ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

UNIVERSIDAD

Computing Networks

Laboratory No. 8

Data Link Layer and Application Layer

Students:

Andrea Camila Torres González

Jorge Andrés Gamboa Sierra

Presented to:

Fabian Eduardo Sierra Sánchez

Semester 2024-2

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

UNIVERSIDAD

Content

Abstract

The development of dynamic web applications, network management, and wireless configuration is fundamental in modern information technology. This document explores the theoretical and practical aspects of configuring basic WiFi networks, setting up dynamic web services on Apache servers, and utilizing essential network management commands on platforms like Slackware, Solaris, and Windows Server. The project includes building a dynamic PHP-based web application that functions as a grade calculator. Additionally, the study emphasizes the importance of understanding network diagnostics through commands such as ifconfig, netstat, and route, presented in an automated shell script. Practical tasks also include configuring VLANs, analyzing wireless traffic with tools like WiFi Analyzer, and deploying WiFi networks with WPA2 security. The results demonstrate an integrative approach to system and network administration, dynamic web development, and the interplay between wired and wireless networks in diverse environments.
Key words: switch, wireless router, wifi, monitoring, deployment

Objective

Review the operation of Ethernet and WiFi networks.

Review the operation of interconnection devices.

Continue installing application layer services.

Tools to be Used

Computers

Virtualization software

Internet access

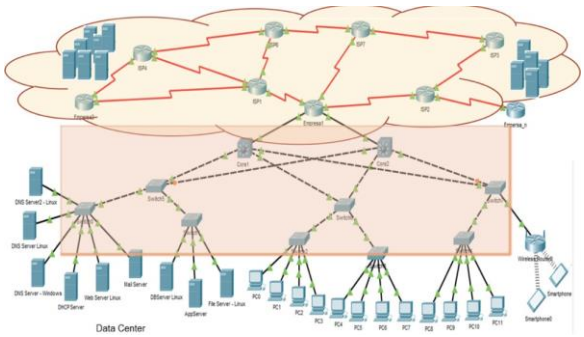
Switches

Packet Tracer

Wireshark

Introduction

We are still working on the infrastructure of a company, which typically includes several IT infrastructure services. It consists of wired and wireless user workstations and servers (both physical and virtualized),all connected through switches (Layer 2 and Layer 3), wireless devices, and routers that connect it to the Internet. It is also common to have cloud infrastructures where resources are provisioned based on the organization's needs. Among the servers, one can find web services, DNS, email, databases, storage, and applications, among others. Let's recall the baseline configuration we are using:



In this part of the lab, we will focus on the LAN infrastructure and other application layer protocols.

Theoretical Framework

1. Dynamic Web Applications

Dynamic web applications are a cornerstone of modern web development. Unlike static web pages that deliver pre-written content to users, dynamic applications respond to user input and retrieve or modify data in real-time. This adaptability makes them ideal for tasks such as managing user accounts, calculating grades, and generating reports.

Key Components:

- Server-Side Scripting: Technologies like PHP, Node.js, or Python enable the server to process logic, interact with databases, and dynamically generate HTML.
- Database Integration: Relational databases, such as PostgreSQL, store structured data in tables. SQL commands allow efficient querying, updating, and deletion of data.
- Web Servers: Apache is a widely used HTTP server that supports the execution of PHP scripts, acting as the intermediary between user requests and server-side logic.

Applications: Dynamic web services are integral to educational systems for tasks such as:

1. Grade Calculation Systems: These automate the computation of student grades based on predefined weightings, such as 30%, 30%, and 40%.
2. Database-Driven Applications: Storing and retrieving student records ensures data persistence, accessibility, and scalability.

2. Wireless Networking

Wireless networking is critical for connecting devices without physical cables, using radio waves to establish communication. Understanding its configuration and management ensures optimal network performance and security.

Key Concepts:

- **SSID and Security:**
  - The Service Set Identifier (SSID) identifies a WiFi network, allowing devices to connect to the correct access point.
  - WPA2-PSK with AES encryption offers robust security, protecting networks against unauthorized access and data interception.
- **Channels:**
  - Wireless routers operate on frequency bands (e.g., 2.4 GHz, 5 GHz). Channels within these bands define specific frequency ranges.
  - Selecting non-overlapping channels minimizes interference, particularly in environments with multiple WiFi networks.

Tools:

- **WiFi Analyzer:**
  - Scans for active networks, identifying SSIDs, channels, and signal strengths.
  - Assists in troubleshooting issues like overlapping channels or weak signals.

Practical Implementation: Setting up a secure wireless network involves configuring IP ranges (e.g., DHCP from 192.168.0.20 to 192.168.0.30), assigning unique channels, and testing connectivity with mobile devices.

3. Network Diagnostics and Management

Effective network management requires tools to monitor, troubleshoot, and optimize connectivity. This is especially crucial for cross-platform environments like Slackware Linux, Solaris, and Windows Server.

Core Tools:

1. ifconfig: Displays and configures network interfaces. Useful for verifying IP assignments and link statuses.
2. netstat: Provides information about network connections, routing tables, and interface statistics.
3. vnstat: Monitors bandwidth usage over time, helping administrators analyze network performance.
4. route: Displays and modifies the routing table, showing how packets travel across the network.
5. ethtool: Retrieves hardware information, such as link speed and duplex settings.

Shell Scripting: Automating these commands into a menu-driven script simplifies diagnostics for users. For example:

- Viewing all active connections.
- Monitoring real-time bandwidth usage.
- Inspecting routes and troubleshooting network failures.

4. Integration of Wired and Wireless Networks

Combining wired and wireless networks ensures seamless communication between devices, enhancing flexibility and scalability.

Key Aspects:

- DHCP (Dynamic Host Configuration Protocol):
  - Dynamically assigns IP addresses, reducing manual configuration.
  - Ensures devices have unique IPs within the defined range (e.g., 192.168.0.X to 192.168.0.Y).
- VLANs (Virtual Local Area Networks):
  - Logically segment networks within the same physical infrastructure.
  - Improve security and reduce congestion by isolating traffic based on roles or groups.
- Ping Testing:
  - Verifies device connectivity within the network and to external destinations.
  - Identifies potential routing or firewall issues.

5. Practical Wireless Applications

Wireless networks are increasingly used in homes, offices, and public spaces. Their configurations vary based on use case:

1. Lab Configurations:
   - Secure networks for student projects, often requiring SSID customization and WPA2-PSK encryption.
   - Testing connectivity with tools like WiFi Analyzer ensures reliable performance.
2. Home Networks:
   - Bandwidth and channel optimization reduce interference from nearby networks.
   - Compatibility with devices like smartphones and smart home gadgets.
3. Advanced Features:
   - Disabling beacon frames (SSID broadcast) for security testing.
   - Verifying network visibility and accessibility in low-profile configurations.

6. NAT and Internet Connectivity

Network Address Translation (NAT) plays a vital role in enabling internet access for devices on private networks. It translates private IP addresses (e.g., 192.168.x.x) to a public IP for outbound traffic. Challenges in NAT configurations can impact connectivity and ping success rates

7. Why is VLAN 1 the default VLAN?

VLAN 1 is the default VLAN in many networking devices, such as switches, due to its designation as the standard VLAN in Ethernet protocols and devices, particularly in Cisco equipment. By default, when a switch port is configured, it is assigned to VLAN 1 unless a different VLAN is explicitly specified. VLAN 1 is used for internal communication within the switch and is typically utilized for management purposes. However, using VLAN 1 for production traffic is not recommended for security reasons. The reason VLAN 1 is the default is that it was the first VLAN defined in the standard, and many networking devices continue to maintain this default configuration.

8. What is the maximum number of VLANs?
The maximum number of VLANs possible in Ethernet networks is determined by the IEEE 802.1Q standard, which is the protocol used for VLAN tagging in Ethernet frames. According to this standard, a total of **4096 VLANs** can be defined, numbered from 0 to 4095. However, some of these VLANs are reserved for special purposes:

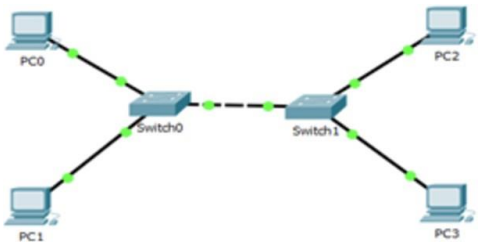
- **VLAN 0**: This VLAN is not used for regular traffic and has a specific purpose in certain implementations.
- **VLAN 4095**: This VLAN is also reserved for internal use and is not intended for user traffic.

Thus, in practice, the maximum number of VLANs available for general use in a network is 4094 (ranging from VLAN 1 to VLAN 4094).

Setup

1. Basic Switch Configuration

Perform the following setup in groups. Each pair configures a switch and their 2 PCs.



We will configure the two devices, in our case **PC2** and **PC3**, with the following network identifiers.183.24.30.193/16 and 183.30.194/16, Below is an example of the configuration for one device. For the other, the process is similar; only the device's IP address changes.

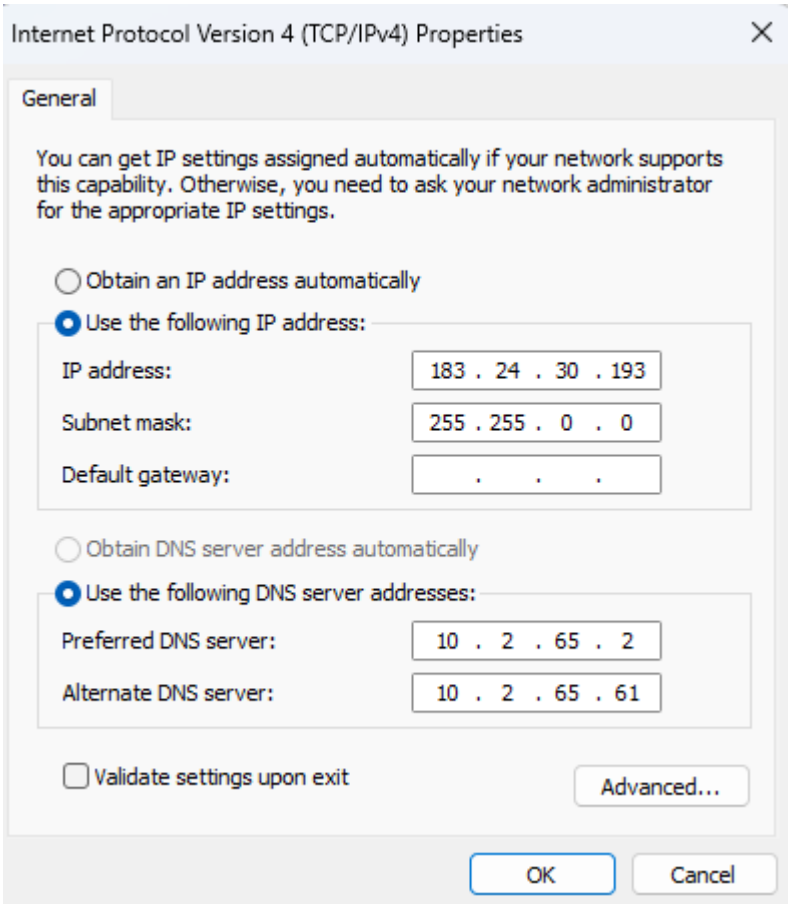


Figure 1 first PC configuration

We verify the connectivity between the computers using the ping command.

- From PC2 to PC3

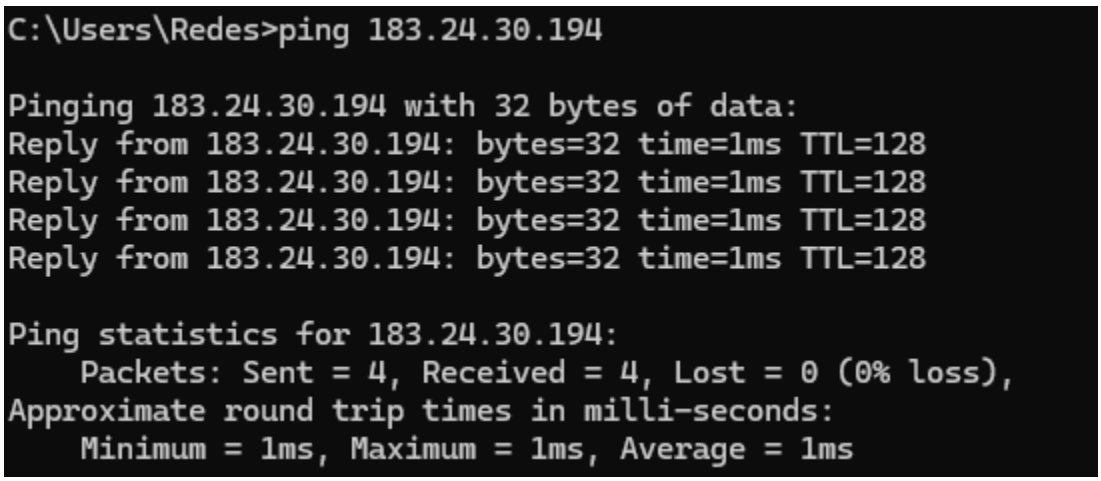


Figure 2 test ping

- From PC3 to PC2

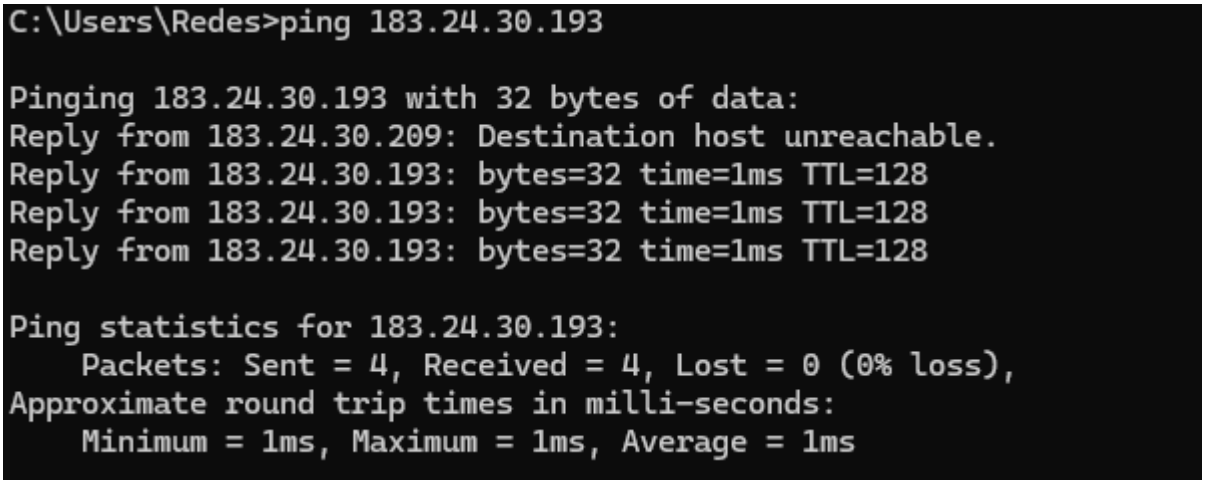


Figure 3 test ping

We Interconnect the setups of the entire group and verify that they can communicate with each other using the ping command.

```
C:\Users\Redes>ping 183.24.30.209

Pinging 183.24.30.209 with 32 bytes of data:
Reply from 183.24.30.209: bytes=32 time=1ms TTL=128
Reply from 183.24.30.209: bytes=32 time=1ms TTL=128
Reply from 183.24.30.209: bytes=32 time=1ms TTL=128
Reply from 183.24.30.209: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.30.209:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Redes>ping 183.24.30.210

Pinging 183.24.30.210 with 32 bytes of data:
Reply from 183.24.30.194: Destination host unreachable.
Reply from 183.24.30.194: Destination host unreachable.
Reply from 183.24.30.194: Destination host unreachable.
Reply from 183.24.30.194: Destination host unreachable.

Ping statistics for 183.24.30.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Redes>
```

Figure 4 test ping to the other group

We use Wireshark to capture a packet and examine the Ethernet frame. Verify the frame structure, MAC addresses, error control, etc. the name file is PC3antesVLan

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	183.24.30.194	183.24.30.209	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 2)
2	0.001156	183.24.30.209	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=128 (request in 1)
3	1.013556	183.24.30.194	183.24.30.209	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 4)
4	1.015027	183.24.30.209	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=128 (request in 3)
5	2.022871	183.24.30.194	183.24.30.209	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 6)
6	2.023951	183.24.30.209	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=128 (request in 5)
7	3.028454	183.24.30.194	183.24.30.209	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 8)
8	3.029162	183.24.30.209	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=128 (request in 7)
9	7.416652	183.24.30.194	183.24.30.210	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 10)
10	7.420311	183.24.30.210	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=128 (request in 9)
11	8.424743	183.24.30.194	183.24.30.210	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 12)
12	8.428983	183.24.30.210	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=128 (request in 11)
13	9.442764	183.24.30.194	183.24.30.210	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 14)
14	9.446034	183.24.30.210	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=128 (request in 13)
15	10.456556	183.24.30.194	183.24.30.210	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 16)
16	10.459707	183.24.30.210	183.24.30.194	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=128 (request in 15)

Figure 5 Packet Tracer screenshot

1	0.000000	183.24.30.194	183.24.30.209	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 2)

Figure 6 Analyzed packet

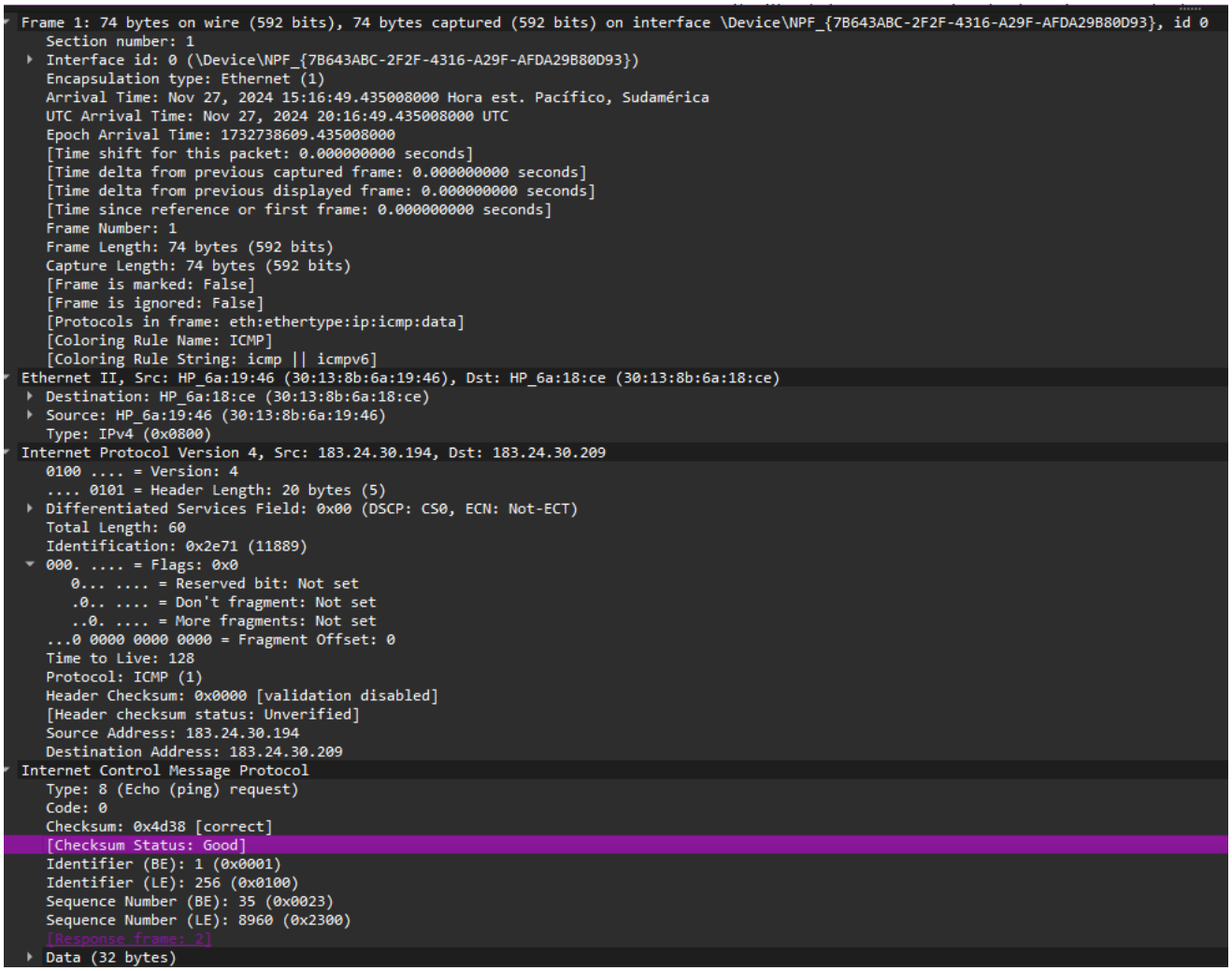


Figure 7 Packet information.

The captured packet is an ICMP "Echo Request" message (ping request), transmitted over Ethernet II, with a total size of 74 bytes (592 bits). The capture was made through the interface \Device\NPF_{7B643ABC-2F2F-4316-A29F-AFDA29B80D93}, associated with a network adapter on the device. The packet is classified under the "ICMP" coloring rule in Wireshark, indicating that it is part of a network control protocol used for connectivity verification.

At the data link layer (Ethernet), the packet has a source MAC address of 30:13:8b:6a:19:46 (HP_6a:19:46) and a destination MAC address of 30:13:8b:6a:18:ce (HP_6a:18:ce). The Ethernet protocol transports an IPv4 payload (type 0x0800), which in turn contains the network layer information.

At the network layer, the packet has a source IP address of 183.24.30.194 and a destination IP address of 183.24.30.209, with a total length of 60 bytes. The IPv4 packet identifier is 0x2e71, and the flags indicate no fragmentation. IPv4 header validation is disabled in this capture, so the header checksum appears as 0x0000.

At the ICMP layer, the packet is a ping request (type 8, code 0), with an identifier of 0x0001 and a sequence number of 0x0003. The ICMP checksum is valid, with a value of 0x4d38, confirming that the ICMP message is intact and has not been altered during transmission. It also contains 32 bytes of data, which is part of the payload of the ICMP message.

2. Basic Switch Configuration

Switches have an operating system specialized in switching tasks. The operating system of Catalystswitches, IOS, has a layered operational structure based on privileges and the configuration activities tobe performed.

Based on the setup from the previous point, we perform the following configuration:

Switch name: Student Name.

Message of the day: ”Exclusive use for RECO students”

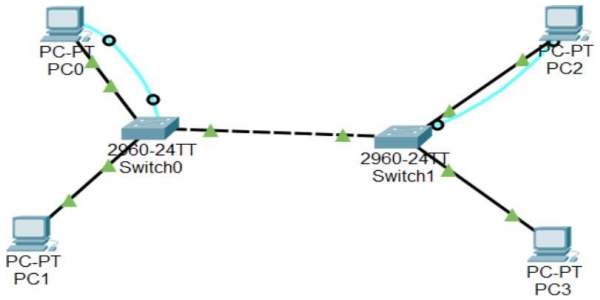
Screen synchronization.

Description of used interfaces.

Access passwords for the device:

- Privileged mode: Key E
- Console key: Key C

- Remote terminal key: Key TTo carry out this task, we first connect to the switch using console cables and the terminalmode on the PCs.



Now we use the following commands to perform the requested configuration.
We manually configure the switch.

- Access privileged mode and enter global configuration mode.
- Switch name.
- Message of the day.
- Screen synchronization and password configuration.
- Disable command lookup on external servers.
- Description of the interfaces.
- Password for privileged mode access.
- Review the device’s configuration.
- Save the configuration.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hosname Jorge
                ^
% Invalid input detected at '^' marker.

Switch(config)#hostname Jorge
Jorge(config)#banner motd "Switch 3"
Jorge(config)#line console 0
Jorge(config-line)#logging synchronous
Jorge(config-line)#password Clave_C
Jorge(config-line)#login
Jorge(config-line)#exit
Jorge(config)#no ip domain-lookup
Jorge(config)#line vty 0 15
Jorge(config-line)#loggin synchronous
Jorge(config-line)#password Clave_T
Jorge(config-line)#login
Jorge(config-line)#exit
```

Figure 8 Basic configuration

```
Jorge#enable
Jorge#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Jorge(config)#interface fa0/1
Jorge(config-if)#description Conexion a computador PC2
Jorge(config-if)#exit
Jorge(config)#interface fa0/3
Jorge(config-if)#description Conexion a computador PC3
Jorge(config-if)#exit
```

Figure 9 interfaces description

```
Jorge(config)#enable secret Clave_E
Jorge(config)#exit
```

Figure 10 enabled secret

```
Jorge#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 11 saving configurations

Now we verify that both the physical and logical connections are configured correctly and that everything is working properly.

```
Jorge>enable
Jorge#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  up                    up
FastEthernet0/4        unassigned      YES unset  down                  down
```

Figure 12 Verification of the switch interfaces

```
Jorge#show running-config
Building configuration...

Current configuration : 3216 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Jorge
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Qz1g$CsRMZ6A3kqjMt/snlK6O9.
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip domain-lookup
!
```

Figure 13 Viewing the configuration file

```
Jorge#show running-config
Building configuration...

Current configuration : 3216 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Jorge
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Qz1g$CsRMZ6A3kqjMt/snlK6O9.
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip domain-lookup
!
```

Figure 14 Viewing the configuration file

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
 description Conexion a computador PC2
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 description Conexion a computador PC3
!
interface FastEthernet0/4
```

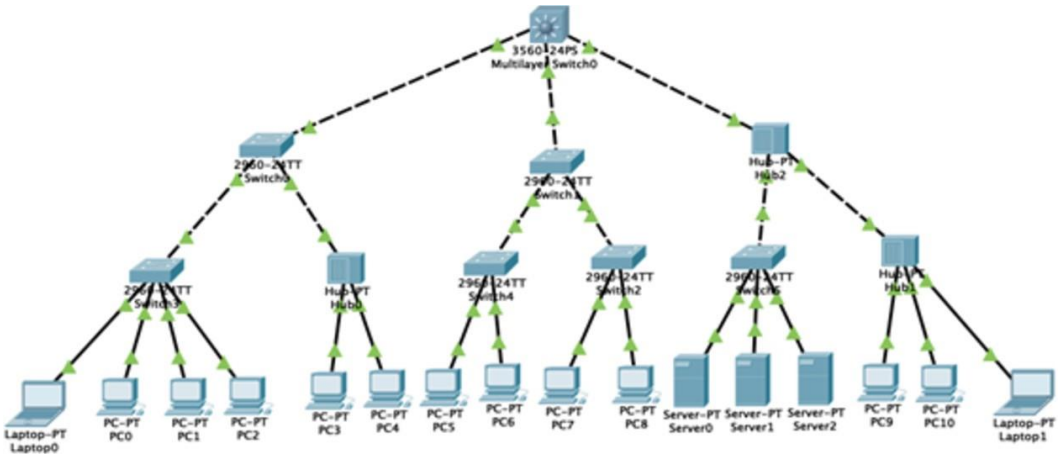
Figure 15 Viewing the configuration file

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
 description Conexion a computador PC2
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 description Conexion a computador PC3
!
interface FastEthernet0/4
```

Figure 16 Viewing the configuration file

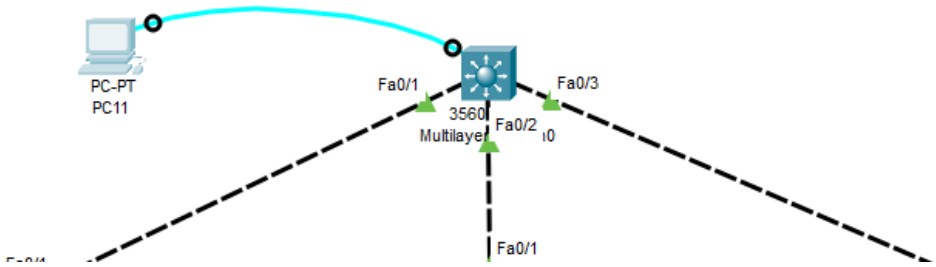
3. Larger Switch Networks

we set up the following network. First, we set up all physical connections and devices



1. We Perform the basic configuration on ALL switches.

   We connect to each router a PC with a console cable



We set the initial configuration, each switch has its owner name

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Jorge
```

```
Jorge(config)#banner motd "Uso exclusivo para estudiantes de RECO / Lab-8"
```

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

```
Jorge(config-line)#logging synchronous
Jorge(config-line)#exit
```

```
Jorge(config)#interface fastEthernet 0/1
Jorge(config-if)#description connection to switch0
Jorge(config-if)#exit
Jorge(config)#interface fastEthernet 0/2
Jorge(config-if)#description connection to switch1
Jorge(config-if)#exit
Jorge(config)#interface fastEthernet 0/3
Jorge(config-if)#description connection to hub0
Jorge(config-if)#exit
```

```
Jorge#write memory
Building configuration...
[OK]
```

Now we will configure the remaining devices using the same settings; since the configuration is identical, we will omit the detailed steps.

2. Configure the computers and servers with the information provided below:

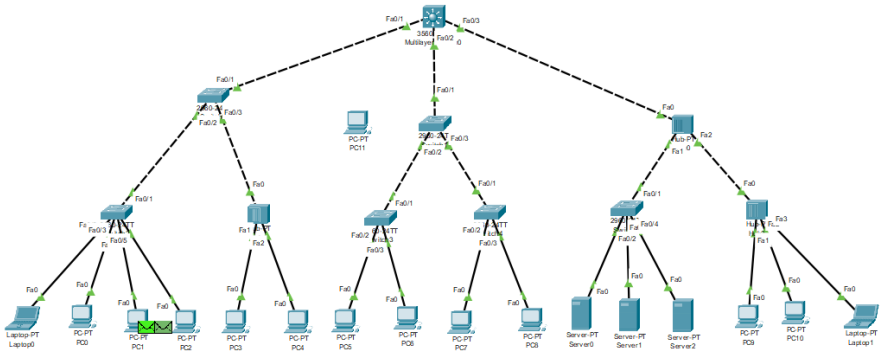
Estudiante1	Estudiante 2
IP: 65.148.77.x (x= número secuencial de 100 a 120) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1	IP: 65.148.77.x (x= número secuencial de 130 a 150) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1

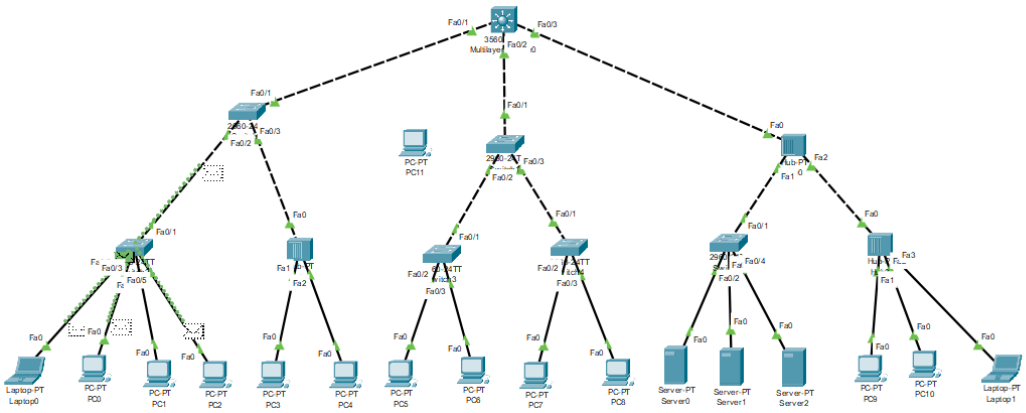
3. We Check the connectivity between the devices.

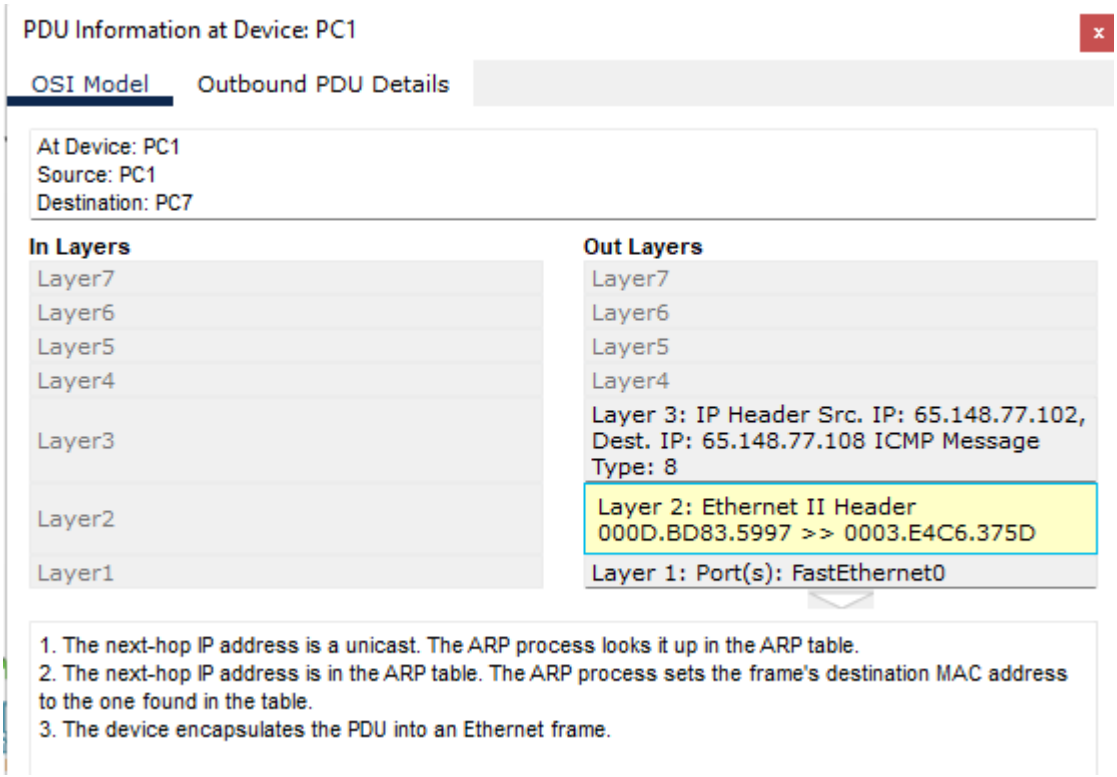
PDU List Window

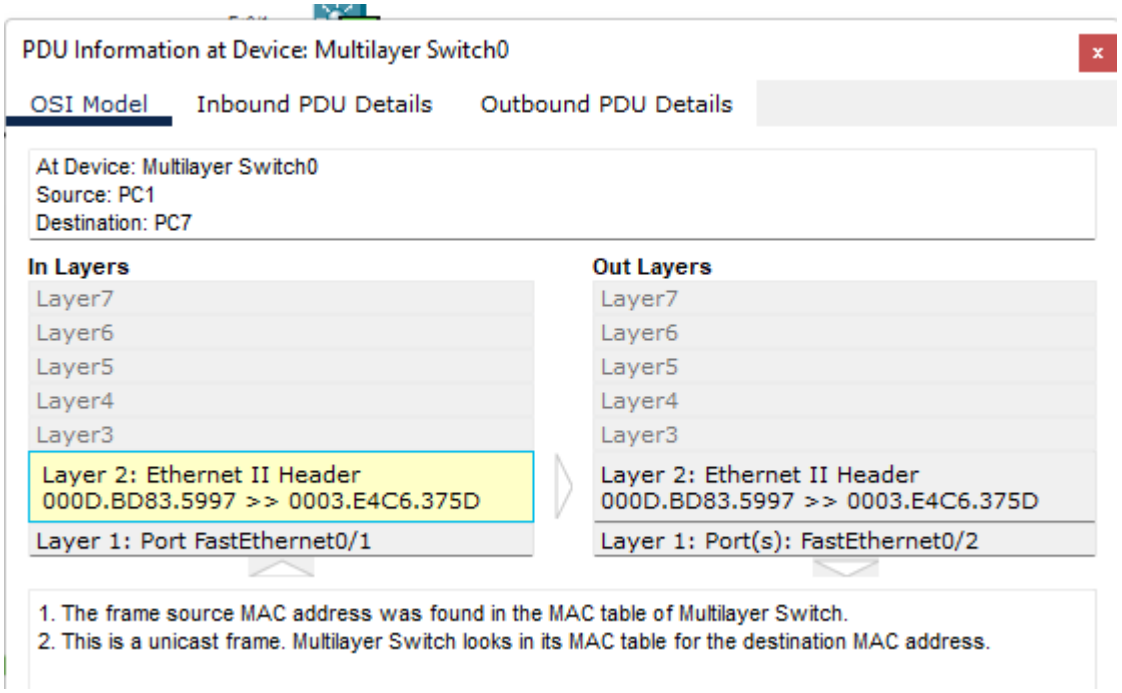
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Laptop0	PC2	ICMP		0.000	N	0
	Successful	Laptop0	PC0	ICMP		0.000	N	1
	Successful	Laptop0	PC1	ICMP		0.000	N	2
	Successful	Laptop0	PC3	ICMP		0.000	N	3
	Successful	Laptop0	PC5	ICMP		0.000	N	4
	Successful	Laptop0	PC5	ICMP		0.000	N	5
	Successful	Laptop0	PC6	ICMP		0.000	N	6
	Successful	Laptop0	Server0	ICMP		0.000	N	7
	Successful	Laptop0	Laptop1	ICMP		0.000	N	8
	Successful	PC8	PC5	ICMP		0.000	N	9
	Successful	PC6	PC5	ICMP		0.000	N	11
	Successful	PC7	PC6	ICMP		0.000	N	12
	Successful	Server0	PC8	ICMP		0.000	N	13
	Successful	Server2	PC9	ICMP		0.000	N	14
	Successful	Server0	Server1	ICMP		0.000	N	15
	Successful	PC7	Server0	ICMP		0.000	N	16
	Successful	Laptop1	PC10	ICMP		0.000	N	17
	Successful	Server1	Server0	ICMP		0.000	N	18
	Successful	PC1	PC3	ICMP		0.000	N	19
	Successful	PC7	PC6	ICMP		0.000	N	20

4. Using simulation mode, we analyze the network behavior and the format of an Ethernet frame bysending the following frames.(Identify the switches' behavior and their forwarding tables.)
   a. From PC1 to PC7.

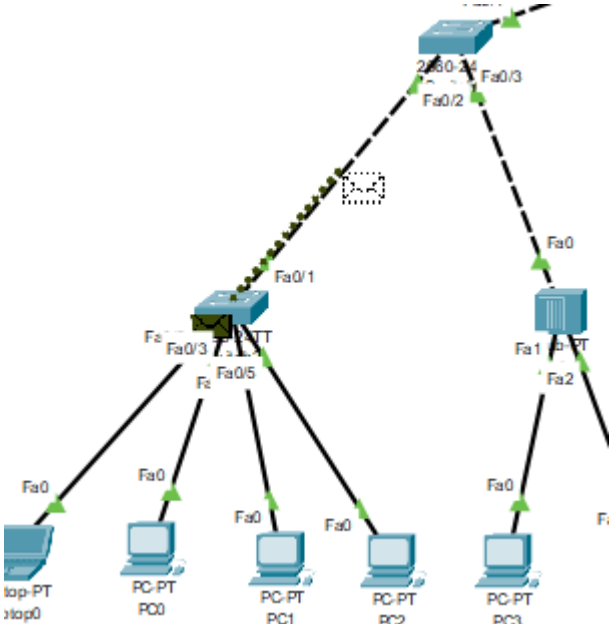


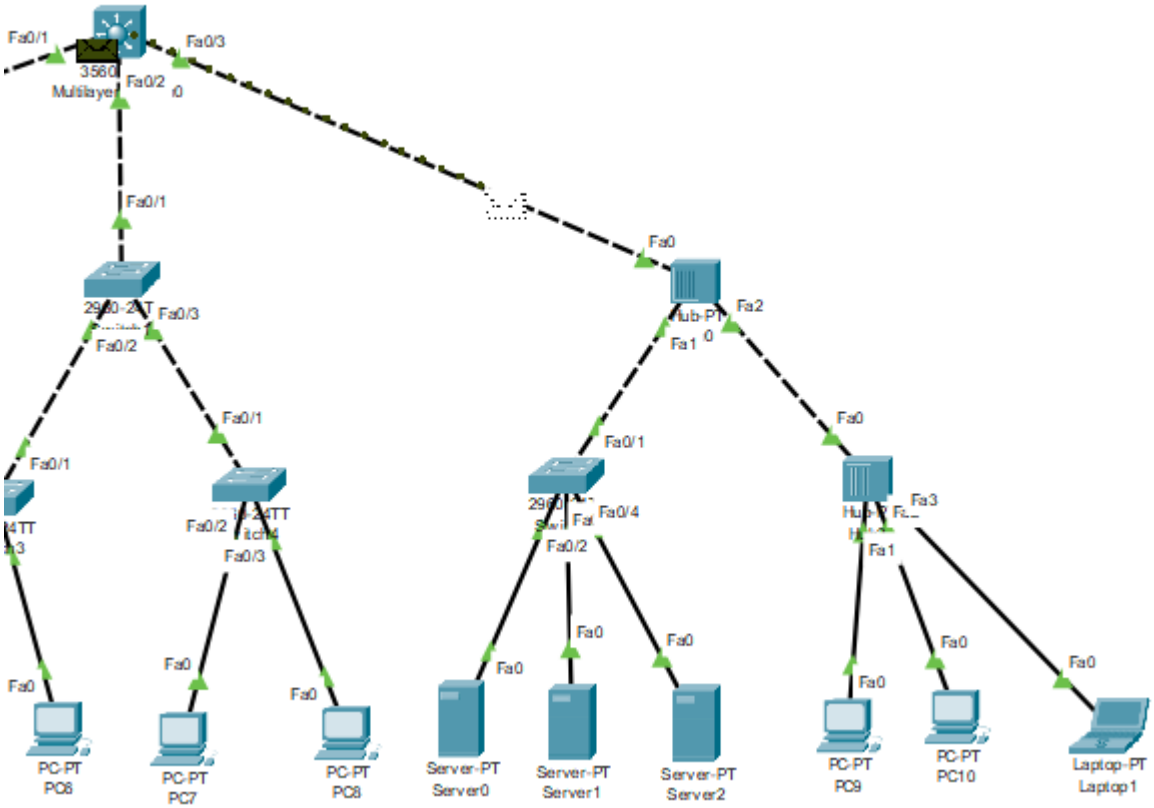

Fa0/1
Fa0/3
Fa0/2
Fa0/1
Fa0
Fa0/1
Fa0/3
Fa0/2
Fa0/1
Fa0
Fa2
Fa1
Fa0/1
Fa0
Fa0/1
Fa0/1
Fa0/2
Fa0/3
Fa0/2
Fa0/1
Fa0/1
Fa0/4
Fa0/2
Fa0
Fa3
Fa1
Fa0/1
Fa0/3
Fa0/5
Fa0
Fa1
Fa2
Fa0/2
Fa0/3
Fa0/2
Fa0/3
Fa0
Fa0
Fa0

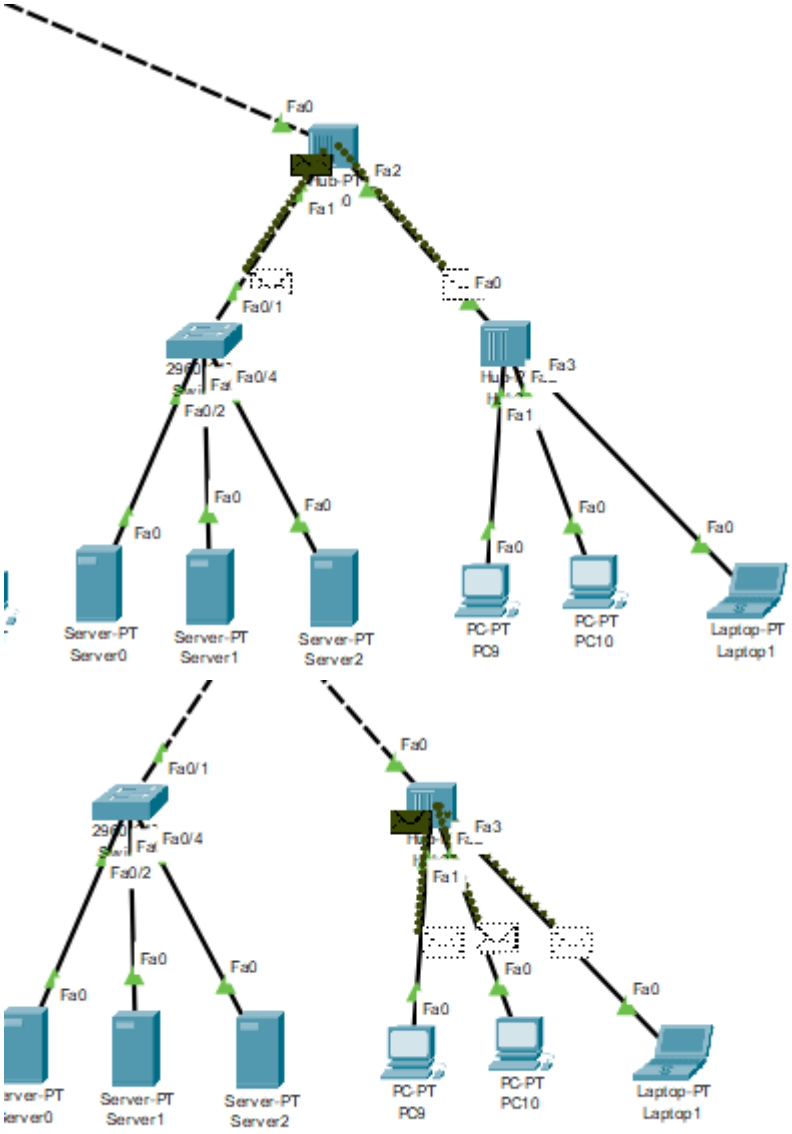


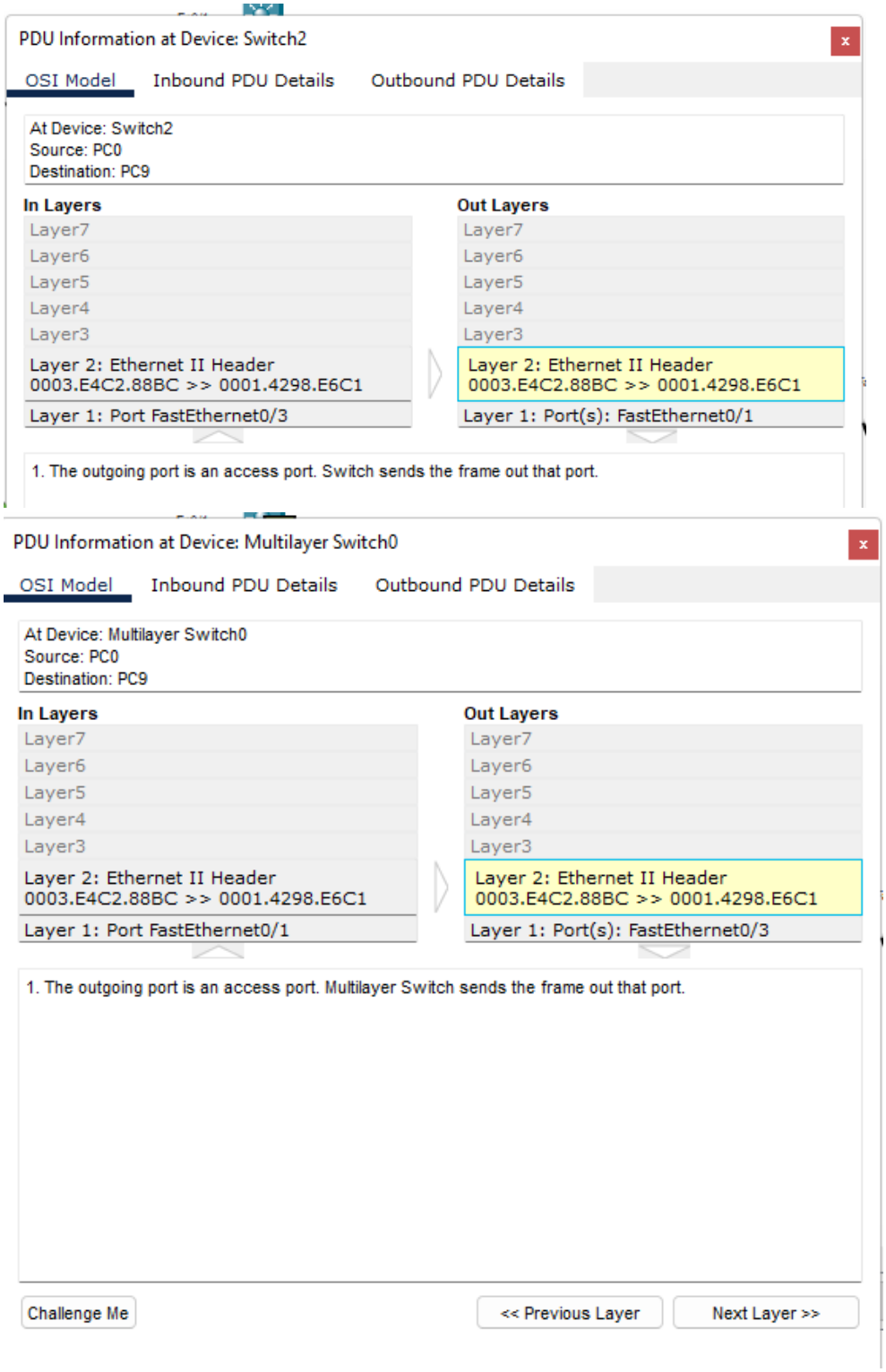


b. From PC0 to PC9.

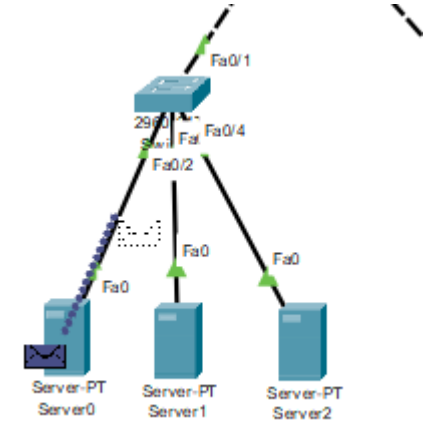

Fa0/3
Fa0/2
Fa0
Fa0/1
Fa0/3
Fa0/5
Fa1
Fa2
Fa0
Fa0
Fa0
Fa0
Fa0
PC-PT
PC-PT
PC-PT
PC-PT
PC-PT

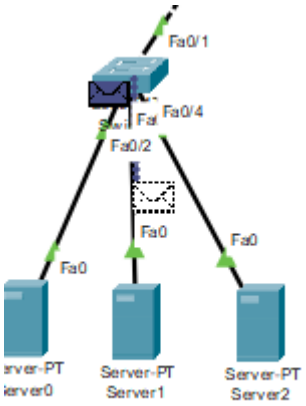

Fa0/1
Fa0/3
Fa0/2
Fa0/1
Fa0
Fa0/3
Fa0/2
Fa1
Fa2
Fa0/1
Fa0/1
Fa0/1
Fa0/2
Fa0/3
Fa0/4
Fa0/2
Fa3
Fa1
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
PC-PT
PC-PT
PC-PT
Server-PT
Server-PT
Server-PT
PC-PT
PC-PT
Laptop-PT

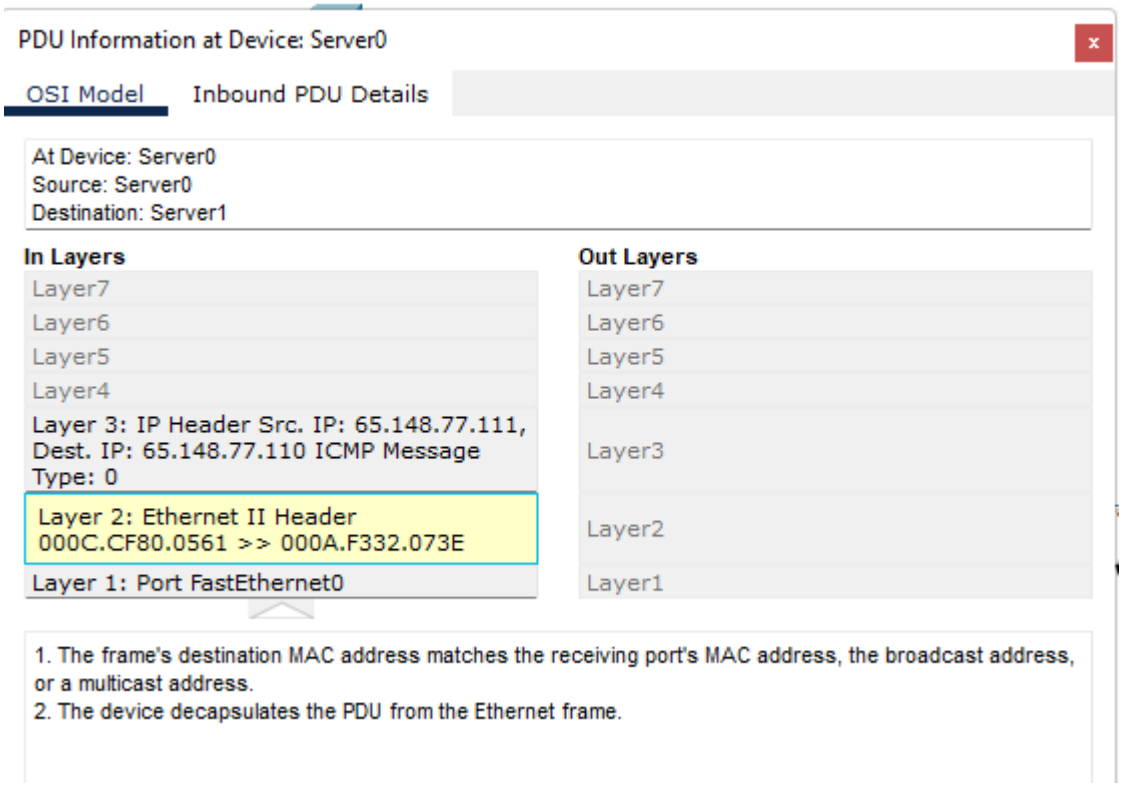

Fa0
Fa2
Fa1
Fa0/1
Fa0/4
Fa0/2
Fa3
Server-PT
Server0
Server-PT
Server1
Server-PT
Server2
PC-PT
PC9
PC-PT
PC10
Laptop-PT
Laptop1



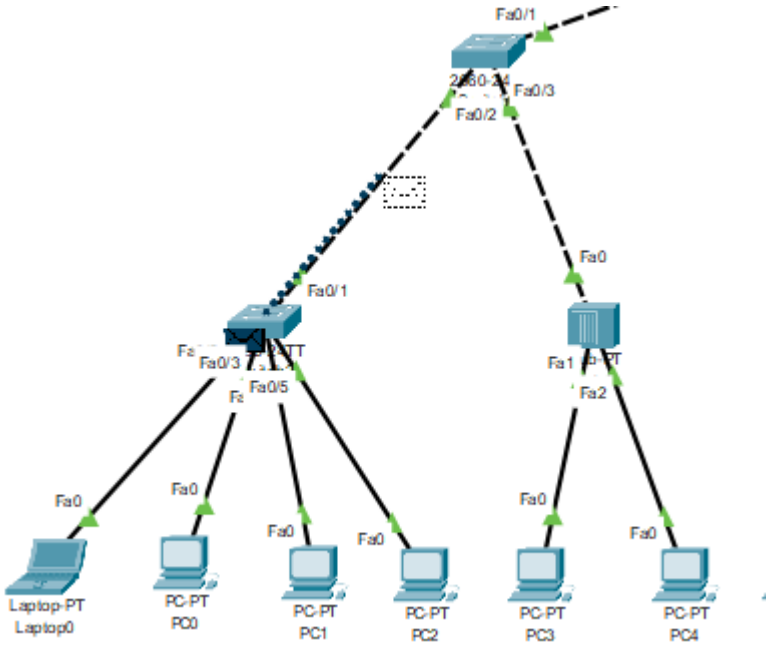
c. From Server0 to Server1.

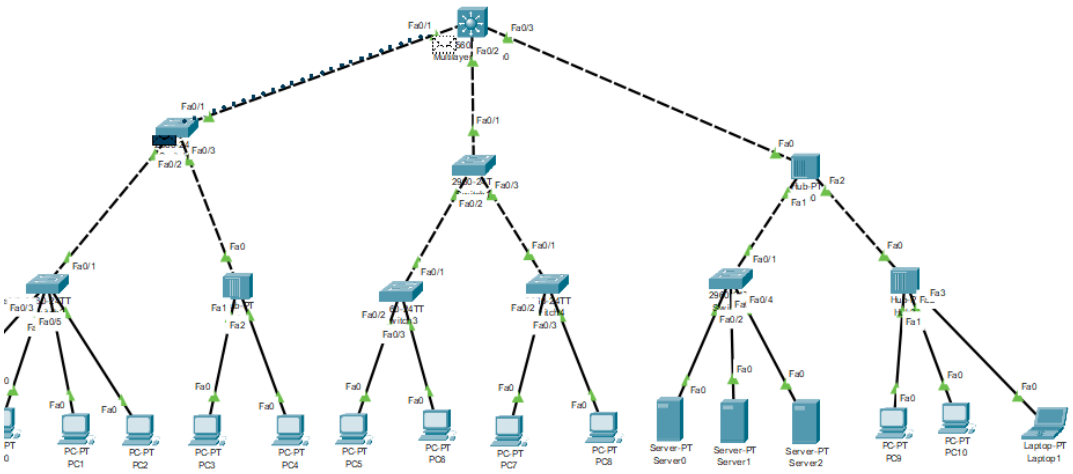


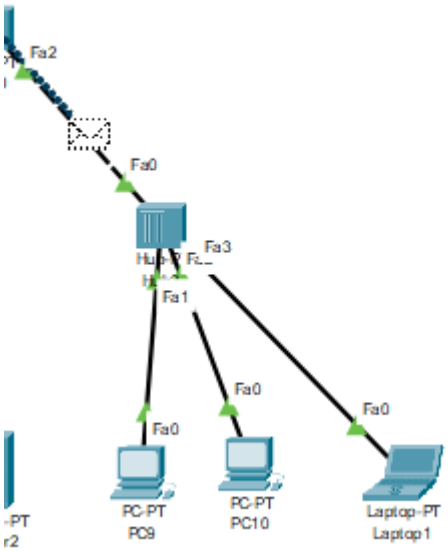


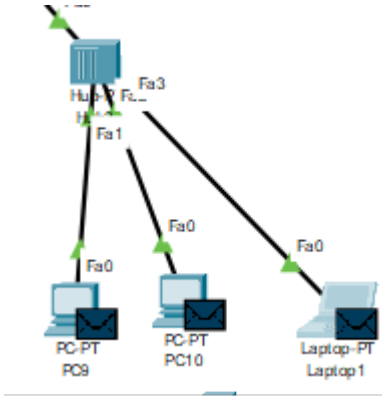


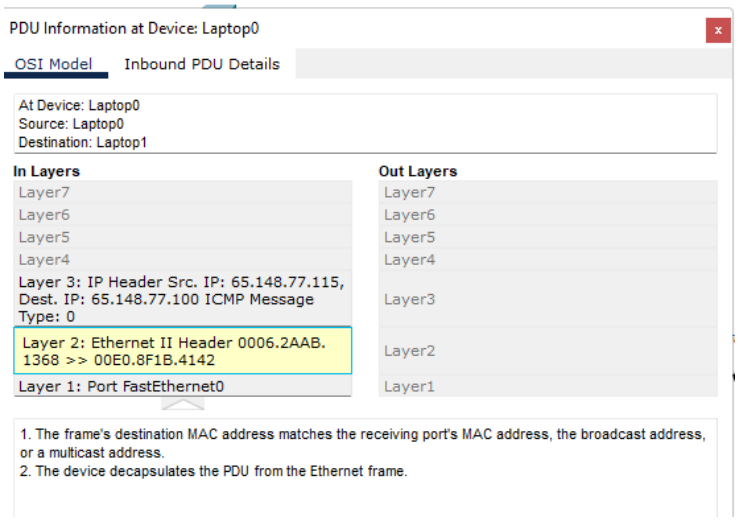
d. From Laptop0 to Laptop1.


Fa0/1
Fa0/3
Fa0/2
Fa0
Fa0/1
Fa0/3
Fa0/5
Fa1
Fa2
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Laptop-PT
Laptop0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4





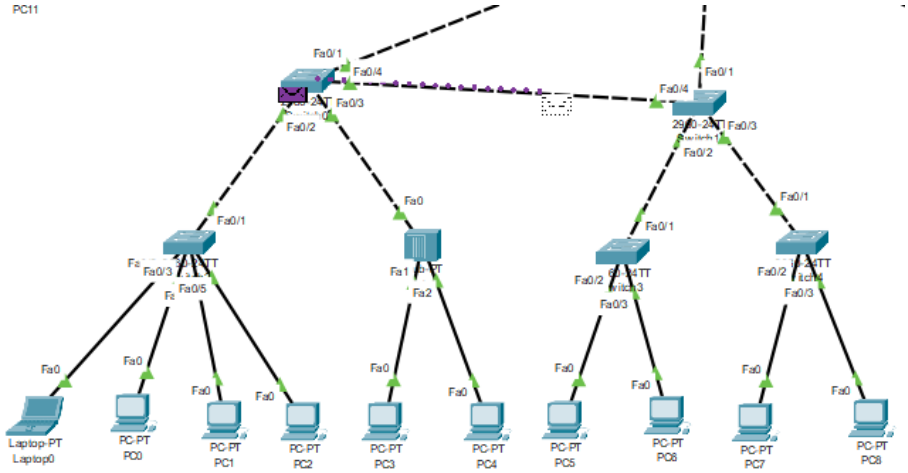




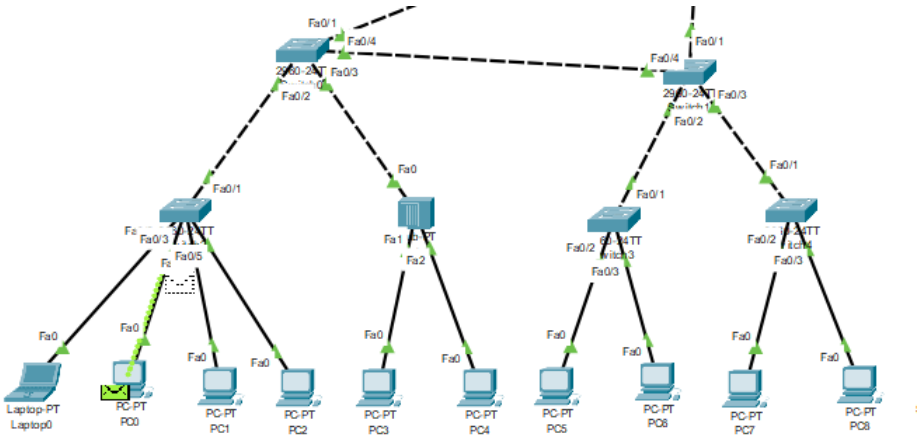
Hint: Observe that at first, the transmission behavior is pure broadcast, and then it starts learning.

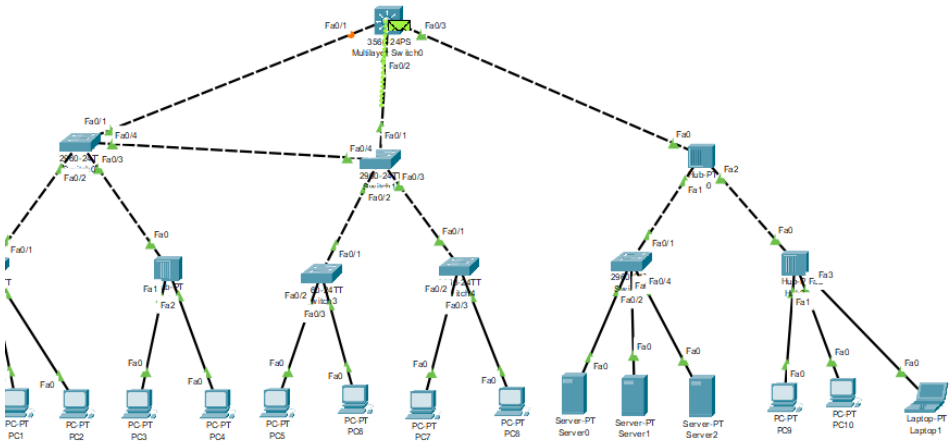
5. We Examine the operation of the spanning tree algorithm. When we interconnect switches 0 and 1 .

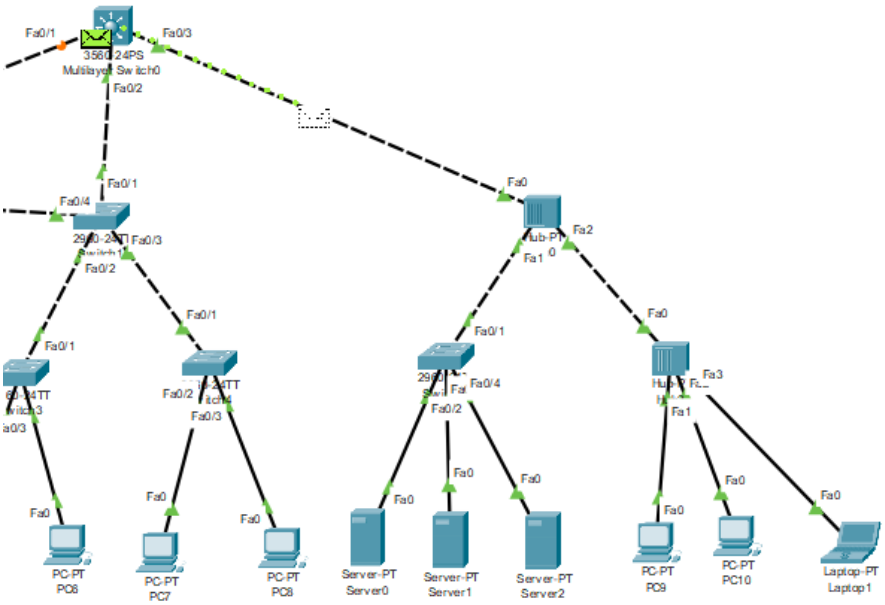
a. From PC1 to PC7

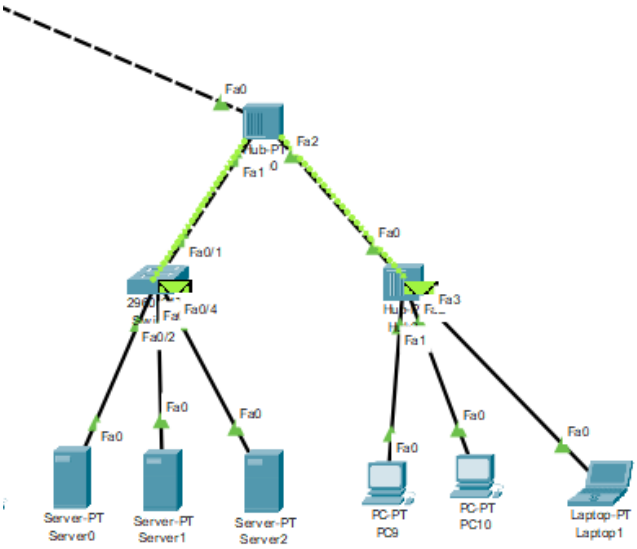


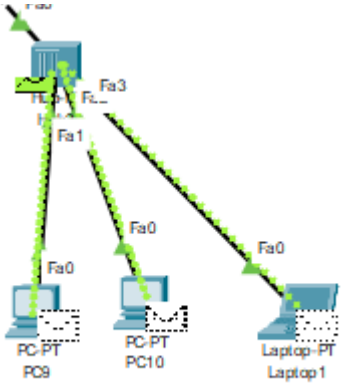
b. . b. From PC0 to PC9



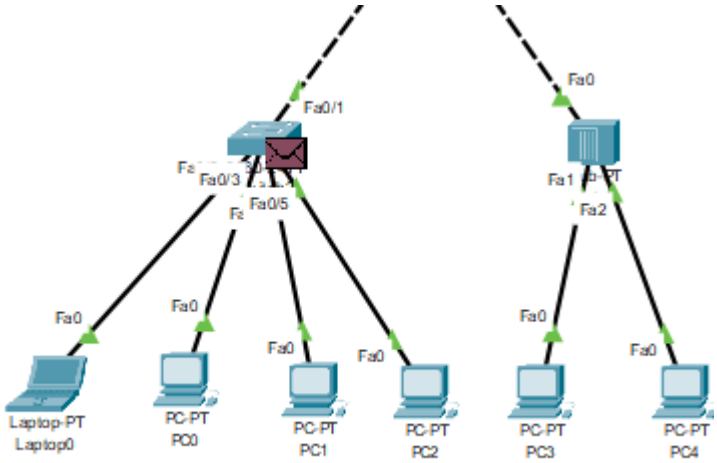


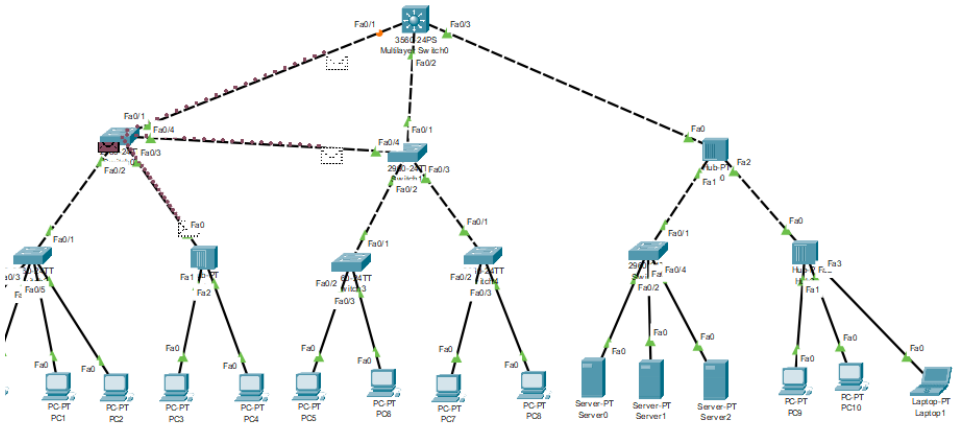

Fa0/1
Fa0/3
Fa0/2
Fa0/4
Fa0
Fa2
Fa1
Fa3
PC-PT PC8
PC-PT PC7
PC-PT PC8
Server-PT Server0
Server-PT Server1
Server-PT Server2
PC-PT PC9
PC-PT PC10
Laptop-PT Laptop1

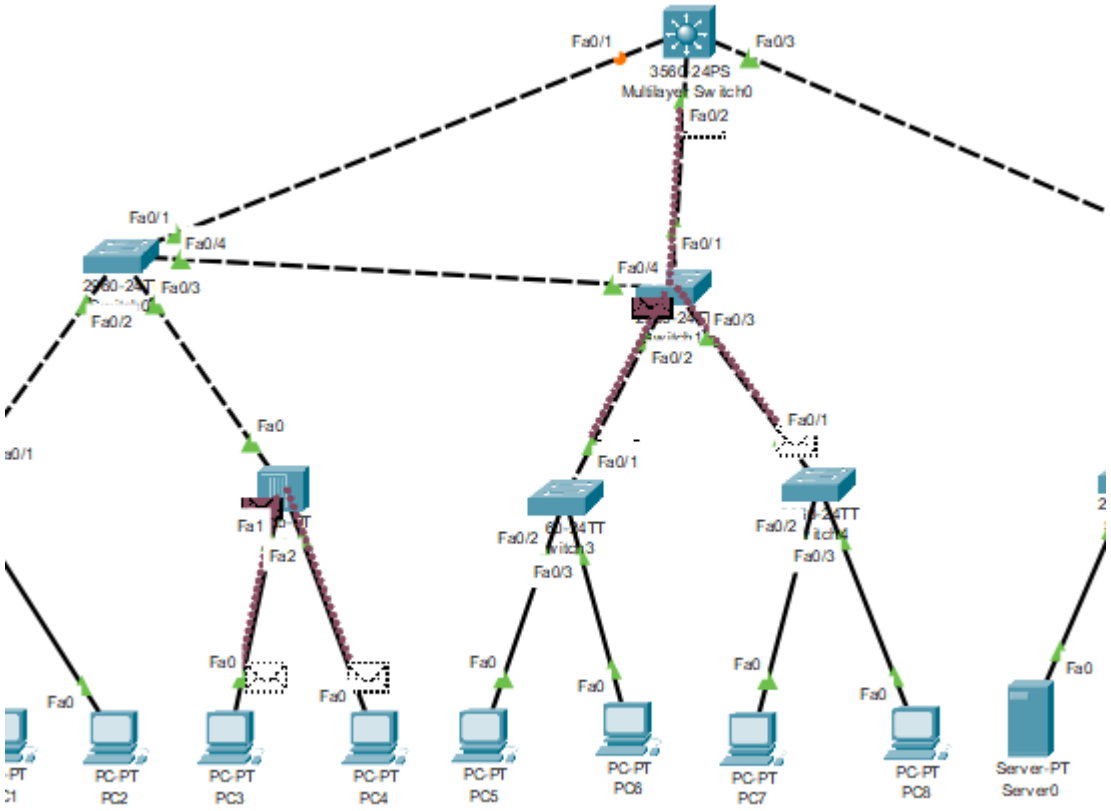

Fa0
Fa2
Fa1
Fa0/1
Fa0/4
Fa0/2
Fa3
Server-PT Server0
Server-PT Server1
Server-PT Server2
PC-PT PC9
PC-PT PC10
Laptop-PT Laptop1

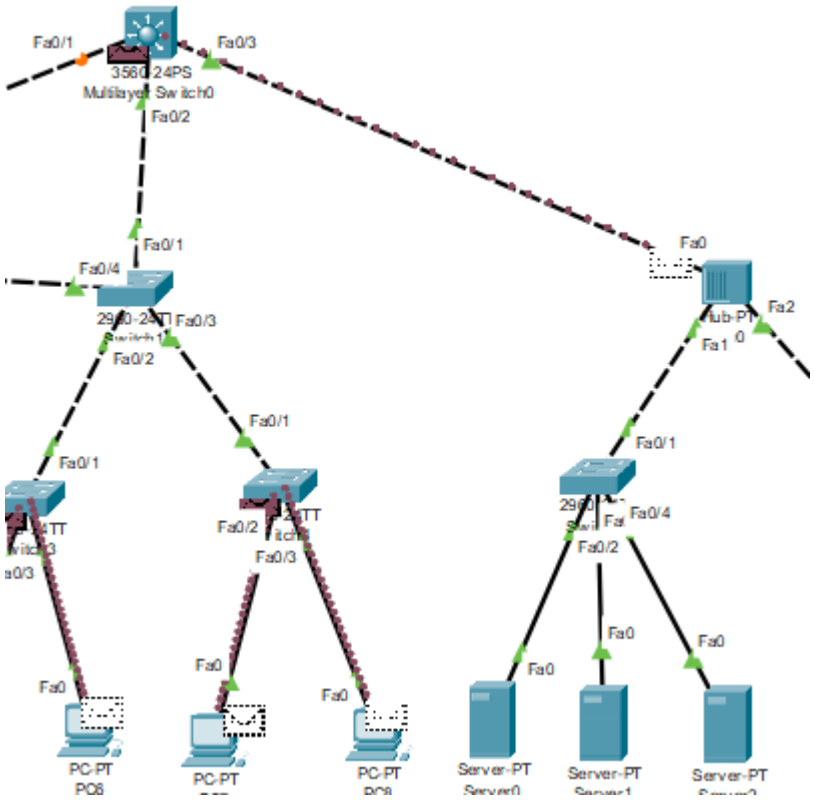


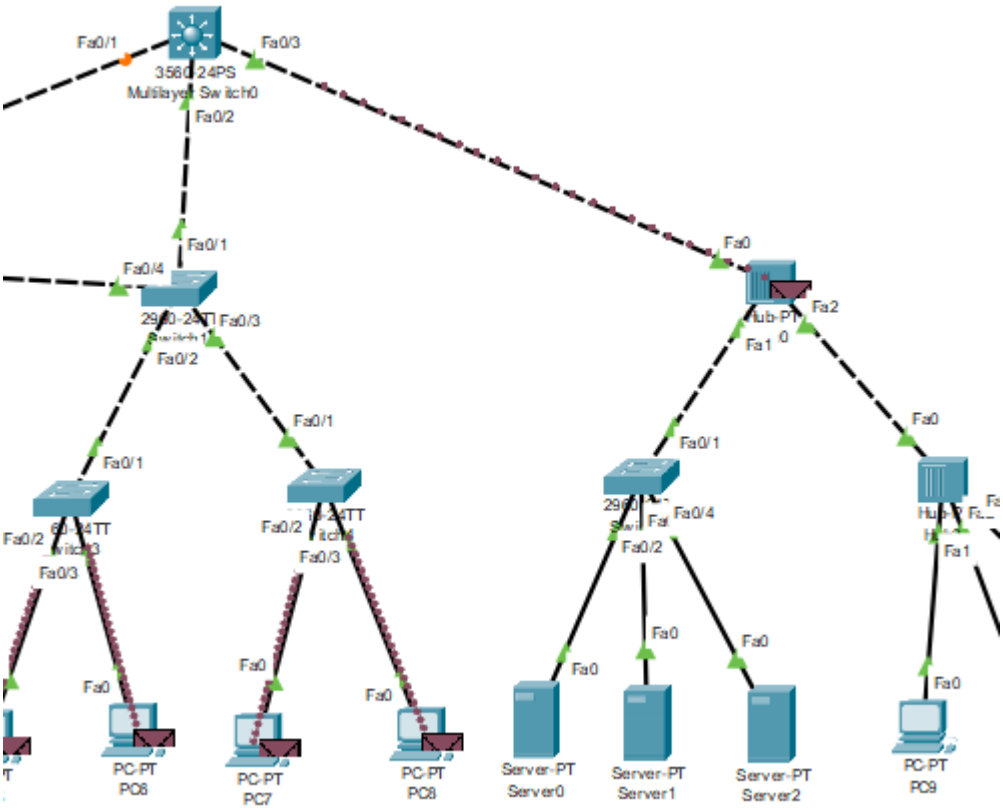
c. . From Laptop0 to Laptop1.

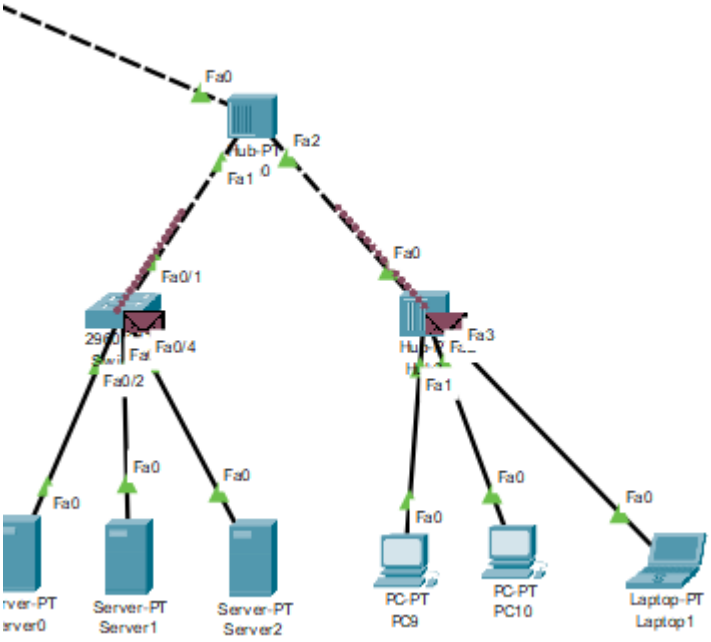


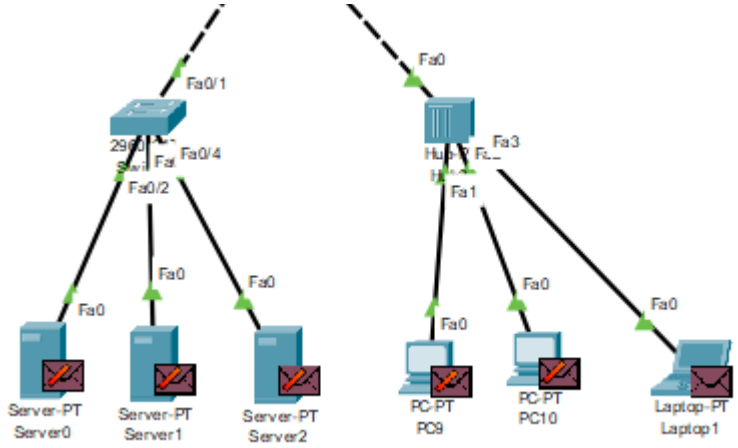



Fa0/1
Fa0/3
Fa0/2
Fa0/4
Fa0
Fa1
Fa2
PC-PT
PC2
PC3
PC4
PC5
PC6
PC7
PC8
Server-PT
Server0

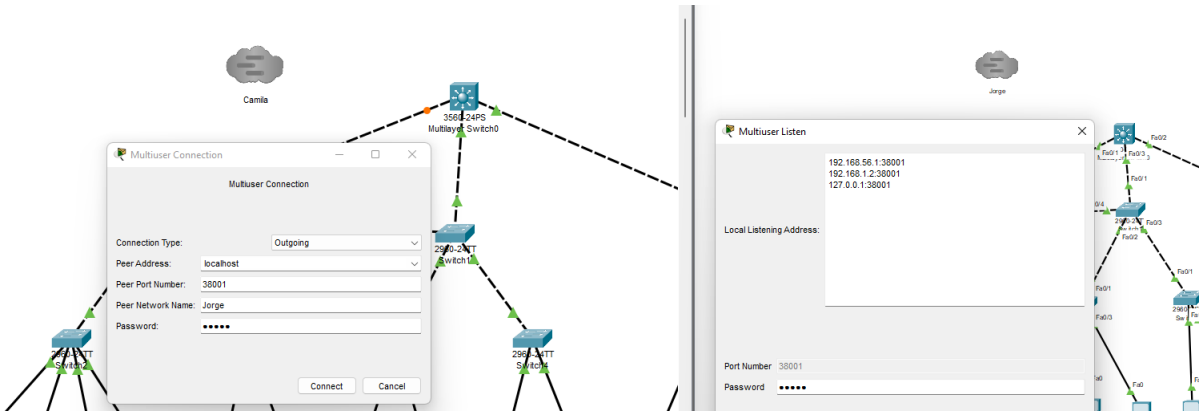

Fa0/1
Fa0/3
Fa0/2
Fa0/4
Fa0
Fa1
Fa2
PC-PT
PC8
Server-PT
Server0
Server-PT
Server-PT

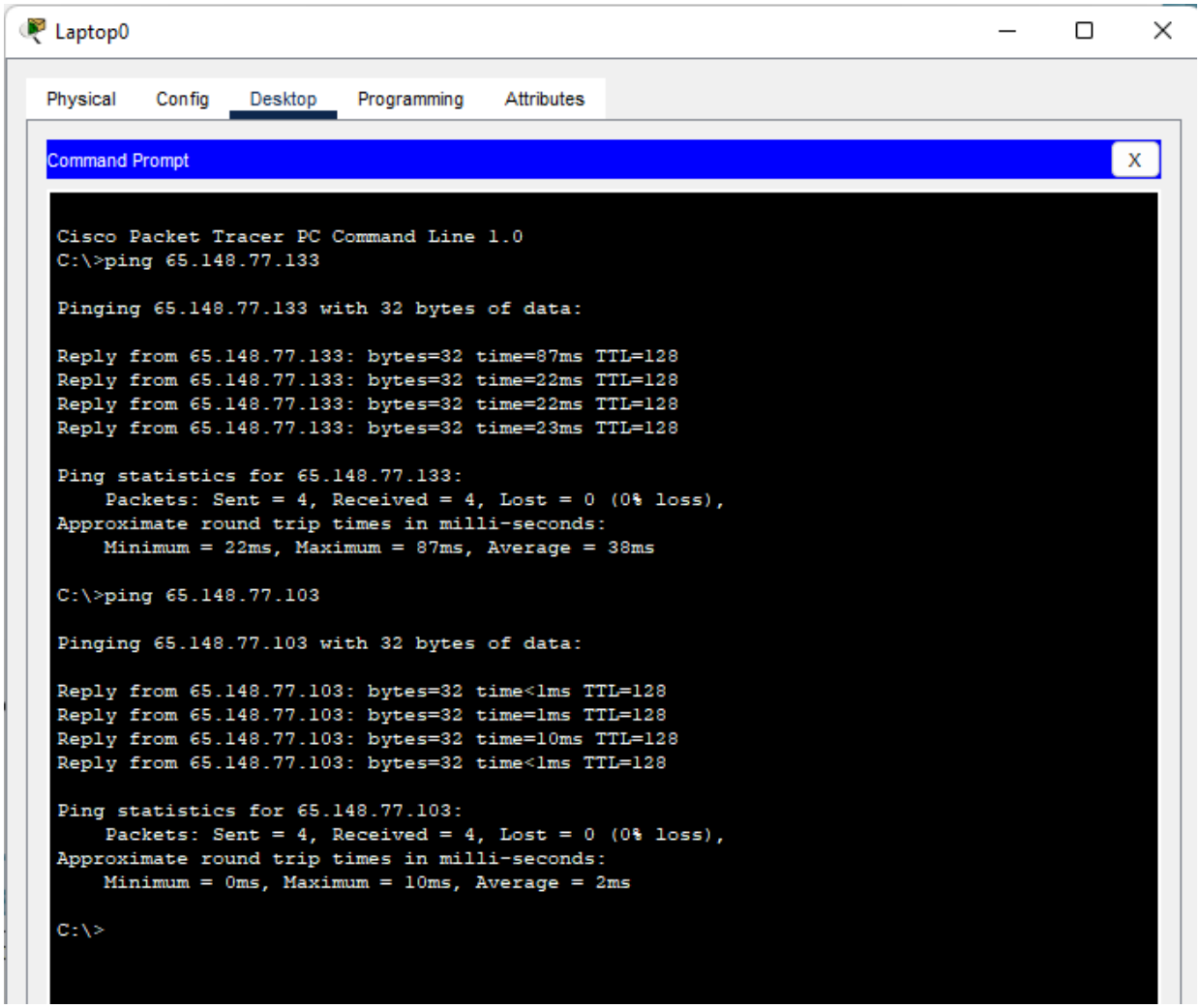

Fa0/1
Fa0/3
Fa0/2
Fa0/1
Fa0/4
Fa0/3
Fa0/2
Fa0/1
Fa0/1
Fa0/2
Fa0/3
Fa0/2
Fa0/3
Fa0/1
Fa0/4
Fa0/2
Fa0
Fa2
Fa1
Fa0
Fa1
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
PC-PT
PC8
PC-PT
PC7
PC-PT
PC8
Server-PT
Server0
Server-PT
Server1
Server-PT
Server2
PC-PT
PC9


Fa0
Fa2
Fa1
Fa0/1
Fa0
Fa0/4
Fa0/2
Fa3
Fa1
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Server-PT
Server1
Server-PT
Server2
PC-PT
PC9
PC-PT
PC10
Laptop-PT
Laptop1



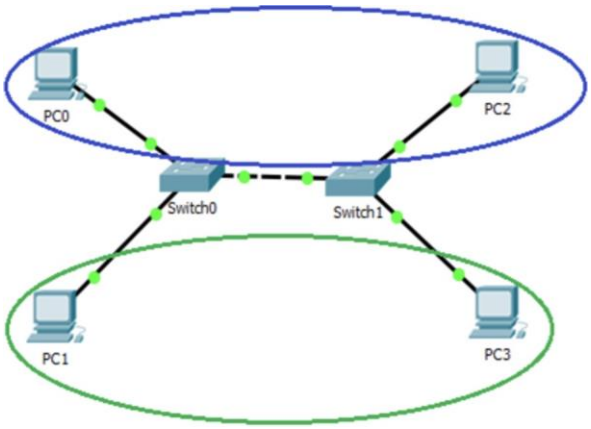
6. Now We Merge the project files of the team members.





4. VLAN Configuration

We Use the configuration from points 1 and 2 as a base, in the small groups and create two VLANs as shown in the diagram.



Enter configuration mode.

Configure two VLANs.

a. systems → VLAN ID 50 (blue circular frame).
b. others → VLAN ID 55 (green circular frame).

We Assign computers PC1 and PC3 to the ”systems” VLAN. Assign computers PC2 and PC0 to the”others” VLAN. Then, We Configure the link between the switches to allow VLAN connections.

Before to start we need to know What are trunk links? What are they used for?

Verify connectivity.

Trunk links are network connections that carry traffic from multiple VLANs between switches, using VLAN tagging to differentiate the traffic. To verify connectivity, check that the trunk link is up, ensure VLAN configurations match on both ends, perform ping tests to confirm device reachability, verify VLAN tagging (usually 802.1Q), and ensure inter-VLAN routing is properly set up if required.

```
Jorge#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Jorge(config)#vlan 50
Jorge(config-vlan)#name sistemas
Jorge(config-vlan)#exit
Jorge(config)#vlan 55
Jorge(config-vlan)#name otros
Jorge(config-vlan)#exit
Jorge(config)#int fa0/1
Jorge(config-if)#switchport mode access
Jorge(config-if)#switchport access vlan 50
Jorge(config-if)#end
Jorge#
*Mar  2 01:35:25.057: %SYS-5-CONFIG_I: Configured from console by console
Jorge#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Jorge(config)#int fa0/3
Jorge(config-if)#switchport mode access
Jorge(config-if)#switchport access
% Incomplete command.

Jorge(config-if)#switchport access 55
                                   ^
% Invalid input detected at '^' marker.

Jorge(config-if)#switchport access 55
*Mar  2 01:36:17.469: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
*Mar  2 01:36:17.469: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar  2 01:36:18.476: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
Jorge(config-if)#switchport access vlan 55
Jorge(config-if)#
*Mar  2 01:36:24.801: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
Jorge(config-if)#
*Mar  2 01:36:25.808: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Jorge(config-if)#end
Jorge#
*Mar  2 01:36:30.740: %SYS-5-CONFIG_I: Configured from console by console
```

Figure 17 Vlan configuration

Now, we verify that the ports have been correctly configured.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   VLAN_ID50                        active
50   sistemas                         active    Fa0/1
55   otros                            active    Fa0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Jorge#
```

Then, we review the interfaces.

```
Jorge#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  down                  down
```

Figure 18 interfaces Verification of interfaces

Now, we configure interface Gig0/1 to be a trunk and allow traffic from all VLANs.

```
Jorge#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Jorge(config)#int gig0/1
Jorge(config-if)#switchport mode trunk
Jorge(config-if)#end
```

Figure 19 gig0/1 configuration

```
Switch 3

User Access Verification

Password:
Password:
Jorge>enable
Password:
Jorge#show mac a
Jorge#show mac
Jorge#show mac adre
Jorge#show mac add
Jorge#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    0024.5143.a019    DYNAMIC     Gi0/1
  50    3013.8b6a.18ce    DYNAMIC     Gi0/1
  50    3013.8b6a.1917    DYNAMIC     Fa0/1
  55    1860.24de.f2a1    DYNAMIC     Gi0/1
  55    3013.8b6a.1946    DYNAMIC     Fa0/3
Total Mac Addresses for this criterion: 25
```

Figure 20 Verification of the MAC address table

Now, we configure port security so that each port is specifically associated with a device's MAC address.

```
Jorge#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Jorge(config)#int
Jorge(config)#interface fa0/1
Jorge(config-if)#siw
Jorge(config-if)#swit
Jorge(config-if)#switchport por
Jorge(config-if)#switchport port-security
Jorge(config-if)#switchport port-security ma
Jorge(config-if)#switchport port-security maxi
Jorge(config-if)#switchport port-security maximum 1
Jorge(config-if)#in
Jorge(config-if)#int
Jorge(config-if)#interface fa0/3
Jorge(config-if)#switchport port-security
Jorge(config-if)#switchport port-security maximum 1
Jorge(config-if)#exit
Jorge(config)#int
Jorge(config)#interface fa0/1
Jorge(config-if)#no shutdown
Jorge(config-if)#exit
Jorge(config)#interface fa0/3
Jorge(config-if)#no shutdown
Jorge(config-if)#exit
Jorge(config)#int
Jorge(config)#interface g0/1
Jorge(config-if)#no shut
Jorge(config-if)#no shutdown
Jorge(config-if)#exit
Jorge(config)#end
```

5. Basic WiFi Configuration

5.1. Configuration Process

- We assigned static IP addresses in the range 65.148.77.1 to 65.148.77.20 with a subnet mask of 255.255.255.0. The configurations are as follows:

  PC0 - 65.148.77.2

  PC1 - 65.148.77.3

  Server0 - 65.148.77.4

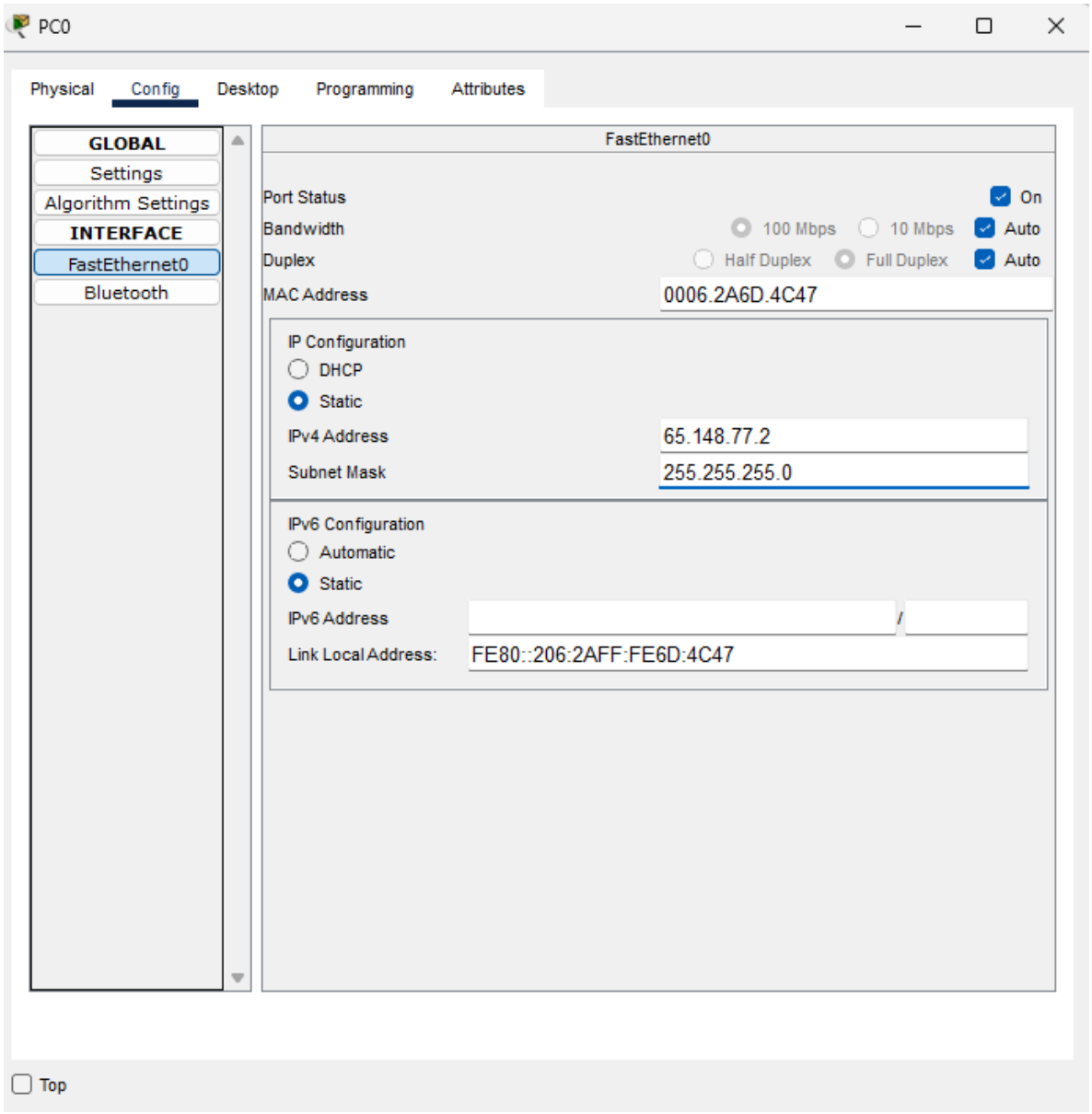


Figure 21. Assigning IP and Subnet Mask to PC0

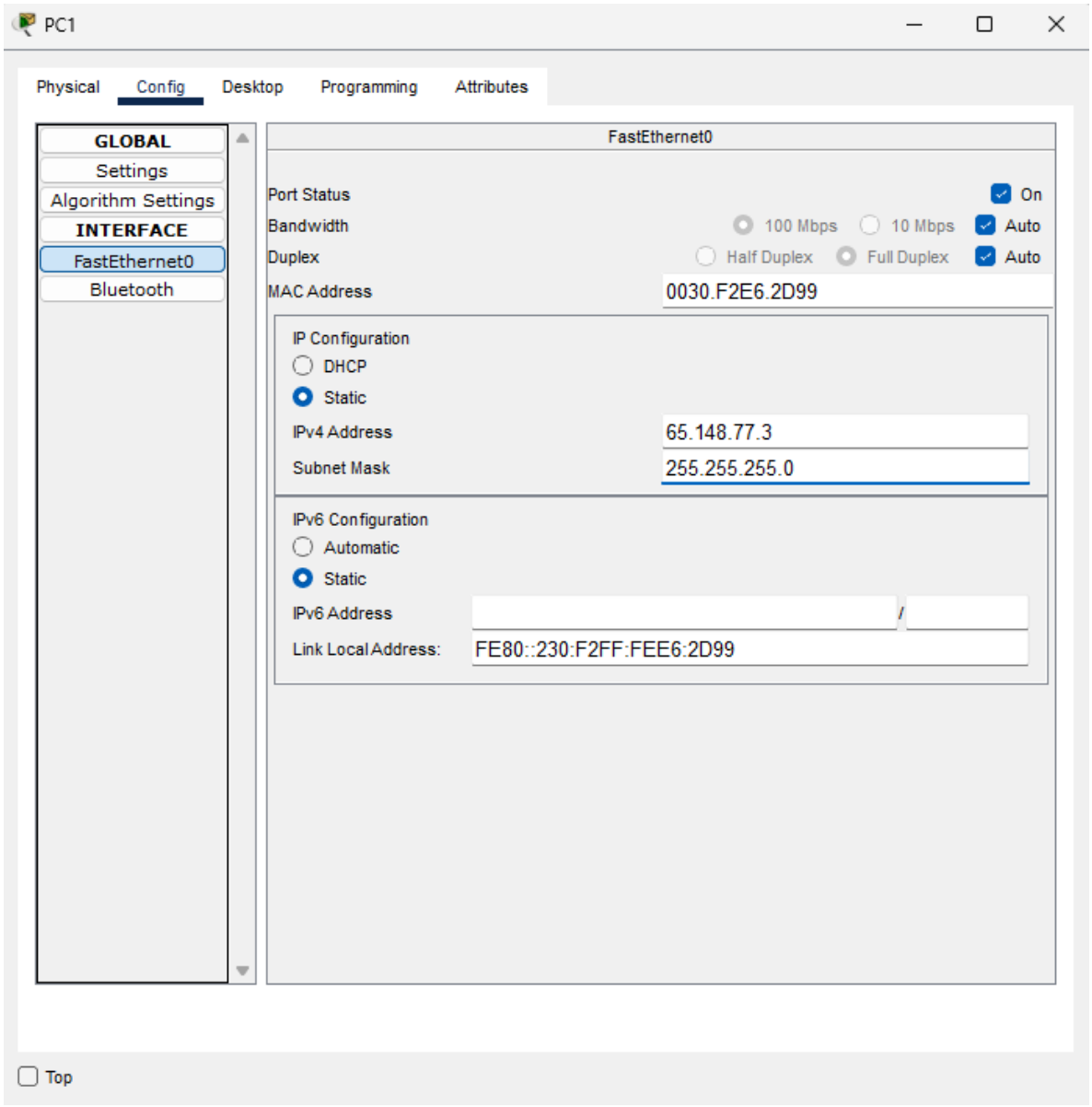


Figure 22. Assigning IP and Subnet Mask to PC1

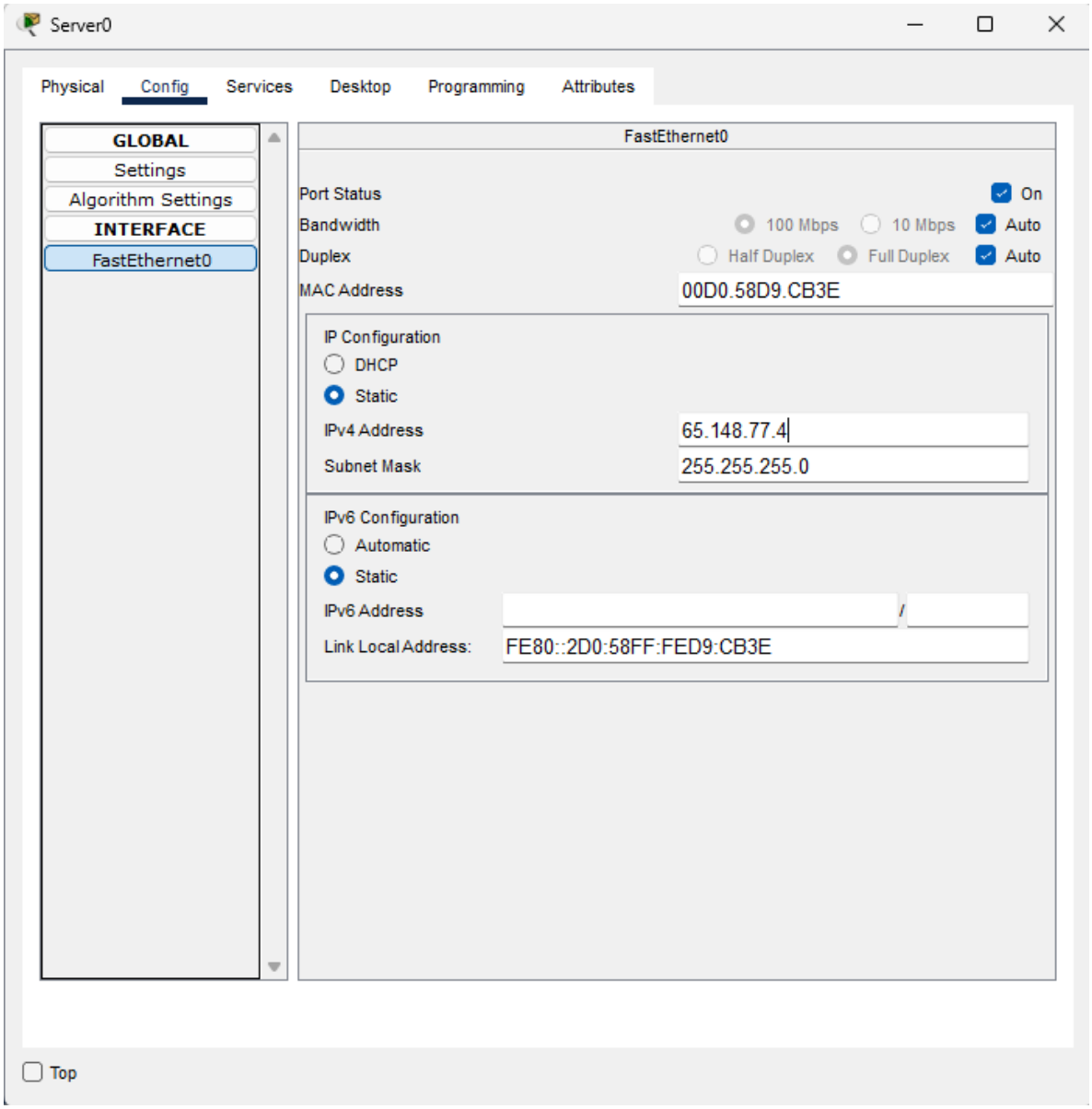


Figure 23. Assigning IP and Subnet Mask to Server0

- We changed the interface of the laptops (Laptop0 and Laptop1) by installing a WPC300N for wireless connectivity

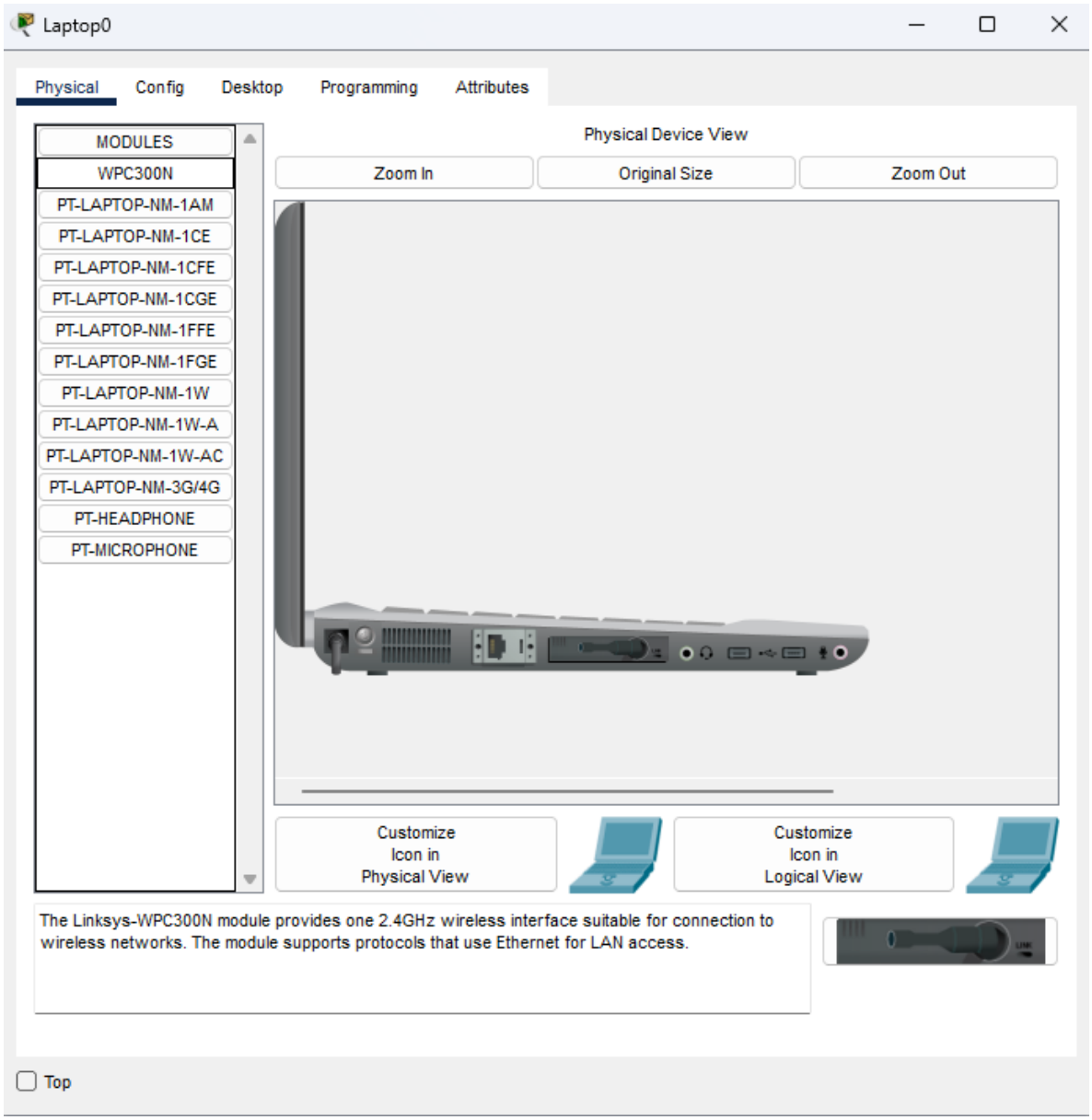


Figure 24. Configuring WPC300N Wireless Port of the Laptops

- We go to the wireless interface configuration of the laptops and enable the DHCP option

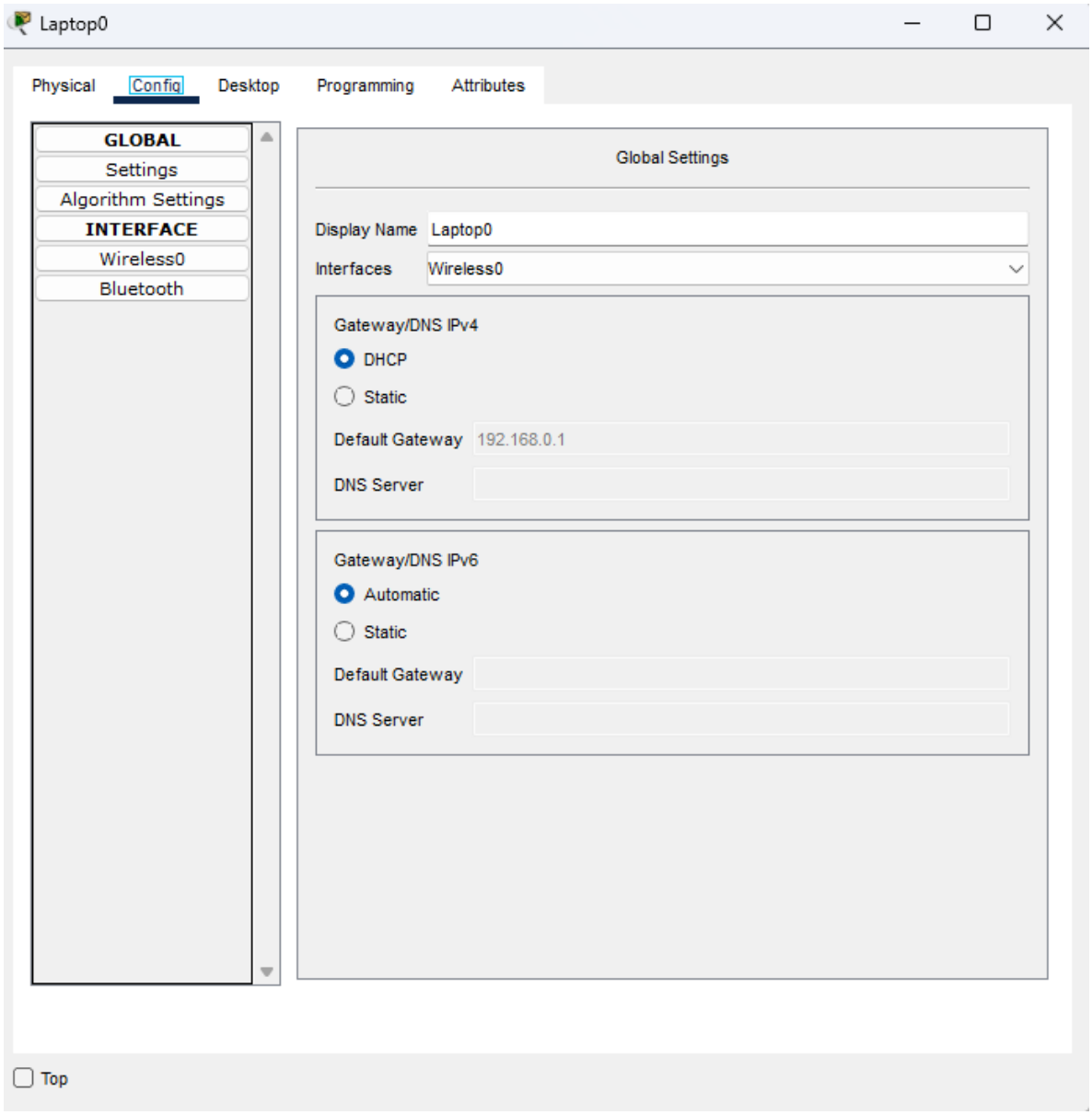


Figure 25. Configuring DHCP in the laptops

- From Laptop0, we go to Web Browser, enter the router's IP address, and authenticate as an administrator

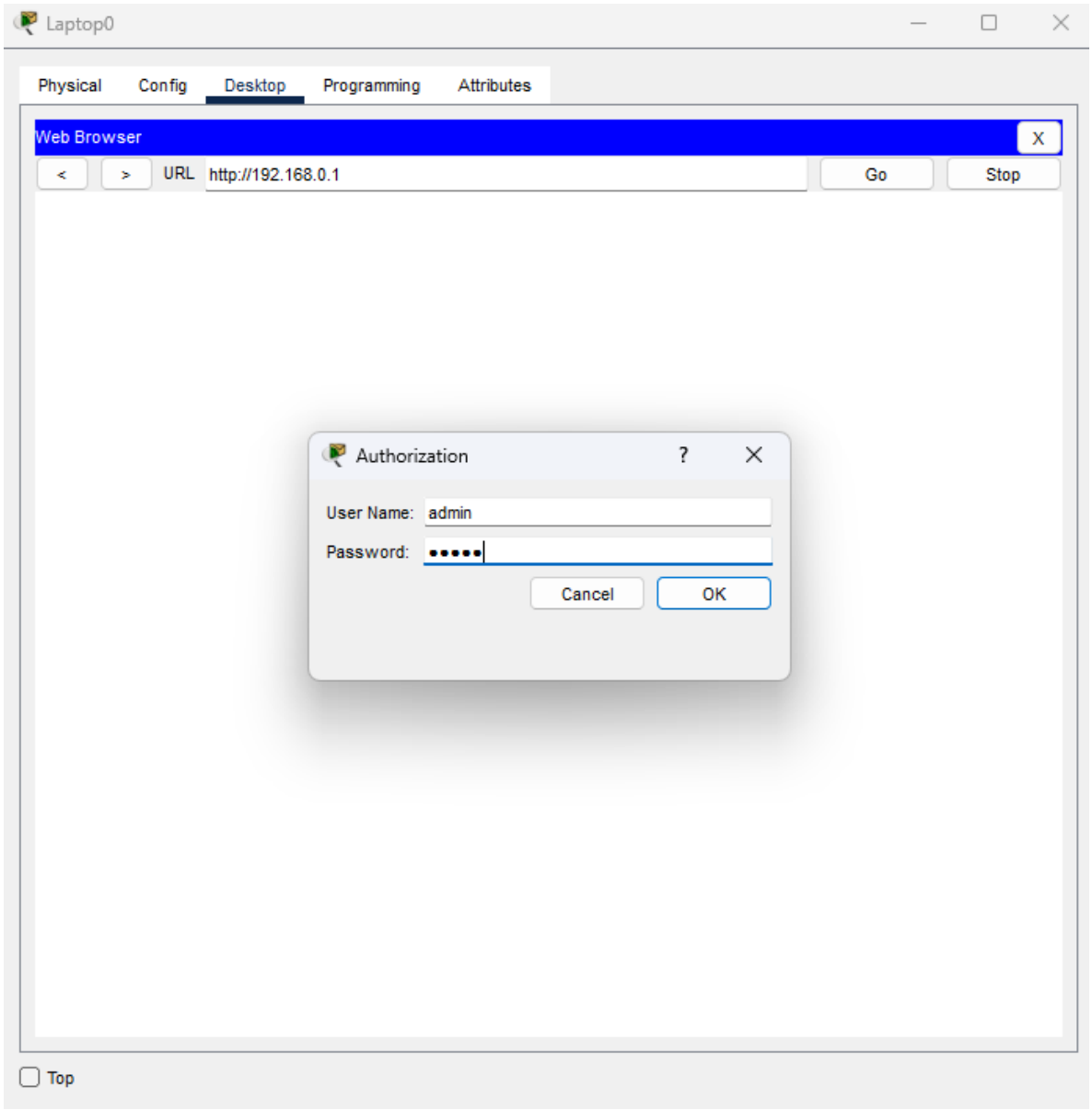


Figure 26. Authenticating to Configure the Router

- In Internet Setup, we select the Static IP option and enter the IP address 65.148.77.200 with a subnet mask of 255.255.255.0

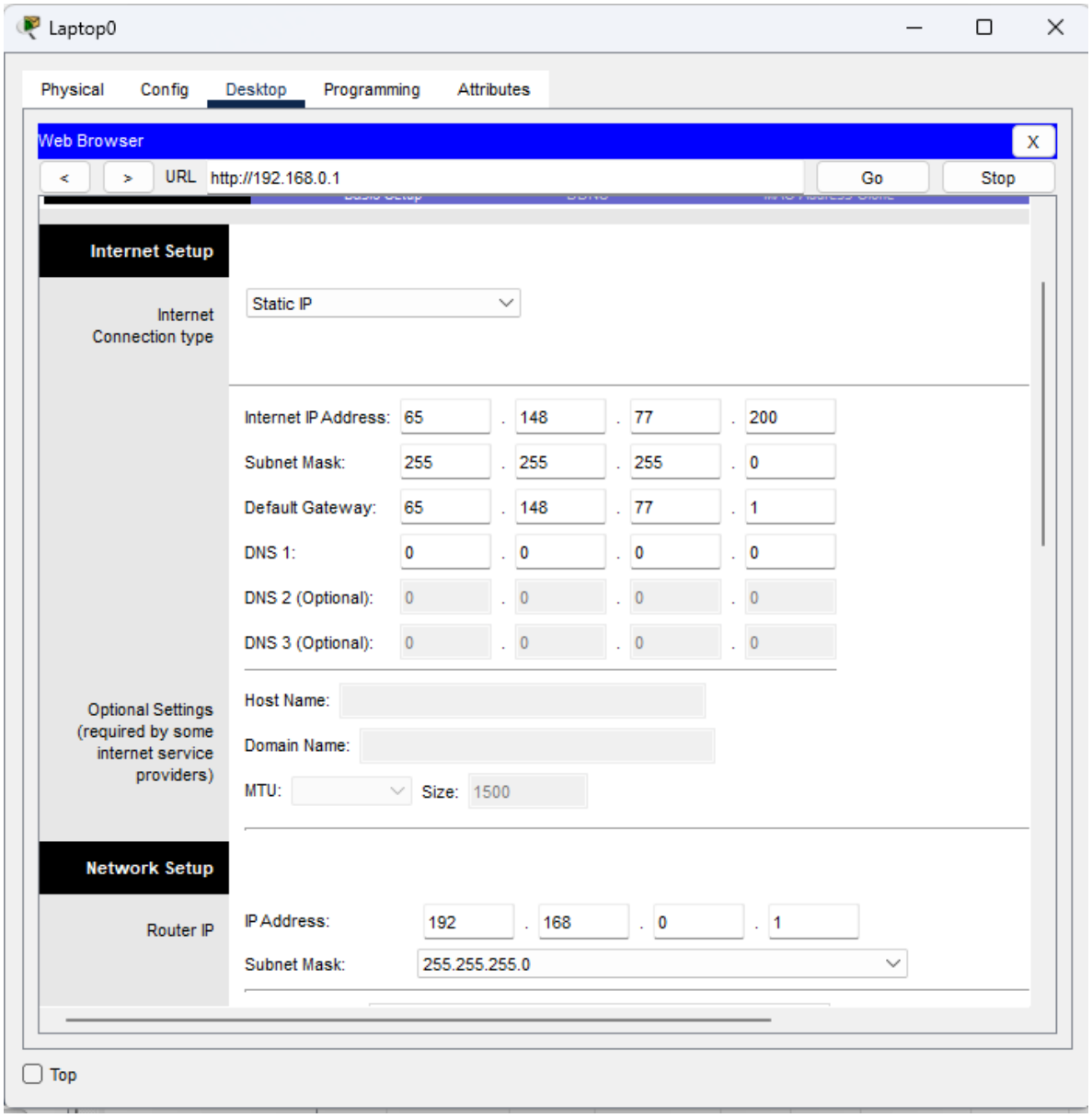


Figure 27. Internet Setup of the Wireless Router

- We go to the "Wireless" tab and enter the wireless network identifier (SSID)

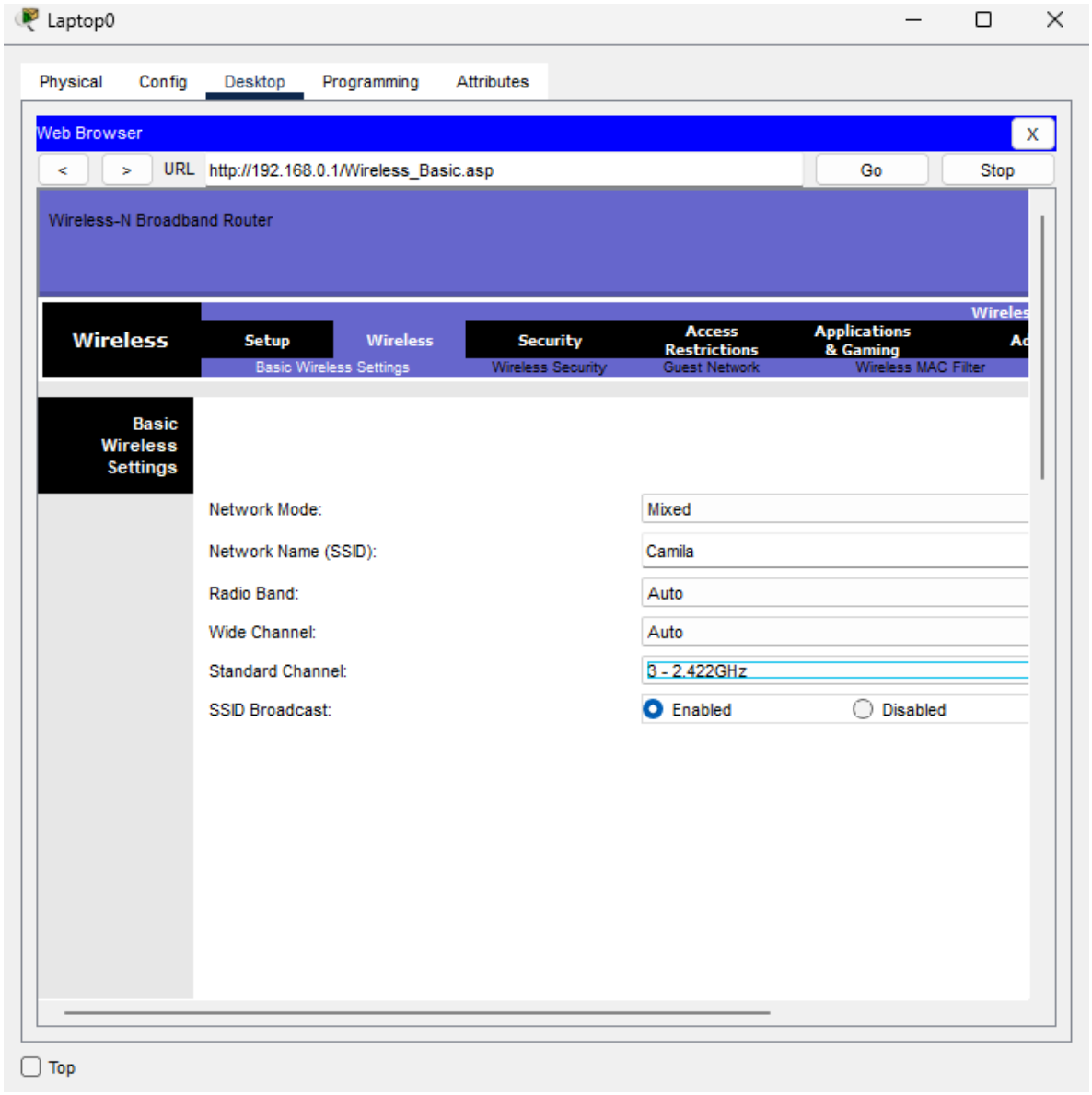


Figure 28. Basic Wireless Settings of the router

- When configuring a specific channel, we can observe that there are 11 options, each indicating the channel and its frequency band. In our case, we select channel 3

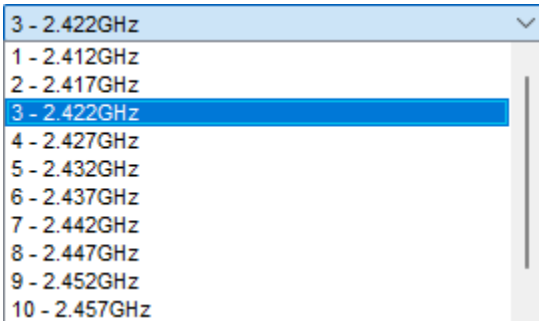


Figure 29. Router Channels Options

- We go to Wireless Security and set the security mode (WPA2-PSK) and encryption (AES). Finally, we set the access key for the router from mobile devices (SEGURIDAD_R)

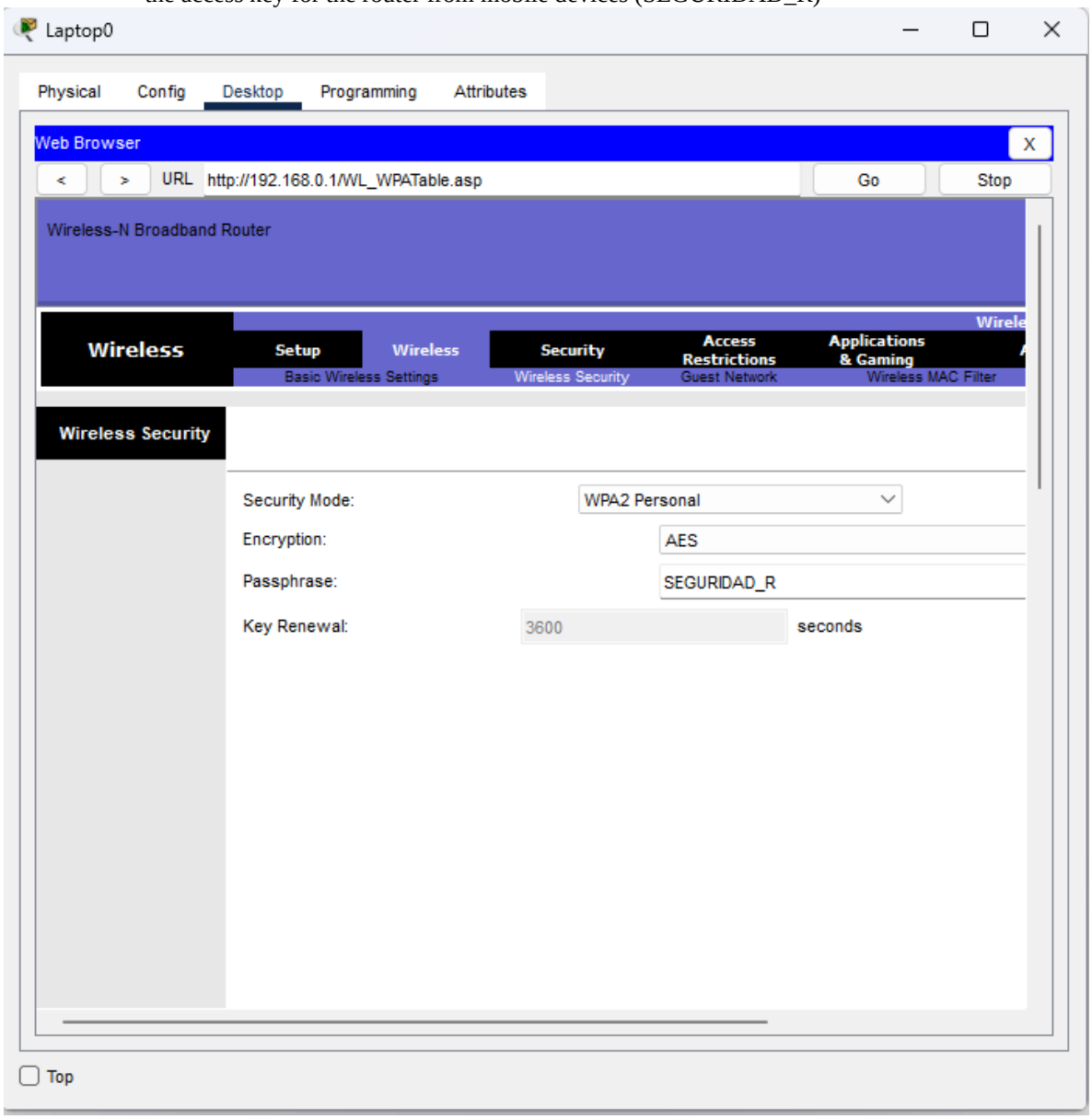


Figure 30. Wireless Security of the router

- We go to Network Setup and in DHCP Settings, we specify the range of IP addresses that the router will

assign

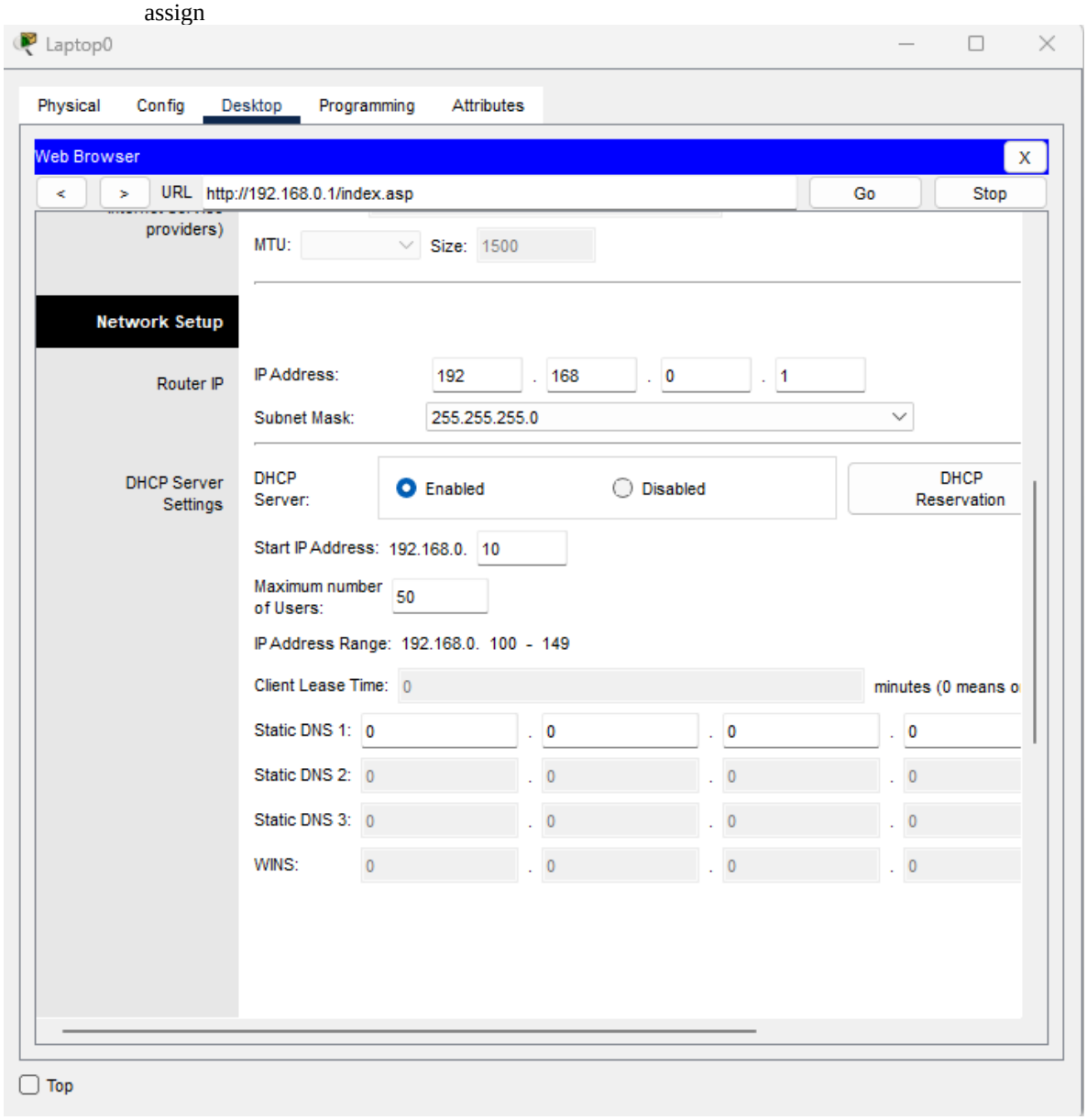


Figure 31. Configuring and Assigning IP Address Range on the Wireless Router

- We save the router configuration and open the access point configuration. There, we set the SSID, security (WPA2-PSK), and the access key (SEGURIDAD_AP)

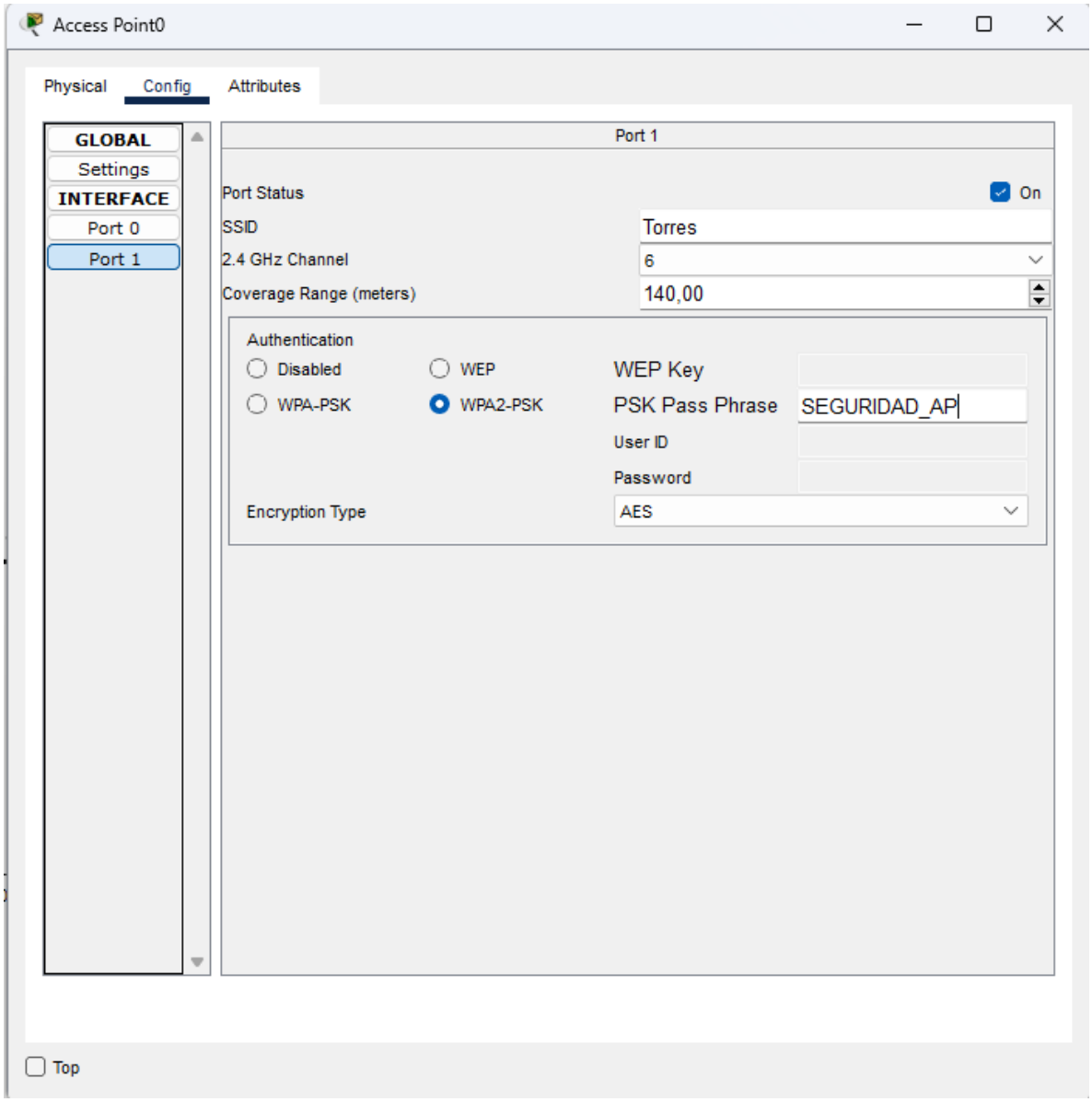


Figure 32. Configuring Access Point

- From Laptop0, we open PC Wireless and connect to the wireless router whose SSID is the one we

configured earlier (*Image 8*)

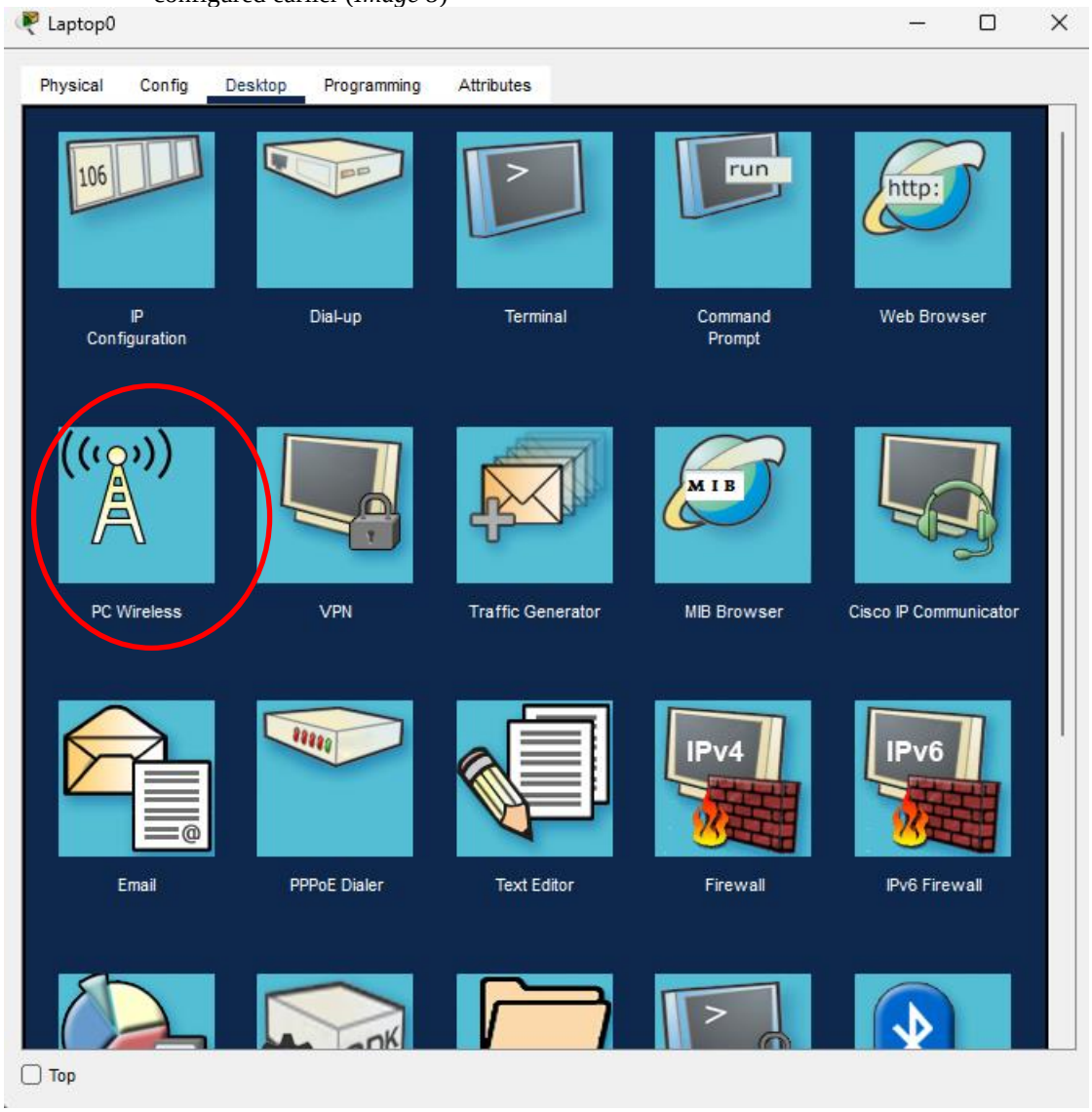


Figure 33. Opening PC Wireless from Laptop0

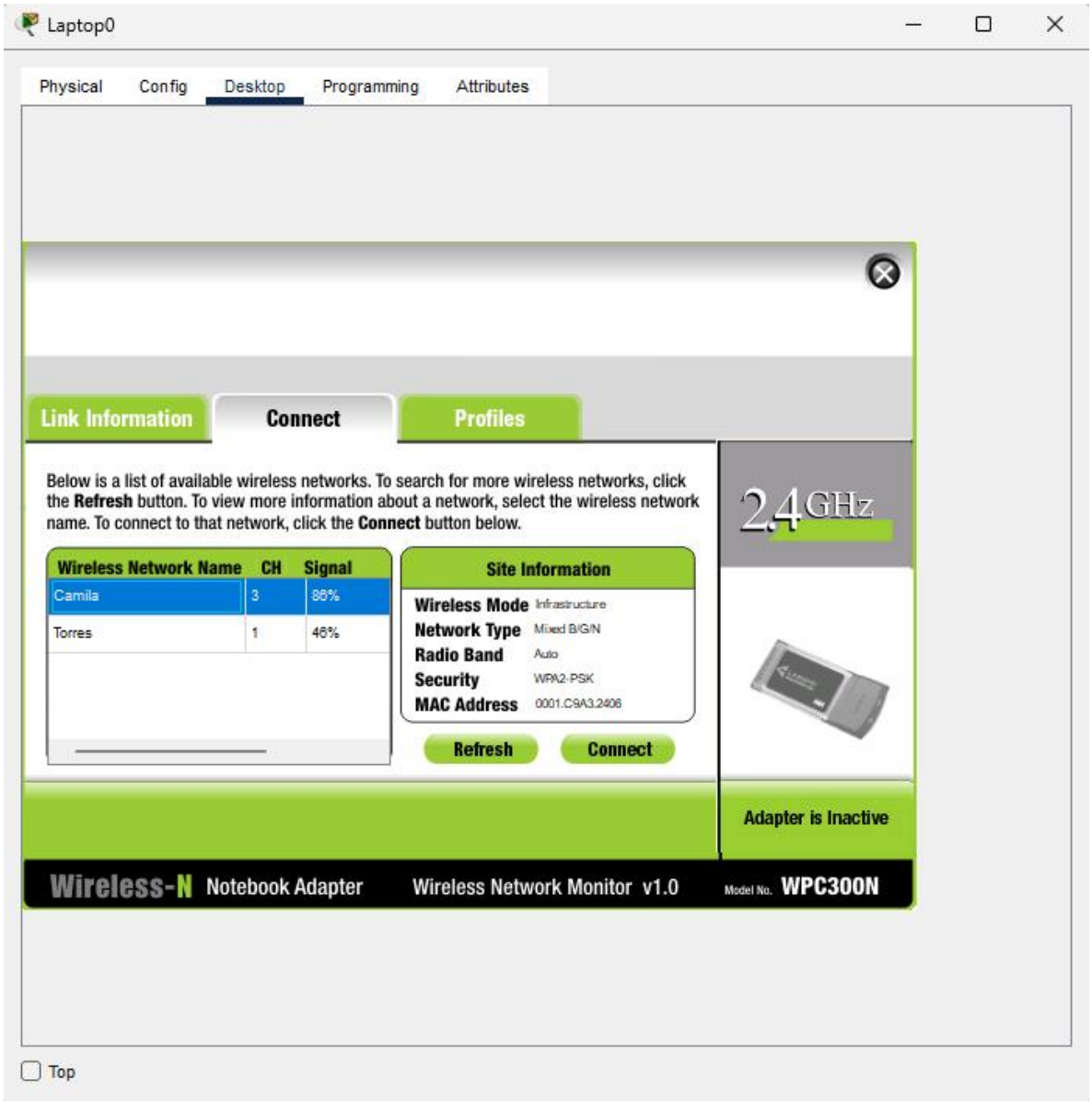


Figure 34. Connecting Laptop0 to the Wireless Router

- We enter the router's access key and connect

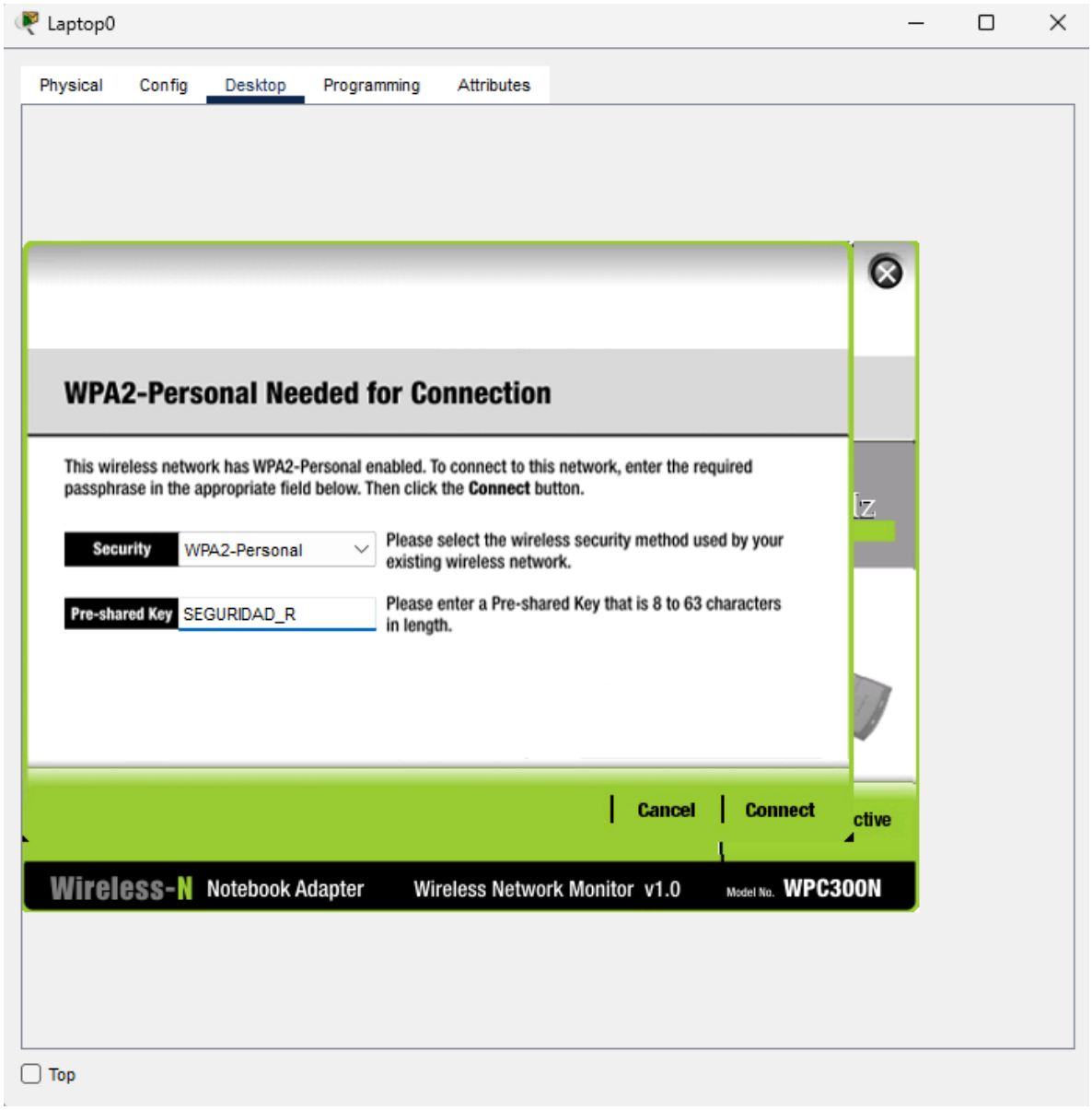


Figure 35. Connecting to the Wireless Router from Laptop0

- From Smartphone0, we go to the settings and enter the SSID, authentication, and security key that we configured on the router

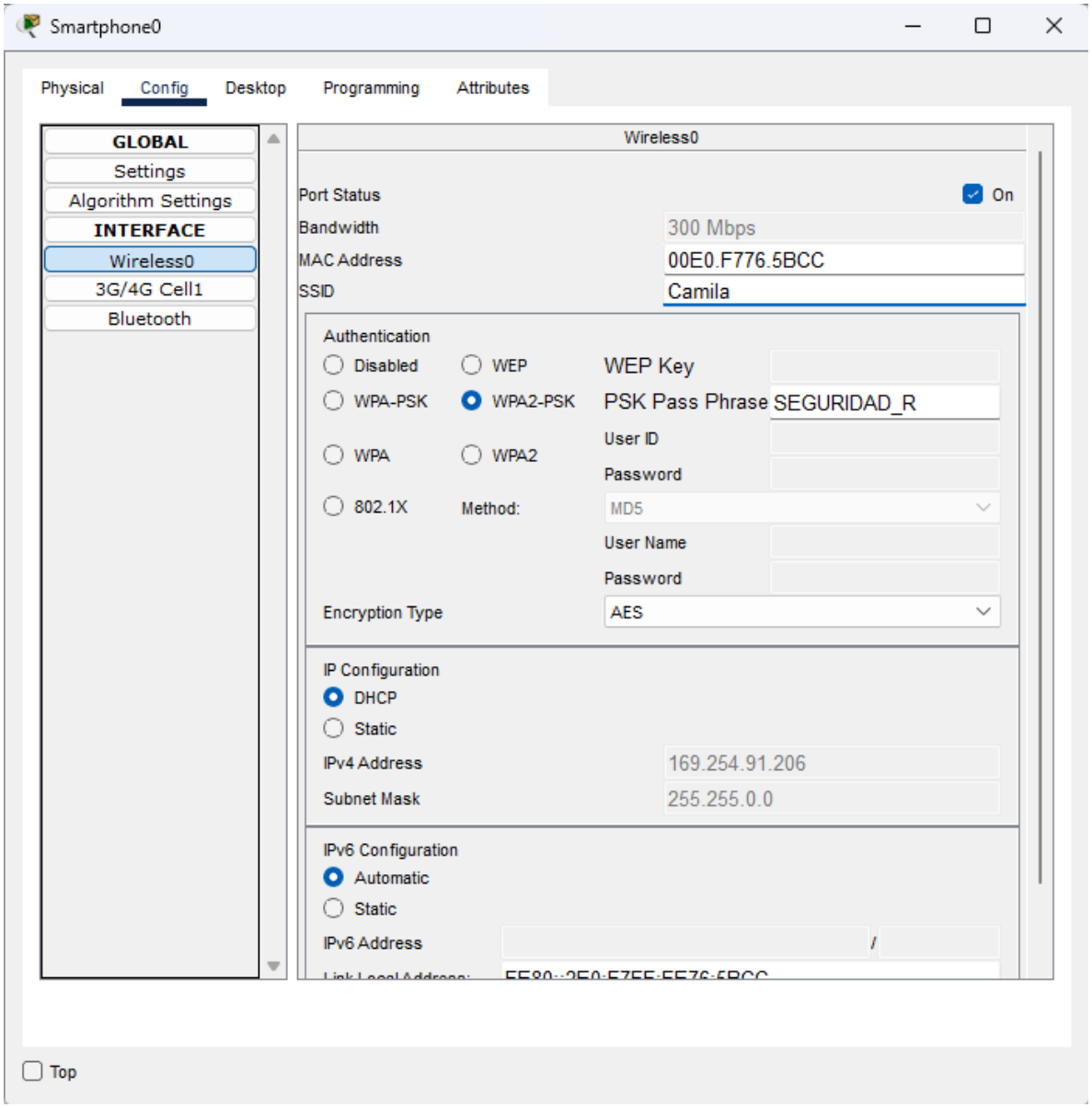


Figure 36. Configuring SmartPhone0 to Establish Connection with the Wireless Router

- Now, from Laptop1, we open PC Wireless and select the Access Point

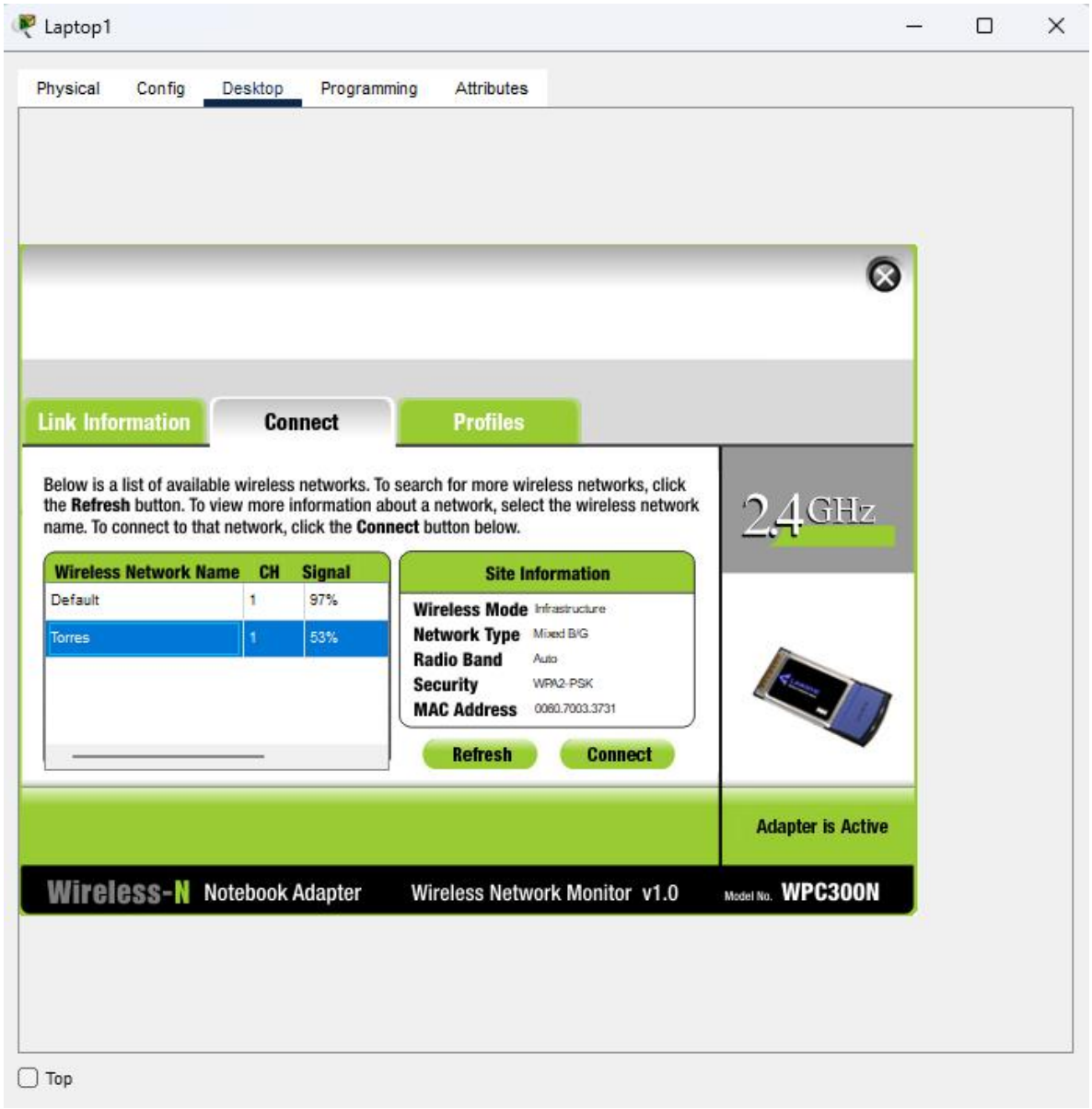


Figure 37. Connecting Laptop1 to Access Point

- We enter the access key for the Access Point and connect

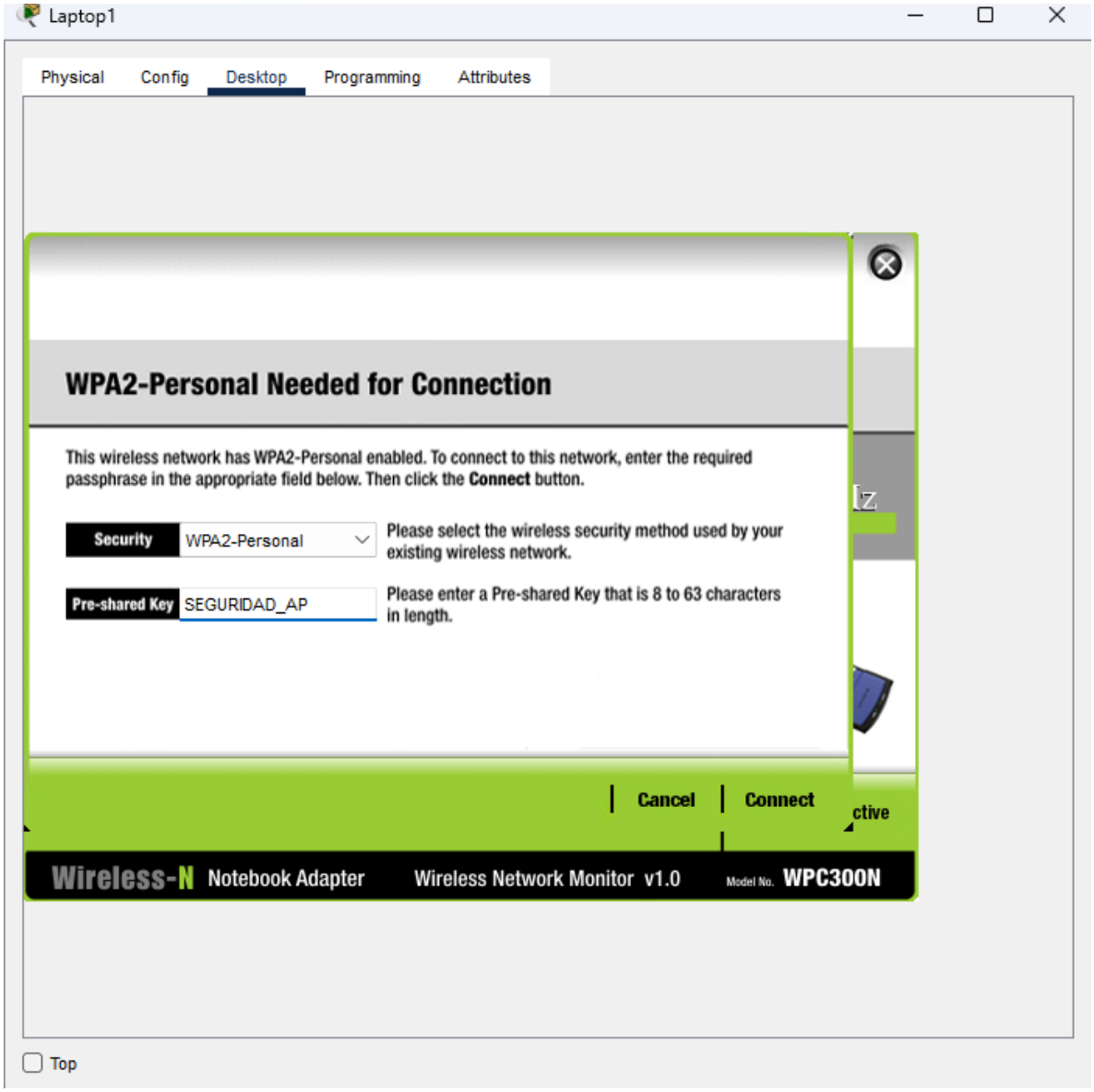


Figure 38. Connecting to Access Point from Laptop1

- From Smartphone1, we go to the settings and enter the SSID, authentication, and security key that we configured on the Access Point

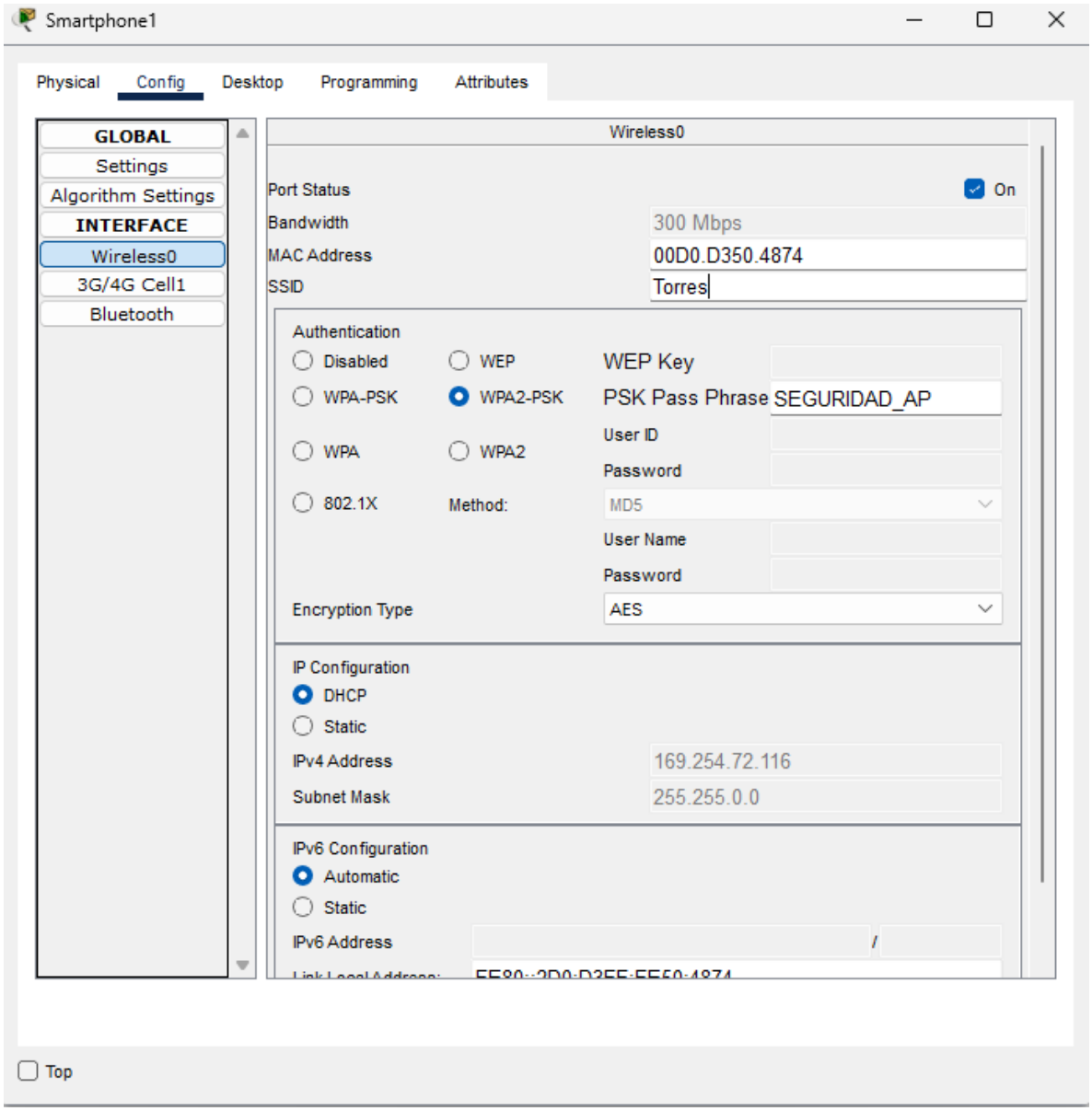


Figure 39. Configuring SmartPhone1 to Connect to the Access Point

- Now, we assign static IP addresses to both Laptop1 and Smartphone1 within the range 65.148.77.100 to 65.148.77.120. In our case, the assignment is as follows: Laptop1 - 65.148.77.101, Smartphone1 - 65.148.77.119

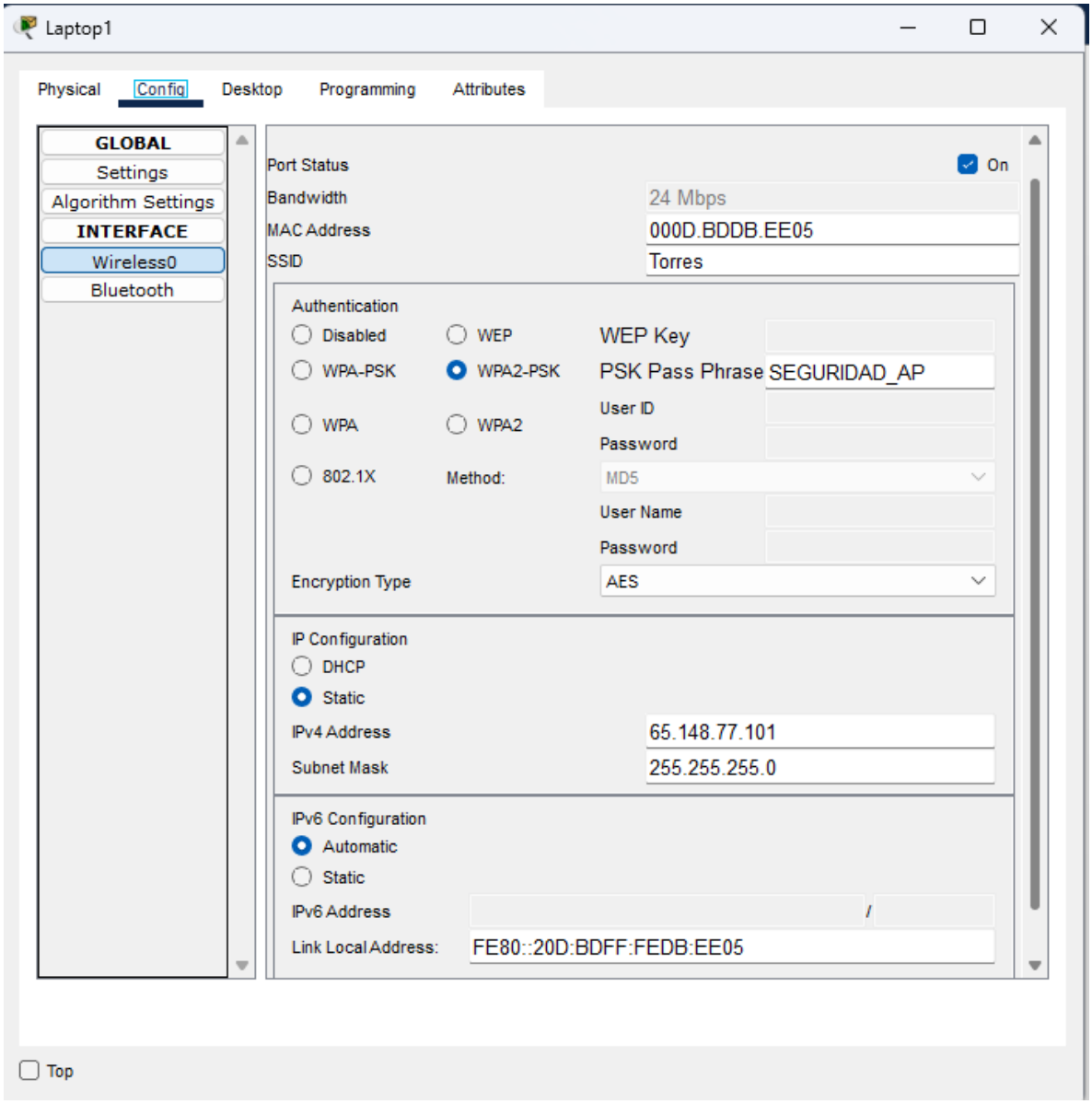


Figure 40. Assigning Static IP and Subnet Mask to Laptop1

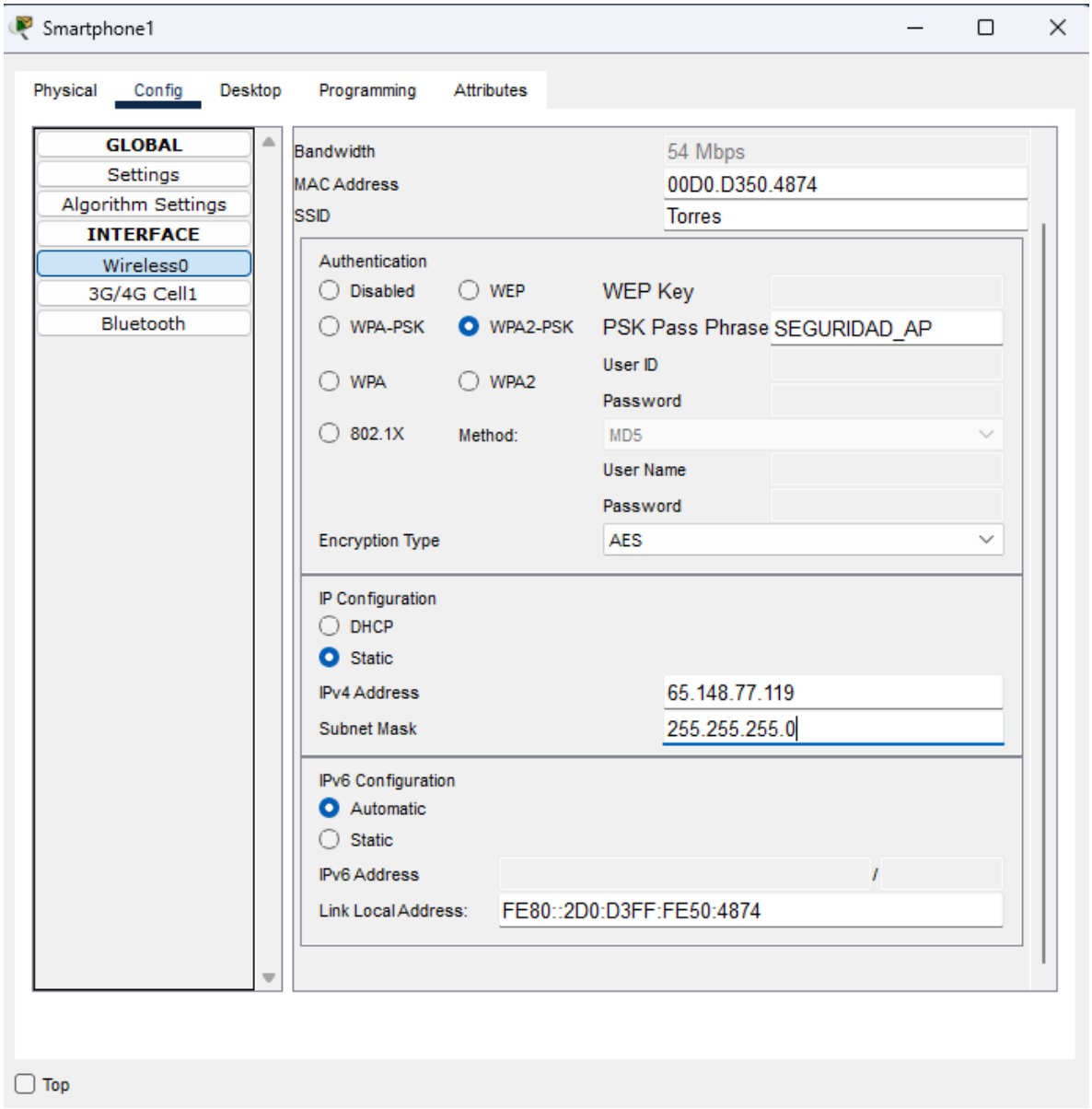


Figure 41. Assigning Static IP and Subnet Mask to Smartphone1

- We obtain our corrected and completed network

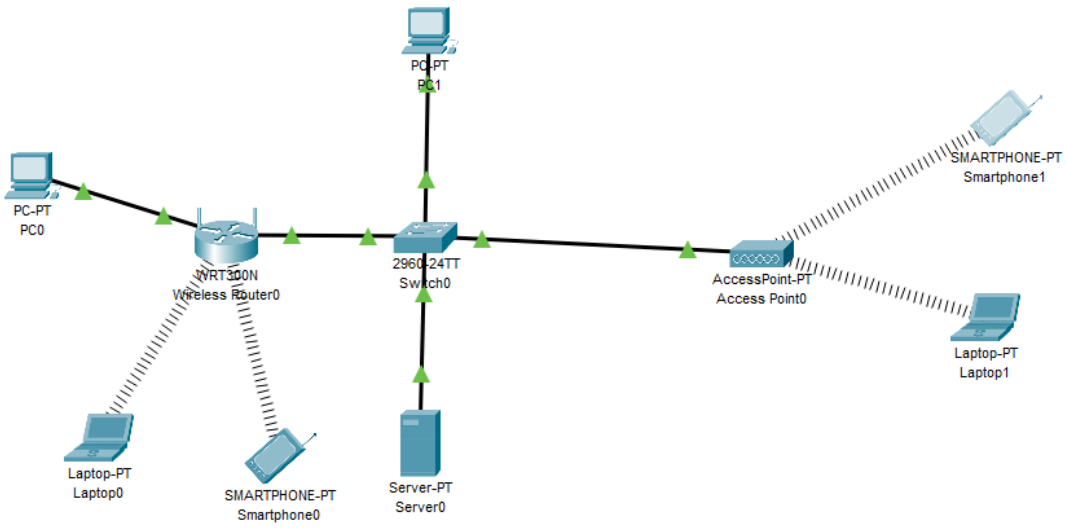


Figure 42. Basic Wi-Fi Configuration Diagram Completed

5.2. Connection tests between devices

- **Pinging from PC0**

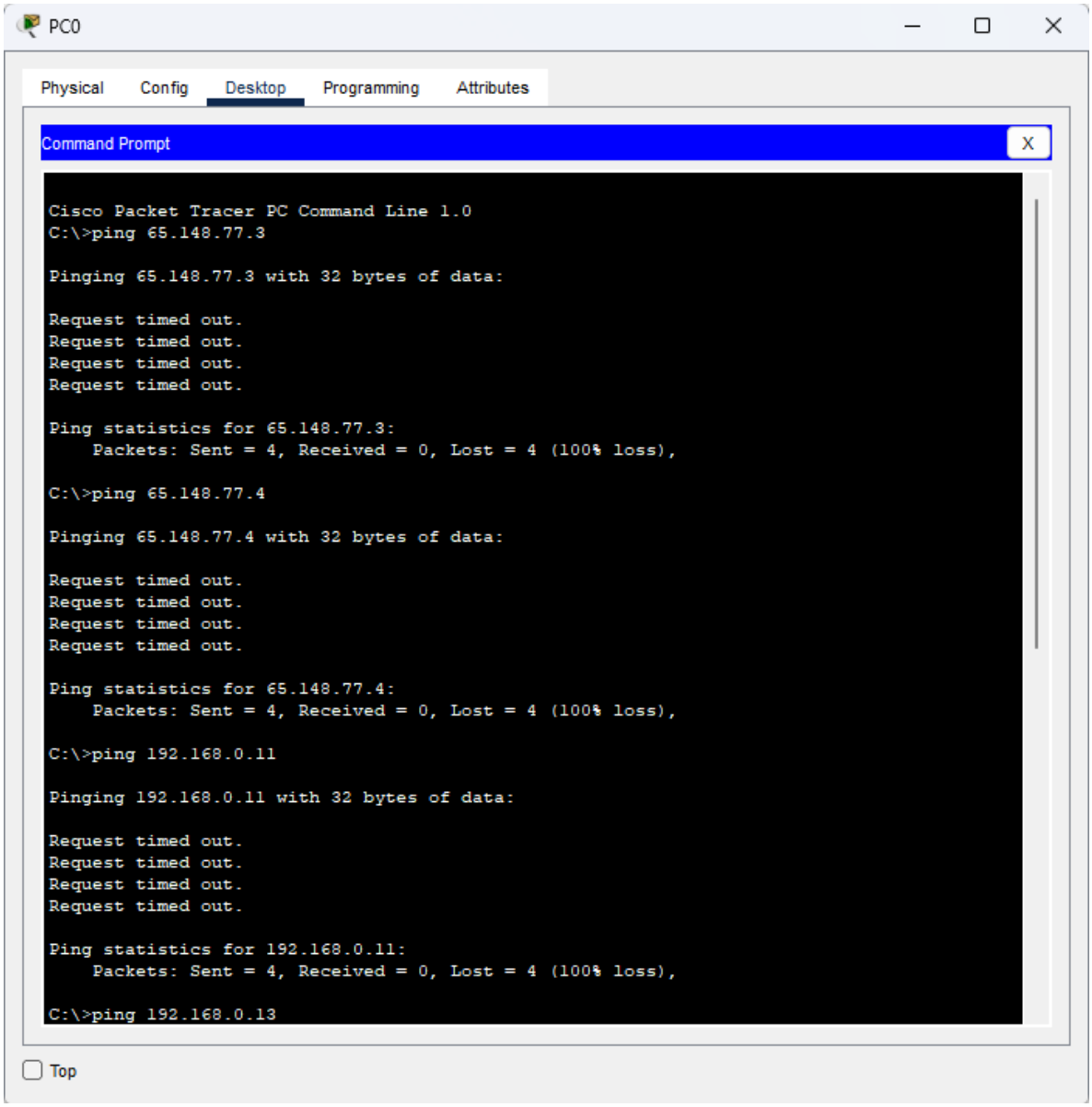


Figure 43. First Ping Tests on PC0

- **Pinging from PC1**

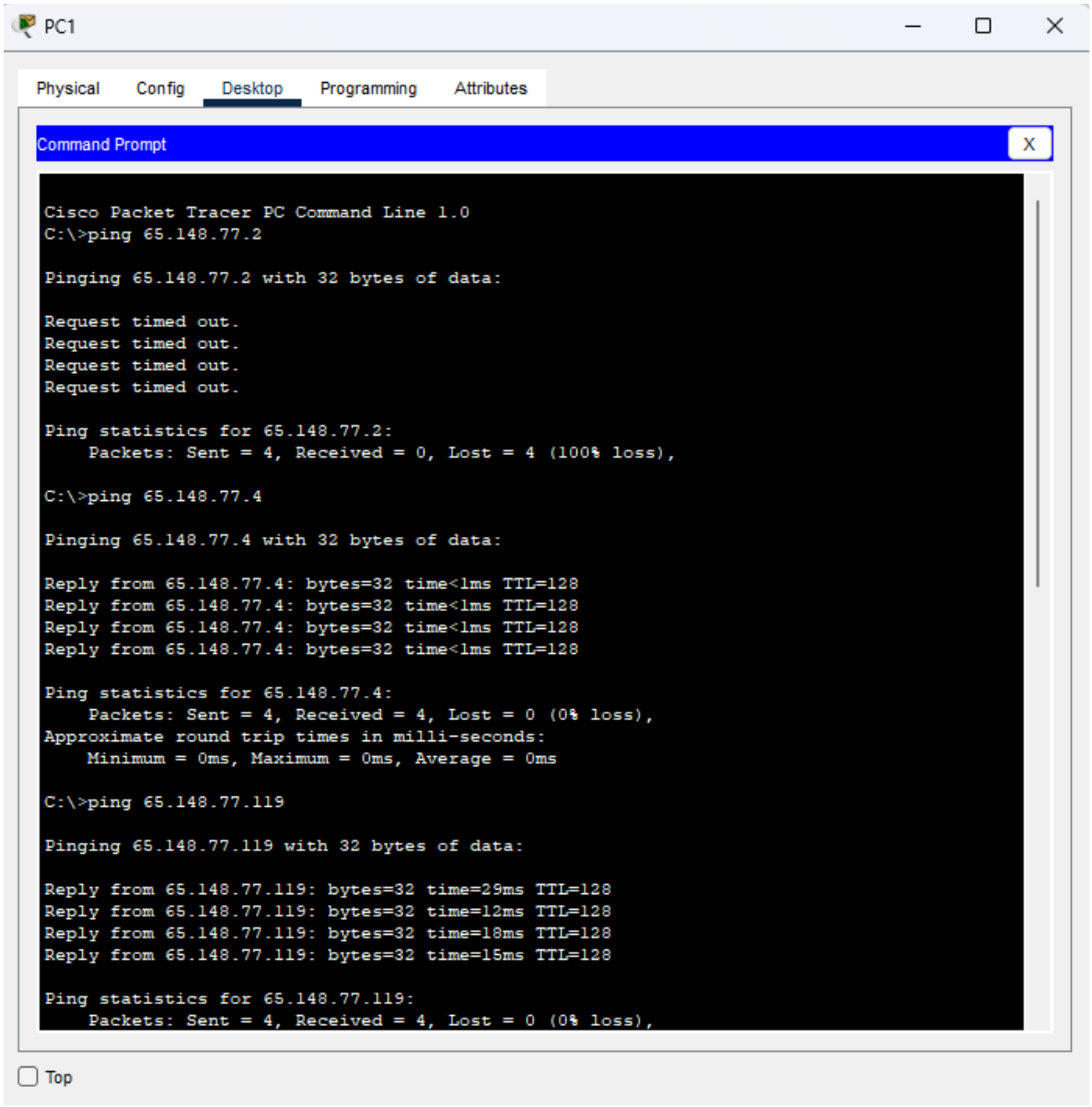


Figure 44. First Ping Tests on PC1

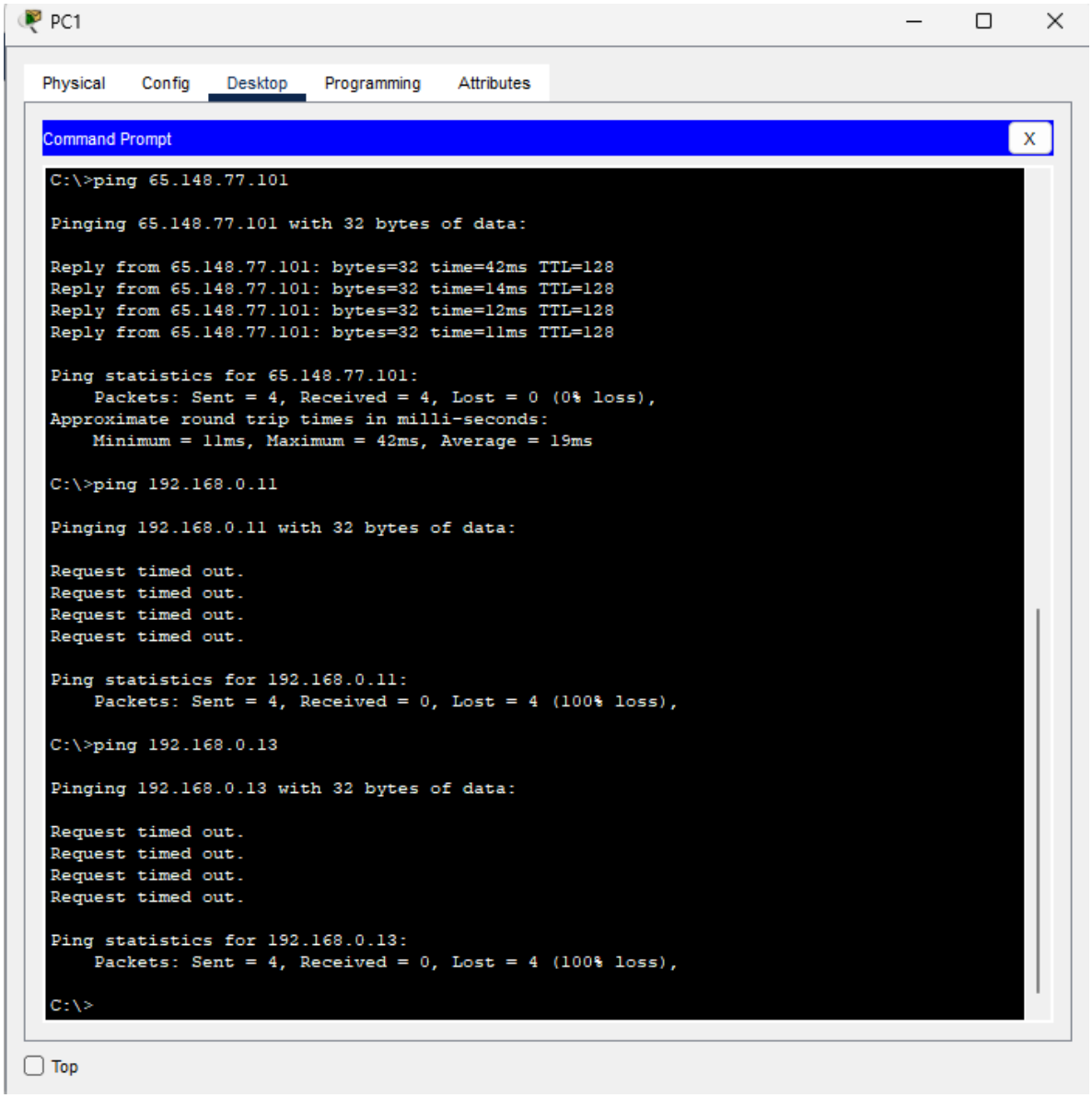


Figure 45. Second Ping Tests on PC1

- **Pinging from Server0**

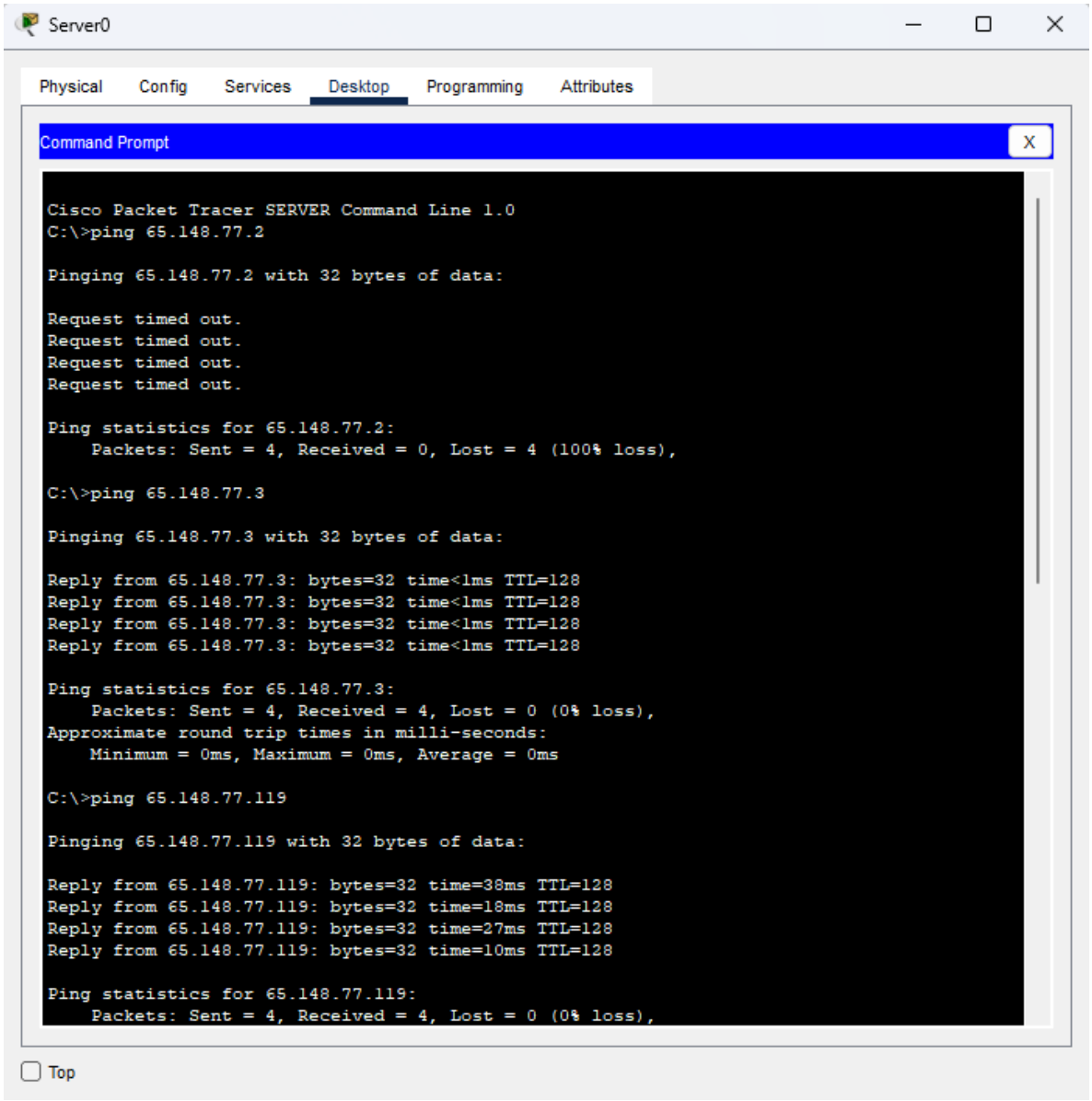


Figure 46. First Ping Tests on Server0

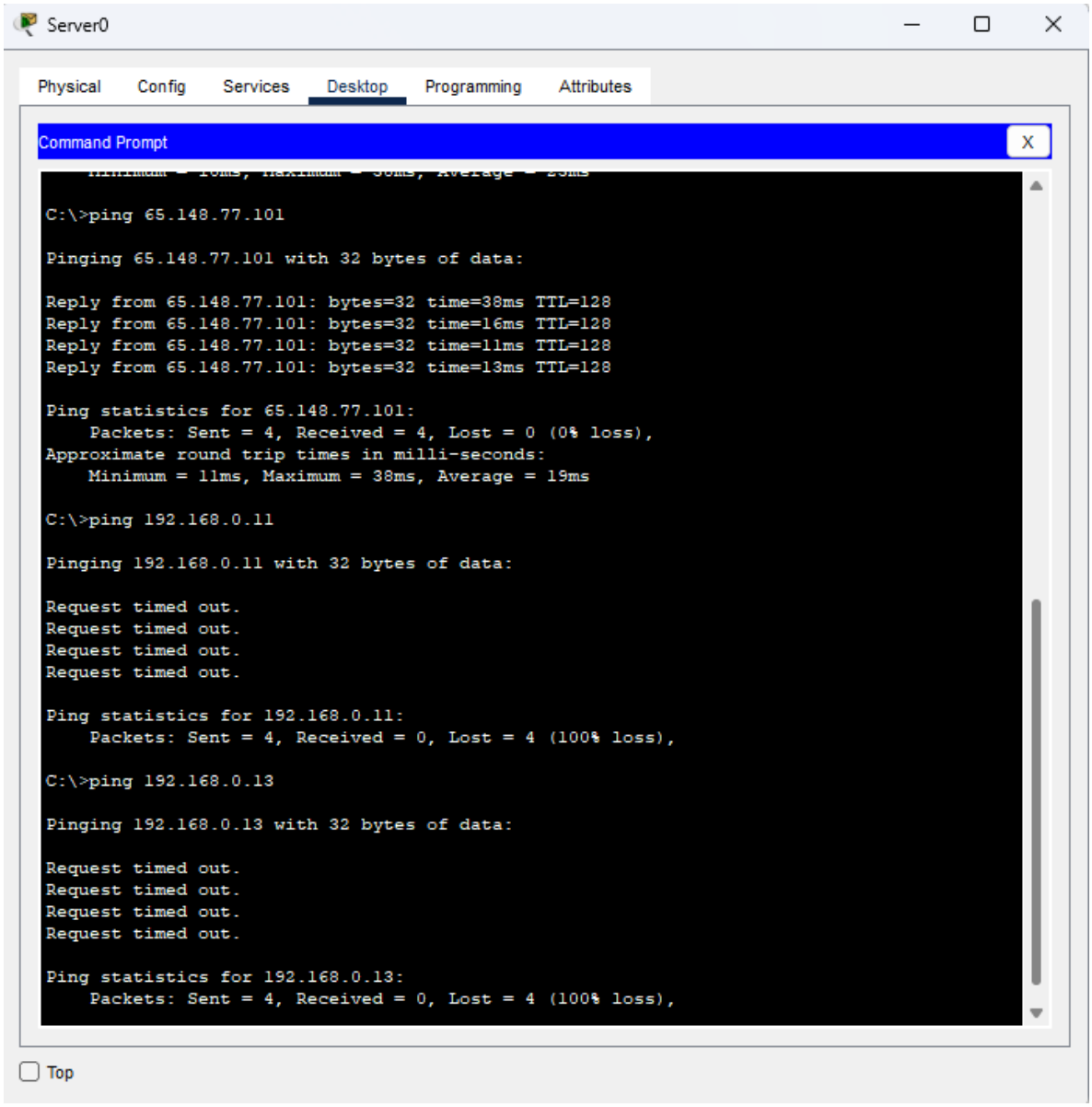


Figure 47. Second Ping Tests on Server0

- **Pinging from Smartphone1**

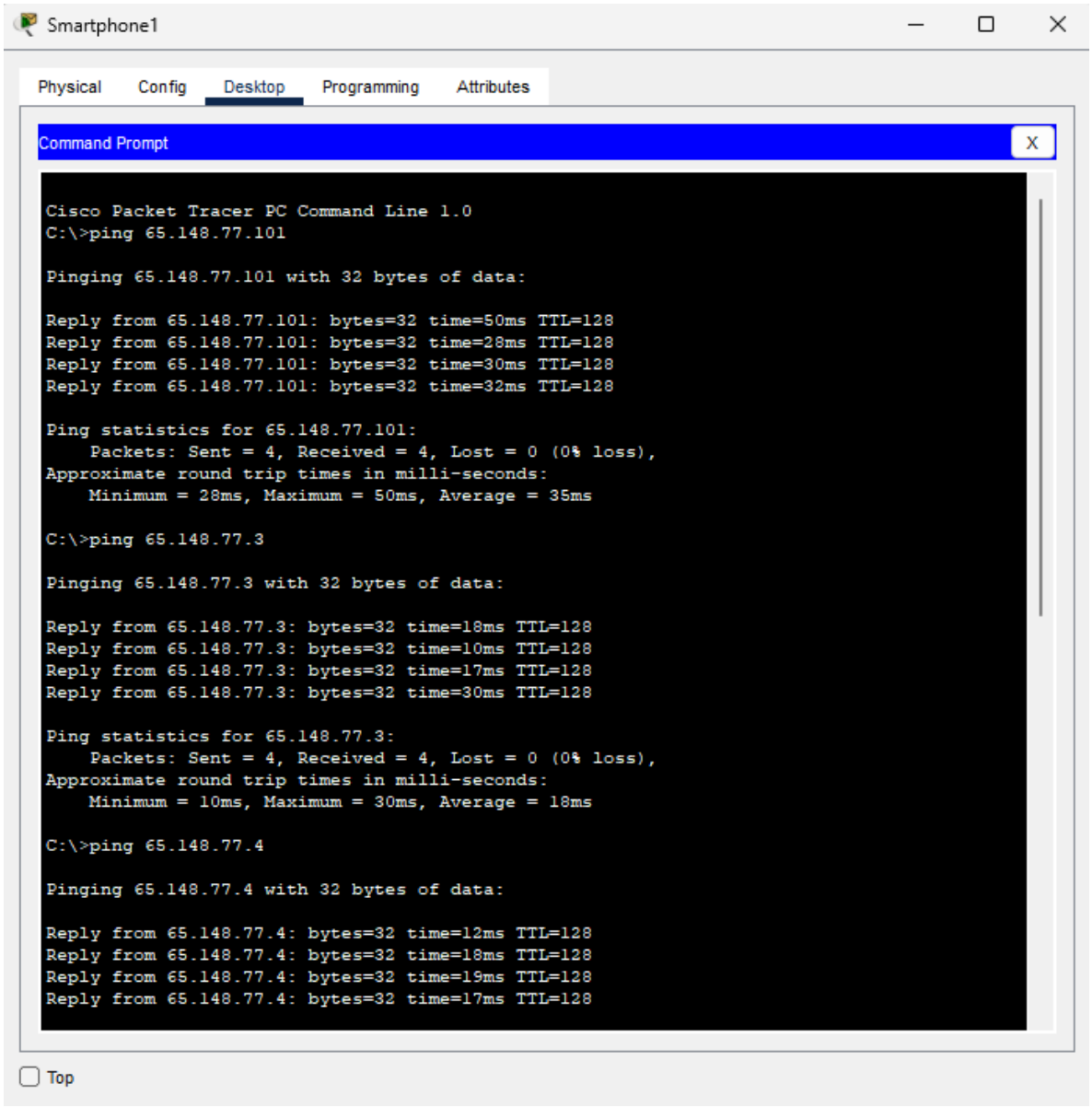


Figure 48. First Ping Tests on Smartphone1

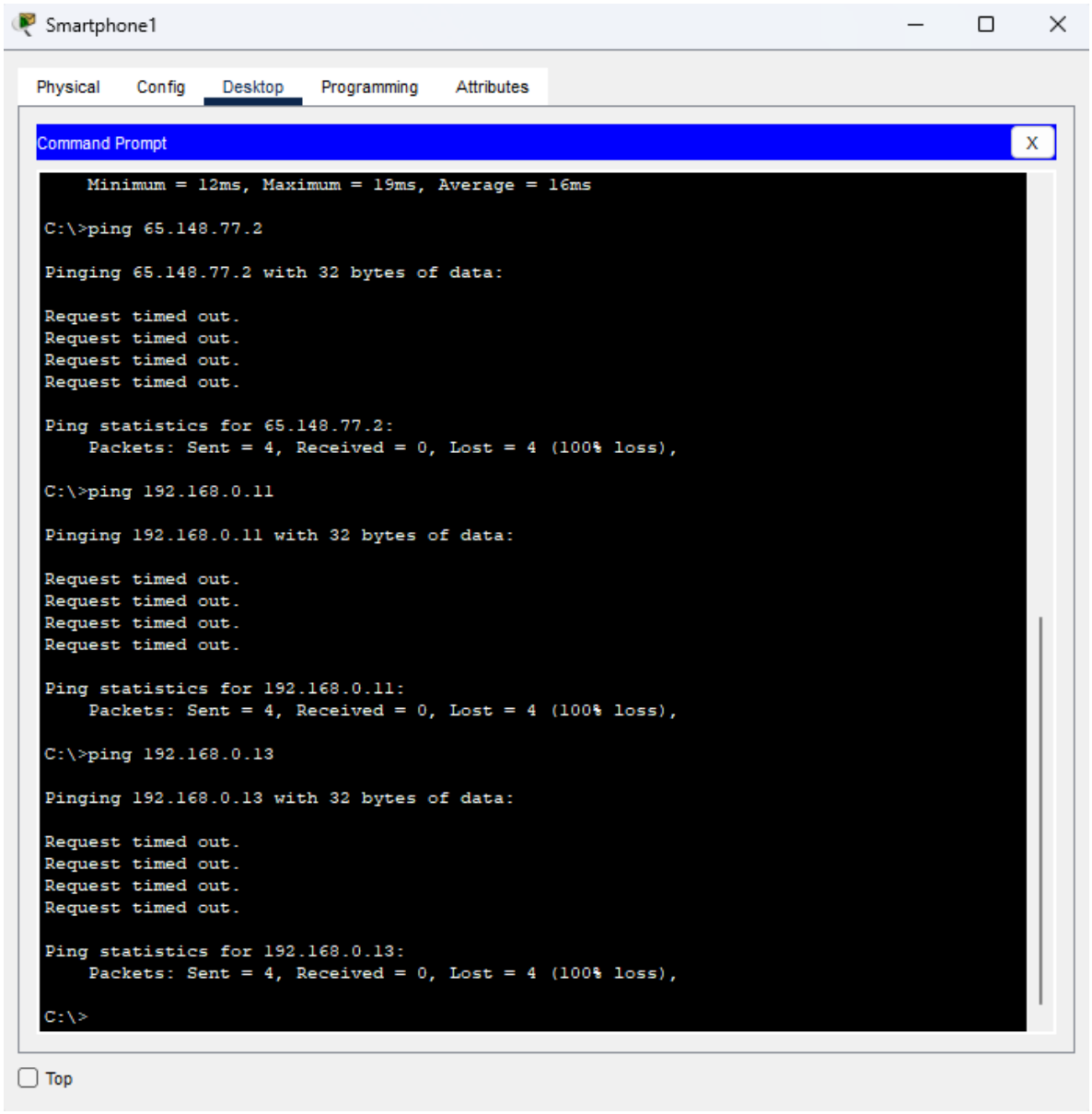


Figure 49. Second Ping Tests on Smartphone1

- **Pinging from Laptop1**

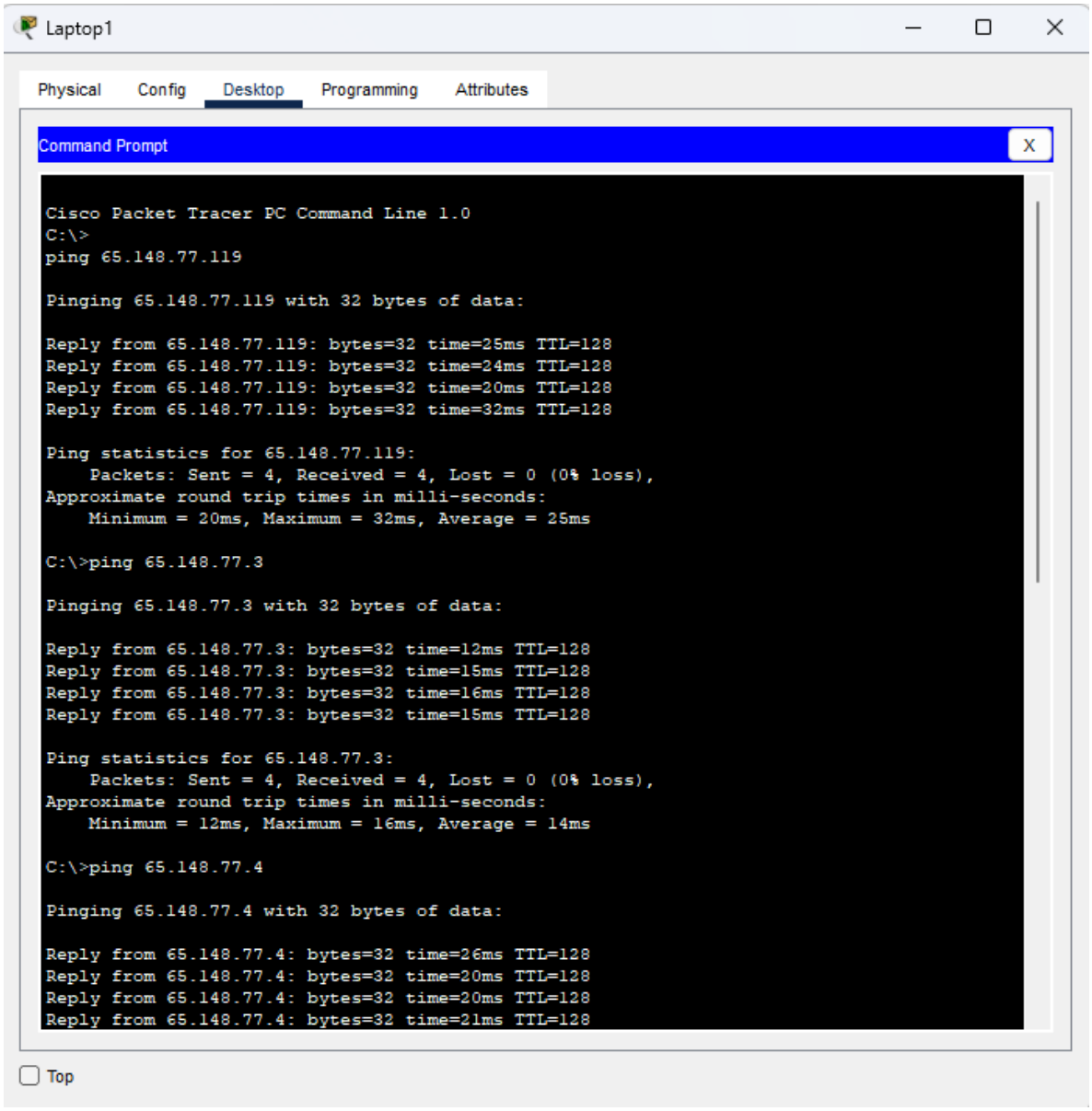


Figure 50. First Ping Tests on Laptop1

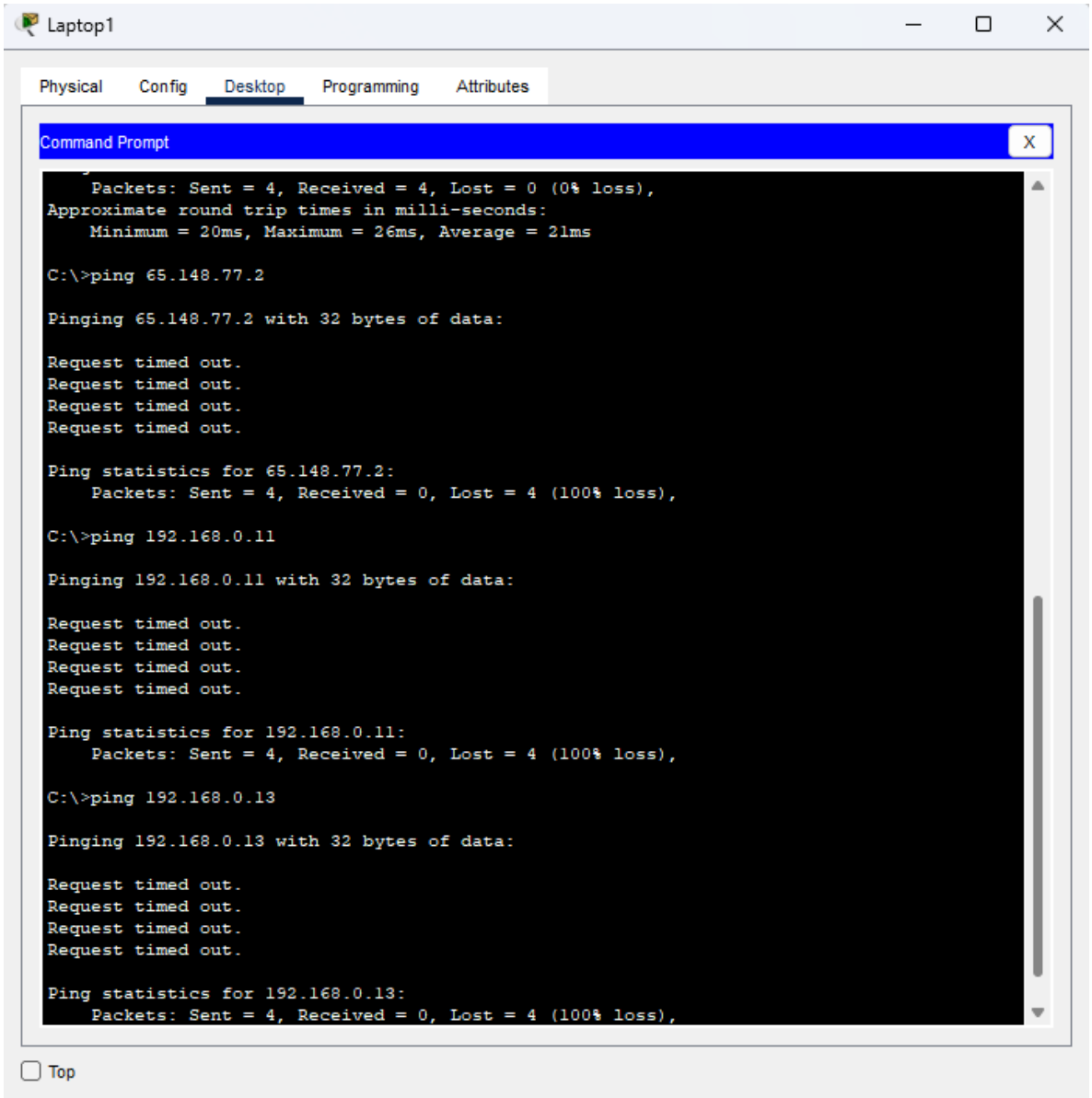


Figure 51. Second Ping Tests on Laptop1

- **Pinging from Smartphone0**

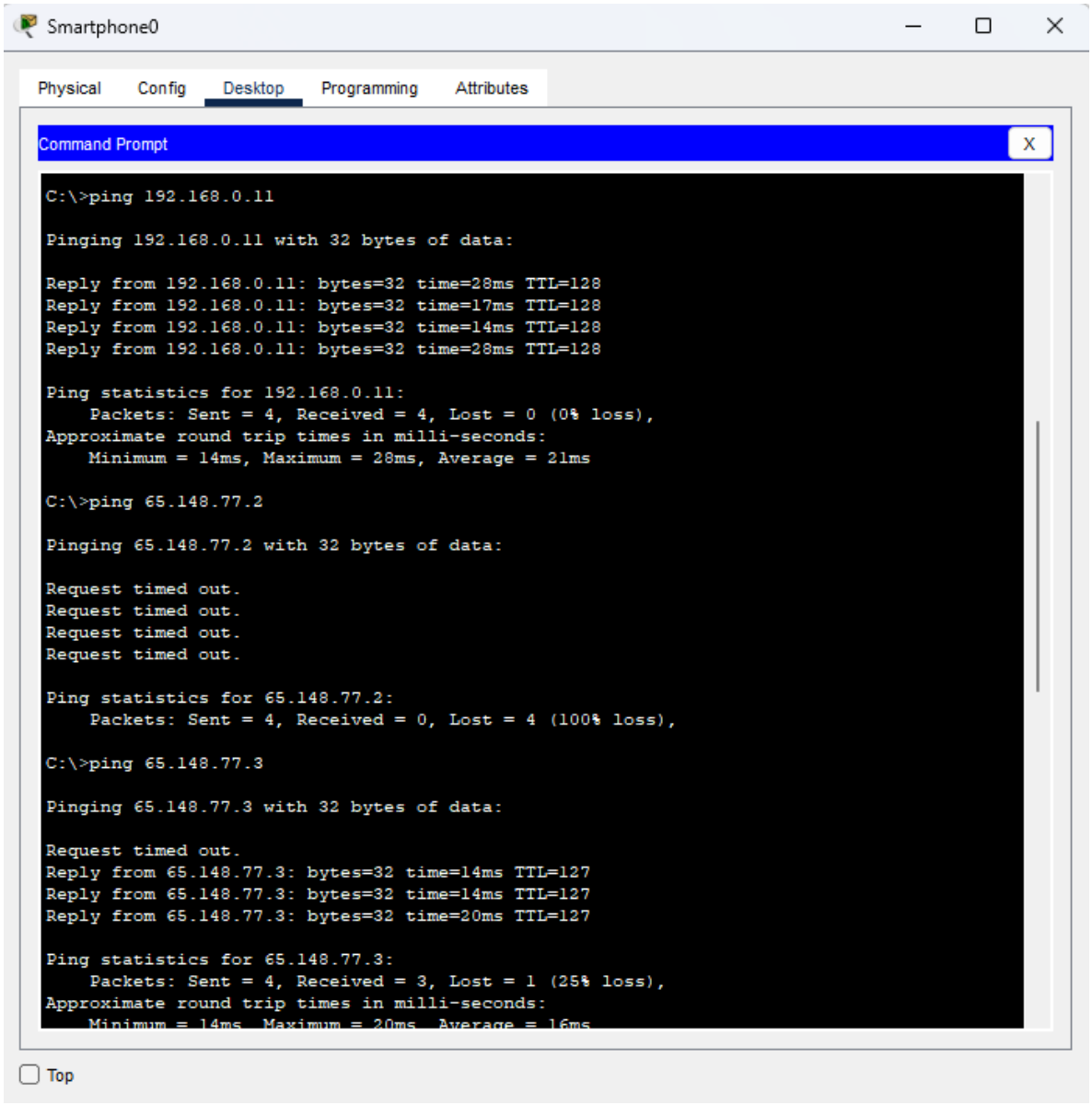


Figure 52. First Ping Tests on Smartphone0

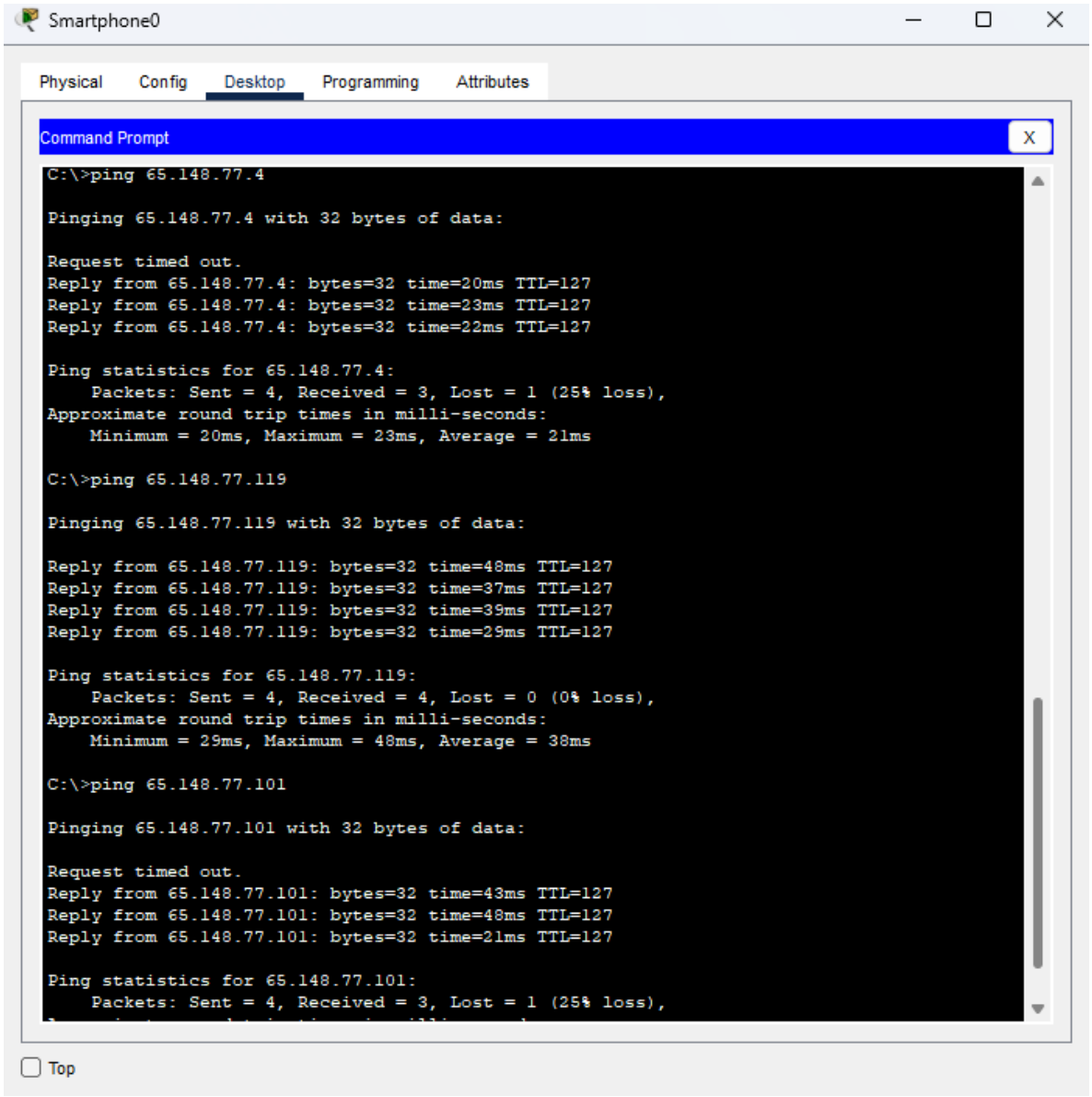


Figure 53. Second Ping Tests on Smartphone0

- **Pinging from Laptop0**

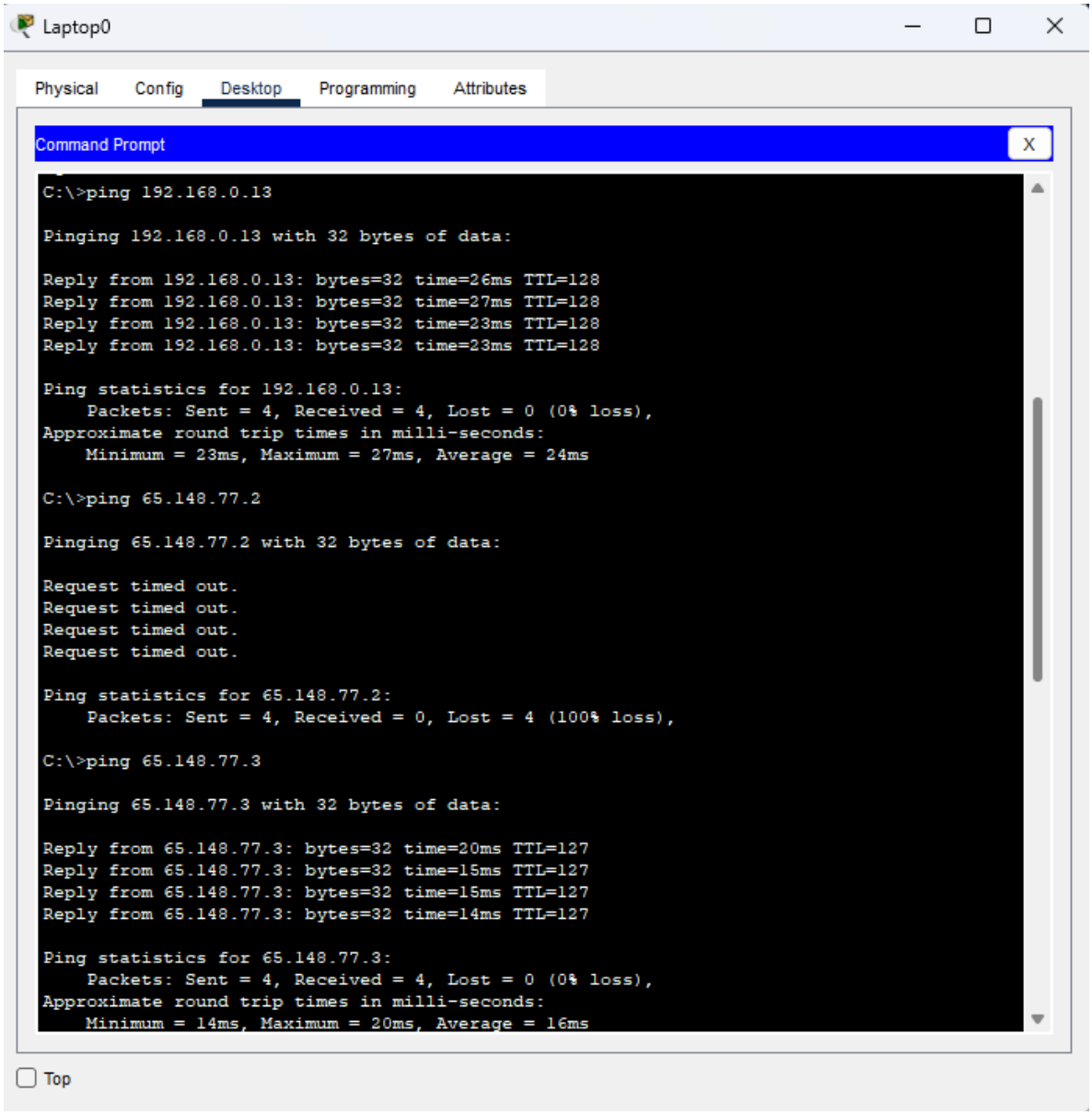


Figure 54. First Ping Tests on Laptop0

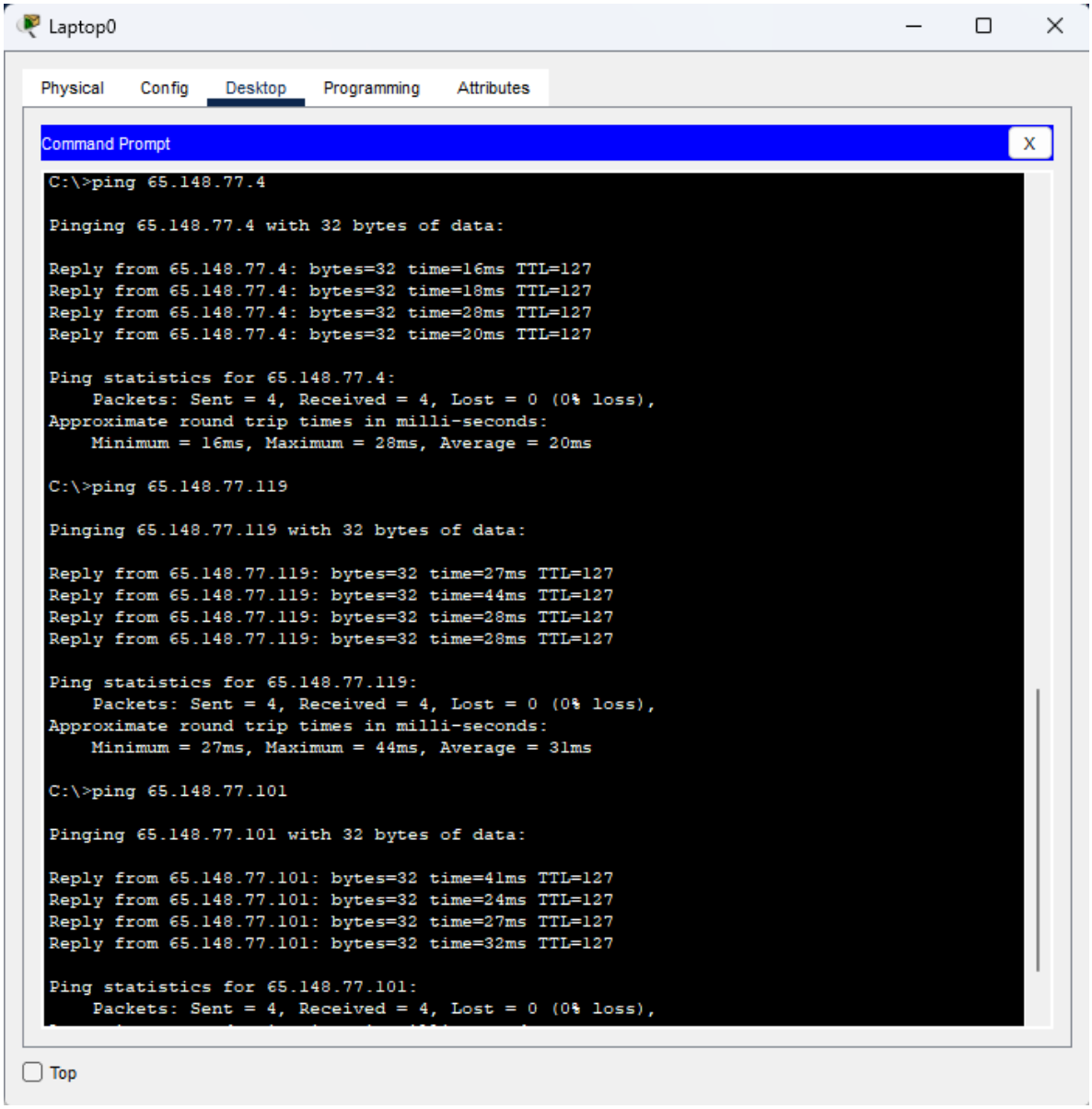
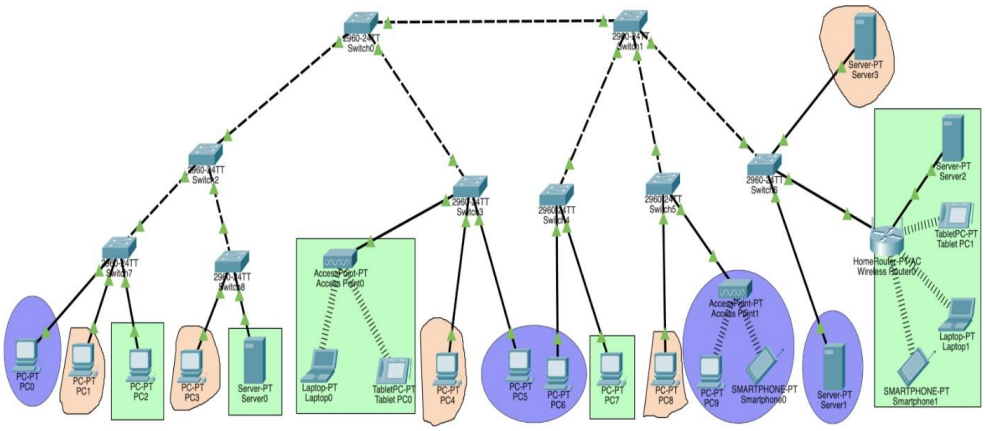


Figure 55. Second Ping Tests on Laptop0

As we can see, some devices cannot ping each other, such as PC1 and Smartphone0, because they are in different subnets. The devices in different subnets require proper routing to communicate. Since they behave as separate private networks, any attempt to communicate across subnets fails.

6. Configuration of Wired and Wireless LAN

Now we are going to create the following Packet Tracer configuration. First, we will establish all the connections, and finally, we will configure the respective VLANs. connections, and finally, we will configure the respective VLANs.



First, we choose the devices we are going to use, including 2960-24T switches, PC-PT, server PT, laptop PT, tabletPC-PT, smartphone-PT, and homeRouter-PT-AC wireless. Then, we establish most of the connections between the devices.

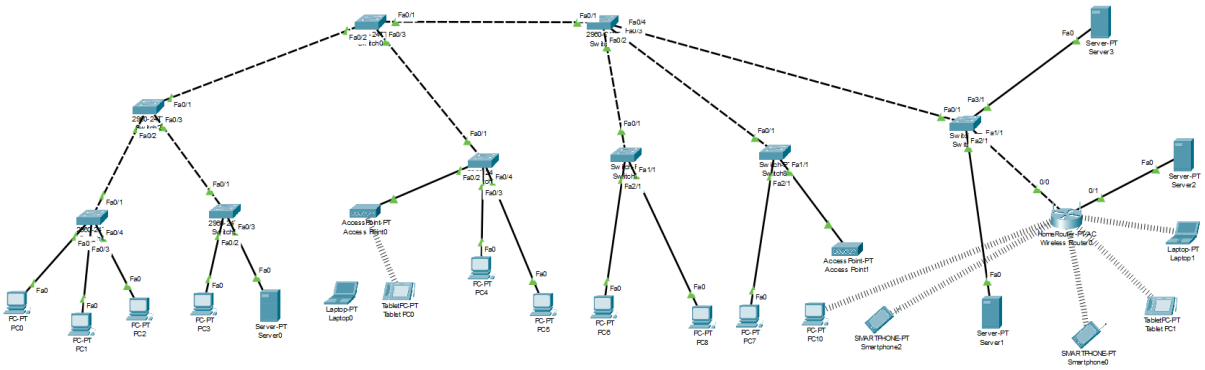
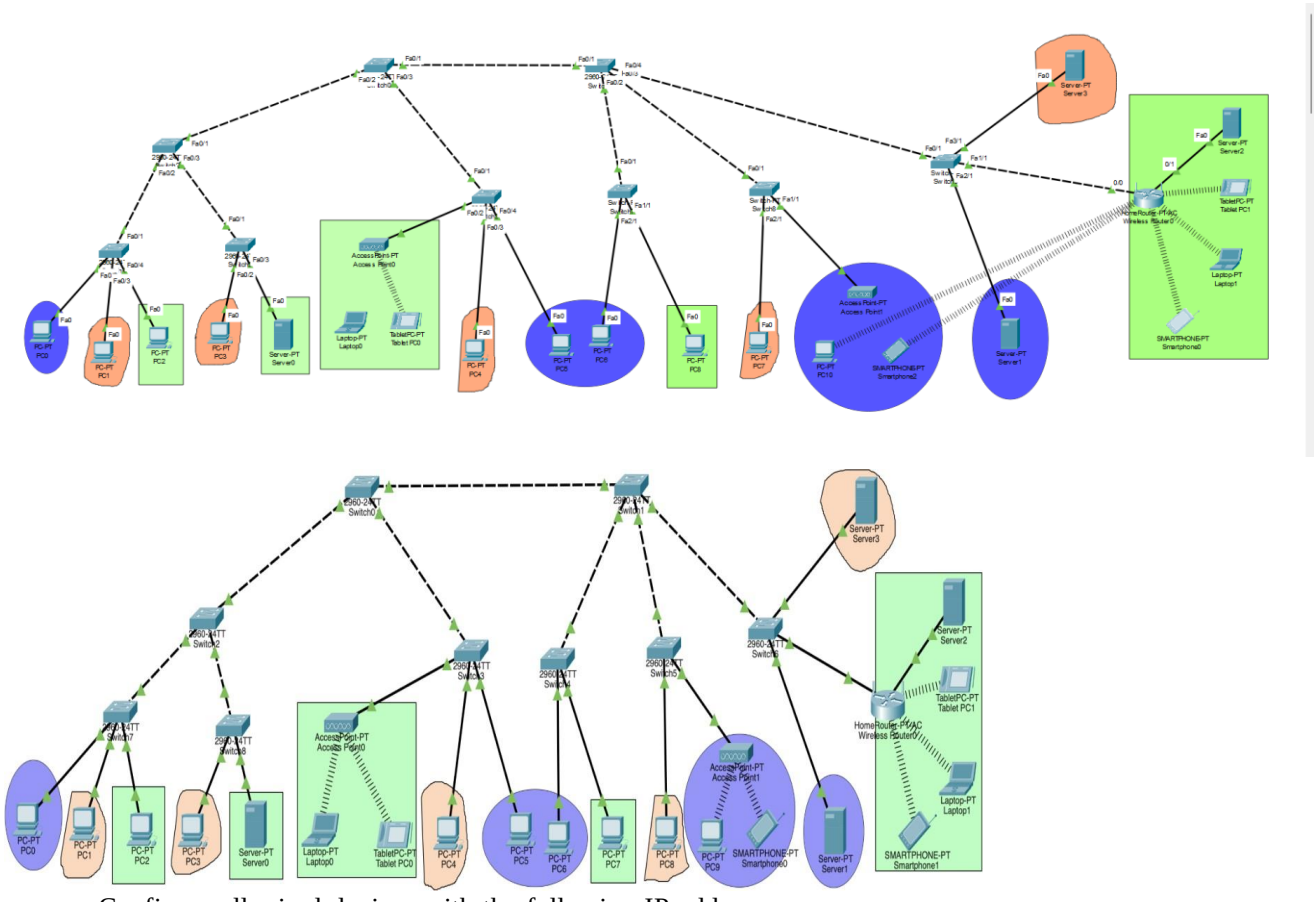


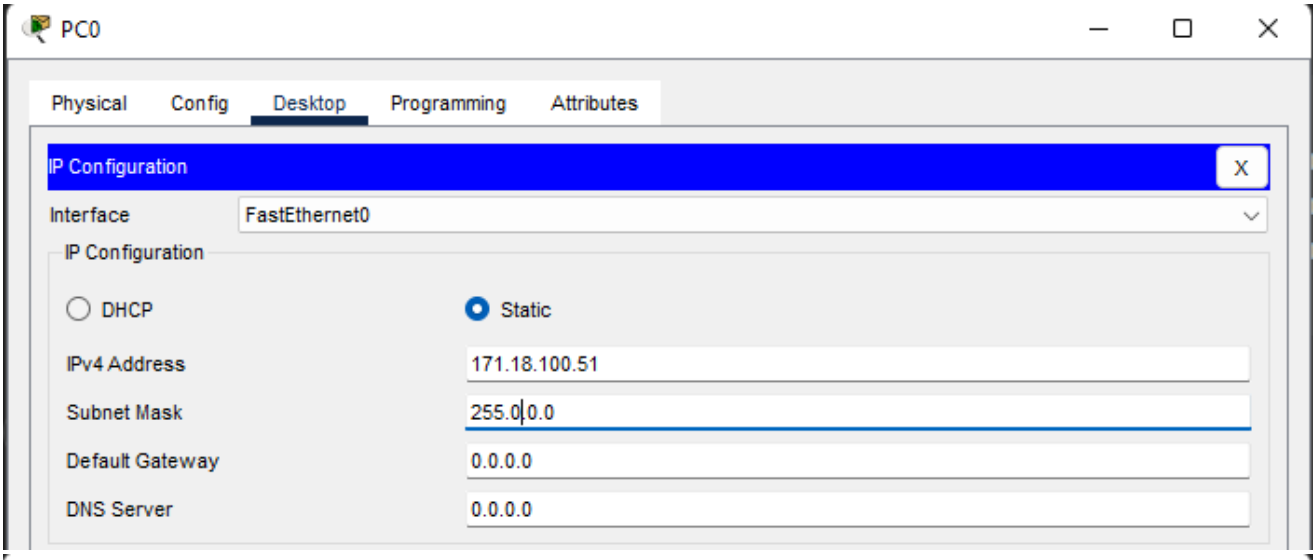
Figure 56 Initial Configuration

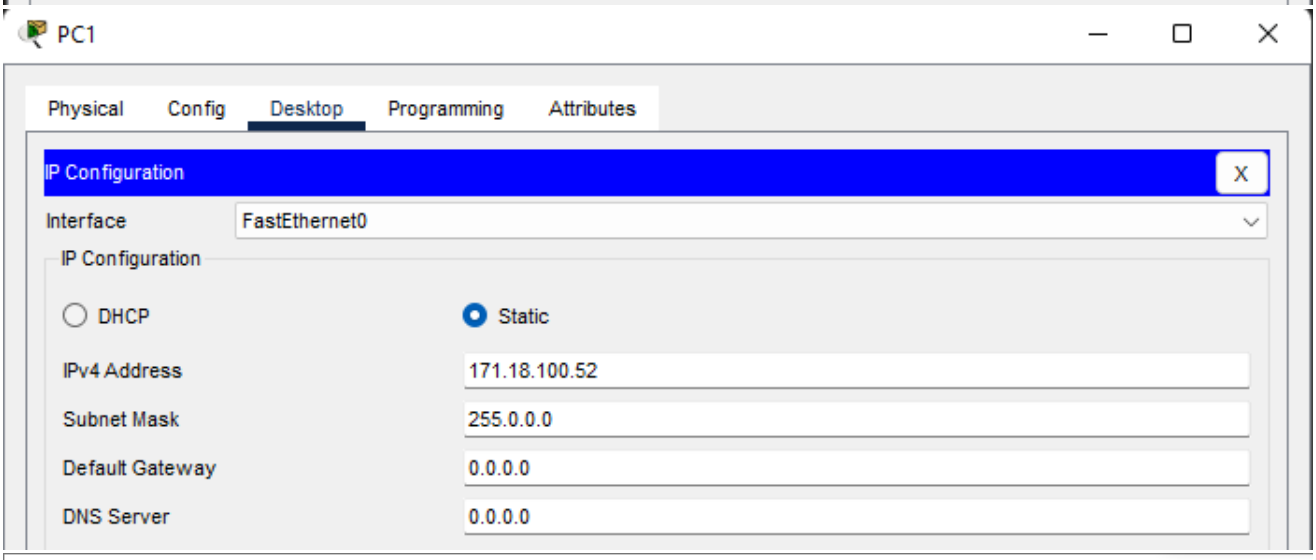
Figure 57 configuration palette dialog

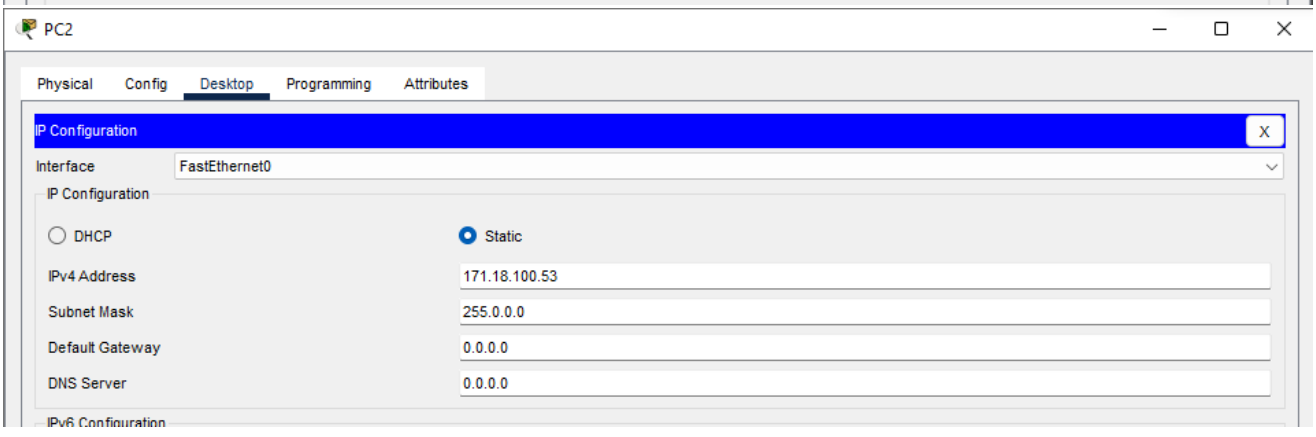


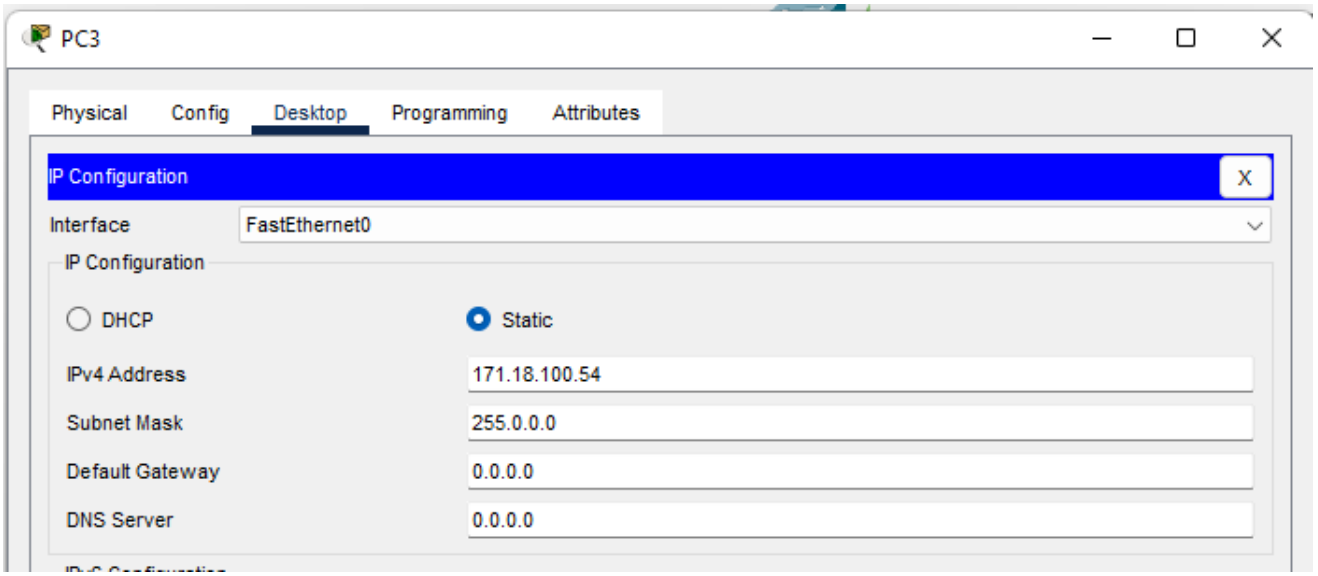
Configure all wired devices with the following IP addresses:

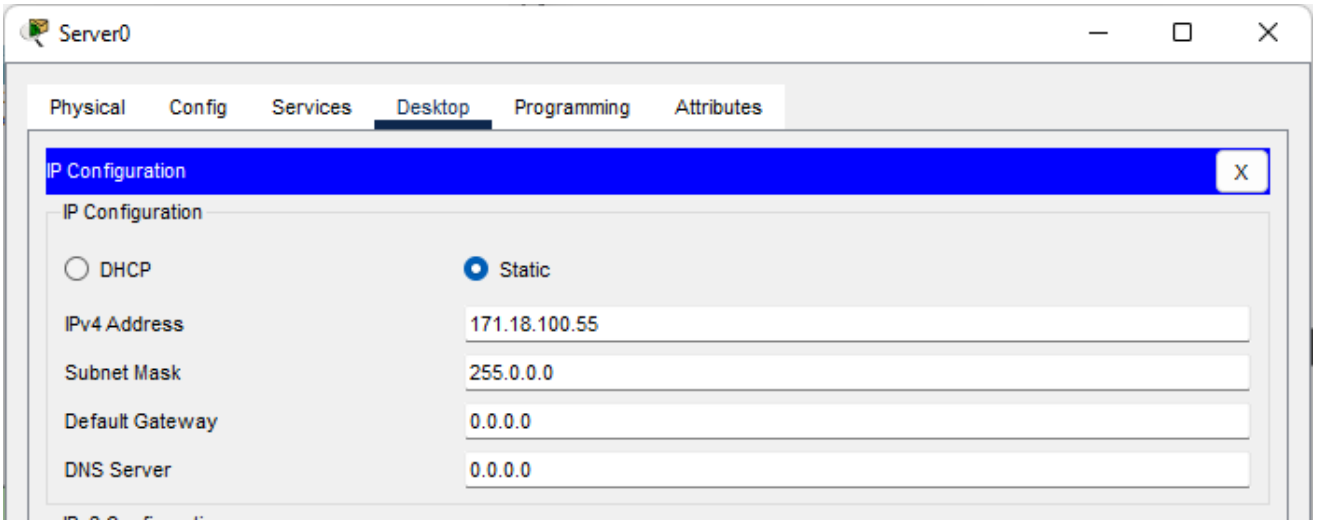
- Student 1: 171.18.100.50 to 171.18.100.80. Subnet mask 255.0.0.0
- Student 2: 171.18.110.50 to 171.18.110.80. Subnet mask 255.0.0.0
- Student 3: 171.18.120.50 to 171.18.120.80. Subnet mask 255.0.0.0

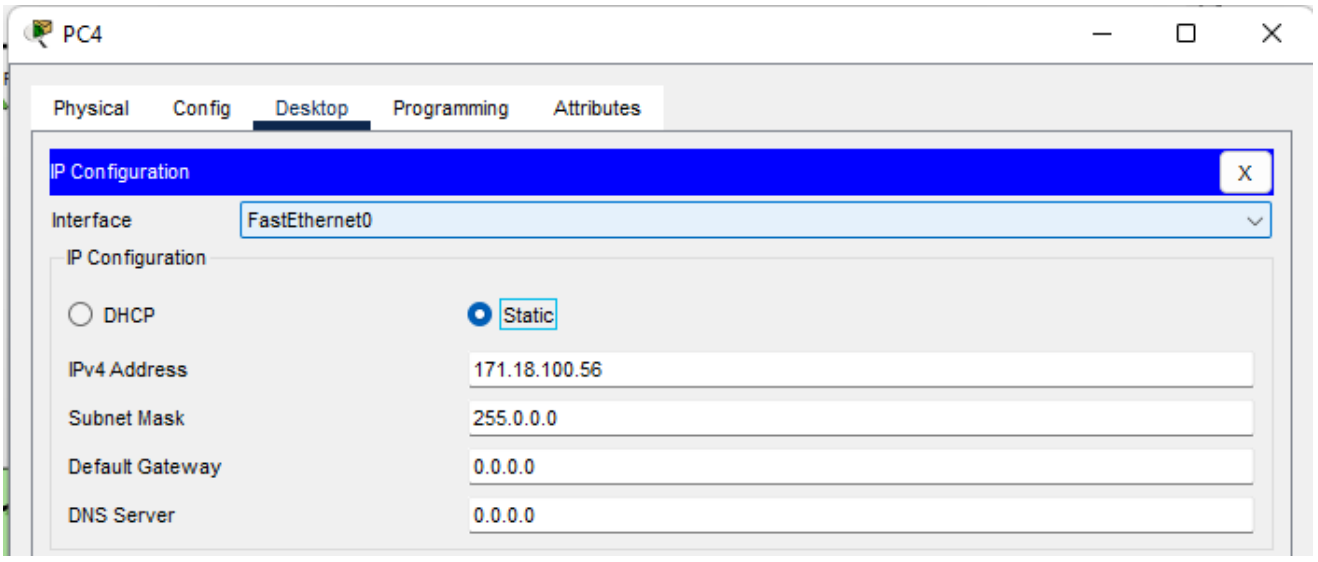

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.51
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

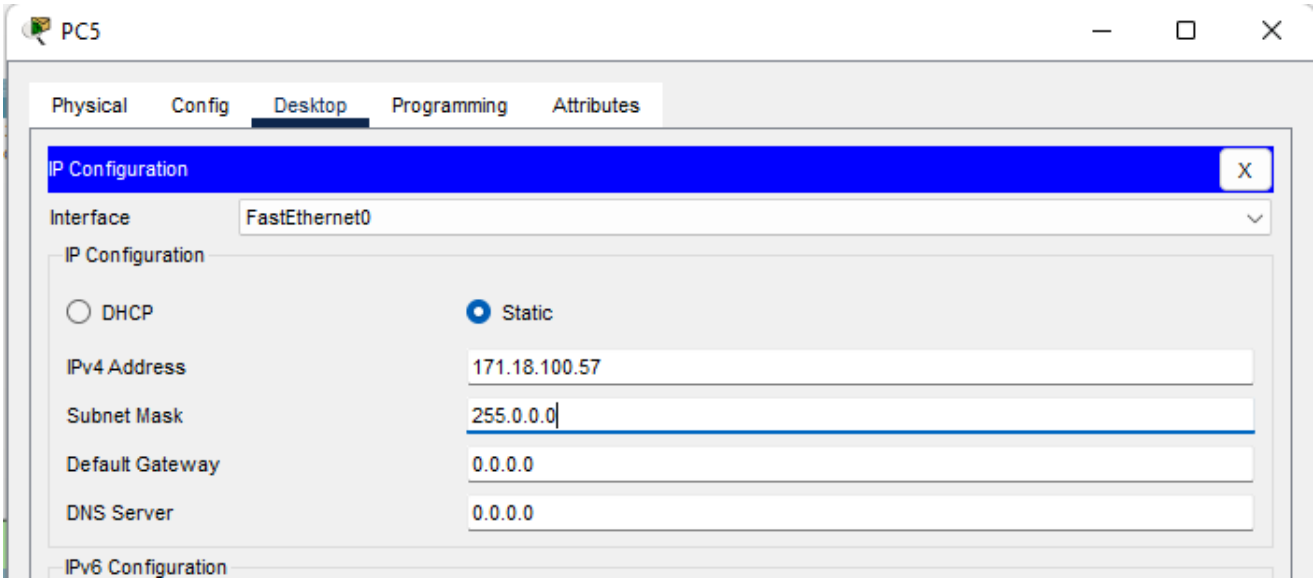

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.52
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

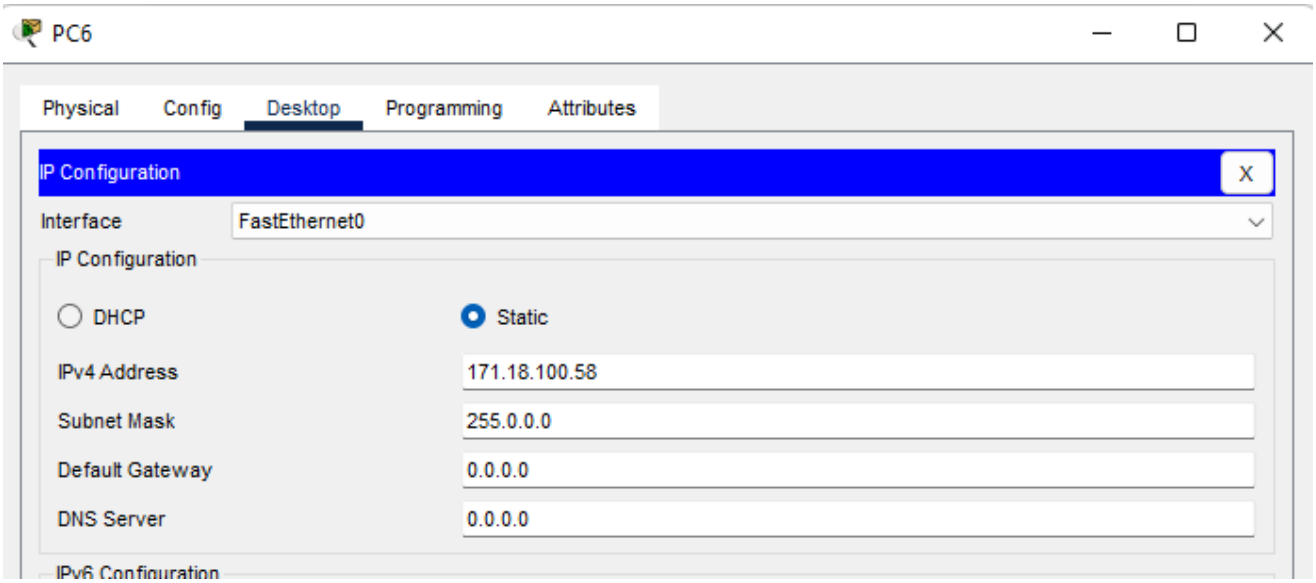

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.53
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration

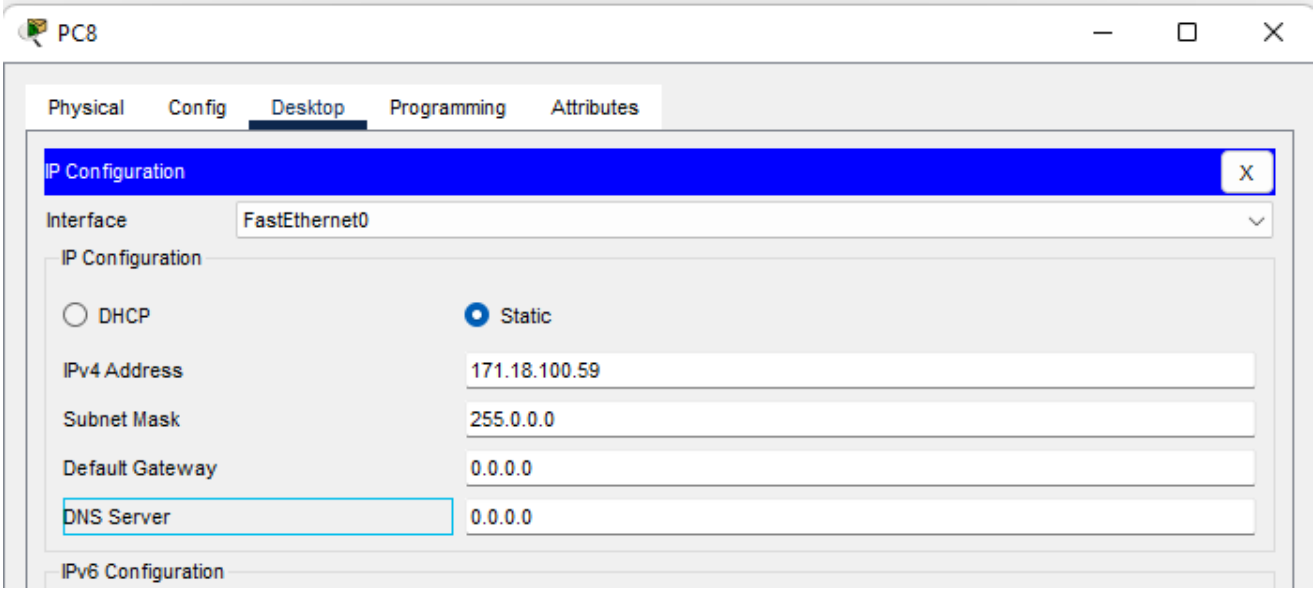

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.54
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

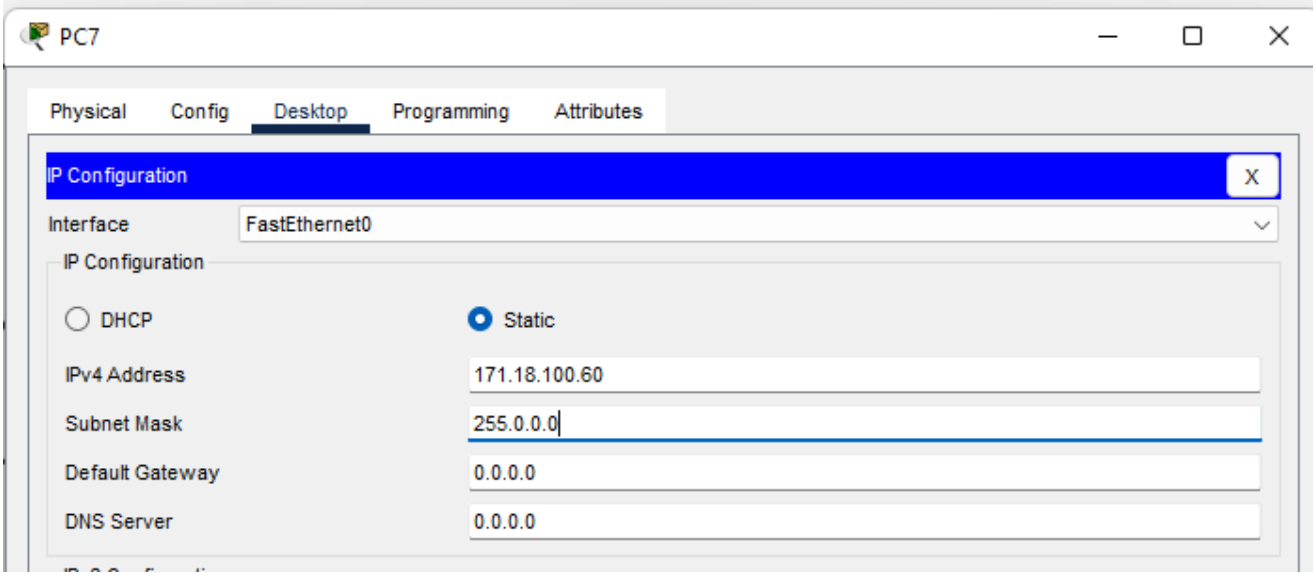

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.55
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

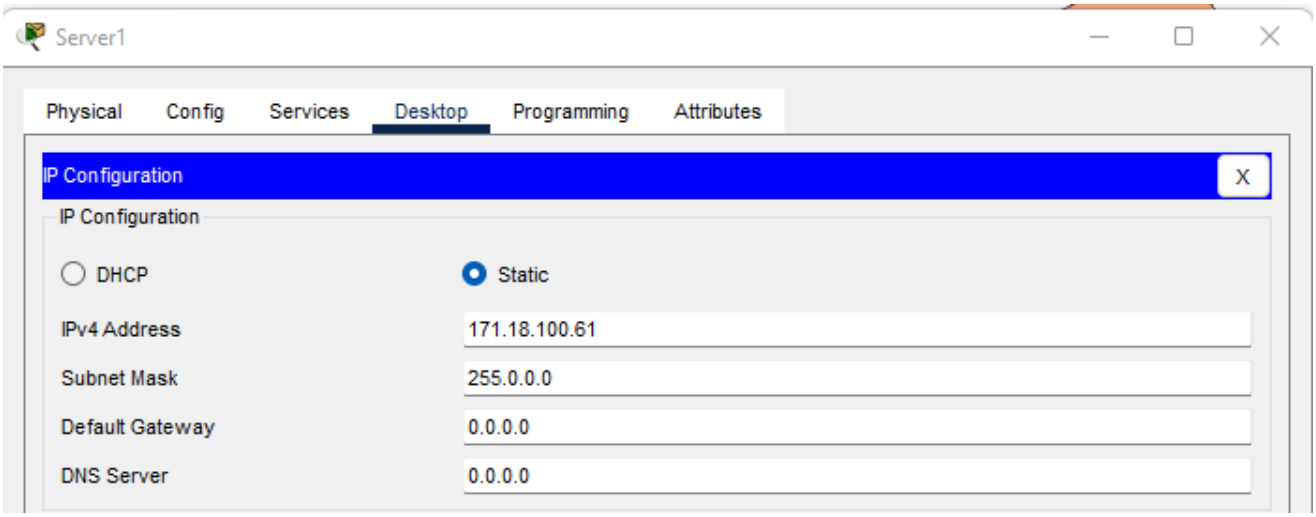

PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.56
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

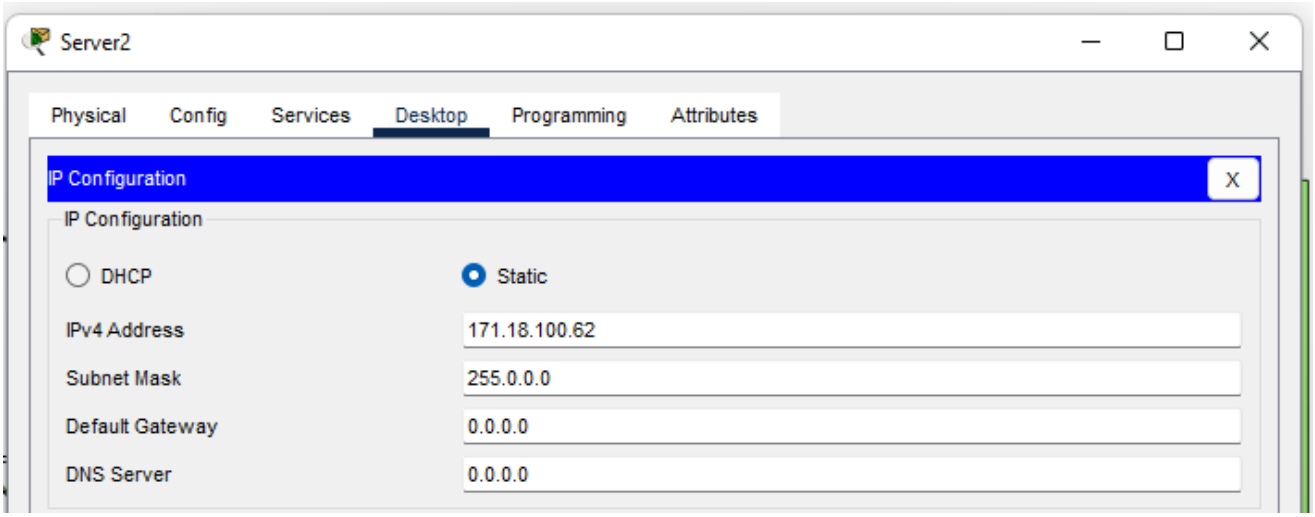

PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.57
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration

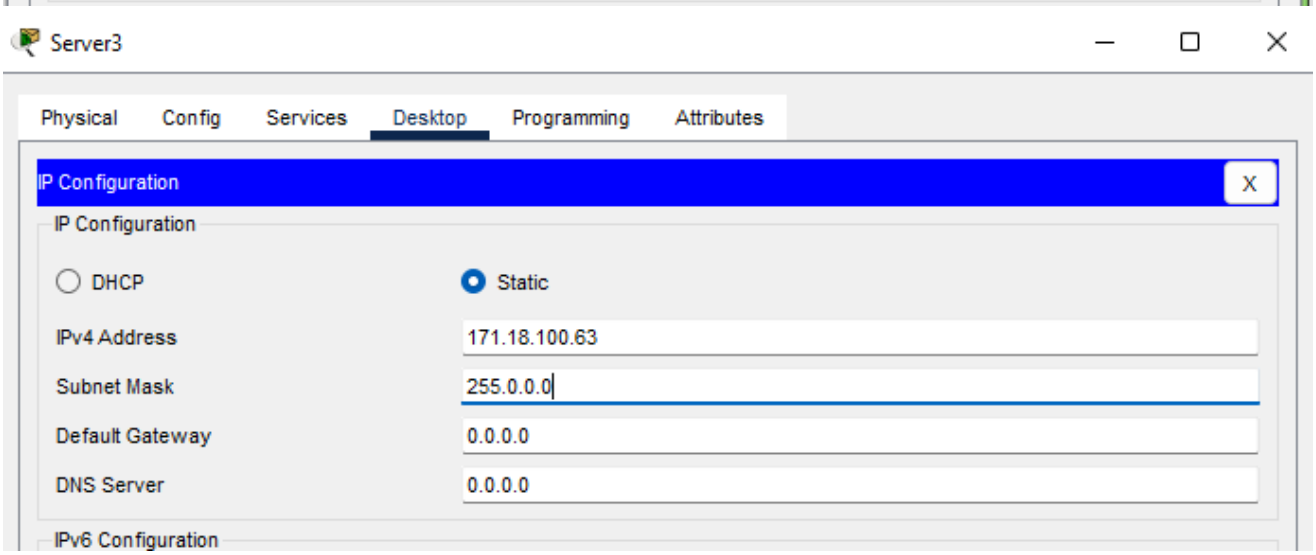

PC6
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.58
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration


PC8
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.59
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration


PC7
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.60
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

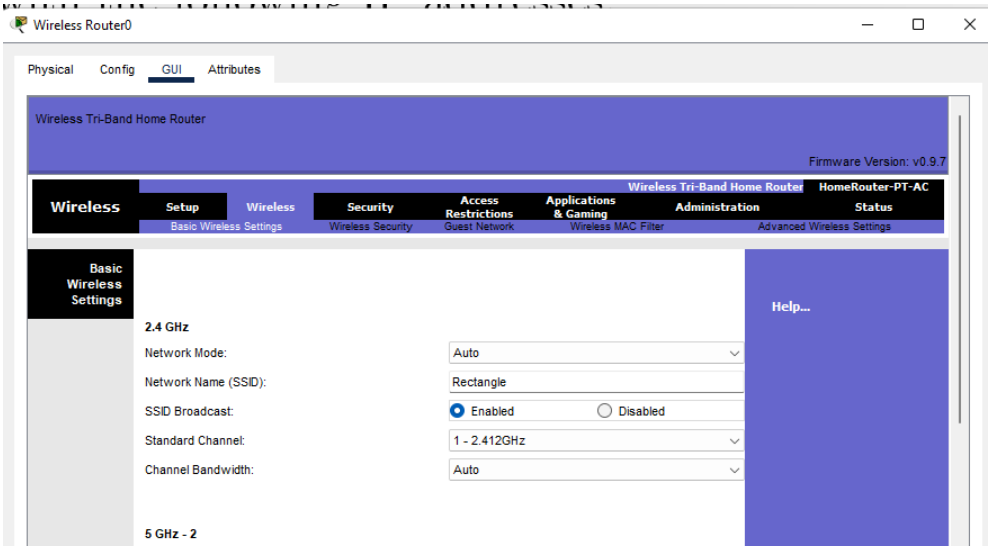

Server1
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
171.18.100.61
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0



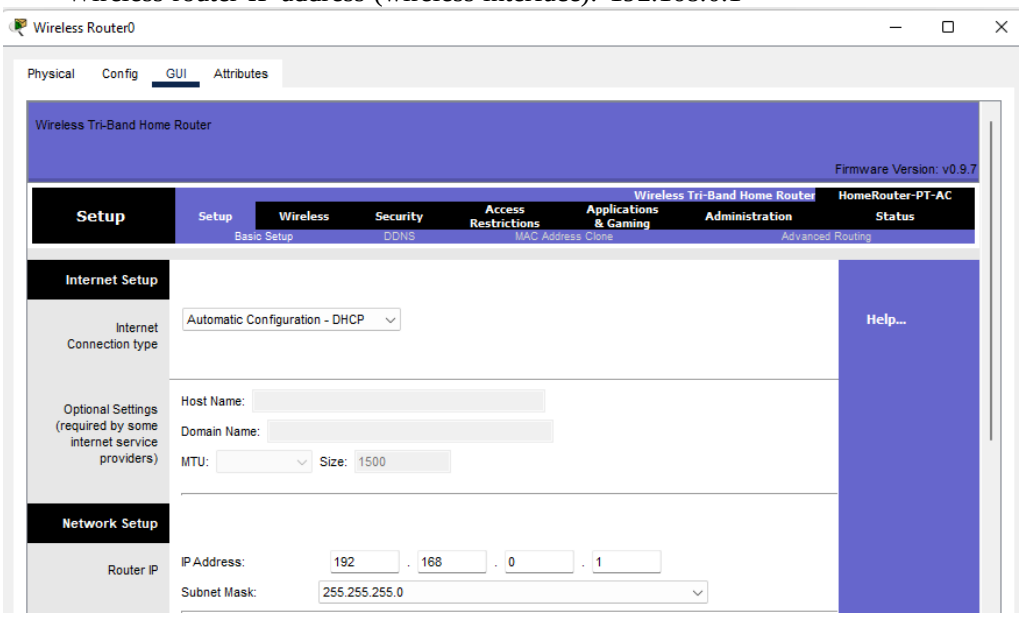


For the wireless network configuration, consider the following:

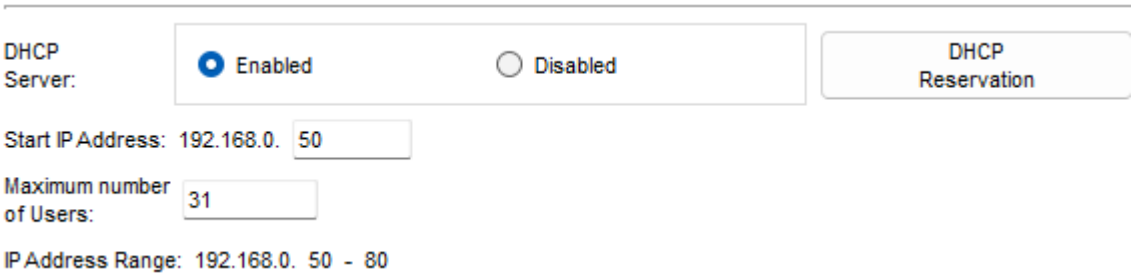
- Green Wireless Network (Rectangles)
  - Wireless network identifier - SSID: Rectangle



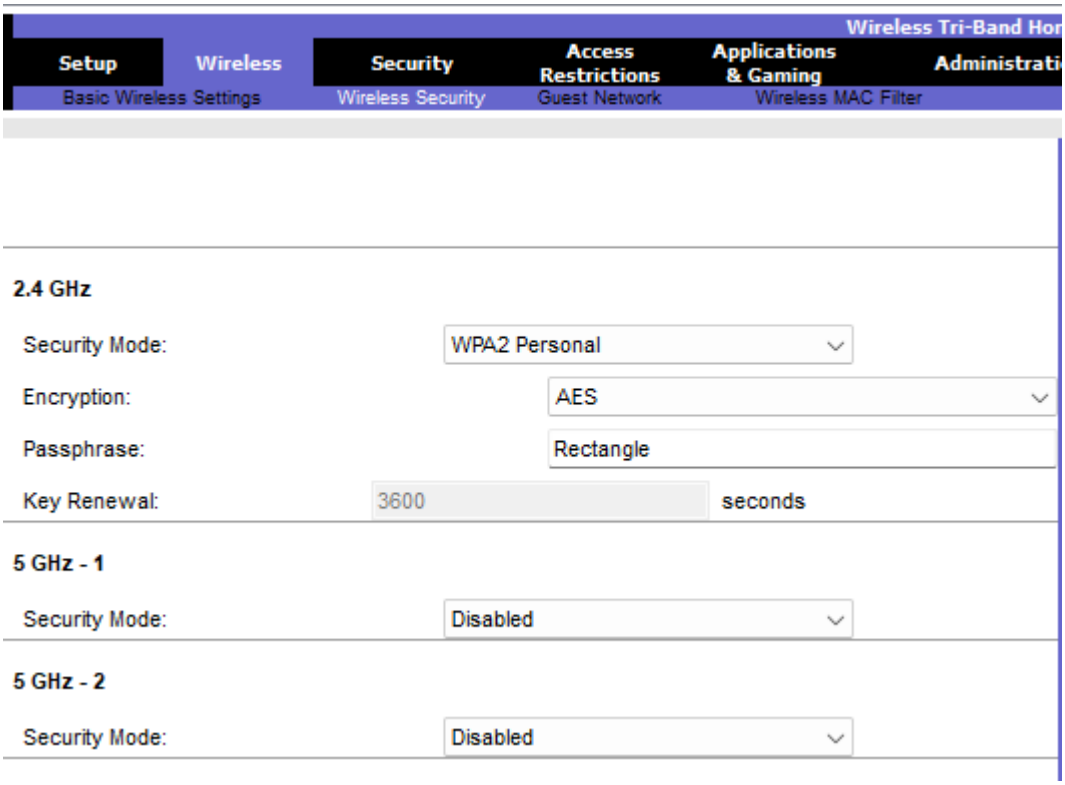
- Wireless network IP: 192.168.0.0/24
- Wireless router IP address (wireless interface): 192.168.0.1



- IP address range for mobile devices: 192.168.0.50 to 192.168.0.80. In this case is the same ranges fromthe previous setup

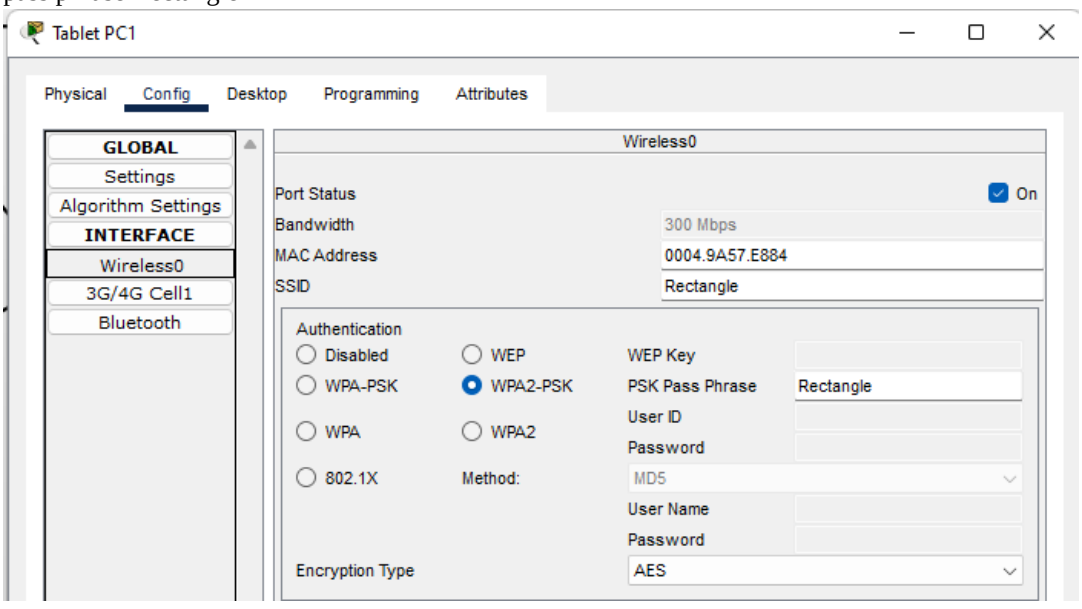


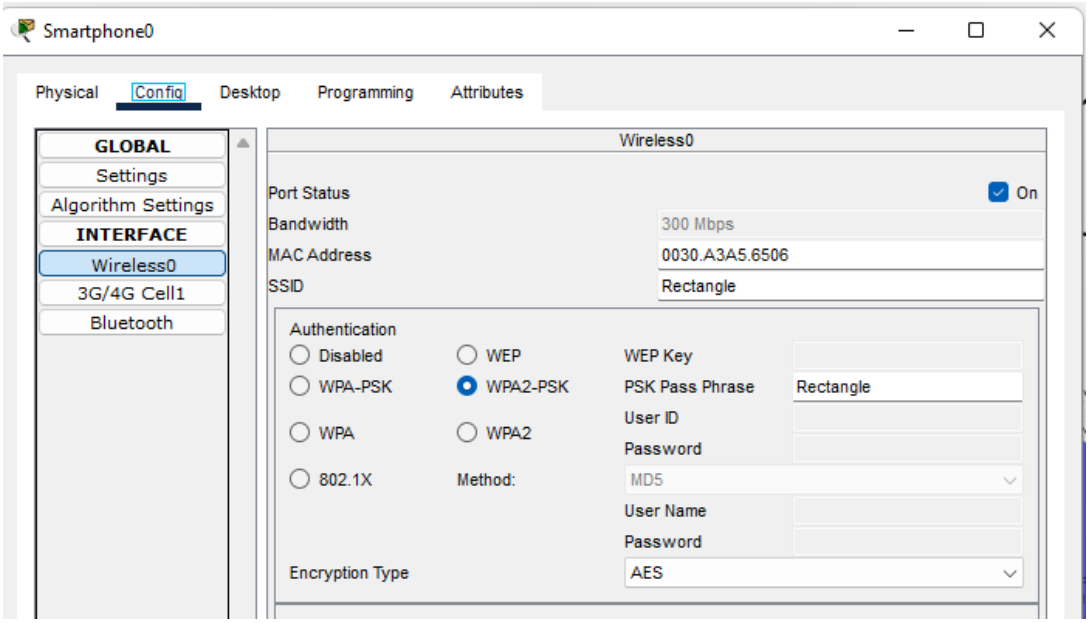
- Access mechanism for wireless clients: WPA2-PSK with AES

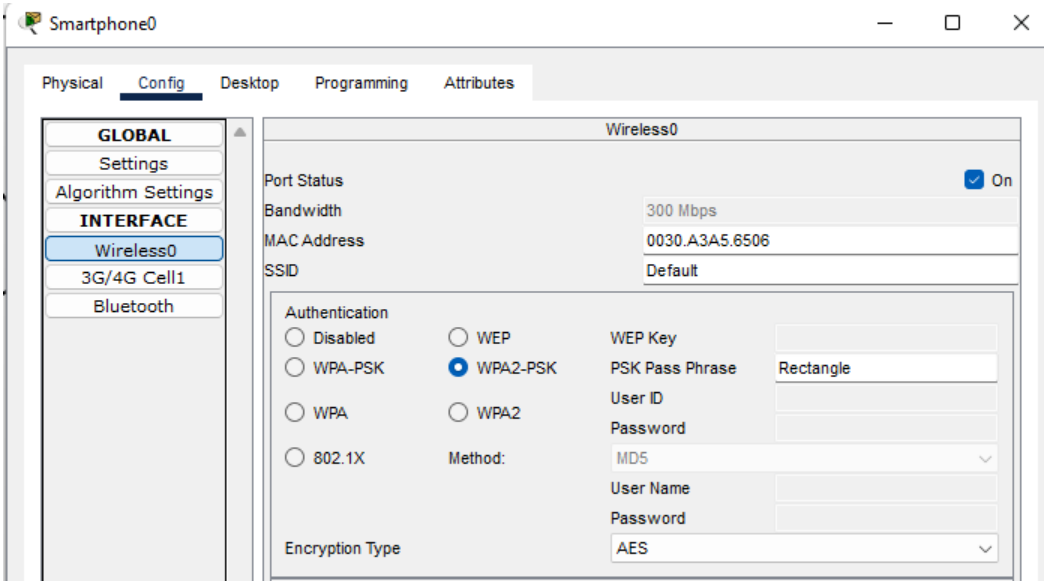


Now we configure the devices

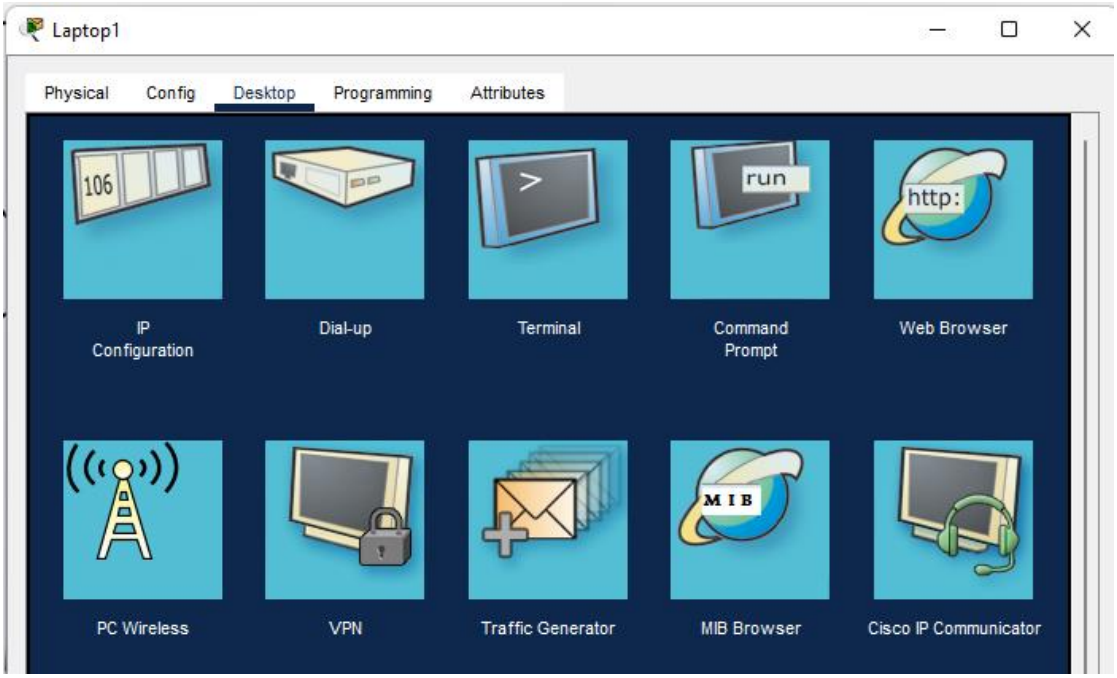
In Tablet PC1 and the Smartphone we go to the wireless0 and set WPA2-PSK and then we put the pass phrase Rectangle



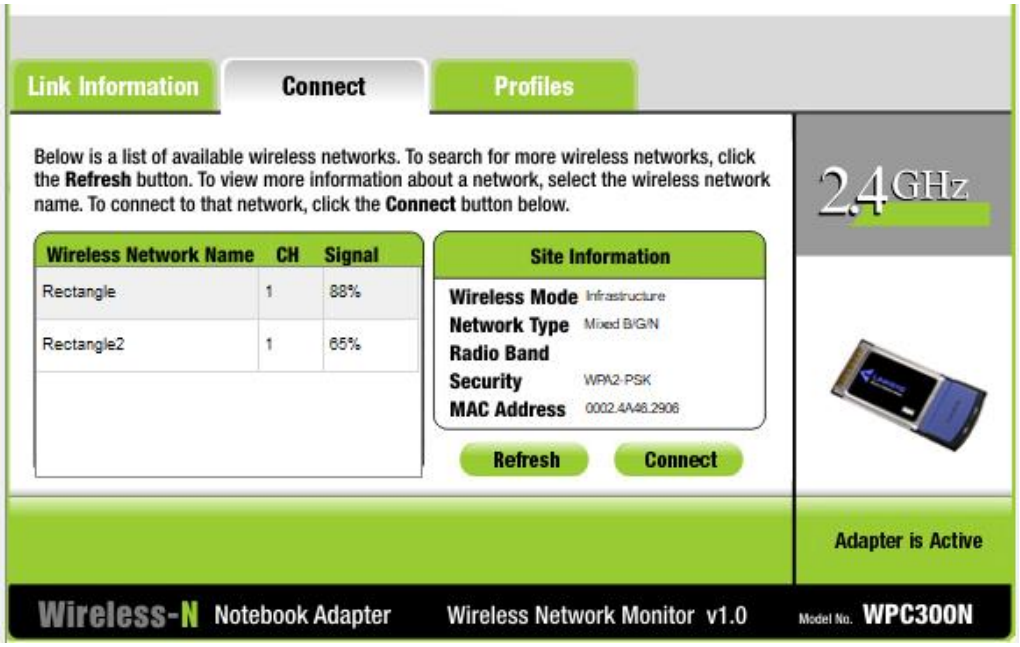


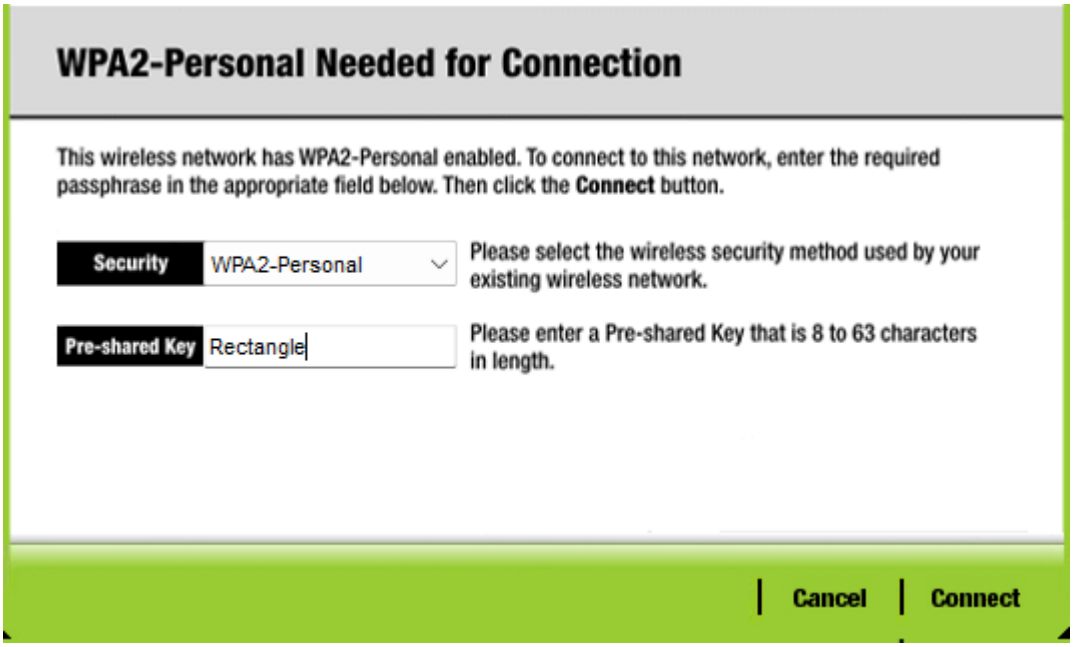


To configure the laptop we go to configuration, then PC Wireless

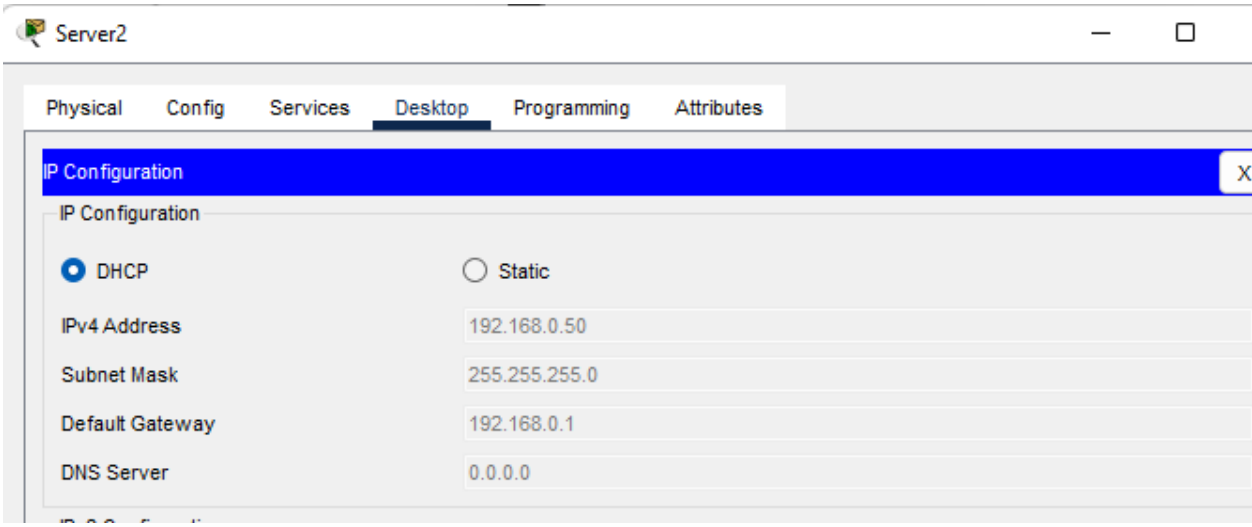


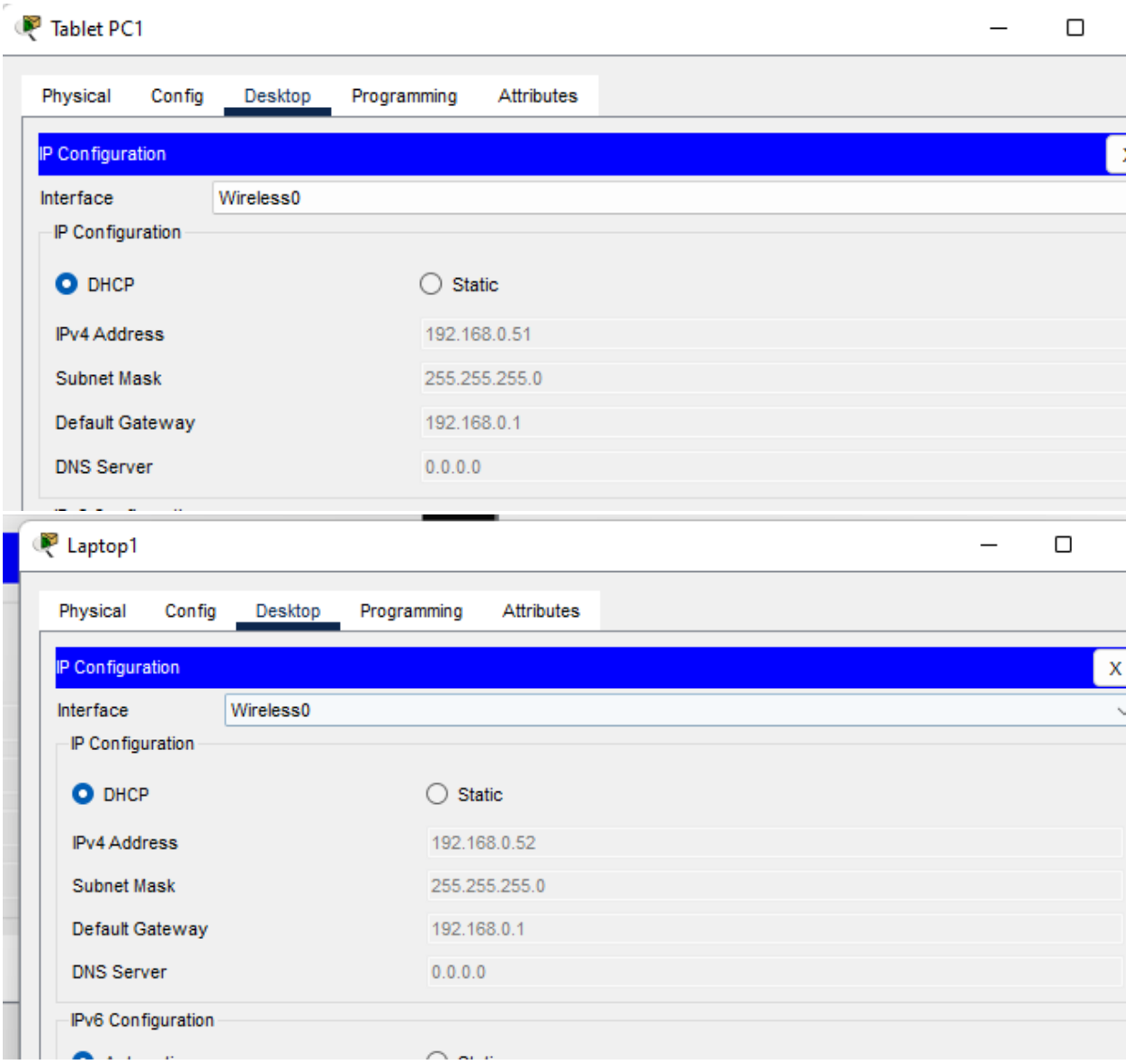
We go to the connection and set the password to the SSID Rectangle

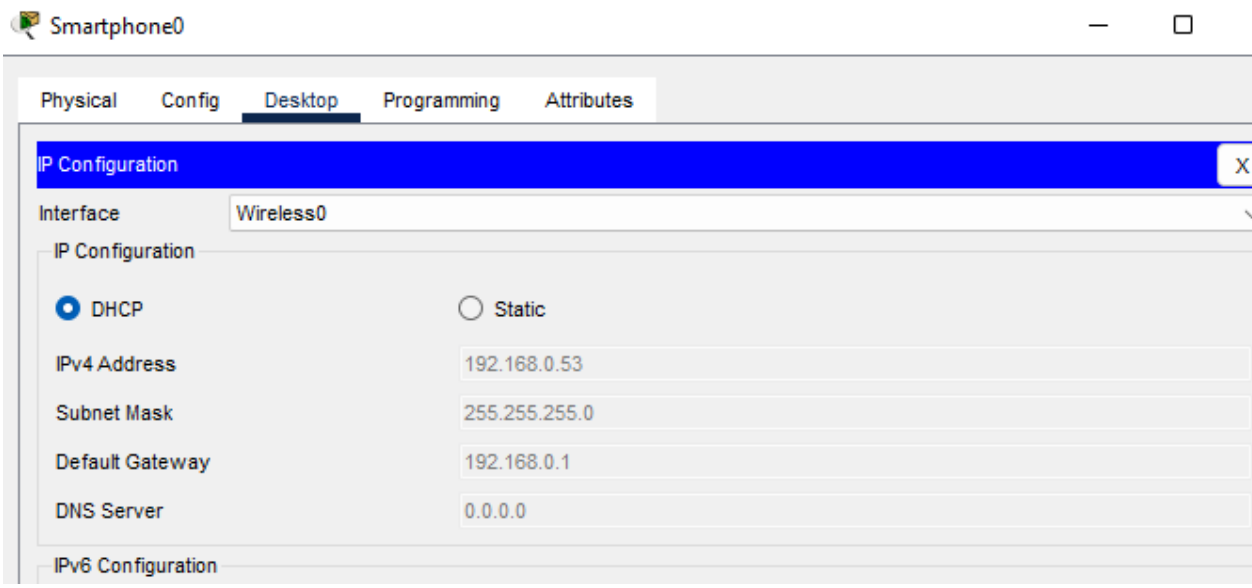




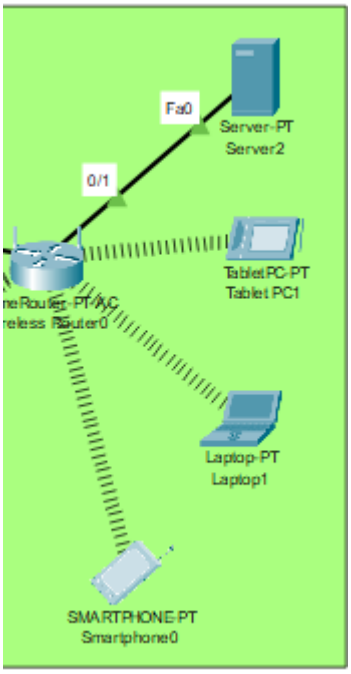
Now we configure the Ips dynamic



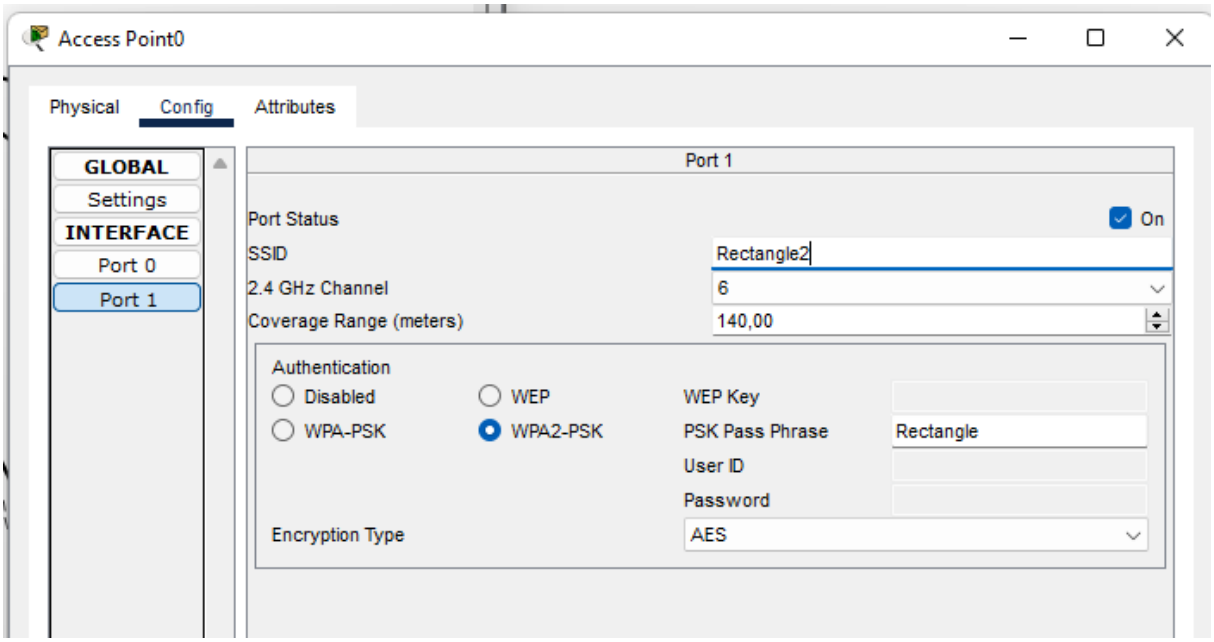

Tablet PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
Wireless0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.51
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
0.0.0.0
Laptop1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
Wireless0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.52
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
0.0.0.0
IPv6 Configuration



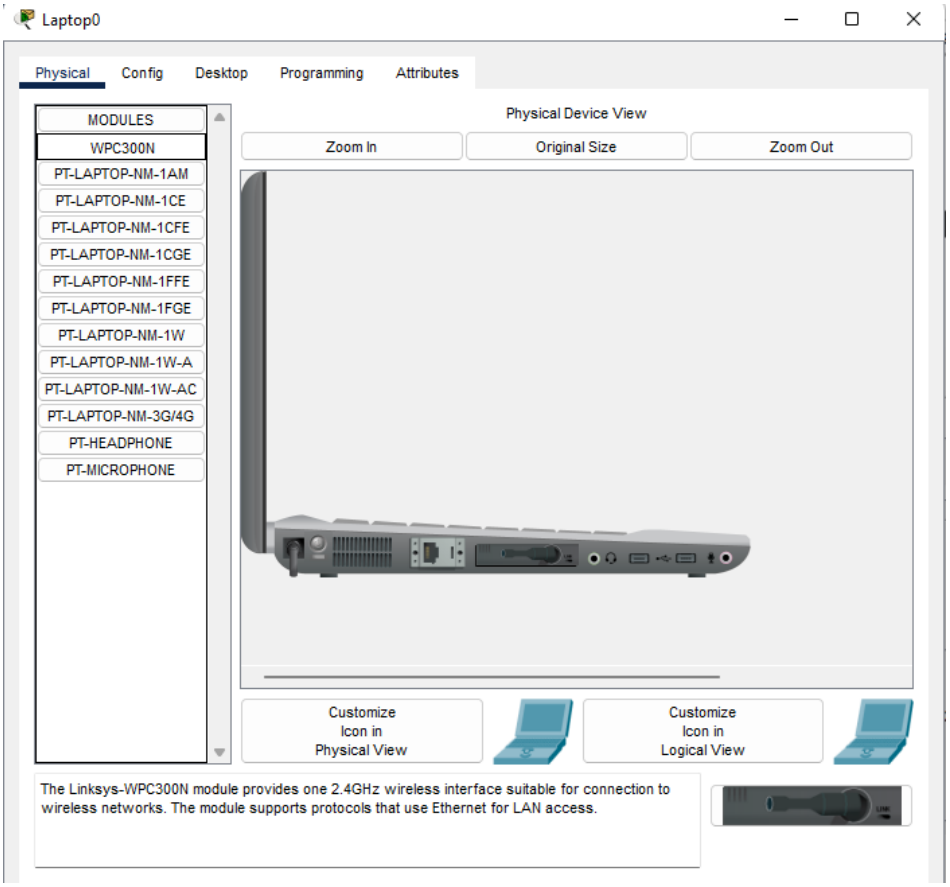
The result is the next one



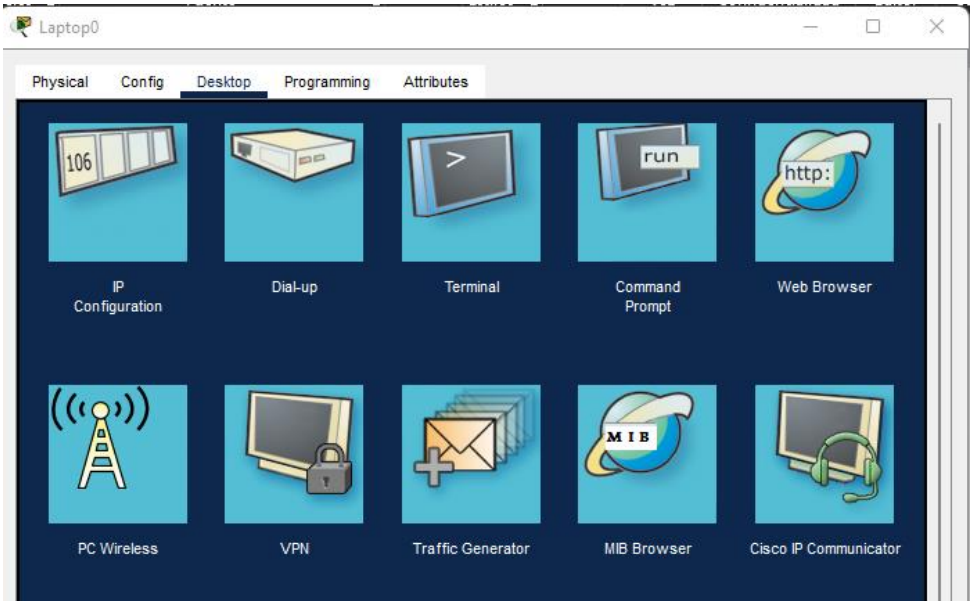
Now we configure the access Point0



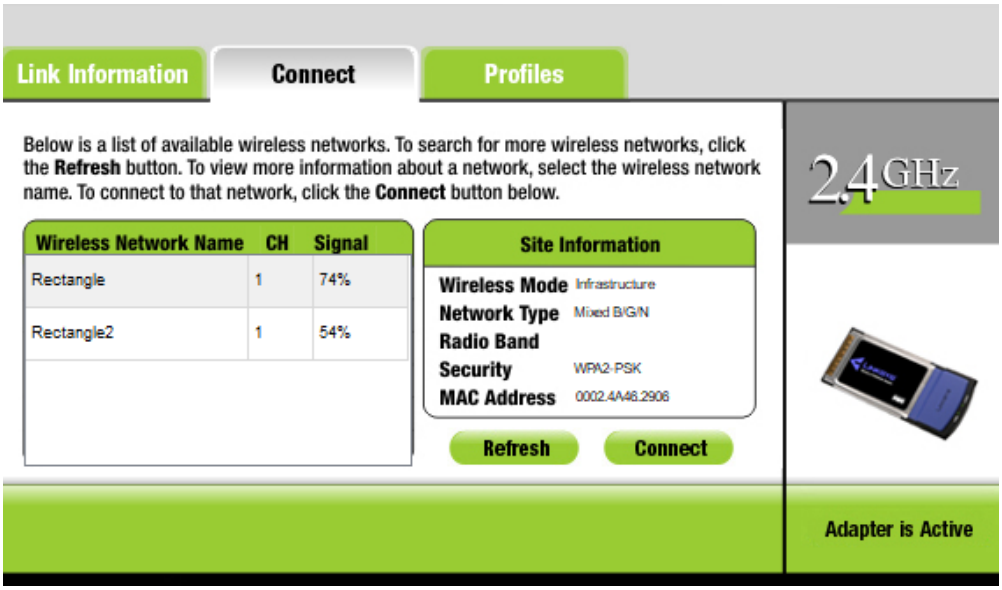
Now we set the WPC300N to connect to the access point0 in the laptop0



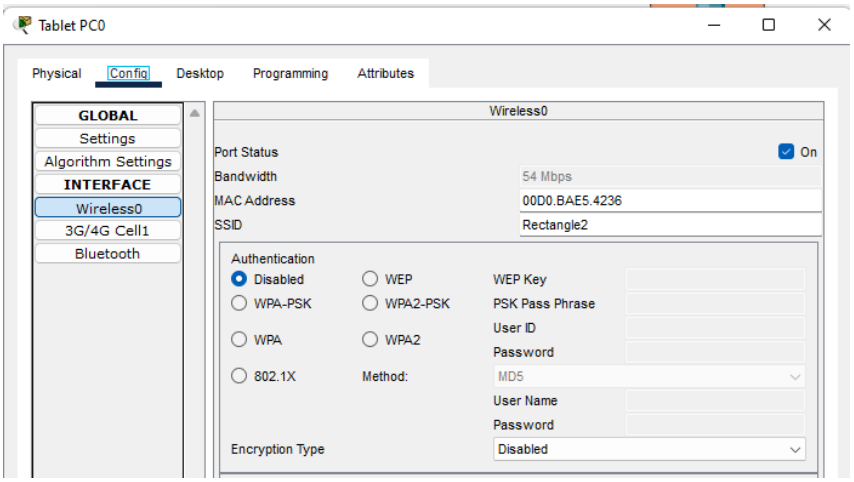
We go to PC wireless connection



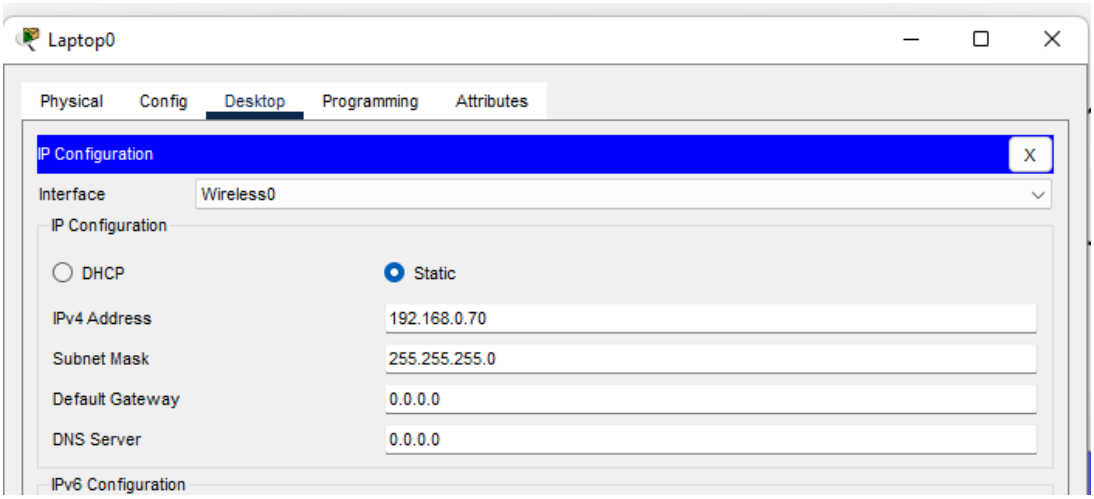
We connect to network SSID with Rectangle2

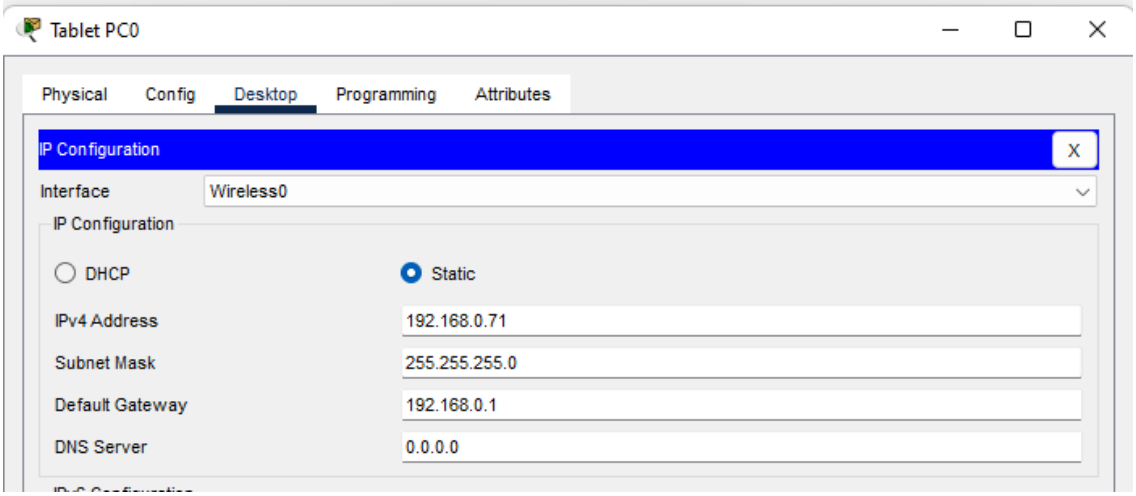


To connect to the tablet PC we go to config and then select Wireless0 and set the SSID Rectangle2

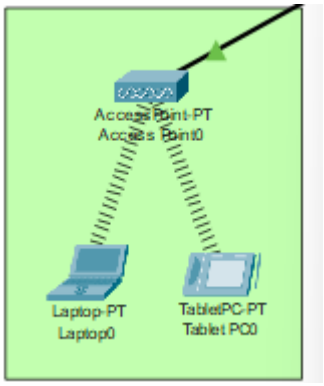


Then we set Ip address and mask, the range is between 192.168.50 - 192.168.80 we select the 192.168.70 and 192.168.71

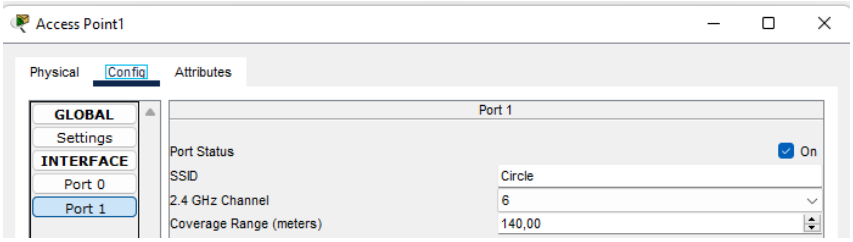




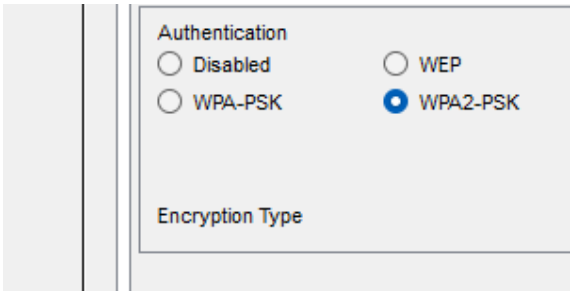
Result is the next one



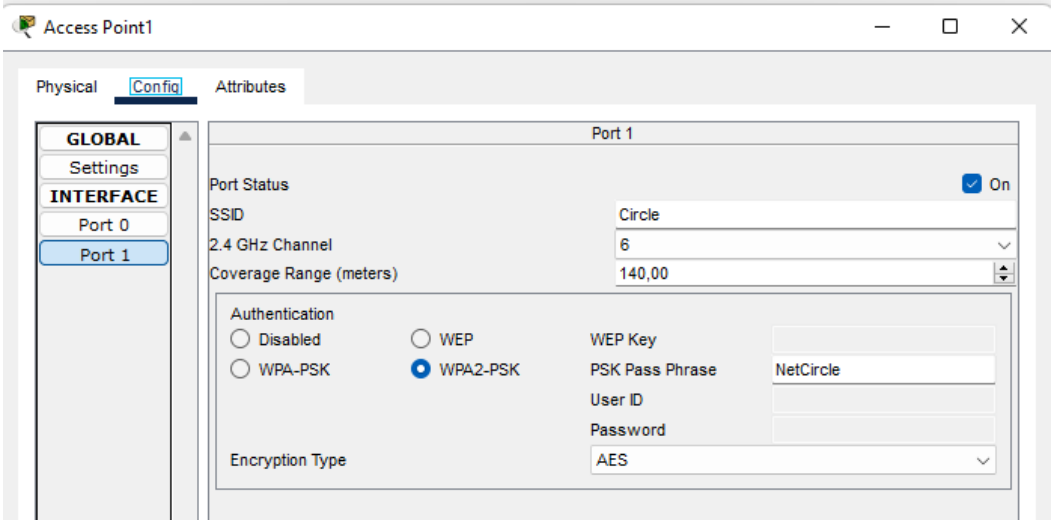
- Purple Wireless Network (Circles)
  - Wireless network identifier - SSID: Circle



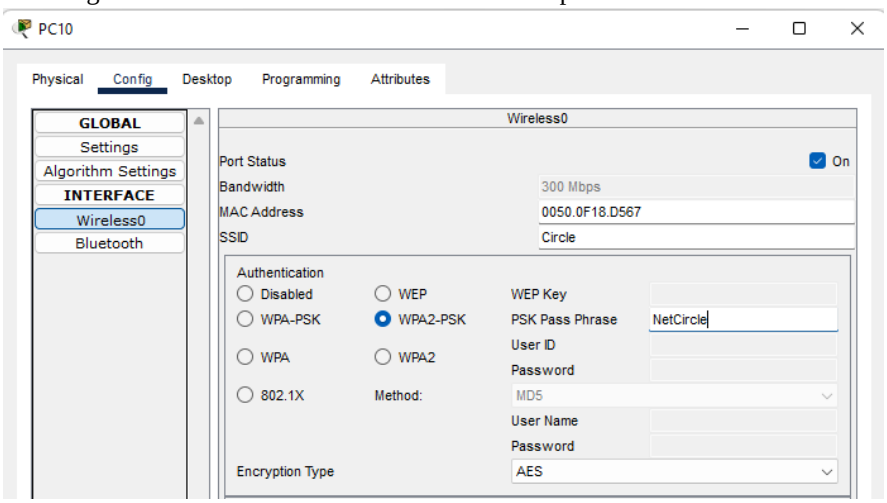
  - Access mechanism for wireless clients: WPA2-PSK with AES

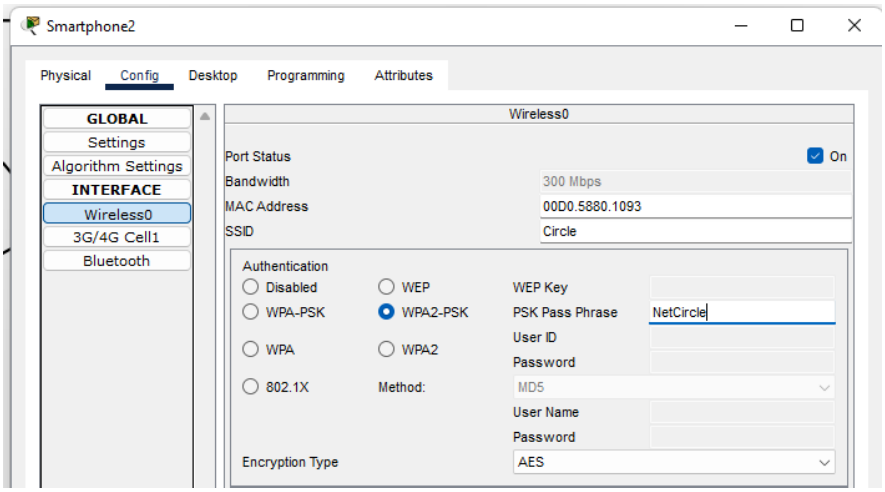


  - Access Point password for mobile devices: NetCircle

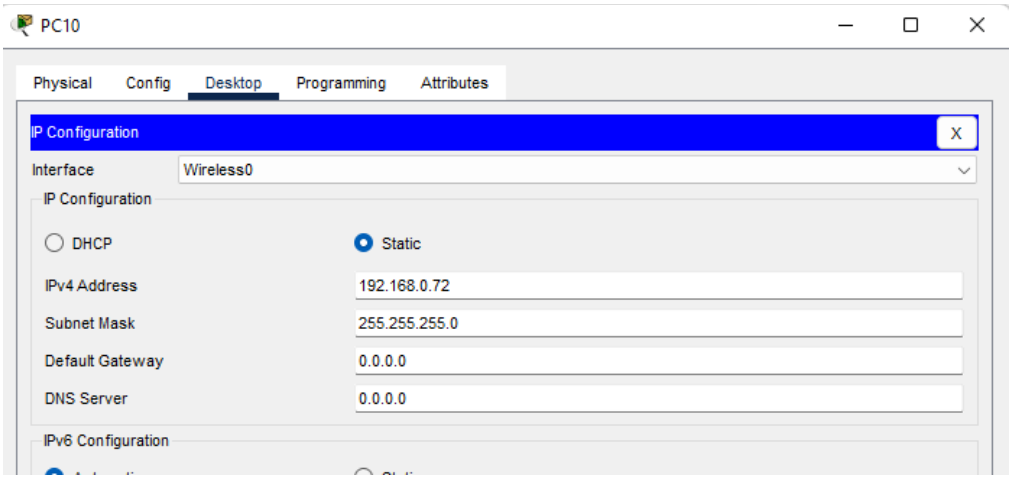


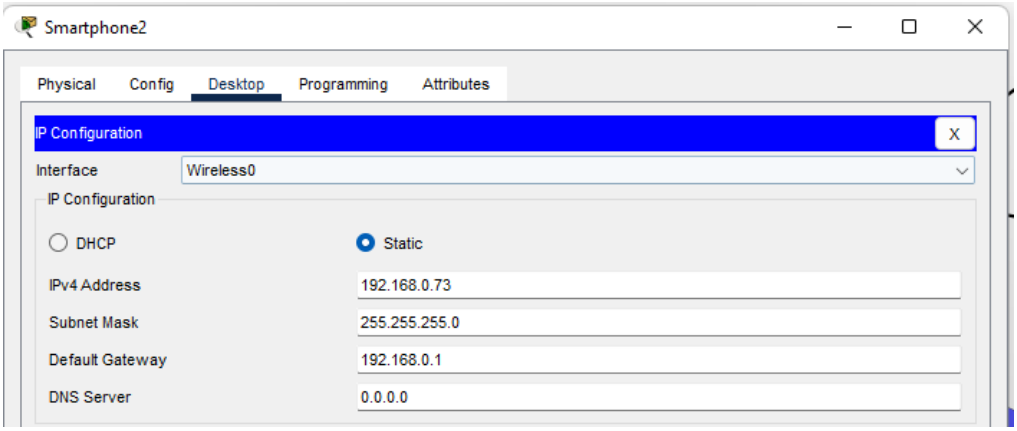
- We assign to each device and wirless0 interface the port1 of the access Point1



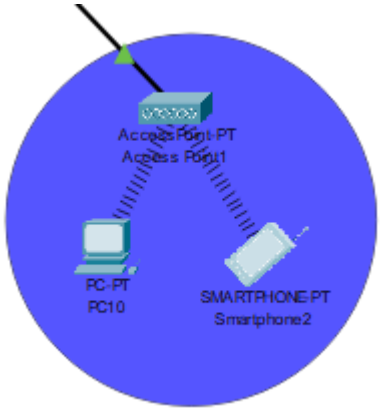


- We assign IP addresses to computers connected to this network based on the range used in thewired network. In this case it will be 192.168.0.72 and 192.168.0.73





- The result is the next one



We verify connectivity between all devices. Packet transmission works between devices with wireless networks or wired networks but not between them. Additionally, devices connected to the homeRouter cannot be accessed from outside of it.

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Server3	Server1	ICMP		0.000	N	0	(edit)	
	Successful	Server2	Tablet PC1	ICMP		0.000	N	1	(edit)	
	Failed	Server2	Server1	ICMP		0.000	N	2	(edit)	
	Successful	Server1	PC5	ICMP		0.000	N	3	(edit)	
	Failed	PC10	PC7	ICMP		0.000	N	4	(edit)	
	Successful	Tablet PC0	PC10	ICMP		0.000	N	5	(edit)	
	Successful	Laptop0	Smartphone2	ICMP		0.000	N	6	(edit)	
	Failed	Tablet PC0	Laptop1	ICMP		0.000	N	7	(edit)	

We configure the VLANs based on the colors in the diagram. First, we configure the interfaces connected to switches and devices, and the interfaces between switches are set as trunk links.

Switch4

Physical | Config | CLI | Attributes

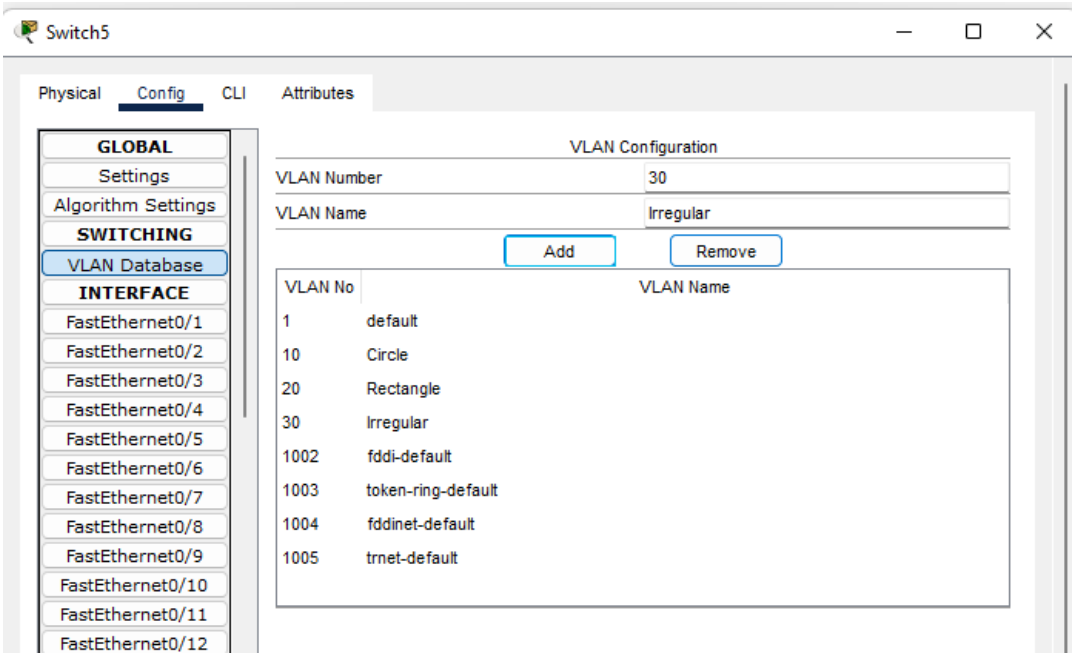
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
FastEthernet0/8
FastEthernet0/9
FastEthernet0/10
FastEthernet0/11
FastEthernet0/12

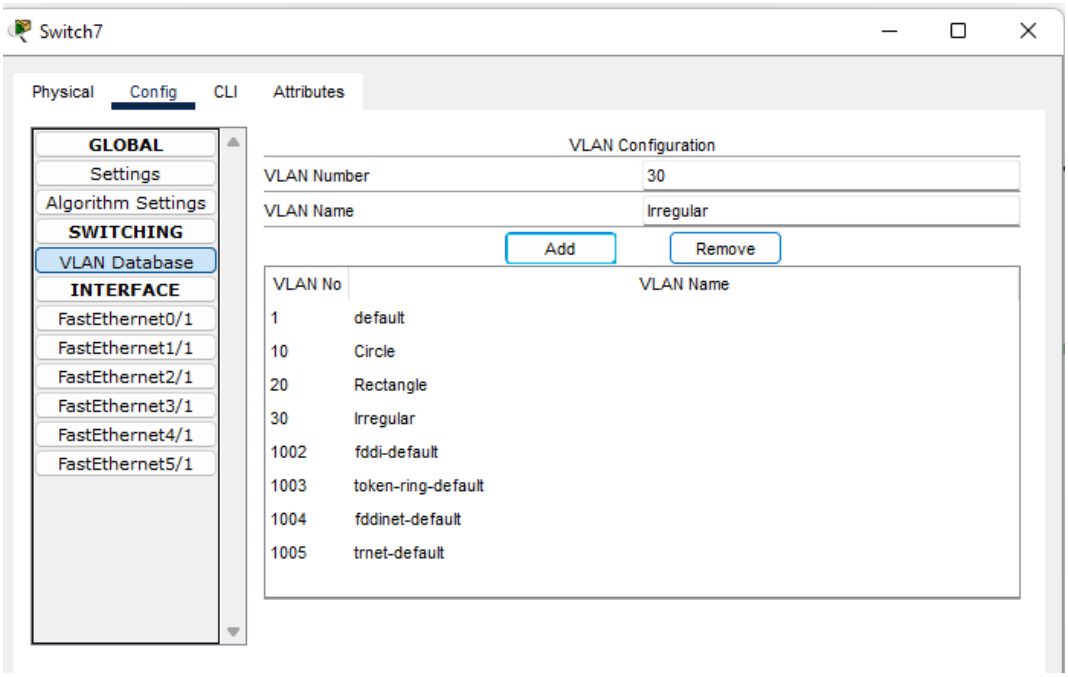
VLAN Configuration

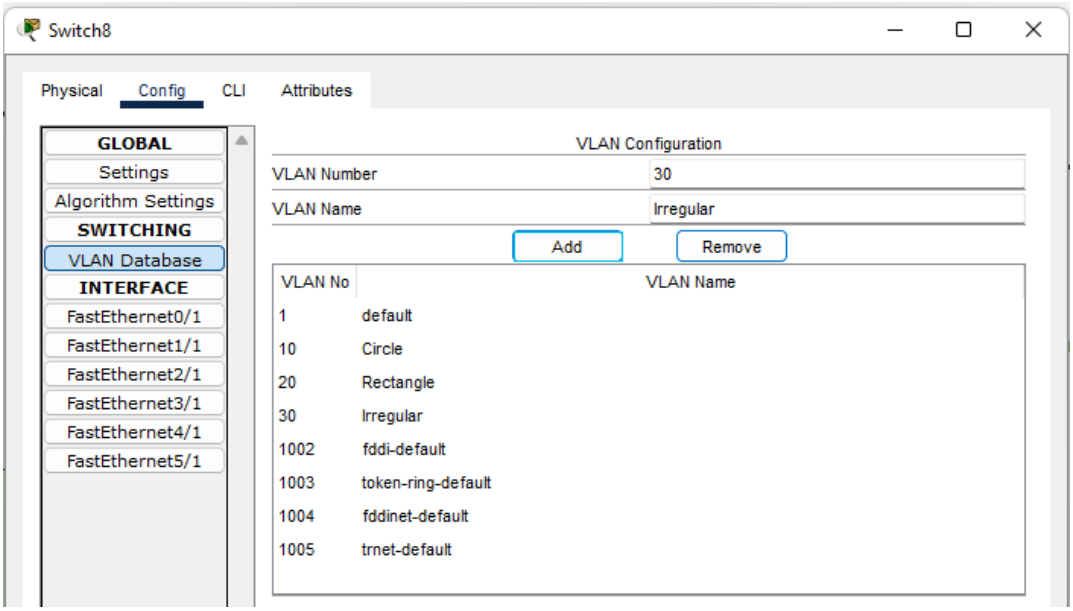
VLAN Number: 10
VLAN Name: Circle

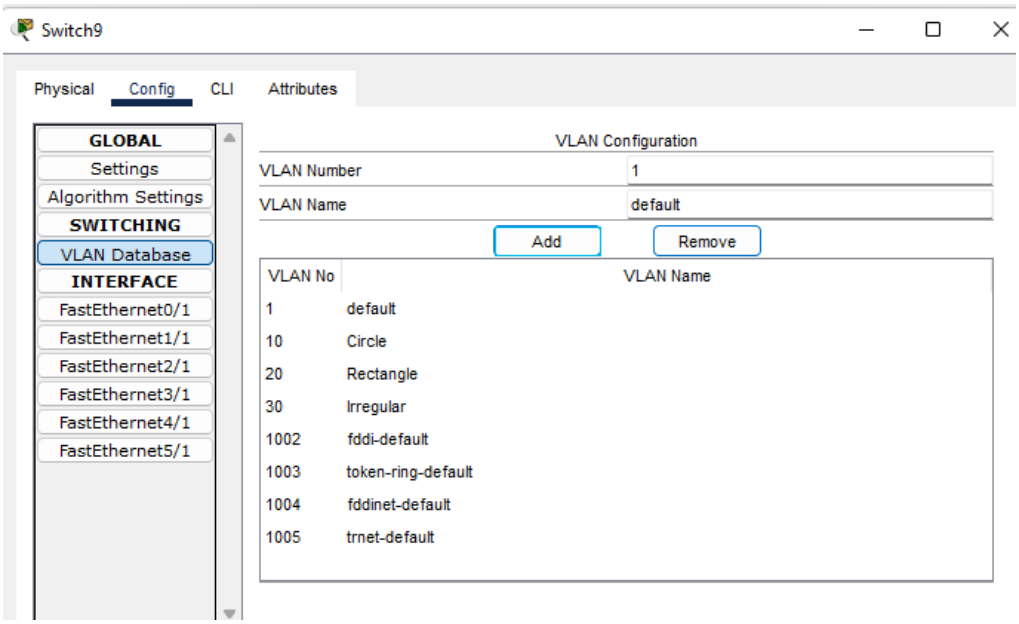
Add | Remove

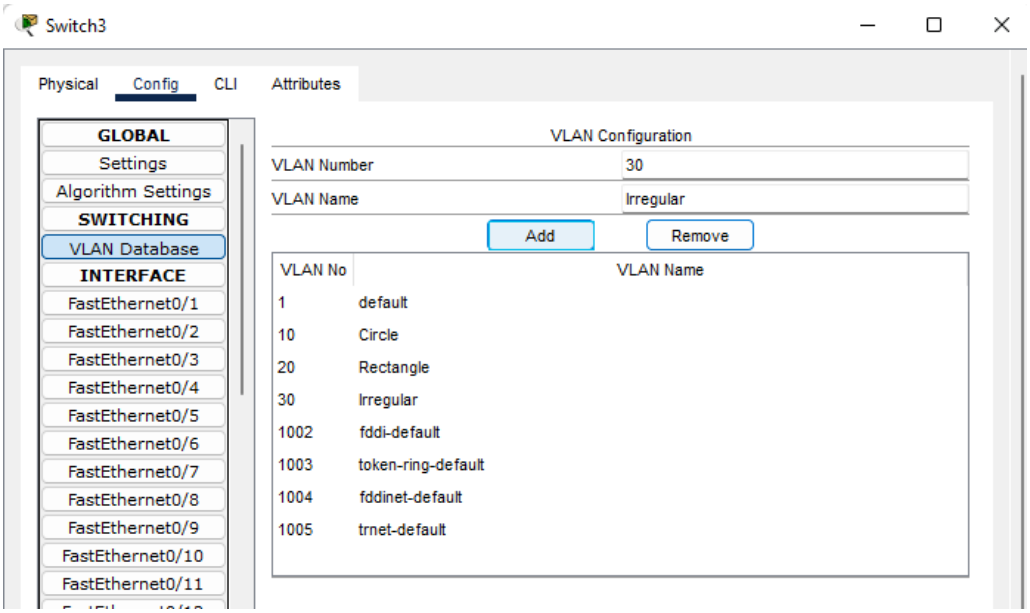
VLAN No	VLAN Name
1	default
10	Circle
20	Rectangle
30	Irregular
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default


Switch5
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
FastEthernet0/8
FastEthernet0/9
FastEthernet0/10
FastEthernet0/11
FastEthernet0/12
VLAN Configuration
VLAN Number
30
VLAN Name
Irregular
Add
Remove
VLAN No
VLAN Name
1 default
10 Circle
20 Rectangle
30 Irregular
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default

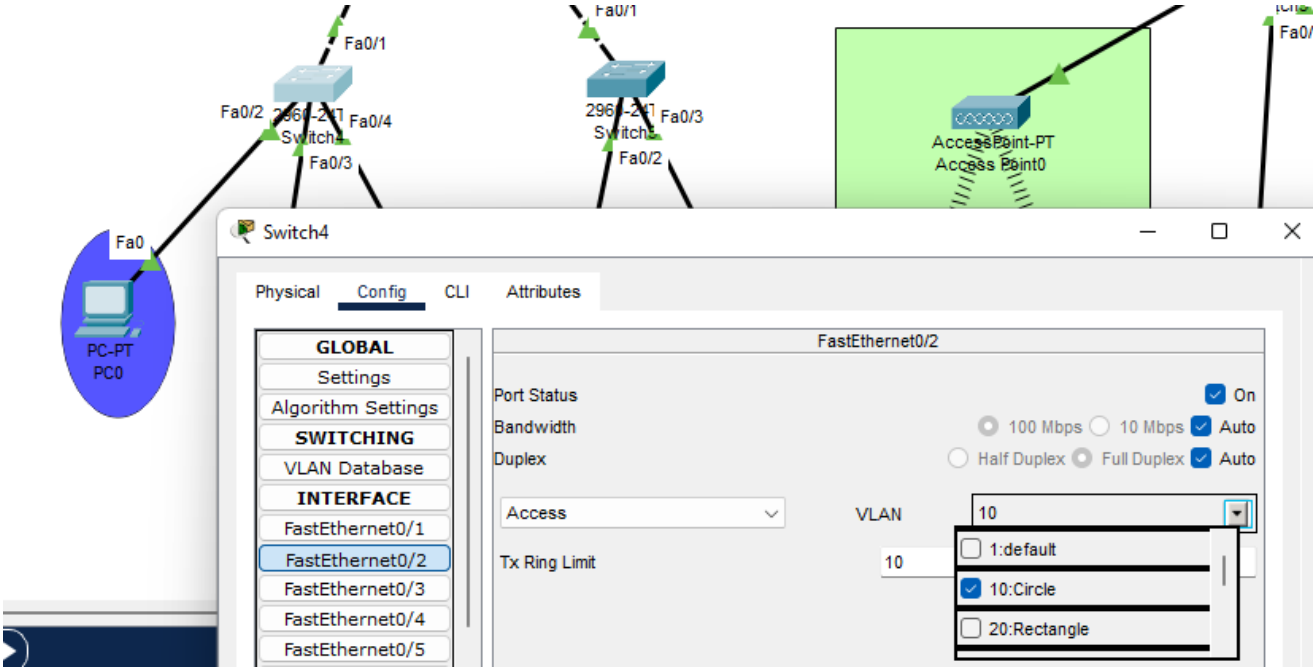

Switch7
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet1/1
FastEthernet2/1
FastEthernet3/1
FastEthernet4/1
FastEthernet5/1
VLAN Configuration
VLAN Number
30
VLAN Name
Irregular
Add
Remove
VLAN No
VLAN Name
1 default
10 Circle
20 Rectangle
30 Irregular
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default

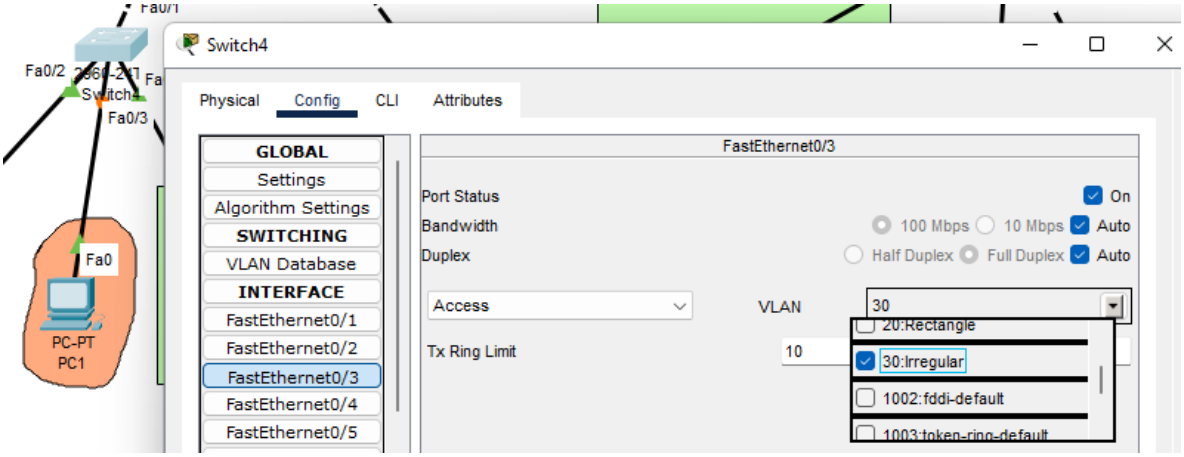

Switch8
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet1/1
FastEthernet2/1
FastEthernet3/1
FastEthernet4/1
FastEthernet5/1
VLAN Configuration
VLAN Number
30
VLAN Name
Irregular
Add
Remove
VLAN No
VLAN Name
1 default
10 Circle
20 Rectangle
30 Irregular
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default

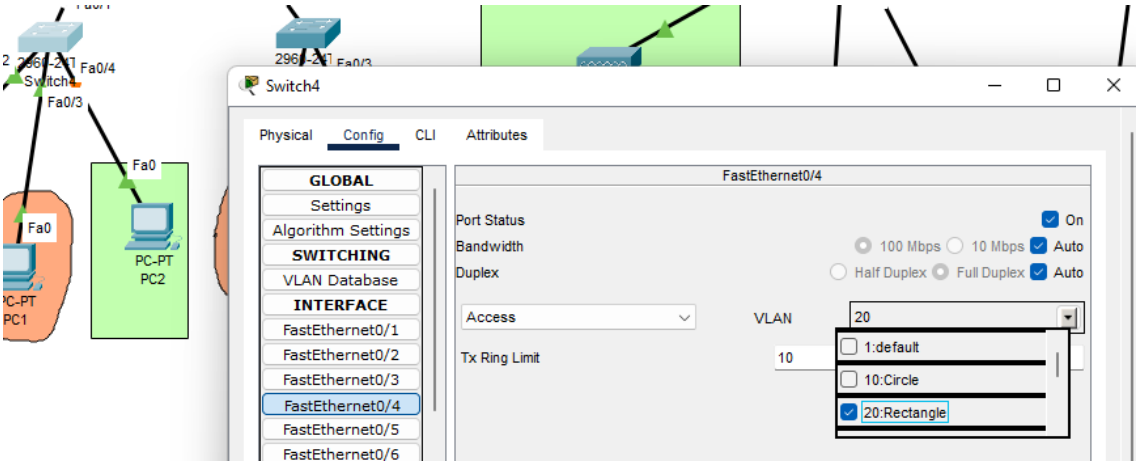

Switch9
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet1/1
FastEthernet2/1
FastEthernet3/1
FastEthernet4/1
FastEthernet5/1
VLAN Configuration
VLAN Number
1
VLAN Name
default
Add
Remove
VLAN No
VLAN Name
1 default
10 Circle
20 Rectangle
30 Irregular
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default

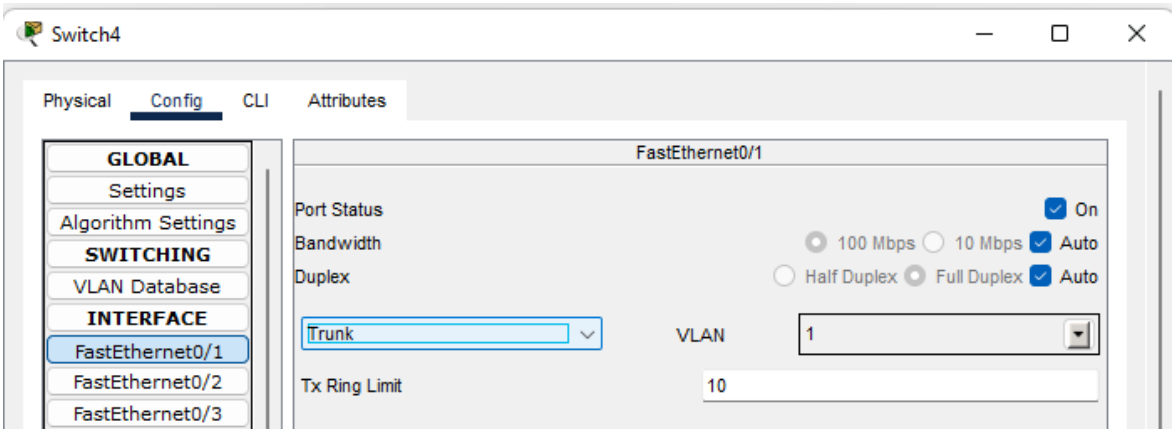


Now we configure the interfaces of each router according to the color. To simplify, only one configuration for each VLAN will be shown, but this process is done on all interfaces that have a device associated with a VLAN.







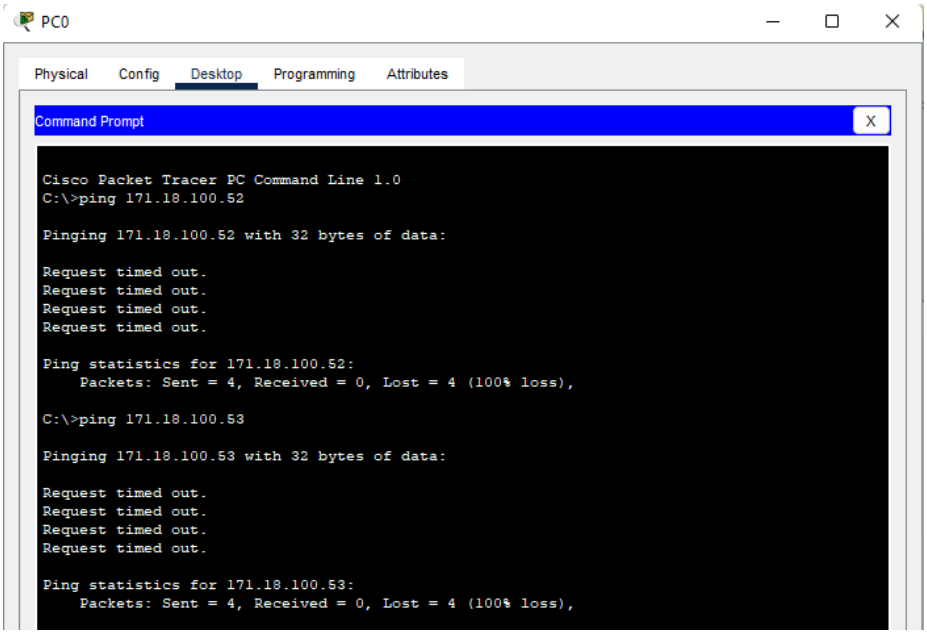


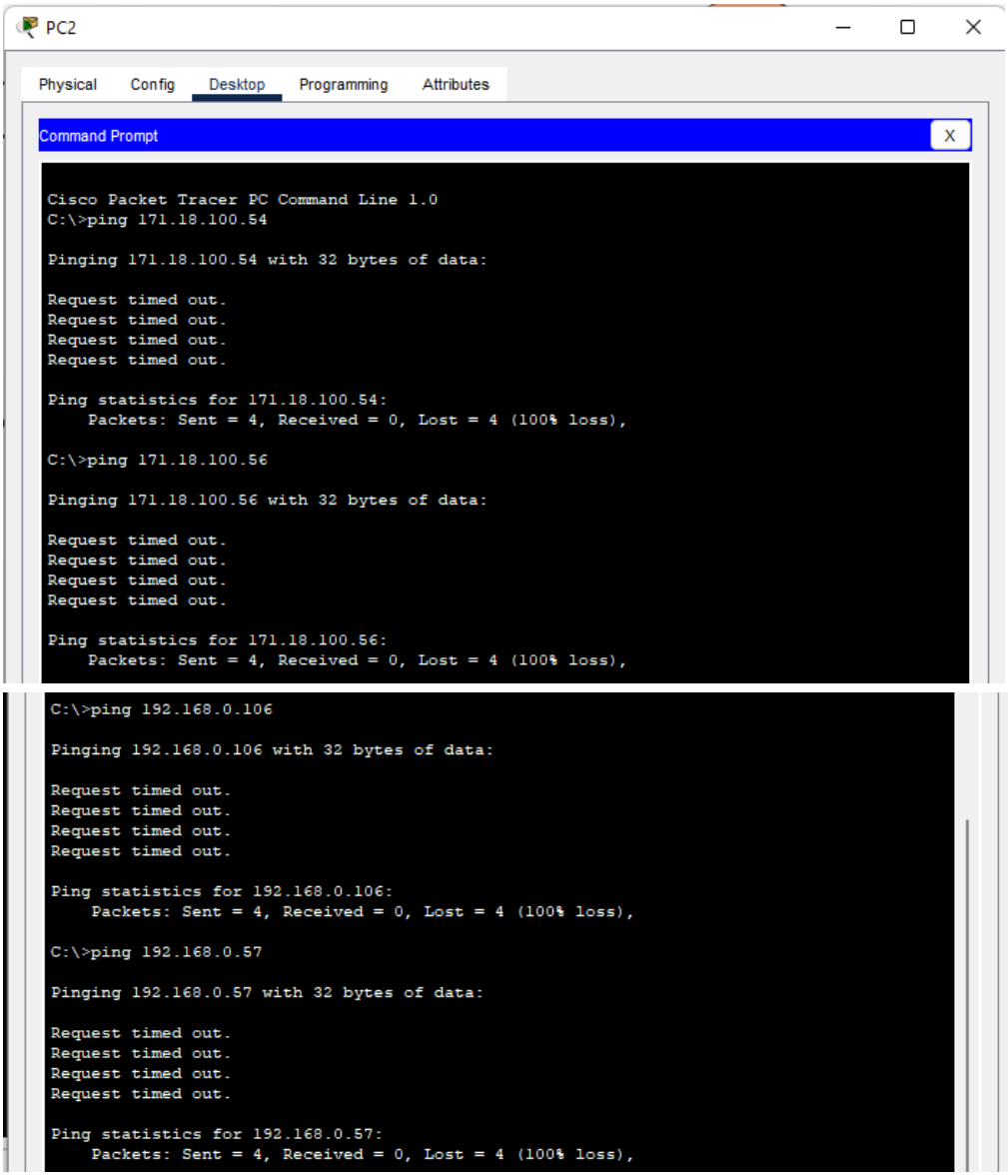
Now we will perform connection tests using the **ping** commands and the packet-sending interface in Packet Tracer. We verify that the network operates as expected according to the configured VLANs.

- Packet sending.

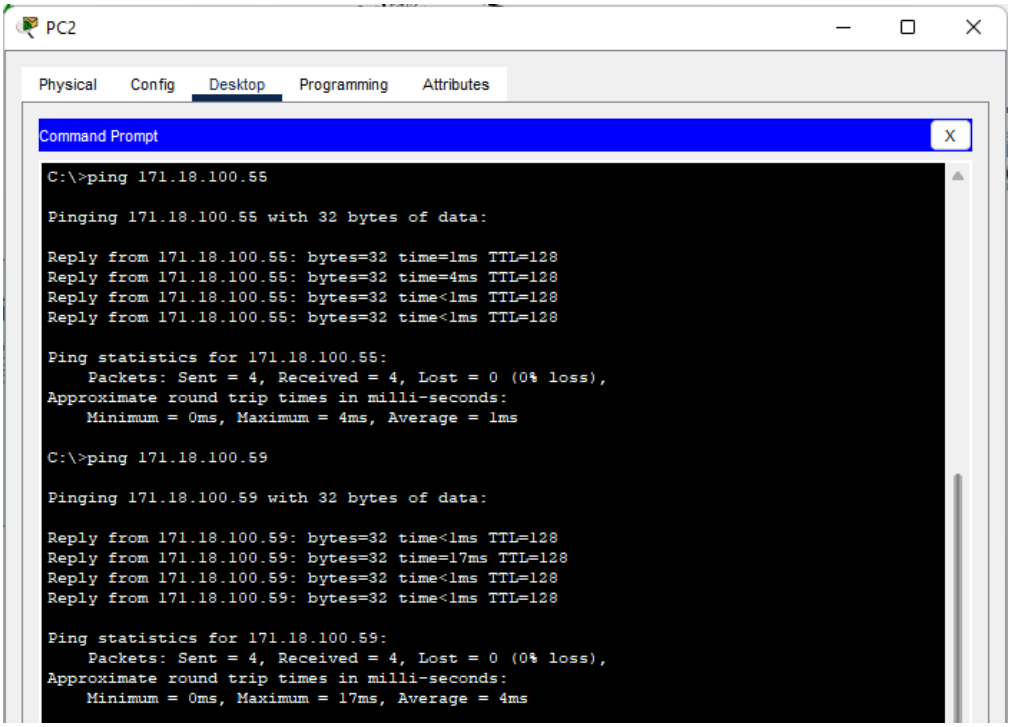
Successful	PC0	PC6	ICMP	
Successful	PC0	PC5	ICMP	
Successful	PC0	PC5	ICMP	
Successful	PC6	PC0	ICMP	
Successful	PC0	Server1	ICMP	
Failed	PC10	PC0	ICMP	
Failed	Smartph...	PC0	ICMP	
Successful	Smartph...	PC10	ICMP	

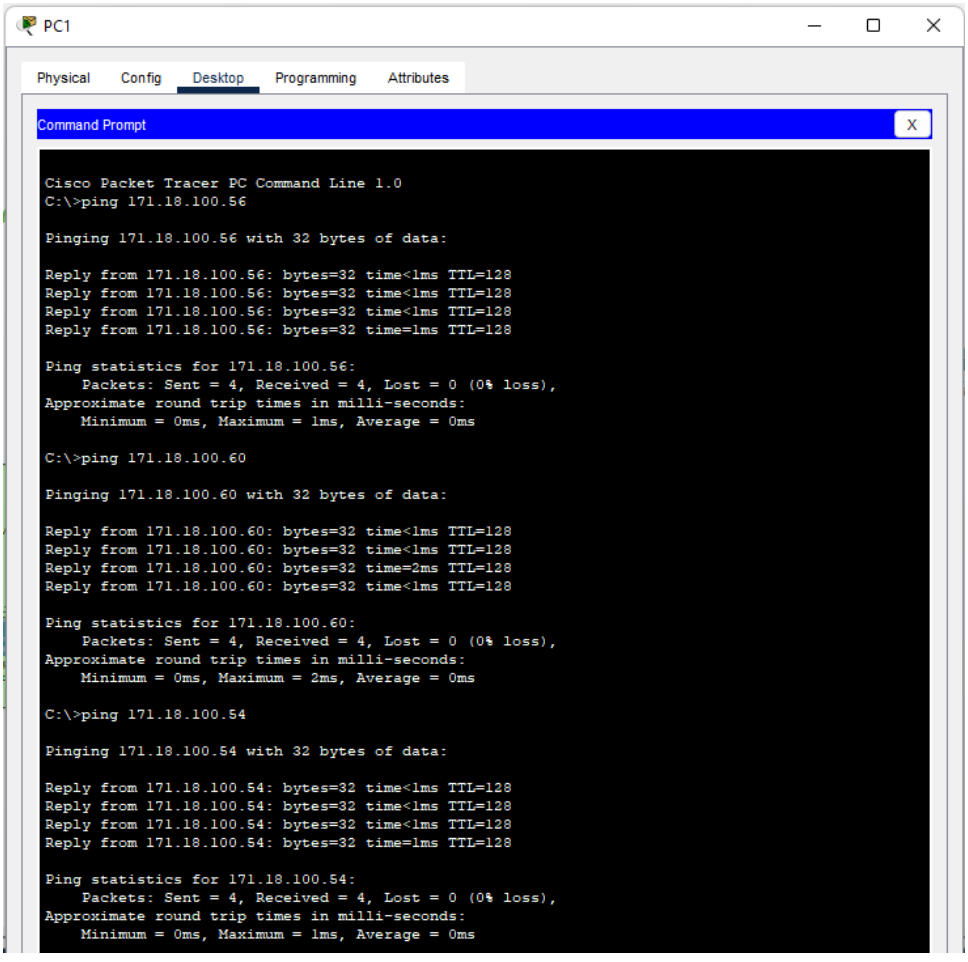
- Pings

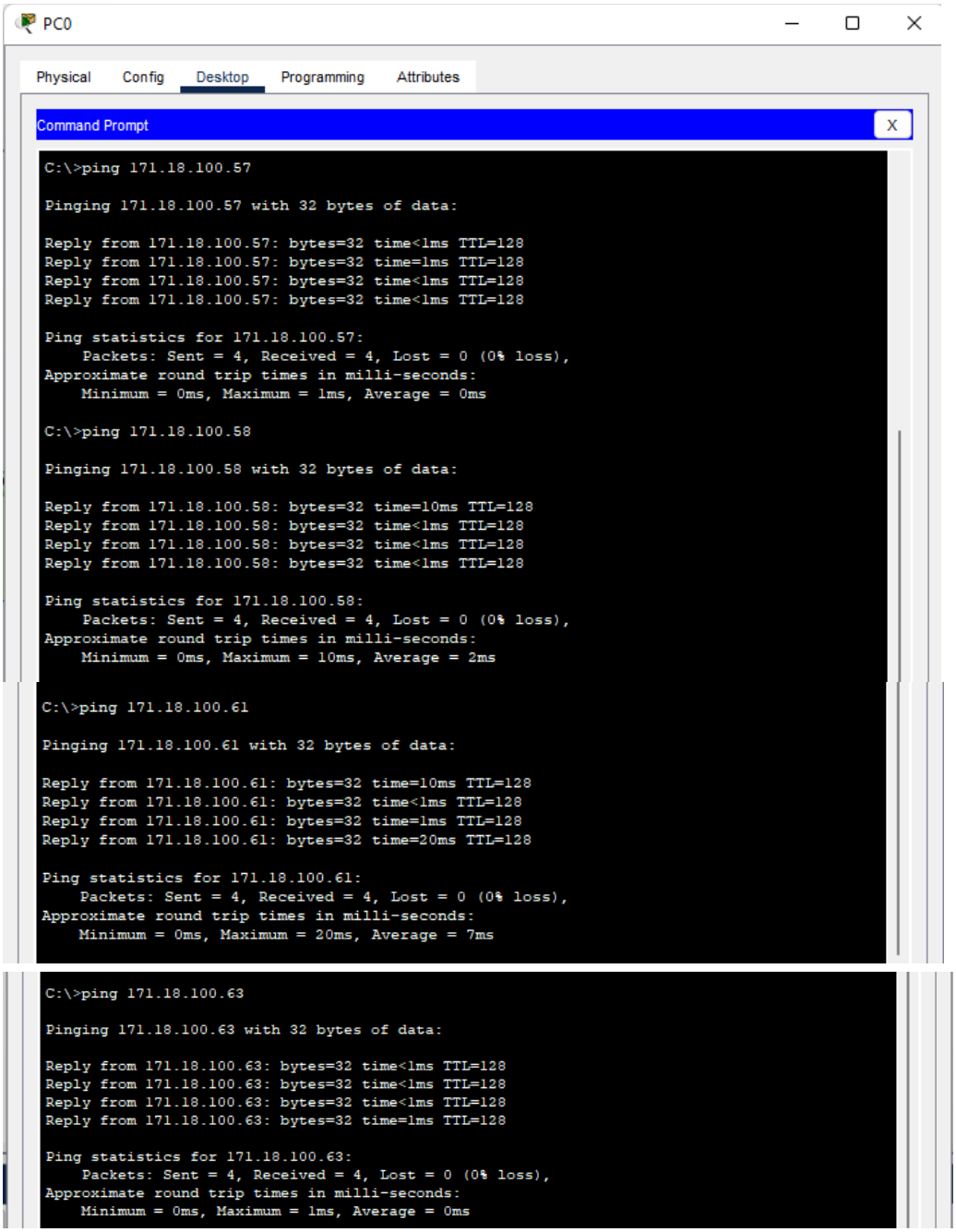



PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 171.18.100.54
Pinging 171.18.100.54 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 171.18.100.54:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 171.18.100.56
Pinging 171.18.100.56 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 171.18.100.56:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

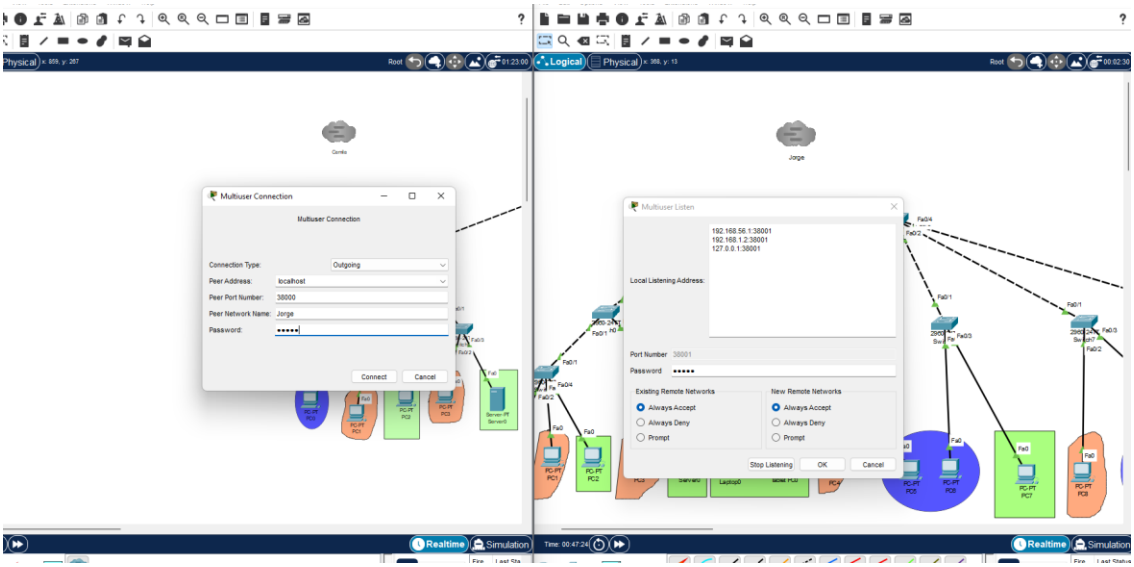
C:\>ping 192.168.0.106
Pinging 192.168.0.106 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.106:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.57
Pinging 192.168.0.57 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.57:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

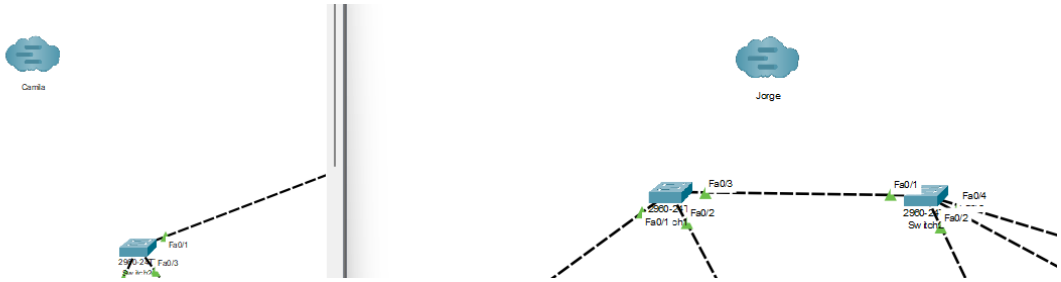

PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 171.18.100.55
Pinging 171.18.100.55 with 32 bytes of data:
Reply from 171.18.100.55: bytes=32 time=1ms TTL=128
Reply from 171.18.100.55: bytes=32 time=4ms TTL=128
Reply from 171.18.100.55: bytes=32 time<1ms TTL=128
Reply from 171.18.100.55: bytes=32 time<1ms TTL=128
Ping statistics for 171.18.100.55:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 1ms
C:\>ping 171.18.100.59
Pinging 171.18.100.59 with 32 bytes of data:
Reply from 171.18.100.59: bytes=32 time<1ms TTL=128
Reply from 171.18.100.59: bytes=32 time=17ms TTL=128
Reply from 171.18.100.59: bytes=32 time<1ms TTL=128
Reply from 171.18.100.59: bytes=32 time<1ms TTL=128
Ping statistics for 171.18.100.59:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 17ms, Average = 4ms

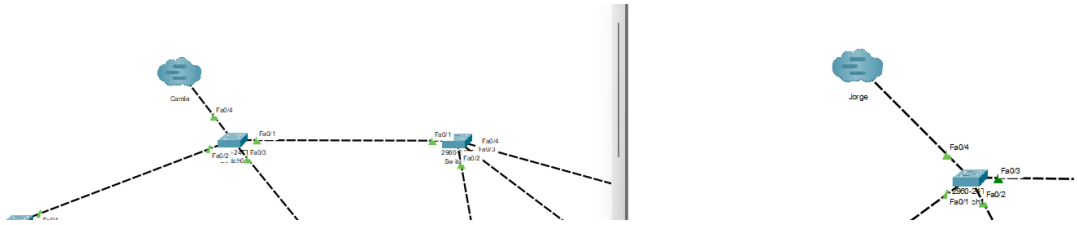

PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 171.18.100.56
Pinging 171.18.100.56 with 32 bytes of data:
Reply from 171.18.100.56: bytes=32 time<1ms TTL=128
Reply from 171.18.100.56: bytes=32 time<1ms TTL=128
Reply from 171.18.100.56: bytes=32 time<1ms TTL=128
Reply from 171.18.100.56: bytes=32 time=1ms TTL=128
Ping statistics for 171.18.100.56:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 171.18.100.60
Pinging 171.18.100.60 with 32 bytes of data:
Reply from 171.18.100.60: bytes=32 time<1ms TTL=128
Reply from 171.18.100.60: bytes=32 time<1ms TTL=128
Reply from 171.18.100.60: bytes=32 time=2ms TTL=128
Reply from 171.18.100.60: bytes=32 time<1ms TTL=128
Ping statistics for 171.18.100.60:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>ping 171.18.100.54
Pinging 171.18.100.54 with 32 bytes of data:
Reply from 171.18.100.54: bytes=32 time<1ms TTL=128
Reply from 171.18.100.54: bytes=32 time<1ms TTL=128
Reply from 171.18.100.54: bytes=32 time<1ms TTL=128
Reply from 171.18.100.54: bytes=32 time=1ms TTL=128
Ping statistics for 171.18.100.54:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms



Finally, Merge the project files from team members.


Multiuser Connection
Connection Type:
Outgoing
Peer Address:
localhost
Peer Port Number:
38000
Peer Network Name:
Jorge
Password:
Connect
Cancel
Multiuser Listen
Local Listening Address:
Port Number
Password
Existing Remote Networks
New Remote Networks
Always Accept
Always Deny
Prompt
Stop Listening
OK
Cancel
Realtime
Simulation

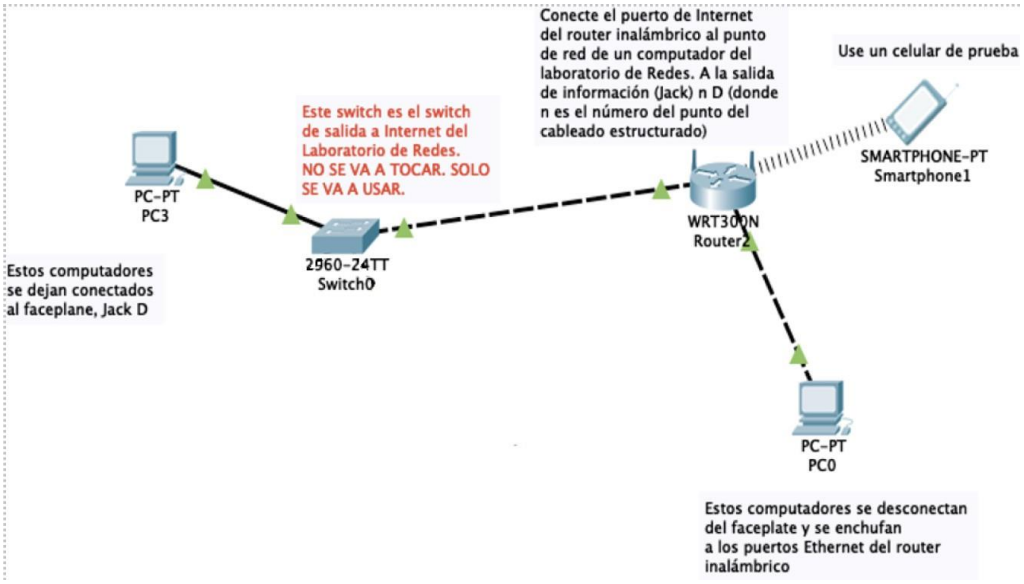

Camila
Jorge
Fa0/1
Fa0/3
Fa0/2
Fa0/4


Camila
Jorge
Fa0/1
Fa0/2
Fa0/3
Fa0/4

```
C:\>ping 171.18.110.51

Pinging 171.18.110.51 with 32 bytes of data:

Reply from 171.18.110.51: bytes=32 time=51ms TTL=128
Reply from 171.18.110.51: bytes=32 time=33ms TTL=128
Reply from 171.18.110.51: bytes=32 time=50ms TTL=128
Reply from 171.18.110.51: bytes=32 time=34ms TTL=128

Ping statistics for 171.18.110.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 51ms, Average = 42ms

C:\>ping 171.18.100.51

Pinging 171.18.100.51 with 32 bytes of data:

Reply from 171.18.100.51: bytes=32 time<1ms TTL=128
Reply from 171.18.100.51: bytes=32 time=5ms TTL=128
Reply from 171.18.100.51: bytes=32 time<1ms TTL=128
Reply from 171.18.100.51: bytes=32 time=4ms TTL=128

Ping statistics for 171.18.100.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 2ms

C:\>
```

7. WiFi

7.1. Configuration Process



- We configure the IP, subnet mask, and gateway of the computer disconnected from the faceplate (PC0 in the diagram)

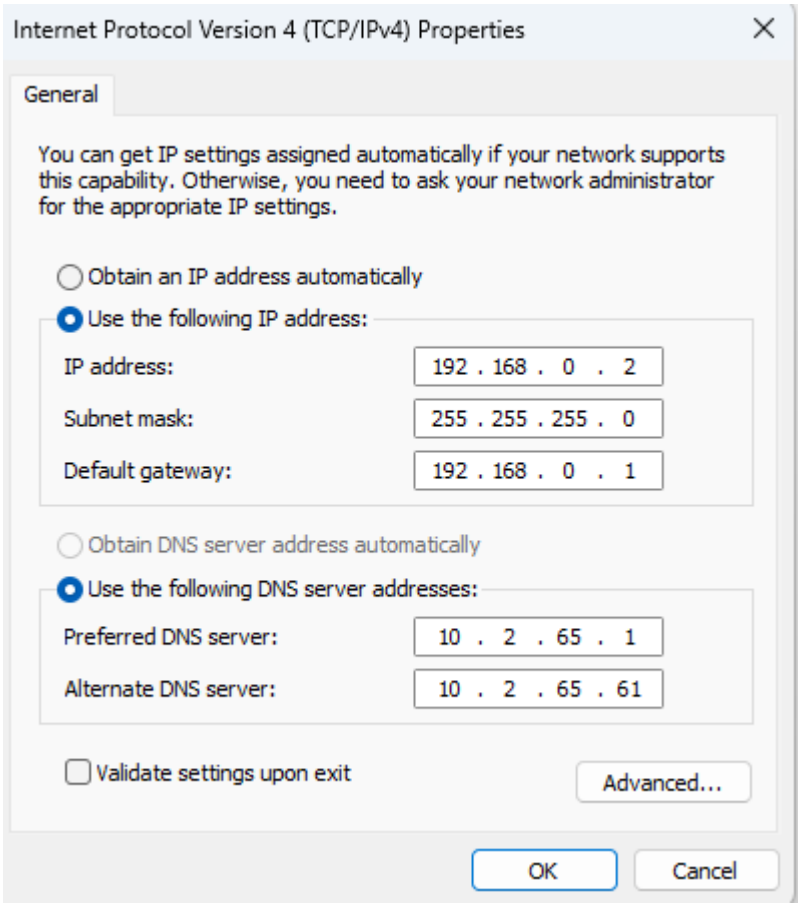


Figure 58. Configuring IP and Subnet Mask on the Computer ("PC0")

- We enter the router's IP address in the browser and authenticate as an administrator

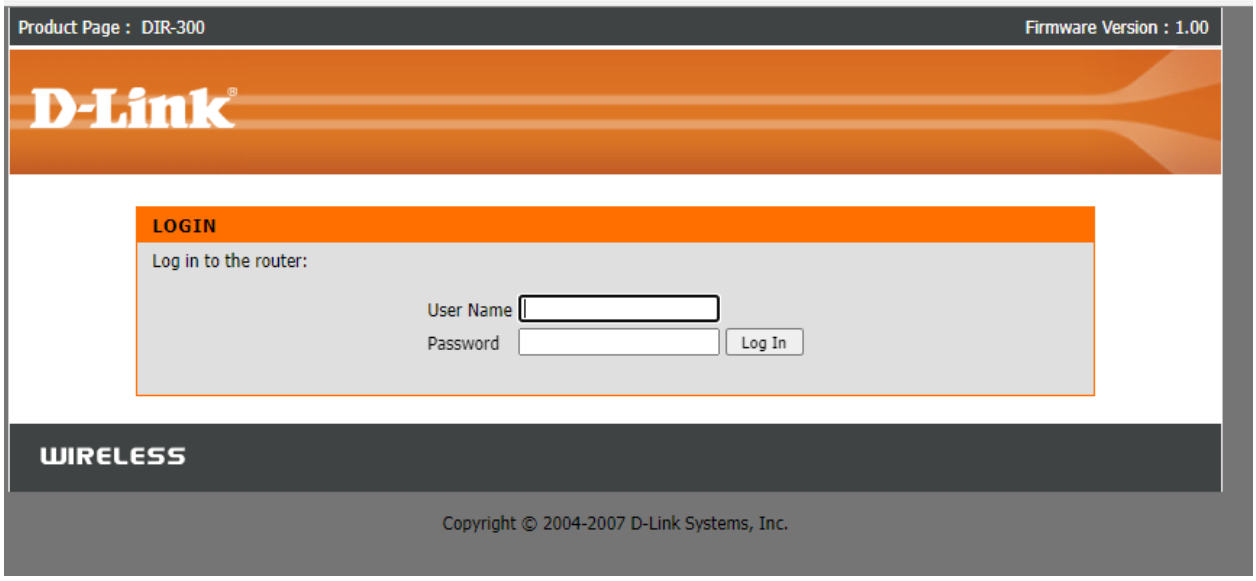


Figure 59. Authenticating to Configure the Wireless Router

- We go to Wireless Setup

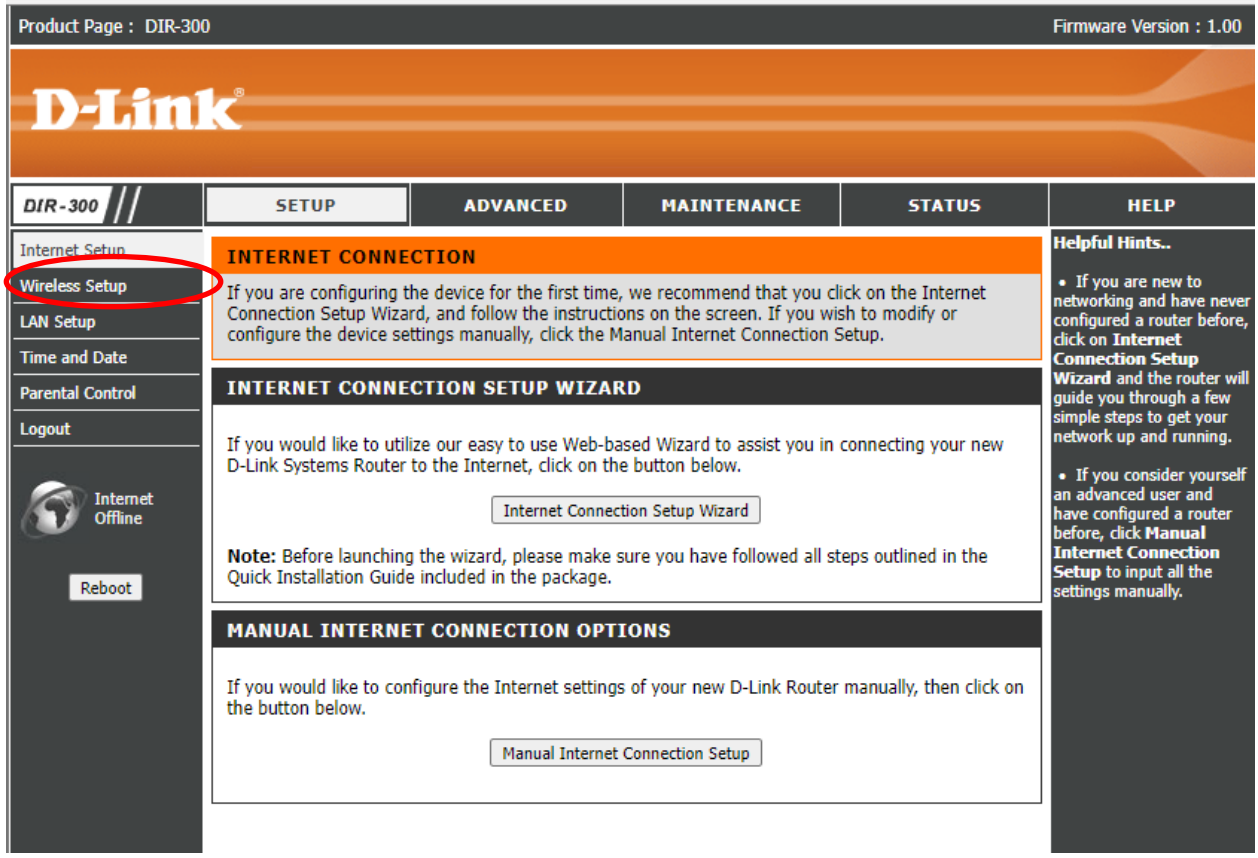


Figure 60. Main Menu of the Wireless Router Configuration

- We enter the wireless network identifier (SSID) and click Next

Figure 61. Assigning a Name to the Wireless Network

- We select the 'BEST' option to use WPA2 as the access mechanism

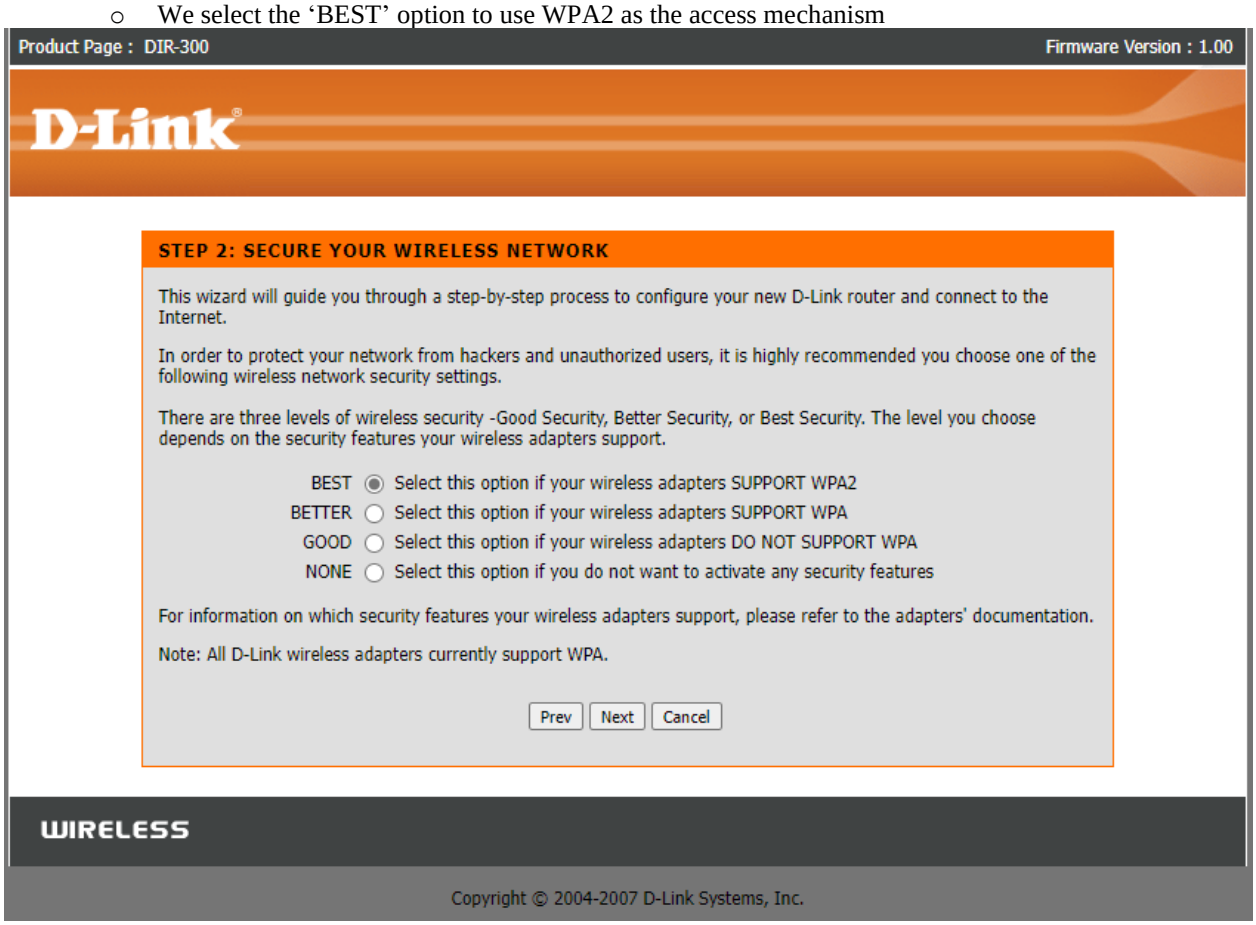


Figure 62. Assigning Access Mechanism to Wireless Clients: WPA2-PSK with AES

- We create the router's access key

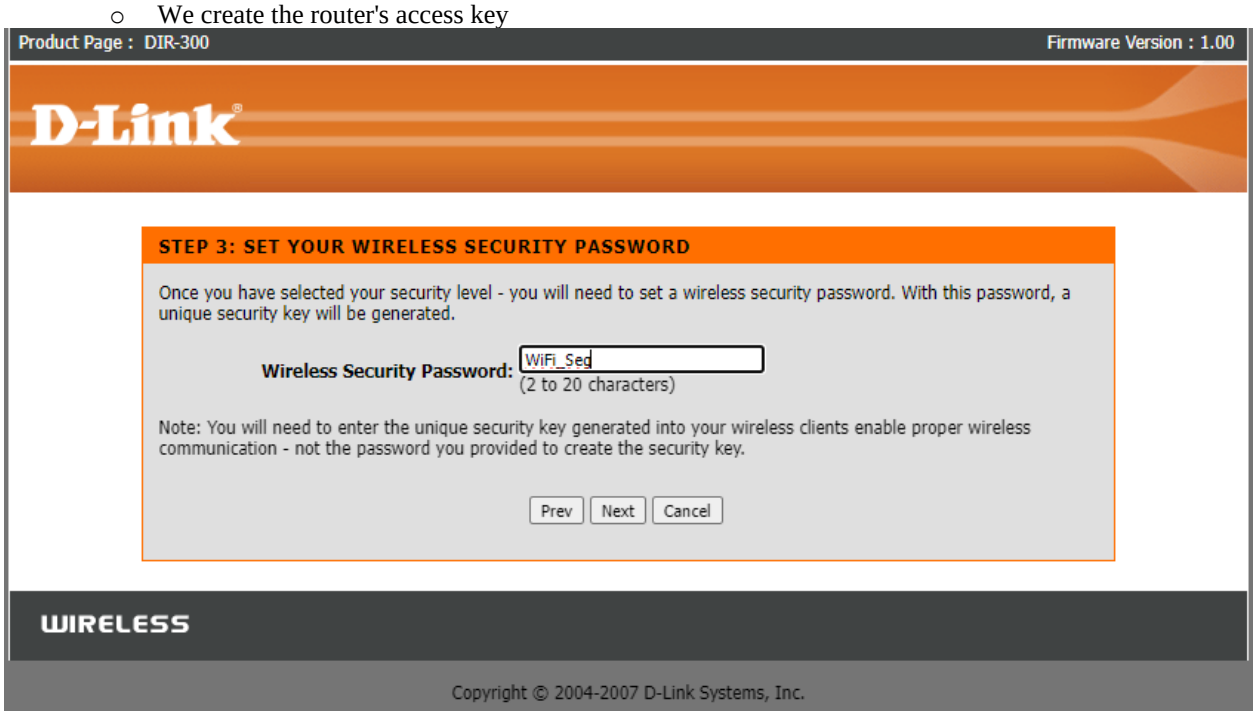


Figure 63. Assigning a Wireless Security Password

- We verify the changes and save them

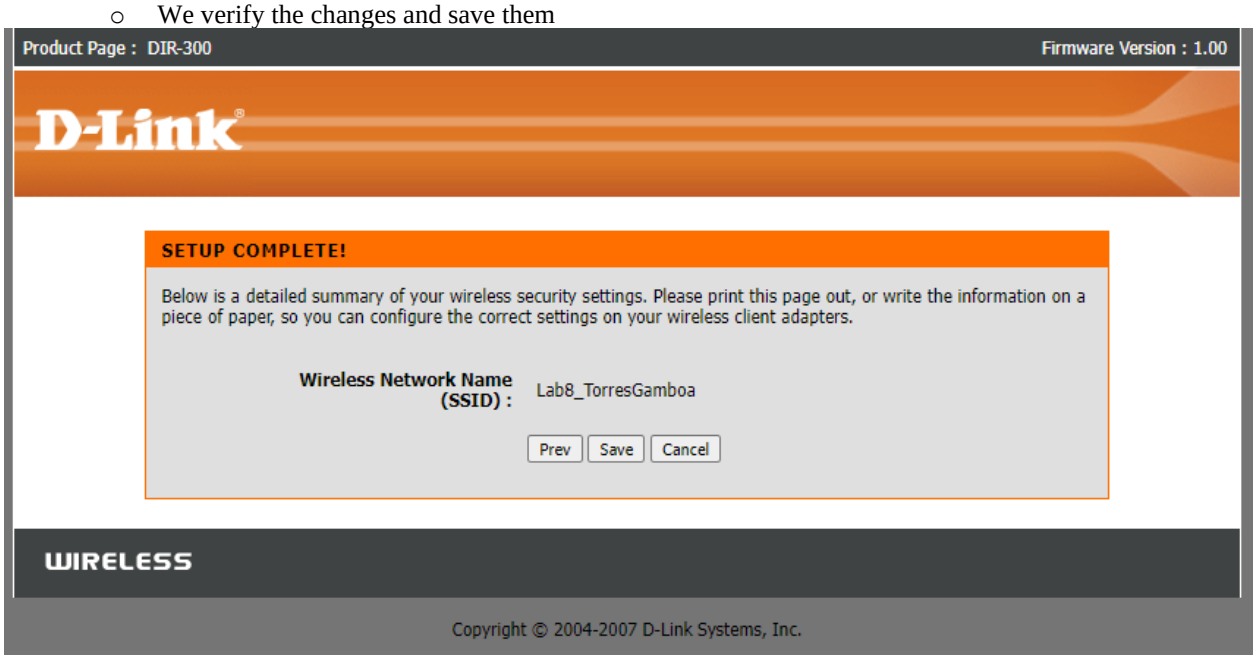


Figure 64. Saving Changes to the Wireless Setup

- Now, we go to the Internet Connection Wizard

Figure 65. Accessing to Internet Connection Setup Wizard

- We assign a password for the administrator's access and click Next

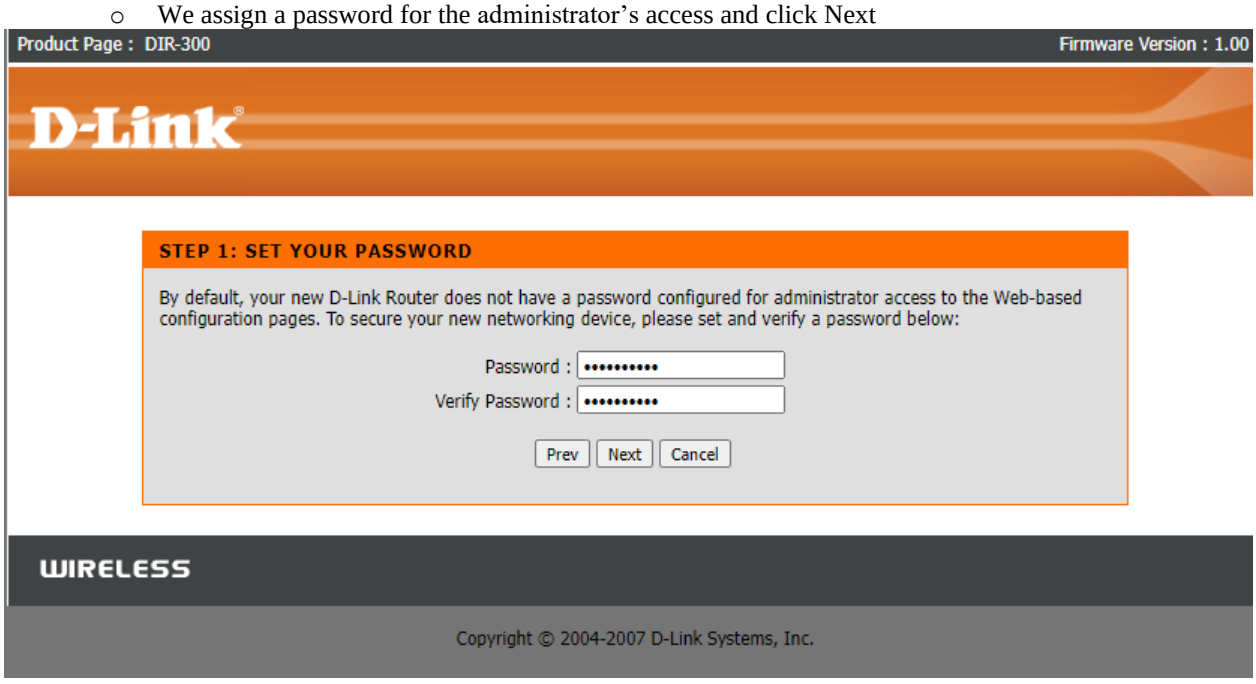


Figure 66. Setting a password for the Administrator

- We configure the Time Zone

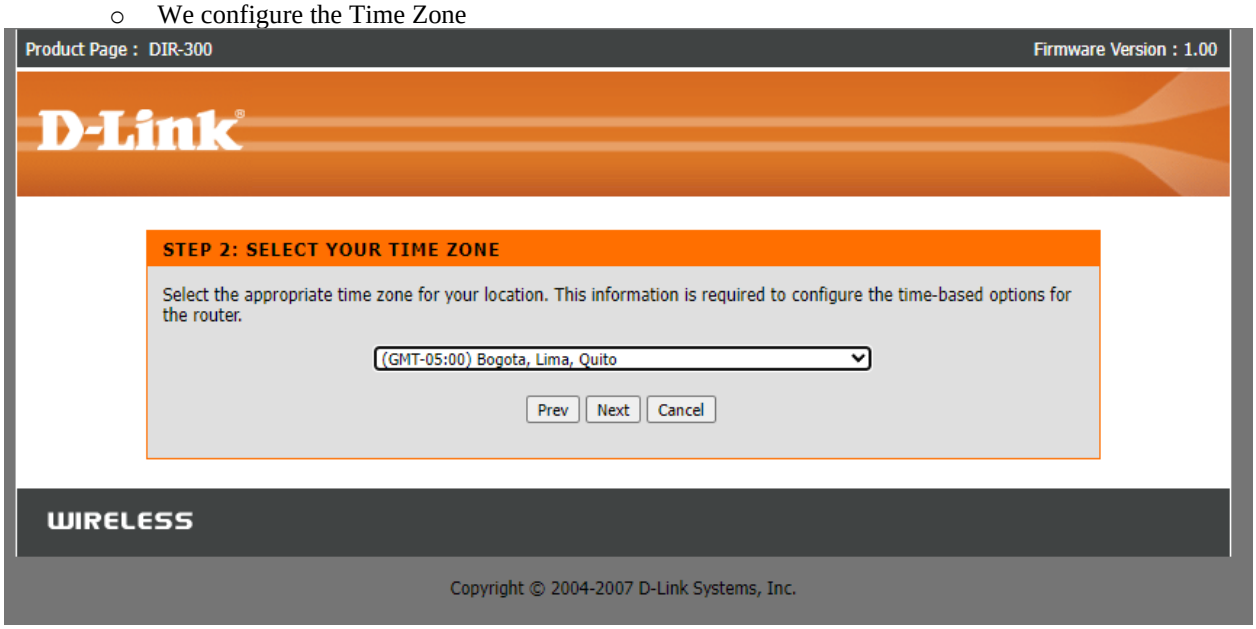


Figure 67. Selecting Time Zone to the router

- For now, we leave the default option of DHCP Connection

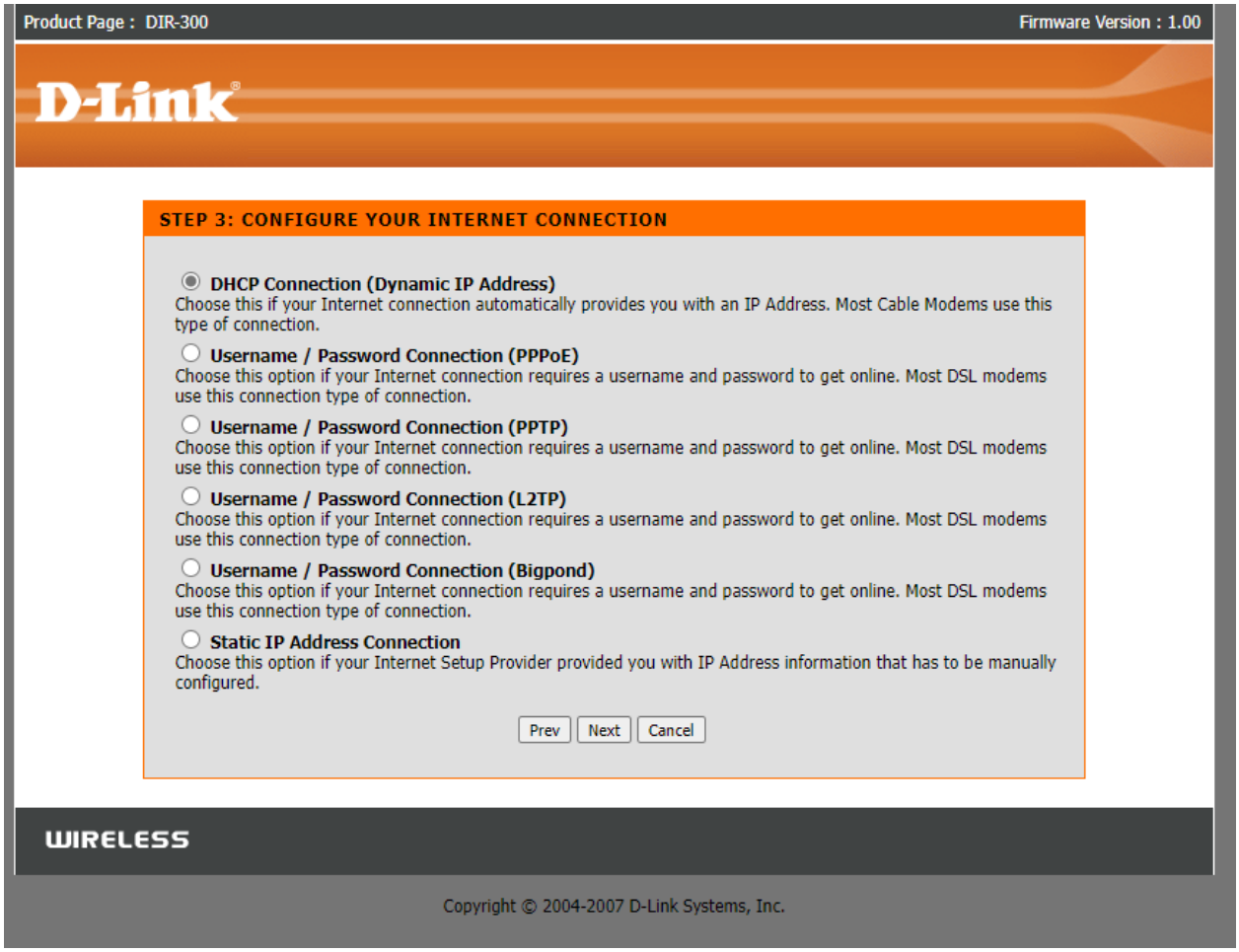


Figure 68. Configuring Internet Connection

- We leave the default option and click Next

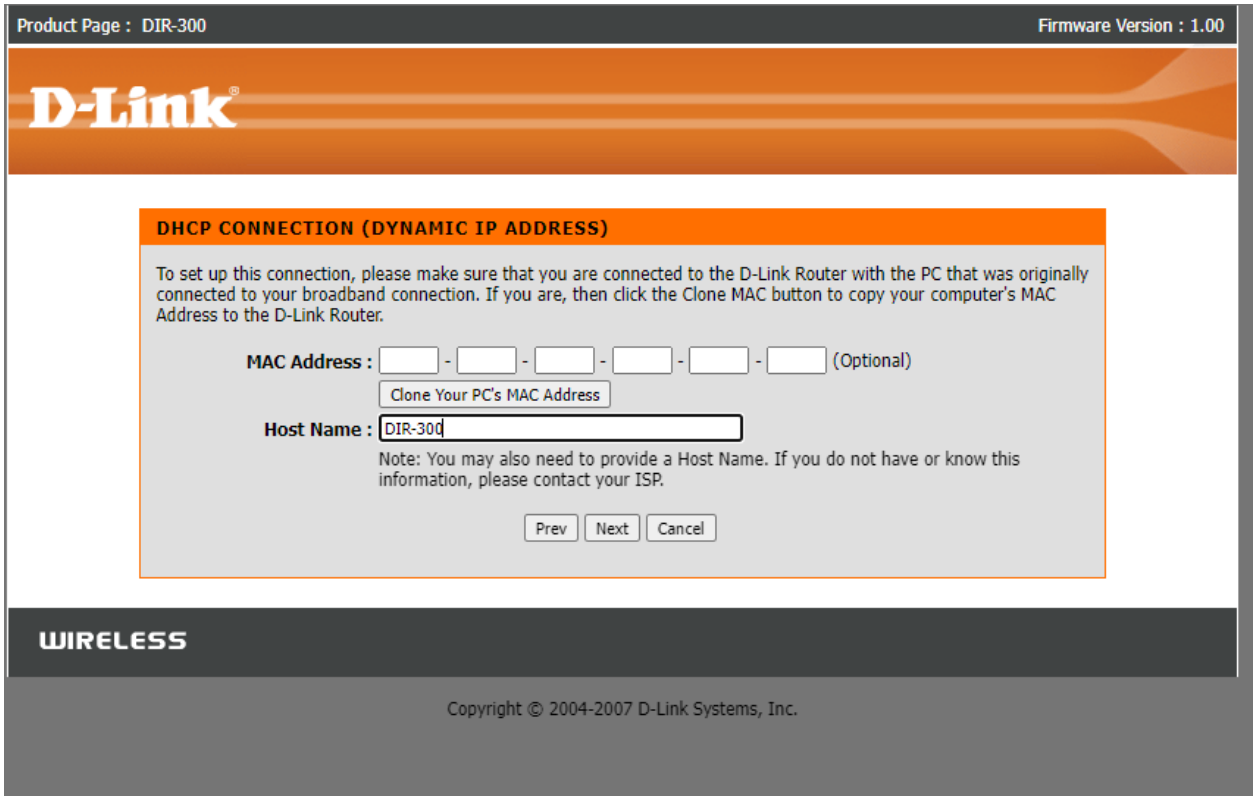


Figure 69. Default Value for the DHCP Connection Section

- We save and go to LAN Setup, where we configure the IP range (from 20 to 30)

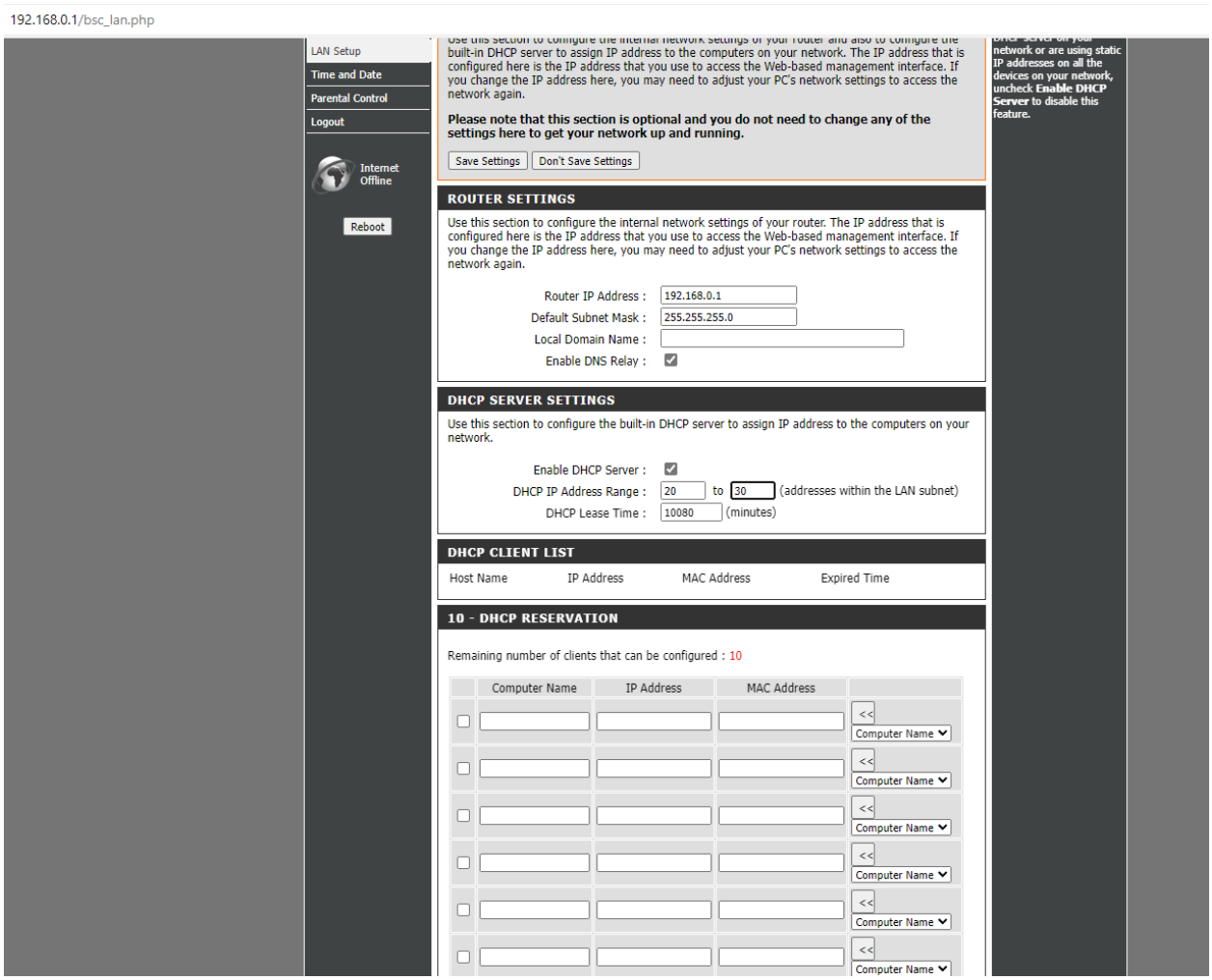


Figure 70. Configuring IP Address Range on the Wireless Router

- Now, we go to Manual Internet Connection Setup

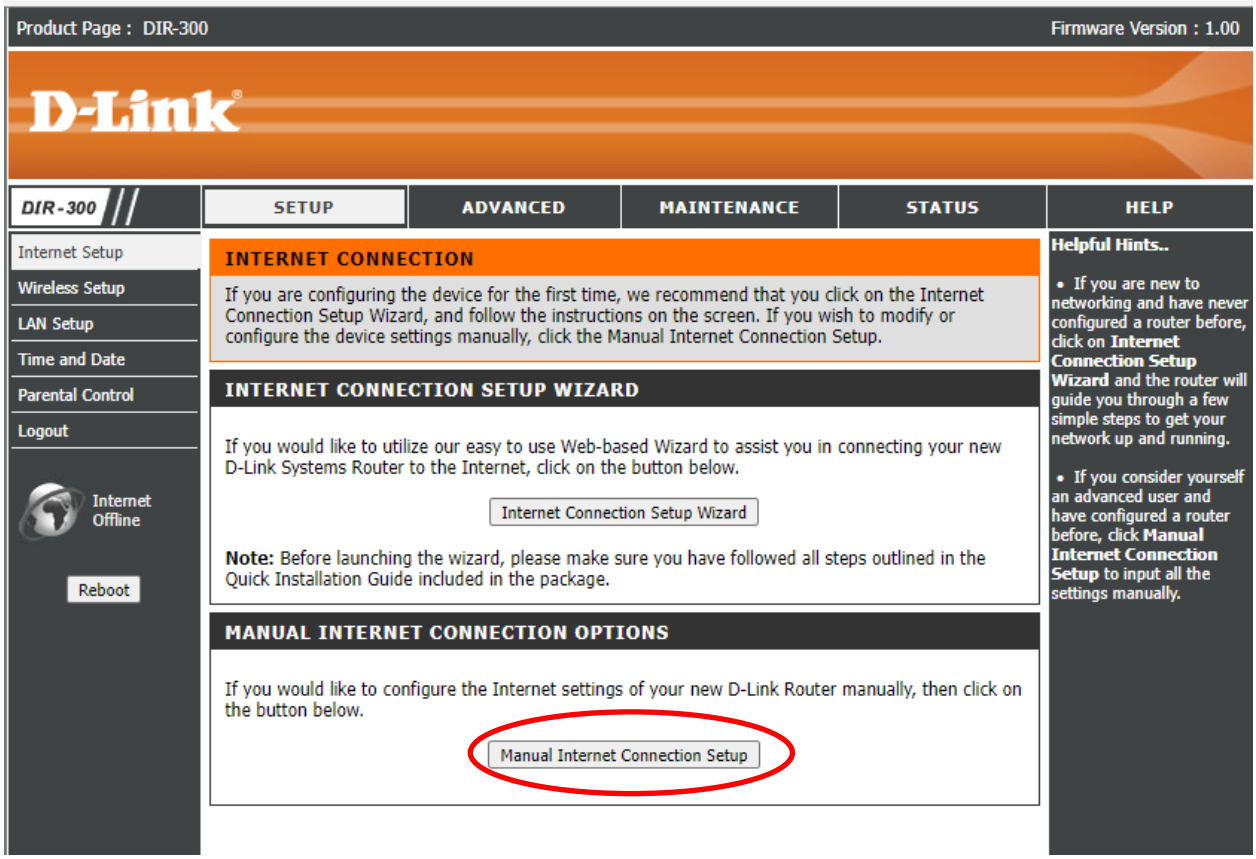


Figure 71. Opening Manual Internet Connection Setup

- We assign the static IP address of the machine we are using (10.2.67.105) and the subnet mask 255.255.0.0

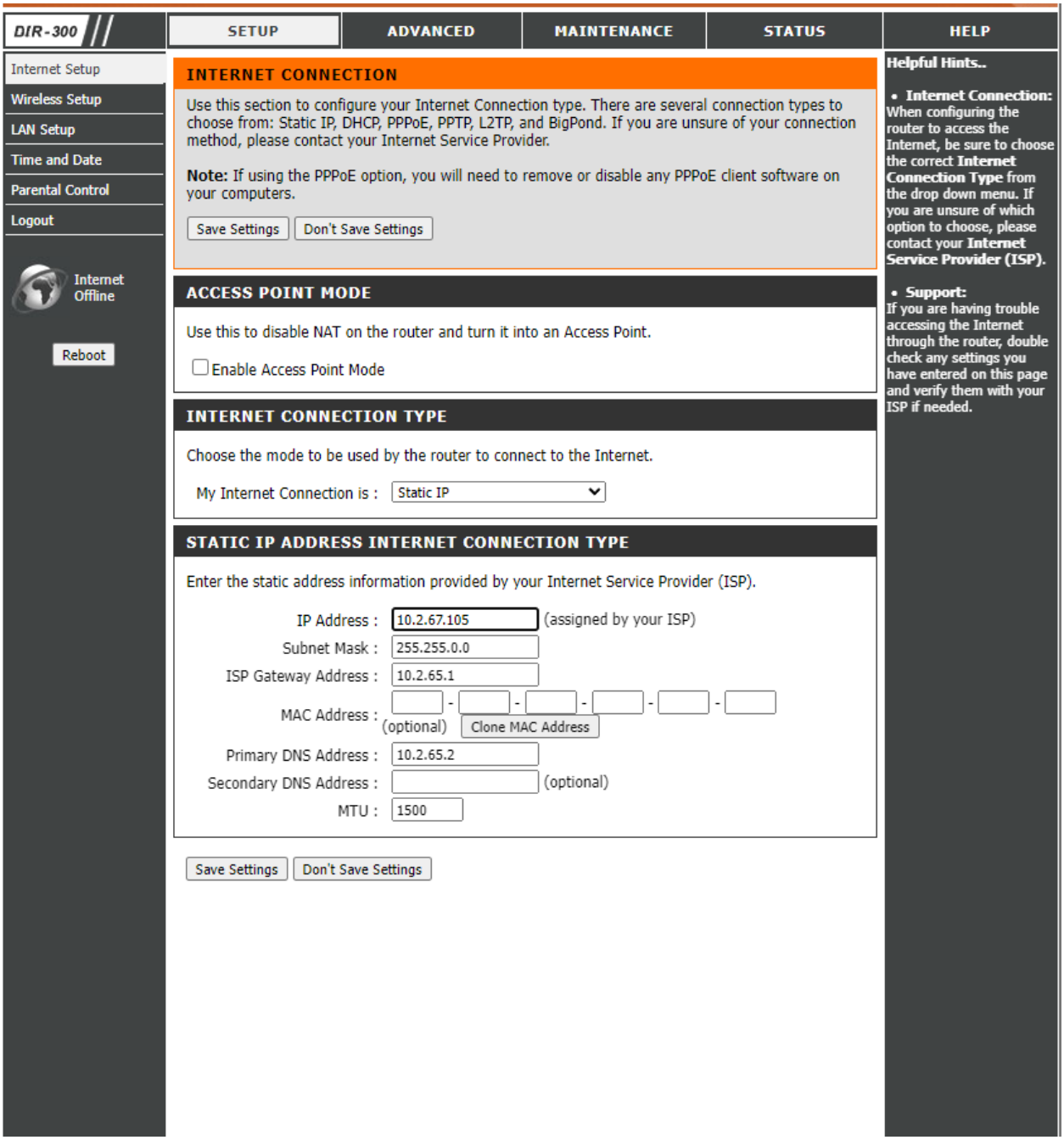


Figure 72. Static IP Address Internet Connection Type of the Wireless Router

- Now, we go to Wireless Network Settings and select a channel. We can observe that these range from 1 to 11

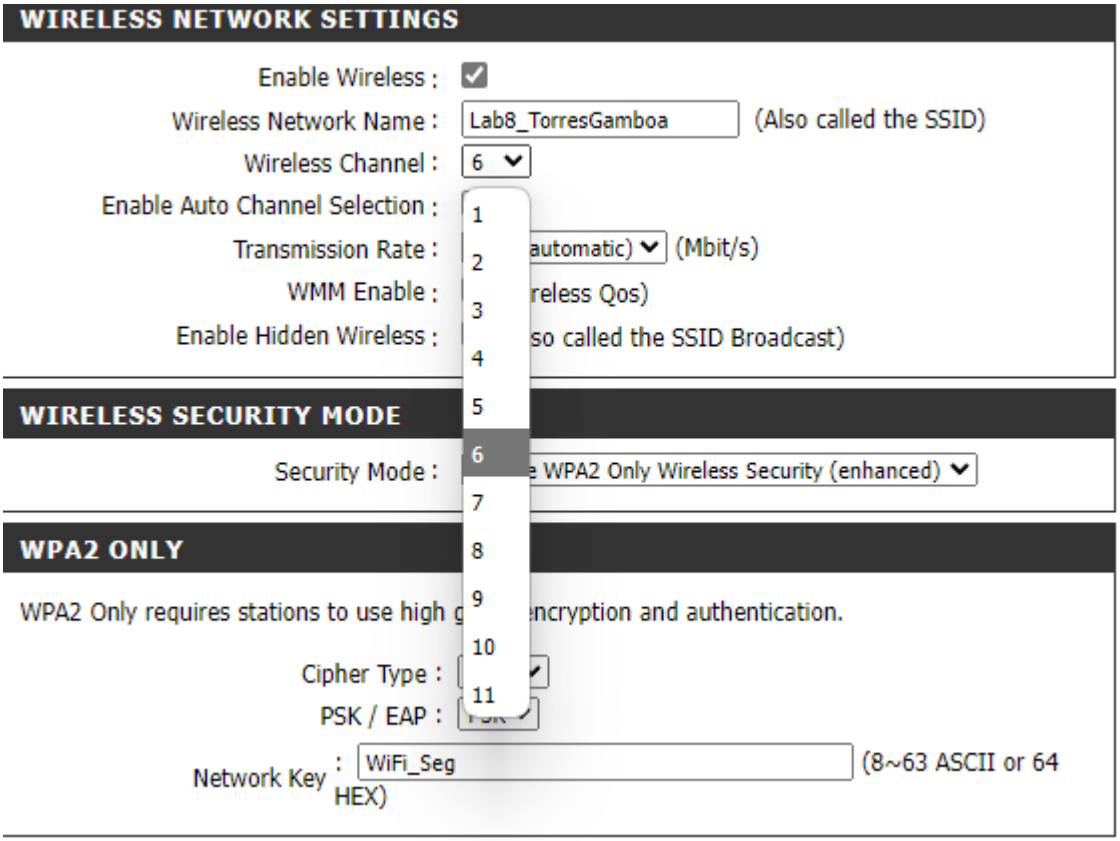


Figure 73. Available Channels of the Wireless Router

- In our case, we select channel 5 and save the configuration

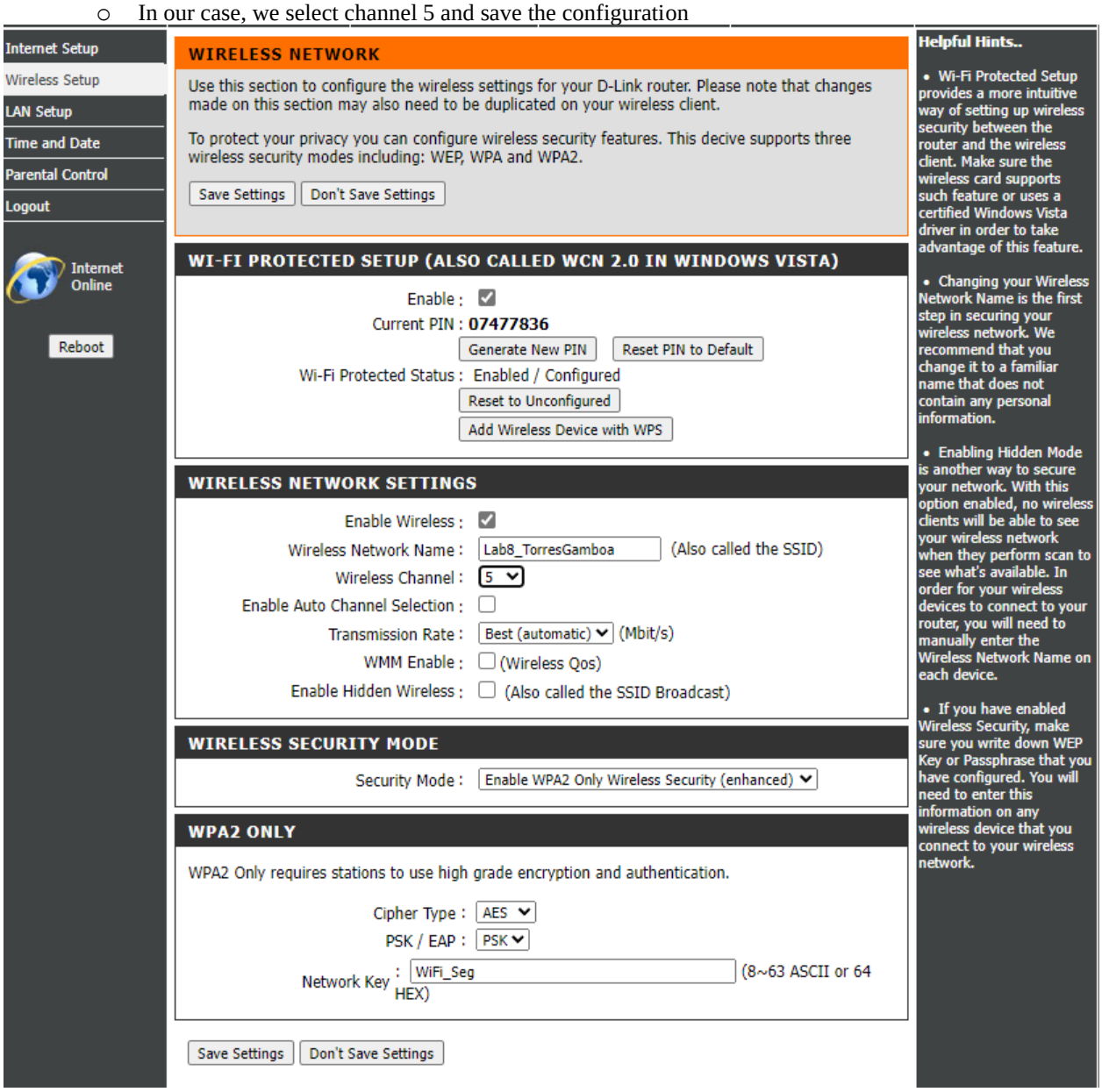


Figure 74. Configuring a Channel on the Wireless Router

7.2. Testing from devices

- From our smartphone, we disable the Wi-Fi network we were using and connect to the router's network, whose SSID is the one we configured earlier

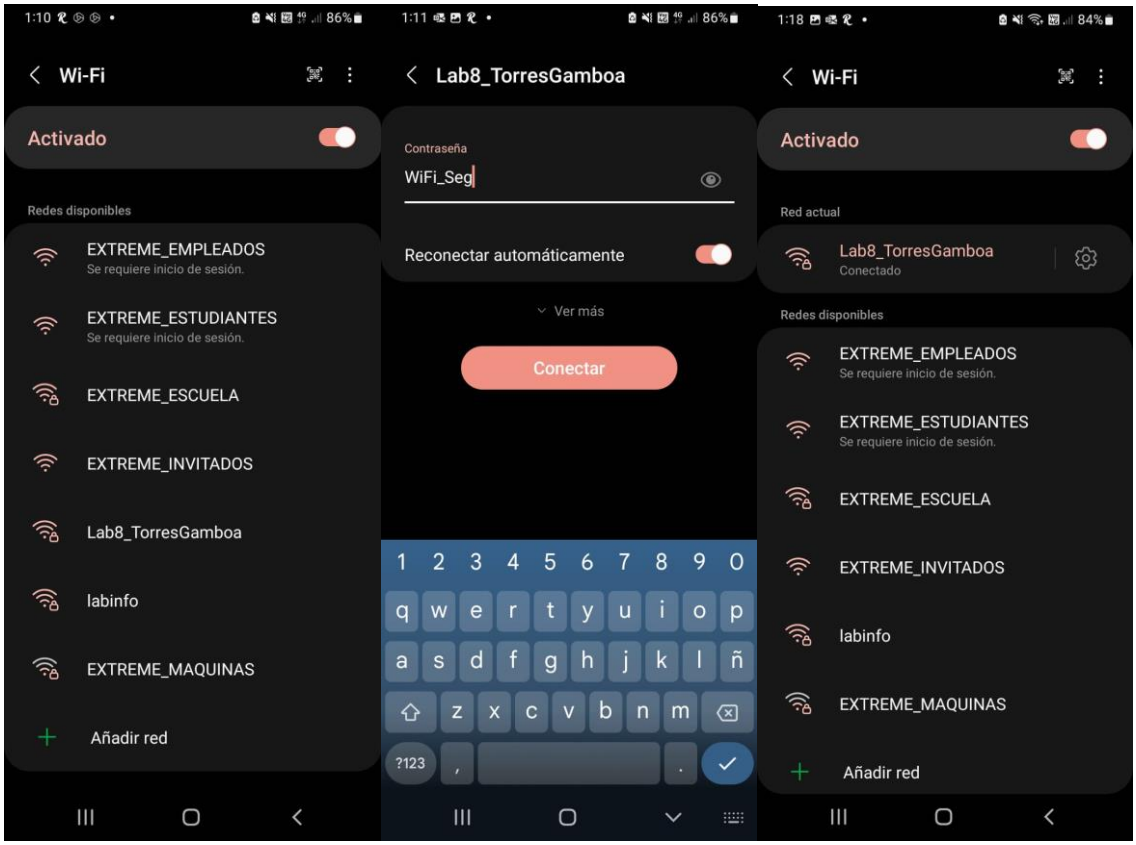


Figure 75. Authenticating and Connecting to the Wireless Network from the Mobile

- We verify that it has assigned us an IP address within the configured range. In this case, it is assigning the address 192.168.0.20

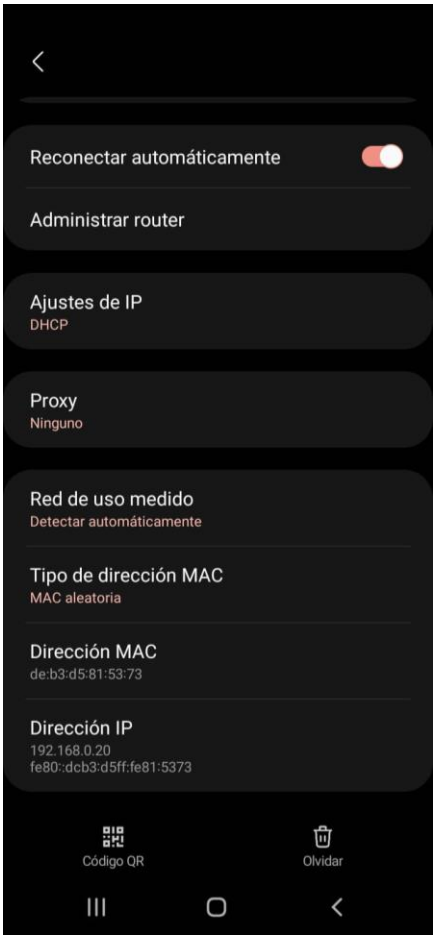


Figure 76. IP Assigned to the Smartphone

- Now, we ping from the smartphone to different devices, such as the computer PC0, Google's services, and another computer in the laboratory that is on the network 10.2.67.x

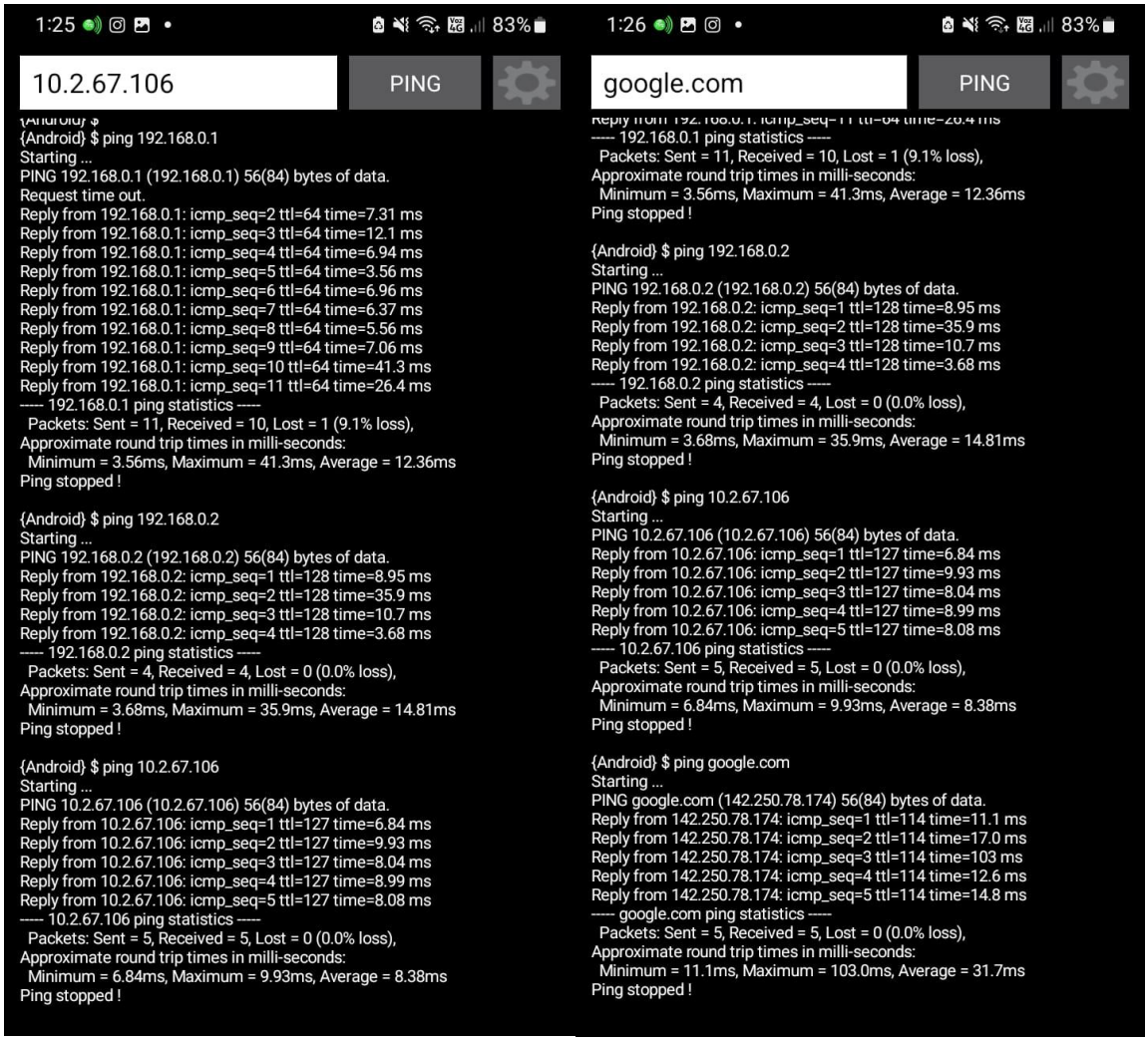


Figure 77. Ping Tests on the Mobile Device

- From the computer (PC0 in the diagram), we perform connectivity tests to the mobile device we connected earlier, Google's services, the internet, and devices in the laboratory with the 10.2.67.x network, as well as

others on different networks

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Redes>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:
Reply from 192.168.0.20: bytes=32 time=419ms TTL=64
Reply from 192.168.0.20: bytes=32 time=118ms TTL=64
Reply from 192.168.0.20: bytes=32 time=27ms TTL=64
Reply from 192.168.0.20: bytes=32 time=36ms TTL=64

Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 419ms, Average = 150ms

C:\Users\Redes>
```

Figure 78. Ping from the Computer (PC0 in the Diagram) to the Smartphone

```
C:\Users\Redes>ping 10.2.67.106

Pinging 10.2.67.106 with 32 bytes of data:
Reply from 10.2.67.106: bytes=32 time=4ms TTL=127
Reply from 10.2.67.106: bytes=32 time=3ms TTL=127
Reply from 10.2.67.106: bytes=32 time=3ms TTL=127
Reply from 10.2.67.106: bytes=32 time=3ms TTL=127

Ping statistics for 10.2.67.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\Redes>
```

Figure 79. Ping from the Computer (PC0 in the Diagram) to a Laboratory Device (PC3 in the Diagram)

```
C:\Users\Redes>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=3ms TTL=115
Reply from 8.8.8.8: bytes=32 time=3ms TTL=115
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=4ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms

C:\Users\Redes>
```

Figure 80. Ping to Internet Devices (Google DNS)

```
C:\Users\Redes>ping google.com

Pinging google.com [142.251.132.78] with 32 bytes of data:
Reply from 142.251.132.78: bytes=32 time=4ms TTL=114
Reply from 142.251.132.78: bytes=32 time=4ms TTL=114
Reply from 142.251.132.78: bytes=32 time=4ms TTL=114
Reply from 142.251.132.78: bytes=32 time=4ms TTL=114

Ping statistics for 142.251.132.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\Redes>
```

Figure 81. Ping to Internet Devices (google.com)

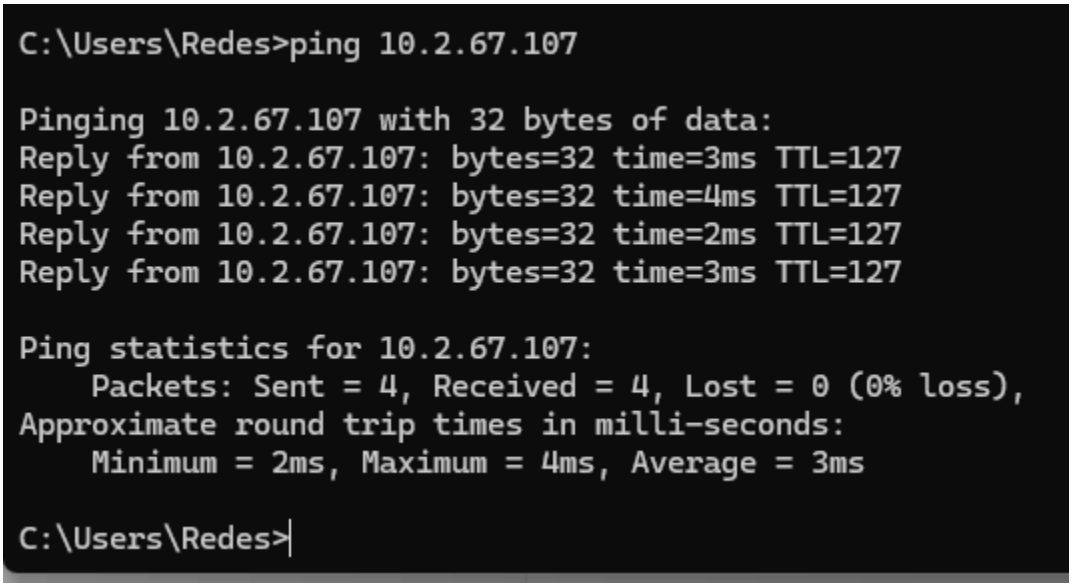


Figure 82. Ping from the Computer (PC0 in the Diagram) to another Laboratory Device

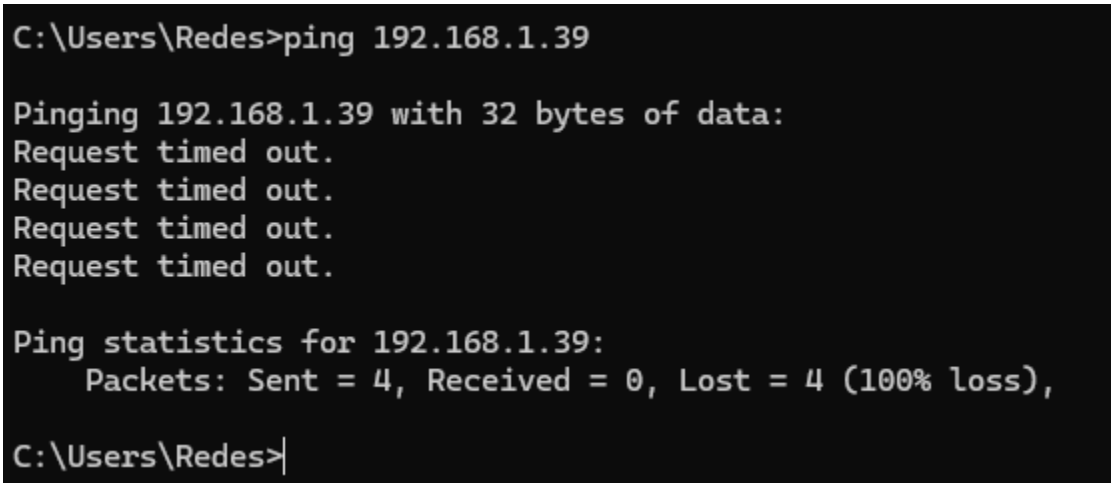


Figure 83. Ping to a Device on Another Network

NAT: Some devices did not respond to ping due to the lack of NAT configuration. This allows devices within a private network (LAN) to communicate with devices on the Internet using a single public IP address assigned to the router

- We use WiFi Analyzer to capture the traffic of nearby Wi-Fi networks. We can observe our wireless network and the university's networks

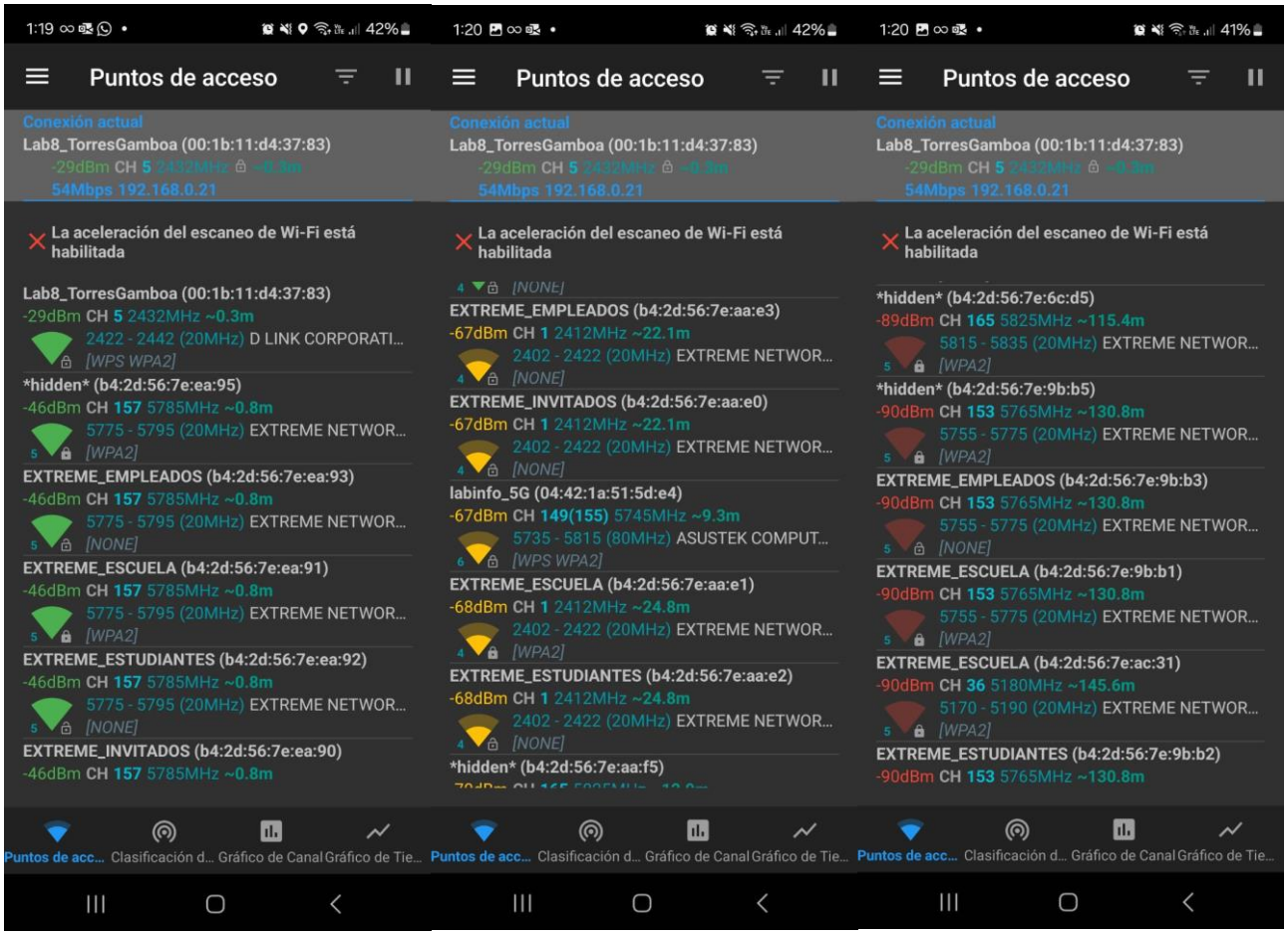


Figure 84. Obtaining Wireless Traffic from Active Networks Nearby Using Wi-Fi Analyzer

- By clicking on our network, we can observe detailed information such as the bandwidth (2.4 GHz), the channel we configured earlier (channel 5), and the signal strength (-29 dBm)

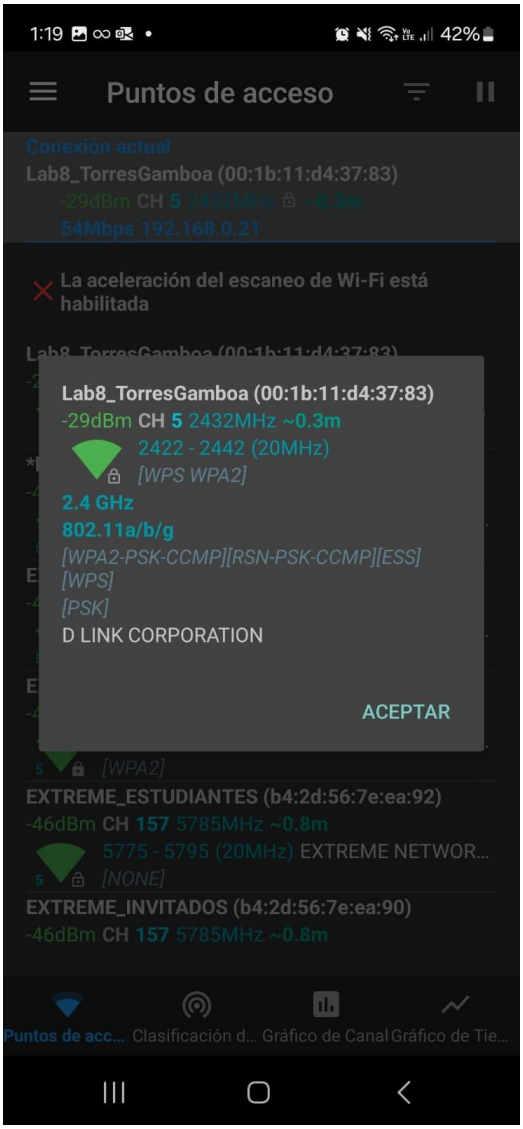


Figure 85. Information from the Wireless Network Capture

- If we look at the channel graph, we can see the networks using the same channel and their signal strength

Figure 86. Information on Router Channels

7.3. disabling the beacon frame

- To disable the Beacon Frame, we go to Wireless Setup and disable the option 'Enable Hidden Wireless (Also called the SSID Broadcast)' and save

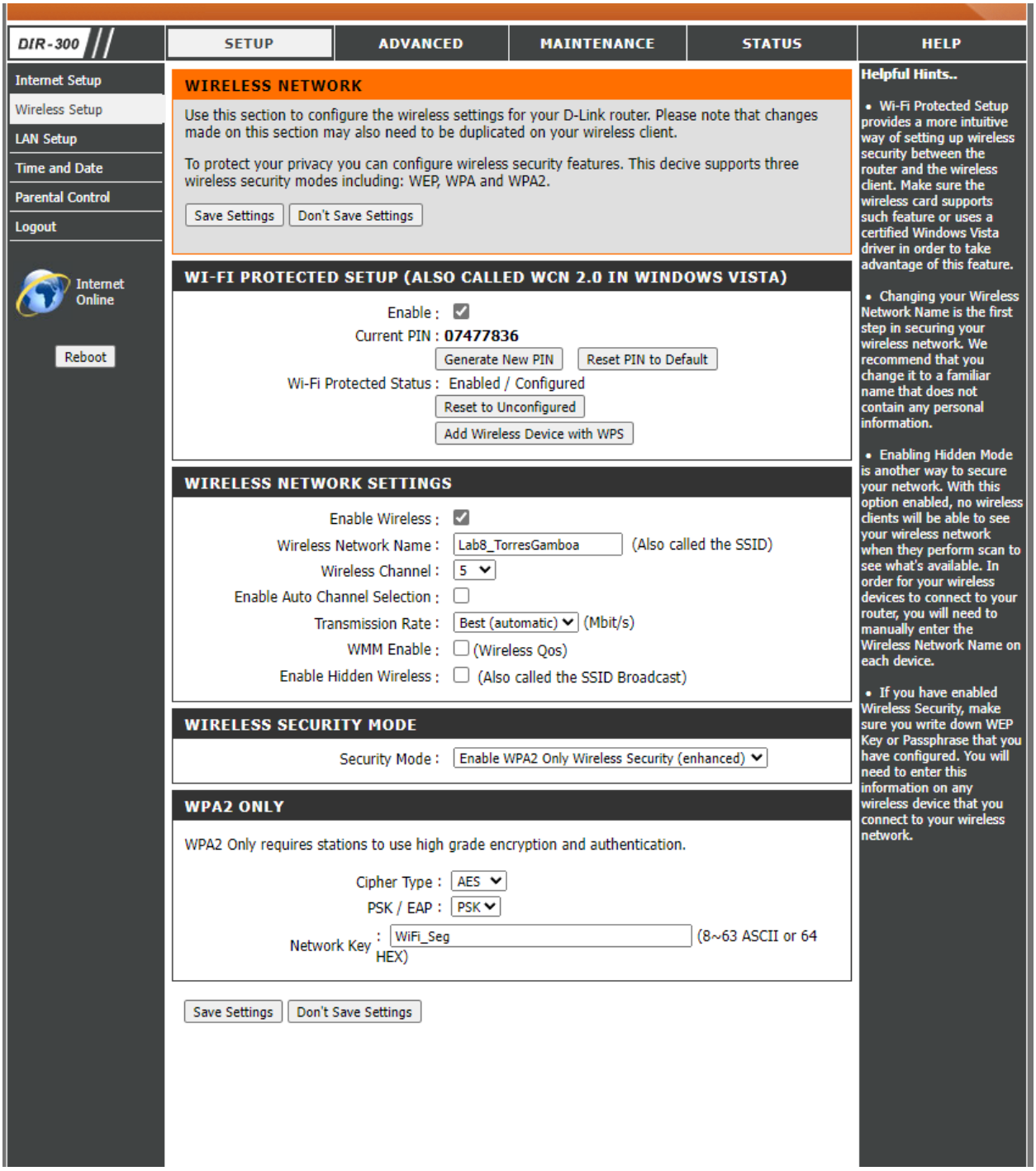


Figure 87. disabling the beacon frame

- If we open WiFi Analyzer, we can see that the network no longer appears. The Beacon Frame allows the network to be visible to nearby devices. When disabled, it remains hidden, and to connect to it, it is essential to know the SSID, security mechanism, and channel

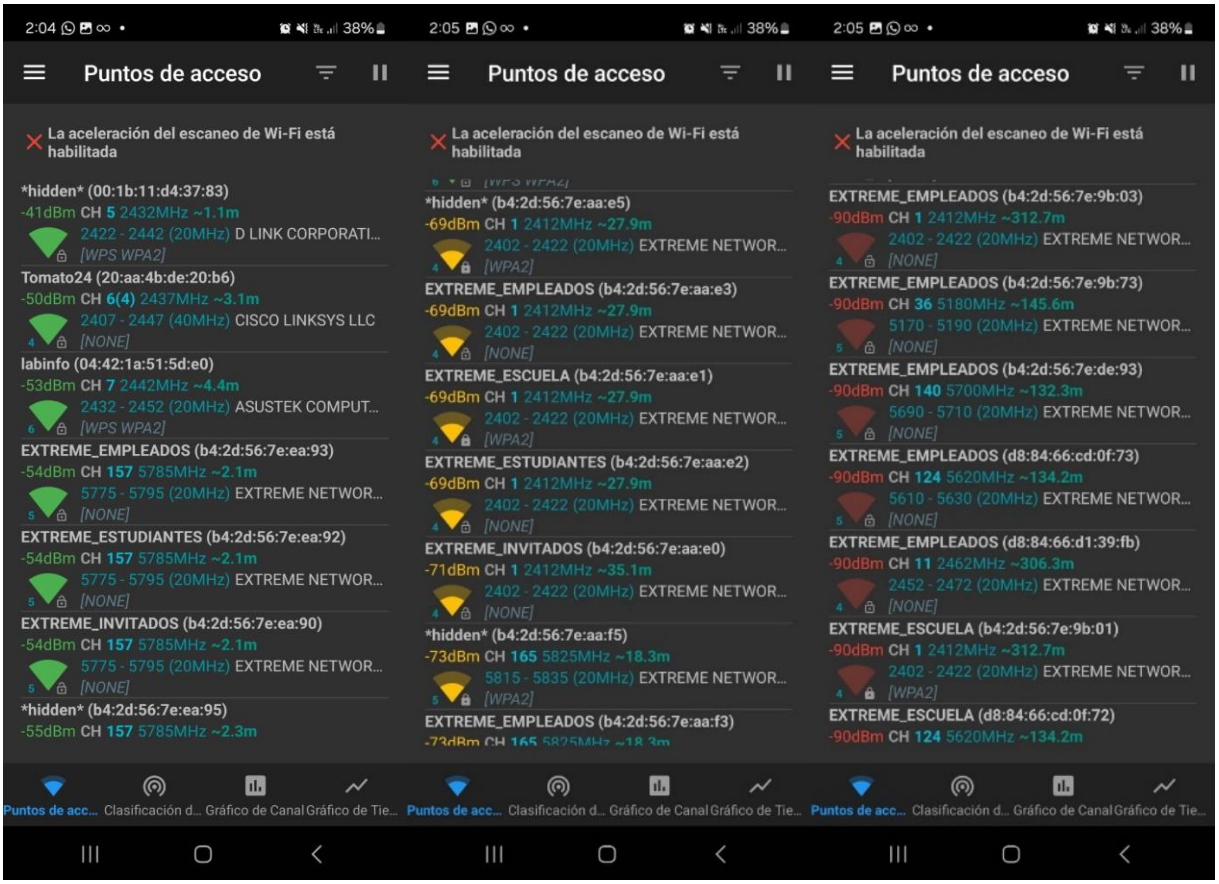


Figure 88. Verifying the Wireless Network with Beacon Frame Disabled in WiFi Analyzer

8. Reviewing WiFi Networks Near Your Home

- When we open WiFi Analyzer, we can see the different nearby wireless networks, as well as detailed information about each one. Networks marked in green indicate those that are closest, while the ones in red are the farthest.

  We can observe networks with 2.4 GHz and 5 GHz bands. The difference between them lies in speed. The 2.4 GHz band has a longer range but transmits data at slower speeds, while the 5 GHz band has a shorter range but transmits at faster speeds.

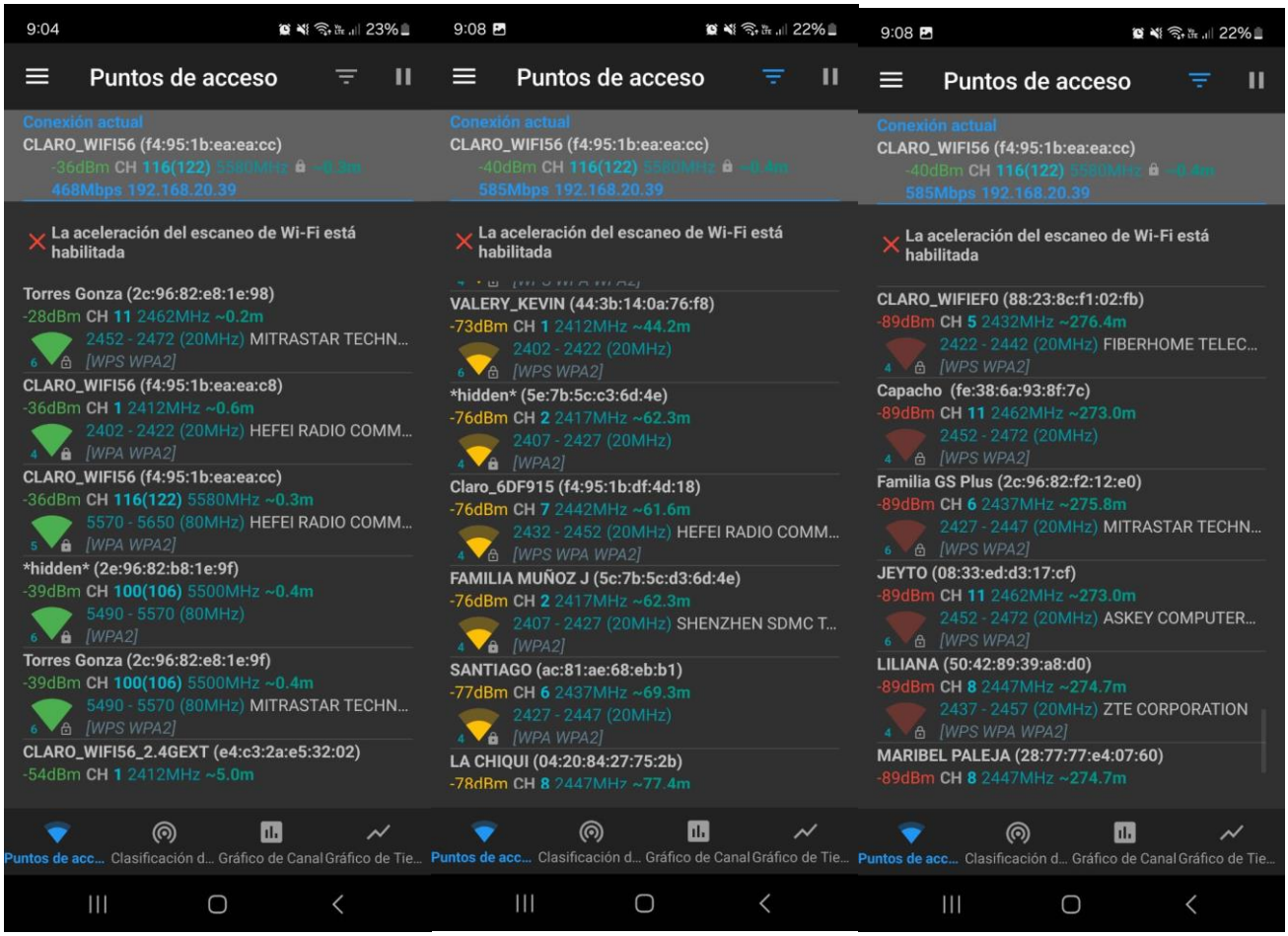


Figure 89. Obtaining Wireless Traffic from Active Networks Near the House with Wi-Fi Analyzer

- When detailing the network being used, we observe that it has a 5 GHz band and a signal strength of -36 dBm, which means it is a fast and strong connection with good signal quality near the access point

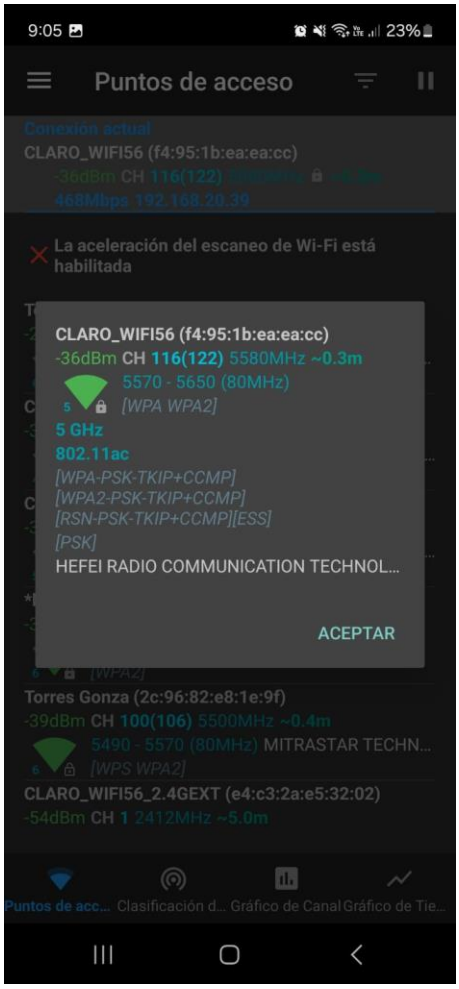


Figure 90. Information from the Wireless Network Capture of the house

- If we look at the channel graph, we can observe that there are many networks using the same channel and

their signal strength

Figure 91. Information on Router Channels and Time Graph

Base Software Installation

As we have seen, part of the foundational platform of an organization is the web server. This server can be static, as we have defined it so far, or dynamic, which allows pages to be built at the moment they are needed. This functionality is useful for applications that, for example, query data stored in databases or the file system directly, perform calculations based on user-provided data, among other tasks.

1. Dynamic Web Service

1.1. Deploying an application on Apache (Solaris)

- Since PHP is already installed in Solaris, we open the file for Apache httpd configuration

```
root@solaris:~# nano /etc/apache2/2.4/httpd.conf
```

Figure 92. Opening httpd.conf file

- We add the following lines to the file so that Apache can read .php files:
  LoadModule php5_module libexec/libphp5.so
  AddType application/x-hhtpd-php .php

```
<IfModule mpm_prefork_module>
<IfDefine prefork>
        LoadModule cgi_module libexec/mod_cgi.so
</IfDefine>
</IfModule>
#LoadModule dav_fs_module libexec/mod_dav_fs.so
#LoadModule dav_lock_module libexec/mod_dav_lock.so
#LoadModule vhost_alias_module libexec/mod_vhost_alias.so
#LoadModule negotiation_module libexec/mod_negotiation.so
LoadModule dir_module libexec/mod_dir.so
#LoadModule actions_module libexec/mod_actions.so
#LoadModule speling_module libexec/mod_speling.so
#LoadModule userdir_module libexec/mod_userdir.so
LoadModule alias_module libexec/mod_alias.so
#LoadModule rewrite_module libexec/mod_rewrite.so
LoadModule php5_module libexec/libphp5.so
<IfModule unixd_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User webservd
Group webservd

</IfModule>
^G Ver ayuda ^O Guardar   ^W
^X Salir     ^R Leer fich.^\ Reemplazar^U Pegar txt ^T OrtografÃ-a^_ Ir a lÃ-nea
```

Figure 93. Adding 'LoadModule php5_module libexec/libphp5.so' into httpd.conf

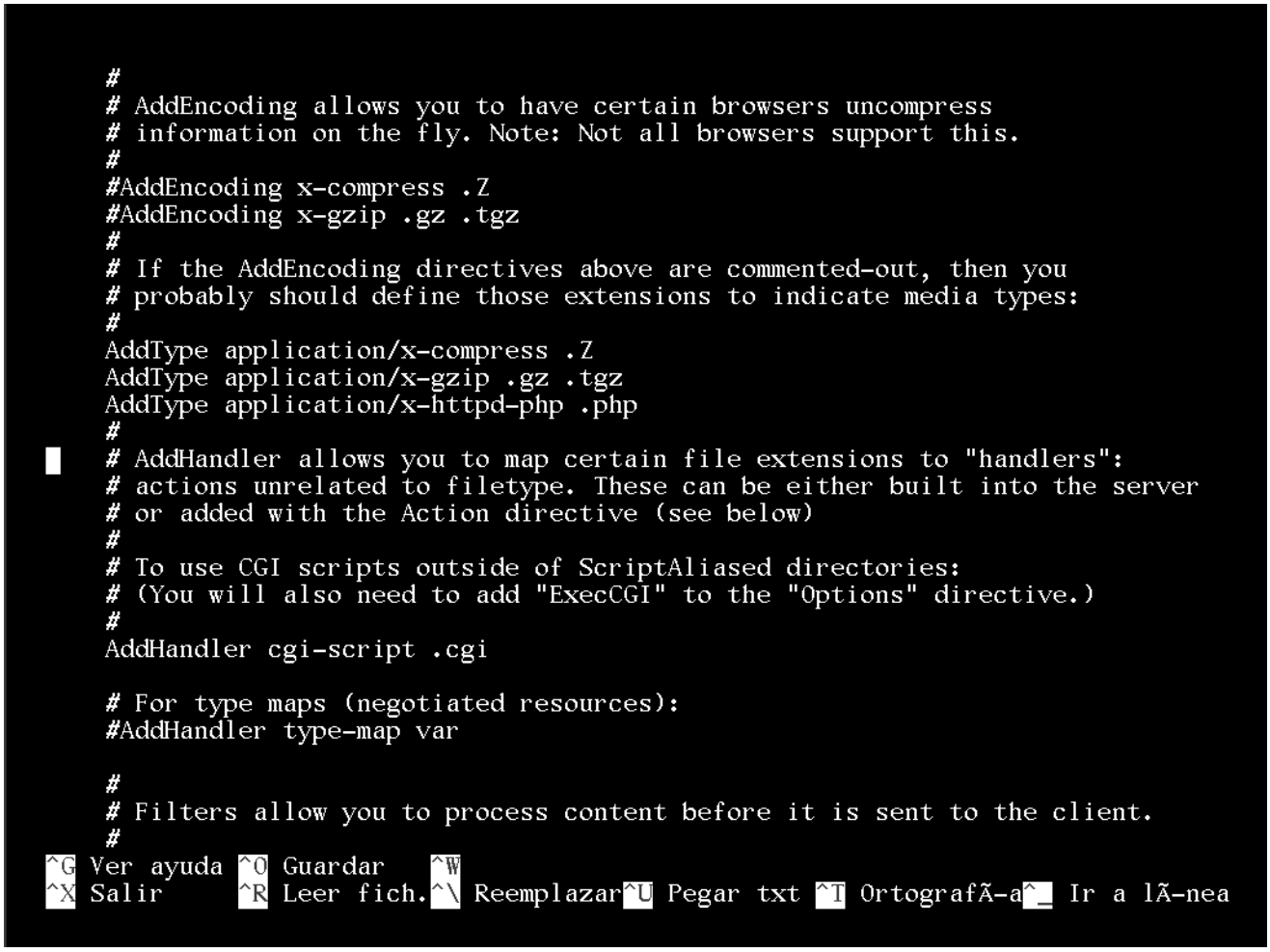


Figure 94. Adding 'AddType application/x-hhtpd-php .php' into httpd.conf

- We add the path where the index.php of our calculator will be located. In this case, it will be **/var/apache2/2.4/htdocs/calculadora**, along with the configuration shown below:

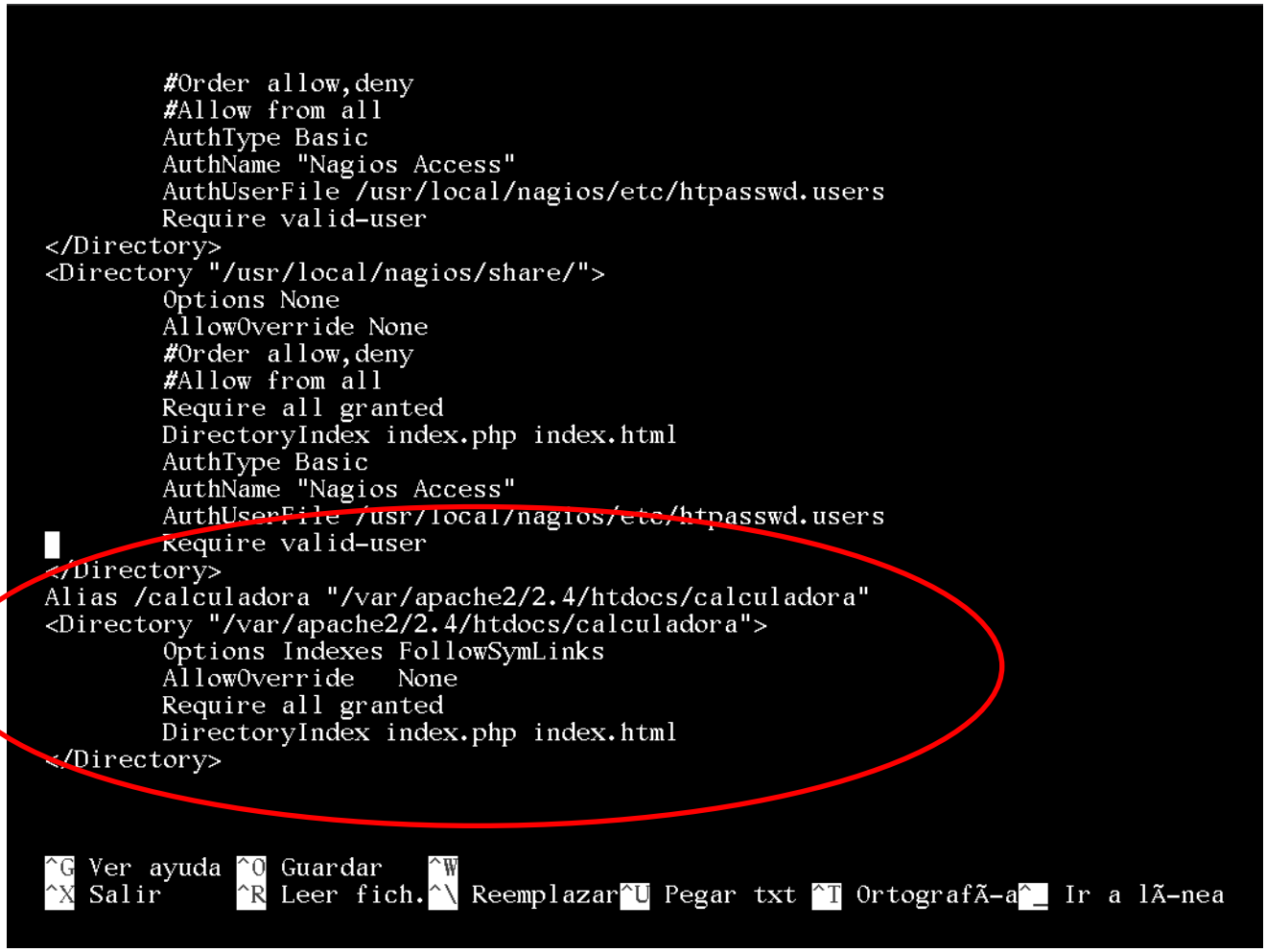


Figure 95. Configuring the location of index.php in the httpd.conf file

- We create the directory specified in the httpd.conf configuration file and then create the index.php file

```
root@solaris:~# mkdir /var/apache2/2.4/htdocs/calculadora
```

Figure 96. Creating the /calculator directory

```
root@solaris:~# cd /var/apache2/2.4/htdocs/calculadora
root@solaris:/var/apache2/2.4/htdocs/calculadora# ls
index.php
root@solaris:/var/apache2/2.4/htdocs/calculadora#
```

Figure 97. Creating index.php file

- We create the calculator and restart Apache using the command **svcadm restart apache24** and **svcadm enable apache24**

```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Calculadora de Notas</title>
    <style>
        body { font-family: Arial, sans-serif; max-width: 600px; margin: auto; $
        form { display: flex; flex-direction: column; gap: 10px; }
        label { font-weight: bold; }
        input[type="text"], input[type="number"] { padding: 8px; width: 100%; }
        button { padding: 10px; background-color: #007bff; color: white; border$
        .result { background-color: #f0f0f0; padding: 10px; border-radius: 5px;$
    </style>
</head>
<body>
    <h1>Calculadora de Notas del Semestre</h1>
    <form method="POST">
        <label for="nombre">Nombre del Estudiante:</label>
        <input type="text" id="nombre" name="nombre" required>

        <label for="tercio1">Nota Primer Tercio (30%):</label>
        <input type="number" id="tercio1" name="tercio1" min="0" max="100" step$

        <label for="tercio2">Nota Segundo Tercio (30%):</label>
        <input type="number" id="tercio2" name="tercio2" min="0" max="100" step$

        <label for="tercio3">Nota Tercer Tercio (40%):</label>
        <input type="number" id="tercio3" name="tercio3" min="0" max="100" step$
^G Ver ayuda ^O Guardar   ^W Buscar    ^K Cortar txt^J Justificar^C PosiciÃ³n
^X Salir     ^R Leer fich.^\ Reemplazar^U Pegar txt ^T OrtografÃ-a^_ Ir a lÃ-nea
```

Figure 98. Calculator program

```
root@solaris:~# svcadm restart apache24
root@solaris:~# svcadm enable apache24
root@solaris:~#
```

Figure 99. Restarting Apache on Solaris

- We open the browser and enter the IP address of Solaris along with the path where the index.php is stored

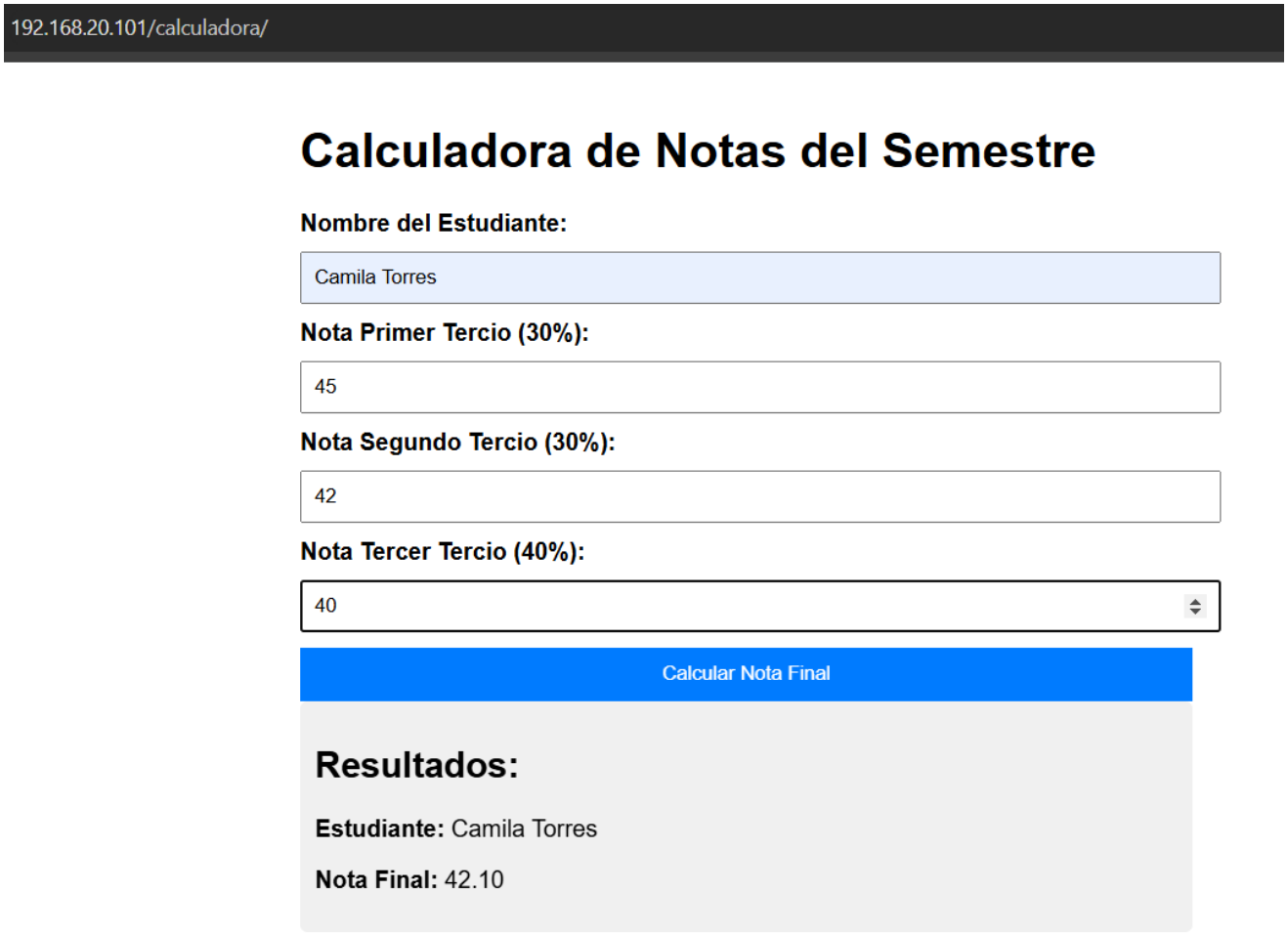


Figure 100. Calculator application on Solaris

1.2. Deploying an application on IIS (Windows Server)

- From the official PHP website, we download version 8.4.1, and once it is downloaded, we extract it. In our case, we extract it to the directory C:\PHP

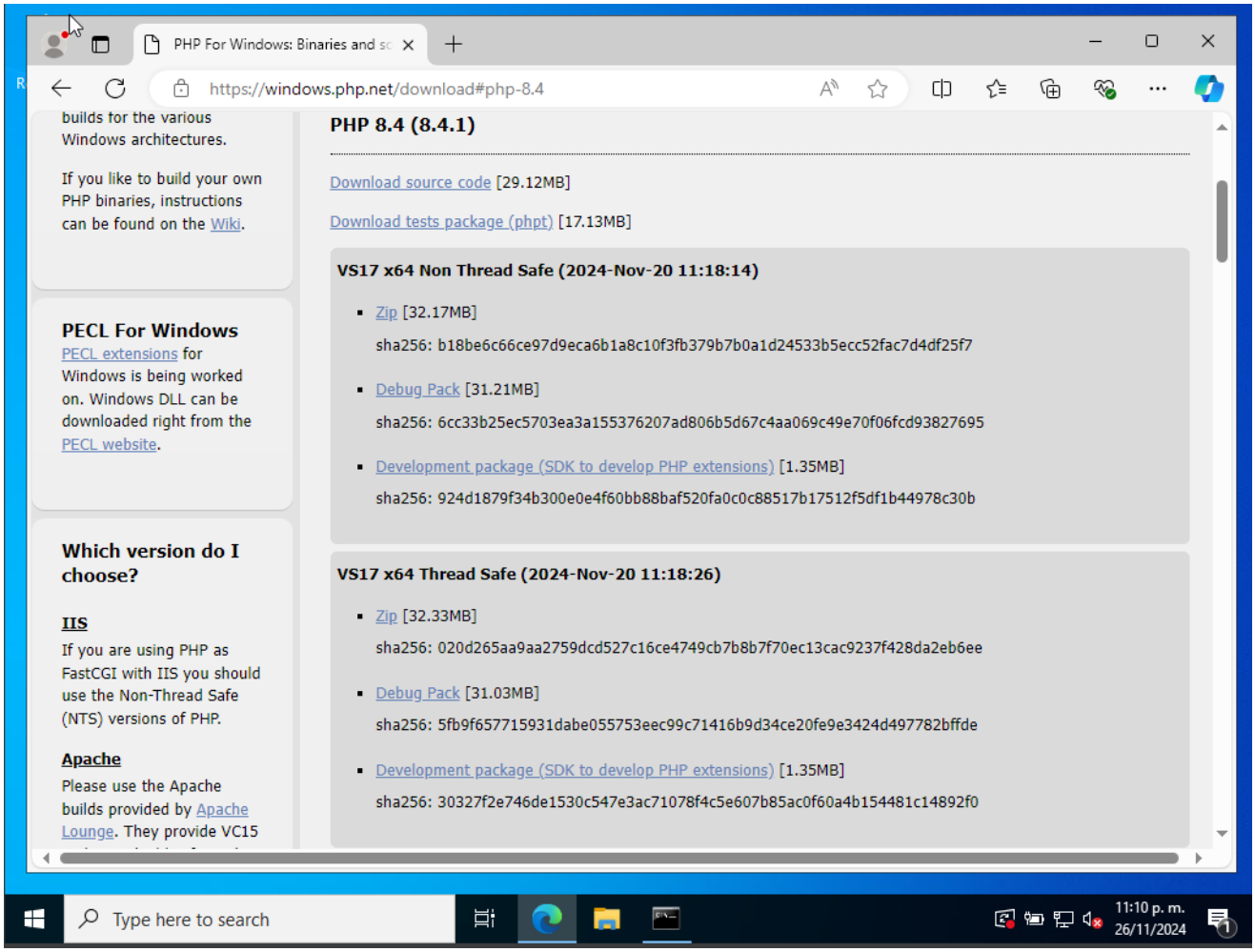


Figure 101. Downloading PHP 8.4.1

- We open Control Panel > System > Advanced system settings > Environment Variables

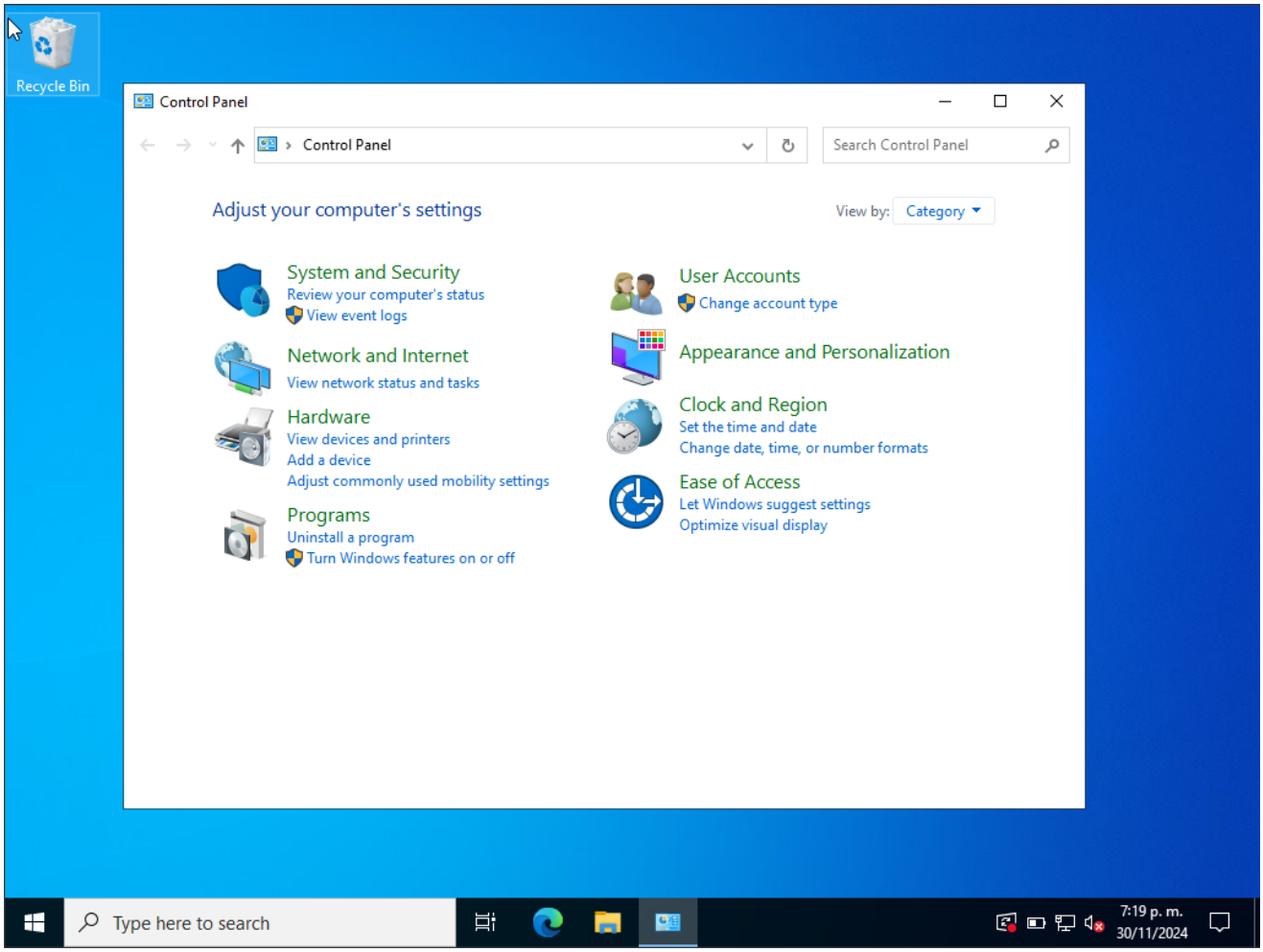


Figure 102. Control Panel in Windows Server

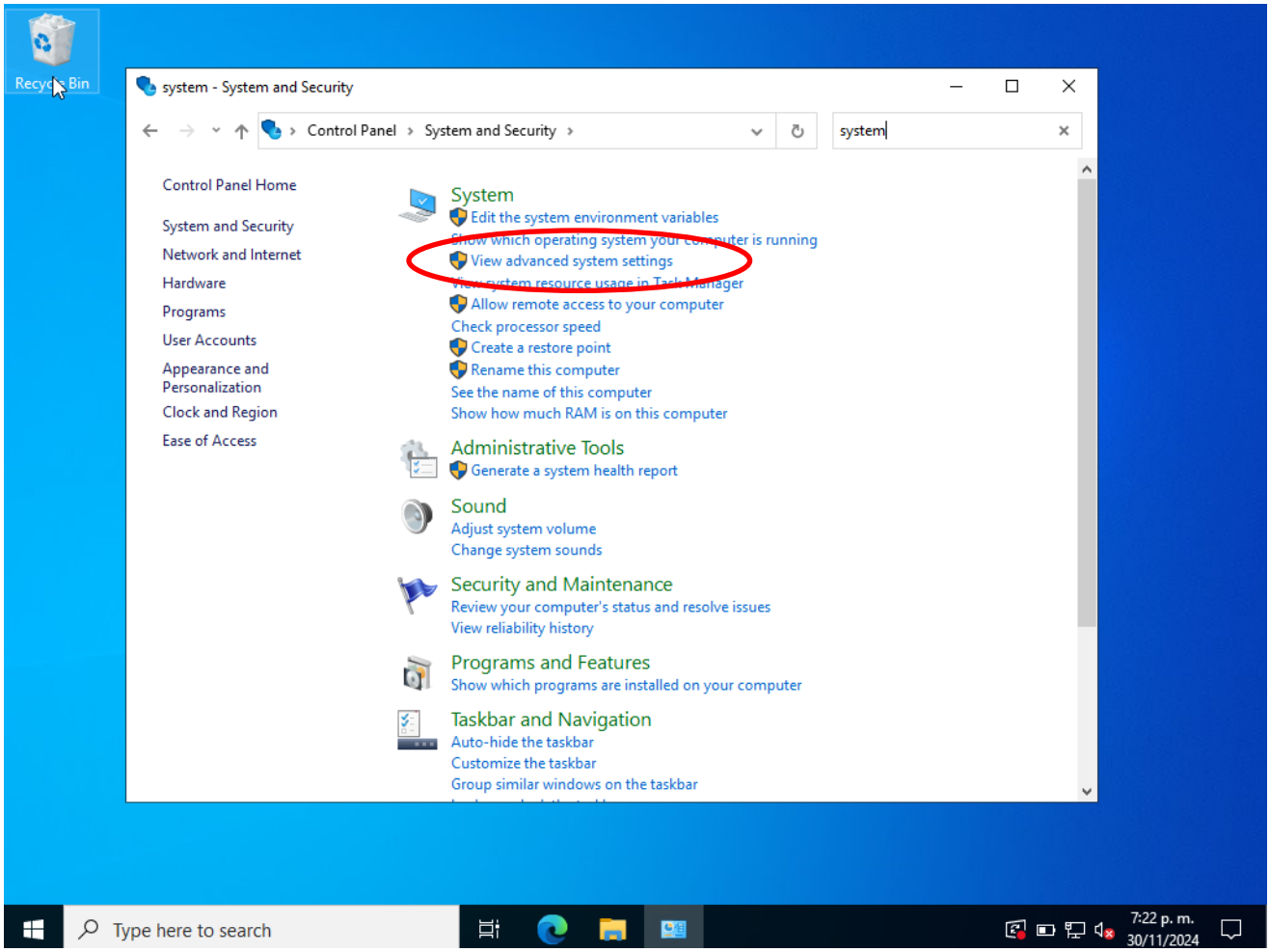


Figure 103. System Settings

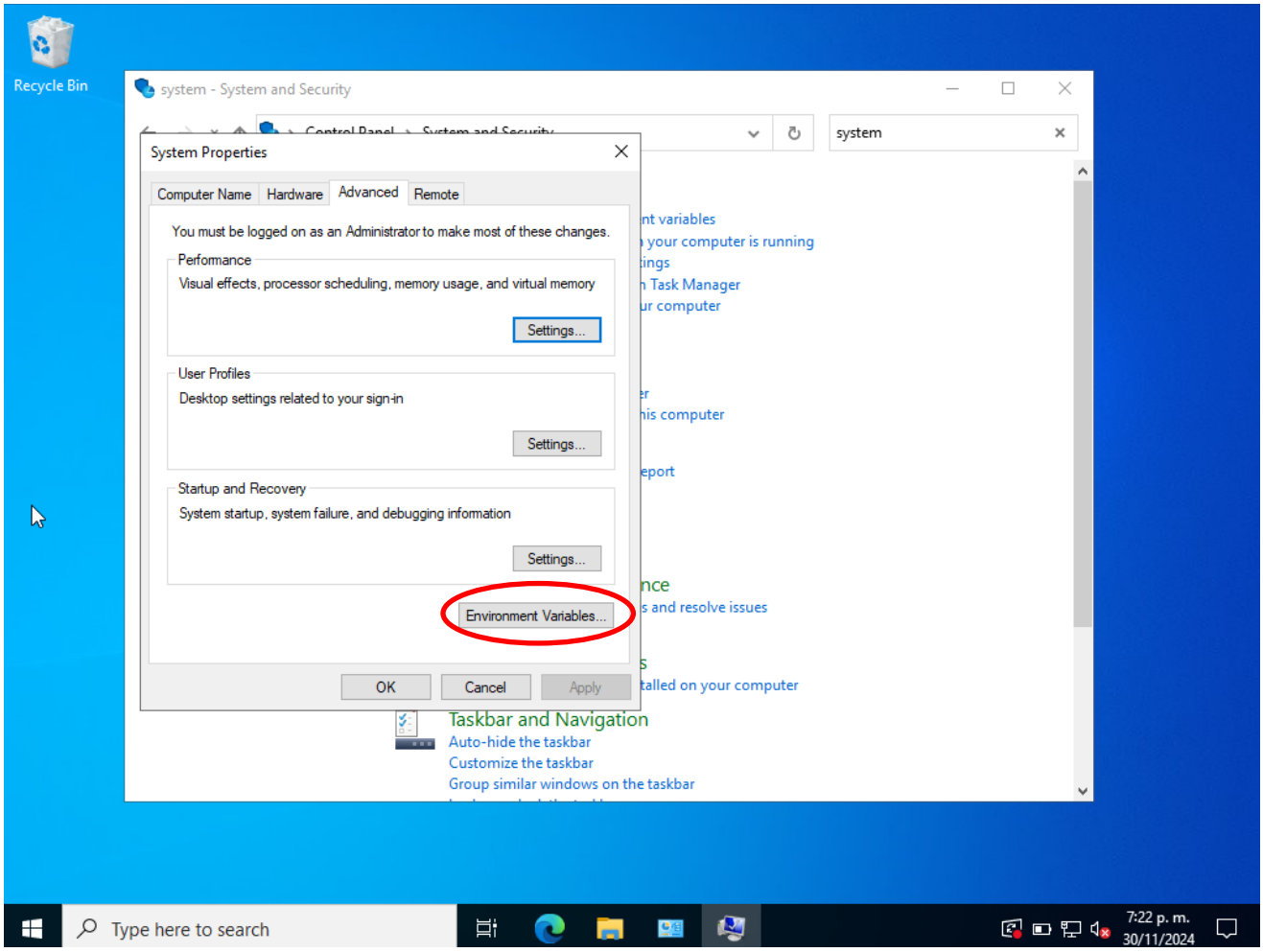


Figure 104. Opening Environment Variables in Windows Server

- In "System variables," we edit the Path variable and add the path where we extracted PHP

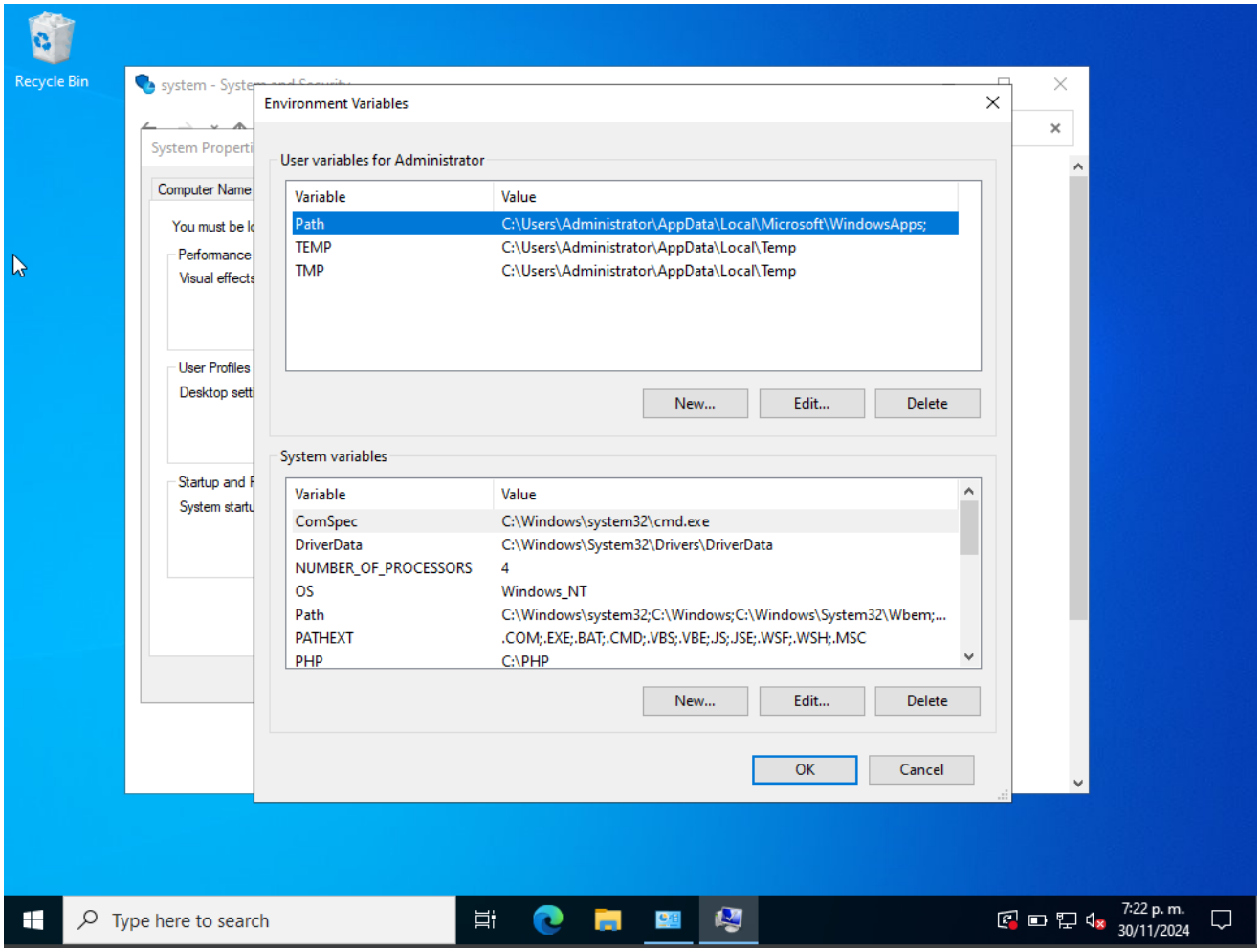


Figure 105. Editing System Variables

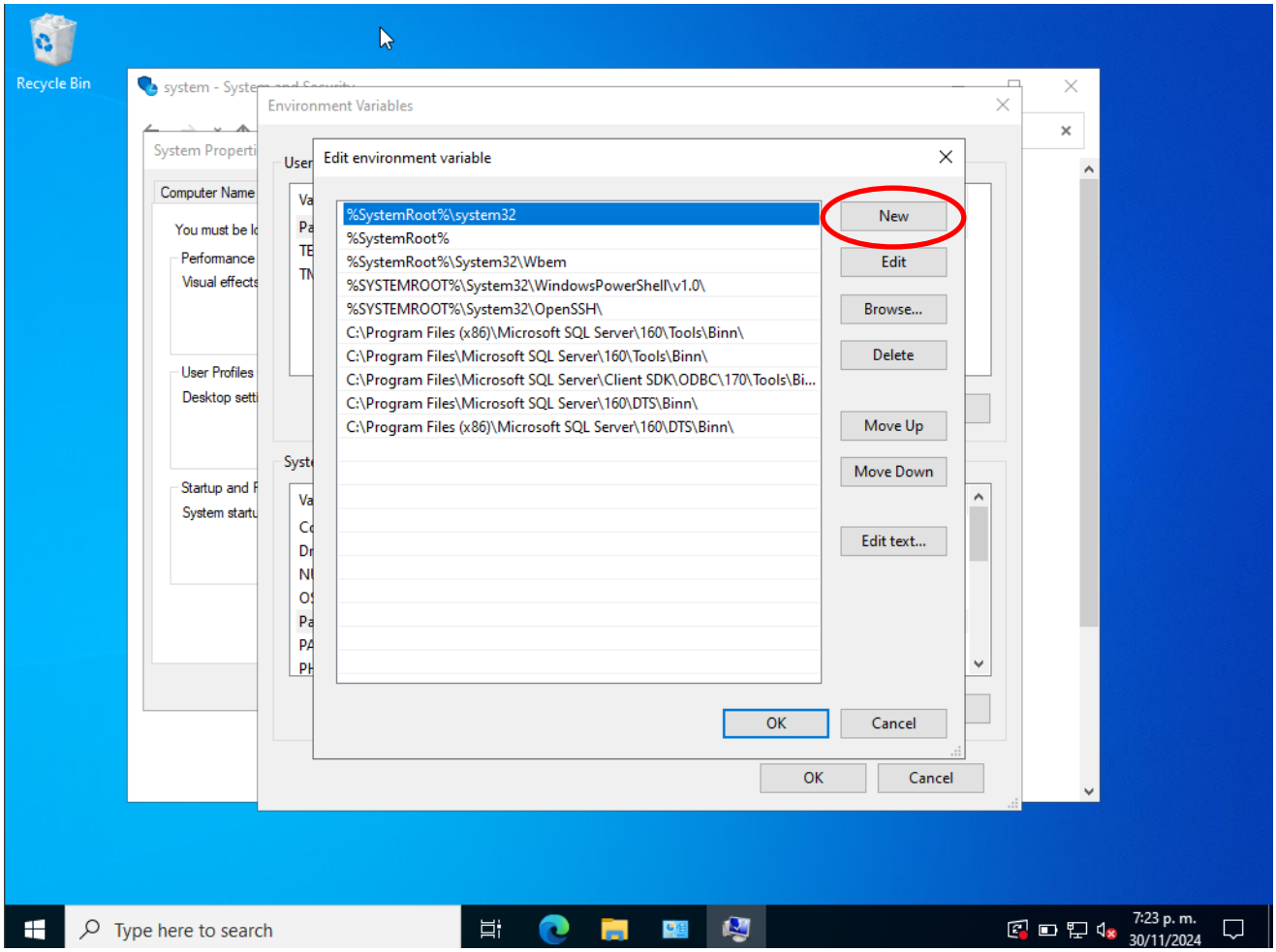


Figure 106. Adding a new path

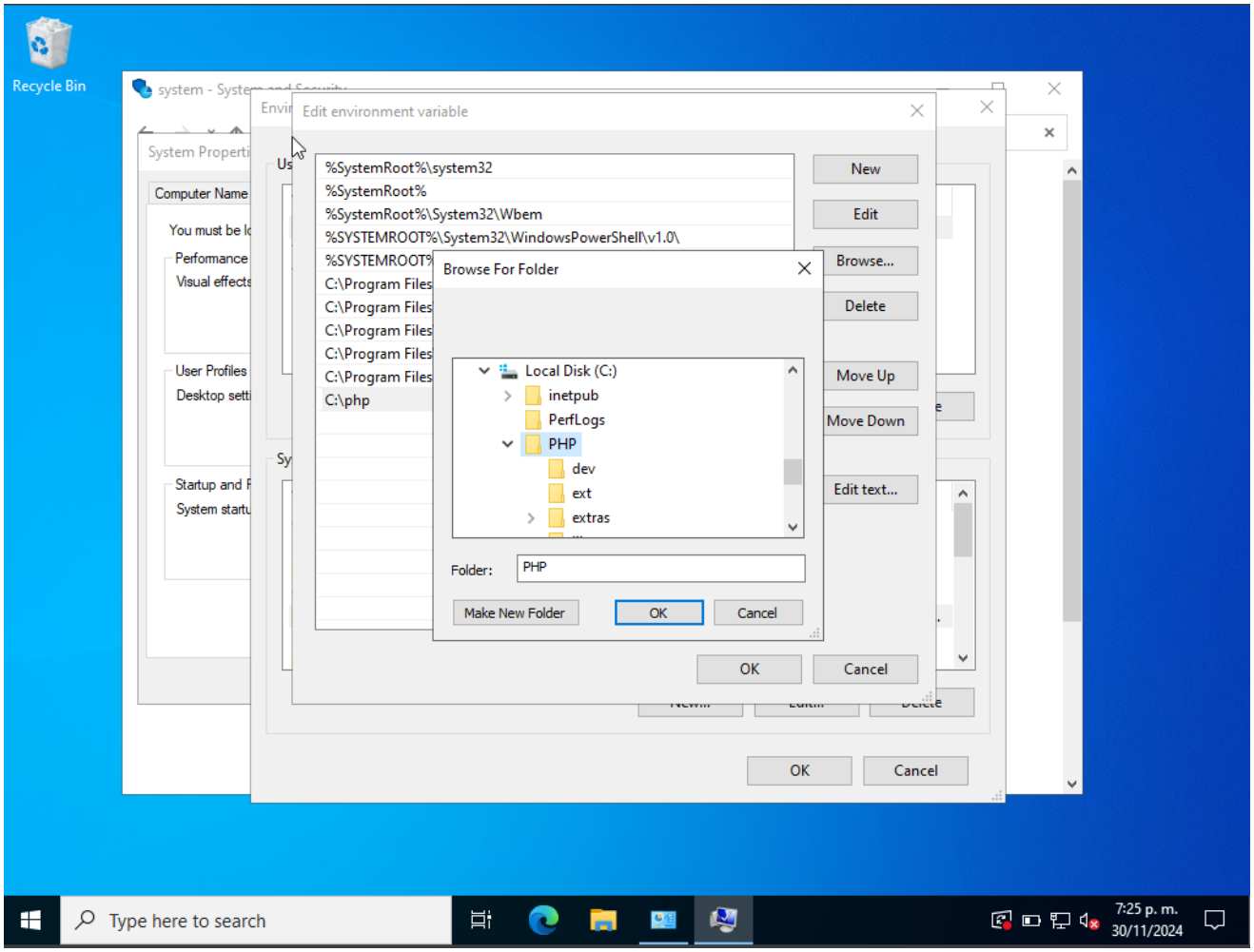


Figure 107. Adding the PHP path in the environment variable configuration

- Inside the PHP folder, we look for a file called php.ini and uncomment the following lines
  cgi.force_redirect = 0
  extension_dir = "ext"
  extension=curl
  extension=mbstring
  extension=mysqli

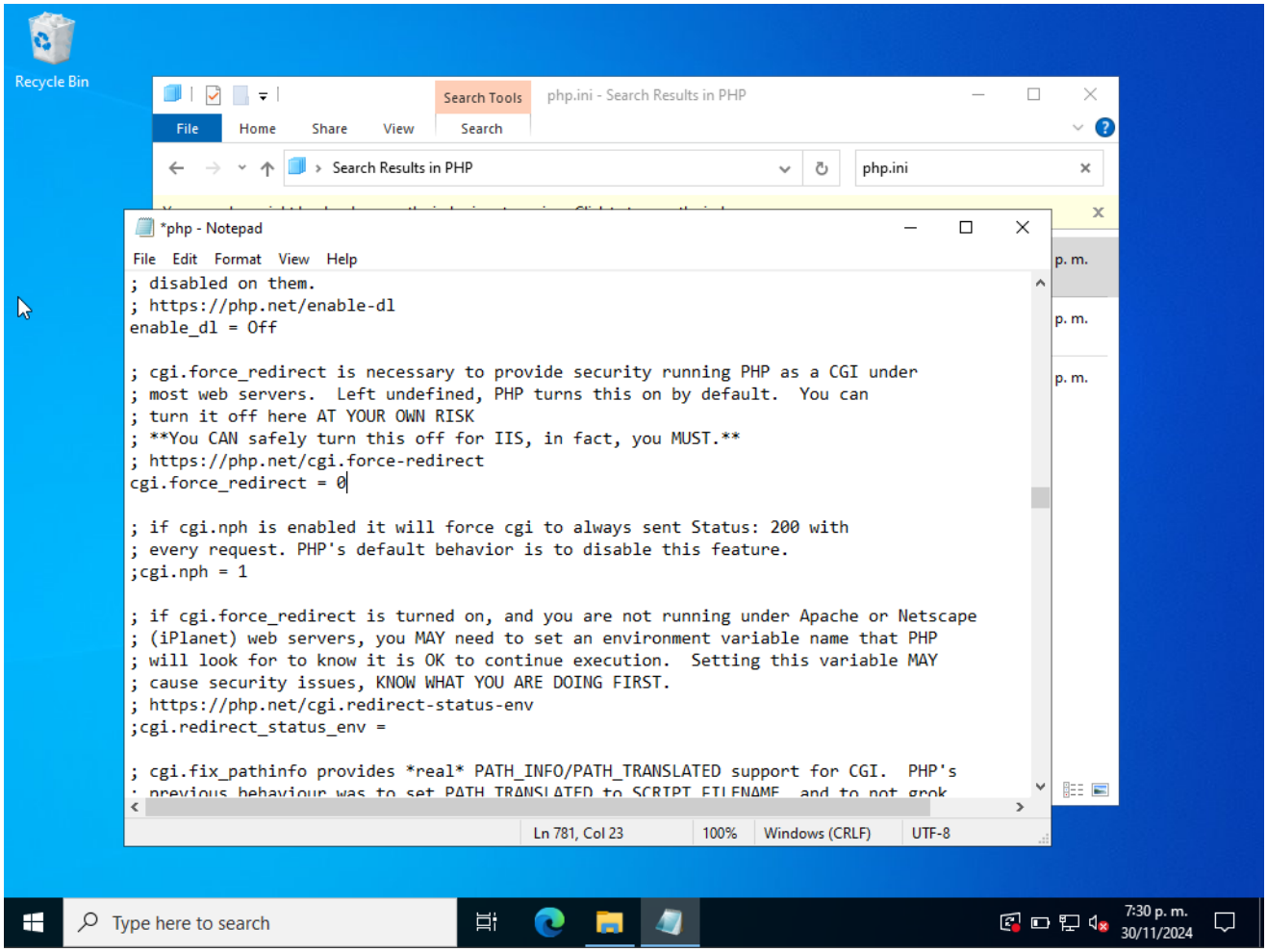


Figure 108. Editing the php.ini file

- To make IIS read CGI files, we go to **IIS Manager** and then to **Handler Mapping**

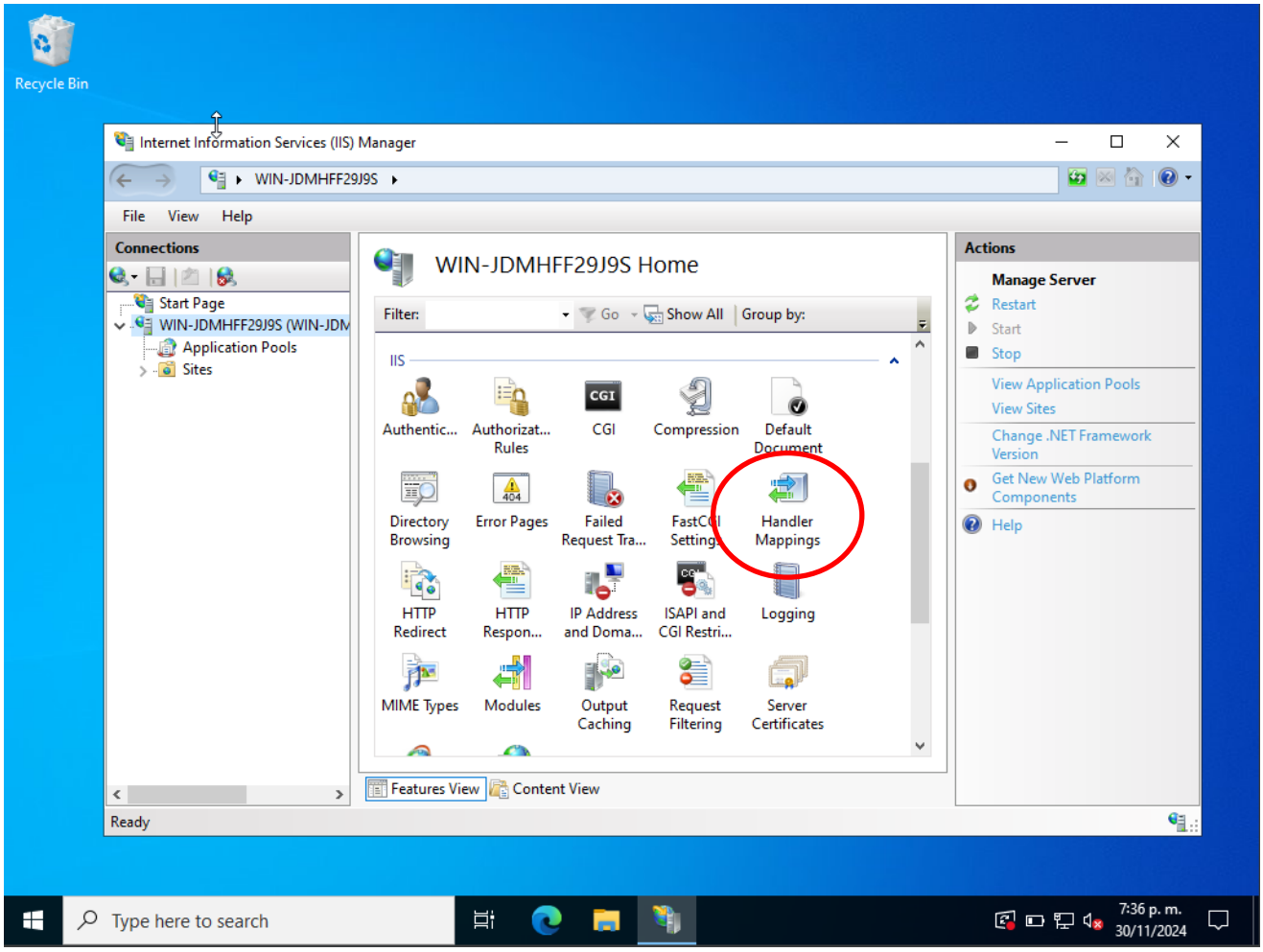


Figure 109. IIS Manager Menu

- Click on **Add Script Map**

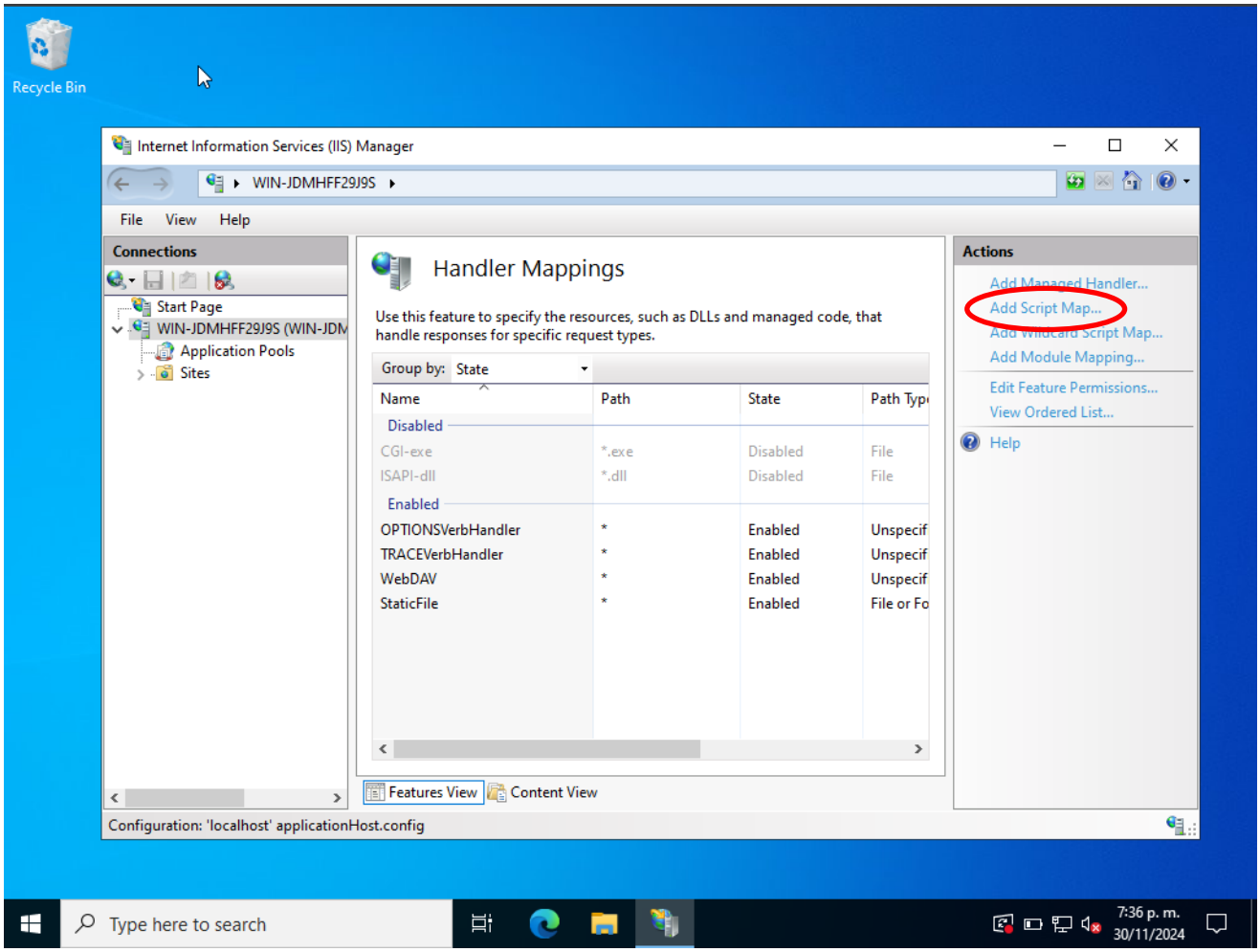


Figure 110. Handler Mappings Section

- We configure the following:

  Request Path: *.php

  Module: FastCGIModule

  Executable Path: C:\PHP\php-cgi.exe

  Name: PHP_via_FastCGI

Finally, we click OK

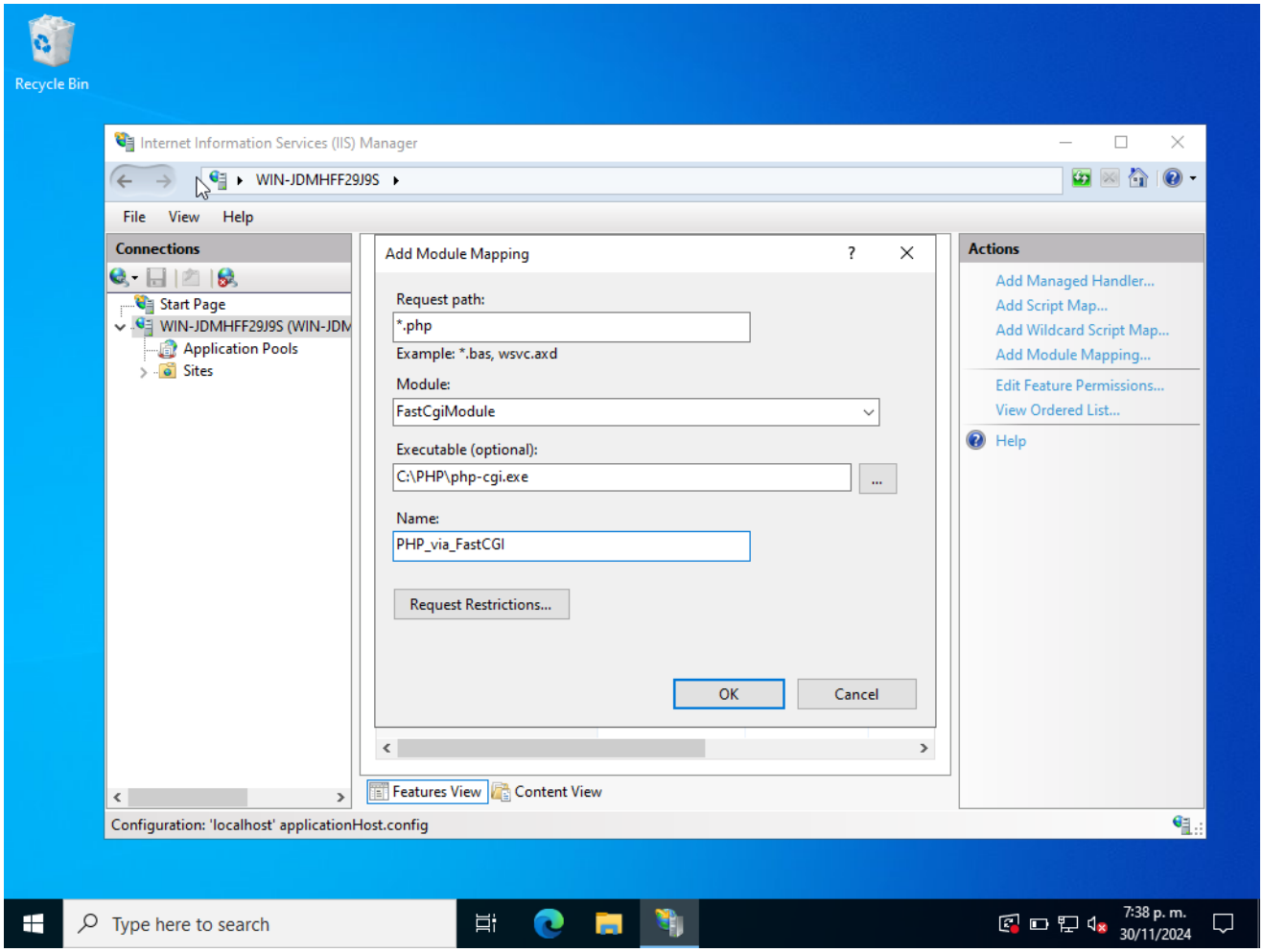


Figure 111. Configuring Module Mapping for PHP

- Now, we go to **FastCGI Settings**

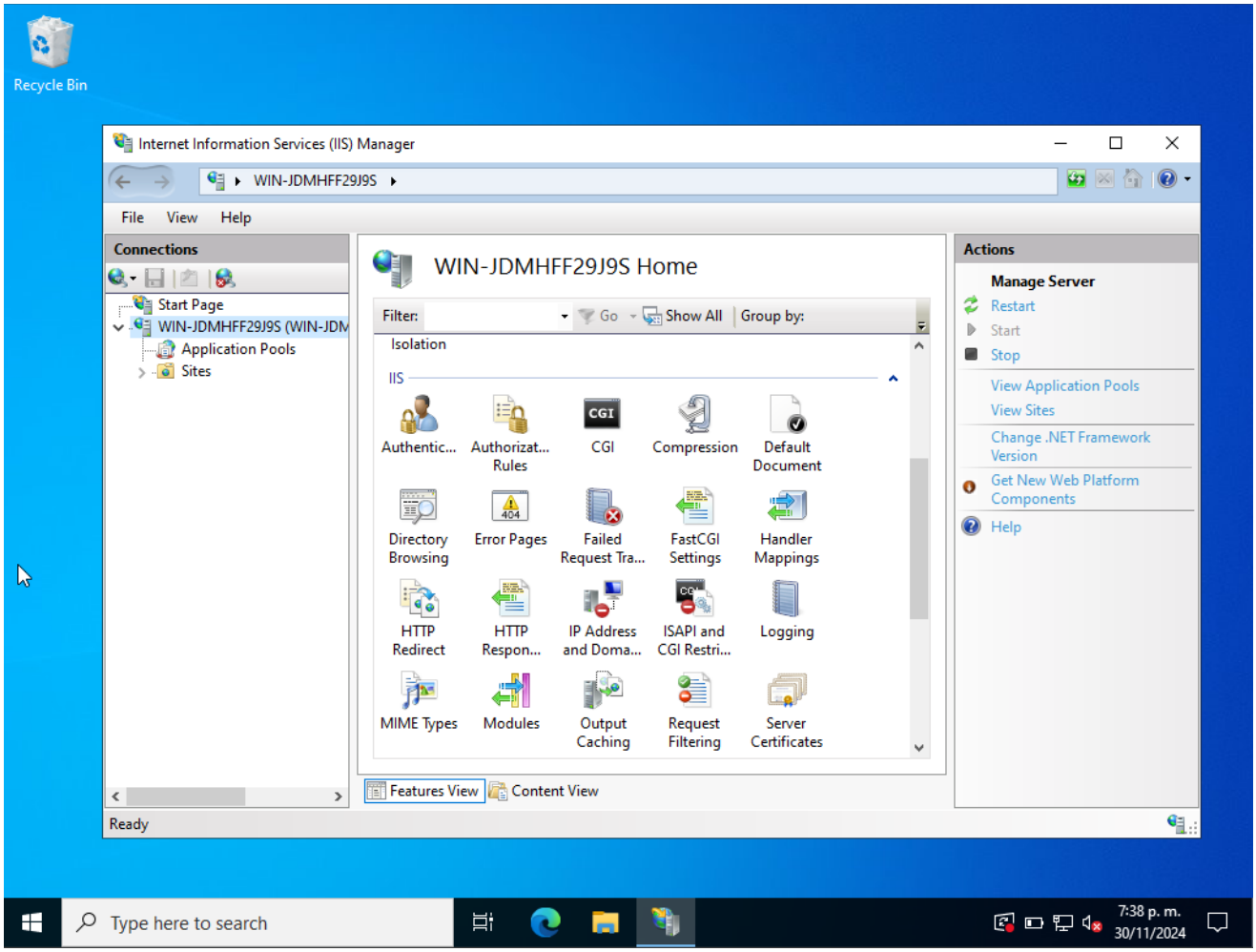


Figure 112. Navigating to FastCGI Settings

- We click on Add Application and add the following:
  - Executable Path: **C:\PHP\php-cgi.exe**
  - Additional Configuration**: We leave it as default and save.**

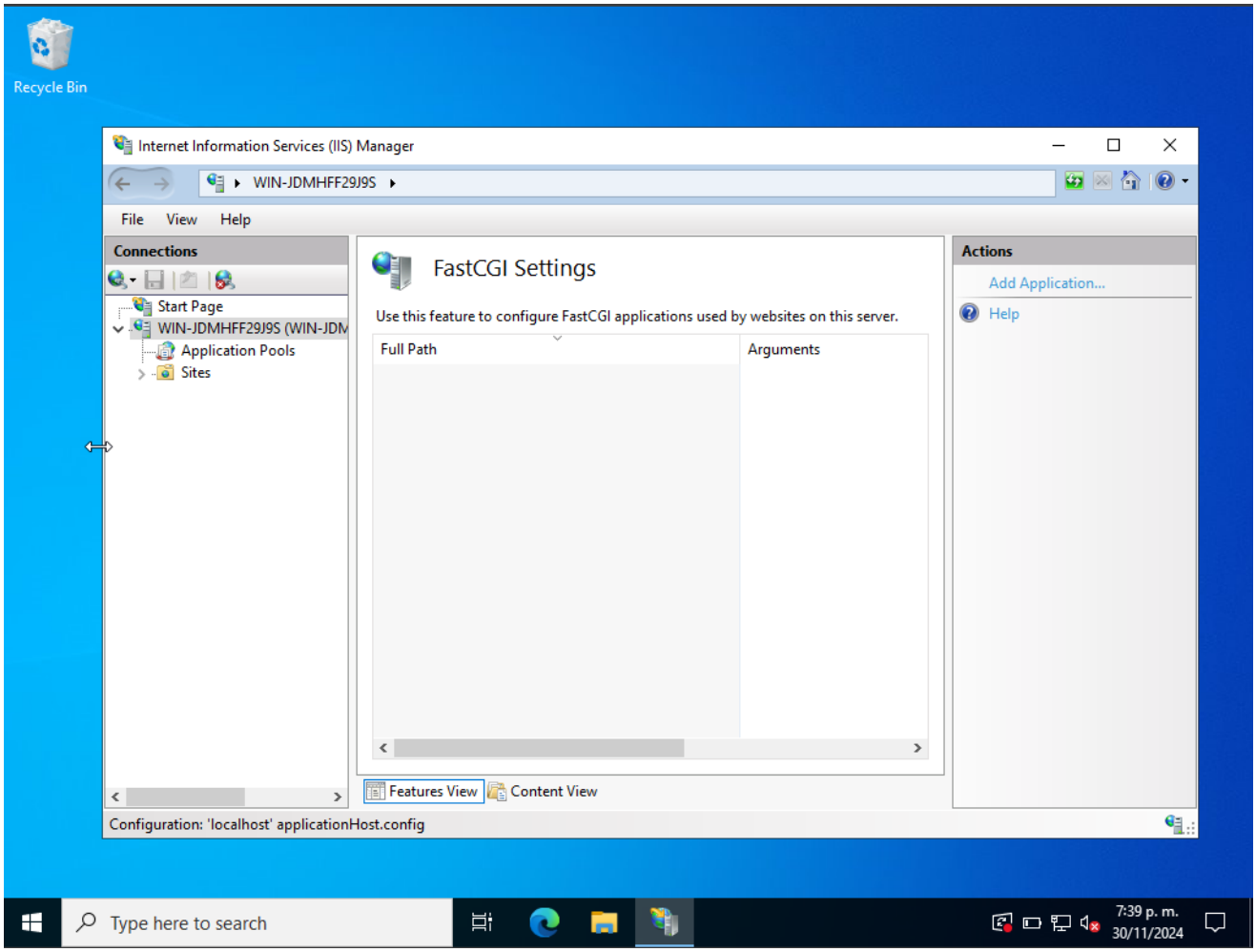


Figure 113. FastCGI Settings section

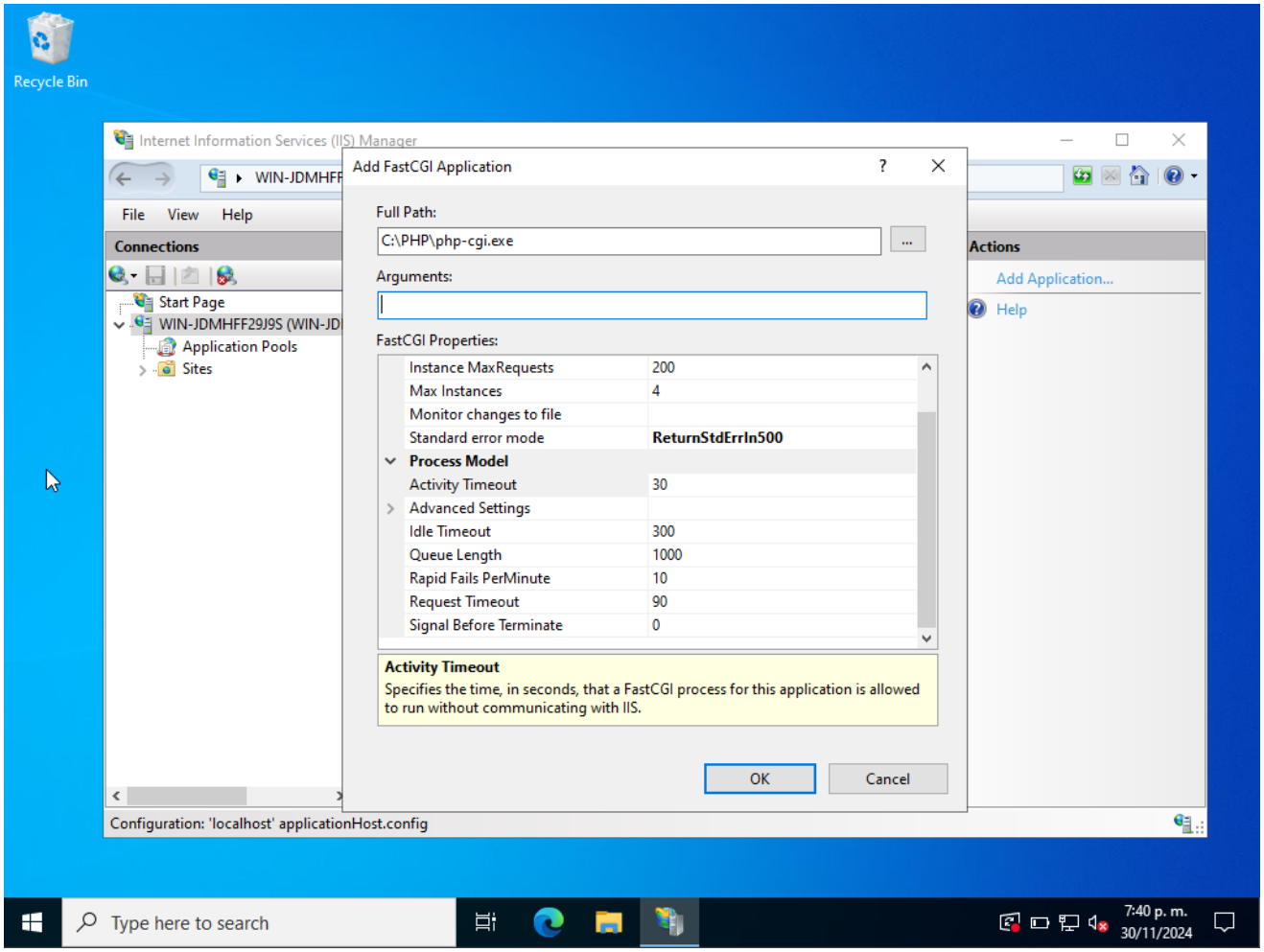


Figure 114. Adding FastCGI Application

- We create an index.php file (the same that we created in Solaris) in the root folder of the site (C:\inetpub\wwwroot) and verify that the IIS user (IIS_IUSR) has read and execute permissions. Then, we save it

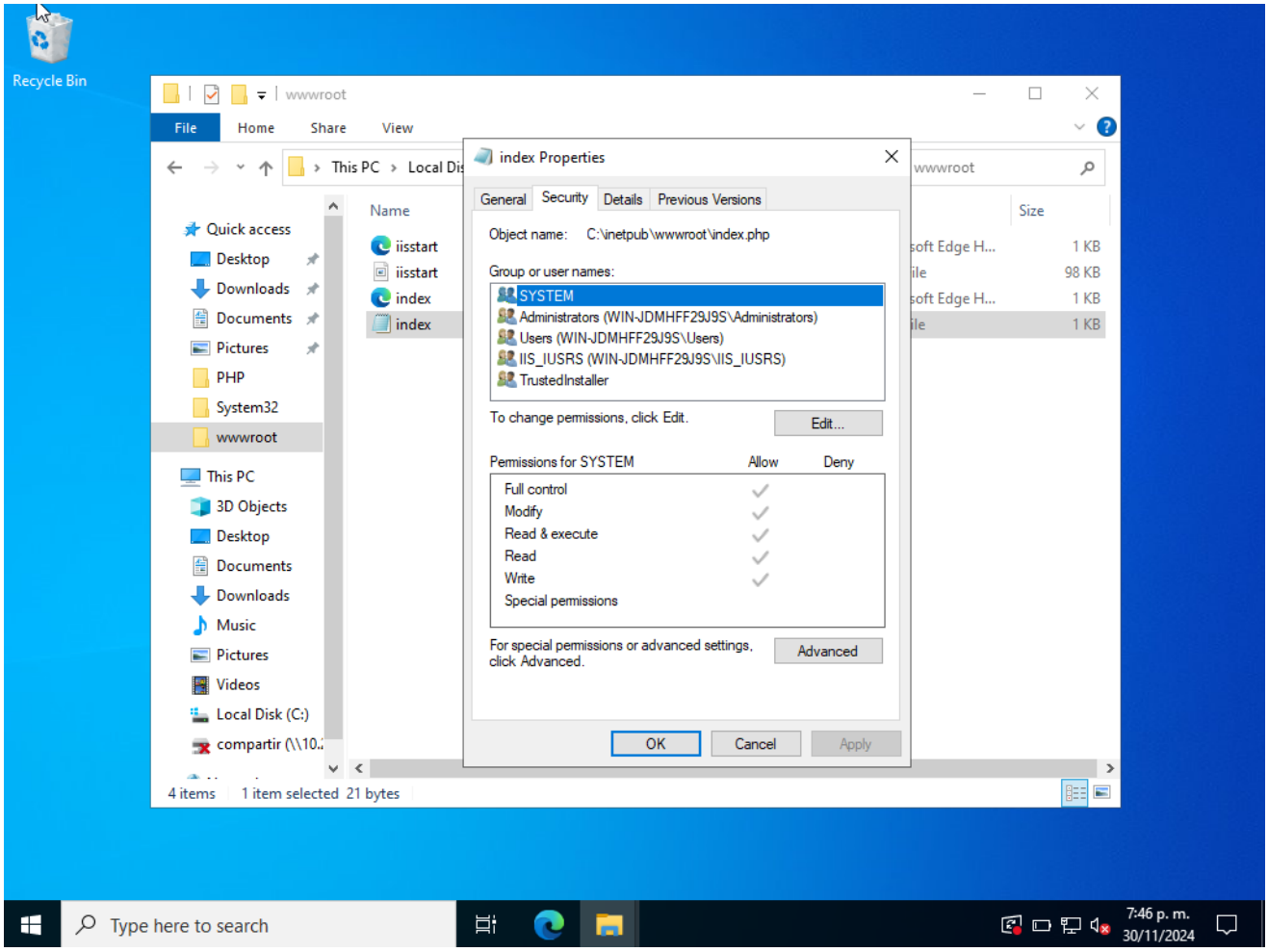


Figure 115. Verifying that the IIS user has the correct permissions for index.php

- We open the browser and enter the IP address of Windows Server along with the path where the index.php is stored

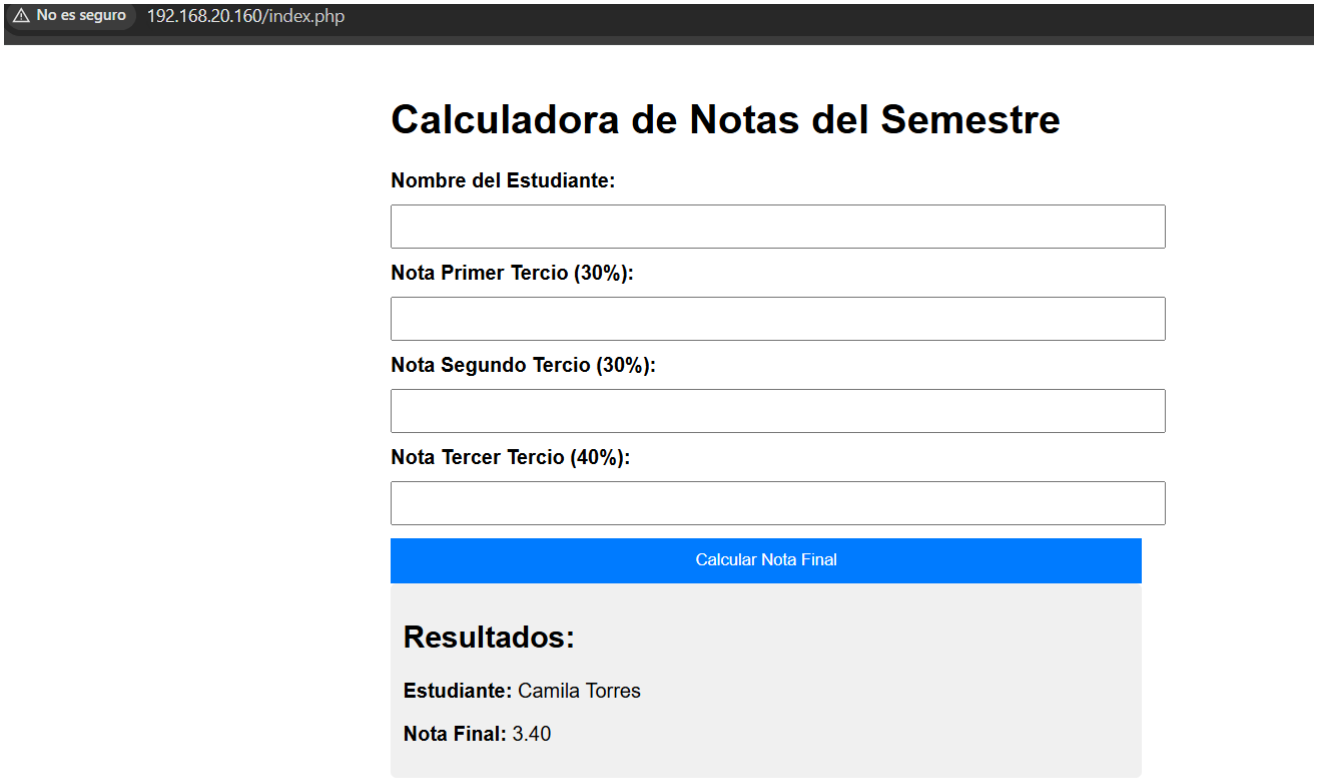


Figure 116. Calculator application on Windows Server

2. Other Useful Commands

- We use netstat to obtain network statistics, ethtool to get information about a specific network interface, route to view the routing table, ifconfig to check network interfaces, and iftop to monitor network traffic. Finally, we display this information through a user-friendly menu

```
 GNU nano 6.0                          network_info.sh
#!/bin/bash

display_menu() {
  clear
  echo "Network Information Menu - Slackware"
  echo "------------------------------------"
  echo "1) Display Network Interfaces (ifconfig/ip)"
  echo "2) Display Network Statistics (netstat)"
  echo "3) Display Bandwidth Usage (vnstat)"
  echo "4) Display Routing Table (route/ip route)"
  echo "5) Display Ethernet Information (ethtool/ip link)"
  echo "6) Exit"
  echo "------------------------------------"
  read -p "Select an option (1-6): " choice
}

execute_command() {
  case $1 in
    1)
      echo -e "\n*** Network Interfaces ***"
      if command -v ifconfig &>/dev/null; then
        ifconfig -a
      else
        ip addr show
      fi
      ;;
    2)
      echo -e "\n*** Network Statistics ***"
      netstat -i
      ;;
    3)
      echo -e "\n*** Bandwidth Usage ***"
      read -p "Enter the interface" interface

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo
```

Figure 117. Shell program part 1

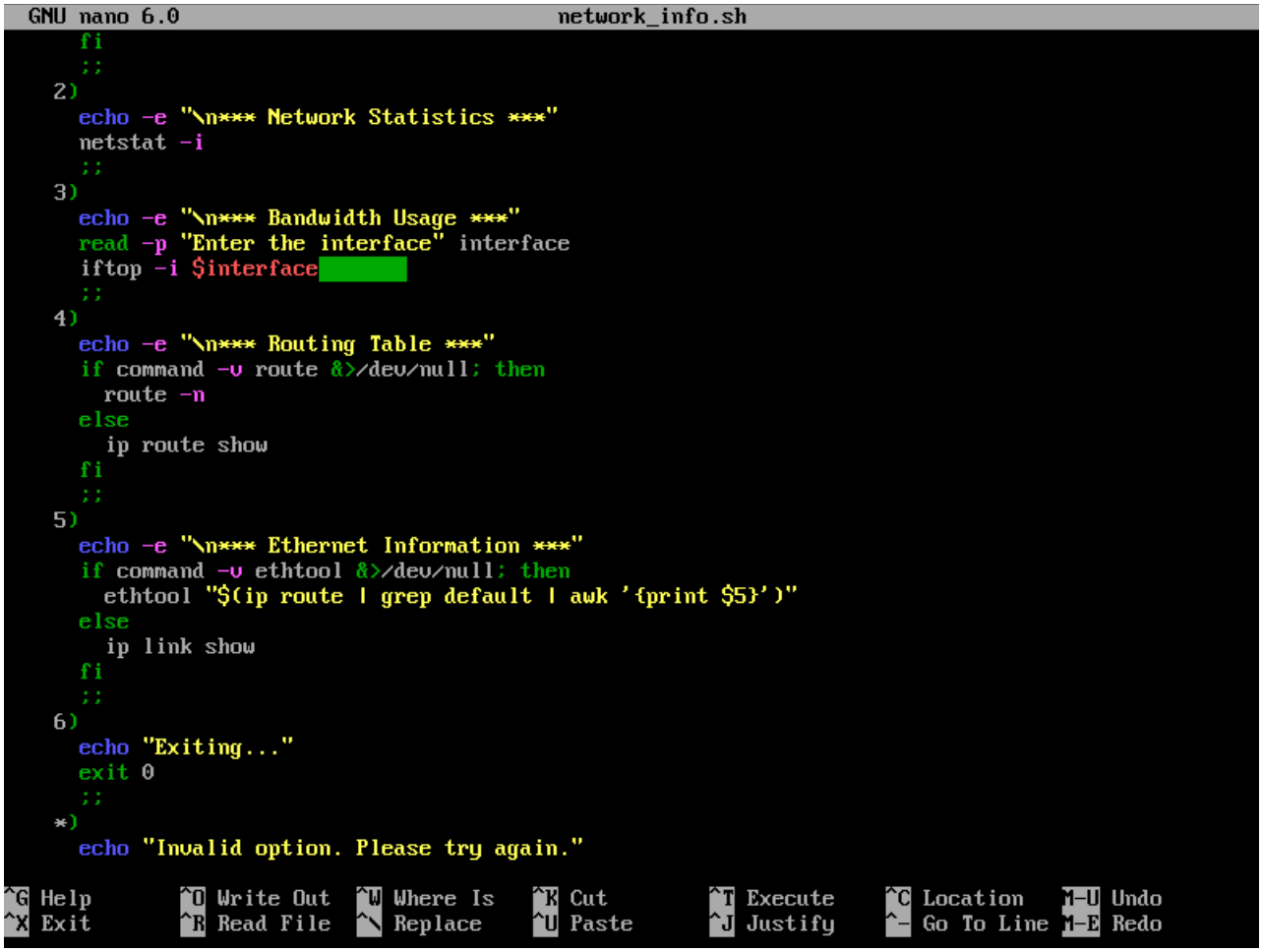


Figure 118. Shell program part 2

```
 GNU nano 6.0                                network_info.sh
      ;;
    4)
      echo -e "\n*** Routing Table ***"
      if command -v route &>/dev/null; then
        route -n
      else
        ip route show
      fi
      ;;
    5)
      echo -e "\n*** Ethernet Information ***"
      if command -v ethtool &>/dev/null; then
        ethtool "$(ip route | grep default | awk '{print $5}')"
      else
        ip link show
      fi
      ;;
    6)
      echo "Exiting..."
      exit 0
      ;;
    *)
      echo "Invalid option. Please try again."
      ;;
  esac
}

while true; do
  display_menu
  execute_command "$choice"
  read -p "Press Enter to continue..."
done

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

Figure 119. Shell program part 3

- Finally, we run the file and perform the respective tests for each item

```
root@andrea:~# ./network_info.sh
Network Information Menu - Slackware
-------------------------------------
1) Display Network Interfaces (ifconfig/ip)
2) Display Network Statistics (netstat)
3) Display Bandwidth Usage (vnstat)
4) Display Routing Table (route/ip route)
5) Display Ethernet Information (ethtool/ip link)
6) Exit
-------------------------------------
Select an option (1-6): 1
```

Figure 120. Shell menu

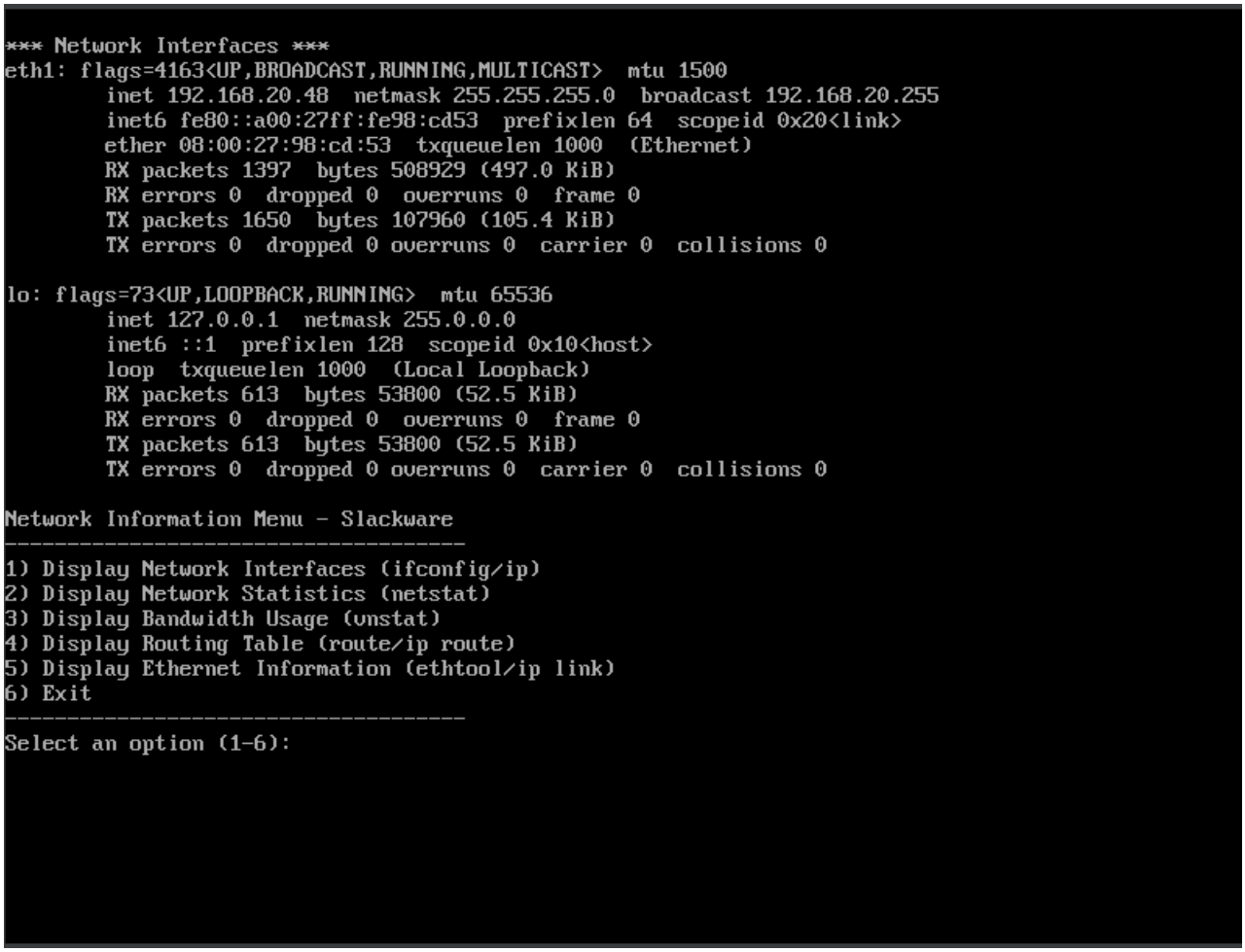


Figure 121. Network interfaces information (ifconfig command)

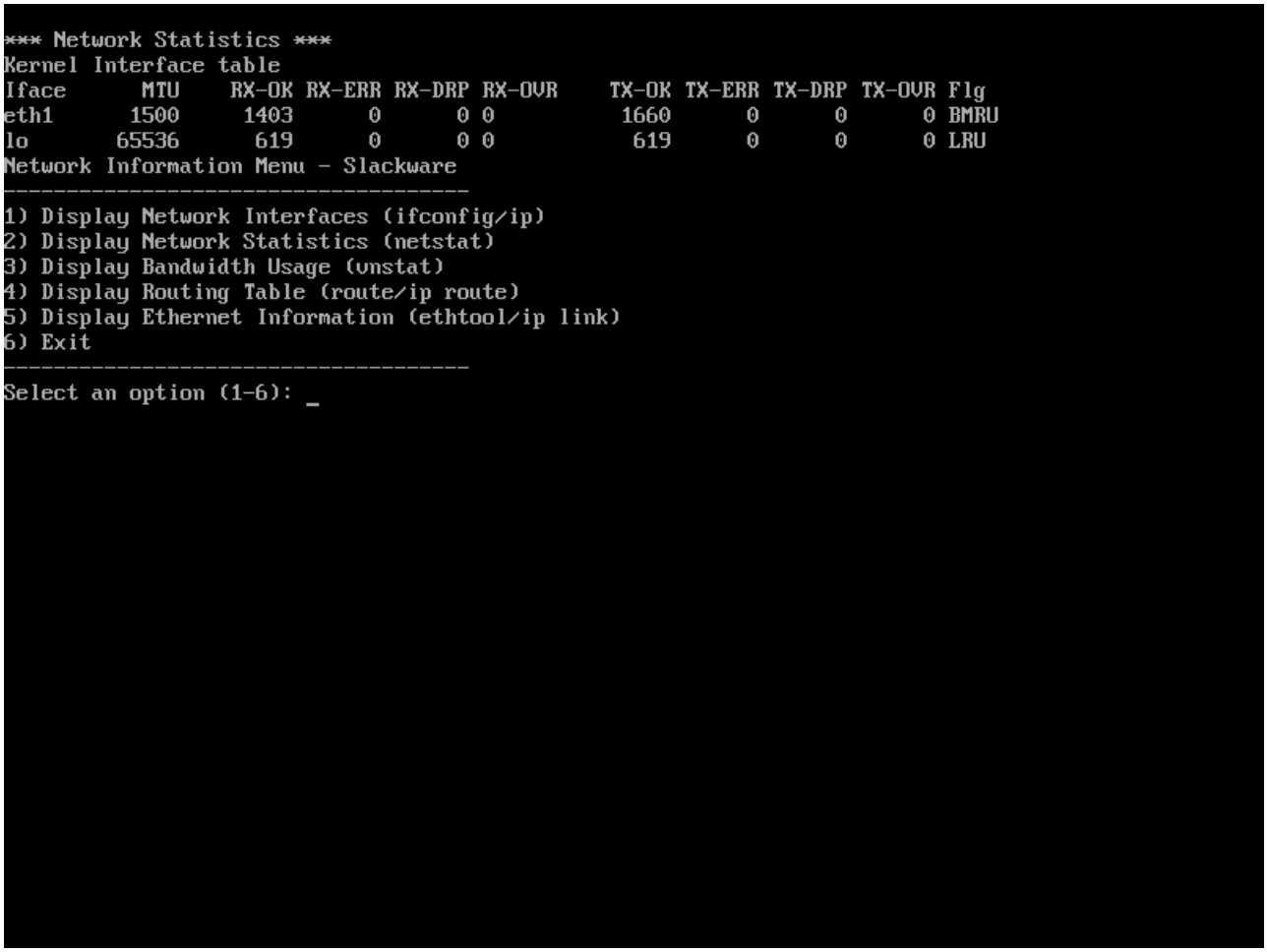


Figure 122. Network Stadistics (netstat command)

Figure 123. Selecting an interface to use in option 3 of the menu (iftop)

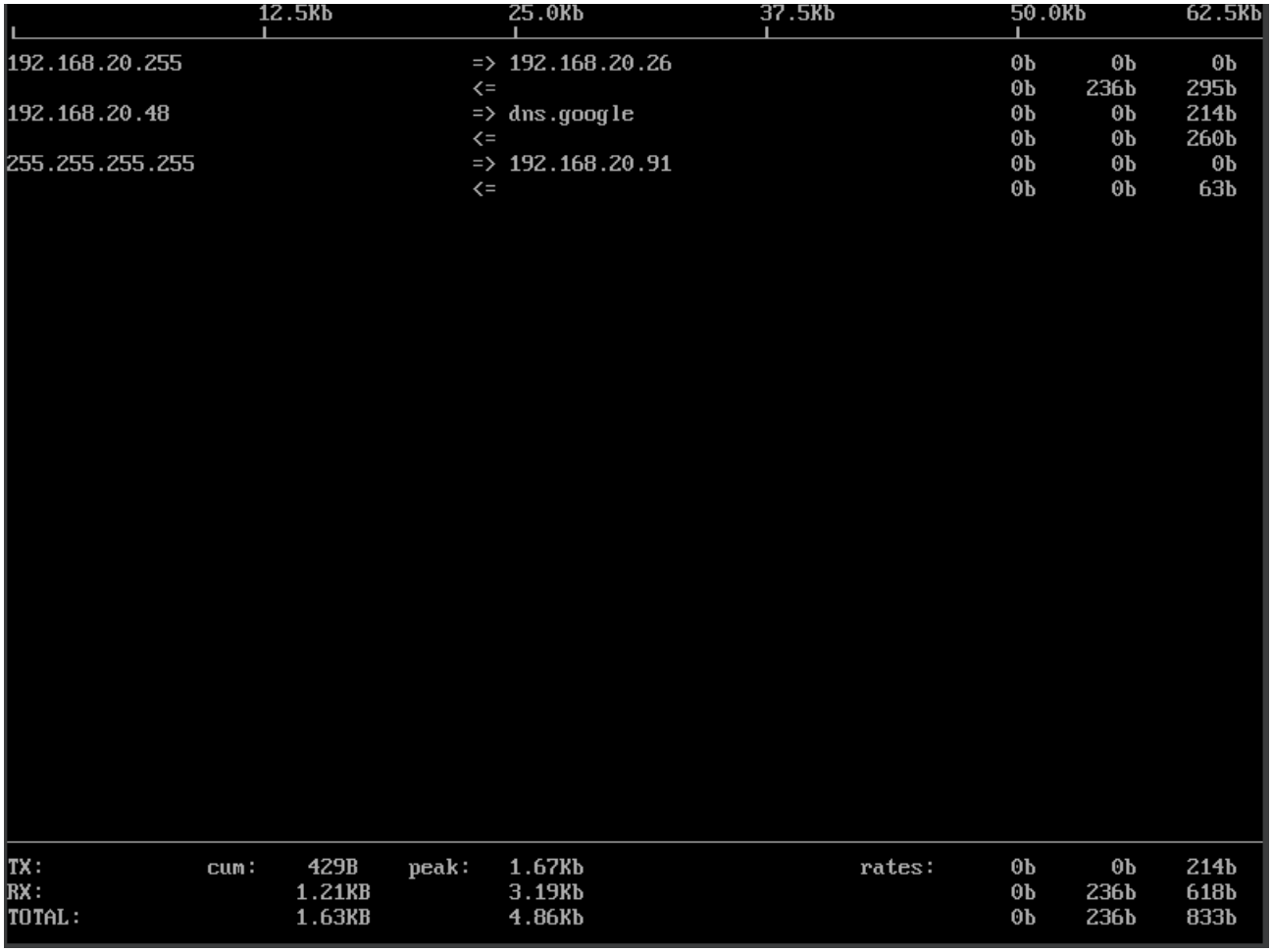


Figure 124. Traffic monitoring of eth1 (iftop command)

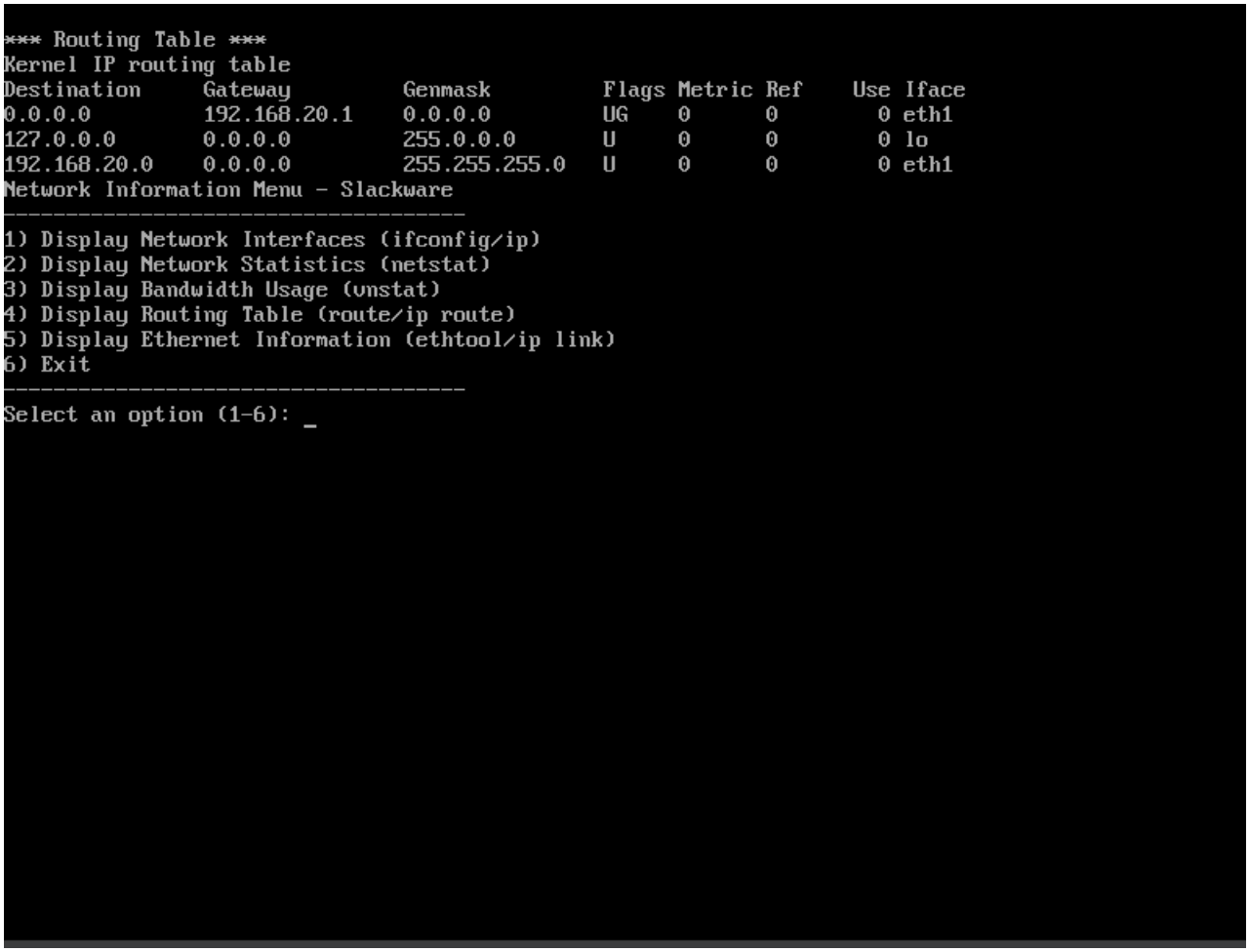


Figure 125. Routing table information (route command)

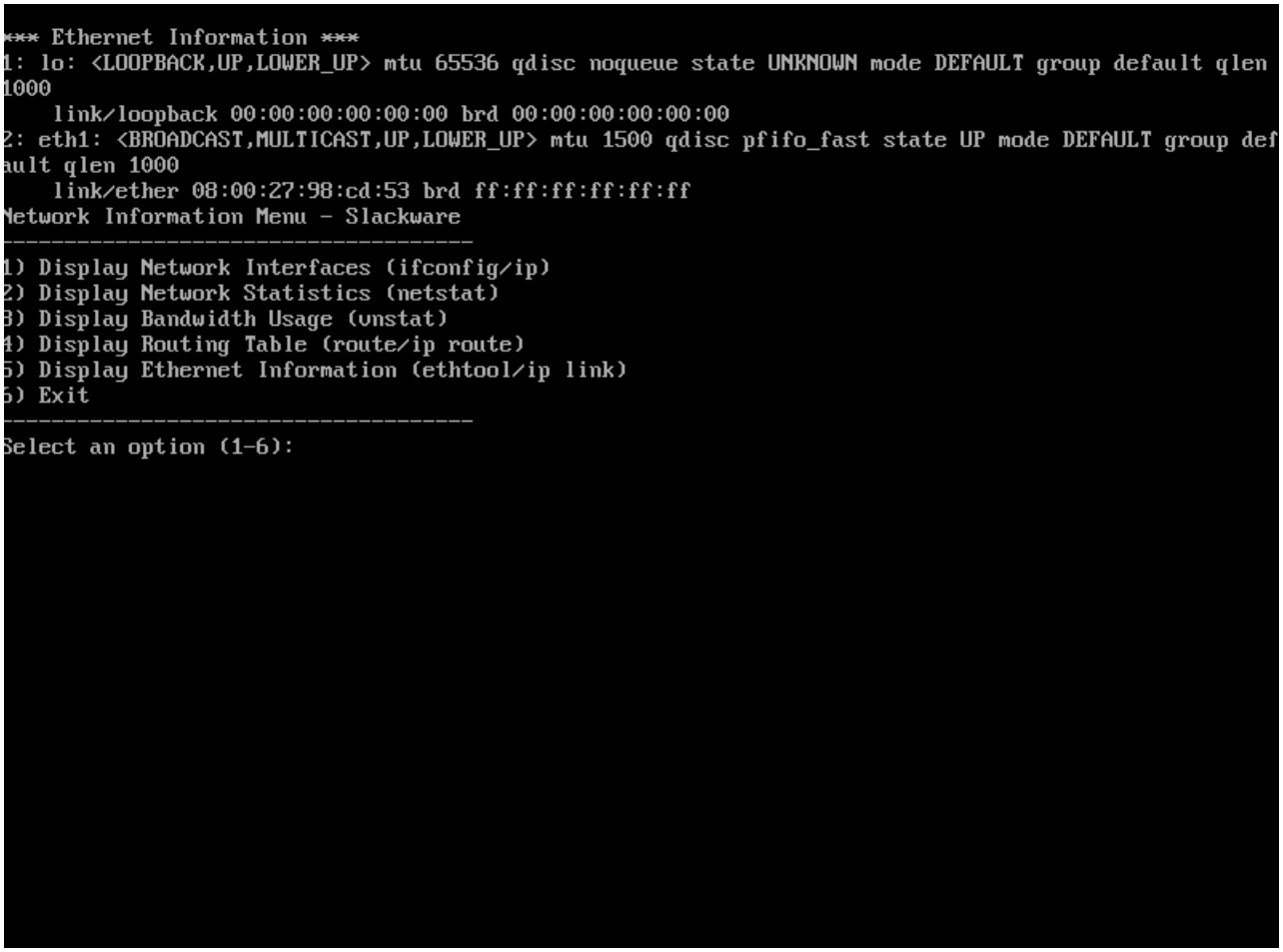


Figure 126. Ethernet information (ethtool command)

Conclusions

- **Fundamentals of Connectivity**: Verifying connectivity with the ping command demonstrates the importance of proper configuration for successful communication between devices.
- **Advanced Switch Configuration:** This laboratory provides practical exposure to configuring network switches and PCs, reinforcing concepts related to device addressing and basic connectivity setup. Using Wireshark to capture and analyze Ethernet frames helps us understand the structure of network packets, including the role of MAC addresses and error control mechanisms.
- **Preparation for Advanced Networking:** By mastering basic switch configuration and packet analysis, we lay a strong foundation for more complex networking topics, such as VLANs, routing, and advanced diagnostics. Interconnecting all setups within the group tests the scalability of the configuration and ensures all devices are properly integrated into the same network.
- **Basic Device Security:** Configuring access passwords (privileged mode, console, and remote terminal) highlights the importance of securing network devices to prevent unauthorized access. Combining the switch name, MOTD, interface descriptions, and passwords illustrates the interplay of security, usability, and documentation in professional network environments.
- **IP Addressing and Subnetting:** The laboratory reinforces the importance of proper **IP address allocation** and subnetting to ensure network devices operate within their designated ranges. Correctly configuring both the wired LAN and wireless networks with unique subnets prevents IP conflicts and supports structured communication.
- **Wireless Network Configuration:** Configuring **SSIDs**, IP ranges for DHCP, and security protocols such as

WPA2-PSK with AES ensures that wireless networks are secure, identifiable, and capable of automatically assigning IP addresses to clients. This highlights the practical application of wireless router setup for distinct user groups. The configuration contrasts with the use of **static IPs** for wired devices and **DHCP** for wireless devices, showcasing the advantages and considerations of each approach in various scenarios.

- **Channel Configuration:** Configuring specific channels for wireless communication ensures **signal optimization and interference minimization**, which is critical in environments with overlapping wireless networks.
- **Use of Packet Tracer for Simulation:** Cisco Packet Tracer provides a controlled environment for configuring and testing complex network setups. This approach helps us visualize data flow, troubleshoot issues, and solidify their understanding of networking concepts.
- **Network Address Translation (NAT):** NAT enables multiple devices connected to the router to share a single public IP for Internet access. Understanding NAT explains why some devices can communicate externally but may face limitations when pinging devices on other subnets.
- **Beacon Frames and Network Visibility:** Disabling beacon frames hide the SSID from casual discovery but does not fully secure the network. Devices configured with the correct SSID and credentials can still connect. Tools like WiFi Analyzer demonstrate that hidden networks remain detectable, albeit without an SSID.
- **WiFi Analyzer and Network Monitoring**: Discovering nearby networks and their channel assignments shows how **interference** impacts performance. This understanding can guide channel planning and deployment of wireless networks in dense areas.
- **Dynamic Grade Calculator**: Configuring Apache and IIS to interpret PHP ensures that the server can execute dynamic scripts, a foundational skill in web development.
- **Network Information Commands:** Commands like ifconfig, netstat, vnstat, route, and ethtool provide critical insights into: Network configurations (ifconfig, route), Active connections and listening ports (netstat), Bandwidth usage statistics (vnstat, iftop), Hardware-level diagnostics (ethtool).
- **Security** Assigning a MAC address to a specific VLAN enhances network security by ensuring that only authorized devices can access designated network segments. This process improves traffic isolation, limits unauthorized access, and reduces the risk of attacks like lateral movement. By restricting devices to their assigned VLANs, sensitive areas of the network are better protected, contributing to stronger control over resources and overall network security

References

- Cisco Systems. (2015). *Configuring VLANs, VTP, and VMPS*. Cisco. Retrieved from https://www.cisco.com/c/en/us/td/docs/iosxr/iosxr_700/iosxr70097/switching/vlancfg/vlancfg_cg/vtp.html

- Cisco Systems. (2018). *Configuring VLANs*. Cisco. Retrieved from https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/l2vpn/l2vpn-l2config/b-l2vpn-l2config-book/b-l2vpn-l2config_chapter_010.html

- IEEE 802.1Q-2018. (2018). *IEEE Standard for Local and Metropolitan Area Network--Bridges and Bridged Networks*. IEEE. https://ieeexplore.ieee.org/document/8403927

- Wikipedia contributors. (2024, December 5). VLAN. Wikipedia. https://en.wikipedia.org/wiki/VLAN

- IEEE 802.1Q. (2023). *IEEE 802.1Q - Wikipedia*. https://en.wikipedia.org/wiki/IEEE_802.1Q

- Wikipedia contributors. (2024, December 5). *VLAN*. Wikipedia. https://en.wikipedia.org/wiki/VLAN