Packet Tracer project

TABLE OF CONTENT

List of figures

List of Tables

1.0 Introduction

A functional and solid network is the backbone of today's business environment. The network should not blink periods, which thereby provides uninterrupted communication, efficient operations, and digital transformation that every organization needs. The networks provide regularity and hassle-free accessibility in communication with colleagues, customers, suppliers, partners, or any other stakeholders both within and outside the company. They facilitate easy and secure data transmission among the employees, the departments, and the external partners, which is indispensable for the maintenance of performance and productivity.

Through the course of this project, we were the main actors with a company that is present in six different locations; the challenge was to create a telecommunication system reliably and securely. The design of the infrastructure makes it possible to use both phone and data communication with the need to add some features that provide both stability and scalability, in this case, to be able to secure more of the system we are talking about. The routing that was carried out was the setting up of OSPF (Open Shortest Path First), which is dynamic, and the RIP (Routing Information Protocol), which we kept static to make sure that it is an easy and efficient way of doing it.

The connectivity was enhanced using WLCs, which linked the device to the access points using modems and were scattered throughout the buildings, and horizontal infrastructure supported by the device ensured that the speed and strength of the signals were achieved at the distant endpoints as well. The access types, different for varied services, were set up through VLANs (Virtual Local Area Networks), with each service getting its separate VLAN (such as IP phones, servers, access points, and users) for better and safe management and control, respectively.

In running our operations, we put in place fundamental electronic devices such as routers, switches, printers, laptops, tablet PCs, smartphones, and desktop PCs, all interlinked to ensure swift management. Through IP address allocation, domain names were resolved, site access was rendered easy, and cloud computing became our way of not only storing data securely but also accomplishing chores from long-distance branches. In addition, the team practically centralized the work of the domain servers and the application servers.

With a centralized setting like this, the network is designed to improve communication and make the operation more efficient in all six branches.

2.0 Main Objective

Most importantly, the project is aimed at creating a secure and effective network infrastructure that will connect six corporate branches through RIP and OSPF routing protocols. In the meantime, the network will be ready to support both wired and wireless communication. But from the beginning, the VLANs have been for the services such as IP phones, servers, and access points for security and performance.

Centralized DNS and web servers are working alongside the cloud, although the access to the cloud is given to the remote branch only to ensure the security of the connection. The project is designed to enable communication, guarantee an easy flow of data and voice, and increase the network reliability and branch coordination.

3.0 Plan

To achieve the project objectives, we have developed a structured implementation plan that covers the following key areas:

1. Network Infrastructure Deployment

Routers & Routing Protocols:

We used 6 routers with customized routing configurations:

RIP between Router 1–3 and 1–2

RIP and OSPF between Router 2–3

OSPF between Router 2–5–6

OSPF between Router 2 and Router 4 through a switch

2. Wired and Wireless Connectivity

Wired LANs are provided in all branches to support stable connections for fixed devices such as PCs, laptops, and IP phones.

Wireless LAN Controllers (WLCs) are deployed with lightweight and traditional Access Points to provide wireless coverage, especially for mobile users.

Wi-Fi coverage is provided selectively in branches with mobile device demands.

3. VLAN Configuration

VLANs are created to logically segment the network:

A dedicated VLAN for every branch

in the Administration branch, there are 3 vlans

VLANs for servers, access points, and end-user devices

This improves security, traffic management, and network isolation.

4. Server & Cloud Integration

DNS and Web Servers are deployed for centralized domain resolution and hosting services.

Cloud access is provided only through Router 4, to support the remote branch and enable secure offsite access to applications.

5. Implementation Steps

Assessment: Analyze each branch's device and connection needs.

Hardware Selection: Choose proper routers, switches, APs, and servers.

Configuration: Set up VLANs, routing protocols (RIP/OSPF), and server roles.

Deployment: Install both wired and wireless networks branch wide.

Testing & Optimization: Conduct full connectivity and performance tests.

4.0 Selected topology

We chose our old topology from Network 315, and it contains 2 routers and 2 multilayer switch 2 IP phone:

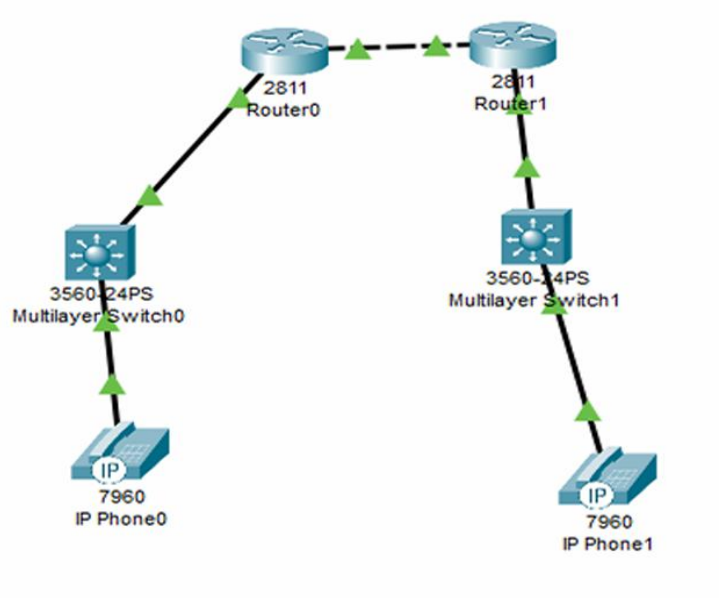


Figure (1): Selected topology

5.0 The result topology

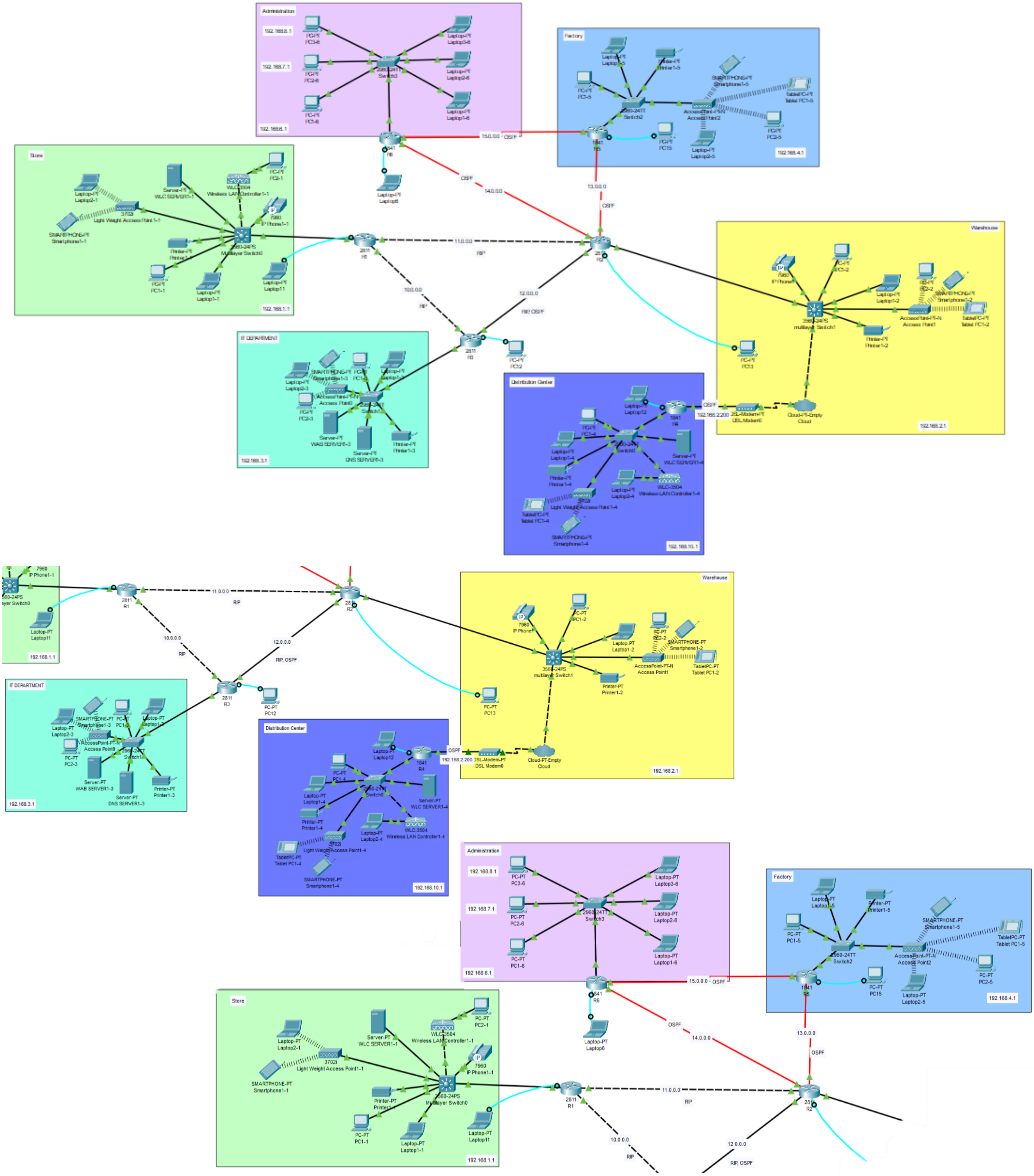


Figure (2): result topology

6.0 Network and End Devices

END DEVICES	NETWORK DEVICES
15 PCs	6 Routers (3R 1841, 3R 2811)
15 Laptops	6 Switches (2 Multilayers “3560-24ps”, 4S 2960-24TT)
5 Smartphones	2 Wireless LAN Controllers (WLC-3504)
3 Tablets	2 Lightweight Access Points (3702i)
2 IP Phones	3 Access Points (Access Point PT-N)
5 Printers	DCL Modem (DSL-Modem-PT)
4 Servers	Cloud (Cloud-PT-Empty)

Table (1): Network and End Devices

7.0 Tools

We used Cisco Packet Tracer to create a network that is efficient and connected.

The methods that we use to finish the project are

1. Dynamic Host Configuration Protocol (DHCP):

It was DHCP that we utilized to allocate IP addresses to devices in the network automatically. Specifically, this simplified the setup of VoIP and end-user devices and the flexibility to distribute the IP addresses over the branches.

2. OSPF and RIP:

To make different branches communicate. The choice of using OSPF and RIP was wise; the RIP protocol was used between Router 1, Router 2, and Router 3, and the OSPF was for the rest of the routers, hence the one that guaranteed high efficiency and low network latency.

3. Interface Configurations:

Router and switch interfaces were arranged effectively to allow VLANs (virtual local area networks) to operate.

4. VLAN Setup:

We carried out the segmentation of data traffic, and we created VLANs that separated the data carried between different branches.

5. Access Point Configuration:

We install access points (APs) for Branches 2, 3, and 5 of the organization so that devices can have Wi-Fi connectivity. Additionally, Router 4 and Router 1 had lightweight access points so devices could have connections to the network.

6. Server Configuration:

We set up the DNS server to store the website's IP address of the company. The WLC servers (wireless LAN controllers) have been installed to take care of the wireless access points in the organization, and a web server to log in to the company website. The Web server was built to have web pages and program by html.

7. Cloud Integration:

A cloud service was implemented, connected to Router 4, to support activities for the distant branch. This provided secure access to shared resources, ensuring the branch was able to interact with the rest of the network.

8.0 Network design

1. Addressing

R1 (Store)

	Interface	Ip address	Subnet mask	Default gateway
R1	Fa0/0.100	192.168.1.1	255.255.255.0	
	Fa0/1	10.0.0.1	255.0.0.0	
	Fa1/0	11.0.0.1	255.0.0.0	
PC1-1	F0	192.168.1.10	255.255.255.0	192.168.1.1
PRINTER1-1	F0	192.168.1.11	255.255.255.0	192.168.1.1
LAPTOP1-1	F0	192.168.1.12	255.255.255.0	192.168.1.1
SMARTPHONE1-1	F0	(DHCP)	255.255.255.0	192.168.1.1
LAPTOP2-1	F0	(DHCP)	255.255.255.0	192.168.1.1
IP PHONE1-1	F0	.....	255.255.255.0	192.168.1.1
WLC SERVER1-1	F0	192.168.1.7	255.255.255.0	192.168.1.1
WIRELESS LAN CONTROLLER1-1	F0	192.168.1.5	255.255.255.0	192.168.1.1
PC2-1	F0	192.168.1.6	255.255.255.0	192.168.1.1
LIGTH WEIGTH ACCESS POINT1-1	F0	DHCP	255.255.255.0	192.168.1.1

Table (2): R1 Addressing

Lightweight Access Point1-1 was configured through the Wireless LAN Controller (WLC)1-1, accessed with:

- **Username:** Admin
- **Password:** Admin@1

Two SSIDs were created:

- **SSID:** GUEST | **Authentication:** WPA2-PSK | **Password:** 12345678
- **SSID:** Employee | **Authentication:** WPA2-PSK | **Password:** 12345678

The access point provides secure wireless connectivity for both guests and employees, with centralized management and security policies handled by the WLC.

R2 (Warehouse)

	Interface	Ip address	Subnet mask	Default gateway
R2	F0/0.400	192.168.2.1	255.255.255.0	
	Fa0/1	12.0.0.2	255.0.0.0	
	Fa1/0	11.0.0.2	255.0.0.0	
	Se0/0/0	13.0.0.1	255.0.0.0	
	Se0/0/1	14.0.0.1	255.0.0.0	
ACCESSPOINT1-2	Port0	---	----	192.168.2.1
PRINTER1-2	F0	192.168.2.11	255.255.255.0	192.168.2.1
PC1-2	F0	192.168.2.10	255.255.255.0	192.168.2.1
LAPTOP1-2	F0	192.168.2.12	255.255.255.0	192.168.2.1
IP PHONE1-2	F0	….....	255.255.255.0	192.168.2.1
PC2-2	F0	192.168.2.102	255.255.255.0	192.168.2.1
TABLET PC1-2	F0	192.168.2.100	255.255.255.0	192.168.2.1
SMARTPHONE1-2	F0	192.168.2.101	255.255.255.0	192.168.2.1
R4	F0/0	192.168.2.200	255.255.255.0	192.168.2.1

Table (3): R2 Addressing

NETWORK NAME “SSID”: ware

PASSWORD: 12345678

AUTHENTICATION: WAP2-PSK

Access Point 1-2, configured as part of the network infrastructure, is connected through Router 2 and identified with the network name (SSID) “ware”. The access point employs WPA2-PSK authentication for securing wireless communication, with a password set as 12345678. This enhanced security protocol ensures robust encryption, protecting the network from unauthorized access. The access point facilitates wireless connectivity for various devices within its coverage area, and we assign IP addresses and provide a default gateway to enable seamless communication within the subnet and beyond.

R3 (IT DEPARTMENT)

	Interface	Ip address	Subnet mask	Default gateway
R3	F0/0	10.0.0.2	255.0.0.0	
	F0/1	12.0.0.1	255.0.0.0	
	Eth1/0.200	192.168.3.1	255.255.255.0	
ACCESSPOINT1-3	Port0	---	----	192.168.3.1
LAPTOP1-3	F0	192.168.3.11	255.255.255.0	192.168.3.1
PC1-3	F0	192.168.3.10	255.255.255.0	192.168.3.1
SMARTPHONE1-3	F0	192.168.3.101	255.255.255.0	192.168.3.1
LAPTOP2-3	F0	192.168.3.102	255.255.255.0	192.168.3.1
PC2-3	F0	192.168.3.100	255.255.255.0	192.168.3.1
WEB SERVER1-3	F0	192.168.3.5	255.255.255.0	192.168.3.1
DNS SERVER1-3	F0	192.168.3.6	255.255.255.0	192.168.3.1
PRINTER1-3	F0	192.168.3.11	255.255.255.0	192.168.3.1

Table (4): R3 Addressing

NETWORK NAME “SSID”: ITd

PASSWORD: 12341234

AUTHENTICATION: WAP2-PSK

Access Point 1-3, configured as part of the network infrastructure, is connected through Router 3 and identified with the network name (SSID) “ITd”. The access point employs WPA2-PSK authentication for securing wireless communication, with a password set as 12341234. This enhanced security protocol ensures robust encryption, protecting the network from unauthorized access. The access point facilitates wireless connectivity for various devices within its coverage area, and we assign IP addresses and provide a default gateway to enable seamless communication within the subnet and beyond.

R4 (Distribution Center)

	Interface	Ip address	Subnet mask	Default gateway
R4	Fa0/1.500	192.168.10.1	255.255.255.0	192.168.10.1
	Fa0/0	192.168.2.200	255.255.255.0	192.168.2.1
PRINTER1-4	F0	192.168.10.10	255.255.255.0	192.168.10.1
LAPTOP1-4	F0	192.168.10.12	255.255.255.0	192.168.10.1
PC1-4	F0	192.168.10.11	255.255.255.0	192.168.10.1
SMARTPHONE1-4	F0	DHCP	255.255.255.0	192.168.10.1
TABLET PC1-4	F0	DHCP	255.255.255.0	192.168.10.1
LIGTH WEIGTH ACCESS POINT1-4	F0	DHCP	255.255.255.0	192.168.10.1
WIRELESS LAN CONTROLLER1-4	F0	192.168.4.5	255.255.255.0	192.168.10.1
WLC SERVER1-4	F0	192.168.4.6	255.255.255.0	192.168.10.1
LAPTOP2-4	F0	192.168.4.7	255.255.255.0	192.168.10.1

Table (5): R4 Addressing

Lightweight Access Point1-4 was configured through the Wireless LAN Controller (WLC)1-4, accessed with:

- **Username:** Admin
- **Password:** Admin@1

One SSID was created:

- **SSID:** employees | **Authentication:** WPA2-PSK | **Password:** 12345678

The access point provides secure wireless connectivity for both employees, with centralized management and security policies handled by the WLC.

R5 (Factory)

	Interface	Ip address	Subnet mask	Default gateway
R5	Fa0/0.300	192.168.4.1	255.255.255.0	
	Se0/0/0	13.0.0.2	255.0.0.0	
	Se0/0/1	15.0.0.2	255.0.0.0	
ACCESSPOINT1-5	Port0	---	----	192.168.4.1
PC1-5	F0	192.168.4.10	255.255.255.0	192.168.4.1
LAPTOP1-5	F0	192.168.4.11	255.255.255.0	192.168.4.1
PRINTER1-5	F0	192.168.4.12	255.255.255.0	192.168.4.1
SMARTPHONE1-5	F0	192.168.4.100	255.255.255.0	192.168.4.1
TABLET PC1-5	F0	192.168.4.101	255.255.255.0	192.168.4.1
PC2-5	F0	192.168.4.102	255.255.255.0	192.168.4.1
LAPTOP2-5	F0	192.168.4.103	255.255.255.0	192.168.4.1

Table (6): R5 Addressing

NETWORK NAME “SSID”: fac

PASSWORD: 12345123

AUTHENTICATION: WAP2-PSK

Access Point 1-5, configured as part of the network infrastructure, is connected through Router 5 and identified with the network name (SSID) “fac”. The access point employs WPA2-PSK authentication for securing wireless communication, with a password set as 12345123. This enhanced security protocol ensures robust encryption, protecting the network from unauthorized access. The access point facilitates wireless connectivity for various devices within its coverage area, and we assign IP addresses and provide a default gateway to enable seamless communication within the subnet and beyond.

R6 (Administration)

	Interface	Ip address	Subnet mask	Default gateway
R6	Se0/0/0	15.0.0.2	255.0.0.0	
	Se0/0/1	14.0.0.2	255.0.0.0	
	Fa0/0.10	192.168.6.1	255.255.255.0	
	Fa0/0.20	192.168.7.1	255.255.255.0	
	Fa0/0.30	192.168.8.1	255.255.255.0	
PC3-6	F0	192.168.8.6	255.255.255.0	192.168.8.1
LAPTOP3-6	F0	192.168.8.7	255.255.255.0	192.168.8.1
PC2-6	F0	192.168.7.6	255.255.255.0	192.168.7.1
LAPTOP2-6	F0	192.168.7.7	255.255.255.0	192.168.7.1
PC1-6	F0	192.168.6.6	255.255.255.0	192.168.6.1
LAPTOP1-6	F0	192.168.6.7	255.255.255.0	192.168.6.1

Table (7): R6 Addressing

9.0 Network implementation

1. Configure IP for routers

In our topology, we utilized the IP addresses for the routers, between them and their interface for switches:

R1

```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip add 10.0.0.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#interface FastEthernet1/0
R1(config-if)#ip add 11.0.0.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#interface FastEthernet0/0.100
R1(config-subif)#en
R1(config-subif)#encapsulation q
R1(config-subif)#encapsulation d
R1(config-subif)#encapsulation dot1Q 100
R1(config-subif)#ip add 192.168.1.1 255.255.255.0
R1(config-subif)#no sh
```

Figure (3): Configure IP R1

FastEthernet0/0.100 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
FastEthernet1/0 is connected to router 2, and we connect it with a copper cross over cable.
FastEthernet0/1 is connected to router 3, and we connect it with a copper cross over cable.

R2

```
R2(config)#int fa1/0
R2(config-if)#ip add 11.0.0.2 255.0.0.0
R2(config-if)#no sh
R2(config-if)#int fa0/0.400
R2(config-subif)#encapsulation dot1Q 400
R2(config-subif)#ip add 192.168.2.1 255.255.255.0
R2(config-subif)#no sh
R2(config-subif)#int fa1/0
R2(config-if)#int fa0/1
R2(config-if)#ip add 12.0.0.2 255.0.0.0
R2(config-if)#no sh
R2(config-if)#int se0/0/0
R2(config-if)#ip add 13.0.0.1 255.0.0.0
R2(config-if)#no sh
R2(config-if)#int se0/0/1
R2(config-if)#ip add 14.0.0.1 255.0.0.0
R2(config-if)#no sh
```

Figure (4): Configure IP R2

FastEthernet0/0.400 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
FastEthernet1/0 is connected to router 1, and we connect it with a copper cross over cable.
FastEthernet0/1 is connected to router 3, and we connect it with a copper straight-through cable “UTP”.
Serial 0/0/0 is connected to router 5, and we connect it with a Serial DCE cable.
Serial 0/0/1 is connected to router 6, and we connect it with a Serial DCE cable.

R3

```
R3(config)#int f0/0
R3(config-if)#ip add 10.0.0.2 255.0.0.0
R3(config-if)#no sh
R3(config-if)#int f0/1
R3(config-if)#ip add 12.0.0.1 255.0.0.0
R3(config-if)#no sh
R3(config-if)#int eth1/0.200
R3(config-subif)#encapsulation dot1Q 200
R3(config-subif)#ip add 192.168.3.1 255.255.255.0
R3(config-subif)#no sh
```

Figure (5): Configure IP R3

Ethernet1/0 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.

FastEthernet0/1 is connected to router 2, and we connect it with a copper straight-through cable “UTP”.

FastEthernet0/0 is connected to router 1, and we connect it with a copper cross over cable.

R4

```
R4(config)#int f0/1.500
R4(config-subif)#encapsulation dot1Q 500
R4(config-subif)#ip add 192.168.10.1 255.255.255.0
R4(config-subif)#no sh
R4(config-subif)#int fa0/0
R4(config-if)#ip add 192.168.2.200 255.255.255.0
R4(config-if)#no sh
```

Figure (6): Configure IP R4

FastEthernet0/1.500 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
FastEthernet0/0 is connected to MSwitch 1, and we connect it with a copper straight-through cable “UTP” to DSL-Modem then to the cloud then to the Multilayer switch 1 that switch is connected to router 2.

R5

```
R5(config)#int f0/0.300
R5(config-subif)#encapsulation dot1Q 300
R5(config-subif)#ip add 192.168.4.1 255.255.255.0
R5(config-subif)#no sh
R5(config-subif)#int se0/0/0
R5(config-if)#ip add 13.0.0.2 255.0.0.0
R5(config-if)#no sh
R5(config-if)#int se0/0/1
R5(config-if)#ip add 15.0.0.2 255.0.0.0
R5(config-if)#no sh
```

Figure (7): Configure IP R5

FastEthernet0/0.300 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
Serial 0/0/0 is connected to router 2, and we connect it with a Serial DCE cable.
Serial 0/0/1 is connected to router 6, and we connect it with a Serial DCE cable.

R6

```
R6(config)#int fa0/0.10
R6(config-subif)#encapsulation dot1Q 10
R6(config-subif)#ip add 192.168.6.1 255.255.255.0
R6(config-subif)#no sh
R6(config-subif)#int fa0/0.20
R6(config-subif)#encapsulation dot1Q 20
R6(config-subif)#ip add 192.168.7.1 255.255.255.0
R6(config-subif)#no sh
R6(config-subif)#int fa0/0.30
R6(config-subif)#encapsulation dot1Q 30
R6(config-subif)#ip add 192.168.8.1 255.255.255.0
R6(config-subif)#no sh
R6(config-subif)#int se0/0/0
R6(config-if)#ip add 15.0.0.2 255.0.0.0
R6(config-if)#no sh
R6(config-if)#int se0/0/1
R6(config-if)#ip add 14.0.0.2 255.0.0.0
R6(config-if)#no sh
```

Figure (8): Configure IP R6

FastEthernet0/0.10 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
FastEthernet0/0.20 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
FastEthernet0/0.30 is connected to the switch, and we connect it with a copper straight-through cable “UTP”.
Serial 0/0/0 is connected to router 5, and we connect it with a Serial DCE cable.
Serial 0/0/1 is connected to router 2, and we connect it with a Serial DCE cable.

2. Ospf

In our topology, we utilized Ospf protocol in some routers to make them communicate with each other and their devices, the routers are:

- R2 with R4
- R2 with R3
- R2 with R5
- R2 with R6
- R5 with R6

The way implementation:

R2

```
R2(config)#router ospf 1
R2(config-router)#net 192.168.2.0 0.0.0.255 area 0
R2(config-router)#net 12.0.0.0 0.255.255.255 area 0
R2(config-router)#net 13.0.0.0 0.255.255.255 area 0
R2(config-router)#net 14.0.0.0 0.255.255.255 area 0
```

Figure (9): OSPF implementation R2

In router 2, we configure router 3,4,5,6 by the network between them and R2 switch network.

R3

```
R3(config)#router ospf 1
R3(config-router)#net 192.168.3.0 0.0.0.255 area 0
R3(config-router)#net 12.0.0.0 0.255.255.255 area 0
```

Figure (10): OSPF implementation R3

In router 3, we configure router 2 by the network between them and R3 switch network.

R4

```
R4(config)#router ospf 1
R4(config-router)#net 192.168.10.0 0.0.0.255 area 0
R4(config-router)#net 192.168.2.0 0.0.0.255 area 0
```

Figure (11): OSPF implementation R4

In router 4, we configure router 2 by the network between them and R4 switch network.

R5

```
R5(config)#router ospf 1
R5(config-router)#net 192.168.4.0 0.0.0.255 area 0
R5(config-router)#net 13.0.0.0 0.255.255.255 area 0
R5(config-router)#net 15.0.0.0 0.255.255.255 area 0
```

Figure (12): OSPF implementation R5

In router 5, we configure router 2,6 by the network between them and R5 switch network.

R6

```
R6(config)#router ospf 1
R6(config-router)#net 192.168.6.0 0.0.0.255 area 0
R6(config-router)#net 192.168.7.0 0.0.0.255 area 0
R6(config-router)#net 192.168.8.0 0.0.0.255 area 0
R6(config-router)#net 15.0.0.0 0.0.0.255 area 0
R6(config-router)#net 14.0.0.0 0.0.0.255 area 0
```

Figure (13): OSPF implementation R6

In router 6, we configure router 2,5 by the network between them and R6 switch network.

3. RIP

In our topology, we utilized Ospf protocol in some routers to make them communicate with each other and their devices, the routers are:

- R1 with R2
- R1 with R3
- R2 with R3

The way implementation:

R1

```
R1(config)#router rip
R1(config-router)#ver 2
R1(config-router)#network 11.0.0.0
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.1.0
```

Figure (14): RIP implementation R1

In router 1, we configure router 2,3 by the network between them and R1 switch network.

R2

```
R2(config)#router rip
R2(config-router)#ver 2
R2(config-router)#network 11.0.0.0
R2(config-router)#network 12.0.0.0
R2(config-router)#network 192.168.2.0
```

Figure (15): RIP implementation R2

In router 2, we configure router 1,3 by the network between them and R2 switch network.

R3

```
R3(config)#router rip
R3(config-router)#ver 2
R3(config-router)#network 10.0.0.0
R3(config-router)#network 12.0.0.0
R3(config-router)#network 192.168.3.0
```

Figure (16): RIP implementation R3

In router 3, we configure router 2,3 by the network between them and R3 switch network.

4. Merge between Ospf and RIP

Finaly, we need to merge the protocols to have connections between devises from other routers so there are 2 commands used for that, and we will use them on router 2 because router 2 is between all routers and he have 2 protocols, the RIP and Ospf so the 2 commands are:

Rip command

redistribute ospf 1 metric 1

Ospf command

redistribute rip subnets

and this is how we implement them:

R2

```
R2(config)#router rip
R2(config-router)#ver 2
R2(config-router)# redistribute ospf 1 metric 1
R2(config-router)#ex
R2(config)#router ospf 1
R2(config-router)#redistribute rip subnets
R2(config-router)#ex
```

Figure (17): Merge between Ospf and RIP

5. IP PHONES

In our topology, we utilized IP phone devices to facilitate telephone calls exclusively between the main office and a unit in the first office. The following sections outline the steps taken to configure the IP phones; we use DHCP to configure IP addresses faster for phones:

We implemented IP phones in two branches 1 (Store) and 2 (Warehouse)

R1

```
Router(config)#
Router(config)#ip dhcp pool voice
Router(dhcp-config)#net 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#op
Router(dhcp-config)#option 150 ip 192.168.1.1
Router(dhcp-config)#
Router(dhcp-config)#ex
Router(config)#ip dhcp ex
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#tele
Router(config)#telephony-service
Router(config-telephony)#max-dn 5
Router(config-telephony)#max-ep
Router(config-telephony)#max-ephones 5
Router(config-telephony)#ip so
Router(config-telephony)#ip source-address 192.168.1.1 port 2000
Router(config-telephony)#auto assign 1 to 2
Router(config-telephony)#ex
Router(config)#eho
Router(config)#eph
Router(config)#ephone-1
                   ^
% Invalid input detected at '^' marker.

Router(config)#ephone-dn 1
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#num 111
Router(config-ephone-dn)#ex
Router(config)#
%IPPHONE-6-REGISTER: ephone-1 IP:192.168.1.2 Socket:2 DeviceType:Phone has registered.
```

IP Phone 1 configure in router 1 with DHCP

```
Switch(config)#int f0/1
Switch(config-if)#sw
Switch(config-if)#switchport voice vlan 1
```

Vlan voice for IP Phone

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session target ipv4:11.0.0.2
Router(config-dial-peer)#destination-pattern 22.
Router(config-dial-peer)#ex
```

IP Phone 2 configure in router 1 by dial-peer

Figure (18): IP PHONE 1-1

R2

IP Phone 2 configure in router 2 with DHCP

```
Router(config)#
Router(config)#
Router(config)#ip dhcp pool voice
Router(dhcp-config)#net 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#option 150 ip 192.168.2.1
Router(dhcp-config)#ex
Router(config)#ip dhcp ex
Router(config)#ip dhcp excluded-address 192.168.2.1
Router(config)#telephony-service
Router(config-telephony)#max-dn 5
Router(config-telephony)#max-ephone 5
                          ^
% Invalid input detected at '^' marker.

Router(config-telephony)#max-ephone 5
Router(config-telephony)#ip source-address 192.168.2.1 porrt 2000
                                                        ^
% Invalid input detected at '^' marker.

Router(config-telephony)#ip source-address 192.168.2.1 port 2000
Router(config-telephony)#auto assign 1 to 2
Router(config-telephony)#ex
Router(config)#ephone-dn 1
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#num 222
```

```
Switch(config)#int f0/1
Switch(config-if)#sw
Switch(config-if)#switchport voice vlan 1
```

Vlan voice for IP Phone

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session target ipv4:11.0.0.1
Router(config-dial-peer)#destination-pattern 11.
Router(config-dial-peer)#ex
```

IP Phone 1 configure in router 2 by dial-peer

Figure (19): IP PHONE 1-2

6. ACCESS POINT

In our topology, we utilized Access point to make the wireless devices inter our network, we make IP configuration static for all devices and make their subnet mask the same as the switch the connect to:

R2

Access point1-2

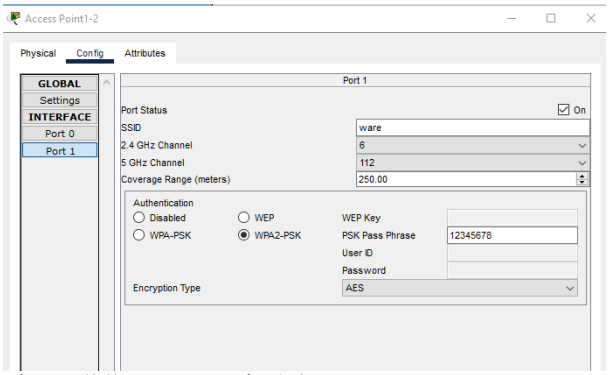


Figure (20): Access point1-2

In access point 1-2 we named it (SSID) **ware** and made the Authentication WPA2-PSK and the password **12345678** For PCs and laptops, we put the module WPC300N to provide a wireless connection.

R3

Access point1-3

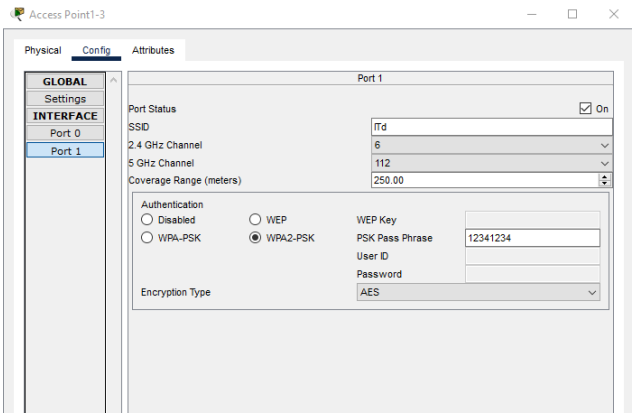


Figure (21): Access point1-2

In access point 1-3 we named it (SSID) **ITd** and made the Authentication WPA2-PSK and the password 12341234 For PCs and laptops, we put the module WPC300N to provide a wireless connection.

R5

Access point1-5

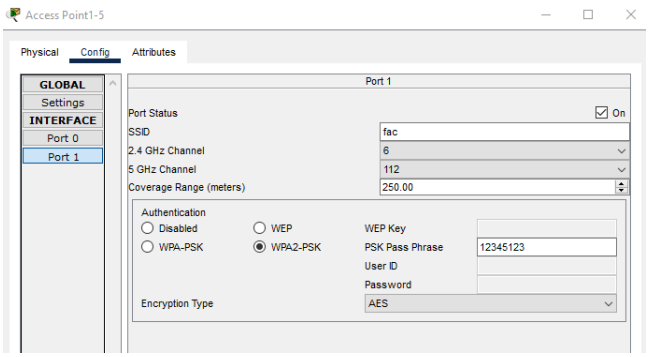


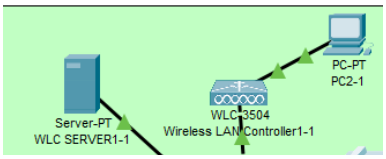
Figure (22): Access point1-2

In access point 1-3 we named it (SSID) **fac** and made the Authentication WPA2-PSK and the password 12345123 For PCs and laptops, we put the module WPC300N to provide a wireless connection.

7. WLC (Wireless LAN Controller)

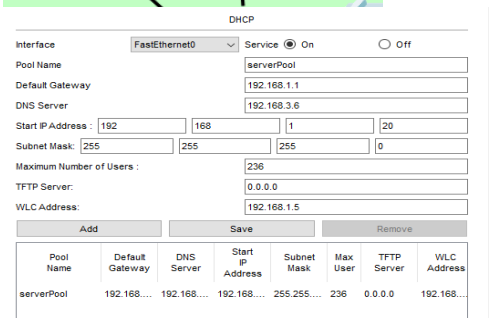
In our topology, we utilized WLC to be able to have a light-weight access point and that will help to make the wireless devices inter our network, we make IP configuration dynamic for all devices and for that we needed to have built a WLC server with DHCP services, and this is how we connect it:

1. R1 WLC1-1



First, we set IP addresses for the WLC1-1 and WLC server1-1 and the PC2-1 that connects to the WLC.

WLC1-1: 192.168.1.5. WLC server1-1:192.168.1.7. PC2-1:192.168.1.6.

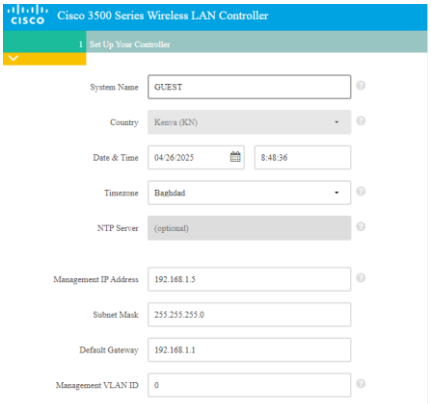


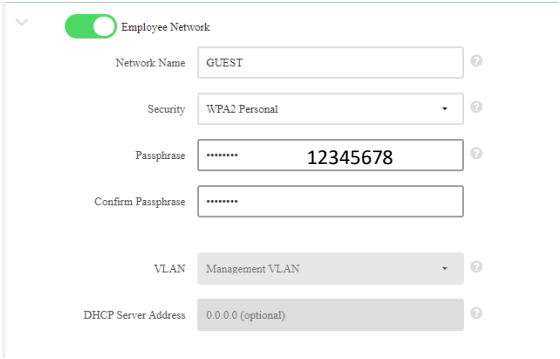
Then we implemented the DHCP services in WLC server:
so, every device connected to this wireless LAN will have dynamic IP address.

Figure (23): R1 WLC server1-1

And then we go to PC2-1 to configure the WLC first we go to http://192.168.1.5 we set a username: **Admin** and password: **Admin@1.**

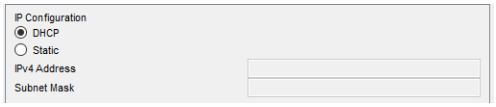
Set up the WLC controller





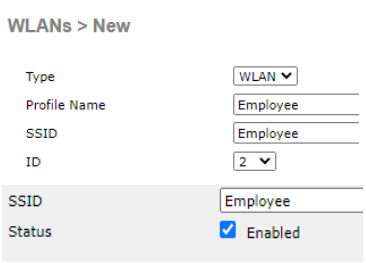
Figures (24,25,26): http://192.168.1.5

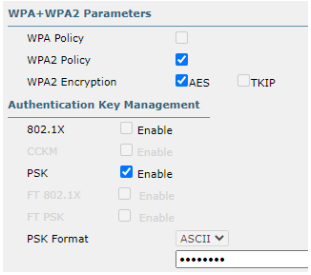
Then, we go to https://192.168.1.5 to check and add other WLAN for Employee because we put the first one for guest.



First, we should make the IP configuration of access point to DHCP.

We found the AP in the wireless of WLC.





we make a new WLAN for Employee and set the security layer 2 with wpa2 policy and encryption

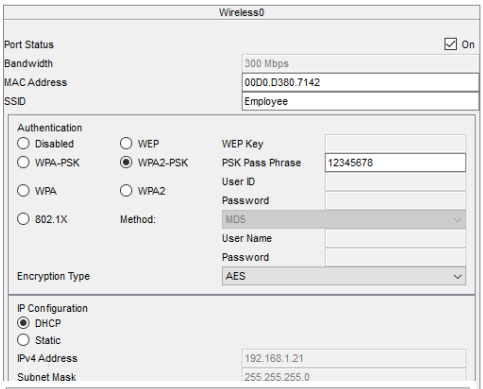
with password 12345678

we have now 2 WLAN in our WLC1-1

Figure (27,28,29): https://192.168.1.5

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

So, for employee they will enter the Employee WLAN and Guest will enter the GUEST WLAN that will improve the security of the wireless network and the strength of it.



Employe laptop enter the WLAN with the SSID and the password and have DHCP IP configuration.

Figure (30): R1 WLC connection employee

A guest enters the WLAN from the phone with SSID and password of guest WLAN and has DHCP IP configuration.

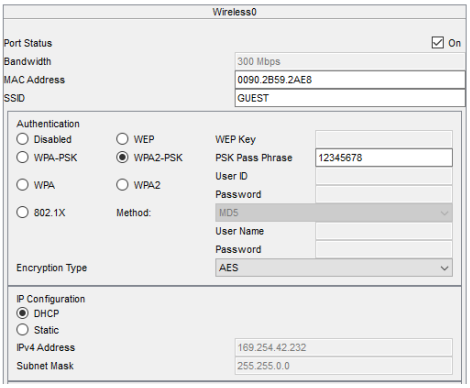


Figure (31): R1 WLC connection guest

2. R4 WLC1-4

We do the same steps of R1 WLC1-1, just change the IP addresses and don't use two WLAN. Because we don't need a guest network in this branch because its Distribution Center. So, we build it in the same way with:

Laptop2-4

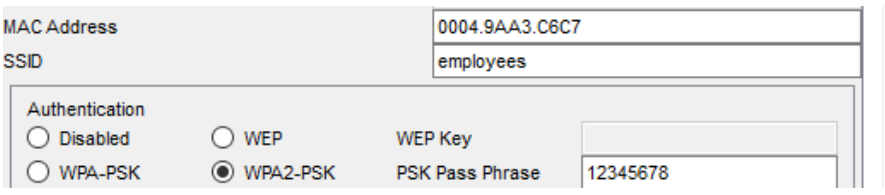
WLC server1-4

WLC1-4

And we name the SSID "employees" and password 12345678

AP Name	IP Address(Ipv4/Ipv6)
Light Weight Access Point1-4	192.168.10.20

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



Employe enter with Tablet PC1-4 and having the SSID and the password of the WLAN of employees. And DHCP IP configuration.

Figure (32): R4 WLC connection

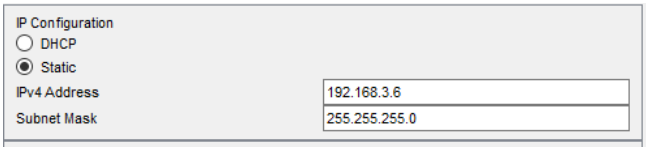
8. Servers

Servers	IP address	Subnet mask	Default gateway
DNS server1-3	192.168.3.6	255.255.255.0	192.168.3.1
Web server1-3	192.168.3.5	255.255.255.0	192.168.3.1
WLC server1-1	192.168.1.5	255.255.255.0	192.168.1.1
WLC server1-4	192.168.10.5	255.255.255.0	192.168.10.1

Table (8): Servers Addressing

1. DNS server

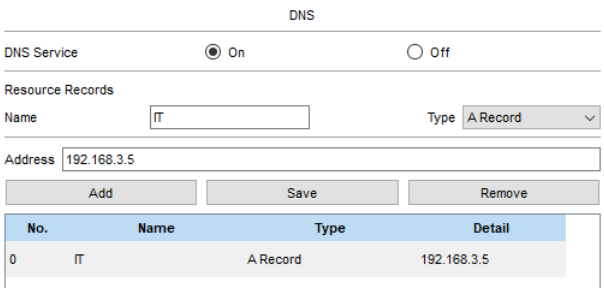
We implemented a DNS server to allow users to access the web server using domain names instead of IP addresses. This approach simplifies the process of reaching the hosted services and resources, making it more convenient and user friendly for everyone.



The IP configuration to this server with 192.168.3.6

So, it's built in the IT Department (R3) branch.

Figure (33): DNS server IP config



We add the Wab server by its address and give its name.

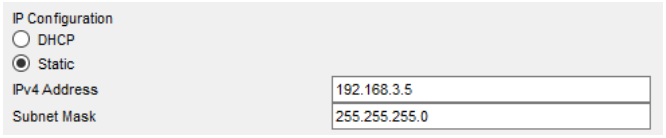
Name: IT

Address: 192.168.3.5

Figure (34): DNS server assign

2. Web server

We have implemented a web server to provide employees with access to company resources, internal communications, and collaboration tools.



The IP configuration to this server with 192.168.3.5

So, it's built in the IT Department (R3) branch.

Figure (35): Web server IP config

We add the http web in this server so we write html code for the website.

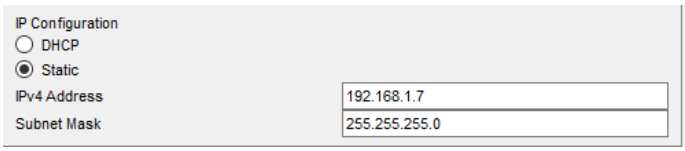
Figure (36): Web server http adding

3. WLC server

We implemented a Wireless LAN Controller (WLC) server to administer and oversee the wireless access points in the network from a central location. With wireless controllers, parameters need to be set once and all the other access points would automatically pick up these wireless settings, this setup simplifies the configuration and monitoring of wireless networks, ensuring seamless connectivity, enhanced security, and improved user experience across all wireless devices.

This design is for WLC server1-1 and WLC server1-4

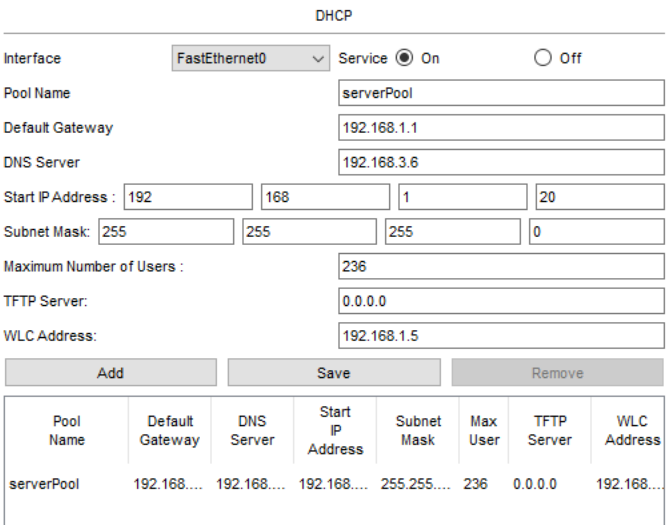
For WLC server1-1:



The IP configuration to this server with 192.168.1.7

And it's built in the store (R1) branch.

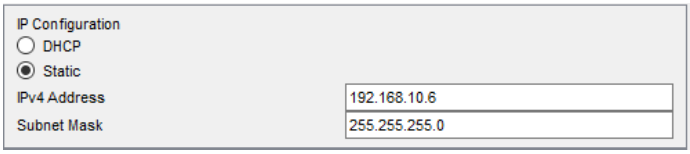
Figure (37): WLC server1-1 configuration



We configured a DHCP pool on the WLC server to provide IP addresses to wireless clients, starting from 192.168.1.20. The WLC will assign IP addresses beginning with this address, with a maximum capacity of 236 users. Additionally, we set the WLC management address to properly handle wireless client connections.

Figure (38): WLC server1-1 DHCP pool

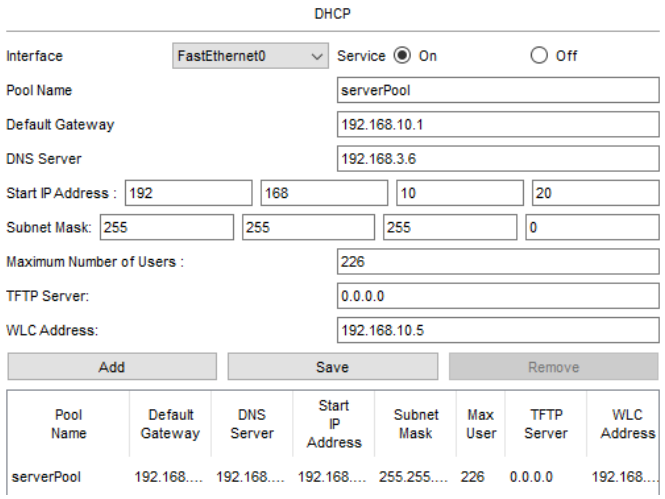
For WLC server1-4:



The IP configuration to this server with 192.168.10.6

And it's built in the Distribution Center (R4) branch.

Figure (39): WLC server1-4 configuration



We configured a DHCP pool on the WLC server to provide IP addresses to wireless clients, starting from 192.168.10.20. The WLC will assign IP addresses beginning with this address, with a maximum capacity of 226 users. Additionally, we set the WLC management address to properly handle wireless client connections.

Figure (40): WLC server1-4 DHCP pool

10.0 General

- We use a PC or a laptop for each router and connect it via console cable, to interact with the CLI from the terminal. These PCs and Laptops are named using only numbers.
- For devices we named them using "**name-of-deviceX-Y**", X is the devices number in the branch, Y is the router number.
- We used a /8 subnet mask for the global network and a /24 subnet mask for router interface and internal networks. This approach ensures IP address space for all global operations while enabling efficient IP management within the internal network.
- We configured interfaces for each router they attached to, with the correct IP addresses and subnet masks.
- We designed the network in the physical mode to simulate the real project as we create it.
- We designed the network in the logical mode to make the configuration and implementation parts easier.
- The design is of the company, and the branches of this company are:
    - "R1" Store
    - "R2" Warehouse
    - "R3" IT Department
    - "R4" Distribution Center
    - "R5" Factory
    - "R6" Administration
- We used the VLANs in the internal network and they were:
    - R1 VLAN number 100 name store IP address 192.168.1.1
    - R2 VLAN number 400 name ware IP address 192.168.2.1
    - R3 VLAN number 200 name ITd IP address 192.168.3.1
    - R4 VLAN number 500 name dis IP address 192.168.10.1
    - R5 VLAN number 300 name fac IP address 192.168.4.1
    - R6 VLAN number 10 name rec IP address 192.168.6.1
    - R6 VLAN number 20 name ser IP address 192.168.7.1
    - R6 VLAN number 30 name mang IP address 192.168.8.1
- IP Phones are used to make calls between the Store and Warehouse to improve communication between the two branches.
- We used a security password to enter the routers CLI and password is "**group1**".

11.0 Logical view

This is a view of our network:

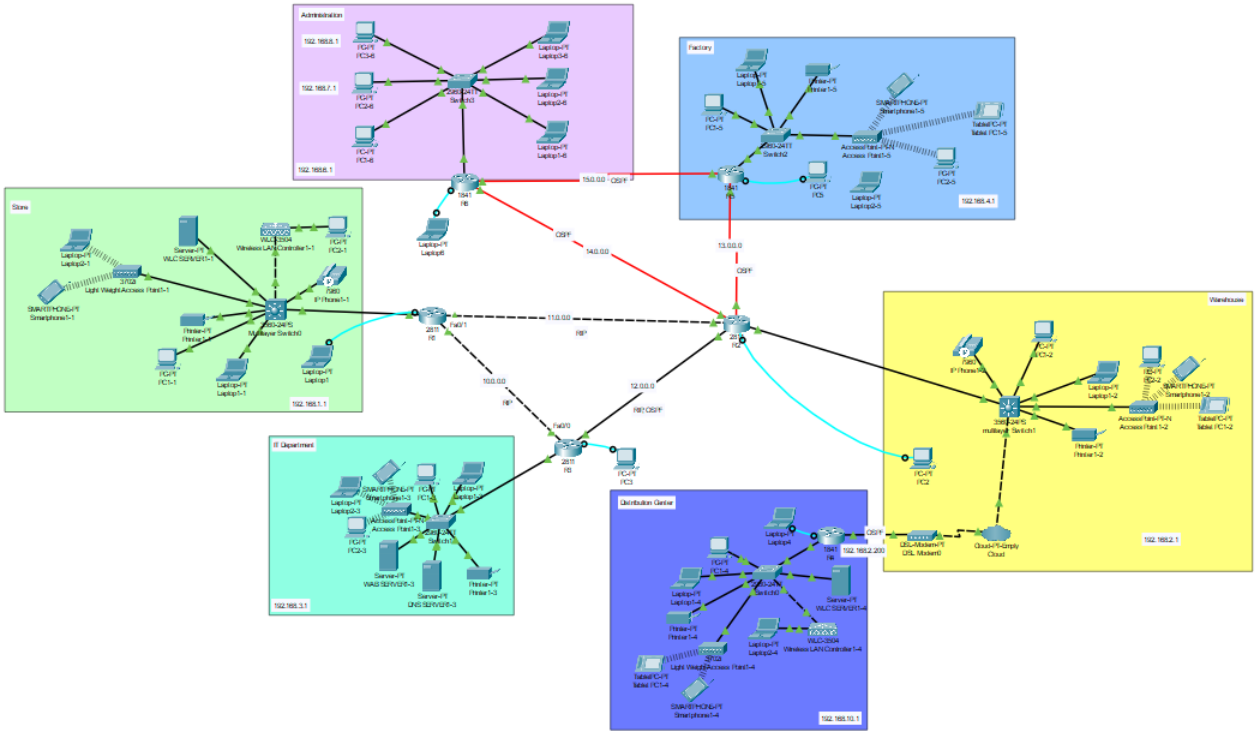
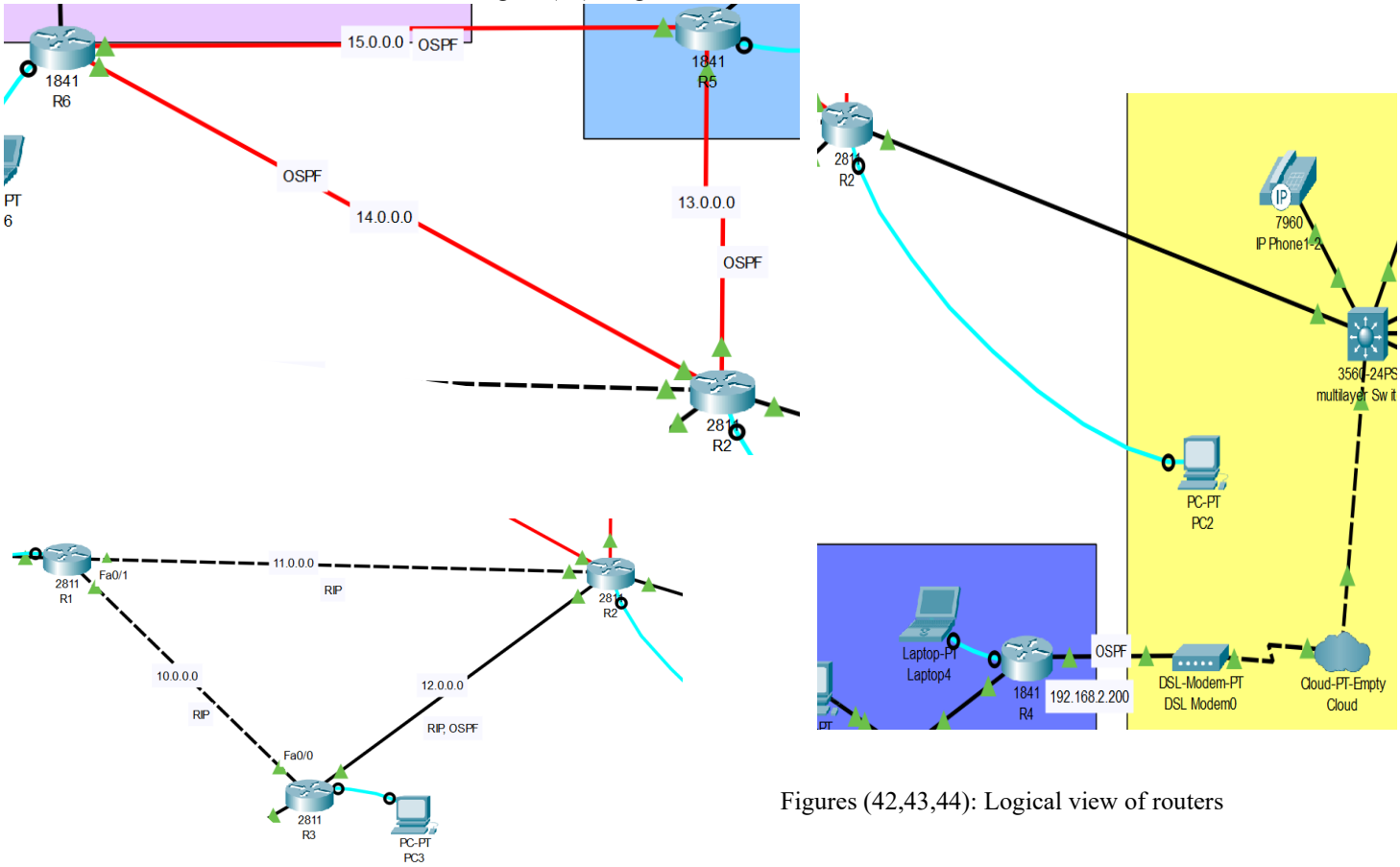


Figure (41): Logical view of the network



Figures (42,43,44): Logical view of routers

R1

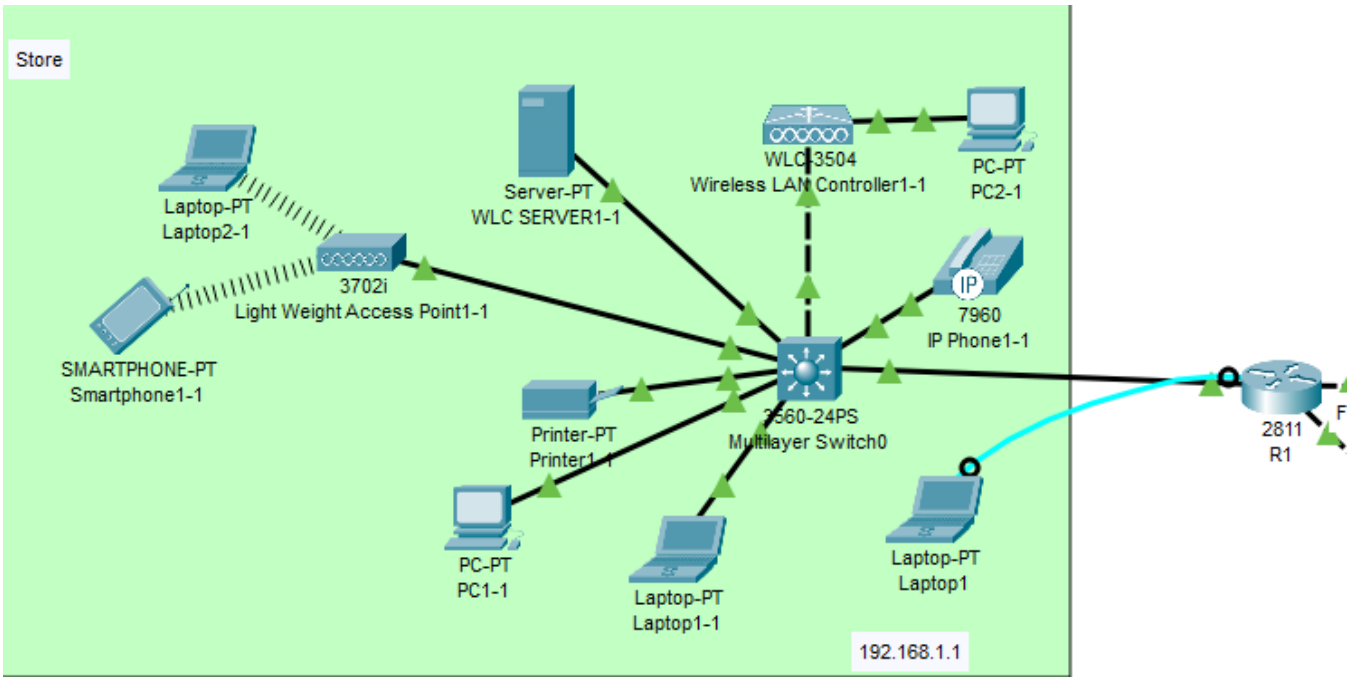


Figure (45): Logical view of R1

R2

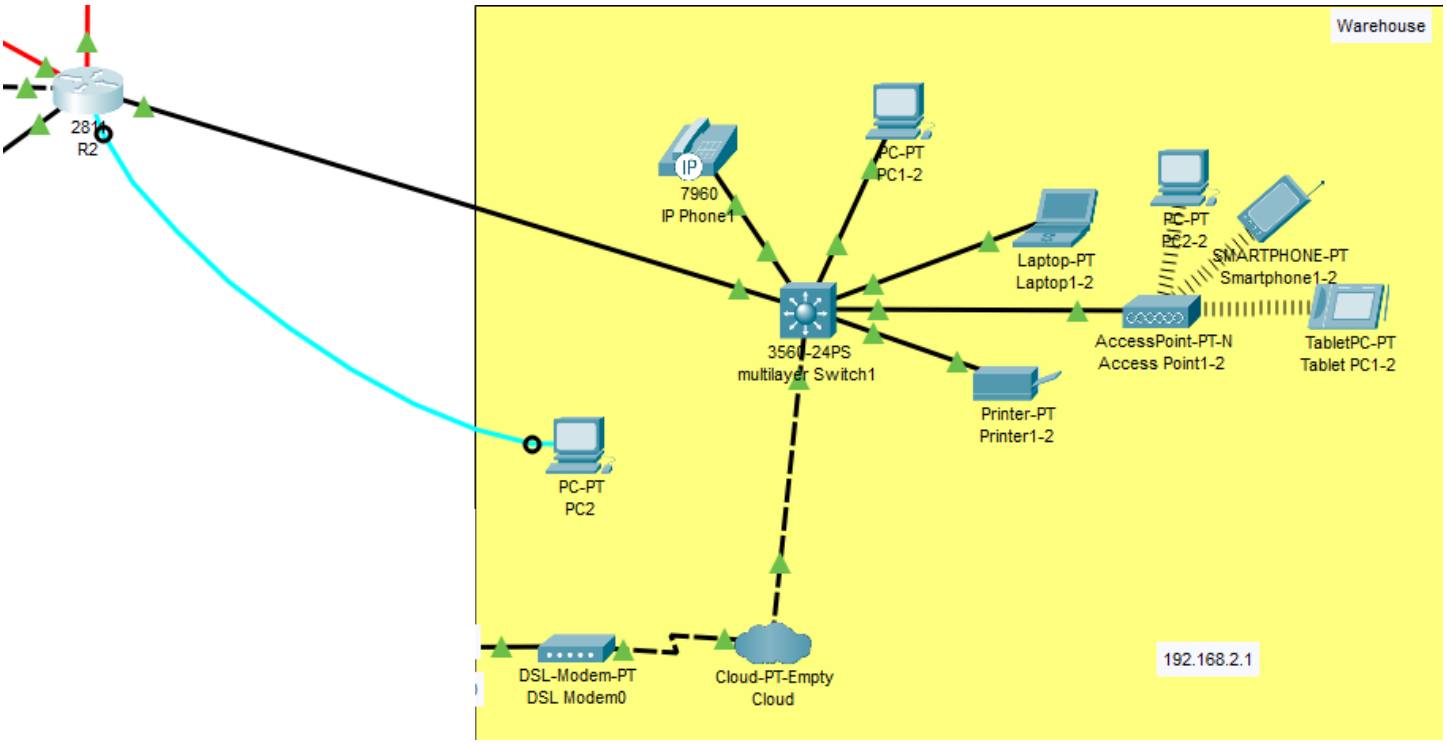


Figure (46): Logical view of R2

R3

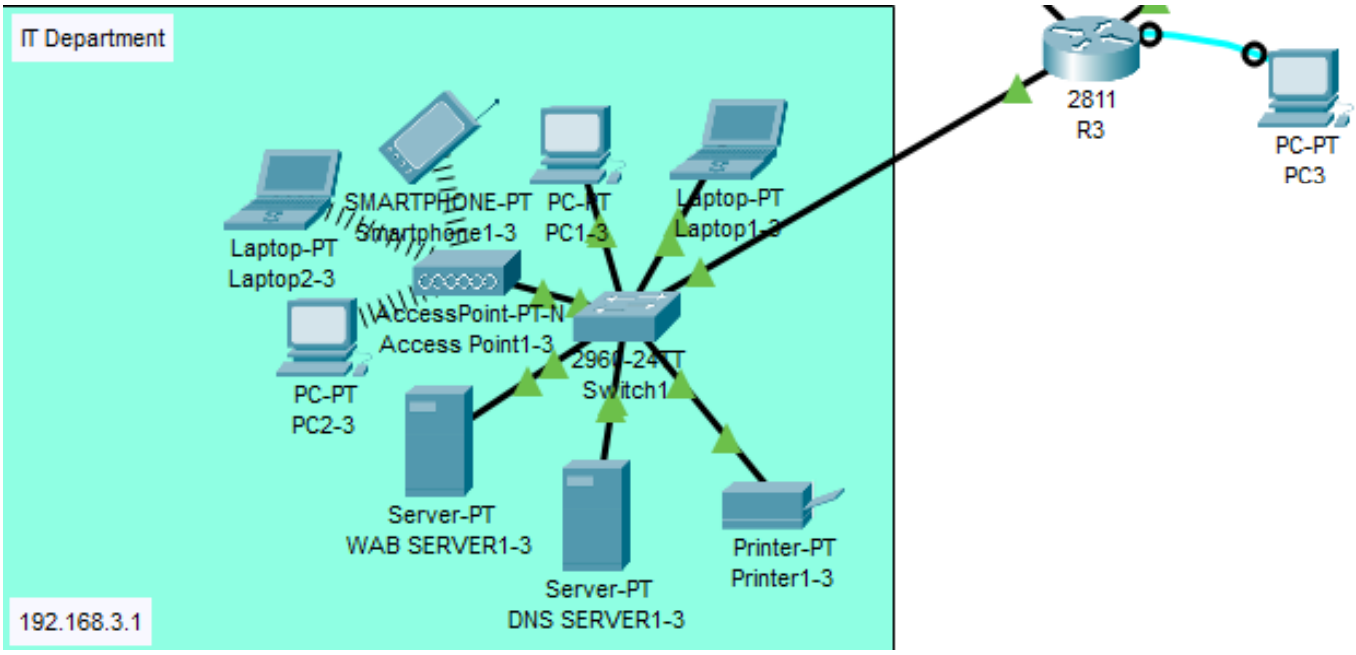


Figure (47): Logical view of R3

R4

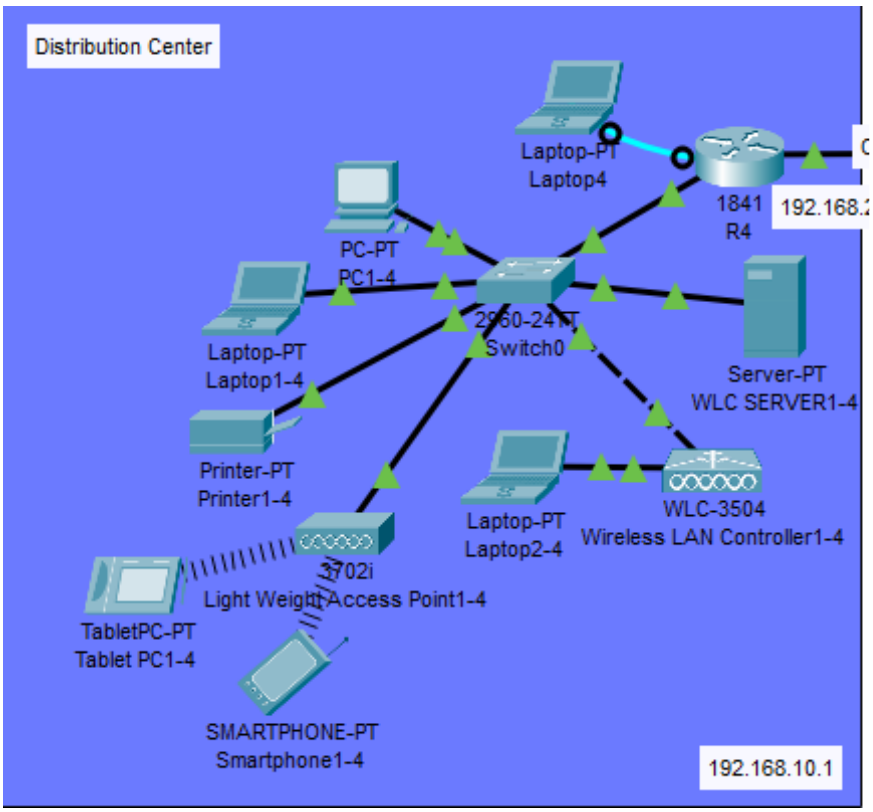


Figure (48): Logical view of R4

R5

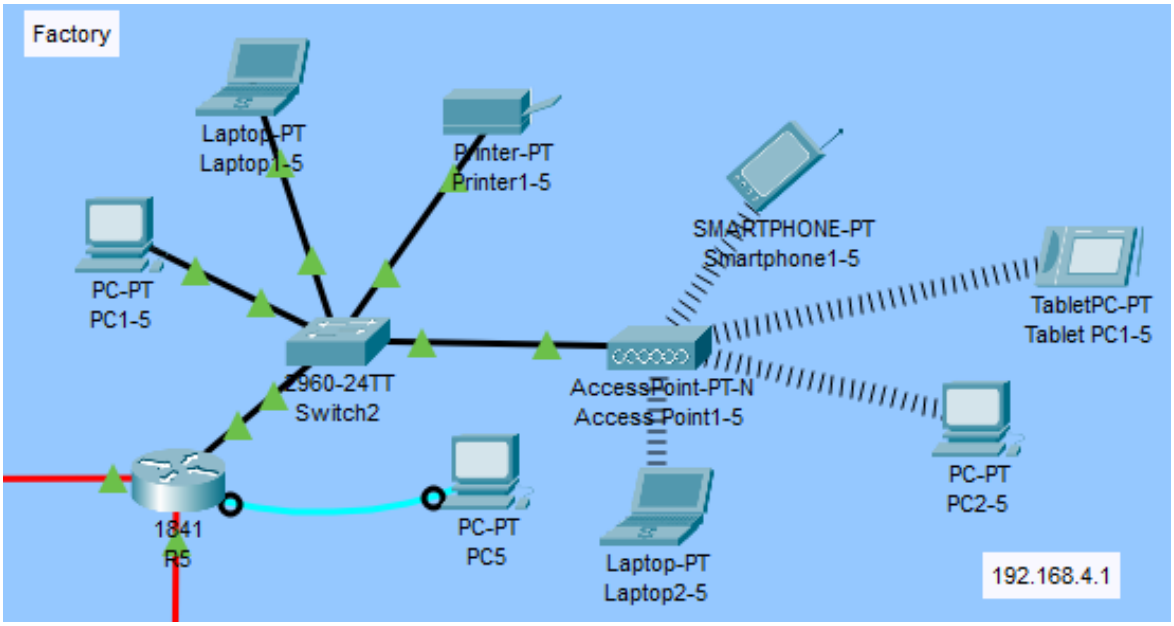


Figure (49): Logical view of R5

R6

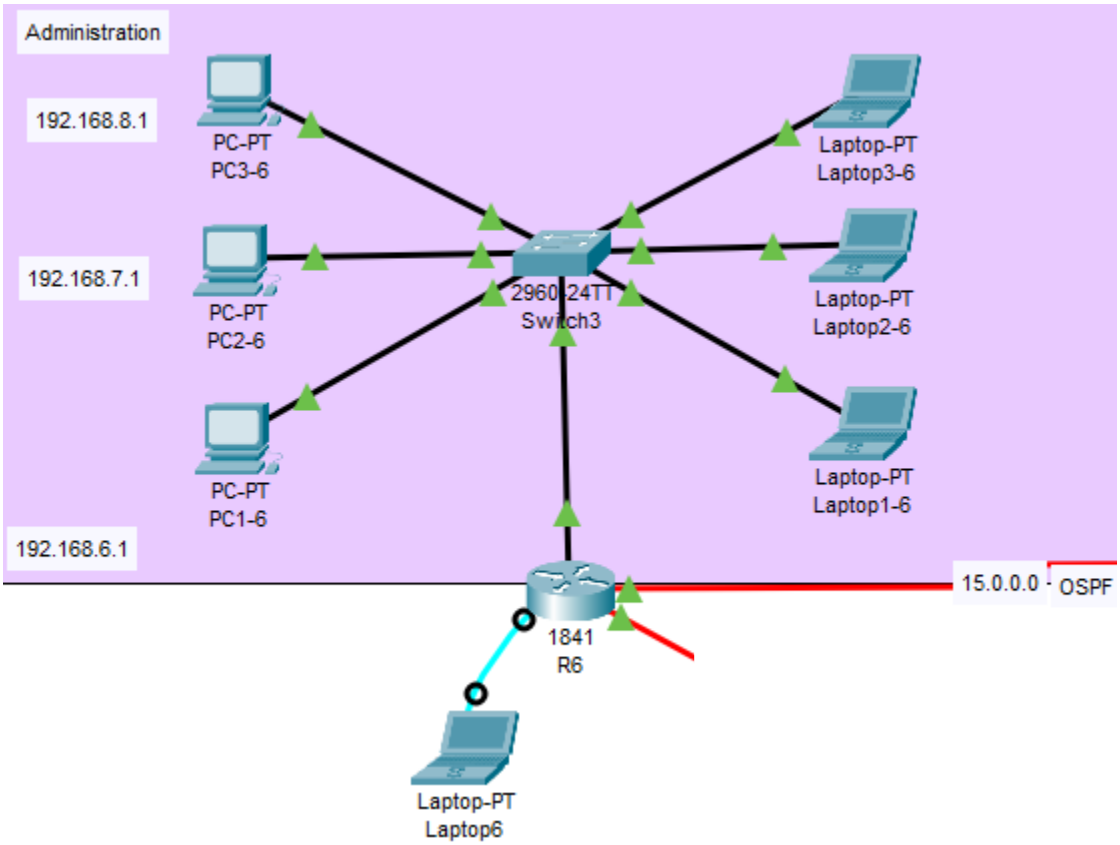


Figure (50): Logical view of R6

12.0 Physical view

This is a view of our network:

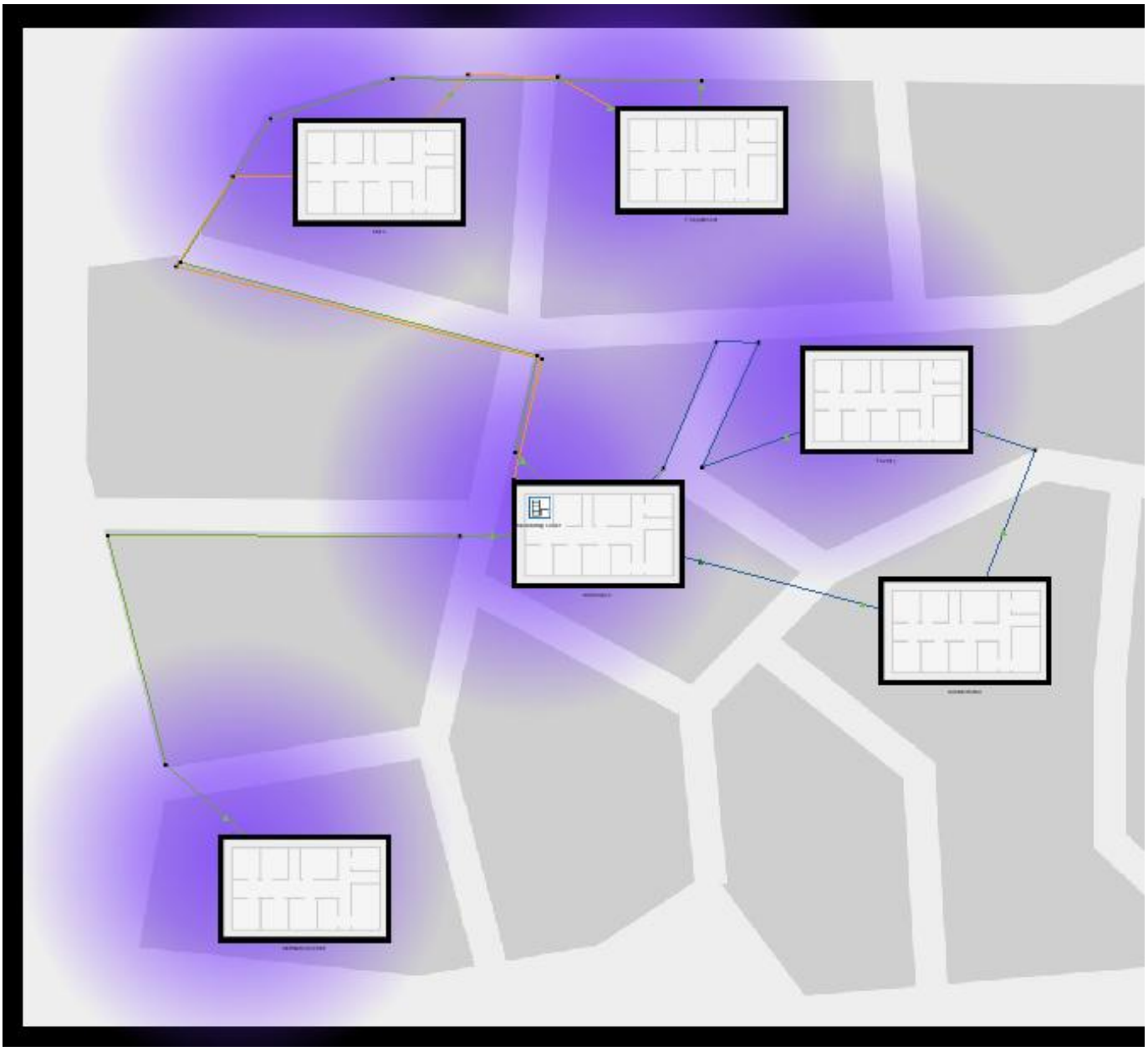


Figure (51): Full physical view

This is the physical view of the company which shows how the branches are distributed:

Store

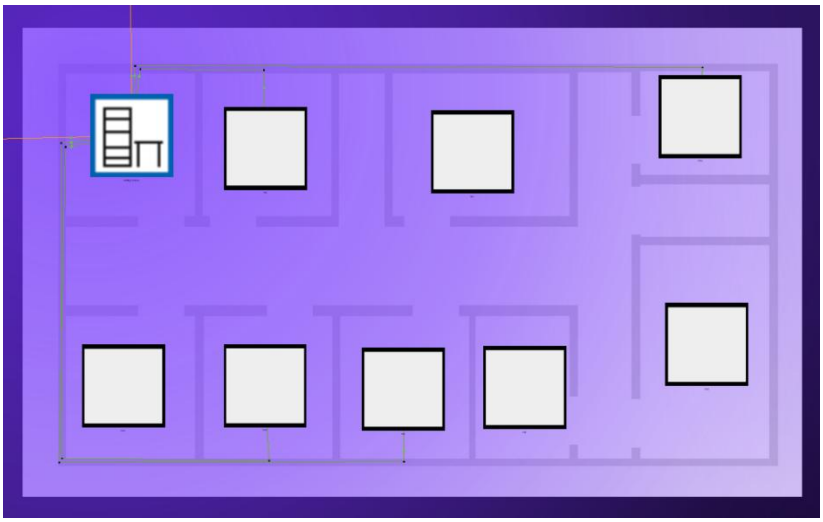


Figure (52): Physical view of Store (R1)

Warehouse

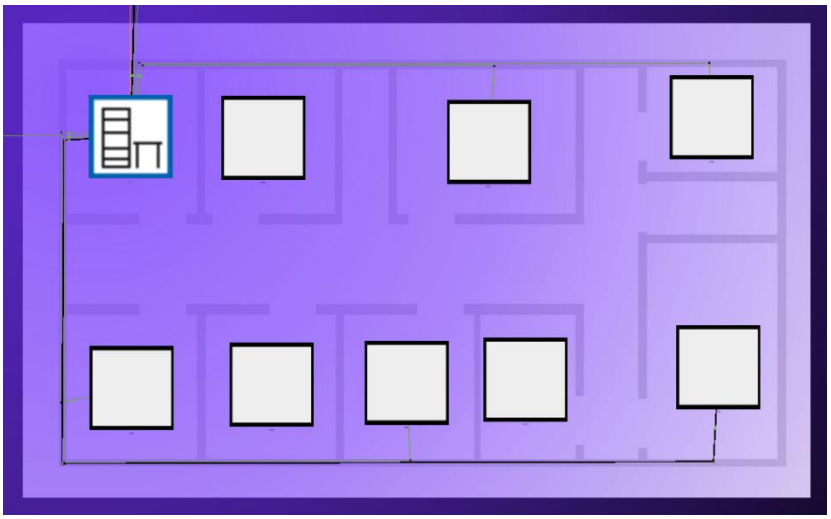


Figure (53): Physical view of Warehouse (R2)

IT department

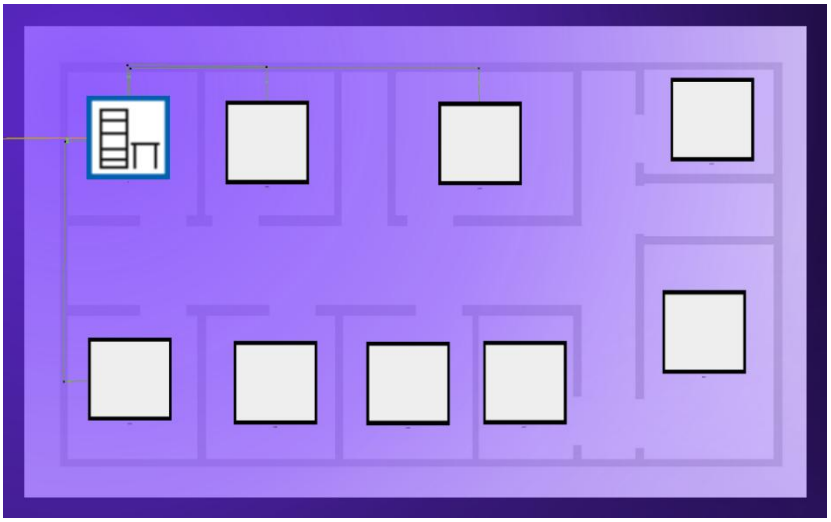


Figure (54): Physical view of IT department (R3)

Distribution Center

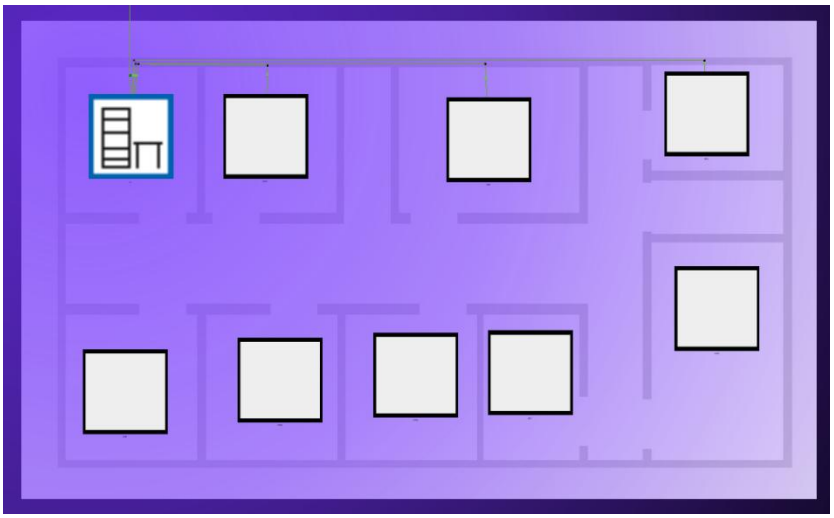


Figure (55): Physical view of Distribution Center (R4)

Factory

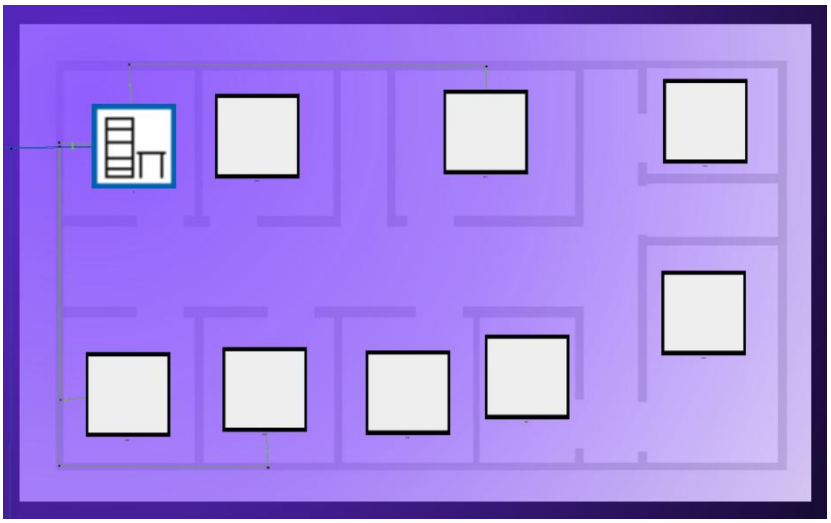


Figure (56): Physical view of Factory (R6)

Administration

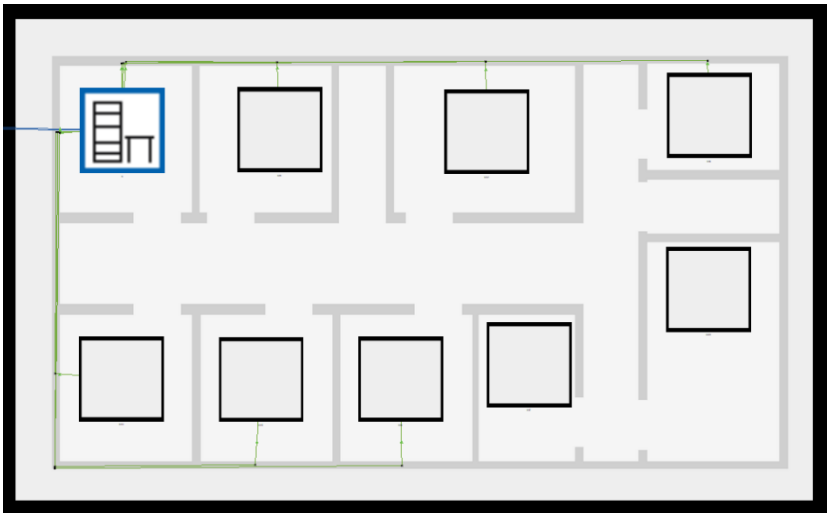


Figure (57): Physical view of Administration (R6)

13.0 Results

We ping from the device **PC1-1** that is in R1 (Store) to other devices in other networks (branches):

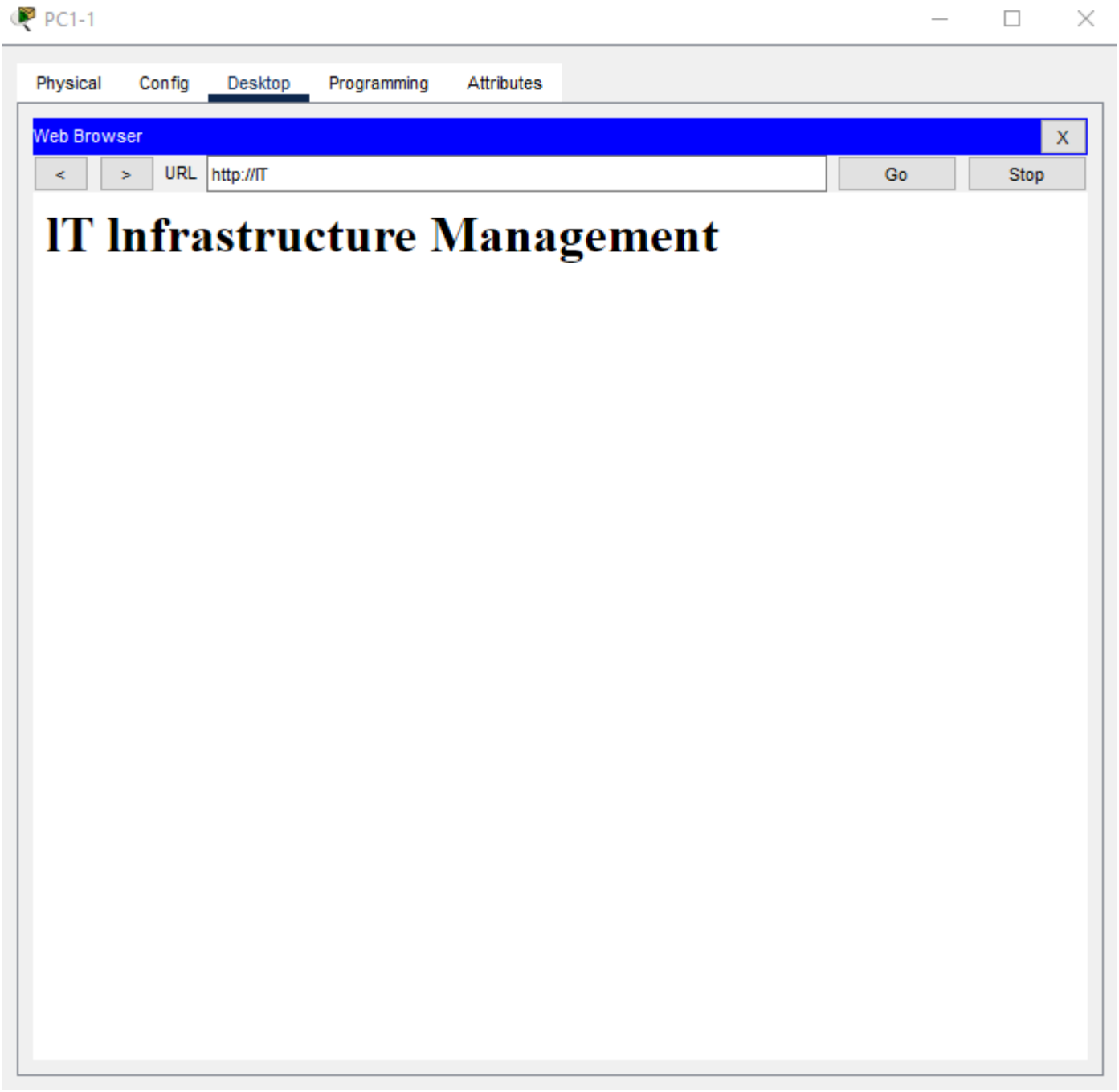
Successful	PC1-1	PC1-2	ICMP		0.000	N	0	(edit) (delete)
Successful	PC1-1	PC1-3	ICMP		0.000	N	1	(edit) (delete)
Successful	PC1-1	PC1-4	ICMP		0.000	N	2	(edit) (delete)
Successful	PC1-1	PC1-5	ICMP		0.000	N	3	(edit) (delete)
Successful	PC1-1	PC1-6	ICMP		0.000	N	4	(edit) (delete)

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.6.6: bytes=32 time=28ms TTL=125
Reply from 192.168.6.6: bytes=32 time=27ms TTL=125
Reply from 192.168.6.6: bytes=32 time=1ms TTL=125
Reply from 192.168.6.6: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 28ms, Average = 14ms

C:\>ping 192.168.7.6

Pinging 192.168.7.6 with 32 bytes of data:

Reply from 192.168.7.6: bytes=32 time=2ms TTL=125
Reply from 192.168.7.6: bytes=32 time=1ms TTL=125
Reply from 192.168.7.6: bytes=32 time=1ms TTL=125
Reply from 192.168.7.6: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.7.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.8.6

Pinging 192.168.8.6 with 32 bytes of data:

Reply from 192.168.8.6: bytes=32 time=2ms TTL=125
Reply from 192.168.8.6: bytes=32 time=2ms TTL=125
Reply from 192.168.8.6: bytes=32 time=2ms TTL=125
Reply from 192.168.8.6: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.8.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time<1ms TTL=125
Reply from 192.168.3.10: bytes=32 time=1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=1ms TTL=125
Reply from 192.168.3.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=58ms TTL=125
Reply from 192.168.10.11: bytes=32 time=60ms TTL=125
Reply from 192.168.10.11: bytes=32 time=42ms TTL=125
Reply from 192.168.10.11: bytes=32 time=83ms TTL=125

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 83ms, Average = 60ms

C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Reply from 192.168.4.10: bytes=32 time=40ms TTL=125
Reply from 192.168.4.10: bytes=32 time=29ms TTL=125
Reply from 192.168.4.10: bytes=32 time=31ms TTL=125
Reply from 192.168.4.10: bytes=32 time=37ms TTL=125

Ping statistics for 192.168.4.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 40ms, Average = 34ms
```

These Figures shows the pinging process to the devices in other networks and that the pinging process was successful.

Figures (58,59): Ping to other devices from PC1-1



Figures (60): Ping to website http://IT

we visit the web from the PC “PC1-1”, from the web browser on the desktop in the URL we write the name of the web server that we configure in the DNS server the name is “**IT**”, and we made that because we want the users to remember the web server and that may no need for recognize the IP address for this server and the visit was Successful because we now see the web.

14.0 Conclusion

The WLC server, which we set up, was created to control the wireless access points in the network through and through. The automatic treatment of the configuration and monitoring of wireless networks is achieved by connecting such networks to this setup. Thus, we can achieve confidence for efficient changes in the network and the dialogue between the access points, which, as a result, will increase the system security and the consumer experience of the staff from any wireless device.

The deployment of a highly scalable and reliable network infrastructure that covers all six establishments of the company, whose details have been amply demonstrated, and the implication of fault tolerance as a logical approach are two of the most significant reasons for making IT decisions (solution selection), paving the road for accelerated day-to-day operations as well as growth. We have used the protocols RIP and OSPF as dynamic routing as well as traffic division through VLANs; therefore, good governance of the data was ensured, congestion was kept to a minimum, and security was greatly improved.

The WLAN controllers that we added, the DNS and web servers, and the cloud services that were put in place created a modern and flexible environment that uses the newest technologies and supports the work of the team wherever they are. The network became robust and secure by configurations incorporated in the planning for the network, supporting all sorts of devices, from smartphones to servers, while still maintaining the level of stability necessary for a good performance.

To summarize, the project brings out the pivotal role of IT infrastructure in breaking barriers to communication, improving the organization's productivity, and meeting the new challenges in a modern, multi-branch operation.

15.0 References

A. & Carter, "DNS in Cisco packet tracer and how to configure DNS on Cisco router," *PacketTracerLab.com*. [Online]. Available: https://www.packettracerlab.com/dns-in-cisco-packet-tracer/. [Accessed: 26-Apr-2025].

B. Record Teros, "KONFIGURASI VOIP v2 (2 Router, 2 Switch & 4 Ip Phone) - Cisco Packet Tracer," *YouTube*, 2022. [Online]. Available: https://www.youtube.com/watch?v=5jeH5lQVF5g&ab_channel=RecordTeros. [Accessed: 26-Apr-2025].

C. [3] Cisco Systems, "Web User Interface Configuration Guide (Catalyst 9000 Switches) - Configuring the Switch Using the Web User Interface," *Cisco.com*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/web_ui/b-web-ui-9000cg/configuring_webui.html. [Accessed: 26-Apr-2025].

D. Cisco Systems, "OSPF Configuration Guide," *Cisco.com*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html. [Accessed: 26-Apr-2025].

E. [5] Study-CCNA, "Configuring RIP v2," *Study-CCNA.com*. [Online]. Available: https://study-ccna.com/configuring-ripv2/. [Accessed: 26-Apr-2025].

F. CloudTechAdmin, "Configure Redistribution Between RIP and OSPF in Cisco IOS Router," *CloudTechAdmin.com*. [Online]. Available: https://www.cloudtechadmin.com/configure-redistribution-between-rip-and-ospf-in-cisco-ios-router/. [Accessed: 26-Apr-2025].