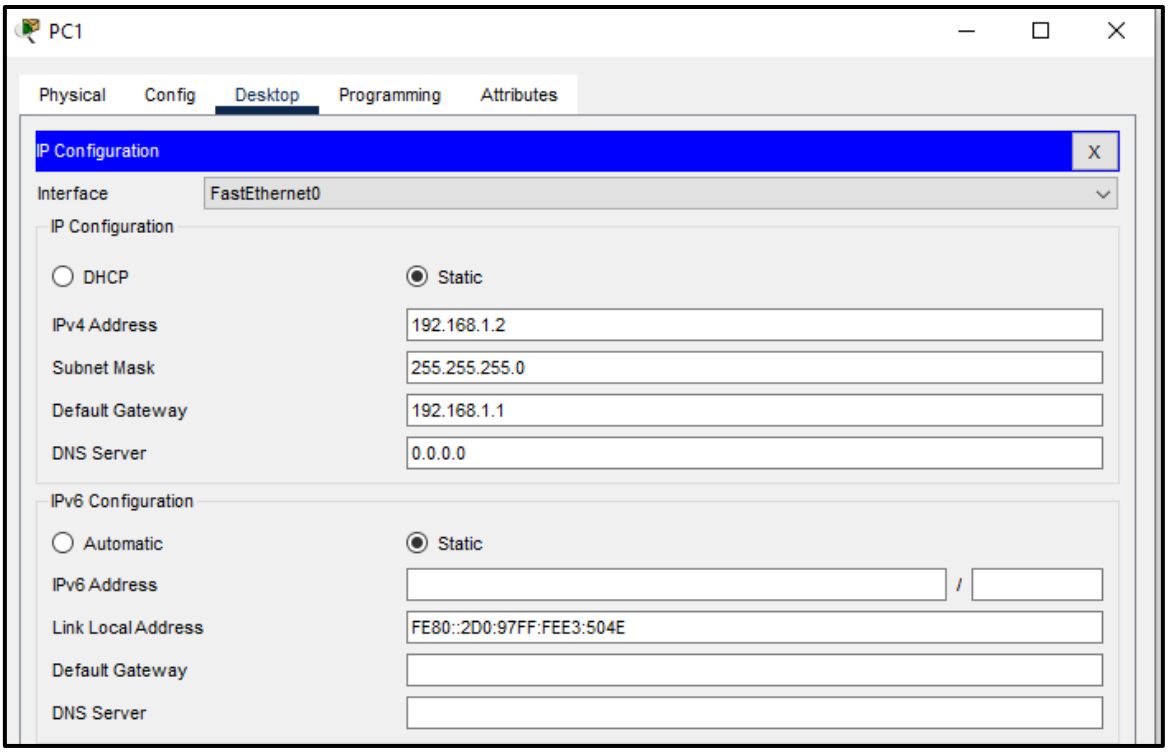
Step 2: Creating connections using Ethernet and serial cable between devices

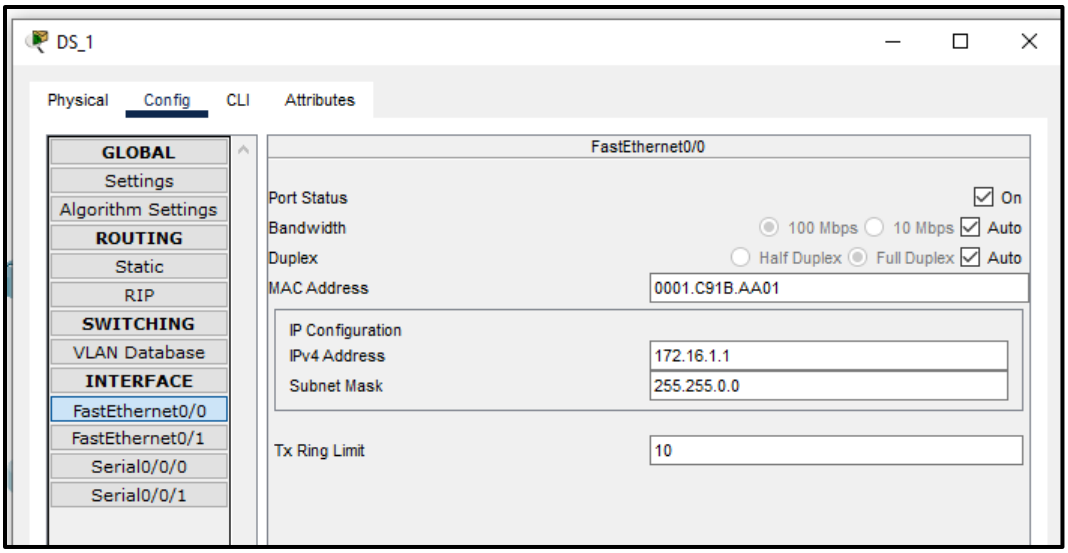


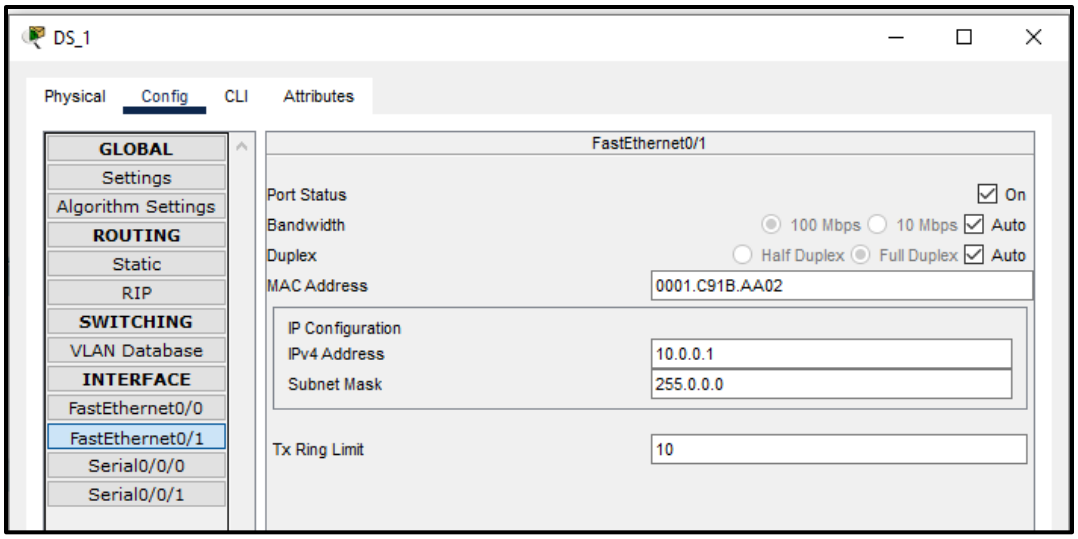
Step 3: Configuring all devices

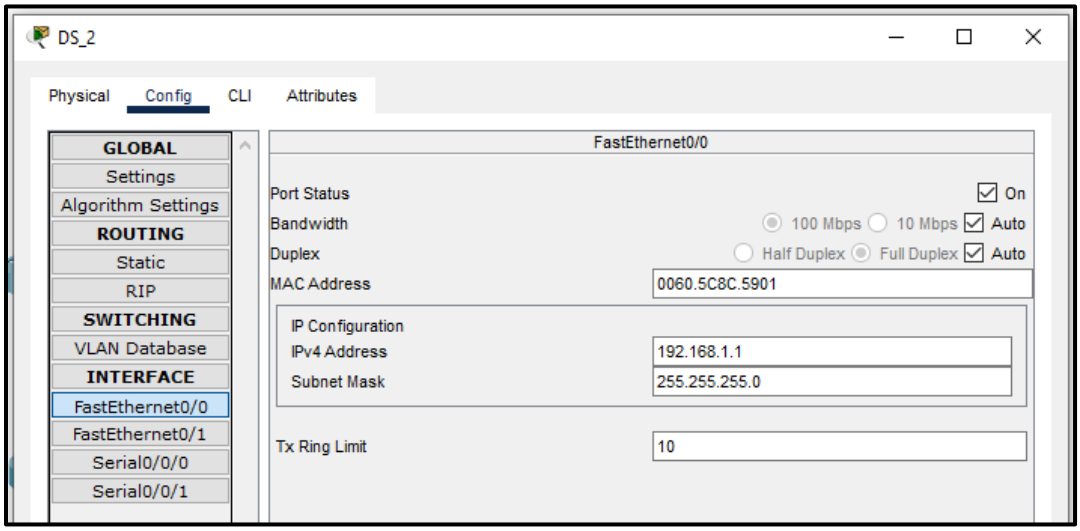


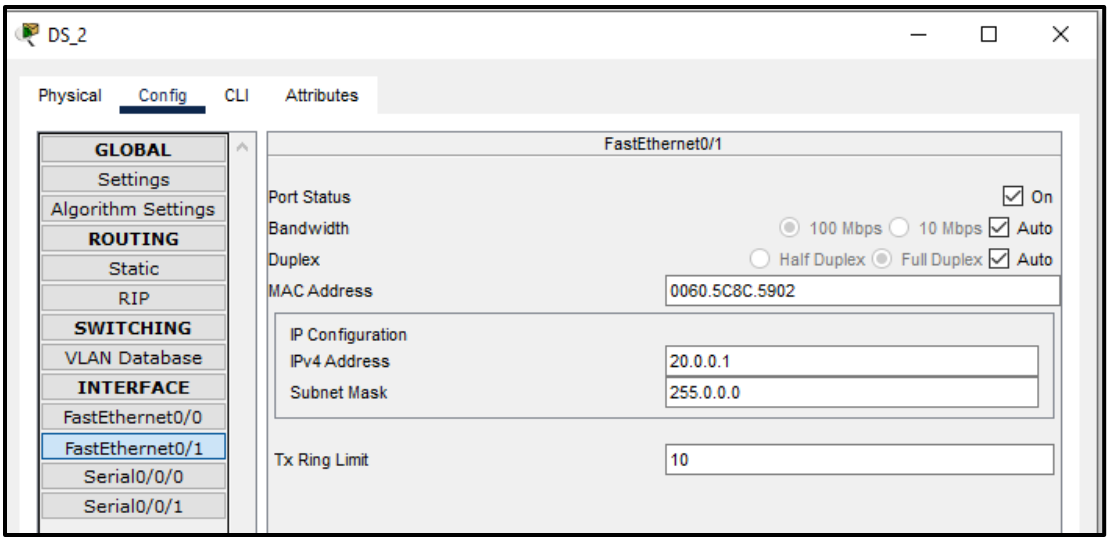
Step 4: Setting up distribution layer using router

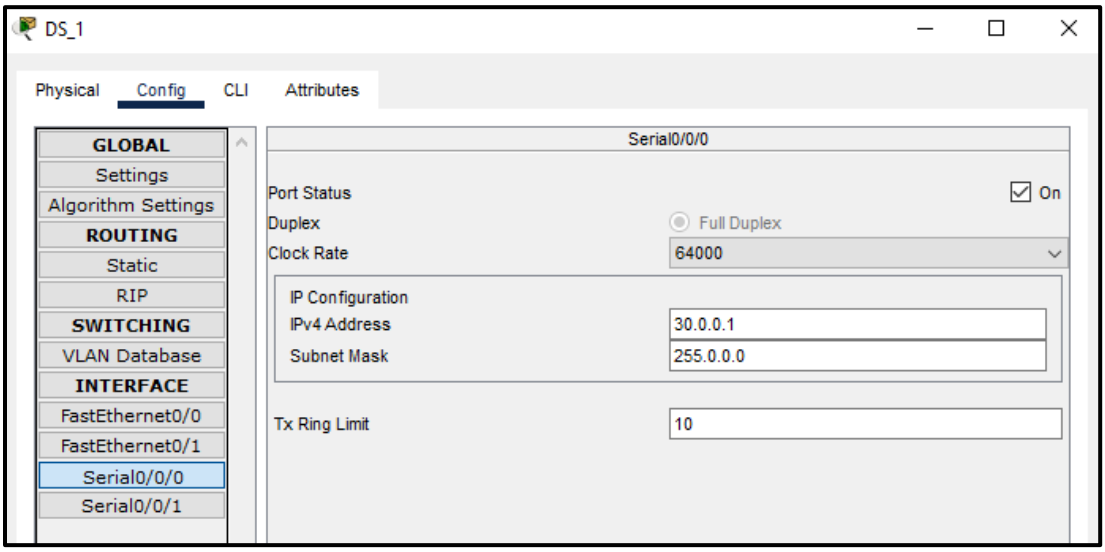


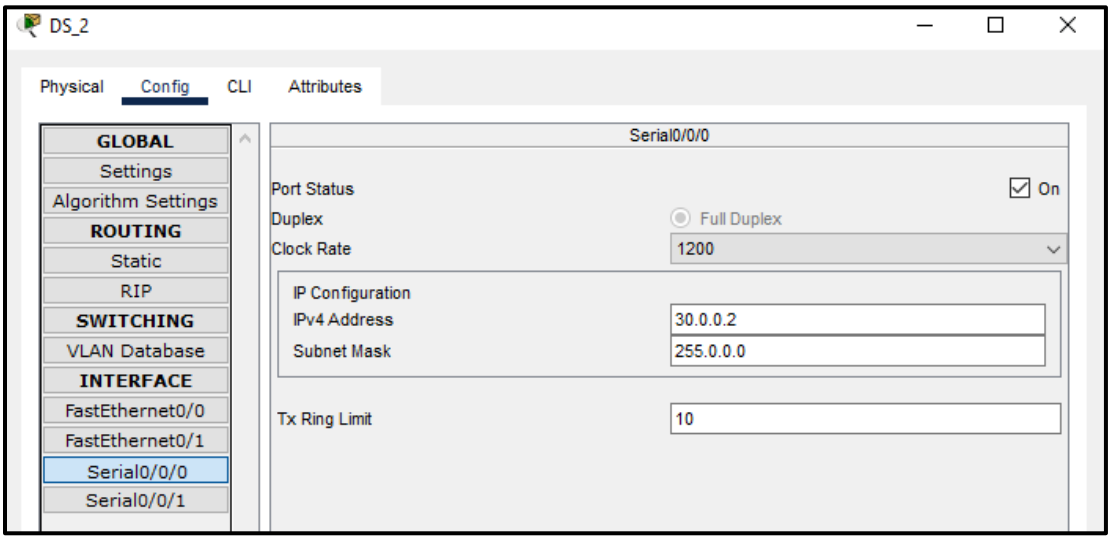

DS_1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C91B.AA01
IP Configuration
IPv4 Address
172.16.1.1
Subnet Mask
255.255.0.0
Tx Ring Limit
10


DS_1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C91B.AA02
IP Configuration
IPv4 Address
10.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

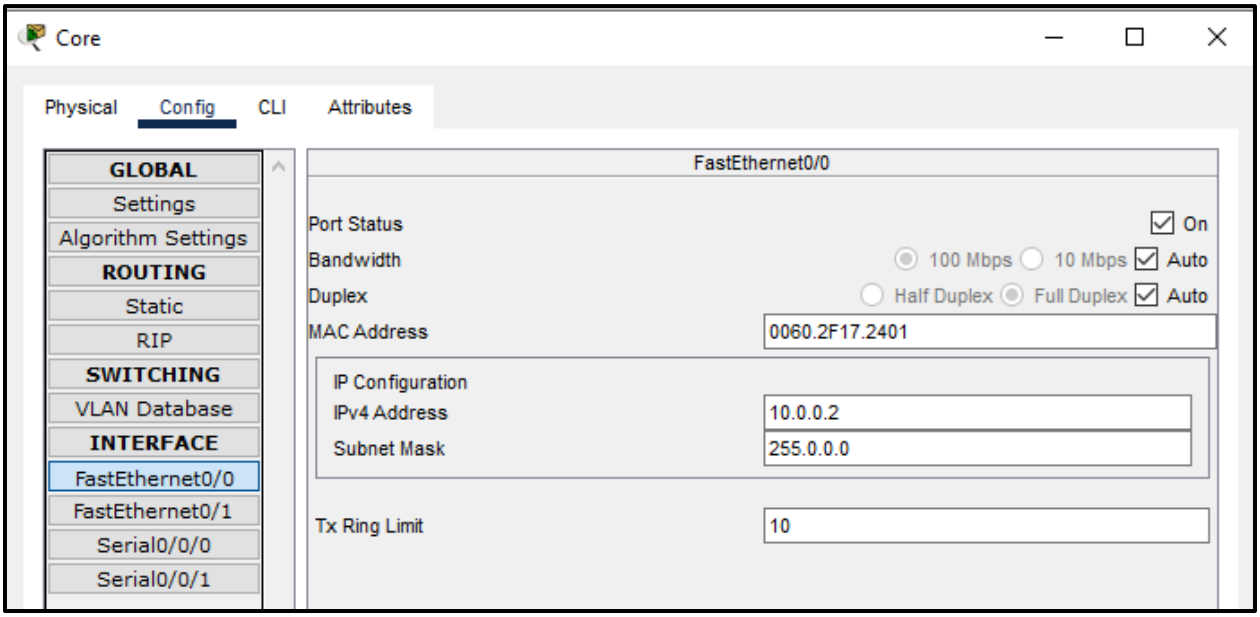

DS_2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.5C8C.5901
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

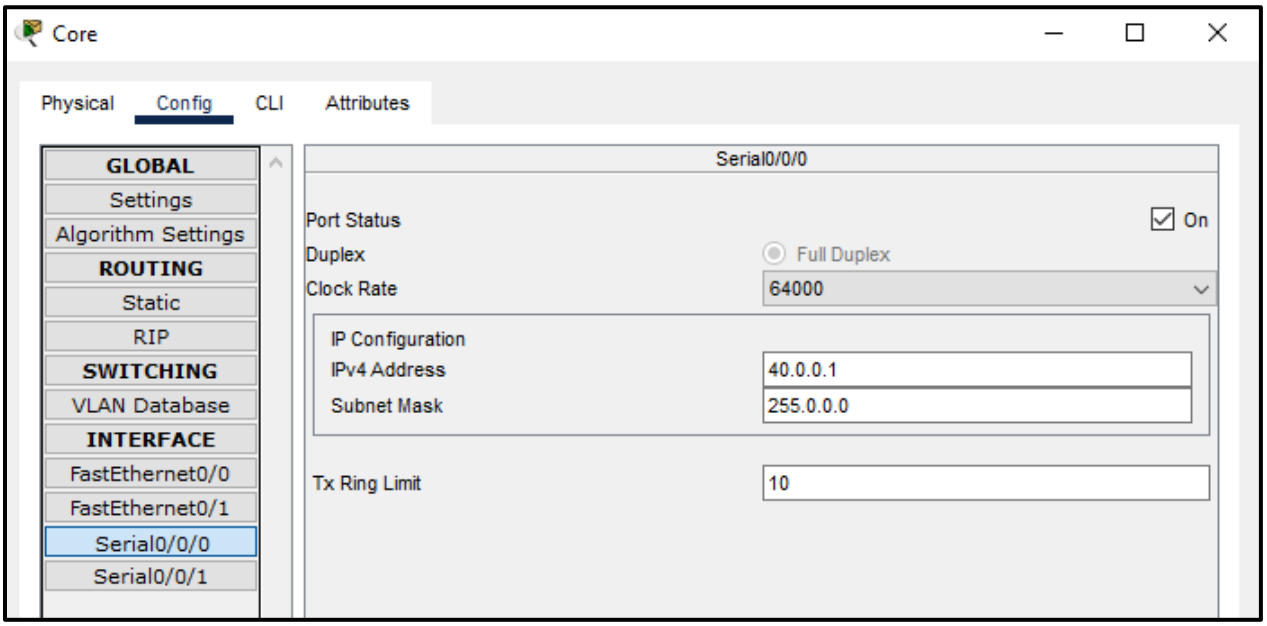

DS_2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.5C8C.5902
IP Configuration
IPv4 Address
20.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

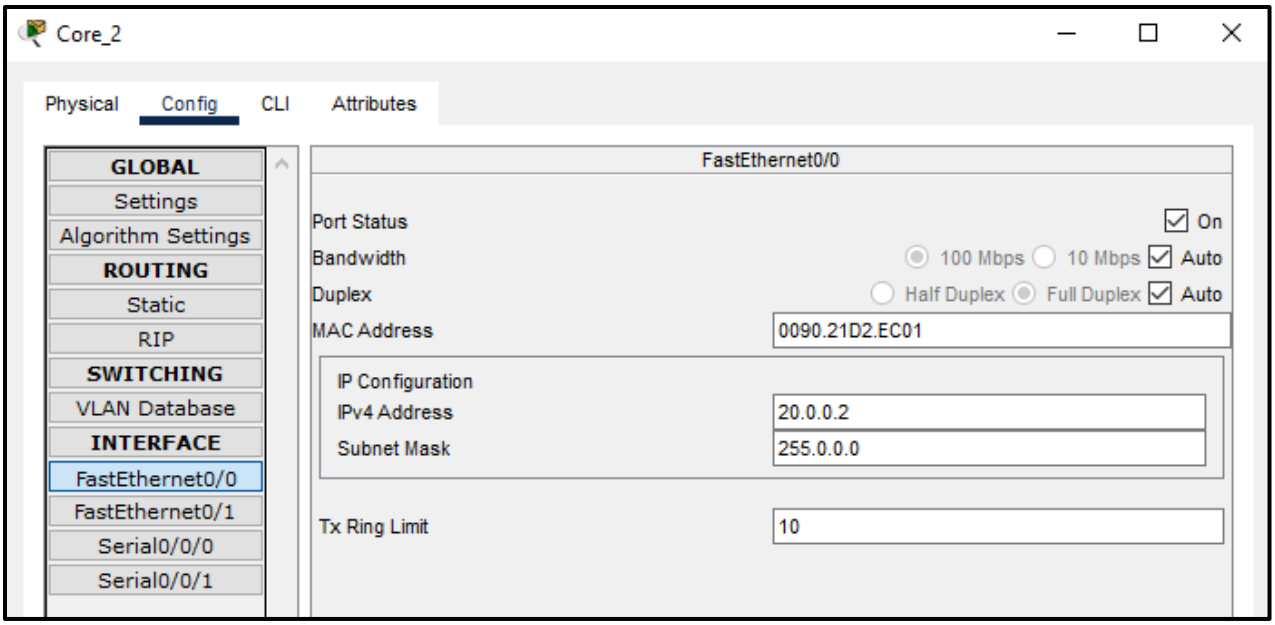

DS_1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
64000
IP Configuration
IPv4 Address
30.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

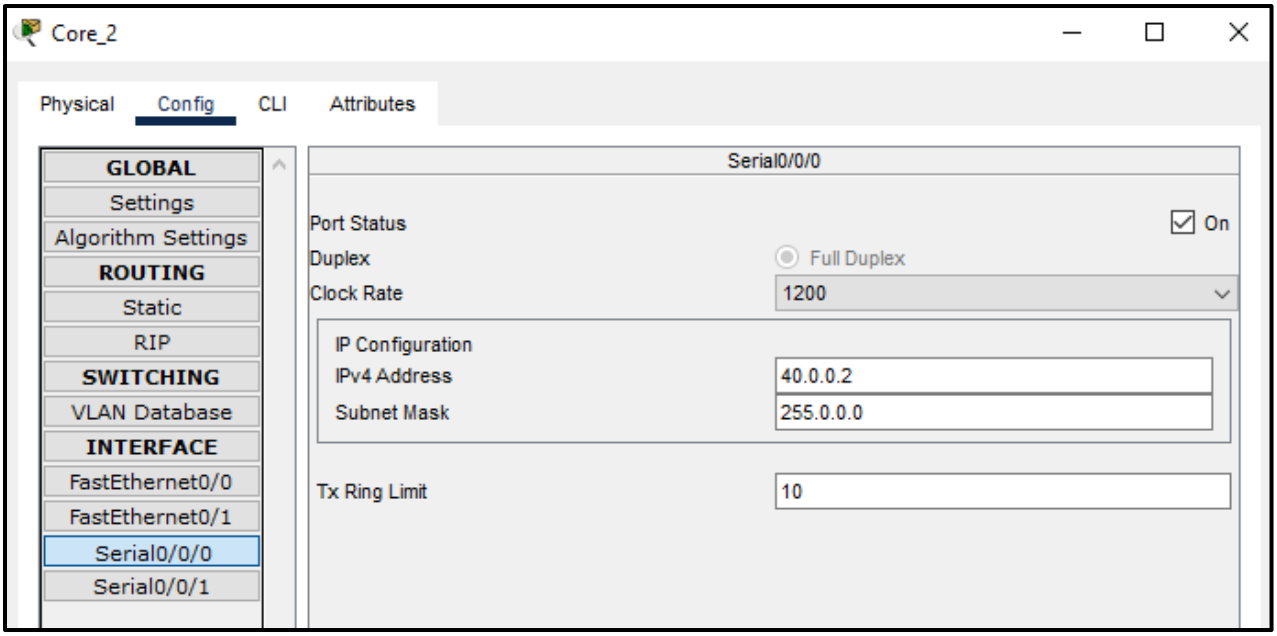

DS_2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
30.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

Step 5: Setting up core routers

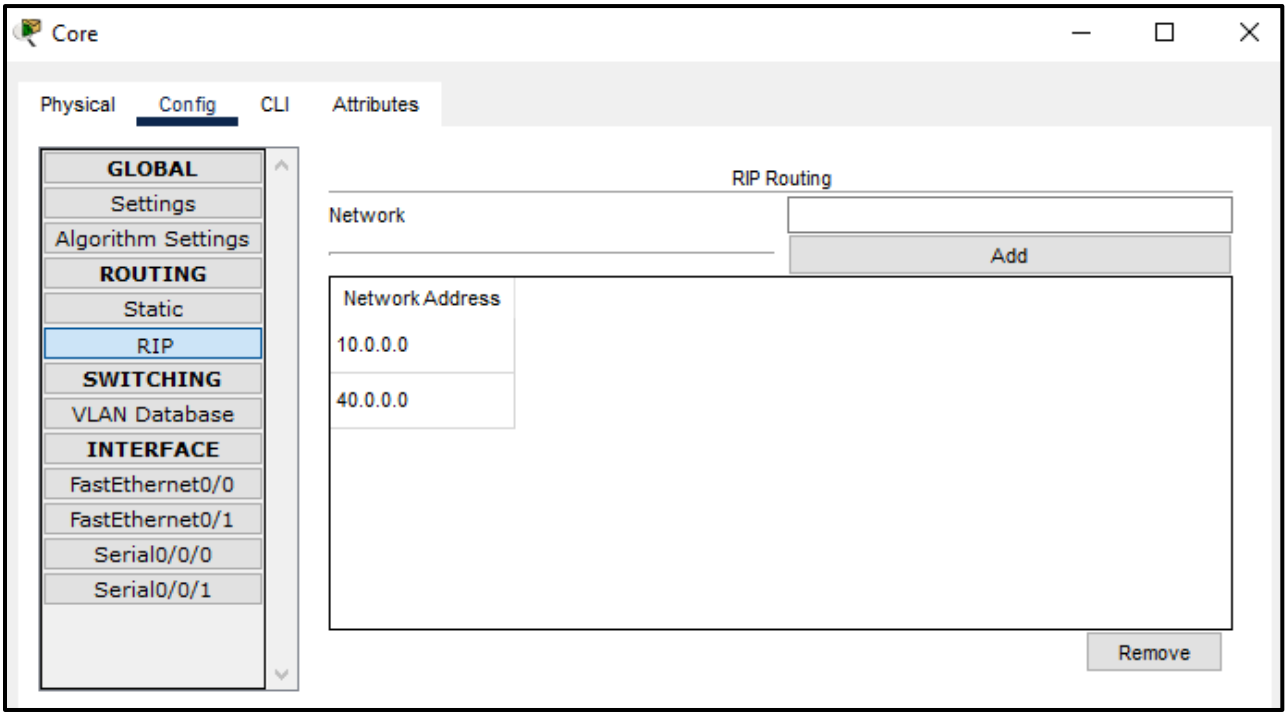


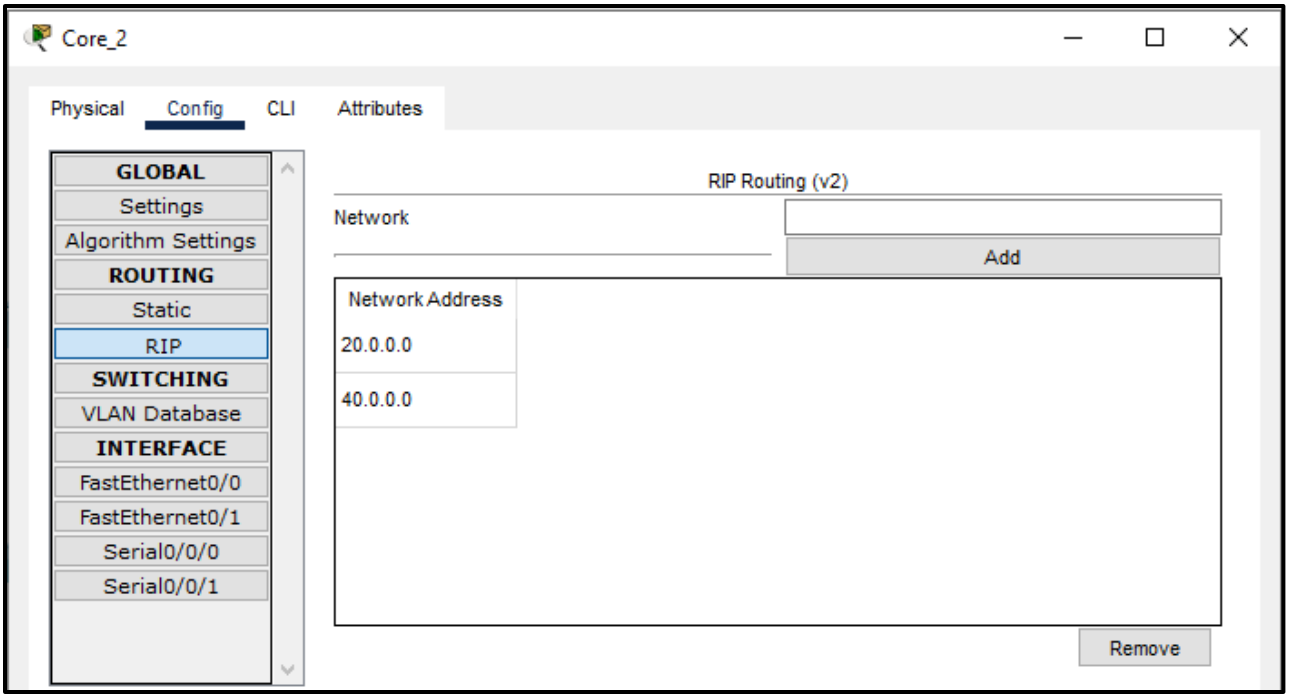


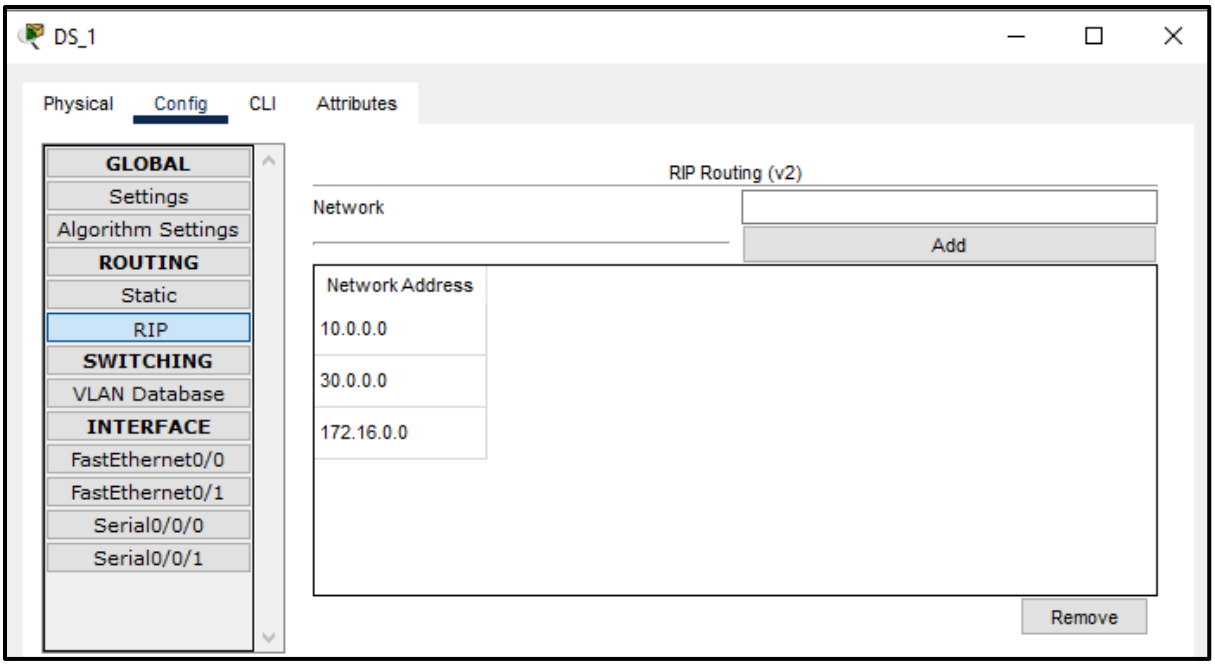

Core_2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.21D2.EC01
IP Configuration
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

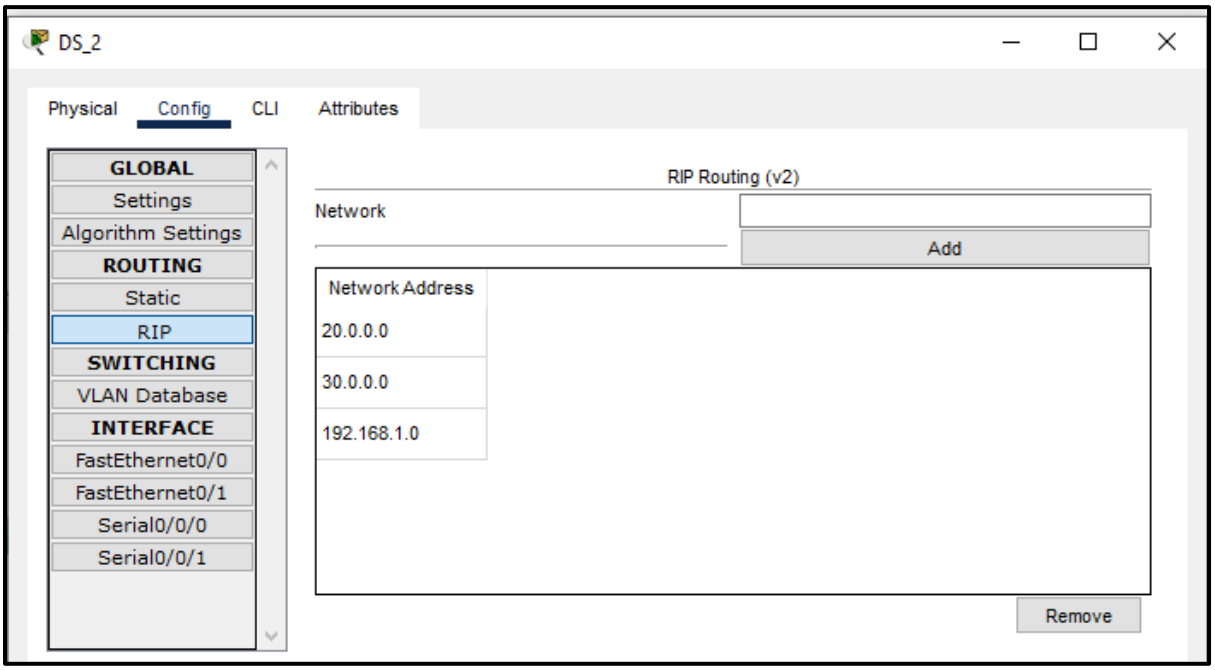

Core_2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
40.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

Step 6: Setting up RIP routing protocol

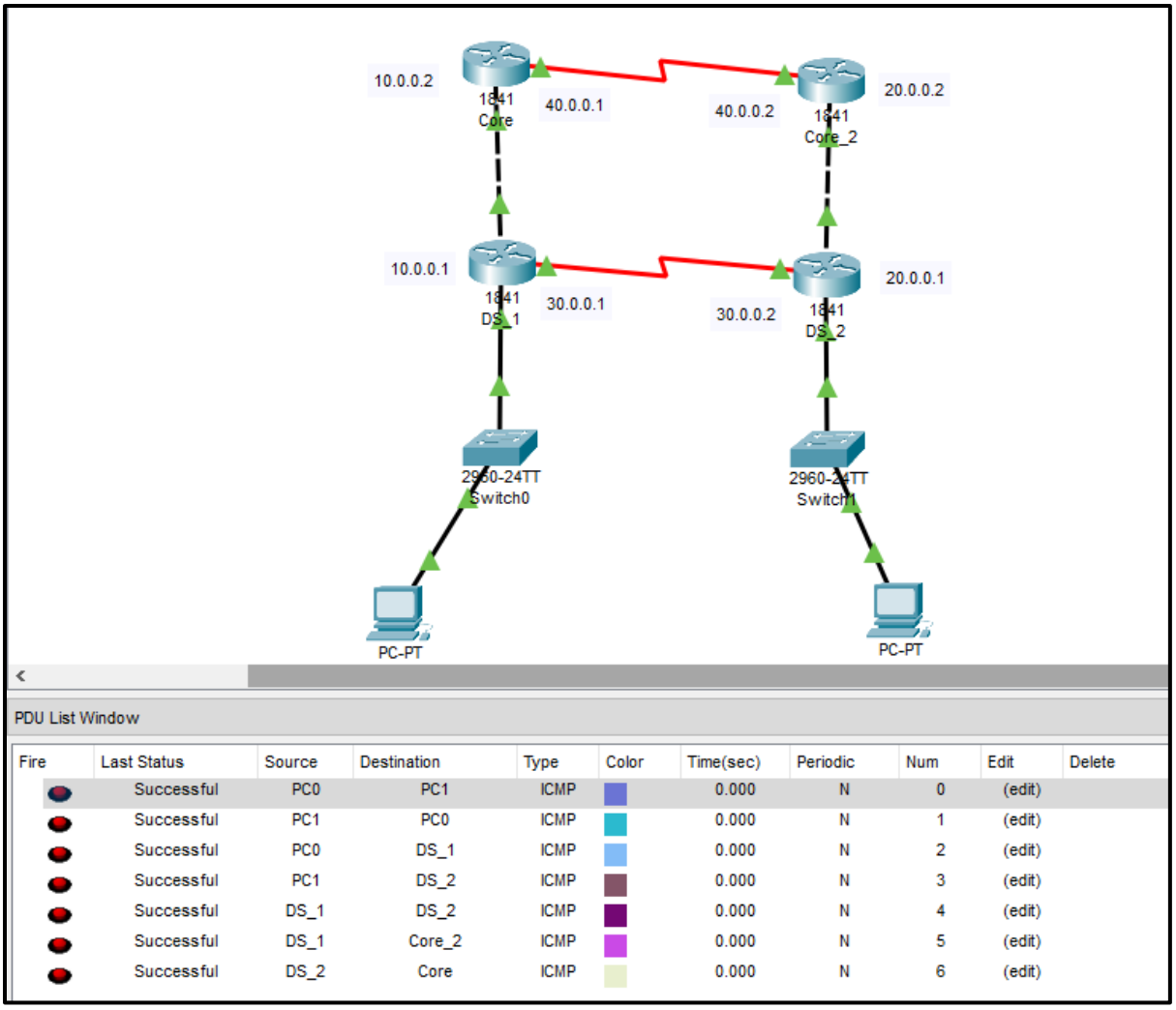





DS_1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
RIP Routing (v2)
Network
Add
Network Address
10.0.0.0
30.0.0.0
172.16.0.0
Remove


DS_2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
RIP Routing (v2)
Network
Add
Network Address
20.0.0.0
30.0.0.0
192.168.1.0
Remove

Checking connection:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	
	Successful	PC1	PC0	ICMP		0.000	N	1	(edit)	
	Successful	PC0	DS_1	ICMP		0.000	N	2	(edit)	
	Successful	PC1	DS_2	ICMP		0.000	N	3	(edit)	
	Successful	DS_1	DS_2	ICMP		0.000	N	4	(edit)	
	Successful	DS_1	Core_2	ICMP		0.000	N	5	(edit)	
	Successful	DS_2	Core	ICMP		0.000	N	6	(edit)	

Practical No: 03

Aim: Placing ACLs

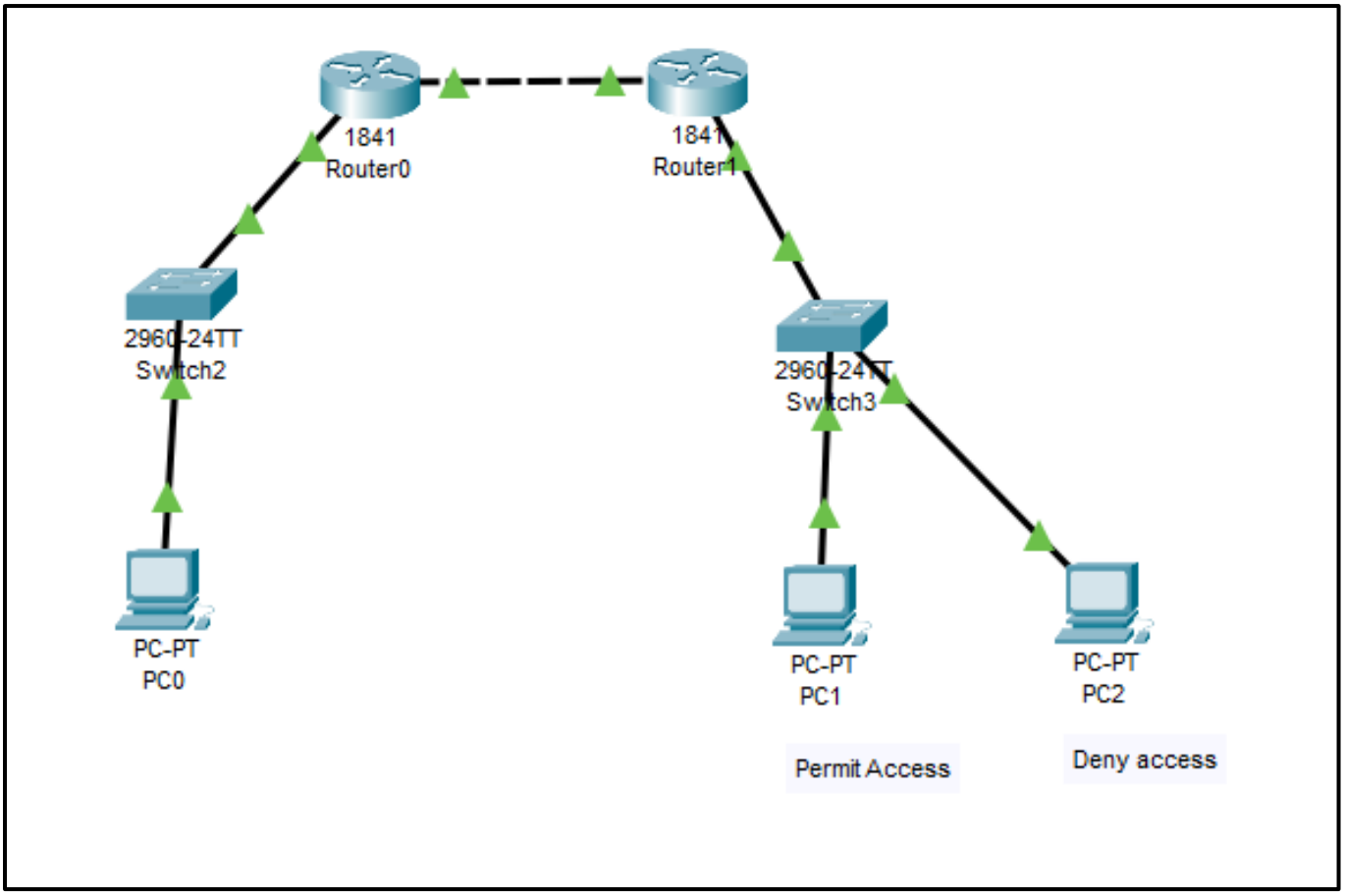
Components: Router, Switch, PC's

Theory: An access control list (ACL) contains rules that grant or deny access to certain digital environments. Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

There are two types of ACLs:

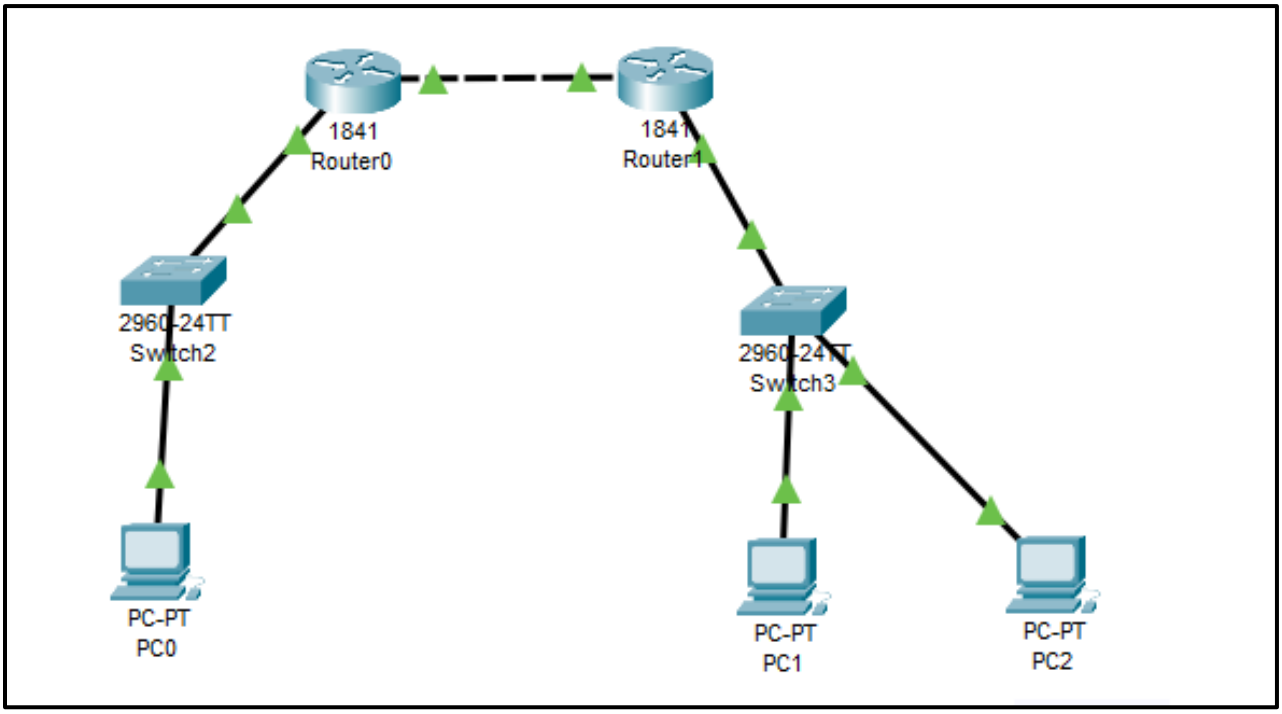
– **Standard ACLs:** These ACLs permit or deny packets based only on the source IPv4 address.

Cisco Packet Tracer Setup:-

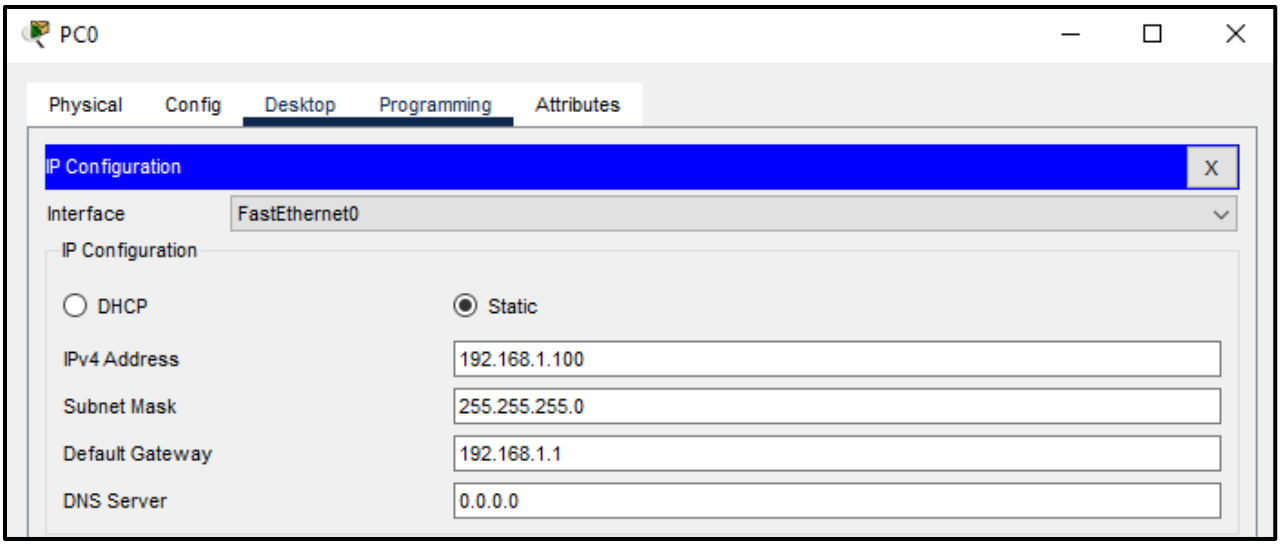


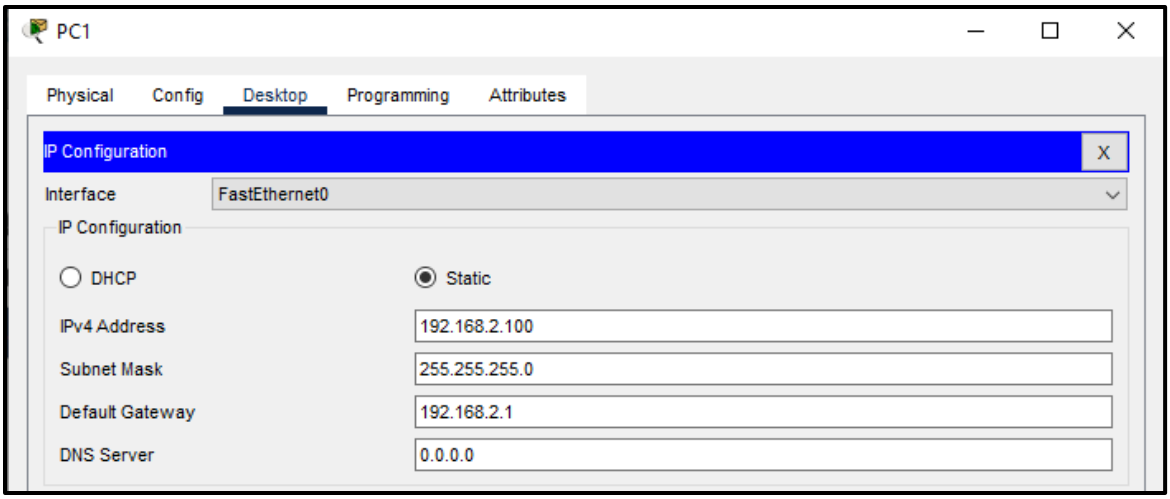
Implementation:

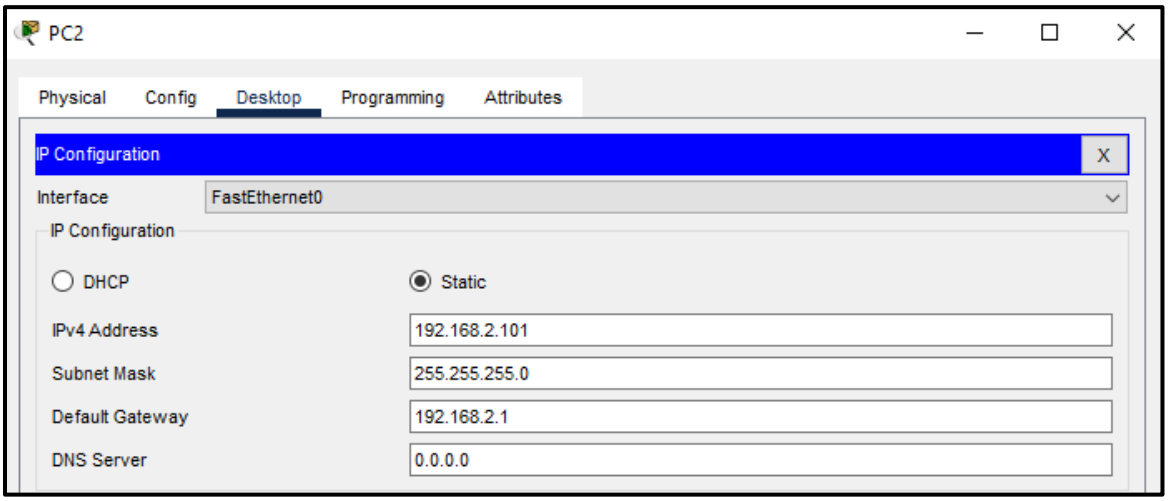
Step 1: Arranging devices and creating connections



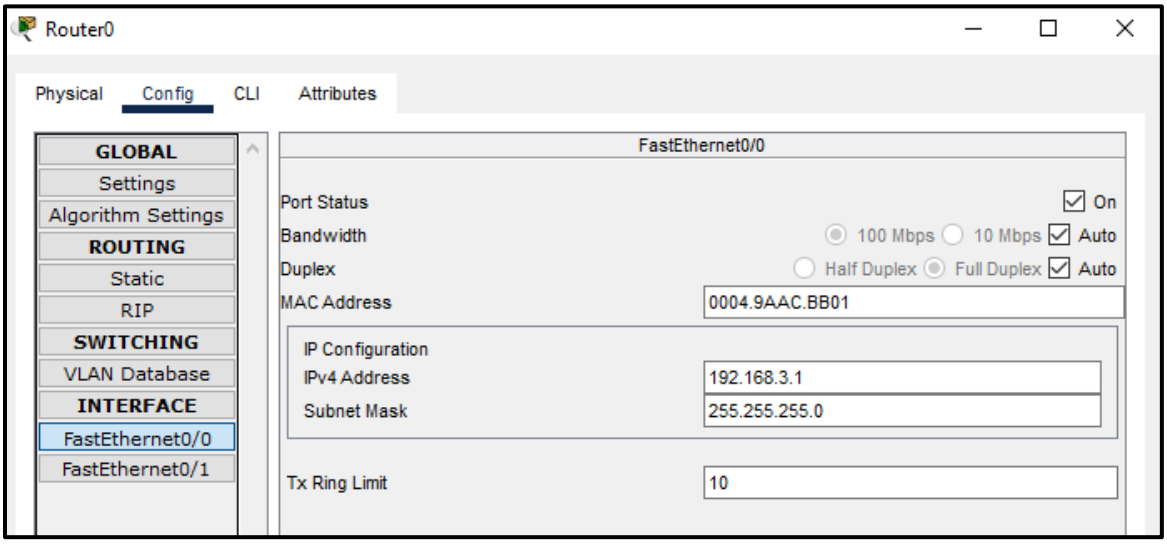
Step 2: Configuring all the PC's And Assigning IP Address

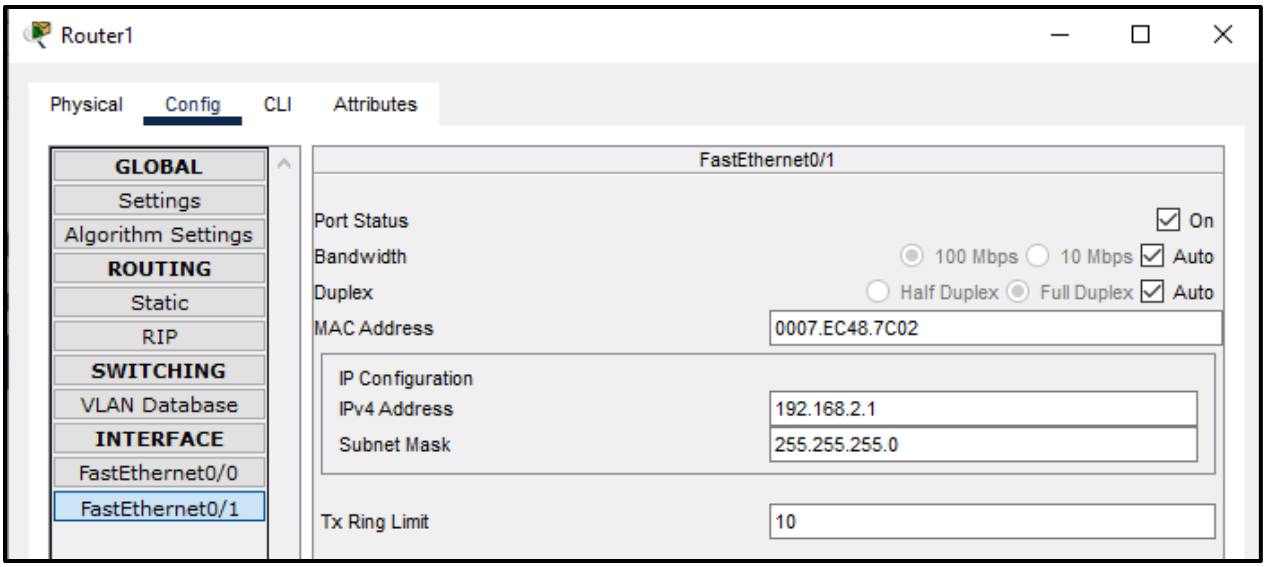




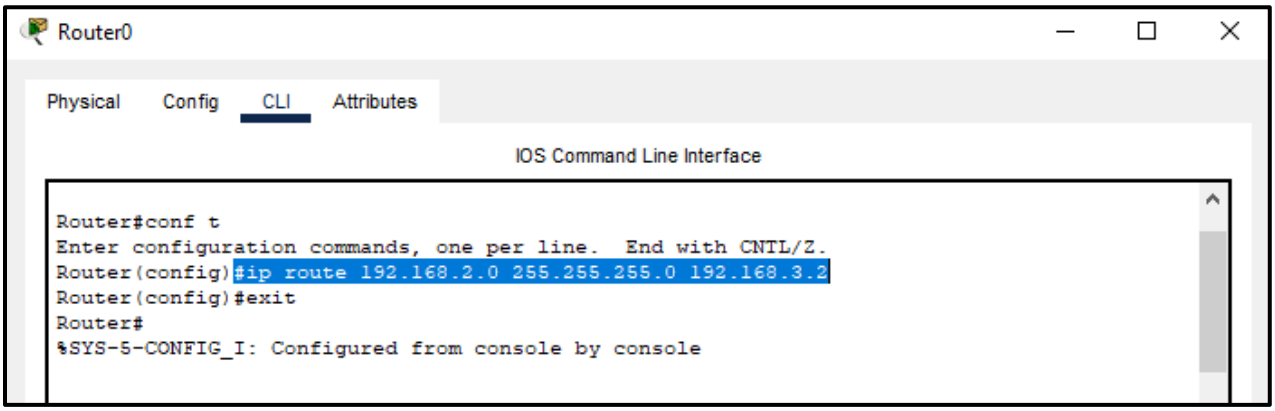


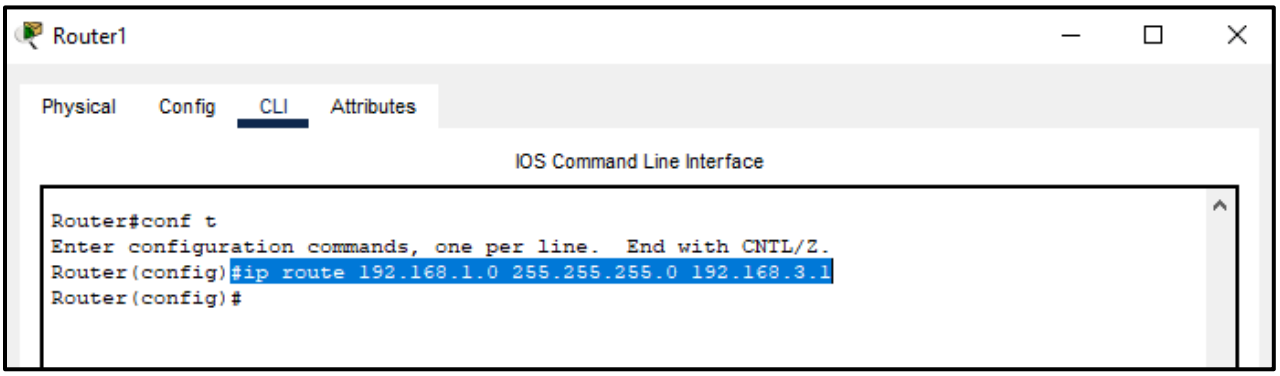
Step 3: Configure Routers and turn them on



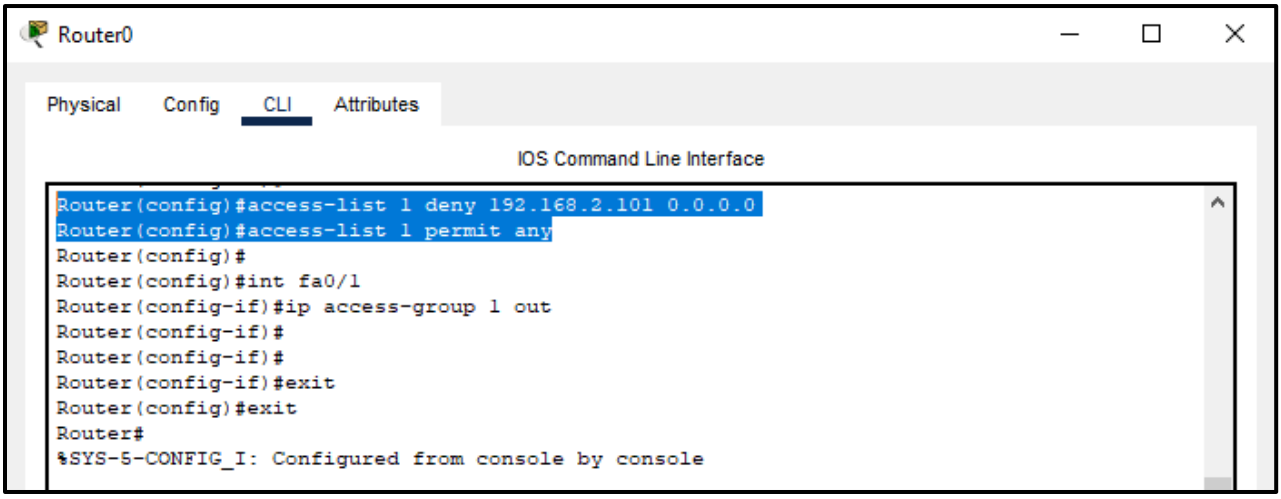


Step 4: Add static routes

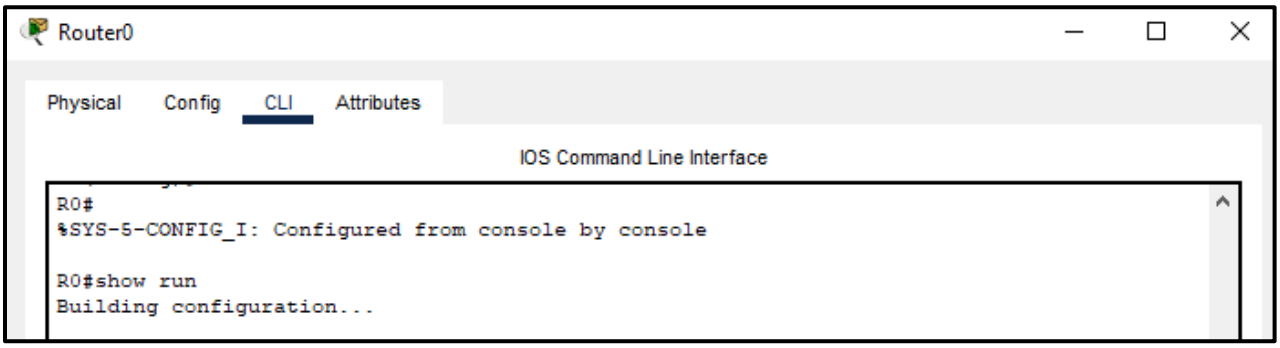




Step 5: Create **Standard ACL**



Check the ACL using show run command



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.3.2
!
ip flow-export version 9
!
!
access-list 1 deny host 192.168.2.101
access-list 1 permit any
!
!
!
!
!
!
line con 0
```

```
R0>en
R0#show access-list
Standard IP access list 1
    10 deny host 192.168.2.101 (12 match(es))
    20 permit any (4 match(es))

R0#
```

Step 6: Apply the access list to the interface

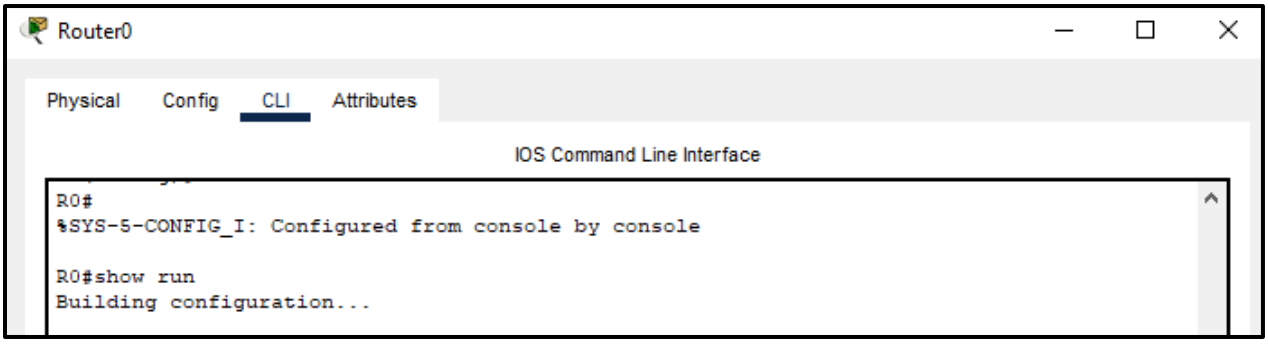
Router0

Physical Config CLI Attributes

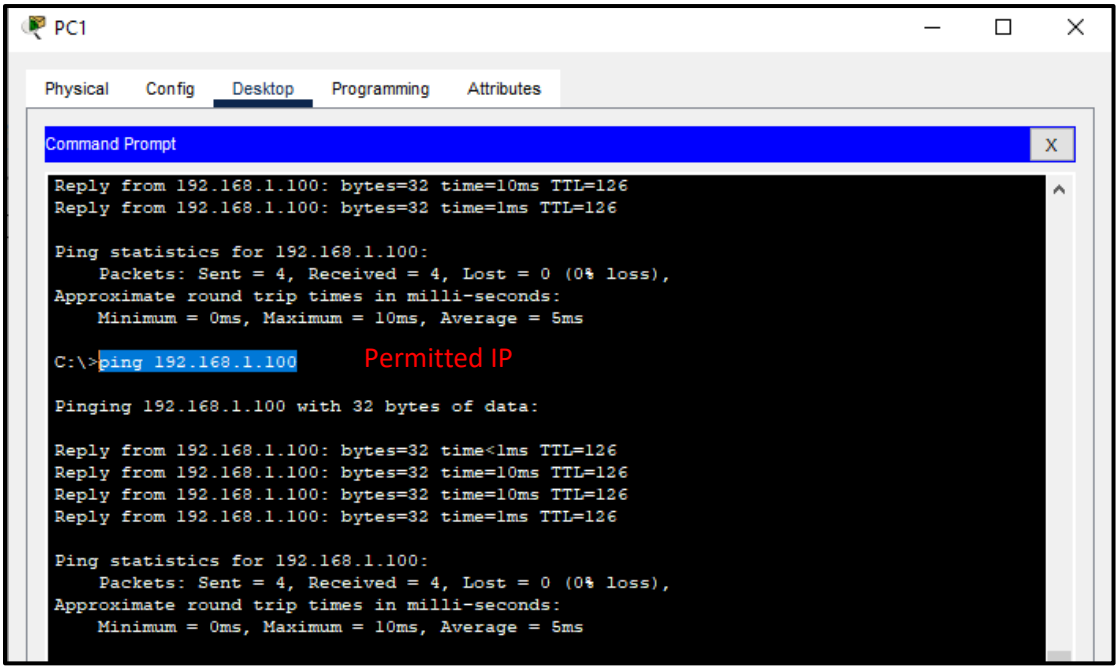
IOS Command Line Interface

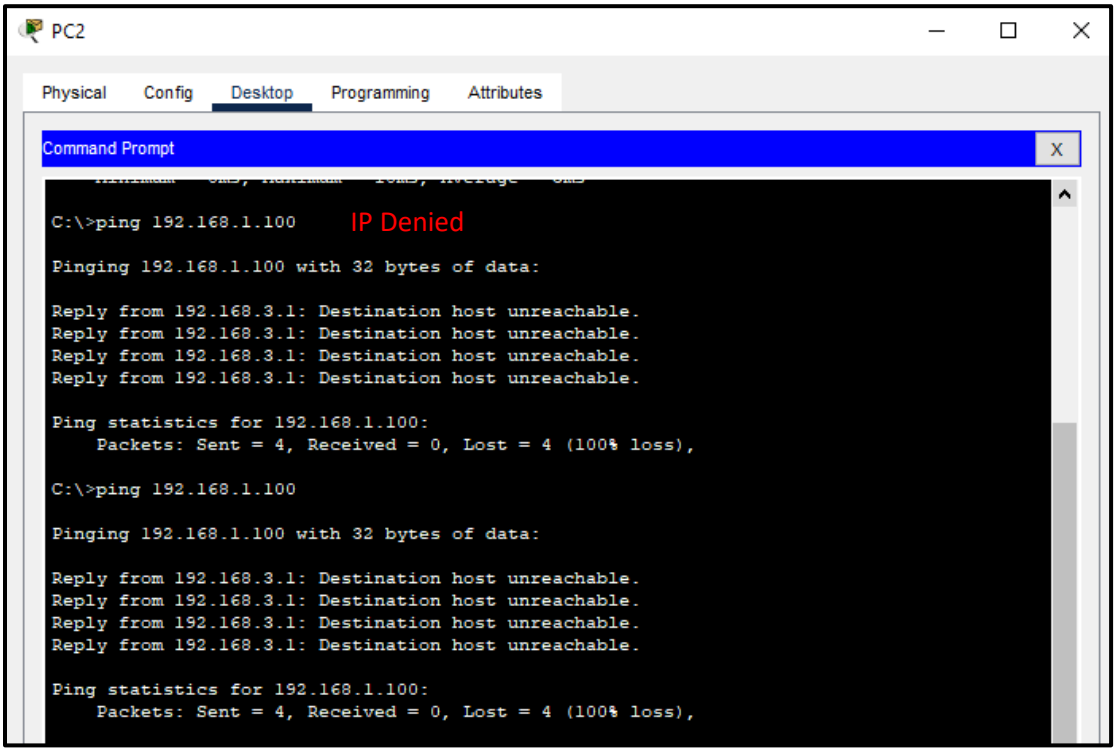
```
Router(config)#
Router(config)#int fa0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Check using show run command



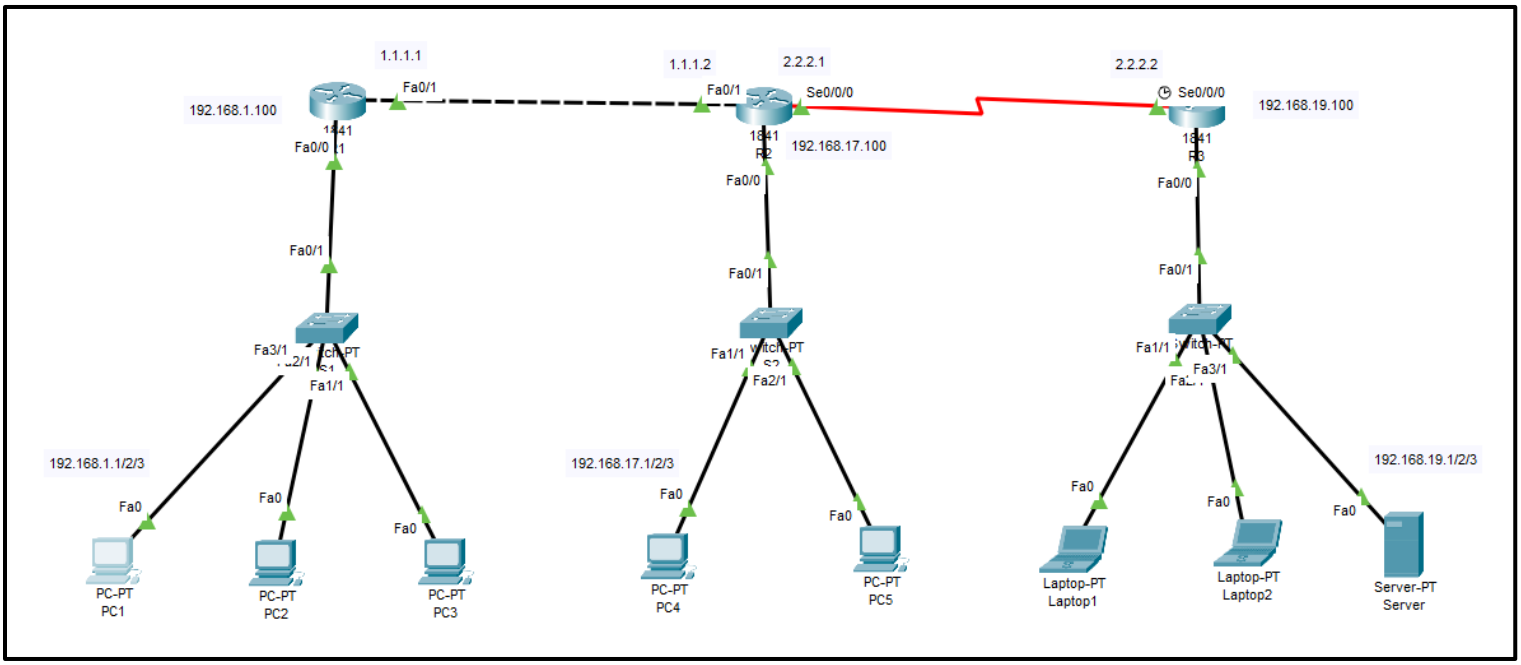
Step 7: Check the connection



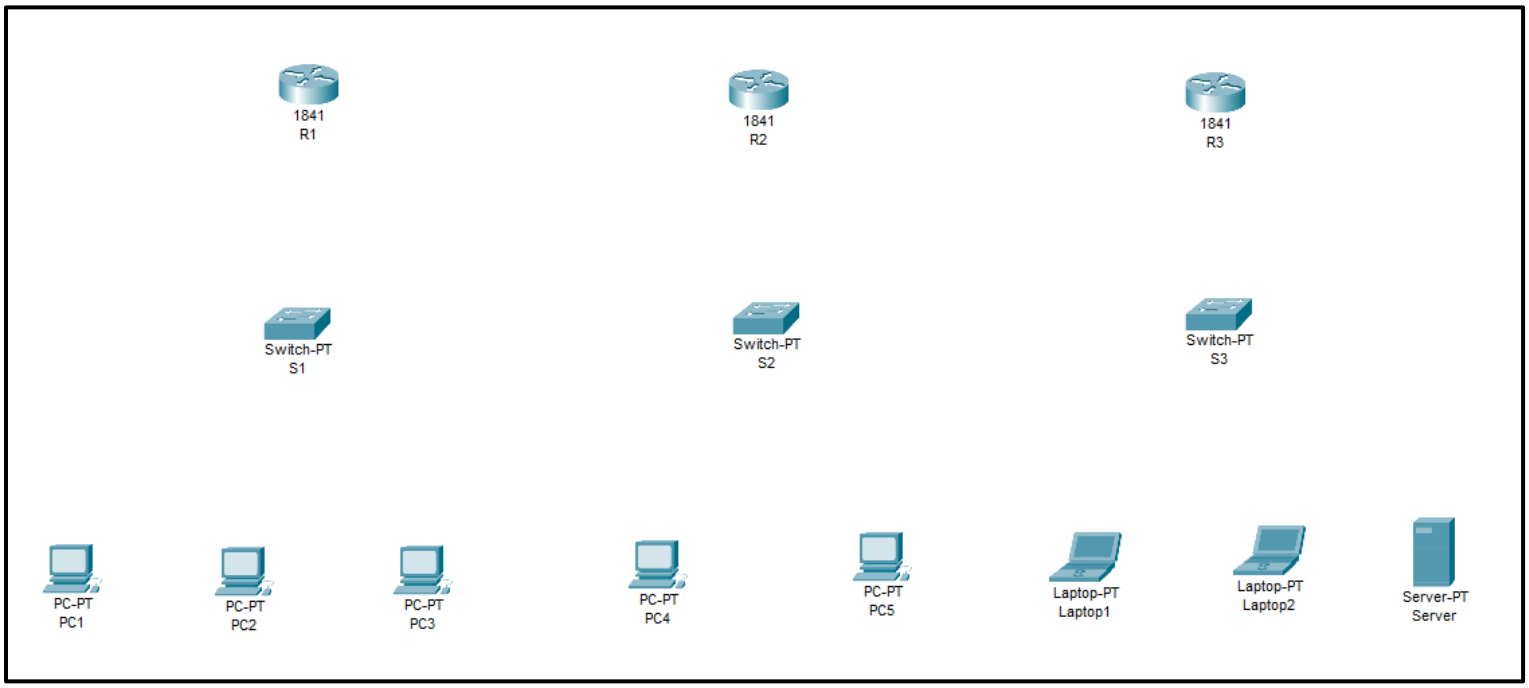


– **Extended ACLs:** These ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more.

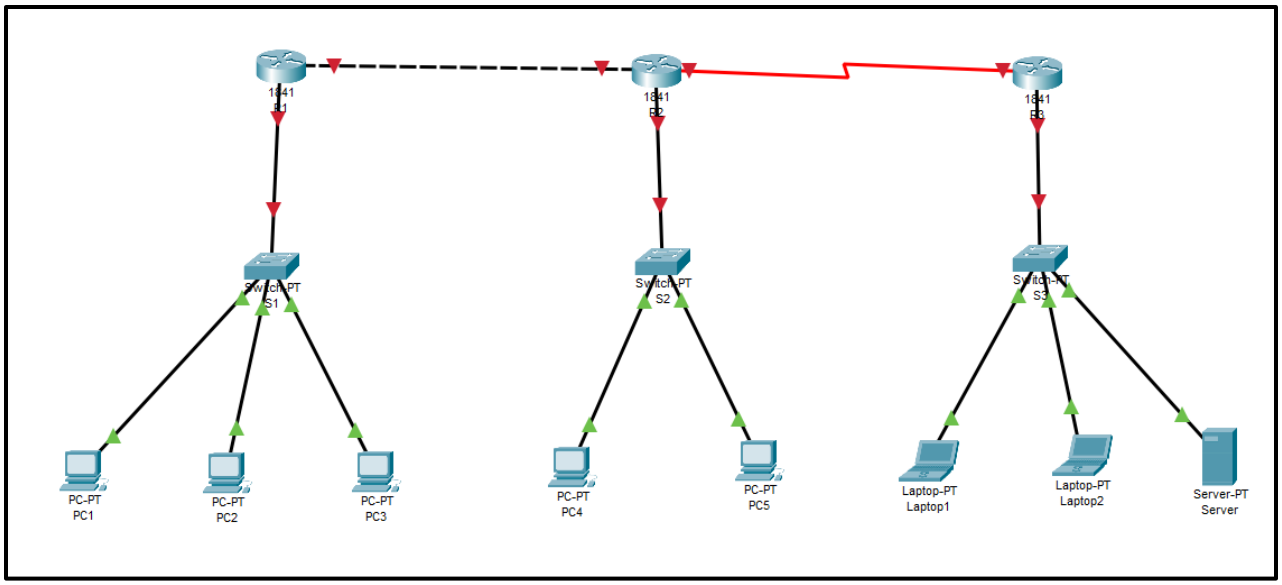
Cisco Packet tracer Setup:



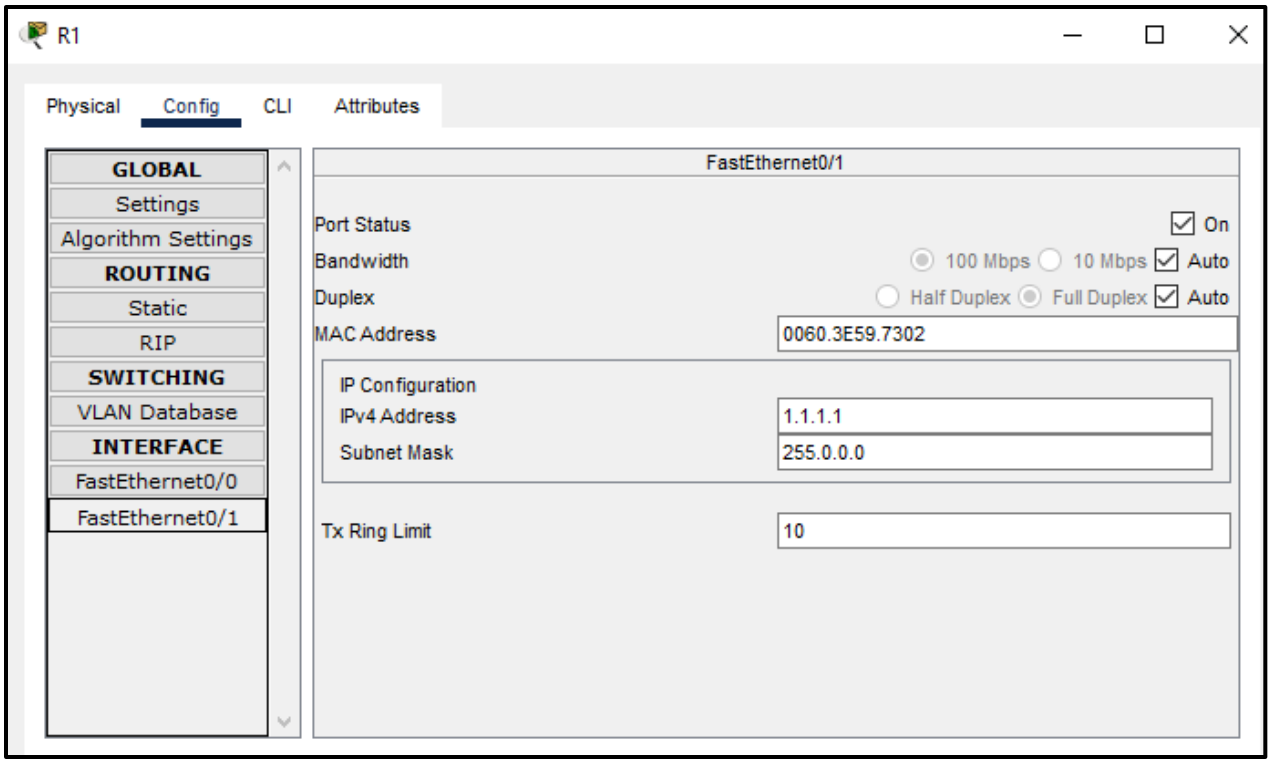
Step 1: Arranging devices

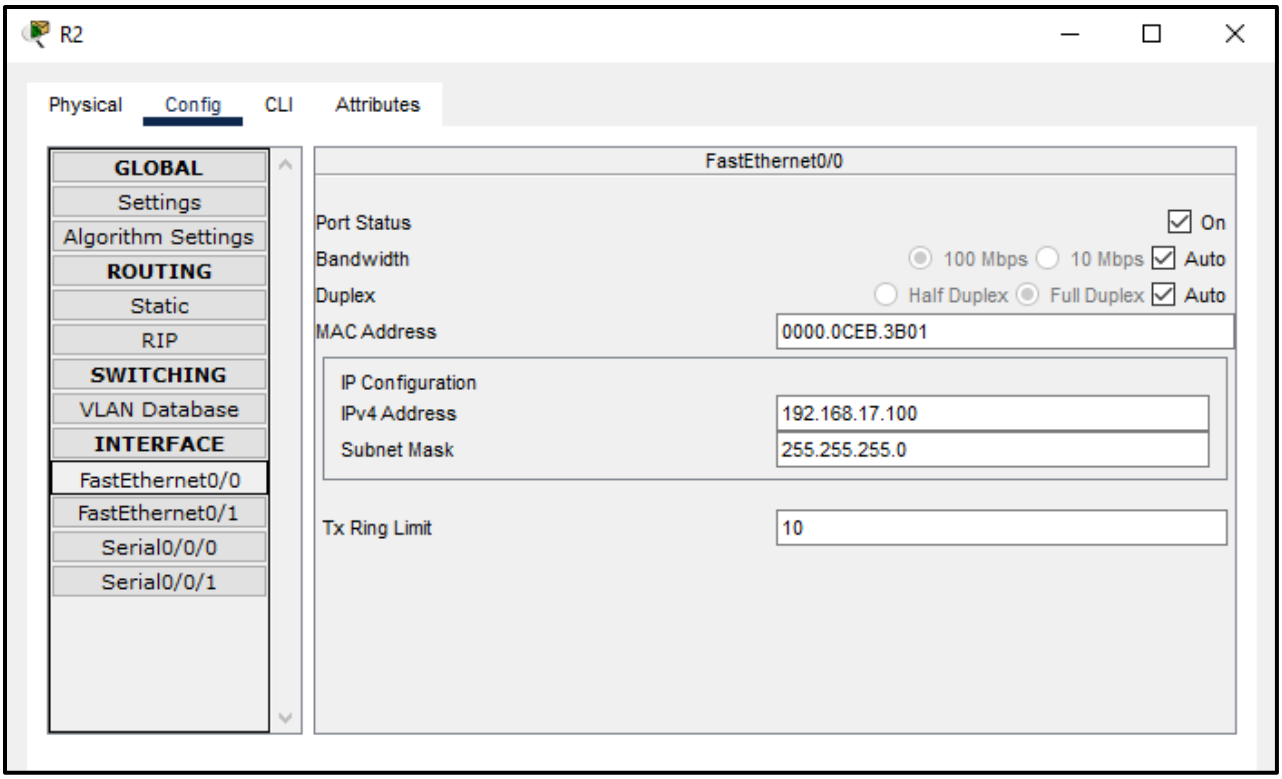


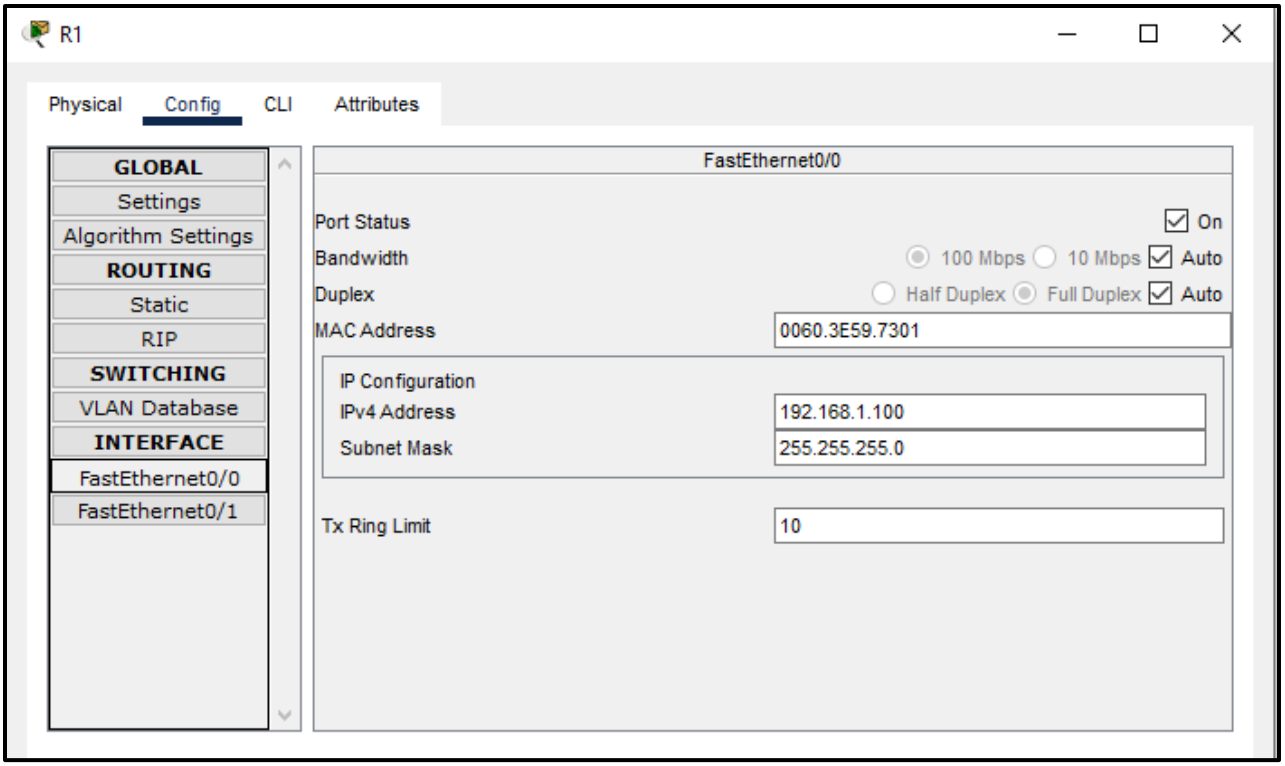
Step 2: Creating connection with respective cable.

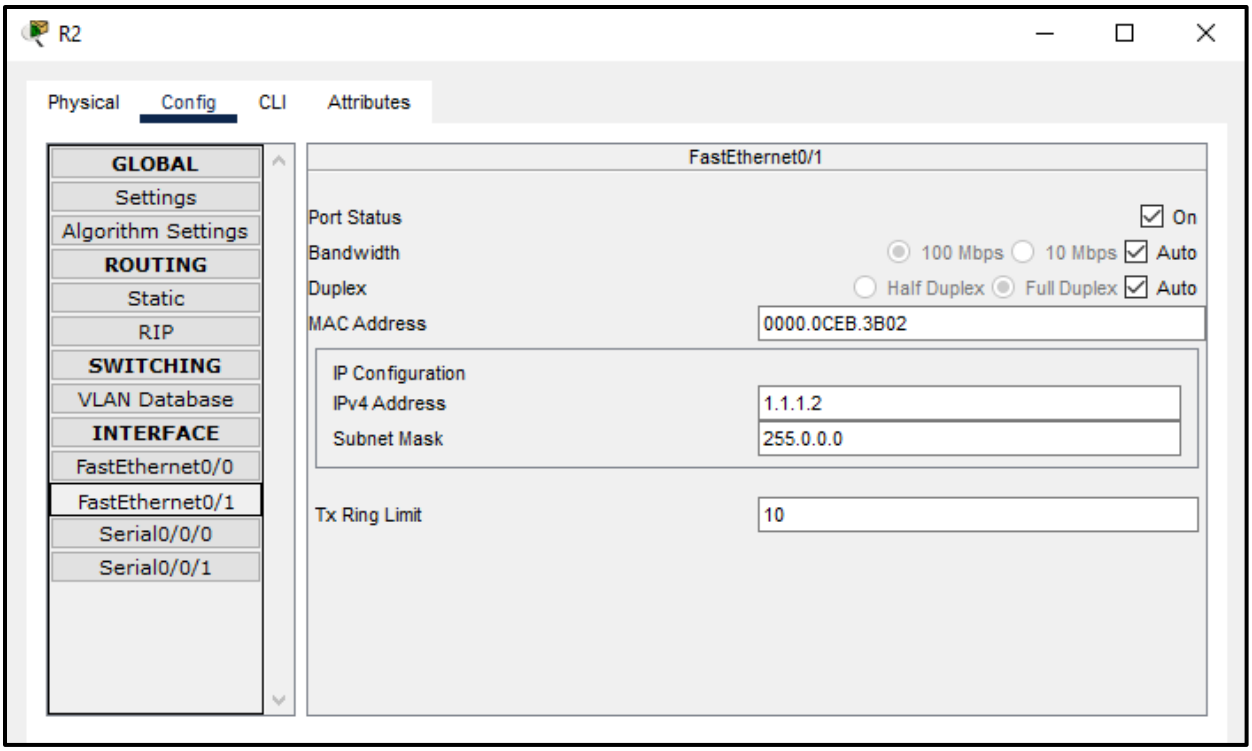


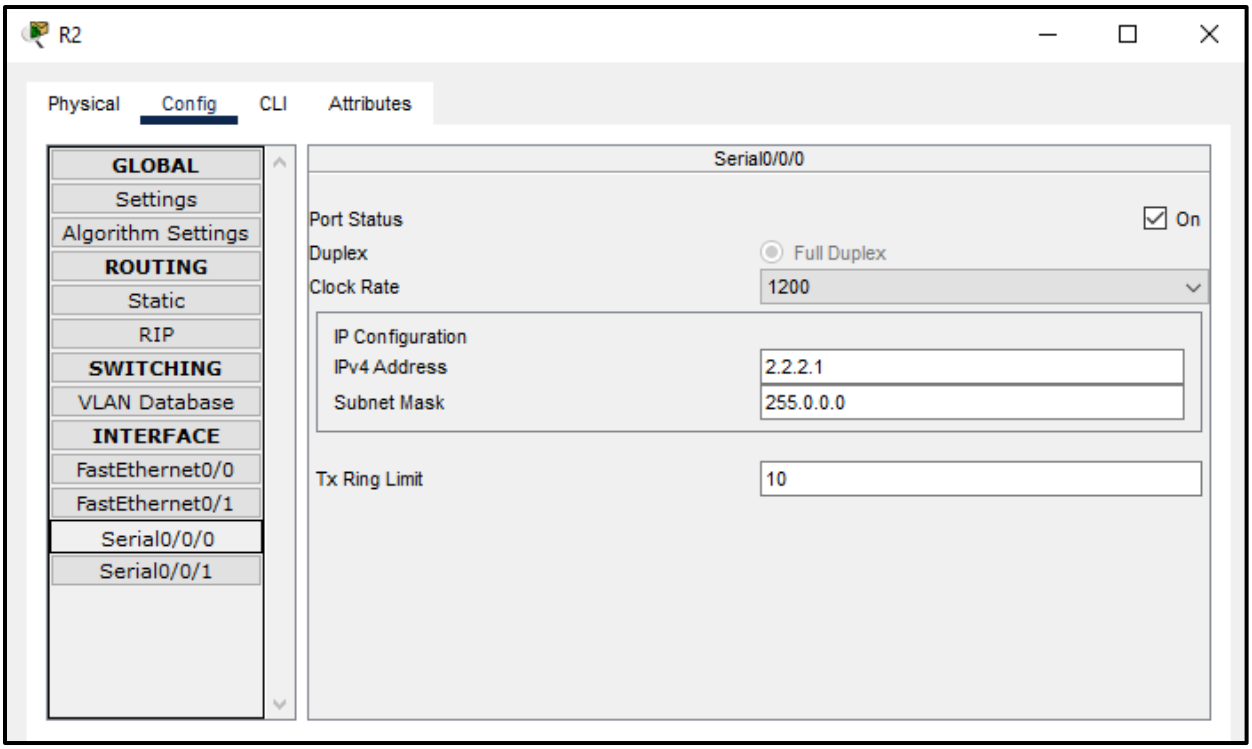
Step 3: Configure all devices and give them IP address. (We can use DHCP also I done by giving IP address manually)

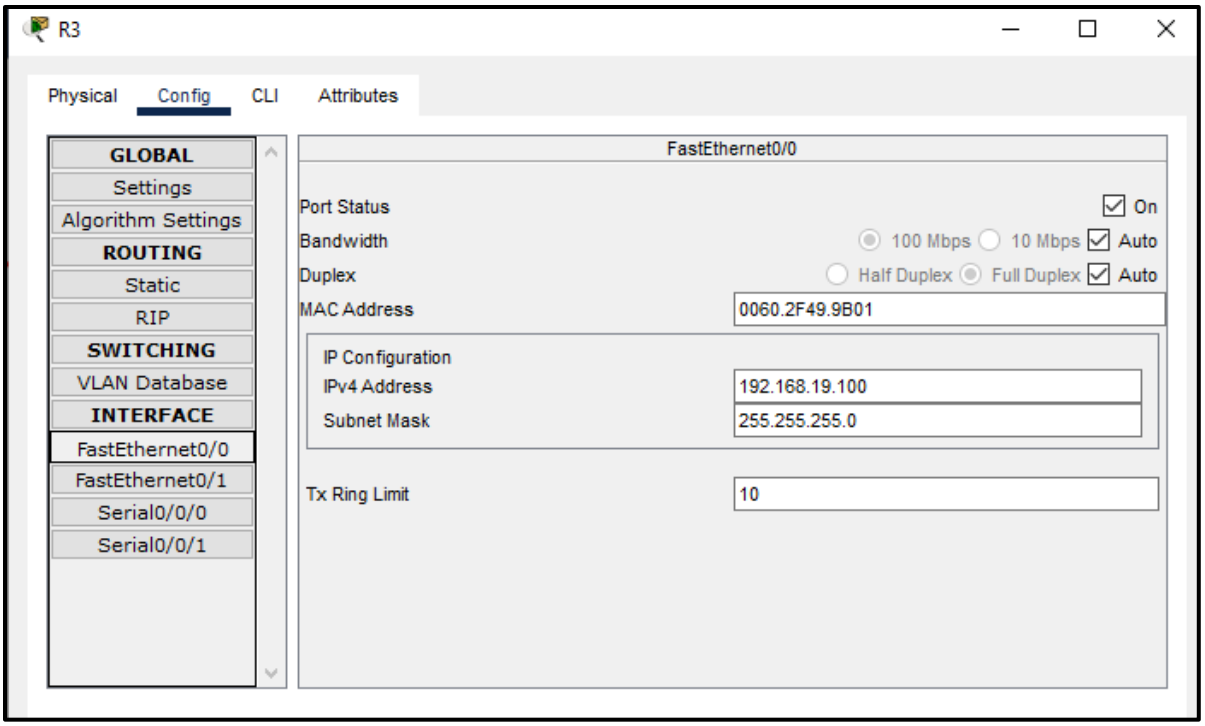


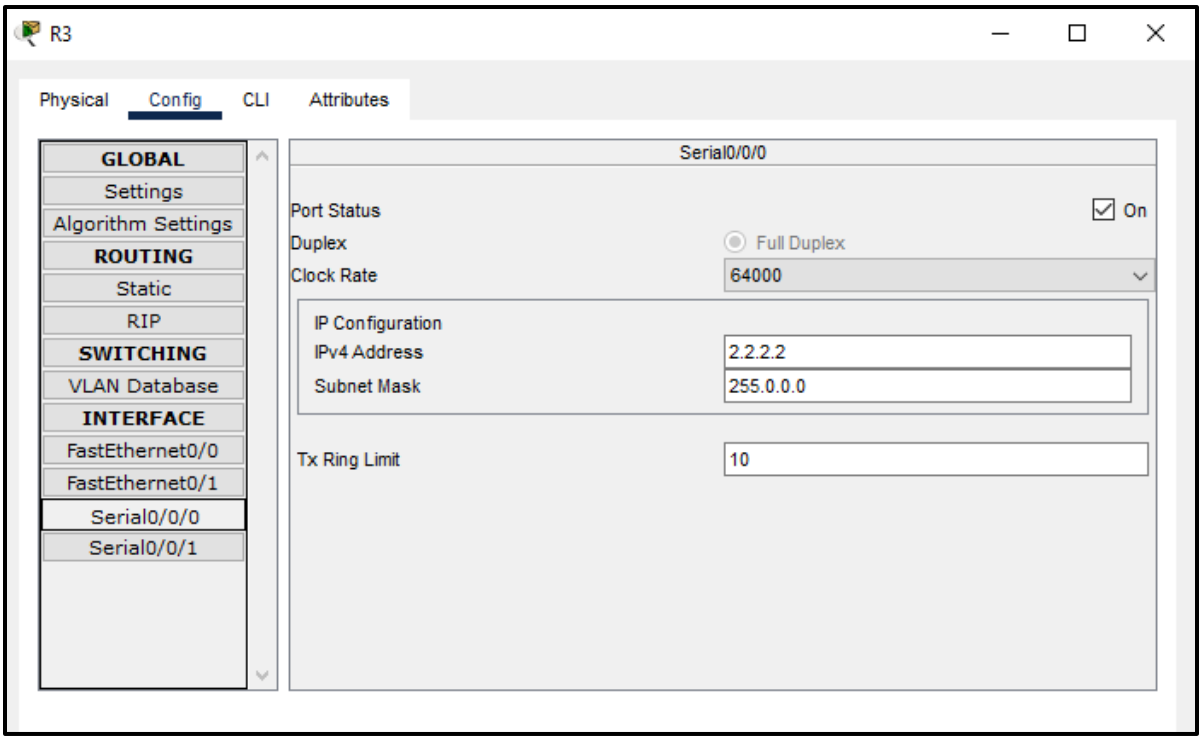

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0000.0CEB.3B01
IP Configuration
IPv4 Address
192.168.17.100
Subnet Mask
255.255.255.0
Tx Ring Limit
10

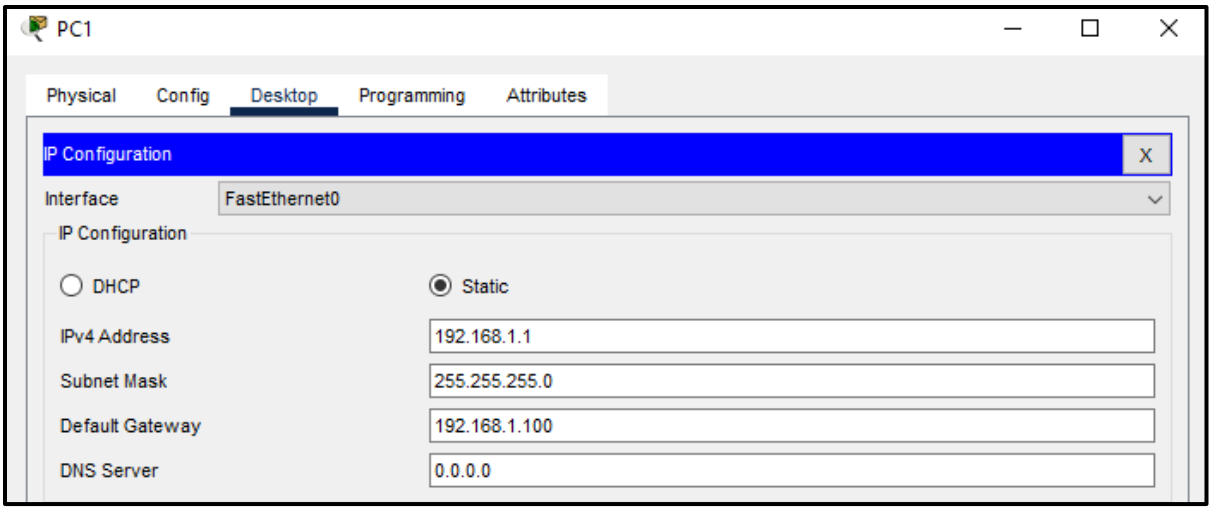

R1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.3E59.7301
IP Configuration
IPv4 Address
192.168.1.100
Subnet Mask
255.255.255.0
Tx Ring Limit
10

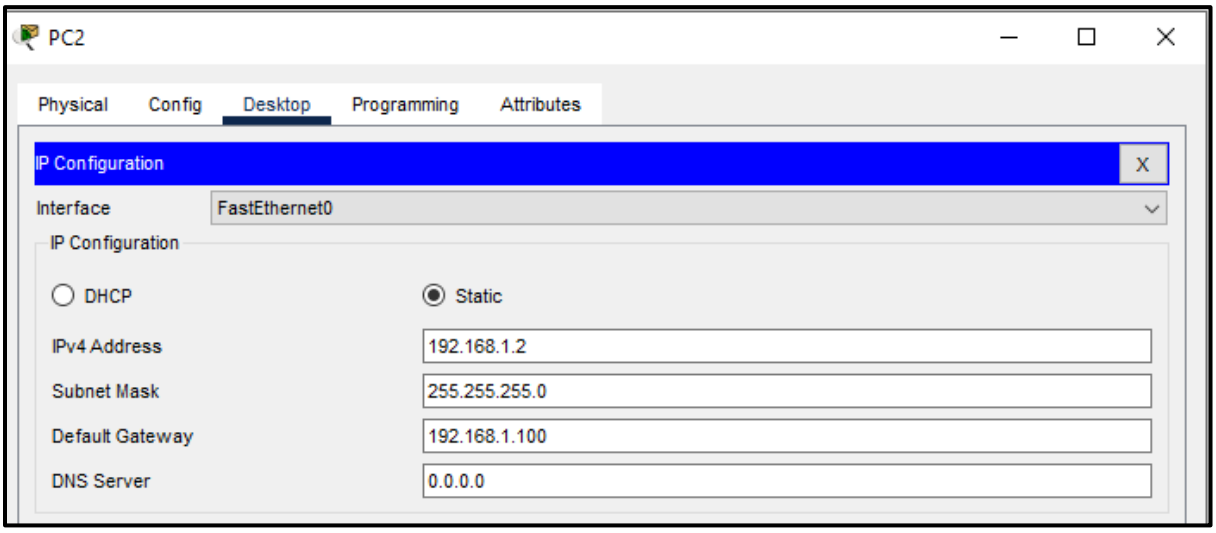

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0000.0CEB.3B02
IP Configuration
IPv4 Address
1.1.1.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

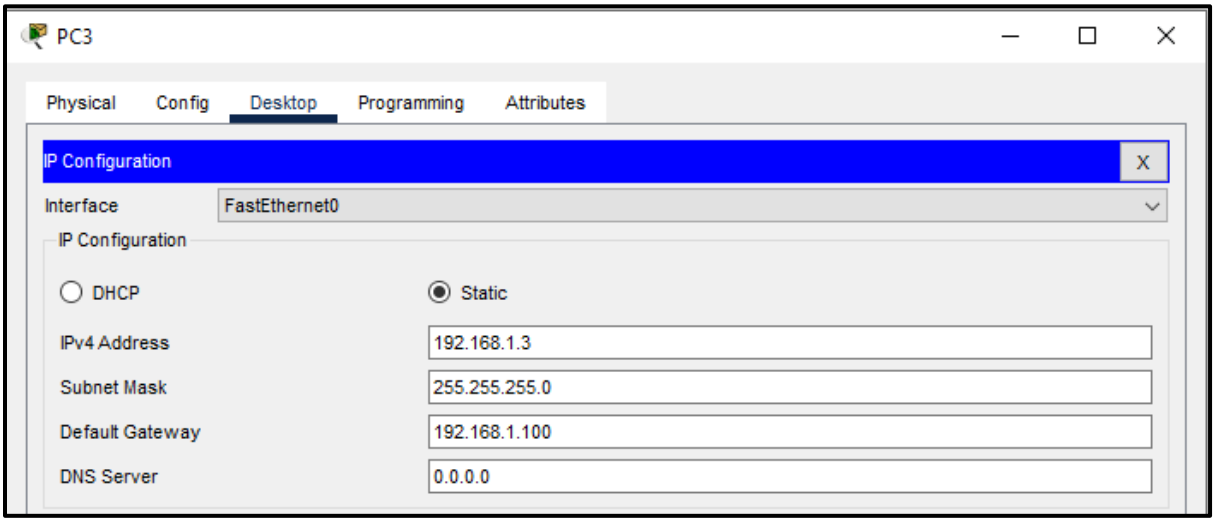

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
2.2.2.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

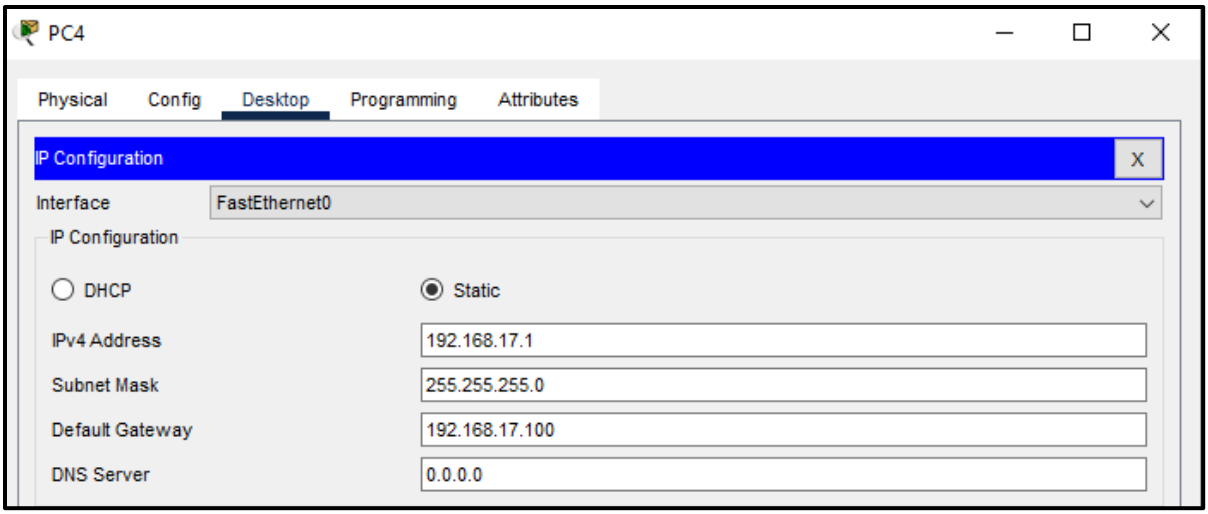

R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.2F49.9B01
IP Configuration
IPv4 Address
192.168.19.100
Subnet Mask
255.255.255.0
Tx Ring Limit
10

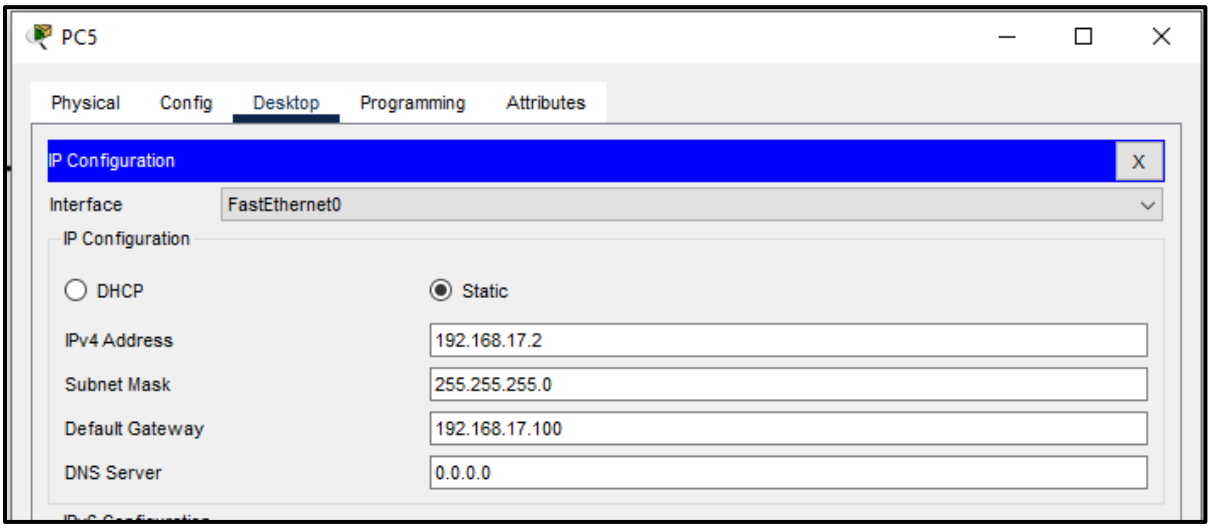

R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
64000
IP Configuration
IPv4 Address
2.2.2.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

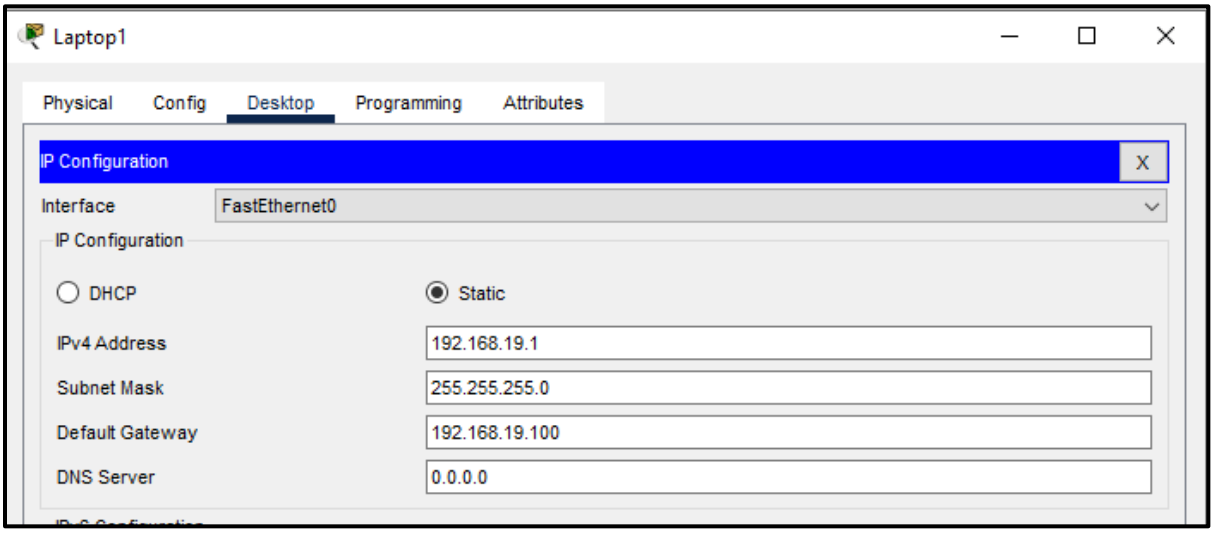

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.100
DNS Server
0.0.0.0

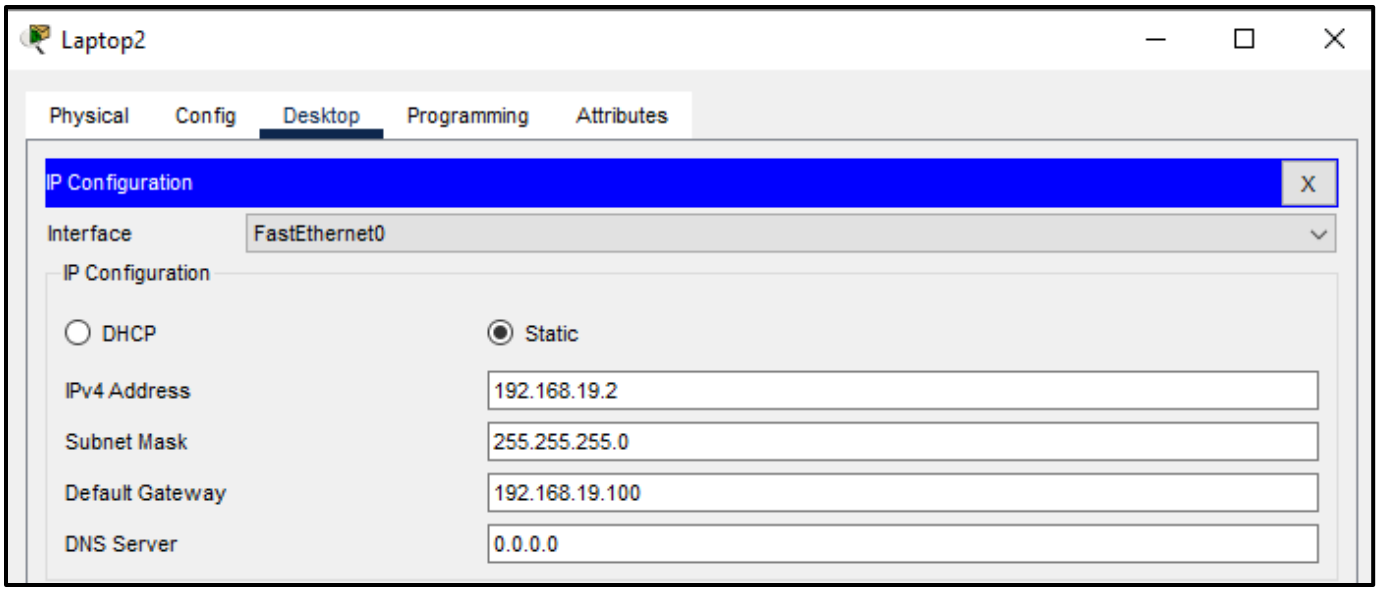

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.100
DNS Server
0.0.0.0

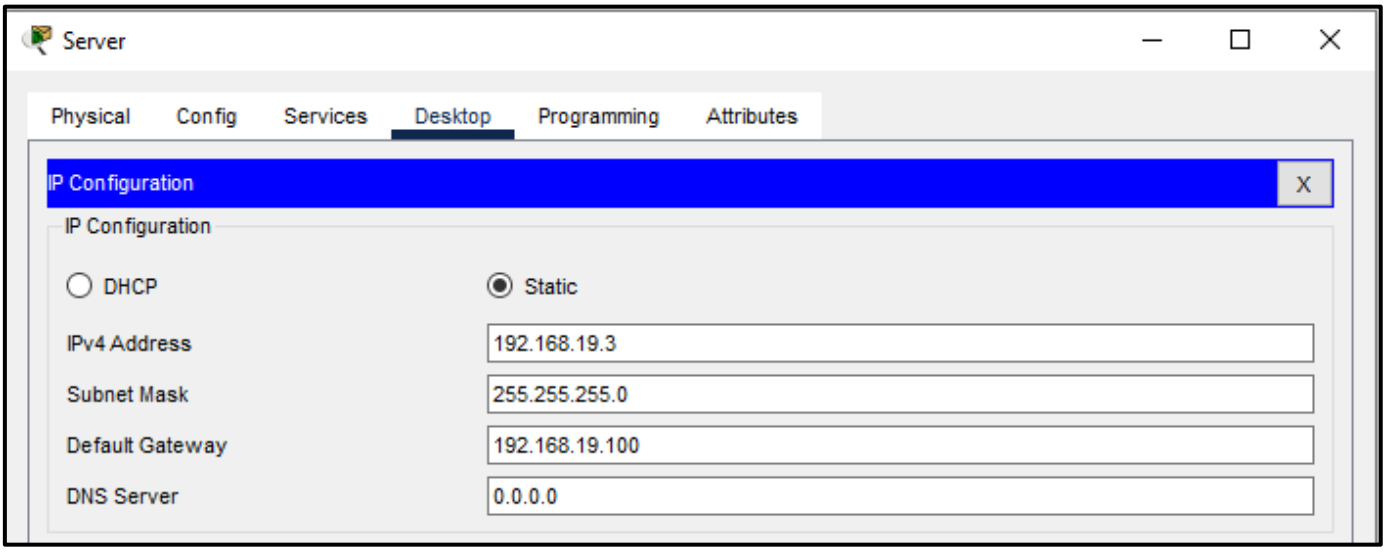

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.100
DNS Server
0.0.0.0


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.17.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.17.100
DNS Server
0.0.0.0

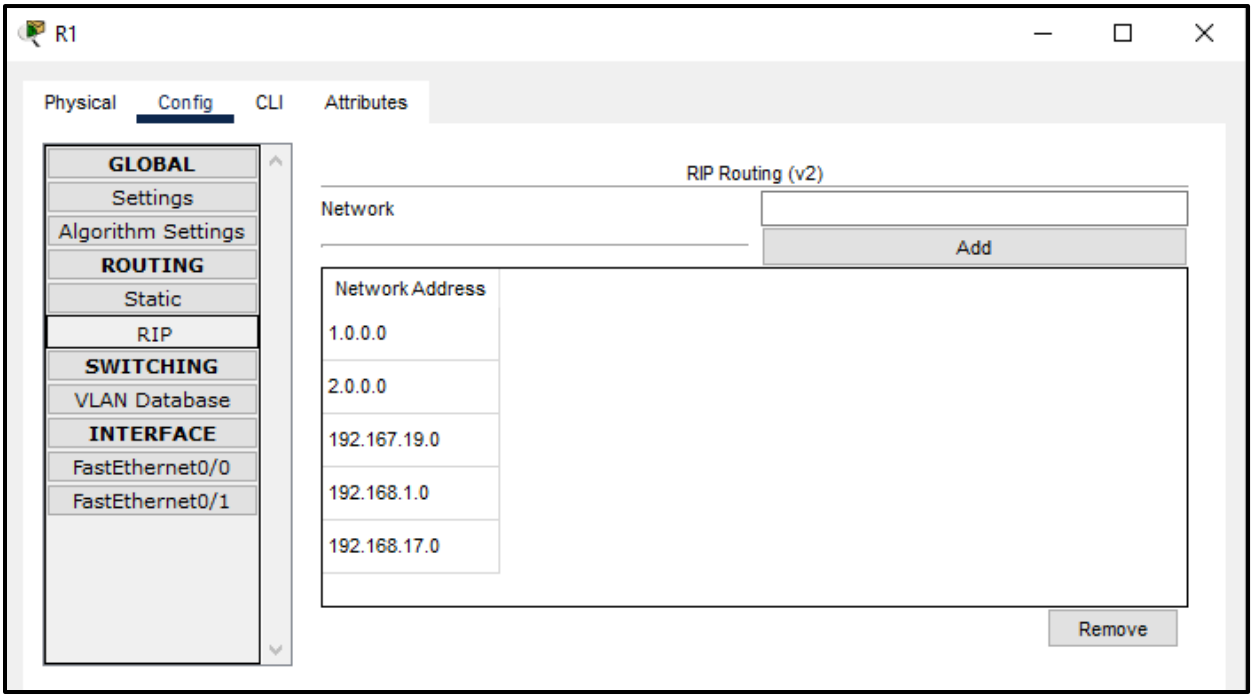

PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.17.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.17.100
DNS Server
0.0.0.0

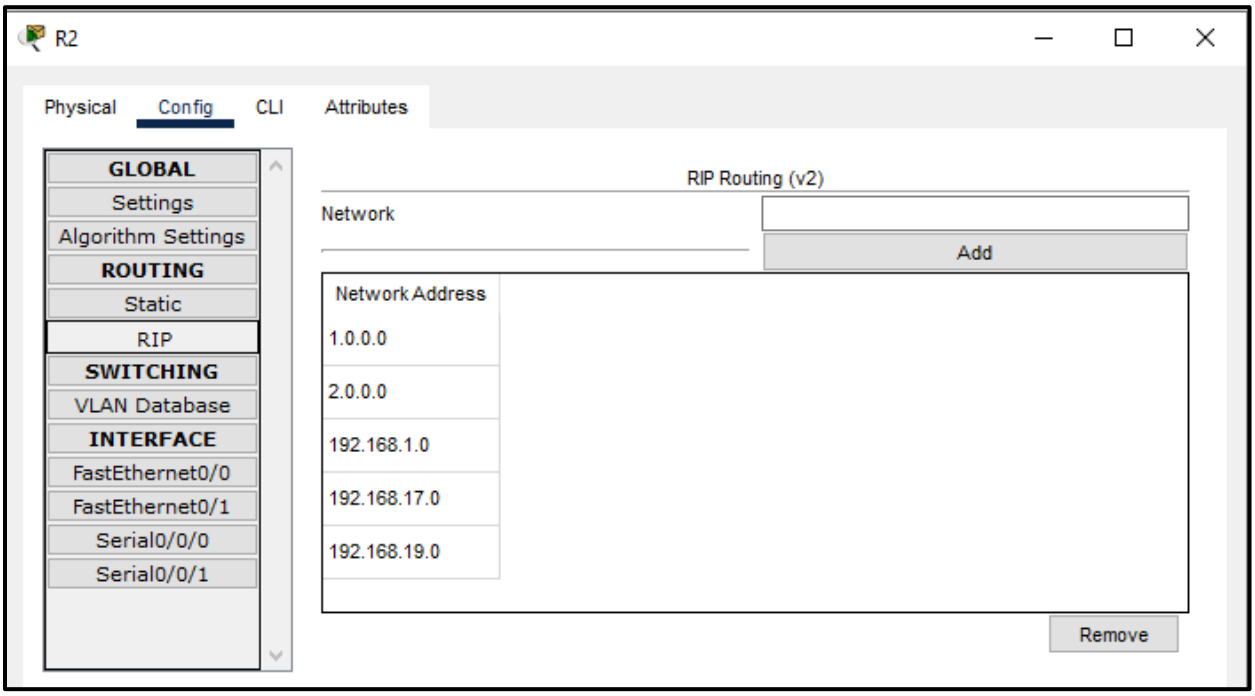

Laptop1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.19.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.19.100
DNS Server
0.0.0.0

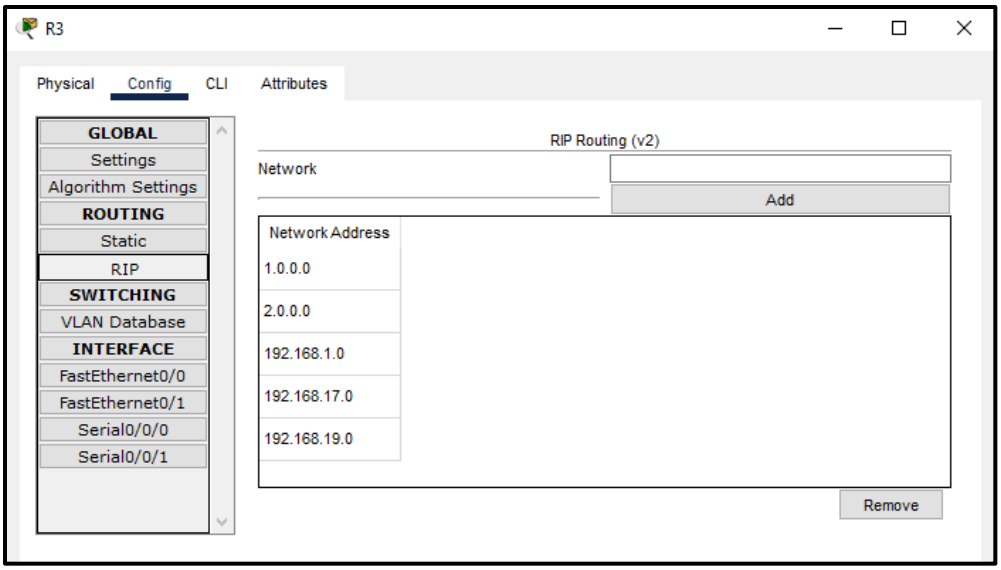

Laptop2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.19.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.19.100
DNS Server
0.0.0.0


Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.19.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.19.100
DNS Server
0.0.0.0

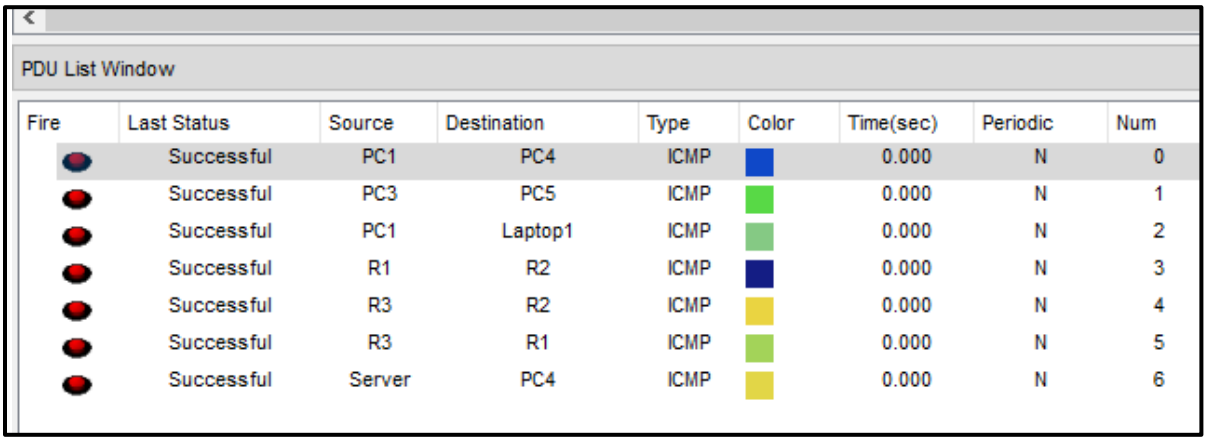
Step 4: Setup the any routing protocol (I used RIP version2 here)







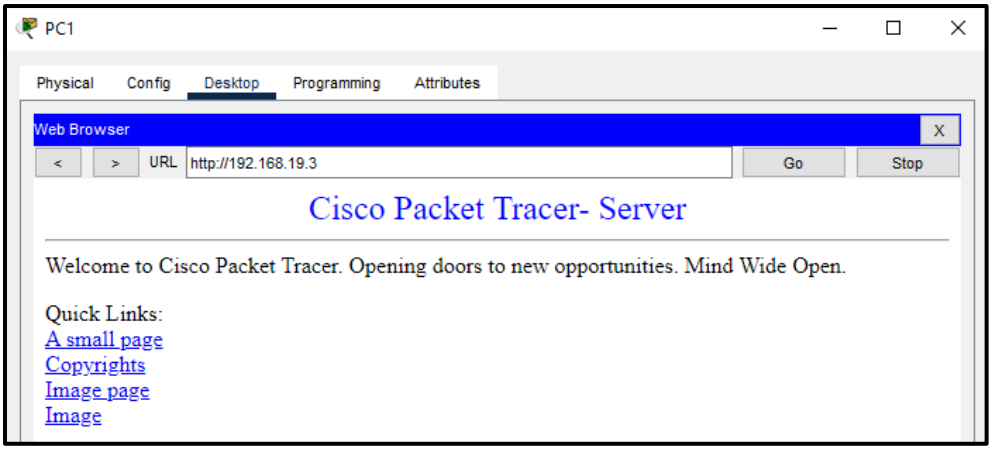
Check the connection:

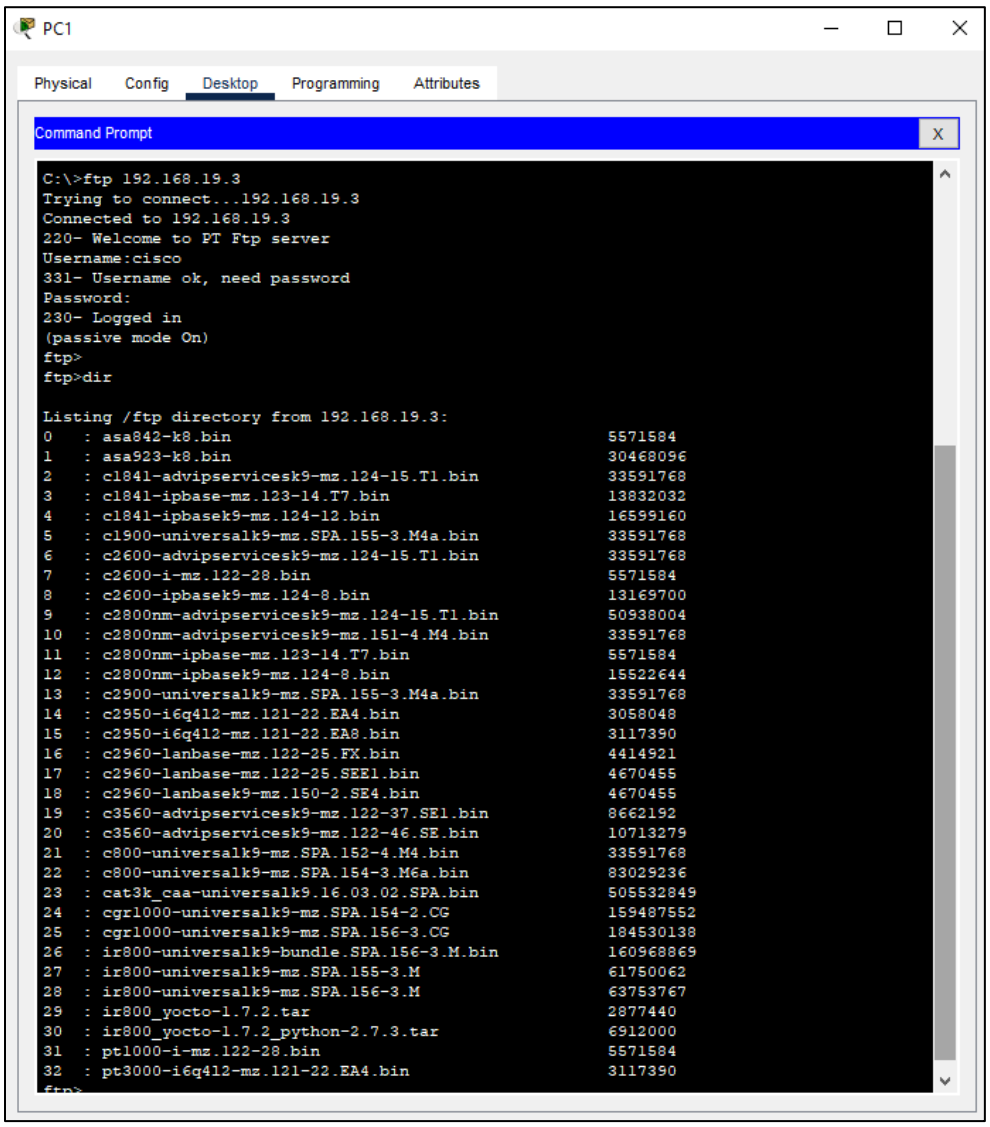


PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC1	PC4	ICMP		0.000	N	0
	Successful	PC3	PC5	ICMP		0.000	N	1
	Successful	PC1	Laptop1	ICMP		0.000	N	2
	Successful	R1	R2	ICMP		0.000	N	3
	Successful	R3	R2	ICMP		0.000	N	4
	Successful	R3	R1	ICMP		0.000	N	5
	Successful	Server	PC4	ICMP		0.000	N	6

(Accessing server by pc1)





Step 5: Implementing extended ACL by blocking follow services to respective machines

192.168.1.1 > webbroser

192.168.17.1 > FTP

192.168.1.5 > ICMP

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
```

```
R2(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

```
R2(config)#access-list 100 deny tcp host 192.168.1.1 host 192.168.19.3 eq www
R2(config)#access-list 100 deny tcp host 192.168.1.1 host 192.168.19.3 eq 80
R2(config)#access-list 100 deny tcp host 192.168.17.1 host 192.168.19.3 eq ftp
R2(config)#access-list 100 deny icmp host 192.168.1.2 host 192.168.19.3
R2(config)#access-list 100 permit ip any any
R2(config)#
R2(config)#
R2(config)#int se0/0/0
R2(config-if)#ip access-group 100 out
R2(config-if)#exit
R2(config)#exit
R2#
```

```
R2#show access-lists
Extended IP access list 100
    10 deny tcp host 192.168.1.1 host 192.168.19.3 eq www
    20 deny tcp host 192.168.17.1 host 192.168.19.3 eq ftp
    30 deny icmp host 192.168.1.2 host 192.168.19.3
    40 permit ip any any

R2#
```

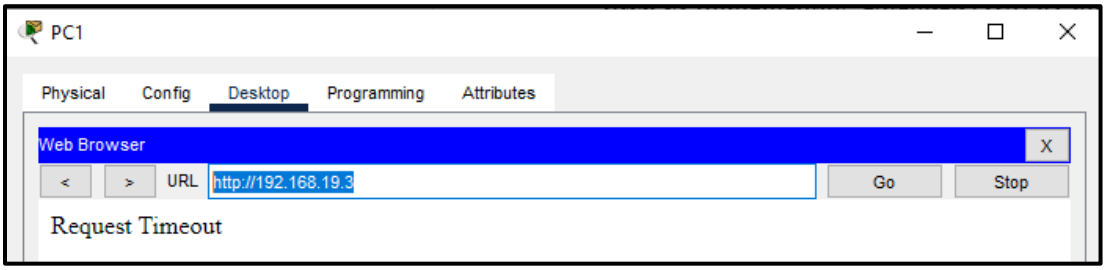
Ctrl+F6 to exit CLI focus

Copy Paste

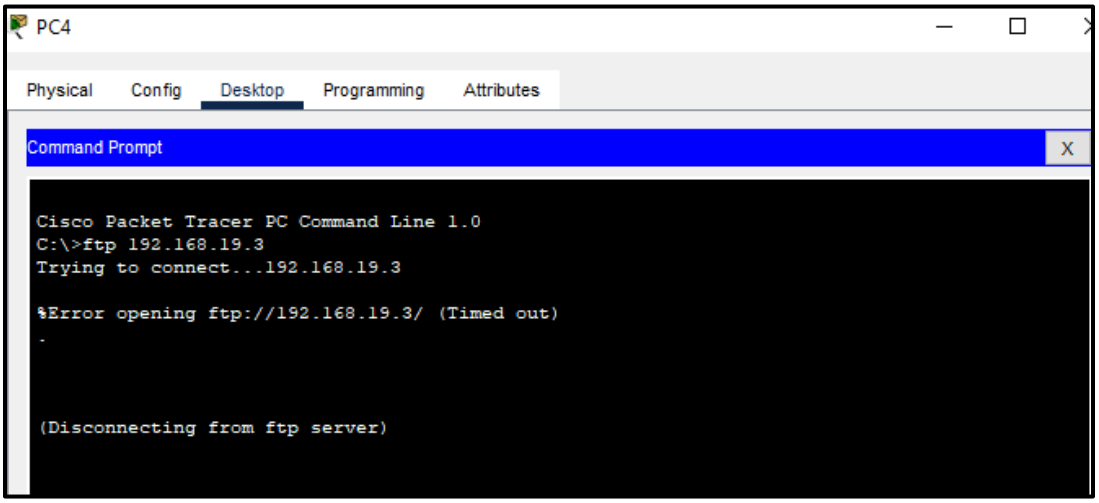
Top

Step 6: Check the blocked IPs and their Blocked Services

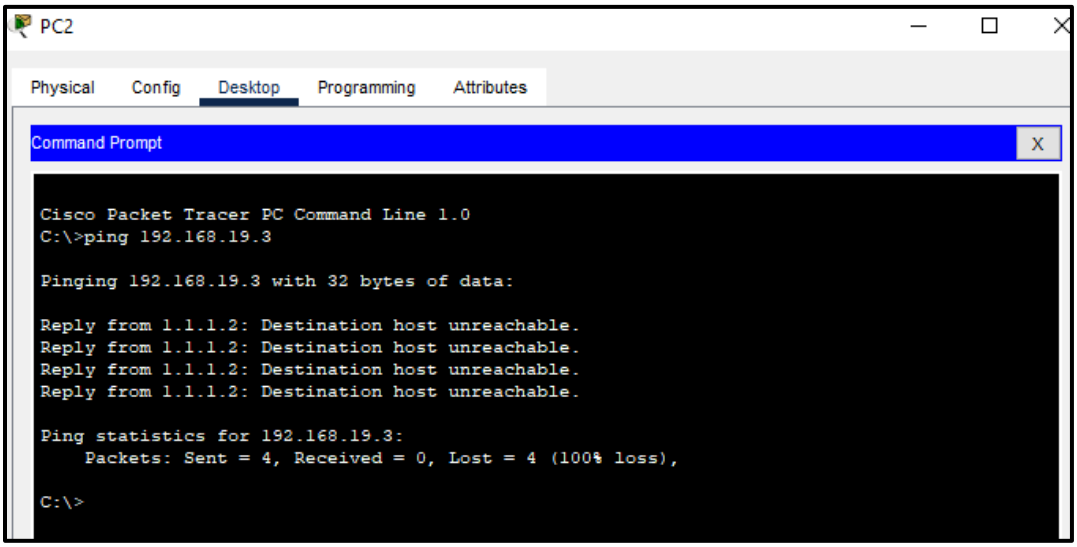
192.168.1.1 > webbroser



192.168.17.1 > FTP



192.168.1.5 > ICMP



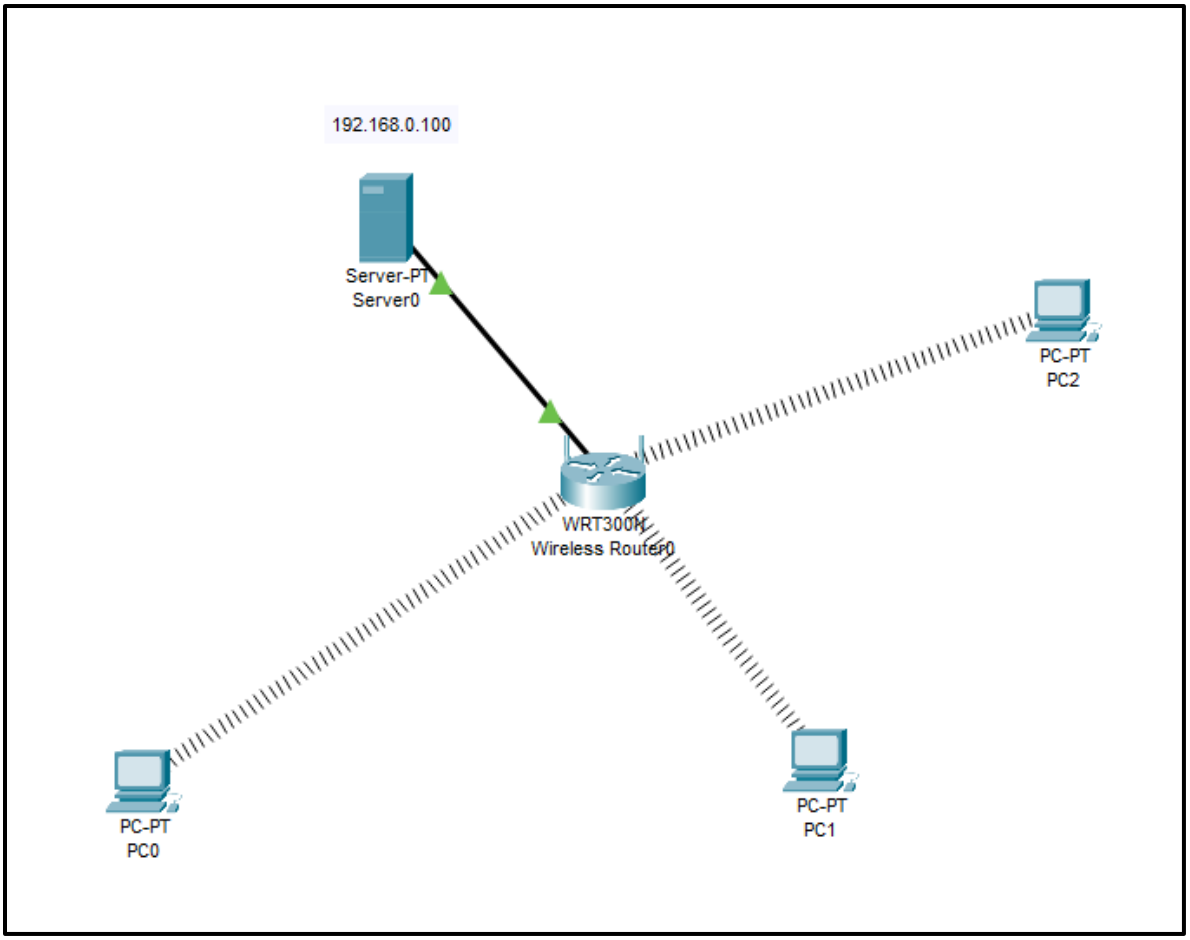
Practical No: 04

Aim: Planning Network-based Firewalls

Components: Wireless Router, Server, PC

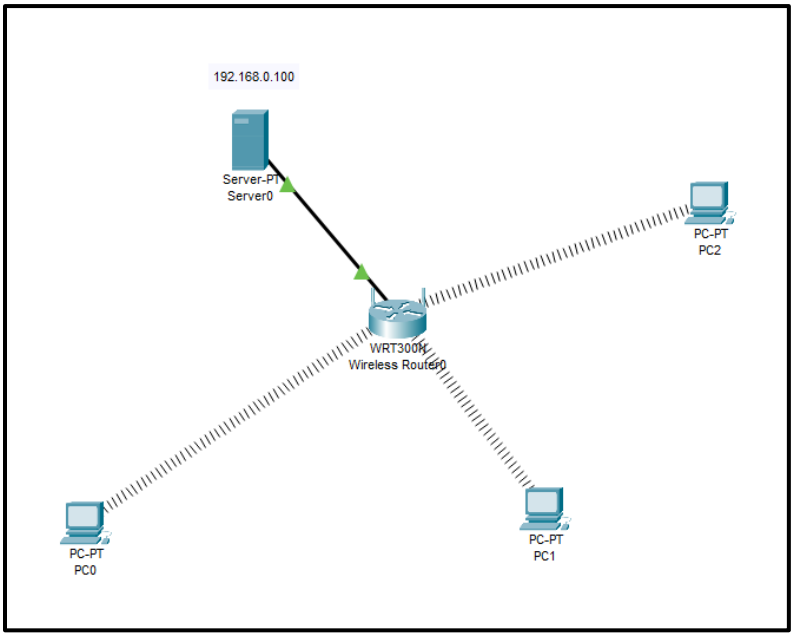
Theory: Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies – any other traffic attempting to access the network is blocked.

Cisco Packet Tracer Setup:-

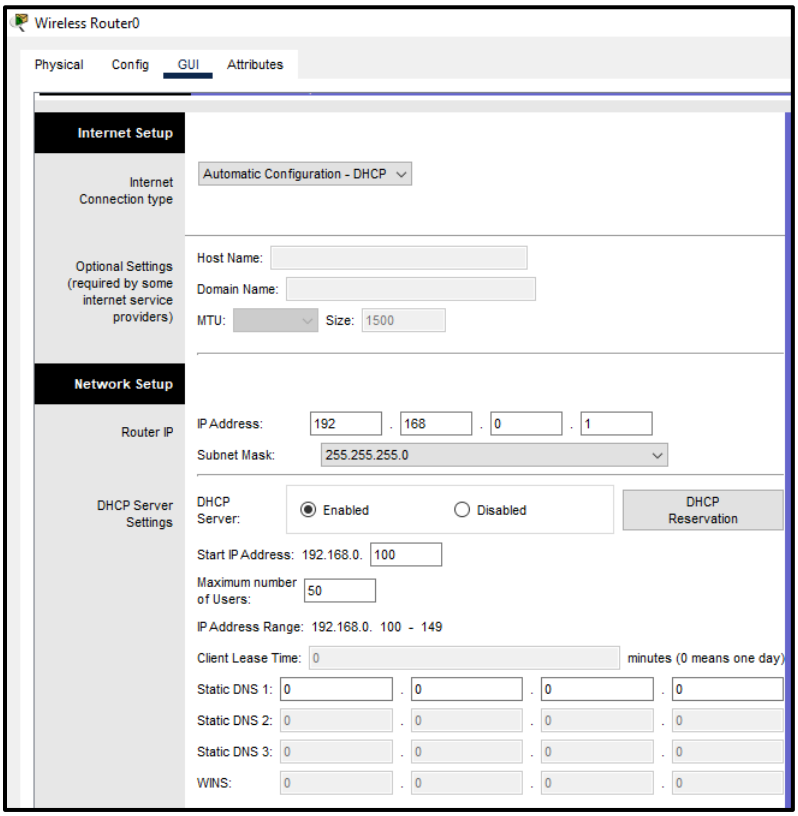


Implementation:

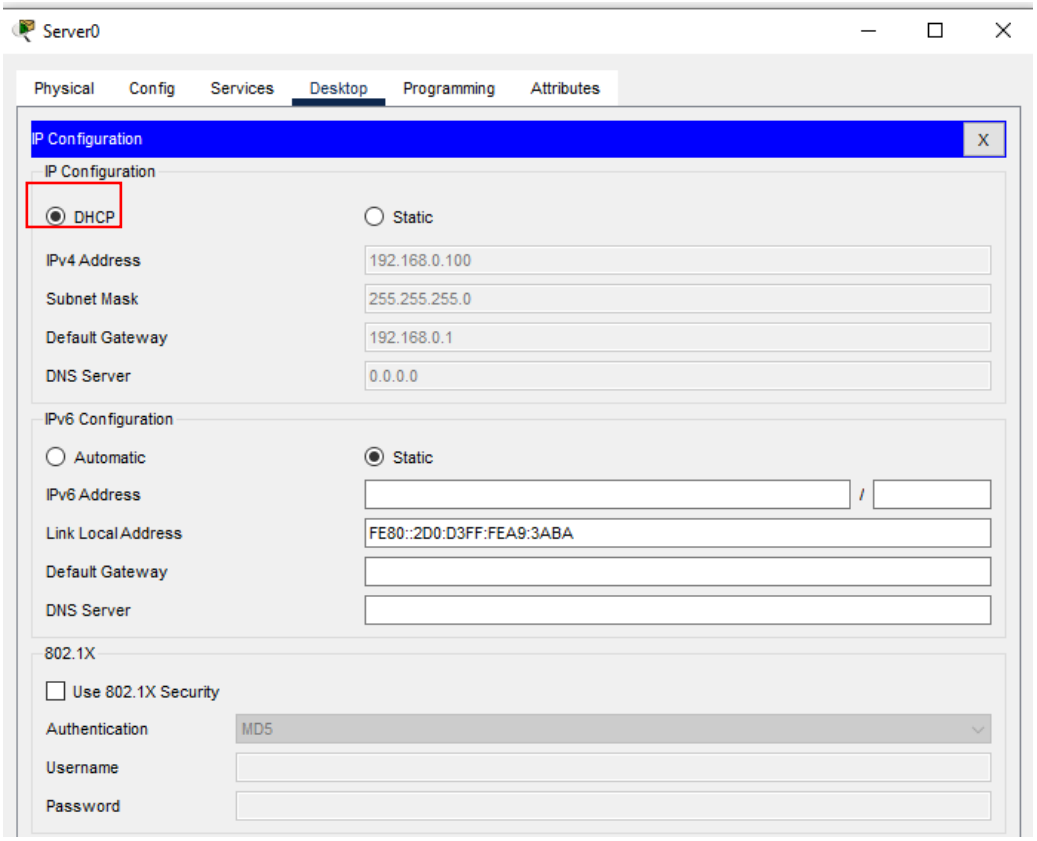
Step 1: Arranging devices and creating connections



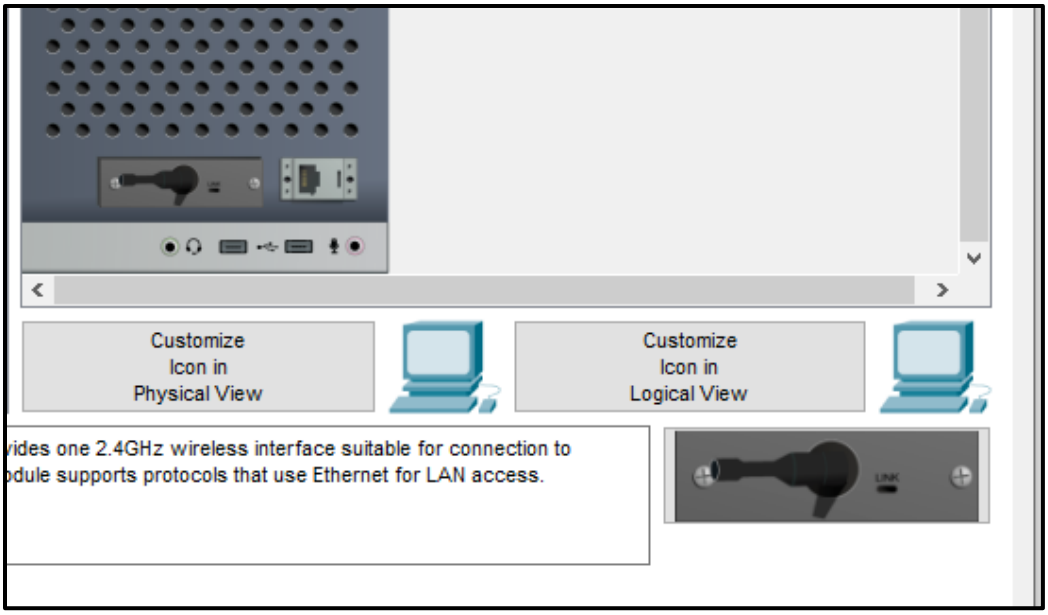
Step 2: Configure wireless router and connect server to wireless router using Ethernet cable



Step 3: Configure Server

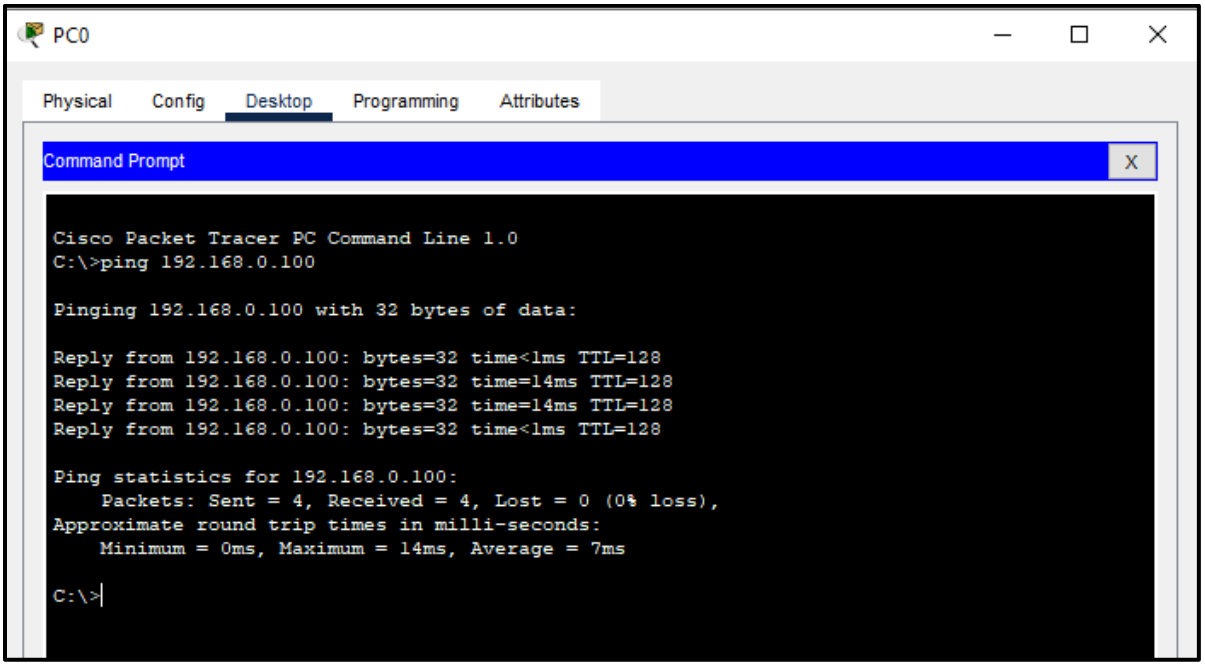


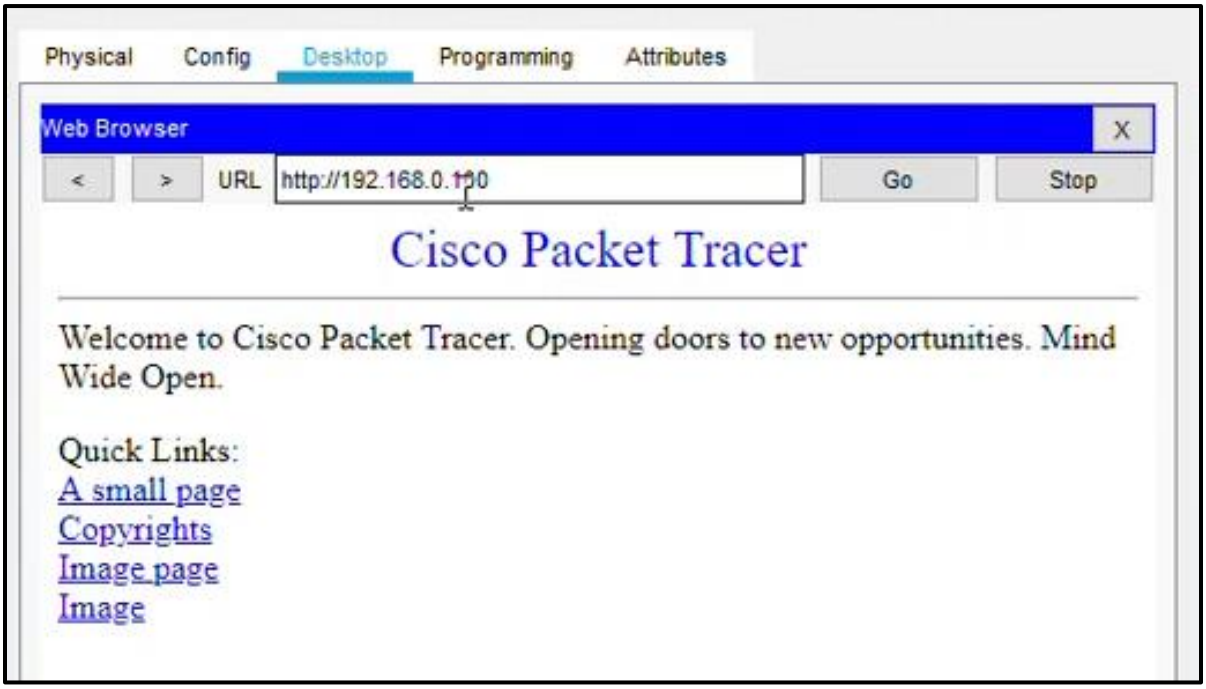
Step 4: Configure and connect all PC's to wireless router Changing port to wireless adapter of all PC's



Step 5: Checking connection of pc's with server

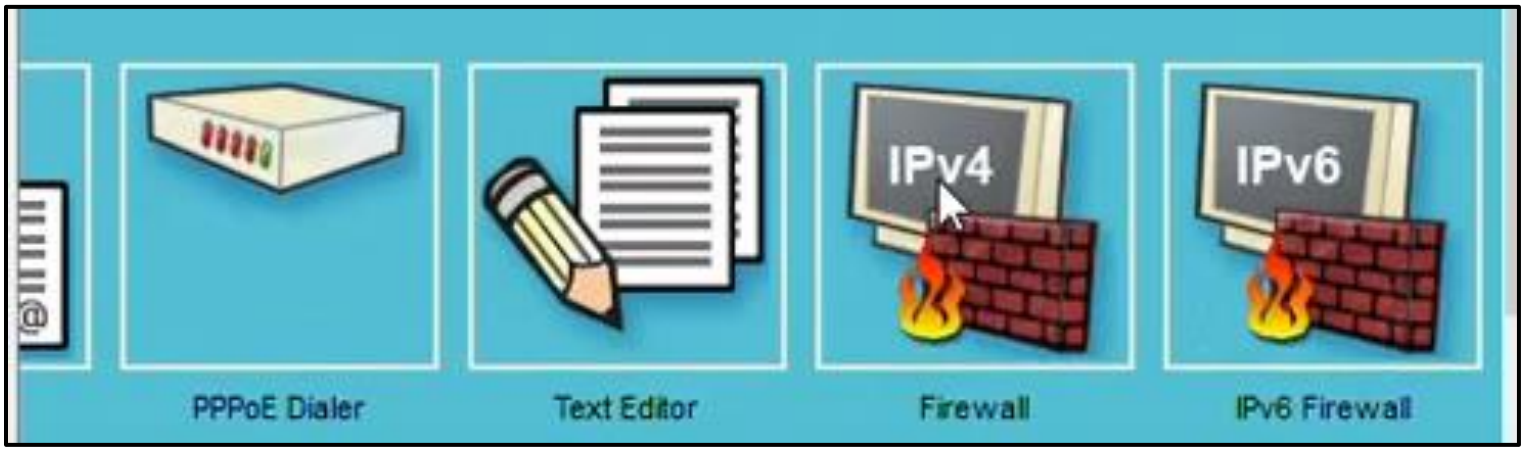
After adding wireless adapter of all PC's they will automatically get connected with wireless outer because of DHCP



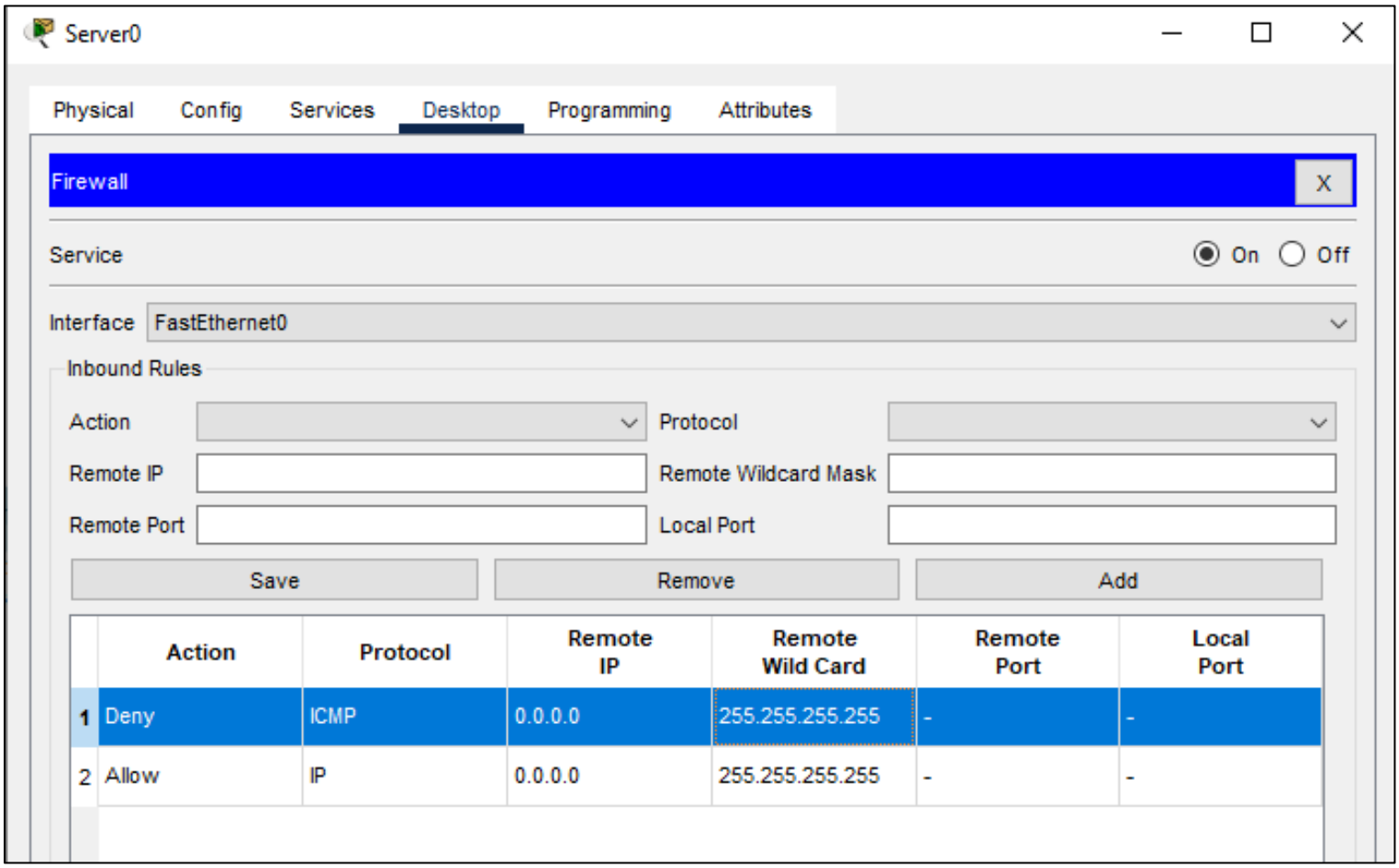


If receiving response from server our connection is done successfully

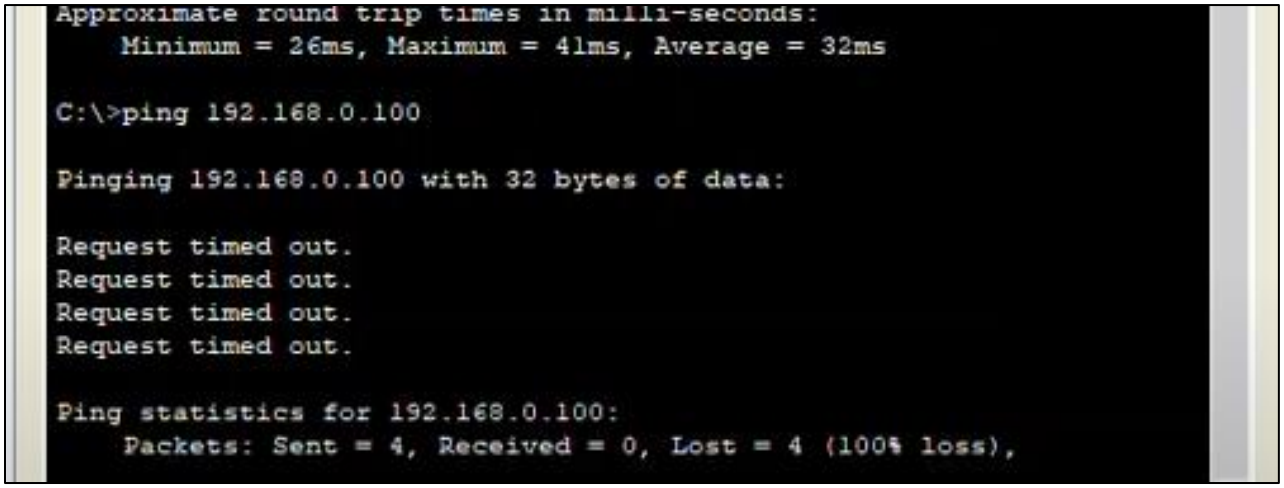
Step 6: Configure IPv4 firewall to setup networks based firewall



Add conditions



After the configuration is done for firewall we are unable to ping to server



But we can access the server data (view)

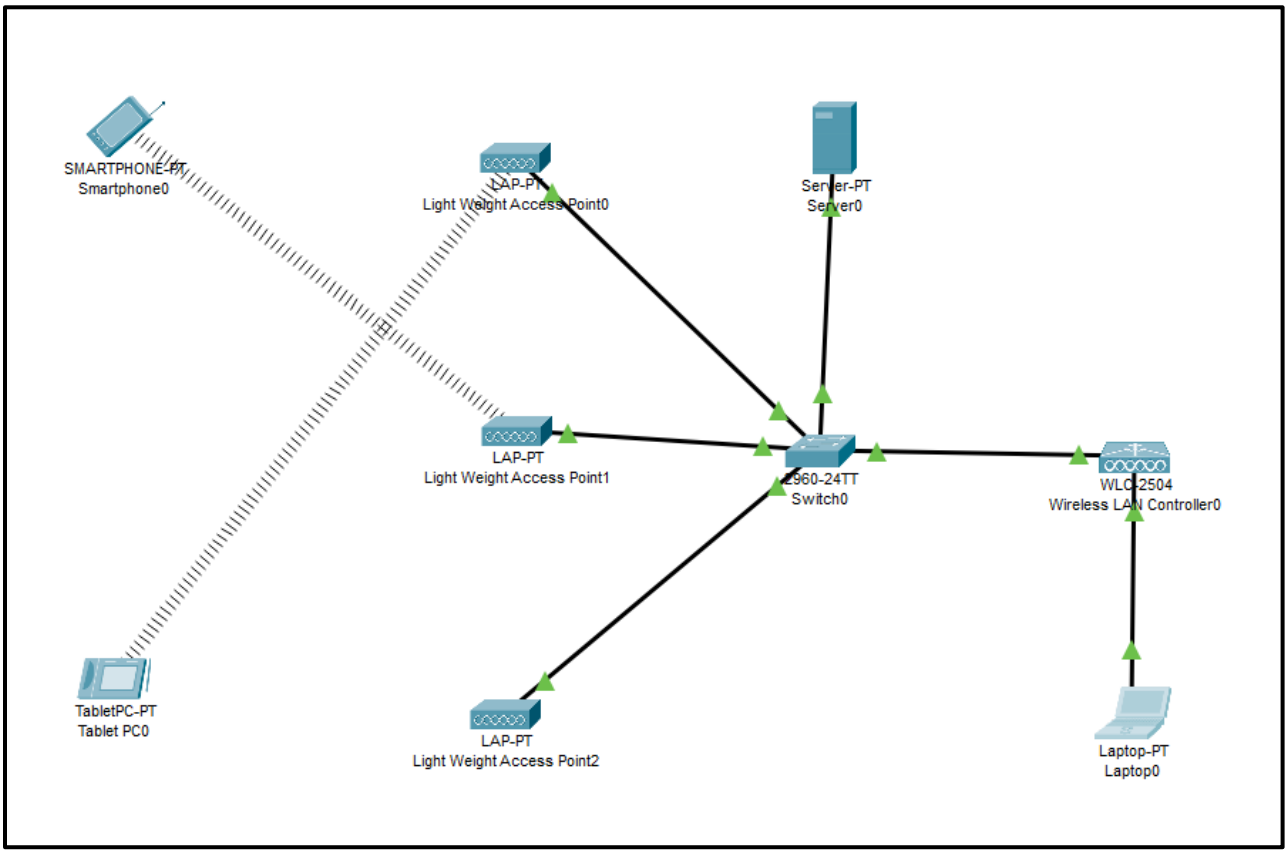
Practical No: 05

Aim: Configure Auto Profiles ACU Utilities

Components: WLC (Wireless LAN Controller), AP (Access point), Switch, Server, Laptop, Smartphone, Tablet

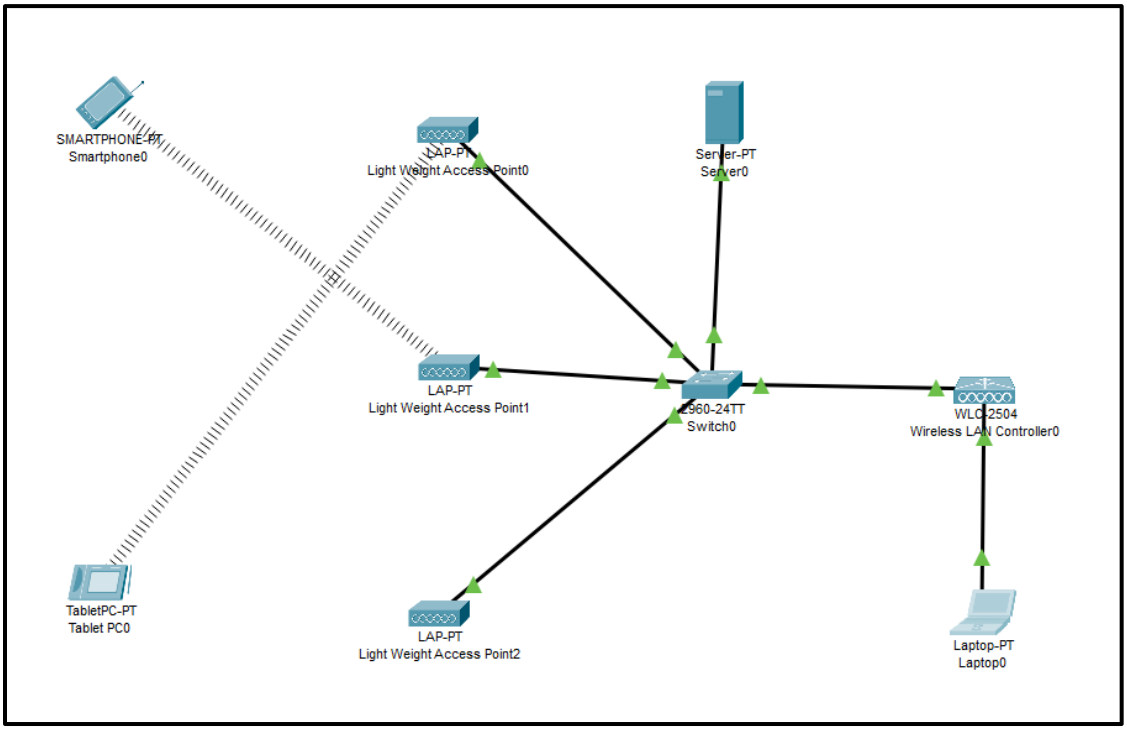
Theory: ACU is a device that enables equipment, such as computers and card dialers, to originate calls automatically over a telecommunications network.

Cisco Packet Tracer Setup:-

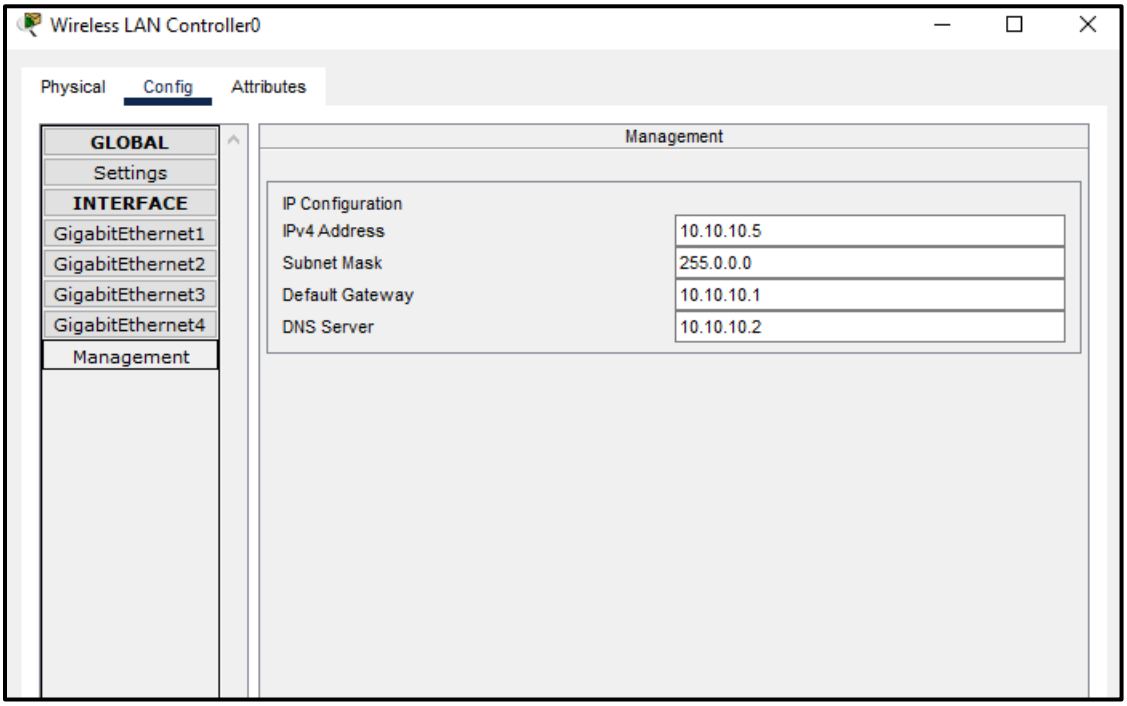


Implementation:

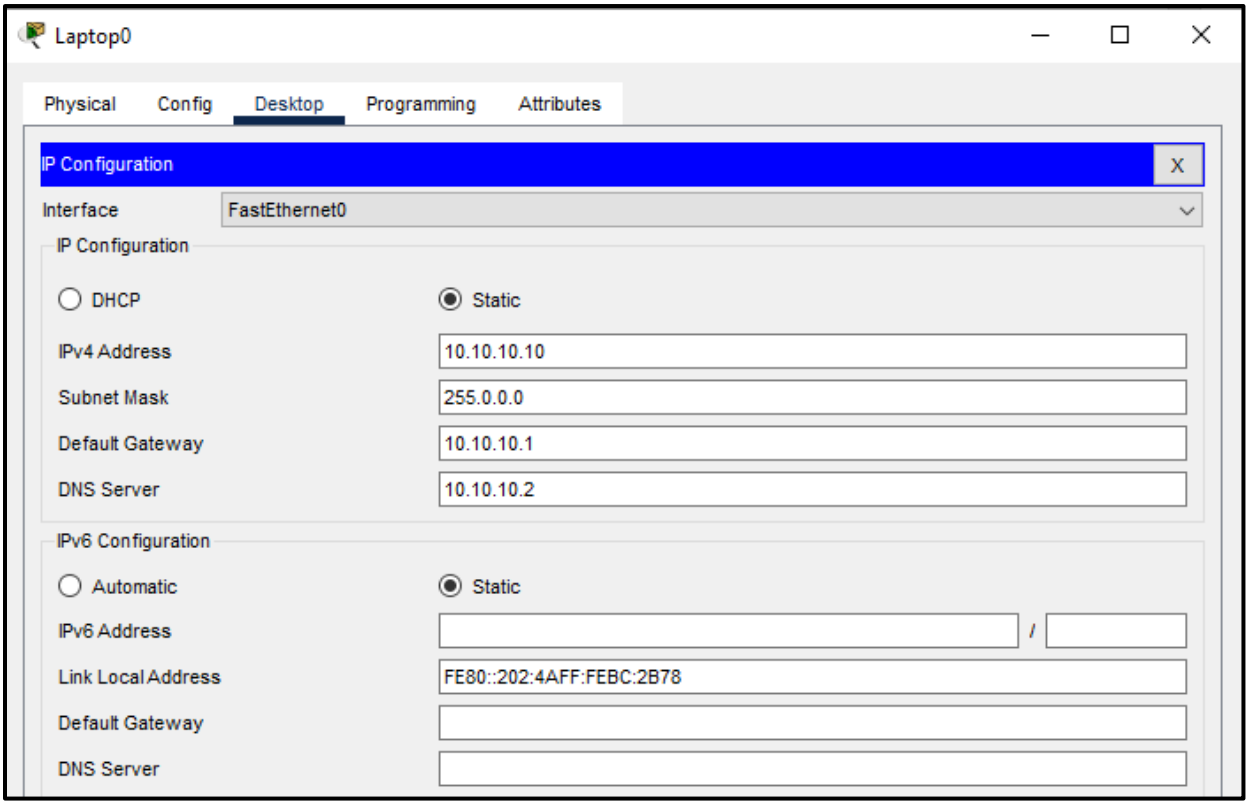
Step 1: Arranging devices and creating connections

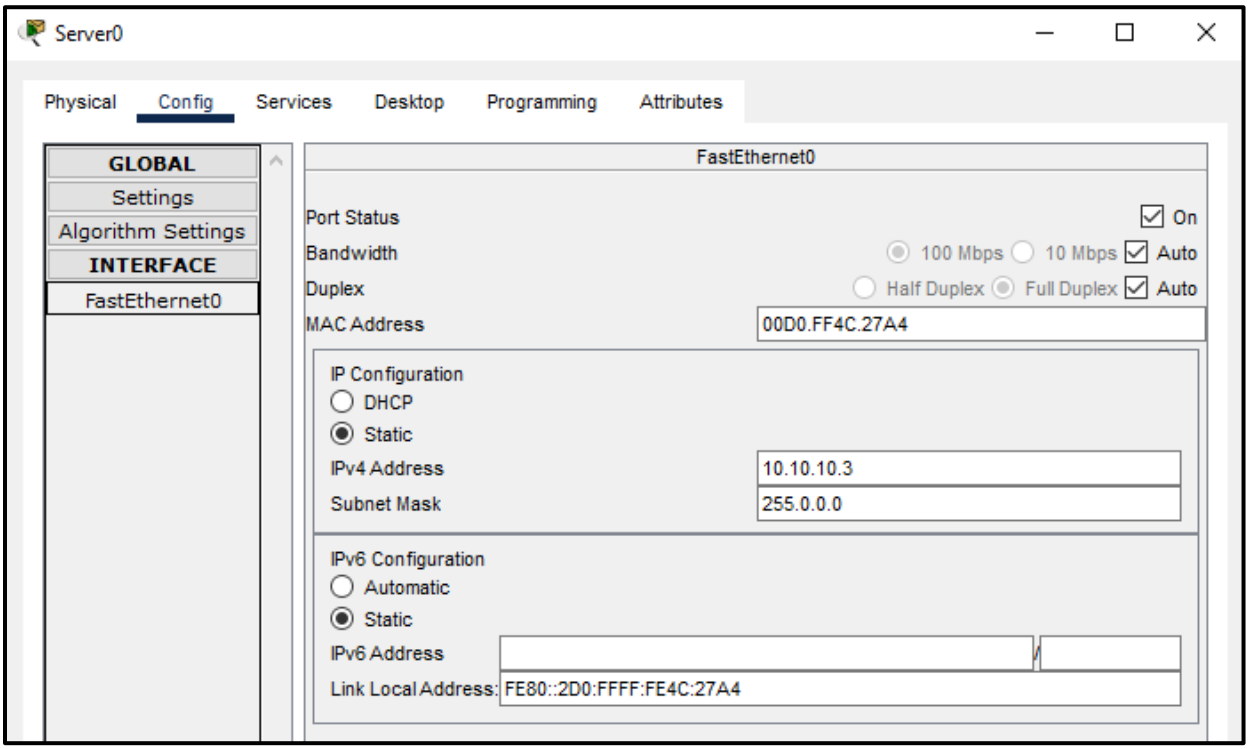


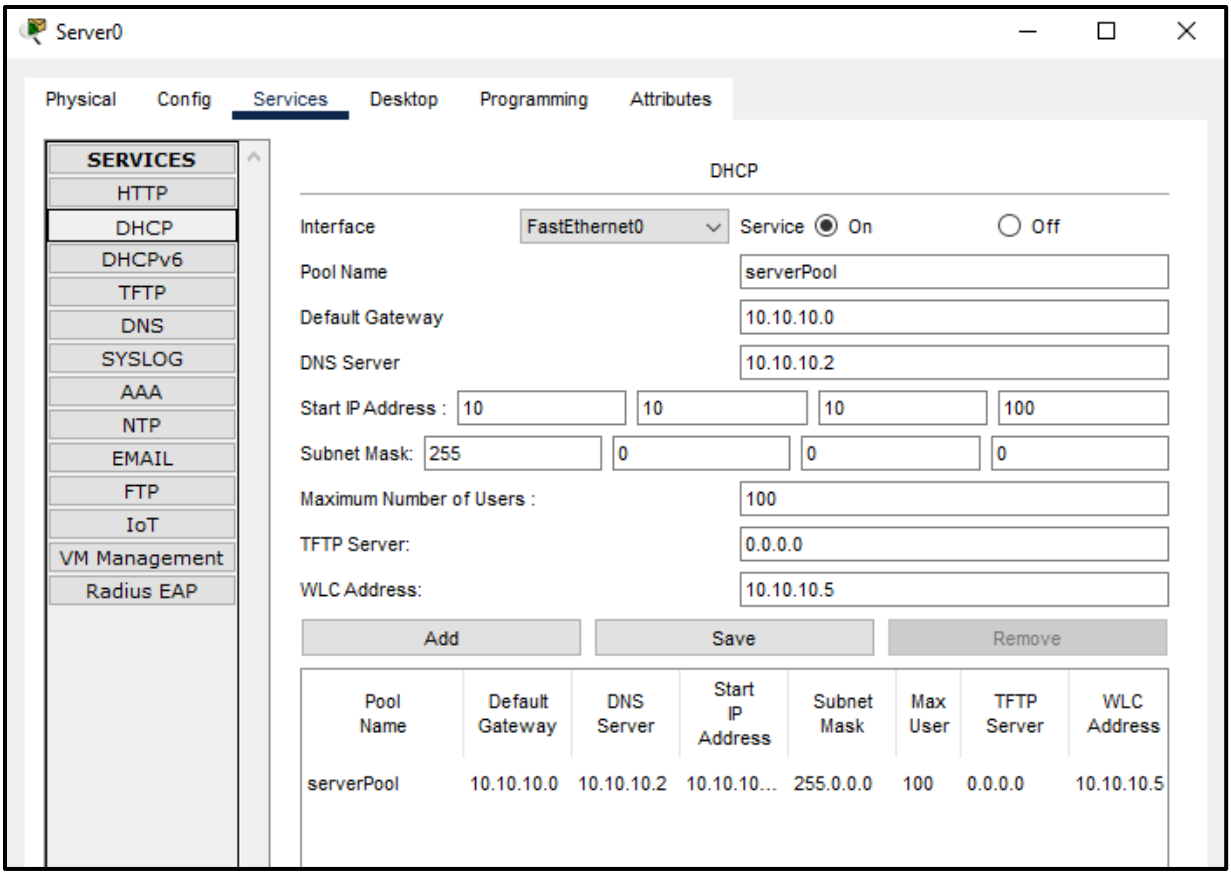
Step 2: WLC (Wireless LAN Controller)



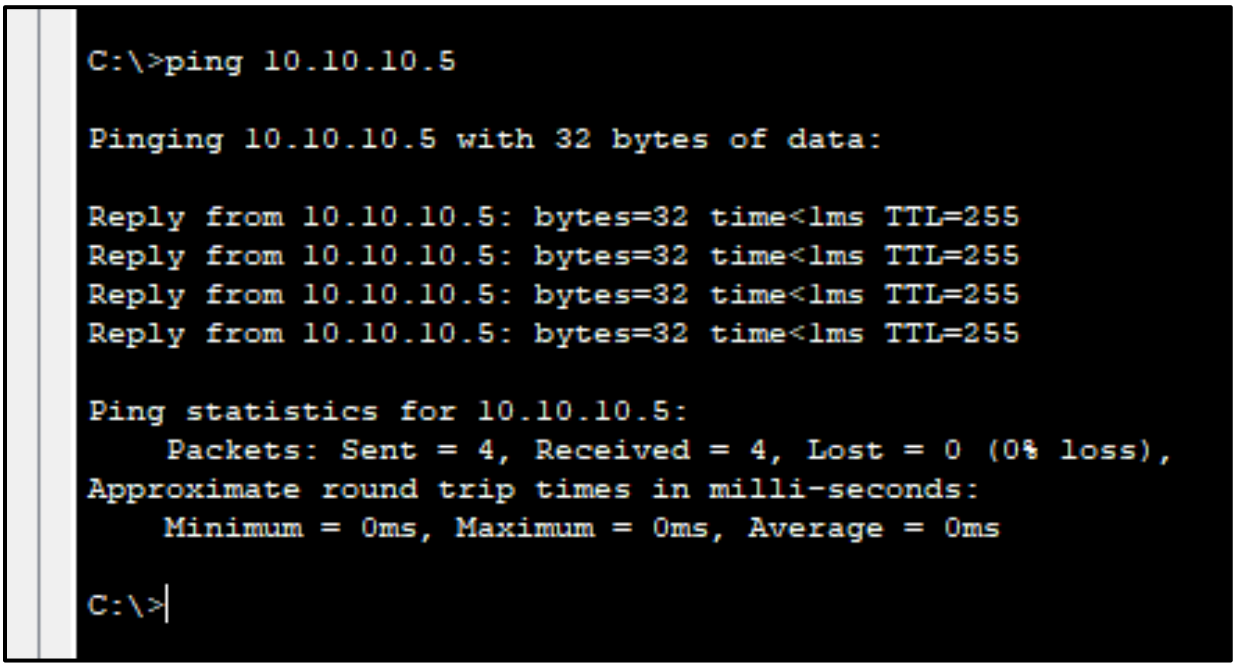
Step 3: Configuring Laptop and server and checking connection





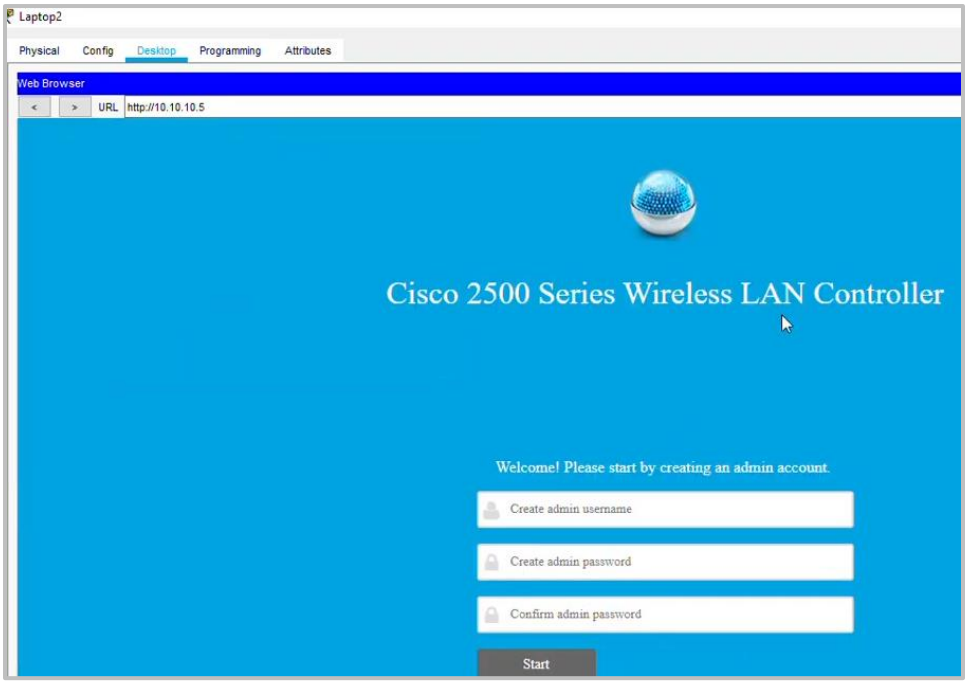


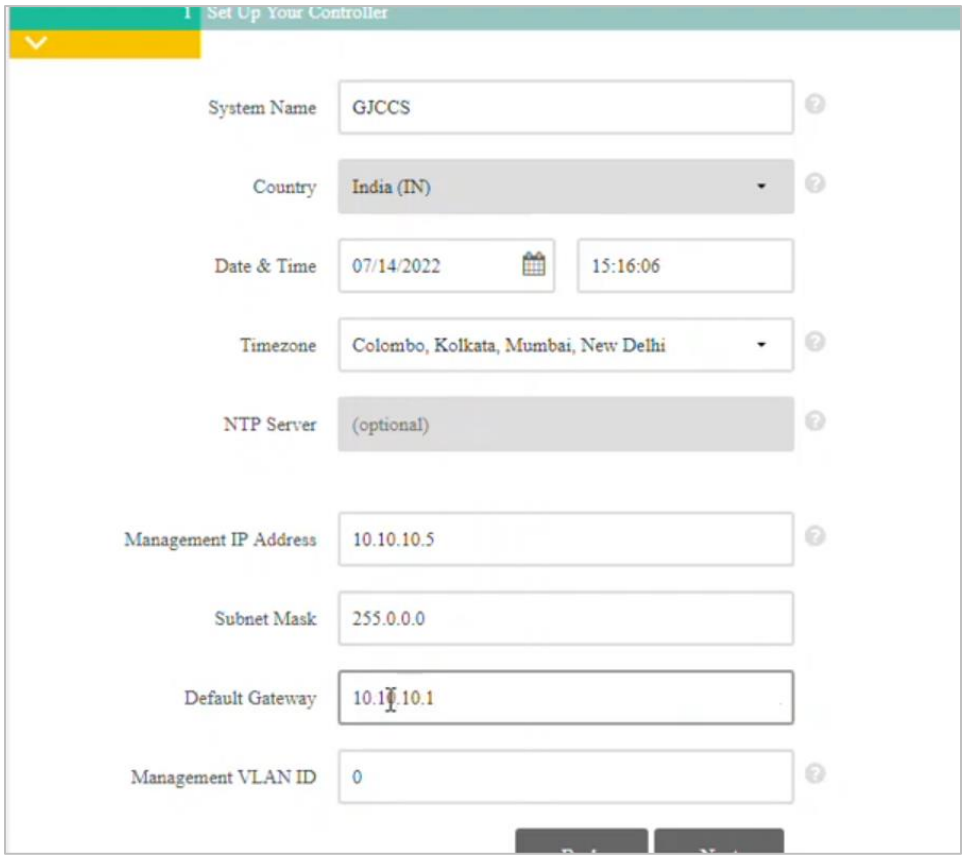
Check the connection

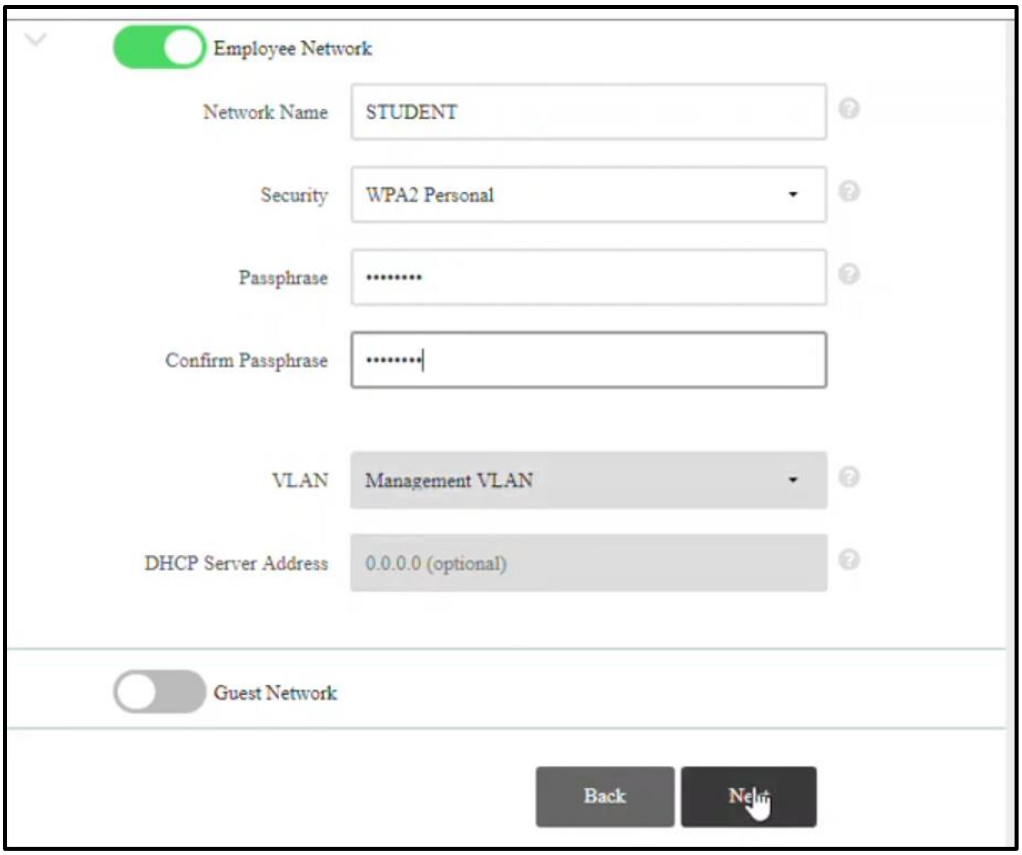


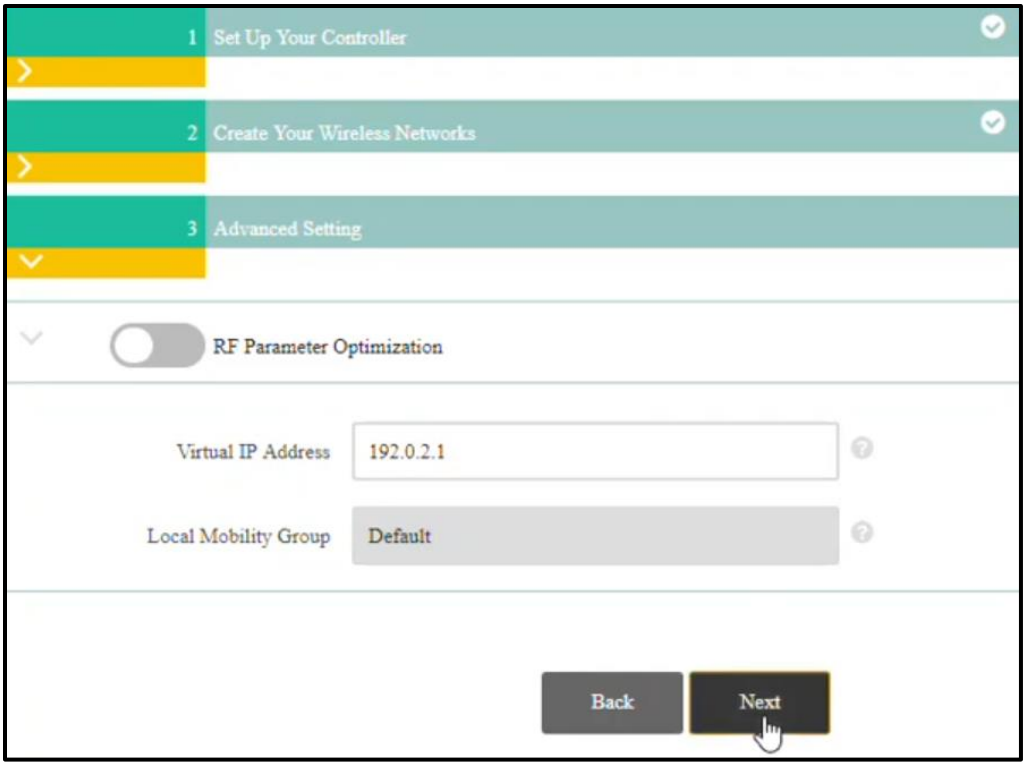
```
C:\>ping 10.10.10.5

Pinging 10.10.10.5 with 32 bytes of data:

Reply from 10.10.10.5: bytes=32 time<1ms TTL=255
Reply from 10.10.10.5: bytes=32 time<1ms TTL=255
Reply from 10.10.10.5: bytes=32 time<1ms TTL=255
Reply from 10.10.10.5: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

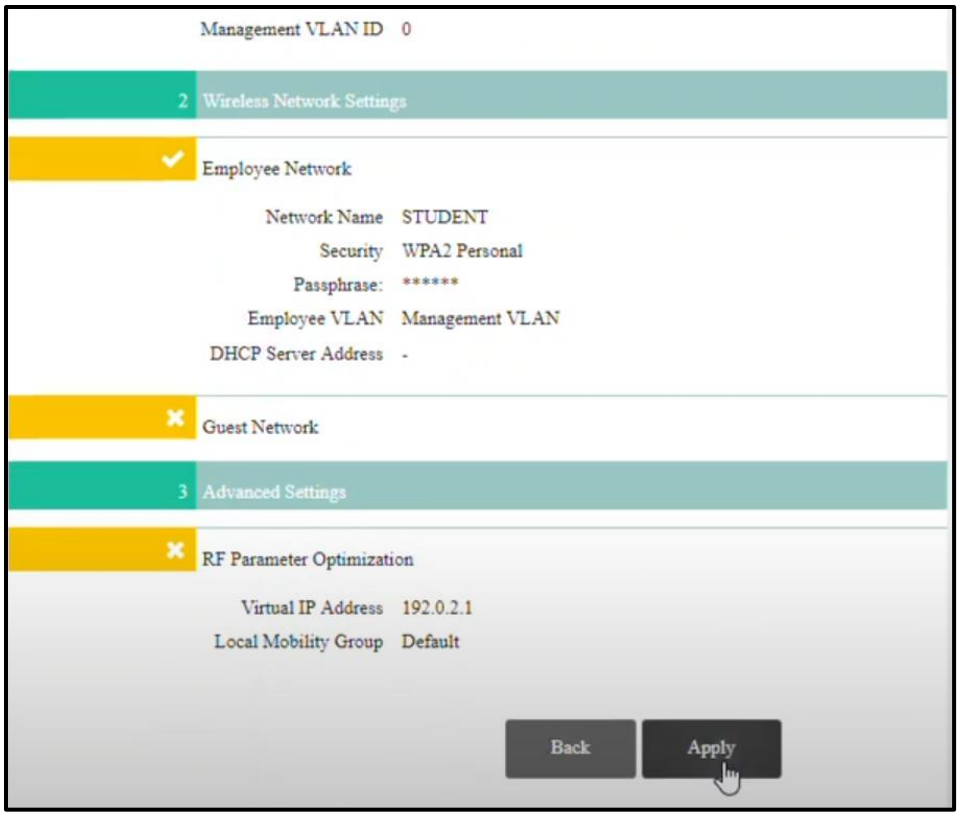
Step 4: Configuring Admin settings using address (http://10.10.10.5)

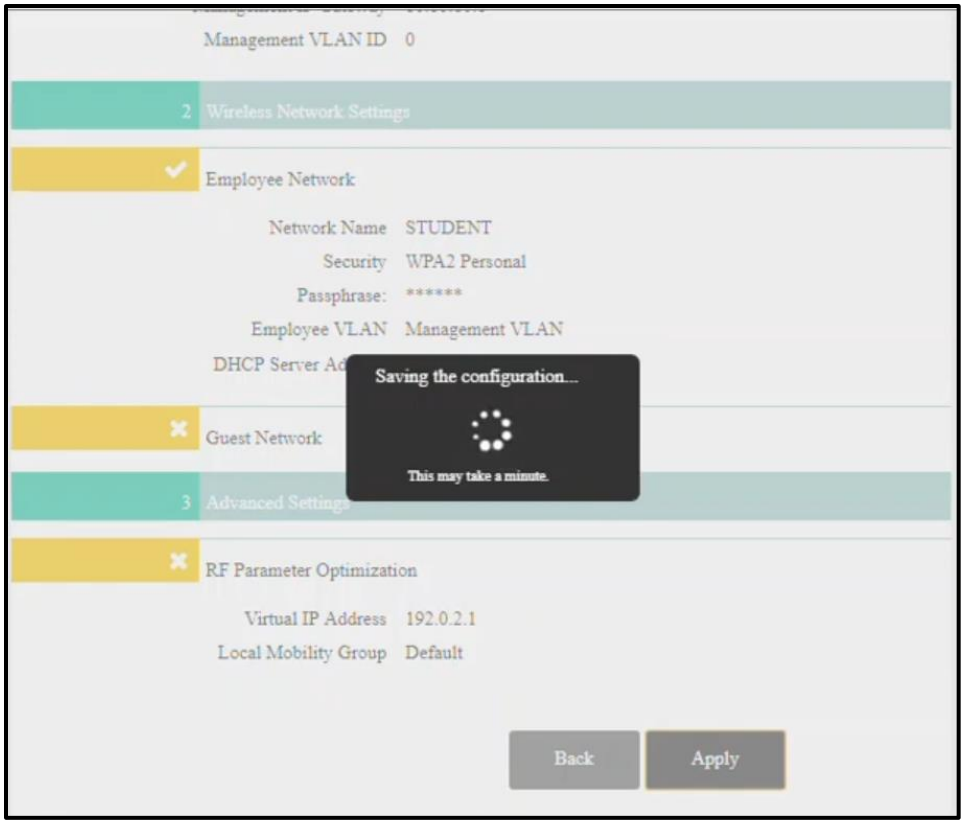




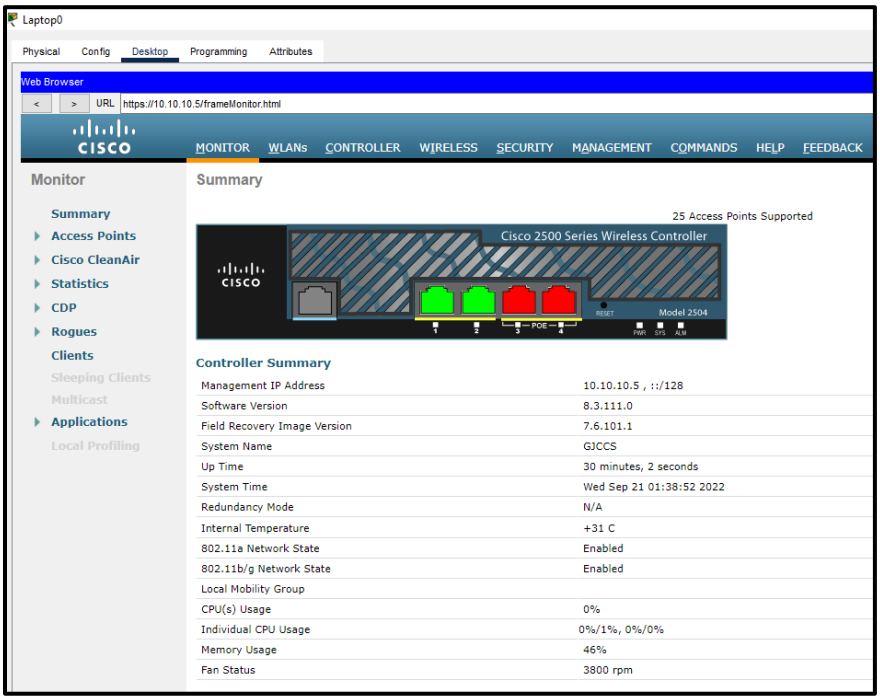

Employee Network
Network Name
STUDENT
Security
WPA2 Personal
Passphrase
Confirm Passphrase
VLAN
Management VLAN
DHCP Server Address
0.0.0.0 (optional)
Guest Network
Back
Next


1 Set Up Your Controller
2 Create Your Wireless Networks
3 Advanced Setting
RF Parameter Optimization
Virtual IP Address
192.0.2.1
Local Mobility Group
Default
Back
Next

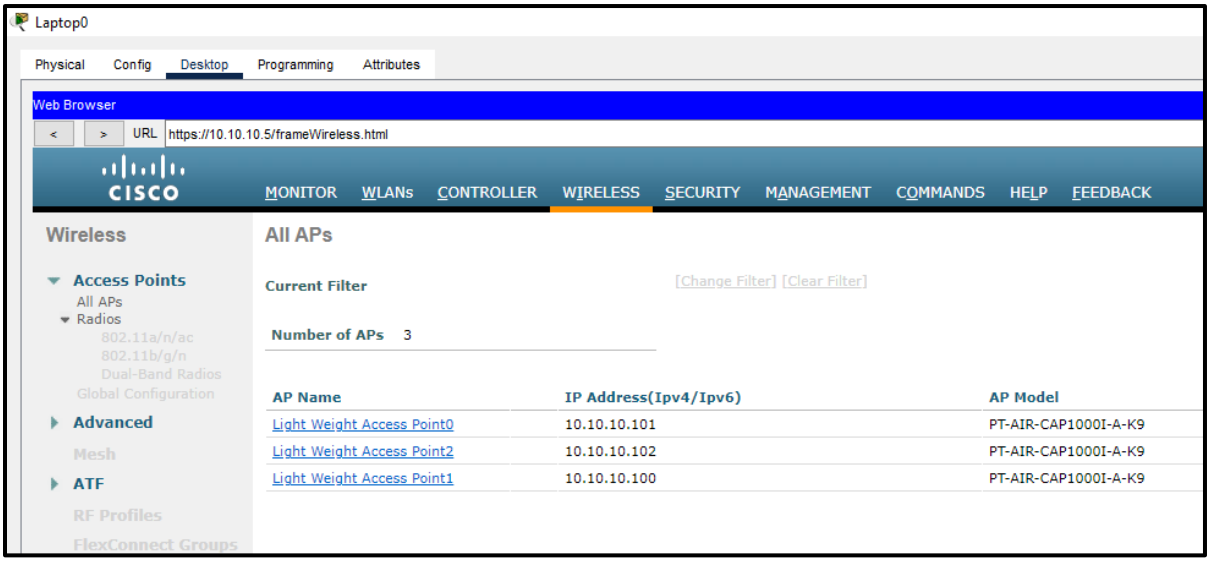

Management VLAN ID 0
2 Wireless Network Settings
Employee Network
Network Name STUDENT
Security WPA2 Personal
Passphrase: ******
Employee VLAN Management VLAN
DHCP Server Address -
Guest Network
3 Advanced Settings
RF Parameter Optimization
Virtual IP Address 192.0.2.1
Local Mobility Group Default
Back
Apply


Management VLAN ID 0
2 Wireless Network Settings
Employee Network
Network Name STUDENT
Security WPA2 Personal
Passphrase: ******
Employee VLAN Management VLAN
Saving the configuration...
This may take a minute.
Guest Network
3 Advanced Settings
RF Parameter Optimization
Virtual IP Address 192.0.2.1
Local Mobility Group Default
Back
Apply

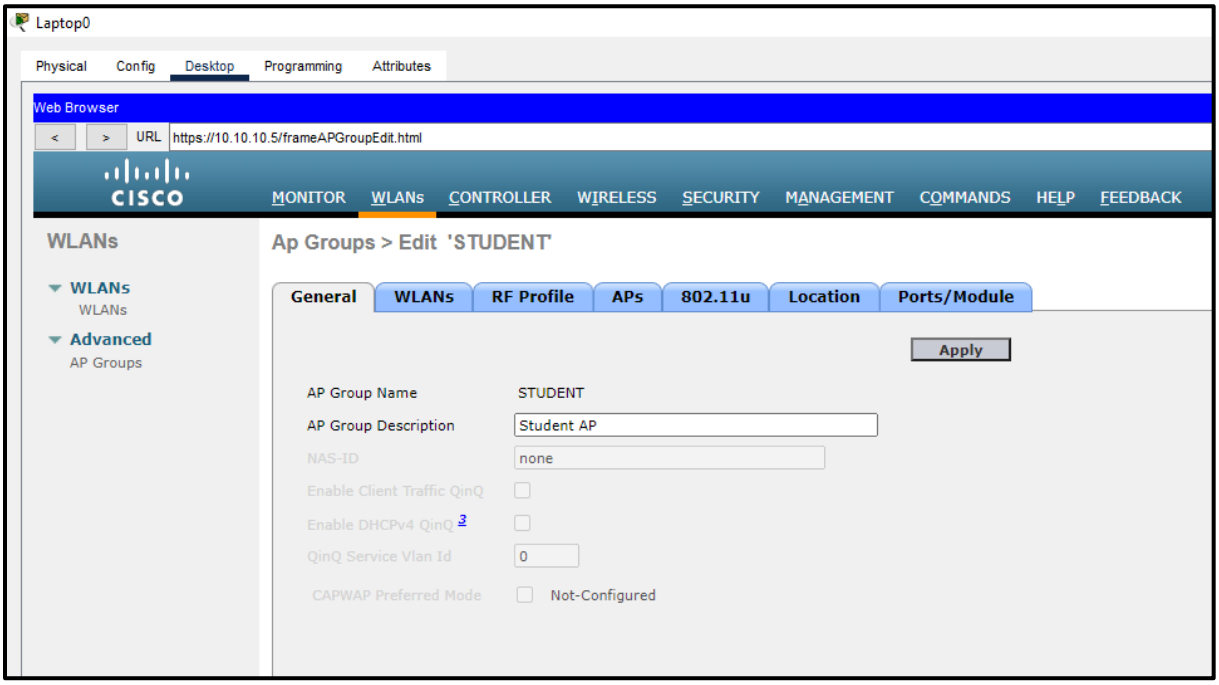
Step 5: Login back to Admin Panel using address (https://10.10.10.5)



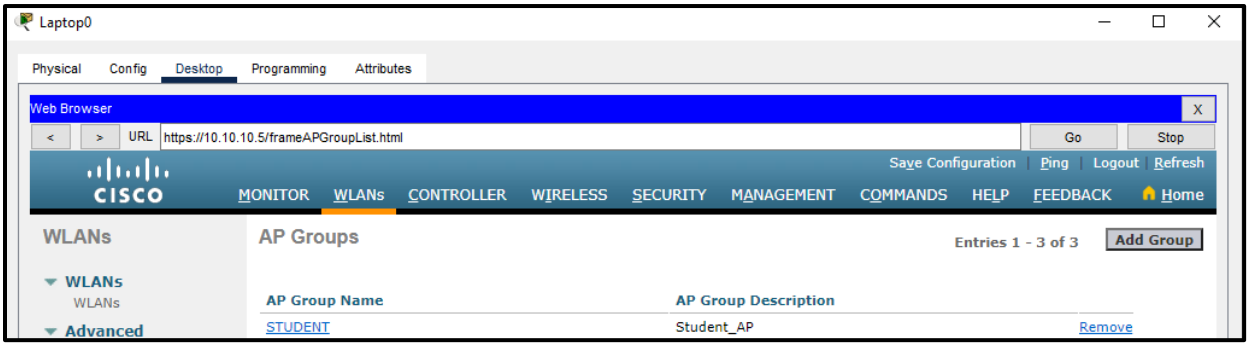
Check the Access points AP'ˢ

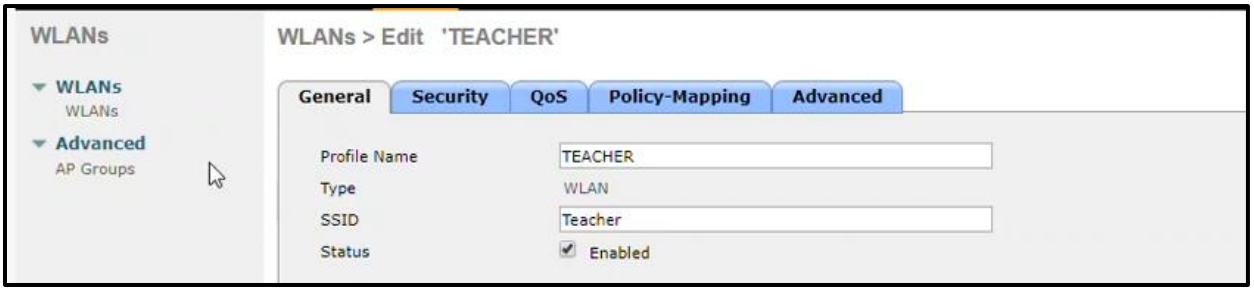


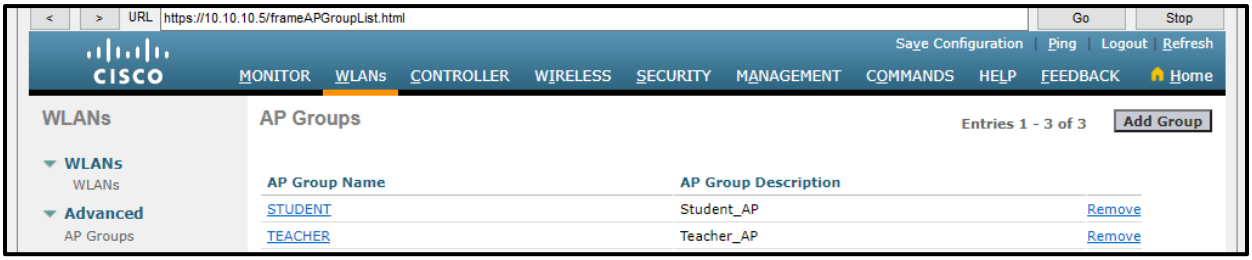
Go to WLAN'ˢ make SSID for STUDENT to Student



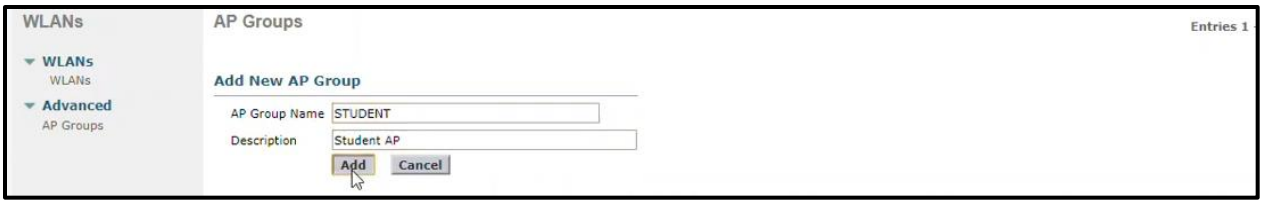
Step 6: Add new wireless LAN as TEACHER with SSID Teacher



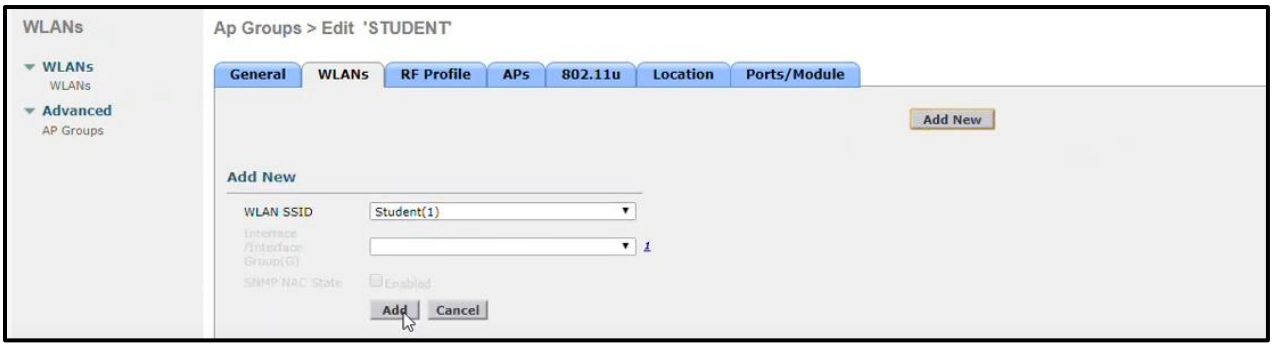


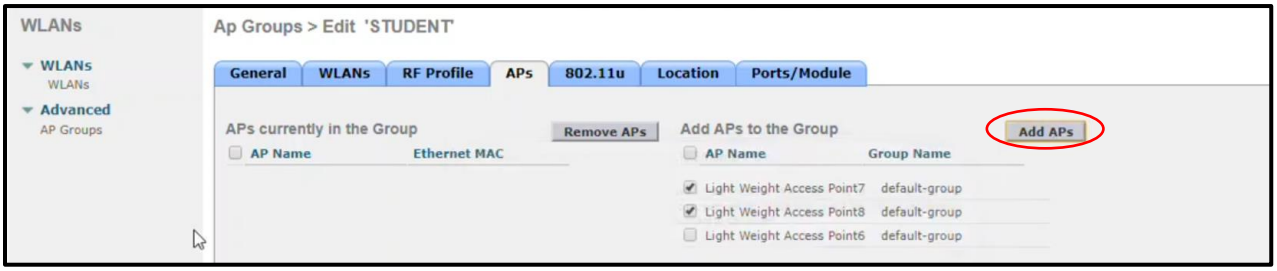


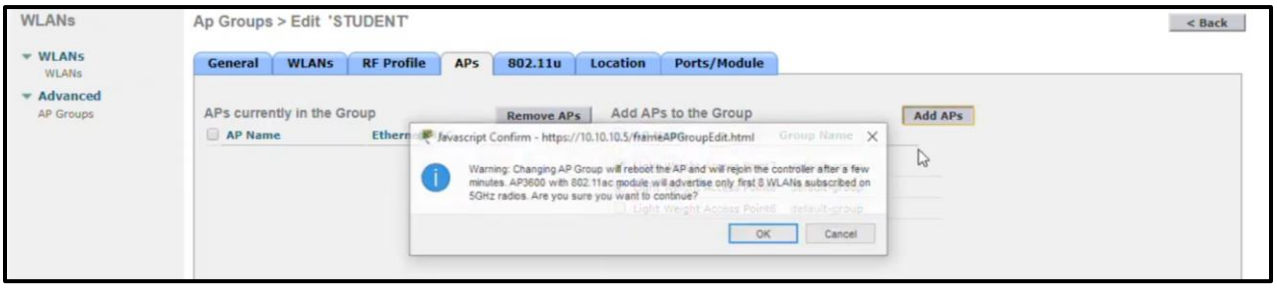
Step 7: Create AP Groups for TEACHER and STUDENT



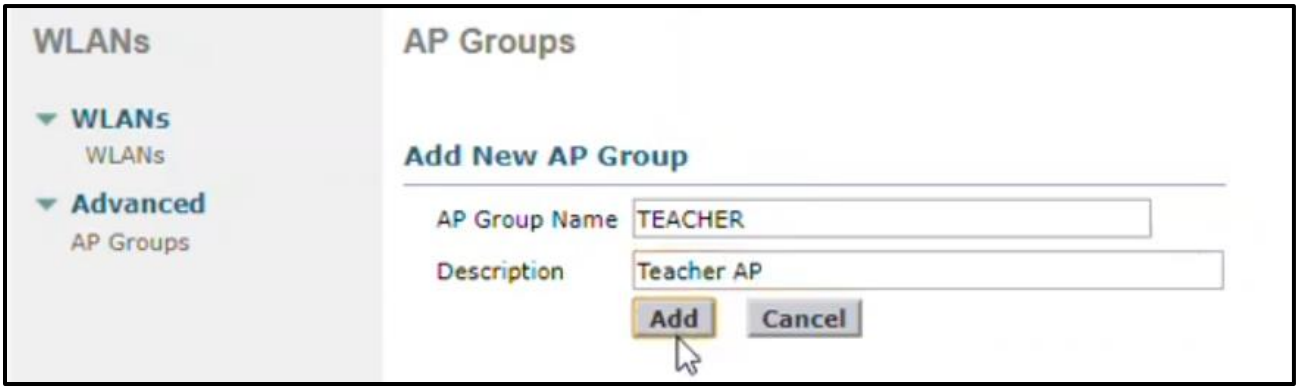
Assign wireless LAN to AP



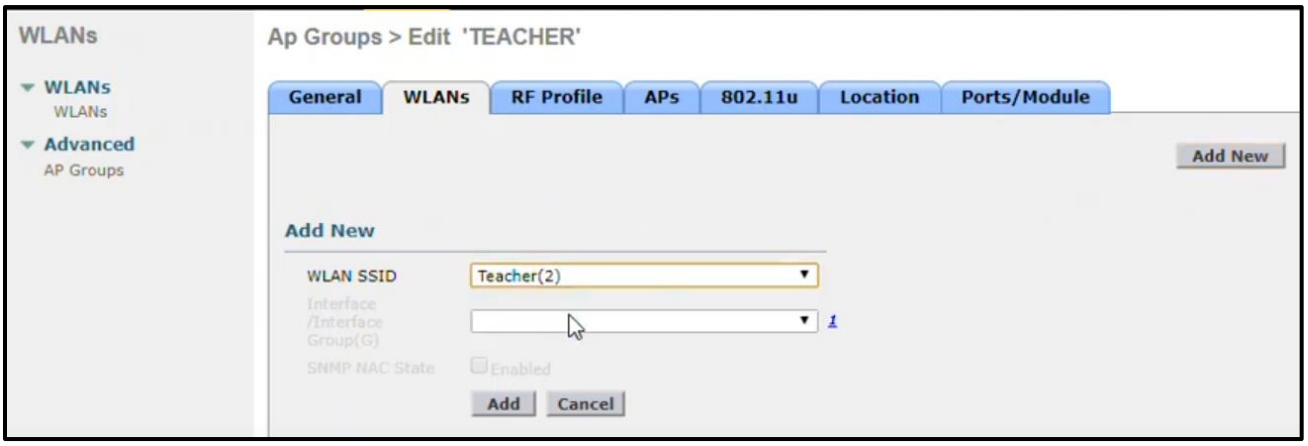




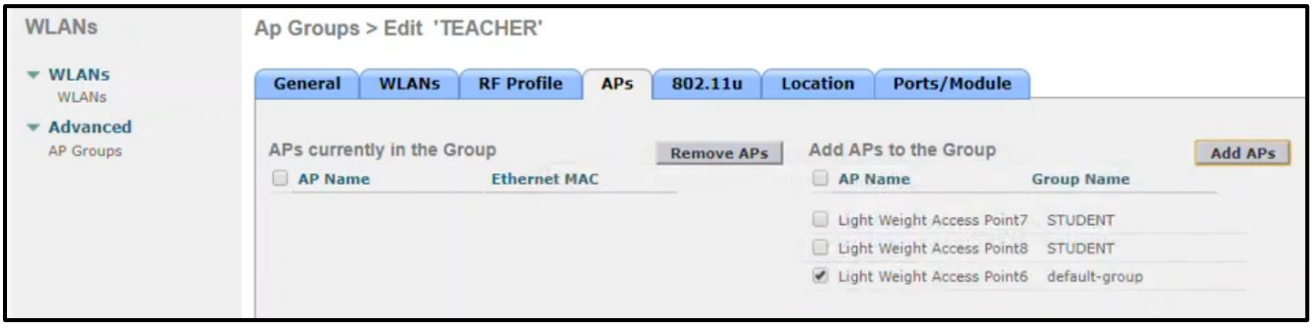
Add AP Group TEACHER



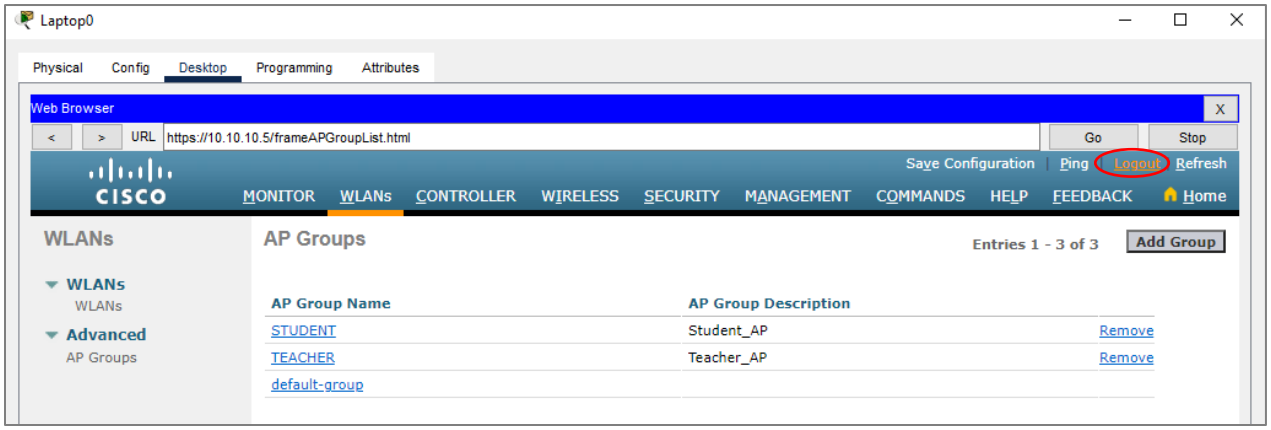
Assign wireless LAN



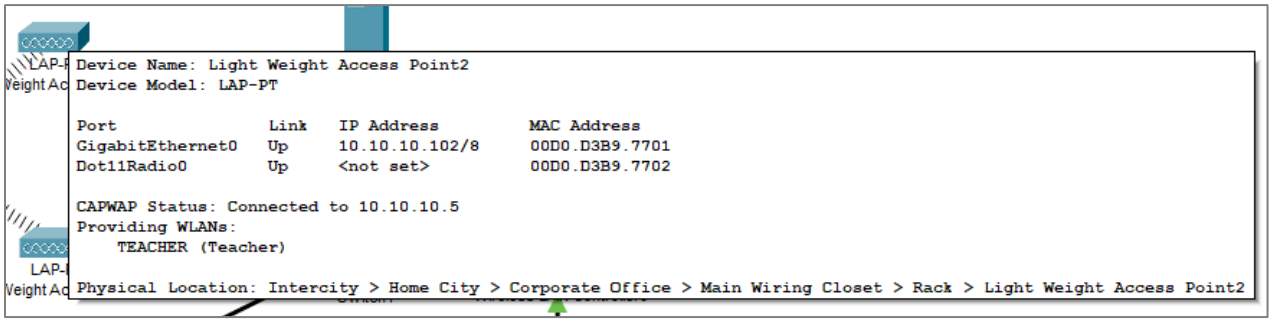
Assign AP

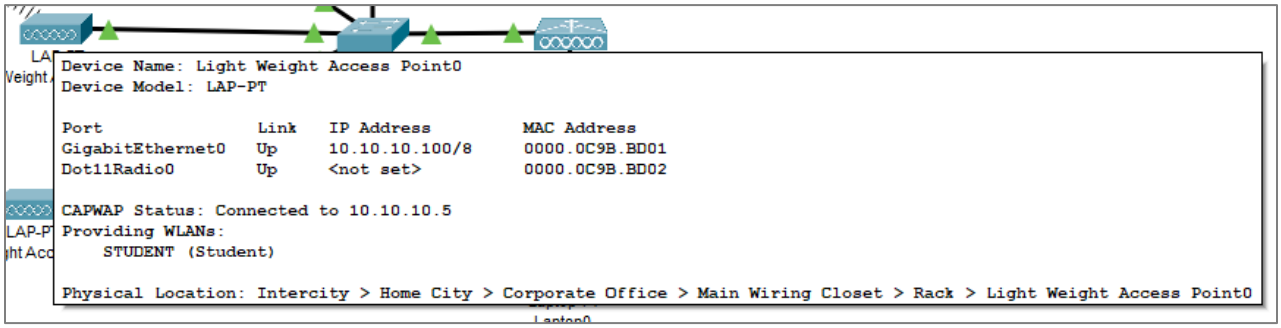


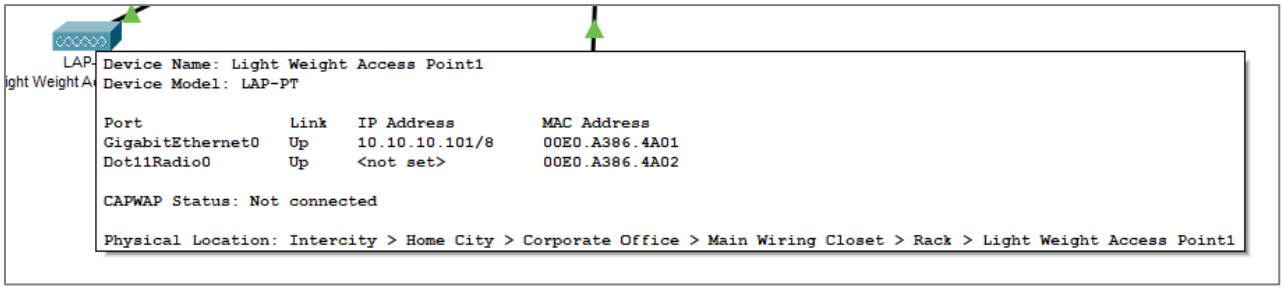
Logout from admin panel



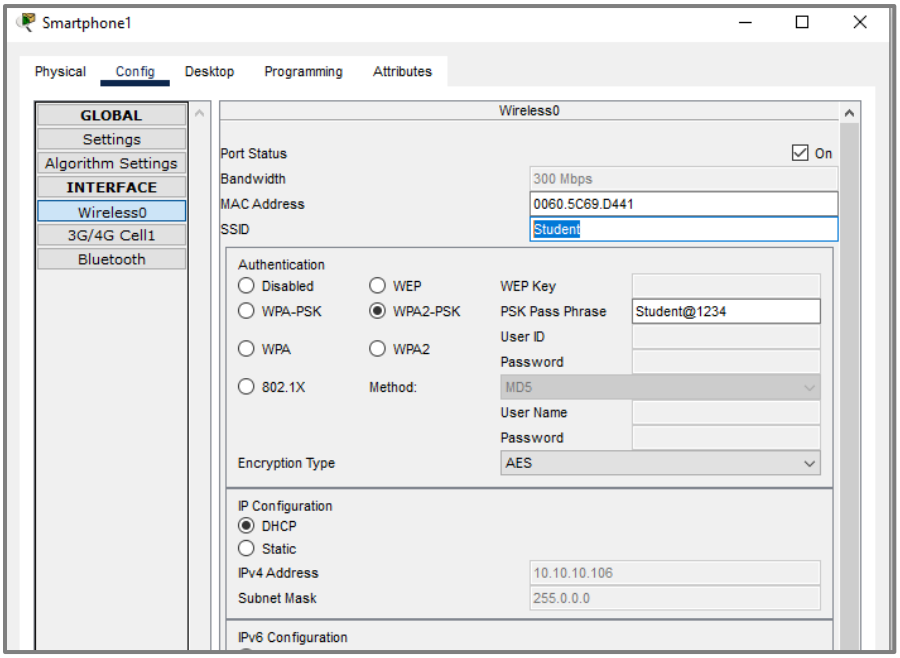
Check the assigned AP's



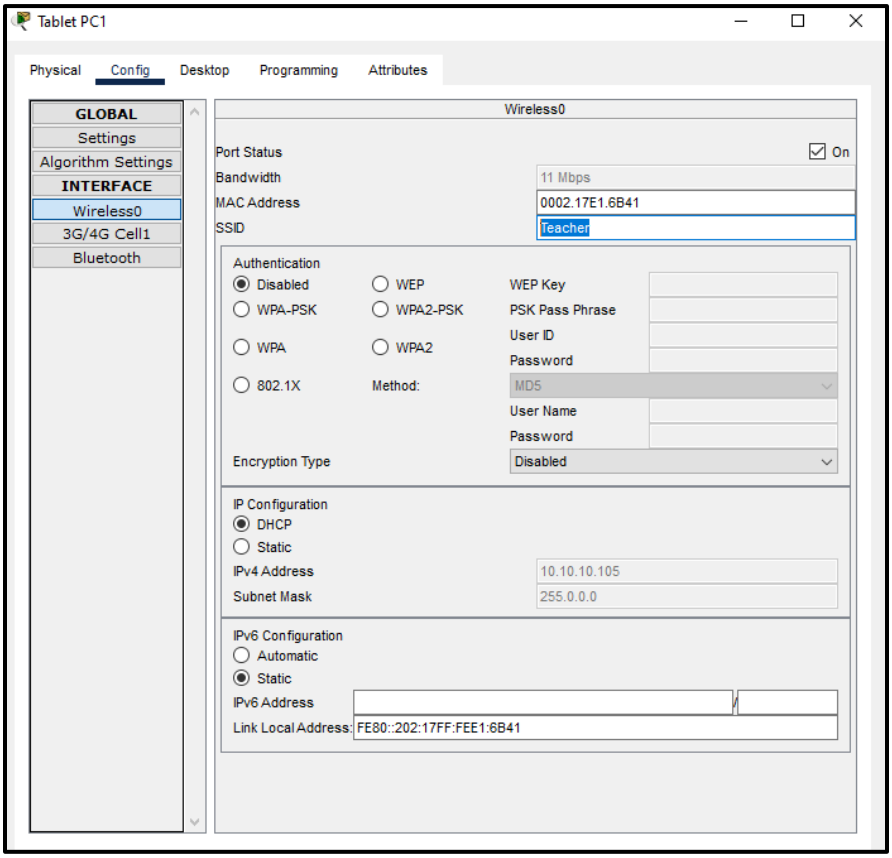




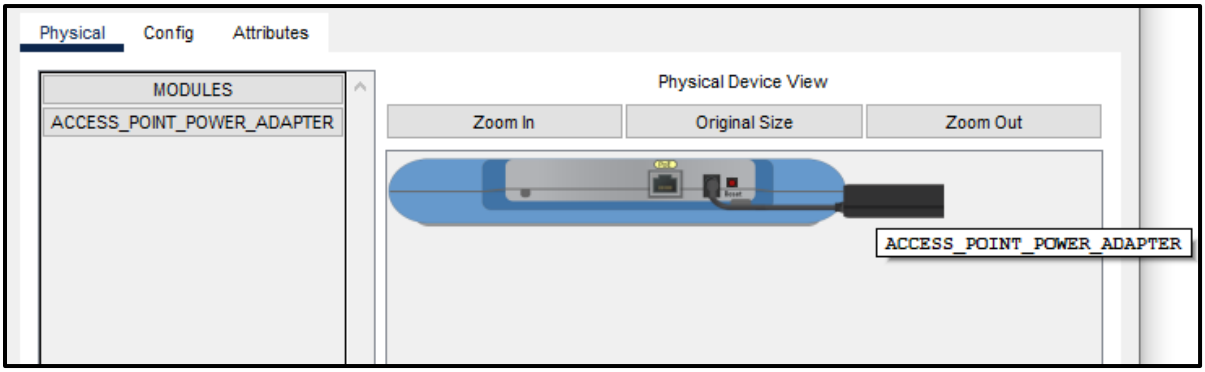
Step 8: Take Smartphone to connect Student AP group with wireless connection using SSID



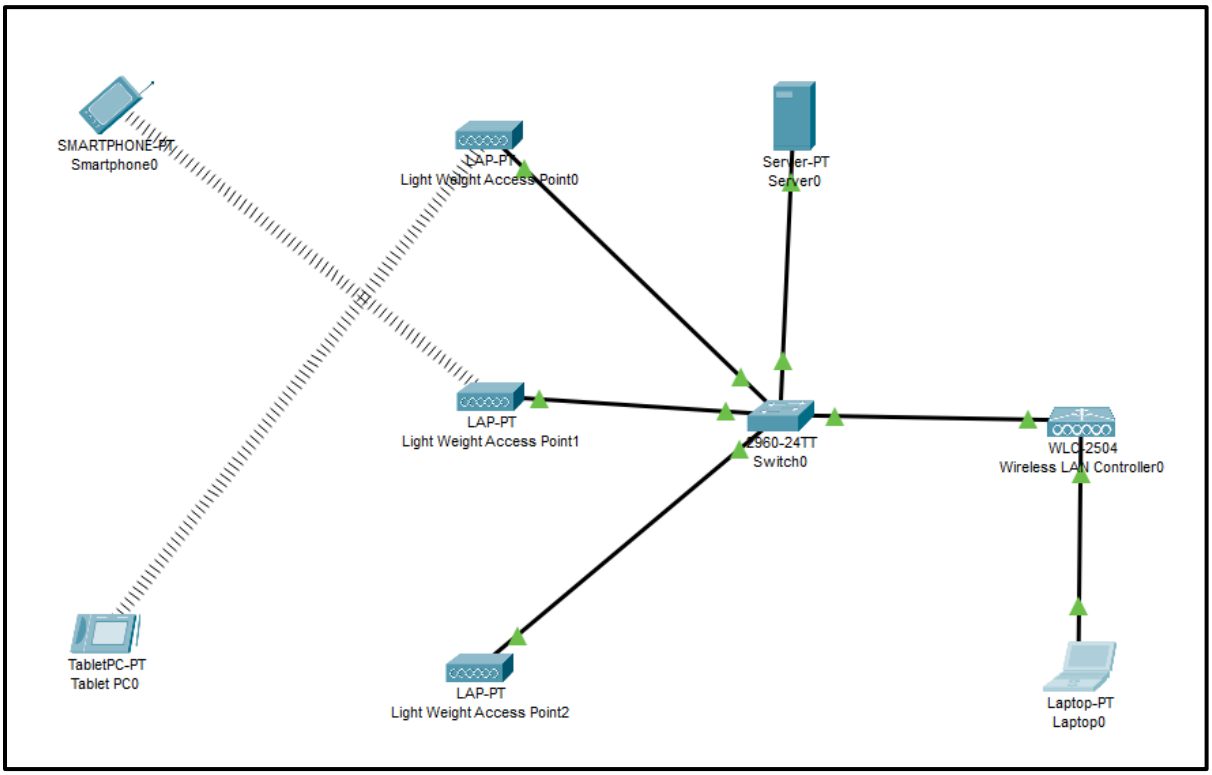
Step 9: Take Tablet to connect Teachers AP group with wireless connection using SSID



Wait for some time (min 30sec to 1min) after that re-plug the adapters of all Access points



Final Output/Connection:



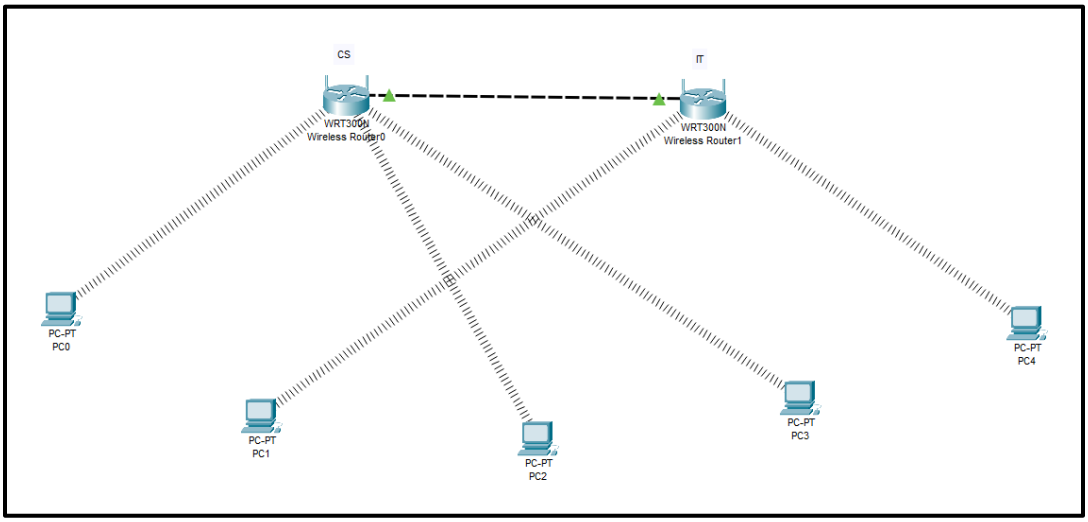
Practical No: 06

Aim: Creating an Adhoc Network

Components: Wireless Router, PC

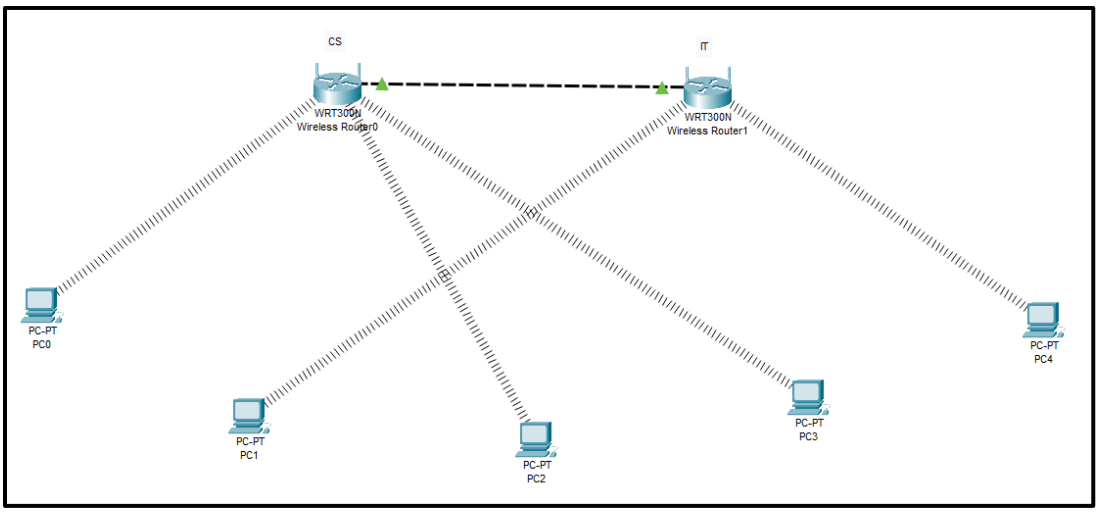
Theory: Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

Cisco Packet Tracer Setup:-

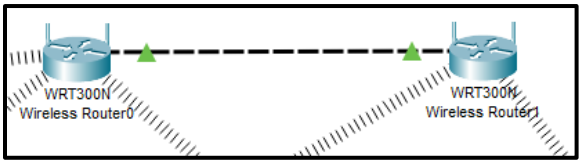


Implementation:-

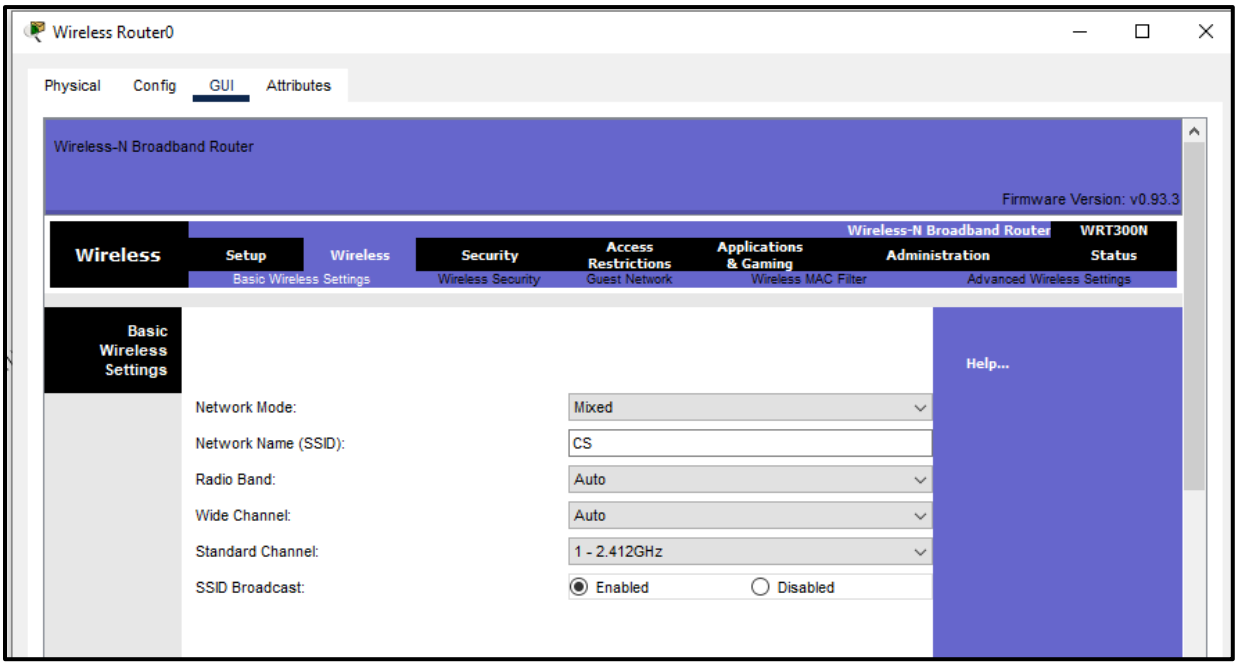
Step1: Arrange all components i.e. Wireless Router and PC's

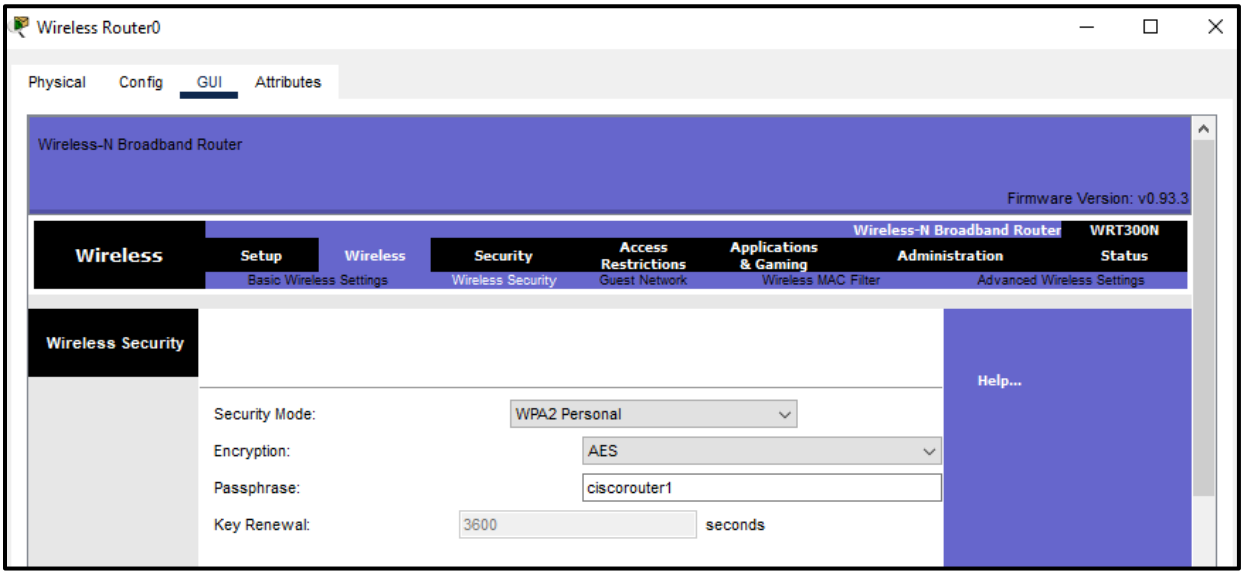


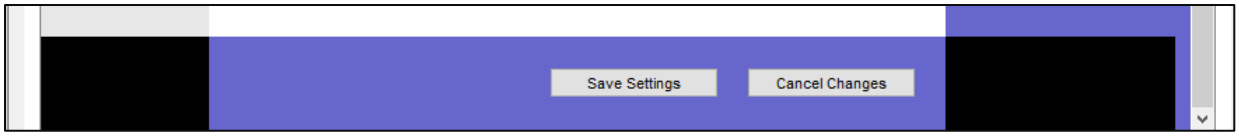
Step2: Configure wireless routers and connect both of them to each other using Ethernet ports



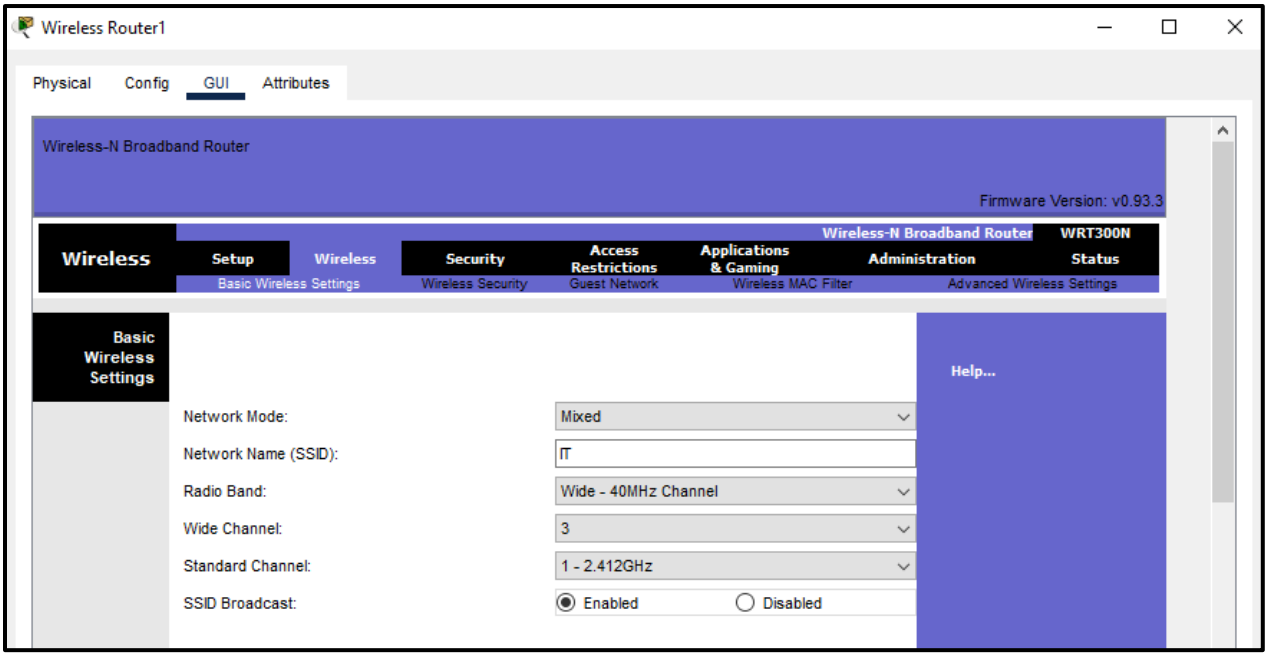
Router 1:

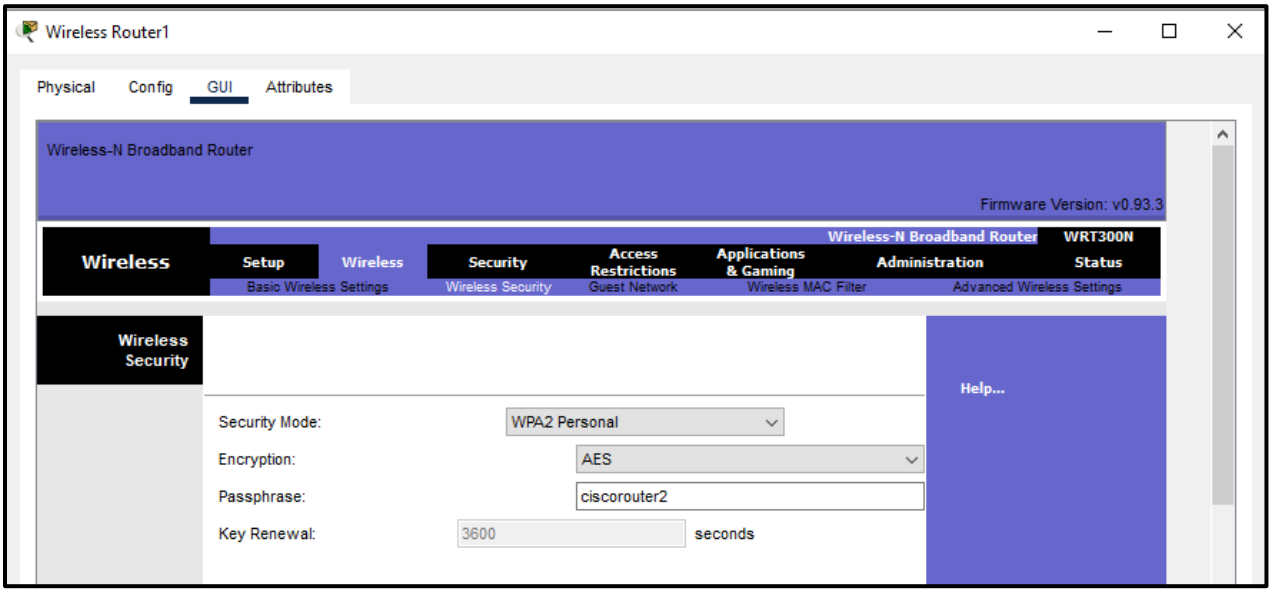





Save Settings
Cancel Changes

Router 2:

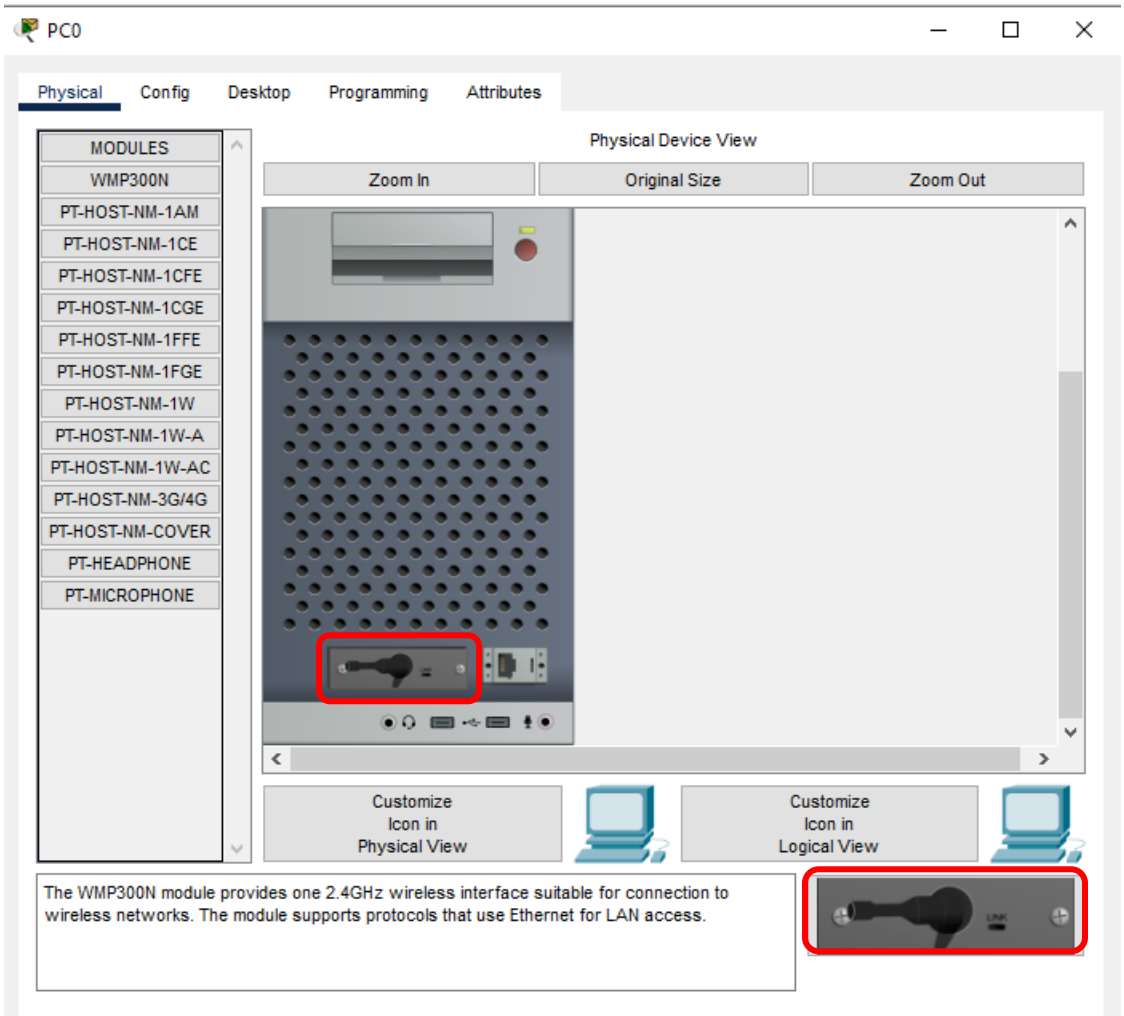

Wireless Router1
Physical
Config
GUI
Attributes
Wireless-N Broadband Router
Firmware Version: v0.93.3
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Wireless-N Broadband Router
WRT300N
Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Advanced Wireless Settings
Basic Wireless Settings
Help...
Network Mode:
Mixed
Network Name (SSID):
IT
Radio Band:
Wide - 40MHz Channel
Wide Channel:
3
Standard Channel:
1 - 2.412GHz
SSID Broadcast:
Enabled
Disabled


Wireless Router1
Physical
Config
GUI
Attributes
Wireless-N Broadband Router
Firmware Version: v0.93.3
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Wireless-N Broadband Router
WRT300N
Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Advanced Wireless Settings
Wireless Security
Help...
Security Mode:
WPA2 Personal
Encryption:
AES
Passphrase:
ciscorouter2
Key Renewal:
3600
seconds


Save Settings
Cancel Changes

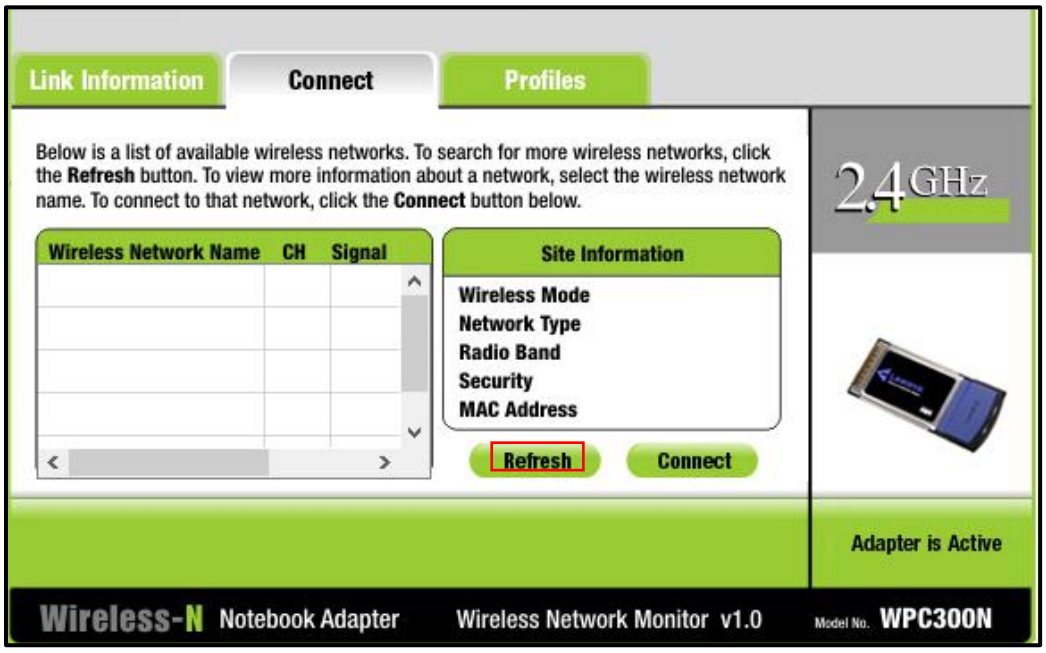
Step3: Connect all machines/devices (PC's) to respective router as per our requirements.

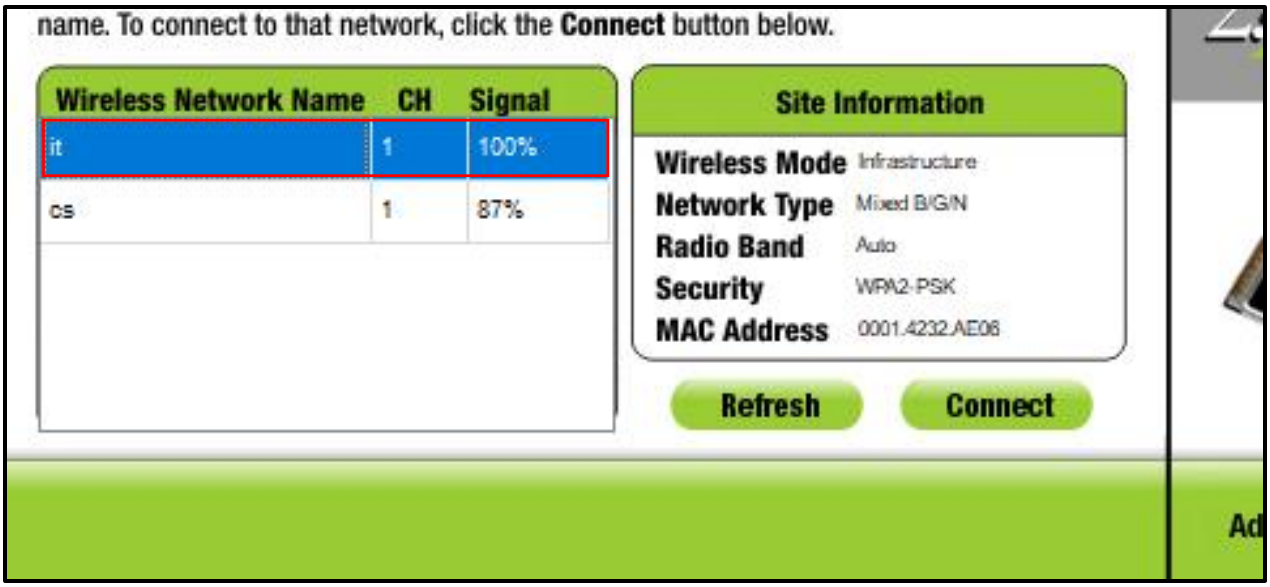
Change the Port of all pc's with wireless adapter

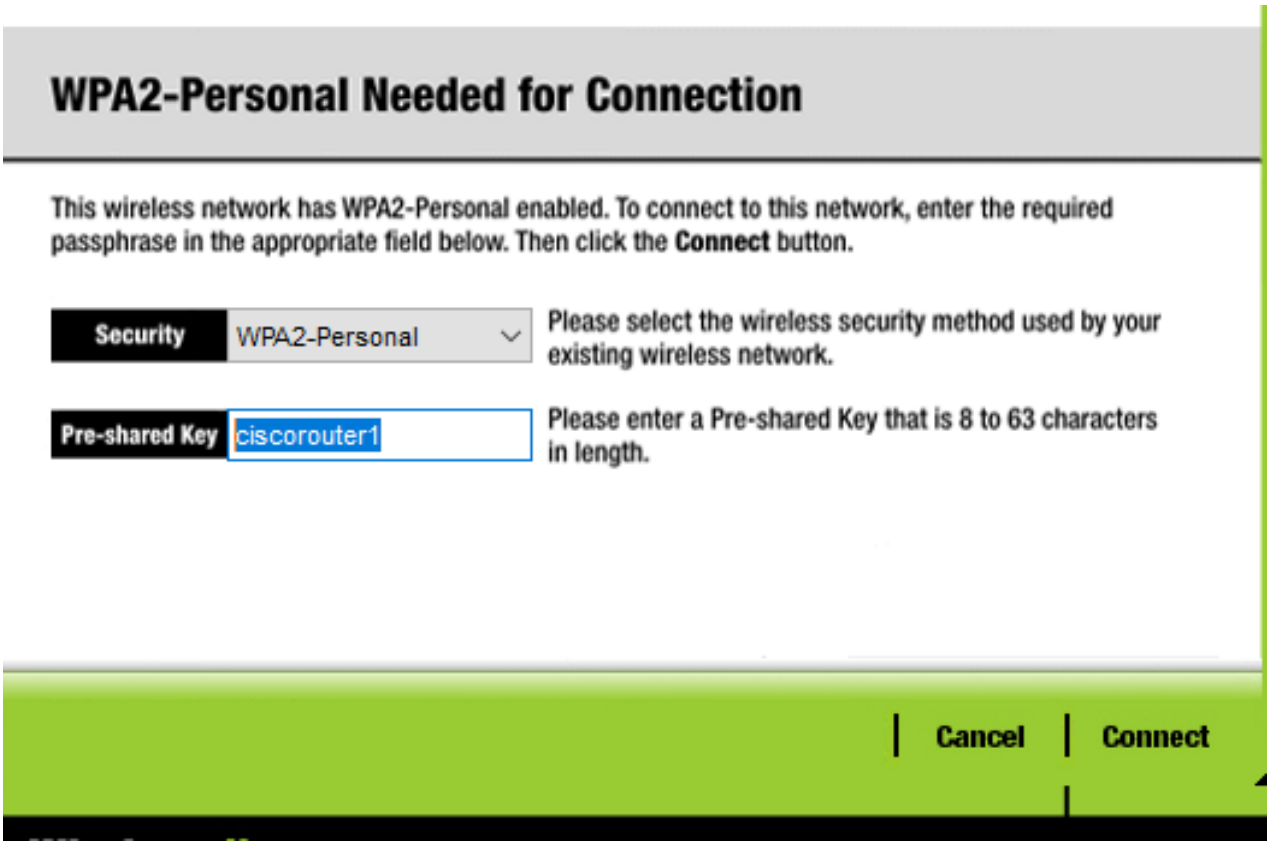


Configure Wireless connection


PC0
Physical
Config
Desktop
Programming
Attributes
Link Information
Connect
Profiles
More Information
Infrastructure Mode
2.4GHz
You have successfully connected to the access point
Signal Strength
Link Quality
Adapter is Active
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N

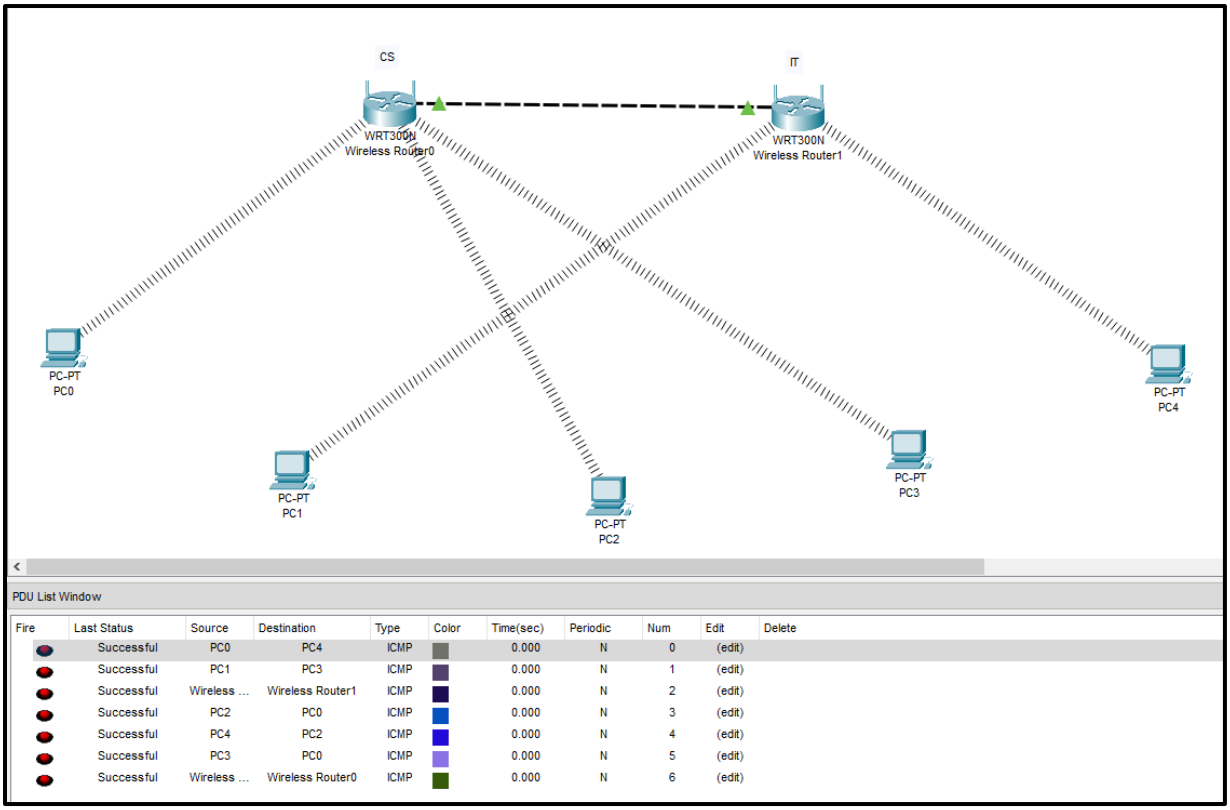

Link Information
Connect
Profiles
Below is a list of available wireless networks. To search for more wireless networks, click the Refresh button. To view more information about a network, select the wireless network name. To connect to that network, click the Connect button below.
2.4GHz
Wireless Network Name
CH
Signal
Site Information
Wireless Mode
Network Type
Radio Band
Security
MAC Address
Refresh
Connect
Adapter is Active
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N





Do similar configuration to all respective PC's

Step4: Check the Connection



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC4	ICMP		0.000	N	0	(edit)	
	Successful	PC1	PC3	ICMP		0.000	N	1	(edit)	
	Successful	Wireless ...	Wireless Router1	ICMP		0.000	N	2	(edit)	
	Successful	PC2	PC0	ICMP		0.000	N	3	(edit)	
	Successful	PC4	PC2	ICMP		0.000	N	4	(edit)	
	Successful	PC3	PC0	ICMP		0.000	N	5	(edit)	
	Successful	Wireless ...	Wireless Router0	ICMP		0.000	N	6	(edit)	

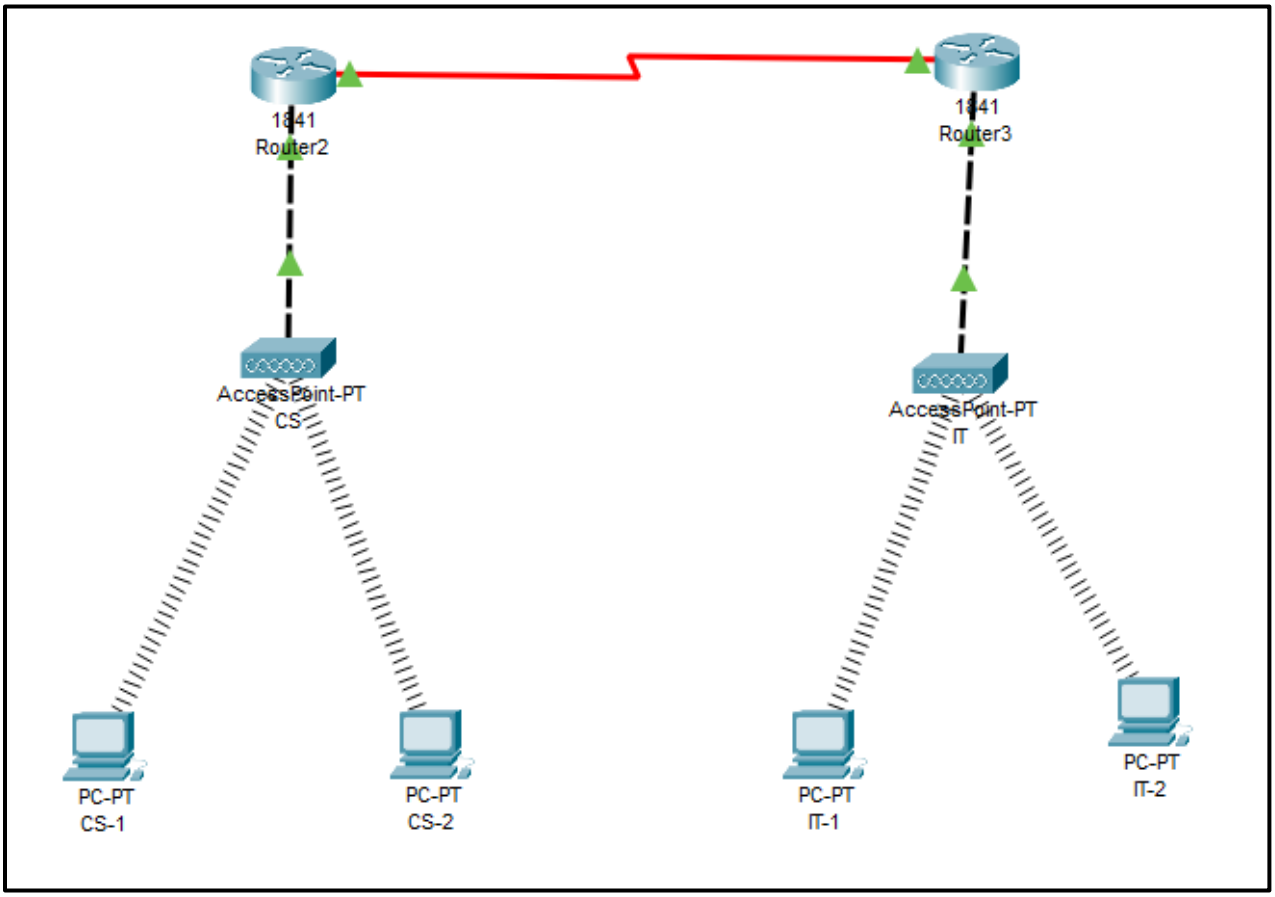
Practical No: 07

Aim: Configuring Basic AP Settings

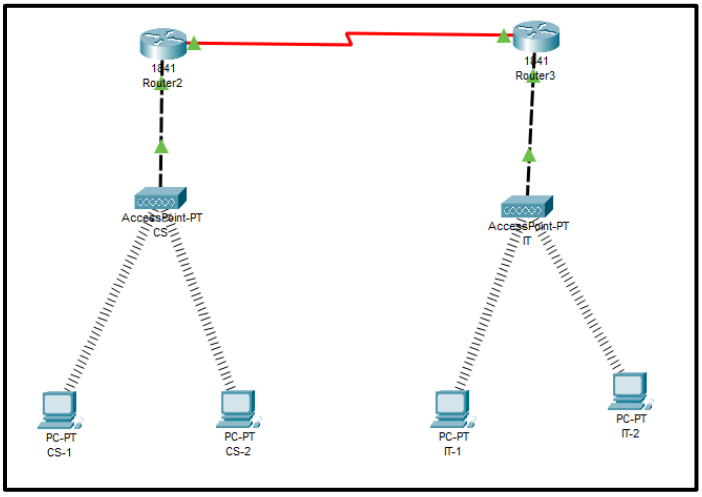
Components: Router, Access points, PC's

Theory: A wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.

Cisco Packet tracer Setup:

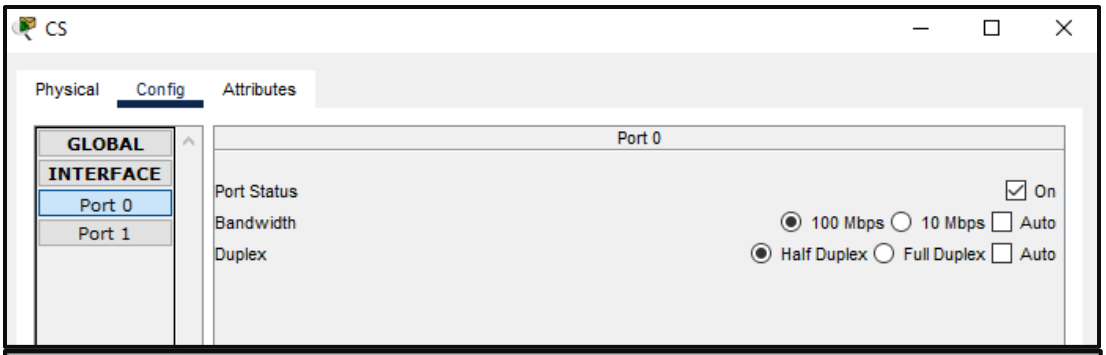


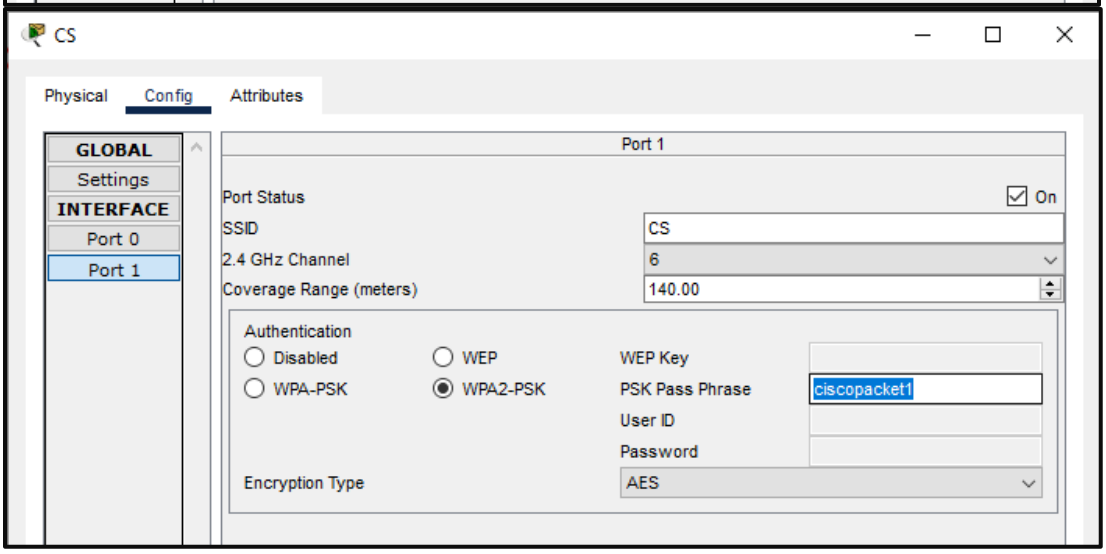
Step 1: Arrange all devices as following



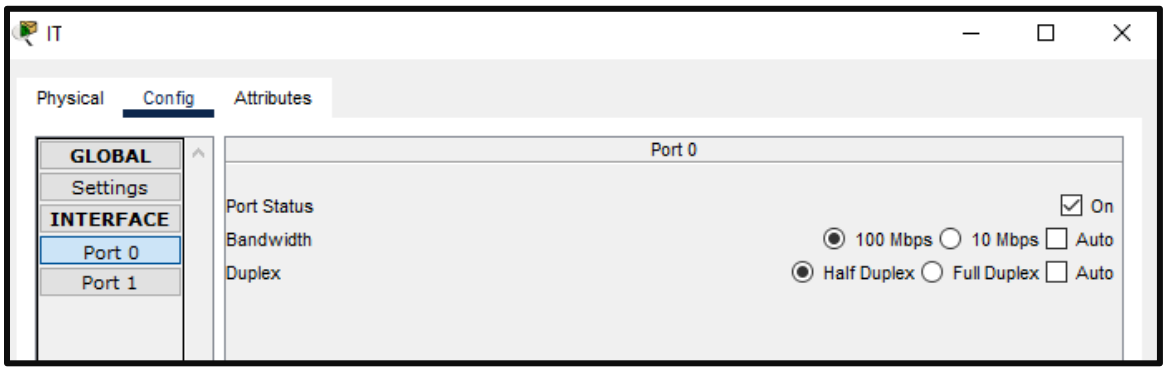
Step 2: Configure Access Points (A)

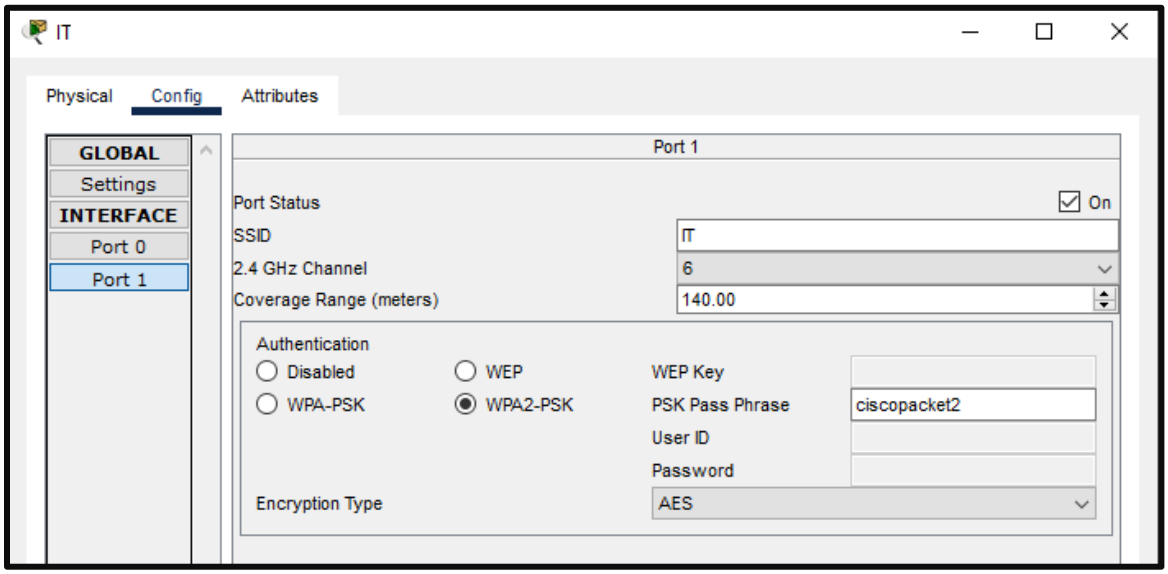
AP-1



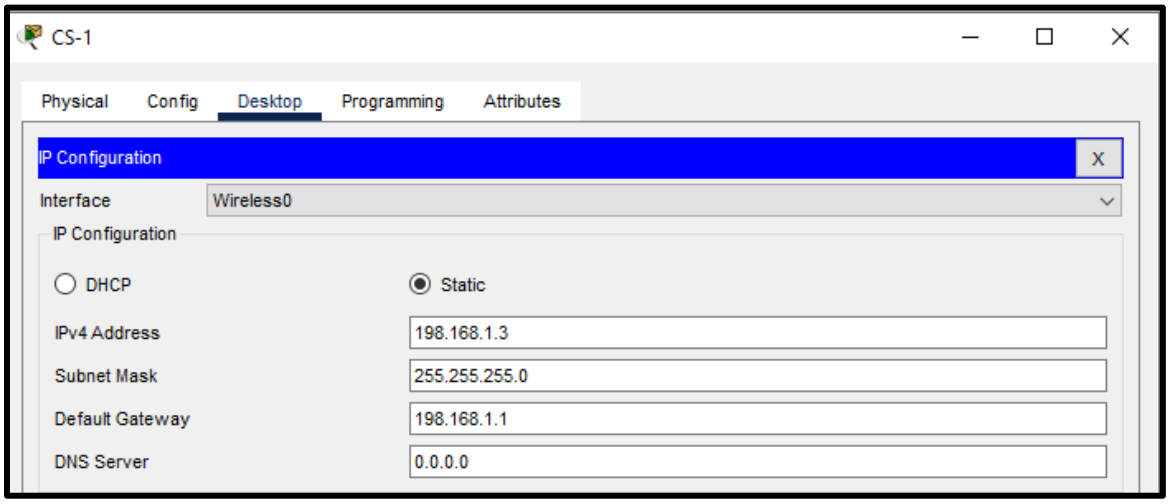


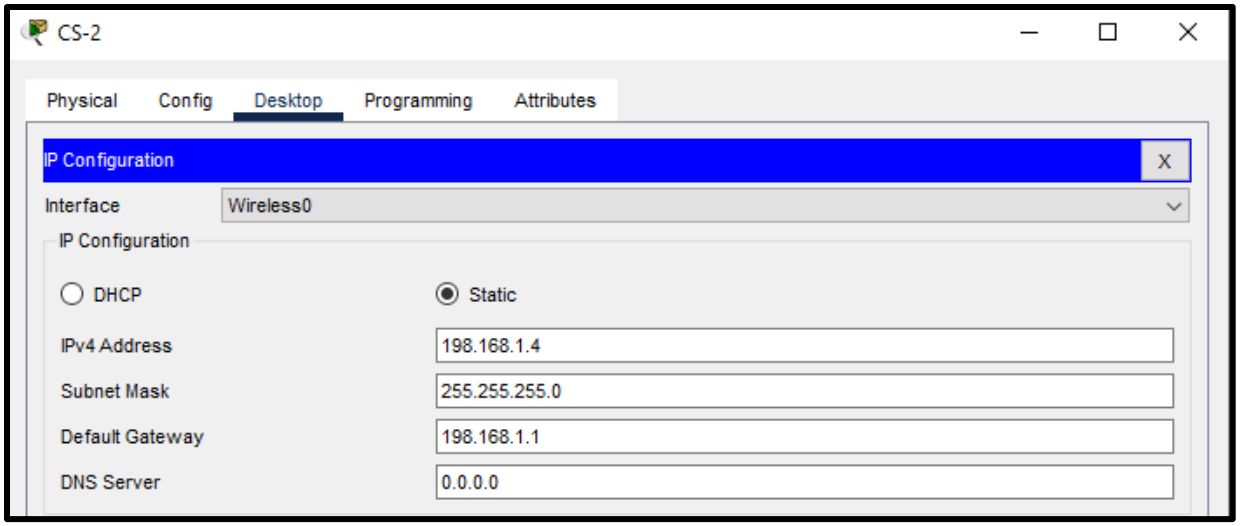
AP-2

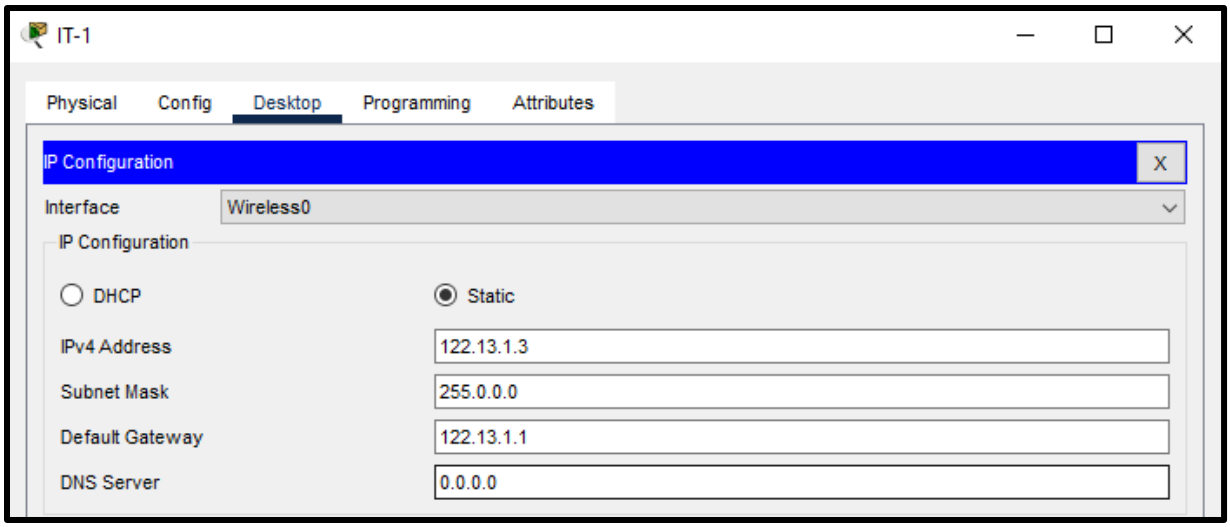


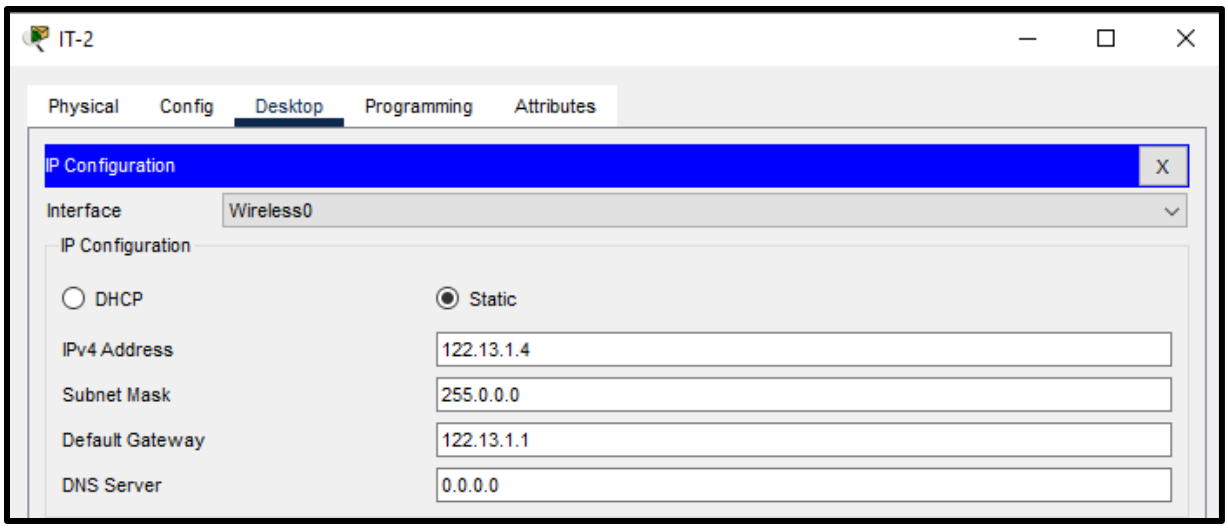


Step 3: Configure and Setup IP Address for all devices (PC's)

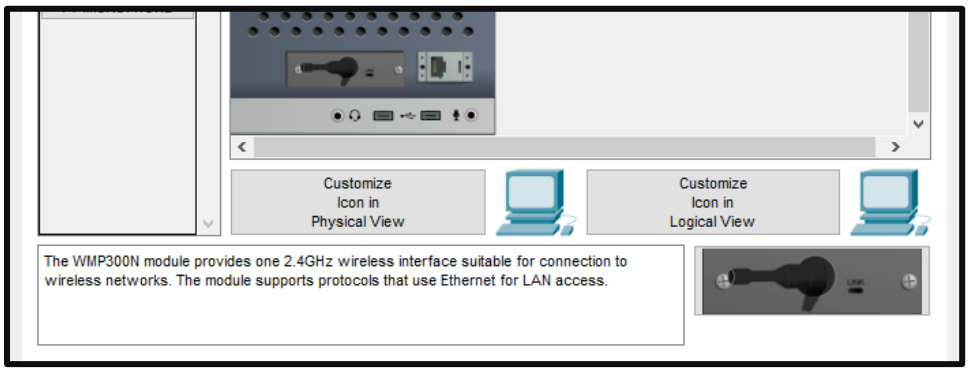



CS-2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
Wireless0
IP Configuration
DHCP
Static
IPv4 Address
198.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
198.168.1.1
DNS Server
0.0.0.0

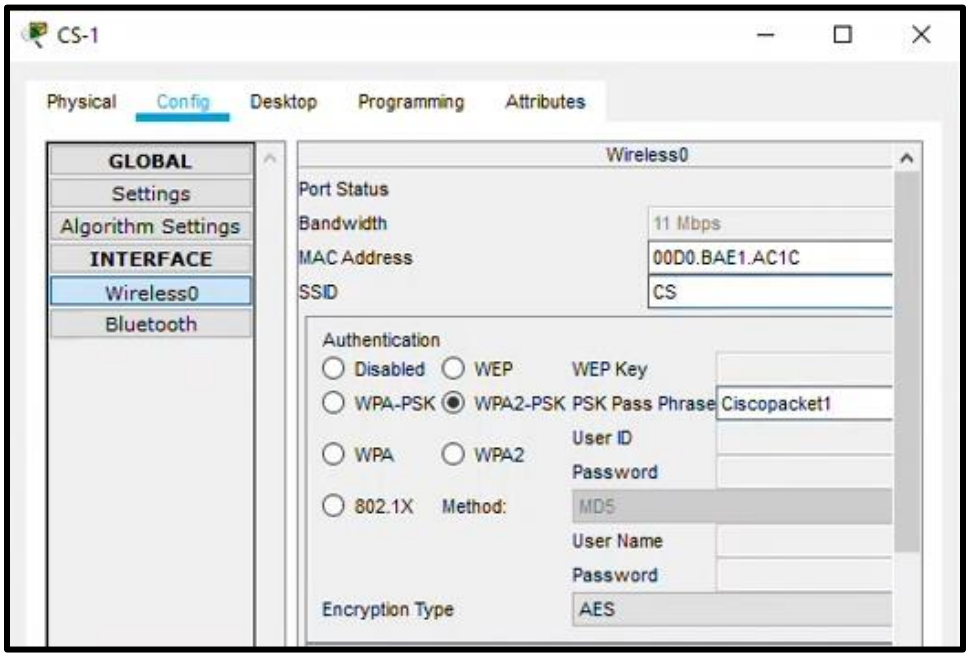

IT-1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
Wireless0
IP Configuration
DHCP
Static
IPv4 Address
122.13.1.3
Subnet Mask
255.0.0.0
Default Gateway
122.13.1.1
DNS Server
0.0.0.0

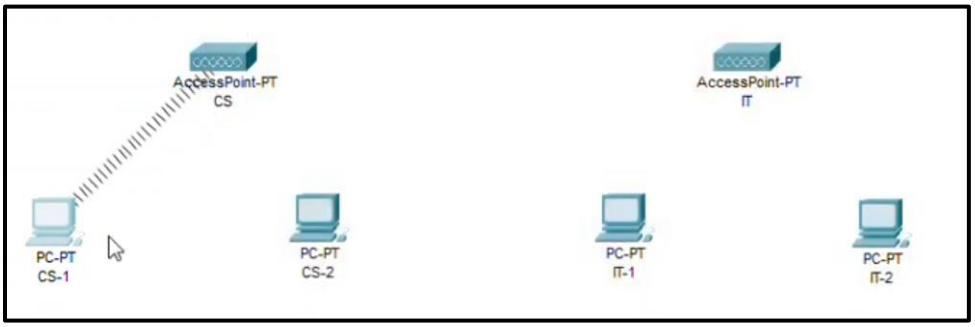

IT-2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
Wireless0
IP Configuration
DHCP
Static
IPv4 Address
122.13.1.4
Subnet Mask
255.0.0.0
Default Gateway
122.13.1.1
DNS Server
0.0.0.0

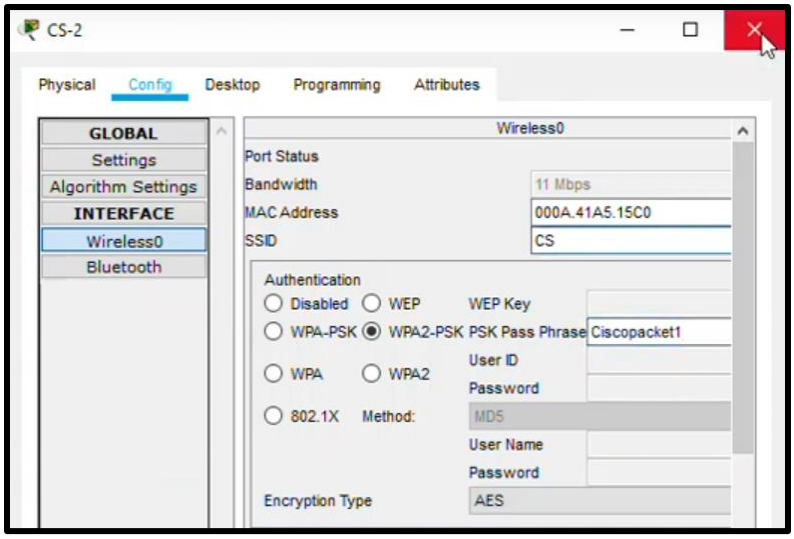
Note: Change all port adapters with wireless adapter for all PC's

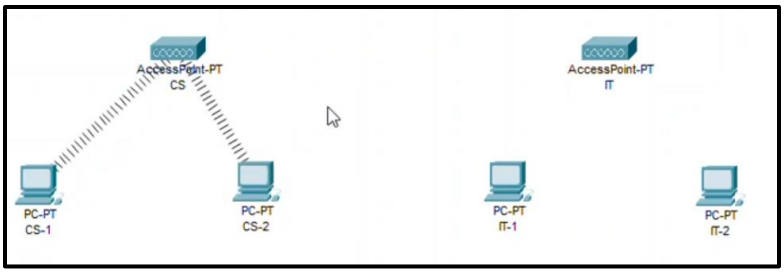


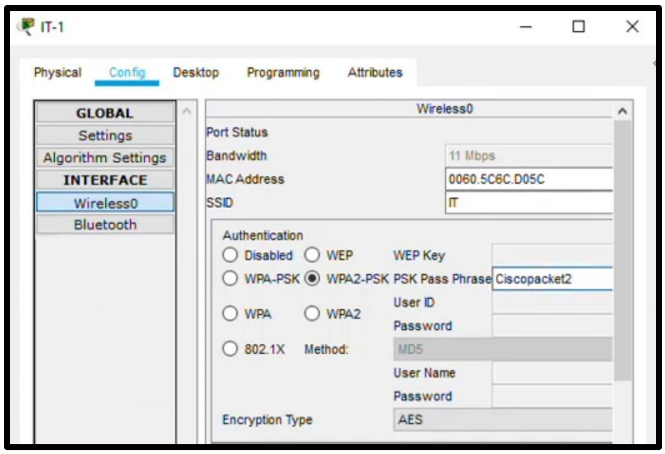
Step 4: Configure Access points with PC's



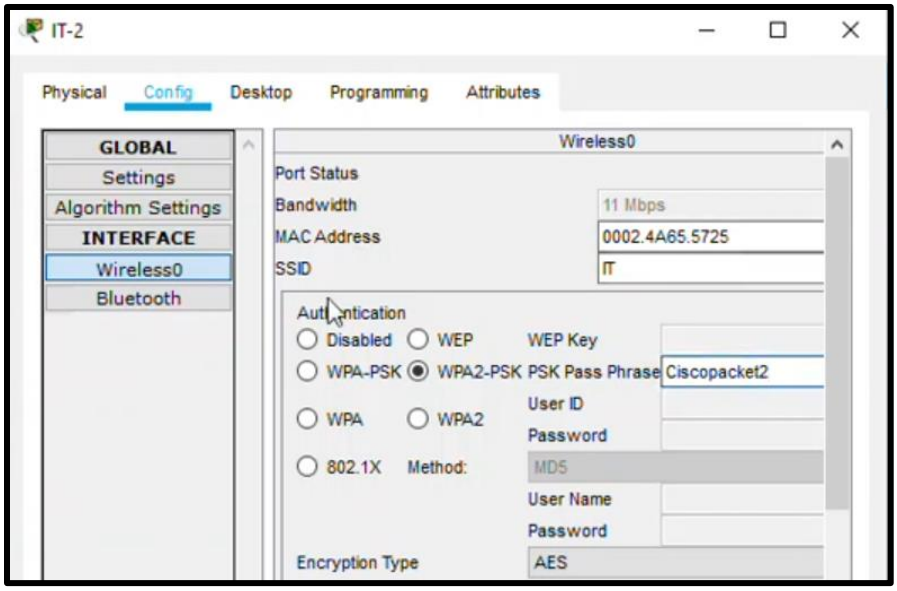


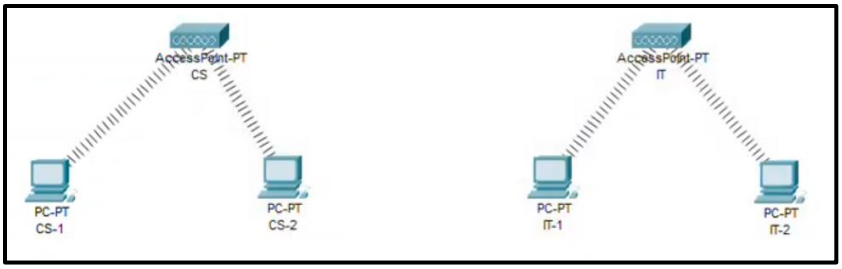

CS-2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
Bandwidth
11 Mbps
MAC Address
000A.41A5.15C0
SSID
CS
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
Ciscopacket1
User ID
WPA
WPA2
Password
802.1X
Method:
MD5
User Name
Password
Encryption Type
AES


AccessPoint-PT
CS
AccessPoint-PT
IT
PC-PT
CS-1
PC-PT
CS-2
PC-PT
IT-1
PC-PT
IT-2

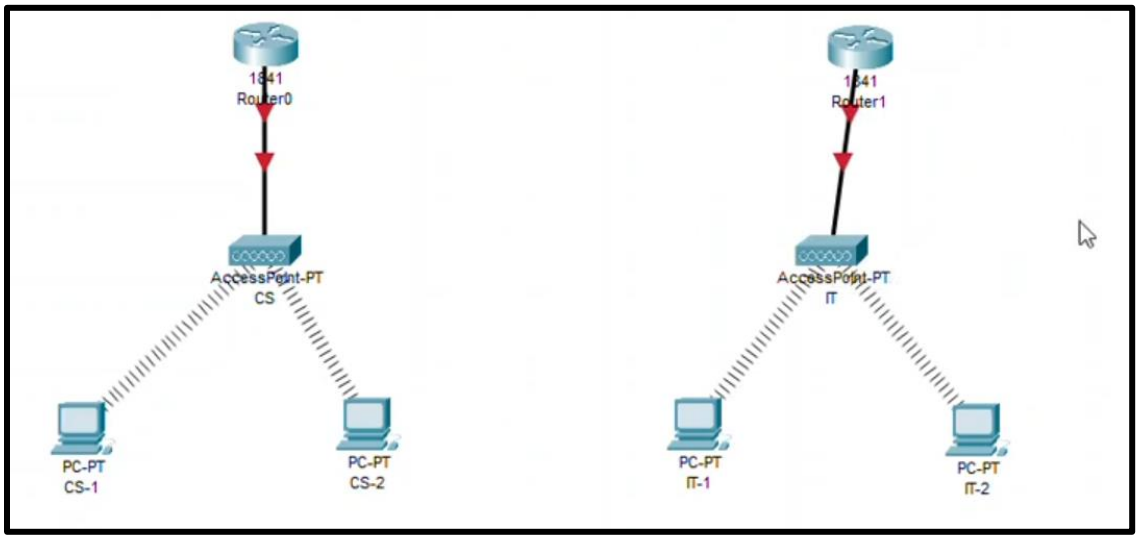

IT-1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
Bandwidth
11 Mbps
MAC Address
0060.5C6C.D05C
SSID
IT
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
Ciscopacket2
User ID
WPA
WPA2
Password
802.1X
Method:
MD5
User Name
Password
Encryption Type
AES

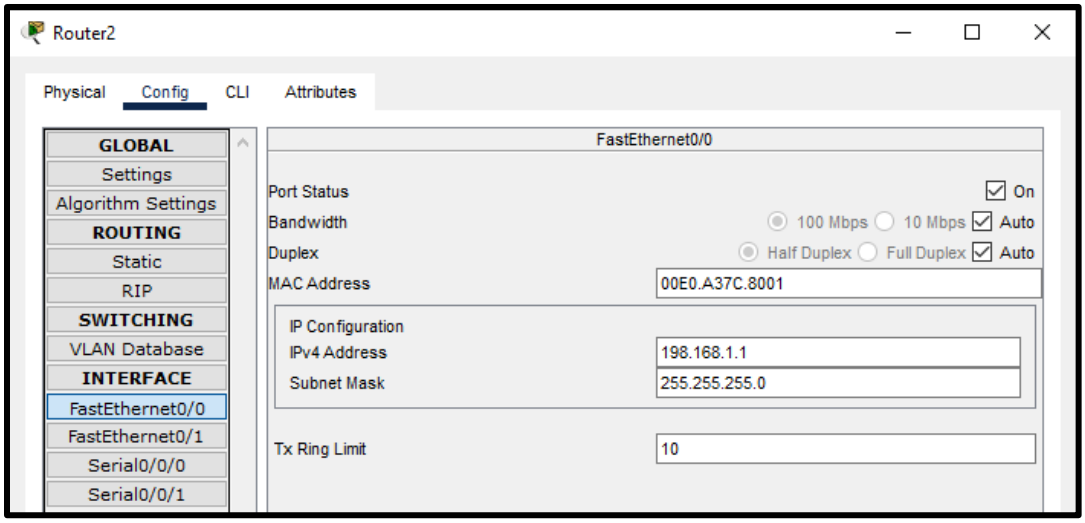

AccessPoint-PT
CS
AccessPoint-PT
IT
PC-PT
CS-1
PC-PT
CS-2
PC-PT
IT-1
PC-PT
IT-2

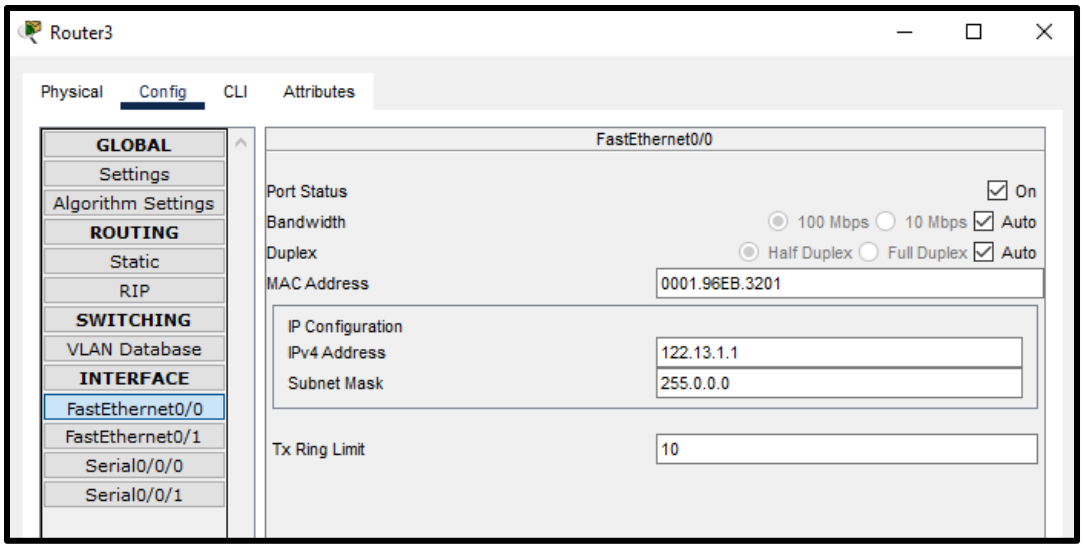




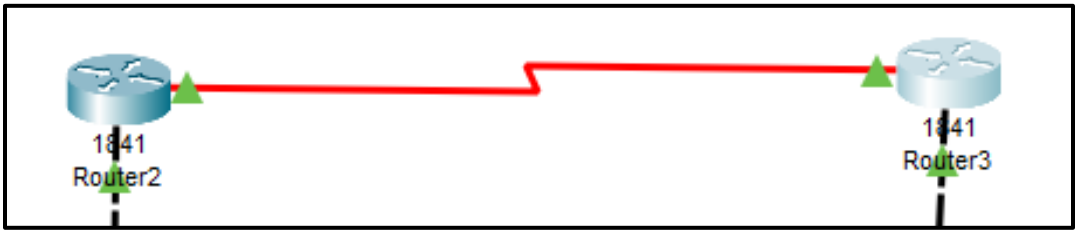
Step 5: Connect routers with Access points and configure them

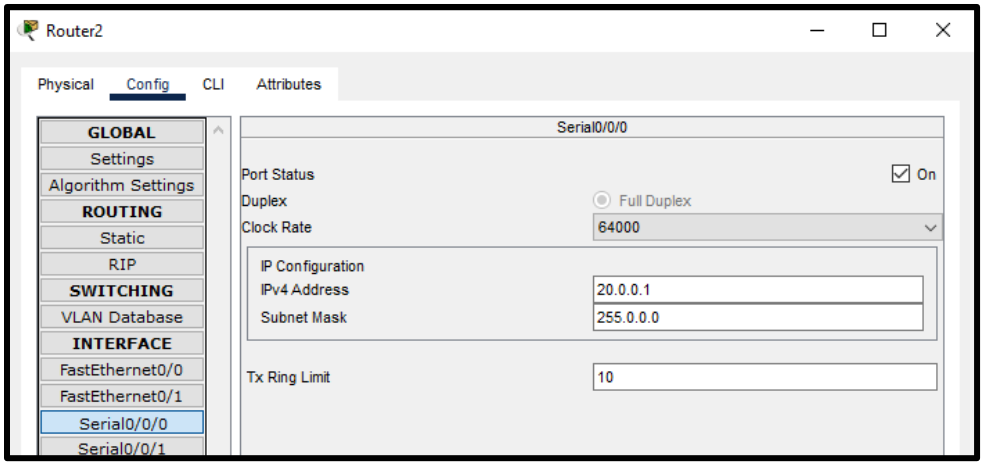


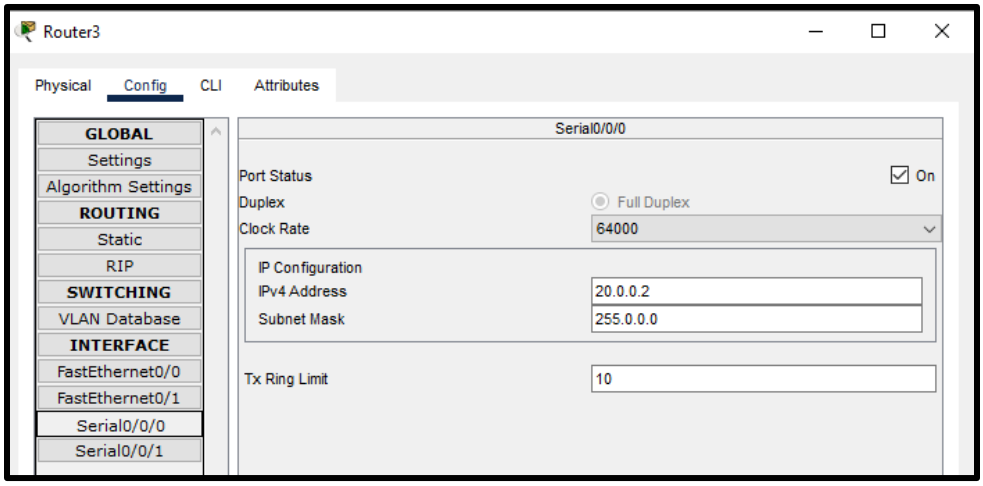


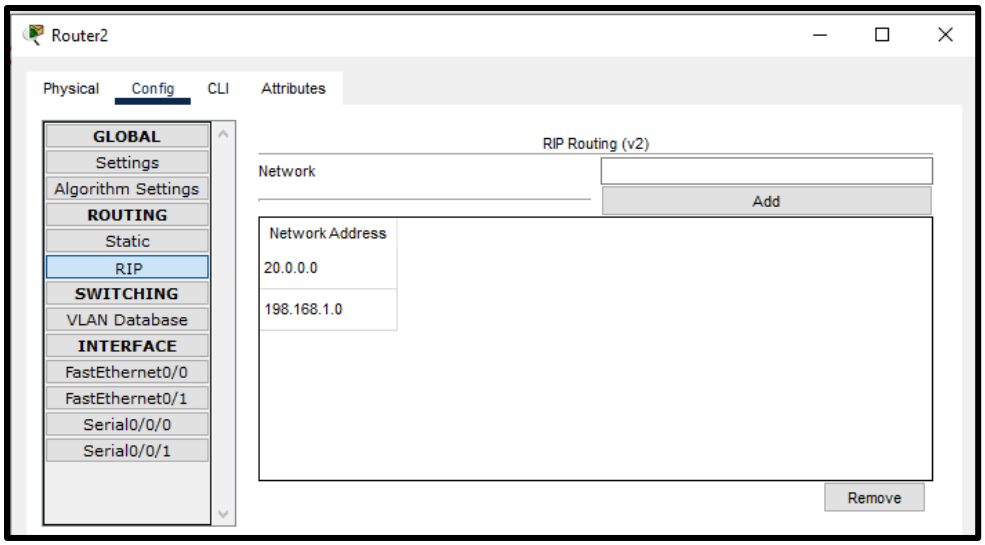


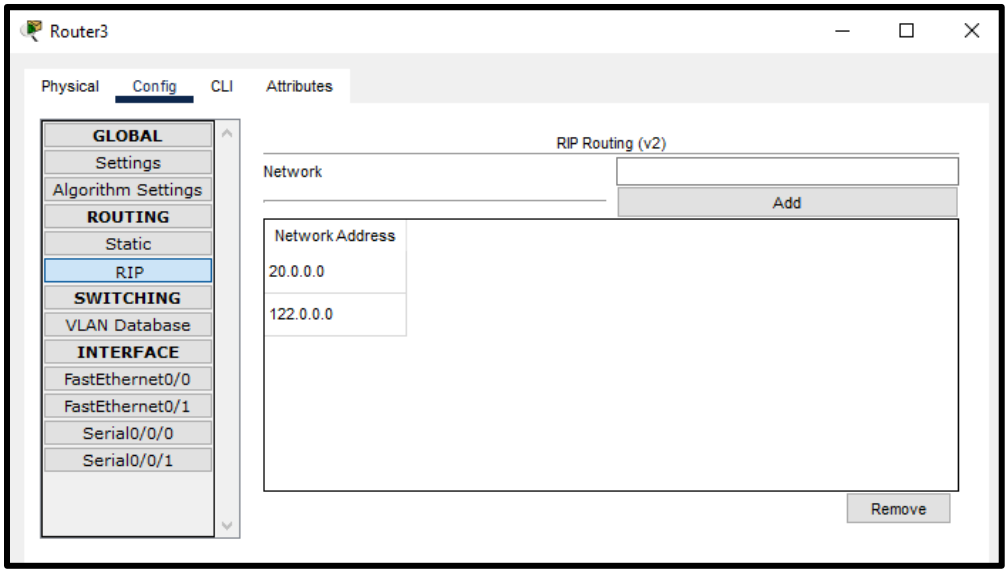
Connect Routers with serial ports and configure



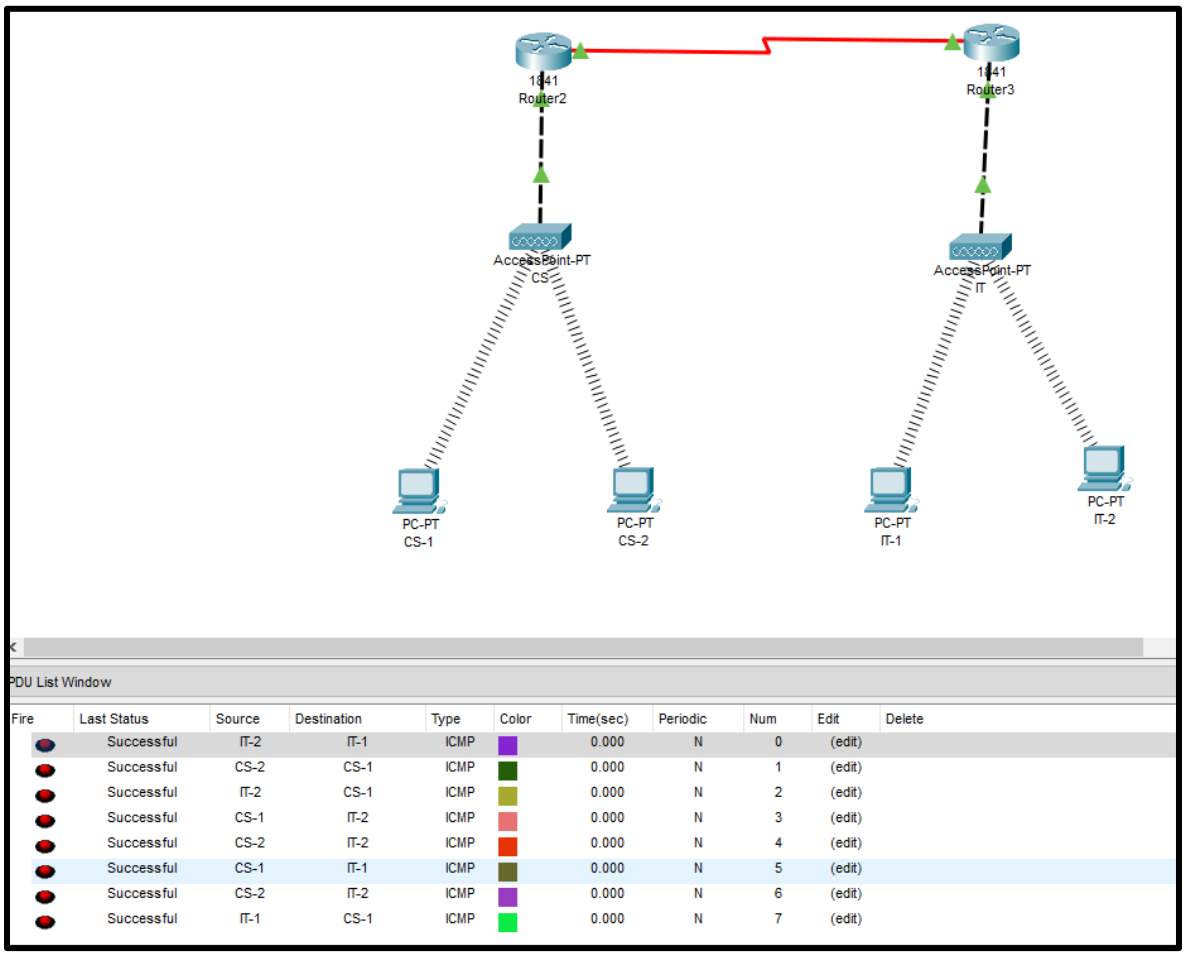

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
64000
IP Configuration
IPv4 Address
20.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
64000
IP Configuration
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
RIP Routing (v2)
Network
Add
Network Address
20.0.0.0
198.168.1.0
Remove



Step 6: Check the connection



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	IT-2	IT-1	ICMP		0.000	N	0	(edit)	
	Successful	CS-2	CS-1	ICMP		0.000	N	1	(edit)	
	Successful	IT-2	CS-1	ICMP		0.000	N	2	(edit)	
	Successful	CS-1	IT-2	ICMP		0.000	N	3	(edit)	
	Successful	CS-2	IT-2	ICMP		0.000	N	4	(edit)	
	Successful	CS-1	IT-1	ICMP		0.000	N	5	(edit)	
	Successful	CS-2	IT-2	ICMP		0.000	N	6	(edit)	
	Successful	IT-1	CS-1	ICMP		0.000	N	7	(edit)	

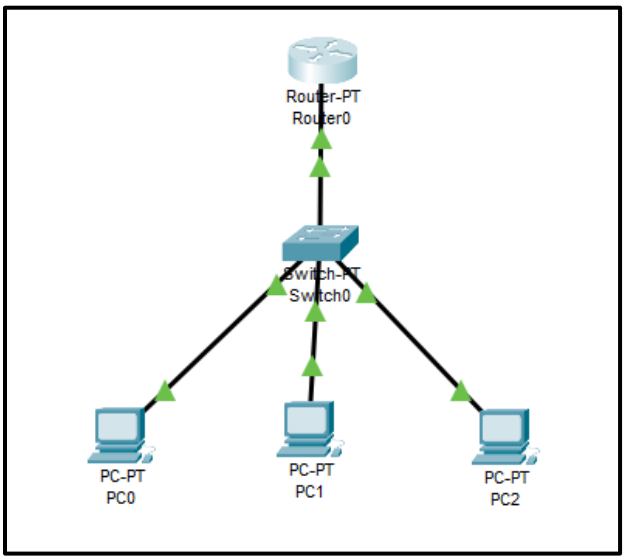
Practical No: 08

Aim: Configure fast Ethernet on router using packet tracer

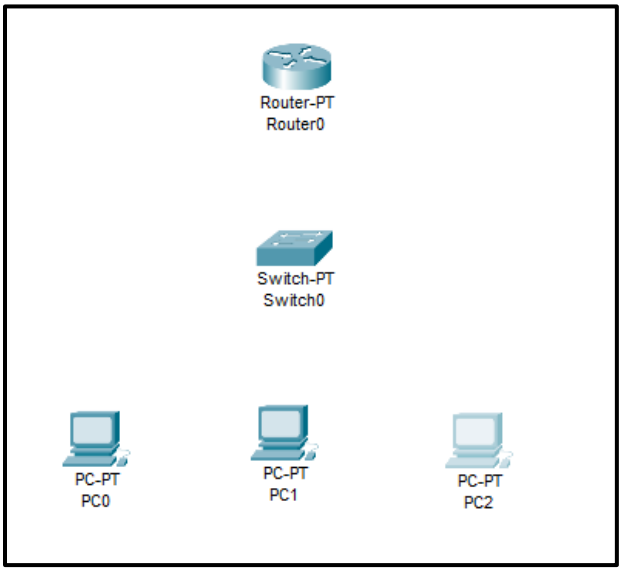
Components: Router, Switches, PC's

Theory: Fast Ethernet is used for departmental backbones, connections to high-speed servers, and connections to workstations running bandwidth-intensive software such as CAD or multimedia applications.

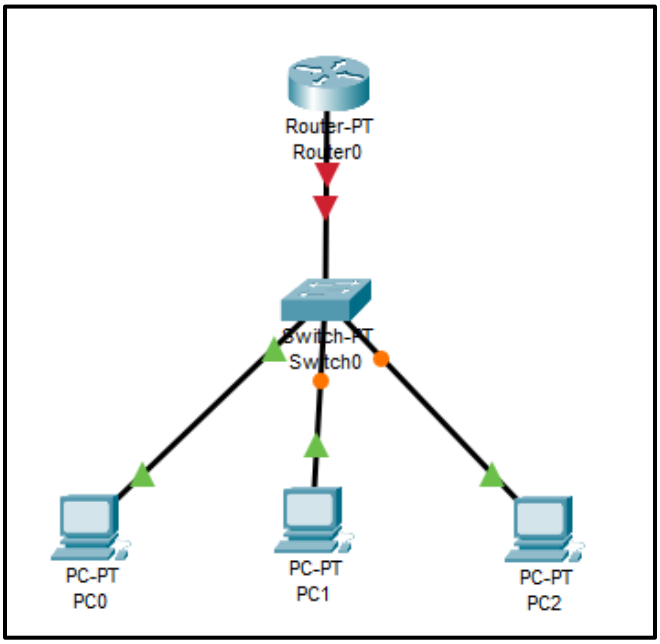
Cisco Packet tracer Setup:



Step 1: Arrange all devices



Step 2: Connect all devices using Ethernet cable



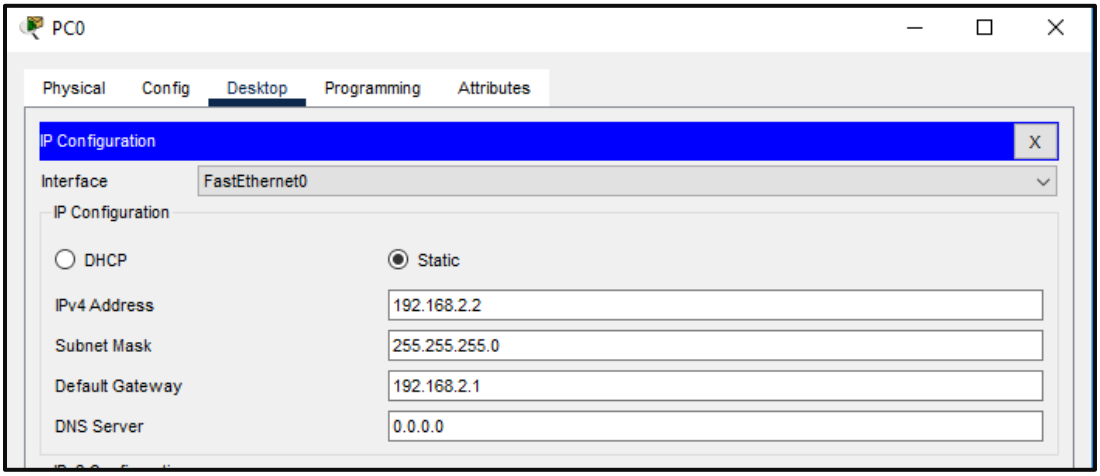
.

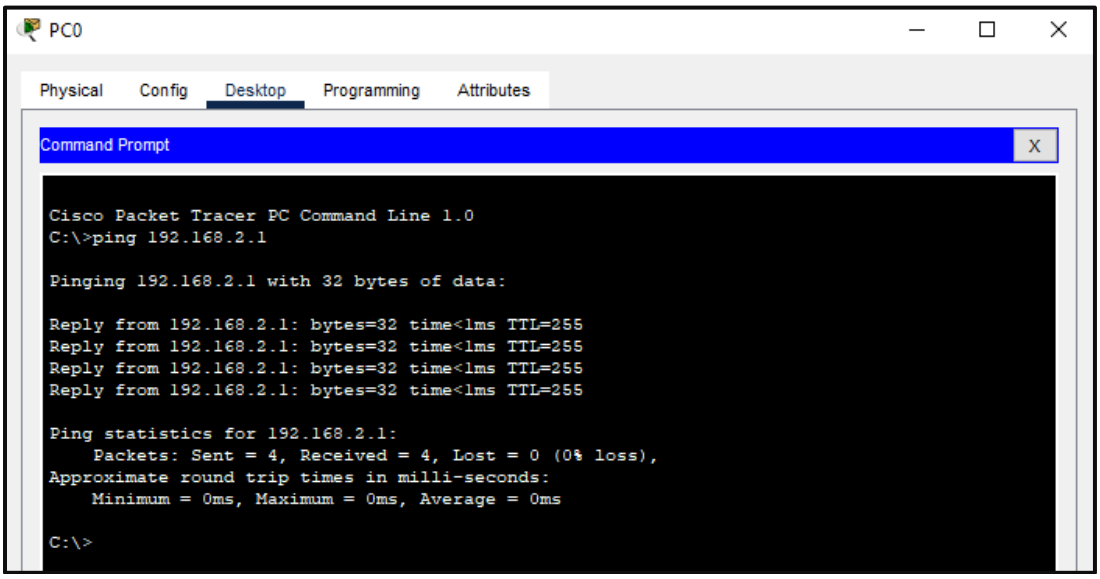
Step 3: Configure Router using CLI

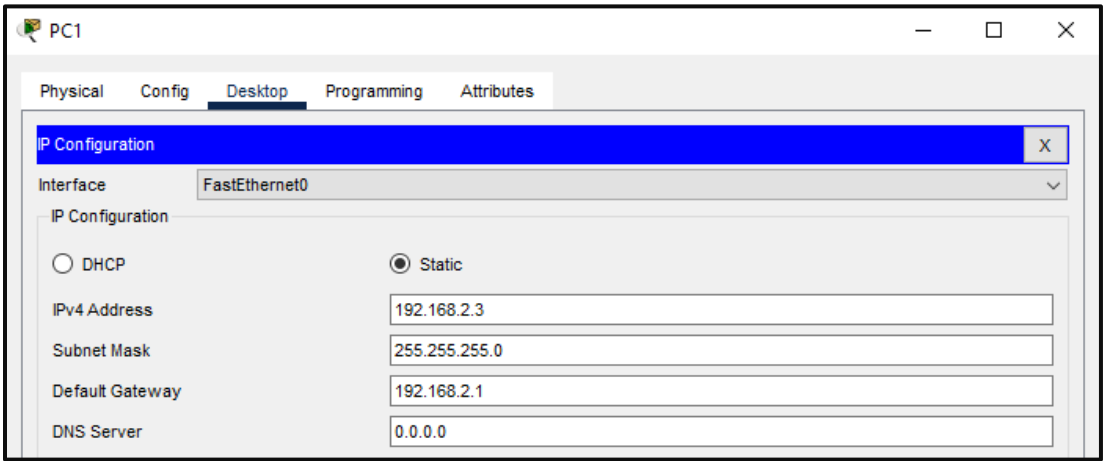
Using following commands:
configure t
hostname R1
enable password cisco
interface fa0/0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
Exit

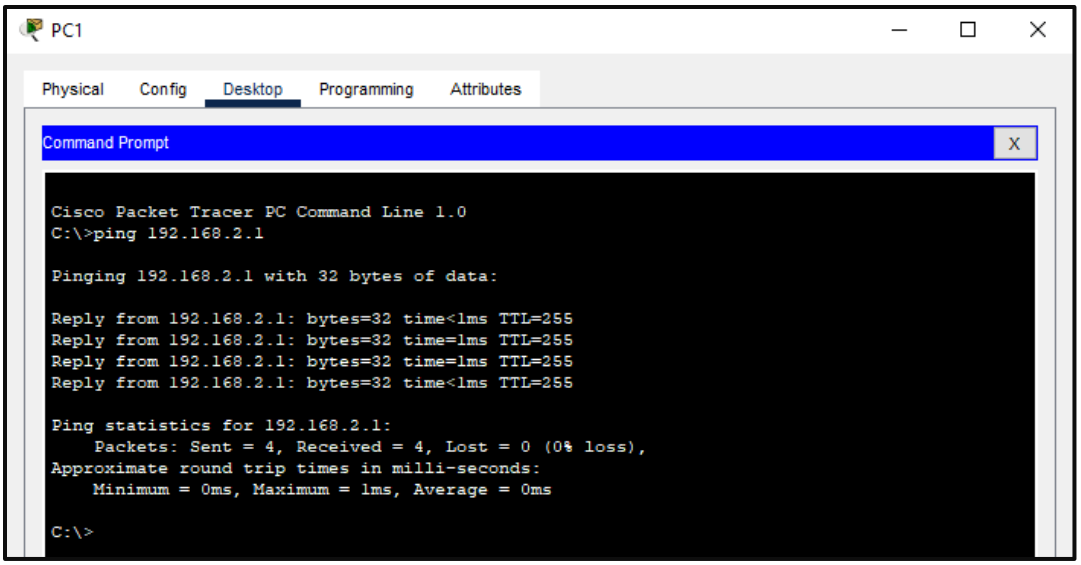
```
R1(config)#enable password cisco
R1>enable
Password:
R1#R1#R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
```

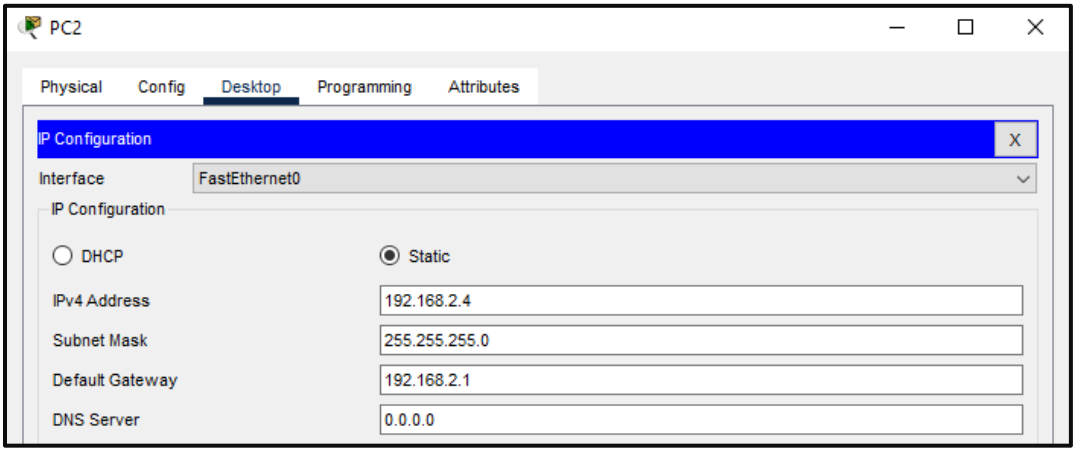
Step 4: Configure All PC's and check the connection

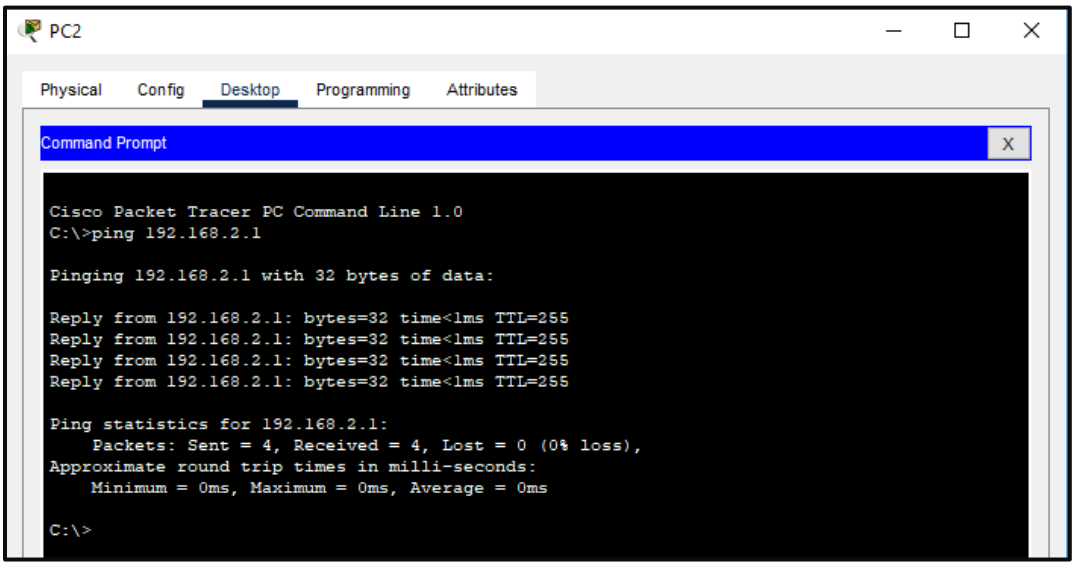




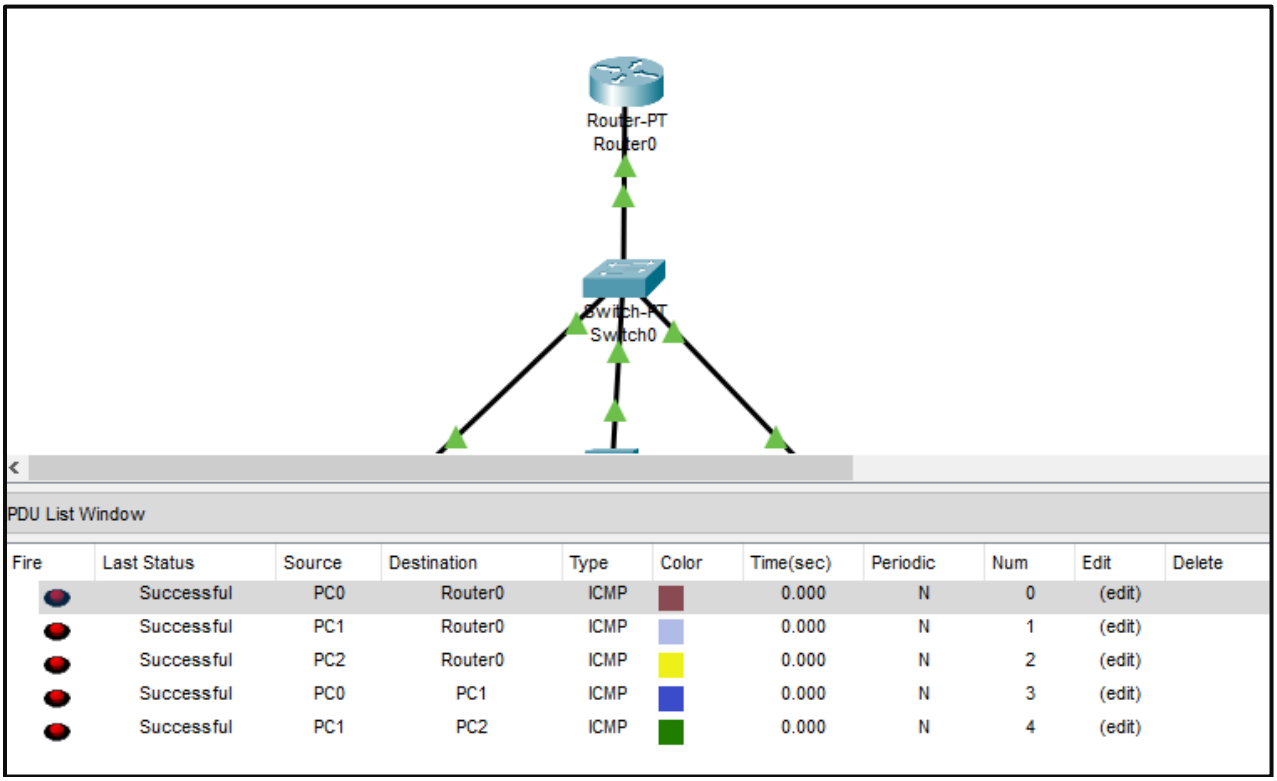



PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>


PC2
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


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

Step 5: Check the connection



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Router0	ICMP		0.000	N	0	(edit)	
	Successful	PC1	Router0	ICMP		0.000	N	1	(edit)	
	Successful	PC2	Router0	ICMP		0.000	N	2	(edit)	
	Successful	PC0	PC1	ICMP		0.000	N	3	(edit)	
	Successful	PC1	PC2	ICMP		0.000	N	4	(edit)	

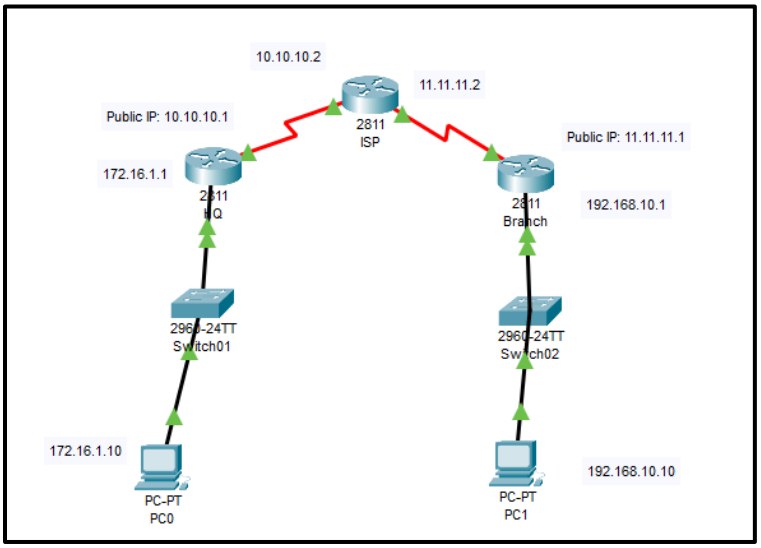
Practical No: 9

Aim: Configure Site-to-Site Wireless Link

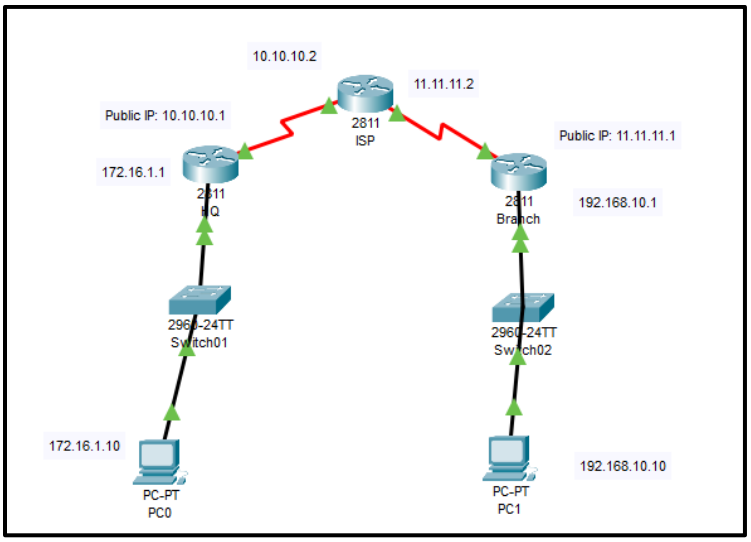
Components: Routers, Switches, Machines (PC's)

Theory: A site-to-site virtual private network (VPN) is a connection between two or more networks, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection for private traffic as an alternative to using private MPLS circuits.

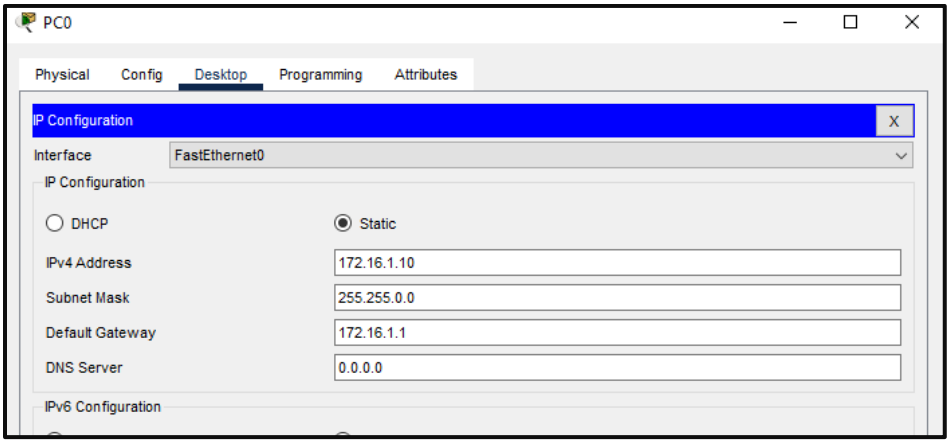
Cisco Packet tracer Setup:

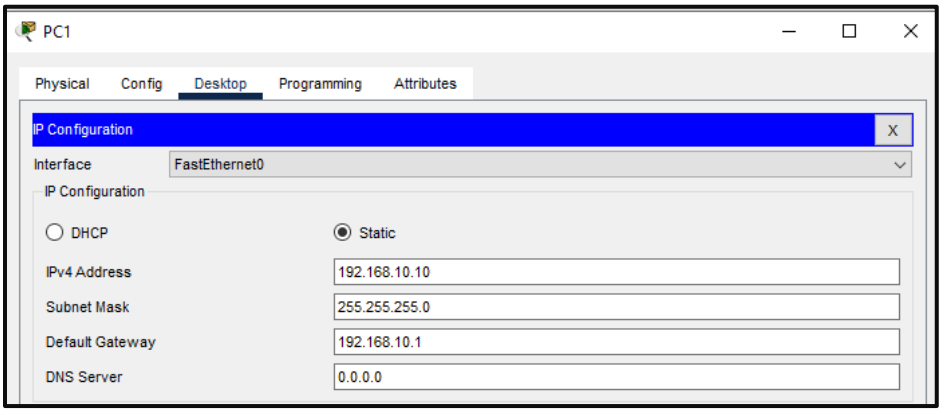


Step 1: Arrange and connect all devices/components

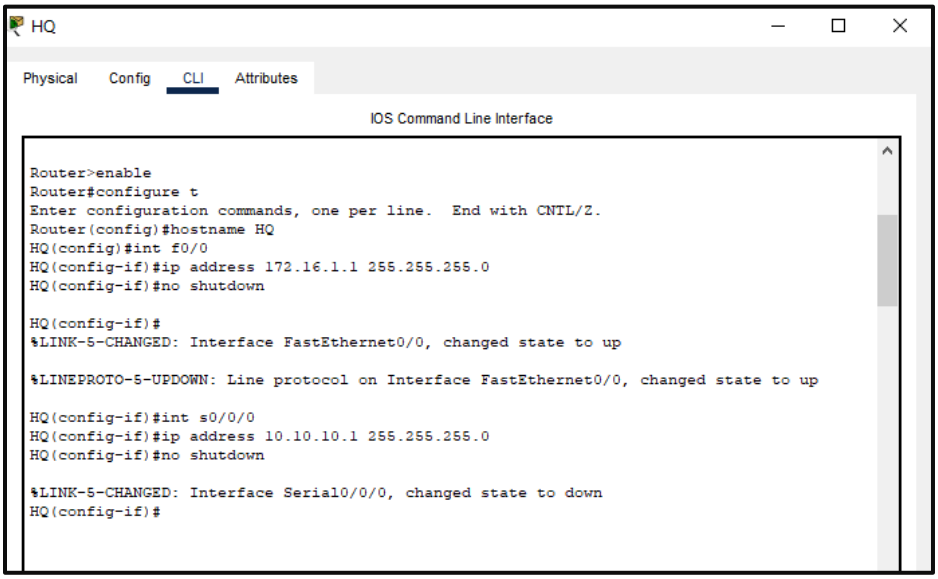


Step 2: Configure PC's





Step 3: Configure and assign Routers



Branch

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Branch
Branch(config)#int f0/0
Branch(config-if)#ip address 192.168.10.1 255.255.255.0
Branch(config-if)#no shutdown

Branch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Branch(config-if)#int s0/0/0
Branch(config-if)#ip address 11.11.11.1 255.255.255.0
Branch(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Branch(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

ISP

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#ip address 10.10.10.2 255.255.255.0
ISP(config-if)#no shutdown

ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

ISP(config-if)#int s0/0/1
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
ip address 11.11.11.2 255.255.255.0
ISP(config-if)#no shutdown

ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

ISP(config-if)#exit
ISP(config)#ip route 172.16.1.0 255.255.255.0 10.10.10.1
ISP(config)#ip route 192.168.10.0 255.255.255.0 11.11.11.1
ISP(config)#
```

Step 4: Configure default router on HQ and Branch and static router from ISP

HQ

Physical Config CLI Attributes

IOS Command Line Interface

```
HQ>en
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
HQ(config)#
```

Branch

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Branch(config-if)#
Branch(config-if)#ip route 0.0.0.0 0.0.0.0 11.11.11.2
Branch(config)#exit
Branch#
%SYS-5-CONFIG_I: Configured from console by console
```

ISP

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

ISP(config-if)#exit
ISP(config)#ip route 172.16.1.0 255.255.255.0 10.10.10.1
ISP(config)#ip route 192.168.10.0 255.255.255.0 11.11.11.1
ISP(config)#
```

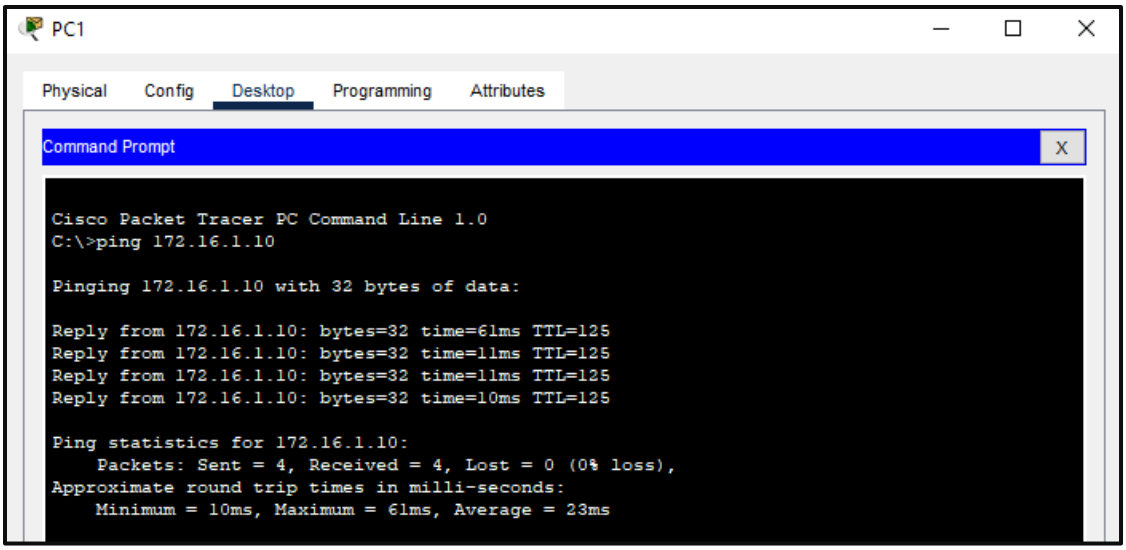
Step 5: Check the connection

PC0

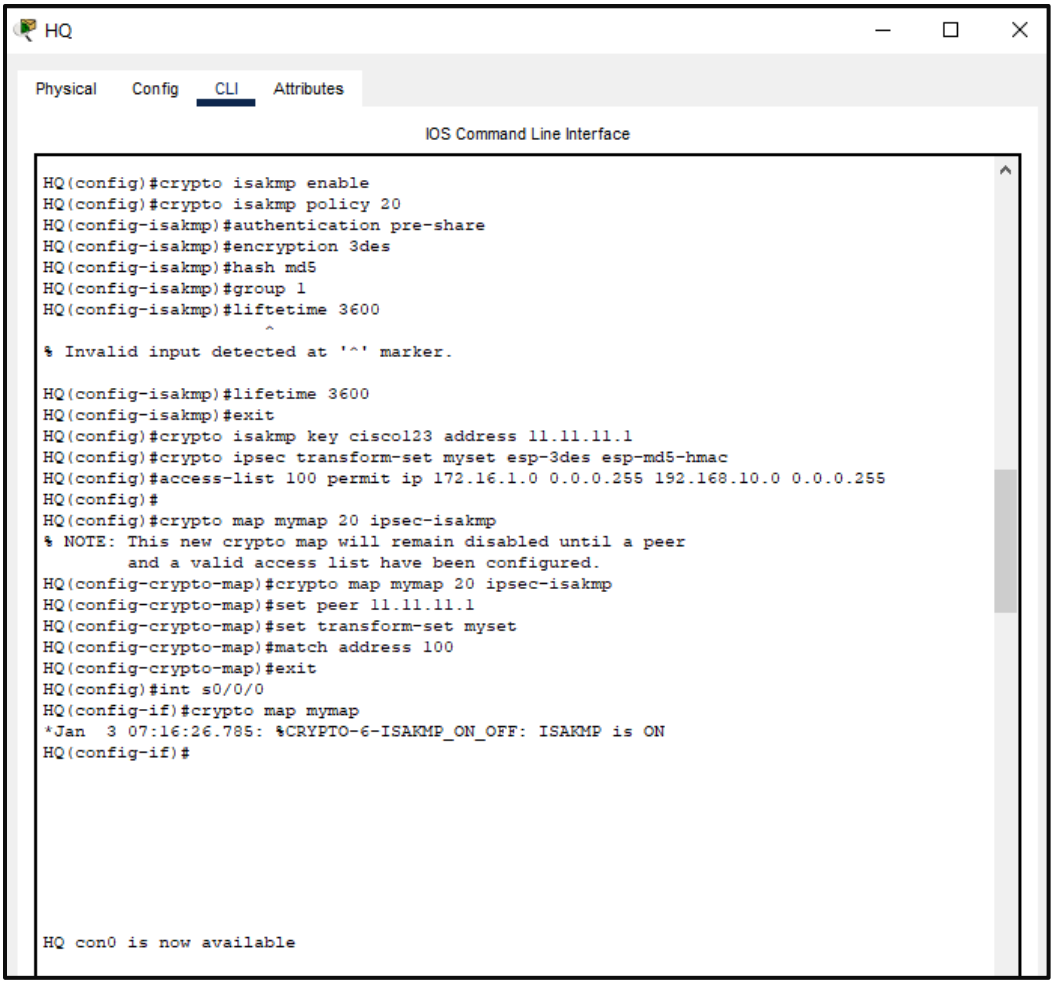
Physical Config Desktop Programming Attributes

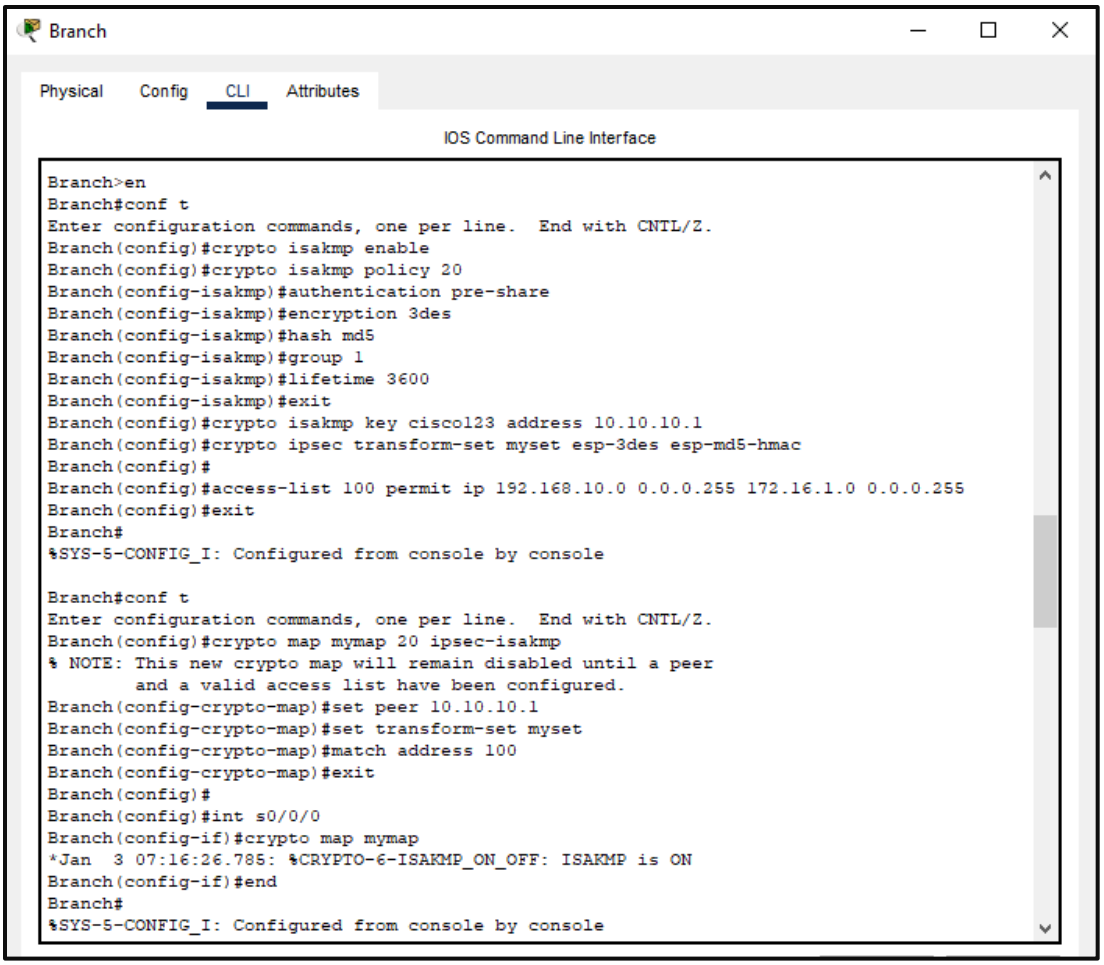
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=57ms TTL=125
Reply from 192.168.10.10: bytes=32 time=11ms TTL=125
Reply from 192.168.10.10: bytes=32 time=3ms TTL=125
Reply from 192.168.10.10: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 57ms, Average = 20ms
```

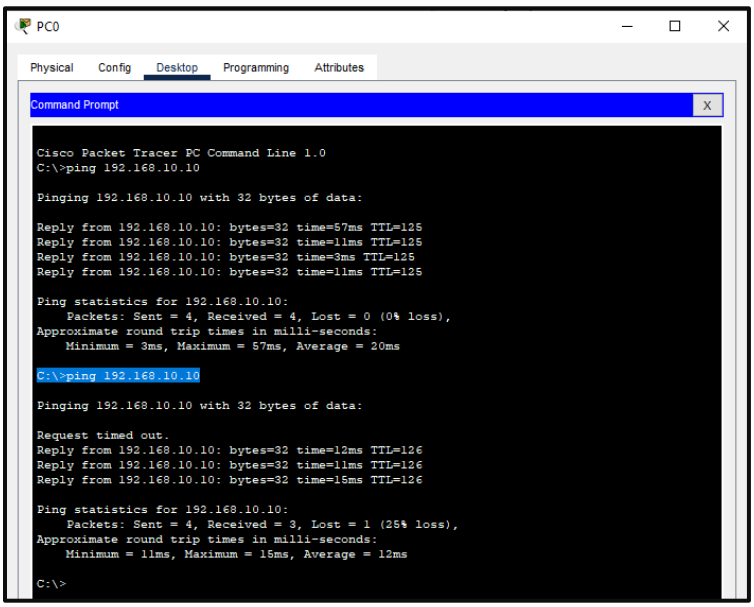


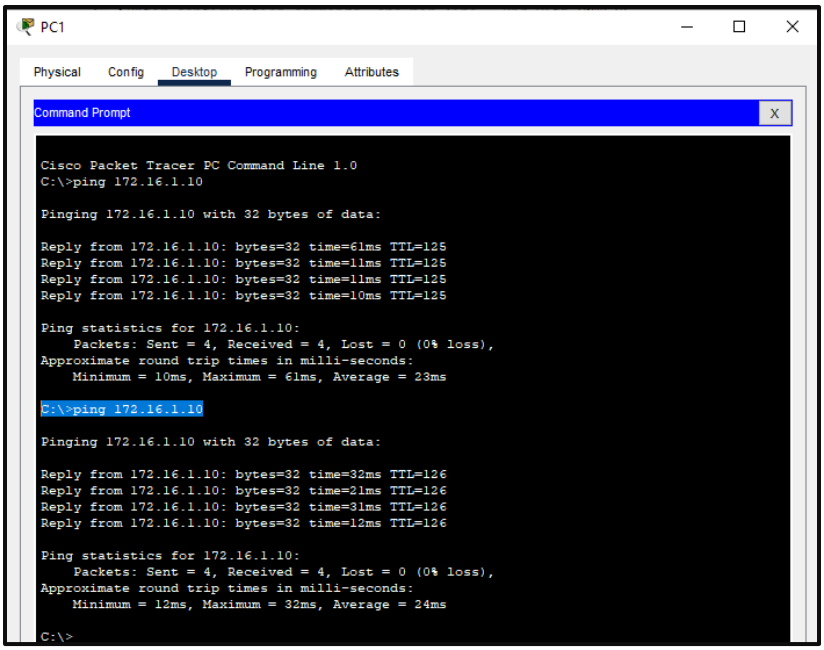
Step 6: Configure site-to-site VPN connection



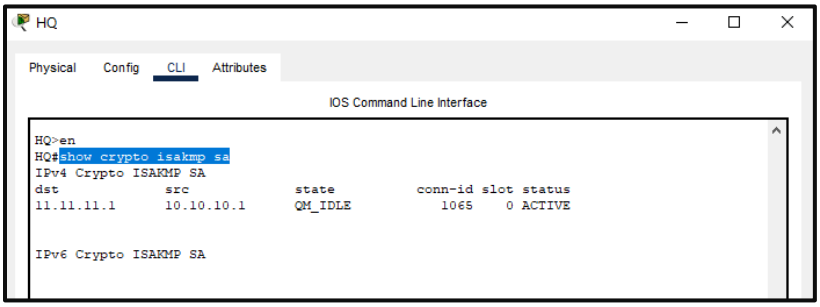


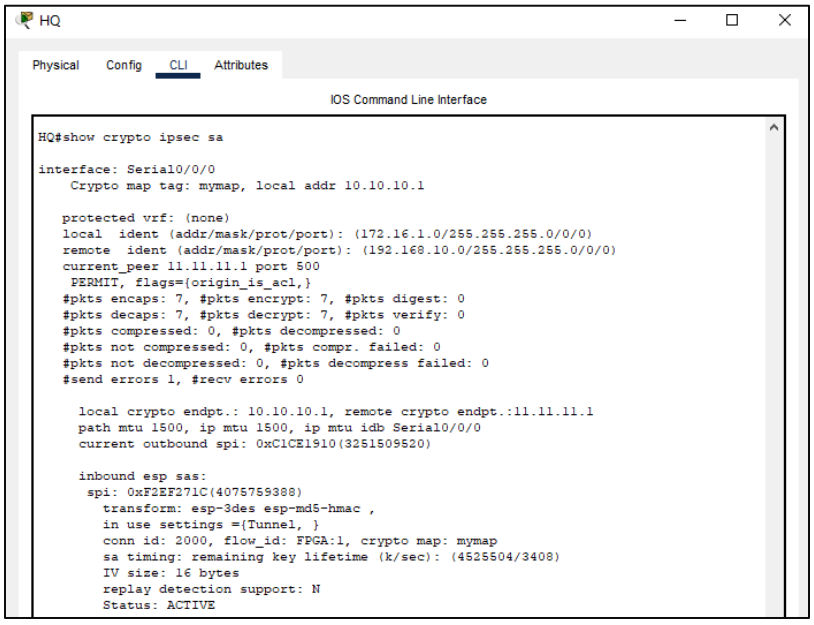
Step 7: Check the connection





Step 8: Verify and Check the site to site VPN connection





```
    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xC1CE1910(3251509520)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 2001, flow_id: FPGA:1, crypto map: mymap
       sa timing: remaining key lifetime (k/sec): (4525504/3408)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:

HQ#
```

Branch

Physical Config CLI Attributes

IOS Command Line Interface

```
Branch#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.10.1      11.11.11.1      QM_IDLE           1013    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Branch

Physical Config CLI Attributes

IOS Command Line Interface

```
Branch#
Branch#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: mymap, local addr 11.11.11.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   current_peer 10.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 11.11.11.1, remote crypto endpt.:10.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xF2EF271C(4075759388)

     inbound esp sas:
      spi: 0xC1CE1910(3251509520)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2000, flow_id: FPGA:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4525504/3313)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF2EF271C(4075759388)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: FPGA:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4525504/3313)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

Branch#
Branch#
```