

Project

Campus Network Design Using Cisco Packet Tracer

ABSTRACT

The main goal of this project is to learn how to use the simulation for designing and studying networks. In order to achieve the defined task, analyze literature sources related to communication networks. Briefly describe the basic network categories. Analyze networks and briefly describe their components and technologies. Explain the Wi-Fi technology.

Analyze literature sources related to network simulators. Analyze the Network simulator ns-2 and give its detailed description. Present a brief comparison of the ns-2 simulator with other open-source network simulators. Specify the configuration for the simple wireless network and create the corresponding model by using the cisco packet tracer simulator. Demonstrate selected characteristics of the specified network configuration using the simulation model.

Contents

ABSTRACT	2
1. Introduction:.....	5
a. Problem Identification.	5
b. Project Business Objectives,	5
c. Requirements Definition,	5
2. Network Scenario	6
3. Network Design Topology	6
3.1. -Campus Interconnection Network	7
3.2. Design campuses	7
3.3. Server	7
3.3.1. DNS Server	8
3.3.2. WEB Server	8
3.3.3. EMAIL Server	8
3.4. Router.....	8
3.5. Switch	9
4. Simulation Environment	9
4.1. Required resources.....	9
4.2. Addressing Table	10
4.3. Router Interface Configuration.....	12
4.4. Routing Information Protocol (RIP).....	13
Versions of RIP	13
Configuring RIP on routers	14
4.5. Securing Routers	14
4.5.1. Network security	15
4.5.2. Router configuration for security.....	15
4.5.3. Secure Router Configuration.....	15
4.6. Whole Router Configurations	17
4.7. Main_router	17
4.8. College Router.....	20
4.9. Hostel Router	22
4.10. SSH Protocol.....	24
4.11. Testing:.....	24

4.11.1.	Connect to AB1	24
4.11.2.	Connect to AB2	25
4.11.3.	Connect to Library.....	25
4.11.4.	Connect to IT consulting	26
4.11.5.	Connect to Boys Block.....	27
4.11.6.	Connect to Girls Block	27
4.12.	Wireless Test	28
4.12.1.	Wireless access point configurations.....	28
4.12.1.	Available wireless networks	31
4.12.2.	Server Configuration	33
4.12.3.	Email Server	33
4.12.4.	DHCP configuration	34
4.12.5.	DNS Server	35
4.12.6.	WEB server.....	36
4.12.7.	Testing Servers	36
4.12.8.	Test Mail server	37
4.12.9.	PING TEST	37
4.12.10.	Check PC configuration	37
4.12.11.	Check router security configuration	39
5.	Challenges and Lessons Learned:.....	40
6.	Conclusions and Recommendations:.....	40
7.	References	41

1. Introduction:

a. Problem Identification.

Security is always important in any network communication, especially with virtual and hierarchical networks, using wireless communication that is less secure than a wired network. The problem investigated in this thesis is about the security issues with wireless networks, especially due to using a registration system process and then forwarding the messages across an unsecured network.

b. Project Business Objectives,

Cisco packet tracer (CPT) is the main technology that we depended on designing and simulating a secure campus network. CPT is a visual simulation tool that has been created and designed by cisco system. CPT has been used as an effective tool to teach and learn network communication in realistic way. It offers a realistic visualization and simulation tool for learning. That what help the users especially students to create, design, configure, and troubleshoot different type of networks such as LAN and WAN. Also, it helps with the security problems by using security protocols. For example, qualifying the use of some protocols like spanning tree protocol which helps with the looping problems; especially when there are three switches connected to each other.

c. Requirements Definition,

- Cisco Packet tracer Simulator
- Routers
- switches
- Cabling
- Servers
- Computers
- Access Points

2. Network Scenario

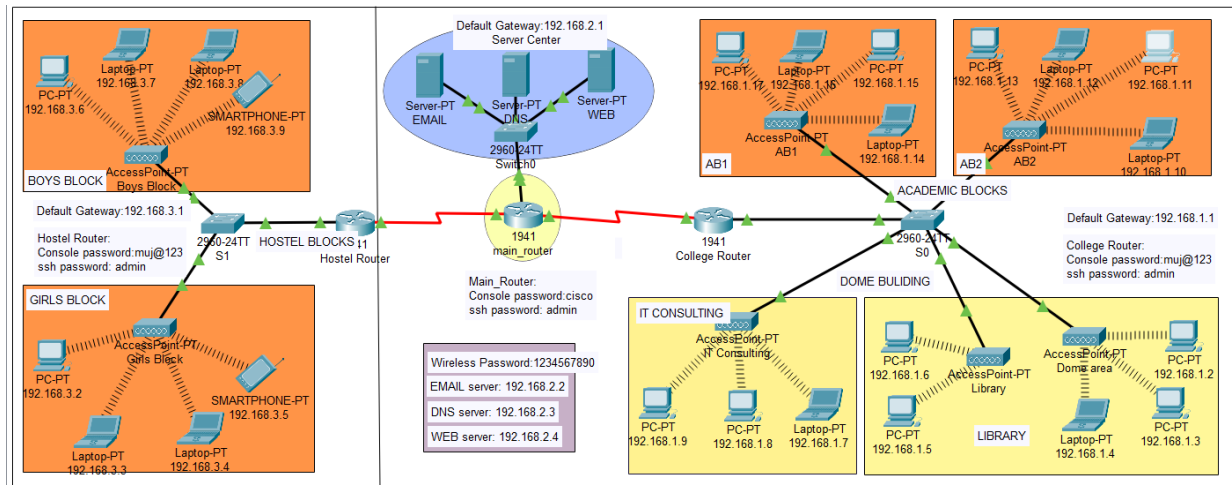
Nowadays, the network has become the need of most people, especially science seekers. A lot of researchers and scientists are depending excessively on networks to get more information. Students' also involved in the case of network-dependent for a lot of reasons like sharing information, and knowledge between themselves. Thus, the network is an important demand of each community and organization.

Nevertheless, the network can fall under many threats and intrusions; and the reason behind that is the development of web technologies and services. Those attacks can occur in many different ways either physically damaging the devices or logically hacking the codes. That type of intrusion can cause a lot of problems because of the lack of veracity. Therefore, security has a significant effect in protecting the network from those types of attacks. Network security can be applied in many aspects of the network in order to keep it from unauthorized access. Thus, network security is now one of the essential issues in many firms like universities.

As consequence, we designed a secure campus network (SCN) which includes many networks and each network consists of many VLANs'. Those networks are supported by a security system that prevents outside access without authentication. Also, it protects the sanctity and privacy of each user, so no one can attack their private information. In section 1, we explained the technologies that we used to implement SCN which is packet tracer. Also, we explained the SCN structure and the required resources that we used to create the SCN topology. In section 2, we explained internet protocol (IP) addressing methods, and the connectivity between the devices in entire network. Whereas, virtual local area network (VLAN) explanation and simulation has been taking part in section 3. After that in section 4, there is a detailed illustration about security and configurations that we applied in the campus topology using packet tracer. Finally, in section 5 a secure network campus scenario will be conclude.

3. Network Design Topology

The topology that is designed for campus network consists of two main parts or buildings. Each part contains different devices as switches, computers, access point, wireless router, and servers. All of those devices are connected with a switch that connects them directly with a router. The routers in the campus are connected with each other dynamically as it's shown in Figure 1.



3.1. -Campus Interconnection Network

In large-scale networking with branch chains or branch offices, branch networks need to access the other branch. In this scenario where interconnection between branches is required.

3.2. Design campuses

There are different departments. Network is divided into two sets: one for the campus area and the other for the hostel area.

3.3. Server

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers.

Many networks contain one or more of the common servers. The servers used in our project are as follows:

3.3.1. DNS Server

DNS stands for Domain Name System servers which are application servers that provide a human-friendly naming method to the user computers in order to make IP addresses readable by users. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a user needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

3.3.2. WEB Server

One of the widely used servers in today's market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services.

3.3.3. EMAIL Server

An e-mail server is a server that handles and delivers e-mail over a network, using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The POP3 protocol receives messages and is used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

3.4. Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divides broadcast domains of hosts connected through it.

3.5. Switch

A network switch (also called switching hub, bridging hub, officially MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

4. Simulation Environment

The simulations of our network topology can be easily achieved using Cisco Packet Tracer. Using a simulation mode, you can see packets flowing from one node to another and can also click on a packet to see detailed information about the OSI layers of the networking. Packet Tracer offers a huge platform to combine realistic simulation and visualize them simultaneously. Cisco Packet Tracer makes learning and teaching significantly easier by supporting multi-user collaboration and by providing a realistic simulation environment for experimenting with projects.

4.1. Required resources

In order to design a secure campus network (SCN), we used different devices wired and wireless. Also, we used different types of communication media to connect the devices. After connecting the devices, we implemented many important configurations as VLANs, dynamic host configuration protocol (DHCP), and RIP. Moreover, we applied security and management techniques in the main devices of the network; to make the campus network safer and to protect it from interior and exterior attackers. So, the sanctity and the privacy of the user will be granted.

We used different types of devices in our work to show different connectivity cases. Most of the devices are connected using cables like PCs.

4.2. Addressing Table

Device	Interface	IP address	Gateway	Switch port
Main_router	SE 0/1/1	11.0.0.1/8		College Router SE 0/1/1
	SE 0/1/0	10.0.0.1/8		Hostel Router SE 0/1/0
	Gig 0/1	192.168.2.1/24		Server Center
College Router	SE 0/1/1	11.0.0.2/8		
	Gig 0/0	192.168.1.1/24		
Hostel Router	SE 0/1/0	10.0.0.2/8		
	Gig 0/0	192.168.3.1/24		
Email Server		192.168.2.2/24		
DNS Server		192.168.2.3/24		
WEB Server		192.168.2.4/24		
PC-PT	192.168.3.6/24		192.168.3.1	Boys Block SSID : muj_boys
Laptop-PT	192.168.3.7/24			
Laptop-PT	192.168.3.8/24			
SMARTPHONE- pt	192.168.3.9/24			
PC-PT	192.168.3.2/24			Girls Block SSID : muj_girls
Laptop-PT	192.168.3.3/24			
Laptop-PT	192.168.3.4/24			
SMARTPHONE- pt	192.168.3.5/24			
PC-PT		192.168.1.17/24	192.168.1.1	AB1 SSID : muj_AB1
Laptop-PT		192.168.1.16/24		
PC-PT		192.168.1.15/24		
PC-PT		192.168.1.13/24		AB2 SSID : muj_AB2
PC-PT		192.168.1.12/24		
PC-PT		192.168.1.11/24		
PC-PT		192.168.1.10/24		
PC-PT		192.168.1.2/24		Demo area

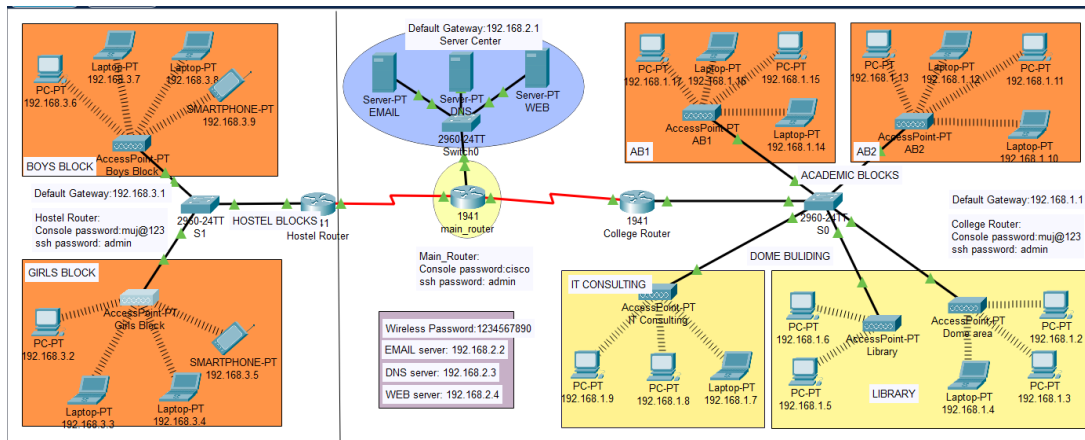
PC-PT		192.168.1.3/24		SSID: muj_dome
PC-PT		192.168.1.4/24		
PC-PT		192.168.1.5/24		Library
PC-PT		192.168.1.6/24		SSID :
PC-PT		192.168.1.9/24		muj_library
PC-PT		192.168.1.8/24		IT Consulting
PC-PT		192.168.1.7/24		SSID : muj_ITC

College Router:
 Console password:muj@123
 ssh password: admin

Main_Router:
 Console password:cisco
 ssh password: admin

Hostel Router:
 Console password:muj@123
 ssh password: admin

Wireless Password:1234567890



4.3. Router Interface Configuration

Router Interfaces

Main_router

```
!
!
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/1/0
ip address 10.0.0.1 255.0.0.0
!
interface Serial0/1/1
ip address 11.0.0.1 255.0.0.0
!
!
```

College Router

```
!
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/1/0
ip address 11.0.0.2 255.0.0.0
```

```
clock rate 2000000
```

```
!  
!
```

Hostel Router

```
!  
!
```

```
interface GigabitEthernet0/0  
ip address 192.168.3.1 255.255.255.0  
duplex auto  
speed auto
```

```
!
```

```
interface Serial0/1/0  
ip address 10.0.0.2 255.0.0.0  
clock rate 1200
```

```
!
```

```
!
```

4.4. Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a **distance-vector routing protocol**. Routers running the distance-vector protocol send all or a portion of their routing tables in routing-update messages to their neighbors. You can use RIP to configure the hosts as part of a RIP network.

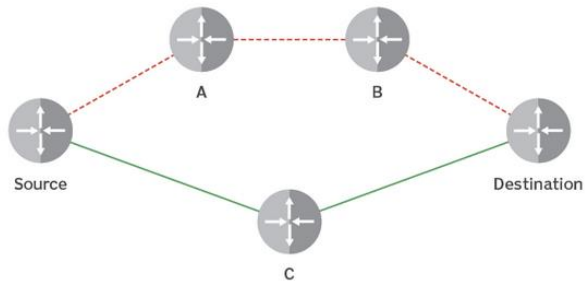
Versions of RIP

There are three versions of the Routing Information Protocol:

1. RIPv1.
2. RIPv2.
3. RIPvng.

Routing information protocol (RIP)

RIP uses the shortest number of hops to determine the best path to a remote network.



Configuring RIP on routers

Main_router

```
!  
router rip  
network 10.0.0.0  
network 11.0.0.0  
network 192.168.1.0  
network 192.168.2.0  
!
```

College Router

```
!  
router rip  
network 11.0.0.0  
network 192.168.1.0  
!
```

Hostel Router

```
!  
router rip  
network 10.0.0.0  
network 192.168.3.0  
!
```

4.5. Securing Routers

4.5.1. Network security

There are a lot of techniques to protect the network from interior and exterior attackers. Attacking could be physical by sabotaging, ruining, or stealing the devices; or it can be by hacking the system and accessing without authorization. Thus, in order to protect the network from those types of attacks, we need a strong security system. Network security is a set of policies and procedures that monitor the entire network continuously to secure and prevent it from unauthorized access. Consequently, in SCN we used a high level of security in the main devices like routers and switches. We secured all the ports so those devices would not accept any access without authentication.

In the routers' case, we secured VTY lines and console lines by adding passwords to require authentication from the user; as it is clear in the following router configuration. In the switch's case, we also secured all ports; also, we disabled some protocols that show the information of the devices to others such as cisco discovery protocol (CDP).

4.5.2. Router configuration for security

- ☐ We start the security process by putting a password for the line console in order to prevent remote access by others.
- ☐ We put a password for line VTY 0 4 to restrict the telnet and SSH unauthorized access.
- ☐ We used the message-digest algorithm MD5 to encrypt passwords.
- ☐ Finally, we put some restricted features in creating new passwords such as minimum length, and the number of attempts. For example, we verified restriction by entering new user with weak password and the router rejected.

4.5.3. Secure Router Configuration

Main_router

```
enable password admin
```

```
ip ssh version 2
```

```
ip domain-name admin
```

```
!
```

```
username admin password 0 admin
```

```
!
```

```
line con 0
```

```
password cisco
login
!
!
line vty 0 4
password cisco
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
```

```
!
```

College Router

```
!
!
!
!
ip ssh version 2
ip domain-name admin
!
!
!
line con 0
password muj@123
login
!
line aux 0
!
line vty 0 4
password cisco
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
```

```
!
```

Hostel Router

```
!
enable password admin
```



```
!  
username admin password 0 admin  
!  
!  
!  
ip ssh version 2  
ip domain-name admin  
!  
line con 0  
password muj@123  
login  
!  
line aux 0  
!  
line vty 0 4  
password cisco  
login local  
transport input ssh  
line vty 5 15  
login local  
transport input ssh  
!  
!  
!  
!  
!
```

4.6. Whole Router Configurations

4.7. Main_router

```
main_router#sh run  
Building configuration...  
  
Current configuration : 1327 bytes  
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname main_router  
!  
!  
!
```

```
enable password admin
!
!
ip dhcp excluded-address 192.168.2.1 192.168.2.3
!
ip dhcp pool netA
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
ip dhcp pool my_lan
ip dhcp pool serverPool
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.3
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 0 admin
!
!
license udi pid CISCO1941/K9 sn FTX1524S0AO-
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name admin
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
```

```
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/1/0
ip address 10.0.0.1 255.0.0.0
!
interface Serial0/1/1
ip address 11.0.0.1 255.0.0.0
!
interface Vlan1
no ip address
shutdown
!
router rip
network 10.0.0.0
network 11.0.0.0
network 192.168.1.0
network 192.168.2.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line 0/0/0 0/0/7
login
!
line vty 0 4
password cisco
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
end
```

4.8. College Router

```
Router1#sh run
Building configuration...

Current configuration : 1033 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router1
!
!
!
enable password admin
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 0 admin
!
!
license udi pid CISCO1941/K9 sn FTX152425G6-
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name admin
!
!
spanning-tree mode pvst
!
!
```

```
!  
!  
!  
!  
interface GigabitEthernet0/0  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial0/1/0  
ip address 11.0.0.2 255.0.0.0  
clock rate 2000000  
!  
interface Serial0/1/1  
no ip address  
clock rate 2000000  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
network 11.0.0.0  
network 192.168.1.0  
!  
ip classless  
!  
ip flow-export version 9  
!  
!  
!  
!  
!  
!  
!  
line con 0  
password muj@123  
login  
!  
line aux 0  
!  
line vty 0 4  
password cisco  
login local
```

```
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
end
```

Router1#

4.9. Hostel Router

```
Router2#sh run
Building configuration...

Current configuration : 1030 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router2
!
!
!
enable password admin
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 0 admin
!
!
license udi pid CISCO1941/K9 sn FTX1524MMMF-
!
!
!
!
```

```
!  
!  
!  
!  
ip ssh version 2  
ip domain-name admin  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
ip address 192.168.3.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial0/1/0  
ip address 10.0.0.2 255.0.0.0  
clock rate 1200  
!  
interface Serial0/1/1  
no ip address  
clock rate 2000000  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
network 10.0.0.0  
network 192.168.3.0  
!  
ip classless  
!  
ip flow-export version 9  
!  
!  
!  
!  
!
```

```
!  
!  
line con 0  
password muj@123  
login  
!  
line aux 0  
!  
line vty 0 4  
password cisco  
login local  
transport input ssh  
line vty 5 15  
login local  
transport input ssh  
!  
!  
!  
end  
  
Router2#
```

4.10. SSH Protocol

Secure Shell enables a user to access a remote device and manage it remotely. However, with SSH, all data transmitted over a network (including usernames and passwords) is encrypted and secure from eavesdropping.

SSH is a client-server protocol, with an SSH client and an SSH server. The client machine (such as a PC) establishes a connection to an SSH server running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

4.11. Testing:

Connect PCs to APs

4.11.1. Connect to AB1

192.168.1.16

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 18 Mbps

MAC Address 0001.64CB.C3C3

SSID muj_AB1

Authentication

☐ Disabled ☒ WEP ☐ WPA2-PSK

☐ WPA ☐ WPA2

☐ 802.1X Method:

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

MD5

User Name

Password

Encryption Type 40/64-Bits (10 Hex digits)

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.16

Subnet Mask 255.255.255.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address /

Link Local Address: FE80::201:64FF:FECD:C3C3

4.11.2. Connect to AB2

192.168.1.12

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 9 Mbps

MAC Address 0004.9A54.4551

SSID muj_AB2

Authentication

☐ Disabled ☒ WEP ☐ WPA2-PSK

☐ WPA ☐ WPA2

☐ 802.1X Method:

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

MD5

User Name

Password

Encryption Type 40/64-Bits (10 Hex digits)

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.12

Subnet Mask 255.255.255.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address /

Link Local Address: FE80::204:9AFF:FE54:4551

4.11.3. Connect to Library

Dome area

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_dome

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA-PSK ☐ WPA2-PSK

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

Encryption Type 40/64-Bits (10 Hex digits)

Library

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_library

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA-PSK ☐ WPA2-PSK

WEP Key 1234567890

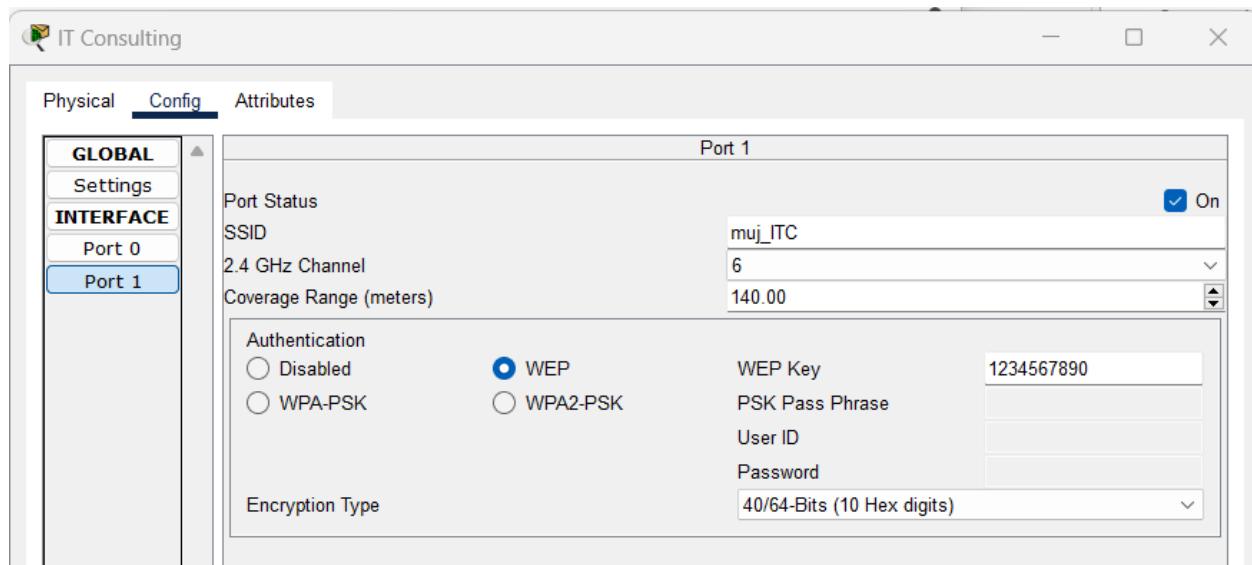
PSK Pass Phrase

User ID

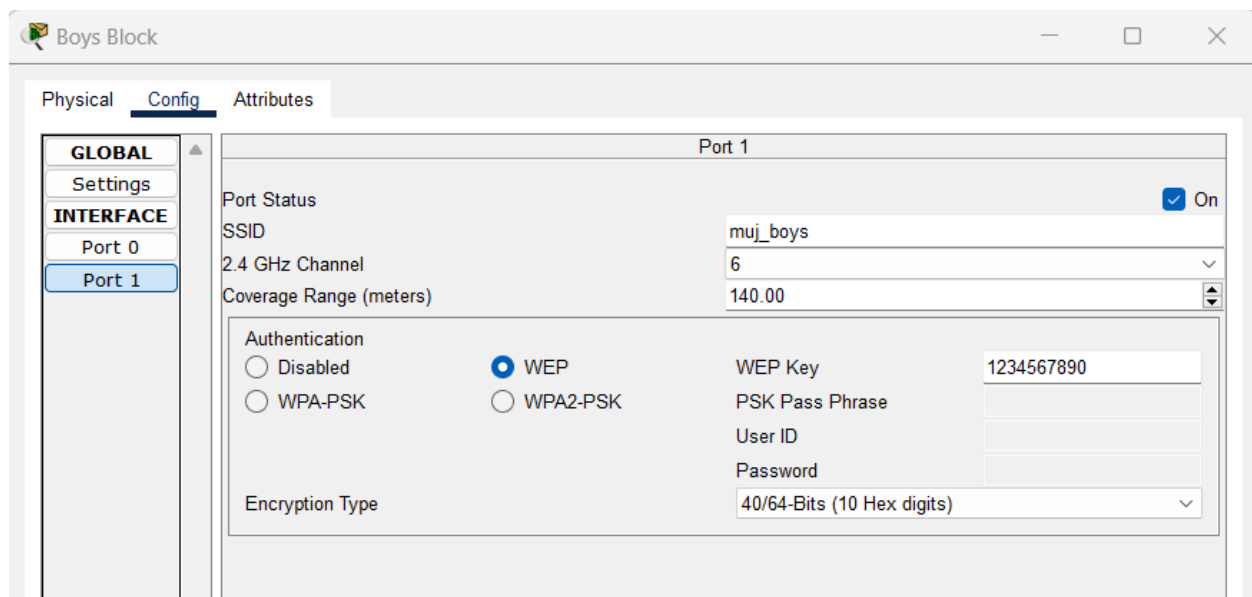
Password

Encryption Type 40/64-Bits (10 Hex digits)

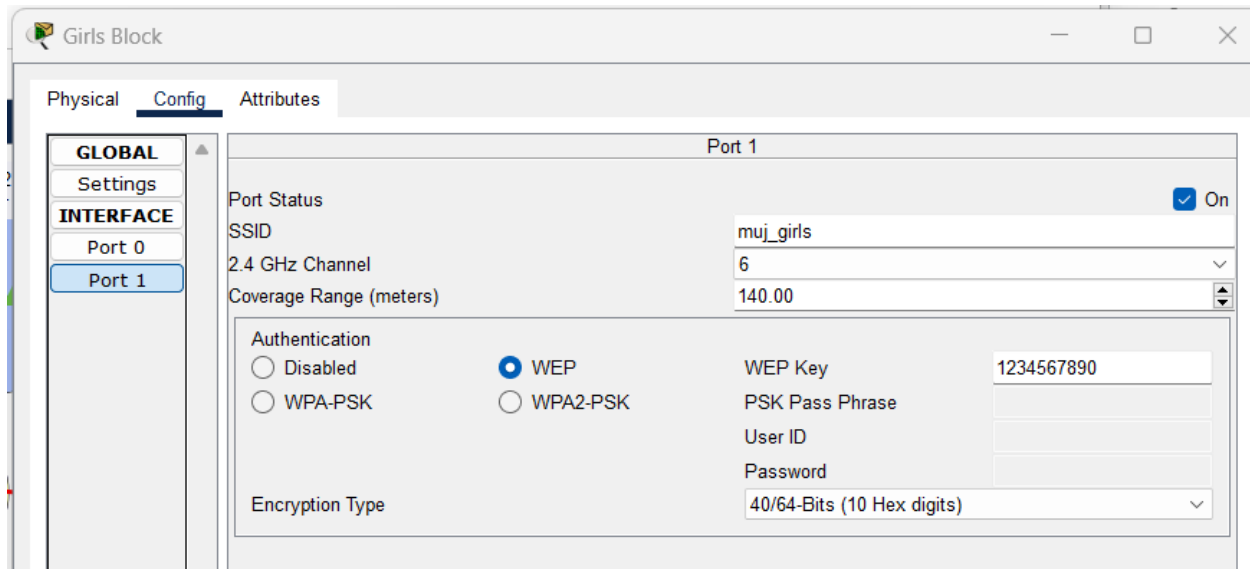
4.11.4. Connect to IT consulting



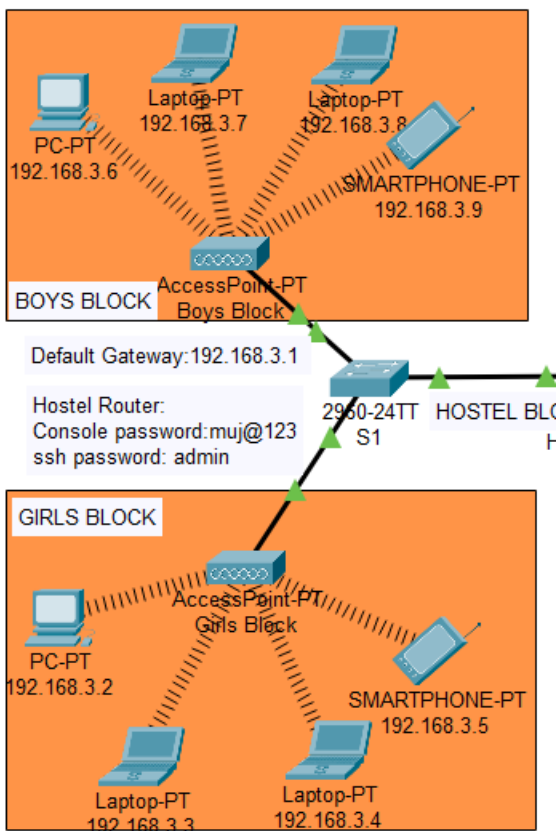
4.11.5. Connect to Boys Block



4.11.6. Connect to Girls Block



4.12. Wireless Test



4.12.1. Wireless access point configurations

Boys Block

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_boys

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA2-PSK

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

Encryption Type 40/64-Bits (10 Hex digits)

Girls Block

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_girls

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA2-PSK

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

Encryption Type 40/64-Bits (10 Hex digits)

AB1

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_AB1

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA2-PSK

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

Encryption Type 40/64-Bits (10 Hex digits)

AB2

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_AB2

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA-PSK ☐ WPA2-PSK

WEP Key 1234567890

PSK Pass Phrase

User ID

Password

Encryption Type 40/64-Bits (10 Hex digits)

Dome area

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID muj_dome

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☒ WEP ☐ WPA-PSK ☐ WPA2-PSK

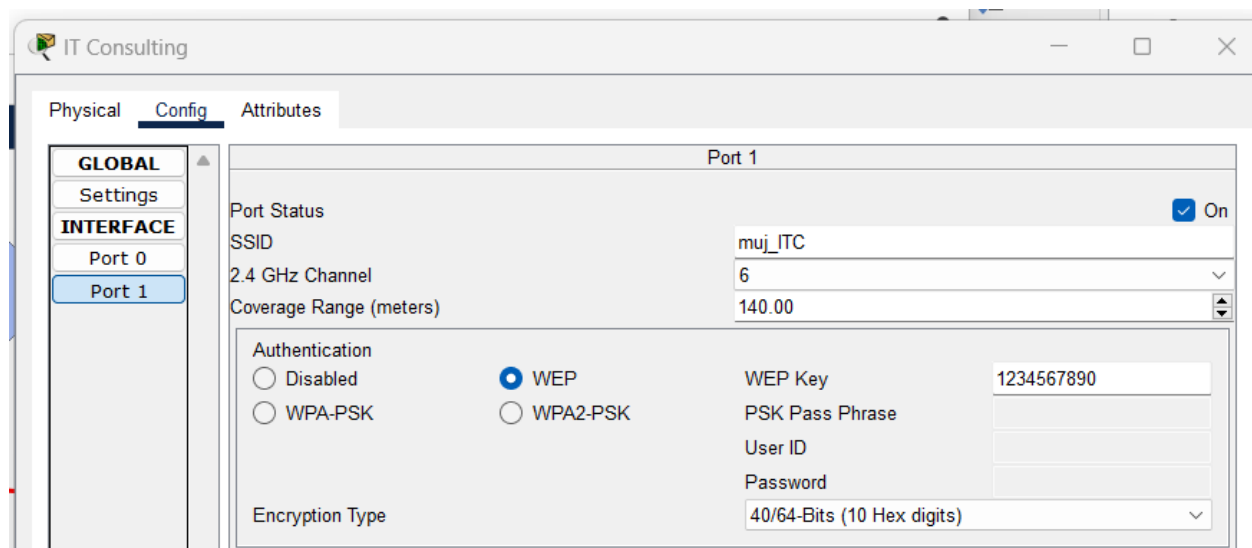
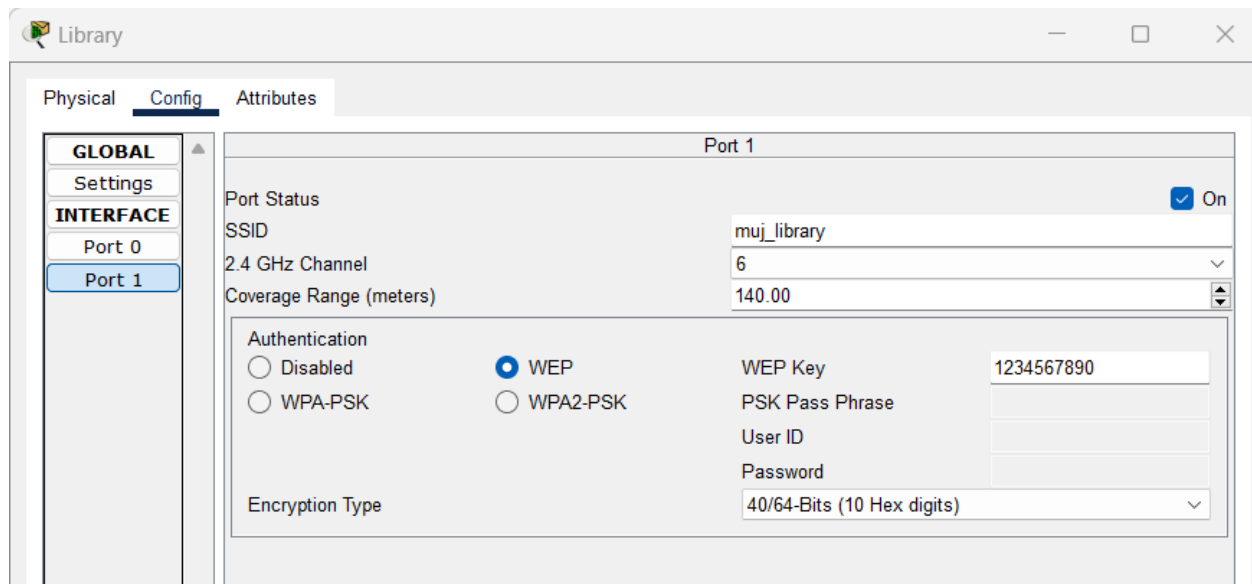
WEP Key 1234567890

PSK Pass Phrase

User ID

Password

Encryption Type 40/64-Bits (10 Hex digits)



4.12.1. Available wireless networks

192.168.1.15

Physical

Config

Desktop

Programming

Attributes

Link Information

Connect

Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
muj_library	1	19%
muj_dome	1	19%
muj_boys	1	19%
muj_ITC	1	19%

Site Information

Wireless Mode

Infrastructure

Network Type

Mixed B/G

Radio Band

Auto

Security

WEP

MAC Address

000A.4167.97C5

Refresh

Connect

2.4GHz



Adapter is Active

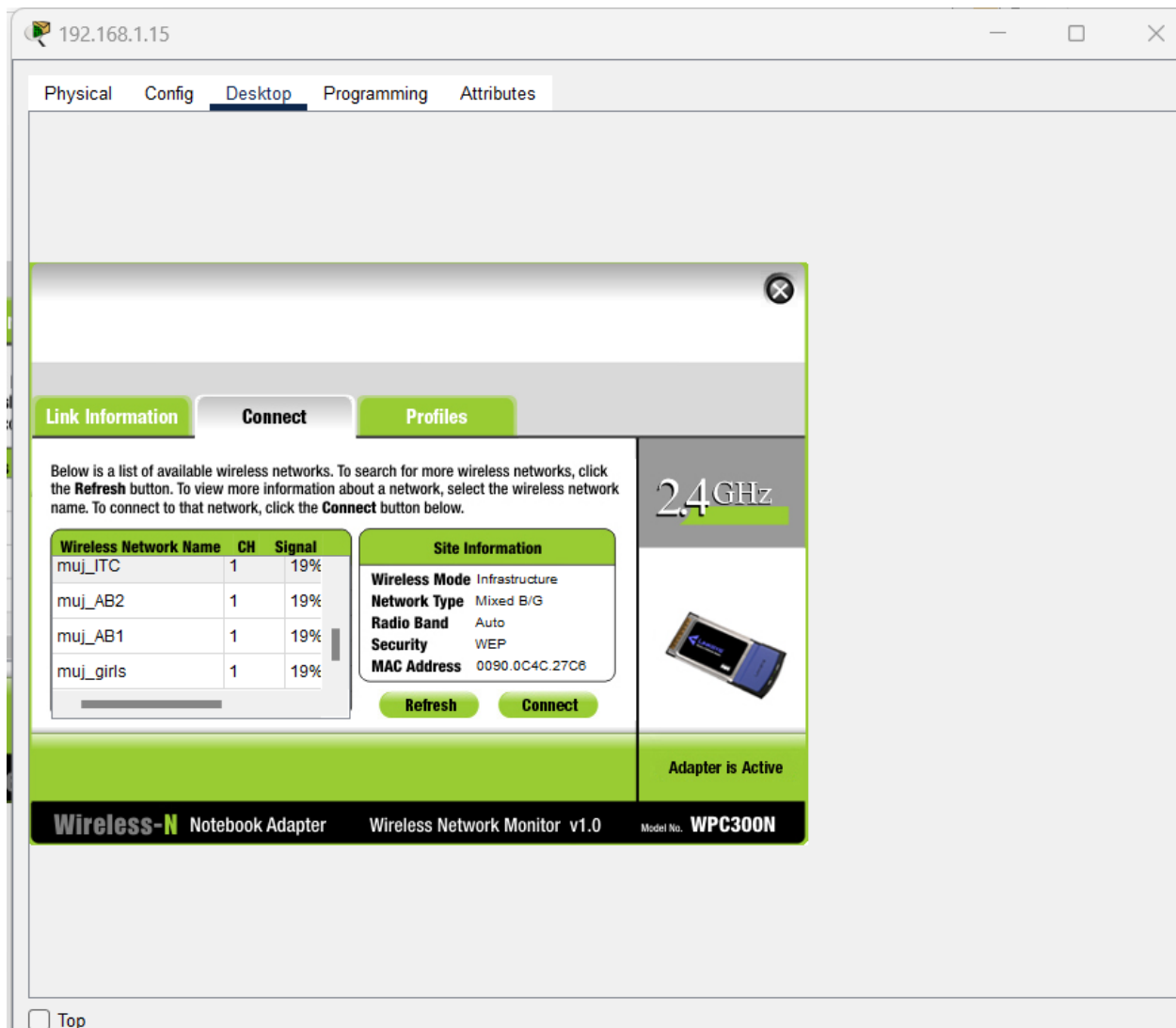
Wireless-N

 Notebook Adapter

Wireless Network Monitor v1.0

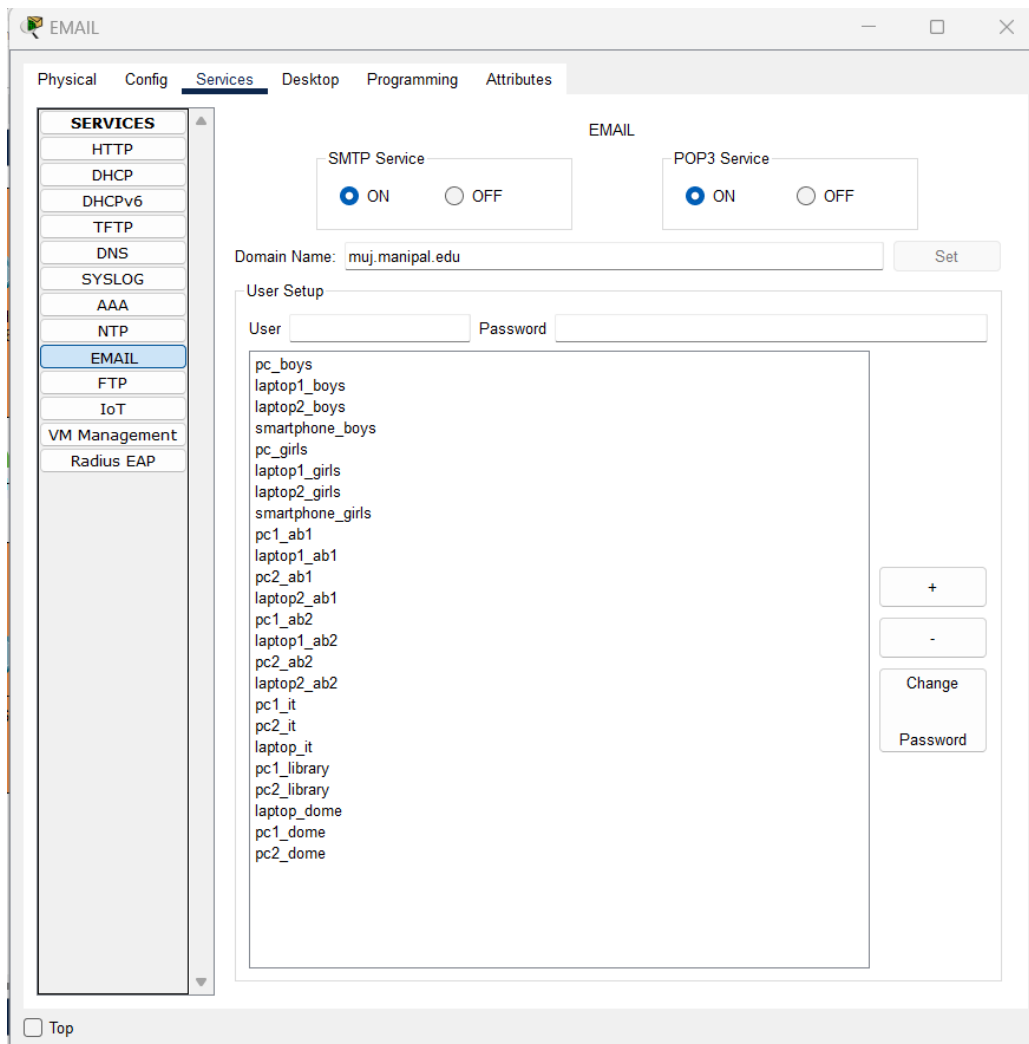
Model No. WPC300N

☐ Top



4.12.2. Server Configuration

4.12.3. Email Server



4.12.4. DHCP configuration

```

!
!
ip dhcp excluded-address 192.168.2.1 192.168.2.3
!
ip dhcp pool netA
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
ip dhcp pool my_lan
ip dhcp pool serverPool
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.3
!
!

```

EMAIL

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

192.168.2.1

DNS Server

192.168.2.3

Start IP Address :

192

168

2

0

Subnet Mask:

255

255

255

0

Maximum Number of Users :

255

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.2.1	192.168.2.3	192.168.2.0	255.255.2...	255	0.0.0.0	0.0.0.0

4.12.5. DNS Server

DNS

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service

On

Off

Resource Records

Name

Type

A Record

Address

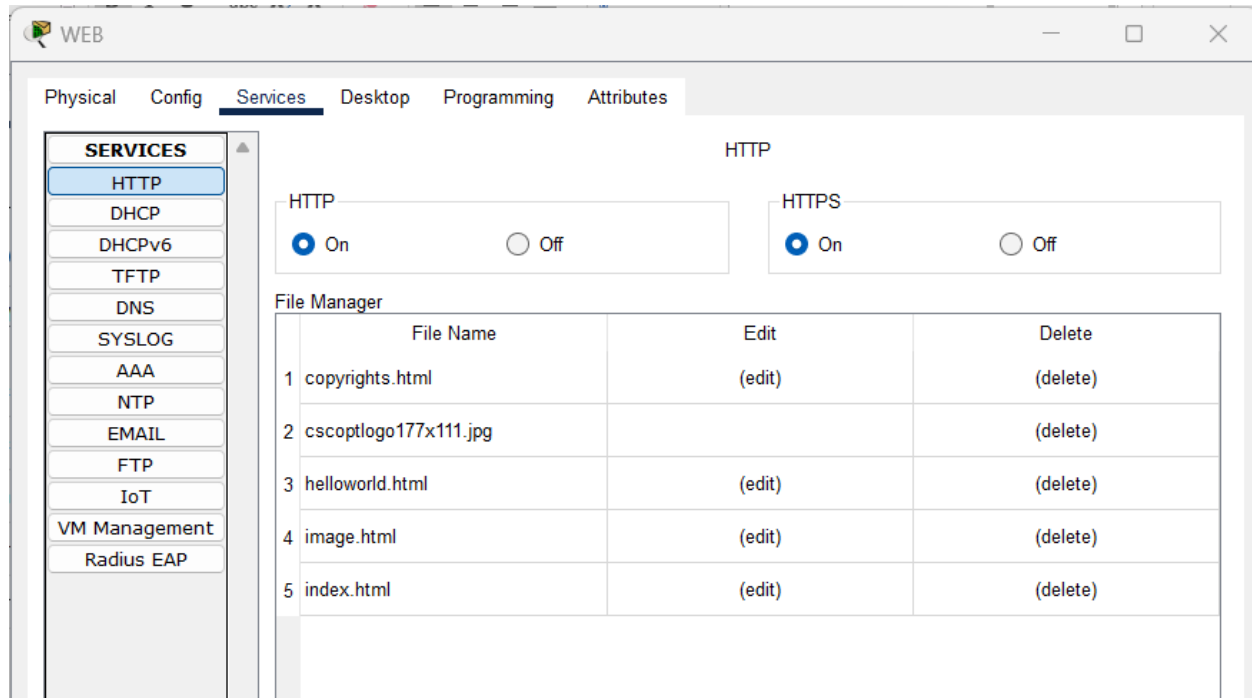
Add

Save

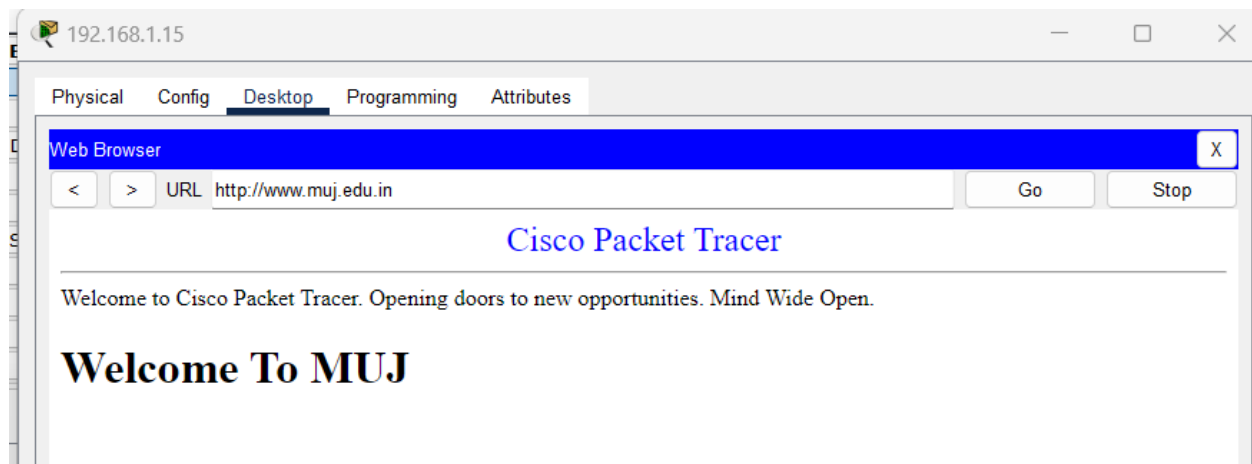
Remove

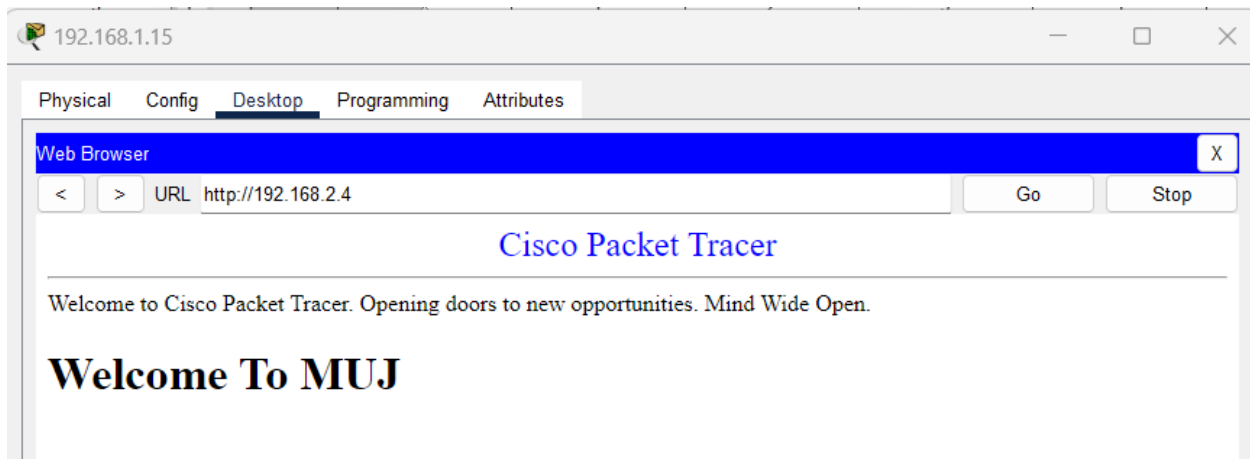
No.	Name	Type	Detail
0	www.muj.edu.in	A Record	192.168.2.4

4.12.6. WEB server



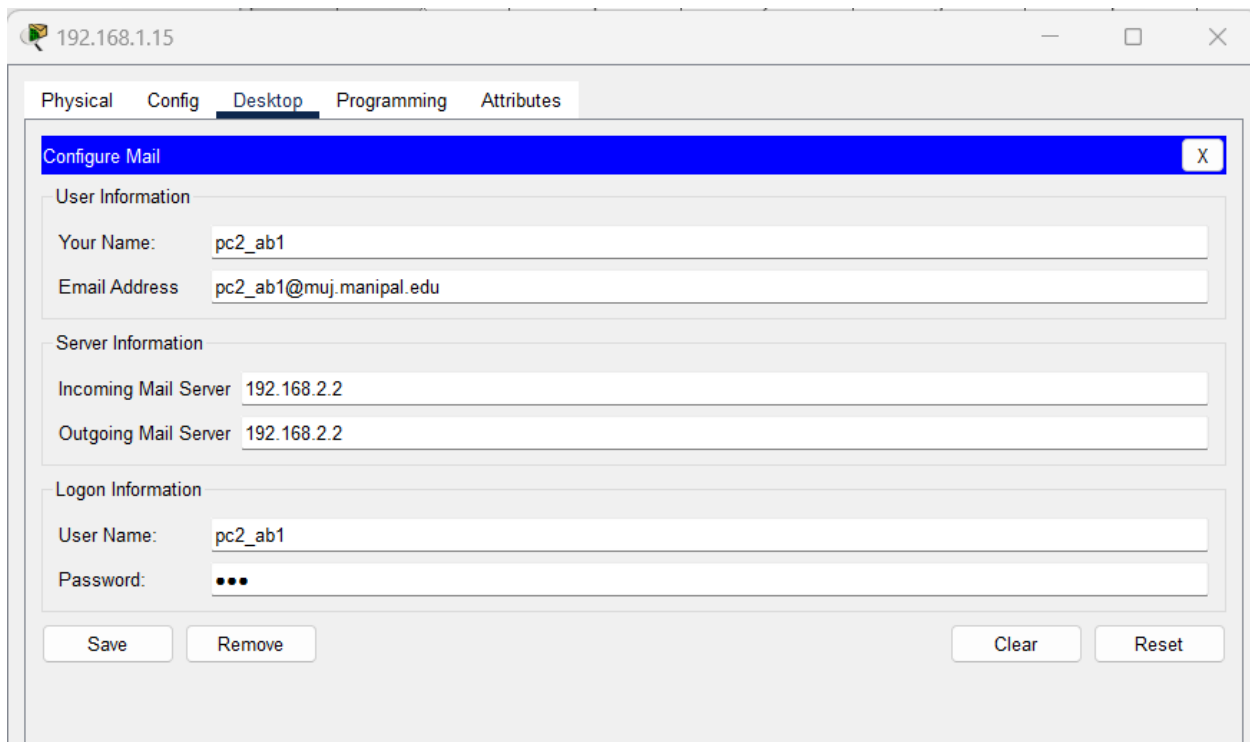
4.12.7. Testing Servers





WEB & DNS successful test

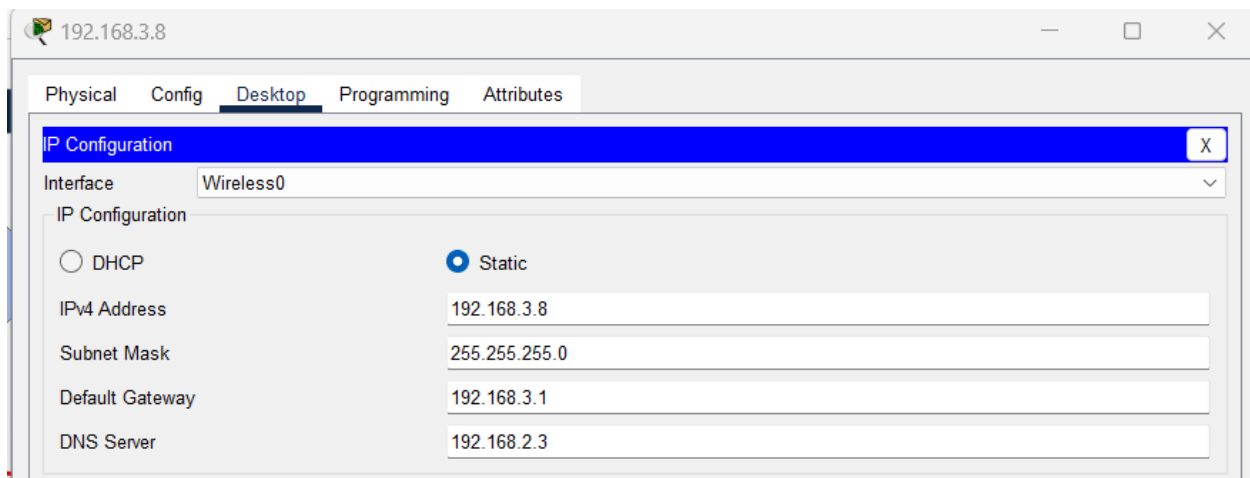
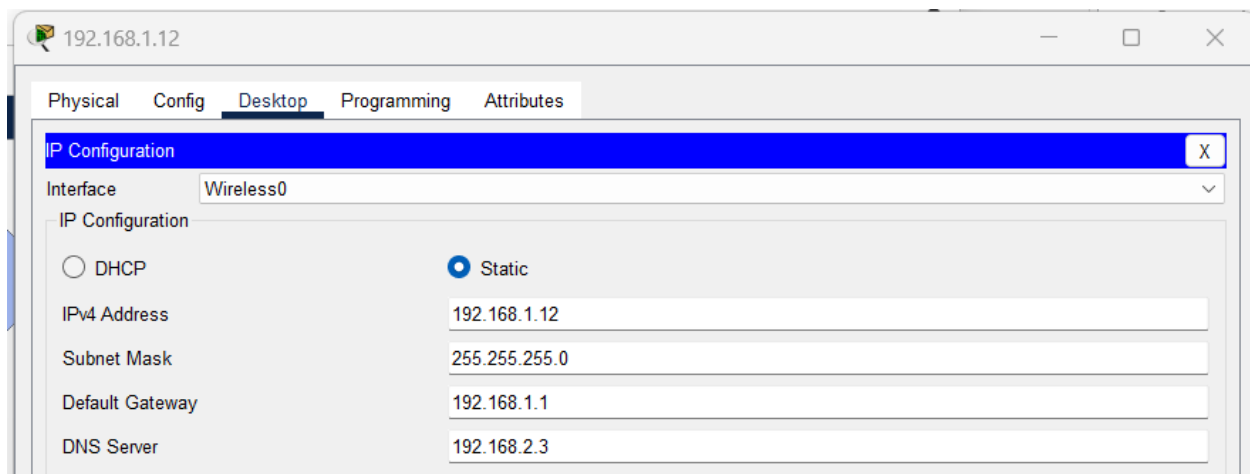
4.12.8. Test Mail server



4.12.9. PING TEST

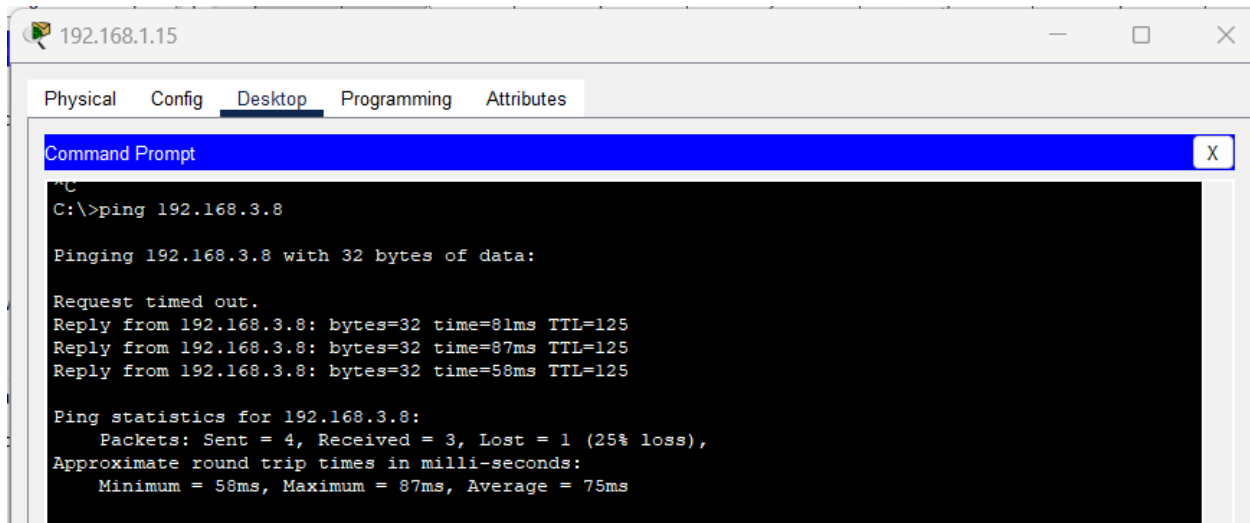
First

4.12.10. Check PC configuration

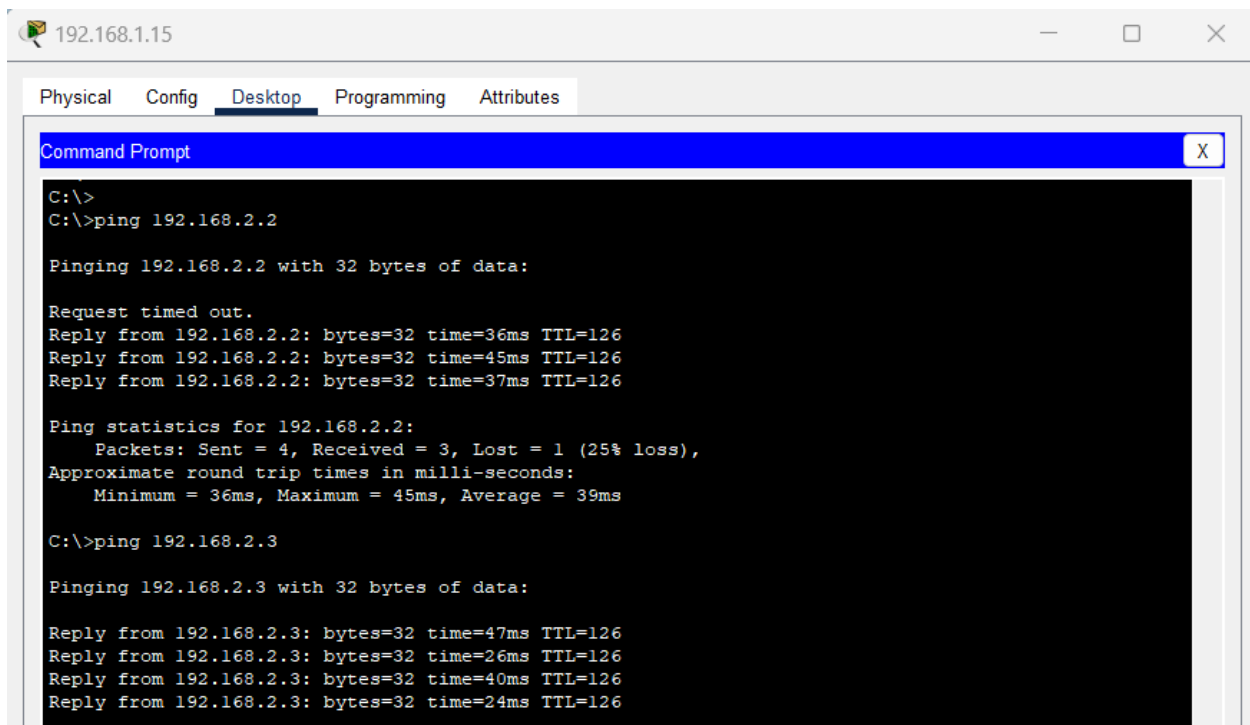


DNS : 192.168.2.3

Ping from 192.168.1.15 to 192.168.3.8



Ping from 192.168.1.15 to 192.168.2.2



```
C:\>
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=36ms TTL=126
Reply from 192.168.2.2: bytes=32 time=45ms TTL=126
Reply from 192.168.2.2: bytes=32 time=37ms TTL=126

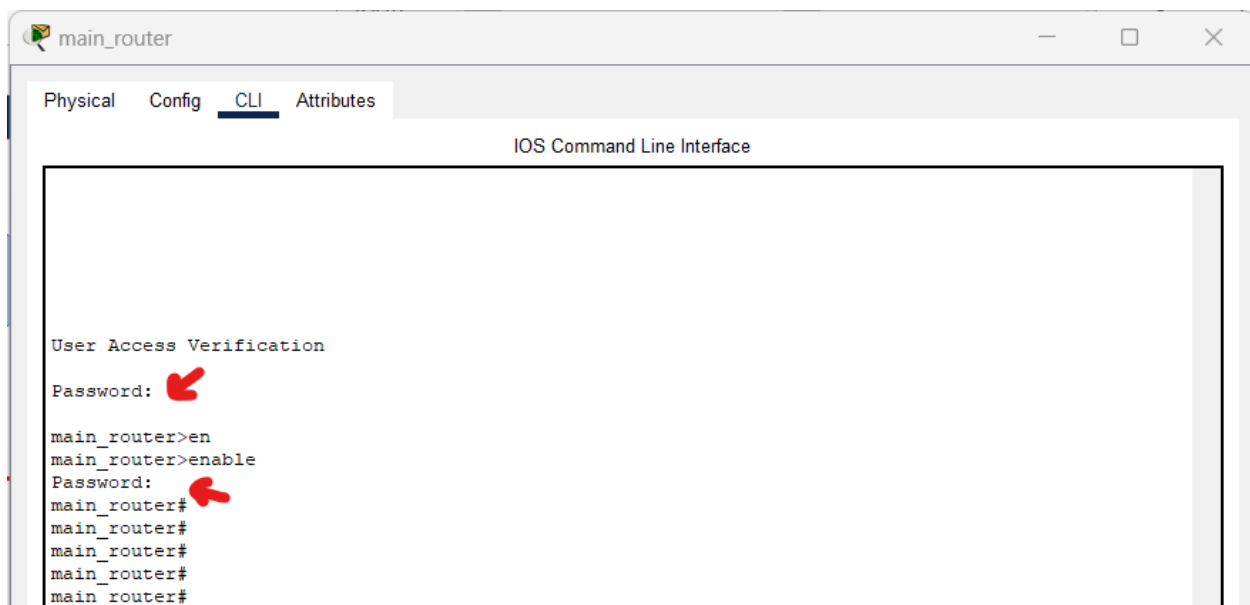
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 45ms, Average = 39ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=47ms TTL=126
Reply from 192.168.2.3: bytes=32 time=26ms TTL=126
Reply from 192.168.2.3: bytes=32 time=40ms TTL=126
Reply from 192.168.2.3: bytes=32 time=24ms TTL=126
```

4.12.11. Check router security configuration



```
main_router
Physical Config CLI Attributes

IOS Command Line Interface

User Access Verification
Password:
main_router>en
main_router>enable
Password:
main_router#
main_router#
main_router#
main_router#
main_router#
```

5. Challenges and Lessons Learned:

- Secret Password
- Vlan (Virtual Lan)
- Inter Vlans
- RIP
- SSH
- Dynamic Host Configuration Protocol DHCP
- Server
- Traceroute
- Inter-VLAN Routing

This relatively short list of configuration tweaks can greatly increase the security of any router.

1. Change the password used to access the router. Anything but the default should be OK, but don't use a word in the dictionary.
2. If your Wi-Fi network(s) is using the default password, change it, even if it appears to be random. A Wi-Fi password should be at least 16 characters long.
3. If you are using a default WiFi network name (SSID) change it. When choosing network names, don't identify yourself.
4. Wi-Fi encryption should be WPA2 (with AES, not TKIP) or WPA3 or both.
5. Turn off WPS .
6. Turn off UPnP
7. Use a password protected Guest Network whenever possible, not just for guests but for IoT devices too.
8. If the router has a web interface, Remote Administration is probably off, but since this is so very dangerous, take the time to verify that it is disabled. If the router is administered with a mobile app and a cloud service.
9. Port forwarding is an opened door (technically an open TCP/IP port). Poke around the router configuration to make sure there is no port forwarding going on. There is a small chance that something on your network needs a port to be forwarded, but every forwarded port is a security risk.
10. Periodically check for new firmware. At some point you will go a year or two, or more, without any updates. That's when it is time for a new router.

6. Conclusions and Recommendations:

To increase the security level in the network's system especially on campuses, we proposed a secure campus network (SCN) scenario designing and simulating using the cisco packet tracer program. This paper presents a topology that contains four-building, with different networks and different types of devices. In each building, we separate the end devices into different VLANs for security purposes. Also, we applied security techniques for the routers that connect the networks and for switches that connect the end devices with each other to prevent outside or unauthorized

accesses. Moreover, this paper shows the real weight of some protocols in connecting and securing the entire campus system.

7. References

- [1] https://en.wikipedia.org/wiki/Packet_Tracer
- [2] <https://www.paessler.com/it-explained/server>
- [3] <https://computernetworking747640215.wordpress.com/2018/07/05/secure-shell-ssh-configuration-on-a-switch-and-router-in-packet-tracer/>
- [4] <http://router.over-blog.com/article-how-to-configure-cisco-router-password-106850439.html>
- [5] <https://www.cognoscape.com/benefits-going-wireless/>