

Index

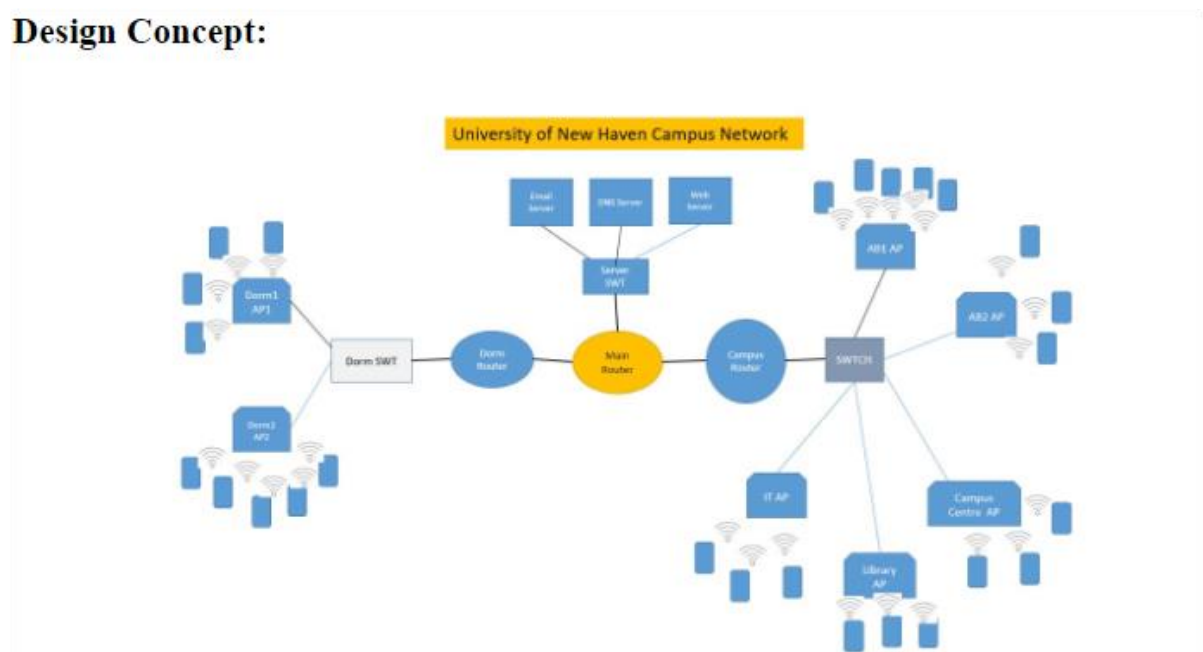
Sr. No	Title	Page. No
1.	<u>Campus Network.</u>	03
2.	<u>Solution.</u>	05
3.	<u>Step 1: Place all the End-Points.</u>	05
4.	<u>Step 2: Connect all devices.</u>	05
	<u>2.1 Router</u>	05
5.	<u>Step 3: Router Configuration.</u>	06
	<u>3.1 Main ISP.</u>	06
	<u>3.2 Campus ISP.</u>	07
	<u>3.3 Student ISP.</u>	07
6.	<u>Step 4: Server Configuration.</u>	08
7.	<u>Step 5: Access Point Configuration.</u>	09
8.	<u>Step 6: PC and Laptop Configuration.</u>	10
	<u>6.1 PC Module Upgradation.</u>	10
	<u>6.2 PC Wireless Connection.</u>	10
	<u>6.3 Laptop Module Upgradation.</u>	12
	<u>6.4 Laptop Wireless Connection.</u>	12
	<u>6.5 Smart Mobile and Tablet Connection.</u>	14
	<u>6.6 PC, Laptop, Smartphone, and Smart-tablet IP Configuration.</u>	14
9.	<u>Step 7: RIP.</u>	17
10.	<u>Step 8: Password Configuration for Routers.</u>	18
	<u>8.1 Main ISP.</u>	19
	<u>8.2 Campus ISP.</u>	20
	<u>8.3 Student ISP.</u>	21
	<u>8.4 Hostname and Password Table.</u>	22
11.	<u>Step 9: Communicate from one network to other.</u>	22
12.	<u>Conclusion.</u>	23

Campus Networking

OBJECTIVE:

The aim of this lab is to design the topology of the university network using the software Cisco Packet Tracer with the implementation of wireless networking systems. The lab provides insights into various concepts such as campus network design, topology design, layout architecture, IP address configuration, and more. In this lab we will learn how to design and setup a campus networking using Cisco packet tracer (simulation software) and test whether the message is passing between the different computer and servers. An efficient network is essential to facilitate the systematic and cost-efficient transfer of information in an organization in the form of messages, files, and resources. Also, the lab will show the wireless connectivity that is used in the university to make the network efficient and mobile at the same time. Mobility is the major concentration of this lab. In order to provide equal functionality to all the users (college staff and students), the lab added DNS, Email, and HTTP servers for the maximum utilization of resources. Hence the campus network provides different services such as connecting the user to the internet, data sharing among users (students, teachers, and different university members), accessing different web services for different functionalities, so it needs wireless networking for smooth processing

Design Concept:



This university network consists of the following devices:

- 1) Router (1941)
- 2) Switches (2960-24TT)
- 3) Email server
- 4) Servers: DNS server, WEB server (HTTP) and Email Server
- 6) Wireless Device (Access Point)
- 7) PCs
- 8) Laptops
- 9) Smartphones

The design includes the following parts of the University:

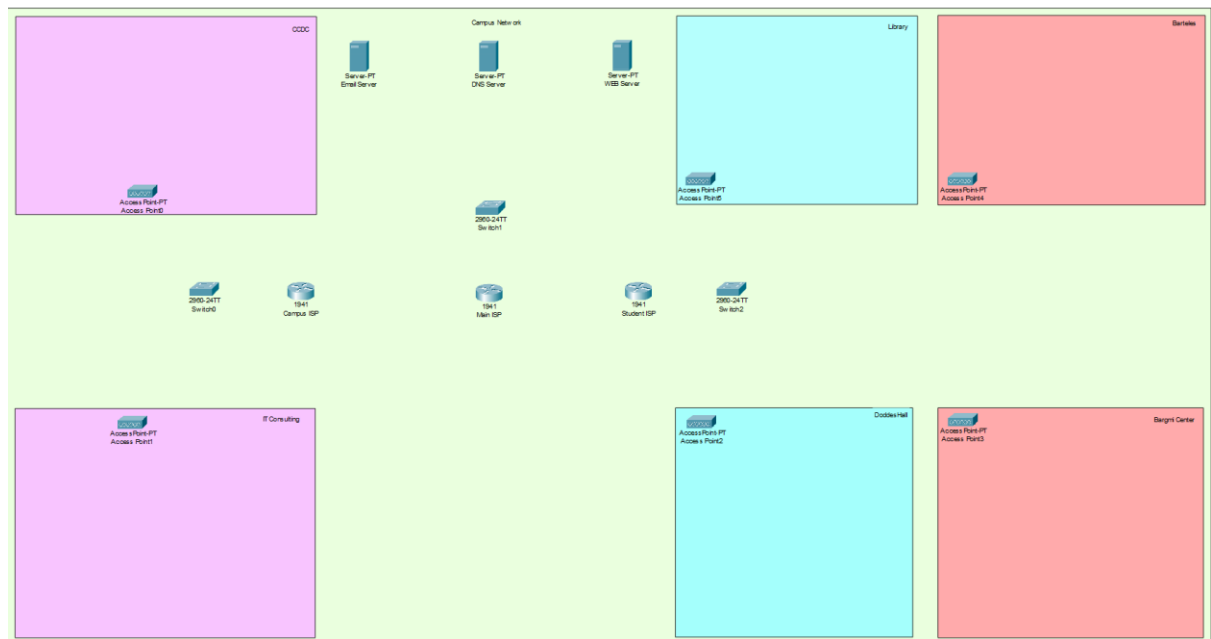
Academic Blocks: Bargmi Center, DoddesHall, Barteles, Library

Main Building: IT Consulting, CCDC

Solution.

Step 1: Place all the End-Points.

- ❖ Open the new file in packet tracer and create a create a six box for different department of the campus.
- ❖ Place all the device in each the box.
- ❖ Place 3 Router (1. Main ISP, 2. Campus ISP, 3. Student ISP)
- ❖ Place 3 Server (1. DNS server, 2. Mail Server, 3. Web Server)
- ❖ Place 6 Access point and rename it in each box for different Department of the Campus.

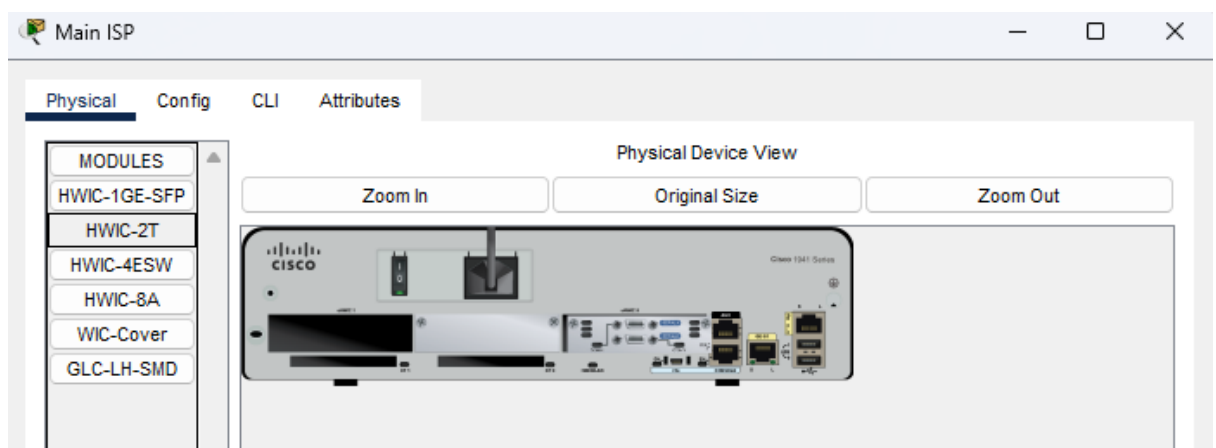


- ❖ Add the end point as the requirement in the department.

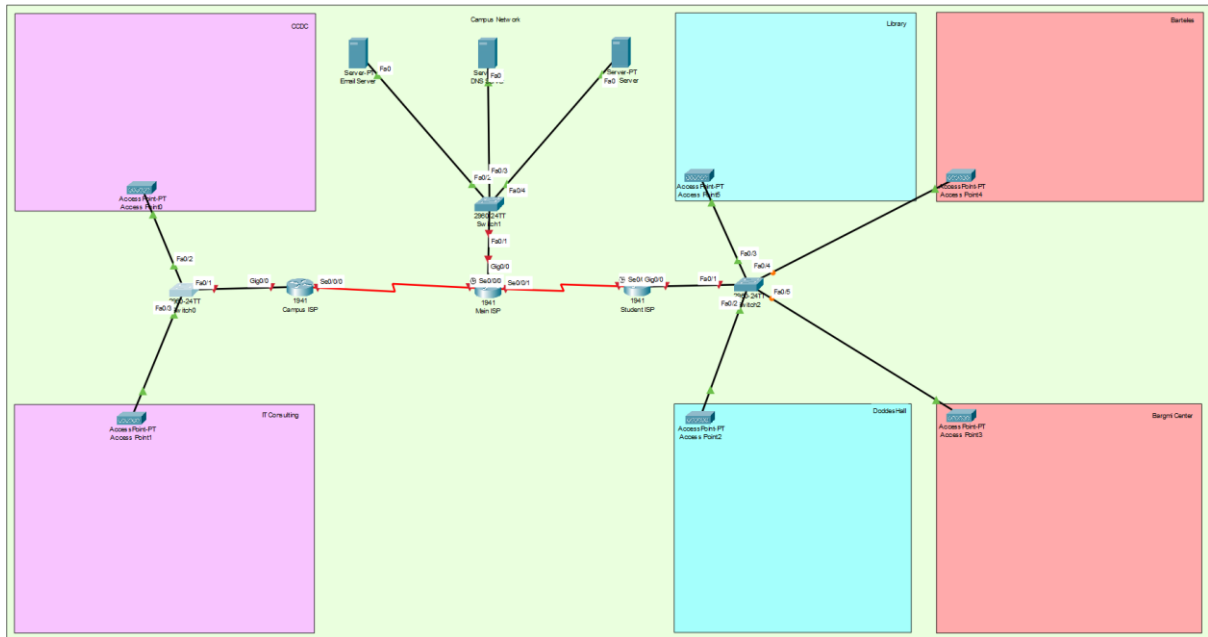
Step 2: Connect all devices.

Router.

- ❖ Power off the router and add the HWIC-2T modules in each router to make the router to communicate with each other and after upgrading on the router back.



- ❖ Connect the Router with Serial DTE cable.
- ❖ Connect all the other end point with Copper Straight Cable as shown in the below figure.



Step 3: Router Configuration.

- ❖ Open the CLI panel and copy or paste the given code.

Main ISP.

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#int se0/1/0
%Invalid interface type and number
Router(config)#int se0/0/0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
Router(config-if)#int se0/0/1
Router(config-if)#ip add 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#
```

Campus ISP.

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int se0/0/0
Router(config-if)#ip add 10.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(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
Router(config-if)#int g0/0
Router(config-if)#ip add 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#
```

Student ISP.

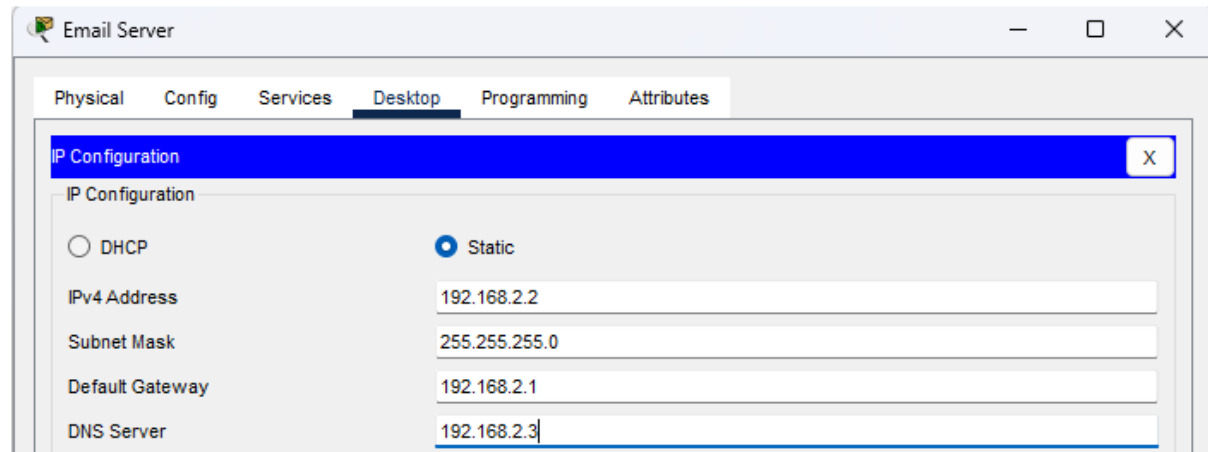
```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#int se0/0/1
Router(config-if)#ip add 11.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(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
Router(config-if)#
```

- ❖ If the connection will get established successfully than all the network flow signal will change to green colour.

Step 4: Server Configuration.

- ❖ Open the IP Configuration from the Desktop tab of the server.
- ❖ Add manually IP and Default Gateways to each server as shown in the figure add the IP and Gateways in Email Server, DNS Server, and Web Server.

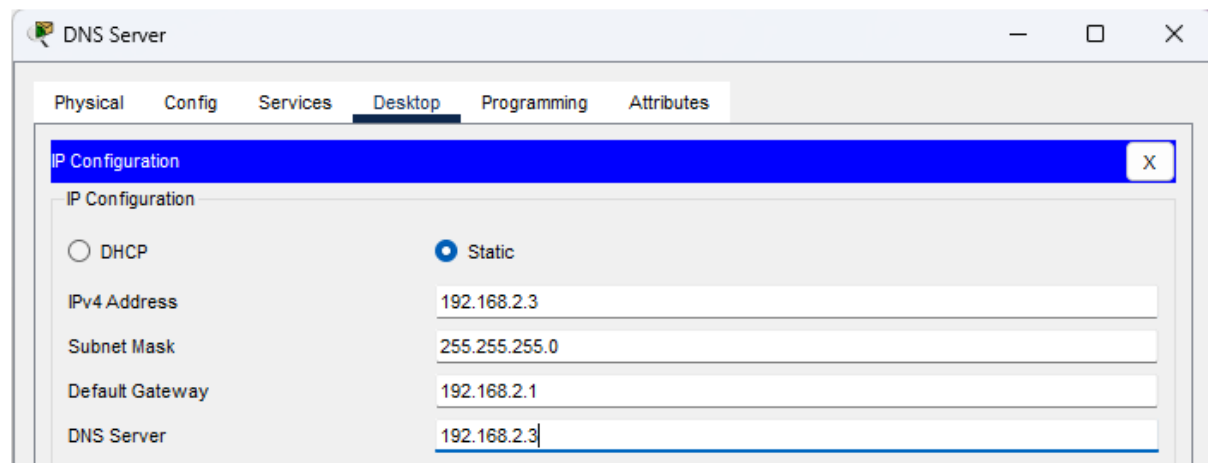
Email Server.



The screenshot shows the 'Email Server' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is active, showing the 'Static' radio button selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.2.3

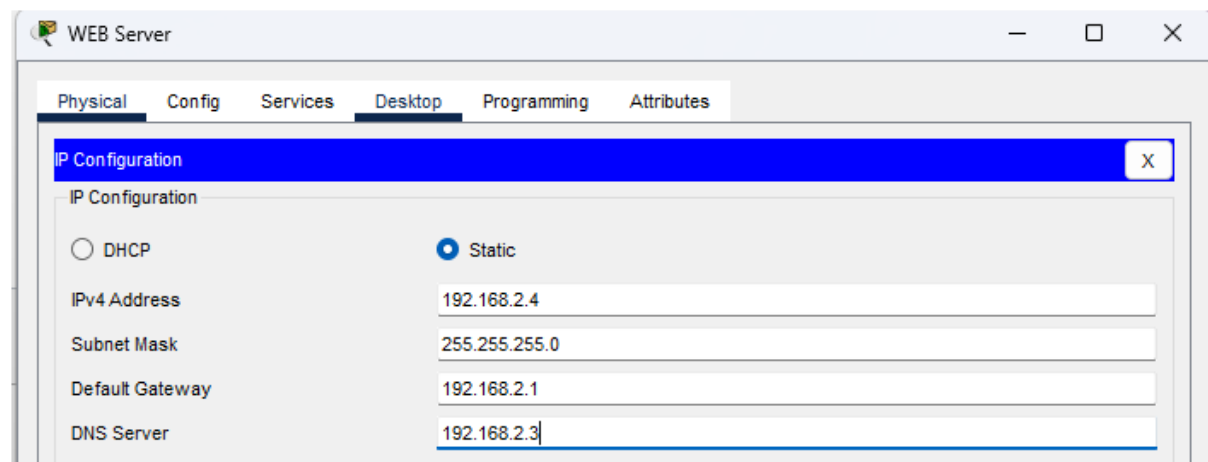
DNS Server.



The screenshot shows the 'DNS Server' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is active, showing the 'Static' radio button selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.2.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.2.3

Web Server.

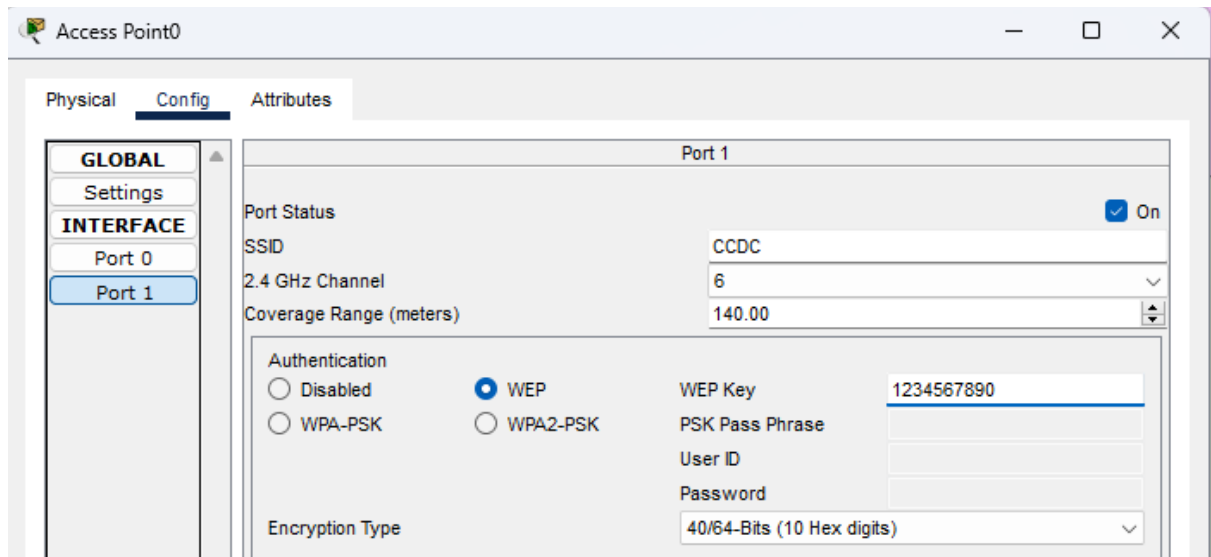


The screenshot shows the 'WEB Server' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is active, showing the 'Static' radio button selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.2.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.2.3

Step 5: Access Point Configuration.

- ❖ We are going to add the WEP Key and Username for each access point of the department for the better connectivity of the devices.
- ❖ For that open the Port 1 which lies under the Interface in the Config Tab.
- ❖ Then Update SSID of the Access point and click the WEP radio button under the authentication part.
- ❖ We had select the 40/64-Bits (10 Hex Digits) Encryption type from the two options.
- ❖ So enter the WEP key of 10 digits.



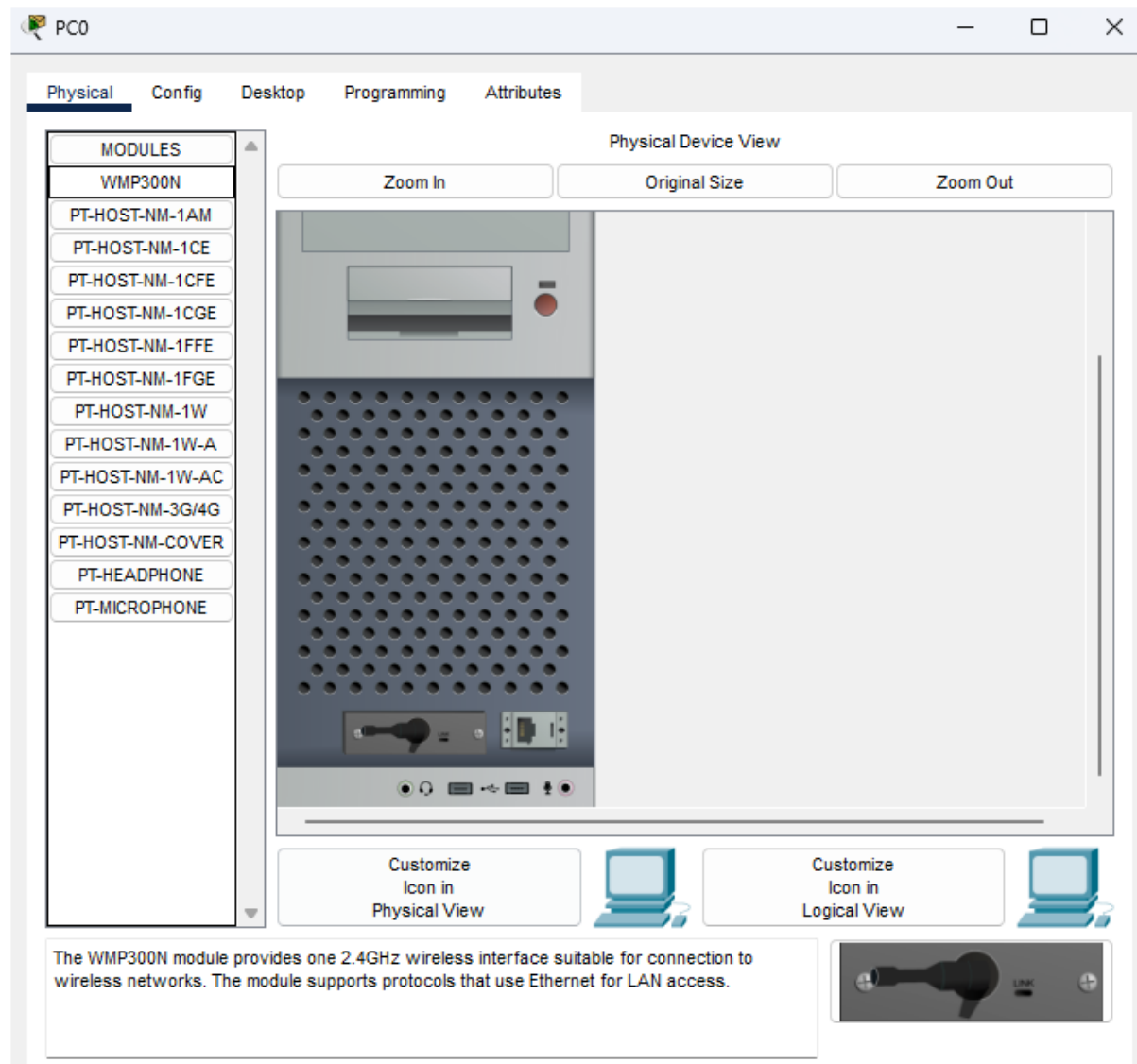
- ❖ The following table show all the SSID and WEP key of all the Access Point.

SR.NO	SSID	WEP-KEY
1	CCDC	1234567890
2	IT Consulting	2345678901
3	Doddes Hall	3456789012
4	Bargmi Center	4567890123
5	Barteles	5678901234
6	Library	6789012345
7	Lib	7890123456

Step 6: PC and Laptop Configuration.

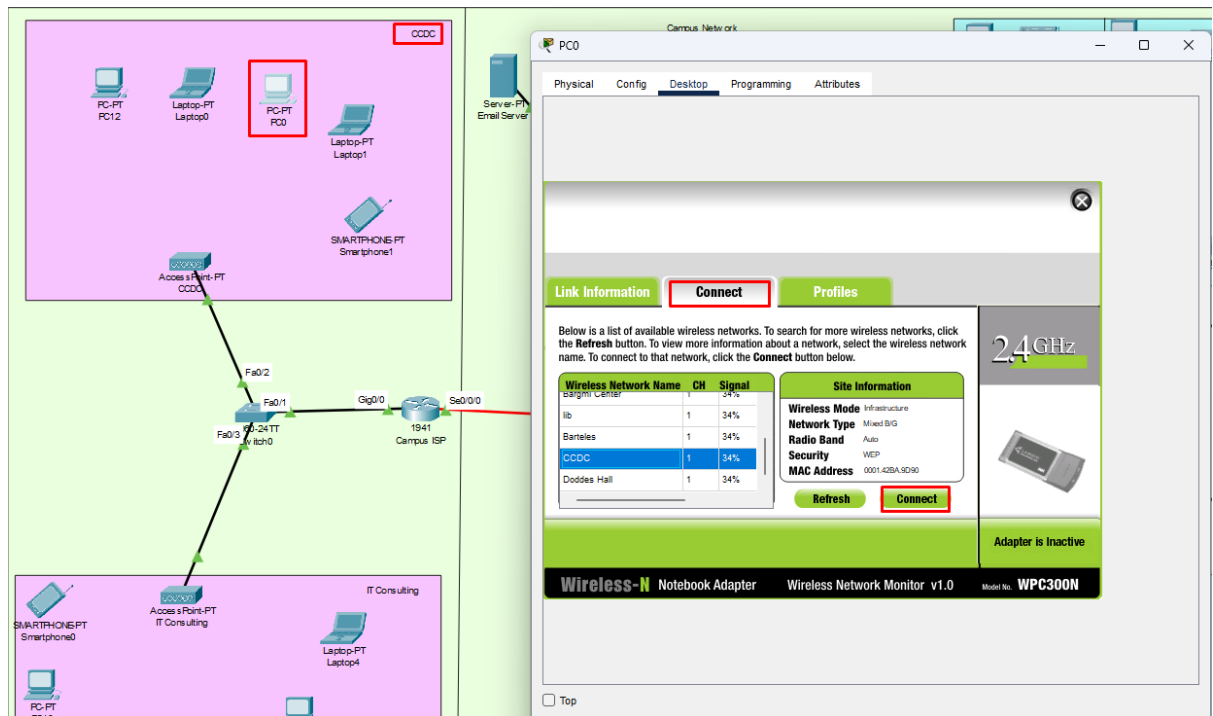
PC Module Upgradation.

- ❖ Power off the PC and Remove the “PT-HOST-NM-1CGE” module and Add the “WMP300N” module to connect the PC wireless to Access Point.
- ❖ After finishing the Upgradation turn on the PC.



PC wireless connection.

- ❖ Open the PC Wireless under the Desktop Tab of the PC.
- ❖ Then click on the connect tab and search for the Department name and connect to it with the WEP-Key.
- ❖ As shown in the figure. Repeat these steps in each PC of any department.

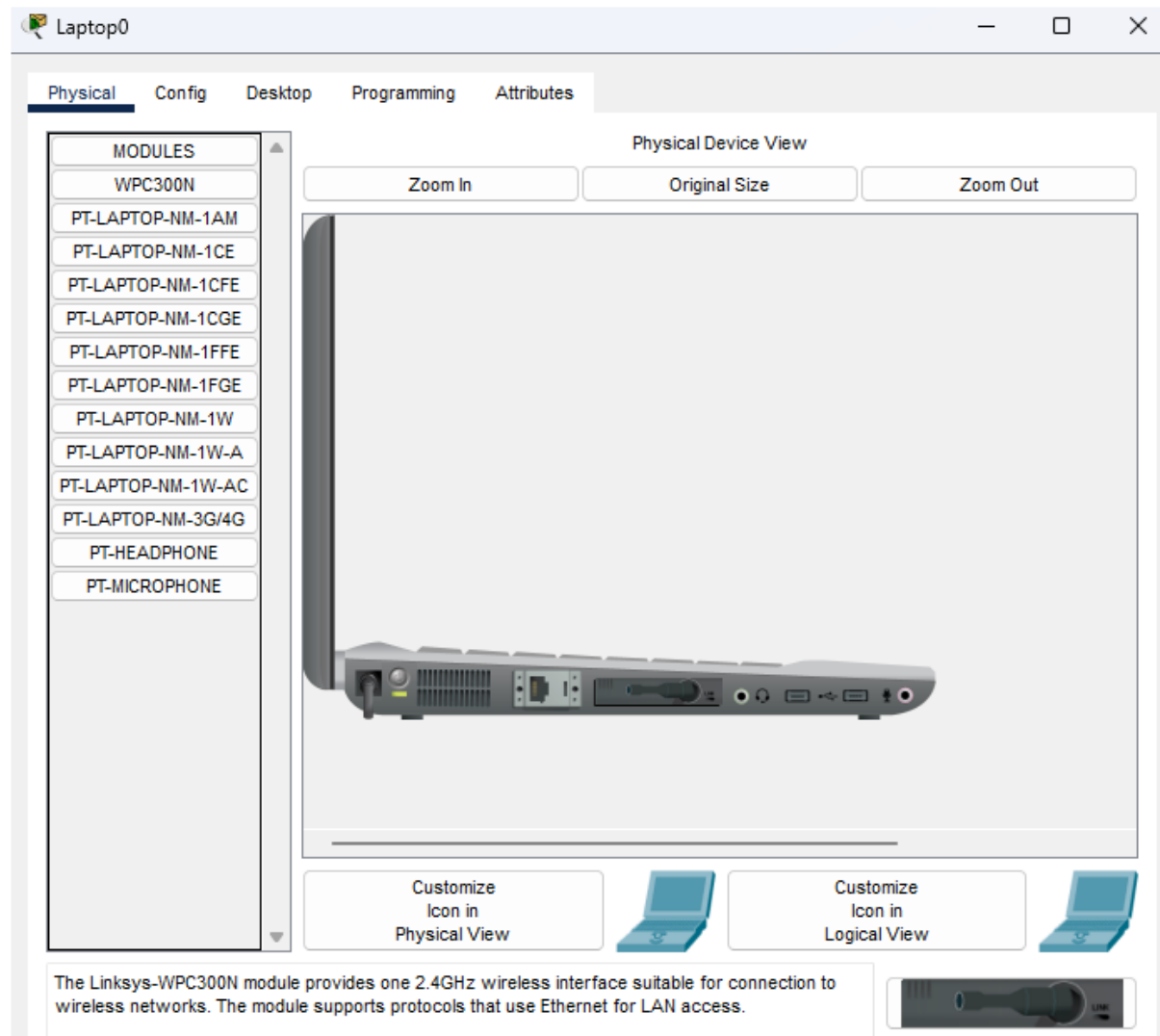


- ❖ After entering the password move back to the link Information to confirm the connection has been established or not.



Laptop Module Upgradation.

- ❖ Power off the Laptop and Remove the “PT-LAPTOP-NM-1CGE” module and Add the “WMP300N” module to connect the Laptop wireless to Access Point.
- ❖ After finishing the Upgradation turn on the Laptop.



Laptop Wireless Connection.

- ❖ Open the PC Wireless under the Desktop Tab of the Laptop.
- ❖ Then click on the connect tab and search for the Department name and connect to it with the WEP-Key.
- ❖ As shown in the figure. Repeat these steps in each Laptop of any department.

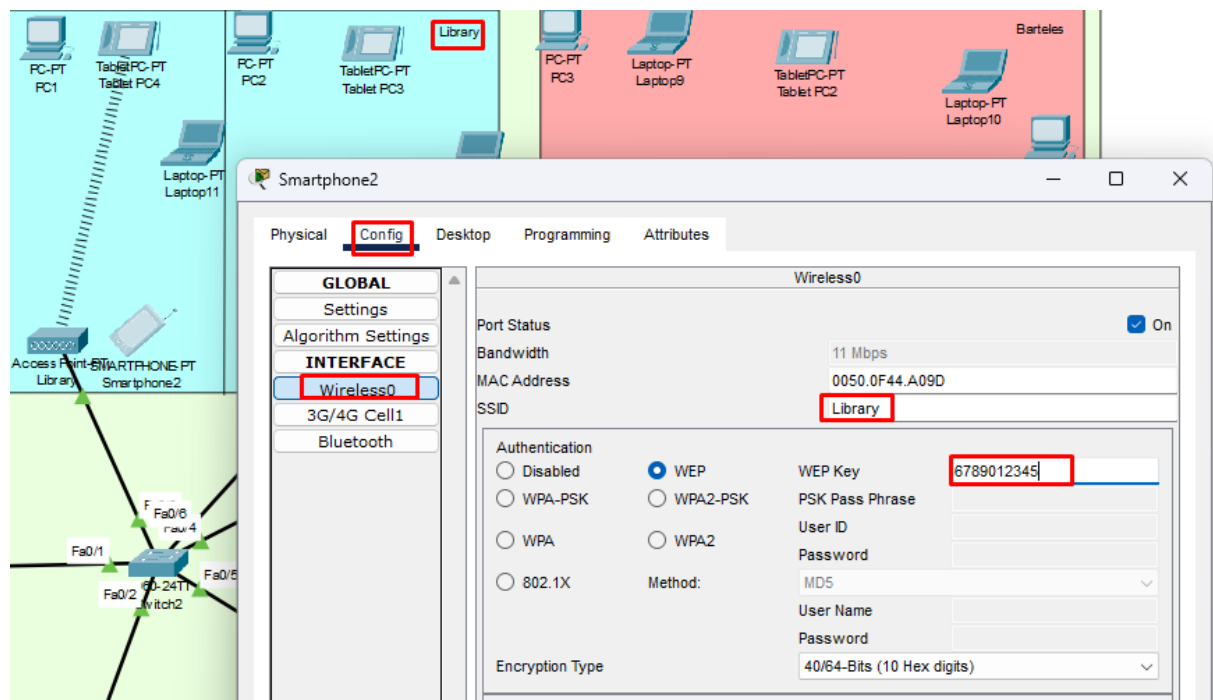


- ❖ After entering the password move back to the link Information to confirm the connection has been established or not.



Smart Mobile or Tablet Connection.

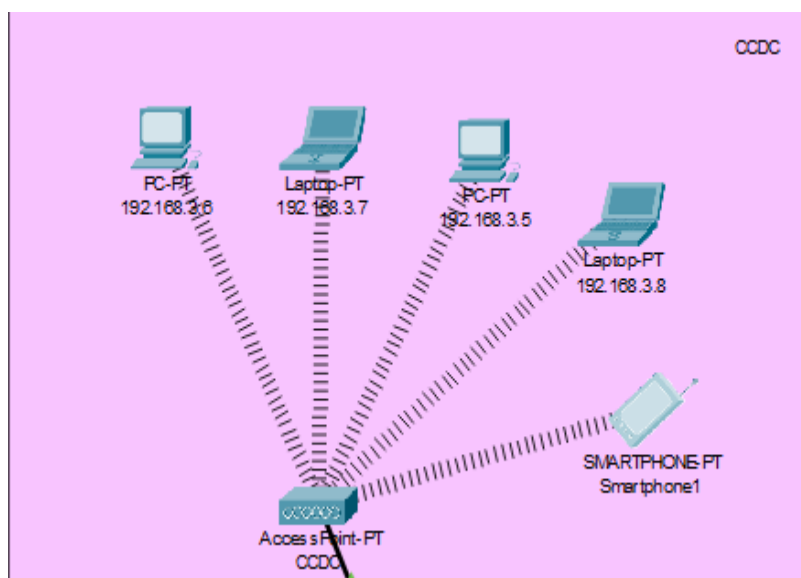
- ❖ Open the wireless interface from the config tab of the Smart device.
- ❖ Add the SSID and WEP-Key of respective department.



PC, Laptop, Smartphone, and Smart-tablet IP Configuration.

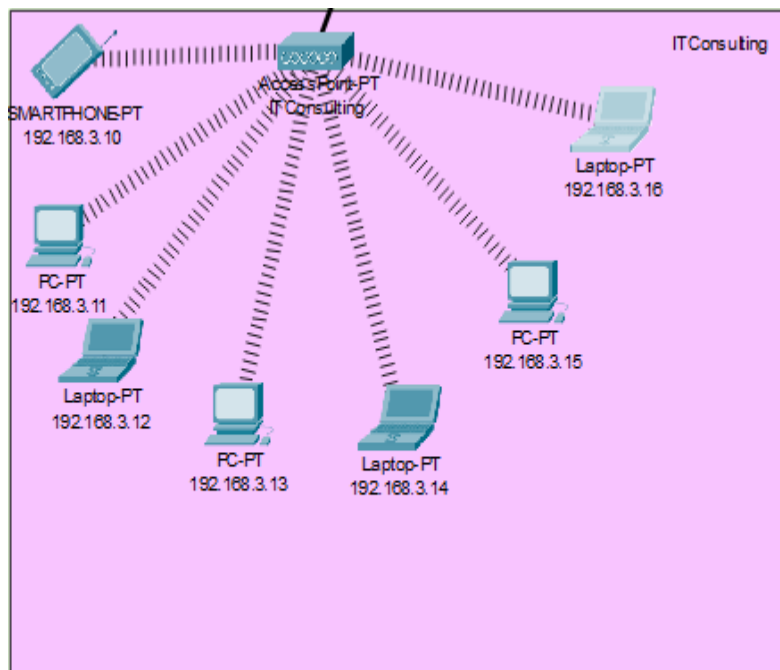
- ❖ Open the IP configuration from the Desktop Tab and click on the Static Ratio Button.
- ❖ Add the IP address, Default Gateway and DNS server for each device.

CCDC Department



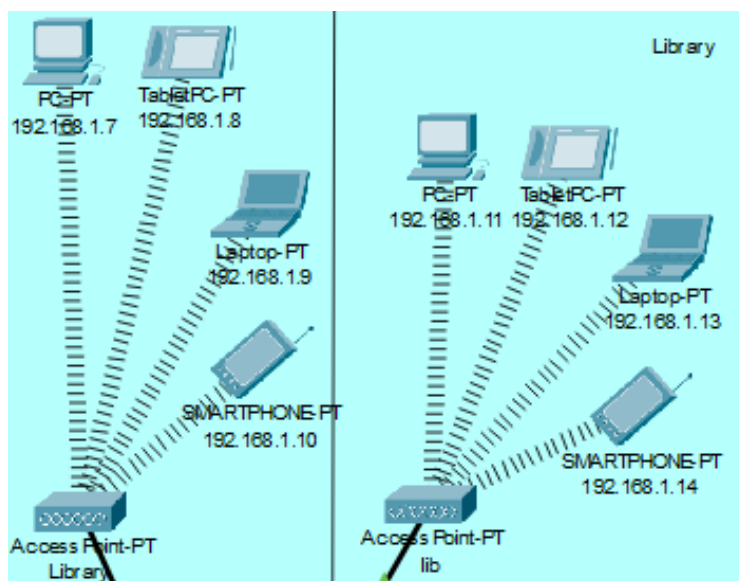
- 192.168.3.5 PC
- 192.168.3.6 PC
- 192.168.3.7 Laptop
- 192.168.3.8 Laptop
- 192.168.3.9 Smartphone
- 192.168.3.1 Default gateway
- 192.168.2.3 DNS Server

IT Consulting Department



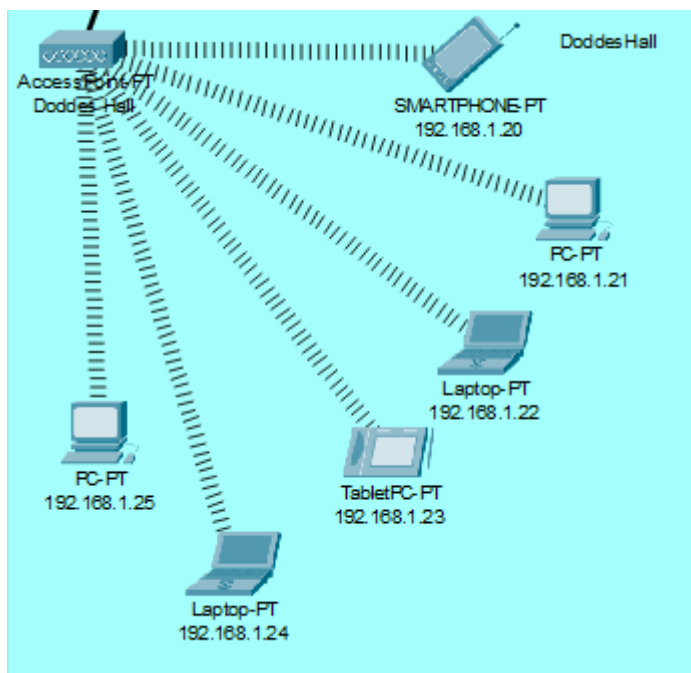
192.168.3.10 Smart Phone
 192.168.3.11 PC
 192.168.3.12 Laptop
 192.168.3.13 PC
 192.168.3.14 Laptop
 192.168.3.15 PC
 192.168.3.16 Laptop
 192.168.3.1 Default gateway
 192.168.2.3 DNS Server

Library Department



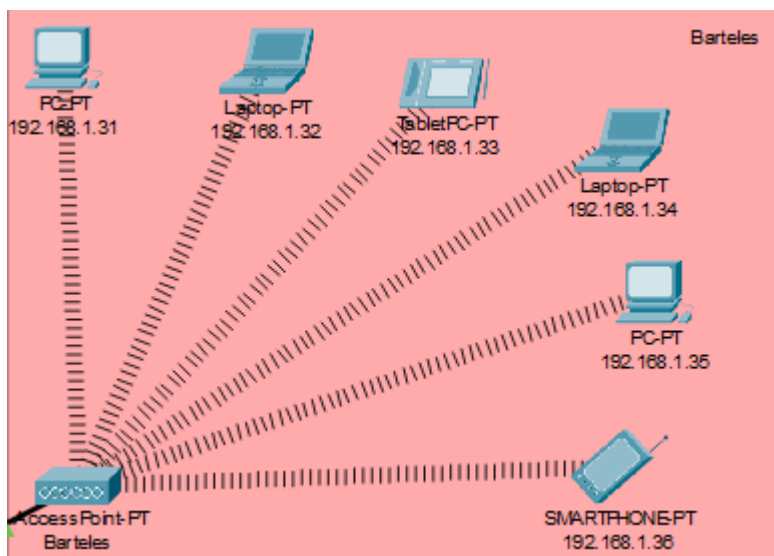
192.168.1.7 PC
 192.168.1.8 Tablet
 192.168.1.9 Laptop
 192.168.1.10 Smart phone
 192.168.1.11 PC
 192.168.1.12 Tablet
 192.168.1.13 Laptop
 192.168.1.14 Smart phone
 192.168.1.1 Default Gateway
 192.168.2.3 DNS Server

Doddes Hall Department



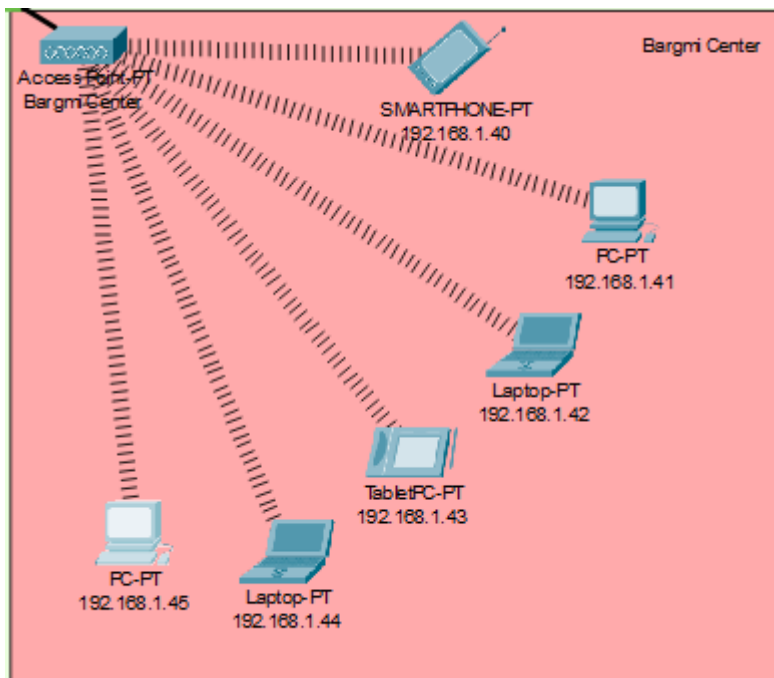
192.168.1.20 Smart phone
 192.168.1.21 PC
 192.168.1.22 Laptop
 192.168.1.23 Tablet
 192.168.1.24 Laptop
 192.168.1.25 PC
 192.168.1.1 Default Gateway
 192.168.2.3 DNS Server

Barteles Department



192.168.1.31 PC
 192.168.1.32 Laptop
 192.168.1.33 Tablet
 192.168.1.34 Laptop
 192.168.1.35 PC
 192.168.1.36 Smart phone
 192.168.1.1 Default Gateway
 192.168.2.3 DNS Server

Bargmi Center Department

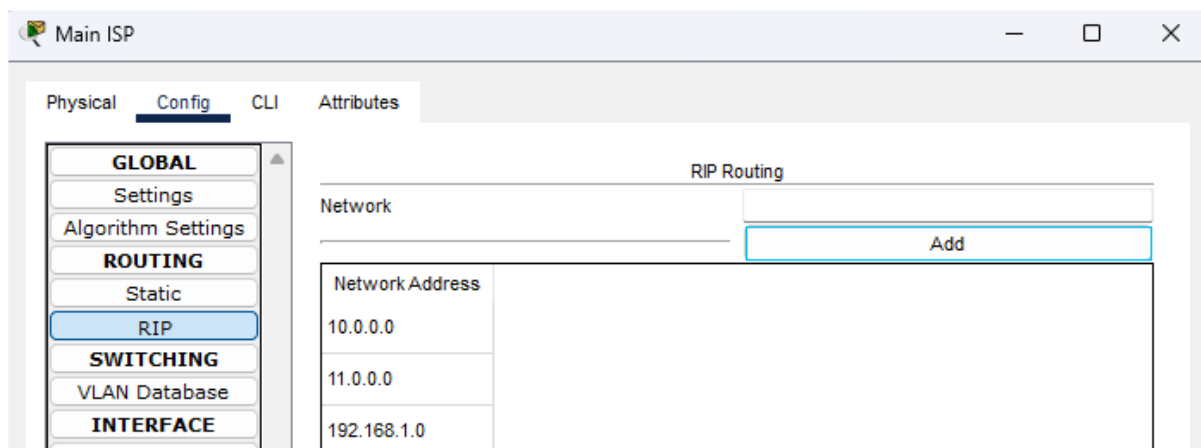


192.168.1.40 Smart phone
 192.168.1.41 PC
 192.168.1.42 Laptop
 192.168.1.43 Tablet
 192.168.1.44 Laptop
 192.168.1.45 PC
 192.168.1.1 Default Gateway
 192.168.2.3 DNS Server

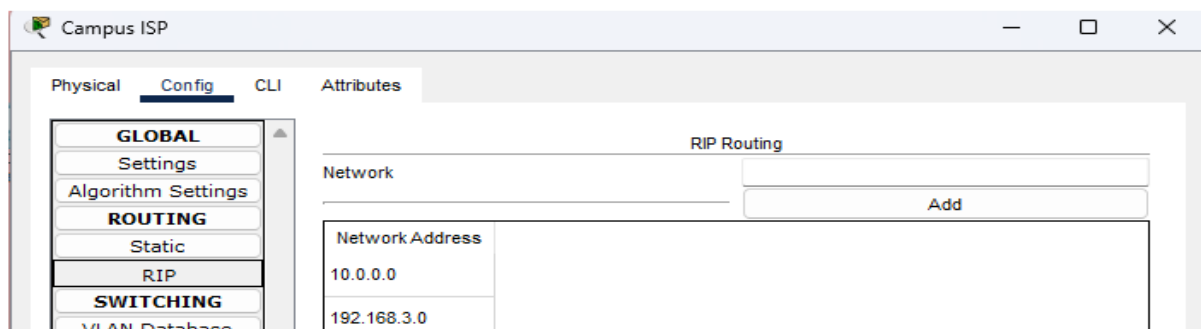
Step 7: RIP.

- ❖ Set the incoming and outgoing network in the router RIP for make the valid address.
- ❖ For that Open the Router Config Tab.
- ❖ And Click on the RIP and add the Network in all the 3 routers.

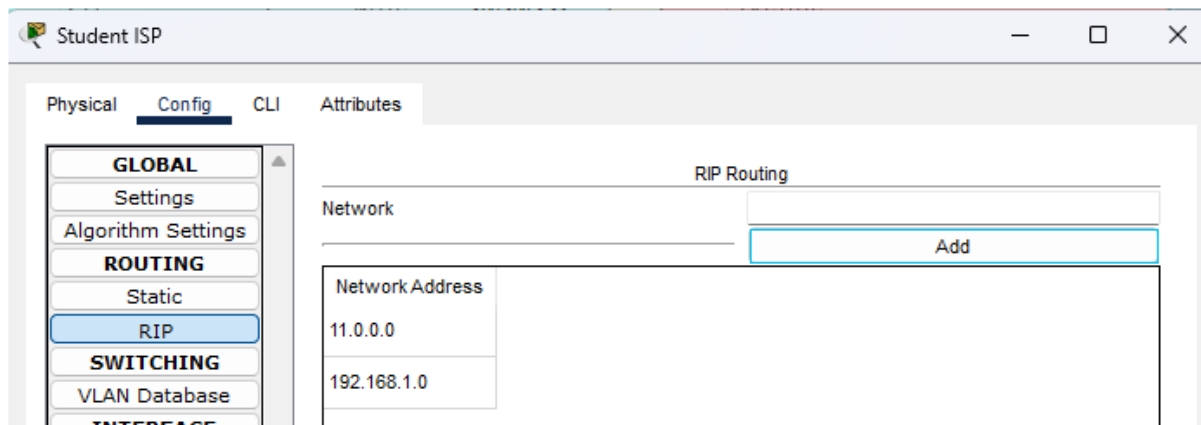
Main ISP



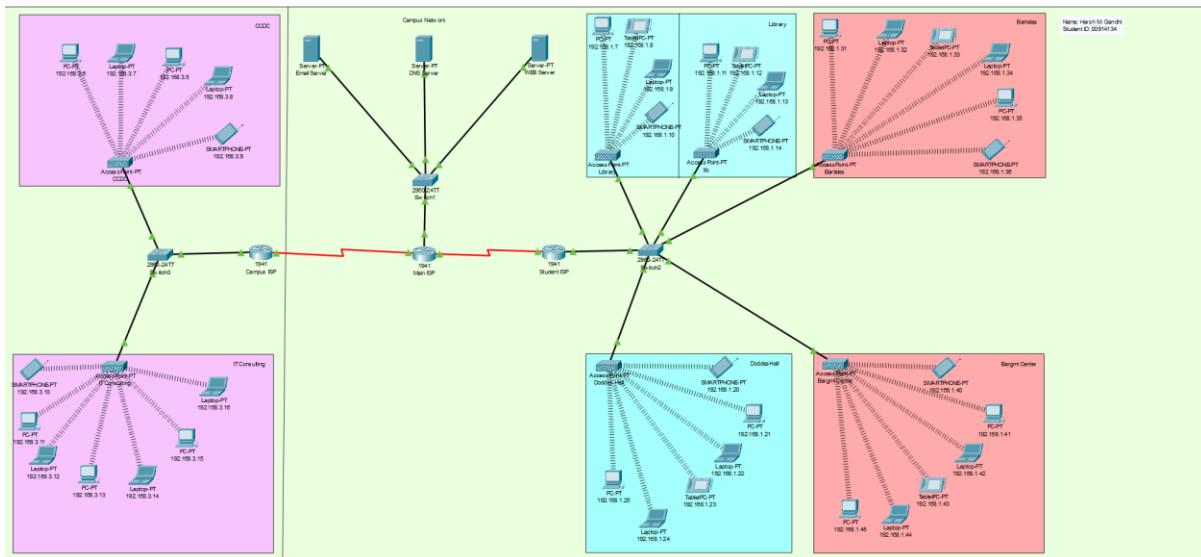
Campus ISP



Student ISP



After Connecting all the Device in the Network it will look like as follows.



Step 8: Password Configuration for the Routers.

- ❖ For make the connection prohibited for the outsider user we have to add the console password and ssh password in all the router.
- ❖ Open the CLI tab of the router.
- ❖ Then take an access to privileged mode.
- ❖ Then select the console for set the password after set the password just check it once is working correct or not.
- ❖ Repeat the same step for set SSH password.
- ❖ Apply the following command for set password and check the password connectivity.

Main ISP.

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password hmgcisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
Router con0 is now available
Press RETURN to get started.
User Access Verification
Password:
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password admin
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
Router con0 is now available
Press RETURN to get started.
User Access Verification
Password:
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip domain name admin
Router(config)#hostname admin
admin(config)#crypto key generate rsa
% You already have RSA keys defined named admin.admin .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: admin.admin
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
admin(config)#enable password admin
*Mar 1 0:15:57.884: %SSH-5-ENABLED: SSH 1.99 has been enabled
admin(config)#username admin password admin
admin(config)#ip ssh version 2
admin(config)#line vty 0 15
```

```
admin(config-line)#transport input ssh
admin(config-line)#login local
admin(config-line)#
```

Campus ISP.

```
Router>en
```

```
Router#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#line console 0
```

```
Router(config-line)#password hmgcisco@123
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

```
Router(config)#exit
```

```
Router#
```

%SYS-5-CONFIG_I: Configured from console by console

```
Router#exit
```

Router con0 is now available

Press RETURN to get started.

User Access Verification

Password:

```
Router>en
```

```
Router#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#line vty 0 4
```

```
Router(config-line)#password admin
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

```
Router(config)#exit
```

```
Router#
```

%SYS-5-CONFIG_I: Configured from console by console

```
Router#exit
```

Router con0 is now available

Press RETURN to get started.

User Access Verification

Password:

```
Router>en
```

```
Router#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#ip domain name admin
```

```
Router(config)#hostname admin
```

```
admin(config)#crypto key generate rsa
```

% You already have RSA keys defined named admin.admin .

% Do you really want to replace them? [yes/no]: yes

The name for the keys will be: admin.admin

Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
admin(config)#enable password admin
```

```
*Mar 1 0:41:6.210: %SSH-5-ENABLED: SSH 1.99 has been enabled
admin(config)#username admin password admin
admin(config)#ip ssh version 2
admin(config)#line vty 0 15
admin(config-line)#transport input ssh
admin(config-line)#login local
admin(config-line)#
```

Student ISP.

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password hmgcisco@321
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
Router con0 is now available
Press RETURN to get started.
User Access Verification
Password:
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password admin
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
Router con0 is now available
Press RETURN to get started.
User Access Verification
Password:
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip domain name admin
Router(config)#hostname admin
admin(config)#crypto key generate rsa
% You already have RSA keys defined named hmgstudentadmin.hmgstudentadmin .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: admin.admin
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
admin(config)#enable password admin
*Mar 1 0:37:6.879: %SSH-5-ENABLED: SSH 1.99 has been enabled
admin(config)#username admin password admin
admin(config)#ip ssh version 2
admin(config)#line vty 0 15
admin(config-line)#transport input ssh
admin(config-line)#login local
admin(config-line)#

```

Hostname and Password Table.

Main ISP	Console hmgcisco Ssh admin
Campus ISP	Console hmgcisco@123 Ssh admin
Student ISP	Console hmgcisco@321 Ssh admin

Step 9: Communicate from One network to other.

- ❖ Open the terminal from any Laptop or PC.
- ❖ Then try to get the RDP(Remote Desktop Protocol) connection by enter the Username and Password which we had set in the above Step.
- ❖ Apply the following commands to transfer the packet from Student Isp to Campus ISP through passing the Main ISP.

```

C:\>ssh -l admin 192.168.1.1
Password:
admin>ssh -l admin 192.168.2.1
Password:
admin>ssh -l admin 192.168.3.1
Password:
admin>ping 192.168.3.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/54 ms

admin>

```

```
192.168.1.25
Physical Config Desktop Programming Attributes
Command Prompt
Password:
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l admin 192.168.1.1
Password:
admin>ssh -l admin 192.168.2.1
Password:
admin>ssh -l admin 192.168.3.1
Password:
admin>ping 192.168.3.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/54 ms
admin>
[Connection to 192.168.3.1 closed by foreign host]
admin>
[Connection to 192.168.2.1 closed by foreign host]
admin>
[Connection to 192.168.1.1 closed by foreign host]
C:\>
Top
```

Conclusion.

By doing these labs we can share the packet from one network to another network if we have the perfect credential and proper destination. It is a secure way to communicate between the network, no one can read the path of the message.