

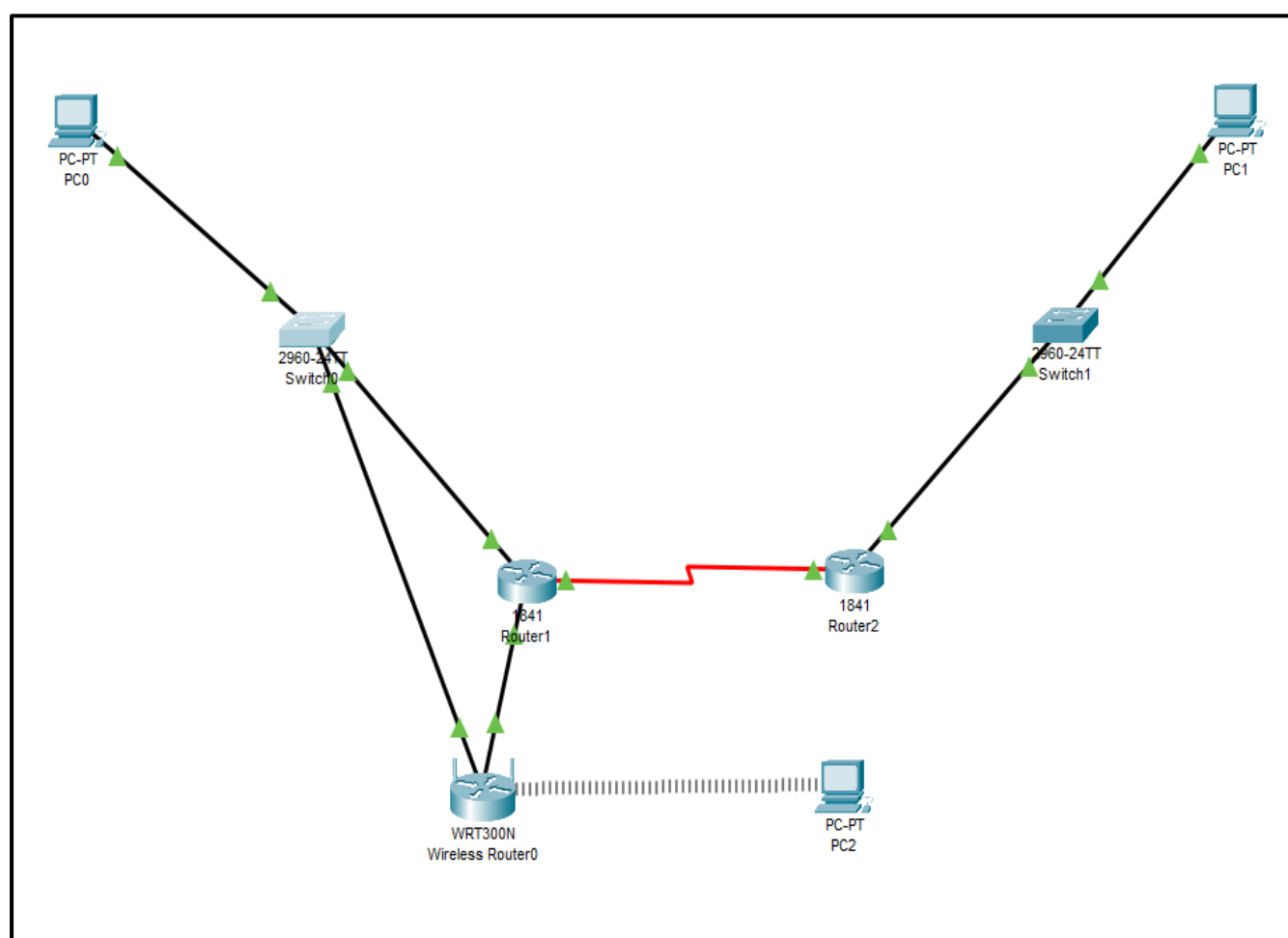
Practical No: 01

Aim: Configuring WEP on a Wireless Router

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

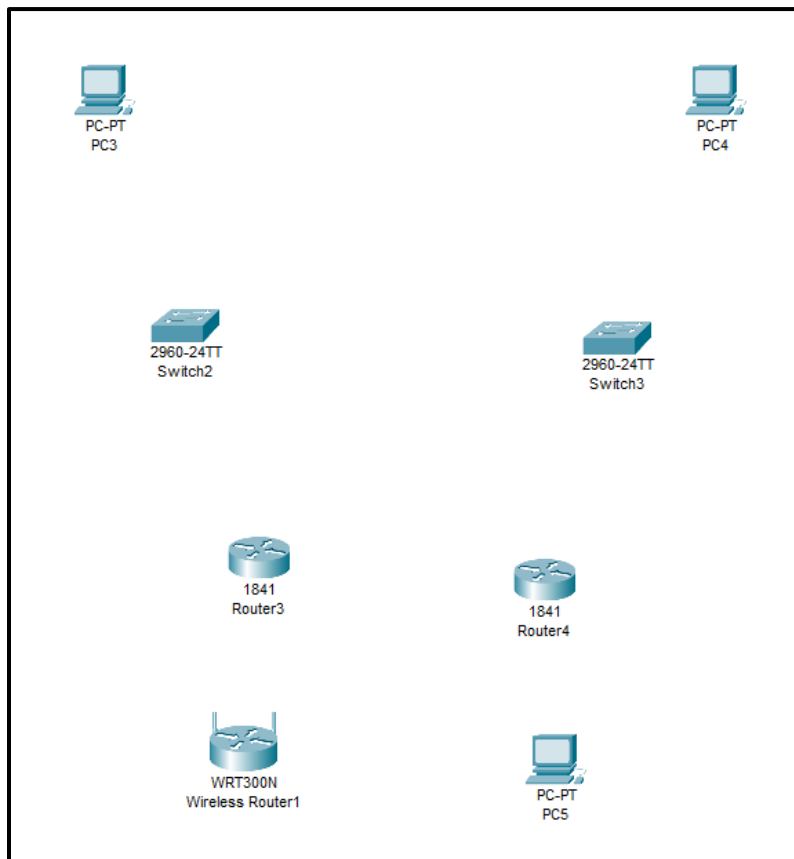
Theory: Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

Cisco Packet Tracer Setup:-

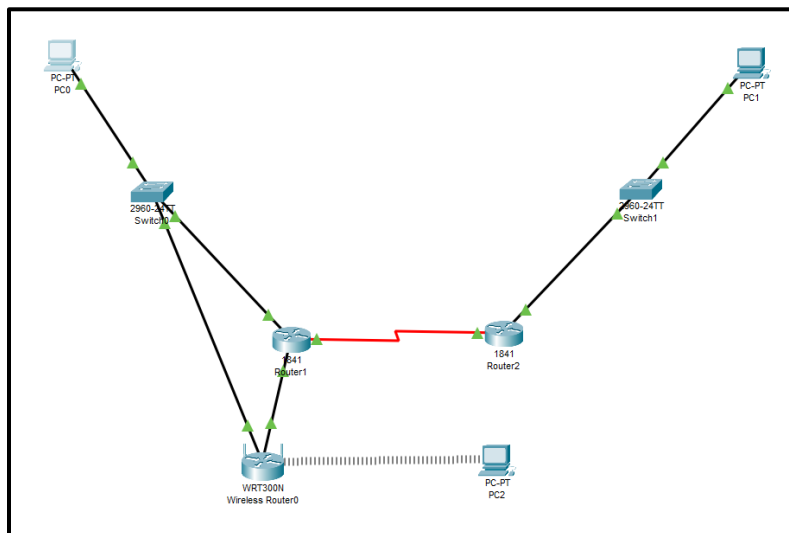


Implementation:

Step 1: Arranging devices



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



Step 3: Configuring all devices

PC0

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: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::203:E4FF:FED2:51D

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:C7FF:FE83:C309

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ 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

FastEthernet0/0

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

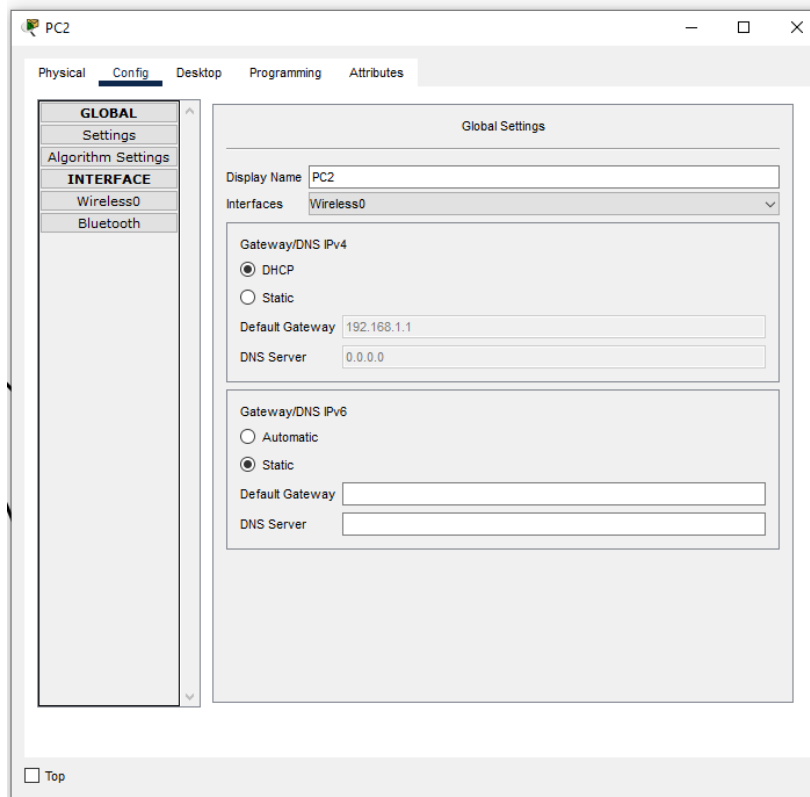
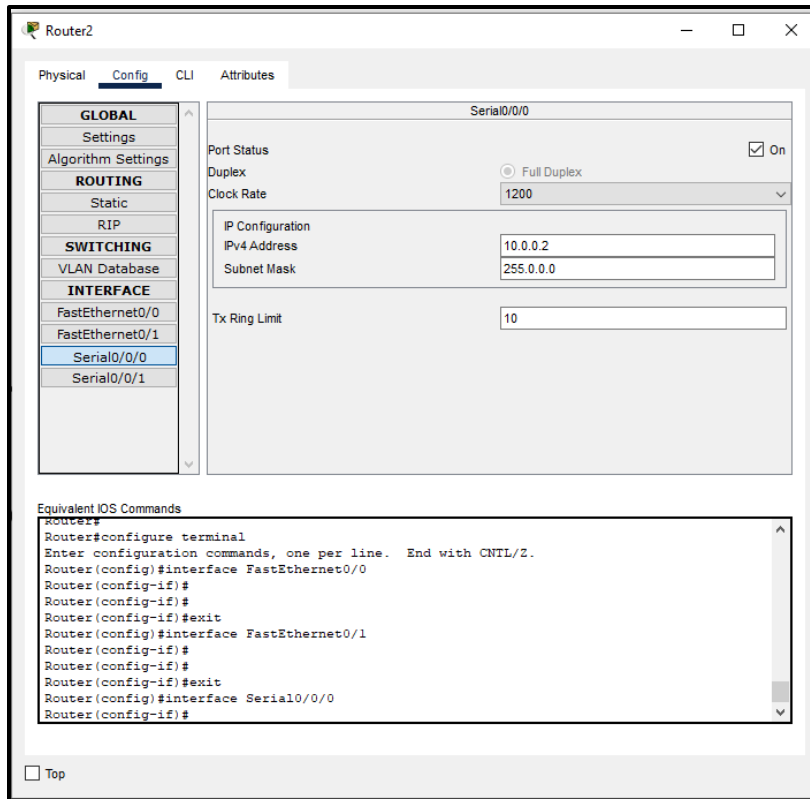
Subnet Mask 255.0.0.0

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



Step 4: Configuring wireless router

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Firmware Version: v0.93.3

Setup Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: . . .

Subnet Mask:

DHCP Server Settings

DHCP Server: ☒ Enabled ☐ Disabled

Start IP Address: 192.168.1.

Maximum number of Users:

IP Address Range: 192.168.1. -

Client Lease Time: minutes (0 means one day)

Static DNS 1: . . .

Static DNS 2: . . .

Static DNS 3: . . .

WINS: . . .

Help...

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

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Firmware Version: v0.93.3

Wireless Setup Wireless **Security** Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter Advanced Wireless Settings

Wireless Security

Security Mode: WEP

40/64-Bits (10 Hex digits)

Encryption:

Passphrase:

Key1: 2a2a2a2a2a

Key2:

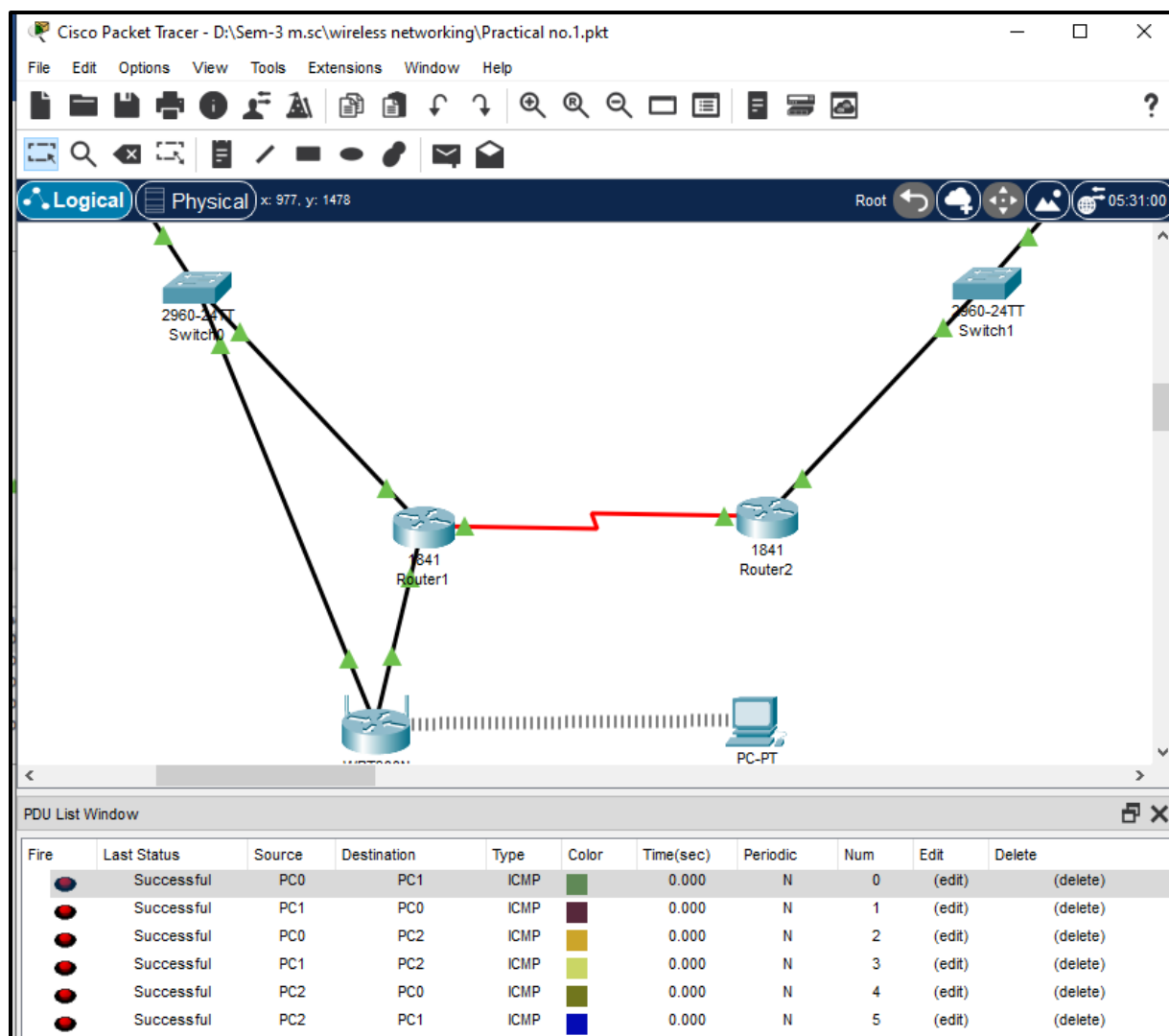
Key3:

Key4:

TX Key: 1

Help...

Checking connection:



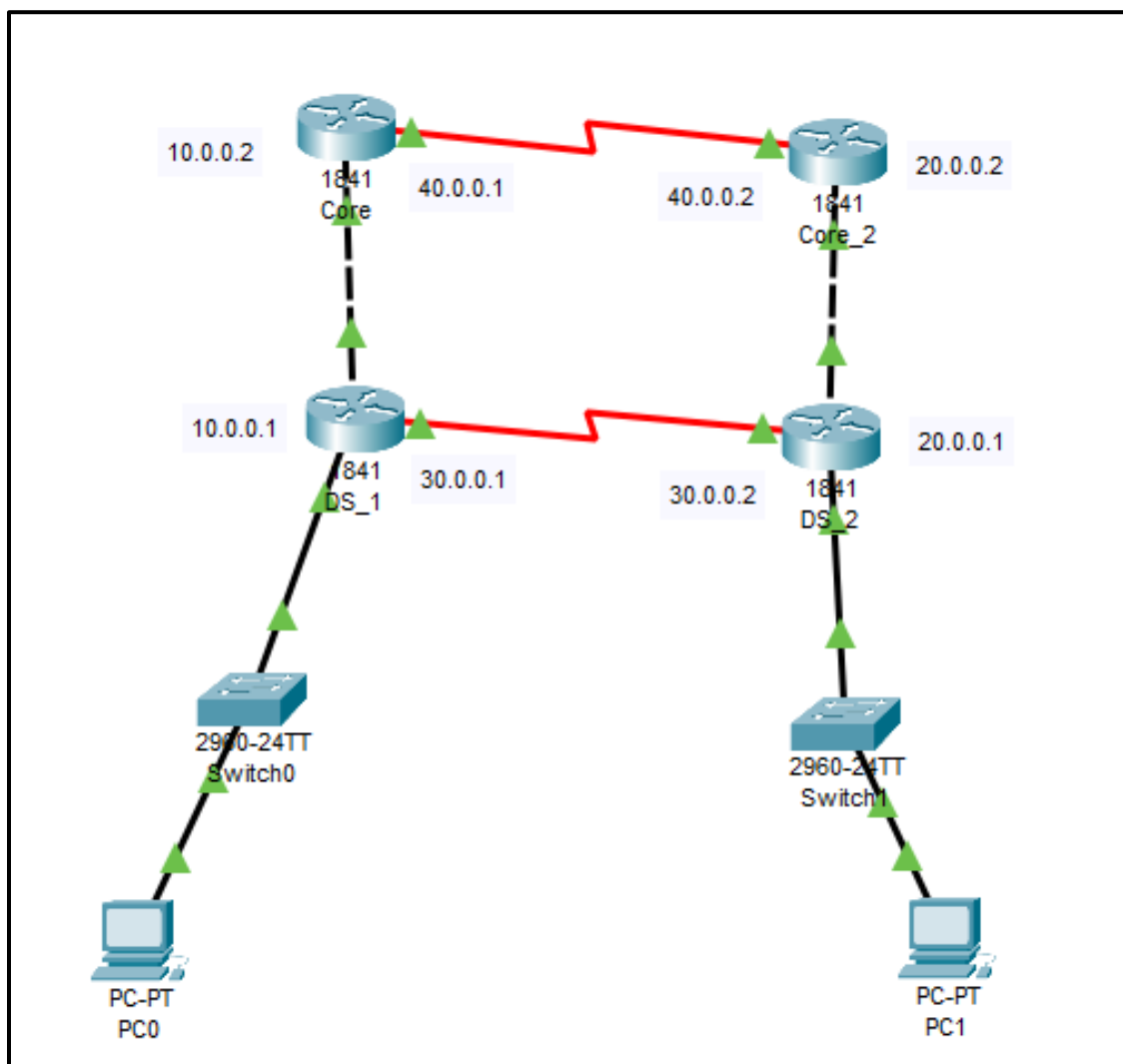
Practical No: 02

Aim: Demonstrating Distribution Layer Functions

Components: Router, Switch, Device (PC)

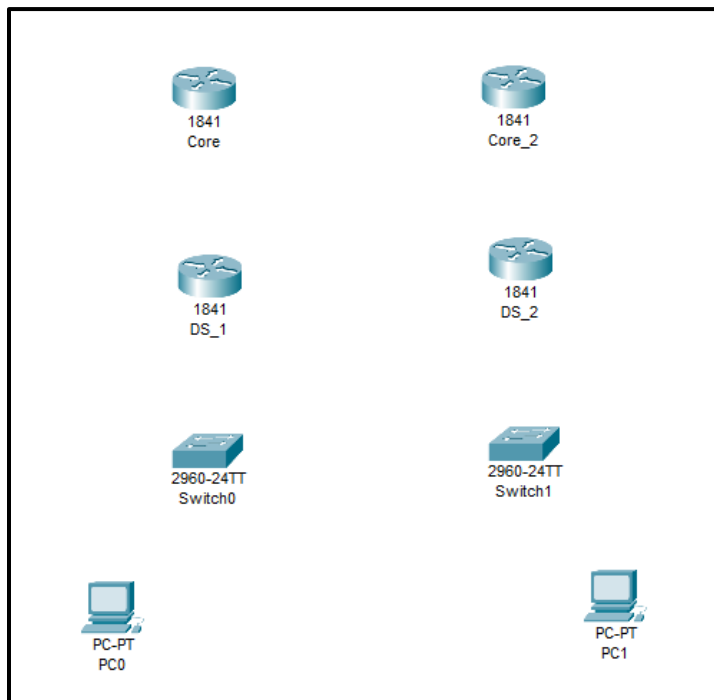
Theory: The distribution layer is the smart layer in the three-layer model. Routing, filtering, and QoS policies are managed at the distribution layer. Distribution layer devices also often manage individual branch-office WAN connections. This layer is also called the Workgroup layer.

Cisco Packet Tracer Setup:-

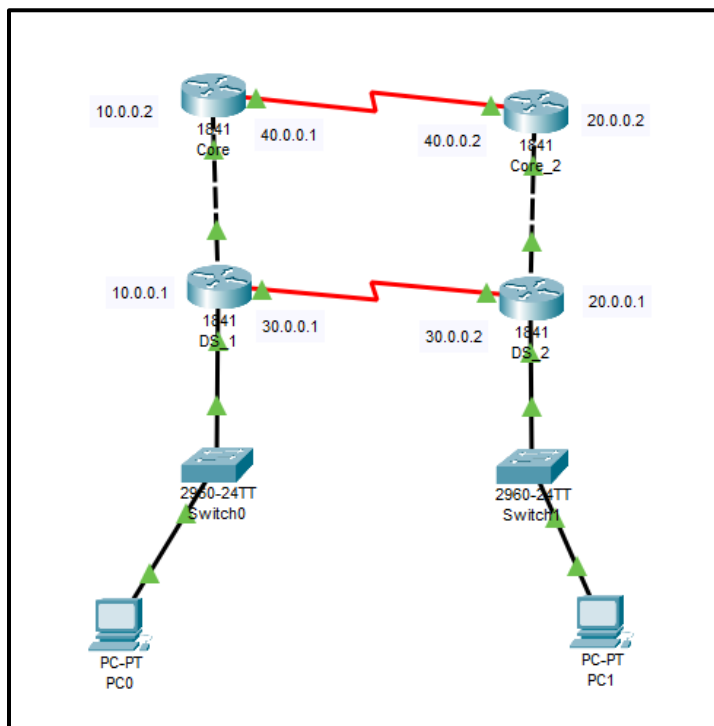


Implementation:

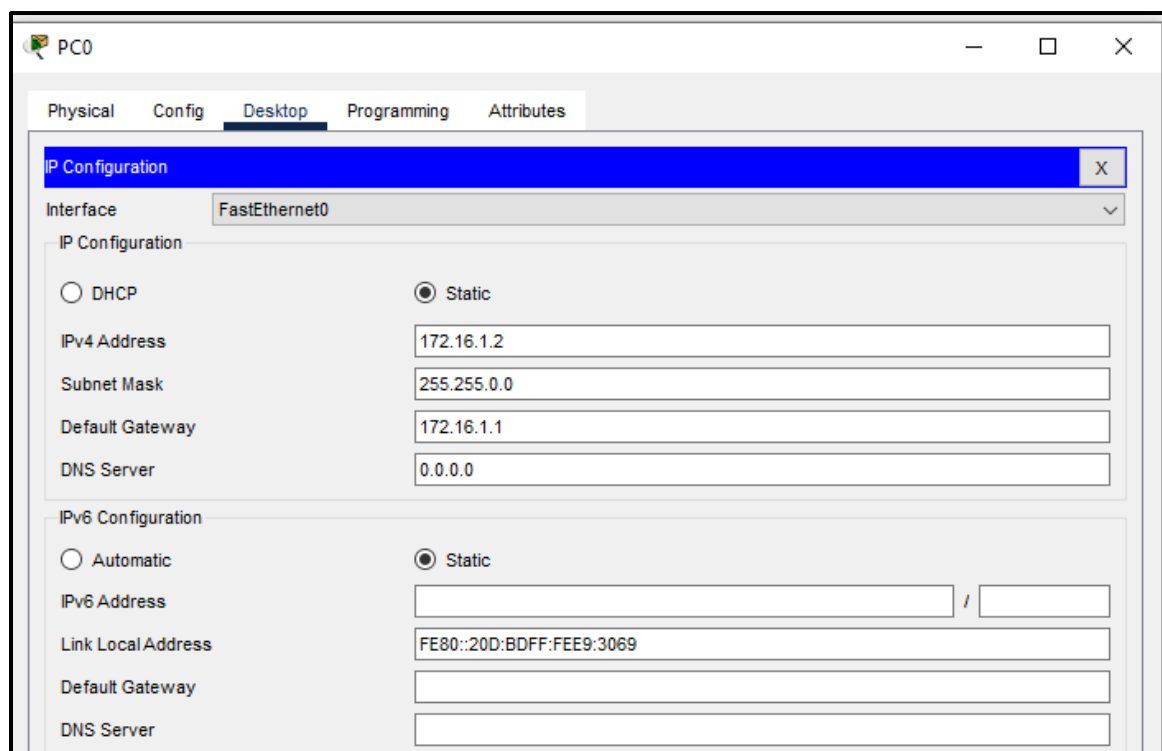
Step 1: Arranging devices



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



Step 3: Configuring all devices



PC0

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 172.16.1.2

Subnet Mask: 255.255.0.0

Default Gateway: 172.16.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

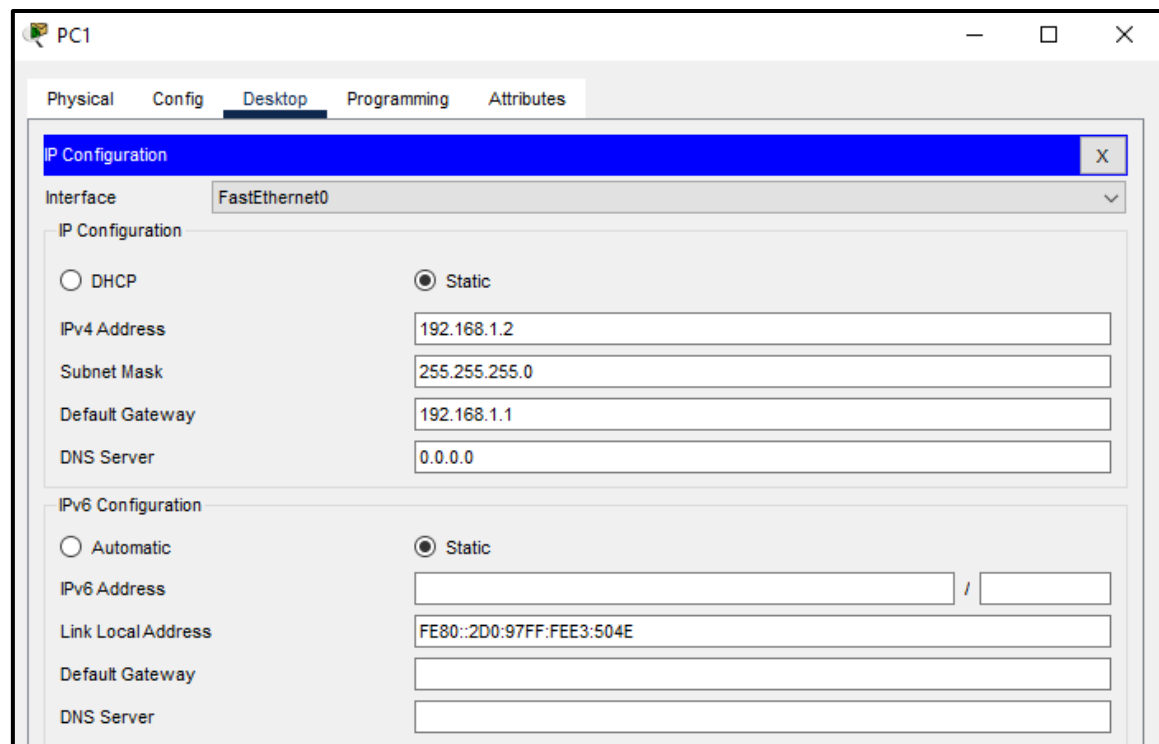
IPv6 Address: /

Link Local Address: FE80::20D:BDFF:FEE9:3069

Default Gateway:

DNS Server:

Step 4: Setting up distribution layer using router



PC1

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: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

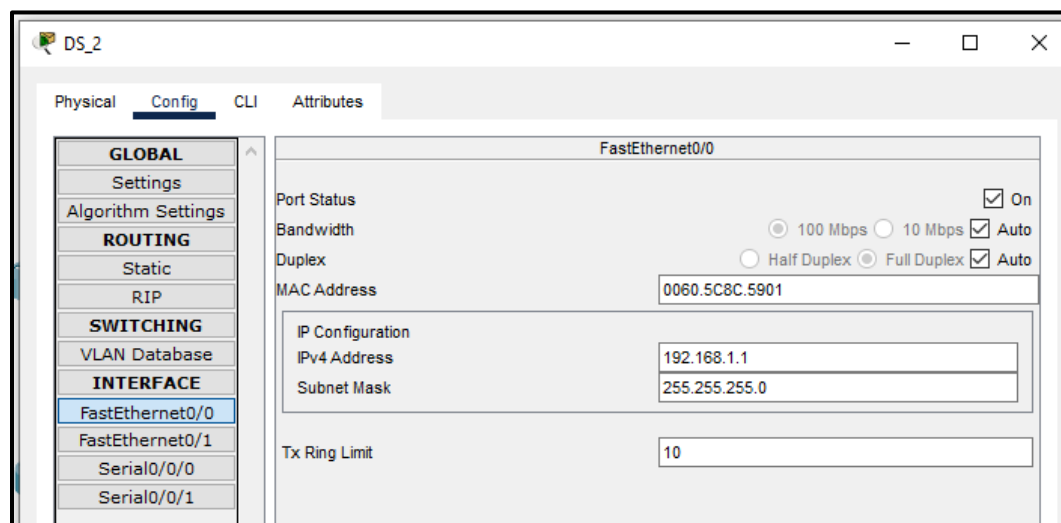
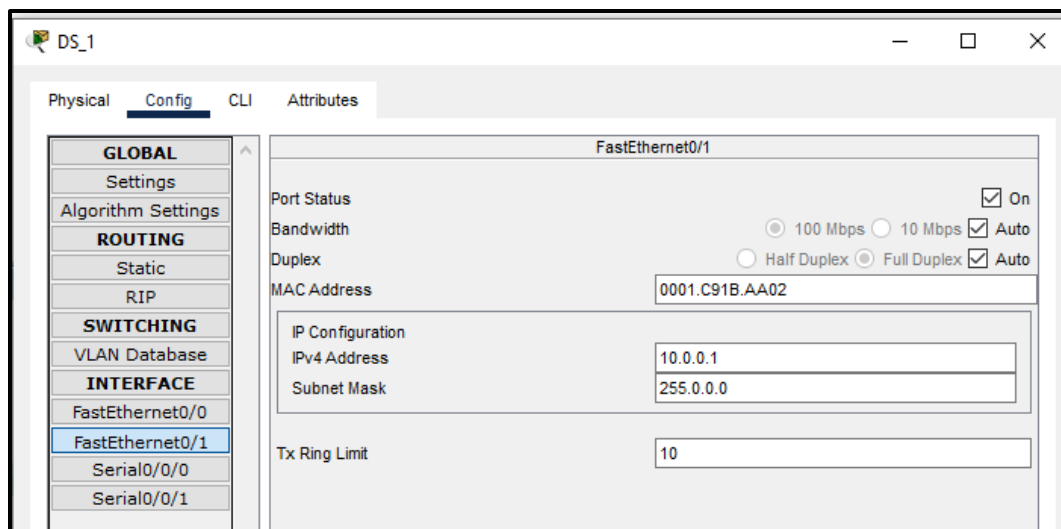
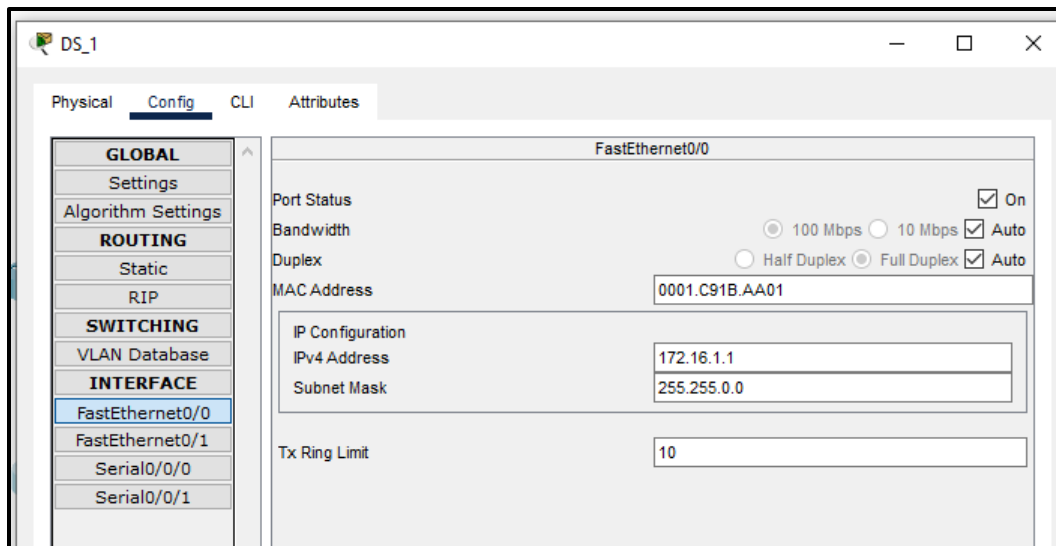
☐ Automatic ☒ Static

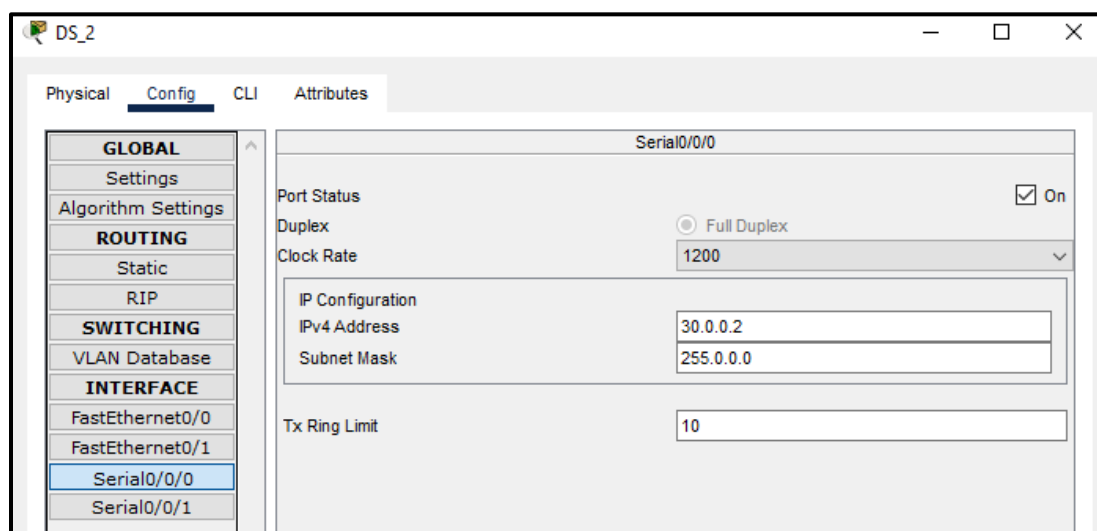
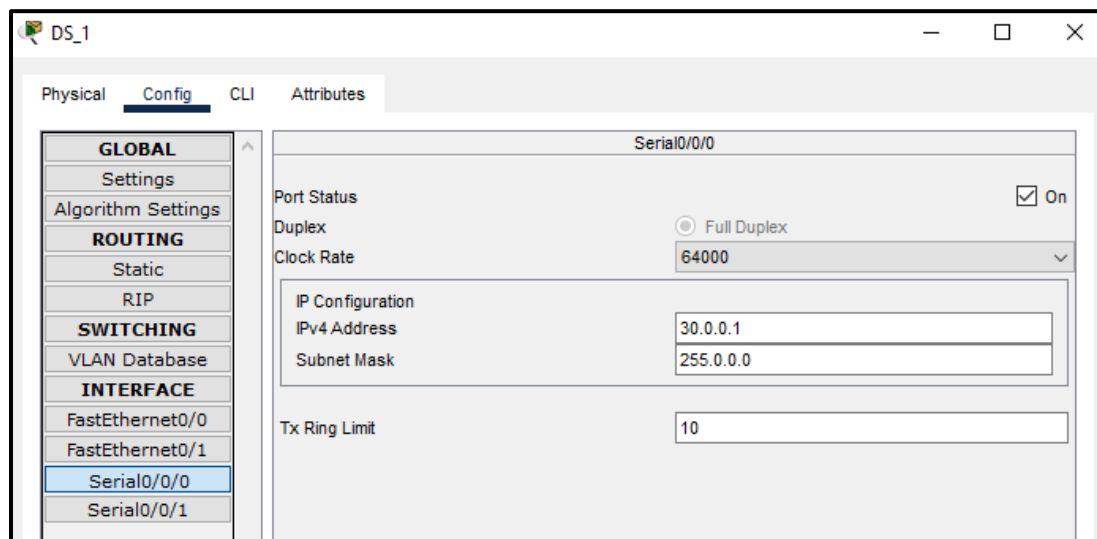
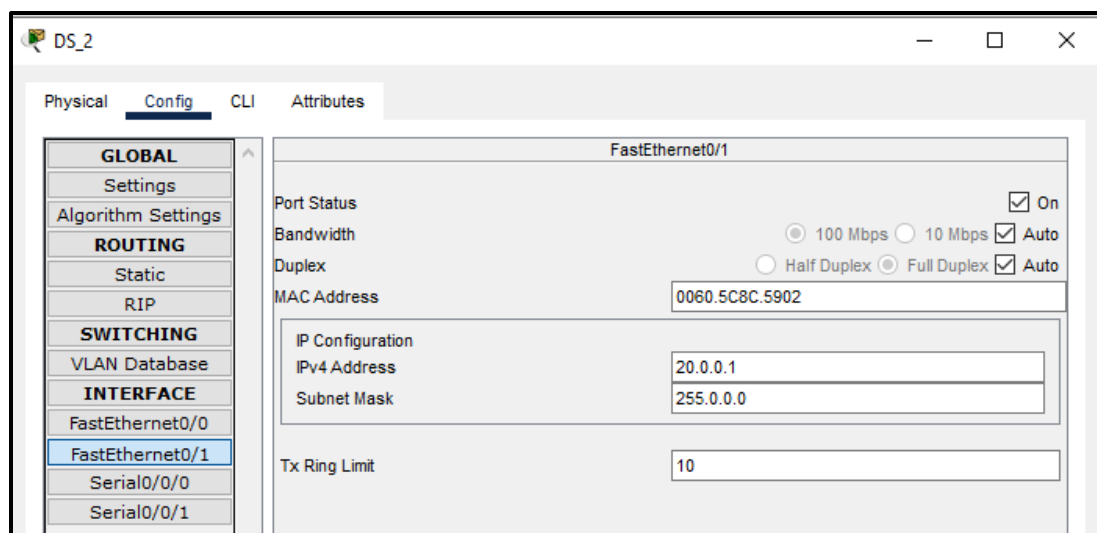
IPv6 Address: /

Link Local Address: FE80::2D0:97FF:FEE3:504E

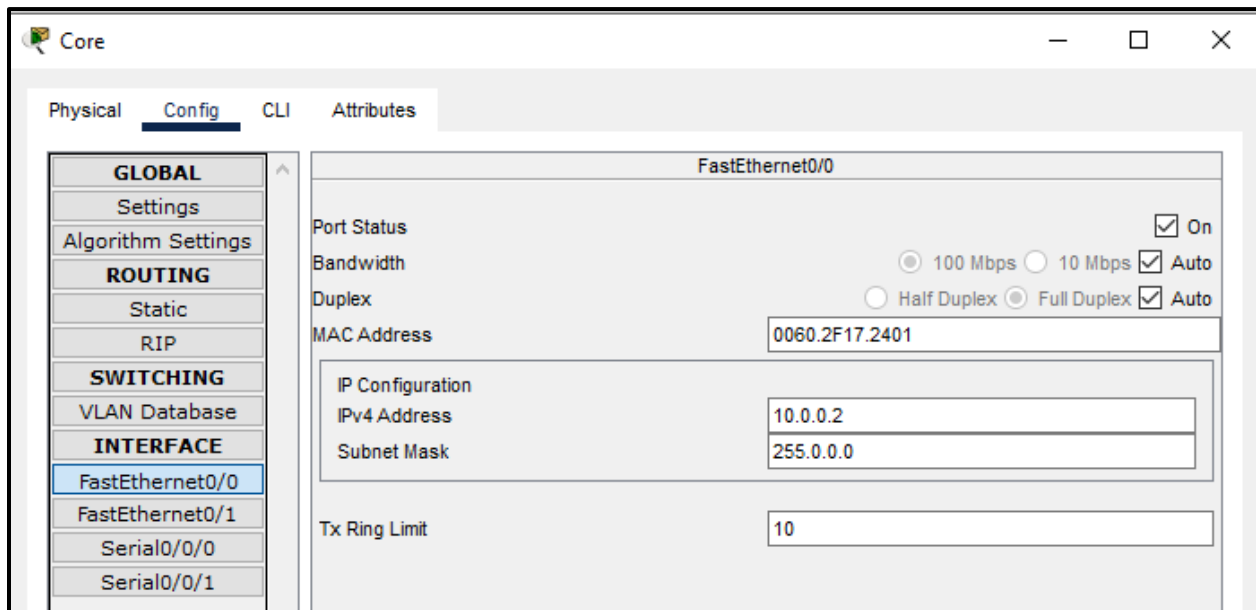
Default Gateway:

DNS Server:



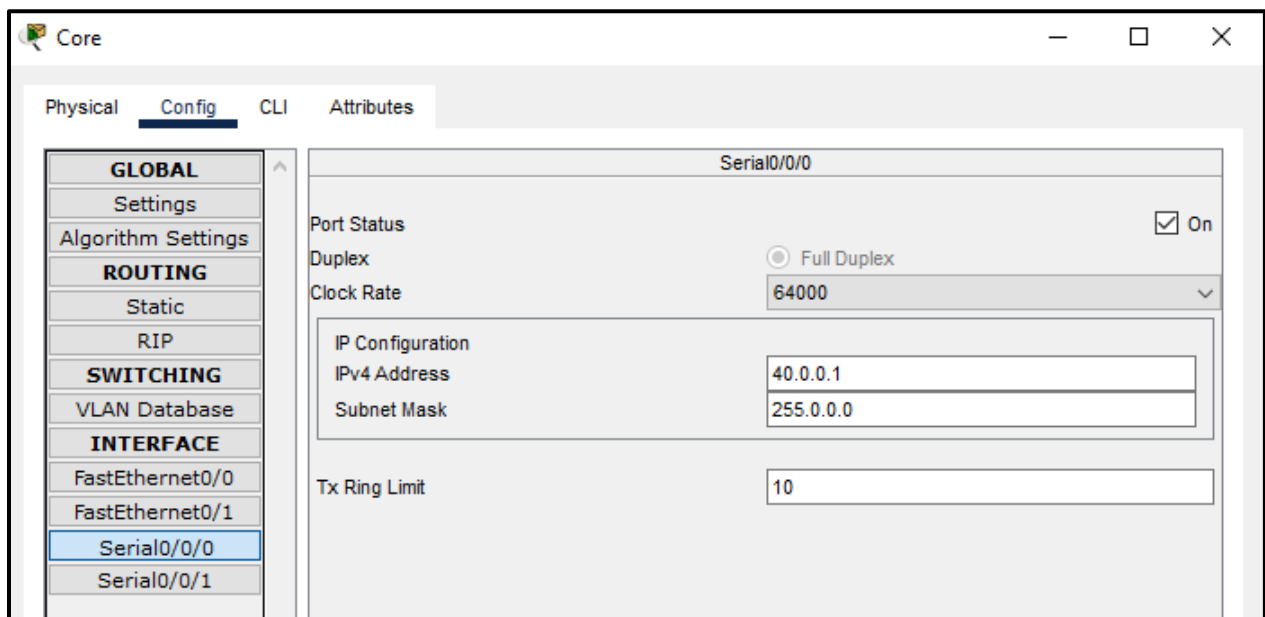


Step 5: Setting up core routers



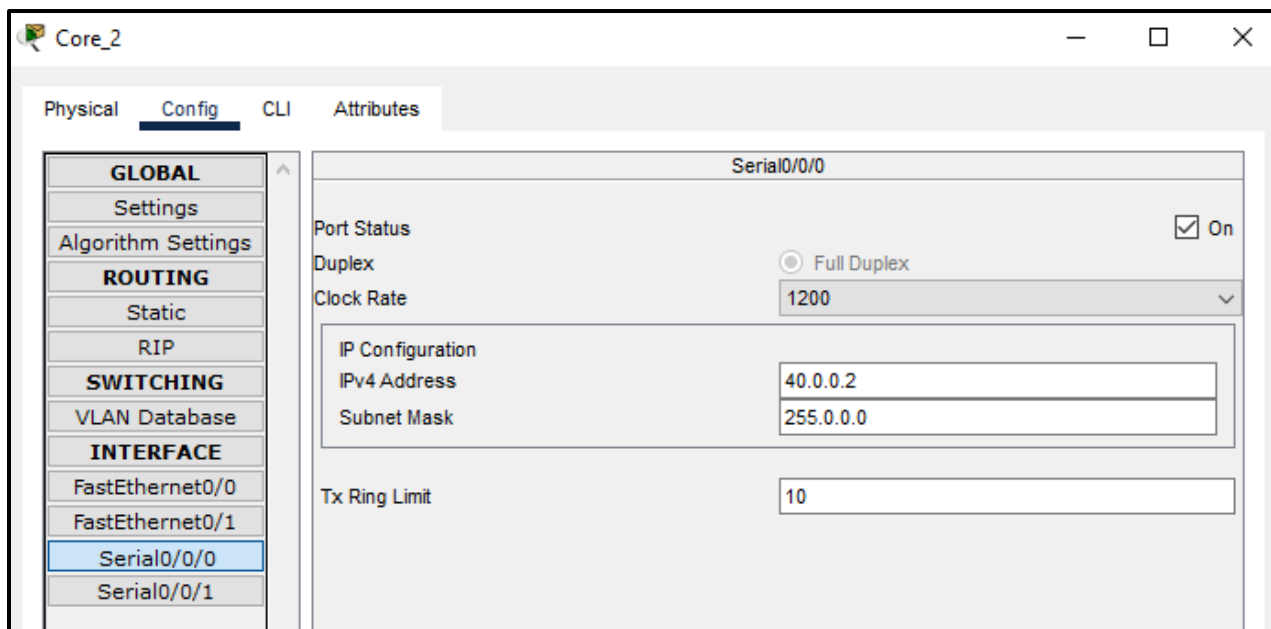
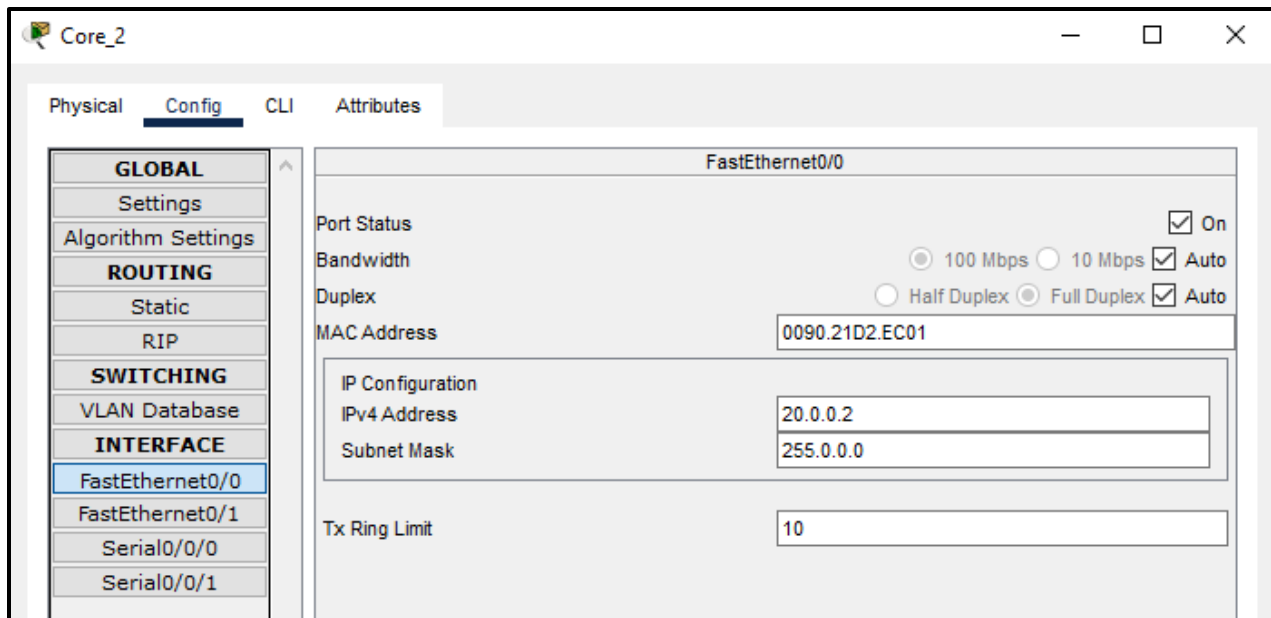
The screenshot shows the configuration window for the Core router, specifically for the FastEthernet0/0 interface. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, FastEthernet0/0 is selected. The main panel shows the configuration for this interface.

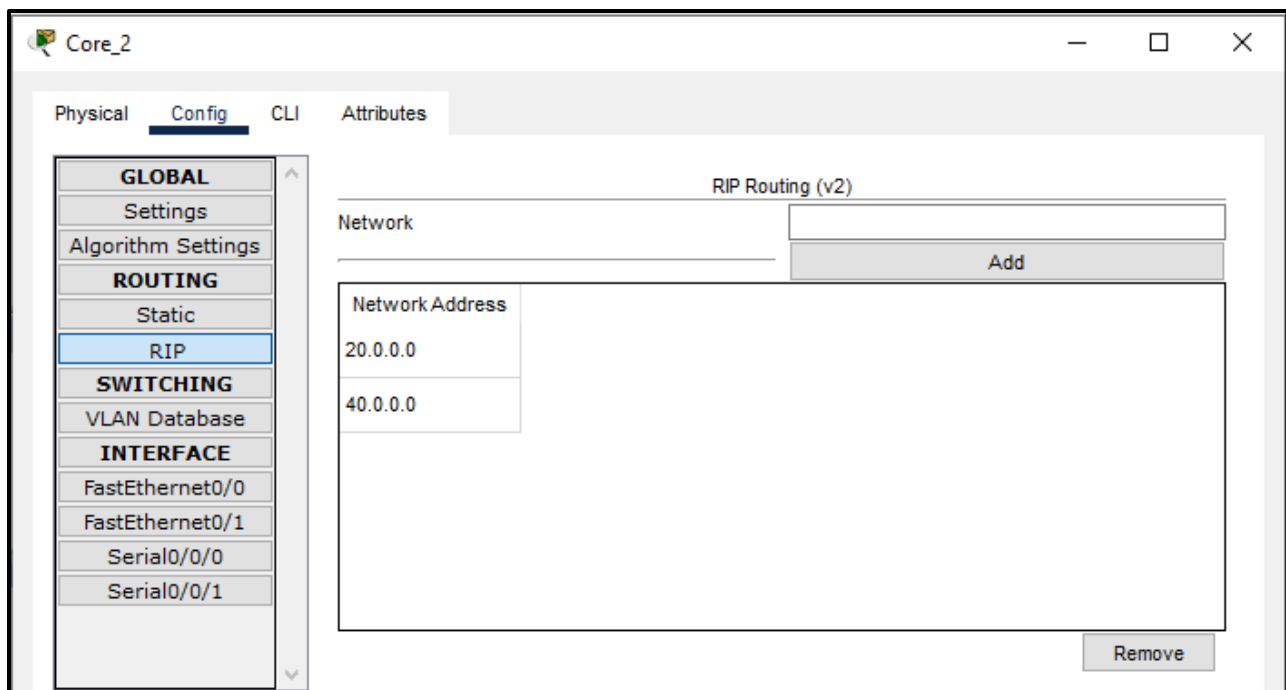
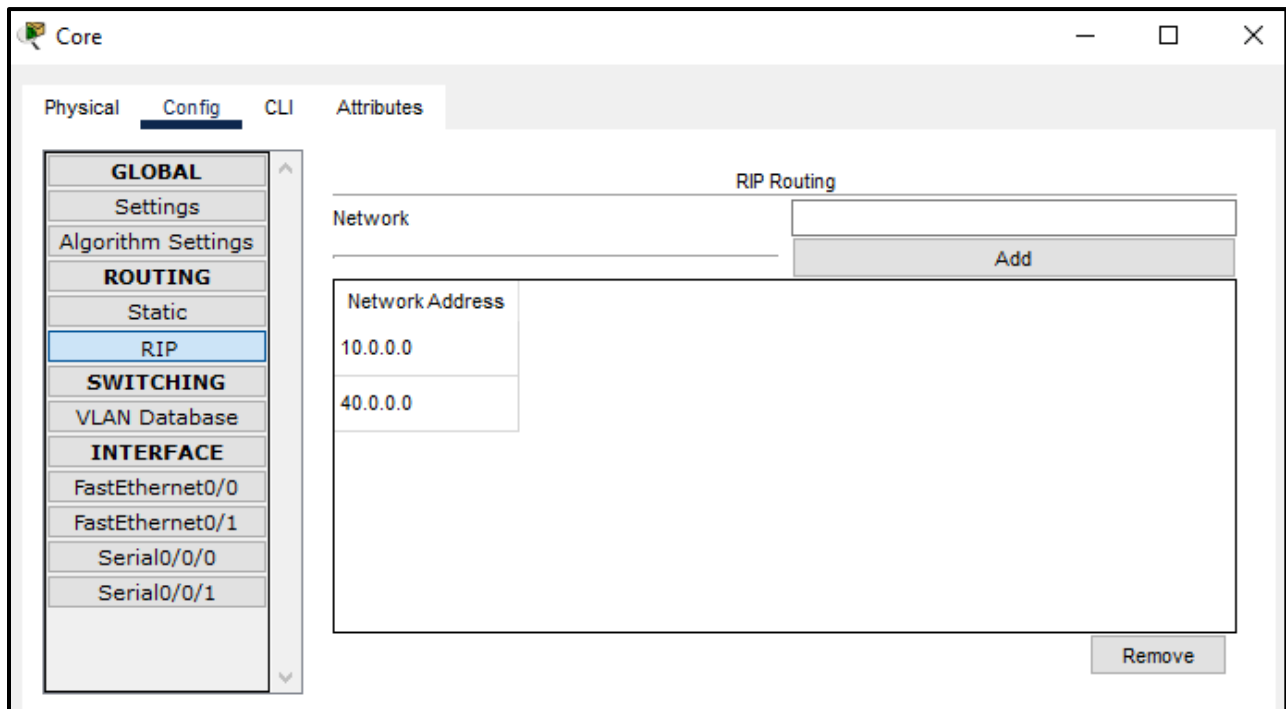
FastEthernet0/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0060.2F17.2401
IP Configuration	
IPv4 Address	10.0.0.2
Subnet Mask	255.0.0.0
Tx Ring Limit	10

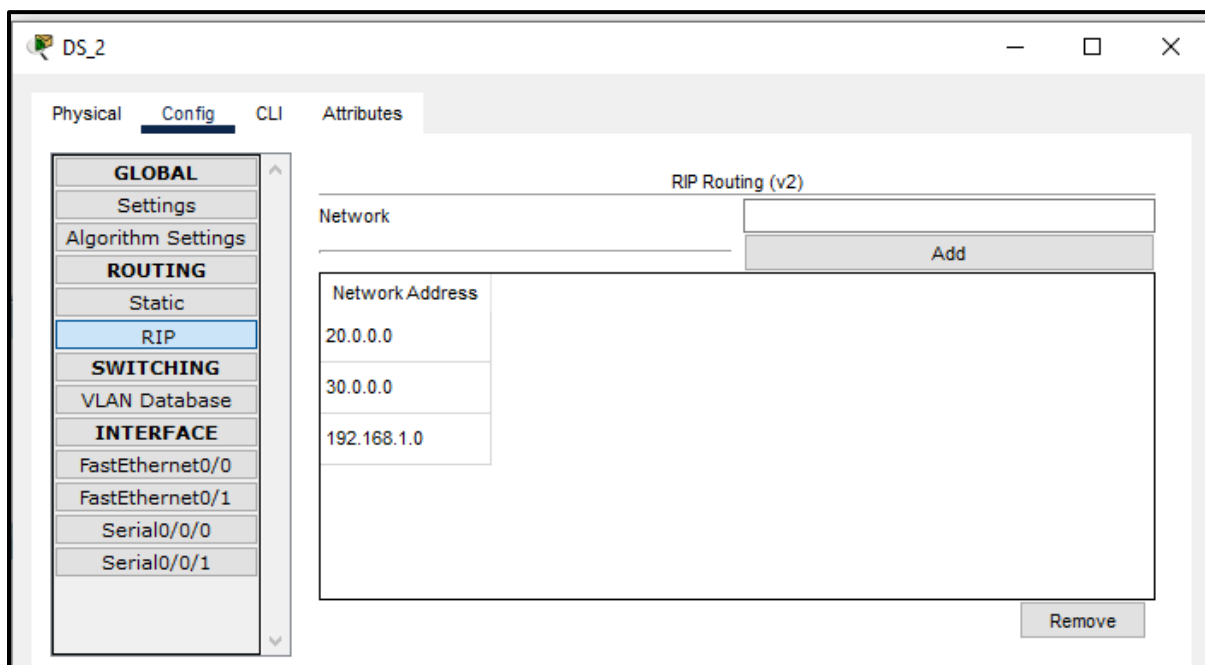
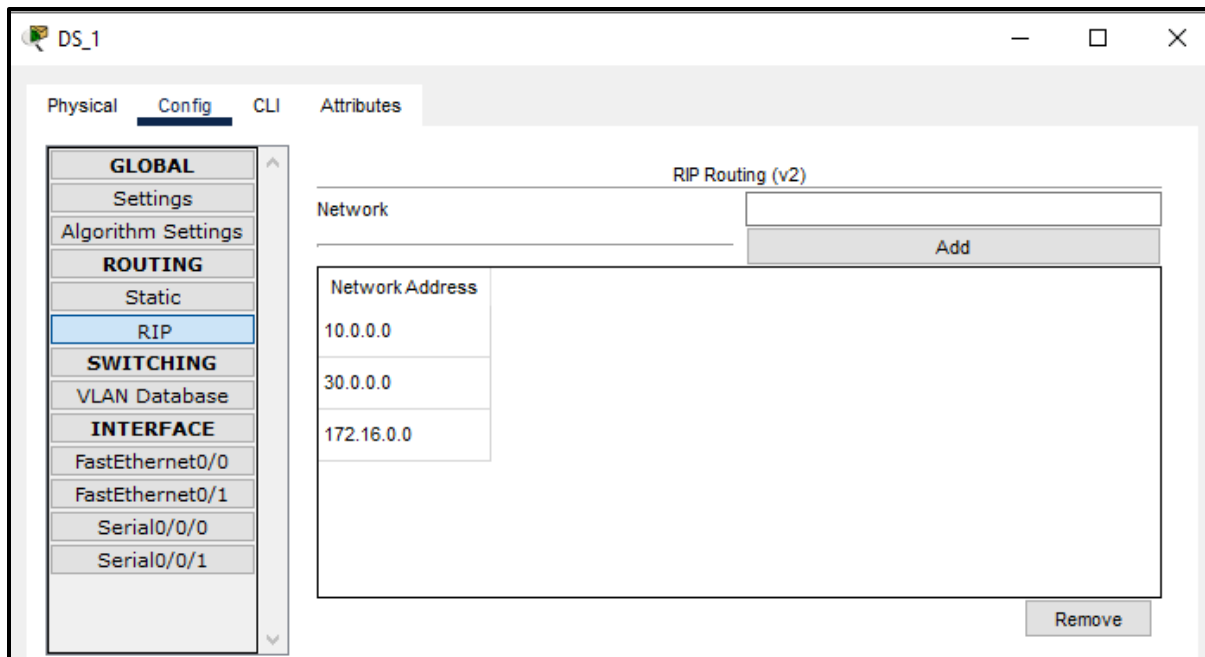


The screenshot shows the configuration window for the Core router, specifically for the Serial0/0/0 interface. The left sidebar is the same as the previous screenshot, but Serial0/0/0 is now selected under the INTERFACE category. The main panel shows the configuration for this serial interface.

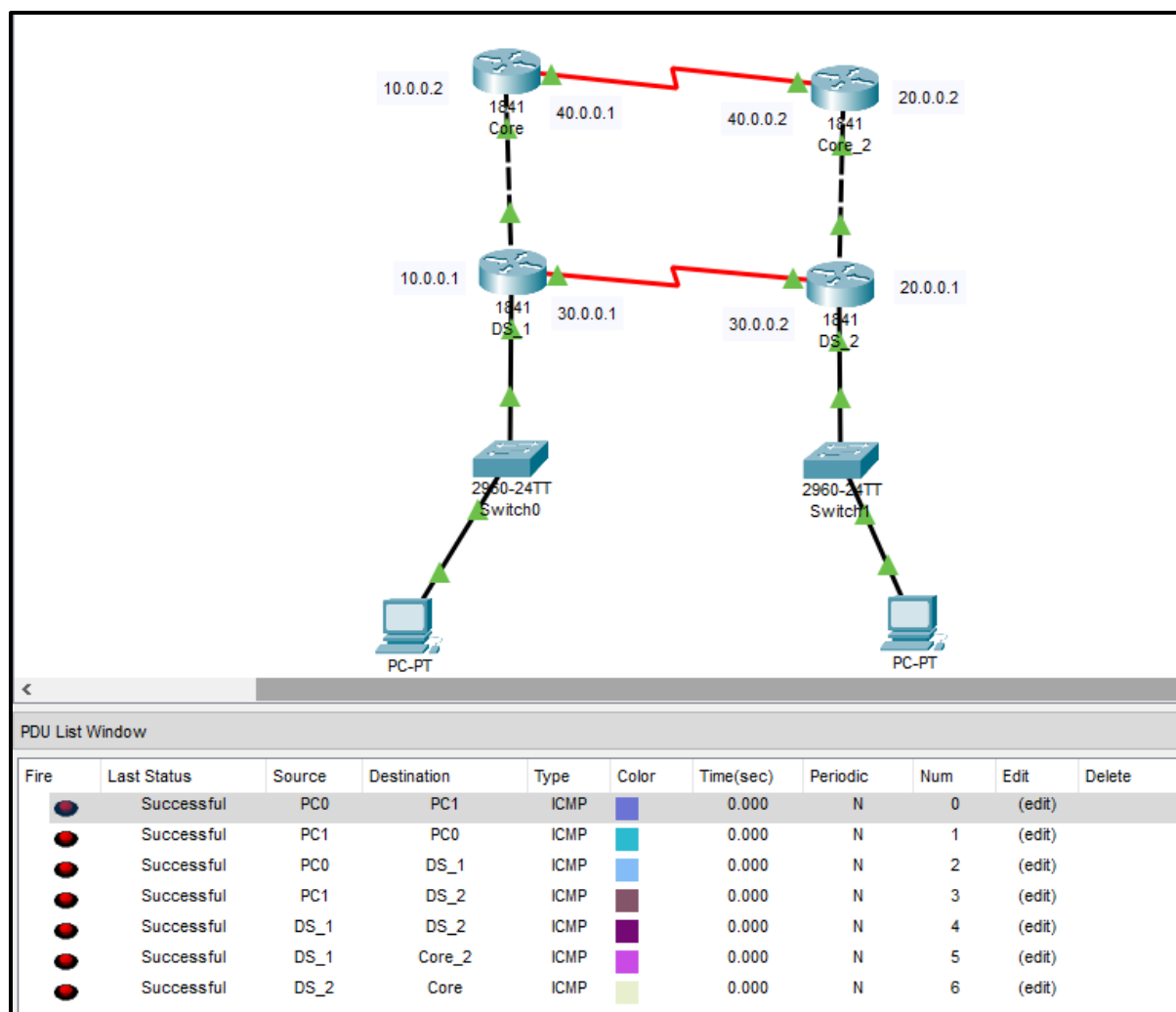
Serial0/0/0	
Port Status	<input checked="" type="checkbox"/> On
Duplex	<input checked="" type="radio"/> Full Duplex
Clock Rate	64000
IP Configuration	
IPv4 Address	40.0.0.1
Subnet Mask	255.0.0.0
Tx Ring Limit	10



Step 6: Setting up RIP routing protocol



Checking connection:



Practical No: 03

Aim: Placing ACLs

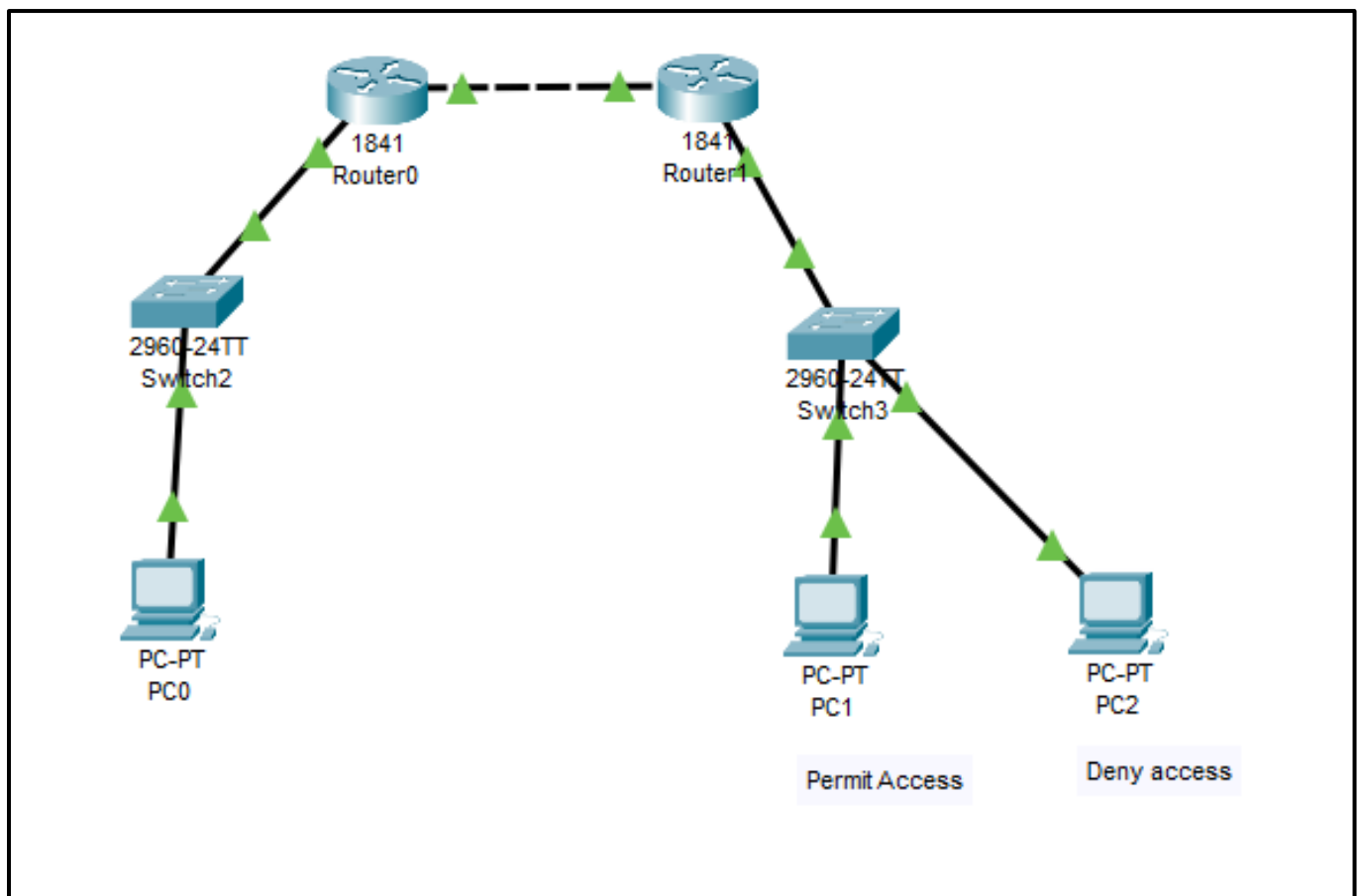
Components: Router, Switch, PC's

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:

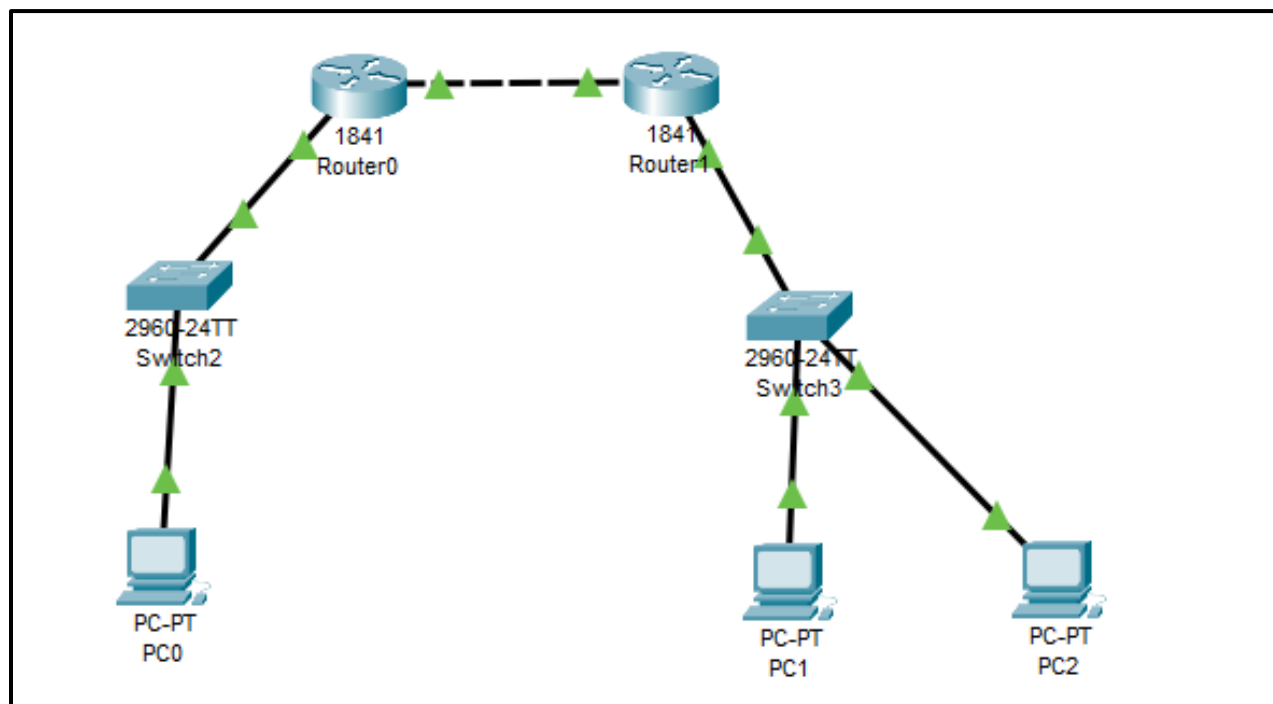
- **Standard ACLs:** These ACLs permit or deny packets based only on the source IPv4 address.

Cisco Packet Tracer Setup:-

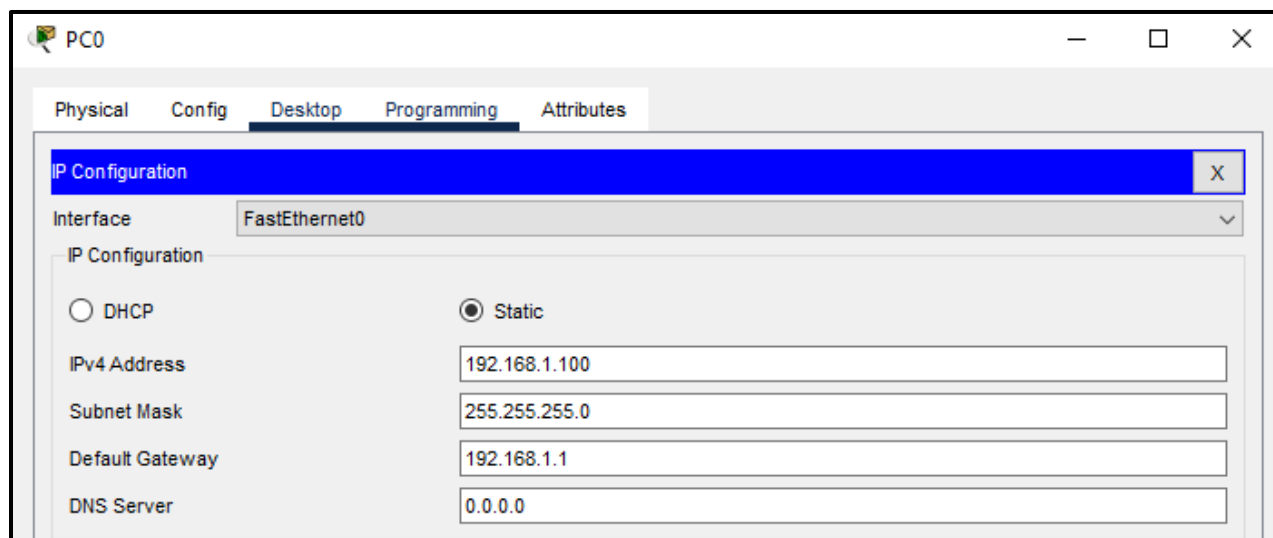


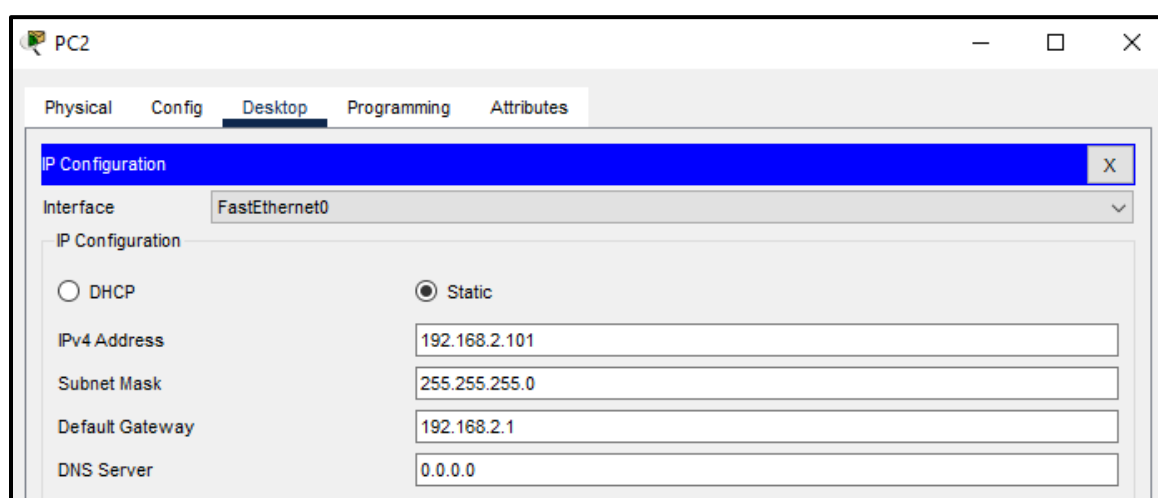
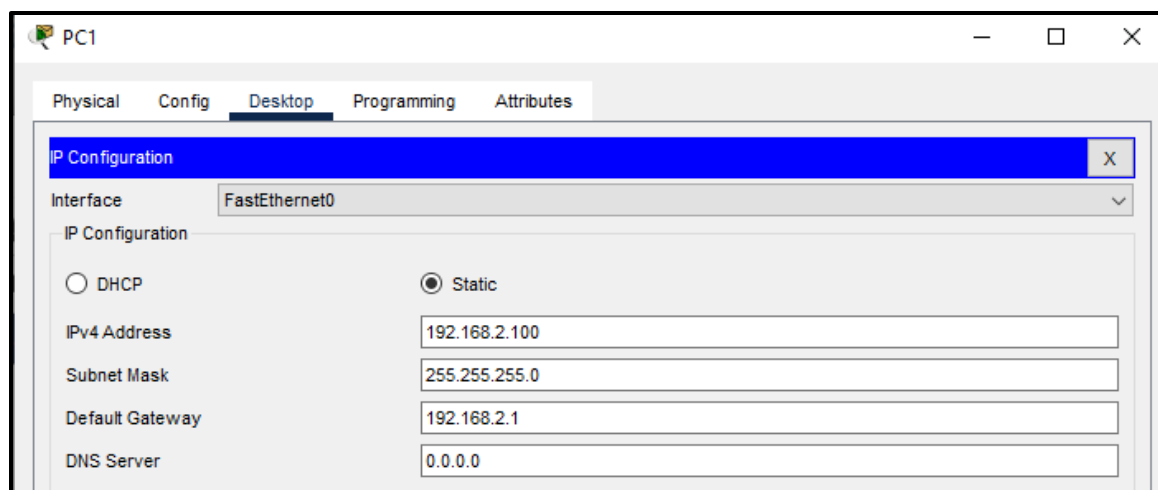
Implementation:

Step 1: Arranging devices and creating connections

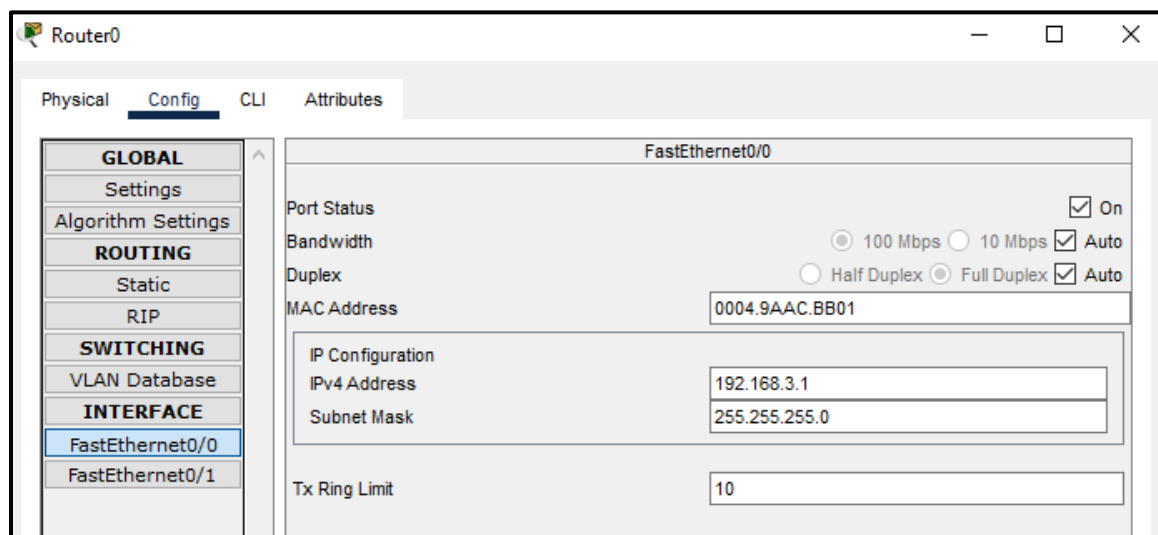


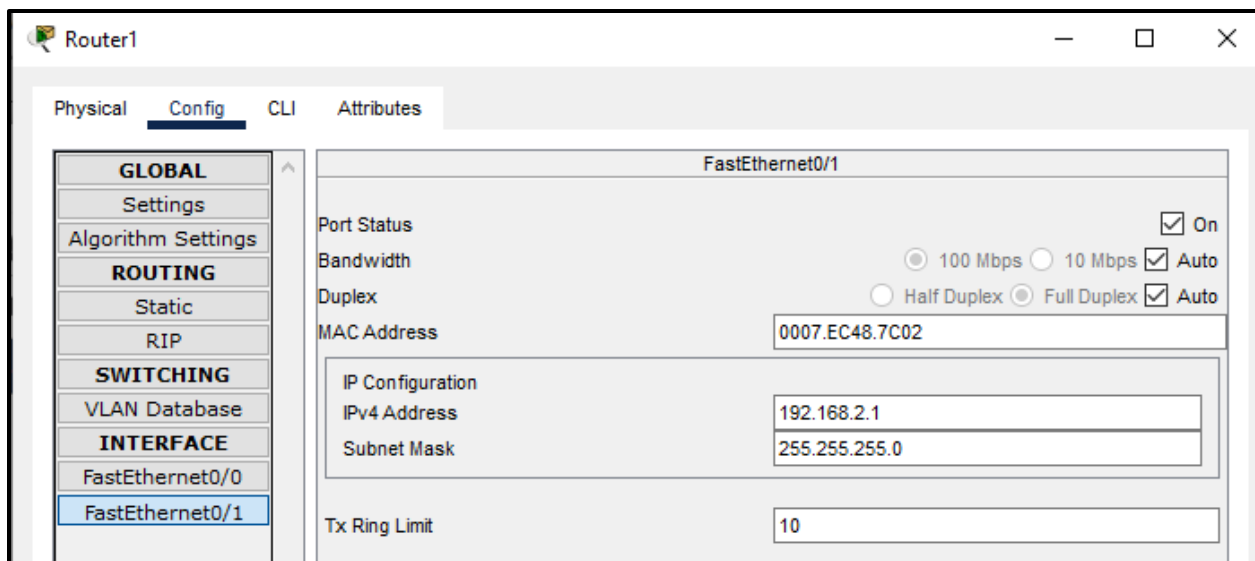
Step 2: Configuring all the PC's And Assigning IP Address



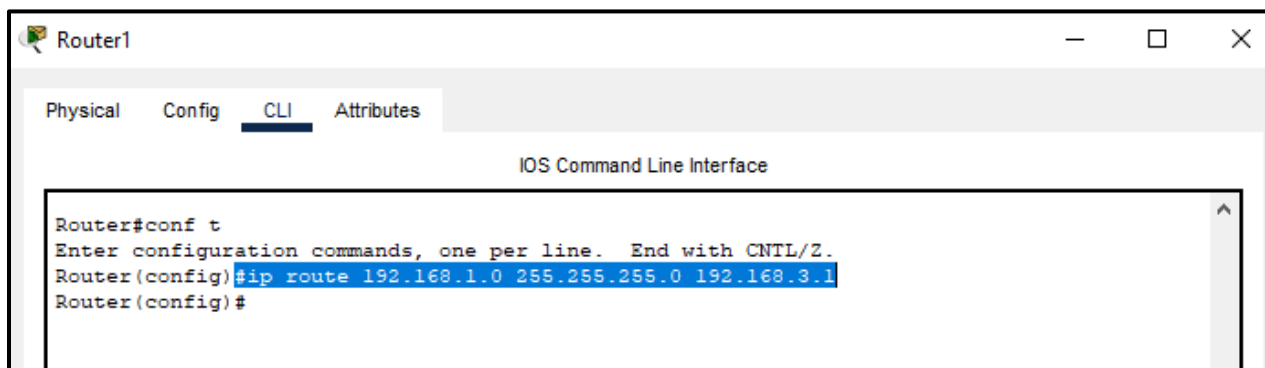
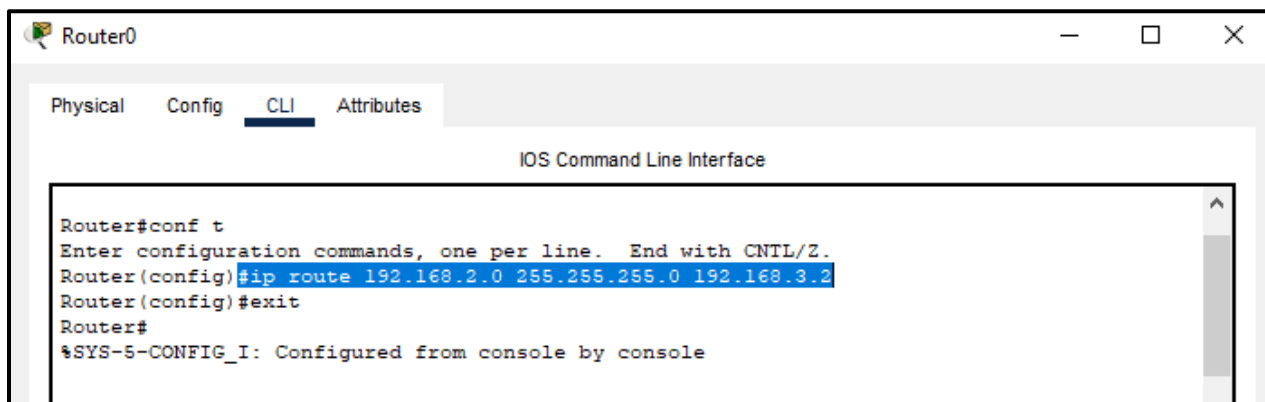


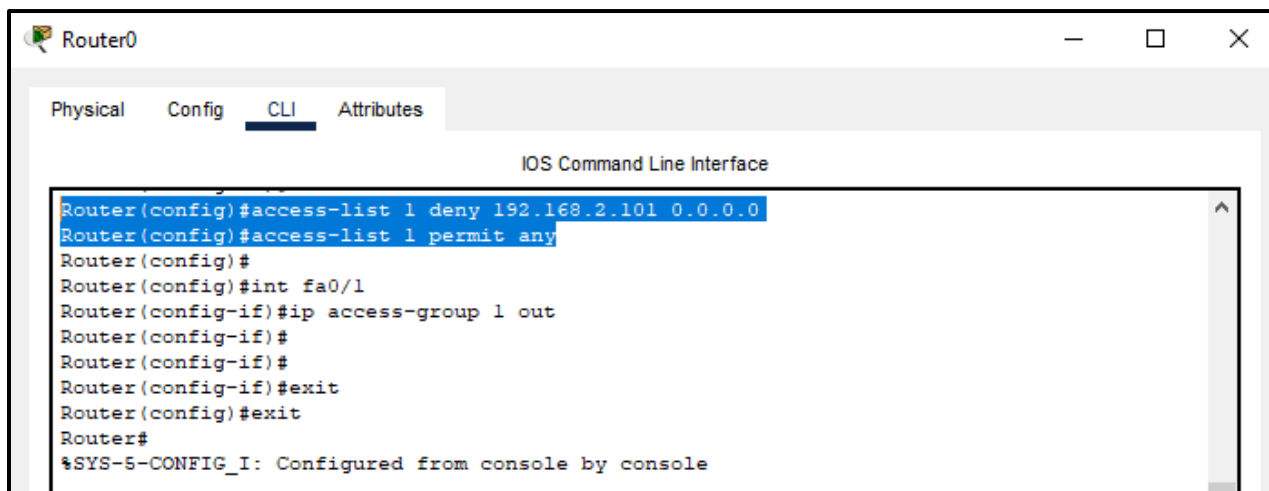
Step 3: Configure Routers and turn them on





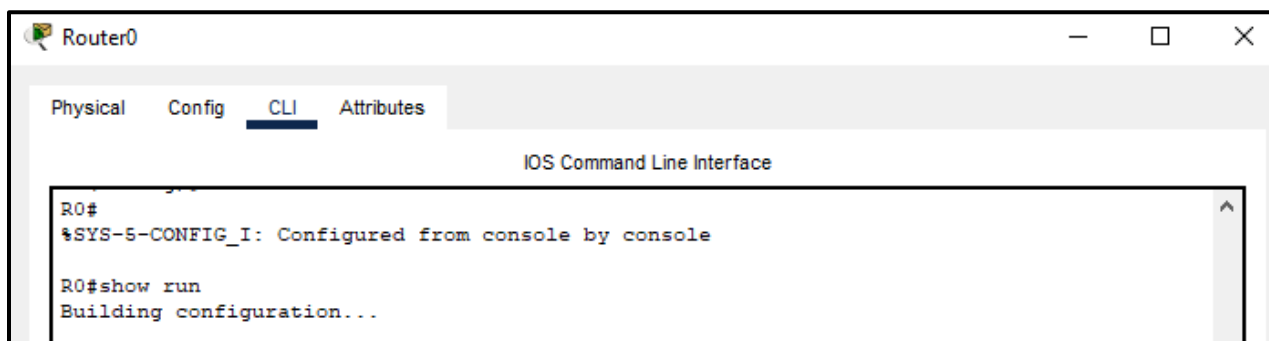
Step 4: Add static routes




Step 5: Create Standard ACLA screenshot of a network simulator window titled 'Router0'. It has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area is titled 'IOS Command Line Interface' and shows a series of commands entered in a terminal. The commands are: 'Router(config)#access-list 1 deny 192.168.2.101 0.0.0.0', 'Router(config)#access-list 1 permit any', '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', and 'Router#'. The last two lines are highlighted in blue. At the bottom, a status message reads '%SYS-5-CONFIG_I: Configured from console by console'.

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#access-list 1 deny 192.168.2.101 0.0.0.0
Router(config)#access-list 1 permit any
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 the ACL using show run command

A screenshot of the same 'Router0' window. The 'CLI' tab is still selected. The terminal shows the command 'R0#show run' and the output 'Building configuration...'. The status message '%SYS-5-CONFIG_I: Configured from console by console' is still visible at the bottom.

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
R0#
%SYS-5-CONFIG_I: Configured from console by console
R0#show run
Building configuration...
```

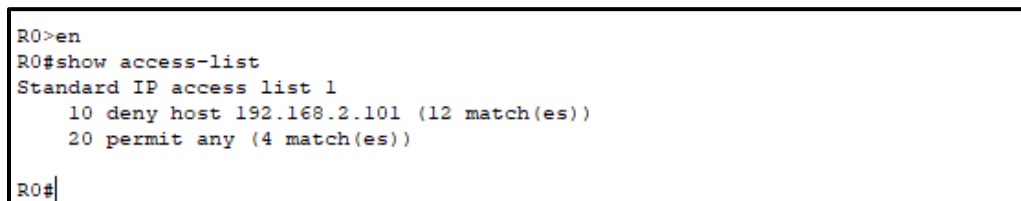


```

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

```

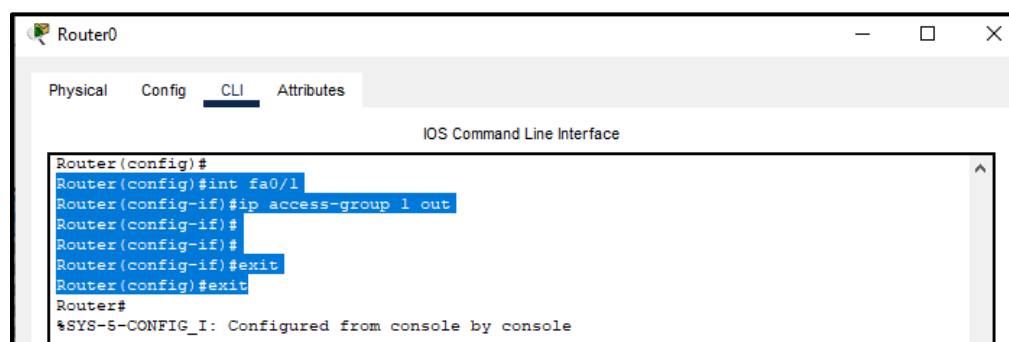


```

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



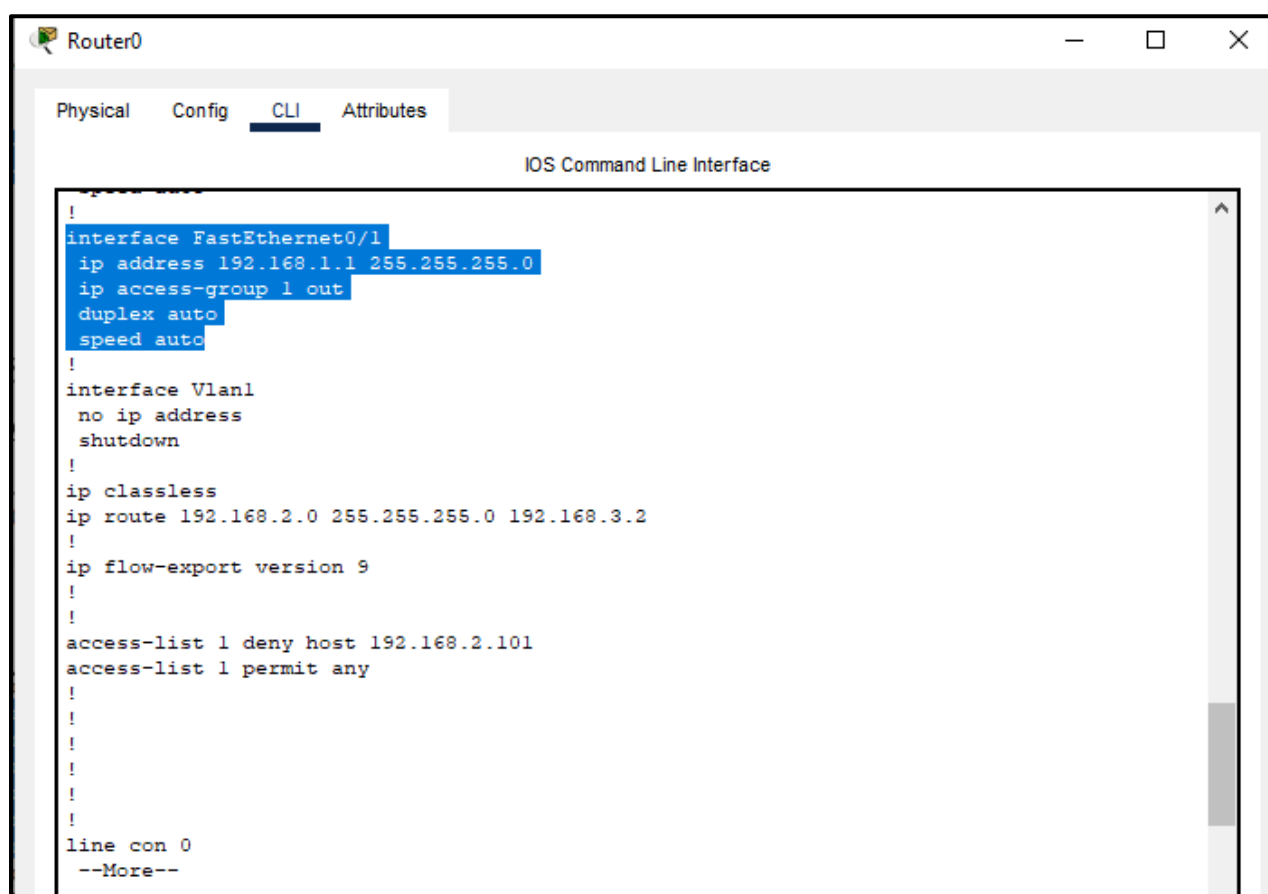
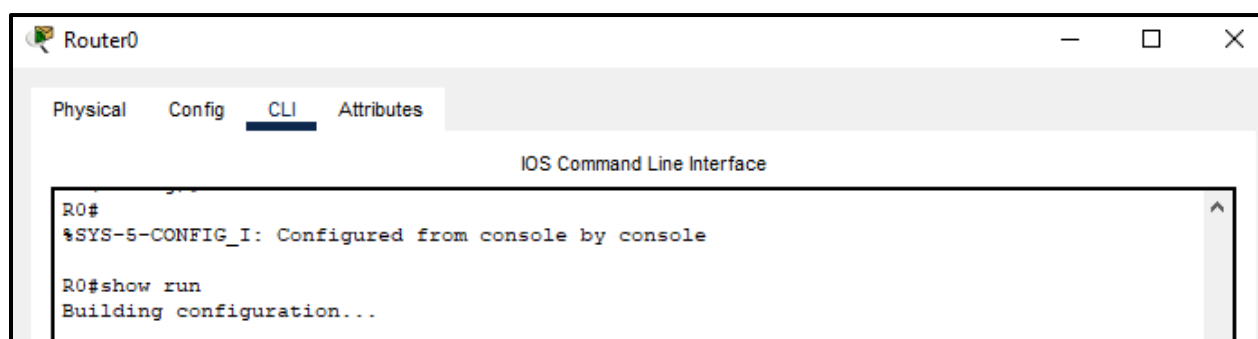
```

Router0
Physical Config CLI Attributes
IOS Command Line Interface

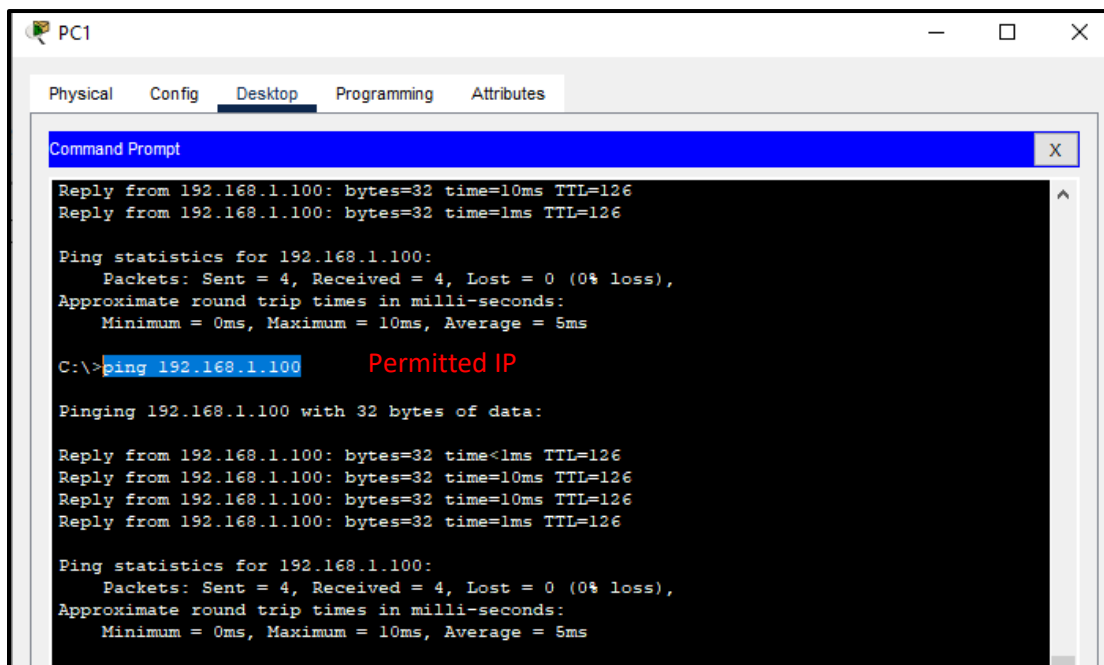
Router(config)#
Router(config)#int fa0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

```


Check using show run command



Step 7: Check the connection



PC1

Physical Config **Desktop** Programming Attributes

Command Prompt

```

Reply from 192.168.1.100: bytes=32 time=10ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

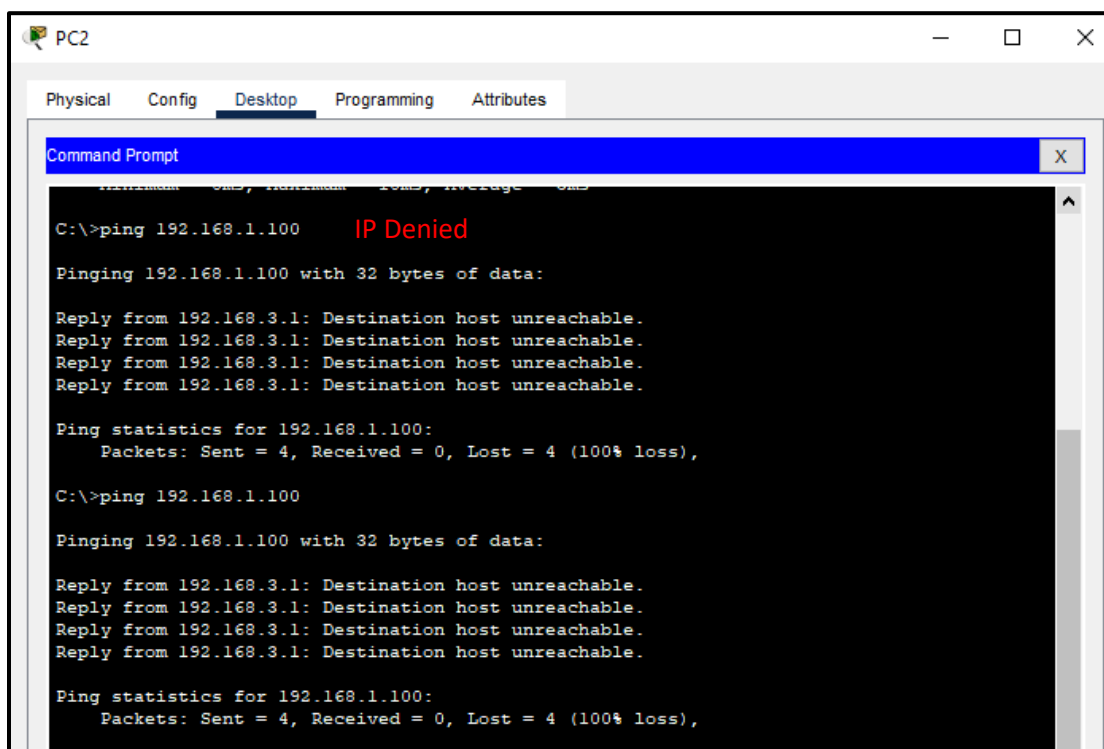
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>ping 192.168.1.100      Permitted IP

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time=10ms TTL=126
Reply from 192.168.1.100: bytes=32 time=10ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 5ms
  
```



PC2

Physical Config **Desktop** Programming Attributes

Command Prompt

```

C:\>ping 192.168.1.100      IP Denied

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.100

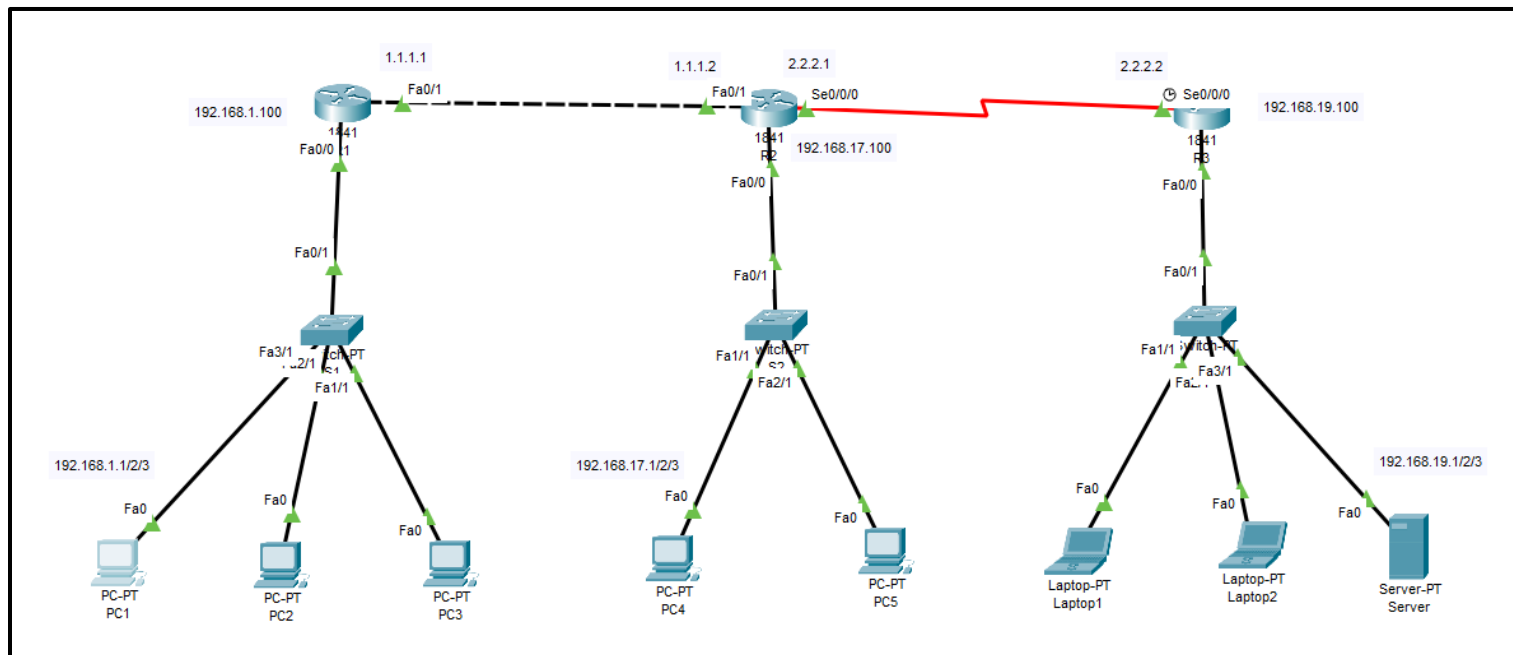
Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

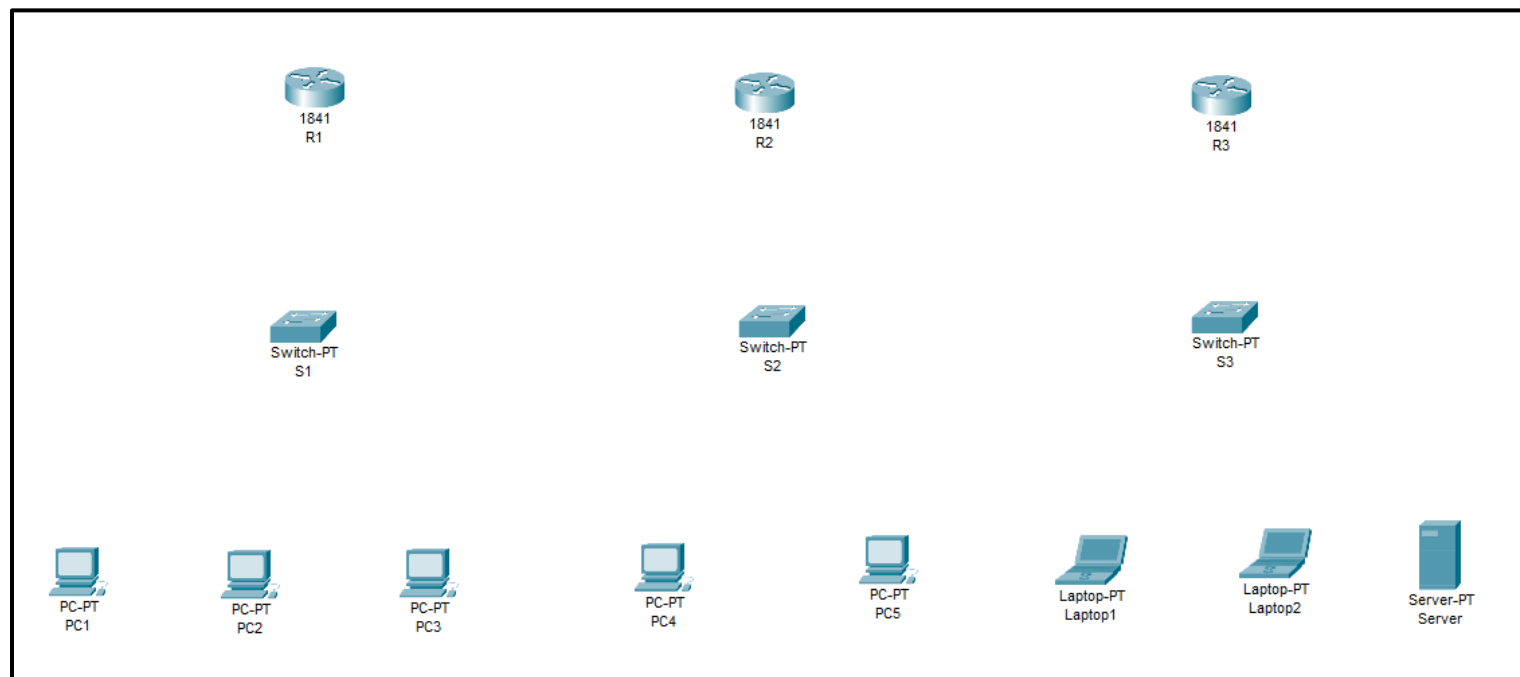
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

- **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.

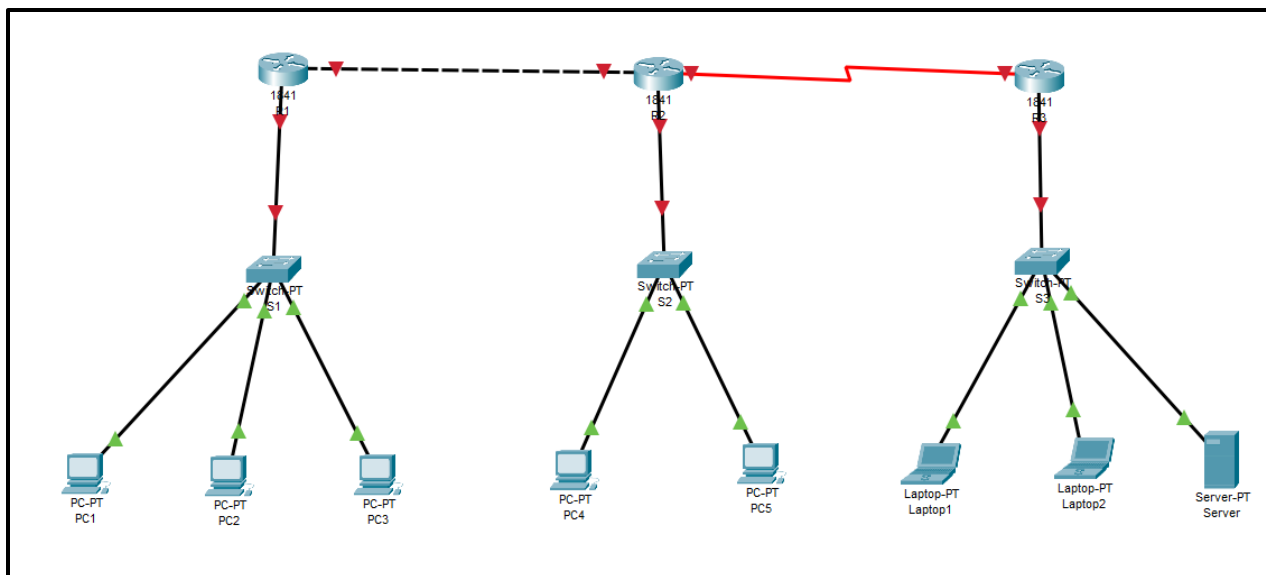
Cisco Packet tracer Setup:



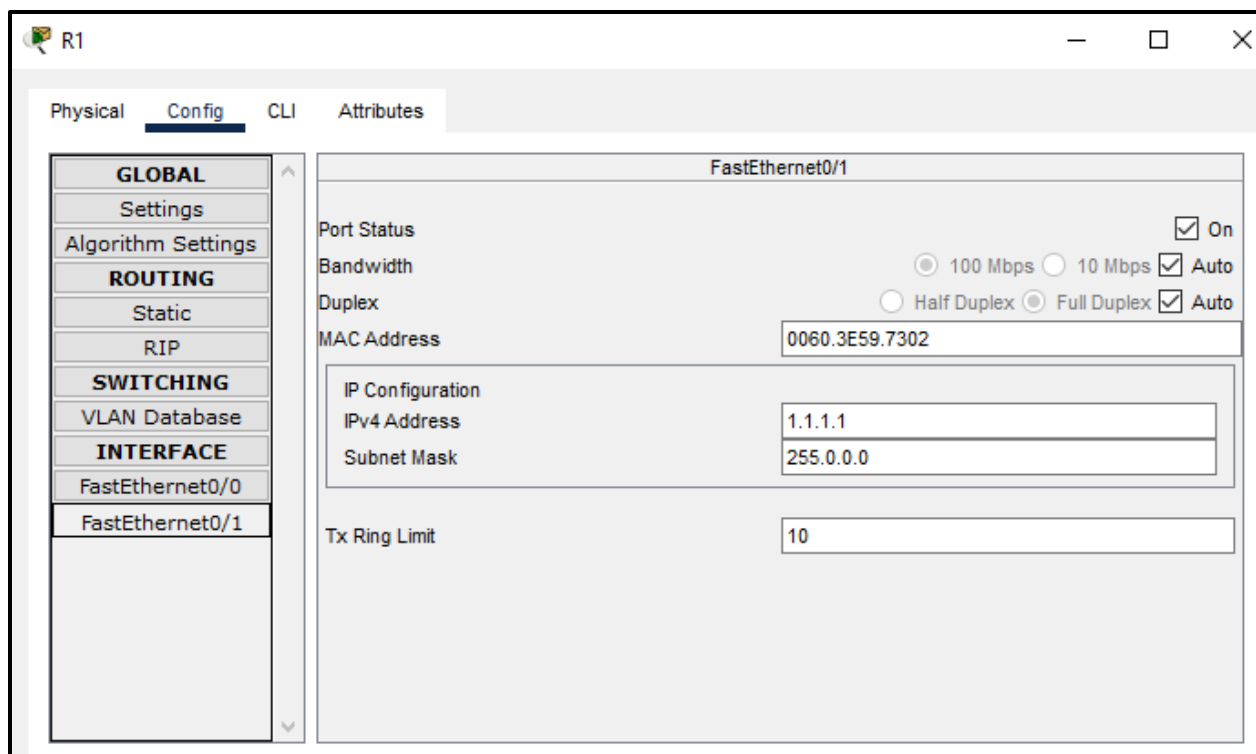
Step 1: Arranging devices

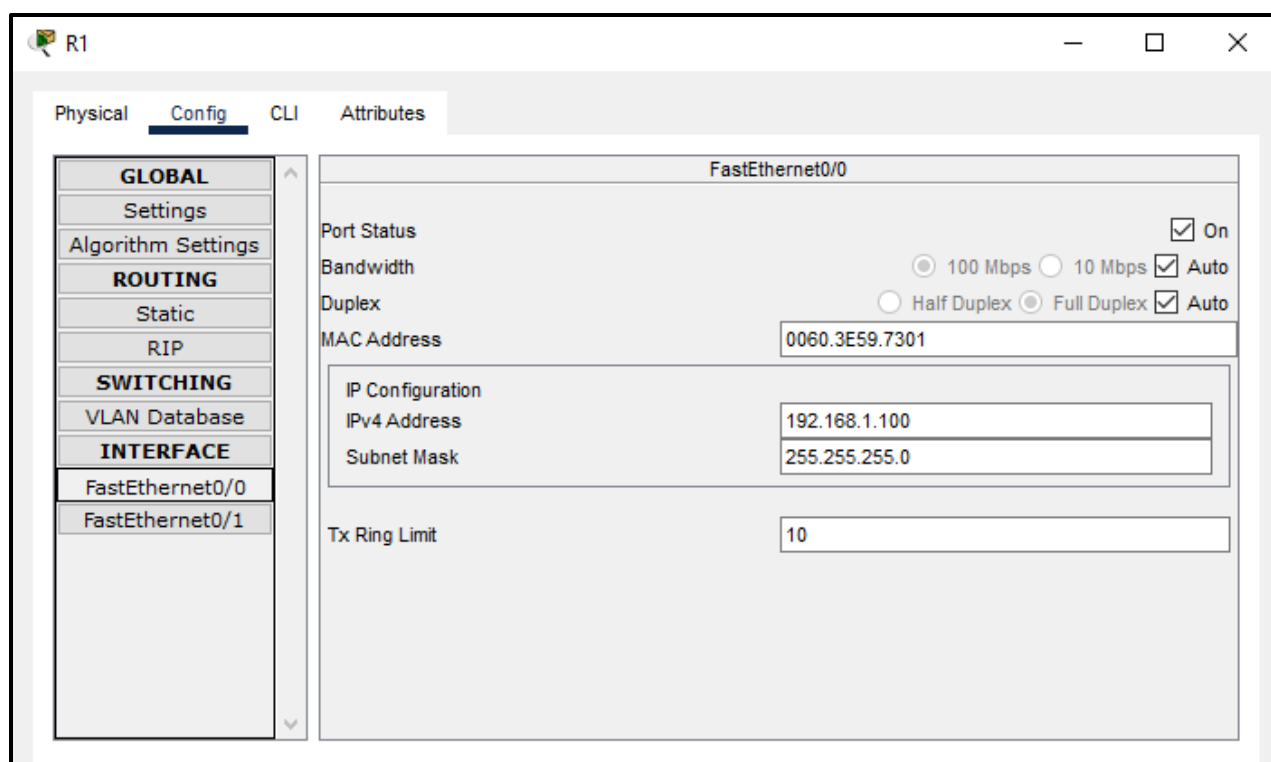
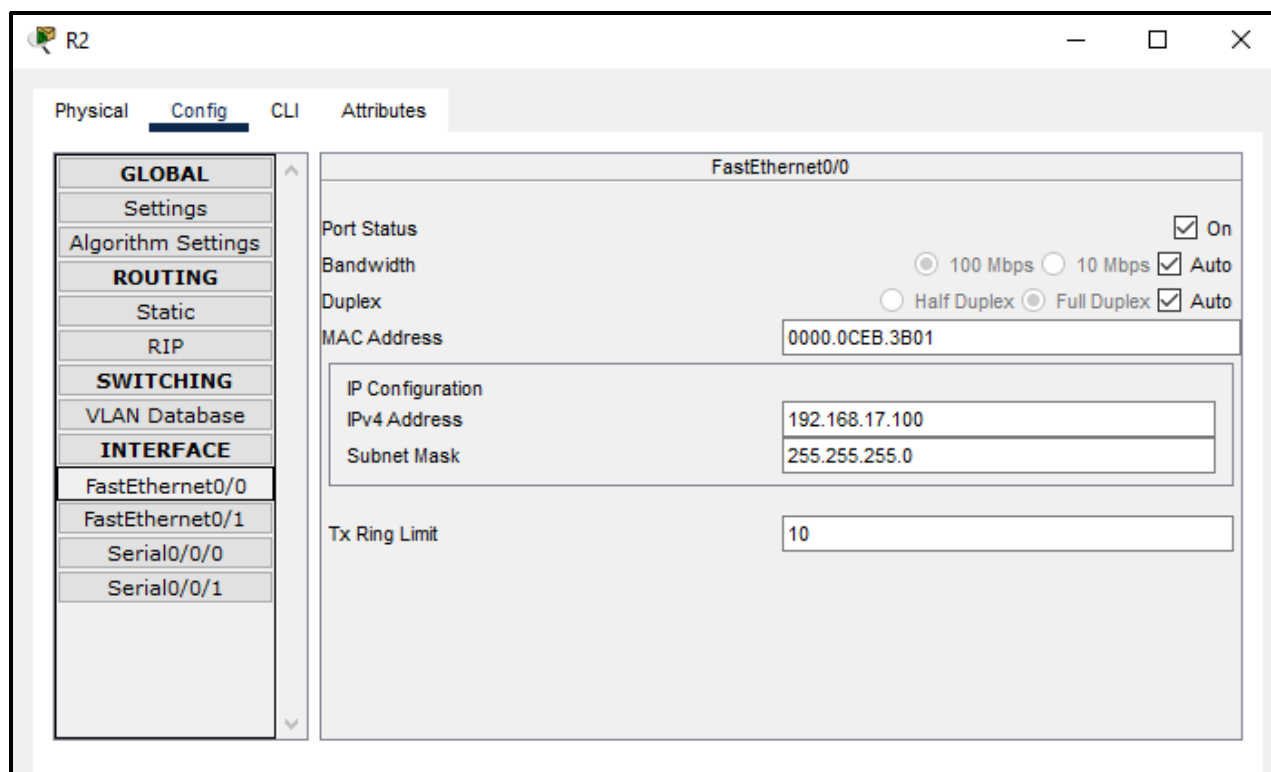


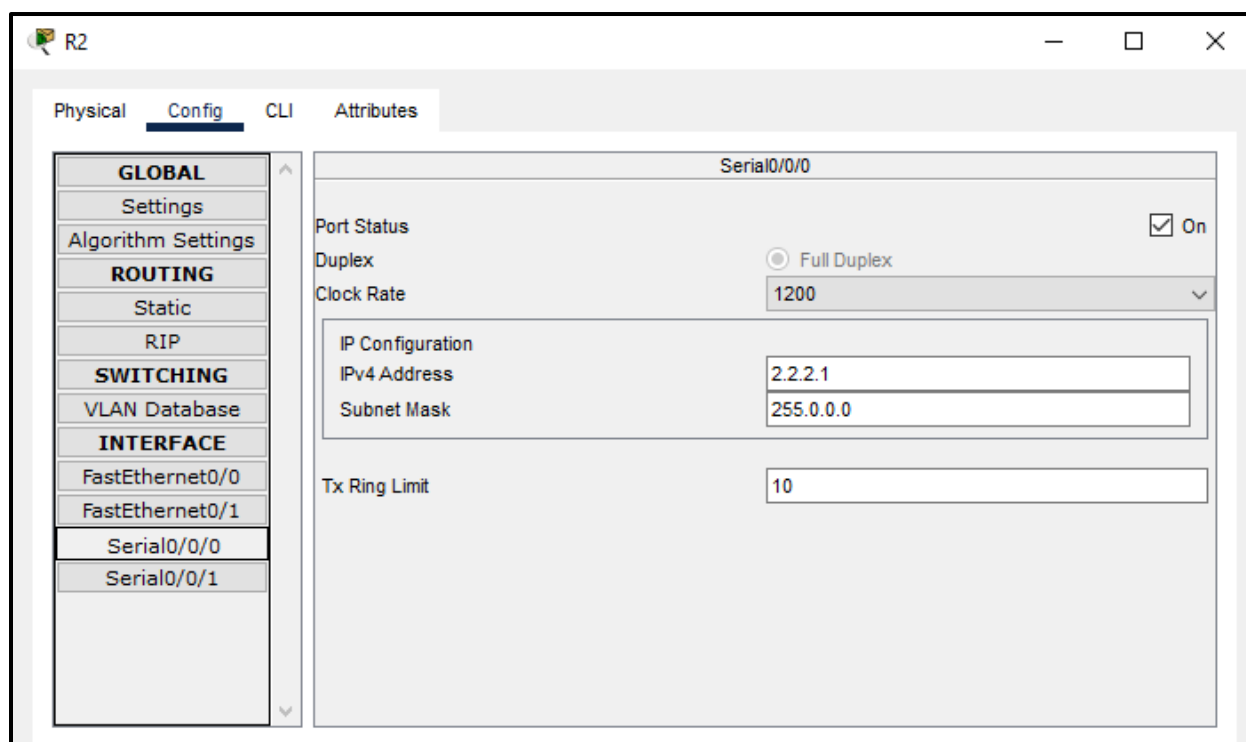
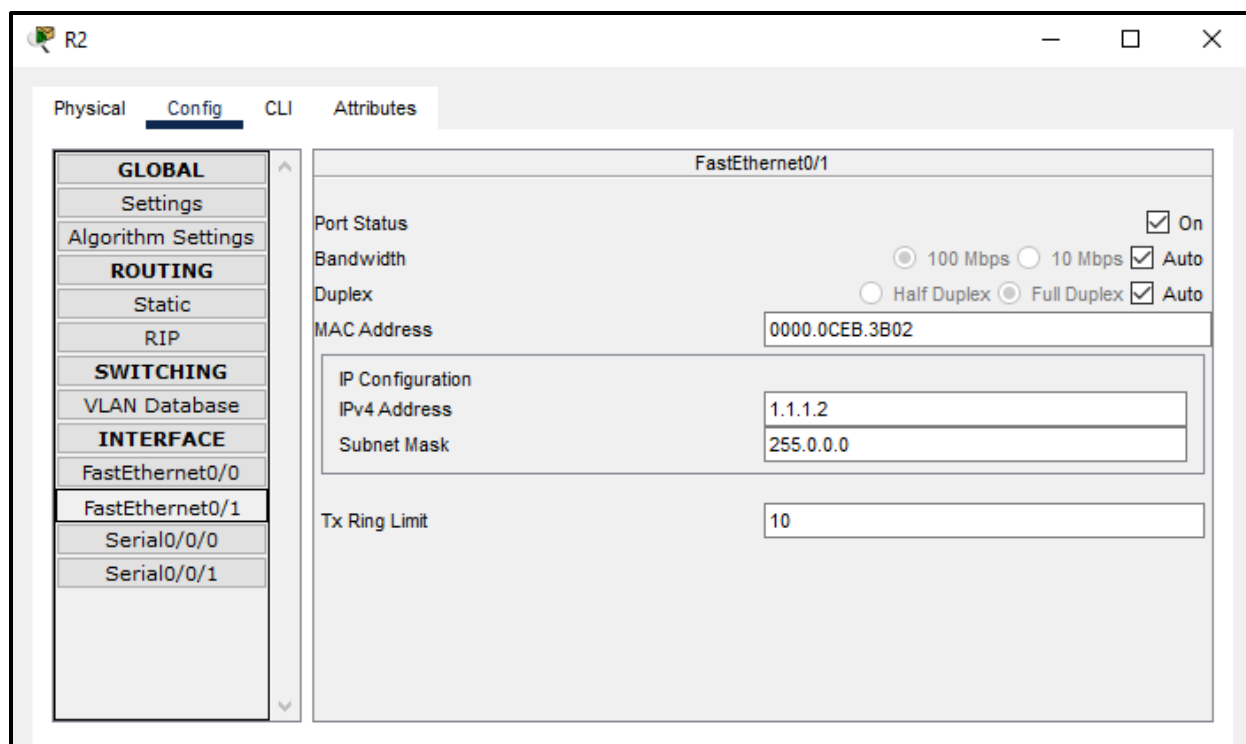
Step 2: Creating connection with respective cable.

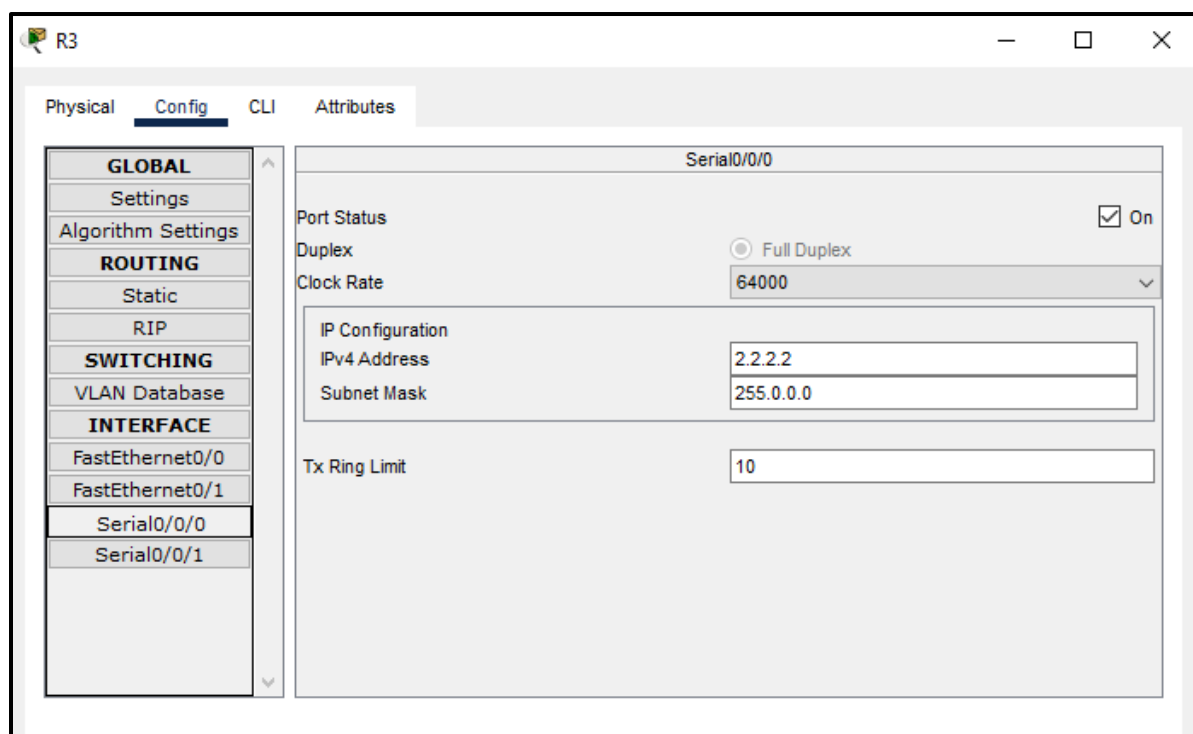
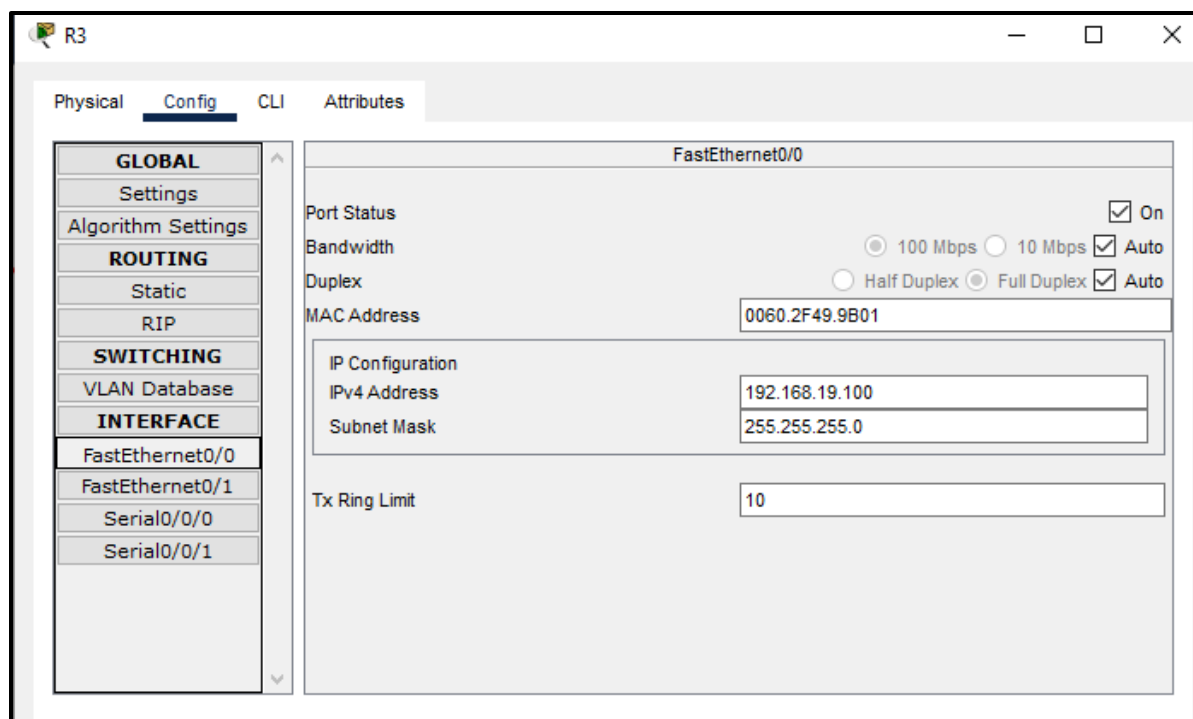


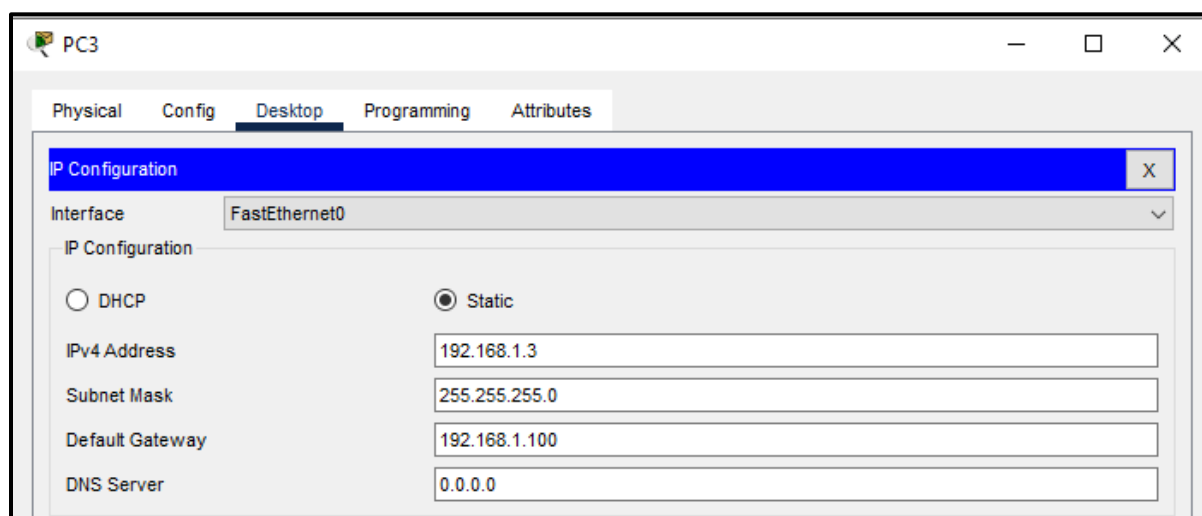
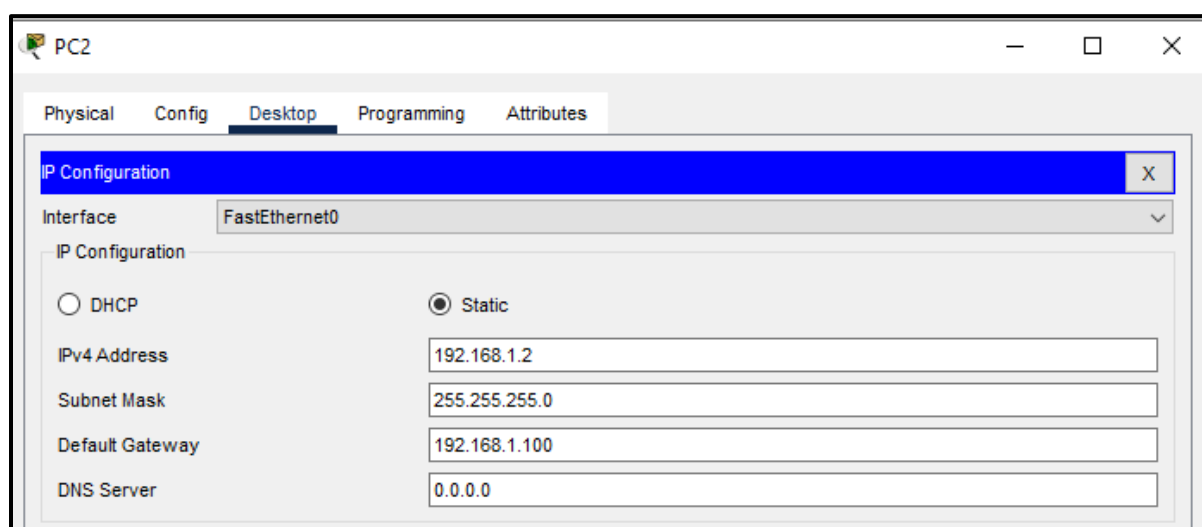
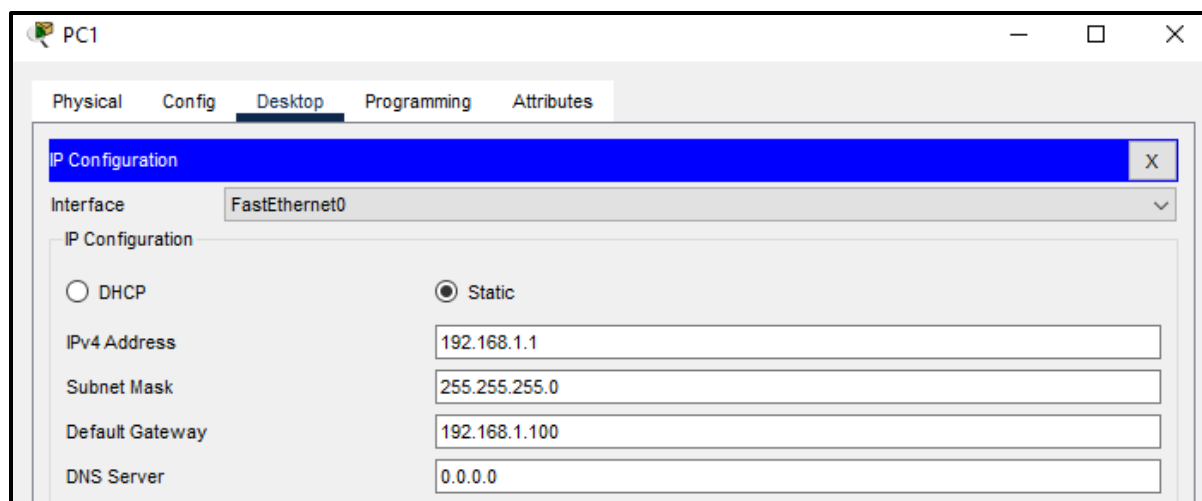
Step 3: Configure all devices and give them IP address. (We can use DHCP also I done by giving IP address manually)

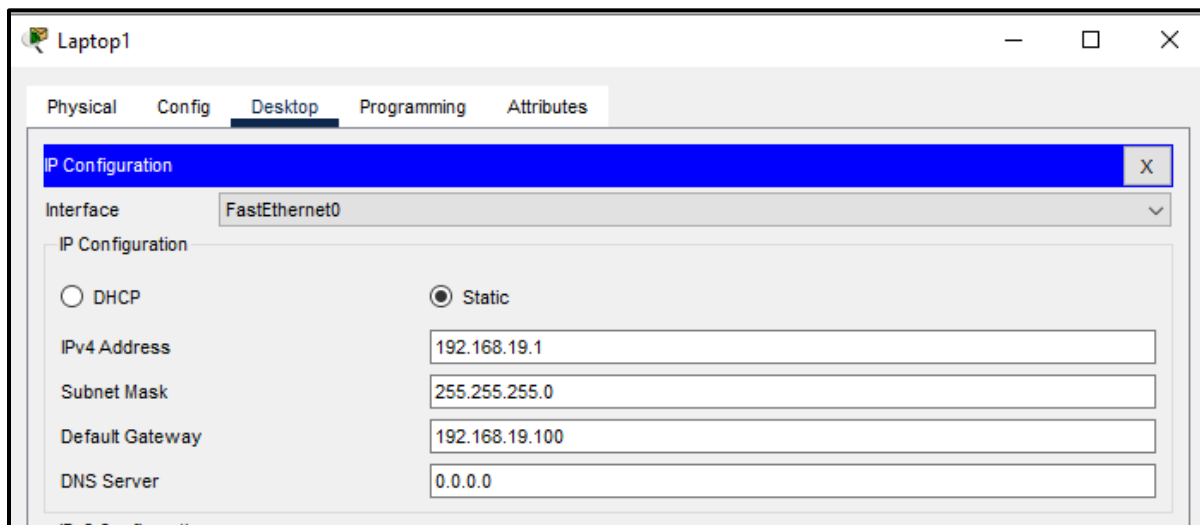
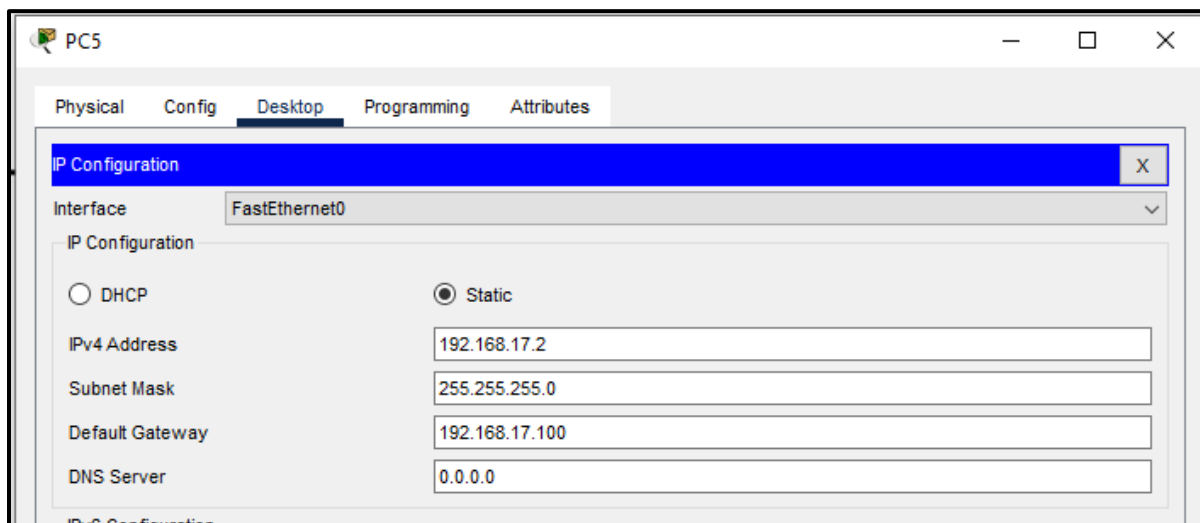
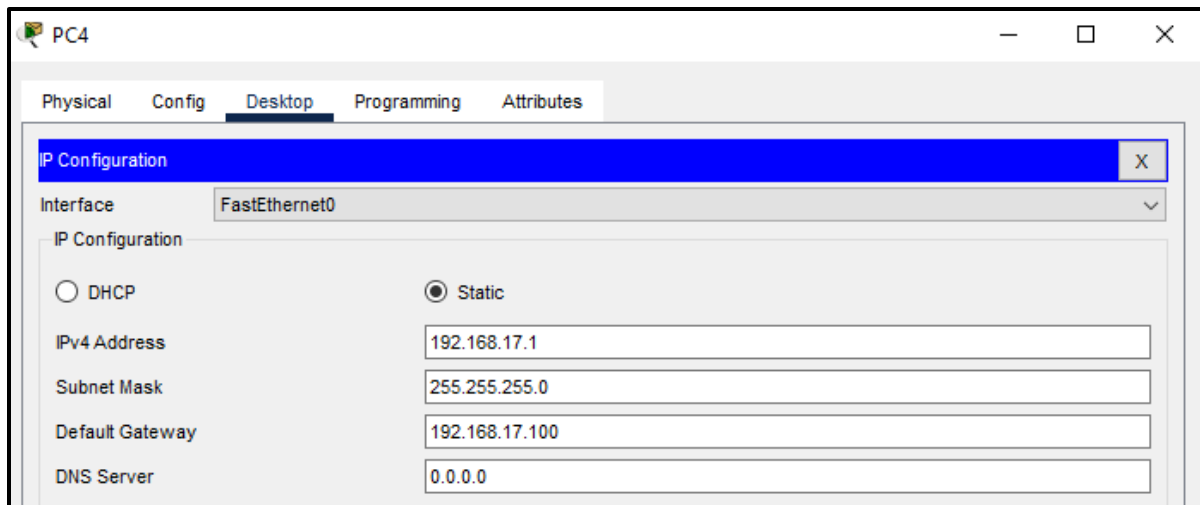












Laptop2

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

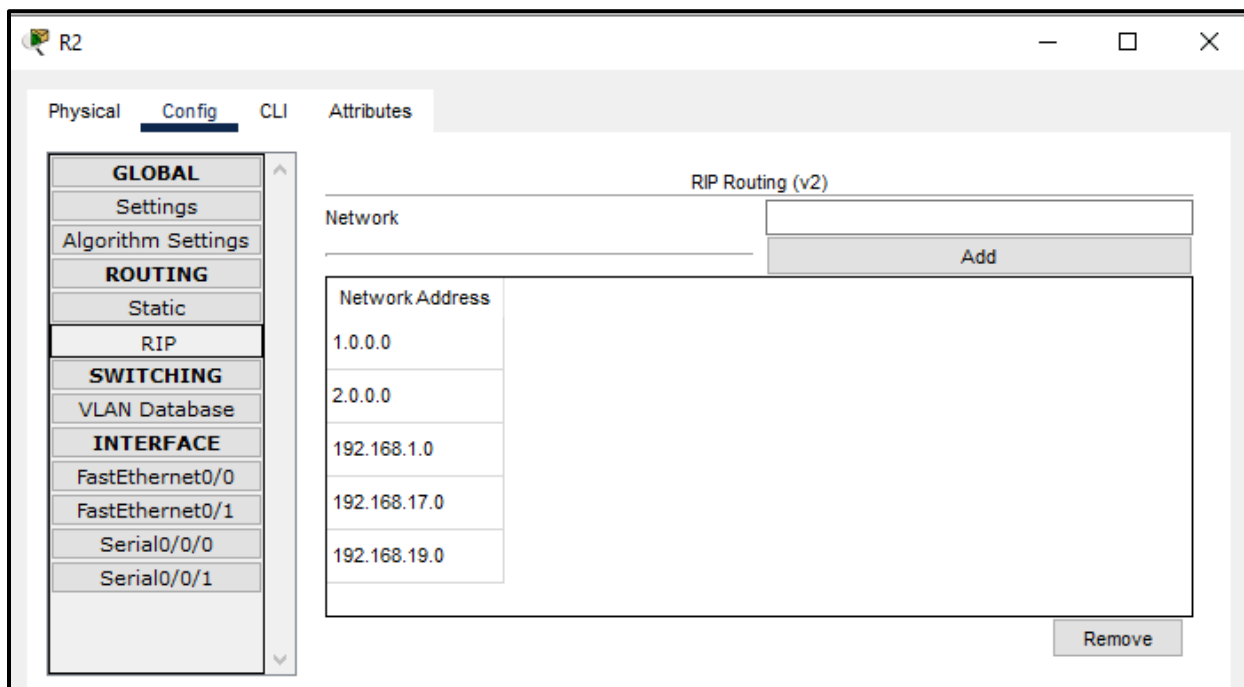
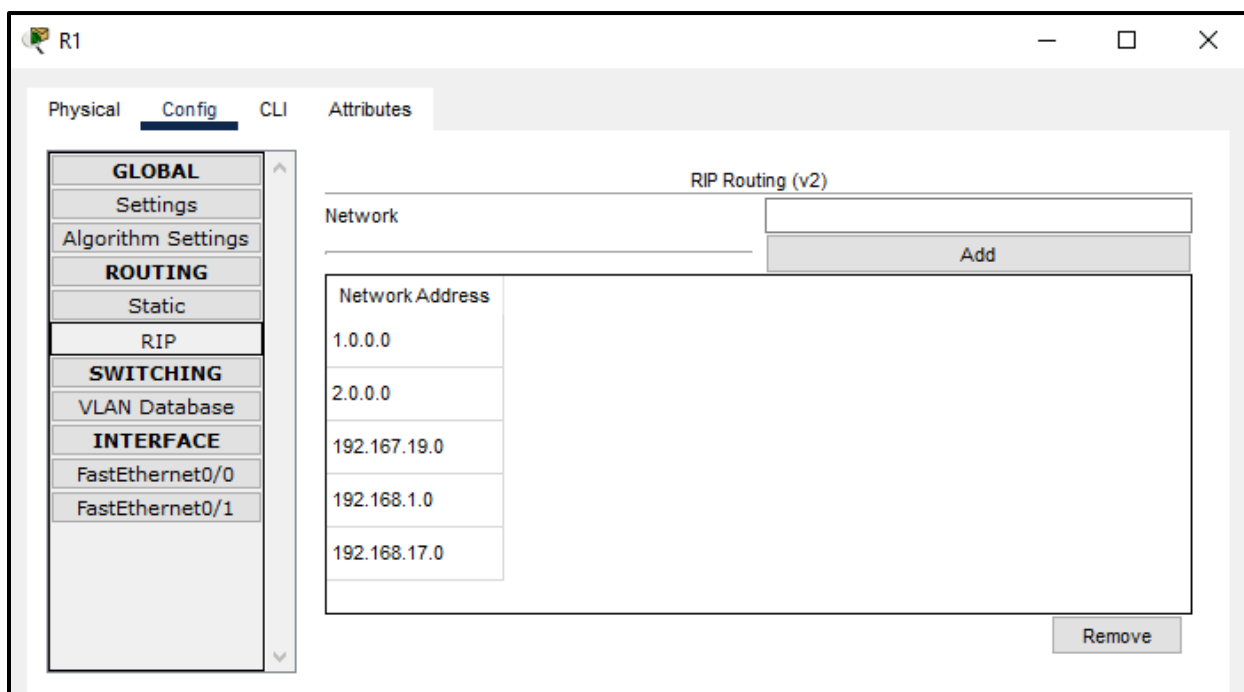
IPv4 Address 192.168.19.3

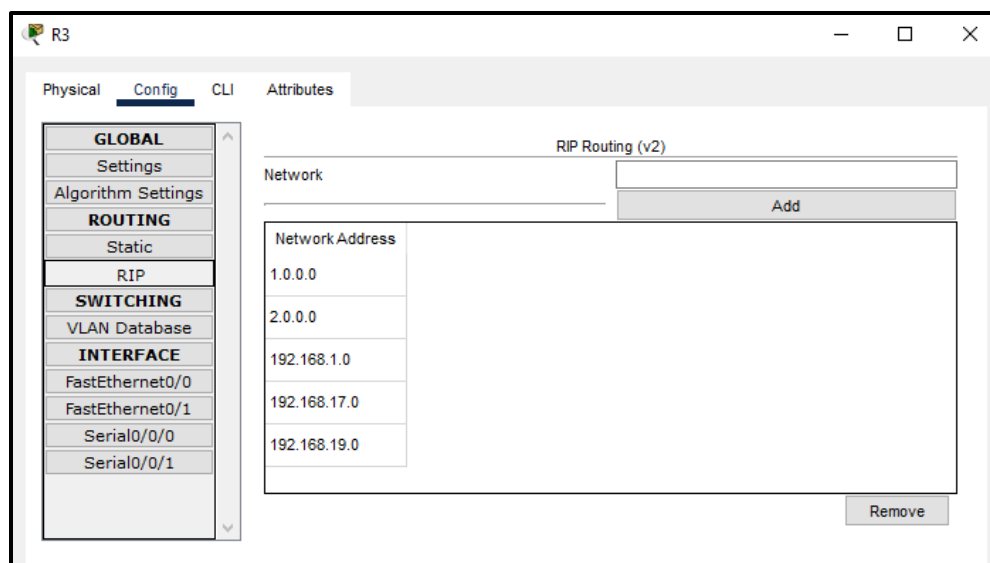
Subnet Mask 255.255.255.0

Default Gateway 192.168.19.100

DNS Server 0.0.0.0

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

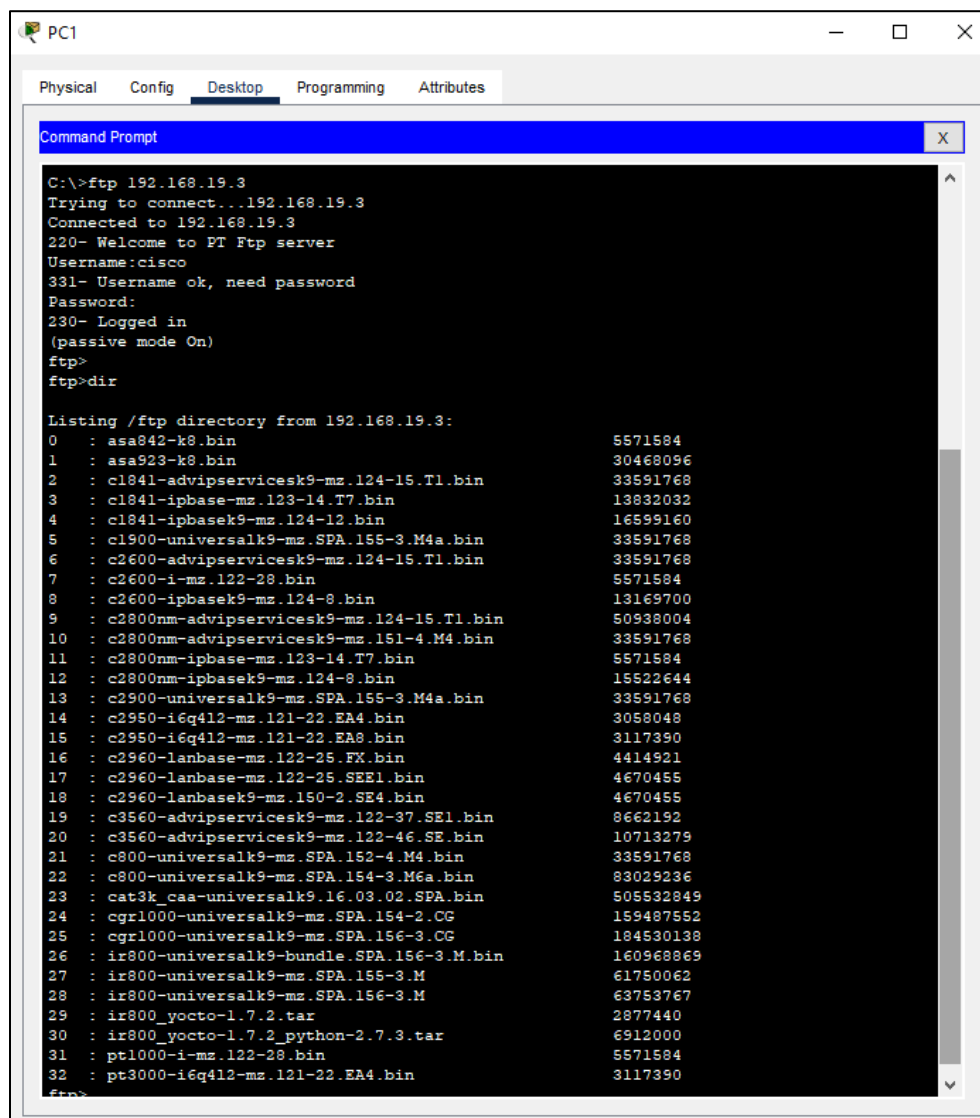
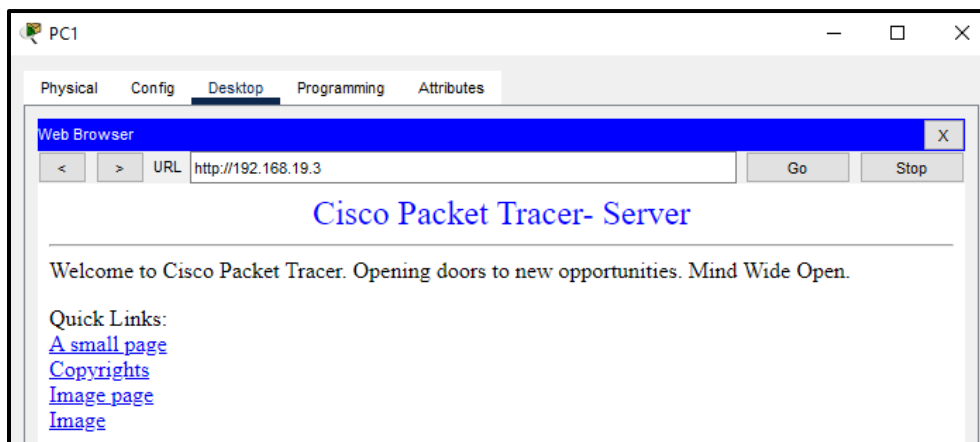




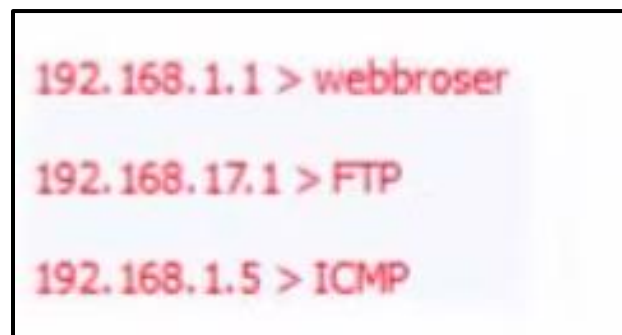
Check the connection:

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



```

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#
  
```

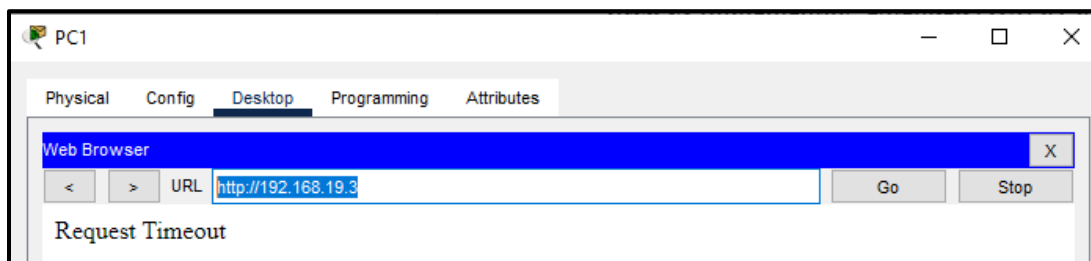
Ctrl+F6 to exit CLI focus

Copy Paste

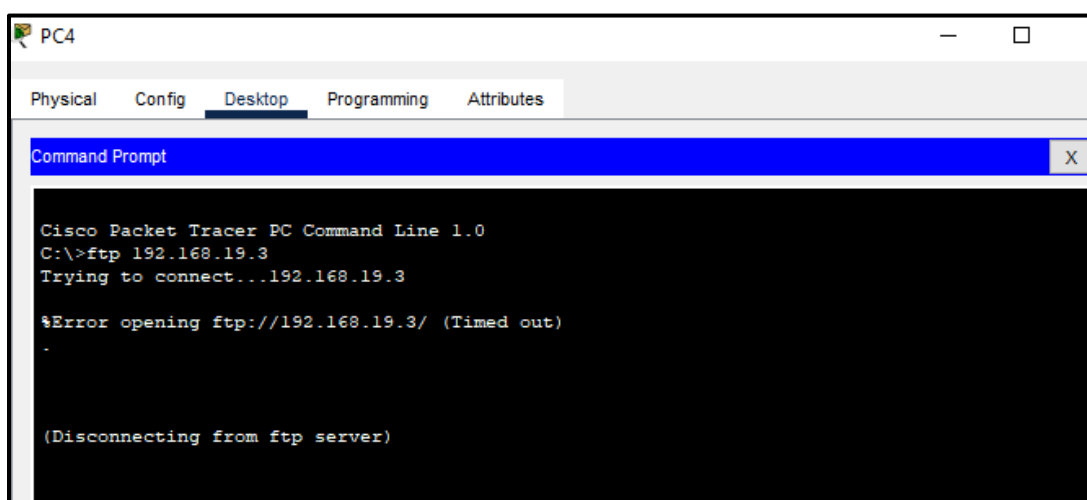
☐ Top

Step 6: Check the blocked IPs and their Blocked Services

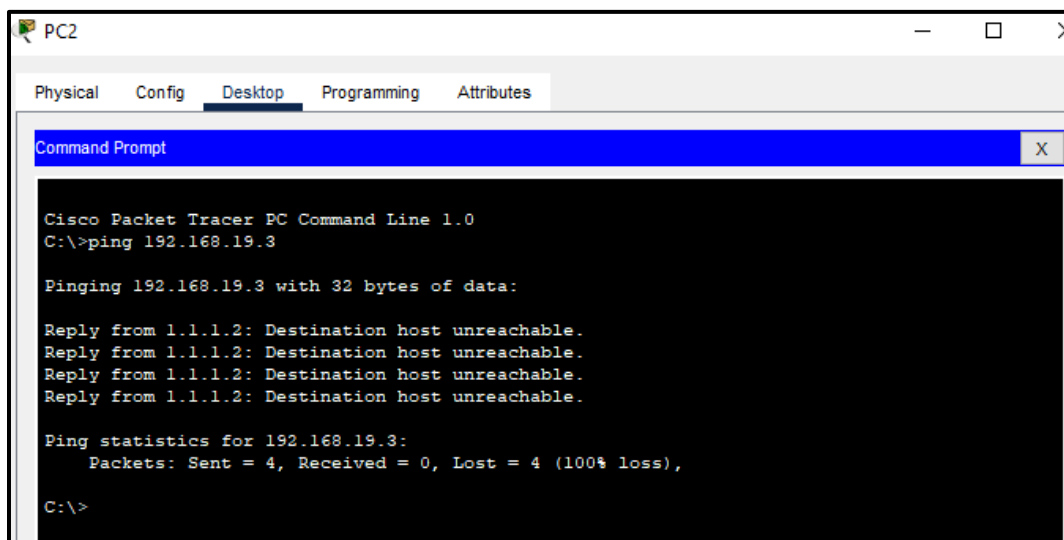
192.168.1.1 > webbroser



192.168.17.1 > FTP



192.168.1.5 > ICMP



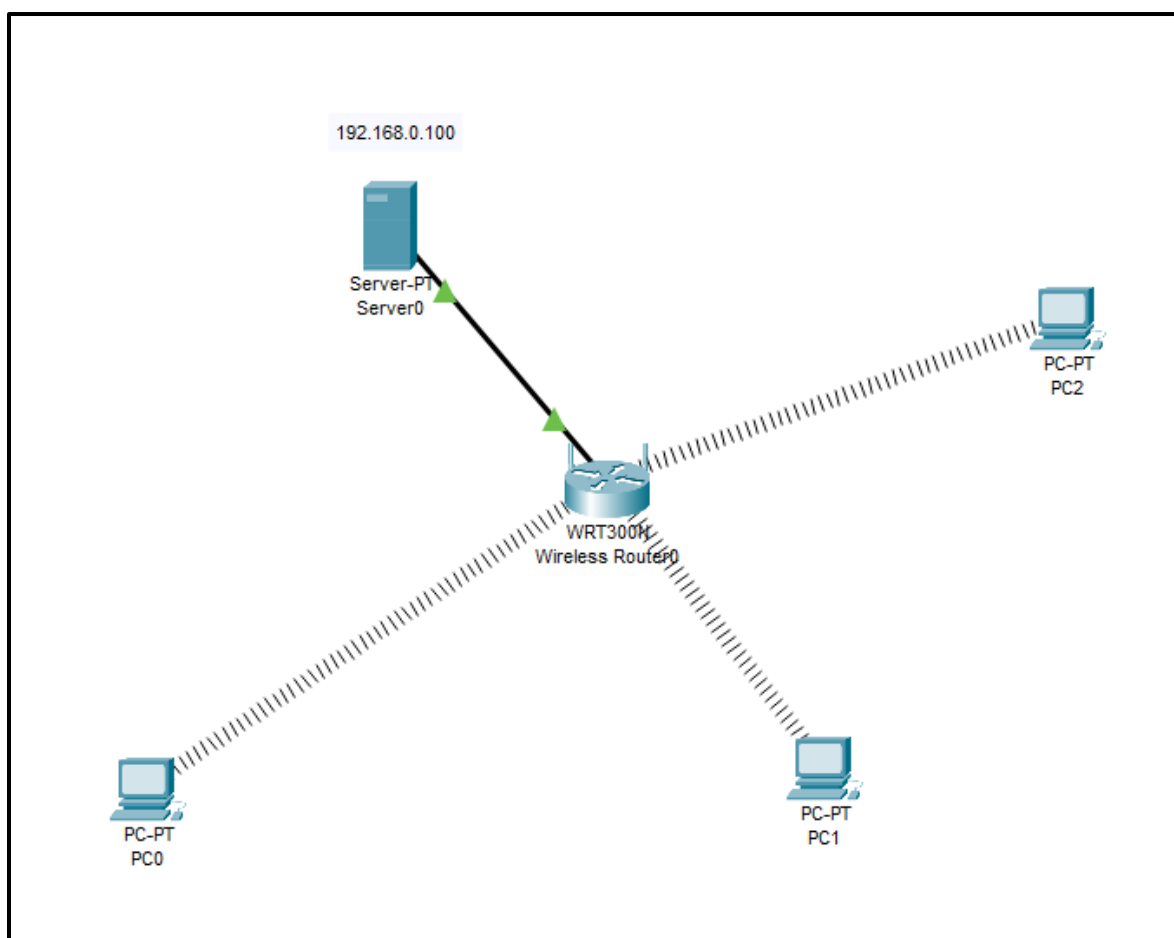
Practical No: 04

Aim: Planning Network-based Firewalls

Components: Wireless Router, Server, PC

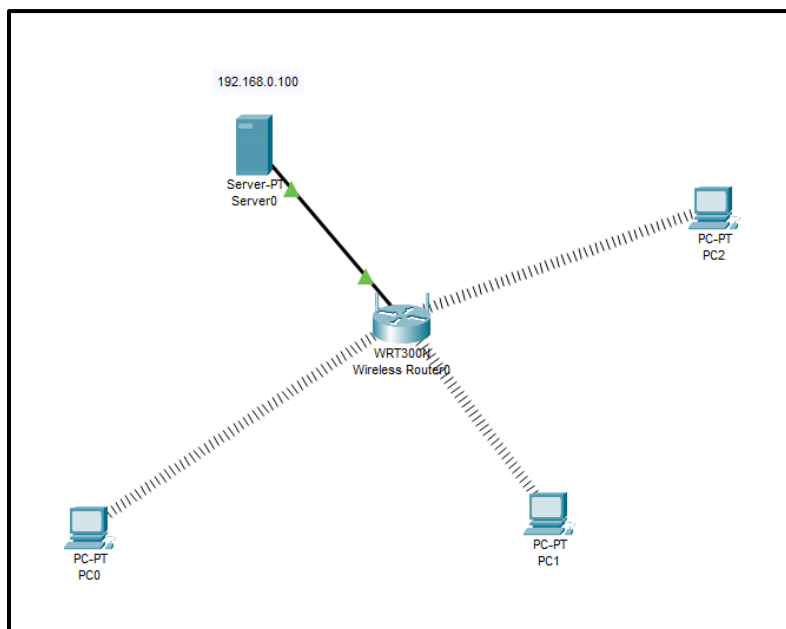
Theory: Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies – any other traffic attempting to access the network is blocked.

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

Wireless Router0

Physical Config GUI Attributes

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ☒ Enabled ☐ Disabled

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

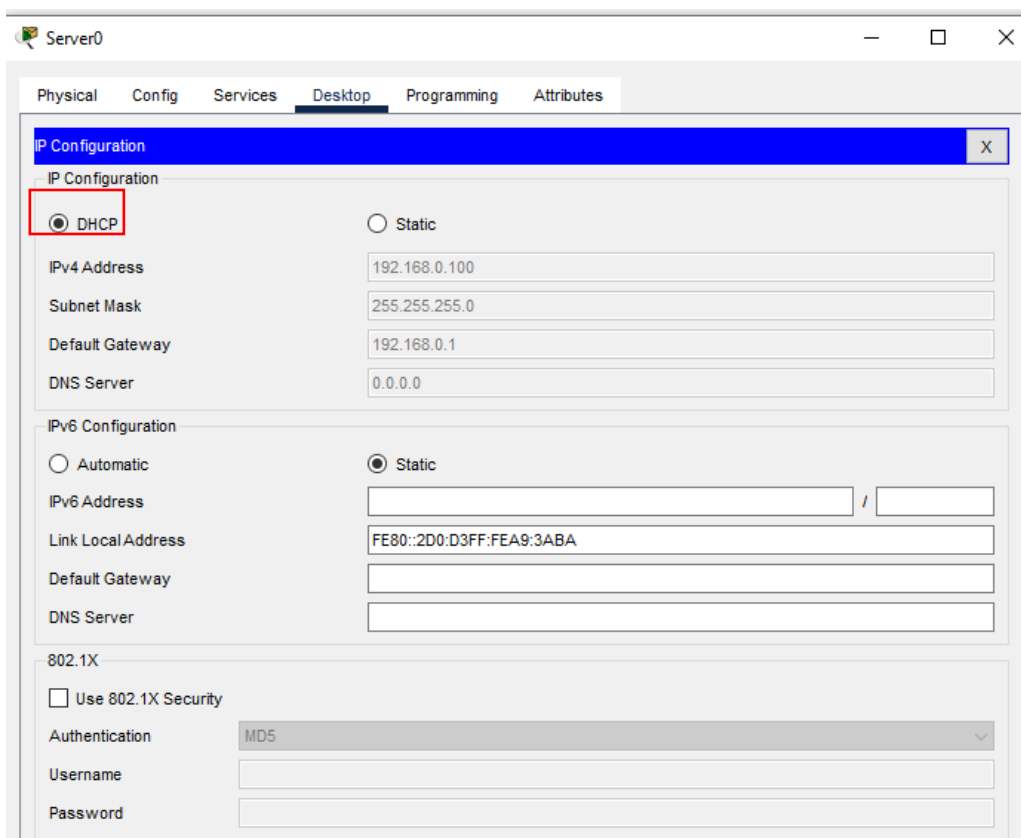
Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

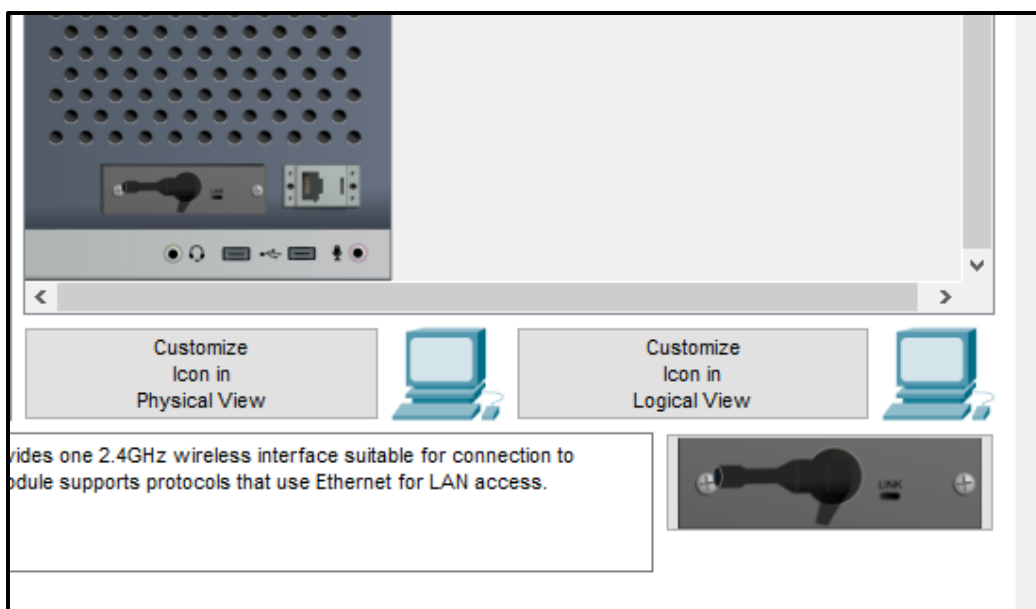
Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Step 3: Configure Server

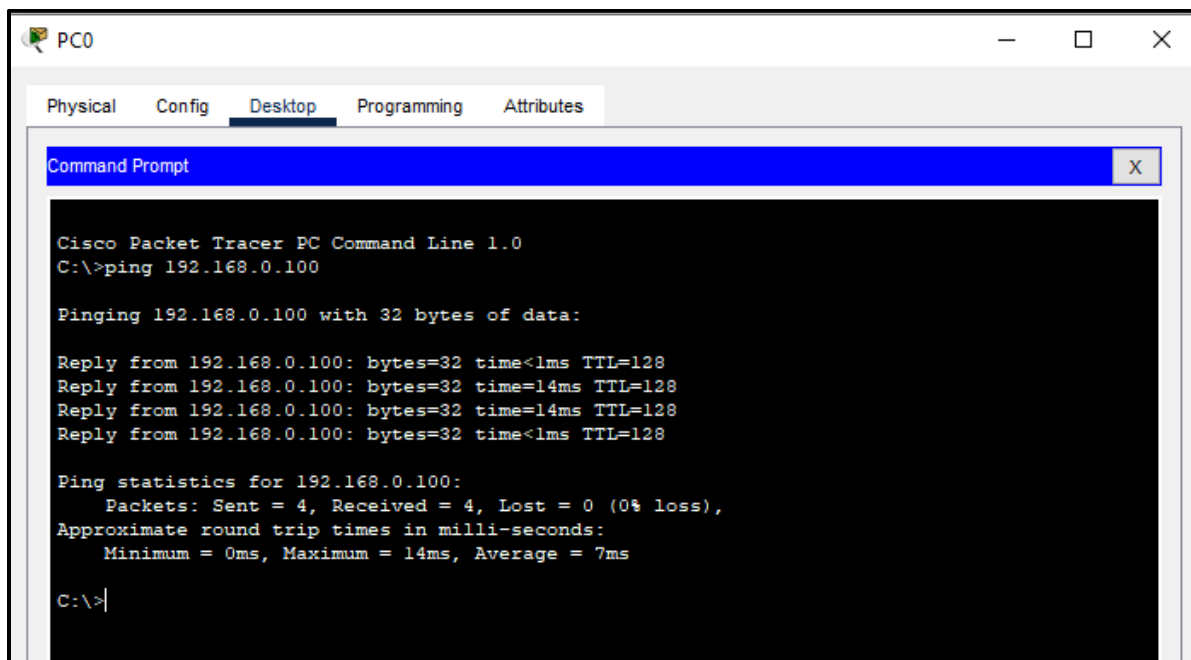


Step 4: Configure and connect all PC's to wireless router Changing port to wireless adapter of all PC's



Step 5: Checking connection of pc's with server

After adding wireless adapter of all PC's they will automatically get connected with wireless router 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

Server0

Physical Config Services **Desktop** Programming Attributes

Firewall X

Service ☒ On ☐ Off

Interface FastEthernet0

Inbound Rules

Action Protocol

Remote IP Remote Wildcard Mask

Remote Port Local Port

Save Remove Add

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Deny	ICMP	0.0.0.0	255.255.255.255	-	-
2	Allow	IP	0.0.0.0	255.255.255.255	-	-

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

```
Approximate round trip times in milli-seconds:
  Minimum = 26ms, Maximum = 41ms, Average = 32ms

C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

But we can access the server data (view)



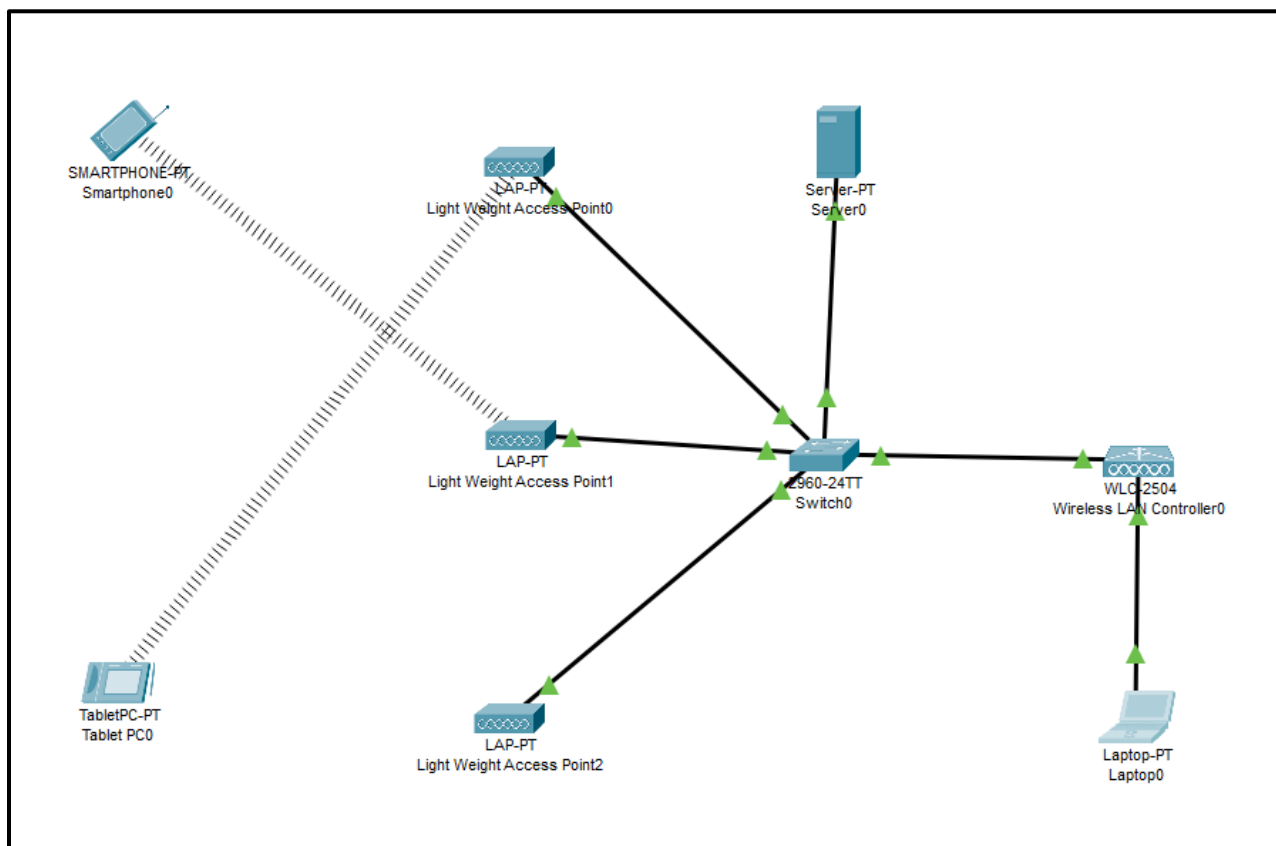
Practical No: 05

Aim: Configure Auto Profiles ACU Utilities

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

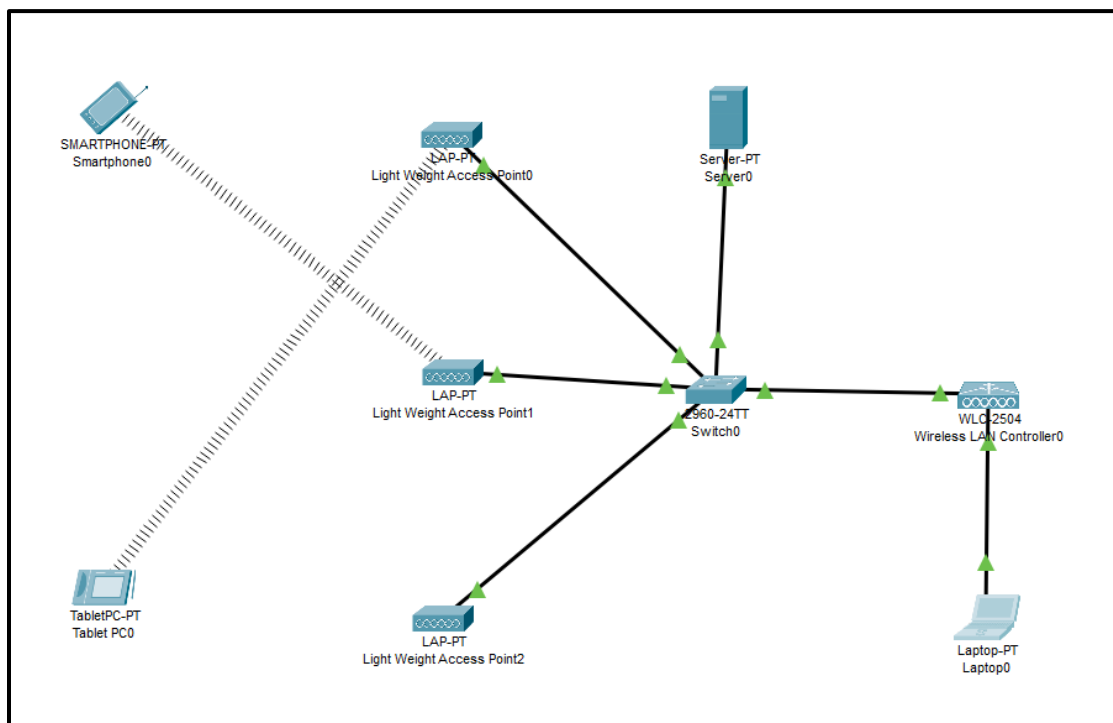
Theory: ACU is a device that enables equipment, such as computers and card dialers, to originate calls automatically over a telecommunications network.

Cisco Packet Tracer Setup:-

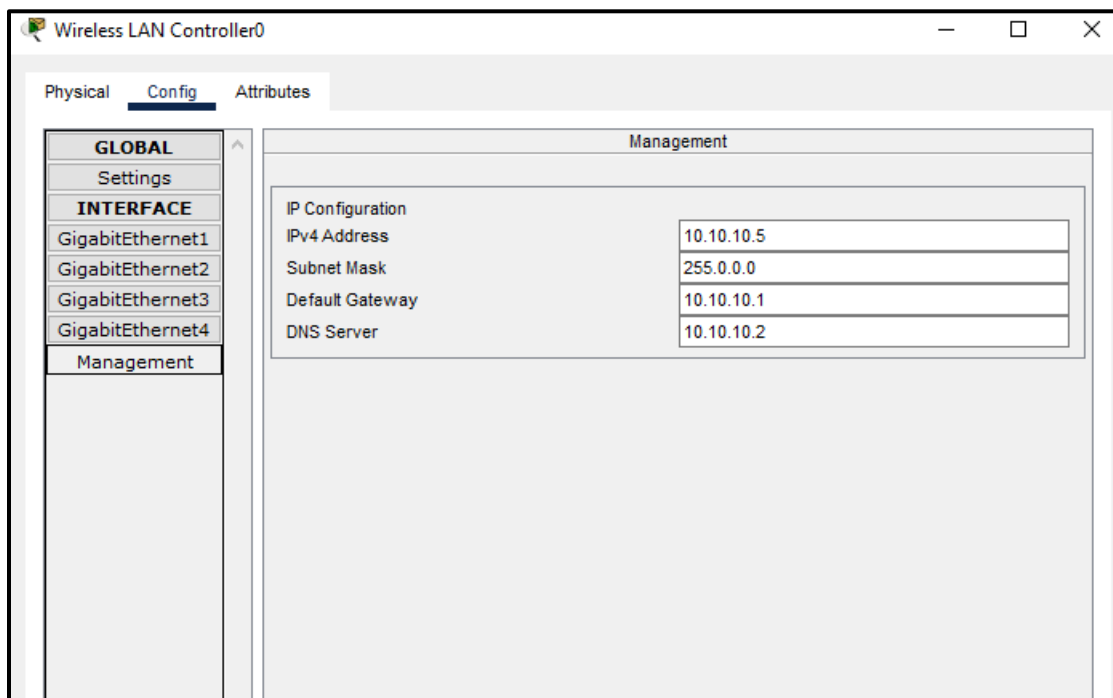


Implementation:

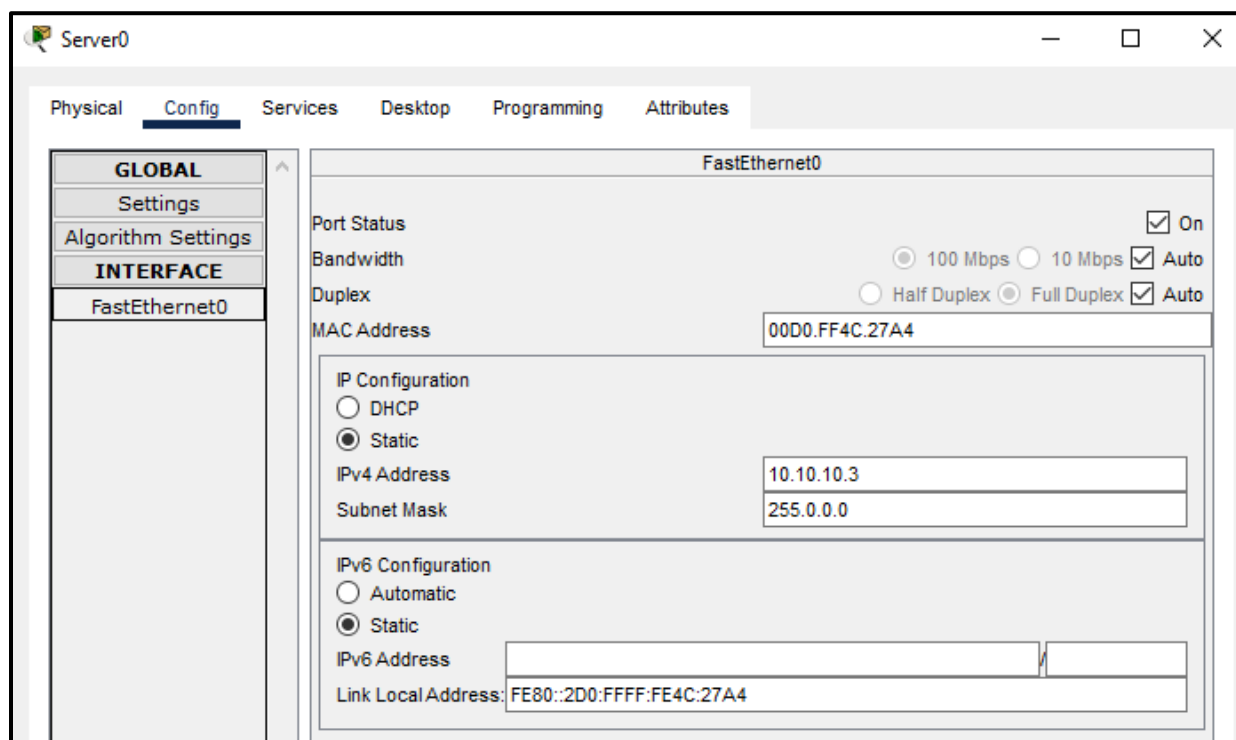
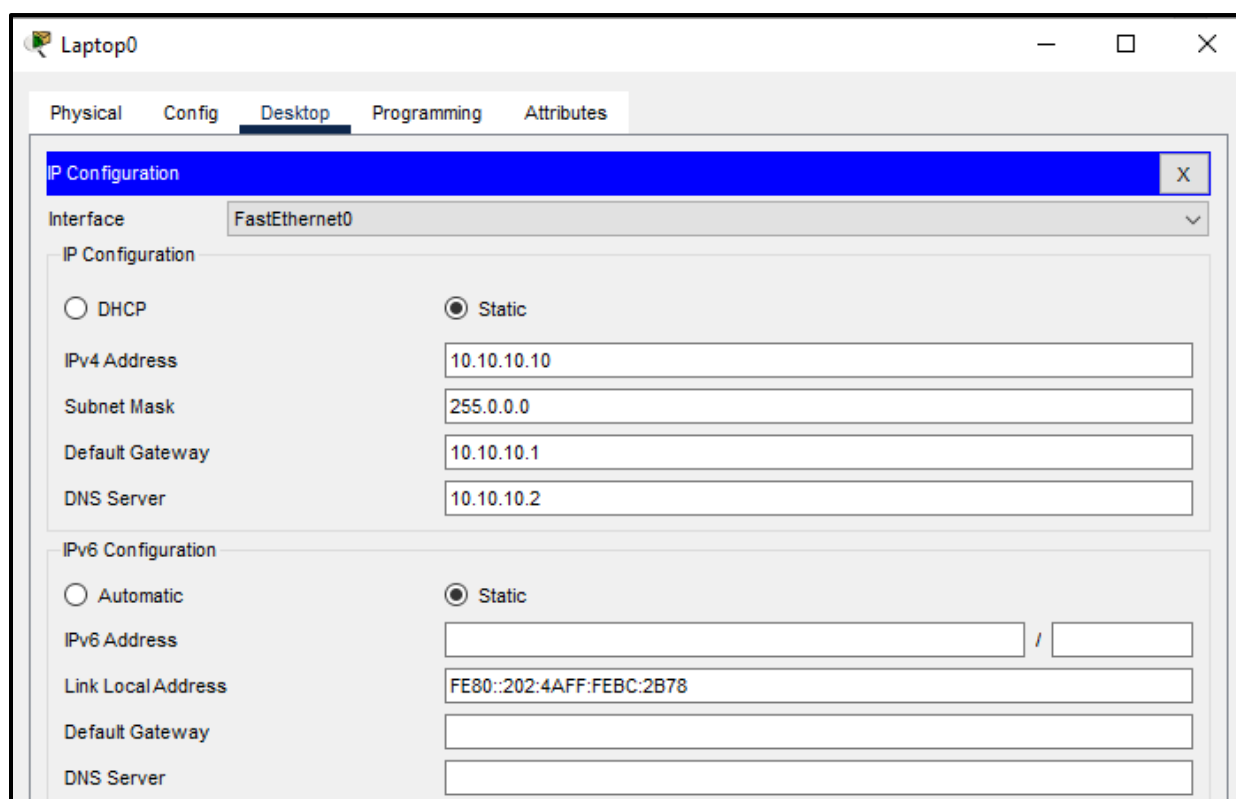
Step 1: Arranging devices and creating connections



Step 2: WLC (Wireless LAN Controller)



Step 3: Configuring Laptop and server and checking connection



Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 10.10.10.0

DNS Server: 10.10.10.2

Start IP Address: 10 10 10 100

Subnet Mask: 255 0 0 0

Maximum Number of Users: 100

TFTP Server: 0.0.0.0

WLC Address: 10.10.10.5

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	10.10.10.0	10.10.10.2	10.10.10.100	255.0.0.0	100	0.0.0.0	10.10.10.5

Check the connection

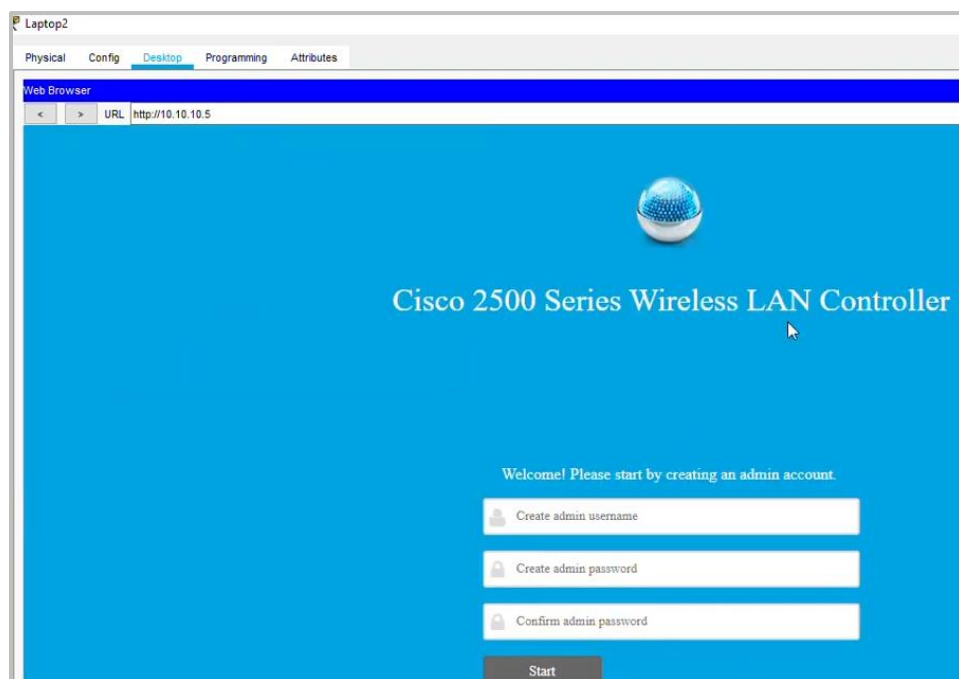
```
C:\>ping 10.10.10.5

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>)

1 Set Up Your Controller

System Name

Country

Date & Time

Timezone

NTP Server

Management IP Address

Subnet Mask

Default Gateway

Management VLAN ID

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

DHCP Server Address -

✗ Guest Network

3 Advanced Settings

✗ RF Parameter Optimization

Virtual IP Address 192.0.2.1

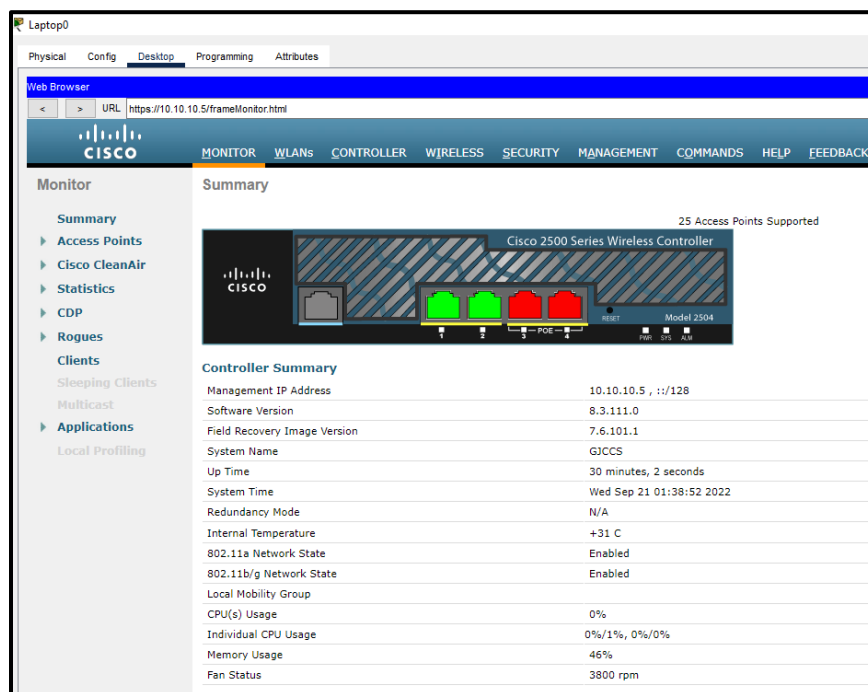
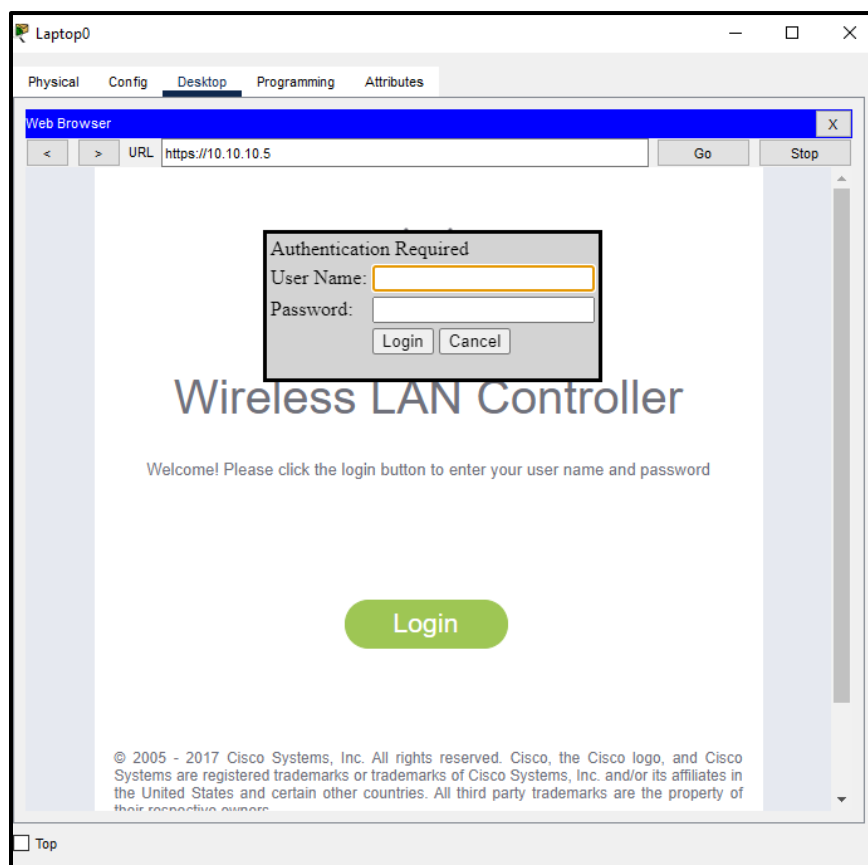
Local Mobility Group Default

Back Apply

Saving the configuration...

This may take a minute.

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



Check the Access points AP's

Web Browser URL: https://10.10.10.5/frameWireless.html

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
- Mesh
- ATF
- RF Profiles
- FlexConnect Groups

All APs

Current Filter: [Change Filter] [Clear Filter]

Number of APs: 3

AP Name	IP Address(Ipv4/Ipv6)	AP Model
Light Weight Access Point0	10.10.10.101	PT-AIR-CAP1000I-A-K9
Light Weight Access Point2	10.10.10.102	PT-AIR-CAP1000I-A-K9
Light Weight Access Point1	10.10.10.100	PT-AIR-CAP1000I-A-K9

Go to WLAN's make SSID for STUDENT to Student

Web Browser URL: https://10.10.10.5/frameWLANs.html

WLANs

- WLANs
- Advanced
 - AP Groups

WLANs

Current Filter: [Change Filter] [Clear Filter]

Create New [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	STUDENT	STUDENT	Enabled	[WPA2][Auth(PSK)]

Web Browser URL: https://10.10.10.5/frameAPGroupEdit.html

WLANs

- WLANs
- Advanced
 - AP Groups

Ap Groups > Edit 'STUDENT'

General [WLANs] [RF Profile] [APs] [802.11u] [Location] [Ports/Module]

Apply

AP Group Name: STUDENT

AP Group Description: Student AP

NAS-ID: none

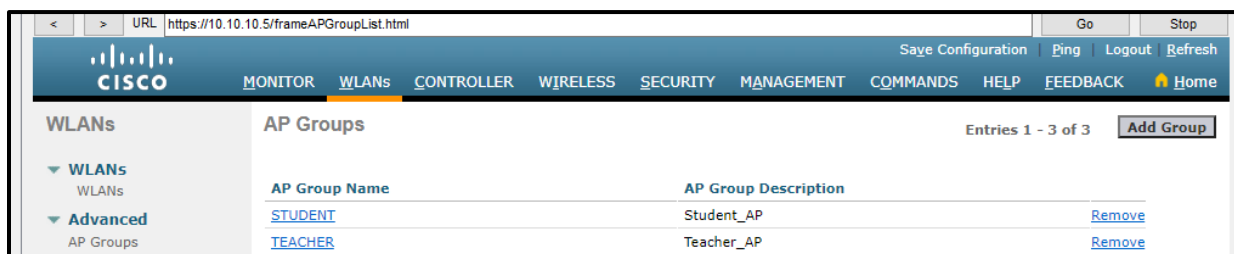
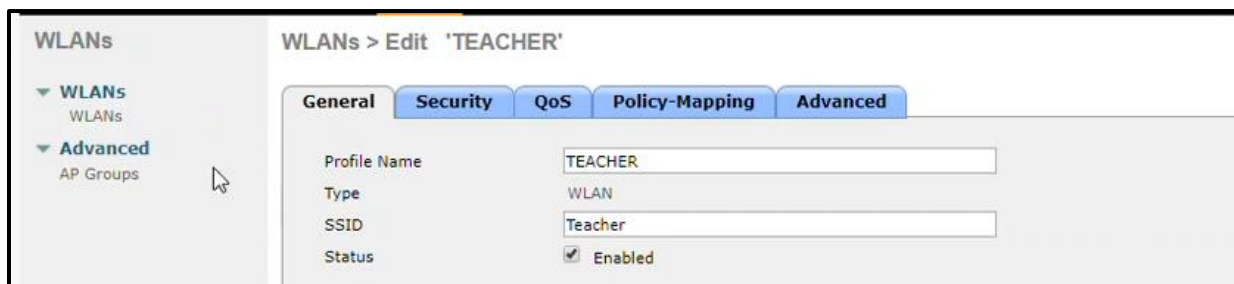
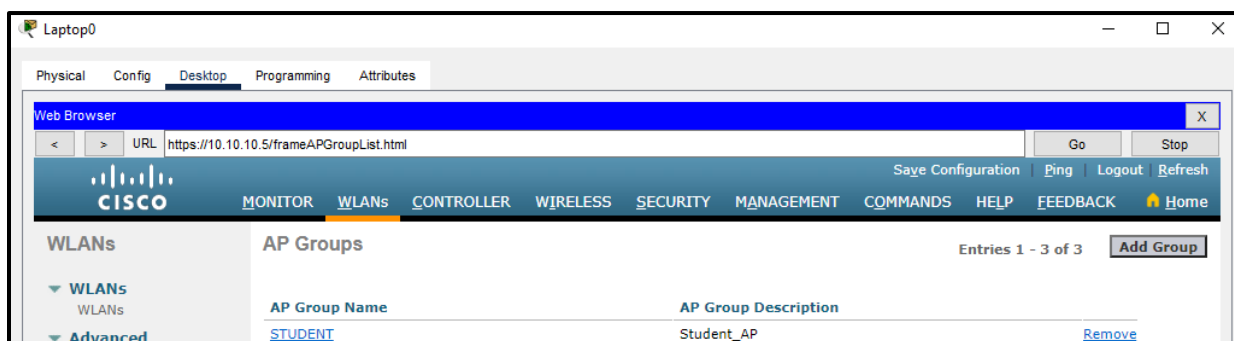
Enable Client Traffic QinQ: ☐

Enable DHCPv4 QinQ: ☐

QinQ Service Vlan Id: 0

CAPWAP Preferred Mode: ☐ Not-Configured

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



Step 7: Create AP Groups for TEACHER and STUDENT



WLANs

▼ WLANs
WLANs

▼ Advanced
AP Groups

AP Groups

Entries 1

Add New AP Group

AP Group Name: STUDENT

Description: Student AP

Add Cancel

Assign wireless LAN to AP

Physical Config Desktop Programming Attributes

Web Browser

URL: https://10.10.10.5/frameAPGroupEdit.html

Go

Save Configuration Ping Logout

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

▼ WLANs
WLANs

▼ Advanced
AP Groups

Ap Groups > Edit 'STUDENT'

< Back

General WLANs RF Profile APs 802.11u Location Ports/Module

Add New

WLANs

▼ WLANs
WLANs

▼ Advanced
AP Groups

Ap Groups > Edit 'STUDENT'

General WLANs RF Profile APs 802.11u Location Ports/Module

Add New

Add New

WLAN SSID: Student(1)

Interface / Interface Group: 1

SNMP NAC State: ☐ Enabled

Add Cancel

WLANs

▼ WLANs
WLANs

▼ Advanced
AP Groups

Ap Groups > Edit 'STUDENT'

General WLANs RF Profile APs 802.11u Location Ports/Module

APs currently in the Group

Remove APs

Add APs to the Group

Add APs

AP Name	Ethernet MAC	AP Name	Group Name
<input type="checkbox"/>		<input checked="" type="checkbox"/> Light Weight Access Point7	default-group
<input type="checkbox"/>		<input checked="" type="checkbox"/> Light Weight Access Point8	default-group
<input type="checkbox"/>		<input type="checkbox"/> Light Weight Access Point6	default-group

WLANs

▼ WLANs
WLANs

▼ Advanced
AP Groups

Ap Groups > Edit 'STUDENT'

General WLANs RF Profile APs 802.11u Location Ports/Module

APs currently in the Group

Remove APs

Add APs to the Group

Add APs

Warning: Changing AP Group will reboot the AP and will repin the controller after a few minutes. AP3600 with 802.11ac module will advertise only first 8 WLANs subscribed on 5GHz radios. Are you sure you want to continue?

OK Cancel

Add AP Group TEACHER

The screenshot shows the 'WLANs' sidebar on the left with 'WLANs' and 'Advanced' sections. The 'Advanced' section is expanded, showing 'AP Groups'. The main content area is titled 'AP Groups' and contains the 'Add New AP Group' form. The form has two input fields: 'AP Group Name' with the value 'TEACHER' and 'Description' with the value 'Teacher AP'. Below these fields are 'Add' and 'Cancel' buttons. A mouse cursor is pointing at the 'Add' button.

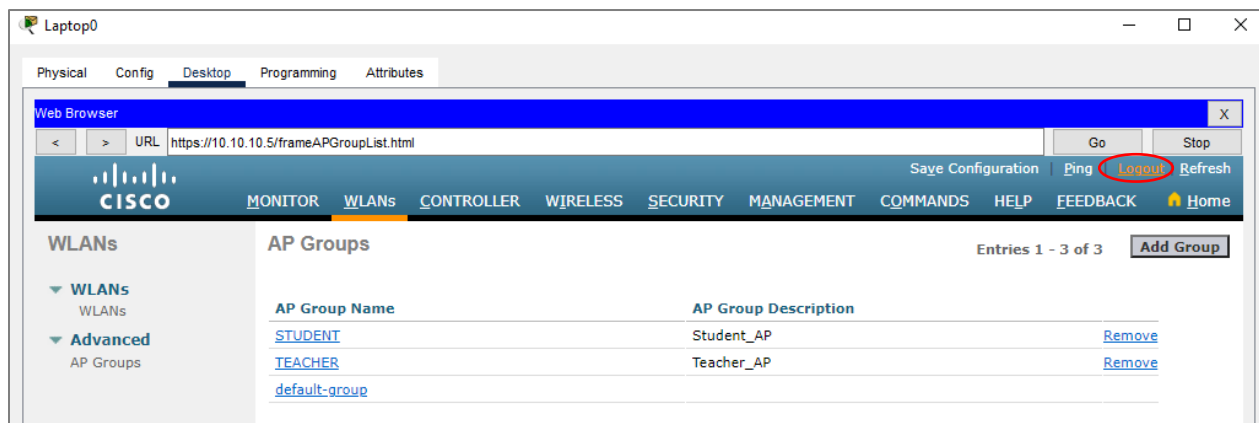
Assign wireless LAN

The screenshot shows the 'Ap Groups > Edit 'TEACHER'' configuration page. The 'WLANs' tab is selected, and the 'Add New' section is visible. The 'WLAN SSID' dropdown is set to 'Teacher(2)'. Below it, the 'Interface /Interface Group(G)' dropdown is empty, and a mouse cursor is hovering over it. There is also a checkbox for 'SNMP NAC State' which is unchecked. 'Add' and 'Cancel' buttons are at the bottom of the 'Add New' section. An 'Add New' button is also present in the top right corner of the main content area.

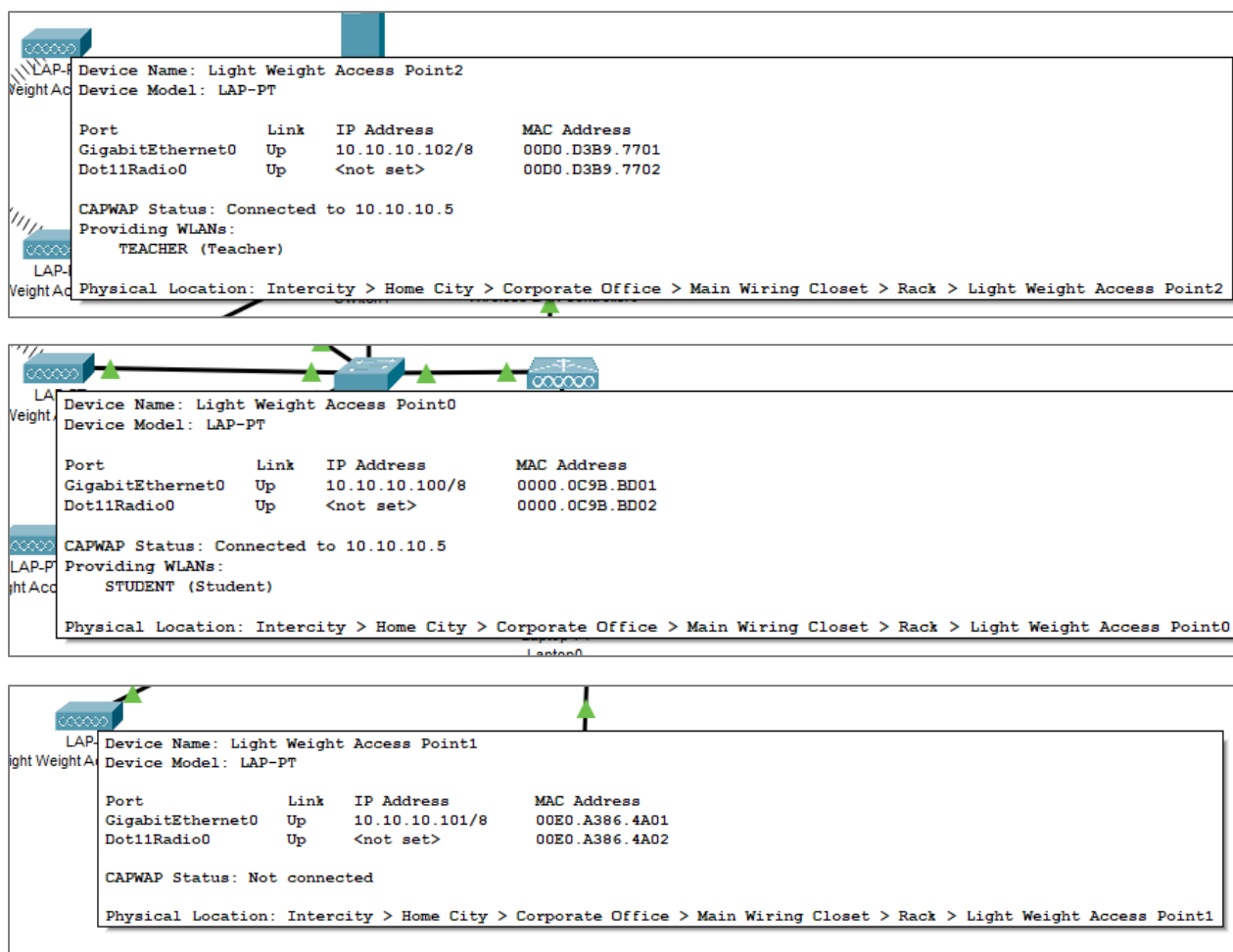
Assign AP

The screenshot shows the 'Ap Groups > Edit 'TEACHER'' configuration page with the 'APs' tab selected. The 'APs currently in the Group' section shows a table with columns 'AP Name' and 'Ethernet MAC'. The 'Add APs to the Group' section shows a table with columns 'AP Name' and 'Group Name'. The table lists three APs: 'Light Weight Access Point7' (STUDENT), 'Light Weight Access Point8' (STUDENT), and 'Light Weight Access Point6' (default-group). The checkbox for 'Light Weight Access Point6' is checked. 'Remove APs' and 'Add APs' buttons are present. An 'Add APs' button is also in the top right corner.

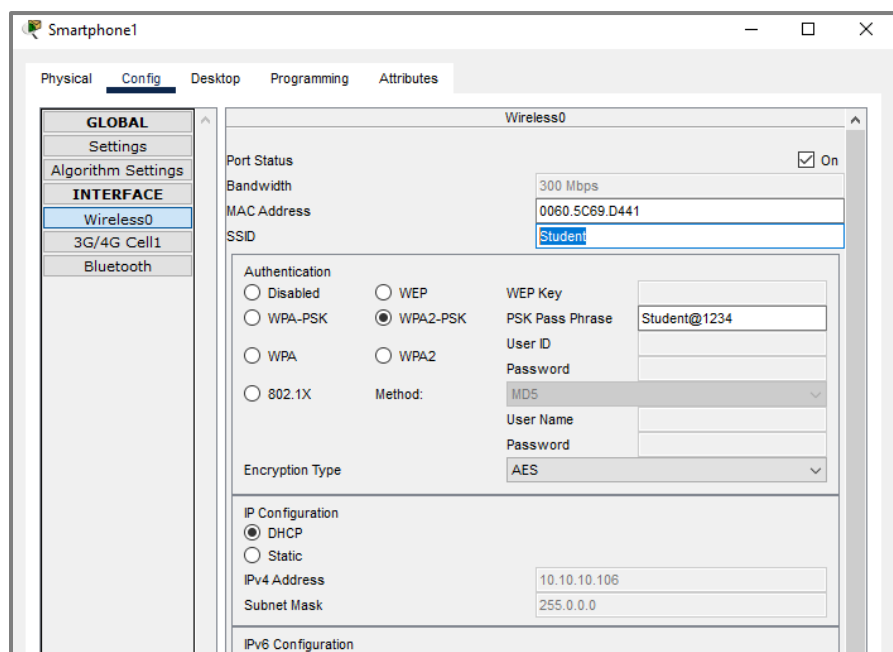
Logout from admin panel



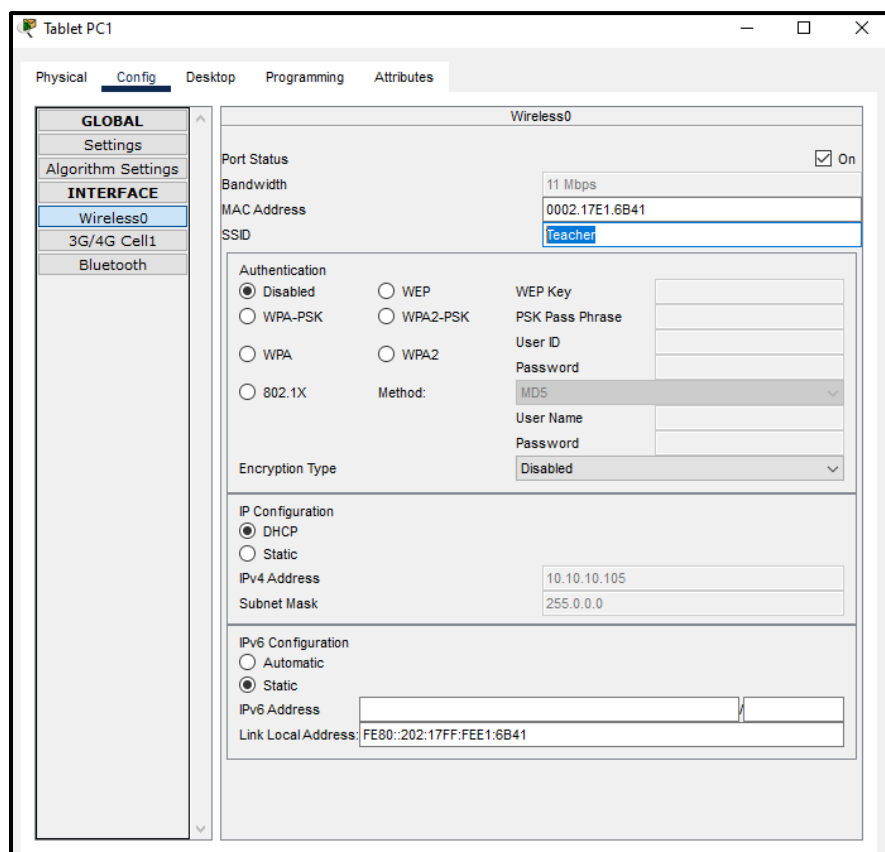
Check the assigned AP's



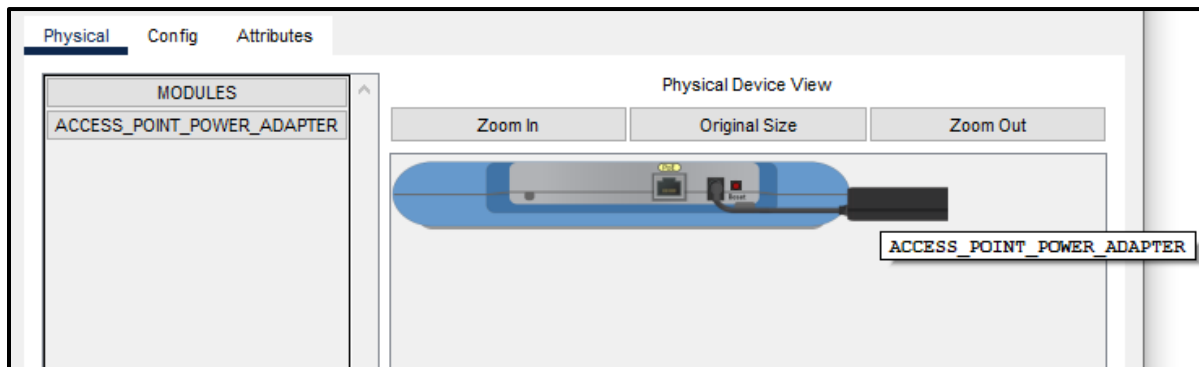
Step 8: Take Smartphone to connect Student AP group with wireless connection using SSID



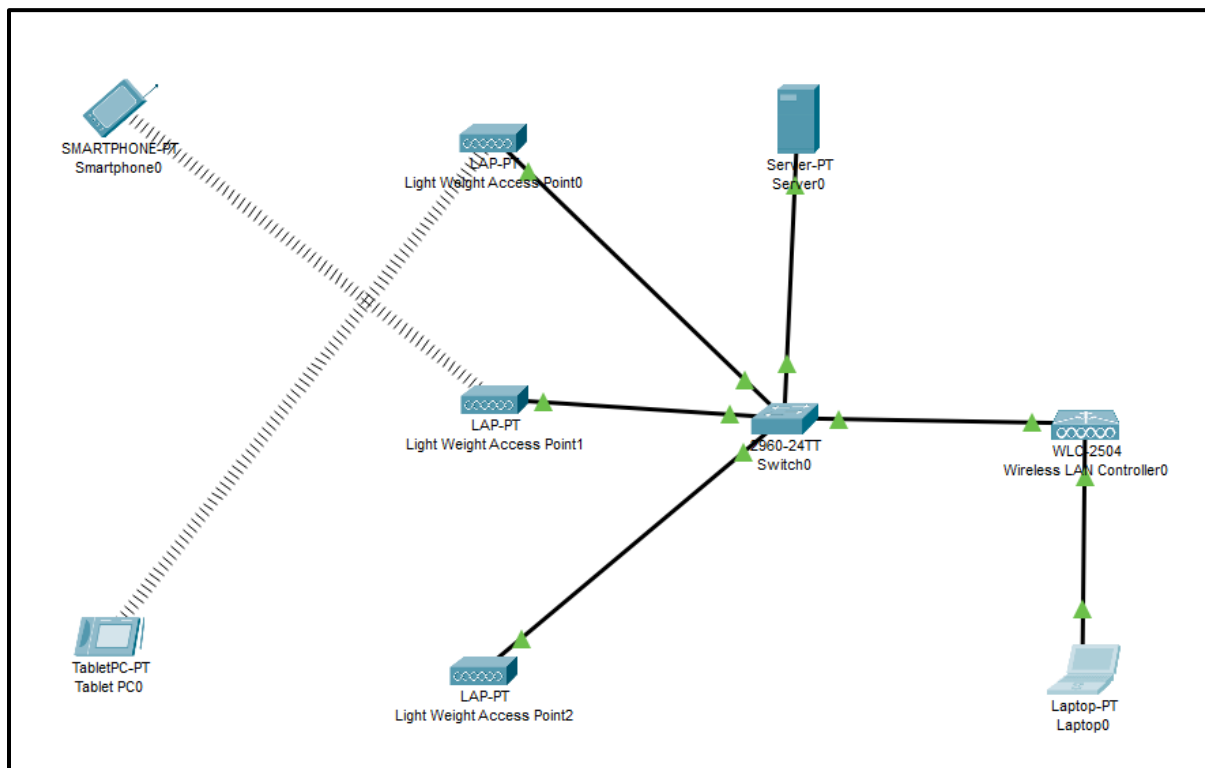
Step 9: Take Tablet to connect Teachers AP group with wireless connection using SSID



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



Final Output/Connection:



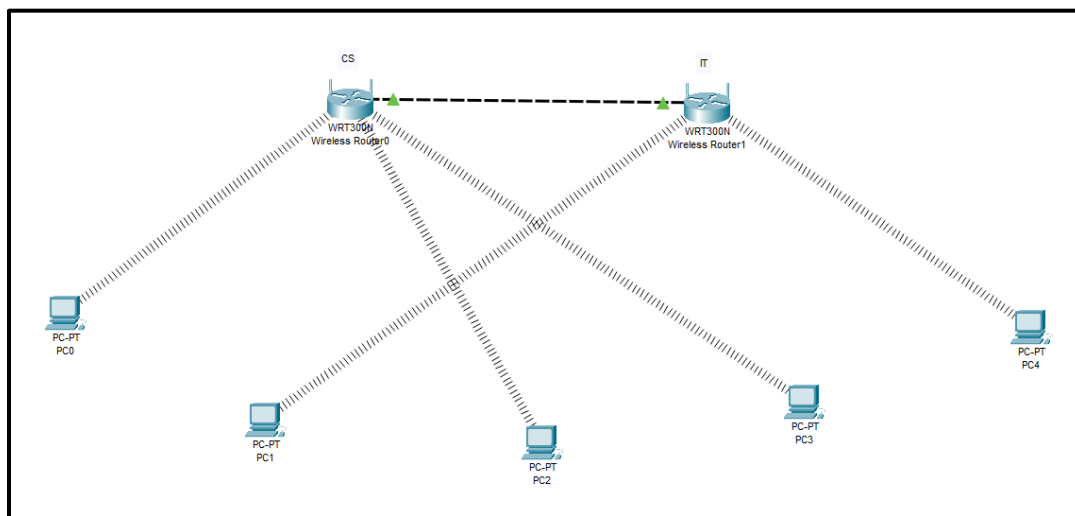
Practical No: 06

Aim: Creating an Adhoc Network

Components: Wireless Router, PC

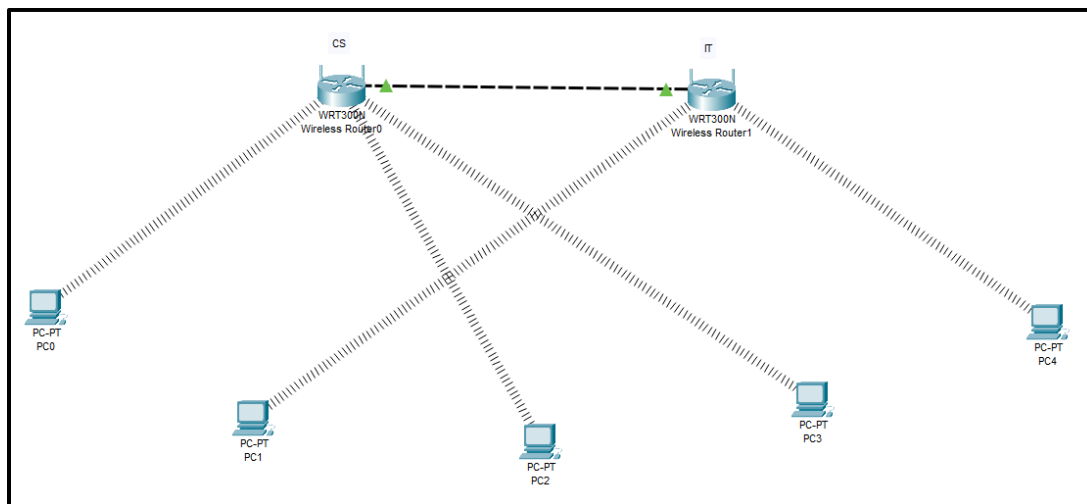
Theory: Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using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

Cisco Packet Tracer Setup:-

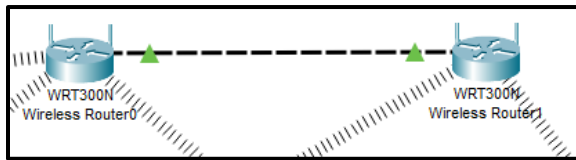


Implementation:-

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:

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router Firmware Version: v0.93.3

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): CS

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ☒ Enabled ☐ Disabled

Help...

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router Firmware Version: v0.93.3

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Wireless Security

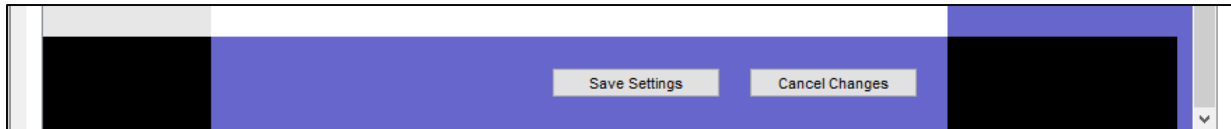
Security Mode: WPA2 Personal

Encryption: AES

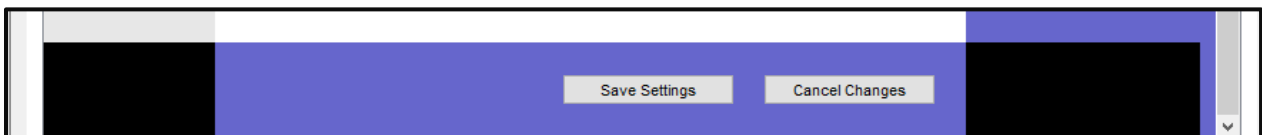
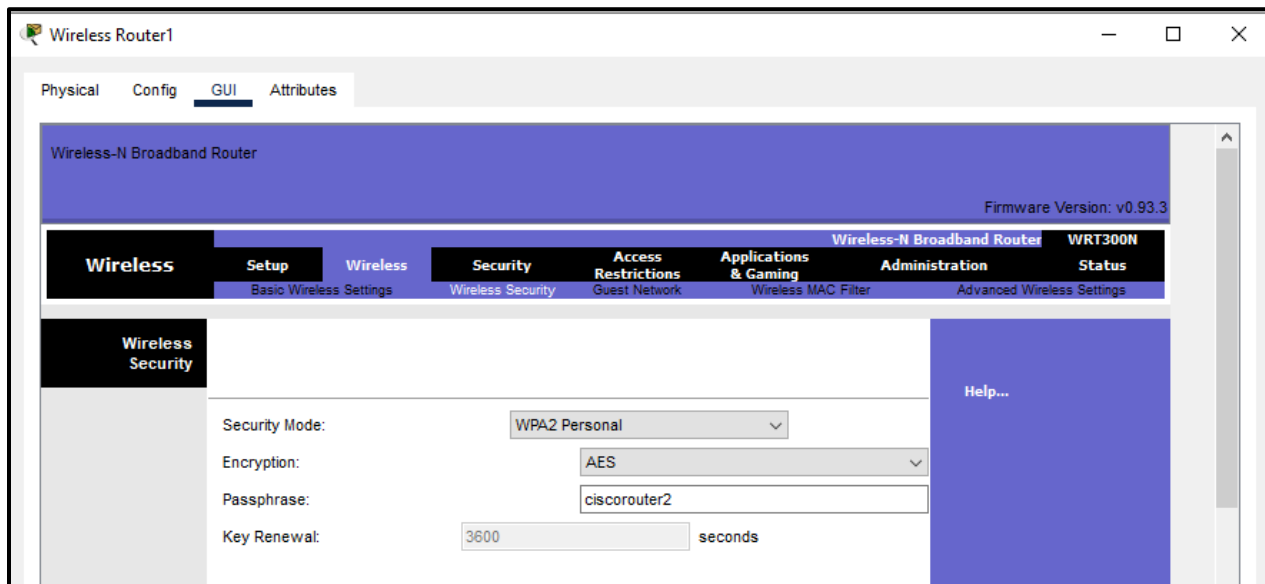
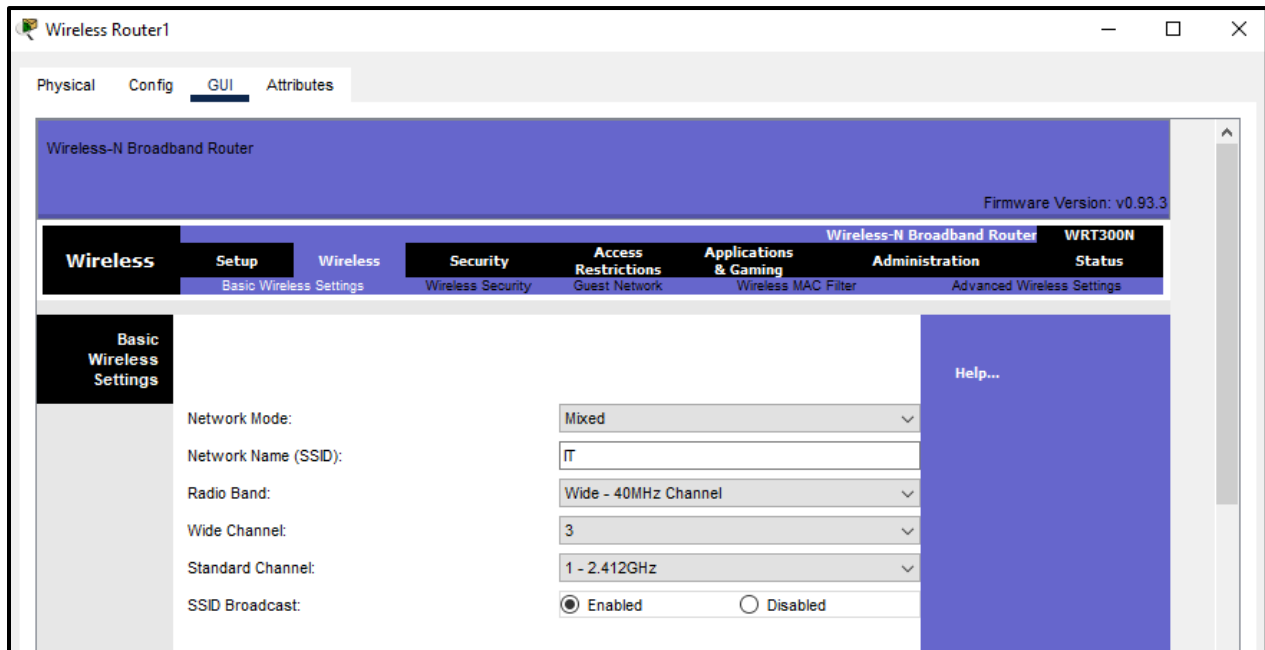
Passphrase: ciscorouter1

Key Renewal: 3600 seconds

Help...

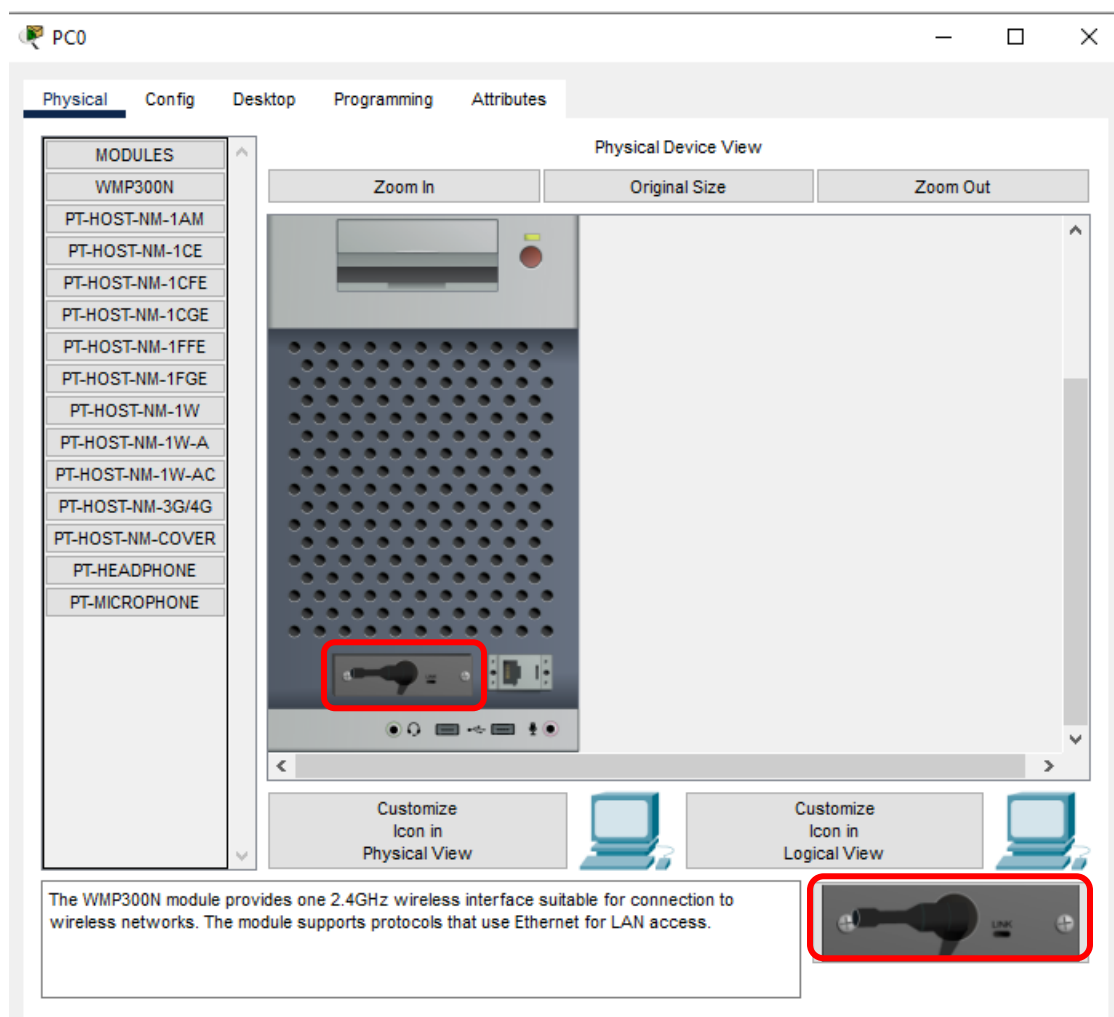


Router 2:



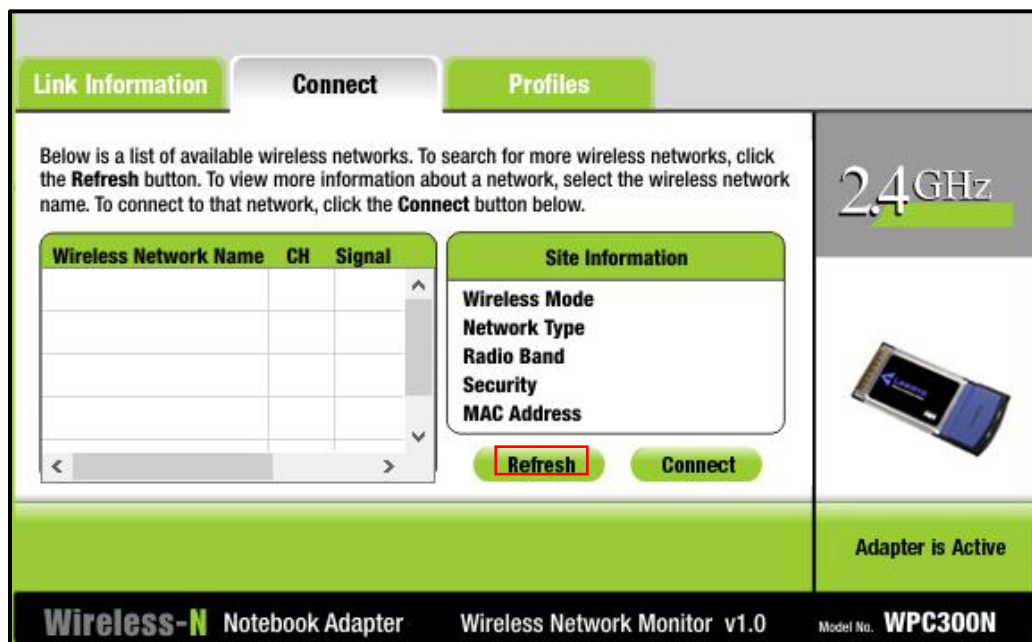
Step3: Connect all machines/devices (PC's) to respective router as per our requirements.

Change the Port of all pc's with wireless adapter



Configure Wireless connection





name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
it	1	100%
CS	1	87%

Site Information
Wireless Mode Infrastructure
Network Type Mixed B/G/N
Radio Band Auto
Security WPA2-PSK
MAC Address 0001.4232.AE08

Refresh
 Connect

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

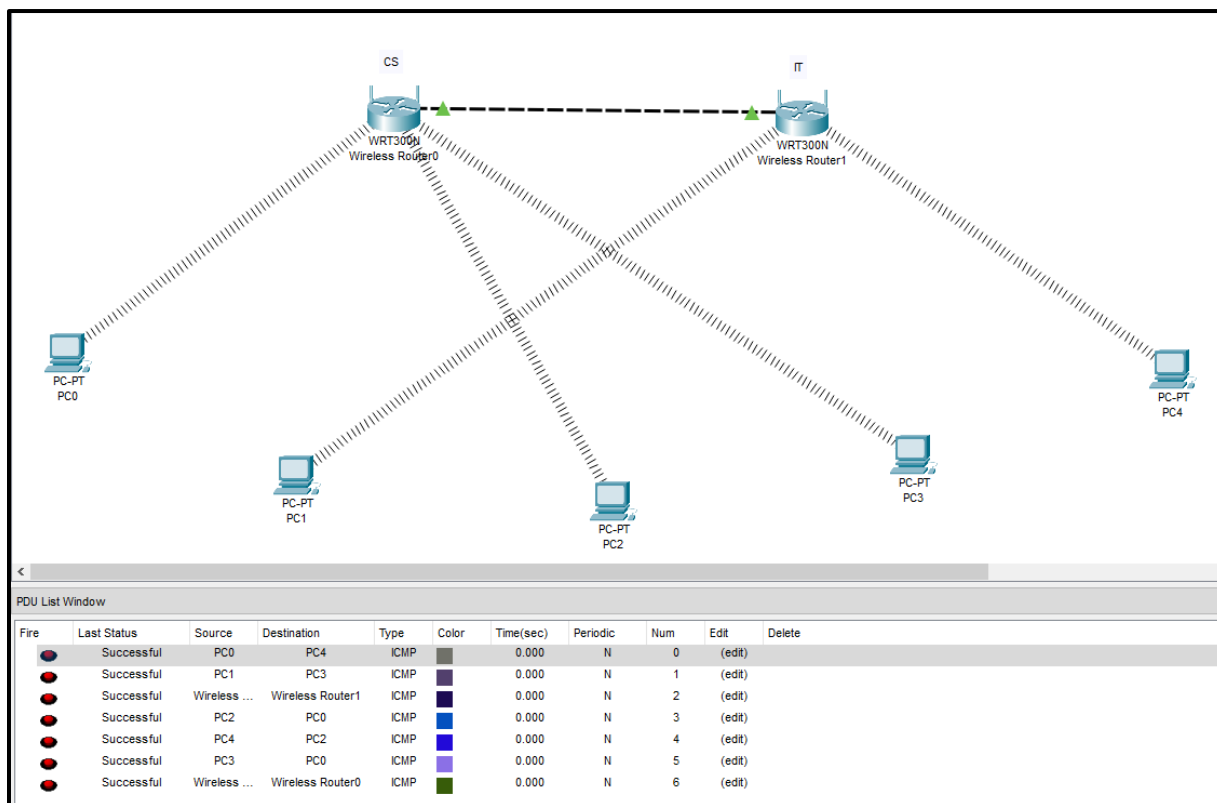
Security
WPA2-Personal
 Please select the wireless security method used by your existing wireless network.

Pre-shared Key
ciscorouter1
 Please enter a Pre-shared Key that is 8 to 63 characters in length.

Cancel Connect

Do similar configuration to all respective PC's

Step4: Check the Connection



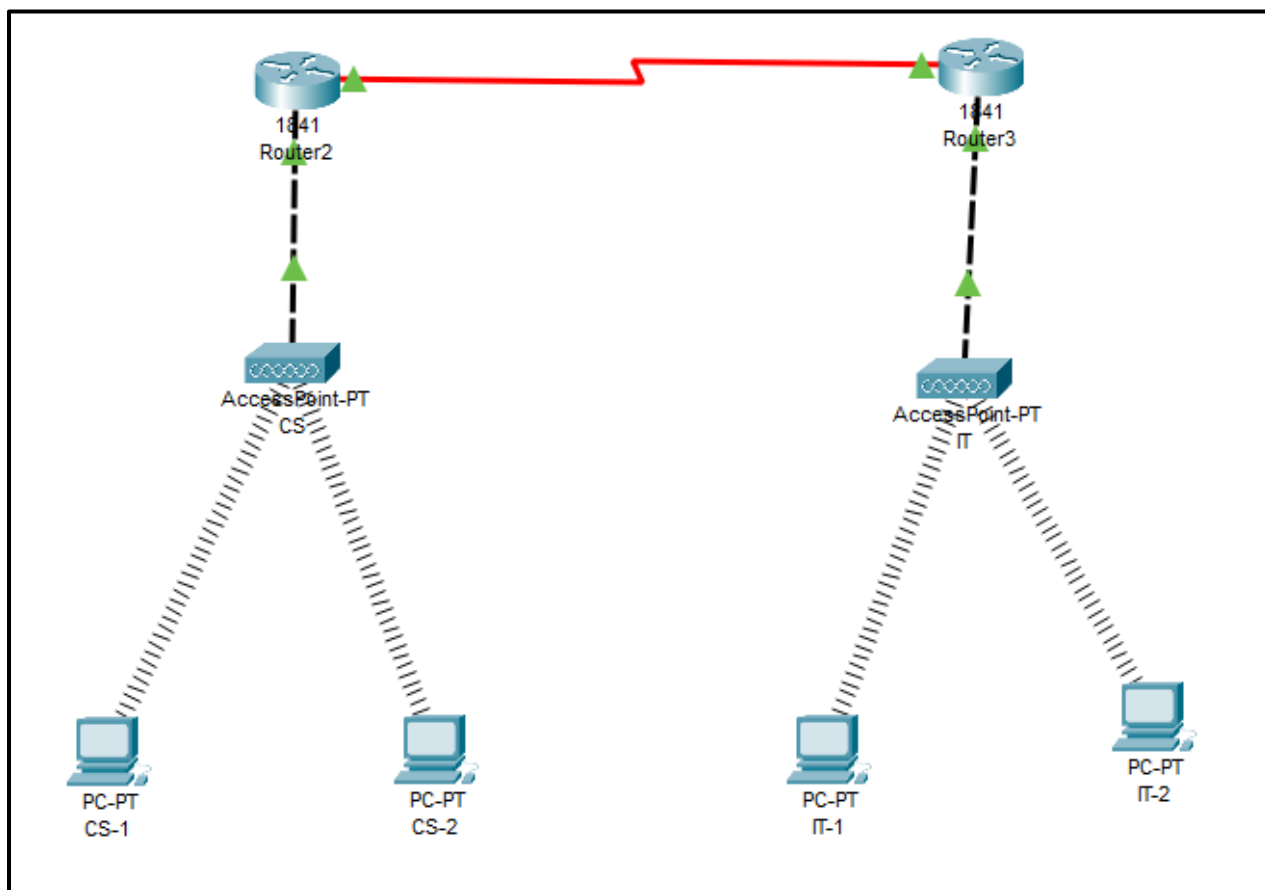
Practical No: 07

Aim: Configuring Basic AP Settings

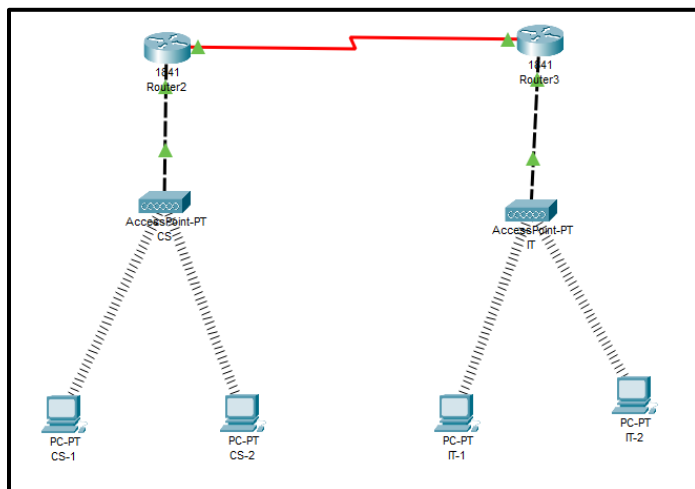
Components: Router, Access points, PC's

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:

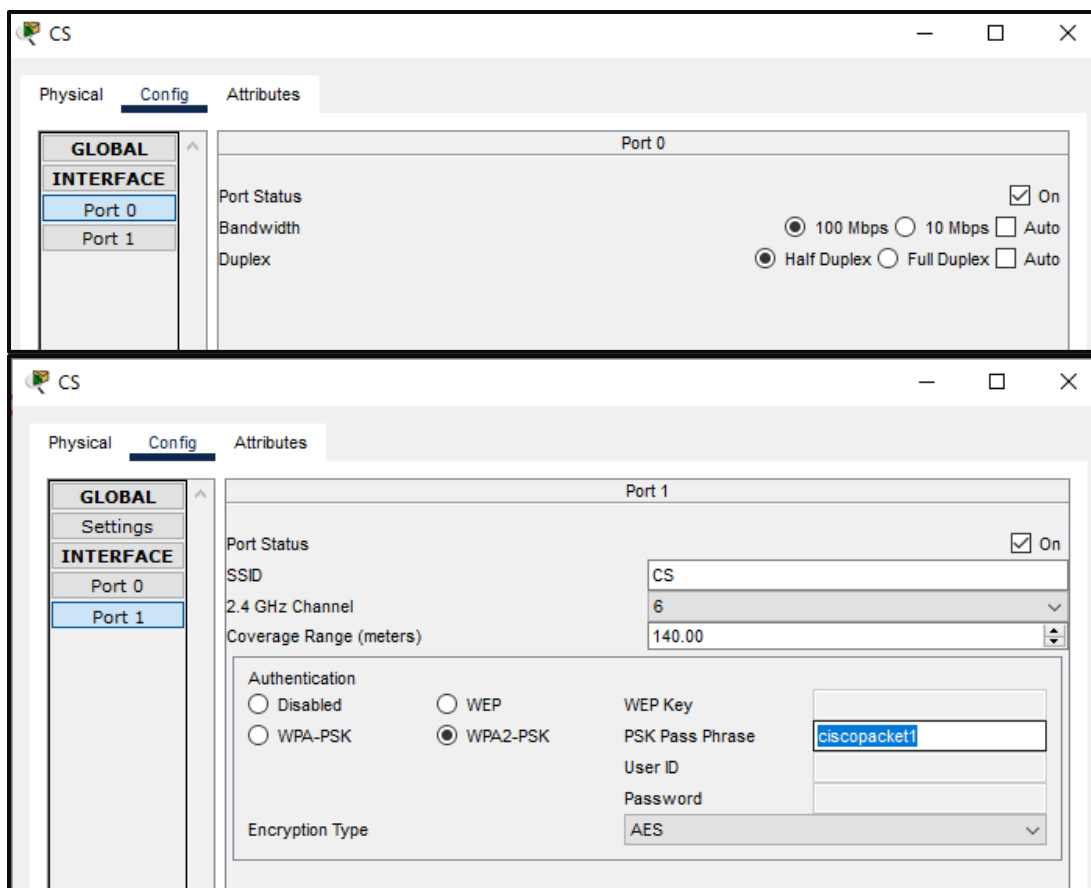


Step 1: Arrange all devices as following

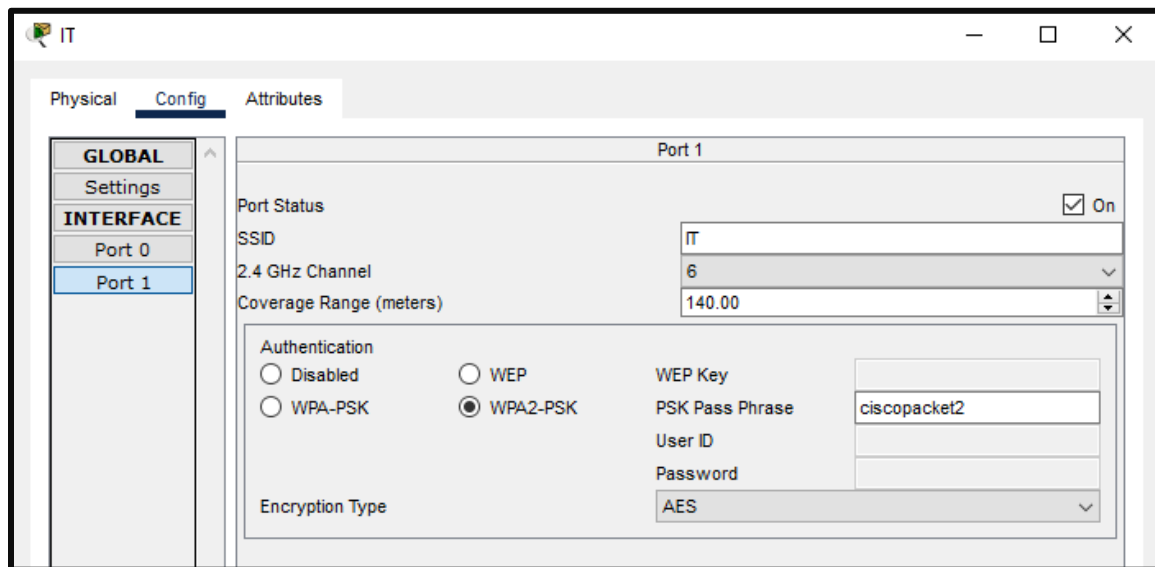
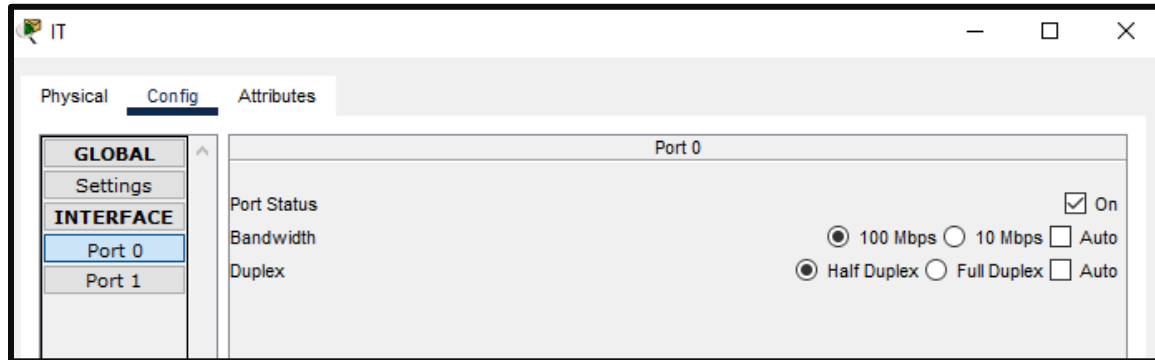
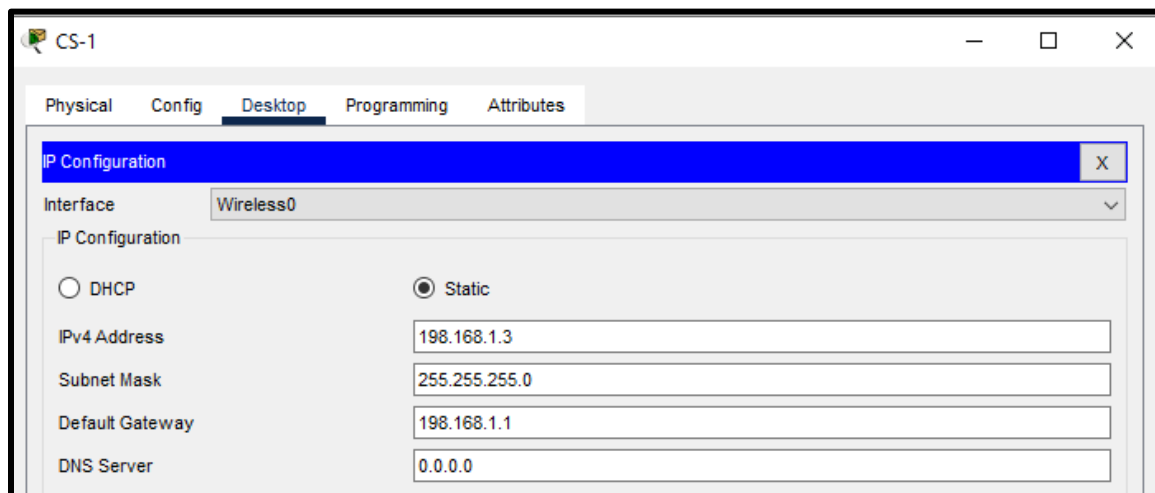


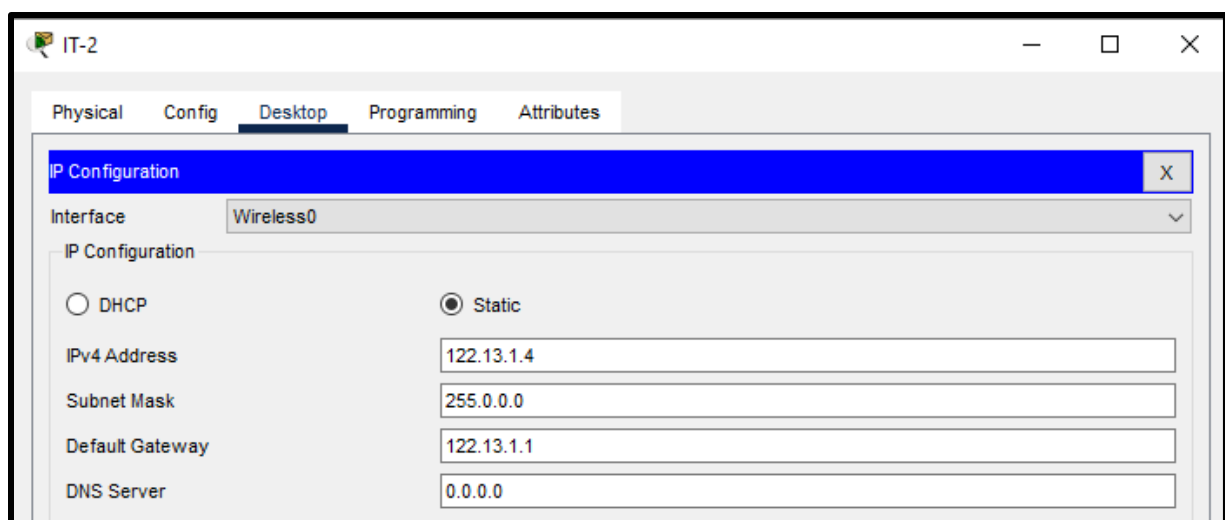
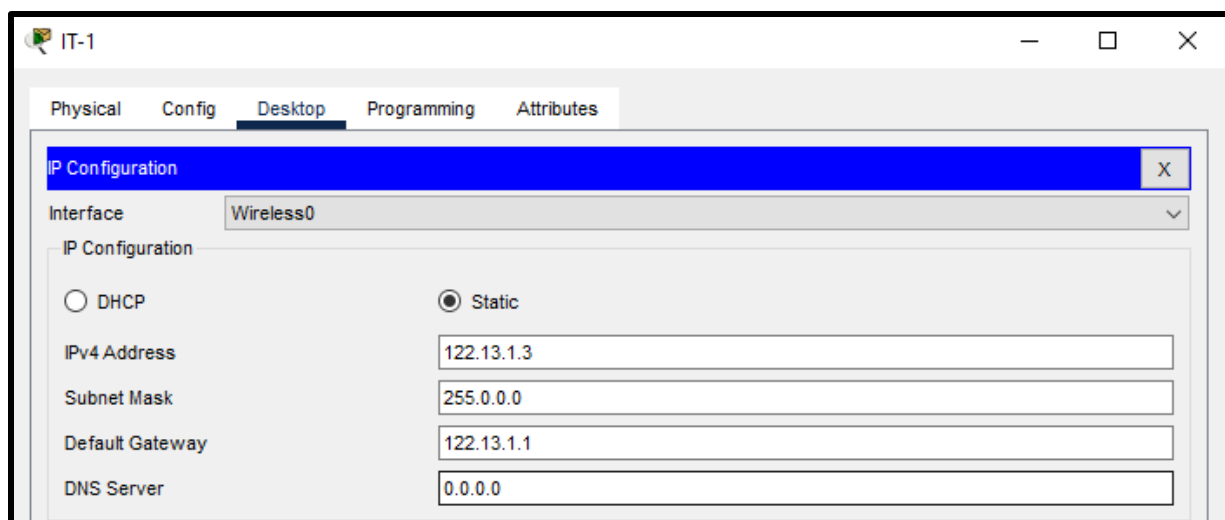
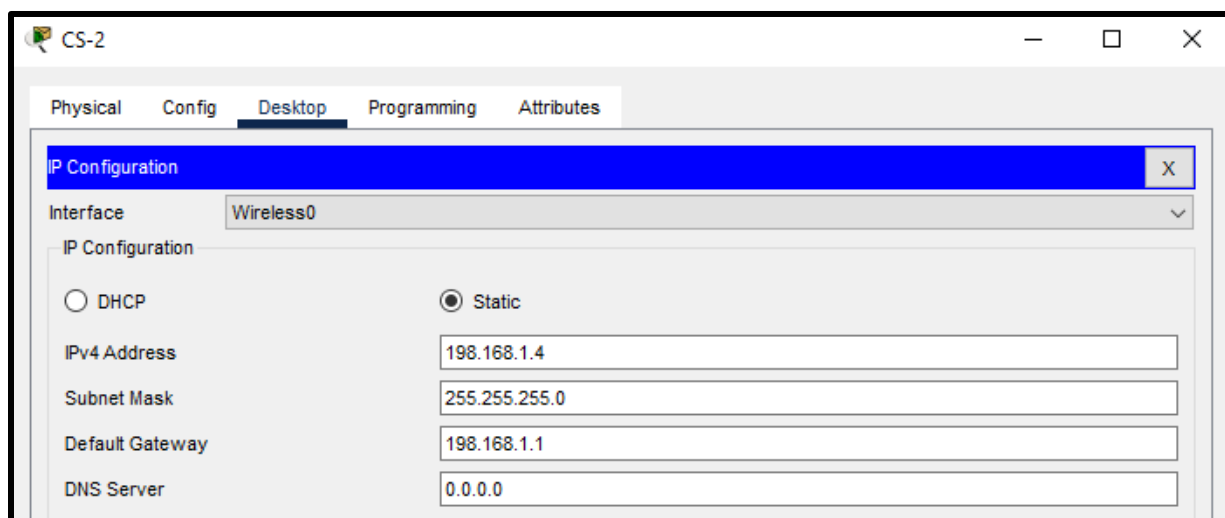
Step 2: Configure Access Points (A)

AP-1

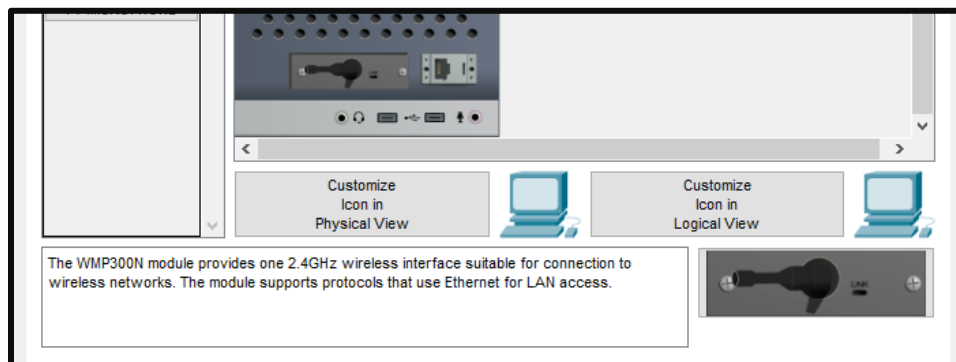


AP-2

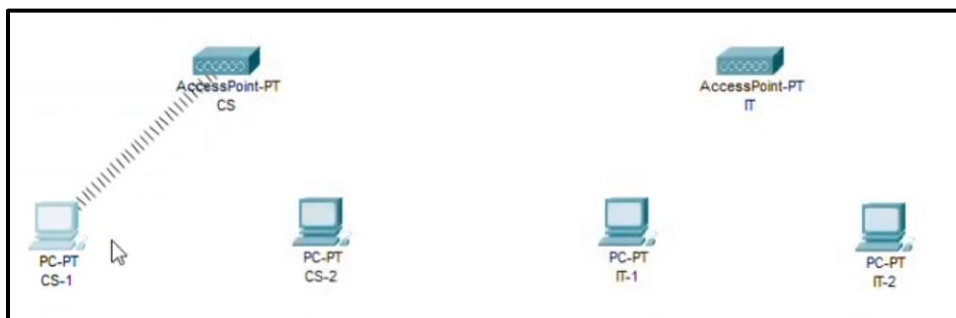
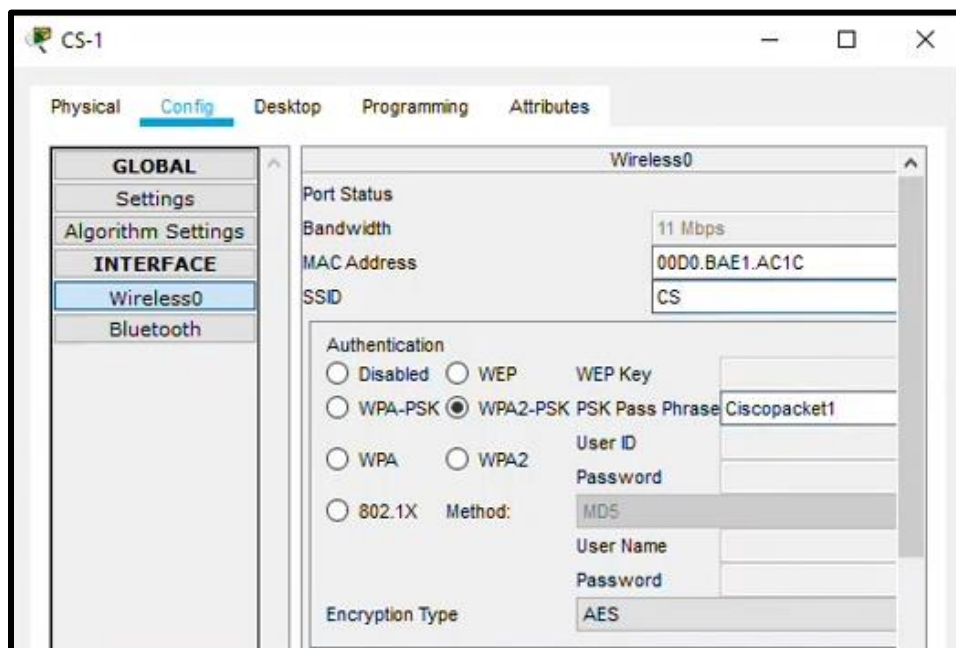
**Step 3:** Configure and Setup IP Address for all devices (PC's)

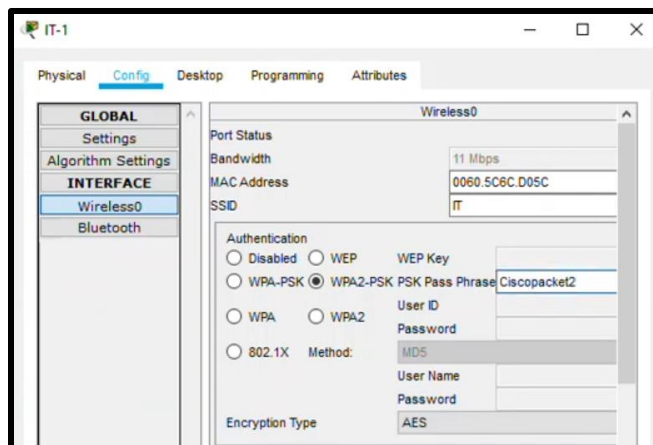
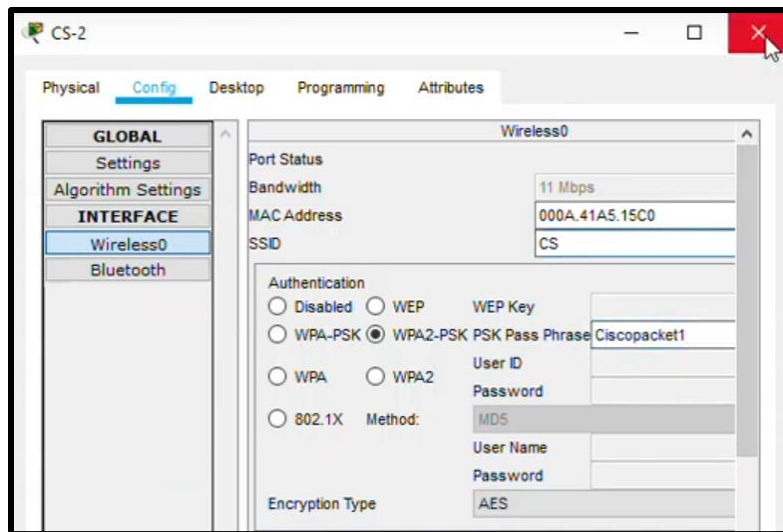


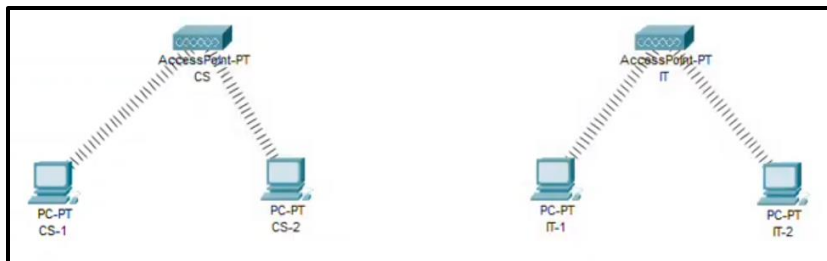
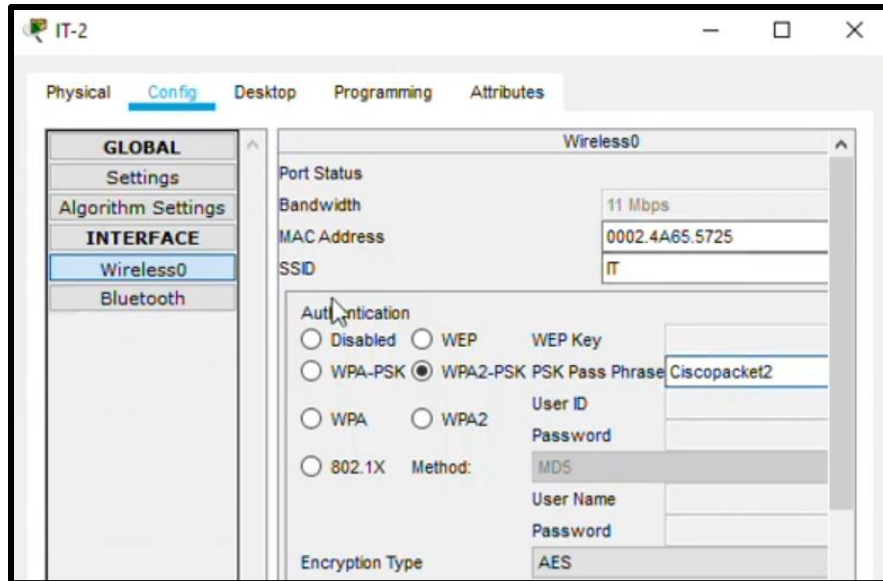
Note: Change all port adapters with wireless adapter for all PC's



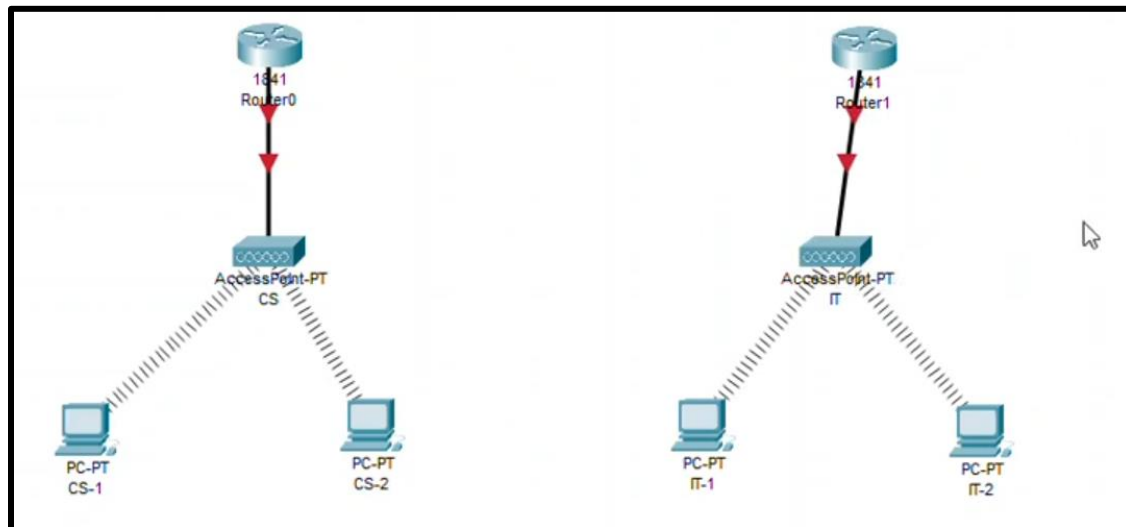
Step 4: Configure Access points with PC's

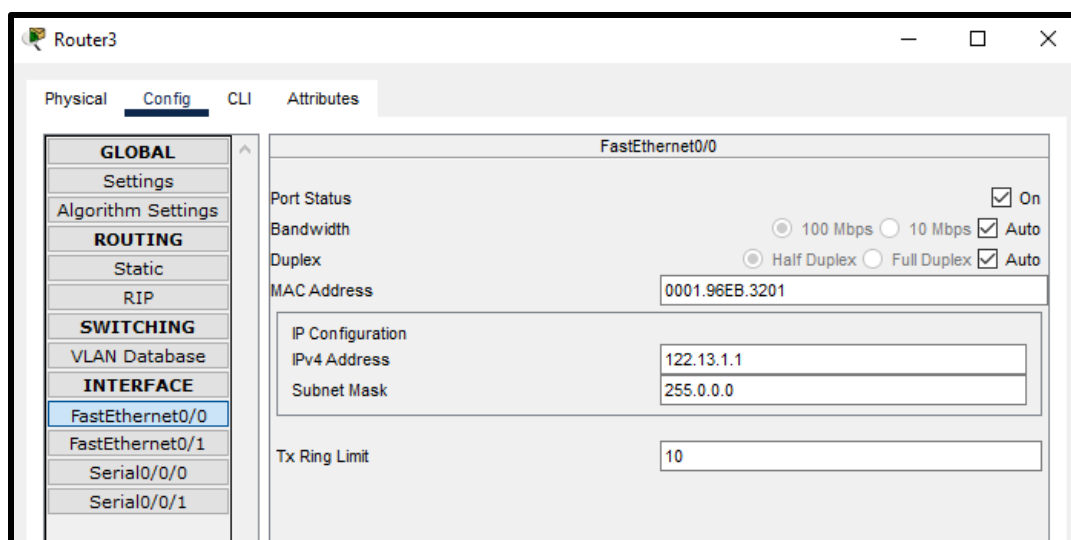
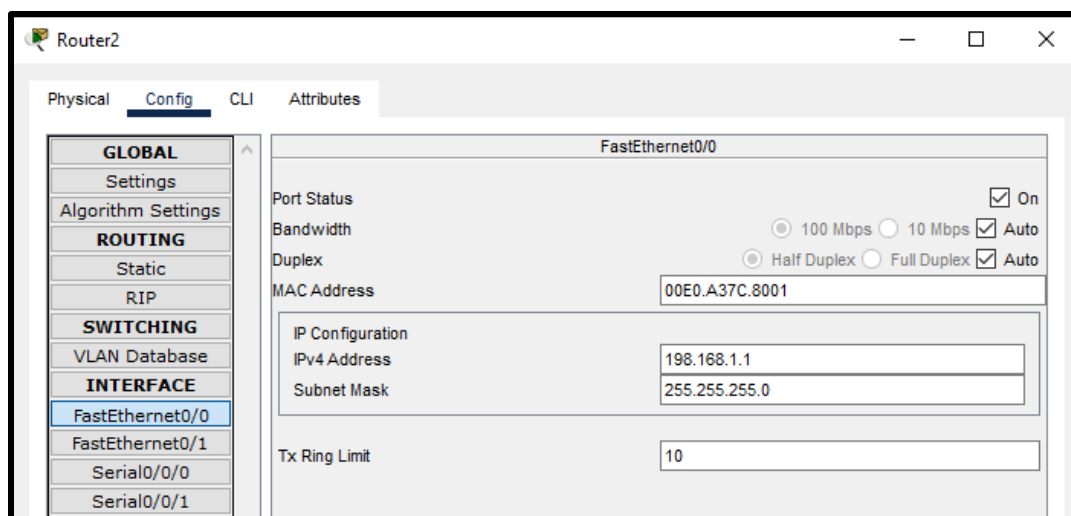




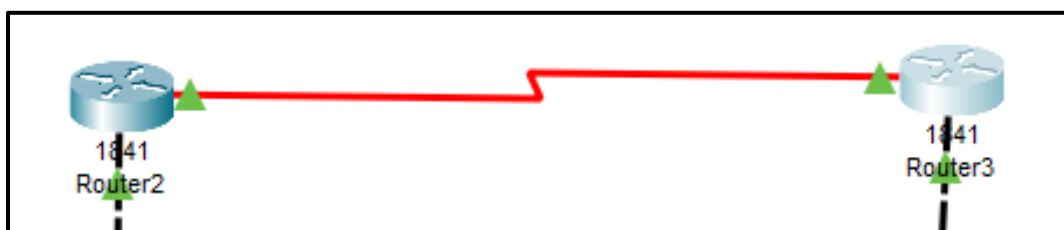


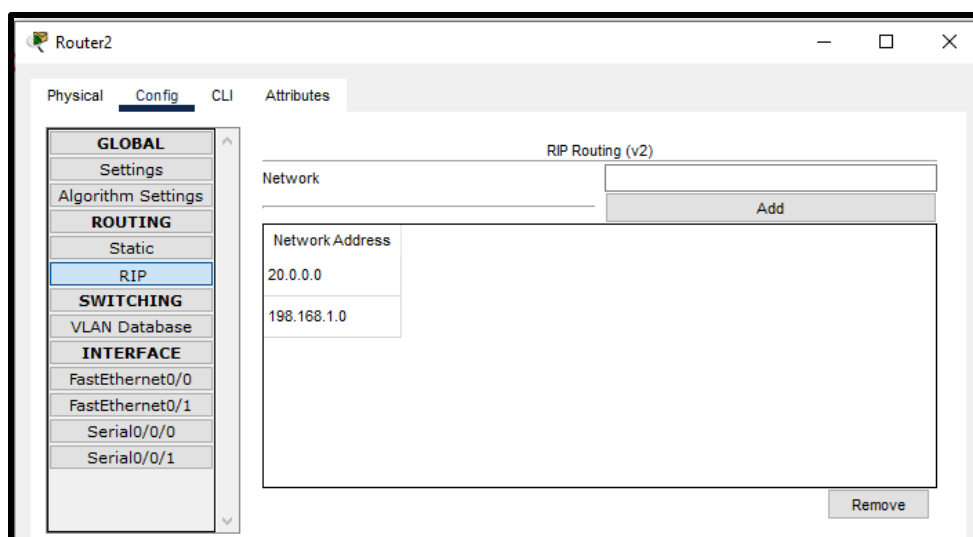
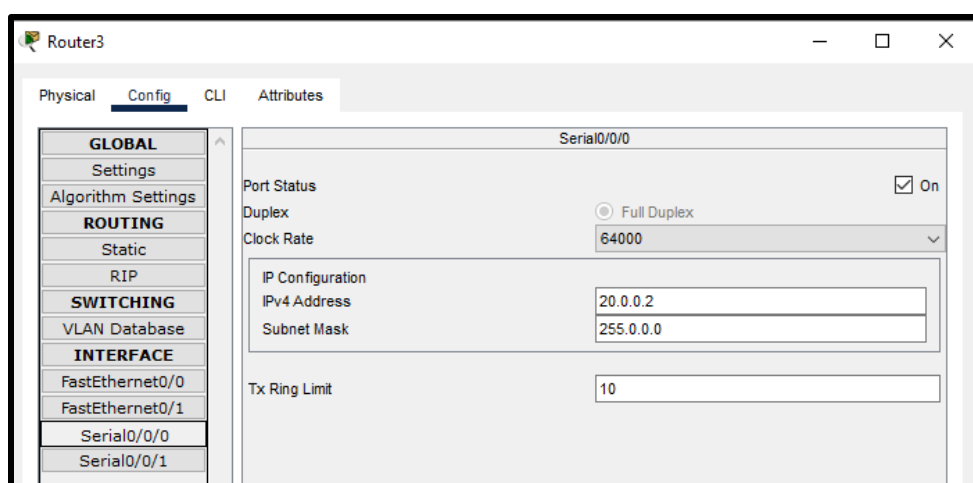
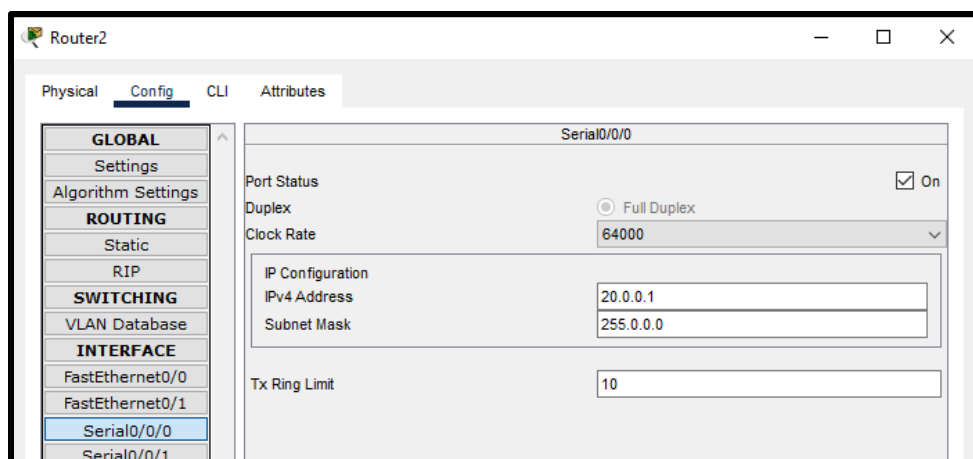
Step 5: Connect routers with Access points and configure them

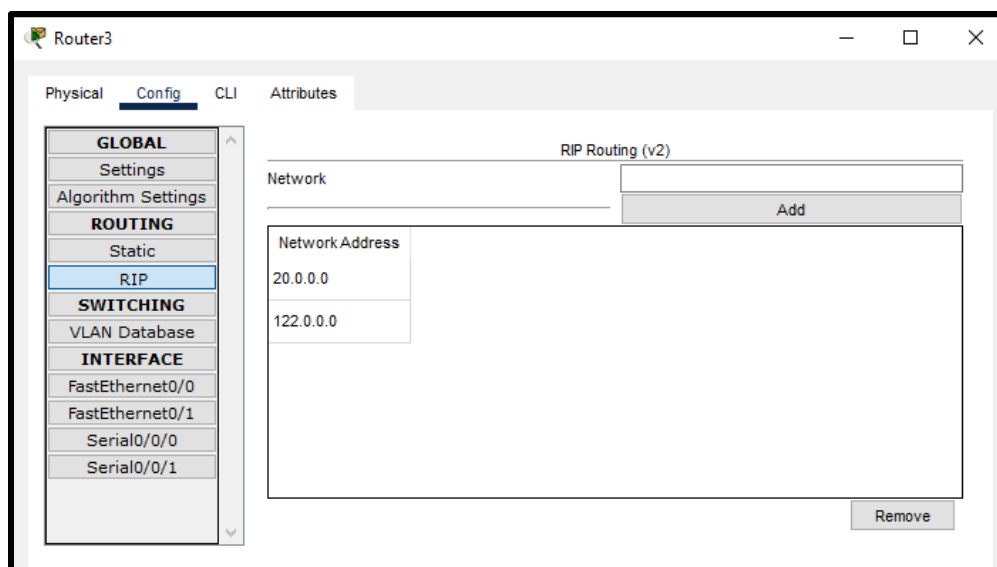




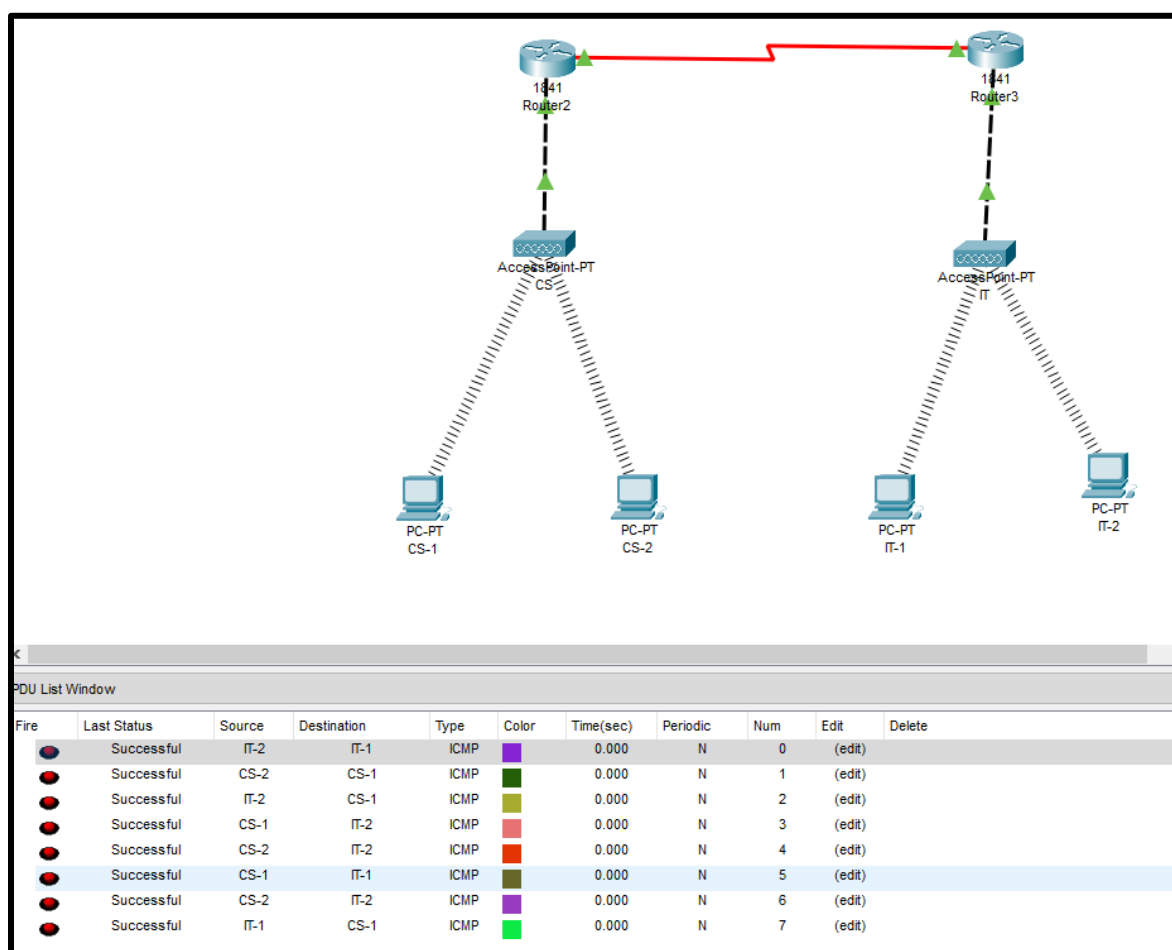
Connect Routers with serial ports and configure







Step 6: Check the connection



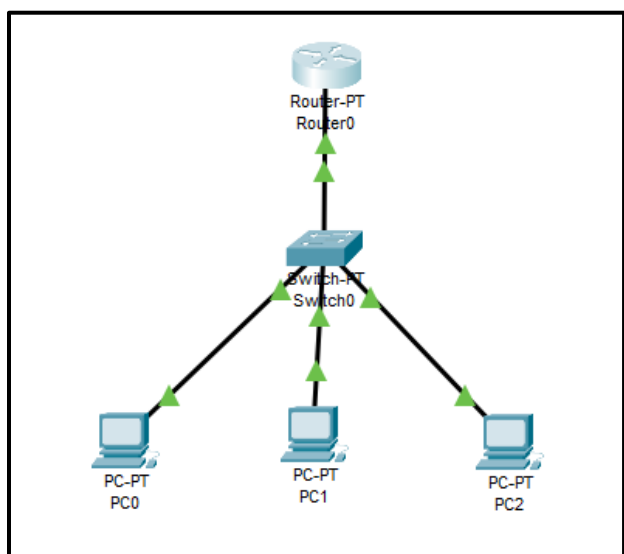
Practical No: 08

Aim: Configure fast Ethernet on router using packet tracer

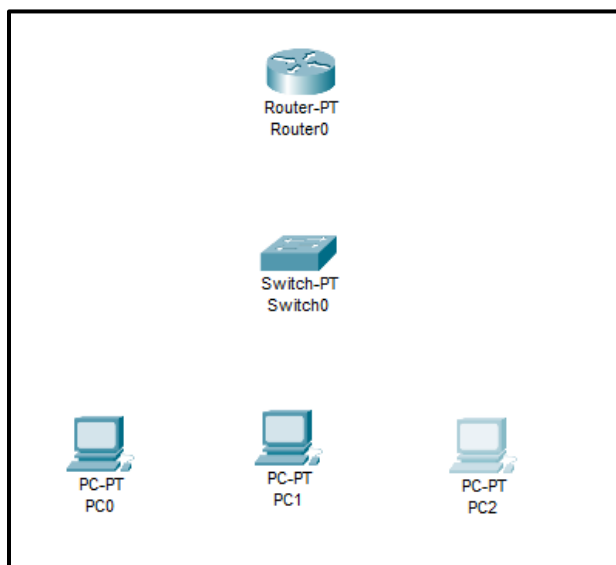
Components: Router, Switches, PC's

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.

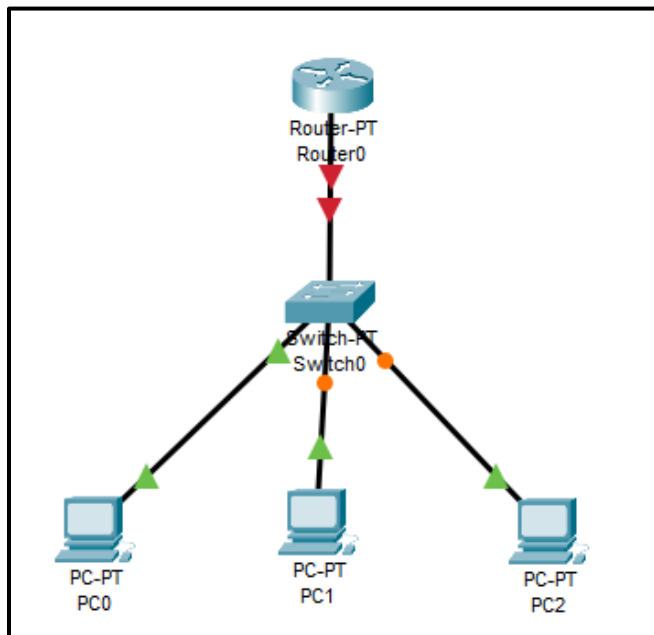
Cisco Packet tracer Setup:



Step 1: Arrange all devices



Step 2: Connect all devices using Ethernet cable



Step 3: Configure Router using CLI

Using following commands:

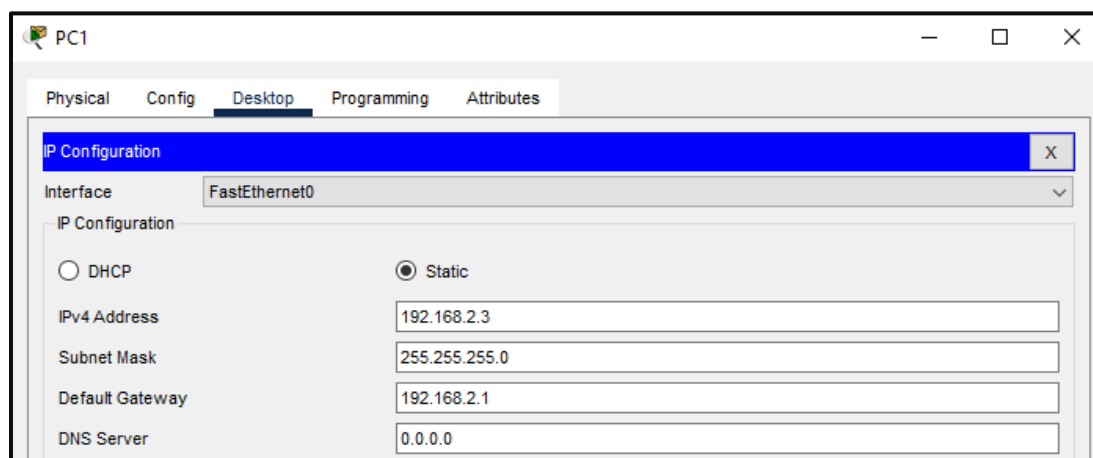
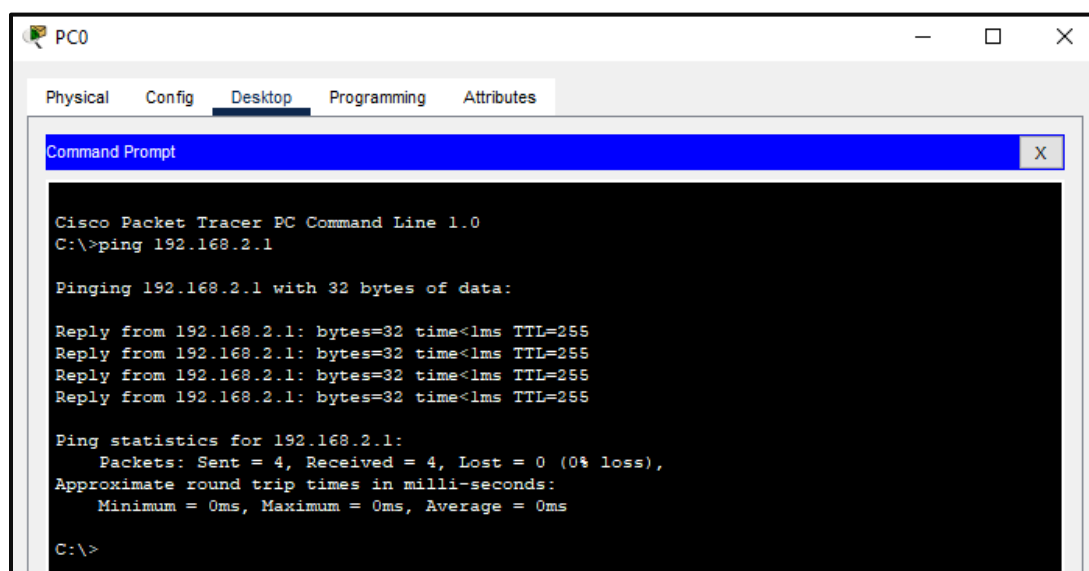
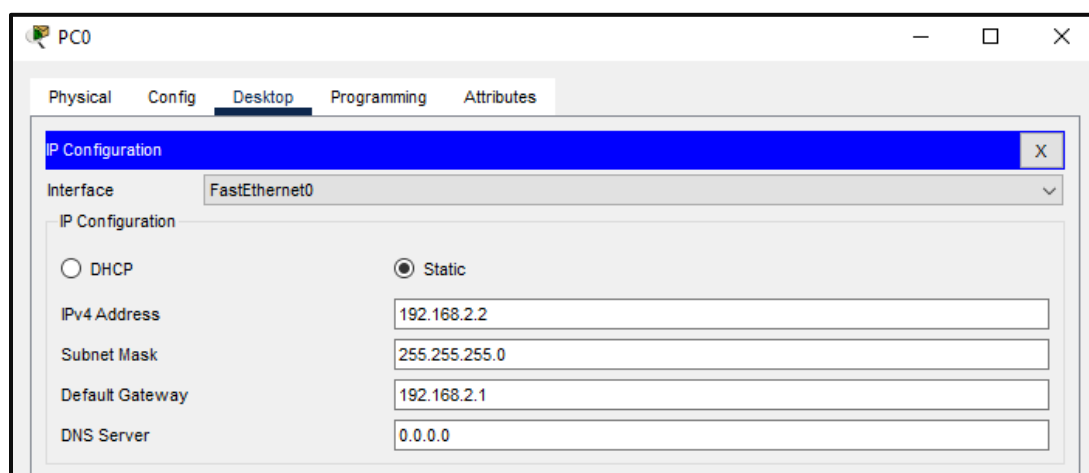
```

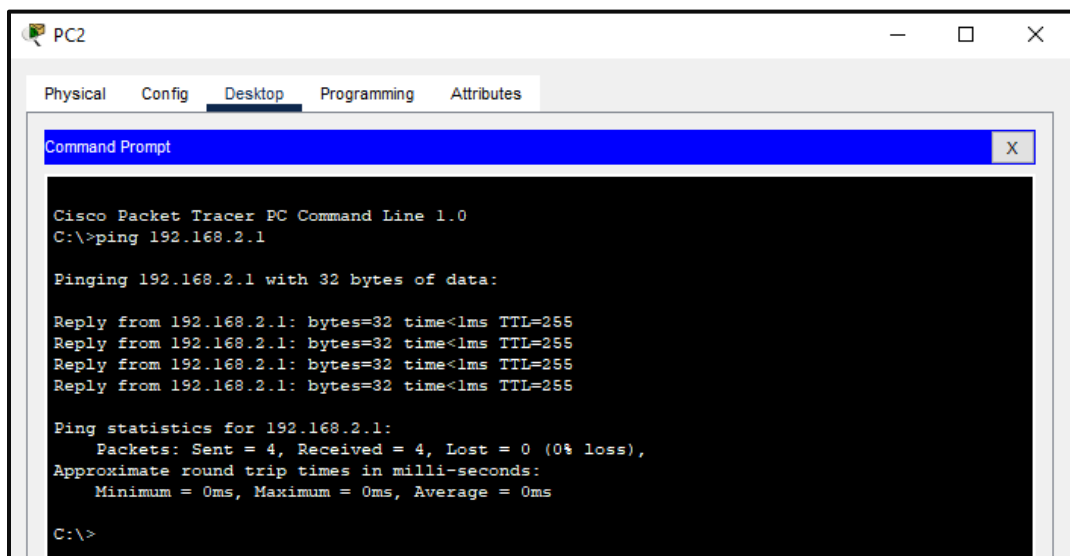
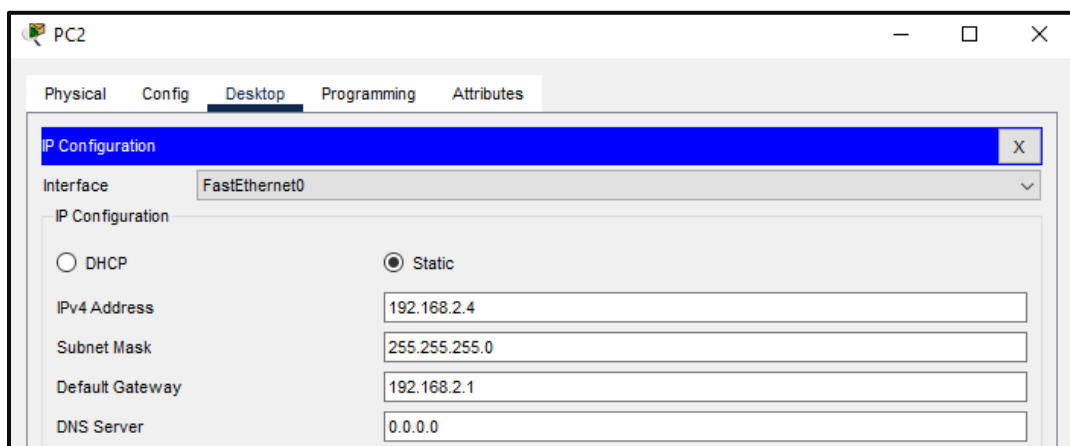
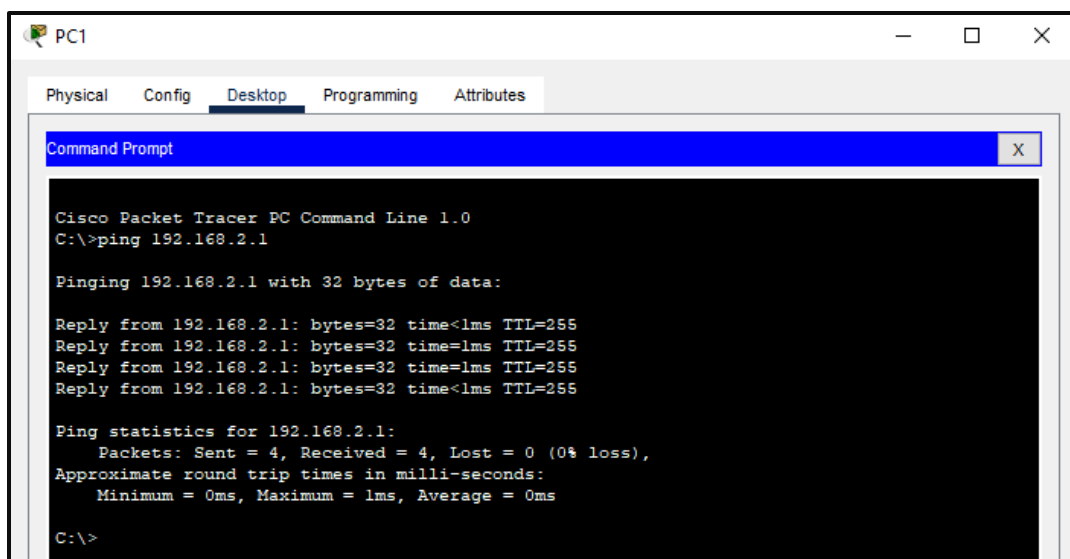
configure t
hostname R1
enable password cisco
interface fa0/0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
Exit
  
```

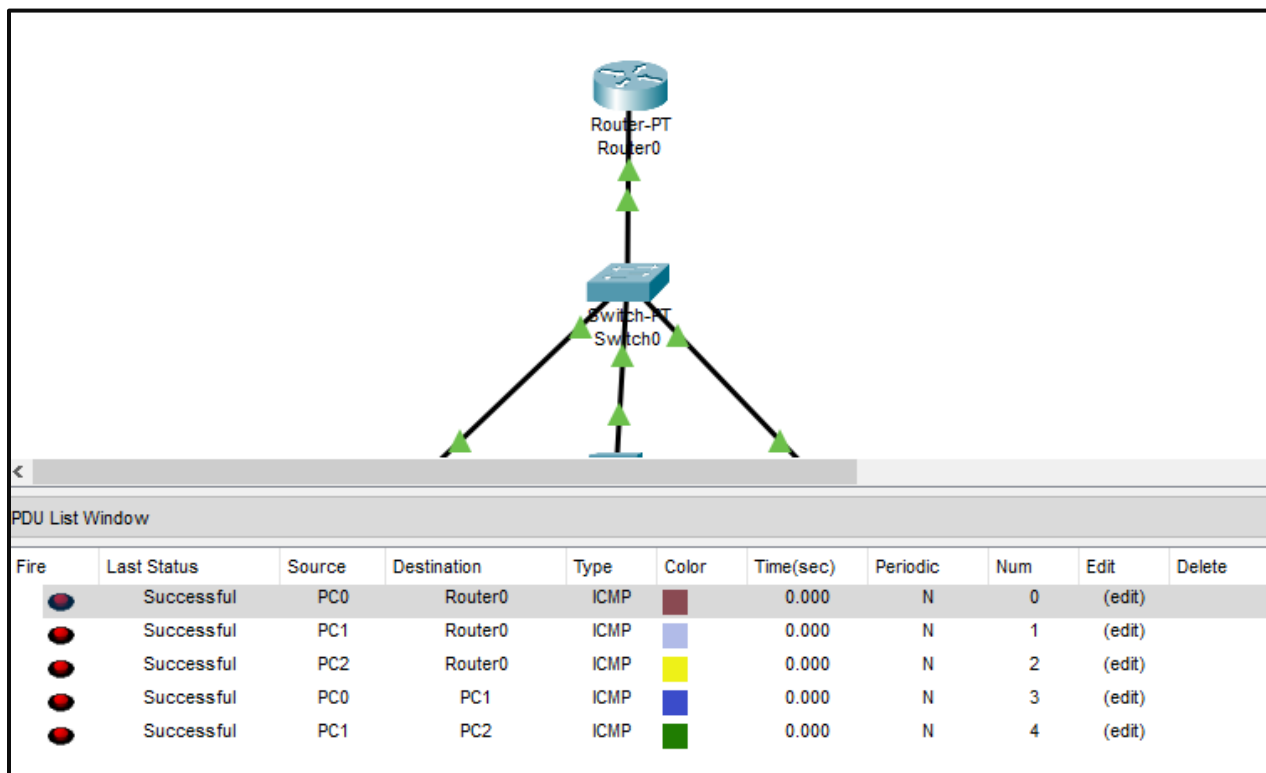
```

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





Step 5: Check the connection

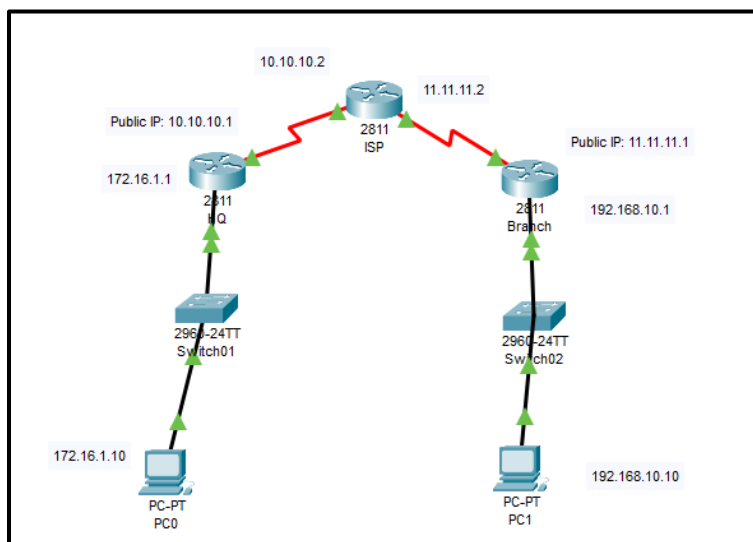
Practical No: 9

Aim: Configure Site-to-Site Wireless Link

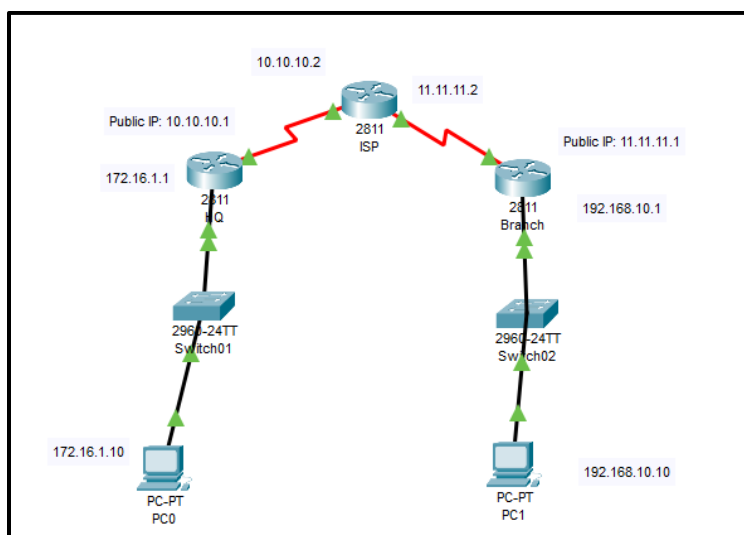
Components: Routers, Switches, Machines (PC's)

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.

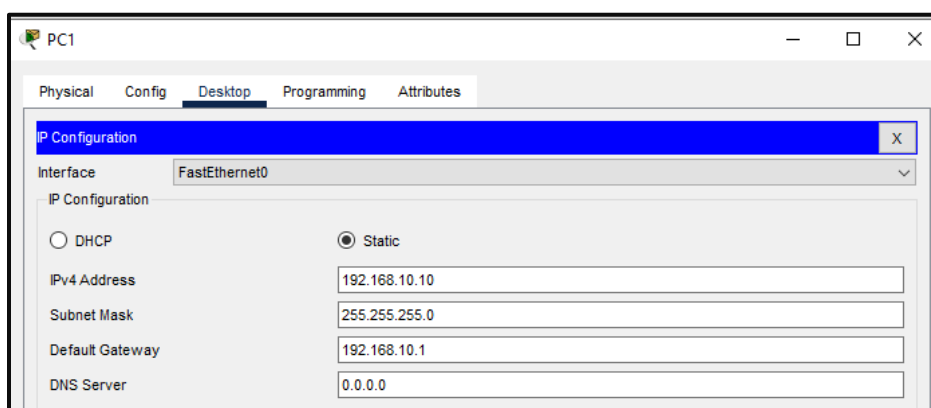
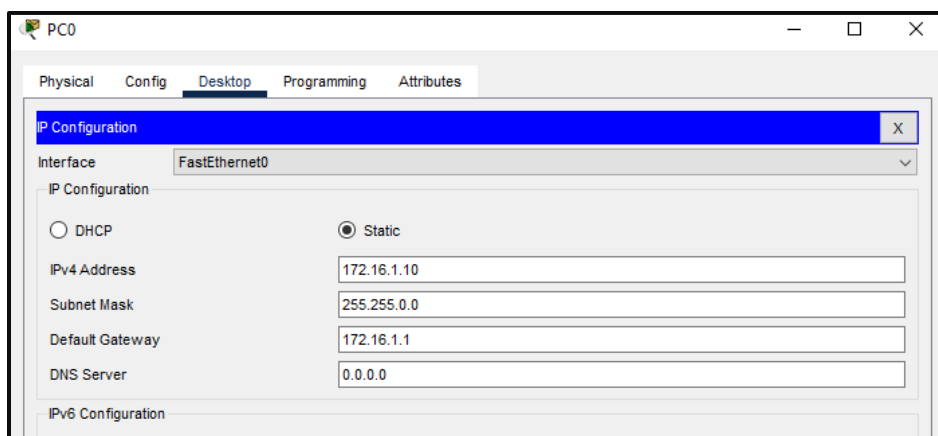
Cisco Packet tracer Setup:



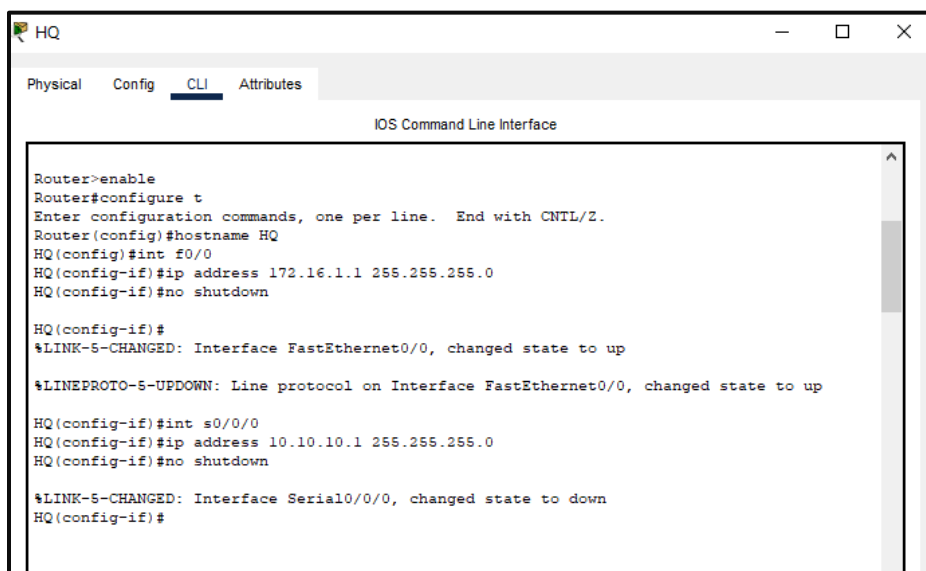
Step 1: Arrange and connect all devices/components

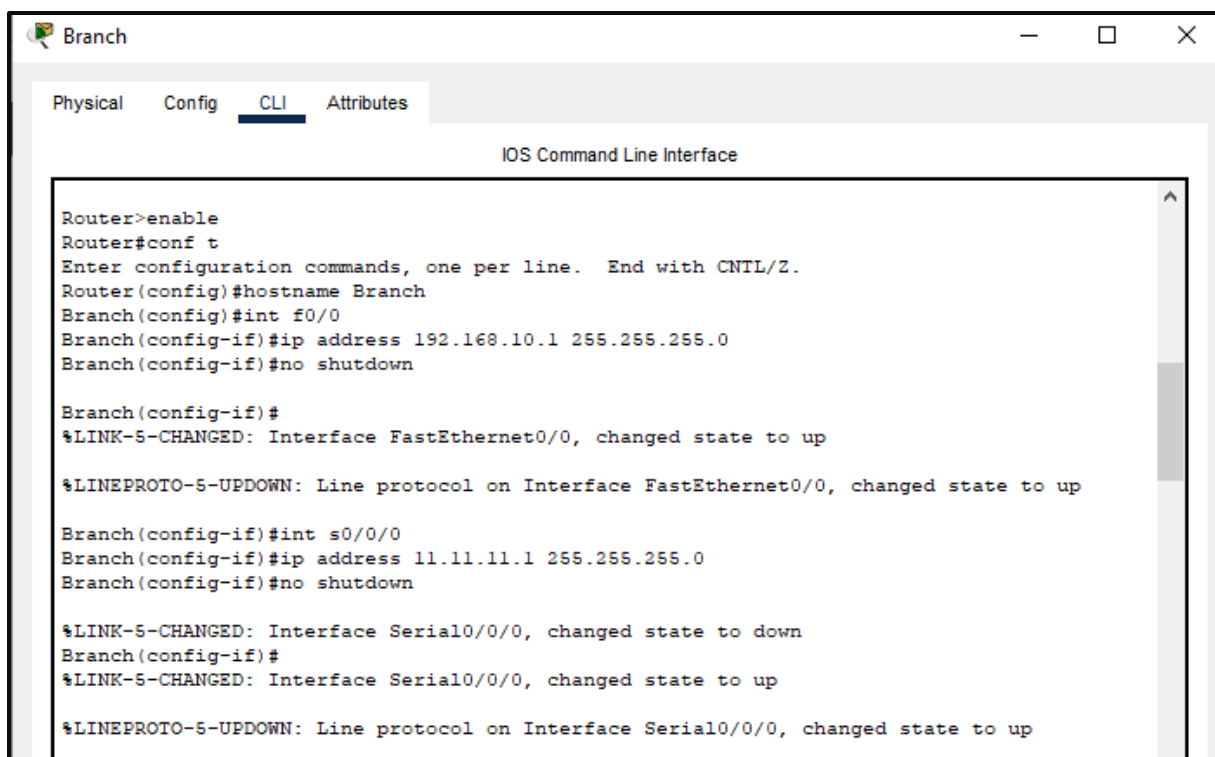


Step 2: Configure PC's



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

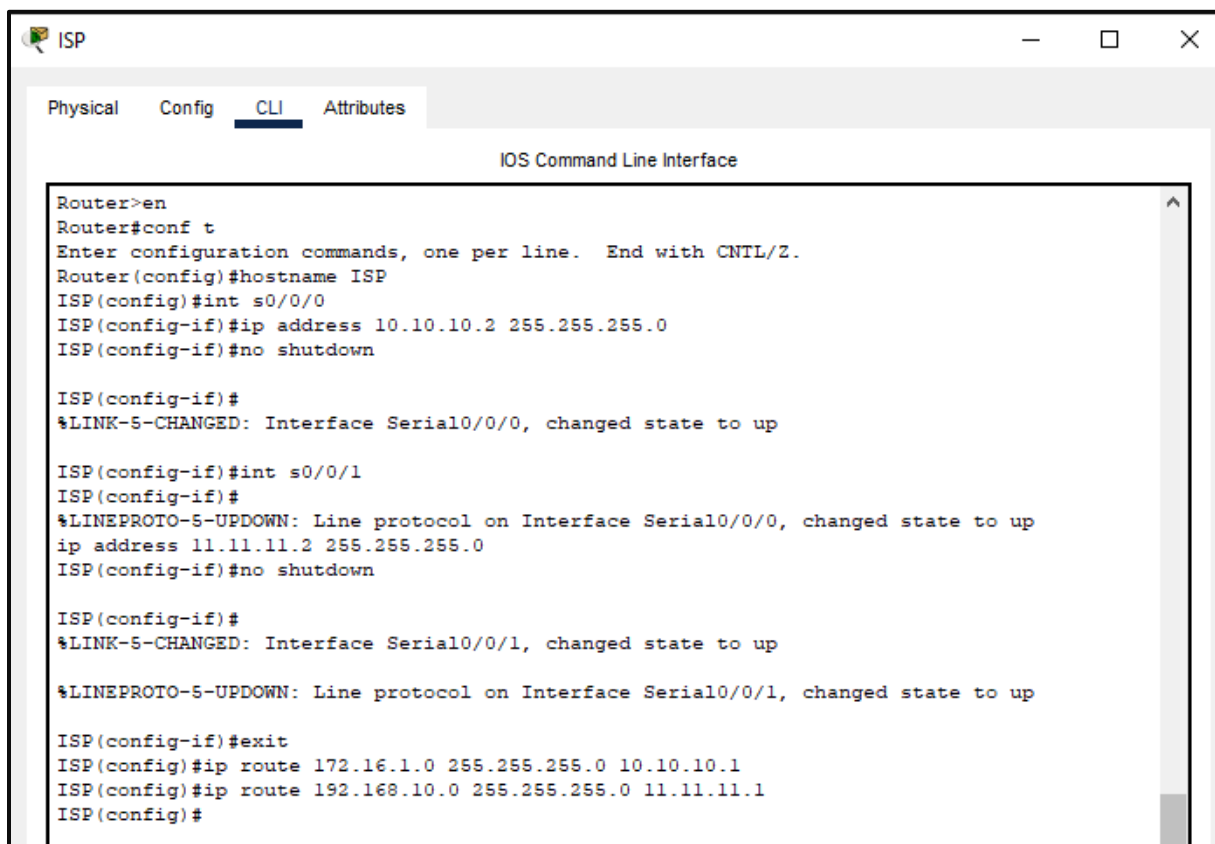
Branch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%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

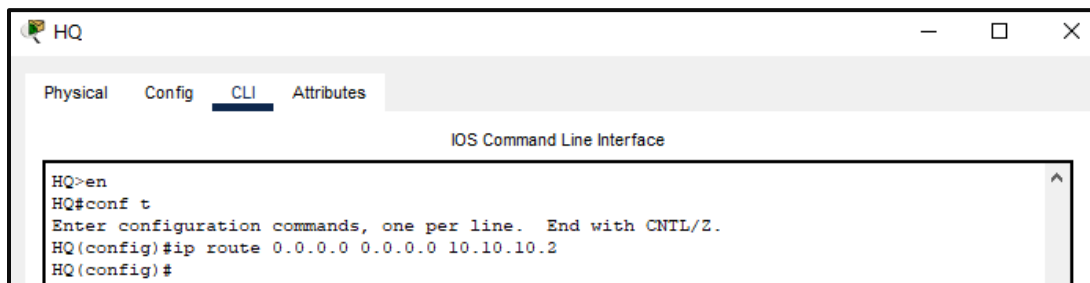
ISP(config-if)#int s0/0/1
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
ip address 11.11.11.2 255.255.255.0
ISP(config-if)#no shutdown

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

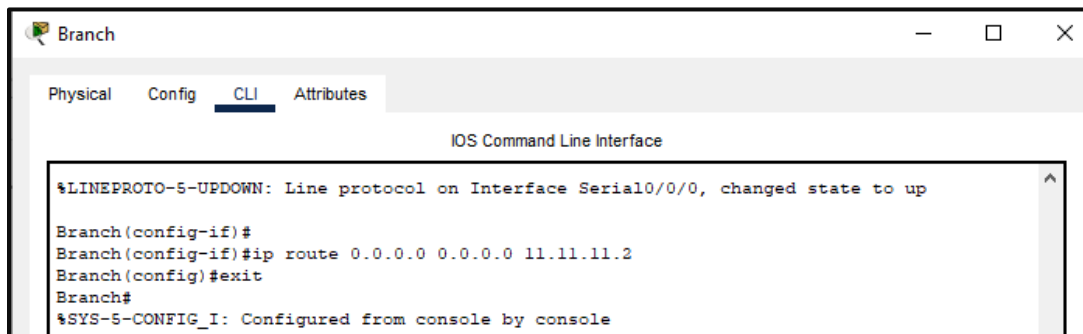
ISP(config-if)#exit
ISP(config)#ip route 172.16.1.0 255.255.255.0 10.10.10.1
ISP(config)#ip route 192.168.10.0 255.255.255.0 11.11.11.1
ISP(config)#
```

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



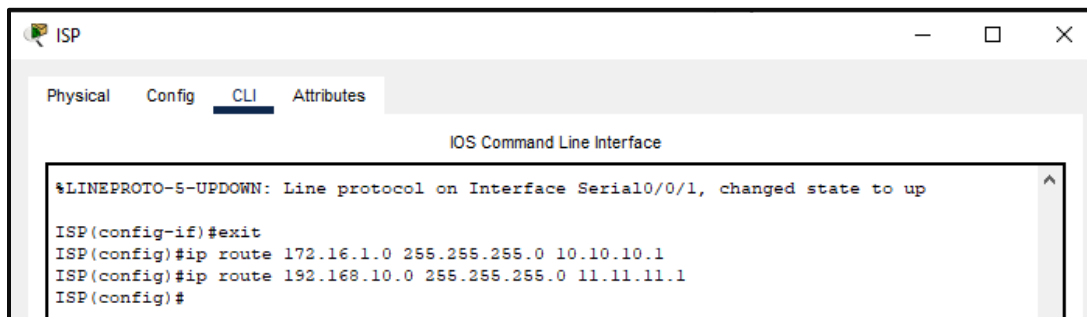
IOS Command Line Interface

```
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)#
```



IOS Command Line Interface

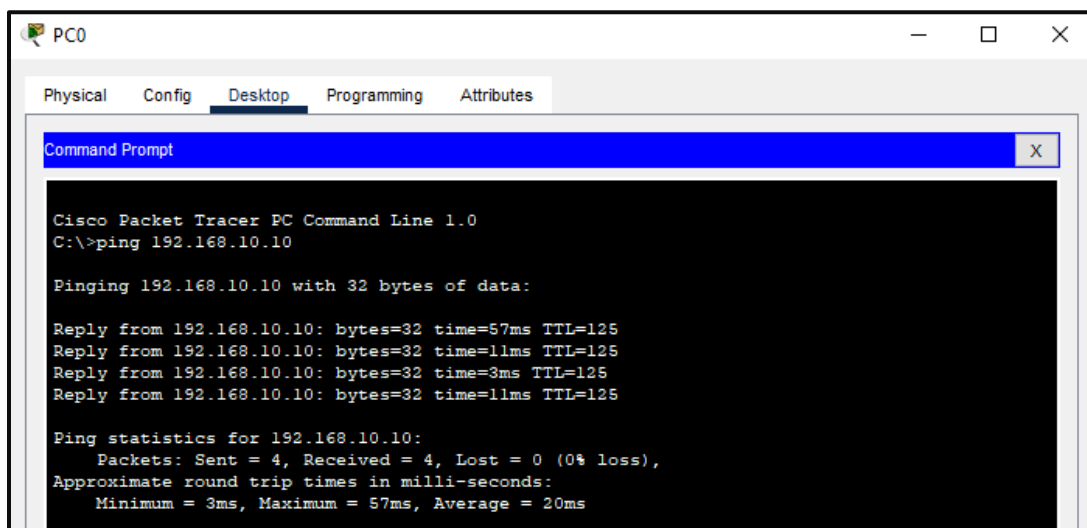
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Branch(config-if)#
Branch(config-if)#ip route 0.0.0.0 0.0.0.0 11.11.11.2
Branch(config)#exit
Branch#
%SYS-5-CONFIG_I: Configured from console by console
```



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



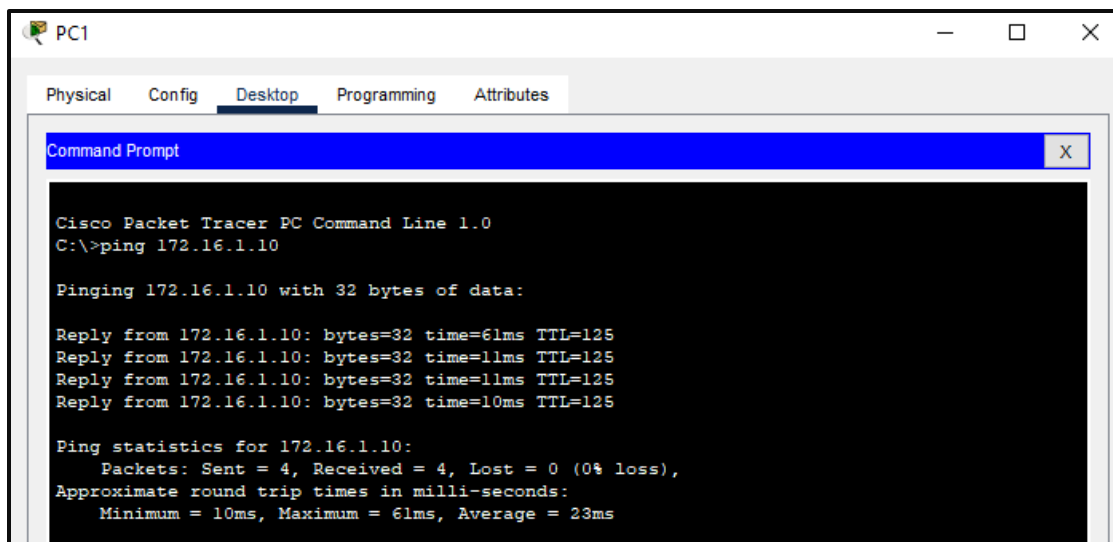
Command Prompt

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

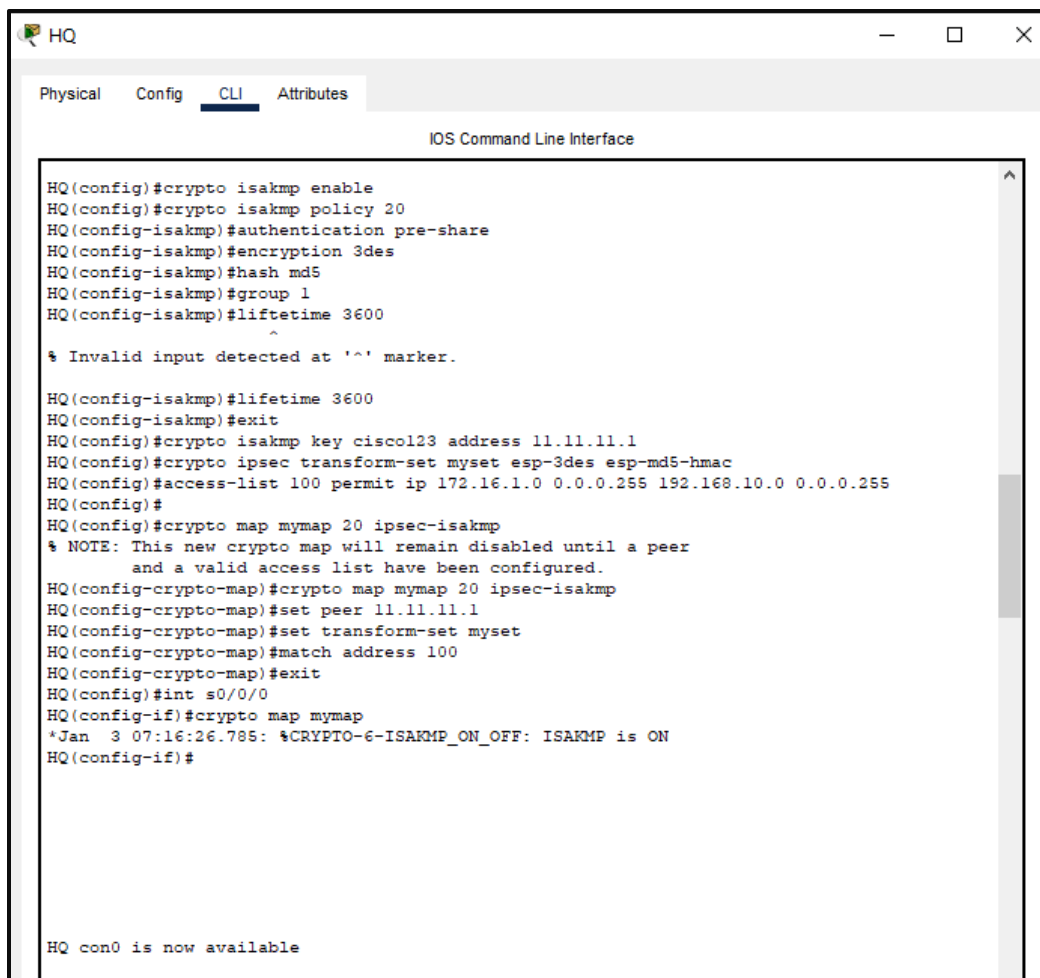
Pinging 192.168.10.10 with 32 bytes of data:

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



```

Branch>en
Branch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#crypto isakmp enable
Branch(config)#crypto isakmp policy 20
Branch(config-isakmp)#authentication pre-share
Branch(config-isakmp)#encryption 3des
Branch(config-isakmp)#hash md5
Branch(config-isakmp)#group 1
Branch(config-isakmp)#lifetime 3600
Branch(config-isakmp)#exit
Branch(config)#crypto isakmp key cisco123 address 10.10.10.1
Branch(config)#crypto ipsec transform-set myset esp-3des esp-md5-hmac
Branch(config)#
Branch(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 172.16.1.0 0.0.0.255
Branch(config)#exit
Branch#
%SYS-5-CONFIG_I: Configured from console by console

Branch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#crypto map mymap 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Branch(config-crypto-map)#set peer 10.10.10.1
Branch(config-crypto-map)#set transform-set myset
Branch(config-crypto-map)#match address 100
Branch(config-crypto-map)#exit
Branch(config)#
Branch(config)#int s0/0/0
Branch(config-if)#crypto map mymap
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Branch(config-if)#end
Branch#
%SYS-5-CONFIG_I: Configured from console by console

```

Step 7: Check the connection

```

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

C:\>ping 192.168.10.10

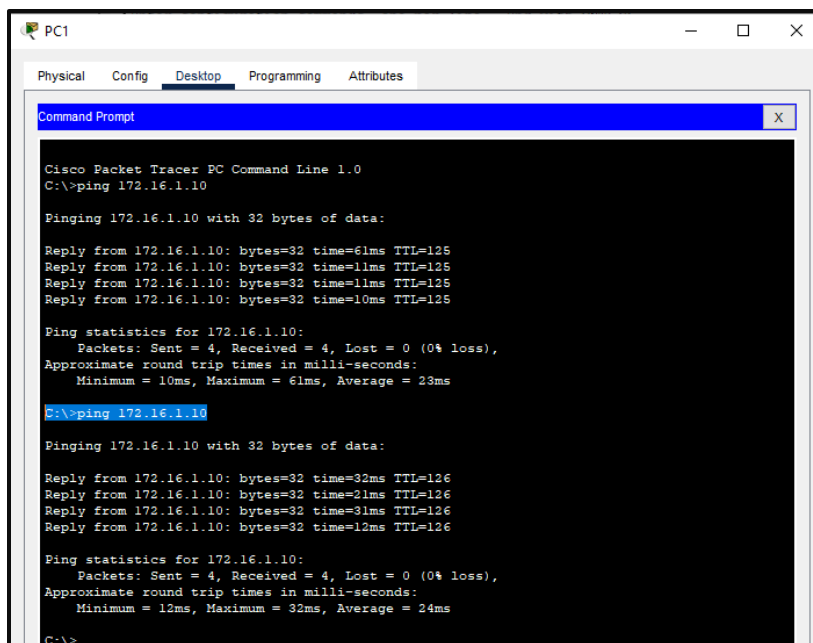
Pinging 192.168.10.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.10: bytes=32 time=12ms TTL=126
Reply from 192.168.10.10: bytes=32 time=11ms TTL=126
Reply from 192.168.10.10: bytes=32 time=16ms TTL=126

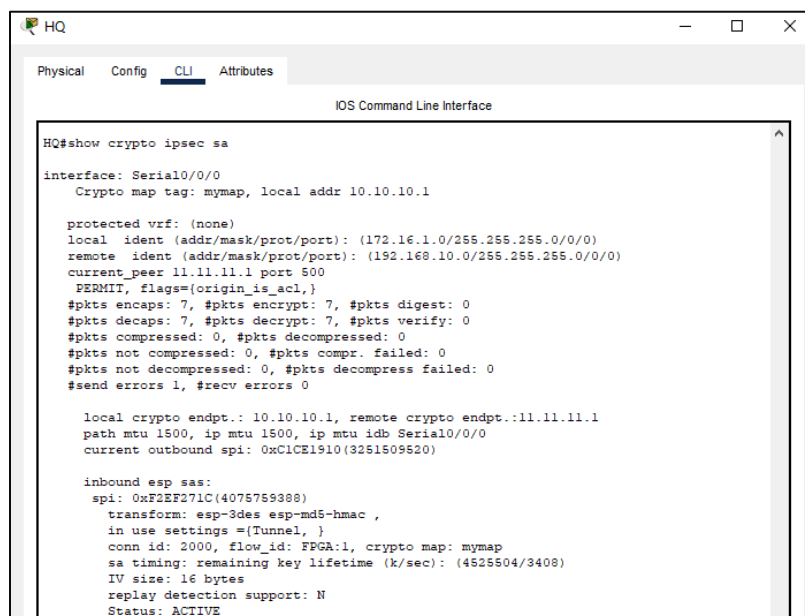
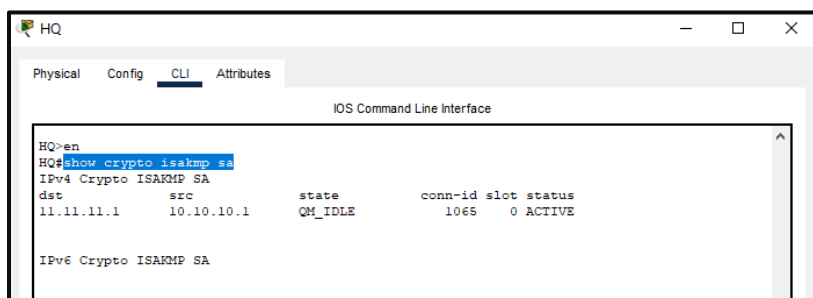
Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 16ms, Average = 12ms

C:\>

```

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



```

inbound ah sas:

inbound pcsp 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 pcsp 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 pcsp 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 pcsp sas:

Branch#
Branch#

```