Ministry of Education
Imam Abdulrahman bin Faisal University
Computer Science department

CIS326: IT Infrastructure Management Report

SMART RAILWAY NETWORK

Students name	**ID**
Hajer Abdulrahman Al-Saadan	2210003576
Lojain Hafez Alibrahim	2220001991
Elaf Mohammed Aljaramez	2220000917
Raghad Ali alzahrani	2220002910
Shatha Ahmed Alanazi	2220006290

Instructors:

Dr. Eman Ferjani - Dr. Eiman Kattan - Dr. Huda Althumail

Academic year 1445 – 2023/2024

Table of Contents

Abstract:

The dynamic world of contemporary transportation infrastructure is ours to explore and learn from! The demand for effective and dependable transportation networks has never been higher than it is in the fast-paced, globally connected society of today. Railways have long been a mainstay of transportation, and with the incorporation of advanced technology, The industry is about to undergo a transformation. In this project, we set out on a quest to learn more about the development of a modern railway network that is seamlessly integrated using mobile technology by Packet Tracer to boost energy efficiency as one of the main factors. Consider a railway network where trains interact with one another and with central authority, assuring efficient operations, safety, and resource management. By combining traditional railway engineering with the miracles of modern networking, this revolution is made feasible. As we delve into the intricacies of designing, simulating, and managing a railway network that can be monitored and controlled right from a smartphone. The foundational ideas of networking, energy efficiency optimization, and network interconnection using IOT will all be covered too.
Index Terms – Cisco, Packet Tracer, CCNA, Network Module, Smart Railway, Computer Networks, IOT.

Introduction:

A network is defined as a group of devices connected to exchange data with each other. In addition to the number of devices they contain, networks differ in terms of type and division based on the geographic area they cover. Because of the useful services they offer, like connecting various devices to the Internet so that everyone can access and browse their websites regardless of location, each network has a specific purpose and coverage area. This has led to the development of new concepts in the computer industry, like databases. But the ill-prepared network could cost the company a lot of money. The most economical and efficient form of transportation, according to users, is rail. Therefore, creating a network with high security and high-quality performance is extremely important. We used an approach that allows the network administrator to monitor both inbound and outbound traffic while adhering to certain security guidelines. We make use of the various routing protocols and networking environment security ideas in this reasoning. It can display the correct packet flow from one Railway Office department to the other departments. The Railway Office is separated into various Departments that go by the names of Ticket counter, security departments, IT departments, HR department, Accounts Department. The project consists of the Access Control & Network Address Translation concept for security purposes. One department has a gateway that communicates with the Internet service provider (ISP), receives data, sends it to the router to translate and distribute to the wireless devices. In other words, with a gateway, Railway gets wireless Internet access (Wi-Fi). In the security Department we used A multilayer switch, it is not the same as the Data Link Layer (DLL) that switches often employ; rather, it is a network device that can function at higher layers of the OSI reference model. At extremely rapid speeds, a multilayer switch can carry out both switch and router duties. To control access to computer resources, enforce policies, and audits usage we used Authentication, authorization, and accounting (AAA).

Objectives:

This project's primary objective is to offer a local area network design that is appropriate for railroad use. Many developing country railways are looking for solutions to integrate networks with features like security and redundancy that are found in developed nation railway networks. It is difficult for the railways in countries that are developing to build a network that meets the same standards as those in advanced countries. A significant budget deficit is the primary issue facing developing nations. These railways will benefit from our research by being able to construct a network that uses affordable solutions without compromising unacceptable levels of quality or security.

Proposed Model

Choosing the Equipment:

For the purpose of transmitting information between nodes or between devices, each network needs a medium. These media are an important factor in deciding the network's transmission speed, maximum distance, interference shielding, and cost. In terms of general use, there are two options: wireless and physical connections. Here are some devices we used to design this network: Router, Switches, Wireless Router, PC, Laptop, Server, Printer, Smart phone, AC, Detector, Speaker, Motion Detector, Smoke Detector, Webcam, Window, Sniffer, Tablets, Ip Phones, Access Point etc.

Connection Setup:

Owing to the constraints, connecting all PCs to switches—which must then be connected to routers—is the obvious way to join devices. That means there are RIP connections on every router. The first router links two switches in separate networks because the Ticket Counter network switch uses an access point to connect the laptops to a printer. The second primary switch is therefore connected to a wireless router, a sniffer, and two more switches. An additional router connects three networks—which are connected to numerous services, such as Email and DHCP servers— to the external networks or the internet.

4 types of cables were used here:

- Copper Straight-through Cable
- Copper Cross-over Cable
- Serial DTE Cable
- Console Cabl

Choosing Network Topology:

The configuration of a computer network's hosts is determined by its topology. It describes the configuration and interconnection of the PCs and other hosts. Network topologies come in a variety of forms, including Point-to-Point, Bus, Star, Ring, and Mesh. Every kind possesses a unique combination of benefits and drawbacks. To take use of both, we have employed two distinct topologies: mesh and star topologies. With a mesh topology, every device in the network is connected to every other device, offering several communication channels for high dependability and redundancy. Although this structure improves fault tolerance, it can be expensive and difficult to build and maintain. In contrast, all the devices in a star topology are connected to a single hub or switch. This setup makes installation and management easier and makes addressing isolated problems simpler. Nevertheless, the network is susceptible to a single point of failure due to its reliance on the central hub. Depending on requirements for redundancy, scalability, simplicity, and the need of continuous network connectivity, one might choose between a mesh or star topology.

Choosing Network Architectures:

It was client-server architectures that we implemented. Considering that client-server architectures are used in the majority of apps produced nowadays. outlined how client-server systems split processing between the client and the server by having each handle part of the logic. The server in these networks is in charge of data storage and data access logic, whereas the client is in charge of present logic. The application functionality might be divided between the client and server, or it could be entirely contained on the client.

DEVICE NAME:	QUANTITY:
PC'S	17
Laptop	8
Switch	12
Router	6
Wireless Switch	1
Ip Phone	3
Access Point	5
Multilayer Switch	1
Sniffer	1
Server	12
Home Getaway	3
AC	5
Security Camera	5
Door	5
Window	5
Motion Detector	1
Smoke Detector	1
Siren	1
Speaker	1
Printer	6
Smart Phone	3
Tablet	2
Console Cable	1
Serial Wire Connection	3

Cross Wire Connection	More than 10
Wireless connection	More than 30
Straight Wire Connection	More than 20

The Methodology Setting Up the Topologies:

Our Final Railway Networks:

Using Cisco Packet Tracer, we created a secure, functional, and integrated railway network for our project. We were able to simulate the network design by using the features of the application. Using the appropriate tools and protocols in the right devices for the needed purposes is an important component of an effective network as shown in Figure 1.

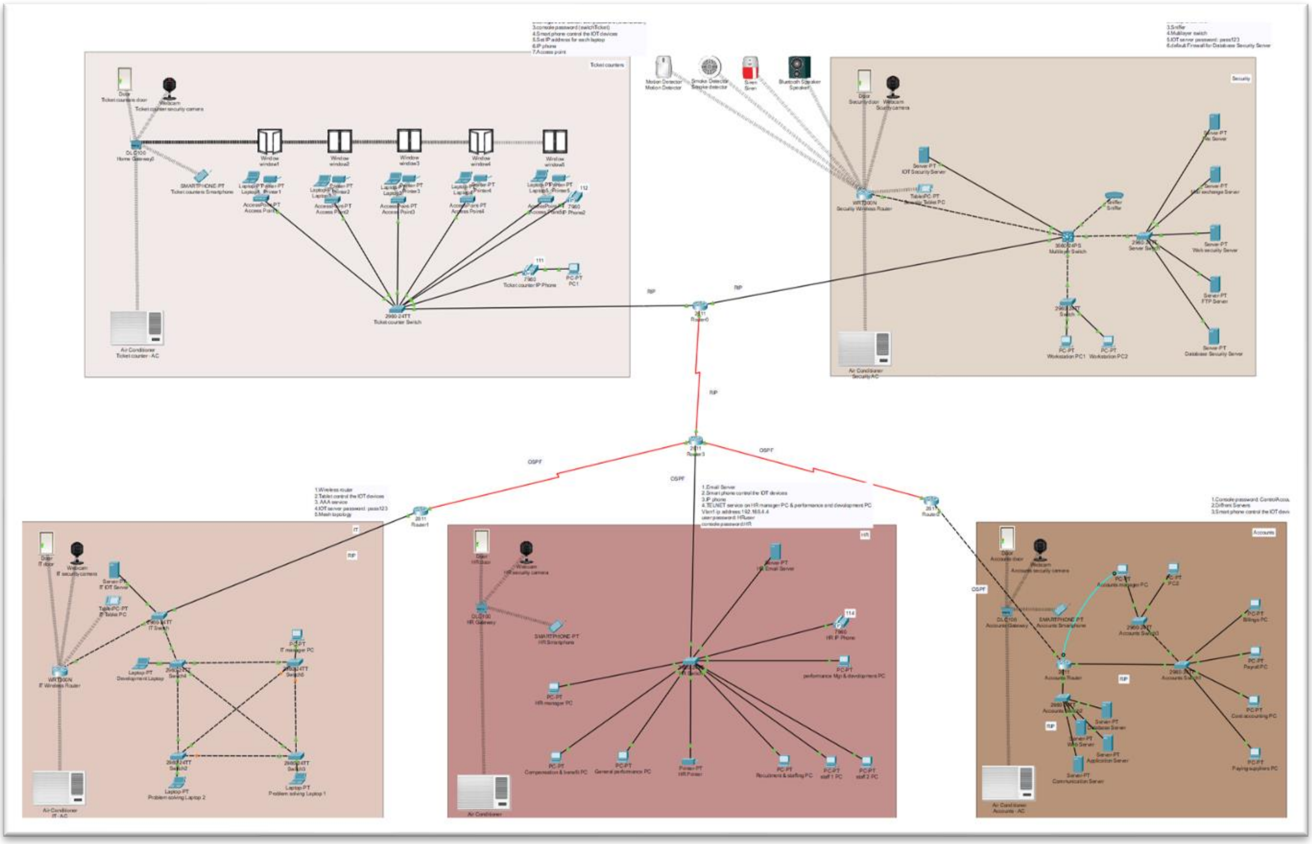


Figure 1: Final Railway Networks

Mesh Topology:

We used mesh topology to connect each device to every device in the network to increase flexibility as shown in Figure 2.

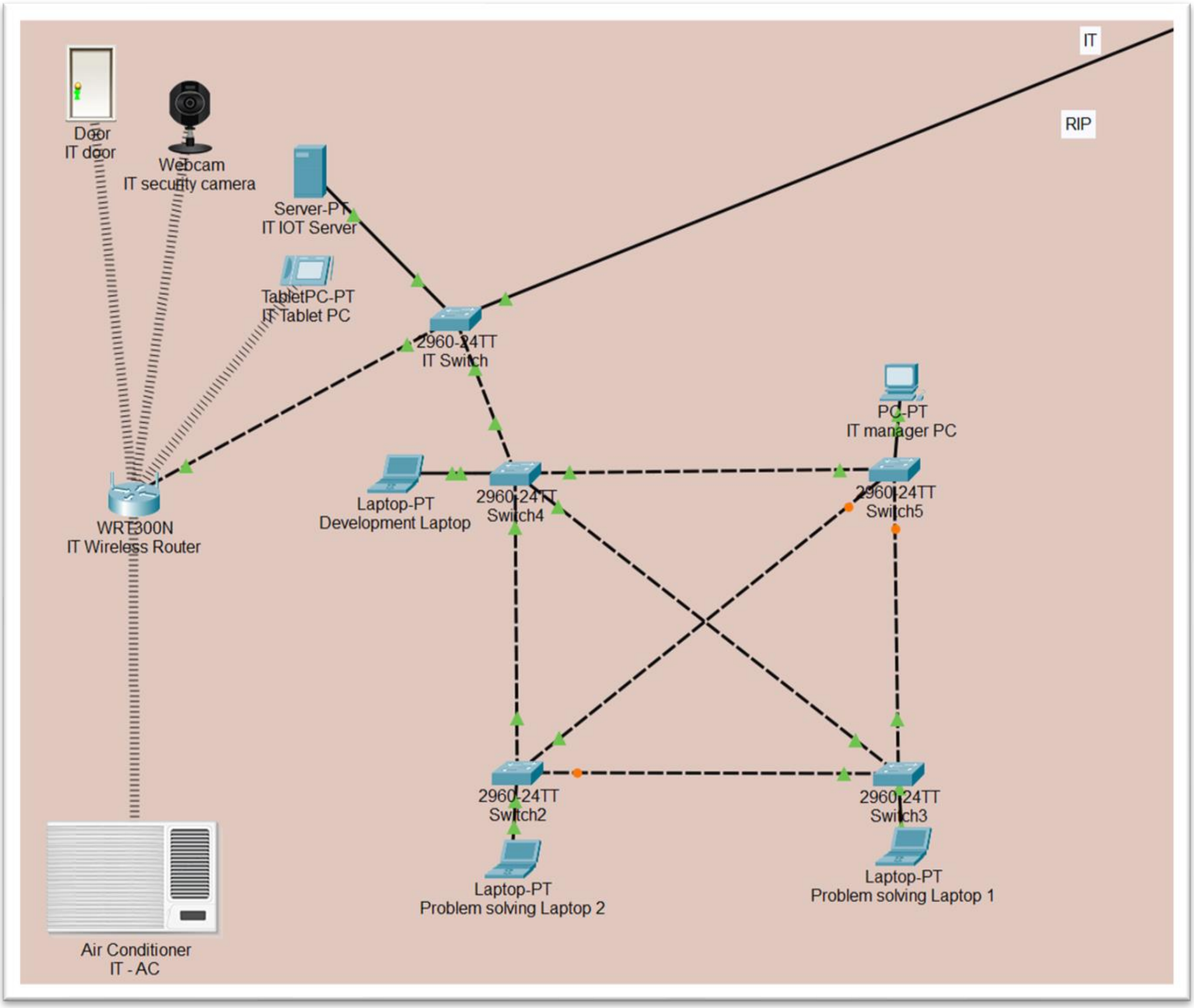
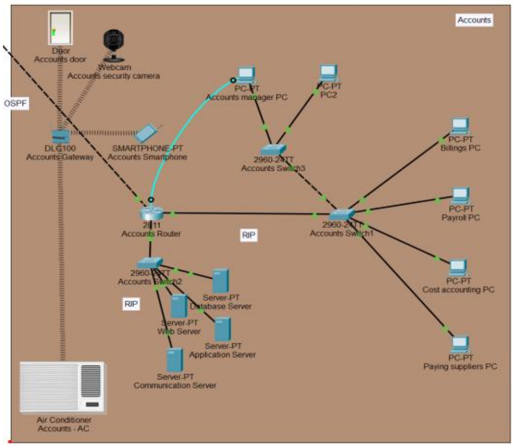


Figure 2:mash topology.

Star Topology:

Star topology in the network in more than one section as shown in Figure 3 and also Figure 4,5and6 is the most effective topology in our network to reduce the costs and facilitate the installing.



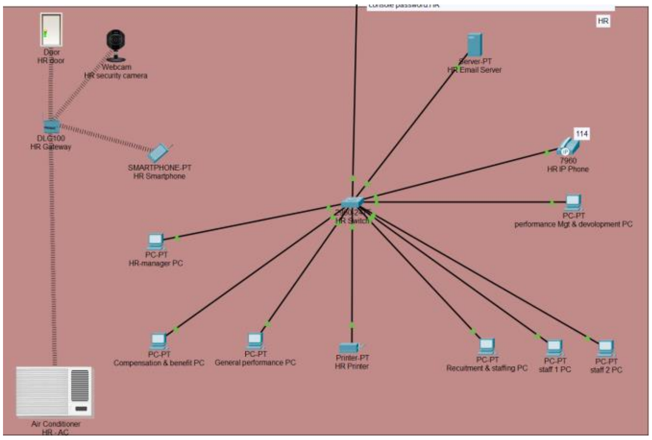


Figure 4: Accounts. *Figure 3: HR.*

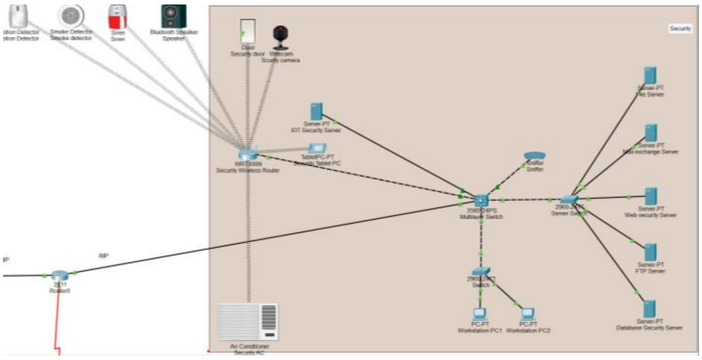


Figure 5: security.

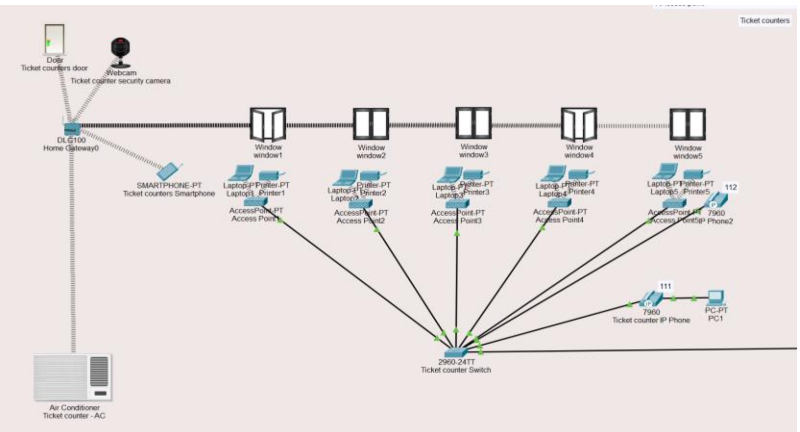


Figure 6: Tickets counters.

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router 0	Fa0/0 Fa0/1 Se1/0	192.168.10.1 192.168.11.1 10.0.0.1	255.255.255.0 255.255.255.0 255.255.0.0	NA
Workstation PC1	NIC	15.0.0.6	255.0.0.0	15.0.0.1
Workstation PC2	NIC	15.0.0.7	255.0.0.0	15.0.0.1
IOT Security Server	NIC	192.168.0.11	255.255.255.0	192.168.0.2
Security Wireless Router	NIC	192.168.0.2	255.255.255.0	192.168.0.2
File Server	NIC	15.0.0.9	255.0.0.0	15.0.0.1
Mail exchange Server	NIC	15.0.0.2	255.0.0.0	15.0.0.1
Web Security server	NIC	15.0.0.3	255.0.0.0	15.0.0.1
FTP server	NIC	15.0.0.4	255.0.0.0	15.0.0.1
Database Security server	NIC	15.0.0.5	255.0.0.0	15.0.0.1
Router 3	Se1/0 Se1/1 Se1/2 Fa0/0	10.0.0.2 192.168.13.3 192.168.17.7 192.168.14.4	255.255.0.0 255.255.255.0 255.255.255.0 255.255.255.0	NA
Router 1	Fa0/0 Se1/0	192.168.12.1 192.168.13.2	255.255.255.0 255.255.255.0	NA
Router 2	Fa0/0 Se1/0	192.168.19.9 192.168.17.8	255.255.255.0 255.255.255.0	NA
IT IOT Server	NIC	192.168.12.2	255.255.255.0	192.168.12.1
IT Wireless Router	NIC	192.168.12.10	255.255.255.0	192.168.12.2
HR Email Server	NIC	192.168.14.120	255.255.255.0	192.168.14.4
Email Router	Gig0/0 Gig0/1	192.168.4.3 192.168.3.1	255.255.255.0 255.255.255.0	NA
Accounts Router	Fa0/0 Fa0/1	192.168.5.3 192.168.4.1	255.255.255.0 255.255.255.0	NA
HR-manager PC	NIC	192.168.14.5	255.255.255.0	192.168.14.4
Performance& Development IP	NIC	192.168.14.6	255.255.255.0	192.168.14.4
Ticket counter IP Phone	Vlan 1	192.168.10.2	255.255.255.0	192.168.10.1
IP phone 2	Vlan 1	192.168.10.3	255.255.255.0	192.168.10.1
PC1	NIC	192.168.10.6	255.255.255.0	192.168.10.1

Implementation and Configuration

Router Configuration:

In Router 0 and 3, we configured the interfaces in the CLI as shown in the figure7and 8 below.

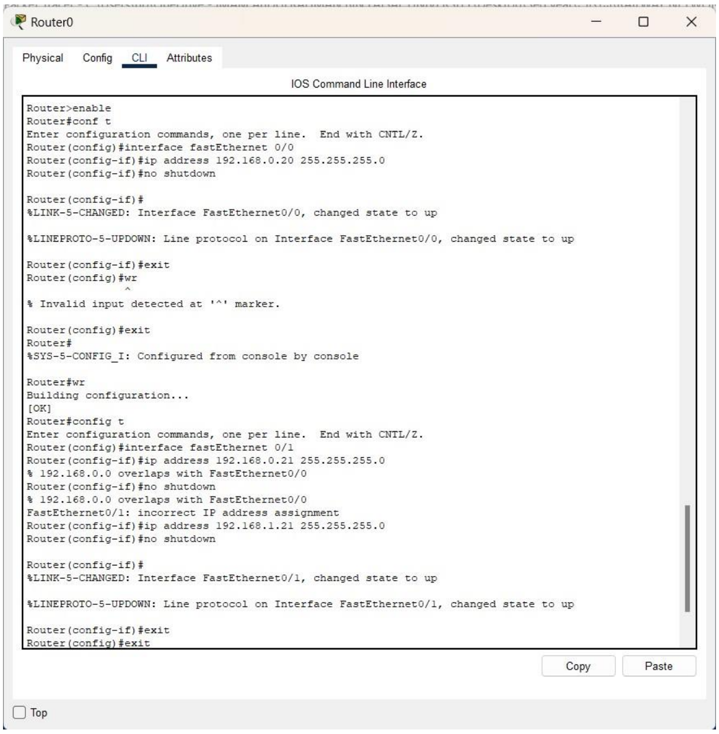


Figure 7

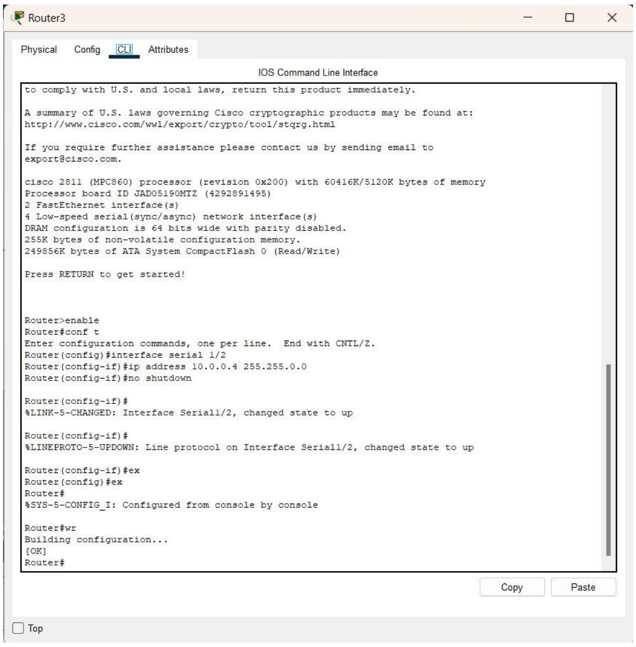
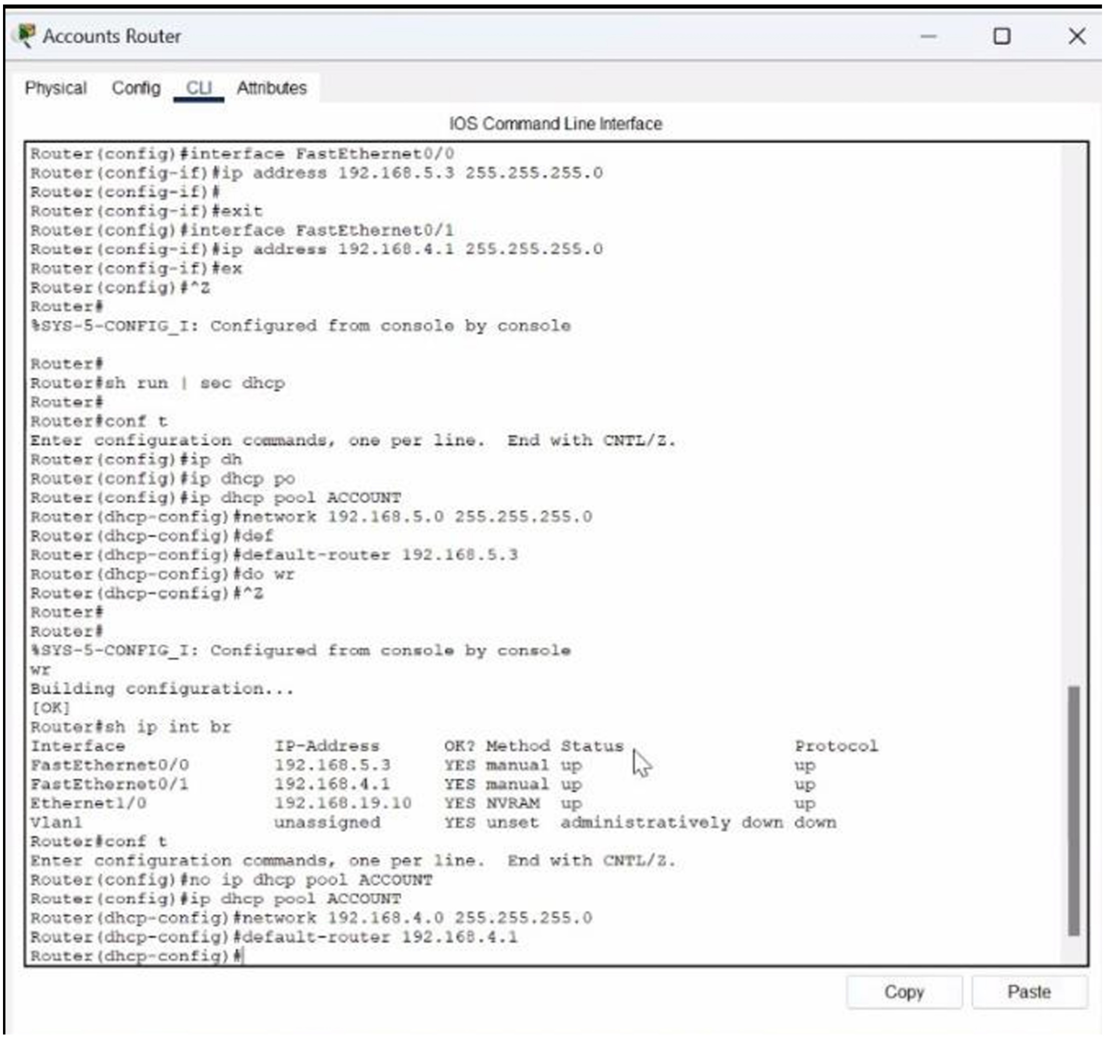


Figure 8

DHCP Protocol:

Her in figure 9 In the accounts router we used the DHCP protocol to facilitate assigning addresses to the devices.




```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.5.3 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#ex
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#sh run | sec dhcp
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dh
Router(config)#ip dhcp po
Router(config)#ip dhcp pool ACCOUNT
Router(dhcp-config)#network 192.168.5.0 255.255.255.0
Router(dhcp-config)#def
Router(dhcp-config)#default-router 192.168.5.3
Router(dhcp-config)#do wr
Router(dhcp-config)#^Z
Router#
Router#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Router#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.5.3     YES manual up                    up
FastEthernet0/1        192.168.4.1     YES manual up                    up
Ethernet1/0            192.168.19.10   YES NVRAM  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip dhcp pool ACCOUNT
Router(config)#ip dhcp pool ACCOUNT
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.4.1
Router(dhcp-config)#
```

Figure 9

RIP Protocol:

In the figure10 below the steps of using the RIP protocol in router 0 to success the ping between all the departments.

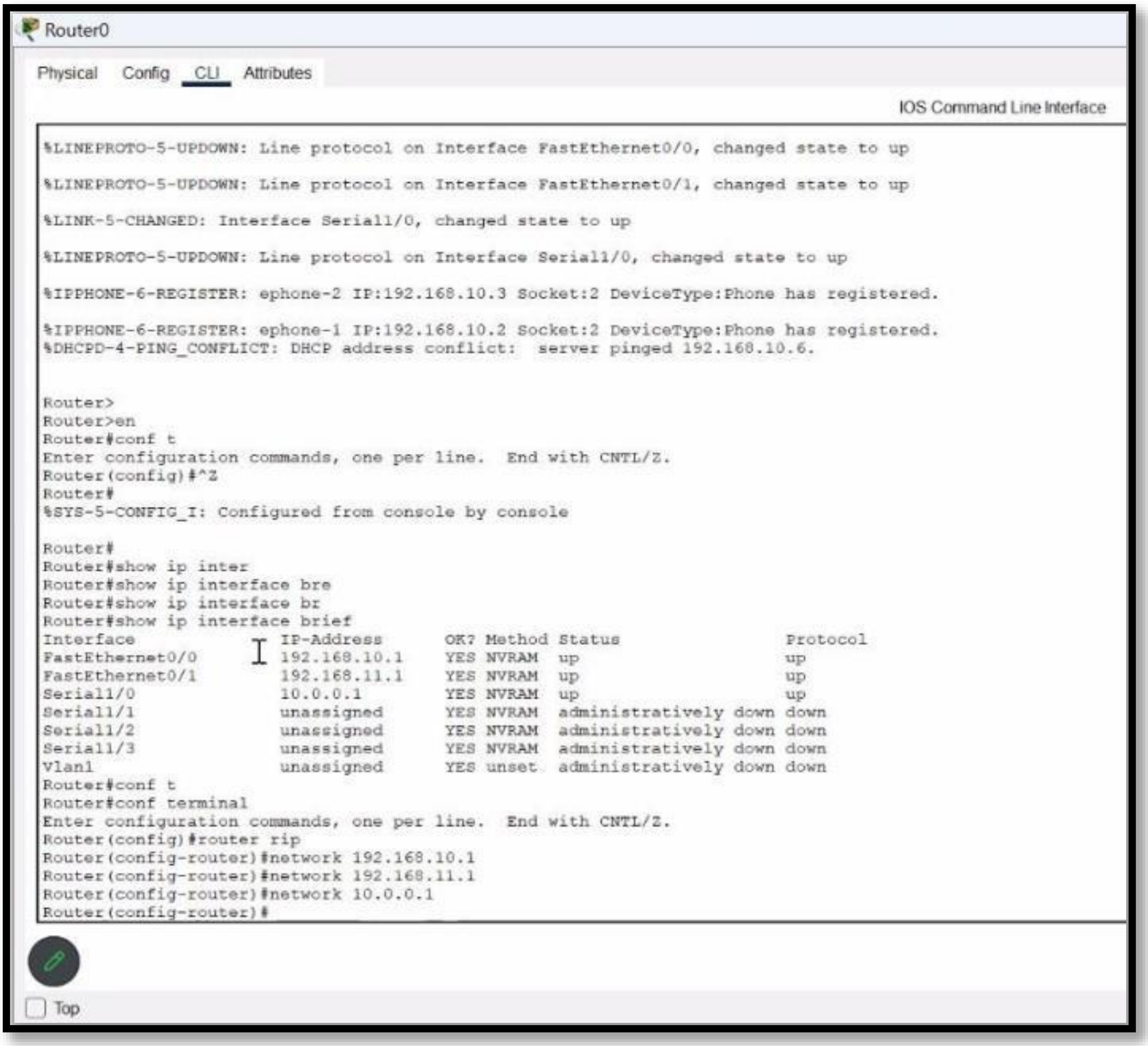


Figure 10

OSPF Protocol:

In the figure11 below the configure of OSPF protocol in Router 3 to success the ping between departments. finale we verify it by show IP route from Account router in figure 12. We did the same in router 0,1,2 and Multilayer Switch.

```
Router(config)#router ospf 1
Router(config-router)# log-adjacency-changes
Router(config-router)# network 192.168.14.0 0.0.0.255 area 0
Router(config-router)# network 192.168.13.0 0.0.0.255 area 0
Router(config-router)# network 192.168.17.0 0.0.0.255 area 0
```

Figure 11

Accounts Router

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/16 is subnetted, 1 subnets
O       10.0.0.0/16 [110/138] via 192.168.19.9, 00:04:23, Ethernet1/0
O    15.0.0.0/8 [110/140] via 192.168.19.9, 00:04:13, Ethernet1/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, FastEthernet0/1
L       192.168.4.1/32 is directly connected, FastEthernet0/1
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, FastEthernet0/0
L       192.168.5.3/32 is directly connected, FastEthernet0/0
O    192.168.10.0/24 [110/139] via 192.168.19.9, 00:04:13, Ethernet1/0
O    192.168.11.0/24 [110/139] via 192.168.19.9, 00:04:13, Ethernet1/0
O    192.168.12.0/24 [110/139] via 192.168.19.9, 00:03:04, Ethernet1/0
O    192.168.13.0/24 [110/138] via 192.168.19.9, 00:12:24, Ethernet1/0
O    192.168.14.0/24 [110/75] via 192.168.19.9, 00:12:24, Ethernet1/0
O    192.168.17.0/24 [110/74] via 192.168.19.9, 00:12:24, Ethernet1/0
     192.168.19.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.19.0/24 is directly connected, Ethernet1/0
L       192.168.19.10/32 is directly connected, Ethernet1/0
```

Figure 12: To verify show IP route from Account router.

Comparison between RIP and OSPF

Routing protocols are essential for exchanging information between routers and enabling efficient data transmission across networks.

Two of the most used routing protocols are RIP (Routing Information Protocol) and OSPF (Open Shortest Path First).

While both protocols serve the same purpose, they differ significantly in their approach and are suited for different network types.

Here is our result for both protocols in our network:

	RIP	OSPF
Paket loss	0	0
CPU Utilization	1.3%	1.8%
Memory Usage	533.8 MB	609.4 MB

Passwords on Switch:

We set “switchTicket” for the user password in figure13 and15 and set “enterSwitch” for the console password in figure 14, then we encrypted both of them so when someone write show running config command as shown in figure 16, he cannot know the passwords.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password enterSwitch
Switch(config)#exit
```

Figure 13.

```
Switch>enable
Password:
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable secret enterSwitch
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
Switch(config)#exit
```

Figure 14.

```
Switch>
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#login
% Login disabled on line 0, until 'password' is set
Switch(config-line)#password switchTicket
Switch(config-line)#exit
Switch(config)#exit
```

Figure 15.

```
User Access Verification

Password:

Switch>enable
Password:
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#service passwoed-encryption
                                 ^
% Invalid input detected at '^' marker.

Switch(config)#service password-encryption
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show running config
                    ^
% Invalid input detected at '^' marker.

Switch#show running-config
Building configuration...

Current configuration : 2391 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$2Lct3ZUM83rTUn0PaKYT1/
enable password 7 0824425A0C0B36001B1F0F0C
!
!
!
!
!
```

Figure 16.

Vlan on Switches:

Here in figure 17, we activate vlan 15 on all switches in the security department to facilitate and succeed in sending messages from and to this department.

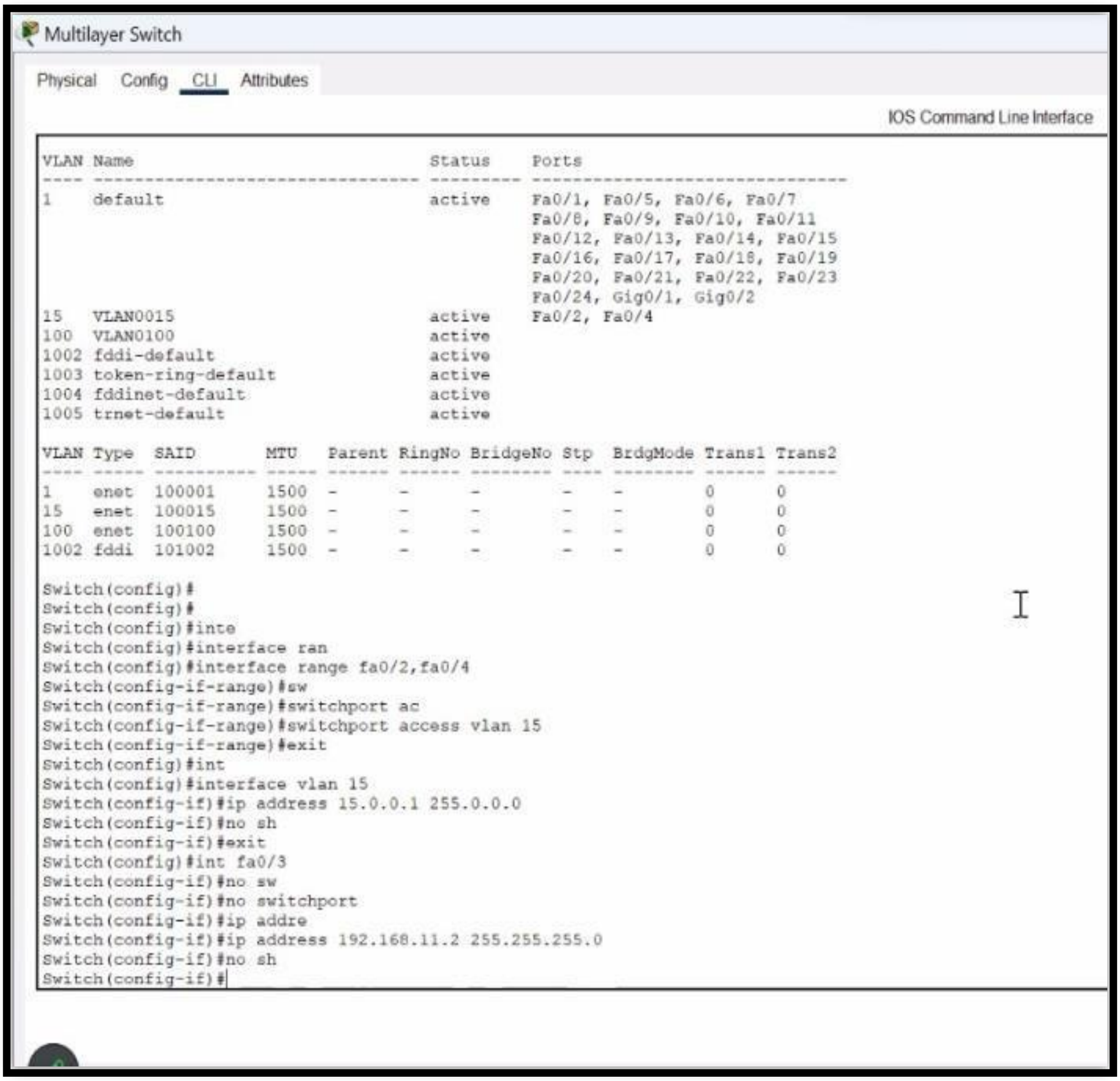


Figure 17.

IP Phone configuration:

We used 3 Ip phones, 2 of them are in the Ticket counter department for people who want to buy an online ticket, and the third is in the HR department so when they need to call someone outside the railway. The configuration is done on the router0 figure 18 and switch CLI figure 19.

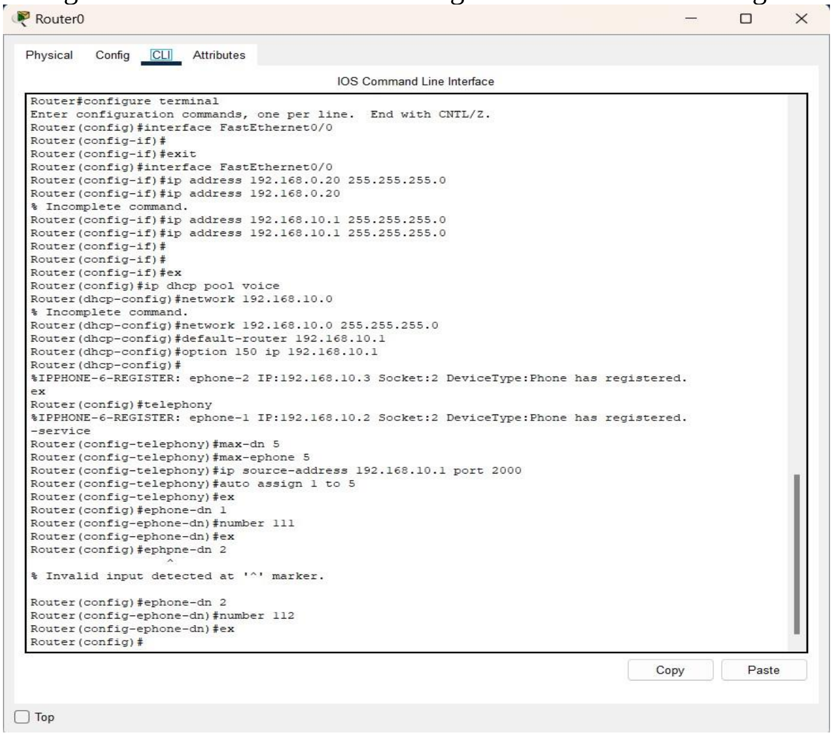


Figure 18.

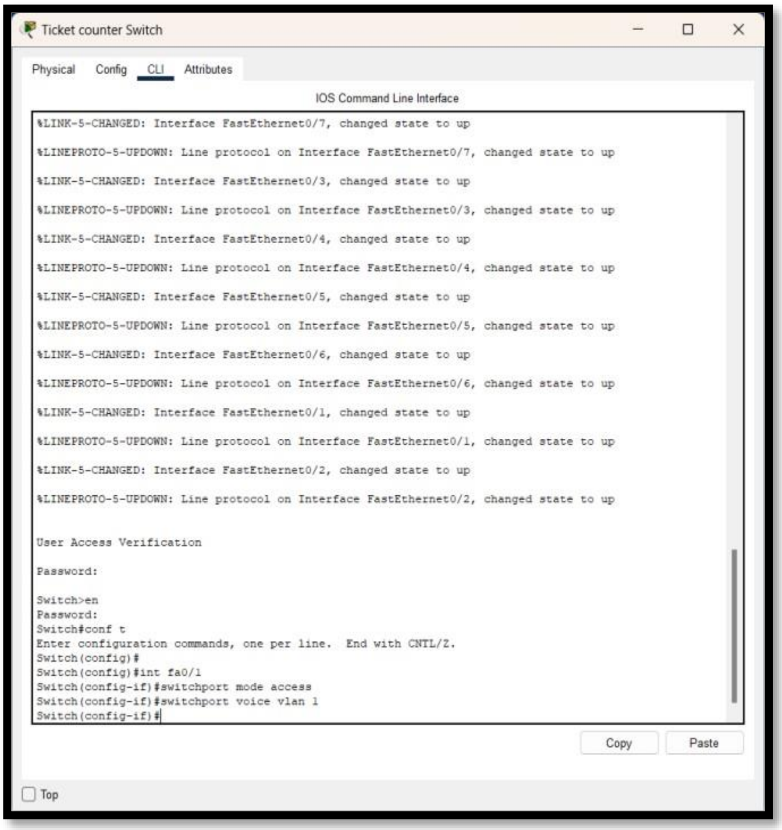


Figure 19

Telnet:

In the HR department, we used the telnet service to reduce the number of devices that can access and control the switch as shown in figure 20.

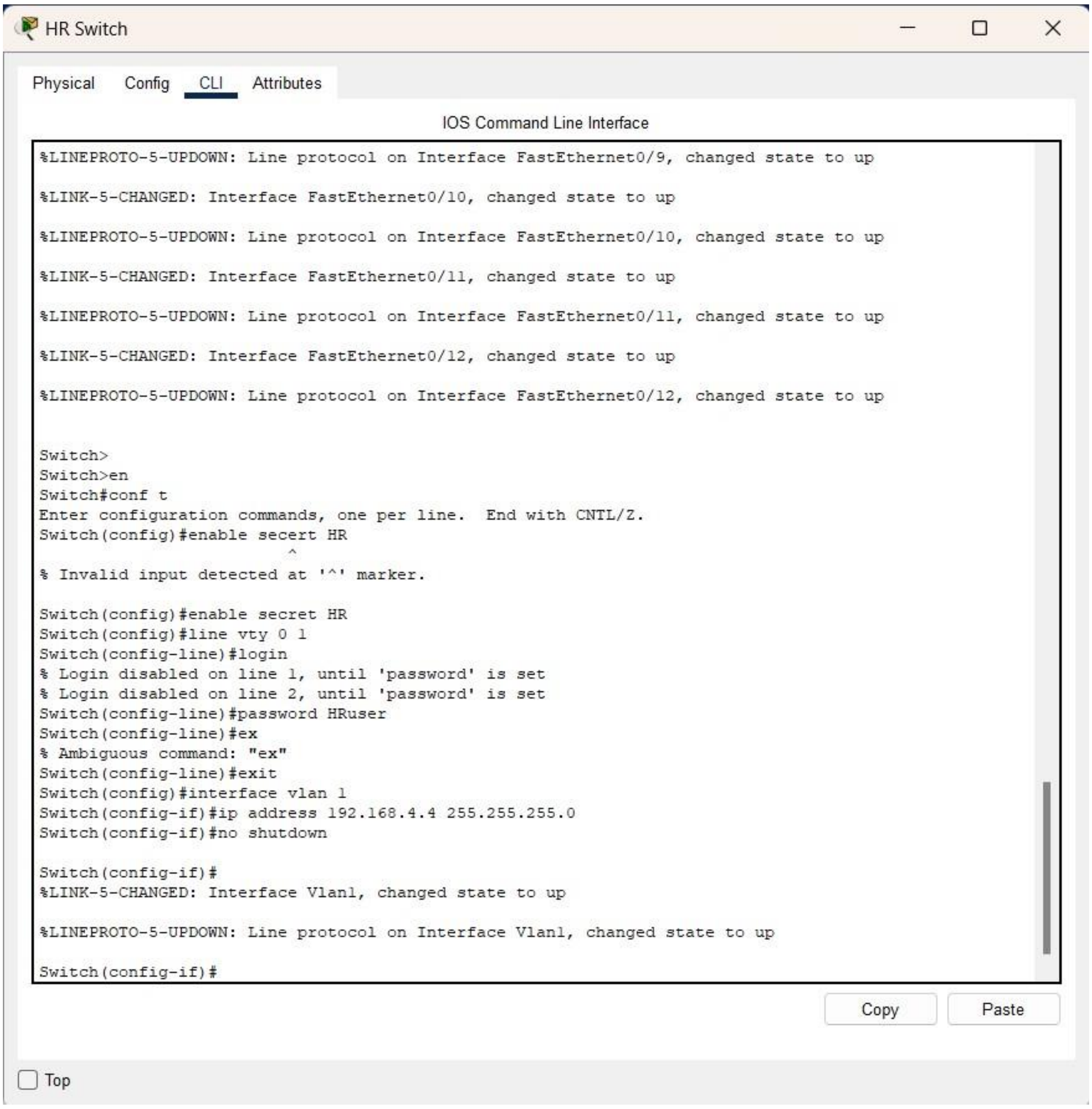


Figure 20.

Firewalls:

In securing our network and increasing efficiency from outsiders and hackers, we set up one default firewall as we can see in figure 21. It is inside the database server directly.

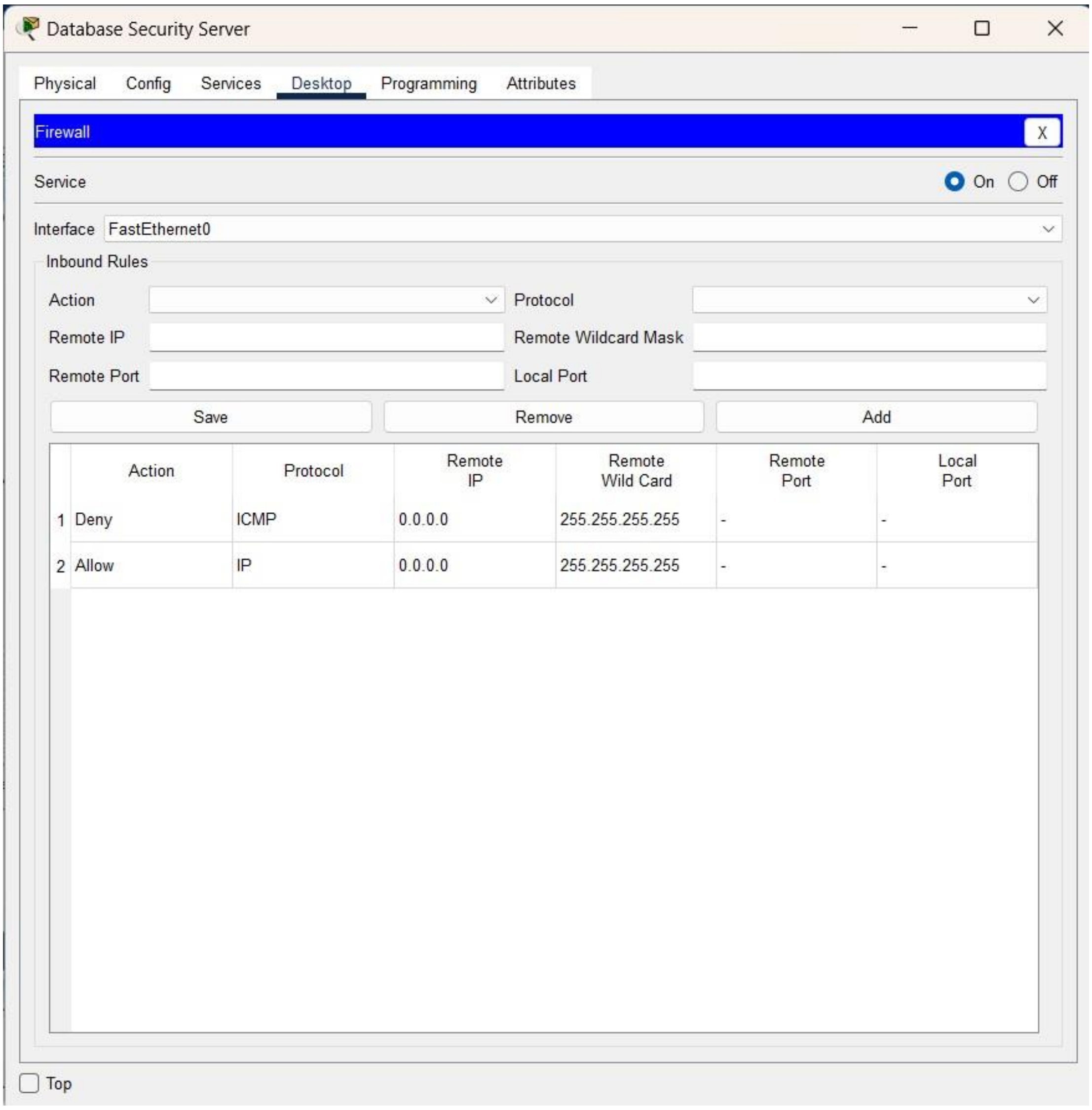


Figure 21.

Email:

In the HR department we decided to activate the Email service as shown in figure 22 to facilitate communication between the employees. Here's in Figure 23 an example on one of the employee PC.

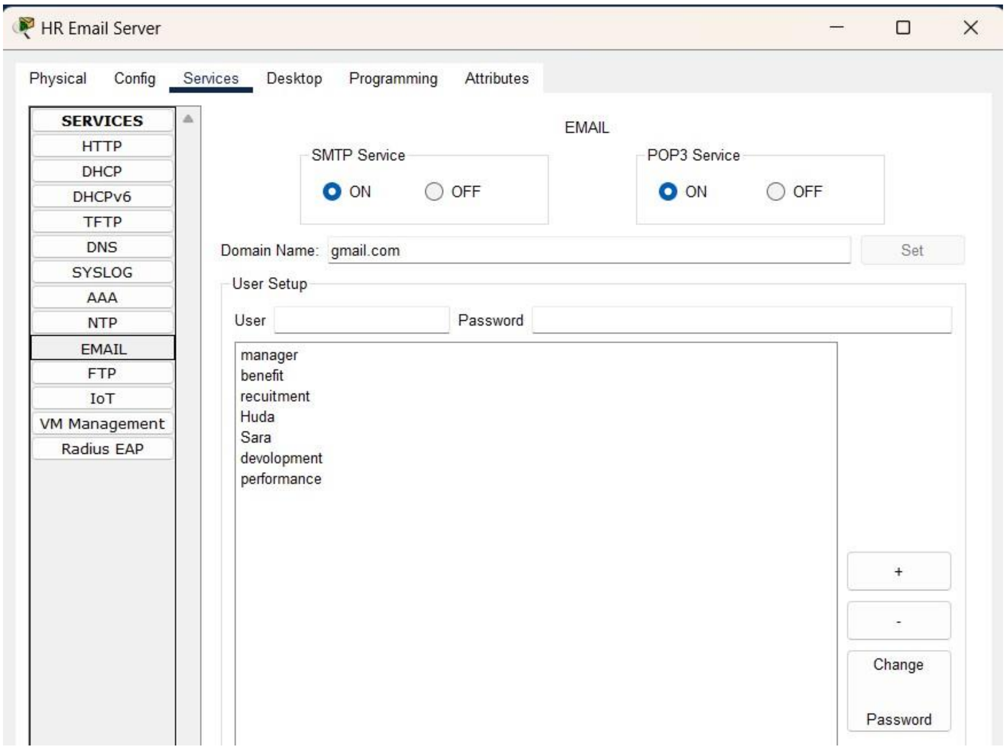


Figure 22

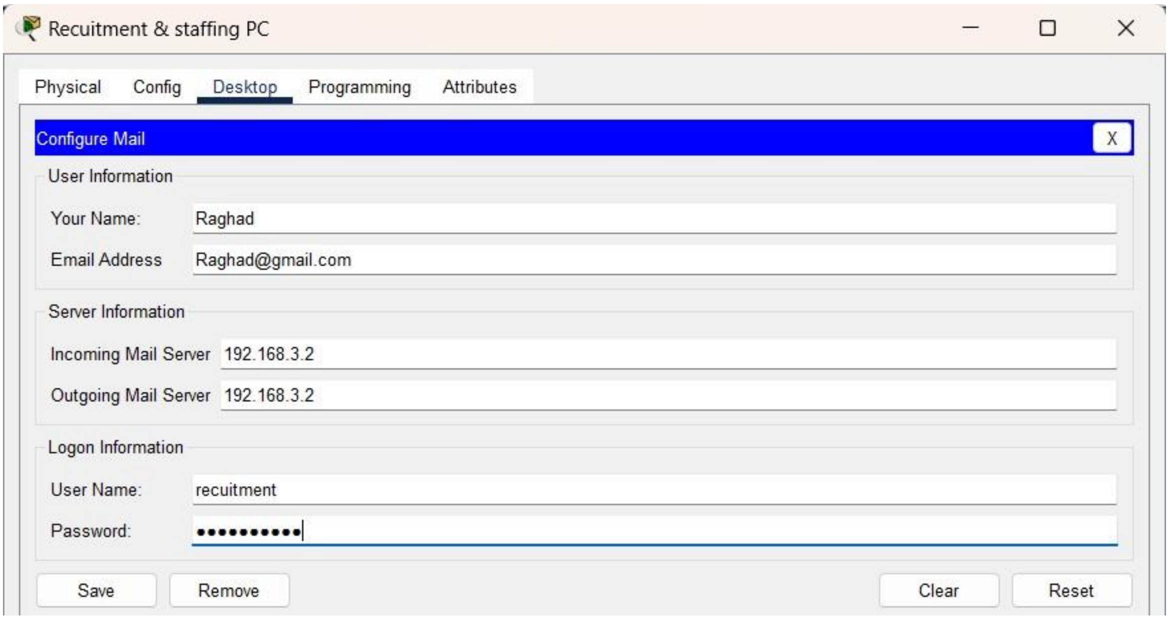


Figure 23

AAA service:

We used AAA service figure 24 in the server to make an effective connection in the Security and IT departments between the wireless router figure 25 and the IOT devices like the door and motion detector.

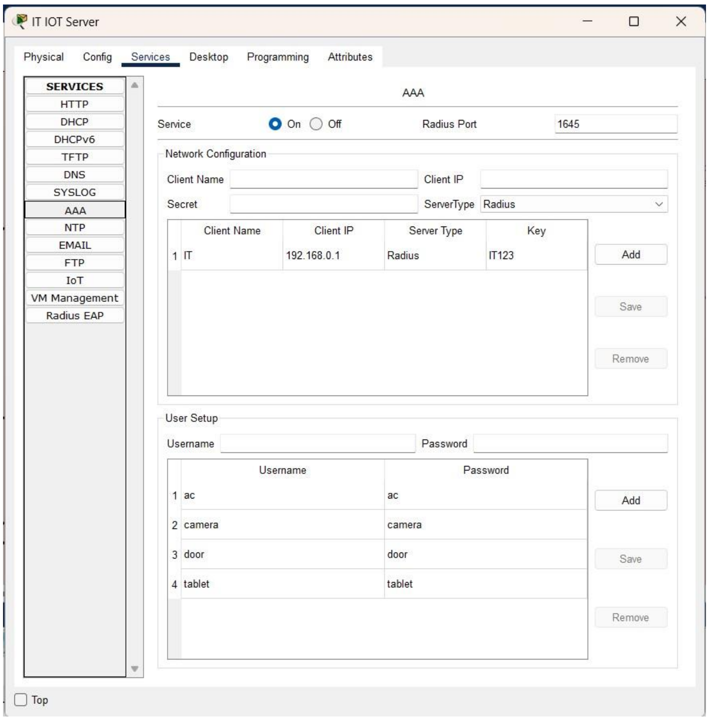


Figure 24: IT IOT Service.

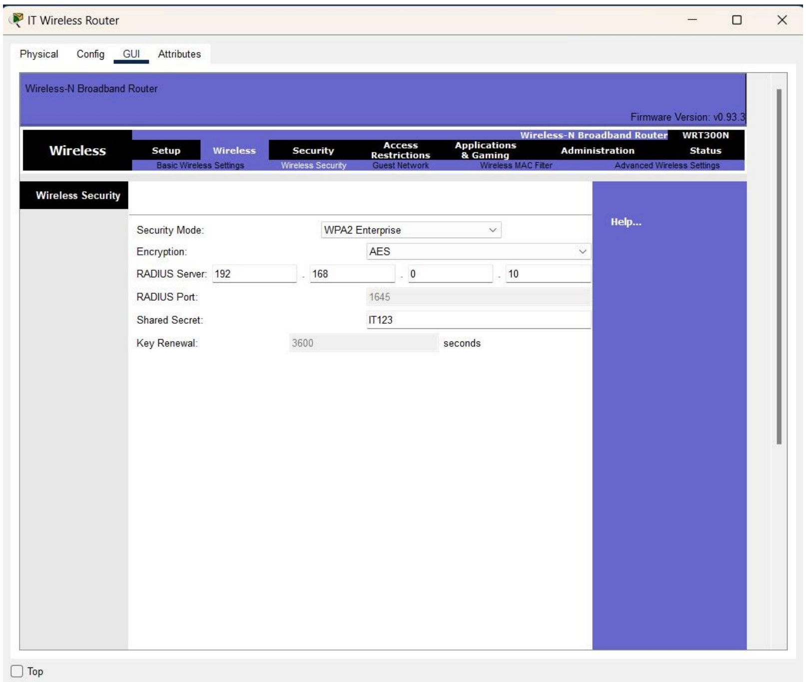
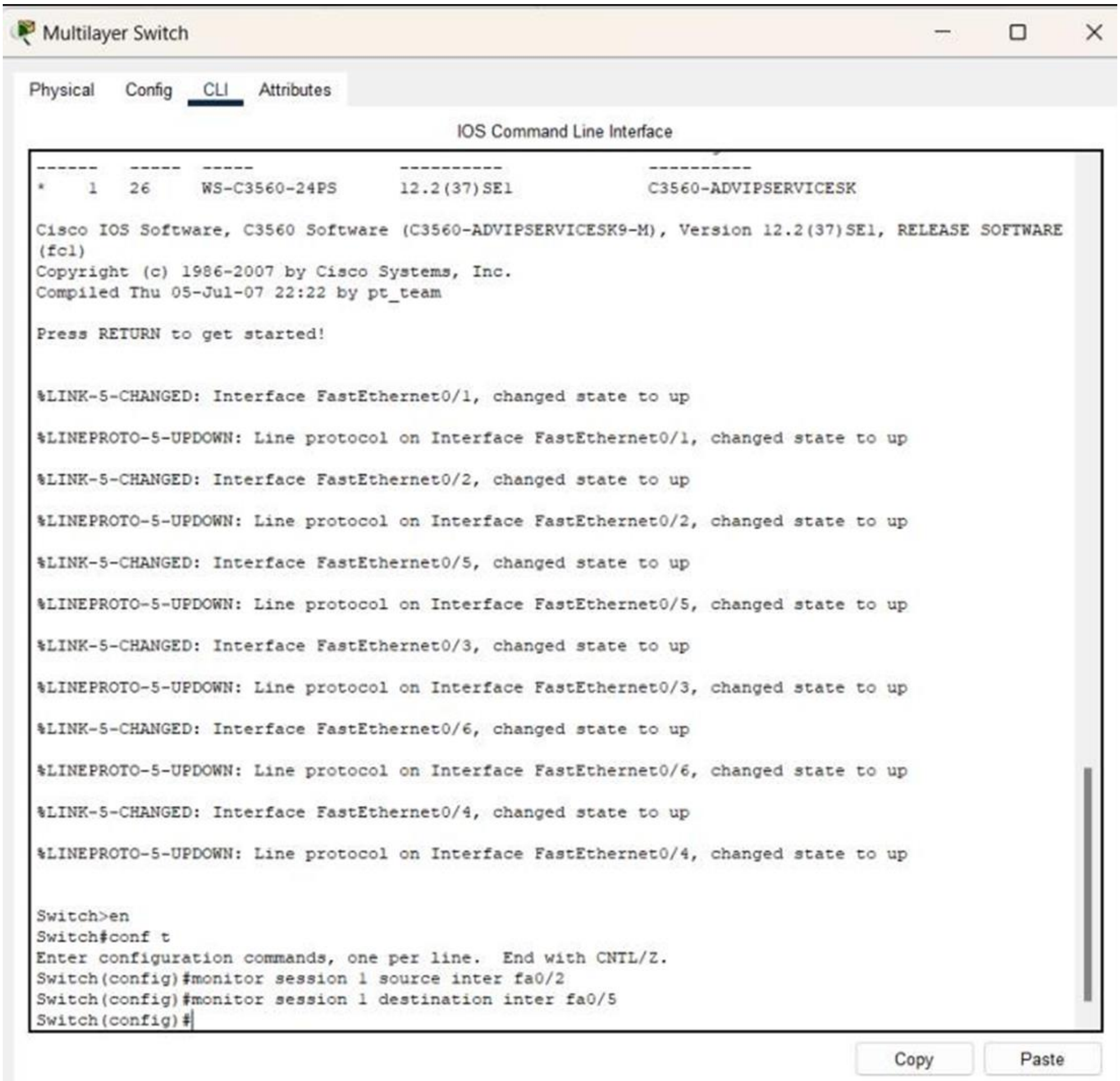


Figure 25: IT Wireless Router.

Sniffer:

To monitor incoming and outgoing messages from any device to any device with precise details, we set up a sniffer in the Security department as shown in figure 26.




```
------  -----  -----         ----------            ----------
*    1   26     WS-C3560-24PS       12.2(37)SE1           C3560-ADVIPSERVICESK

Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source inter fa0/2
Switch(config)#monitor session 1 destination inter fa0/5
Switch(config)#
```


Figure 26

Simulations and Results:

In these figures below a simple simulation of the services we used and explained before.

- In this figure 27 below, the status of the messages sent and delivered is a success exceptfor the first status because we set a firewall on the server.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Workstation PC2	Database Security Server	ICMP		0.000	N	7	(edit)	(delete)
	Successful	Recuitment & staffing PC	staff 1 PC	ICMP		0.000	N	8	(edit)	(delete)
	Successful	IT manager PC	Problem solving Laptop 2	ICMP		0.000	N	9	(edit)	(delete)
	Successful	HR-manager PC	performance Mgt & developme	ICMP		0.000	N	10	(edit)	(delete)

Figure 27

- Here is the Ip phone simulation as it is ringing to the other one.

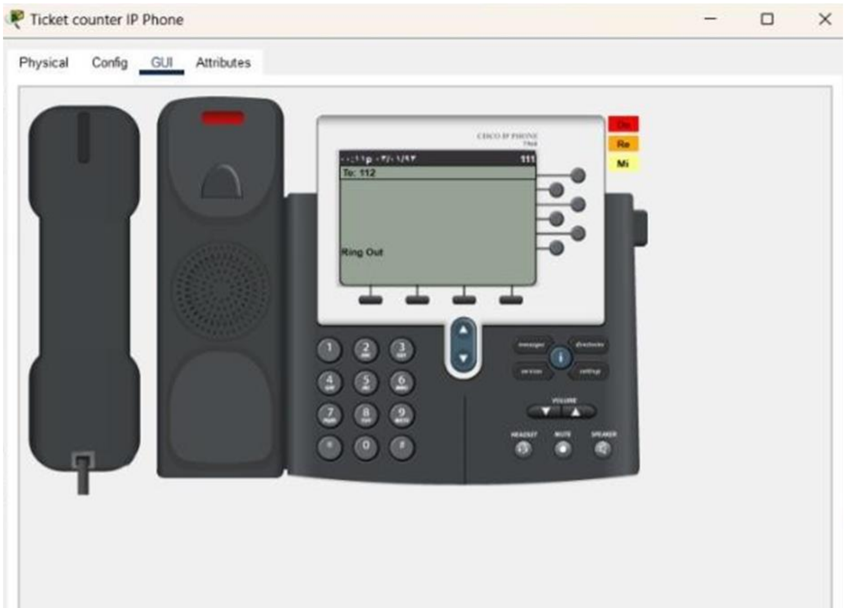


Figure 28

- The command prompt below is for the Telnet service from one of the authorized PC in figure 29.

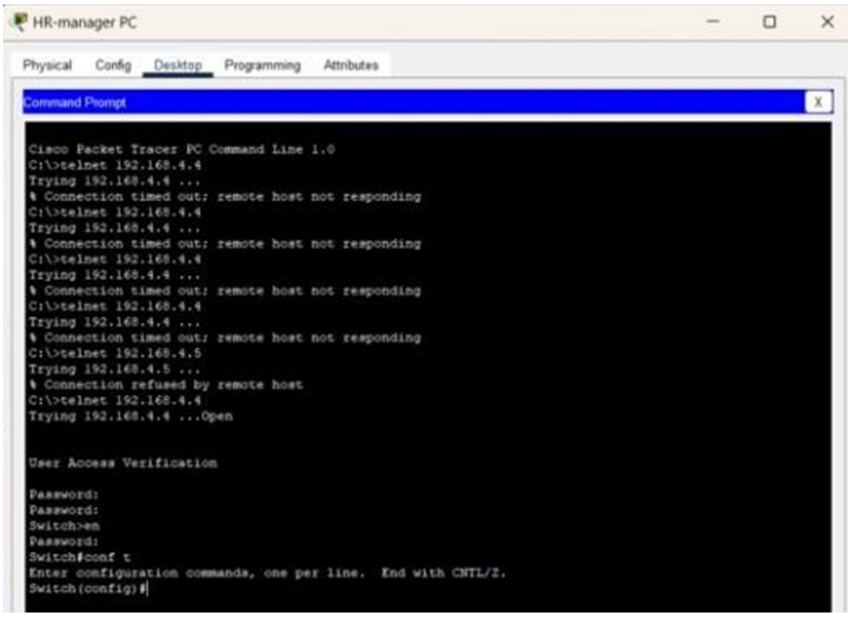


Figure 29

- The two next figures 30,31 are about the Email service, sending and receiving.

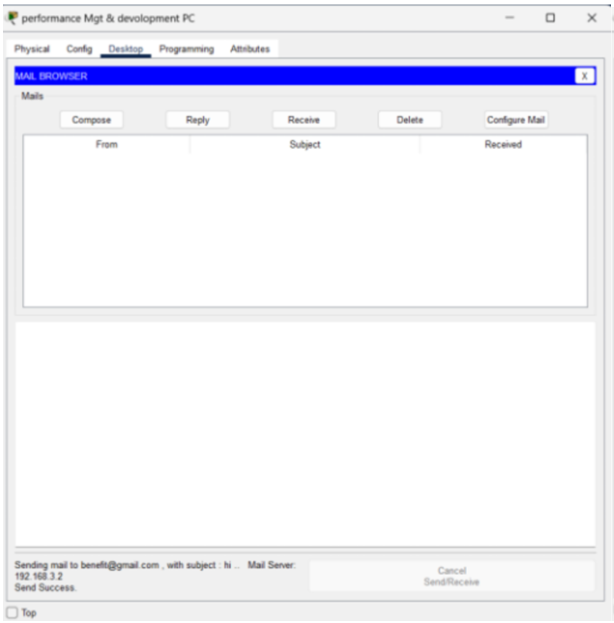


Figure 30

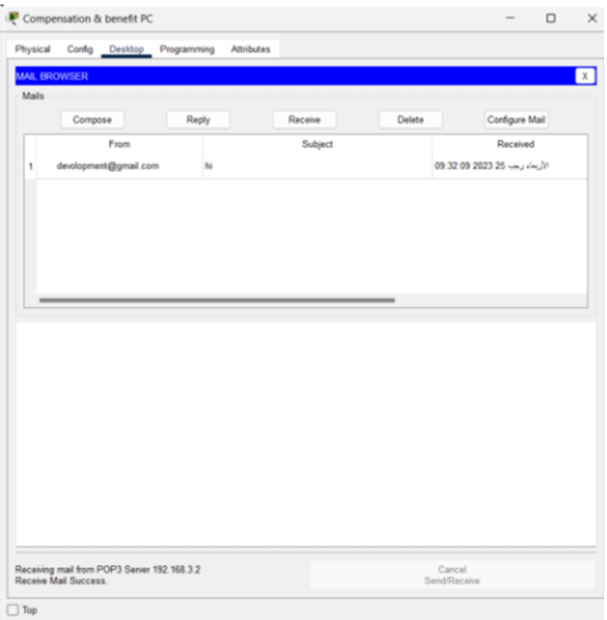


Figure31

- The Configured IOT devices by the wireless router and a server are controlled by a tablet as shown in figure 32.

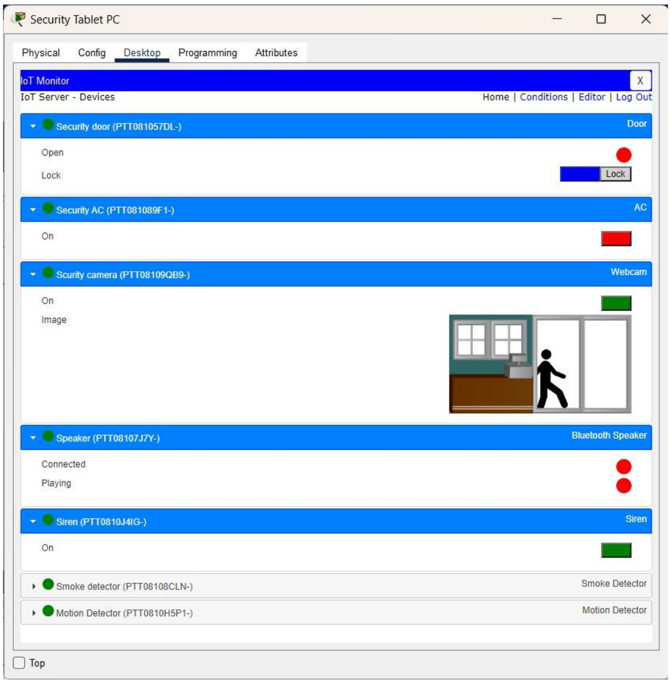


Figure 32

- Down below in figure 33 is a simple simulation of the sniffer work.

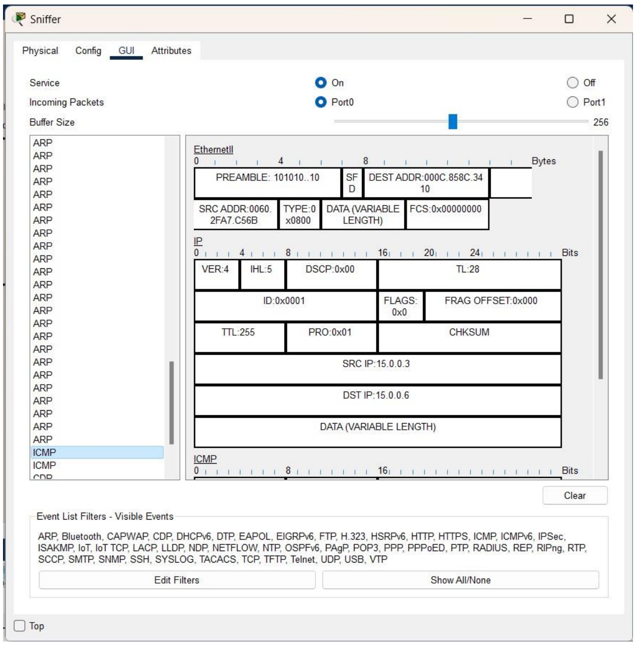


Figure 33

Future Work:

Our project aspires to development in the future, and one of the most important developments that we seek to achieve is increasing the efficiency of the devices within the railway network. As well as facilitating communication to become more flexible between railway sections, with diversity in the use of topology So that each topology carries modern and distinctive technologies that help in the success of the network and make it easy to use and serve the railway.

Conclusion:

The project ensures the development of one of the most important developments on the railway networks. prepare a secure and effective network for the railway due to multiple attacks or terminating it for specific purposes by using routing protocols commonly used in today's networks: RIP. The Inside Railway server has been implemented to manage the work of the network and the internal network database in a better and accurate way, and this is the most important thing that will preserve the data. Firewall administration is an important topic in network security courses providing protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. At the end we did a comparison between the two protocols to see the differences and what will happened.

References:

[1] Almalki, F. A. (2020). Implementation of 5G IoT based smart buildings using VLAN configuration via cisco packet tracer. International Journal of Electronics Communication and Computer Engineering, 11(4), 56-67.

[2] Basic Switch Configuration in Cisco. (2022, June 22). GeeksforGeeks.

[3] Deepa, T. P. (2018). Simulating of internet surveillance using packet tracer. International Journal of Scientific Research in Computer Science, Engineering, and Information Technology, 3(3), 1288-1295.

[4] Gwangwava, N., & Mubvirwi, T. B. (2021). Design and simulation of IoT systems using the Cisco packet tracer. Advances in Internet of Things, 11(02), 59.

[5] How to Create Web Server On Packet Tracer. (2022, November 22). GeeksforGeeks.

[6] Implementing Local Area Network for a New HR Department in EMU. (2023, October 30).

[7] Kimanzi, S. (2020, March 19). Configuring Telnet on a switch and a router in Packet Tracer. Computer Networking Tips.

[8] Kurniati, K., & Dasmen, R. N. (2019). The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang. Lontar Komputer Jurnal Ilmiah Teknologi Informasi, 10(1), 49-61.

[9] Packet Tracer 8.1.1 tutorial - IP telephony basic configuration - Packet Tracer Network. (2023, May 4). Packet Tracer Network.

[10] Performing a sniffer trace or packet capture | Administration Guide.

[11] Rahman, M. A., & Kabir, A. I. (2023). A network design and simulation of a Smart Railway Station using Cisco Packet Tracer.

[12] Raj, J. S., & Basar, D. A. (2019). QoS optimization of energy efficient routing in IoT wireless sensor networks. Journal of IoT in Social, Mobile, Analytics, and Cloud, 1(1), 12-23