

## **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**

## Content

Objective .....	6
Tools to be Used.....	6
Introduction .....	6
Setup .....	9
1. Basic Switch Configuration .....	9
2. Basic Switch Configuration .....	13
3. Larger Switch Networks .....	18
4. VLAN Configuration .....	35
5. Basic WiFi Configuration.....	39
<b>5.1. Configuration Process .....</b>	39
<b>5.2. Connection tests between devices .....</b>	60
6. Configuration of Wired and Wireless LAN.....	74
7. WiFi .....	104
<b>7.1. Configuration Process .....</b>	104
<b>7.2. Testing from devices.....</b>	117
<b>7.3. disabling the beacon frame .....</b>	126
8. Reviewing WiFi Networks Near Your Home .....	128
Base Software Installation.....	131
1. Dynamic Web Service .....	131
<b>1.1. Deploying an application on Apache (Solaris) .....</b>	131
<b>1.2. Deploying an application on IIS (Windows Server).....</b>	136
2. Other Useful Commands .....	152
Conclusions .....	160
References .....	161

Figure 1 first PC configuration .....	10
Figure 2 test ping .....	10
Figure 3 test ping .....	11
Figure 4 test ping to the other group .....	12
Figure 5 Packet Tracer screenshot .....	12
Figure 6 Analyzed packet.....	12
Figure 7 Packet information. ....	13
Figure 8 Basic configuration .....	15
Figure 9 interfaces description.....	15
Figure 10 enabled secret .....	15
Figure 11 saving configurations.....	15
Figure 12 Verification of the switch interfaces .....	16
Figure 13 Viewing the configuration file .....	16
Figure 14 Viewing the configuration file .....	17
Figure 15 Viewing the configuration file .....	17
Figure 16 Viewing the configuration file .....	18
Figure 17 Vlan configuration .....	36
Figure 18 interfaces Verification of interfaces .....	37
Figure 19 gig0/1 configuration .....	38
Figure 20 Verification of the MAC address table .....	38
Figure . Assigning IP and Subnet Mask to PC0.....	40
Figure . Assigning IP and Subnet Mask to PC1.....	41
Figure . Assigning IP and Subnet Mask to Server0 .....	42
Figure . Configuring WPC300N Wireless Port of the Laptops .....	43
Figure . Configuring DHCP in the laptops .....	44
Figure . Authenticating to Configure the Router.....	45
Figure . Internet Setup of the Wireless Router .....	46
Figure . Basic Wireless Settings of the router.....	47
Figure . Router Channels Options.....	47
Figure . Wireless Security of the router.....	48
Figure . Configuring and Assigning IP Address Range on the Wireless Router .....	49
Figure . Configuring Access Point .....	50
Figure . Opening PC Wireless from Laptop0.....	51
Figure . Connecting Laptop0 to the Wireless Router .....	52
Figure . Connecting to the Wireless Router from Laptop0 .....	53
Figure . Configuring SmartPhone0 to Establish Connection with the Wireless Router .....	54
Figure . Connecting Laptop1 to Access Point .....	55
Figure . Connecting to Access Point from Laptop1 .....	56
Figure . Configuring SmartPhone1 to Connect to the Access Point .....	57
Figure . Assigning Static IP and Subnet Mask to Laptop1.....	58
Figure . Assigning Static IP and Subnet Mask to Smartphone1.....	59
Figure . Basic Wi-Fi Configuration Diagram Completed .....	60
Figure . First Ping Tests on PC0.....	61
Figure . First Ping Tests on PC1.....	62
Figure . Second Ping Tests on PC1 .....	63
Figure . First Ping Tests on Server0.....	64
Figure . Second Ping Tests on Server0.....	65
Figure . First Ping Tests on Smartphone1 .....	66

Figure . Second Ping Tests on Smartphone1 .....	67
Figure . First Ping Tests on Laptop1.....	68
Figure . Second Ping Tests on Laptop1 .....	69
Figure . First Ping Tests on Smartphone0.....	70
Figure . Second Ping Tests on Smartphone0 .....	71
Figure . First Ping Tests on Laptop0.....	72
Figure . Second Ping Tests on Laptop0.....	73
Figure Initial Configuration .....	74
Figure configuration palette dialog .....	75
Figure . Configuring IP and Subnet Mask on the Computer (“PC0”) .....	105
Figure . Authenticating to Configure the Wireless Router .....	106
Figure . Main Menu of the Wireless Router Configuration .....	106
Figure . Assigning a Name to the Wireless Network .....	107
Figure . Assigning Access Mechanism to Wireless Clients: WPA2-PSK with AES .....	107
Figure . Assigning a Wireless Security Password .....	108
Figure . Saving Changes to the Wireless Setup .....	108
Figure . Accessing to Internet Connection Setup Wizard .....	109
Figure . Setting a password for the Administrator .....	109
Figure . Selecting Time Zone to the router.....	110
Figure . Configuring Internet Connection.....	111
Figure . Default Value for the DHCP Connection Section .....	112
Figure . Configuring IP Address Range on the Wireless Router .....	113
Figure . Opening Manual Internet Connection Setup .....	114
Figure . Static IP Address Internet Connection Type of the Wireless Router.....	115
Figure . Available Channels of the Wireless Router .....	116
Figure . Configuring a Channel on the Wireless Router .....	117
Figure . Authenticating and Connecting to the Wireless Network from the Mobile .....	118
Figure . IP Assigned to the Smartphone .....	119
Figure . Ping Tests on the Mobile Device .....	120
Figure . Ping from the Computer (PC0 in the Diagram) to the Smartphone .....	121
Figure . Ping from the Computer (PC0 in the Diagram) to a Laboratory Device (PC3 in the Diagram).....	121
Figure . Ping to Internet Devices (Google DNS).....	122
Figure . Ping to Internet Devices (google.com) .....	122
Figure . Ping from the Computer (PC0 in the Diagram) to another Laboratory Device .....	123
Figure . Ping to a Device on Another Network .....	123
Figure . Obtaining Wireless Traffic from Active Networks Nearby Using Wi-Fi Analyzer .....	124
Figure . Information from the Wireless Network Capture .....	125
Figure . Information on Router Channels .....	126
Figure . disabling the beacon frame .....	127
Figure . Verifying the Wireless Network with Beacon Frame Disabled in WiFi Analyzer.....	128
Figure . Obtaining Wireless Traffic from Active Networks Near the House with Wi-Fi Analyzer.....	129
Figure . Information from the Wireless Network Capture of the house .....	130
Figure . Information on Router Channels and Time Graph .....	131
Figure . Opening httpd.conf file .....	131
Figure . Adding ‘LoadModule php5_module libexec/libphp5.so’ into httpd.conf .....	132
Figure . Adding ‘AddType application/x-hhtpd-php .php’ into httpd.conf .....	133
Figure . Configuring the location of index.php in the httpd.conf file.....	134
Figure . Creating the /calculator directory .....	134

Figure . Creating index.php file .....	134
Figure . Calculator program.....	135
Figure . Restarting Apache on Solaris.....	135
Figure . Calculator application on Solaris .....	136
Figure . Downloading PHP 8.4.1 .....	137
Figure . Control Panel in Windows Server .....	138
Figure . System Settings.....	139
Figure . Opening Environment Variables in Windows Server .....	140
Figure . Editing System Variables .....	141
Figure . Adding a new path.....	142
Figure . Adding the PHP path in the environment variable configuration .....	143
Figure . Editing the php.ini file.....	144
Figure . IIS Manager Menu .....	145
Figure . Handler Mappings Section .....	146
Figure . Configuring Module Mapping for PHP .....	147
Figure . Navigating to FastCGI Settings.....	148
Figure . FastCGI Settings section .....	149
Figure . Adding FastCGI Application .....	150
Figure . Verifying that the IIS user has the correct permissions for index.php.....	151
Figure . Calculator application on Windows Server .....	152
Figure . Shell program part 1 .....	153
Figure . Shell program part 2 .....	154
Figure . Shell program part 3 .....	155
Figure . Shell menu .....	155
Figure . Network interfaces information (ifconfig command) .....	156
Figure . Network Stadistics (netstat command) .....	157
Figure . Selecting an interface to use in option 3 of the menu (iftop) .....	157
Figure . Traffic monitoring of eth1 (iftop command) .....	158
Figure . Routing table information (route command).....	159
Figure . Ethernet information (ethtool command) .....	160

---

## 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

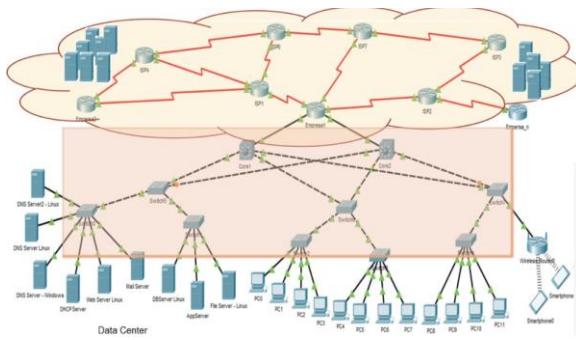
Packet Tracer

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:

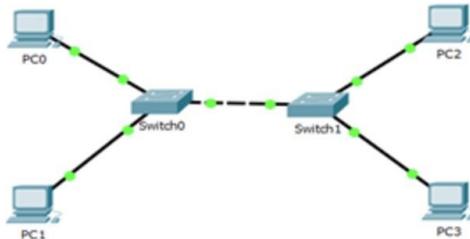
- **VLAN 0:** This VLAN is not used for regular traffic and has a specific purpose in certain implementations.
- **VLAN 4095:** This VLAN is also reserved for internal use and is not intended for user traffic.

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.

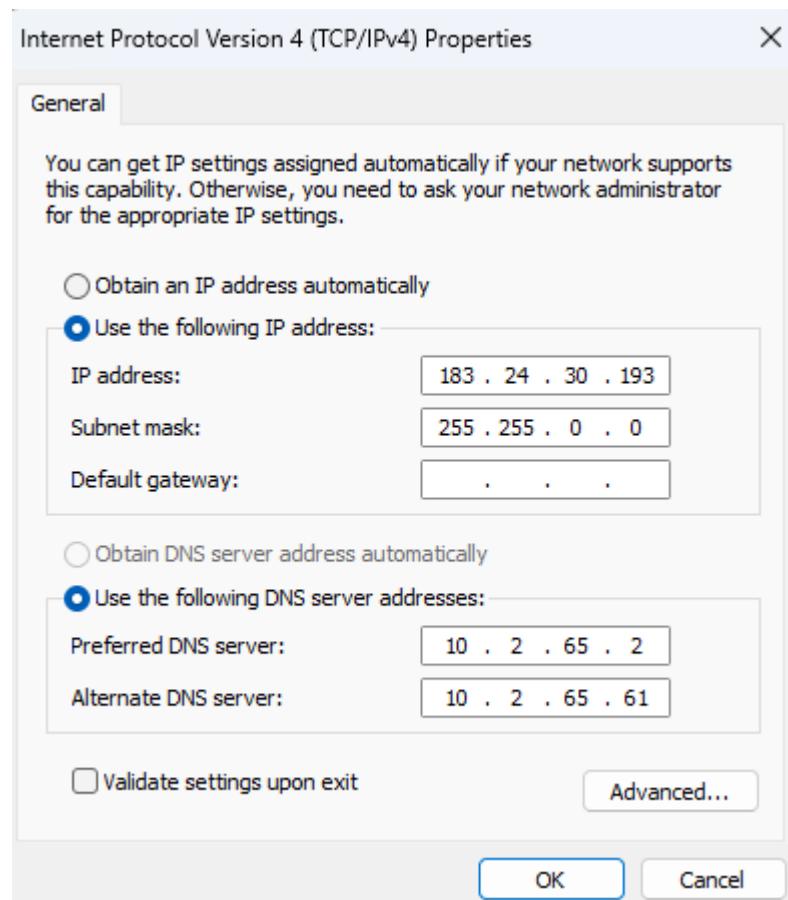


Figure 1 first PC configuration

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

- From PC2 to PC3

```
C:\Users\Redes>ping 183.24.30.194

Pinging 183.24.30.194 with 32 bytes of data:
Reply from 183.24.30.194: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.30.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 2 test ping

- From PC3 to PC2

```
C:\Users\Redes>ping 183.24.30.193

Pinging 183.24.30.193 with 32 bytes of data:
Reply from 183.24.30.209: Destination host unreachable.
Reply from 183.24.30.193: bytes=32 time=1ms TTL=128
Reply from 183.24.30.193: bytes=32 time=1ms TTL=128
Reply from 183.24.30.193: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.30.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

*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

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.

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

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

No.	Name	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)

Figure 6 Analyzed packet

```

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{7B643ABC-2F2F-4316-A29F-AFDA29B80D93}, id 0
  Section number: 1
  Interface id: 0 (\Device\NPF_{7B643ABC-2F2F-4316-A29F-AFDA29B80D93})
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 27, 2024 15:16:49.435008000 Hora est. Pacífico, Sudamérica
  UTC Arrival Time: Nov 27, 2024 20:16:49.435008000 UTC
  Epoch Arrival Time: 1732738609.435008000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ether:type:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: HP_6a:19:46 (30:13:8b:6a:19:46), Dst: HP_6a:18:ce (30:13:8b:6a:18:ce)
  ▶ Destination: HP_6a:18:ce (30:13:8b:6a:18:ce)
  ▶ Source: HP_6a:19:46 (30:13:8b:6a:19:46)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 183.24.30.194, Dst: 183.24.30.209
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x2e71 (11889)
  ▶ 000. .... = Flags: 0x0
    0.... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 183.24.30.194
  Destination Address: 183.24.30.209
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d38 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 35 (0x0023)
    Sequence Number (LE): 8960 (0x2300)
    [Response frame: 2]
  ▶ Data (32 bytes)

```

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 Catalyst switches, IOS, has a layered operational structure based on privileges and the configuration activities to be 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"

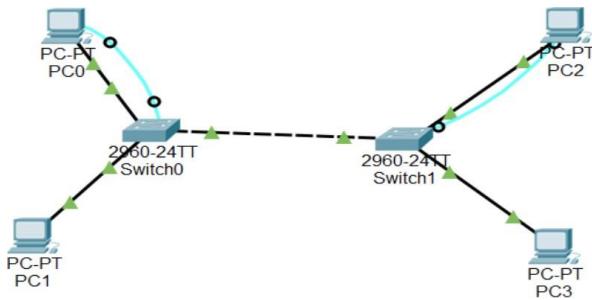
Screen synchronization.

Description of used interfaces.

Access passwords for the device:

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

- Remote terminal key: Key T To carry out this task, we first connect to the switch using console cables and the terminal mode 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)#hostname 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 $1$Qzlg$CsRMZ6A3kqjMt/sn1K6O9.
!
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 $1$Qzlg$CsRMZ6A3kqjMt/sn1K609.
!
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
```

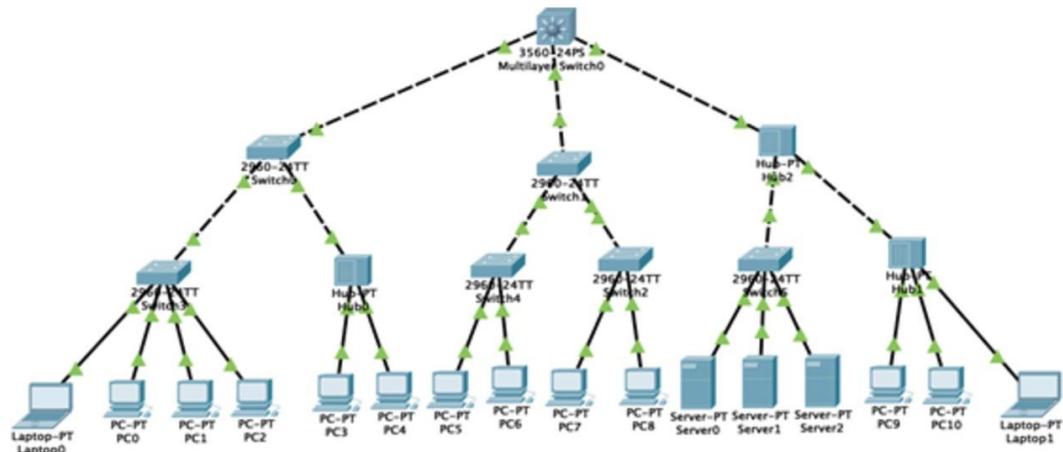
Figure 15 Viewing the configuration file

```
!
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*

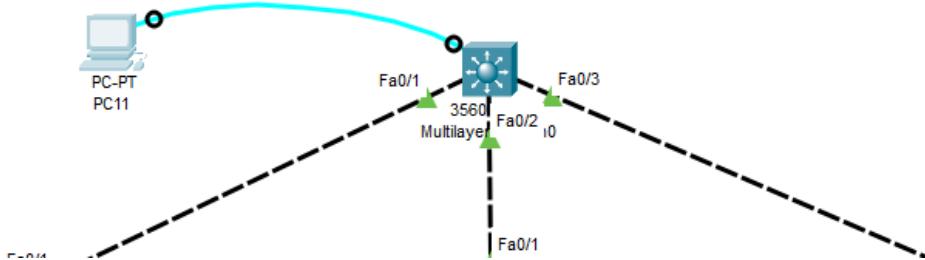
### 3. Larger Switch Networks

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.

- Configure the computers and servers with the information provided below:

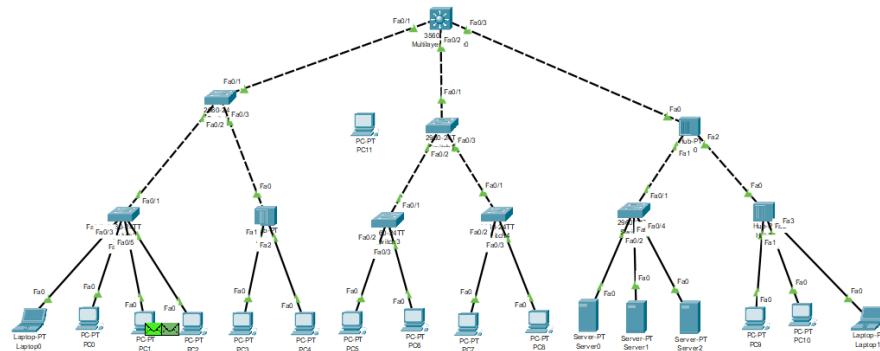
Estudiante1	Estudiante 2
IP: 65.148.77.x (x= número secuencial de 100 a 120) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1	IP: 65.148.77.x (x= número secuencial de 130 a 150) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1

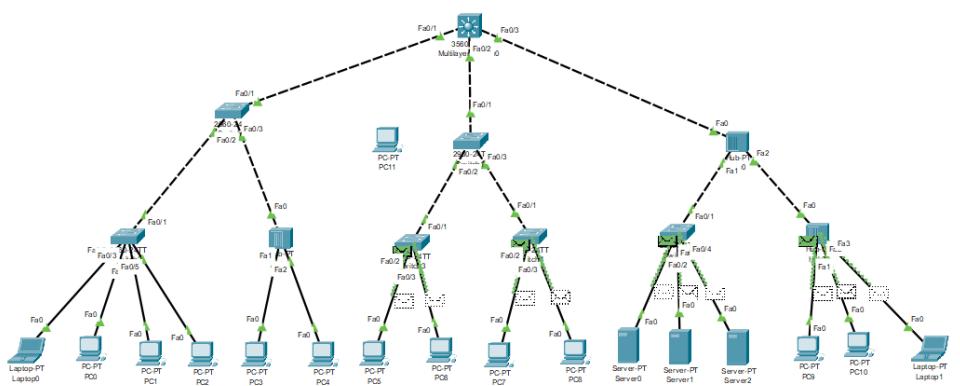
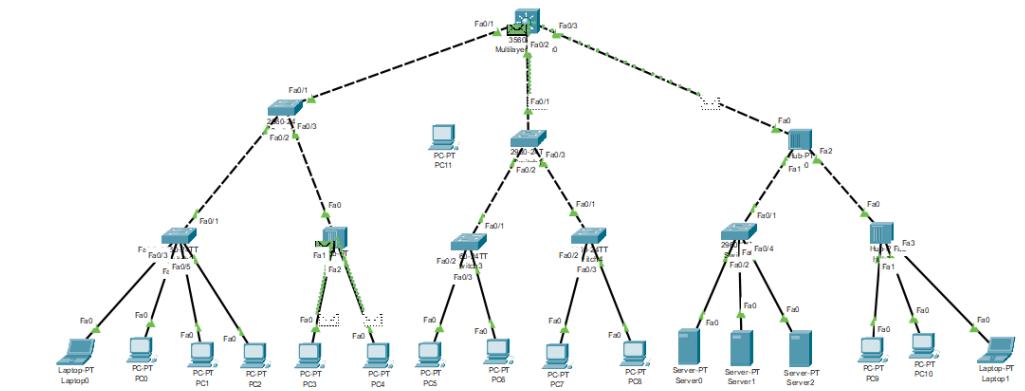
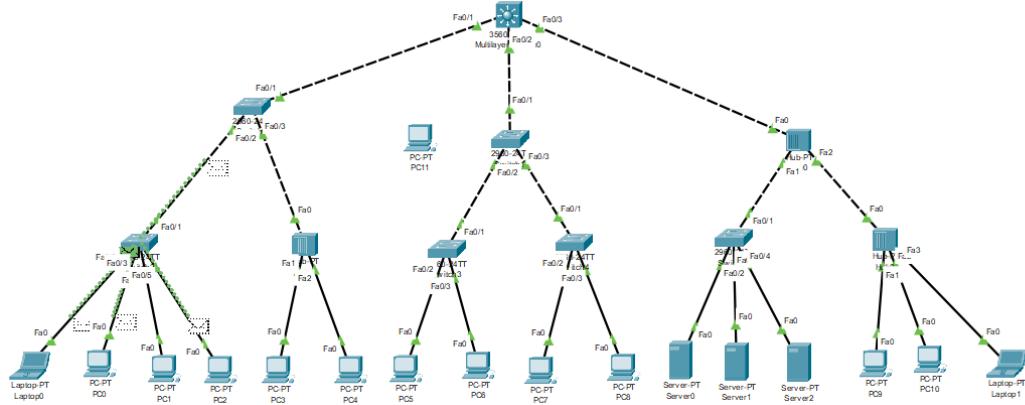
3. We Check the connectivity between the devices.

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 by sending the following frames.( Identify the switches' behavior and their forwarding tables.)

a. From PC1 to PC7.





### PDU Information at Device: PC1

OSI Model      Outbound PDU Details

At Device: PC1  
Source: PC1  
Destination: PC7

#### In Layers

Layer7  
Layer6  
Layer5  
Layer4  
  
Layer3  
  
Layer2  
  
Layer1

#### Out Layers

Layer7  
Layer6  
Layer5  
Layer4  
  
Layer 3: IP Header Src. IP: 65.148.77.102,  
Dest. IP: 65.148.77.108 ICMP Message  
Type: 8  
  
Layer 2: Ethernet II Header  
000D.BD83.5997 >> 0003.E4C6.375D  
  
Layer 1: Port(s): FastEthernet0

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

### PDU Information at Device: Multilayer Switch0

OSI Model      Inbound PDU Details      Outbound PDU Details

At Device: Multilayer Switch0  
Source: PC1  
Destination: PC7

#### In Layers

Layer7  
Layer6  
Layer5  
Layer4  
Layer3

Layer 2: Ethernet II Header  
000D.BD83.5997 >> 0003.E4C6.375D

Layer 1: Port FastEthernet0/1

#### Out Layers

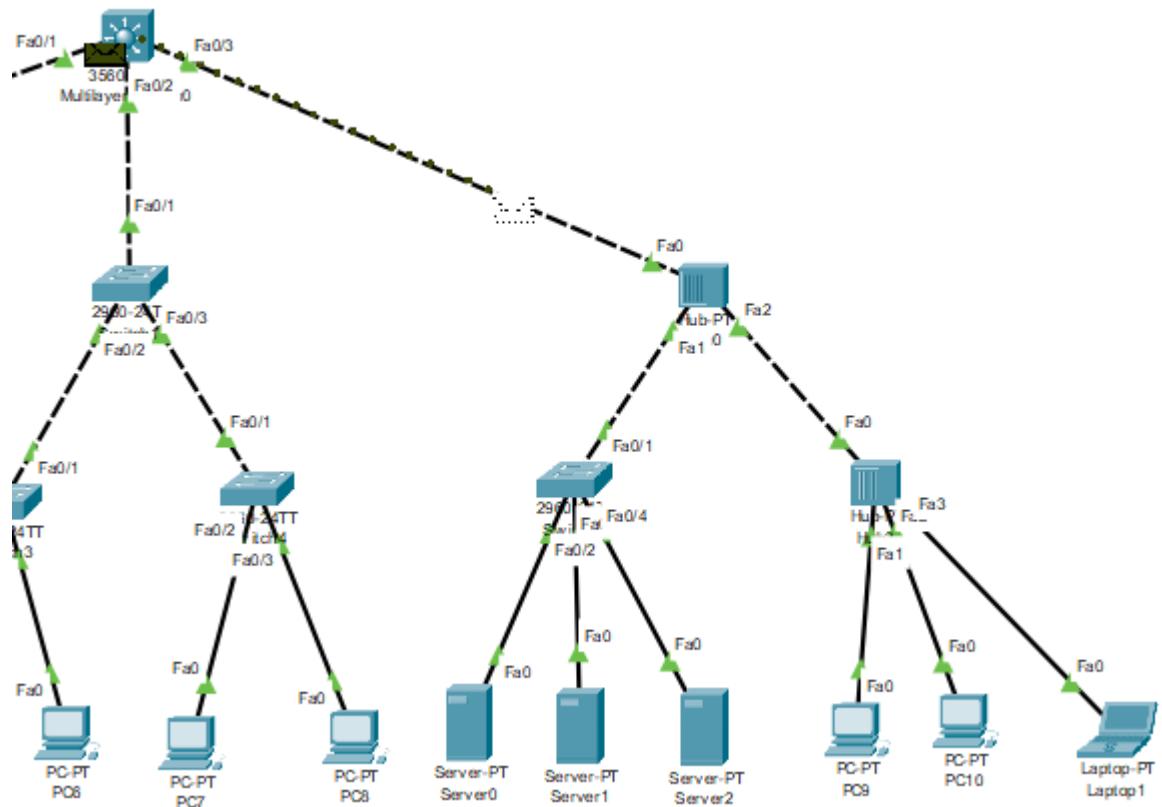
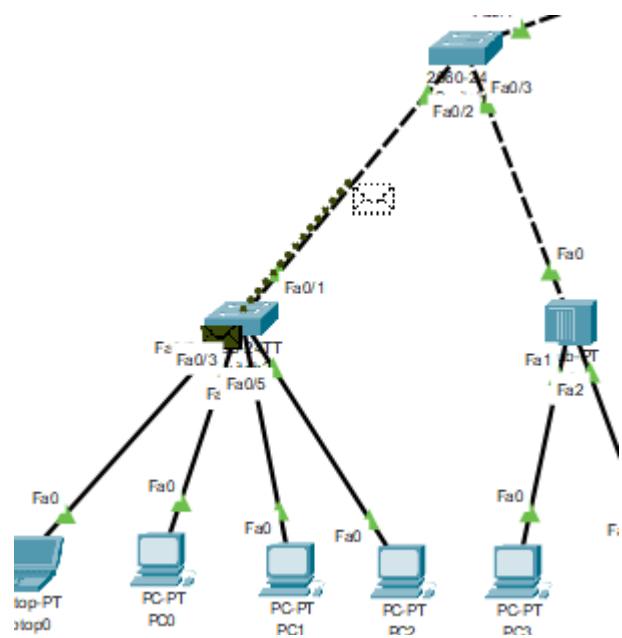
Layer7  
Layer6  
Layer5  
Layer4  
Layer3

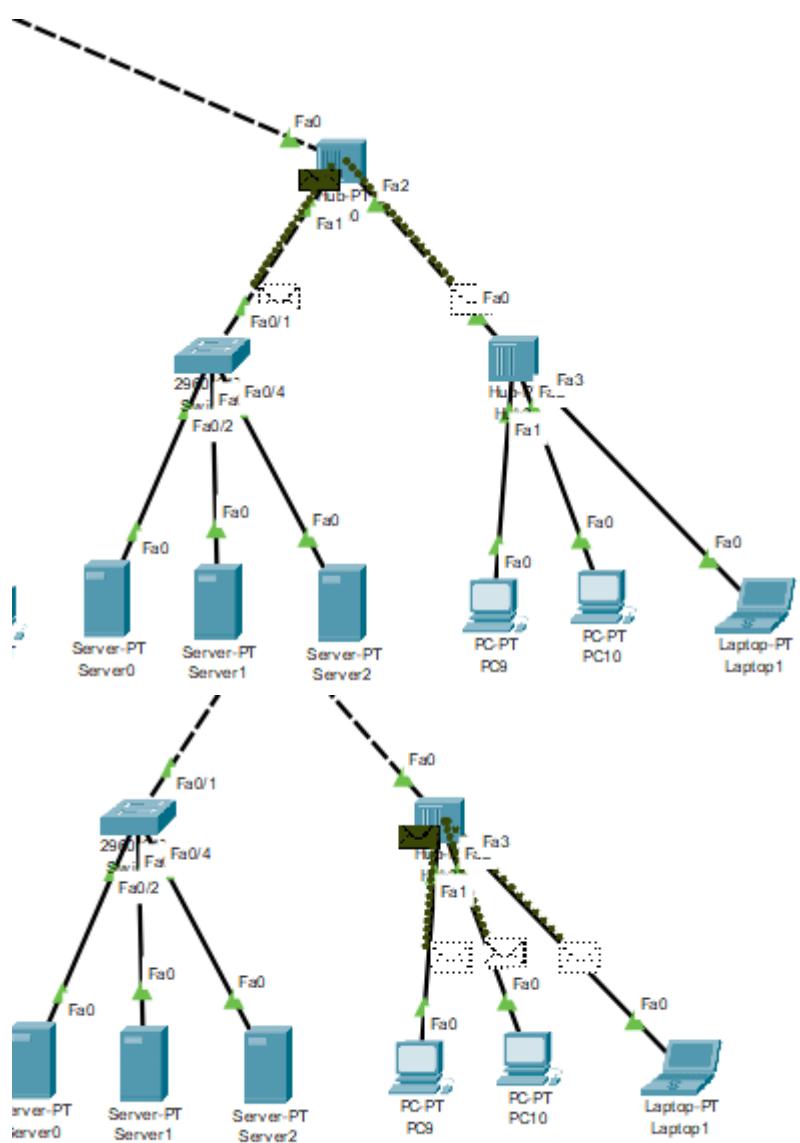
Layer 2: Ethernet II Header  
000D.BD83.5997 >> 0003.E4C6.375D

Layer 1: Port(s): FastEthernet0/2

1. The frame source MAC address was found in the MAC table of Multilayer Switch.
2. This is a unicast frame. Multilayer Switch looks in its MAC table for the destination MAC address.

b. From PC0 to PC9.





**PDU Information at Device: Switch2**

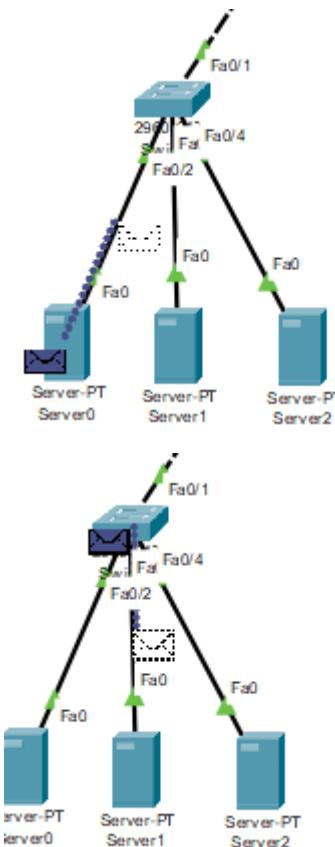
OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: Switch2 Source: PC0 Destination: PC9		
<b>In Layers</b>	<b>Out Layers</b>	
Layer7 Layer6 Layer5 Layer4 Layer3	Layer7 Layer6 Layer5 Layer4 Layer3	Layer 2: Ethernet II Header 0003.E4C2.88BC >> 0001.4298.E6C1
Layer 1: Port FastEthernet0/3		Layer 1: Port(s): FastEthernet0/1
1. The outgoing port is an access port. Switch sends the frame out that port.		

**PDU Information at Device: Multilayer Switch0**

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: Multilayer Switch0 Source: PC0 Destination: PC9		
<b>In Layers</b>	<b>Out Layers</b>	
Layer7 Layer6 Layer5 Layer4 Layer3	Layer7 Layer6 Layer5 Layer4 Layer3	Layer 2: Ethernet II Header 0003.E4C2.88BC >> 0001.4298.E6C1
Layer 1: Port FastEthernet0/1		Layer 1: Port(s): FastEthernet0/3
1. The outgoing port is an access port. Multilayer Switch sends the frame out that port.		

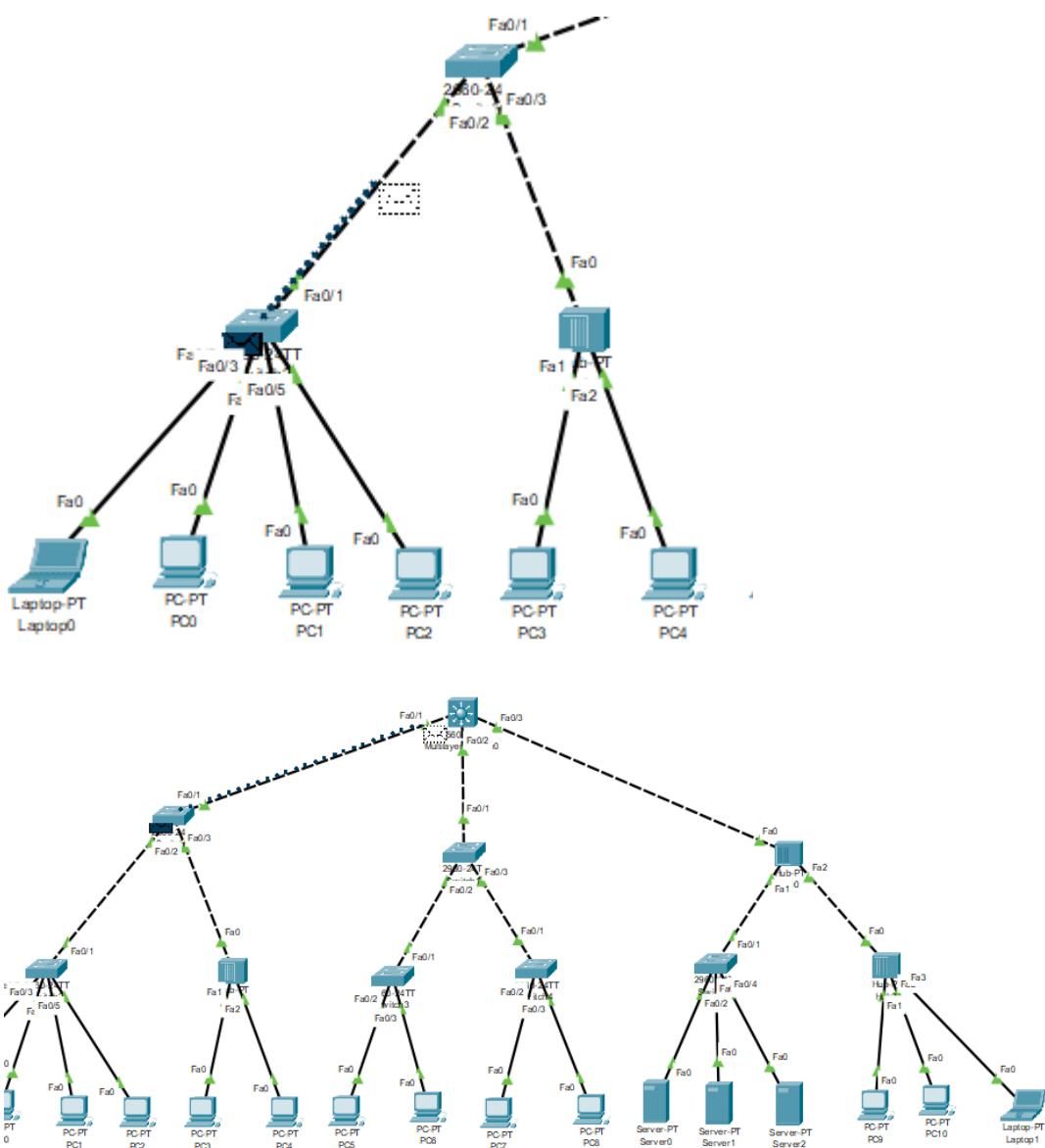
**Challenge Me**    << Previous Layer    Next Layer >>

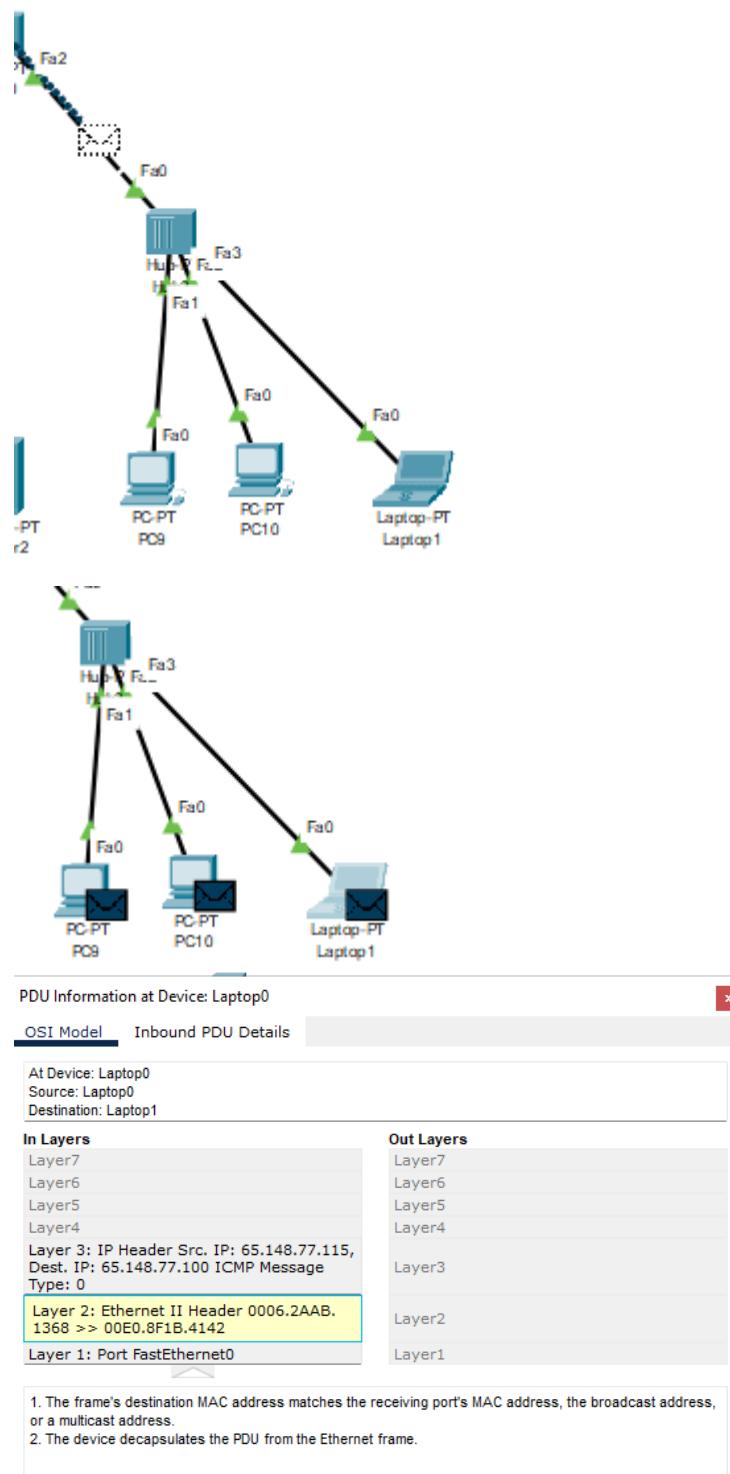
c. From Server0 to Server1.



PDU Information at Device: Server0	
OSI Model	Inbound PDU Details
<p>At Device: Server0 Source: Server0 Destination: Server1</p>	
<p><b>In Layers</b></p> <p>Layer7 Layer6 Layer5 Layer4 <b>Layer 3: IP Header Src. IP: 65.148.77.111, Dest. IP: 65.148.77.110 ICMP Message Type: 0</b> <b>Layer 2: Ethernet II Header 000C.CF80.0561 &gt;&gt; 000A.F332.073E</b> Layer 1: Port FastEthernet0</p>	
Out Layers	Layer7 Layer6 Layer5 Layer4 Layer3 Layer2 Layer1
<p>1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address. 2. The device decapsulates the PDU from the Ethernet frame.</p>	

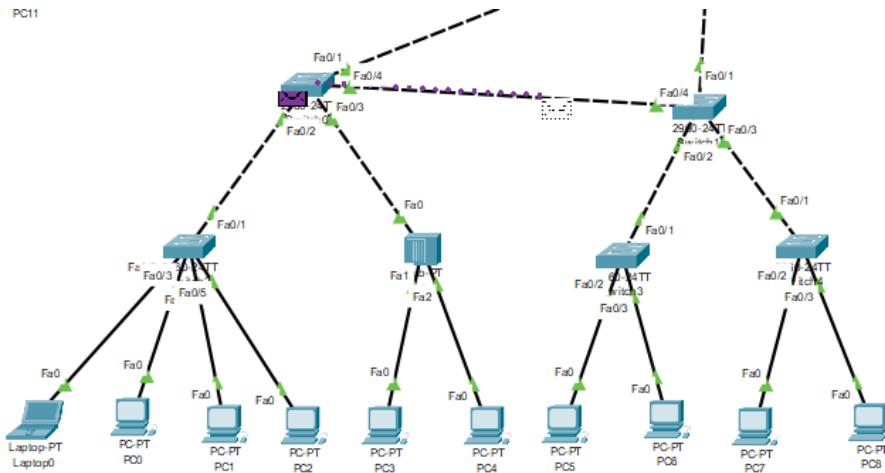
d. From Laptop0 to Laptop1.



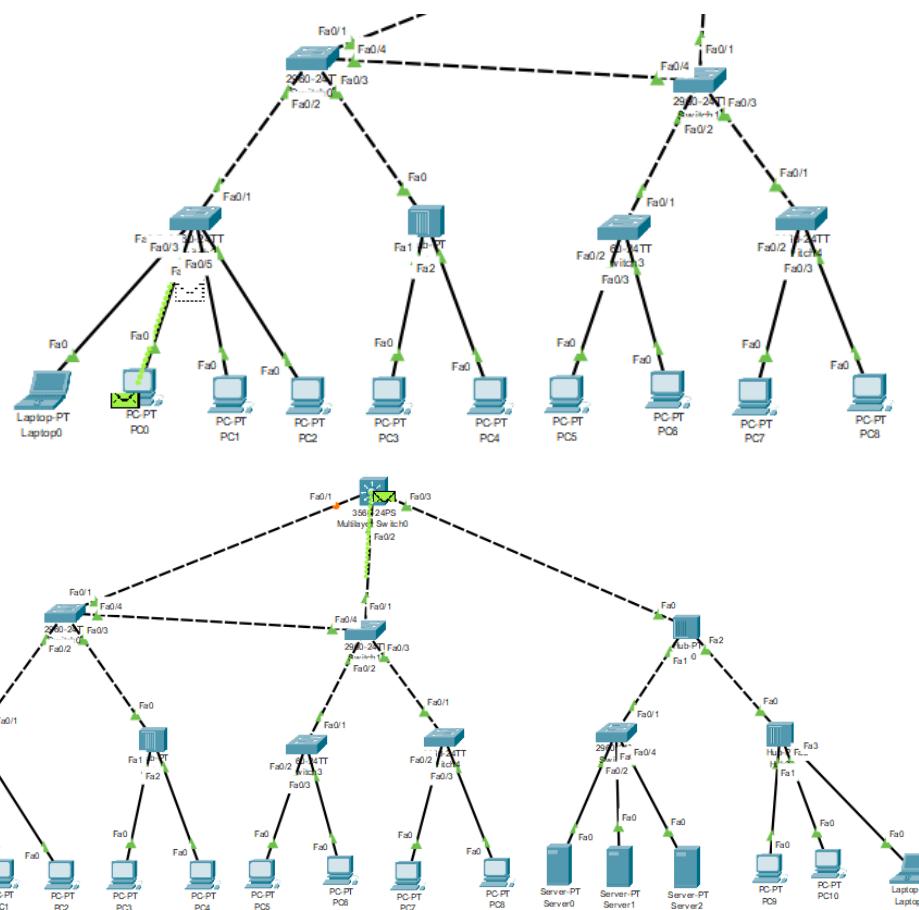


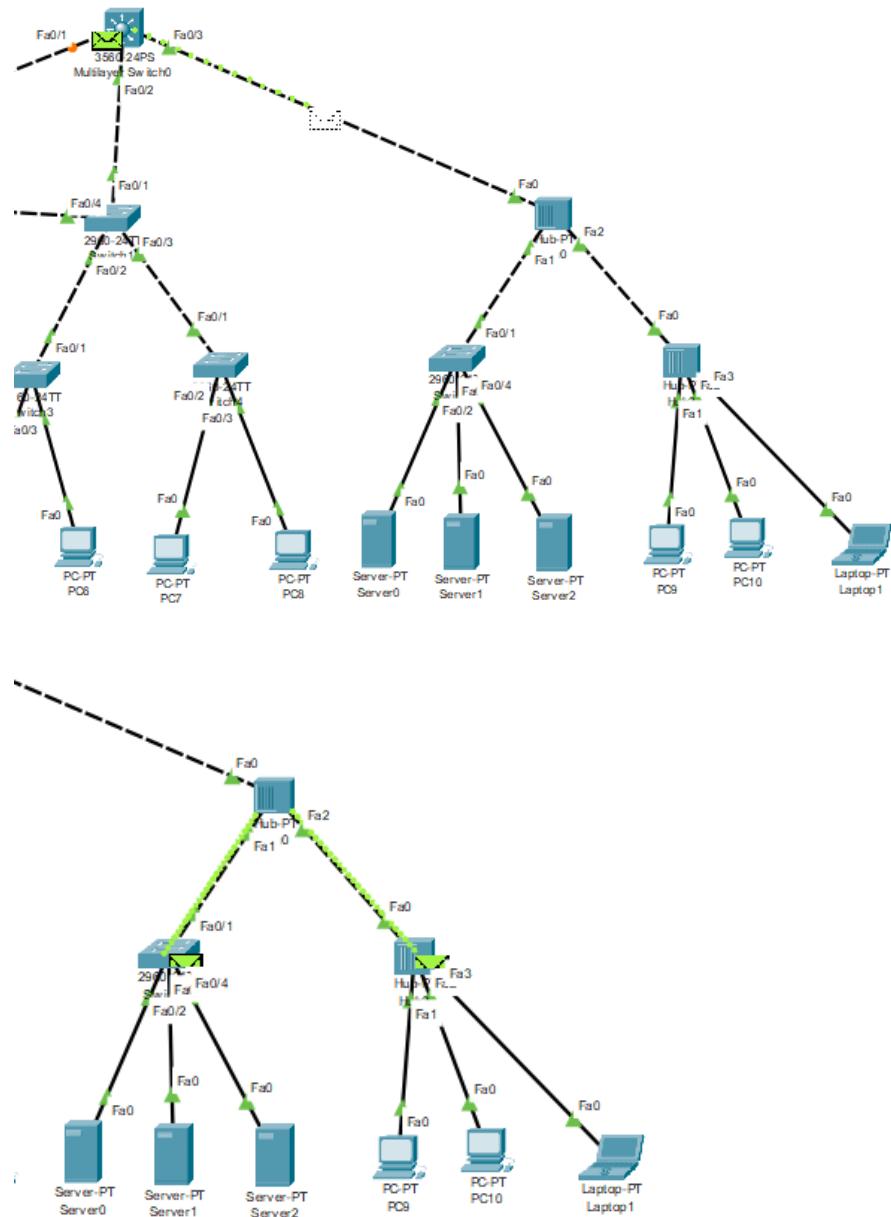
**Hint:** Observe that at first, the transmission behavior is pure broadcast, and then it starts learning.  
 5. We Examine the operation of the spanning tree algorithm. When we interconnect switches 0 and 1

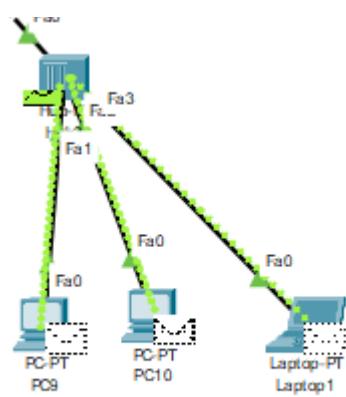
a. From PC1 to PC7



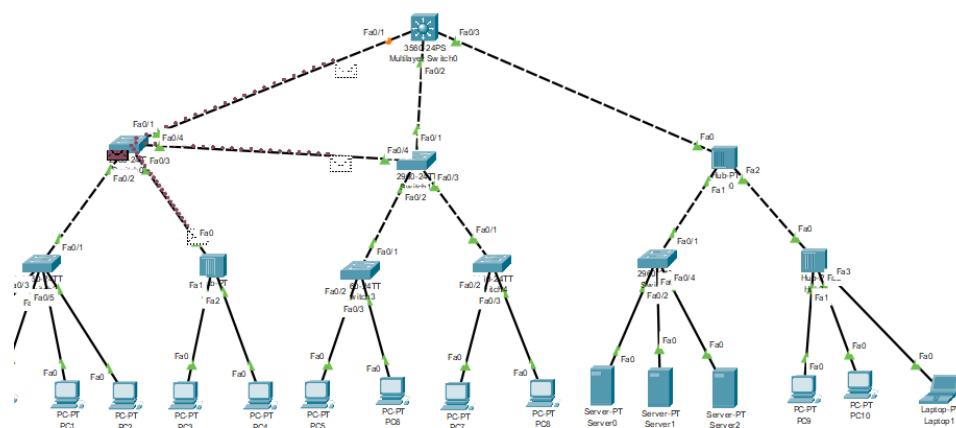
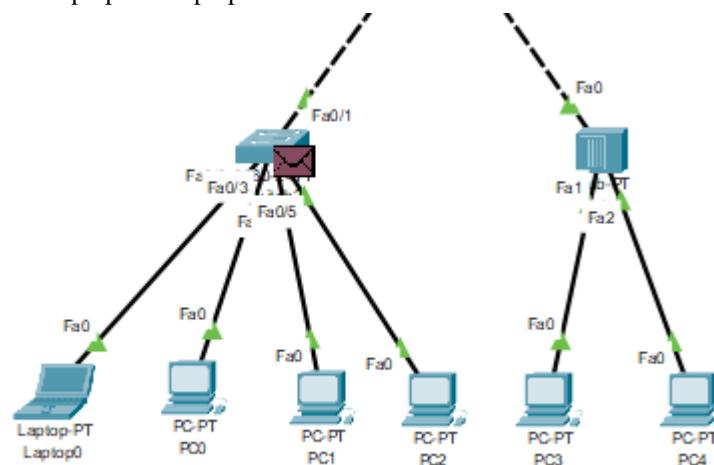
b. . b. From PC0 to PC9

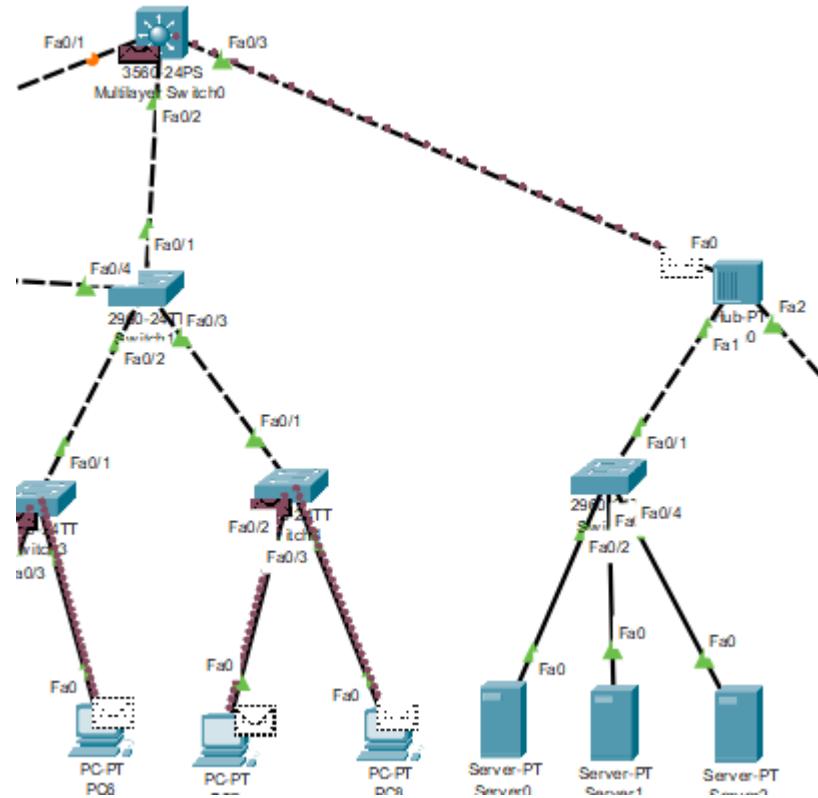
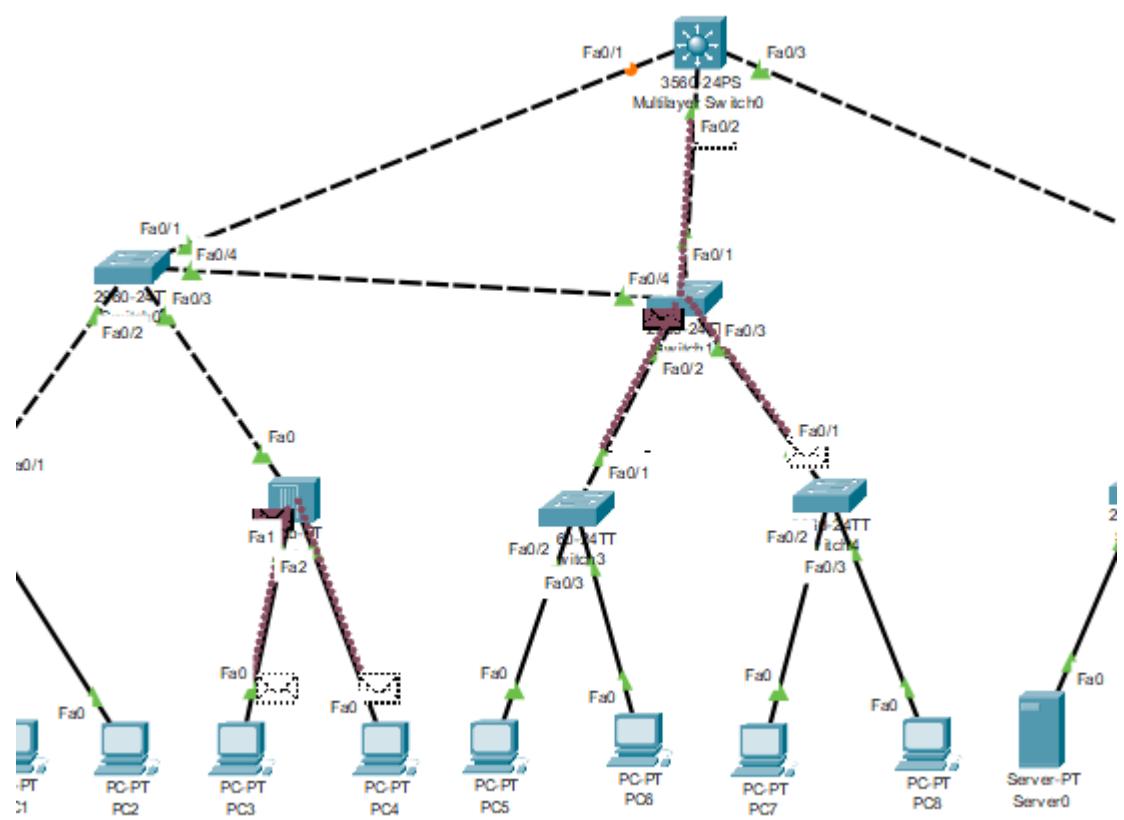


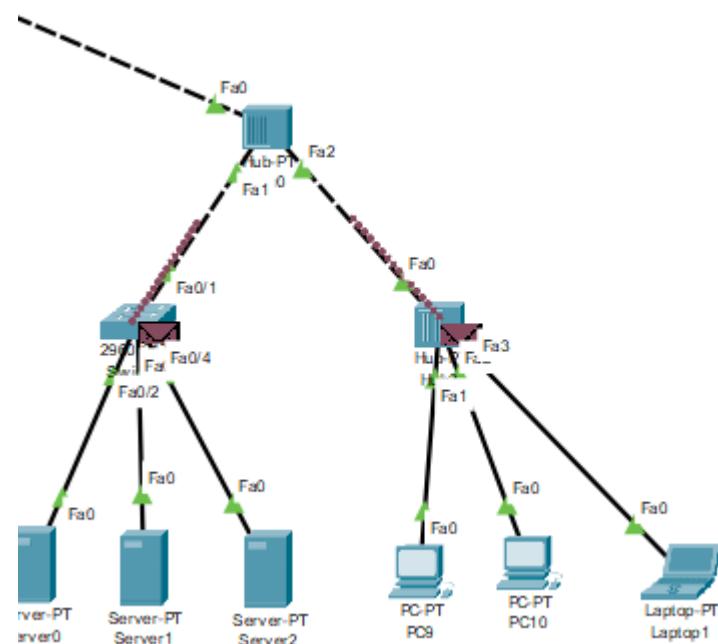
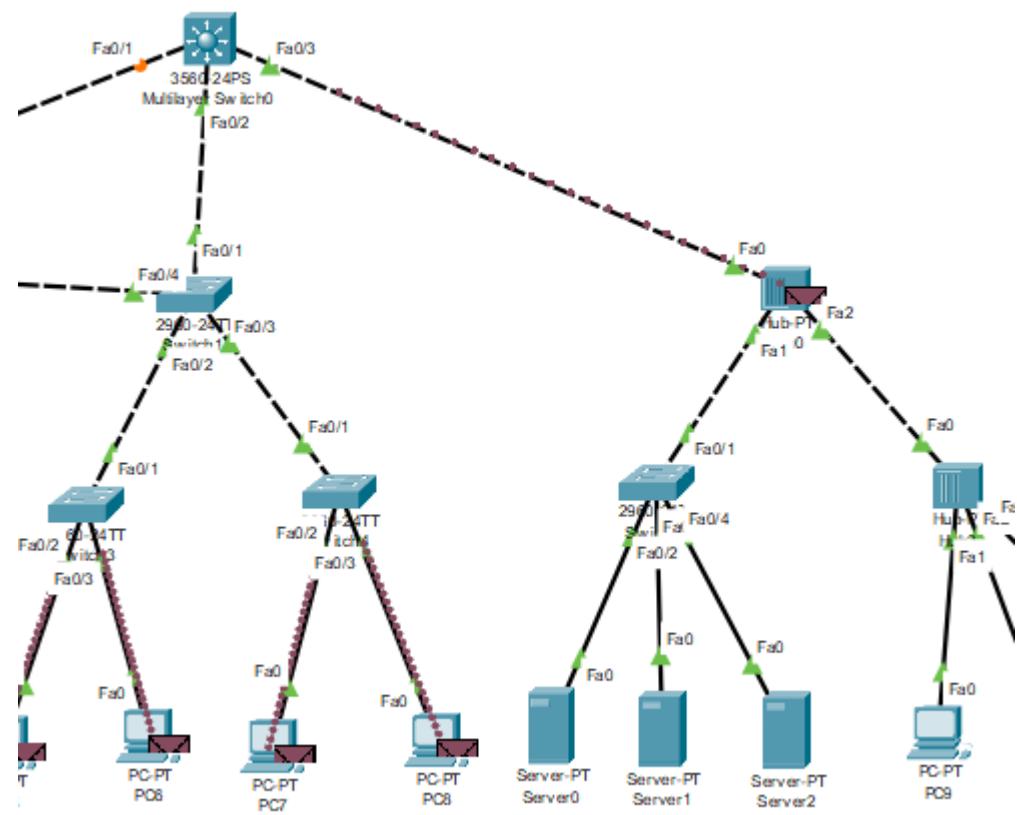


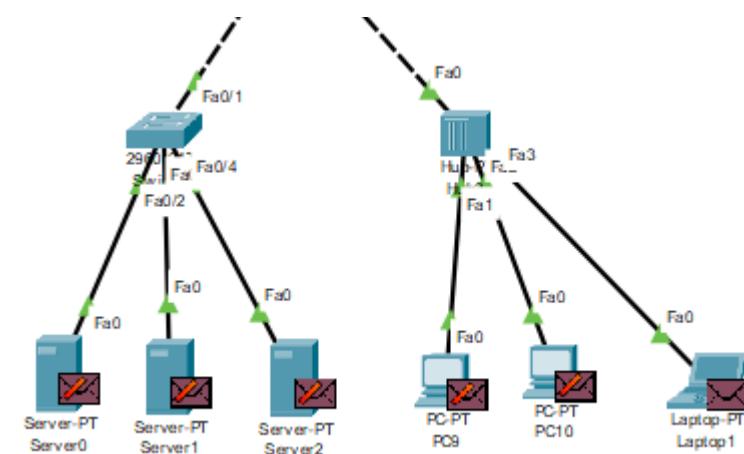


c. . . From Laptop0 to Laptop1.

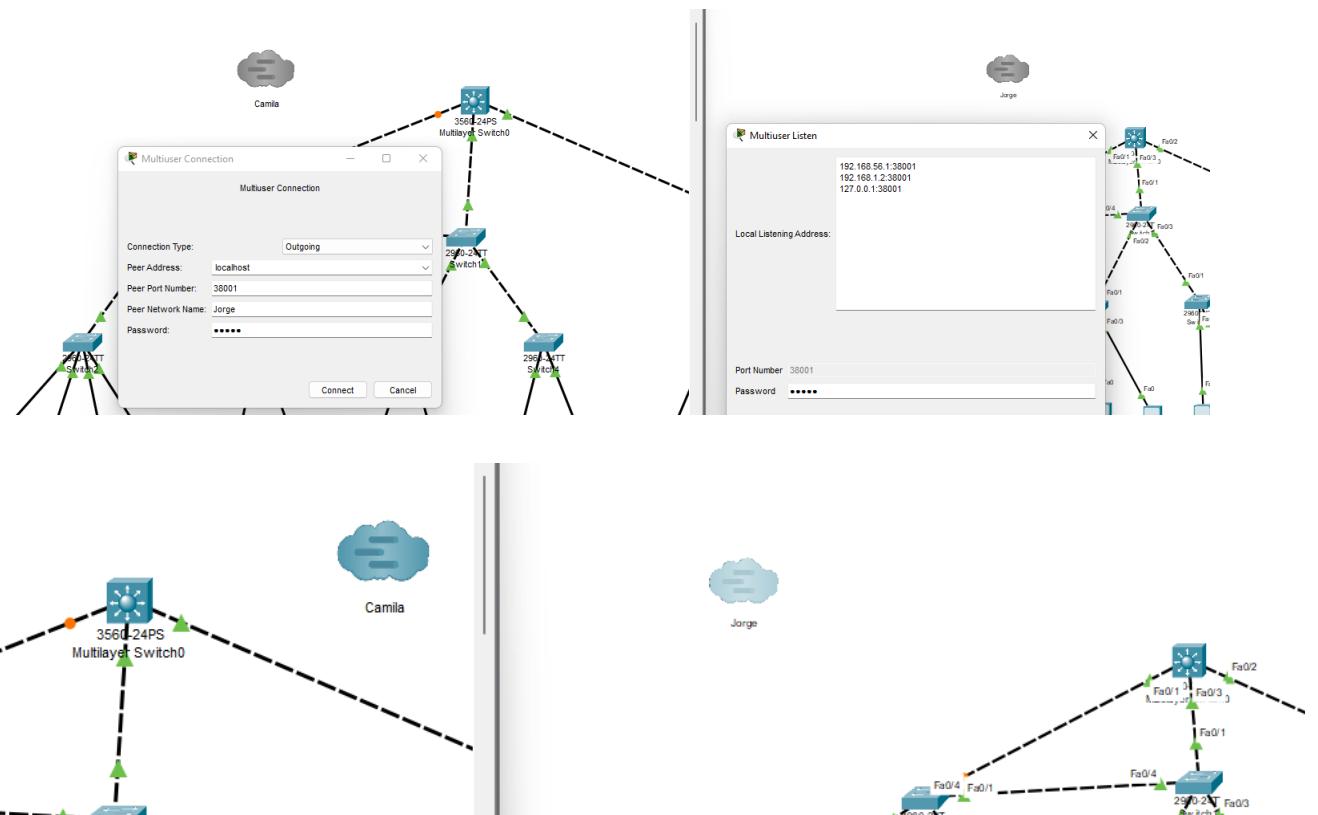








6. Now We Merge the project files of the team members.



Laptop0

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 65.148.77.133

Pinging 65.148.77.133 with 32 bytes of data:

Reply from 65.148.77.133: bytes=32 time=87ms TTL=128
Reply from 65.148.77.133: bytes=32 time=22ms TTL=128
Reply from 65.148.77.133: bytes=32 time=22ms TTL=128
Reply from 65.148.77.133: bytes=32 time=23ms TTL=128

Ping statistics for 65.148.77.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 87ms, Average = 38ms

C:\>ping 65.148.77.103

Pinging 65.148.77.103 with 32 bytes of data:

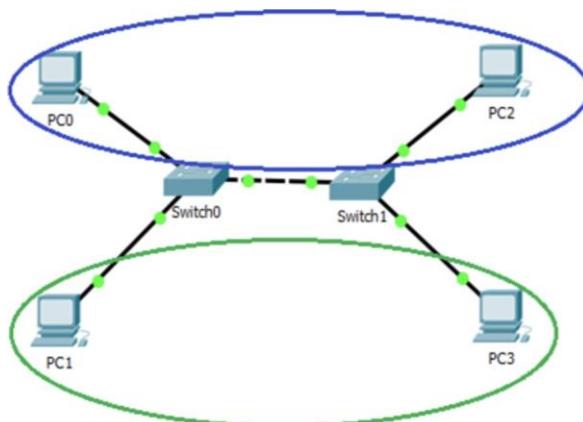
Reply from 65.148.77.103: bytes=32 time<1ms TTL=128
Reply from 65.148.77.103: bytes=32 time=1ms TTL=128
Reply from 65.148.77.103: bytes=32 time=10ms TTL=128
Reply from 65.148.77.103: bytes=32 time<1ms TTL=128

Ping statistics for 65.148.77.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```

#### 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	fdmi-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.

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 adres
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       fffff.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

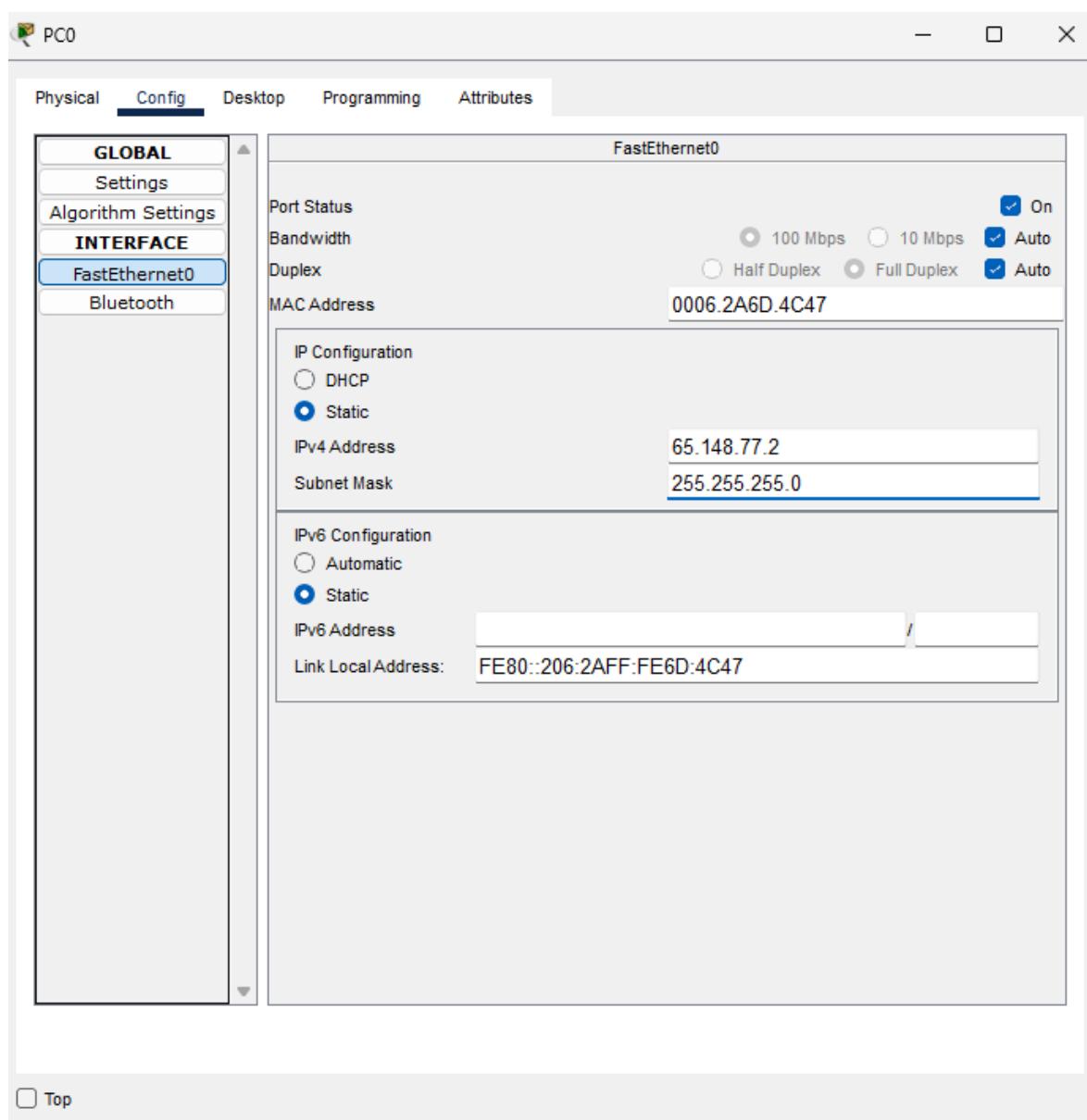


Figure 21. Assigning IP and Subnet Mask to PC0

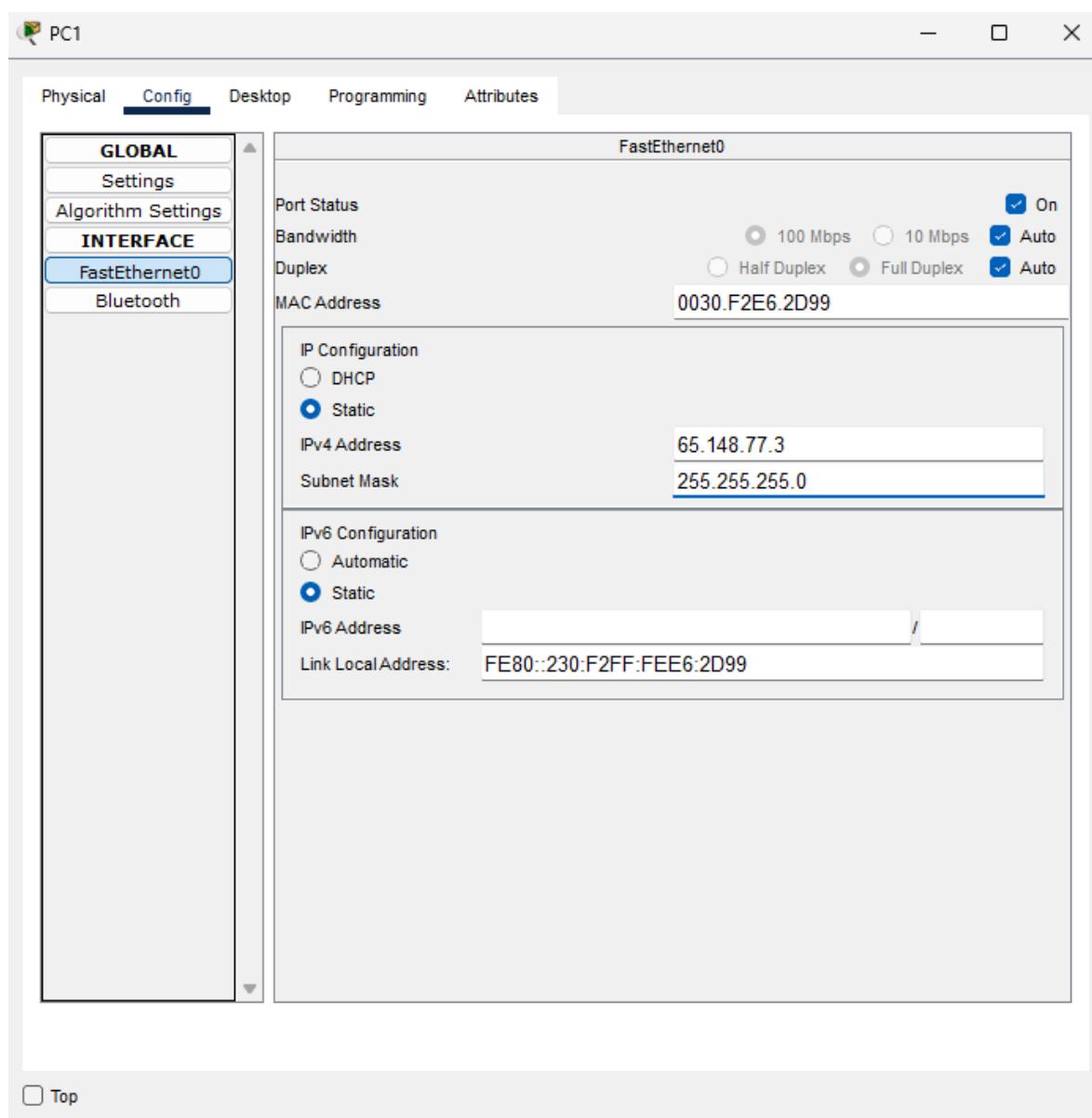


Figure 22. Assigning IP and Subnet Mask to PC1

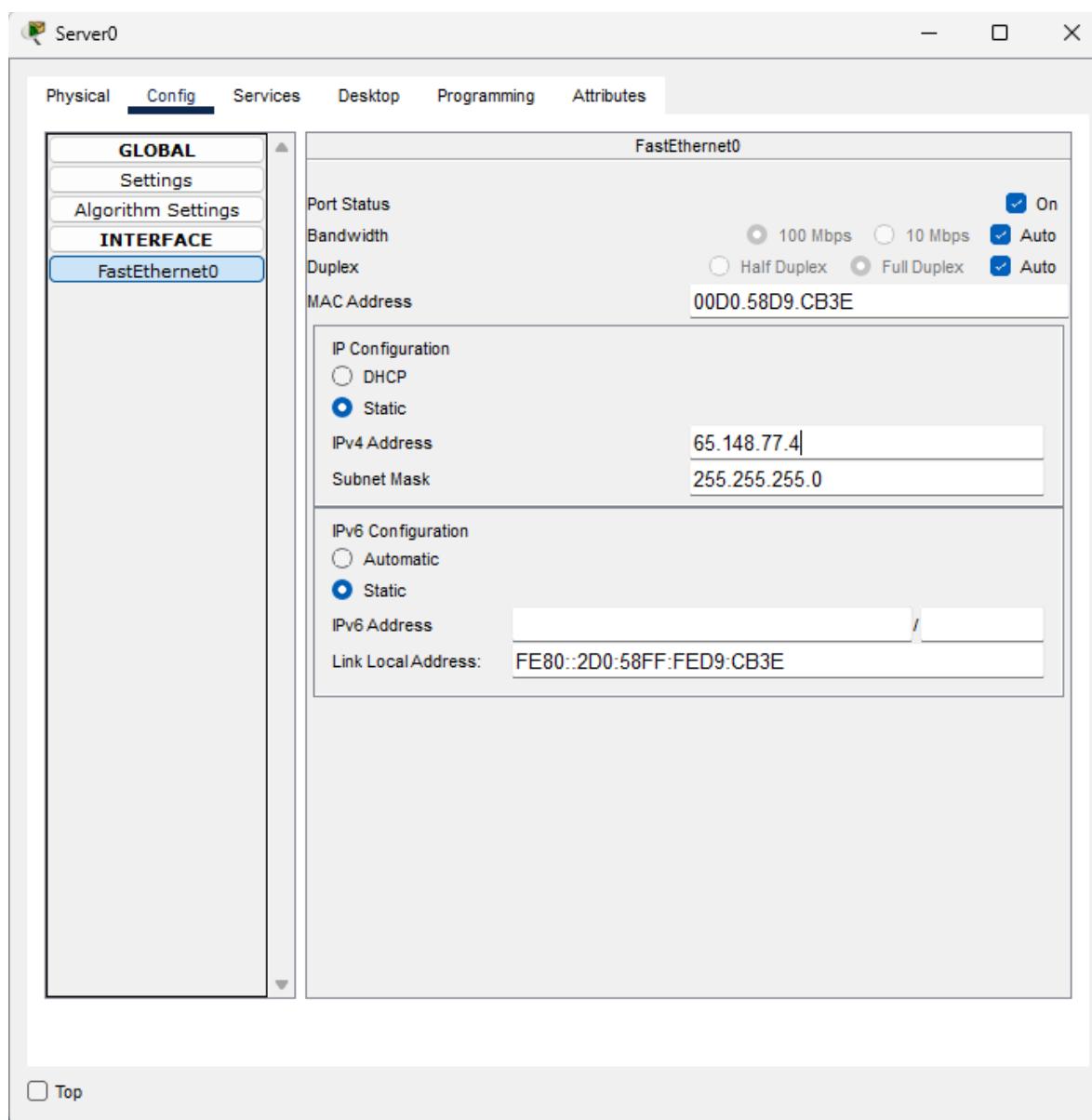
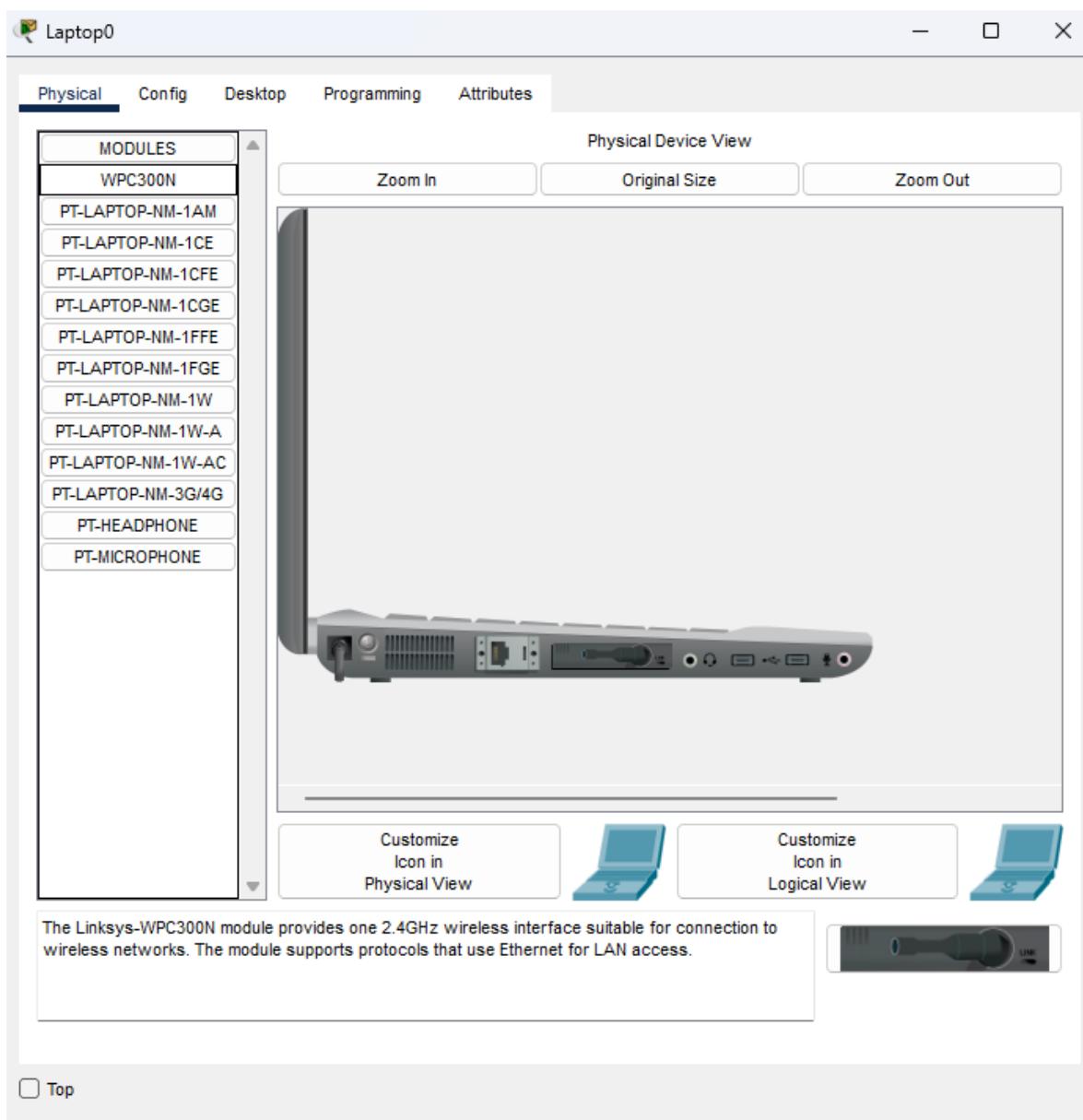


Figure 23. Assigning IP and Subnet Mask to Server0

- 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

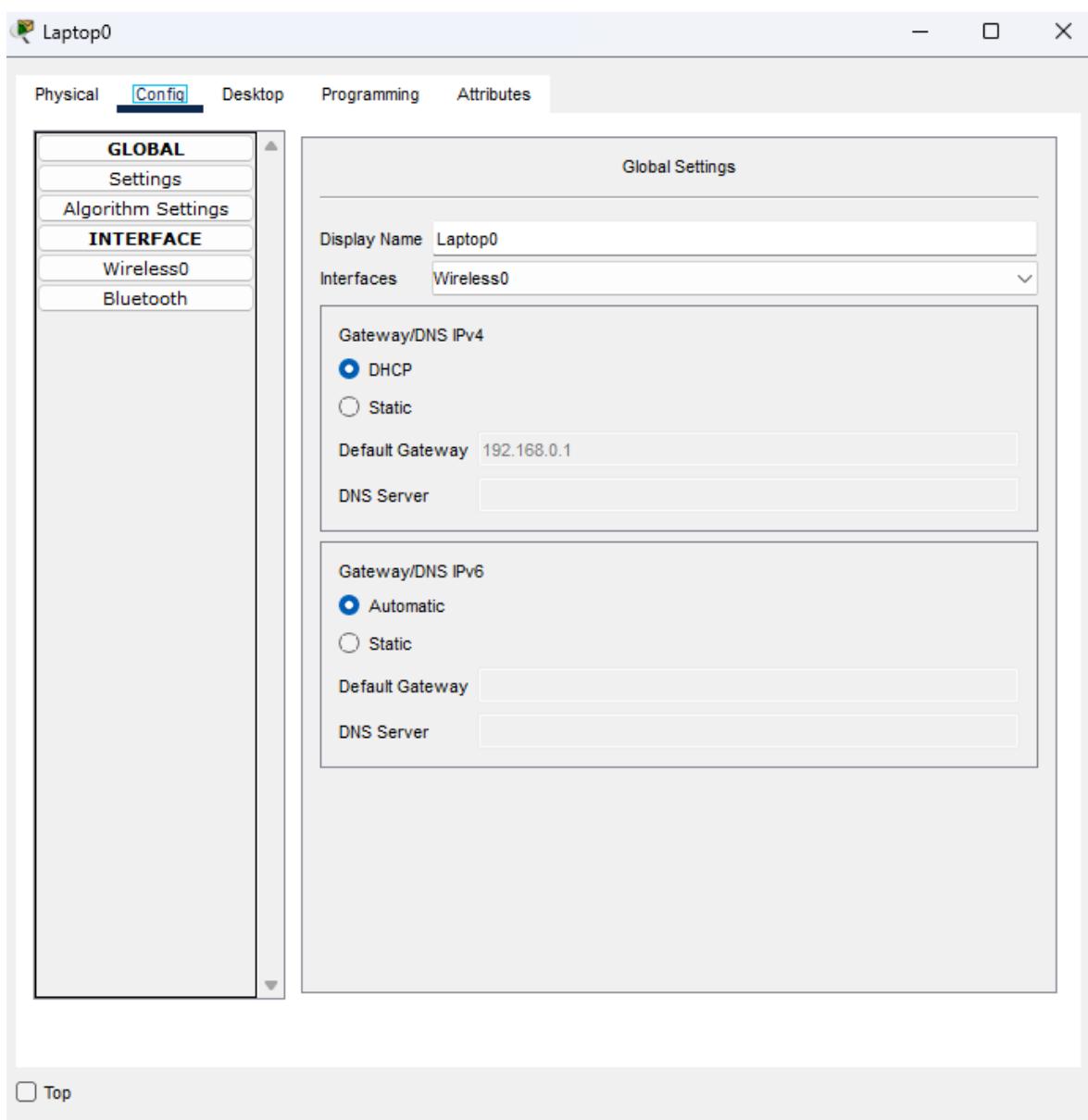


Figure 25. Configuring DHCP in the laptops

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

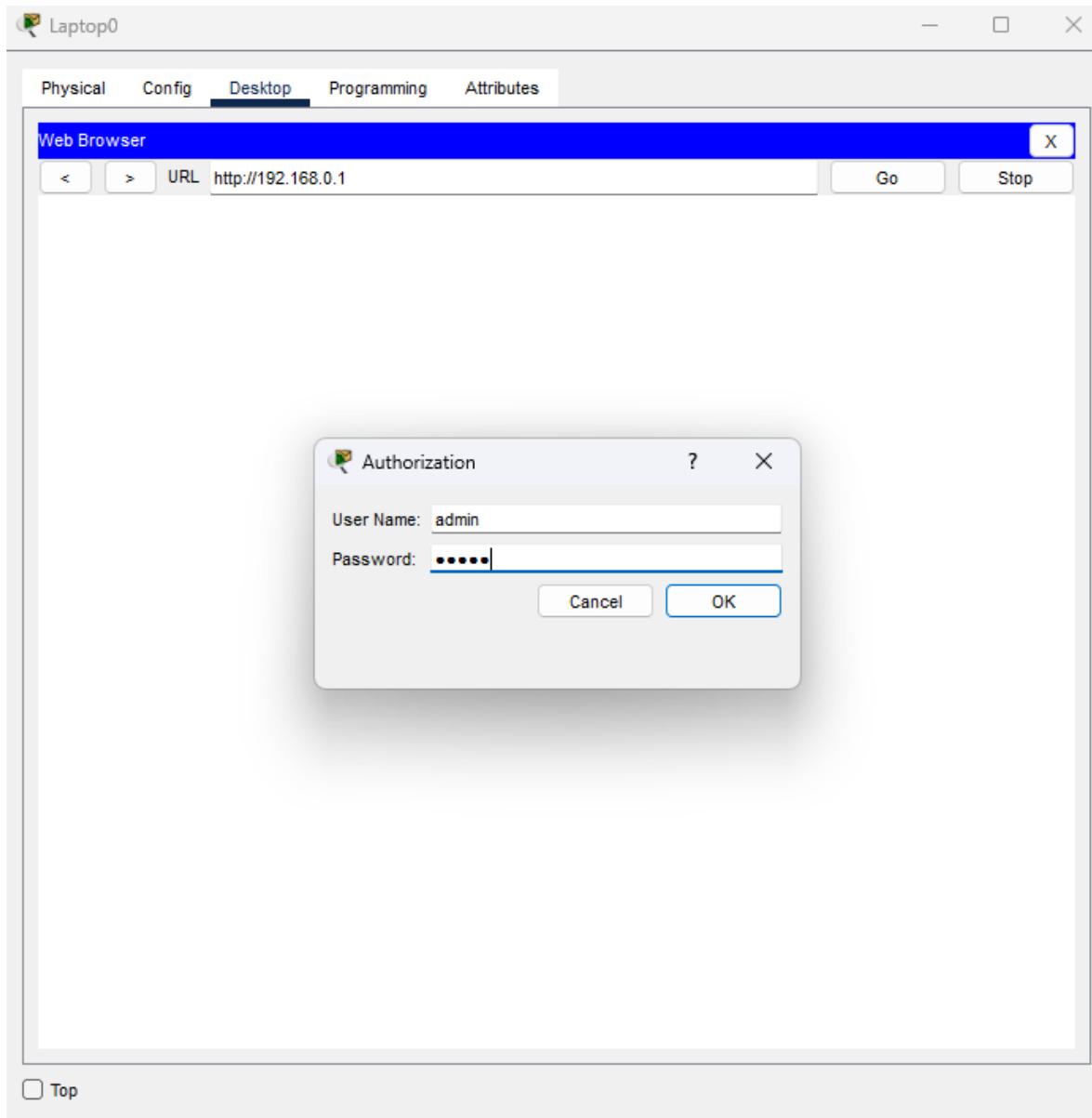


Figure 26. Authenticating to Configure the Router

- 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

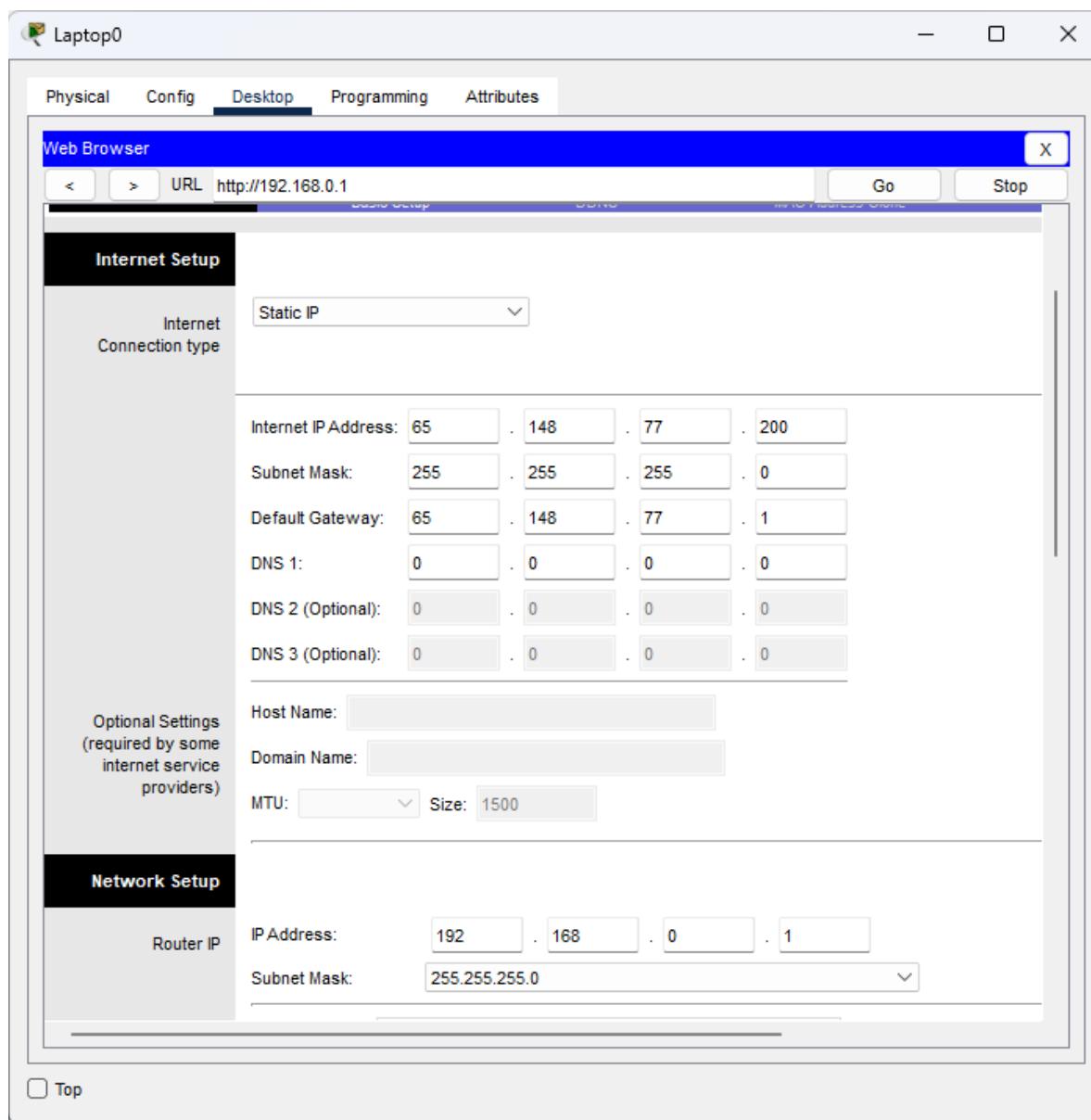


Figure 27. Internet Setup of the Wireless Router

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

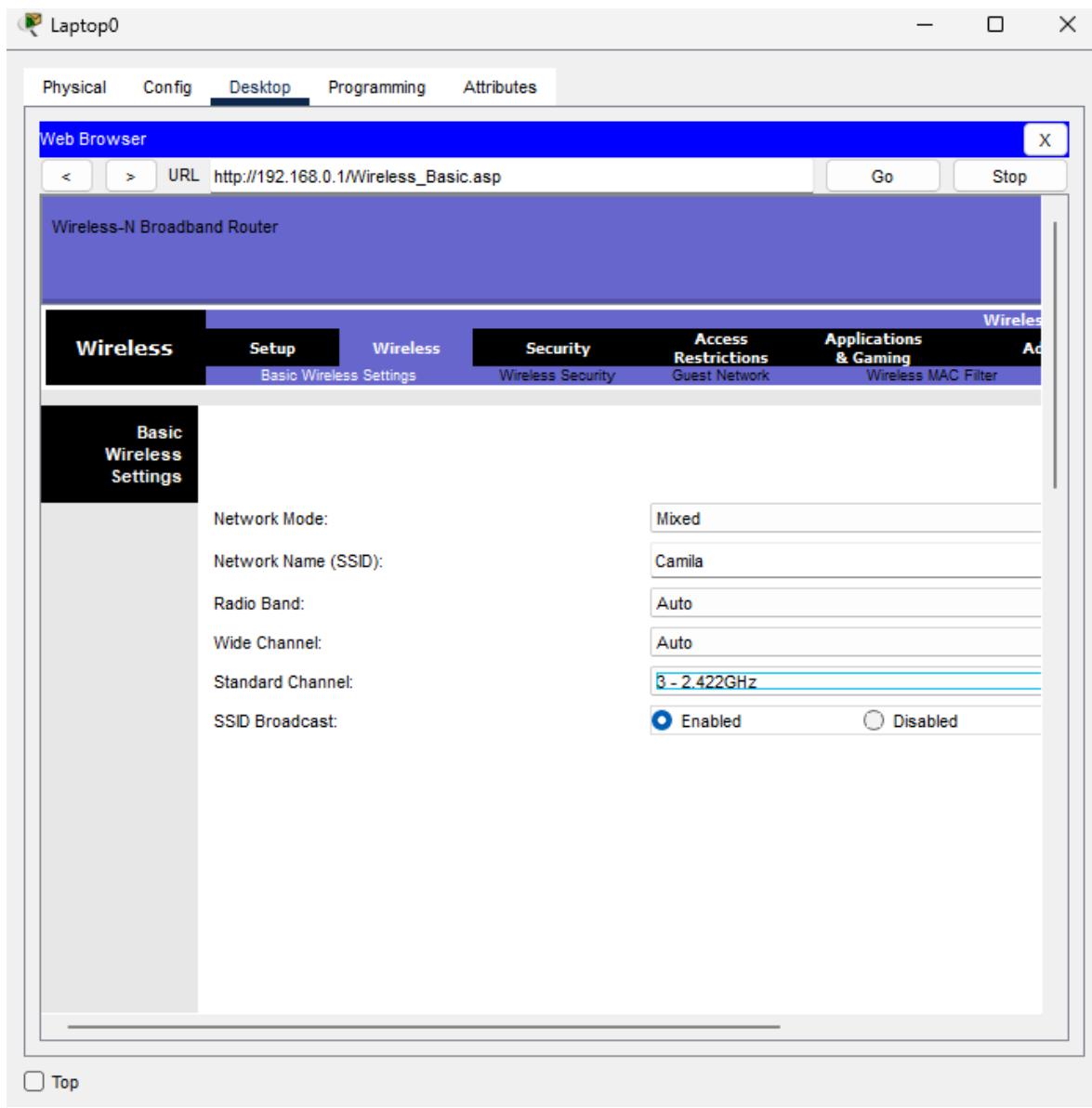


Figure 28. Basic Wireless Settings of the router

- 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

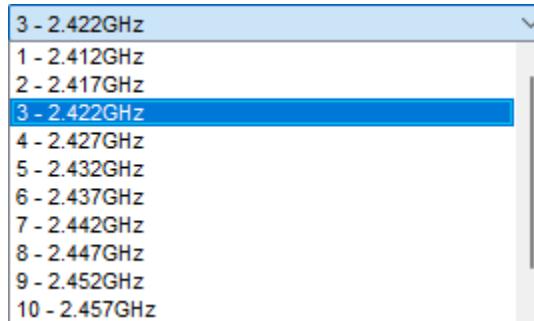


Figure 29. Router Channels Options

- 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)

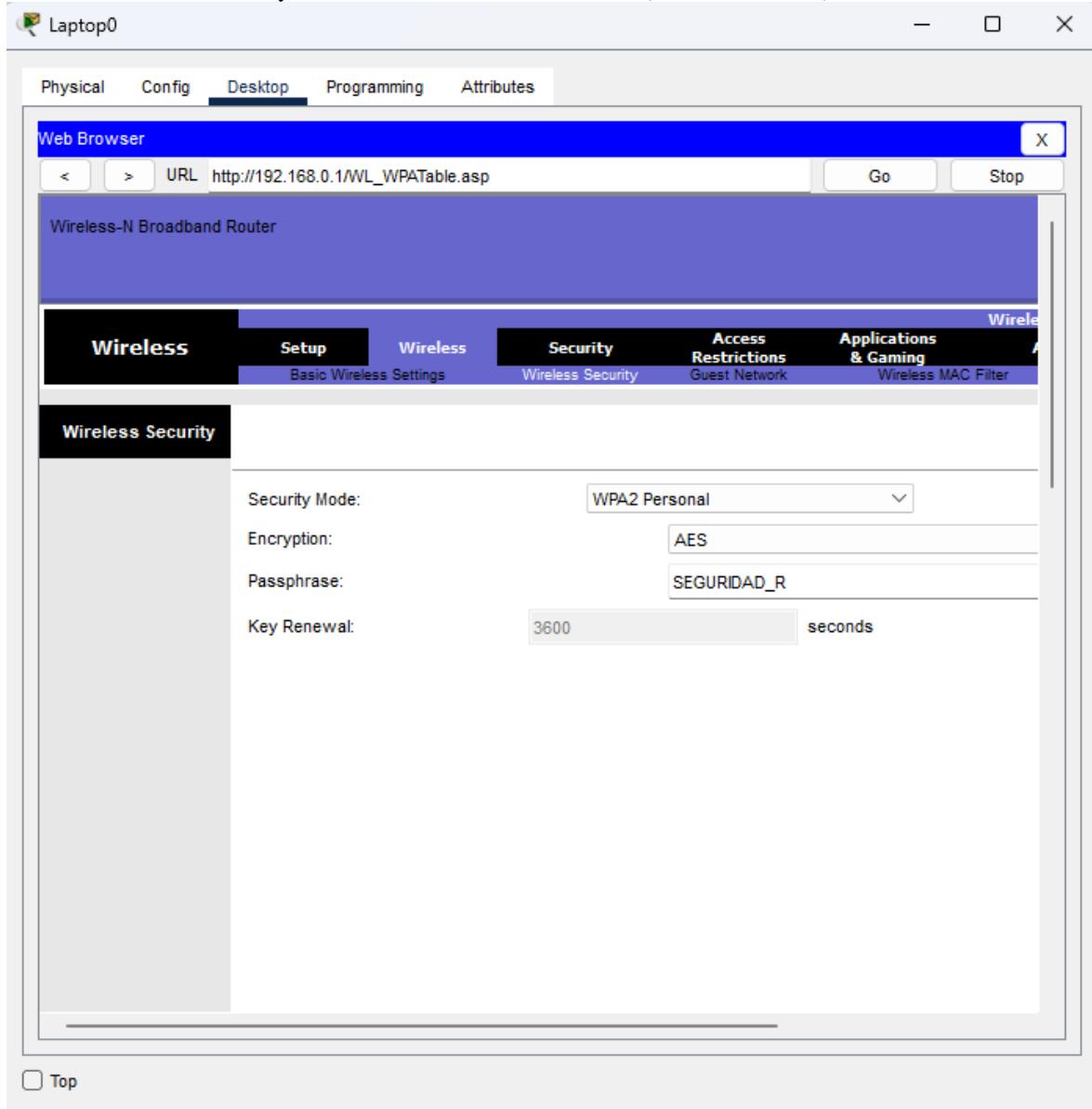


Figure 30. Wireless Security of the router

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

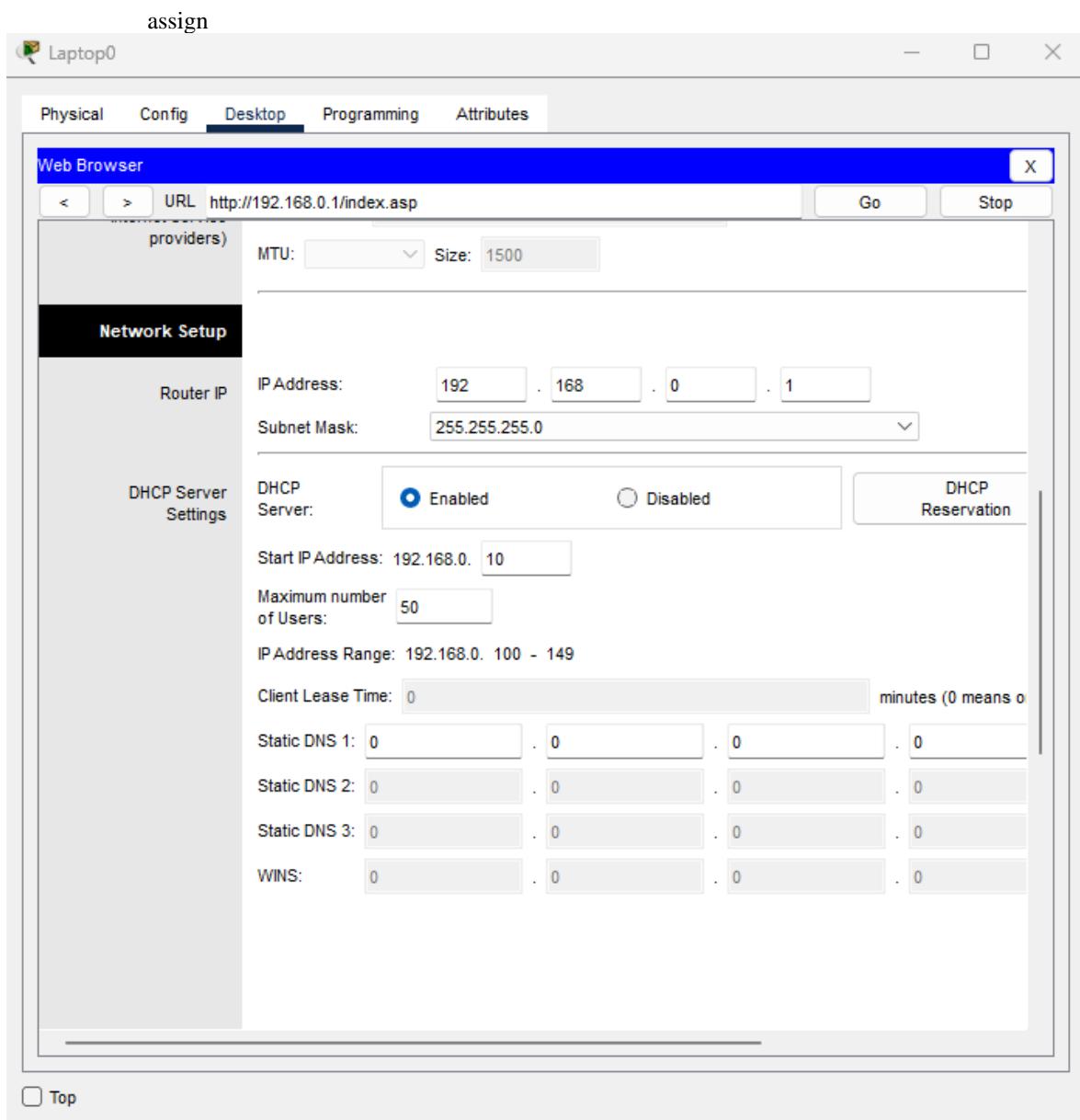


Figure 31. Configuring and Assigning IP Address Range on the Wireless Router

- 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)

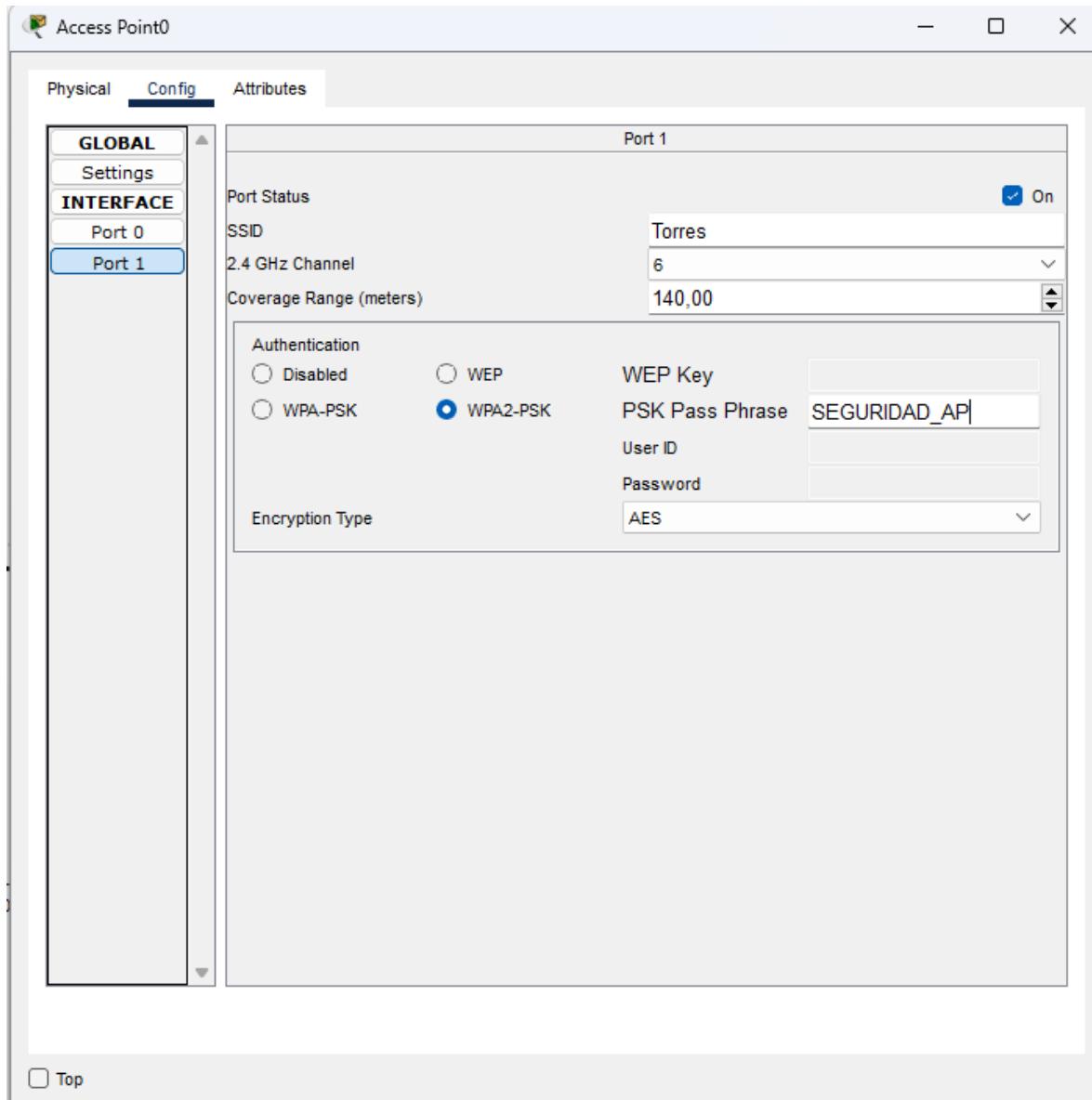


Figure 32. Configuring Access Point

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

configured earlier (*Image 8*)

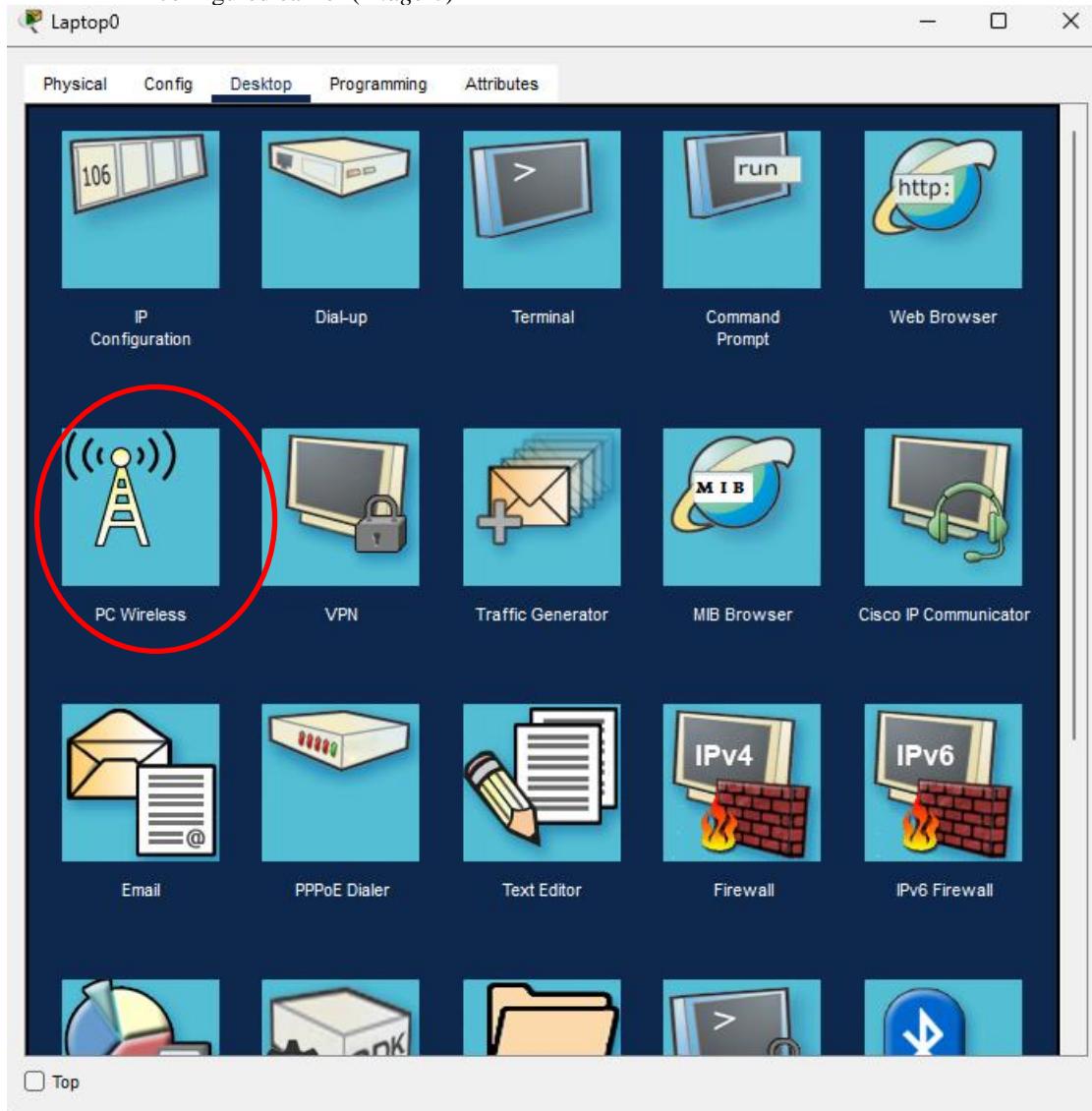


Figure 33. Opening PC Wireless from Laptop0

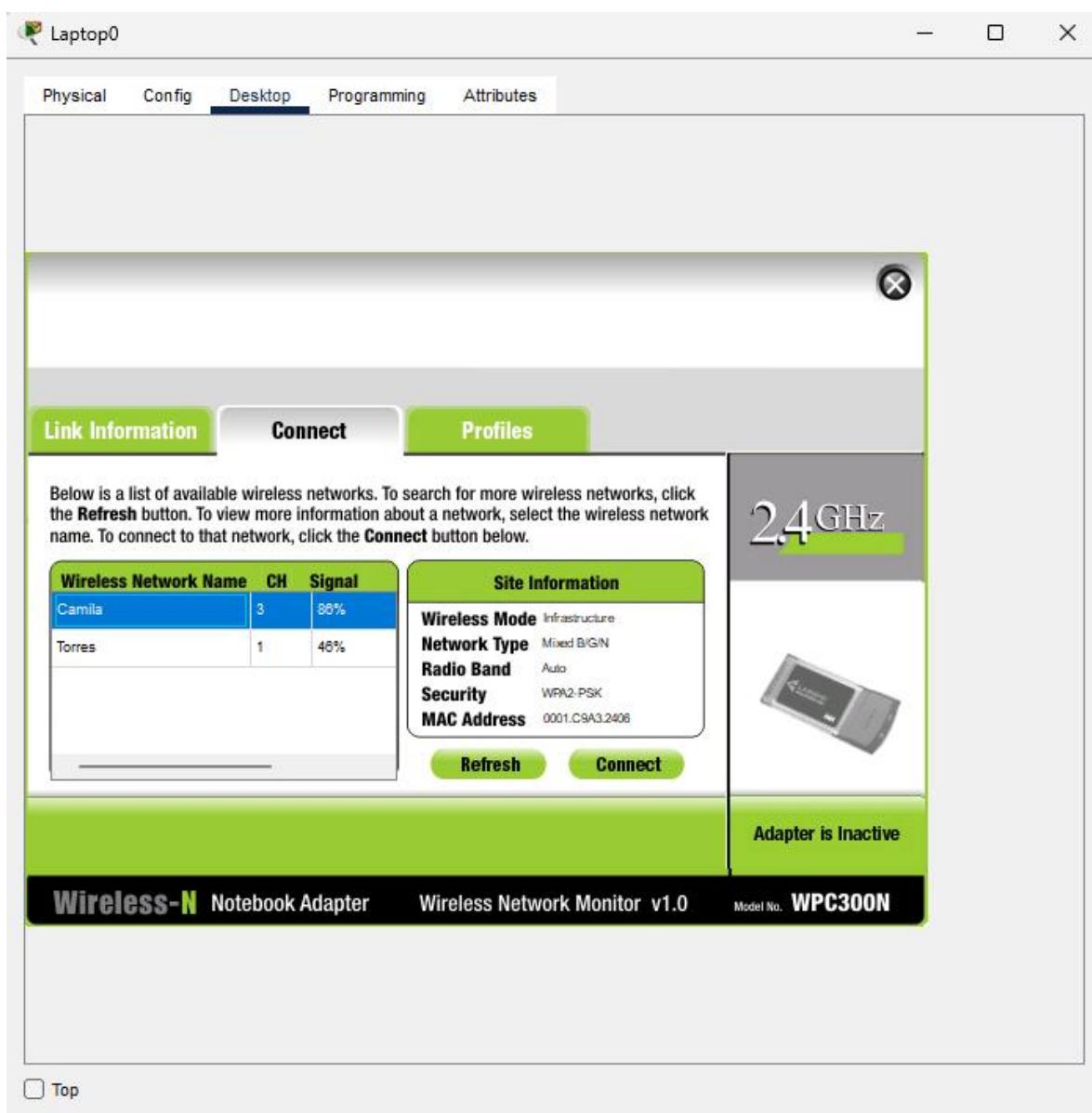


Figure 34. Connecting Laptop0 to the Wireless Router

- We enter the router's access key and connect

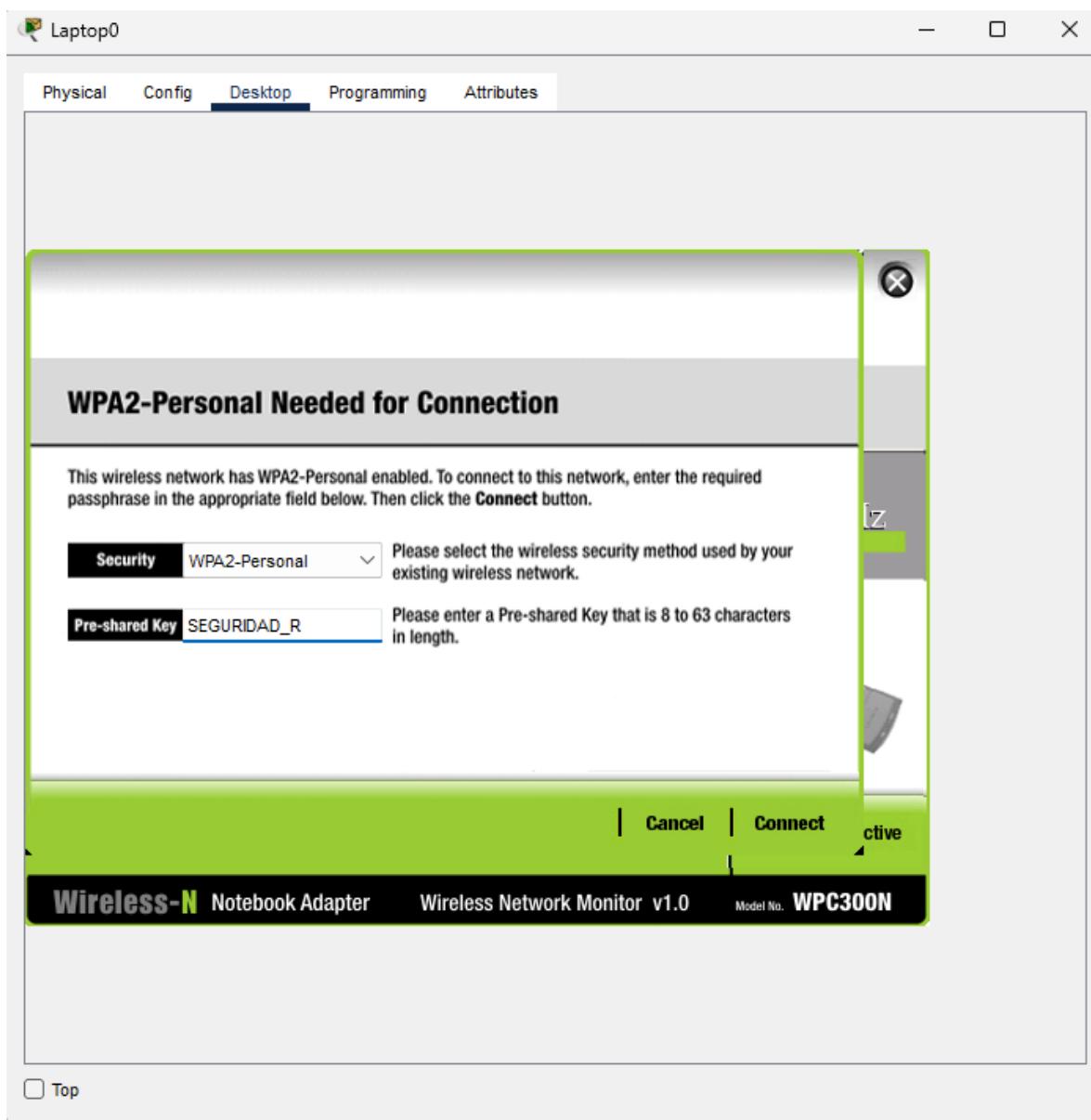


Figure 35. Connecting to the Wireless Router from Laptop0

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

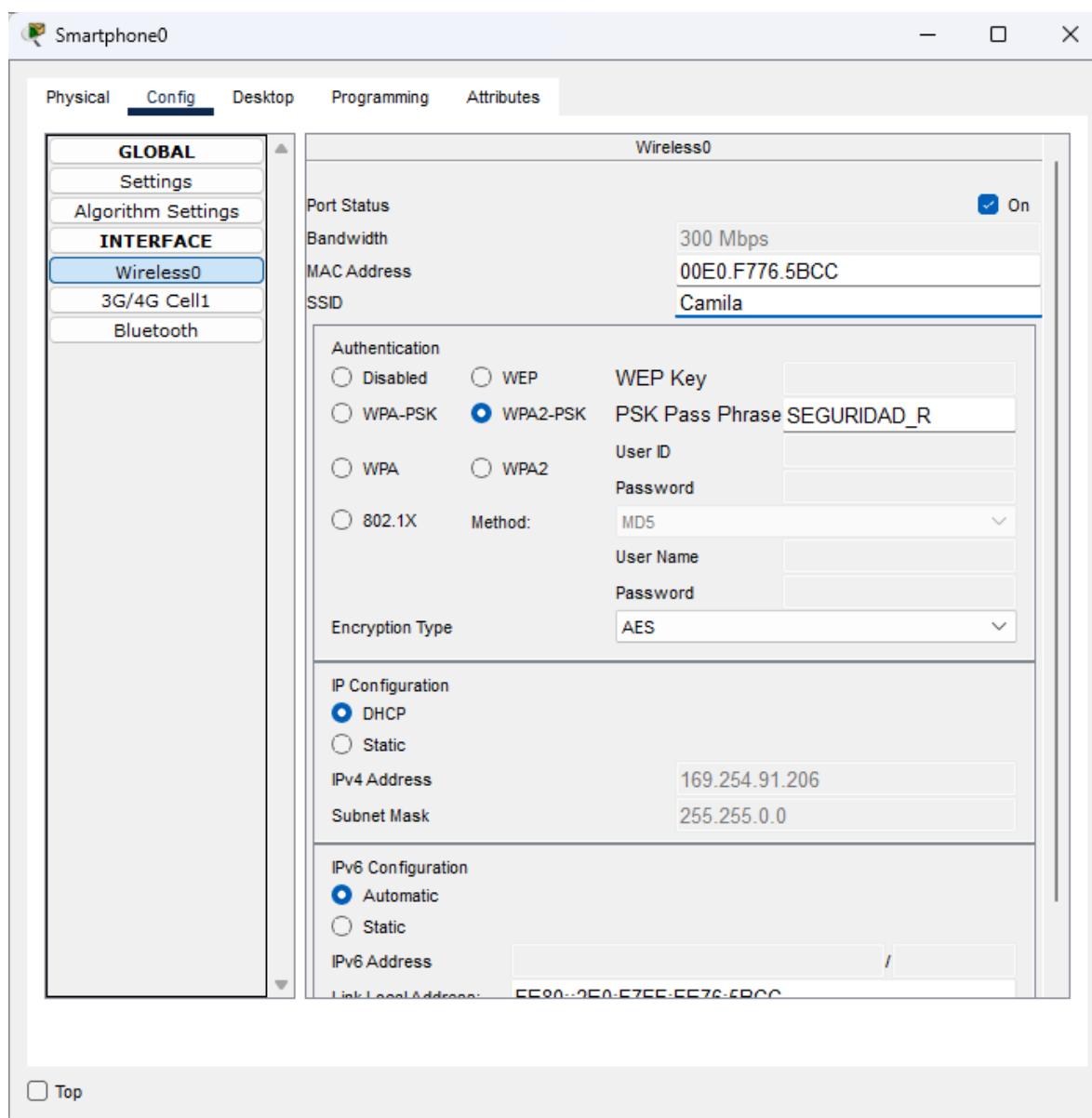


Figure 36. Configuring SmartPhone0 to Establish Connection with the Wireless Router

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

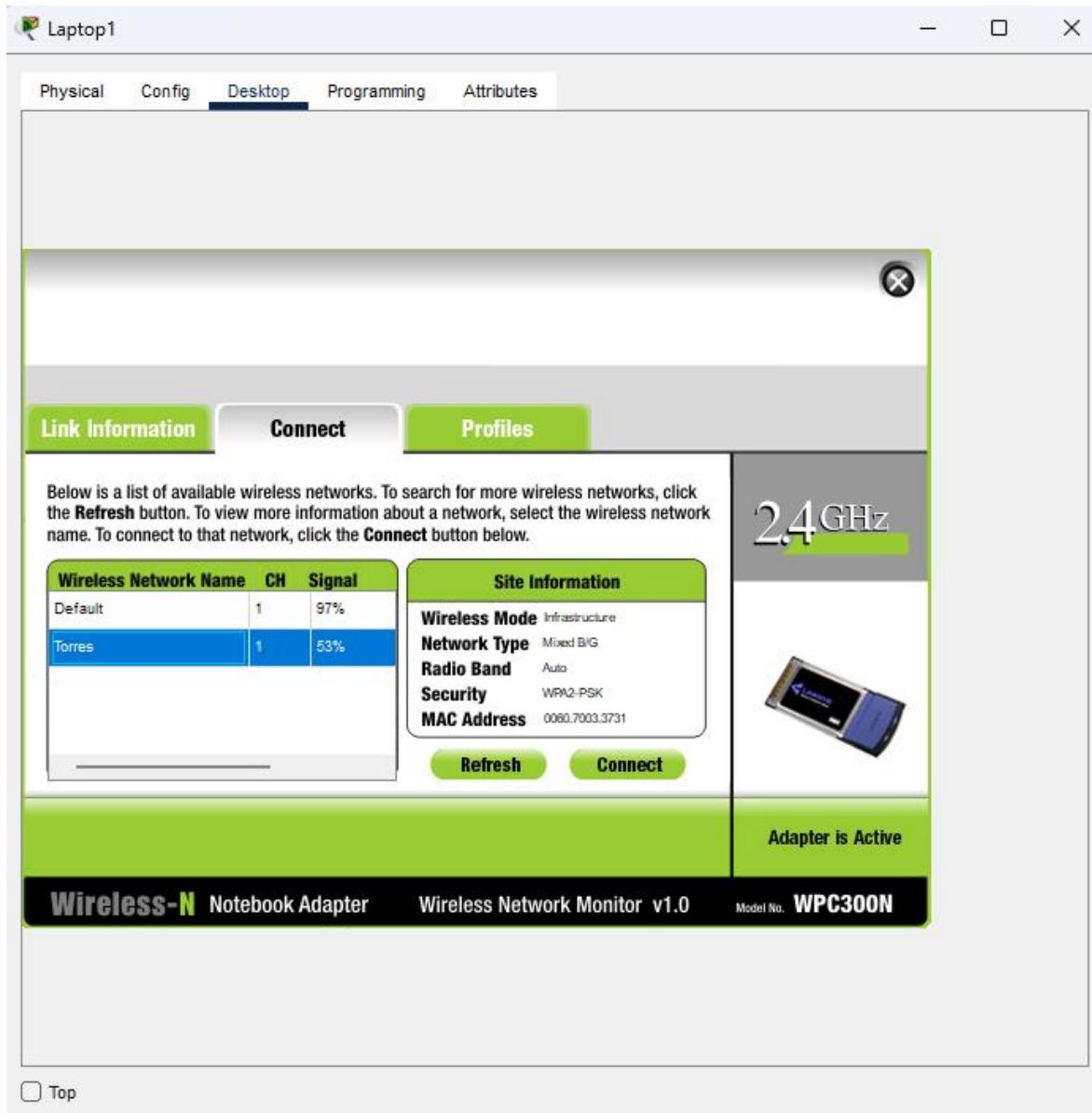


Figure 37. Connecting Laptop1 to Access Point

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

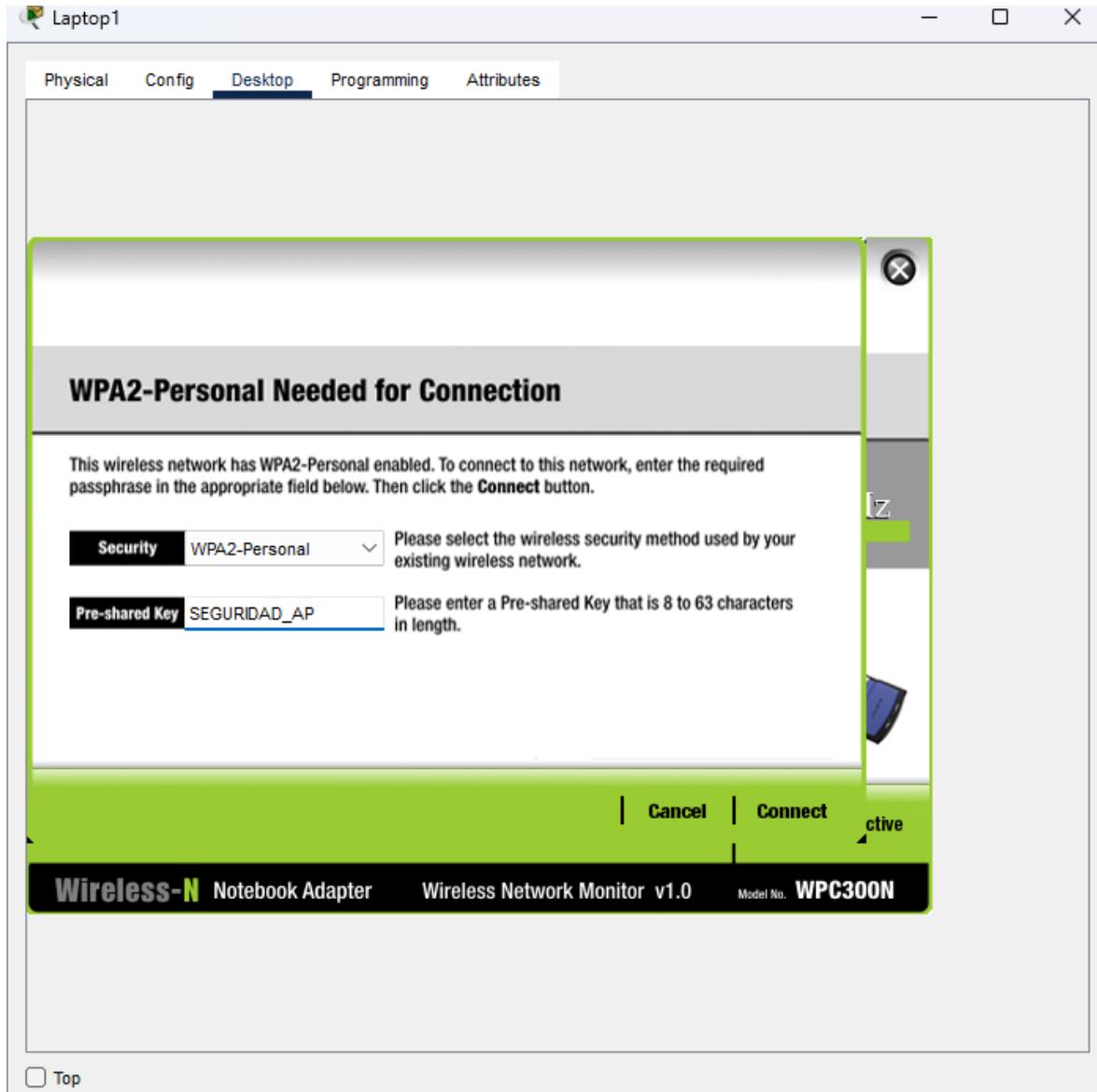


Figure 38. Connecting to Access Point from Laptop1

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

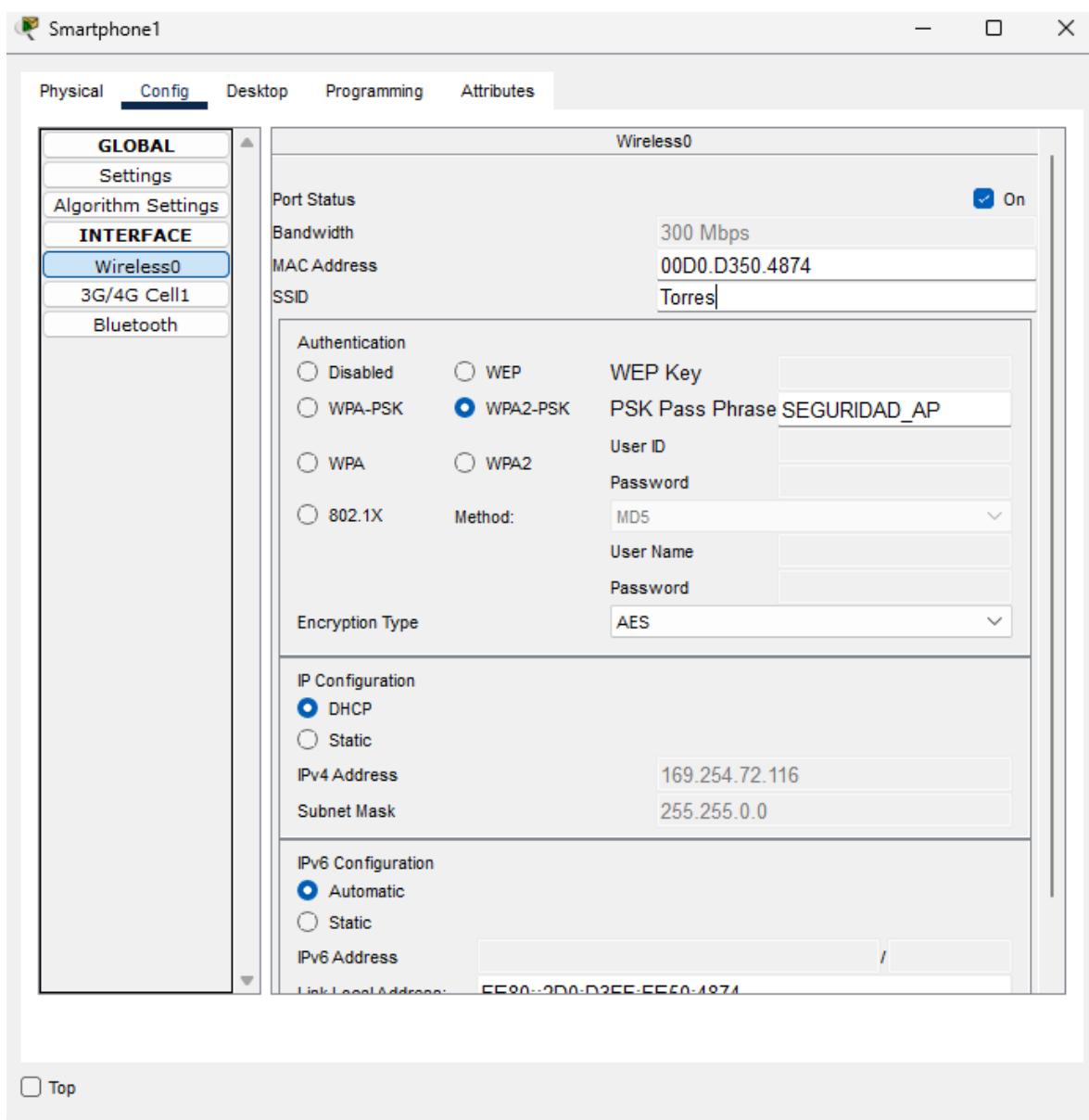


Figure 39. Configuring SmartPhone1 to Connect to the Access Point

- 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

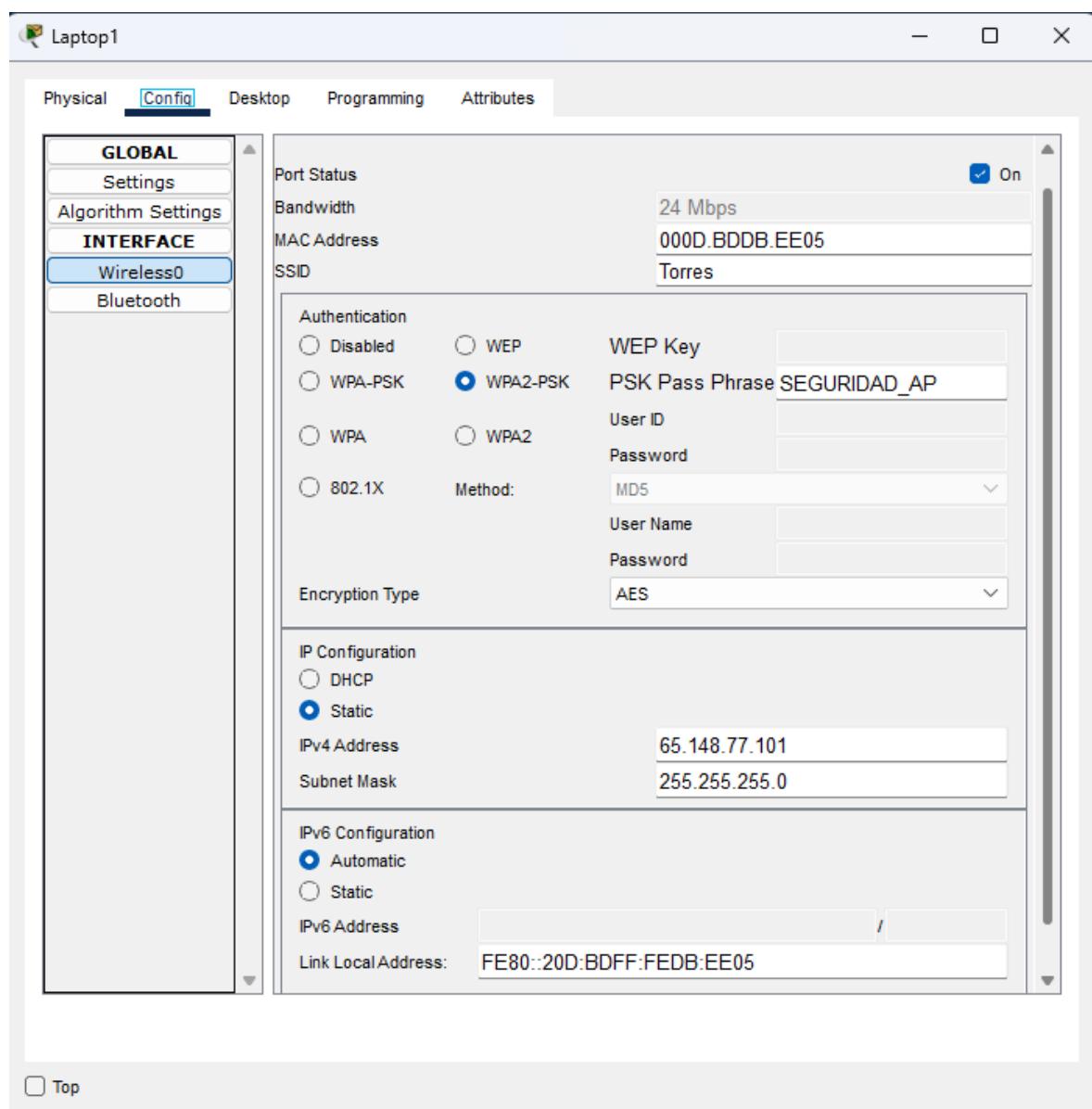


Figure 40. Assigning Static IP and Subnet Mask to Laptop1

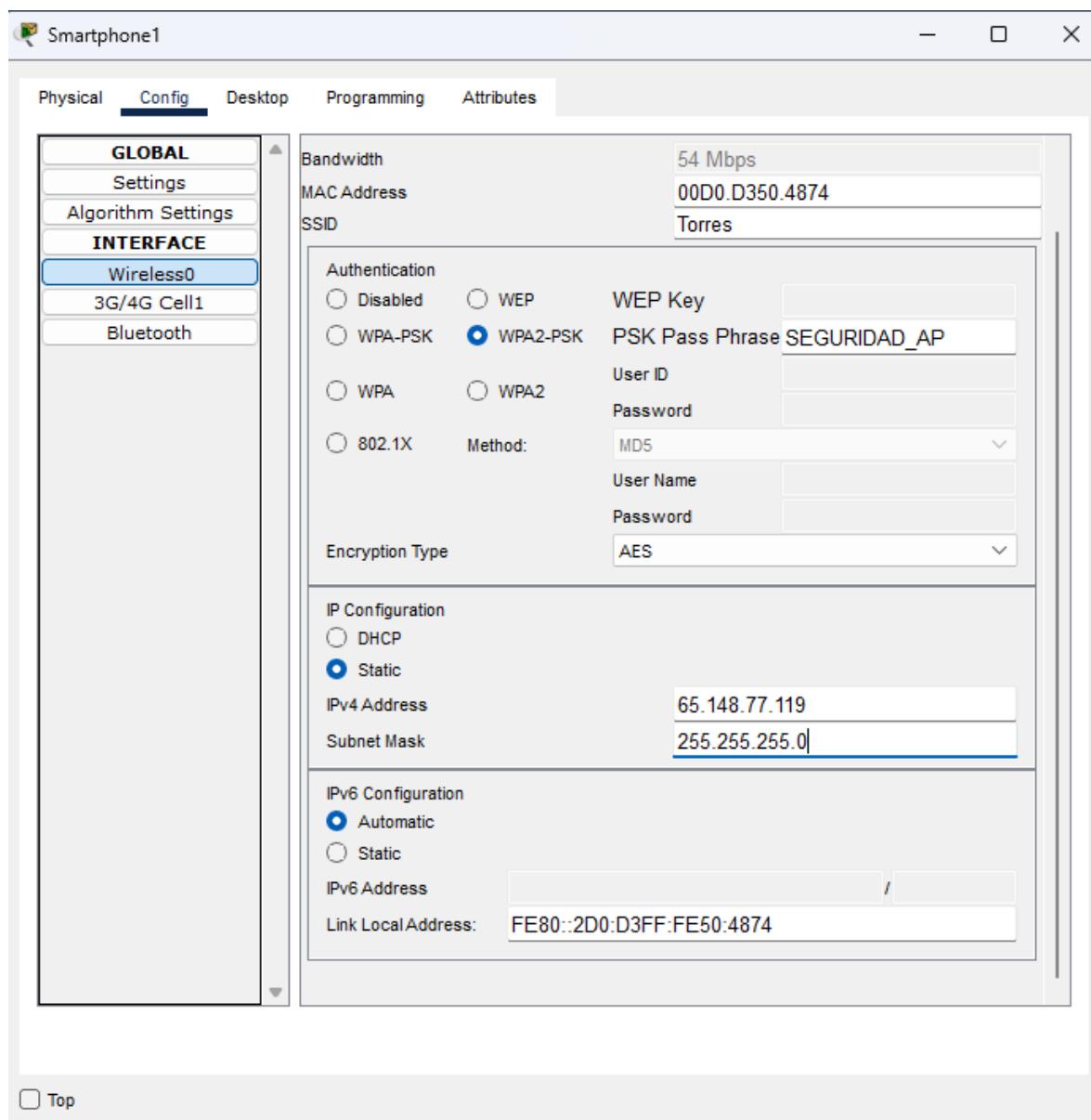


Figure 41. Assigning Static IP and Subnet Mask to Smartphone1

- We obtain our corrected and completed network

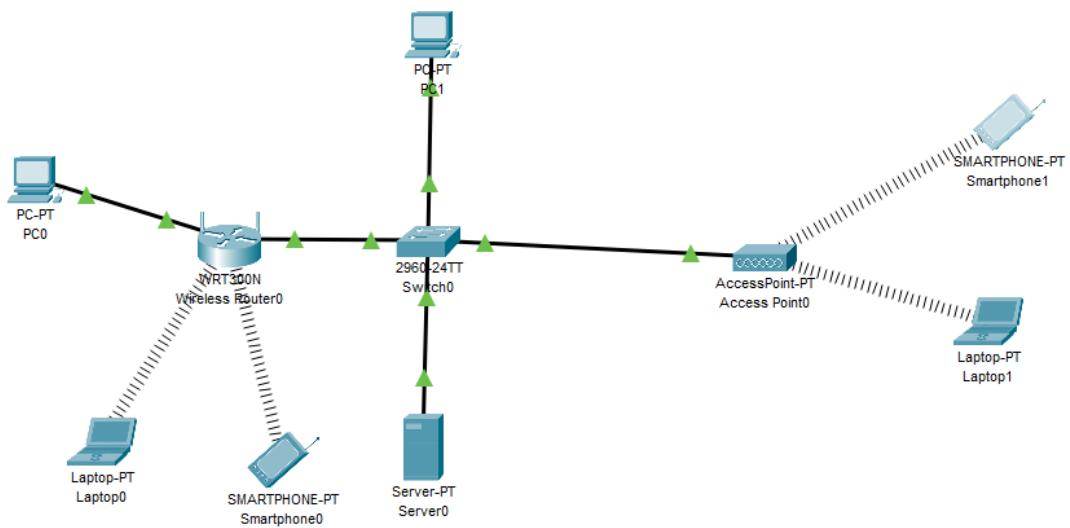
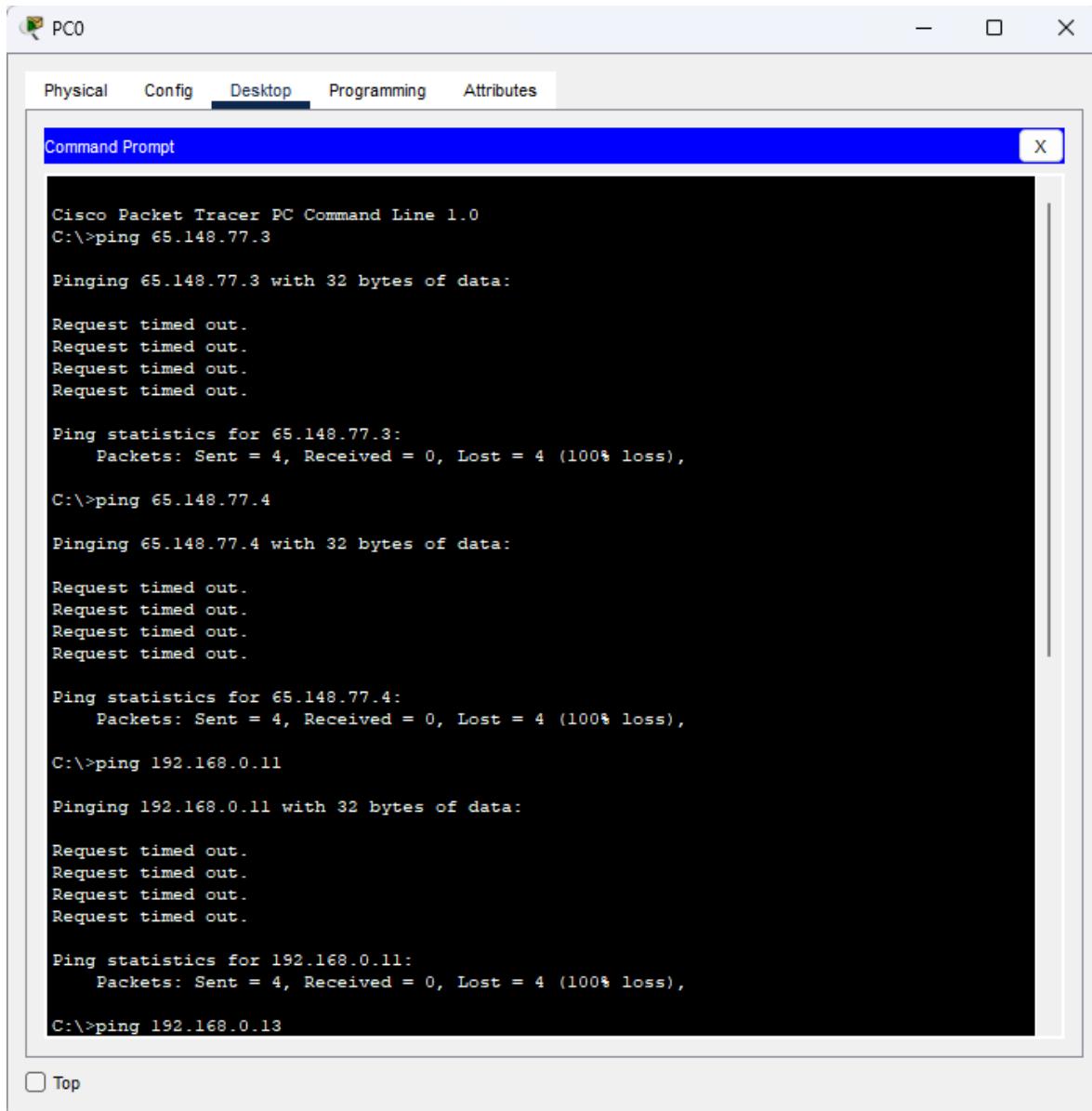


Figure 42. Basic Wi-Fi Configuration Diagram Completed

## 5.2. Connection tests between devices

- Pinging from **PC0**



PC0

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 65.148.77.3

Pinging 65.148.77.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.3:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 65.148.77.4

Pinging 65.148.77.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.4:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:

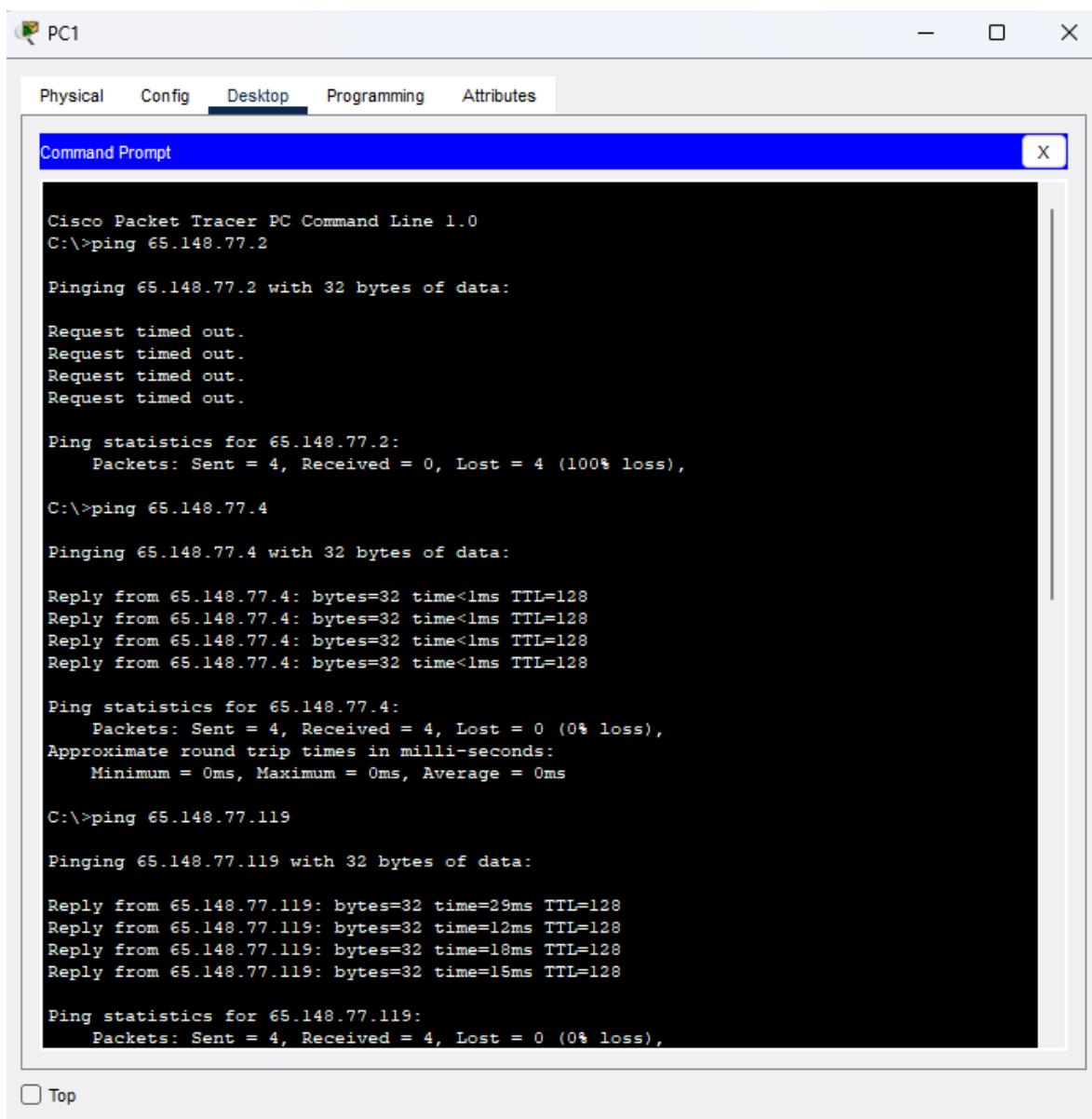
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 192.168.0.13
```

Top

Figure 43. First Ping Tests on PC0

- Pinging from PC1



PC1

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 65.148.77.2

Pinging 65.148.77.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 65.148.77.4

Pinging 65.148.77.4 with 32 bytes of data:

Reply from 65.148.77.4: bytes=32 time<1ms TTL=128

Ping statistics for 65.148.77.4:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 65.148.77.119

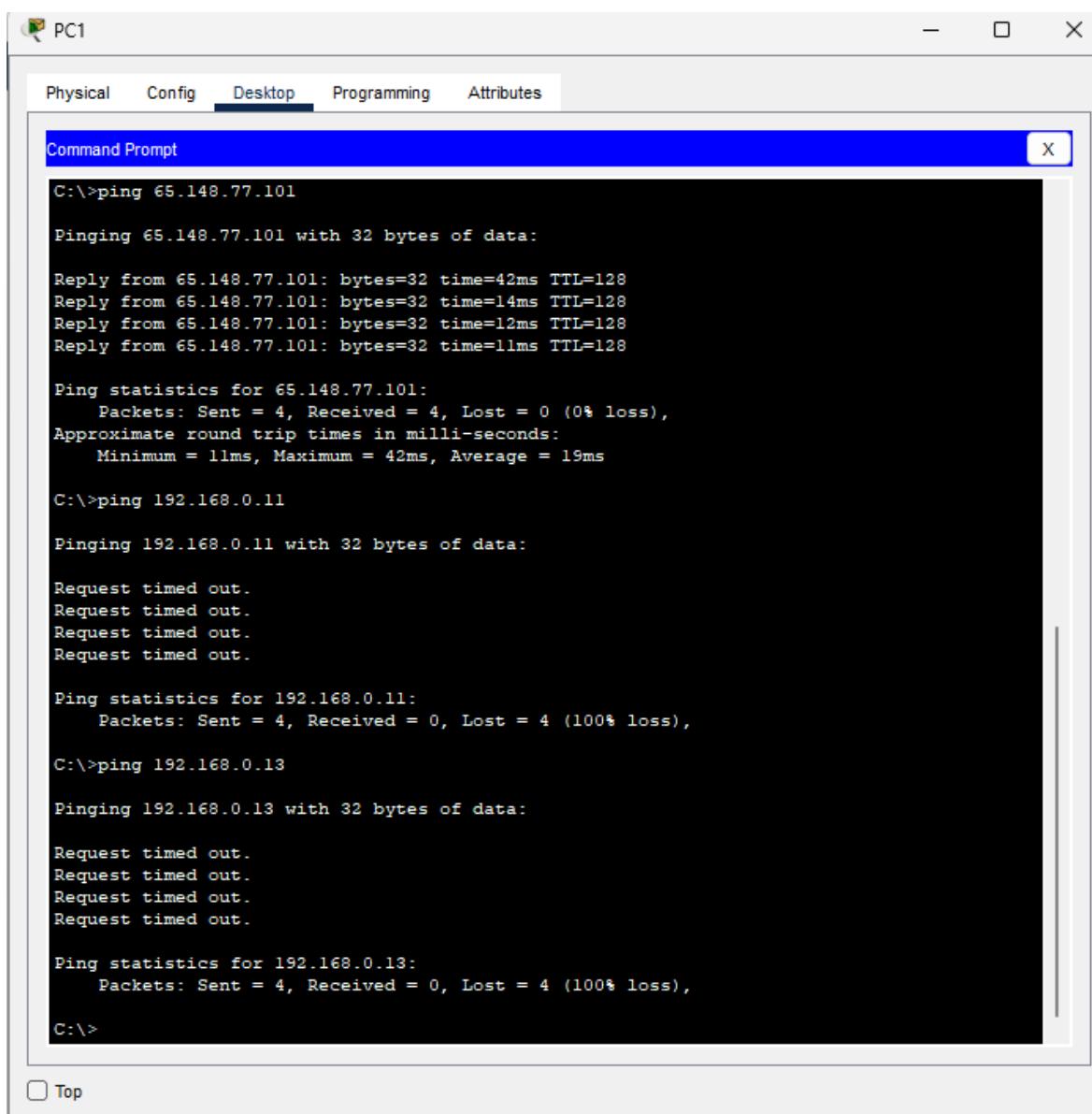
Pinging 65.148.77.119 with 32 bytes of data:

Reply from 65.148.77.119: bytes=32 time=29ms TTL=128
Reply from 65.148.77.119: bytes=32 time=12ms TTL=128
Reply from 65.148.77.119: bytes=32 time=18ms TTL=128
Reply from 65.148.77.119: bytes=32 time=15ms TTL=128

Ping statistics for 65.148.77.119:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Top

Figure 44. First Ping Tests on PC1



The screenshot shows a Windows Command Prompt window titled "PC1". The window has a blue header bar with tabs: Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is selected. Below the header is a title bar labeled "Command Prompt" with a close button "X". The main area of the window displays the output of several ping commands:

```
C:\>ping 65.148.77.101

Pinging 65.148.77.101 with 32 bytes of data:

Reply from 65.148.77.101: bytes=32 time=42ms TTL=128
Reply from 65.148.77.101: bytes=32 time=14ms TTL=128
Reply from 65.148.77.101: bytes=32 time=12ms TTL=128
Reply from 65.148.77.101: bytes=32 time=11ms TTL=128

Ping statistics for 65.148.77.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 42ms, Average = 19ms

C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.13

Pinging 192.168.0.13 with 32 bytes of data:

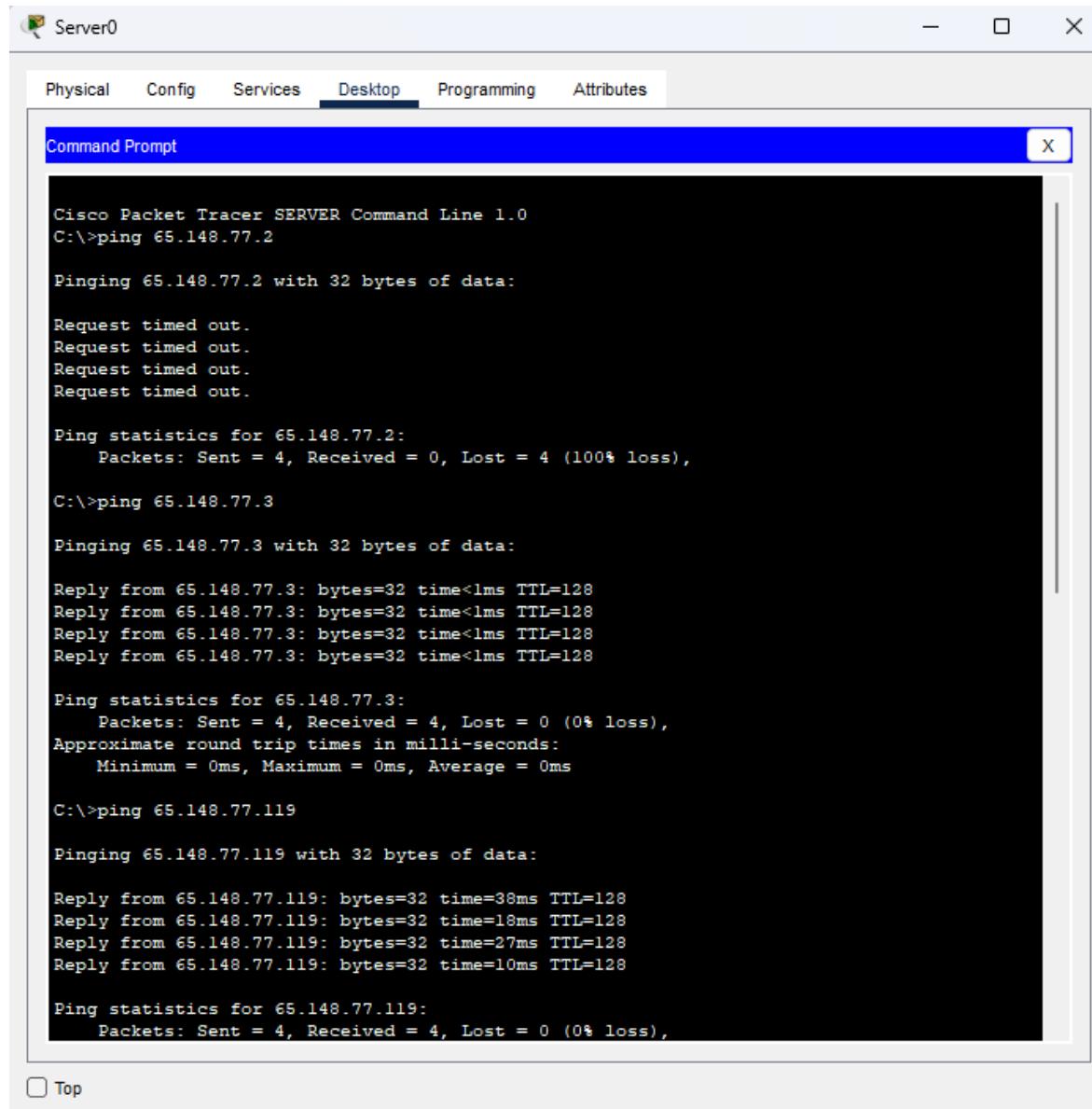
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Top

Figure 45. Second Ping Tests on PC1

- **Pinging from Server0**



The screenshot shows a Cisco Packet Tracer interface with a window titled "Server0". The window has tabs: Physical, Config, Services, Desktop (which is selected), Programming, and Attributes. Inside the window, a Command Prompt window is open with the following text:

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 65.148.77.2

Pinging 65.148.77.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 65.148.77.3

Pinging 65.148.77.3 with 32 bytes of data:

Reply from 65.148.77.3: bytes=32 time<1ms TTL=128

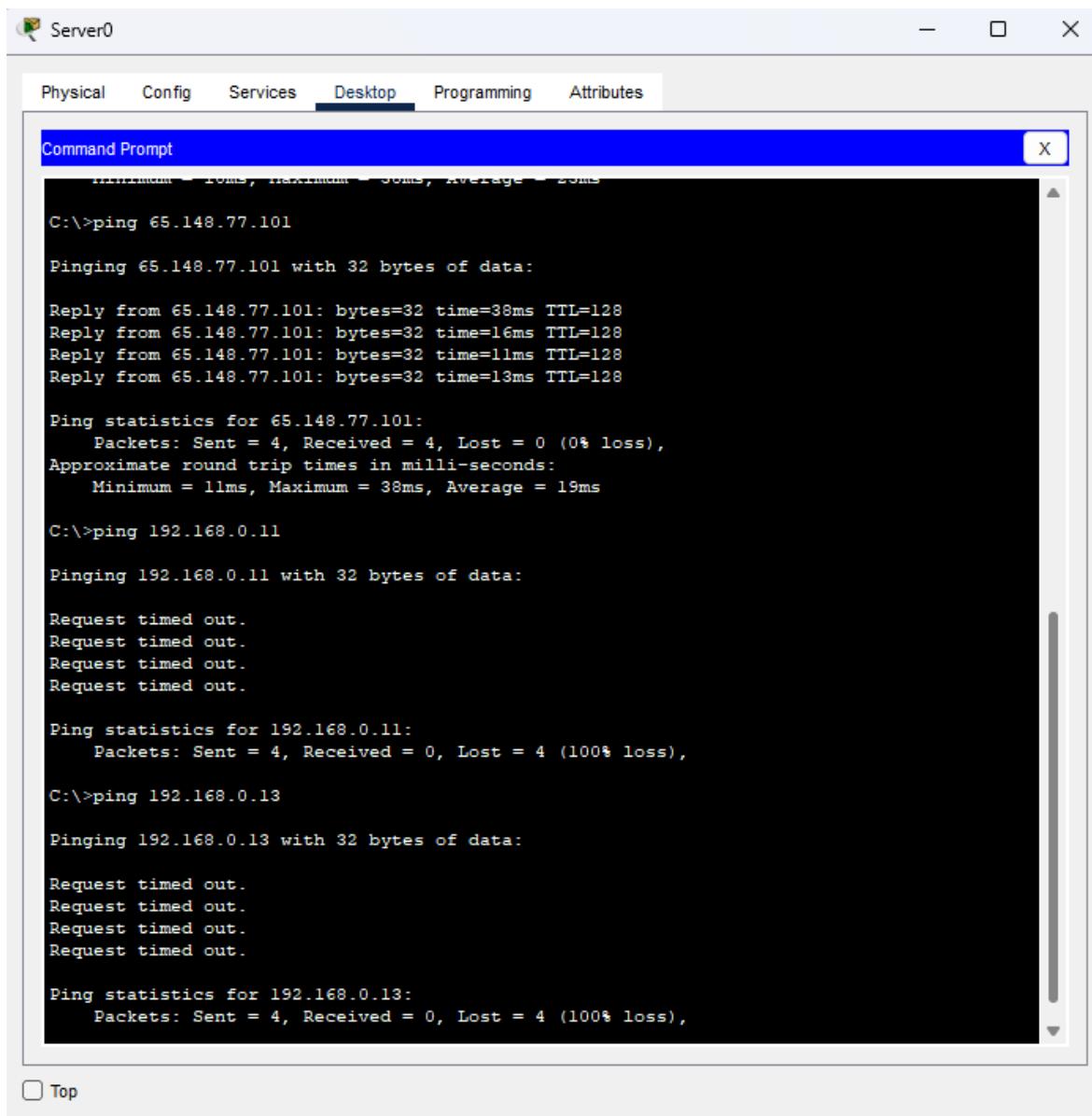
Ping statistics for 65.148.77.3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 65.148.77.119

Pinging 65.148.77.119 with 32 bytes of data:

Reply from 65.148.77.119: bytes=32 time=38ms TTL=128
Reply from 65.148.77.119: bytes=32 time=18ms TTL=128
Reply from 65.148.77.119: bytes=32 time=27ms TTL=128
Reply from 65.148.77.119: bytes=32 time=10ms TTL=128

Ping statistics for 65.148.77.119:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure 46. First Ping Tests on Server0



The screenshot shows a Windows Command Prompt window titled "Server0". The window has a blue header bar with tabs: Physical, Config, Services, Desktop (which is selected), Programming, and Attributes. Below the header is a title bar for "Command Prompt" with an "X" button. The main area of the window displays the output of several ping commands:

```
Minimum = 11ms, Maximum = 38ms, Average = 20ms
C:\>ping 65.148.77.101

Pinging 65.148.77.101 with 32 bytes of data:

Reply from 65.148.77.101: bytes=32 time=38ms TTL=128
Reply from 65.148.77.101: bytes=32 time=16ms TTL=128
Reply from 65.148.77.101: bytes=32 time=11ms TTL=128
Reply from 65.148.77.101: bytes=32 time=13ms TTL=128

Ping statistics for 65.148.77.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 38ms, Average = 19ms

C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.13

Pinging 192.168.0.13 with 32 bytes of data:

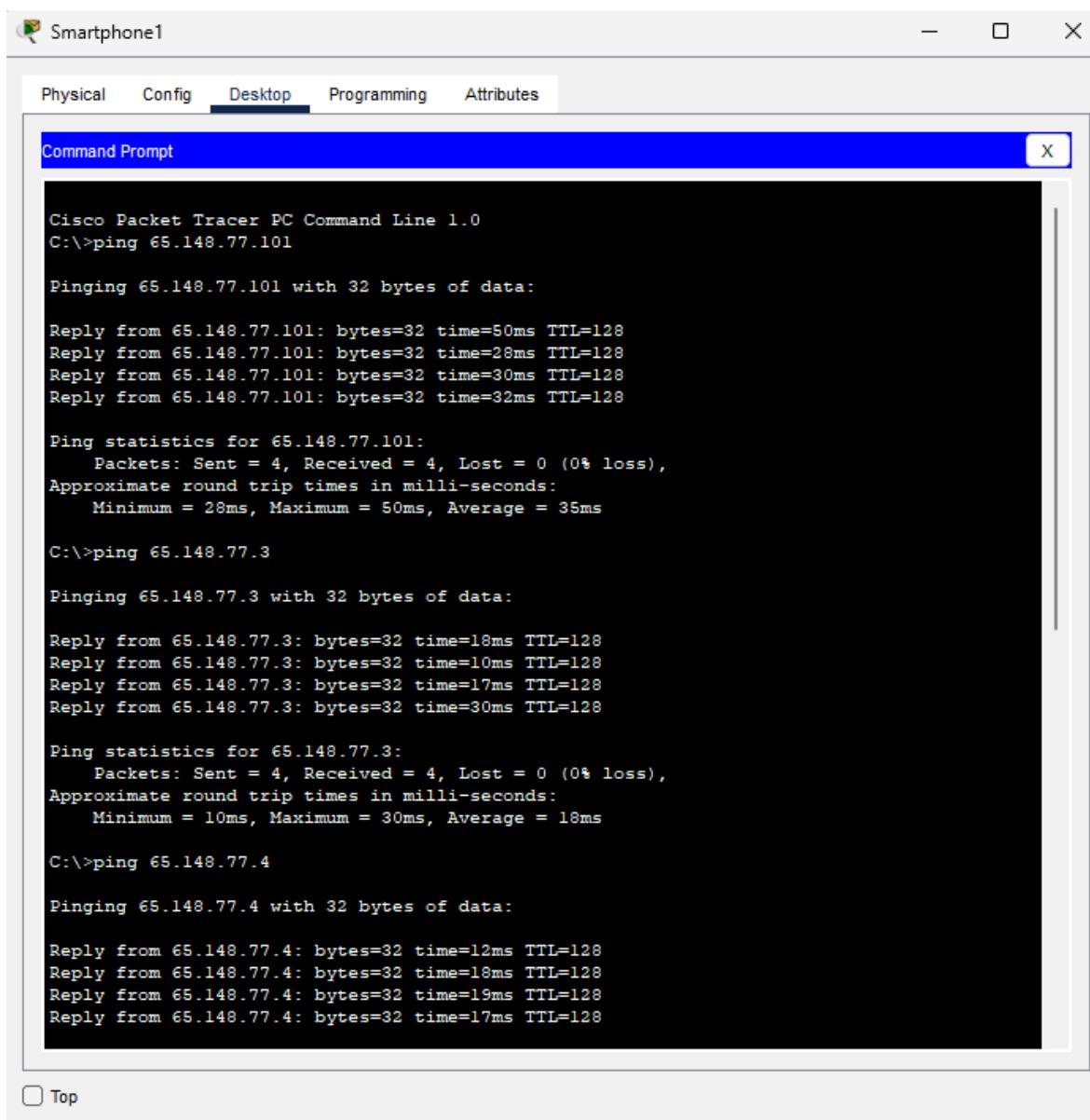
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Top

Figure 47. Second Ping Tests on Server0

- **Pinging from Smartphone1**



The screenshot shows a window titled "Smartphone1" with a tab bar at the top containing "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". Below the tab bar is a blue header bar with the title "Command Prompt" and a close button "X". The main area of the window is a black terminal window displaying the output of several ping commands. The text in the terminal is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 65.148.77.101

Pinging 65.148.77.101 with 32 bytes of data:

Reply from 65.148.77.101: bytes=32 time=50ms TTL=128
Reply from 65.148.77.101: bytes=32 time=28ms TTL=128
Reply from 65.148.77.101: bytes=32 time=30ms TTL=128
Reply from 65.148.77.101: bytes=32 time=32ms TTL=128

Ping statistics for 65.148.77.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 50ms, Average = 35ms

C:\>ping 65.148.77.3

Pinging 65.148.77.3 with 32 bytes of data:

Reply from 65.148.77.3: bytes=32 time=18ms TTL=128
Reply from 65.148.77.3: bytes=32 time=10ms TTL=128
Reply from 65.148.77.3: bytes=32 time=17ms TTL=128
Reply from 65.148.77.3: bytes=32 time=30ms TTL=128

Ping statistics for 65.148.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 30ms, Average = 18ms

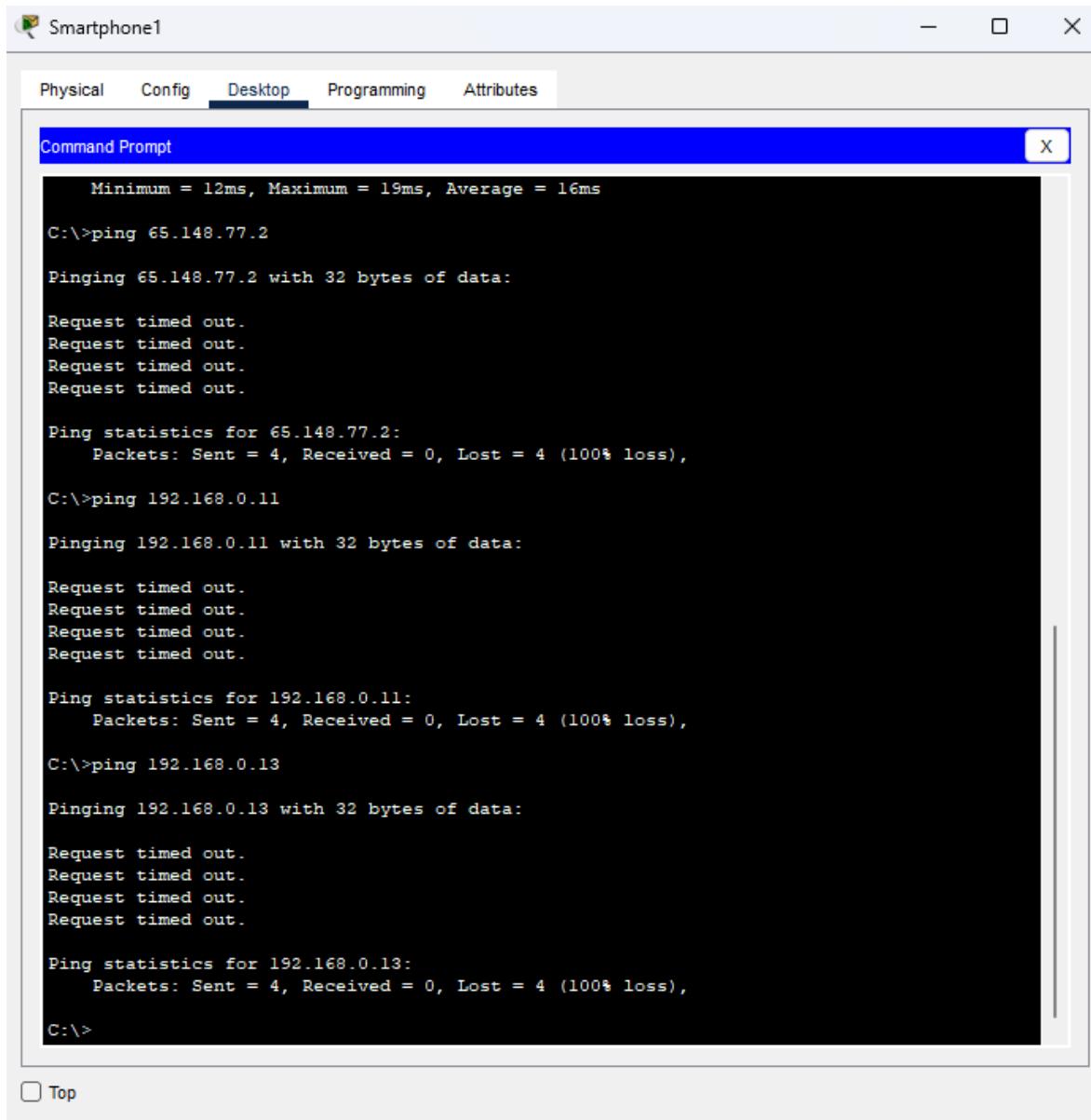
C:\>ping 65.148.77.4

Pinging 65.148.77.4 with 32 bytes of data:

Reply from 65.148.77.4: bytes=32 time=12ms TTL=128
Reply from 65.148.77.4: bytes=32 time=18ms TTL=128
Reply from 65.148.77.4: bytes=32 time=19ms TTL=128
Reply from 65.148.77.4: bytes=32 time=17ms TTL=128
```

At the bottom left of the terminal window, there is a small checkbox labeled "Top".

Figure 48. First Ping Tests on Smartphone1



The screenshot shows a smartphone screen with a terminal application open. The title bar says "Smartphone1". The tabs at the top are "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". The main area is a "Command Prompt" window with the following text:

```
Minimum = 12ms, Maximum = 19ms, Average = 16ms
C:\>ping 65.148.77.2
Pinging 65.148.77.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.11
Pinging 192.168.0.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

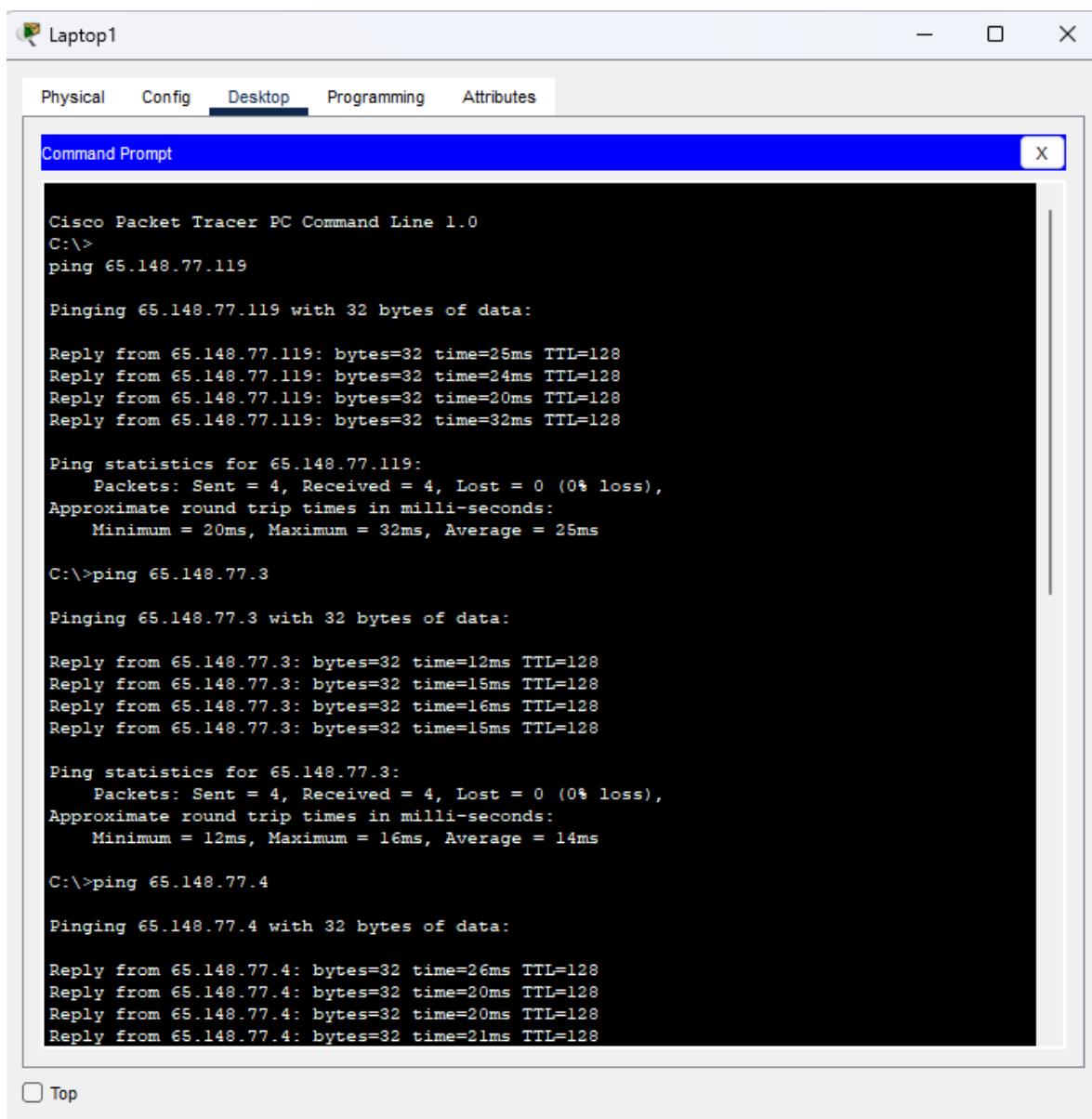
Ping statistics for 192.168.0.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.13
Pinging 192.168.0.13 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.13:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

At the bottom left of the terminal window, there is a checkbox labeled "Top".

Figure 49. Second Ping Tests on Smartphone1

- **Pinging from Laptop1**



Laptop1

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:>
ping 65.148.77.119

Pinging 65.148.77.119 with 32 bytes of data:

Reply from 65.148.77.119: bytes=32 time=25ms TTL=128
Reply from 65.148.77.119: bytes=32 time=24ms TTL=128
Reply from 65.148.77.119: bytes=32 time=20ms TTL=128
Reply from 65.148.77.119: bytes=32 time=32ms TTL=128

Ping statistics for 65.148.77.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 32ms, Average = 25ms

C:>ping 65.148.77.3

Pinging 65.148.77.3 with 32 bytes of data:

Reply from 65.148.77.3: bytes=32 time=12ms TTL=128
Reply from 65.148.77.3: bytes=32 time=15ms TTL=128
Reply from 65.148.77.3: bytes=32 time=16ms TTL=128
Reply from 65.148.77.3: bytes=32 time=15ms TTL=128

Ping statistics for 65.148.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 16ms, Average = 14ms

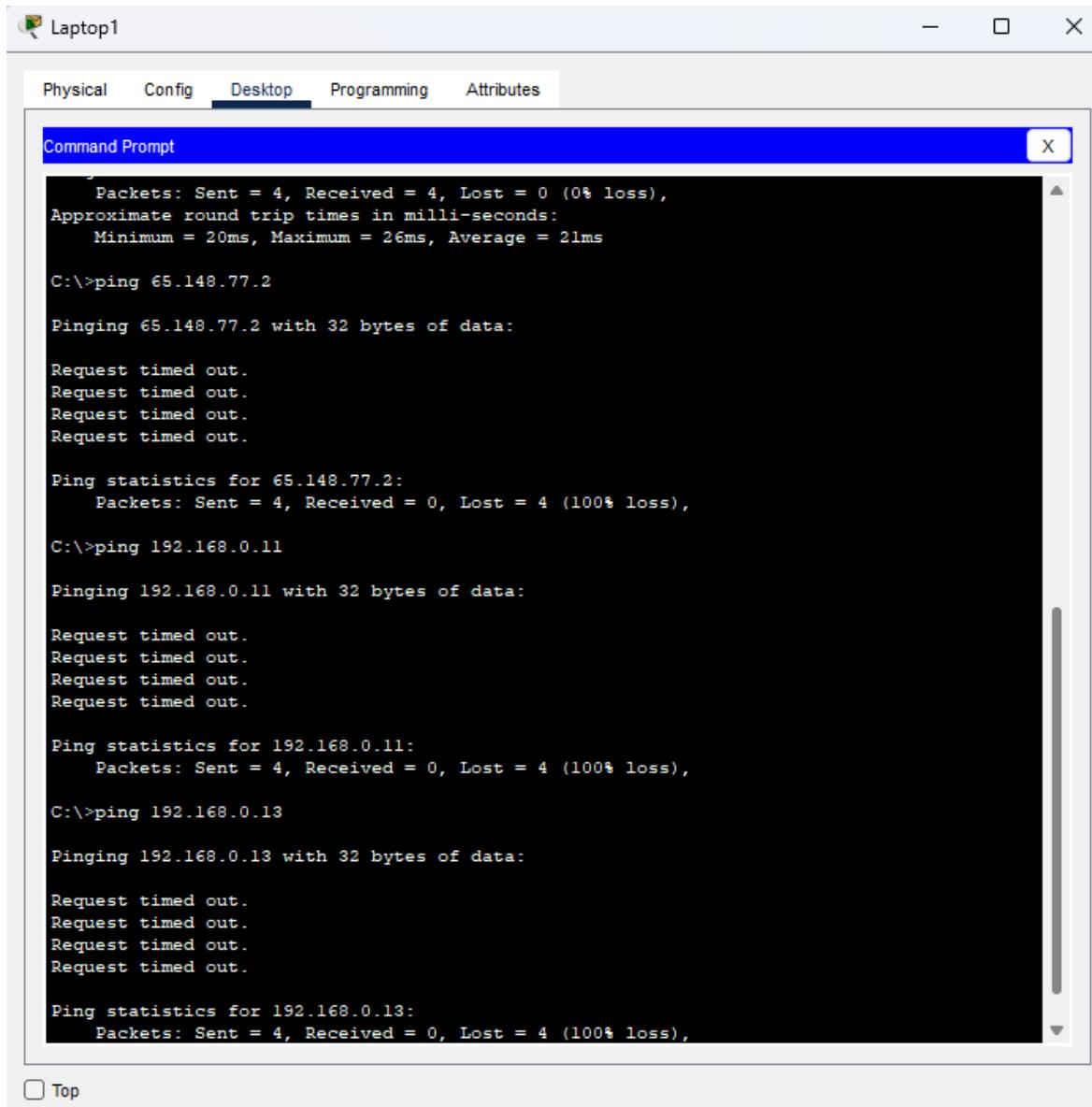
C:>ping 65.148.77.4

Pinging 65.148.77.4 with 32 bytes of data:

Reply from 65.148.77.4: bytes=32 time=26ms TTL=128
Reply from 65.148.77.4: bytes=32 time=20ms TTL=128
Reply from 65.148.77.4: bytes=32 time=20ms TTL=128
Reply from 65.148.77.4: bytes=32 time=21ms TTL=128
```

Top

Figure 50. First Ping Tests on Laptop1



Laptop1

Physical Config Desktop Programming Attributes

Command Prompt X

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 20ms, Maximum = 26ms, Average = 21ms

C:\>ping 65.148.77.2

Pinging 65.148.77.2 with 32 bytes of data:

Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 65.148.77.2:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:

Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 192.168.0.11:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.0.13

Pinging 192.168.0.13 with 32 bytes of data:

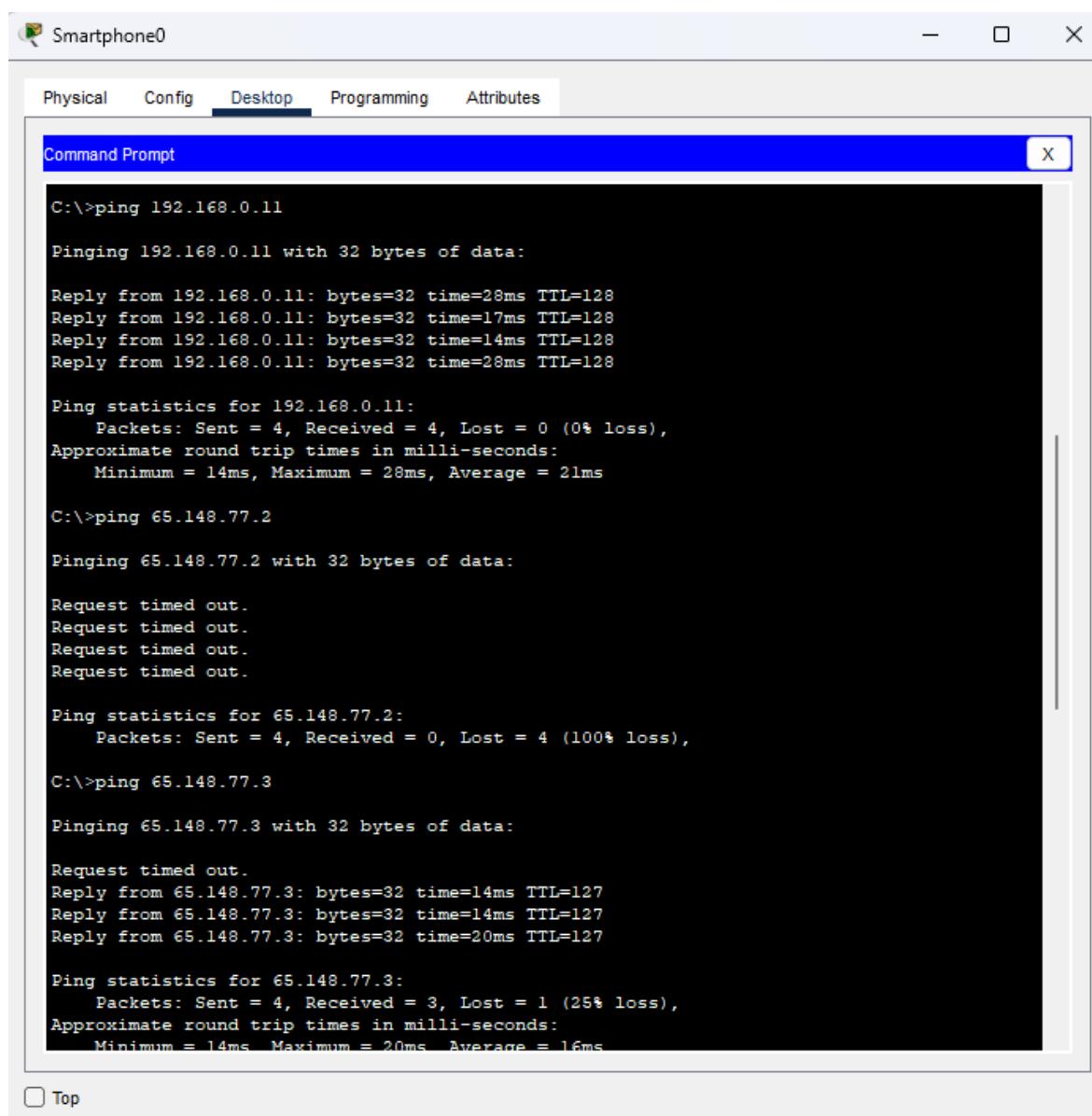
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 192.168.0.13:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Top

Figure 51. Second Ping Tests on Laptop1

- Pinging from Smartphone0



Smartphone0

Physical Config Desktop Programming Attributes

Command Prompt X

```
C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:

Reply from 192.168.0.11: bytes=32 time=28ms TTL=128
Reply from 192.168.0.11: bytes=32 time=17ms TTL=128
Reply from 192.168.0.11: bytes=32 time=14ms TTL=128
Reply from 192.168.0.11: bytes=32 time=28ms TTL=128

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 28ms, Average = 21ms

C:\>ping 65.148.77.2

Pinging 65.148.77.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 65.148.77.3

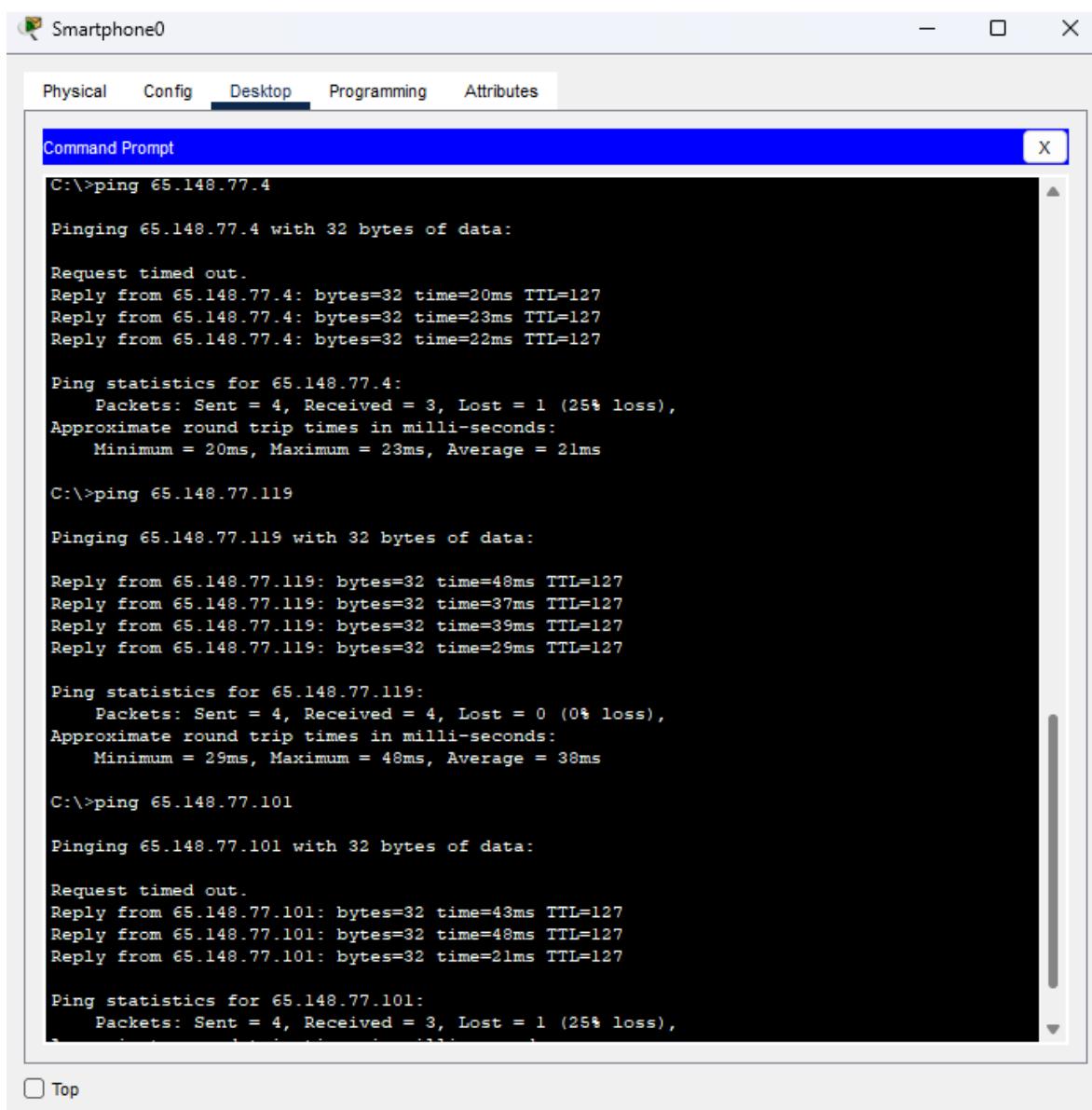
Pinging 65.148.77.3 with 32 bytes of data:

Request timed out.
Reply from 65.148.77.3: bytes=32 time=14ms TTL=127
Reply from 65.148.77.3: bytes=32 time=14ms TTL=127
Reply from 65.148.77.3: bytes=32 time=20ms TTL=127

Ping statistics for 65.148.77.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 20ms, Average = 16ms
```

Top

Figure 52. First Ping Tests on Smartphone0



The screenshot shows a Windows Command Prompt window titled "Smartphone0". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is selected. Below the tabs is a title bar labeled "Command Prompt" and an "X" button. The main area of the window displays the output of several "ping" commands:

```
C:\>ping 65.148.77.4

Pinging 65.148.77.4 with 32 bytes of data:

Request timed out.
Reply from 65.148.77.4: bytes=32 time=20ms TTL=127
Reply from 65.148.77.4: bytes=32 time=23ms TTL=127
Reply from 65.148.77.4: bytes=32 time=22ms TTL=127

Ping statistics for 65.148.77.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 23ms, Average = 21ms

C:\>ping 65.148.77.119

Pinging 65.148.77.119 with 32 bytes of data:

Reply from 65.148.77.119: bytes=32 time=48ms TTL=127
Reply from 65.148.77.119: bytes=32 time=37ms TTL=127
Reply from 65.148.77.119: bytes=32 time=39ms TTL=127
Reply from 65.148.77.119: bytes=32 time=29ms TTL=127

Ping statistics for 65.148.77.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 48ms, Average = 38ms

C:\>ping 65.148.77.101

Pinging 65.148.77.101 with 32 bytes of data:

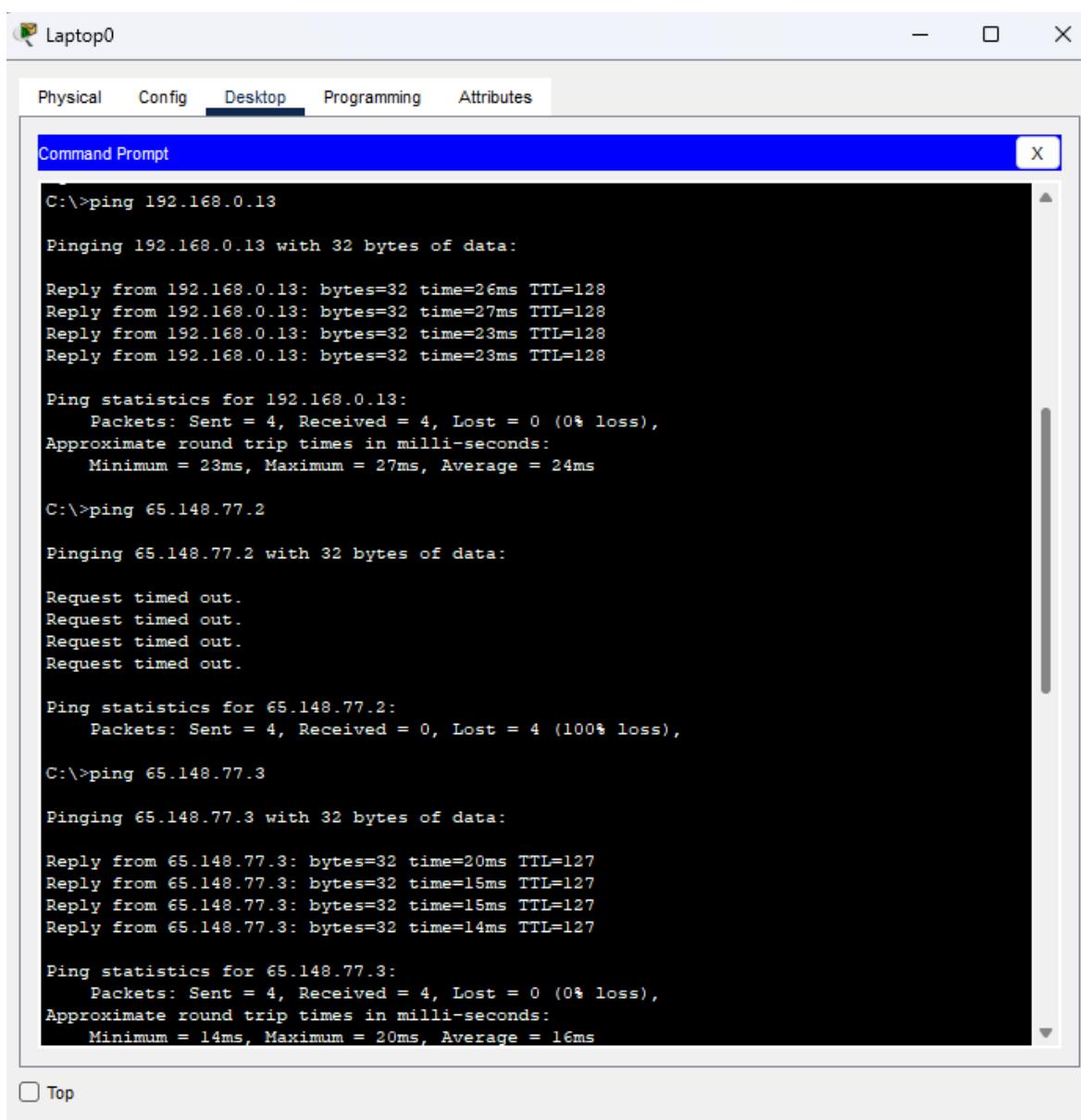
Request timed out.
Reply from 65.148.77.101: bytes=32 time=43ms TTL=127
Reply from 65.148.77.101: bytes=32 time=48ms TTL=127
Reply from 65.148.77.101: bytes=32 time=21ms TTL=127

Ping statistics for 65.148.77.101:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

Top

Figure 53. Second Ping Tests on Smartphone0

- Pinging from Laptop0



Laptop0

Physical Config Desktop Programming Attributes

Command Prompt X

```
C:\>ping 192.168.0.13

Pinging 192.168.0.13 with 32 bytes of data:

Reply from 192.168.0.13: bytes=32 time=26ms TTL=128
Reply from 192.168.0.13: bytes=32 time=27ms TTL=128
Reply from 192.168.0.13: bytes=32 time=23ms TTL=128
Reply from 192.168.0.13: bytes=32 time=23ms TTL=128

Ping statistics for 192.168.0.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 27ms, Average = 24ms

C:\>ping 65.148.77.2

Pinging 65.148.77.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.148.77.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 65.148.77.3

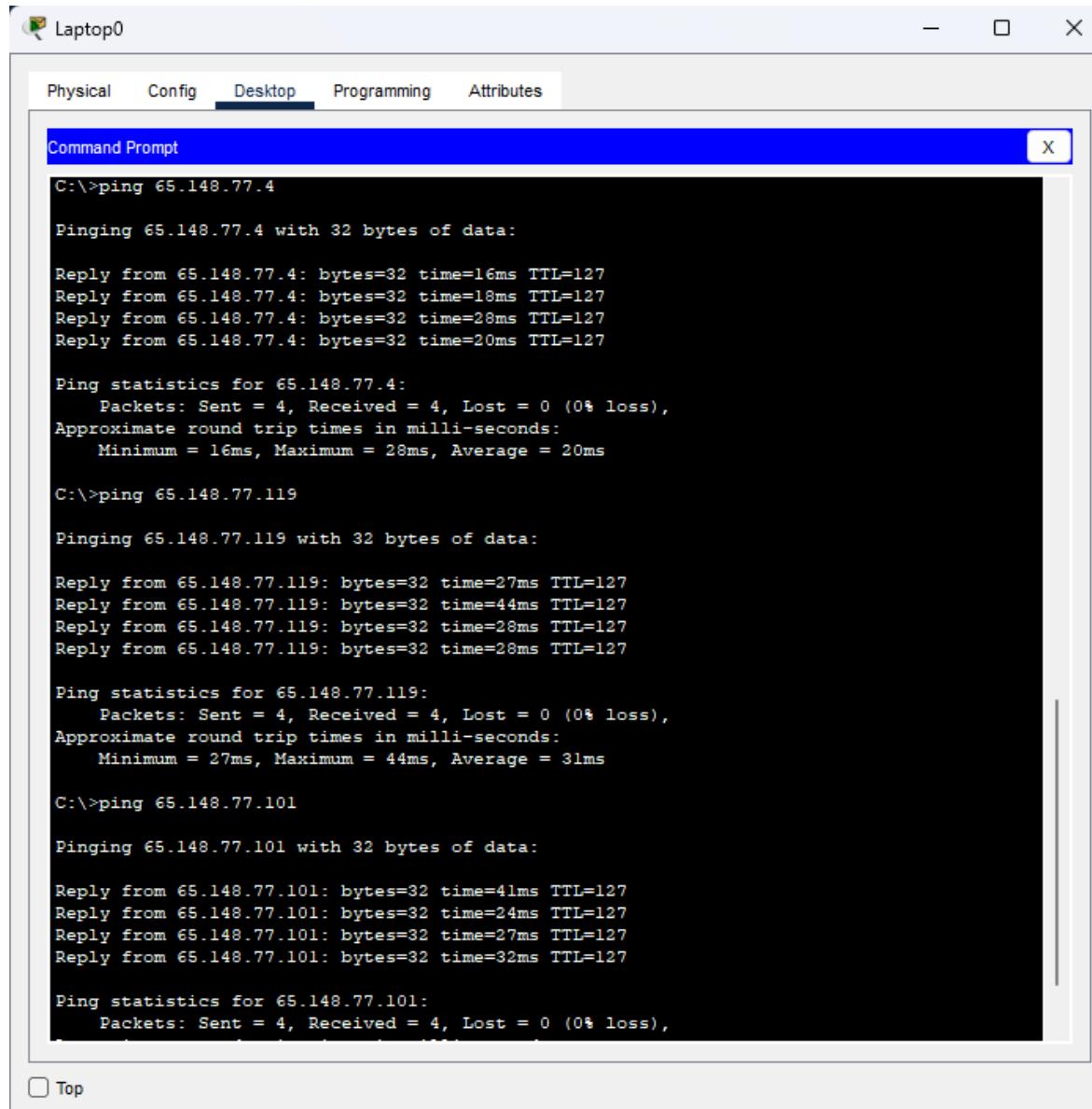
Pinging 65.148.77.3 with 32 bytes of data:

Reply from 65.148.77.3: bytes=32 time=20ms TTL=127
Reply from 65.148.77.3: bytes=32 time=15ms TTL=127
Reply from 65.148.77.3: bytes=32 time=15ms TTL=127
Reply from 65.148.77.3: bytes=32 time=14ms TTL=127

Ping statistics for 65.148.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 20ms, Average = 16ms
```

Top

Figure 54. First Ping Tests on Laptop0



```

Laptop0

Physical Config Desktop Programming Attributes

Command Prompt X

C:\>ping 65.148.77.4

Pinging 65.148.77.4 with 32 bytes of data:

Reply from 65.148.77.4: bytes=32 time=16ms TTL=127
Reply from 65.148.77.4: bytes=32 time=18ms TTL=127
Reply from 65.148.77.4: bytes=32 time=28ms TTL=127
Reply from 65.148.77.4: bytes=32 time=20ms TTL=127

Ping statistics for 65.148.77.4:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 28ms, Average = 20ms

C:\>ping 65.148.77.119

Pinging 65.148.77.119 with 32 bytes of data:

Reply from 65.148.77.119: bytes=32 time=27ms TTL=127
Reply from 65.148.77.119: bytes=32 time=44ms TTL=127
Reply from 65.148.77.119: bytes=32 time=28ms TTL=127
Reply from 65.148.77.119: bytes=32 time=28ms TTL=127

Ping statistics for 65.148.77.119:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 44ms, Average = 31ms

C:\>ping 65.148.77.101

Pinging 65.148.77.101 with 32 bytes of data:

Reply from 65.148.77.101: bytes=32 time=41ms TTL=127
Reply from 65.148.77.101: bytes=32 time=24ms TTL=127
Reply from 65.148.77.101: bytes=32 time=27ms TTL=127
Reply from 65.148.77.101: bytes=32 time=32ms TTL=127

Ping statistics for 65.148.77.101:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

```

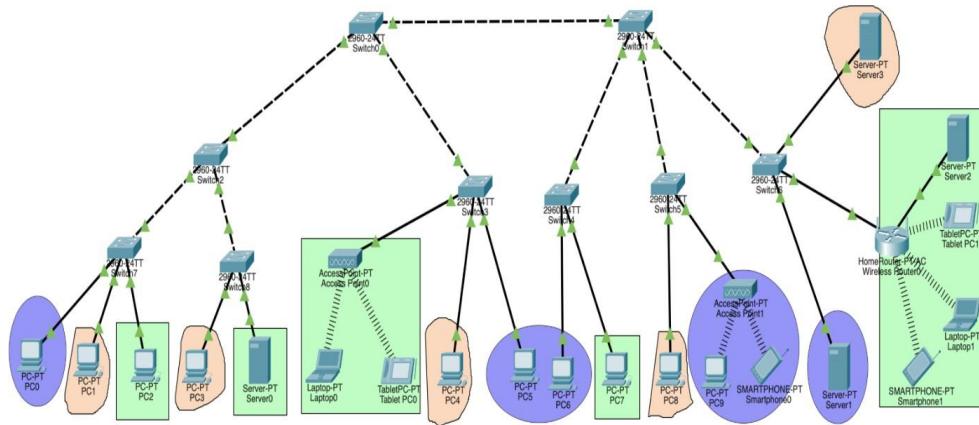
Top

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.

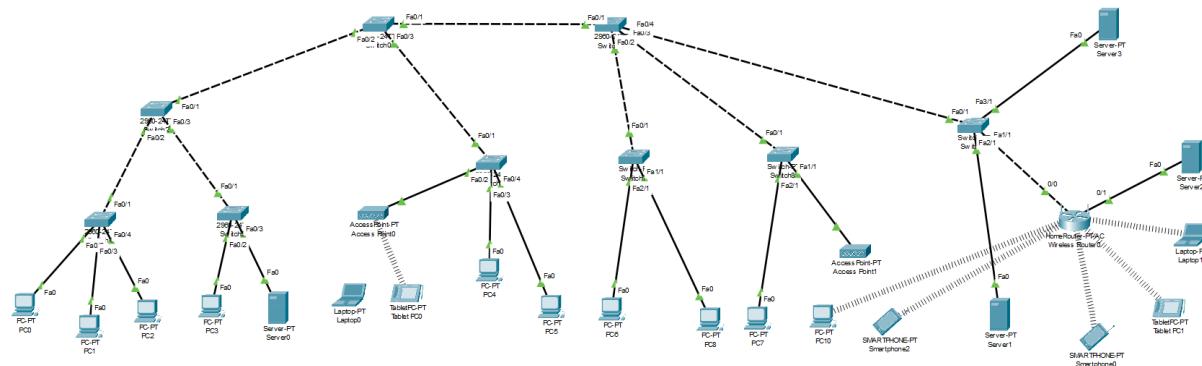


Figure 56 Initial Configuration

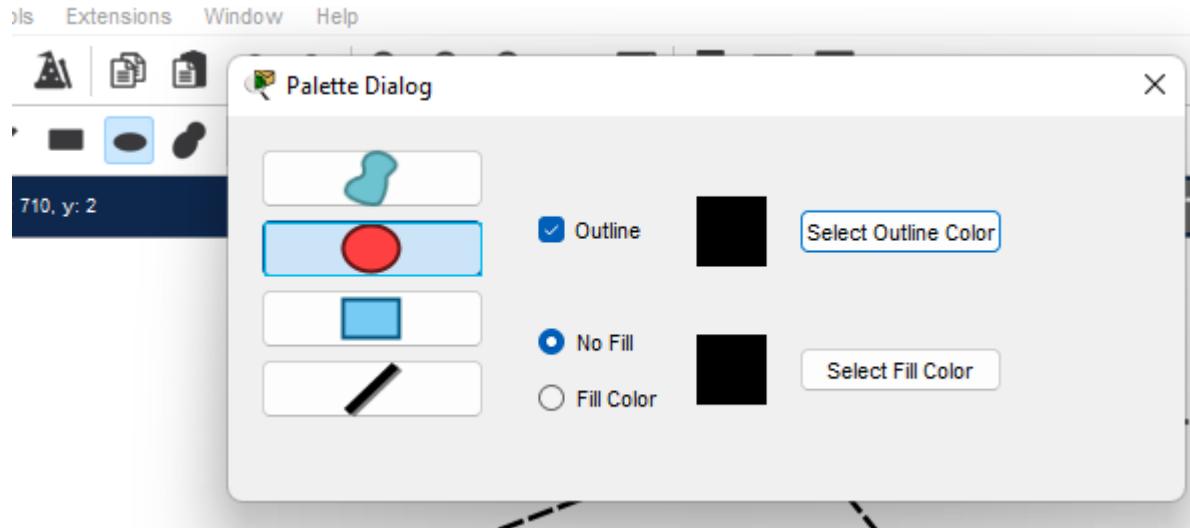
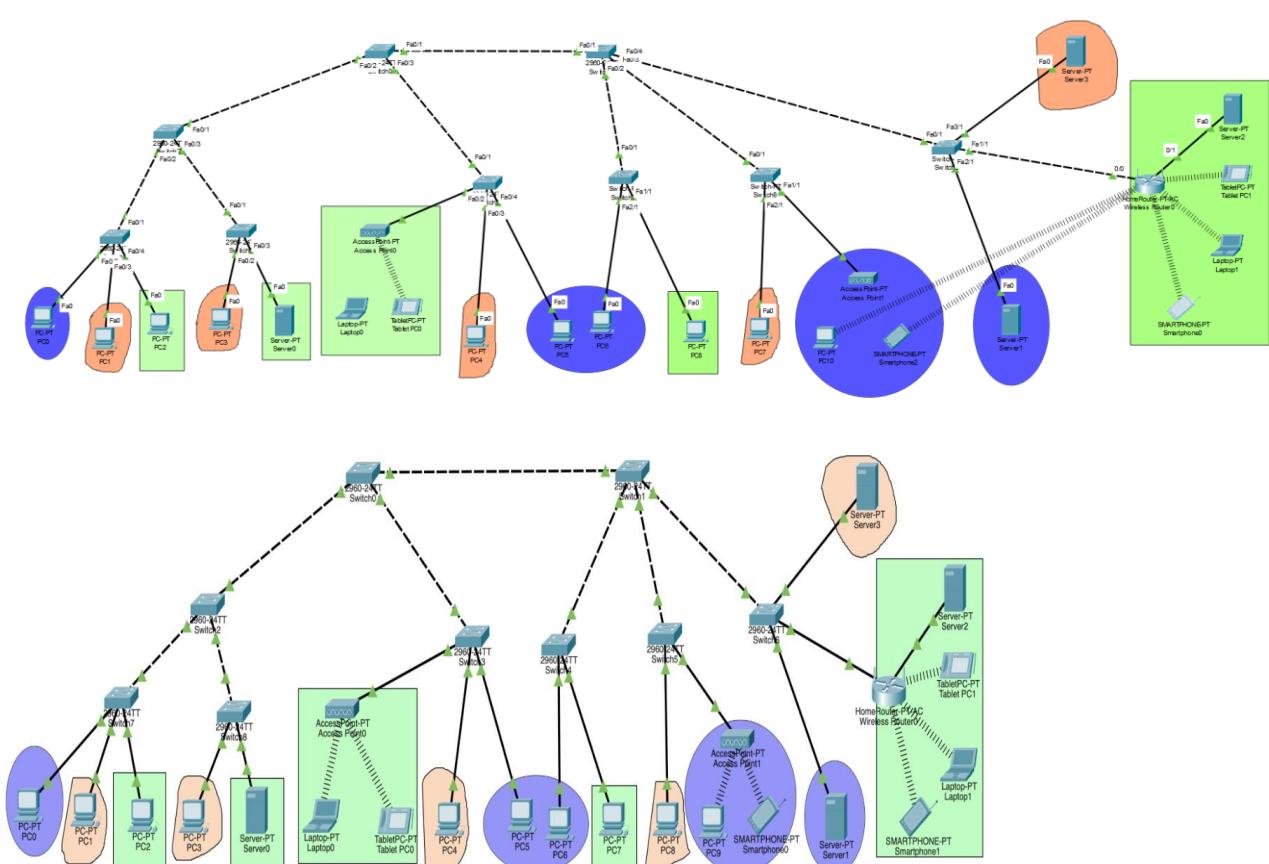
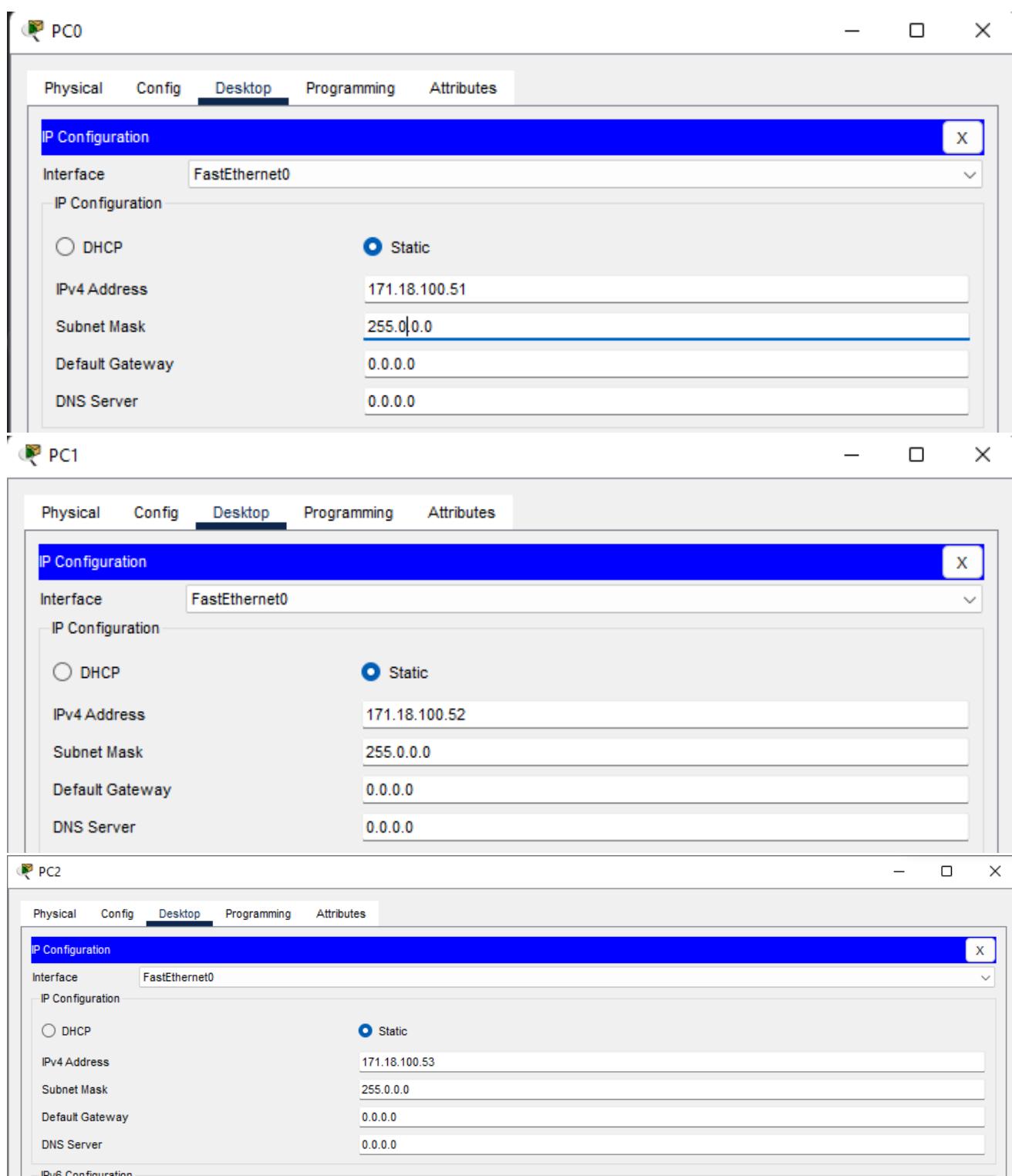


Figure 57 configuration palette dialog



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



The image displays three separate windows, each titled "PC0", "PC1", and "PC2" respectively, showing the "IP Configuration" settings for a "FastEthernet0" interface. The "Desktop" tab is selected in all three windows.

**PC0 IP Configuration:**

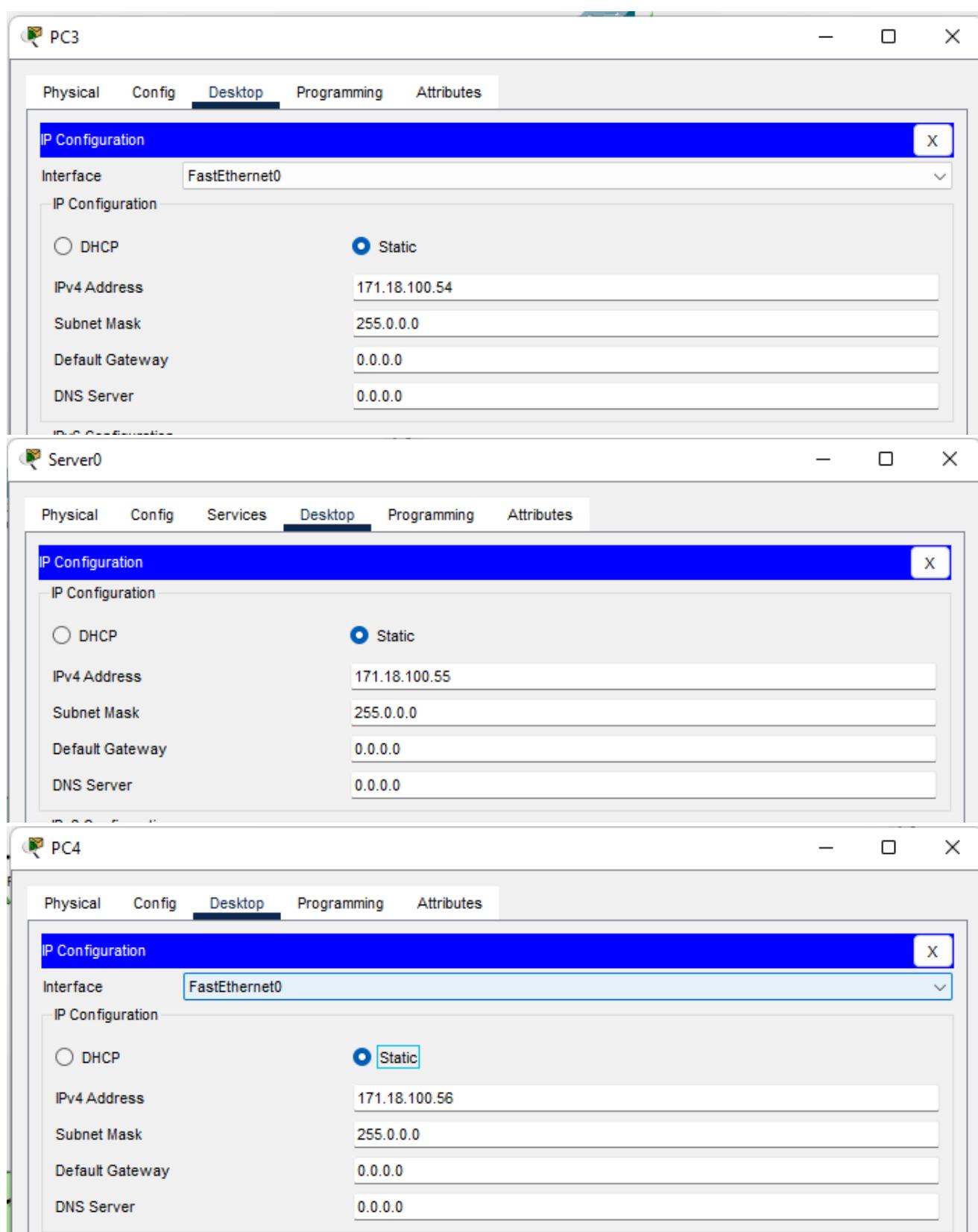
- Interface: FastEthernet0
- IP Configuration:
  - DHCP
  - Static
- IPv4 Address: 171.18.100.51
- Subnet Mask: 255.0.0.0
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0

**PC1 IP Configuration:**

- 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 IP Configuration:**

- 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



The image displays three separate windows, each titled with a computer name (PC3, Server0, or PC4) and showing the 'IP Configuration' settings for its respective network interface (FastEthernet0). Each window has tabs for Physical, Config, Desktop, Programming, and Attributes, with the Desktop tab selected.

**PC3 IP Configuration:**

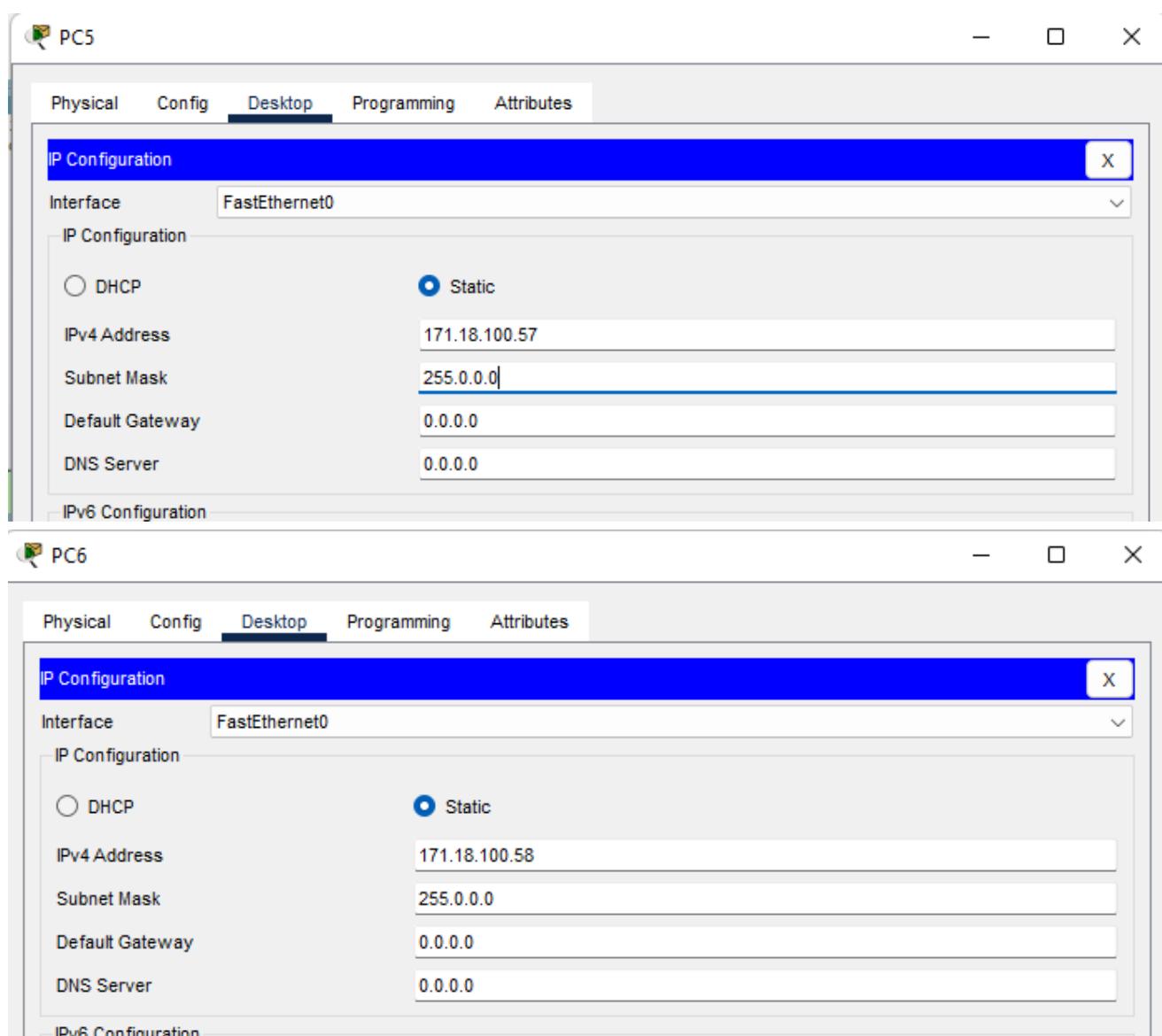
- Interface: FastEthernet0
- IP Configuration:
  - DHCP
  - Static
- IPv4 Address: 171.18.100.54
- Subnet Mask: 255.0.0.0
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0

**Server0 IP Configuration:**

- Interface: FastEthernet0
- 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 IP Configuration:**

- 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



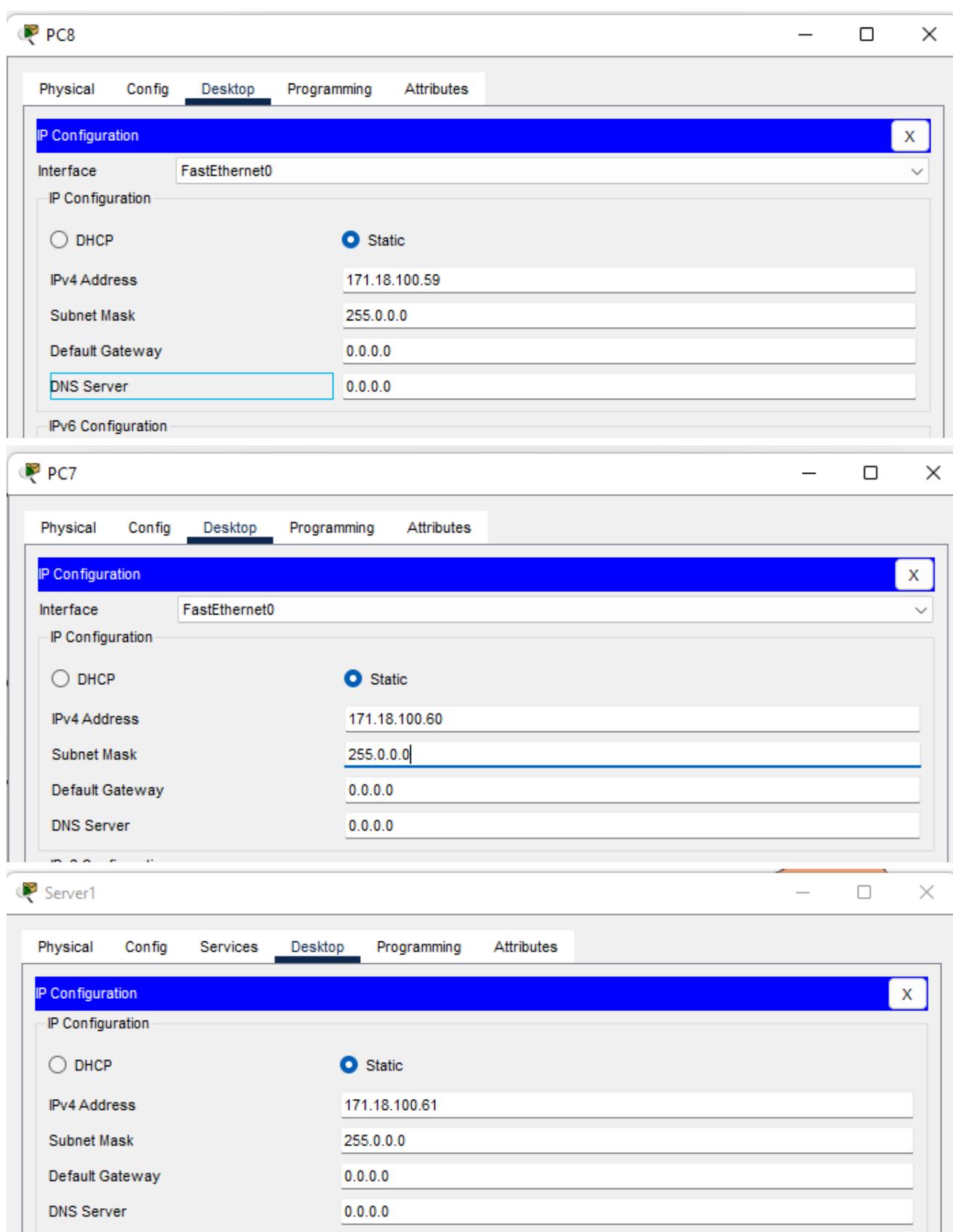
The image shows two separate computer desktop environments, labeled PC5 and PC6, both displaying the same IP configuration dialog box.

**PC5 IP Configuration:**

- 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

**PC6 IP Configuration:**

- 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



The image displays three separate windows, each titled with a computer icon and a name: PC8, PC7, and Server1. Each window shows the 'Desktop' tab selected in a navigation bar. Below the tabs, there is a blue header bar labeled 'IP Configuration'. Each window contains a form for configuring network interfaces. The 'Interface' dropdown in all three windows is set to 'FastEthernet0'. The 'IP Configuration' section includes fields for 'IPv4 Address', 'Subnet Mask', 'Default Gateway', and 'DNS Server'. In PC8, the IPv4 address is 171.18.100.59, subnet mask is 255.0.0.0, default gateway is 0.0.0.0, and DNS server is 0.0.0.0. In PC7, the IPv4 address is 171.18.100.60, subnet mask is 255.0.0.0, default gateway is 0.0.0.0, and DNS server is 0.0.0.0. In Server1, the IPv4 address is 171.18.100.61, subnet mask is 255.0.0.0, default gateway is 0.0.0.0, and DNS server is 0.0.0.0.

**PC8**

Physical Config Desktop Programming Attributes

**IP Configuration**

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**

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**

IP Configuration

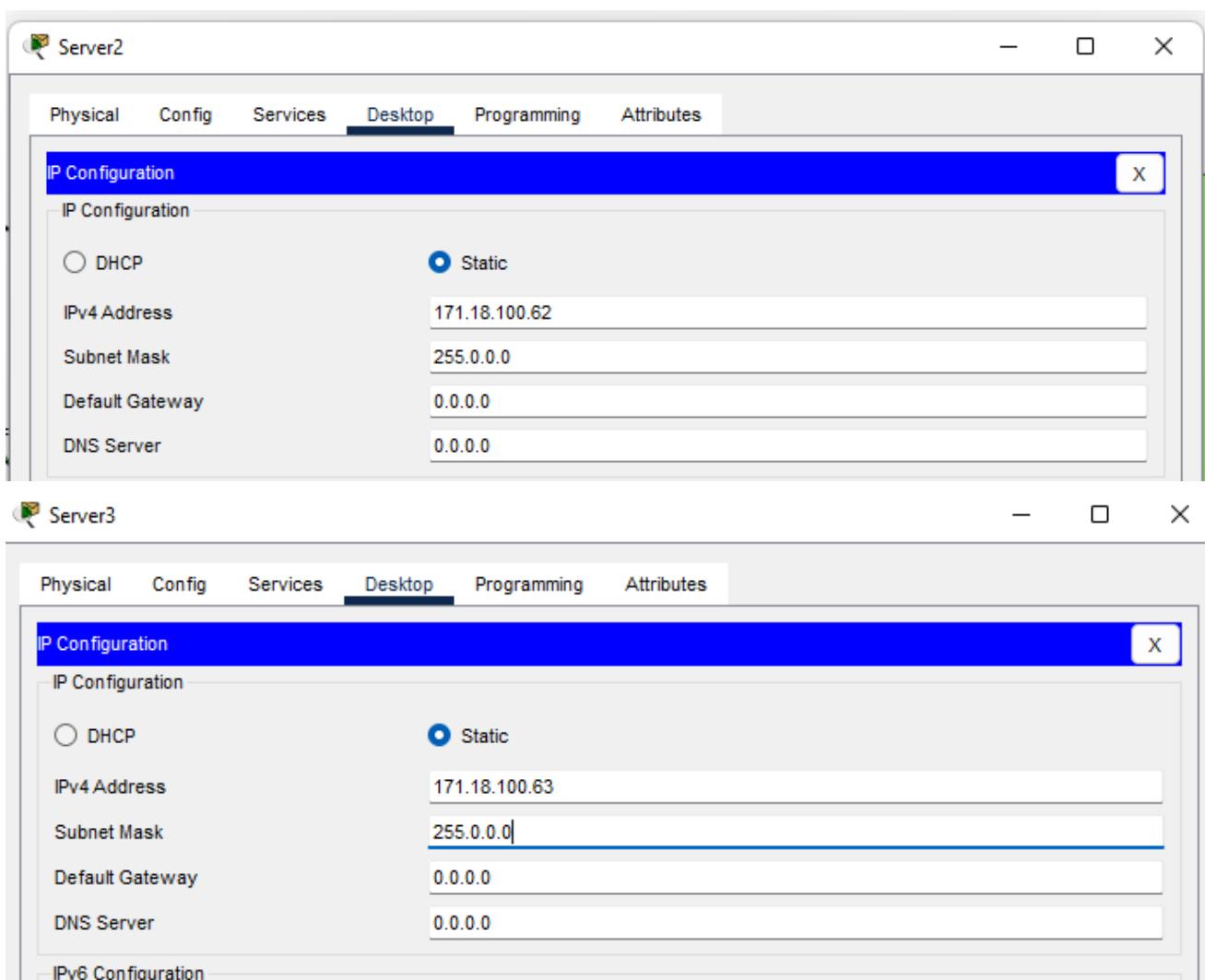
DHCP  Static

IPv4 Address 171.18.100.61

Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0



**Server2**

Physical Config Services Desktop **Programming** Attributes

**IP Configuration**

IP Configuration

DHCP  Static

IPv4 Address: 171.18.100.62

Subnet Mask: 255.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

**Server3**

Physical Config Services Desktop **Programming** Attributes

**IP Configuration**

IP Configuration

DHCP  Static

IPv4 Address: 171.18.100.63

Subnet Mask: 255.0.0.0

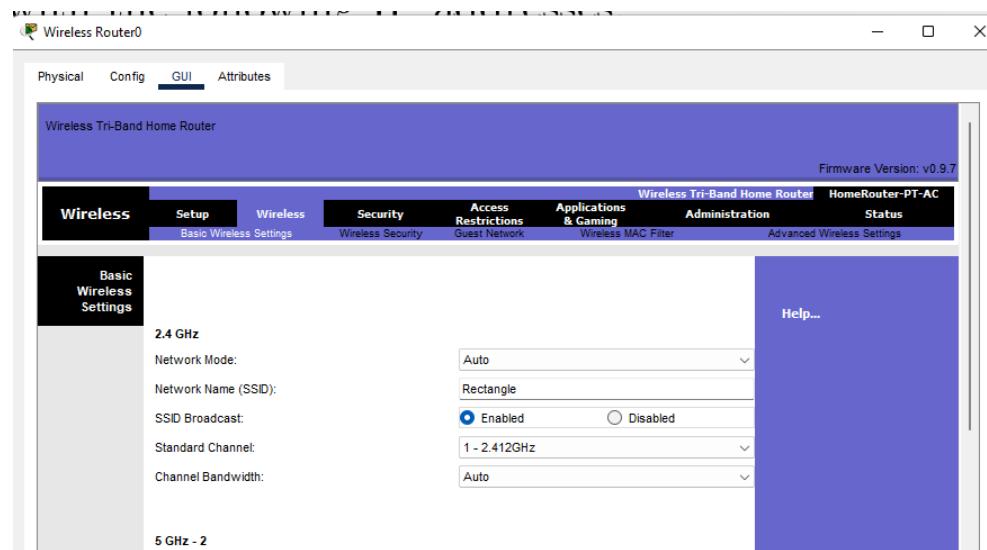
Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

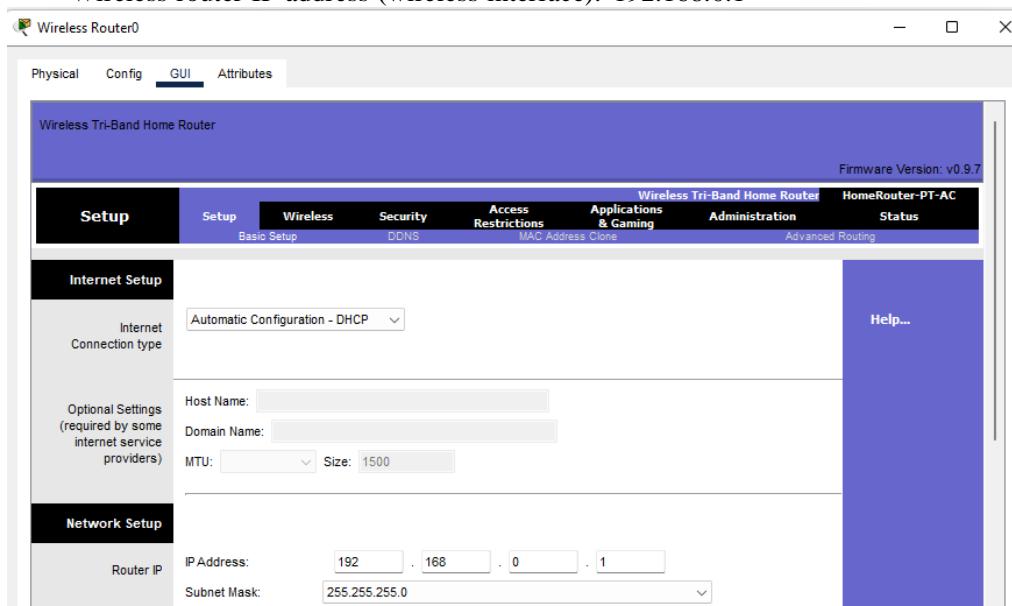
IPv6 Configuration

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 from the previous setup

<b>DHCP Server:</b>	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	<a href="#">DHCP Reservation</a>
<b>Start IP Address:</b> 192.168.0. 50			
<b>Maximum number of Users:</b> 31			
<b>IP Address Range:</b> 192.168.0. 50 - 80			

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

Wireless Tri-Band Hor					
Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administrati
<a href="#">Basic Wireless Settings</a>	<a href="#">Wireless Security</a>	<a href="#">Guest Network</a>		<a href="#">Wireless MAC Filter</a>	
<b>2.4 GHz</b>					
Security Mode:	<input type="button" value="WPA2 Personal"/>				
Encryption:	<input type="button" value="AES"/>				
Passphrase:	<input type="button" value="Rectangle"/>				
Key Renewal:	3600	seconds			
<b>5 GHz - 1</b>					
Security Mode:	<input type="button" value="Disabled"/>				
<b>5 GHz - 2</b>					
Security Mode:	<input type="button" value="Disabled"/>				

Now we configure the devices

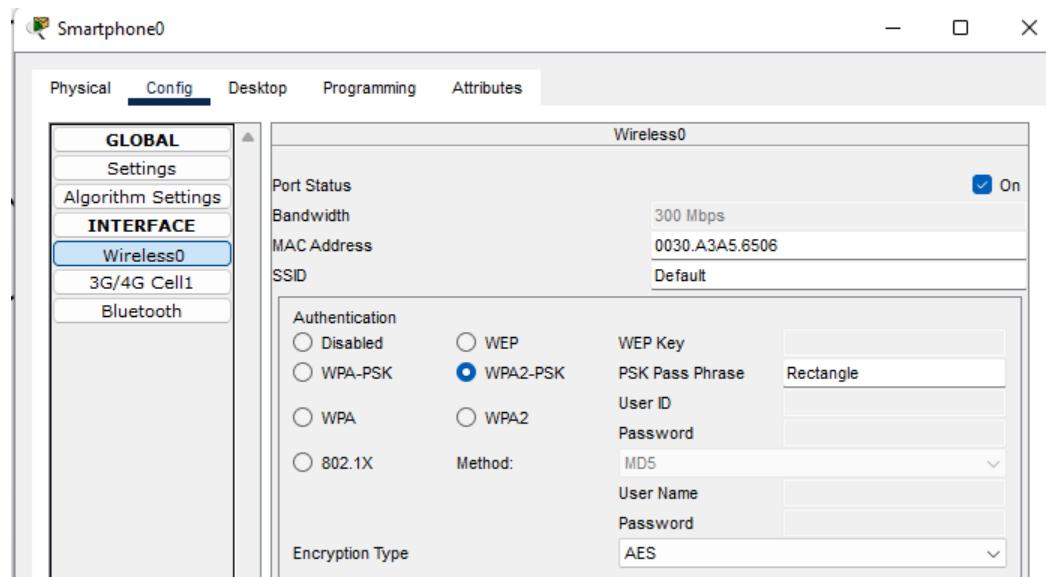
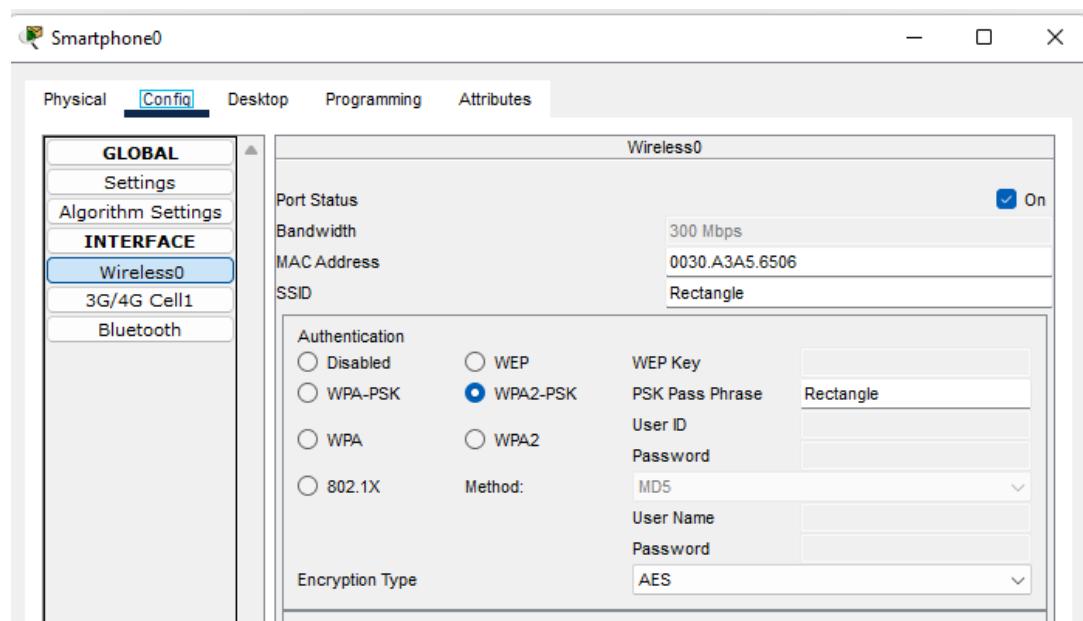
In Tablet PC1 and the Smartphone we go to the wireless0 and set WPA2-PSK and then we put the pass phrase Rectangle

The screenshot shows the configuration interface for a tablet device named "Tablet PC1". The main window title is "Tablet PC1". The top navigation bar includes tabs for Physical, Config, Desktop, Programming, and Attributes. The "Config" tab is currently selected.

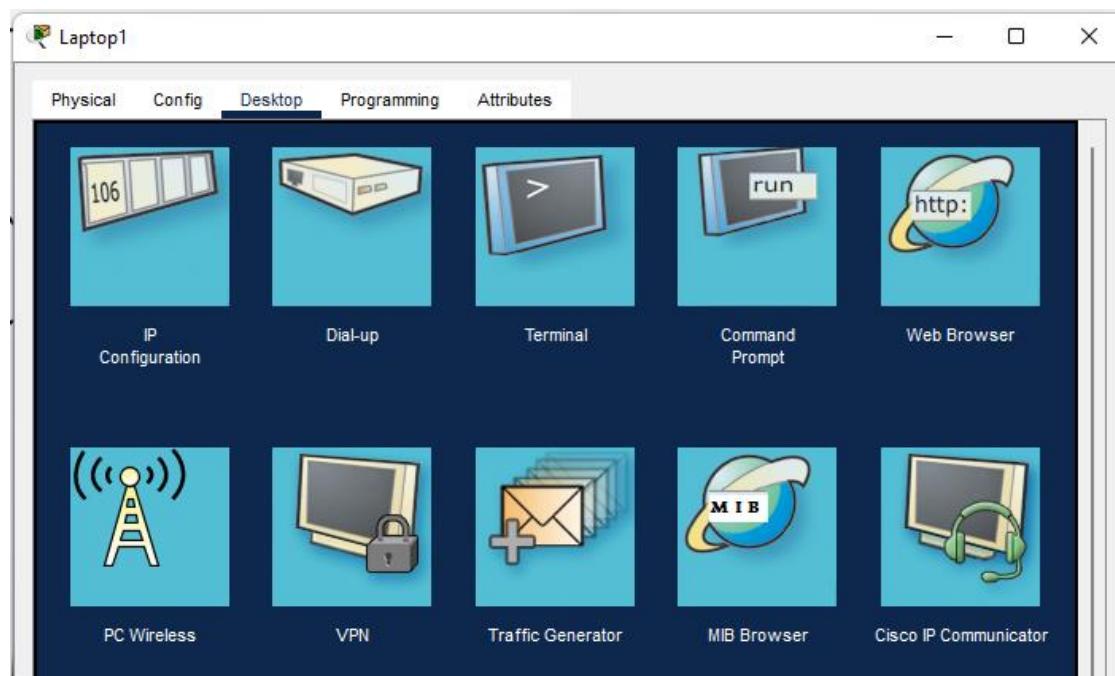
The left sidebar contains a tree view with nodes: GLOBAL, Settings, Algorithm Settings, INTERFACE, Wireless0, 3G/4G Cell1, and Bluetooth. The "INTERFACE" node is expanded, and "Wireless0" is selected.

The right panel displays the "Wireless0" configuration details:

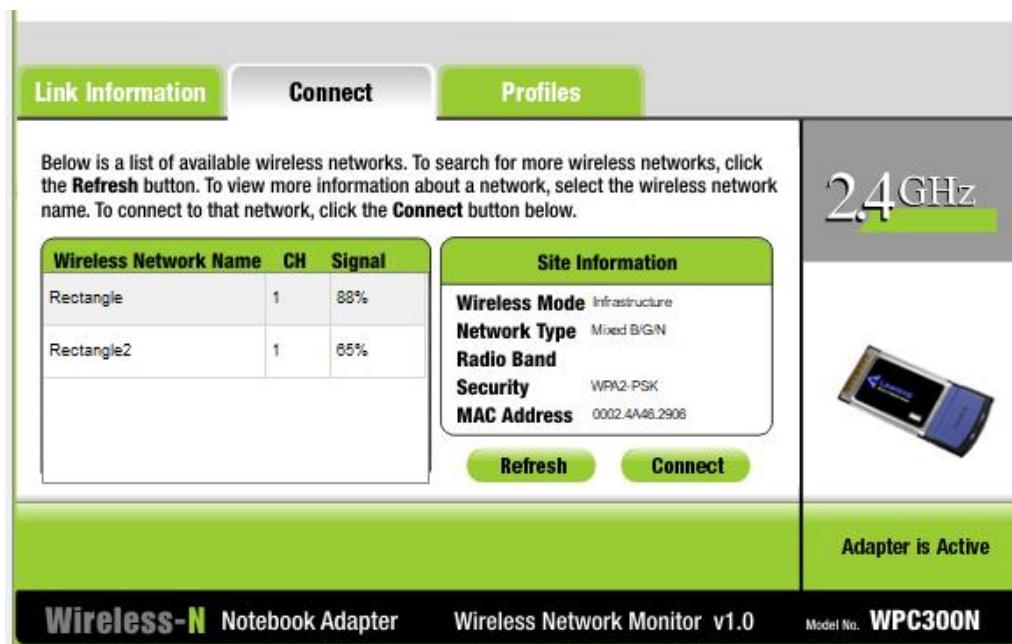
- Port Status:** On (checkbox checked)
- Bandwidth:** 300 Mbps
- MAC Address:** 0004.9A57.E884
- SSID:** Rectangle
- Authentication:** WPA2-PSK (radio button selected)
  - WEP Key: Rectangle
  - PSK Pass Phrase: Rectangle
  - User ID: (empty input field)
  - Password: (empty input field)
- Method:** MD5 (radio button selected)
  - User Name: (empty input field)
  - Password: (empty input field)
- Encryption Type:** AES



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



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



The interface has three tabs at the top: **Link Information**, **Connect** (selected), and **Profiles**.

**Link Information:** Displays a list of available wireless networks:

Wireless Network Name	CH	Signal
Rectangle	1	88%
Rectangle2	1	65%

**Site Information:** Displays details about the selected network:

- Wireless Mode:** Infrastructure
- Network Type:** Mixed B/G/N
- Radio Band:** 2.4 GHz
- Security:** WPA2-PSK
- MAC Address:** 0002-4A48-2906

**Buttons:** Refresh, Connect

**Right Panel:** Shows a 2.4 GHz band icon and an image of a blue and black wireless adapter. Below it, the text 'Adapter is Active'.

**Bottom Bar:** Wireless-N Notebook Adapter, Wireless Network Monitor v1.0, Model No. WPC300N

## WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security    WPA2-Personal

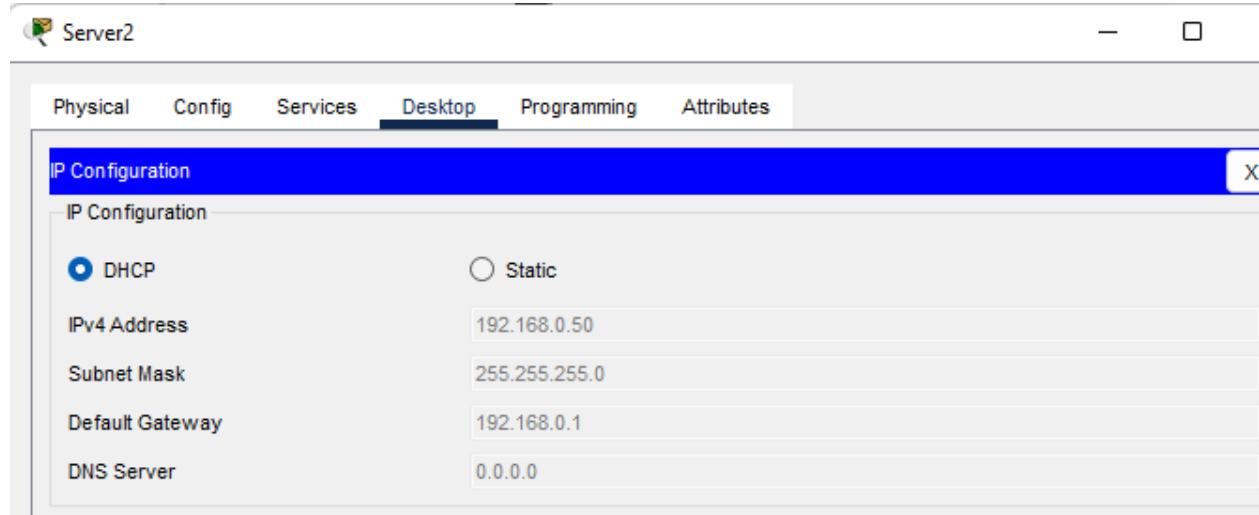
Please select the wireless security method used by your existing wireless network.

Pre-shared Key Rectangle|

Please enter a Pre-shared Key that is 8 to 63 characters in length.

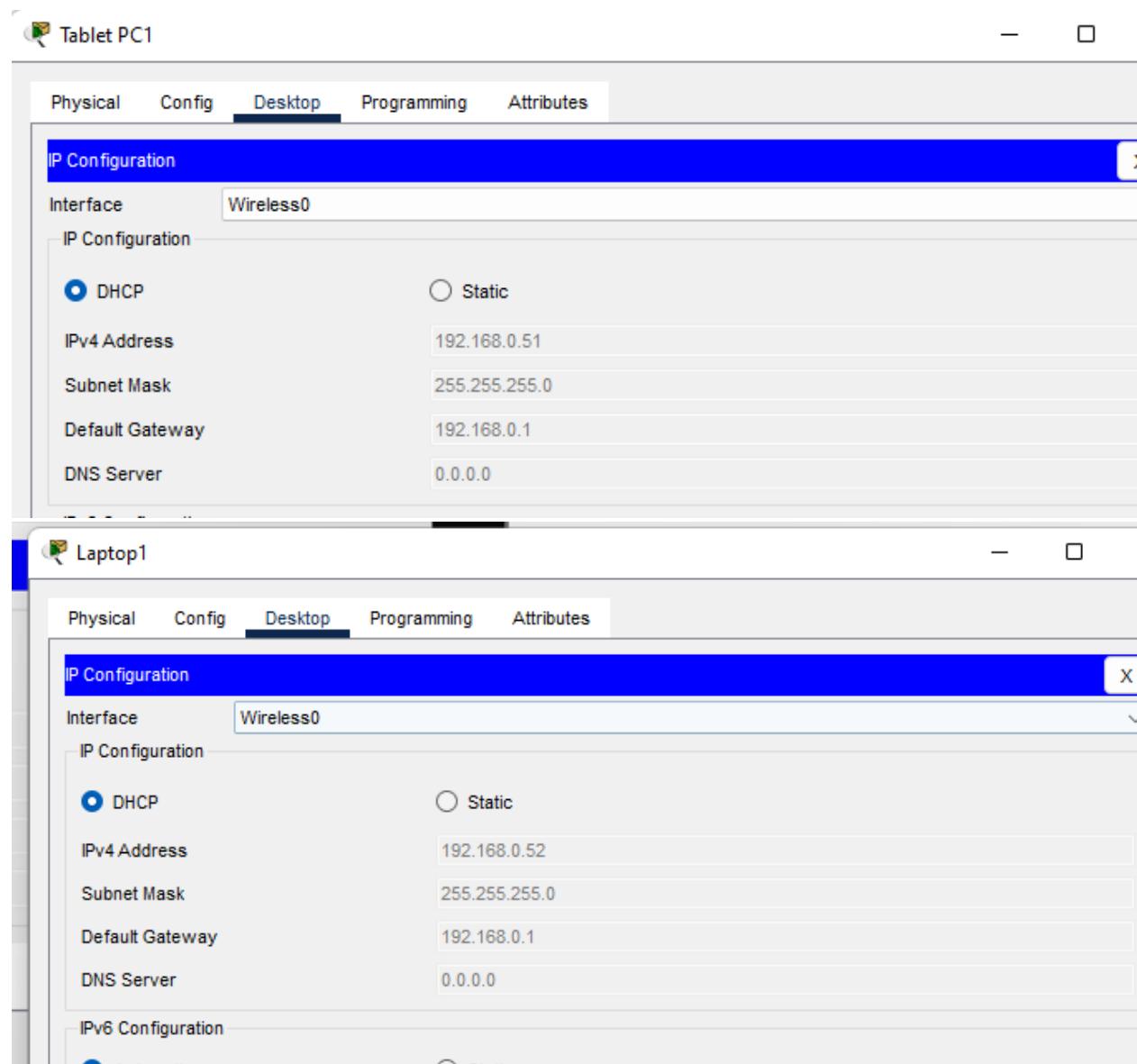
| Cancel | Connect |

Now we configure the Ips dynamic



The screenshot shows a desktop configuration interface for a server named "Server2". The top navigation bar includes tabs for Physical, Config, Services, Desktop (which is selected), Programming, and Attributes. Below the navigation bar, a blue header bar displays "IP Configuration". The main content area is titled "IP Configuration" and contains the following settings:

Setting	Value
DHCP	<input checked="" type="radio"/>
IPv4 Address	192.168.0.50
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	0.0.0.0



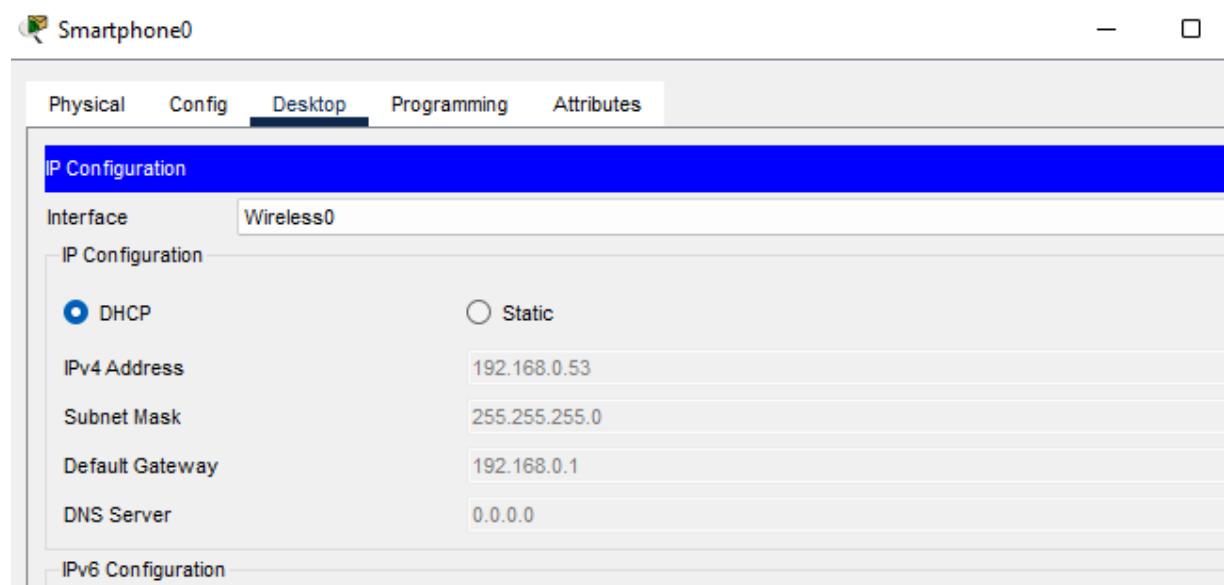
The image shows two separate windows for managing network configurations on different devices.

**Tablet PC1 Configuration:**

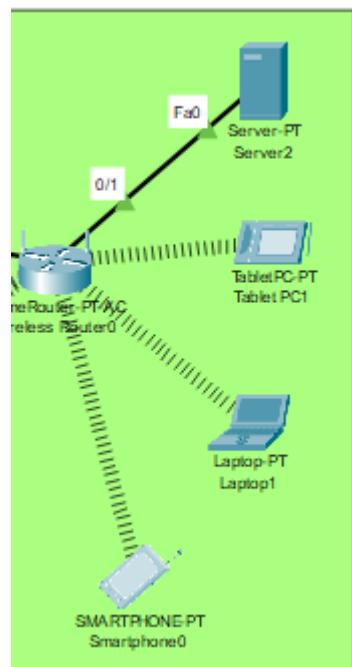
- Interface:** Wireless0
- IP Configuration:**
  - Method:** DHCP (selected)
  - IPv4 Address:** 192.168.0.51
  - Subnet Mask:** 255.255.255.0
  - Default Gateway:** 192.168.0.1
  - DNS Server:** 0.0.0.0

**Laptop1 Configuration:**

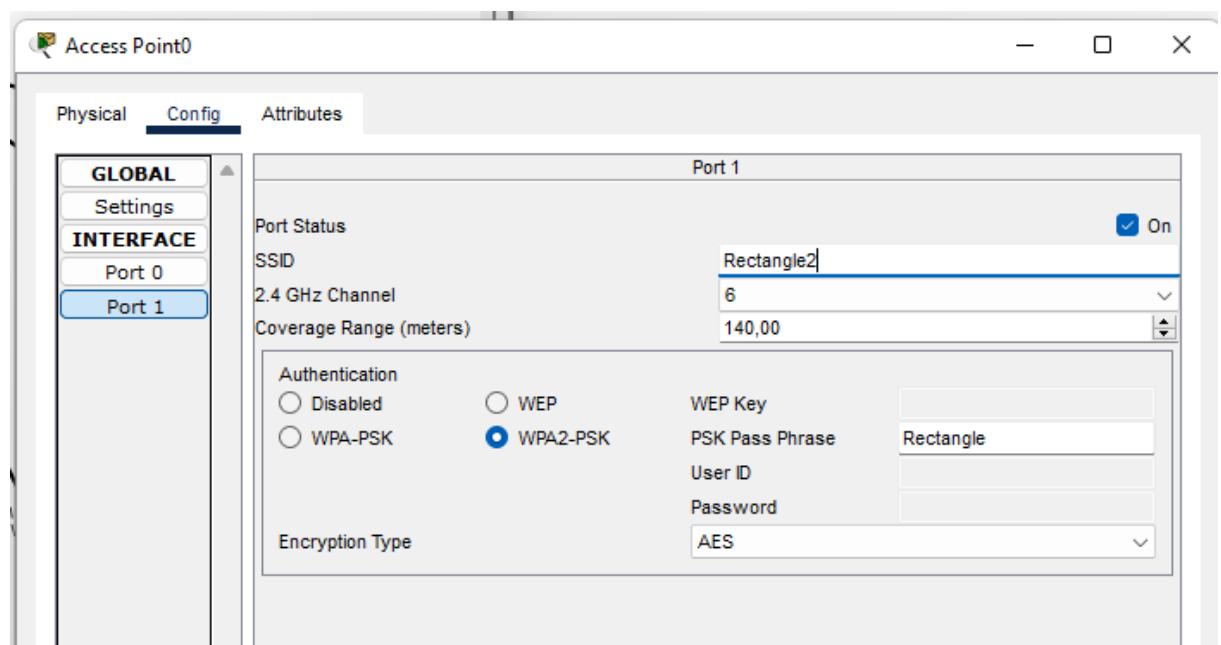
- Interface:** Wireless0
- IP Configuration:**
  - Method:** DHCP (selected)
  - IPv4 Address:** 192.168.0.52
  - Subnet Mask:** 255.255.255.0
  - Default Gateway:** 192.168.0.1
  - DNS Server:** 0.0.0.0
- IPv6 Configuration:** (This section is partially visible at the bottom of the window)



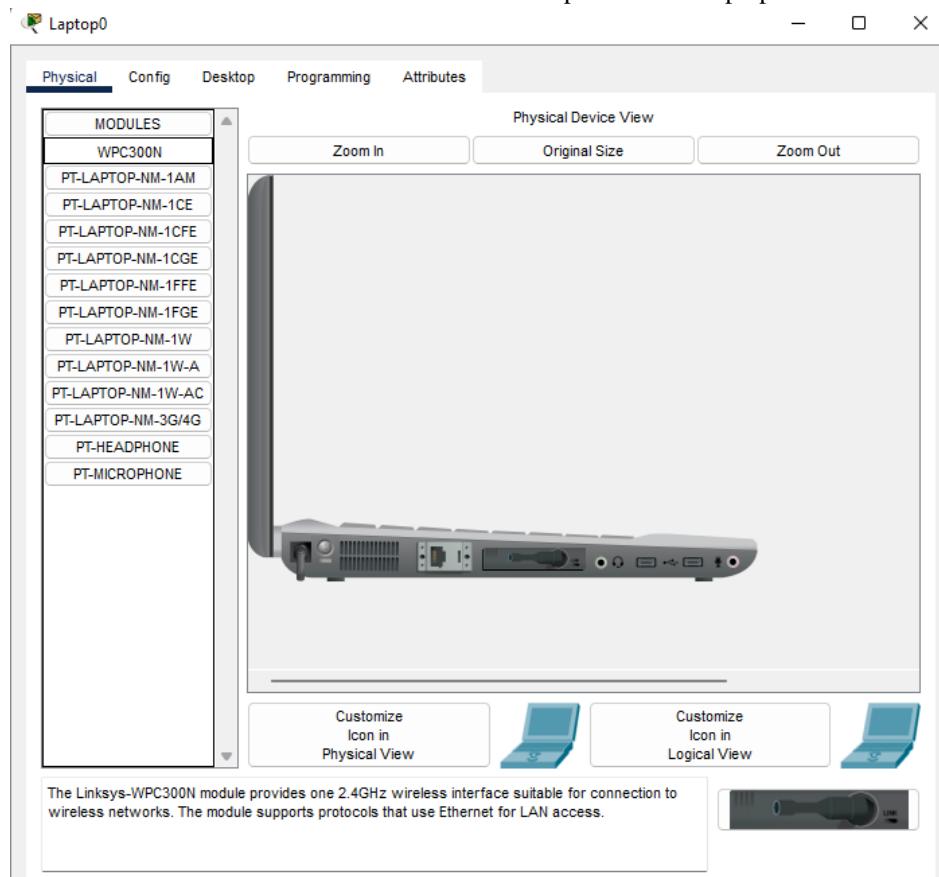
The result is the next one



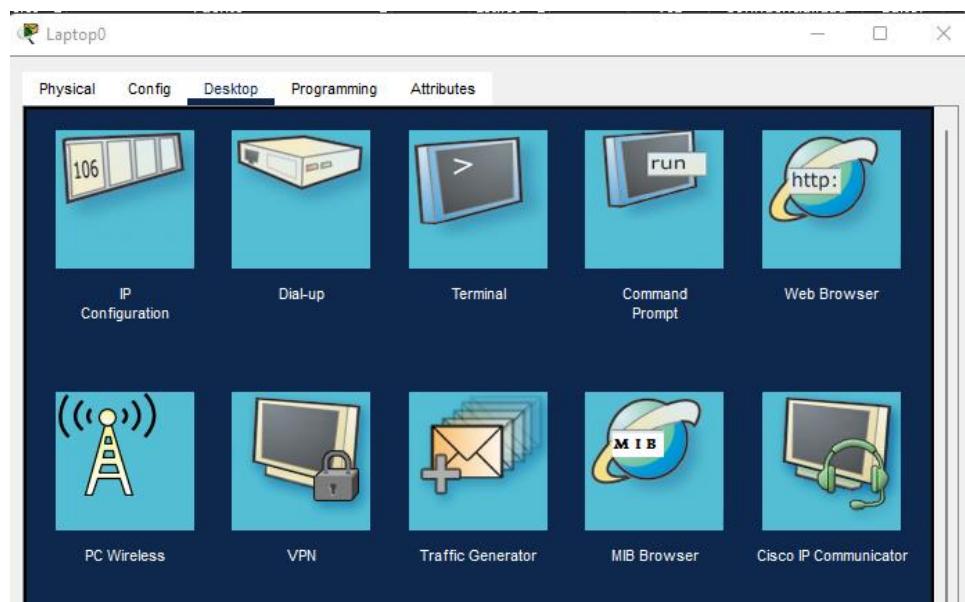
Now we configure the access Point0



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



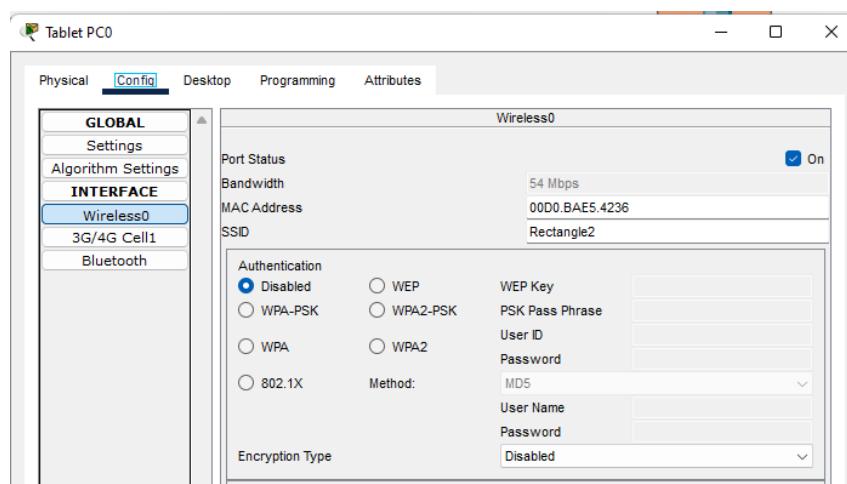
We go to PC wireless connection



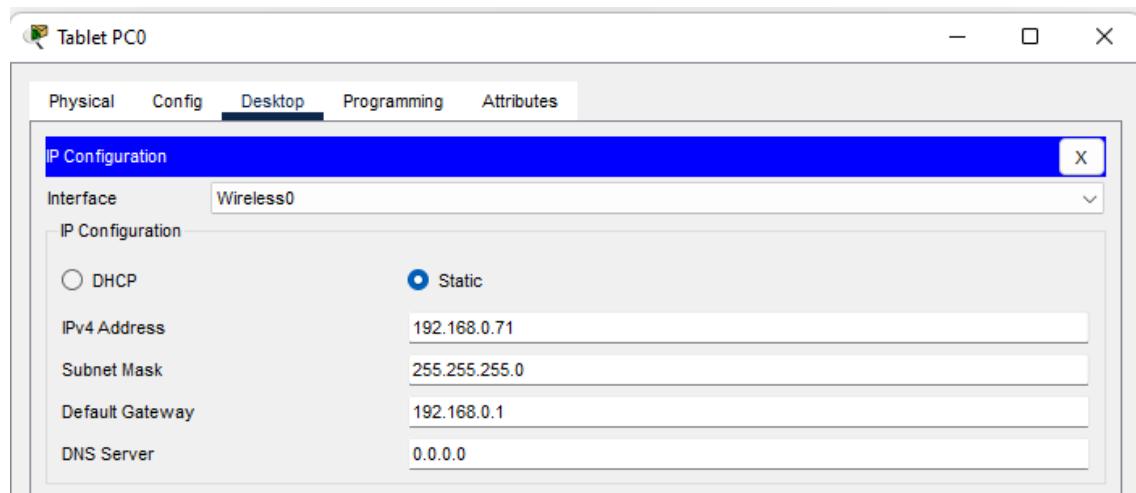
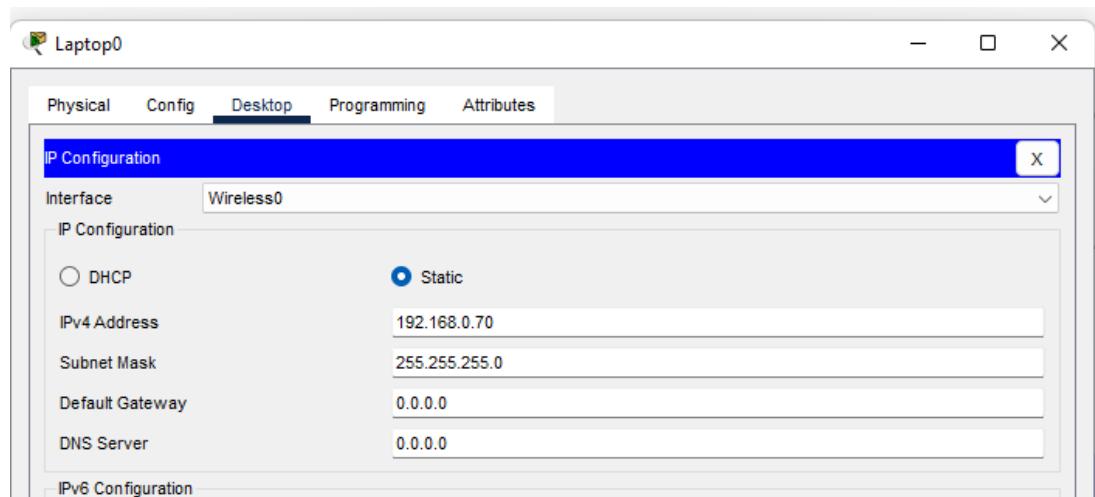
We connect to network SSID with Rectangle2

Wireless Network Name	CH	Signal
Rectangle	1	74%
Rectangle2	1	54%

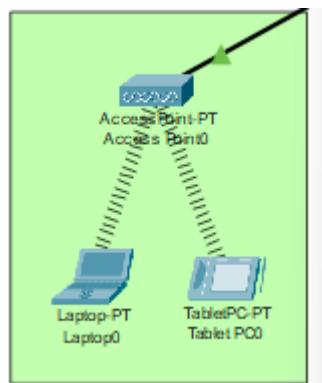
To connect to the tablet PC we go to config and then select Wireless0 and set the SSID Rectangle2



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



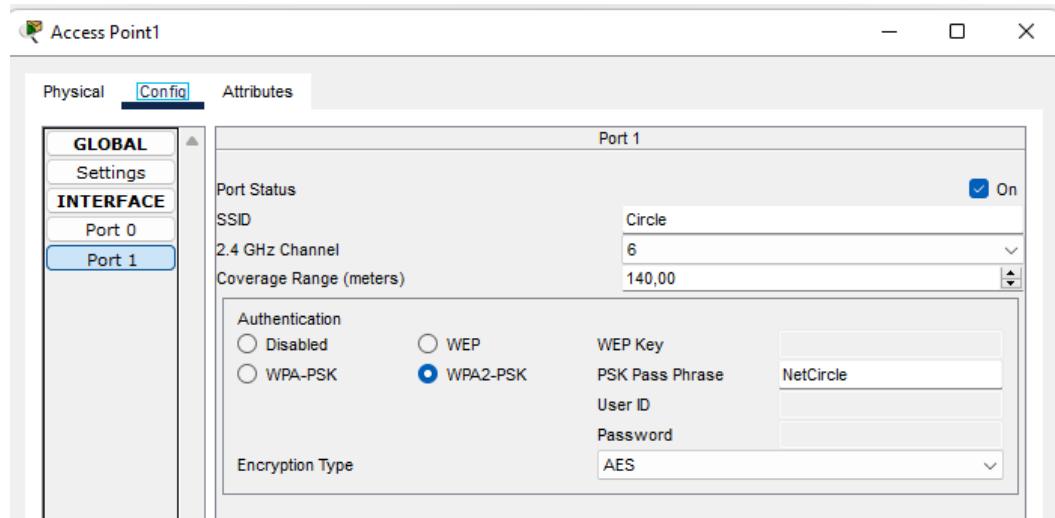
- Purple Wireless Network (Circles)
  - ~ Wireless network identifier - SSID: Circle



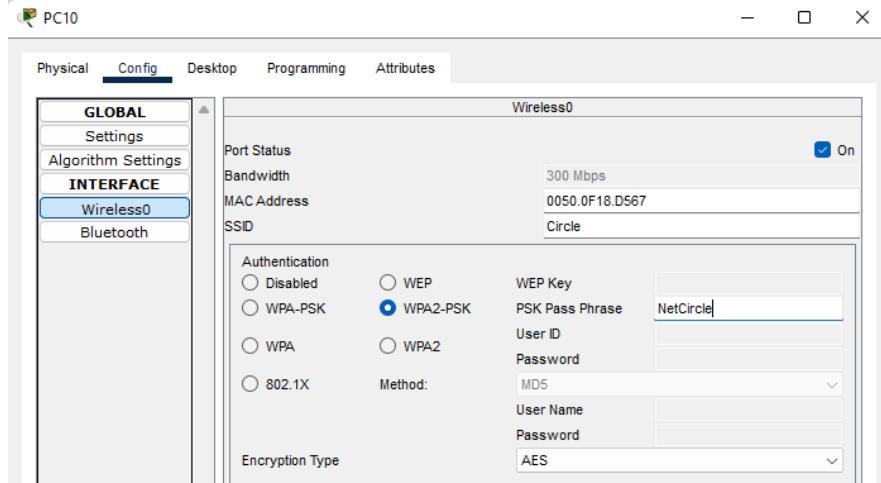
- ~ Access mechanism for wireless clients: WPA2-PSK with AES



- ~ Access Point password for mobile devices: NetCircle



- We assign to each device and wireless0 interface the port1 of the access Point1



**PC10**

**Wireless0**

Port Status: On  
 Bandwidth: 300 Mbps  
 MAC Address: 0050.0F18.D567  
 SSID: Circle

Authentication:

- Disabled
- WEP
- WPA-PSK (selected)
- WPA
- 802.1X

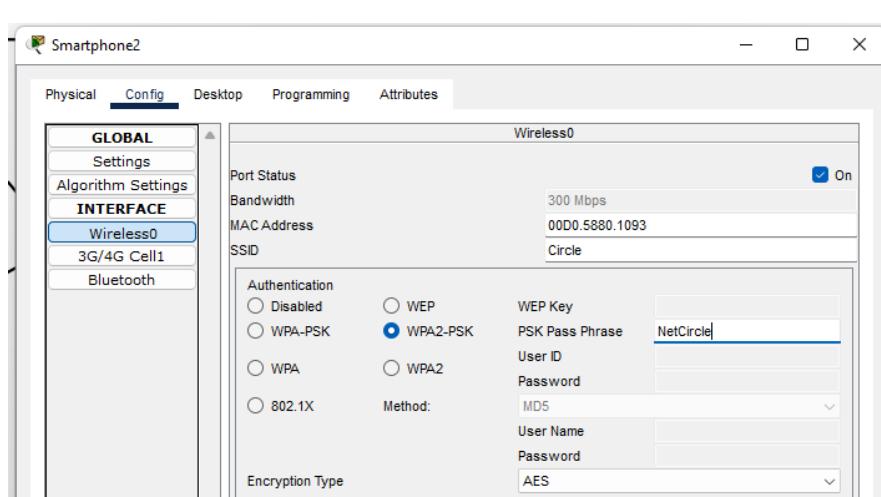
Method: MD5

PSK Pass Phrase: NetCircle

User ID:

Password:

Encryption Type: AES

**Smartphone2**

**Wireless0**

Port Status: On  
 Bandwidth: 300 Mbps  
 MAC Address: 00D0.5880.1093  
 SSID: Circle

Authentication:

- Disabled
- WEP
- WPA-PSK (selected)
- WPA
- 802.1X

Method: MD5

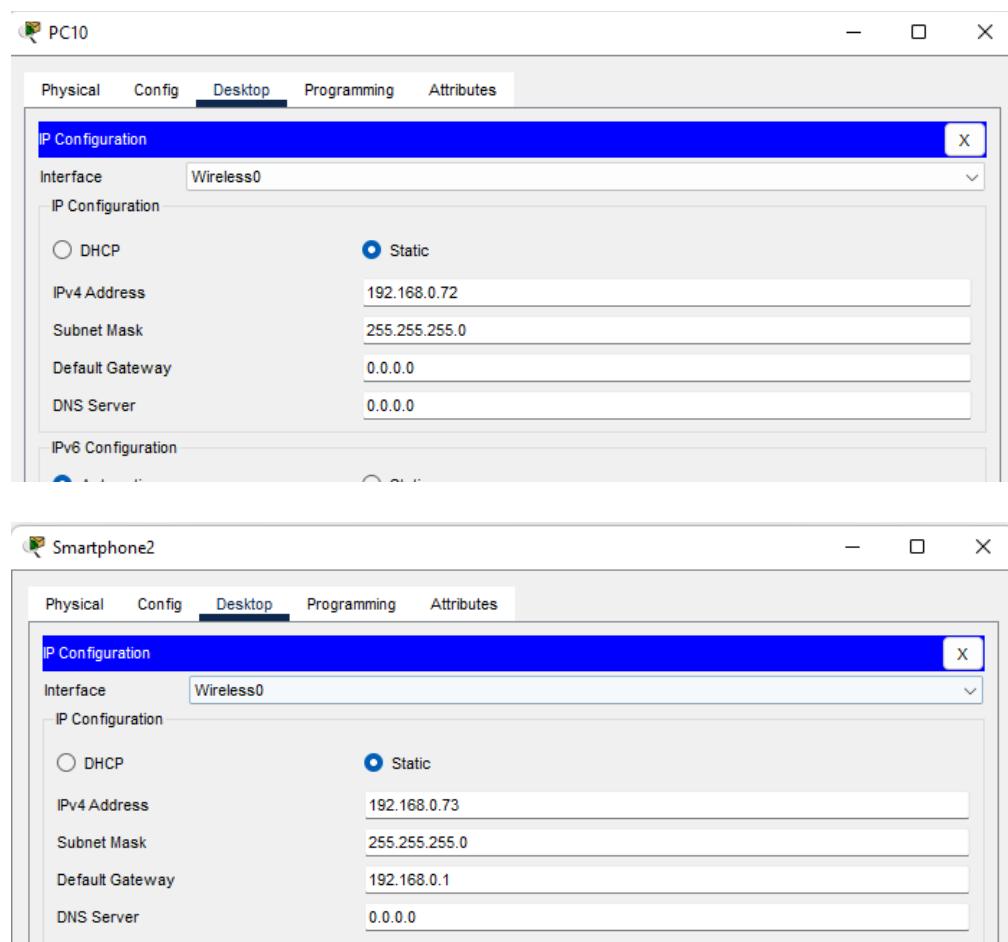
PSK Pass Phrase: NetCircle

User ID:

Password:

Encryption Type: AES

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



The image shows two windows from the WinBox network configuration tool.

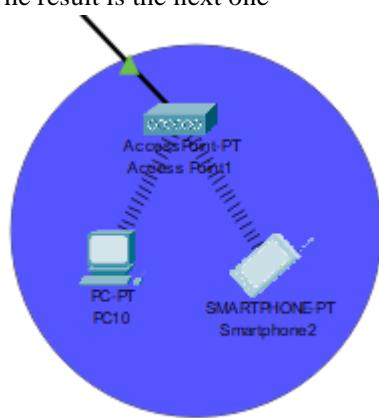
**PC10 Configuration:**

Setting	Value
Interface	Wireless0
IP Configuration	Static (selected)
IPv4 Address	192.168.0.72
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

**Smartphone2 Configuration:**

Setting	Value
Interface	Wireless0
IP Configuration	Static (selected)
IPv4 Address	192.168.0.73
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	0.0.0.0

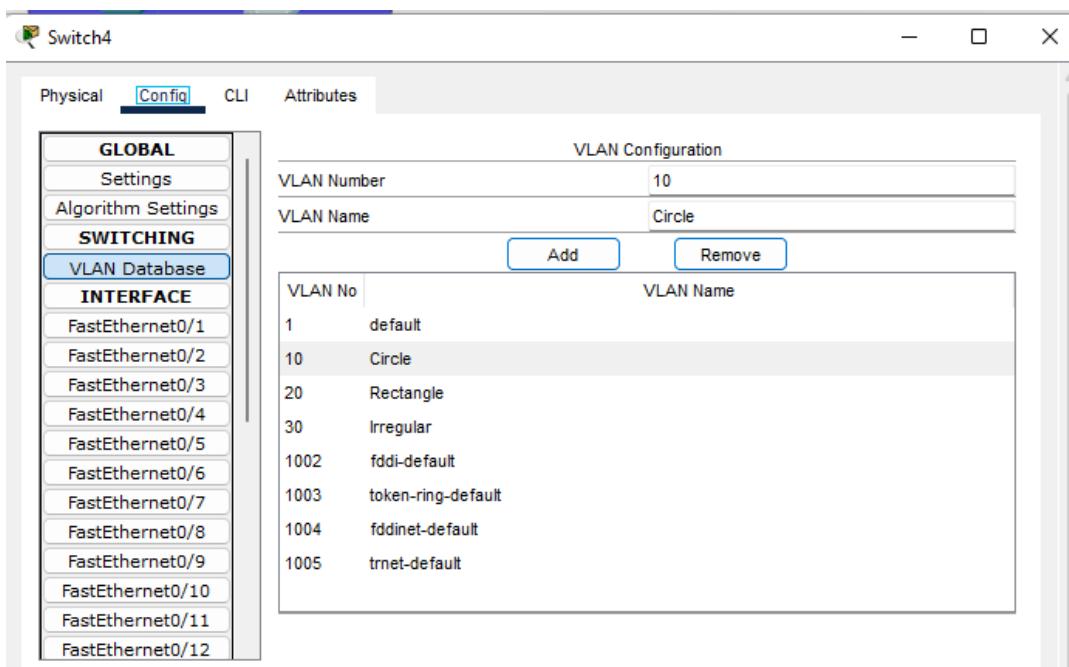
- The result is the next one

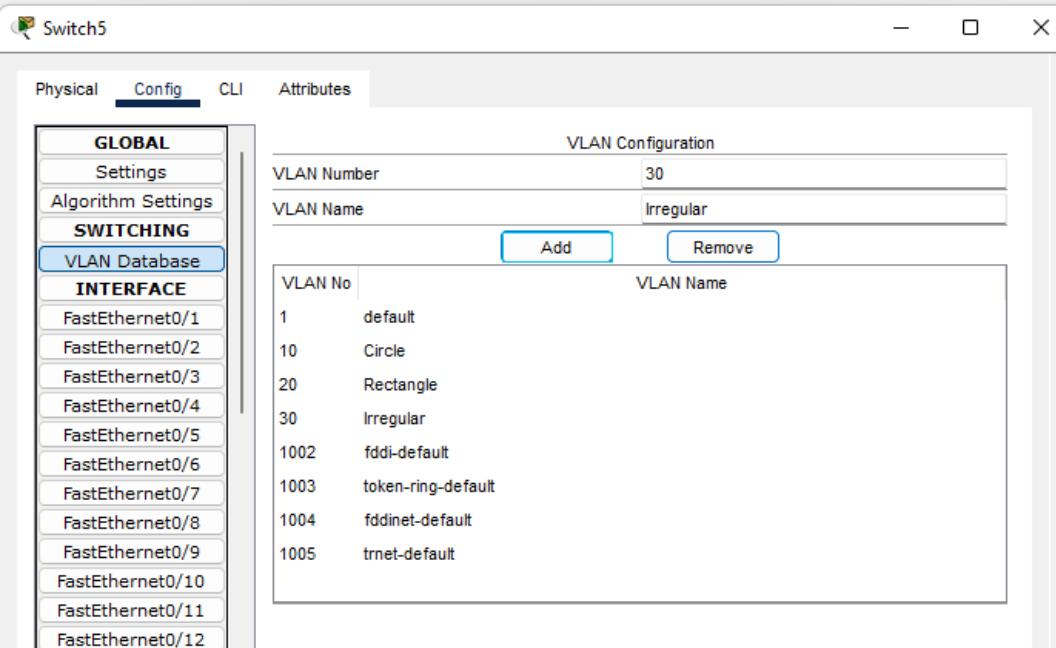


We verify connectivity between all devices. Packet transmission works between devices with wireless networks or wired networks but not between them. Additionally, devices connected to the homeRouter cannot be accessed from outside of it.

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Server3	Server1	ICMP	Black	0.000	N	0	(edit)	
●	Successful	Server2	Tablet PC1	ICMP	Magenta	0.000	N	1	(edit)	
●	Failed	Server2	Server1	ICMP	Dark Green	0.000	N	2	(edit)	
●	Successful	Server1	PC5	ICMP	Magenta	0.000	N	3	(edit)	
●	Failed	PC10	PC7	ICMP	Cyan	0.000	N	4	(edit)	
●	Successful	Tablet PC0	PC10	ICMP	Magenta	0.000	N	5	(edit)	
●	Successful	Laptop0	Smartphone2	ICMP	Magenta	0.000	N	6	(edit)	
●	Failed	Tablet PC0	Laptop1	ICMP	Brown	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.





Switch5

Physical Config CLI Attributes

**GLOBAL**

Settings Algorithm Settings **SWITCHING**

**VLAN Database**

**INTERFACE**

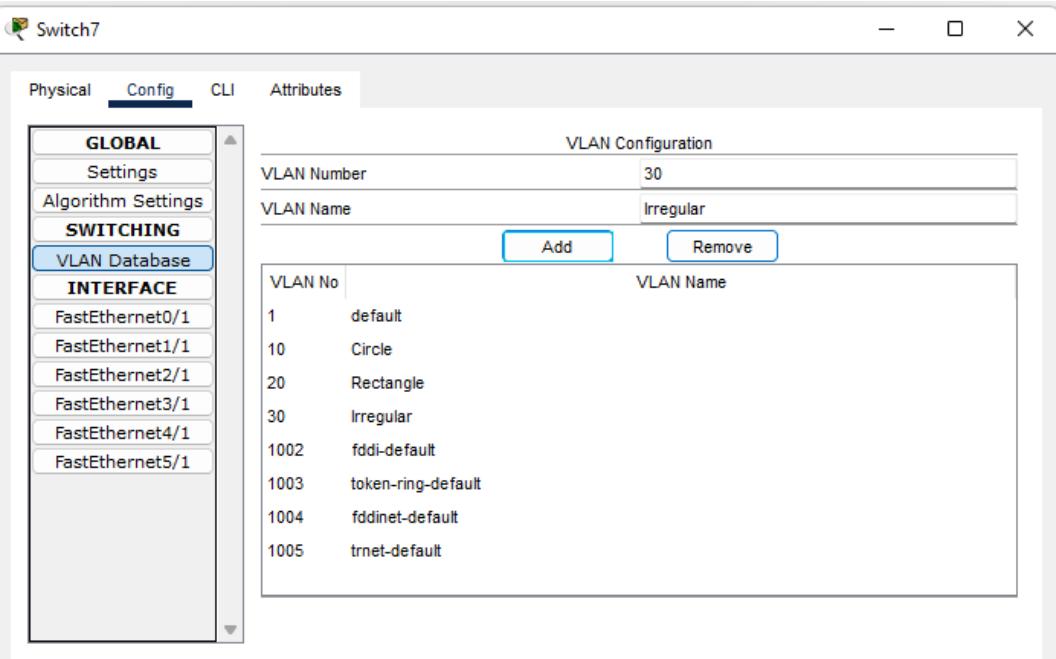
FastEthernet0/1 FastEthernet0/2 FastEthernet0/3 FastEthernet0/4 FastEthernet0/5 FastEthernet0/6 FastEthernet0/7 FastEthernet0/8 FastEthernet0/9 FastEthernet0/10 FastEthernet0/11 FastEthernet0/12

**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**

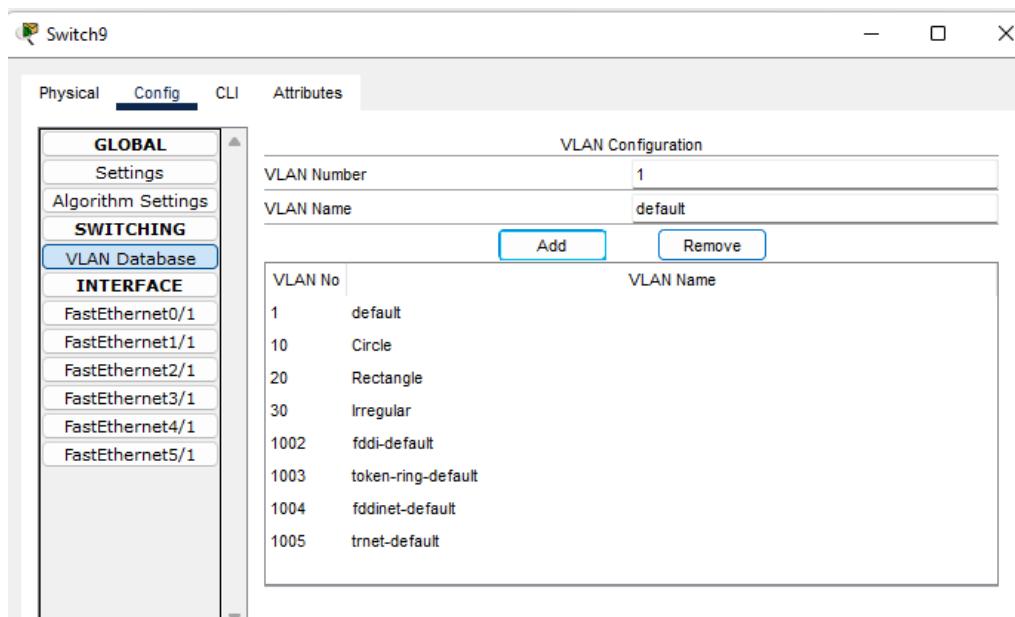
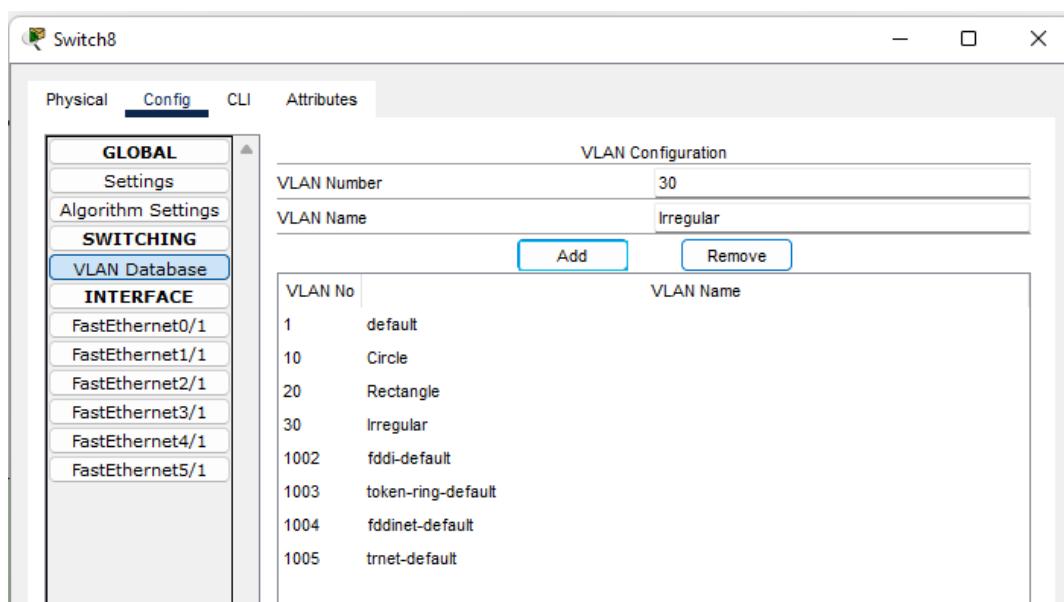
FastEthernet0/1 FastEthernet1/1 FastEthernet2/1 FastEthernet3/1 FastEthernet4/1 FastEthernet5/1

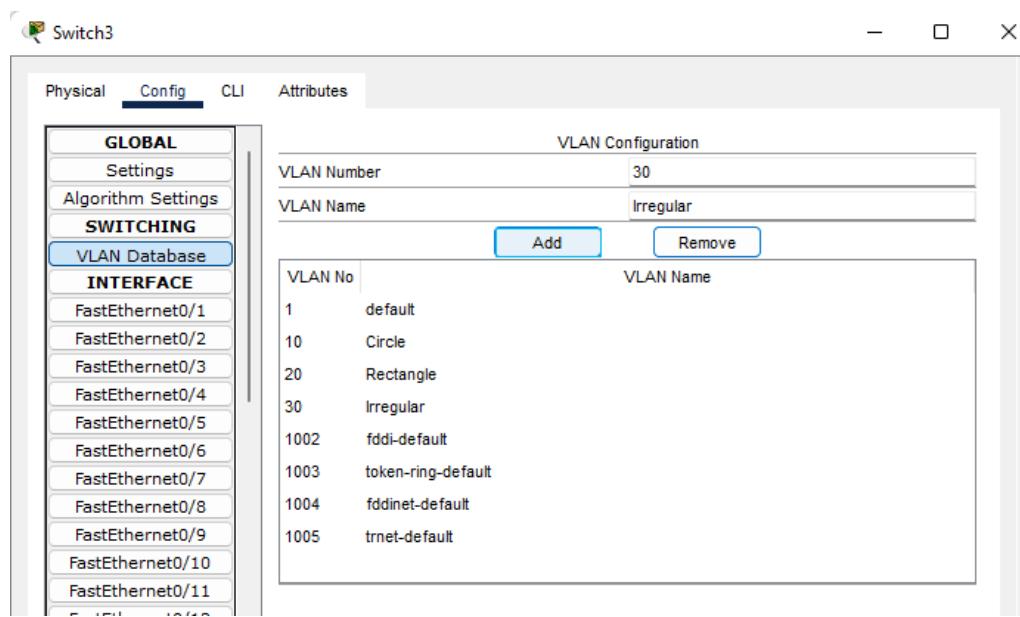
**VLAN Configuration**

VLAN Number	30
VLAN Name	Irregular

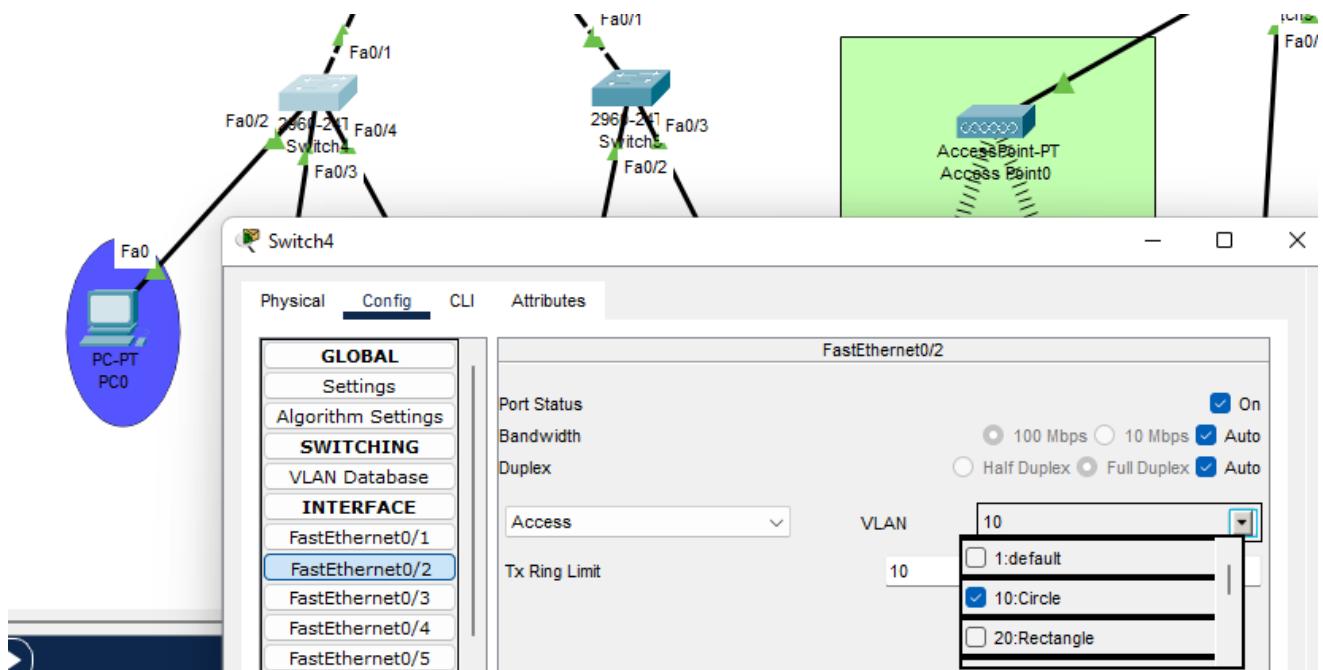
Add Remove

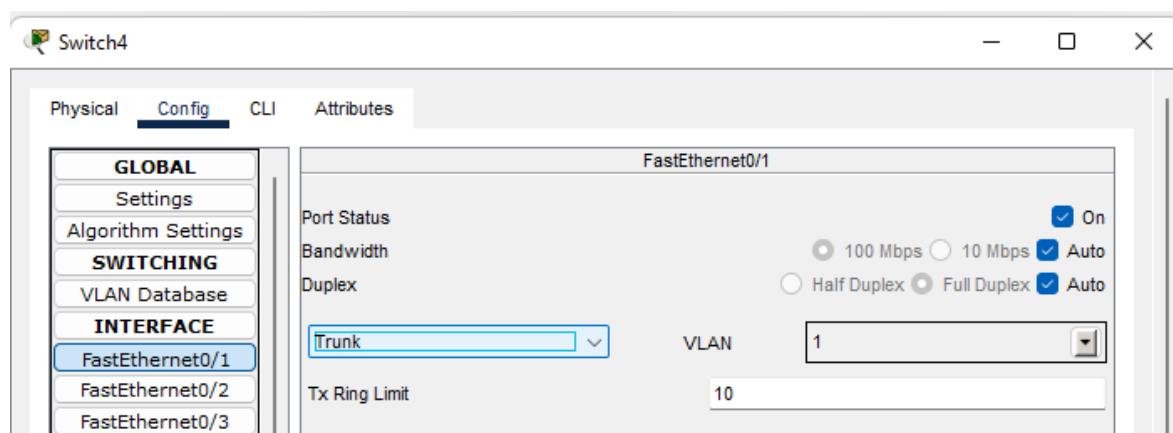
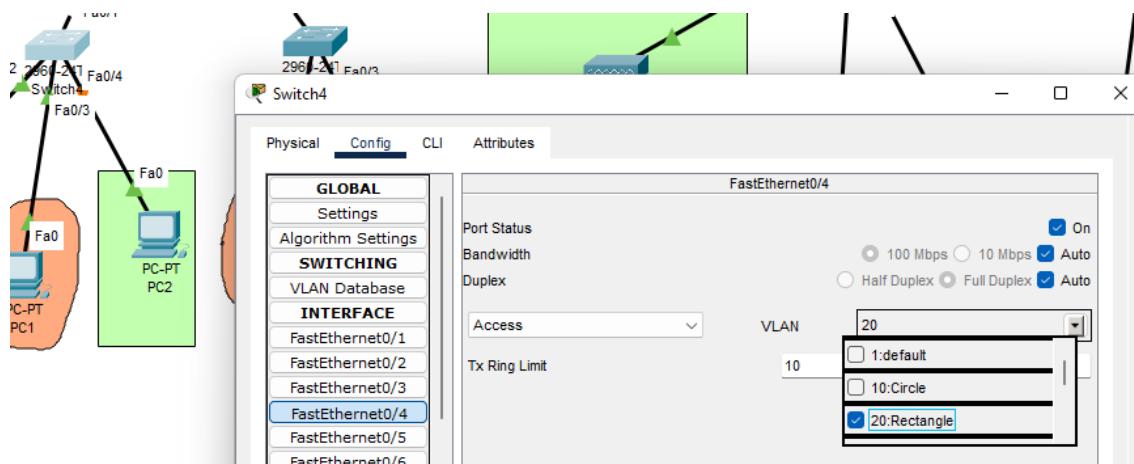
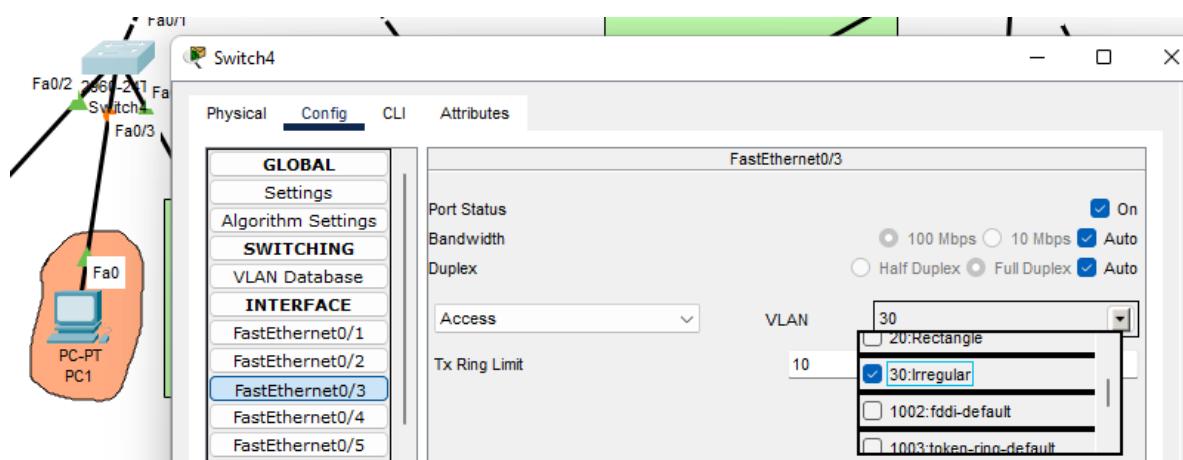
VLAN No	VLAN Name
1	default
10	Circle
20	Rectangle
30	Irregular
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default





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.



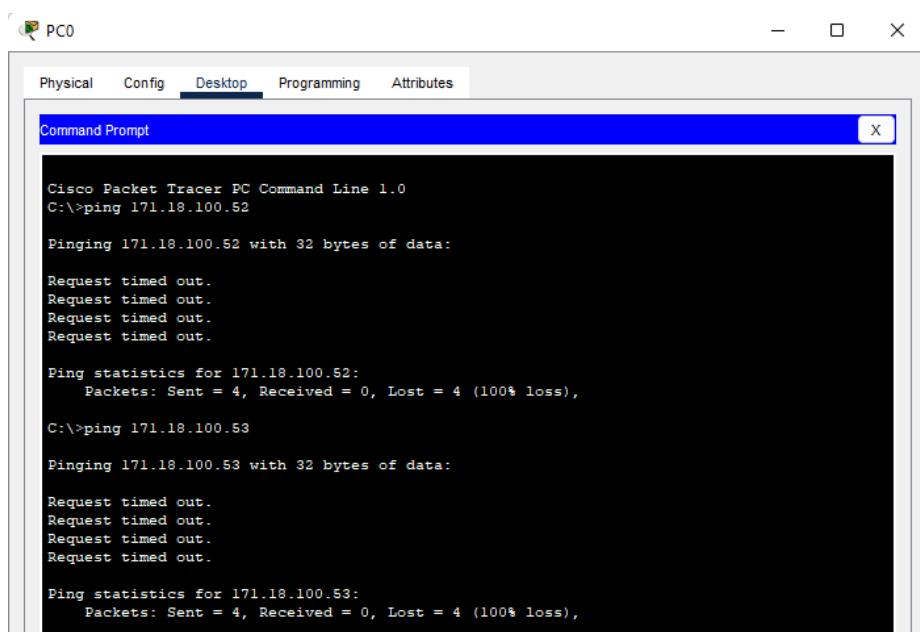


Now we will perform connection tests using the **ping** commands and the packet-sending interface in Packet Tracer. We verify that the network operates as expected according to the configured VLANs.

- Packet sending.

●	Successful	PC0	PC6	ICMP	[Color Box]
●	Successful	PC0	PC5	ICMP	[Color Box]
●	Successful	PC0	PC5	ICMP	[Color Box]
●	Successful	PC6	PC0	ICMP	[Color Box]
●	Successful	PC0	Server1	ICMP	[Color Box]
●	Failed	PC10	PC0	ICMP	[Color Box]
●	Failed	Smartph...	PC0	ICMP	[Color Box]
●	Successful	Smartph...	PC10	ICMP	[Color Box]

- Pings



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 171.18.100.52

Pinging 171.18.100.52 with 32 bytes of data:

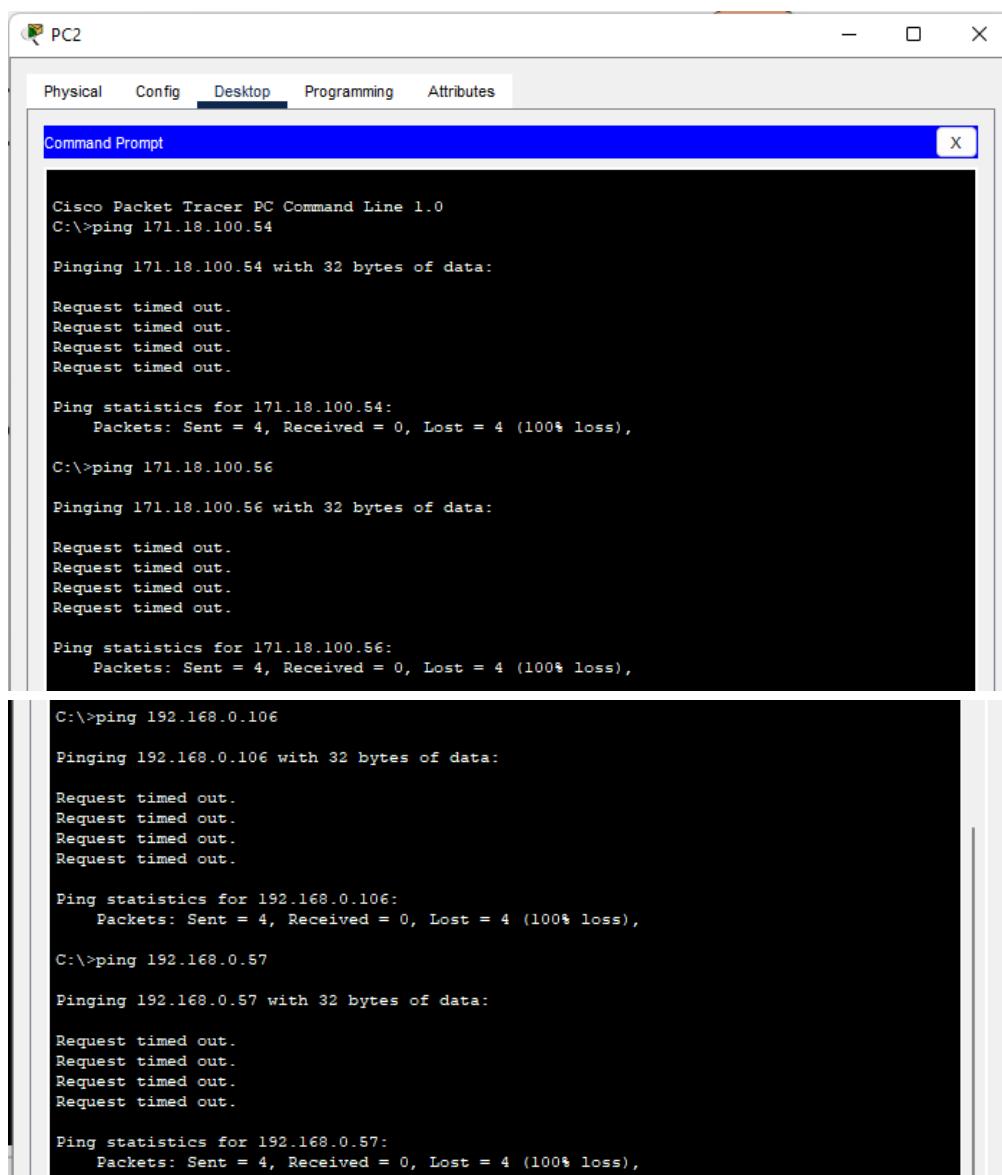
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 171.18.100.52:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 171.18.100.53

Pinging 171.18.100.53 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 171.18.100.53:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



```
PC2

Physical Config Desktop Programming Attributes

Command Prompt

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

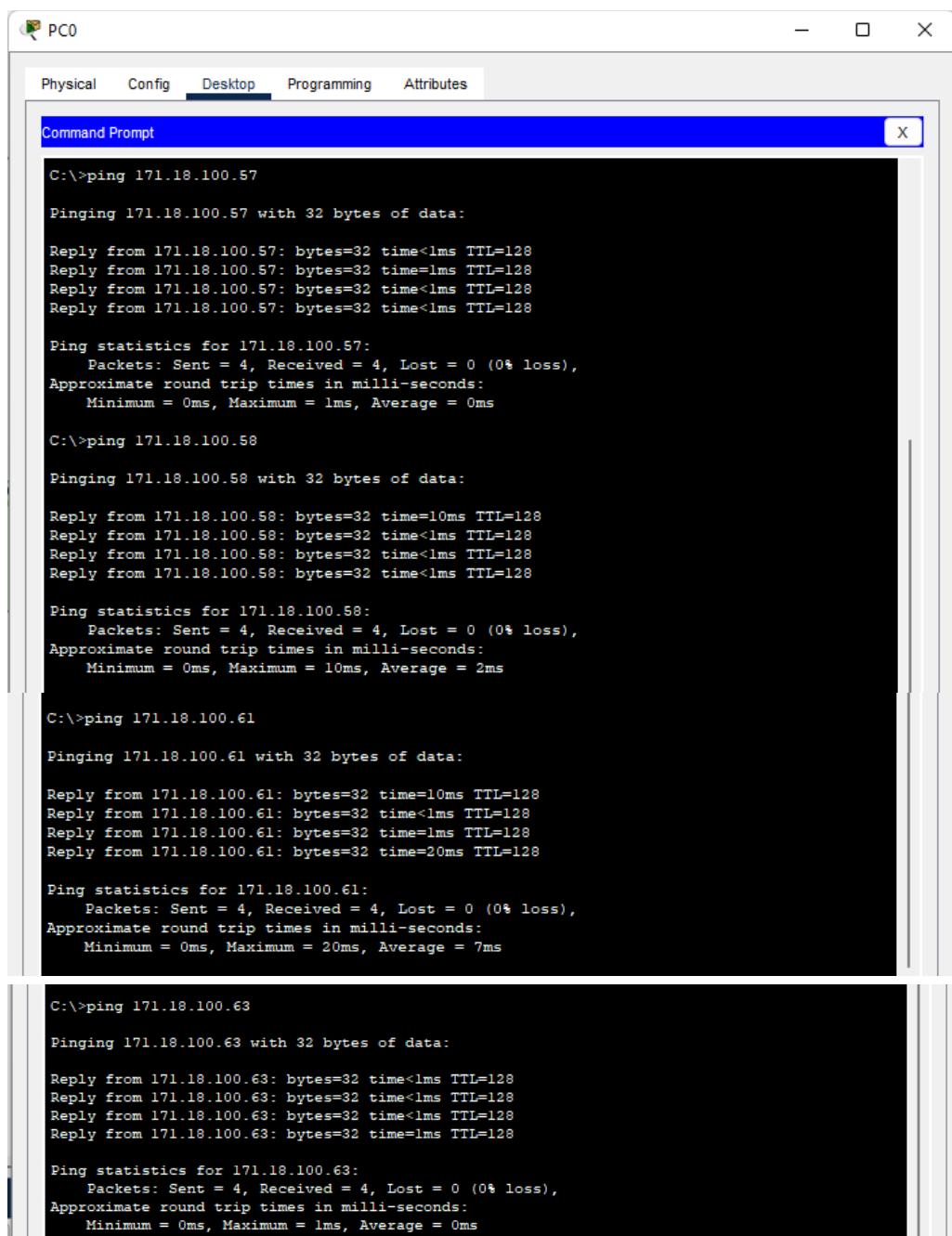
Ping statistics for 171.18.100.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

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
```



The screenshot shows a Windows Command Prompt window titled "PC0" with the "Desktop" tab selected. The window displays the output of several "ping" commands:

```
C:\>ping 171.18.100.57
Pinging 171.18.100.57 with 32 bytes of data:
Reply from 171.18.100.57: bytes=32 time<1ms TTL=128
Reply from 171.18.100.57: bytes=32 time=1ms TTL=128
Reply from 171.18.100.57: bytes=32 time<1ms TTL=128
Reply from 171.18.100.57: bytes=32 time<1ms TTL=128

Ping statistics for 171.18.100.57:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 171.18.100.58
Pinging 171.18.100.58 with 32 bytes of data:
Reply from 171.18.100.58: bytes=32 time=10ms TTL=128
Reply from 171.18.100.58: bytes=32 time<1ms TTL=128
Reply from 171.18.100.58: bytes=32 time<1ms TTL=128
Reply from 171.18.100.58: bytes=32 time<1ms TTL=128

Ping statistics for 171.18.100.58:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

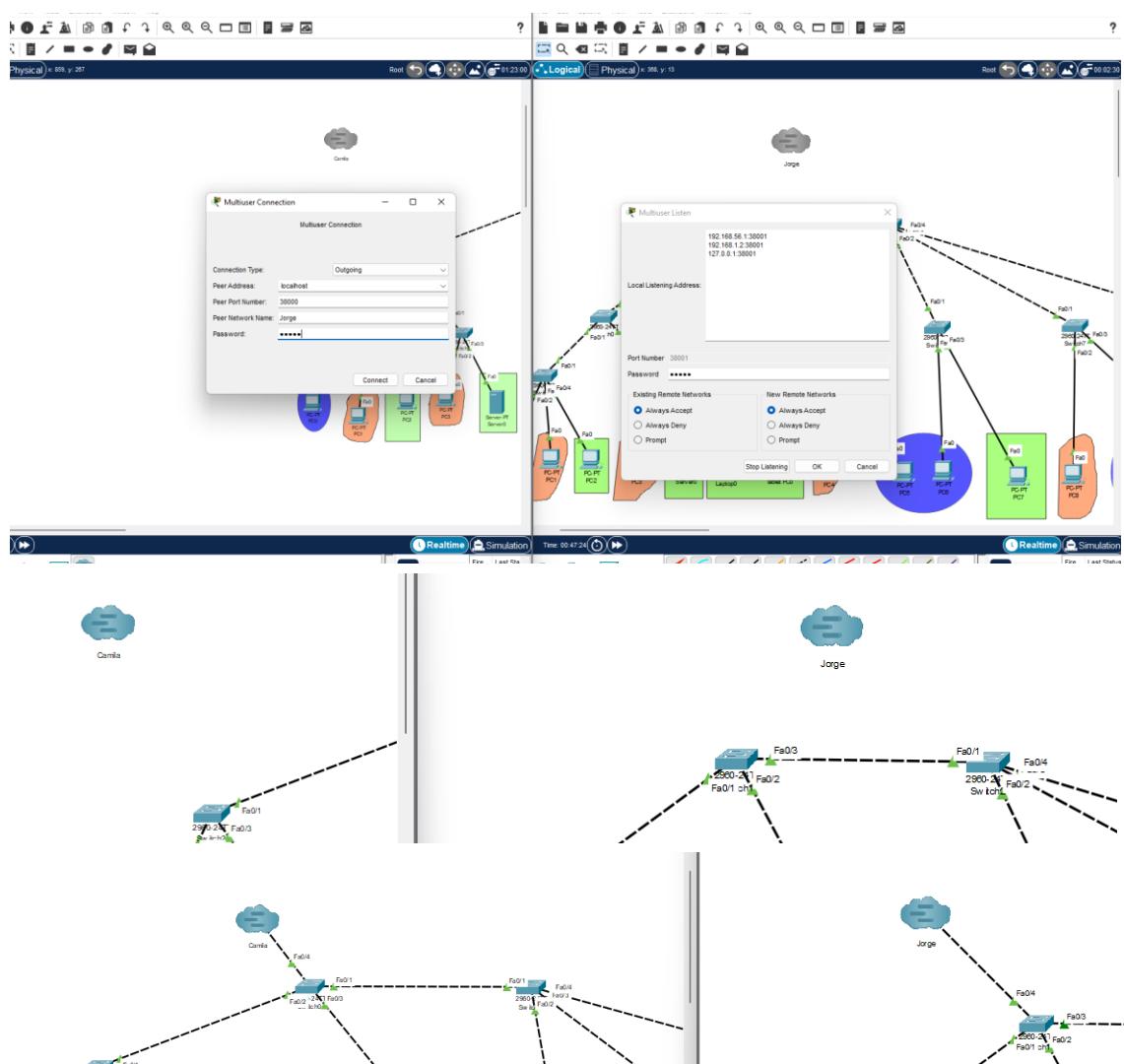
C:\>ping 171.18.100.61
Pinging 171.18.100.61 with 32 bytes of data:
Reply from 171.18.100.61: bytes=32 time=10ms TTL=128
Reply from 171.18.100.61: bytes=32 time<1ms TTL=128
Reply from 171.18.100.61: bytes=32 time=1ms TTL=128
Reply from 171.18.100.61: bytes=32 time=20ms TTL=128

Ping statistics for 171.18.100.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 7ms

C:\>ping 171.18.100.63
Pinging 171.18.100.63 with 32 bytes of data:
Reply from 171.18.100.63: bytes=32 time<1ms TTL=128
Reply from 171.18.100.63: bytes=32 time<1ms TTL=128
Reply from 171.18.100.63: bytes=32 time<1ms TTL=128
Reply from 171.18.100.63: bytes=32 time=1ms TTL=128

Ping statistics for 171.18.100.63:
    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.



```
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:

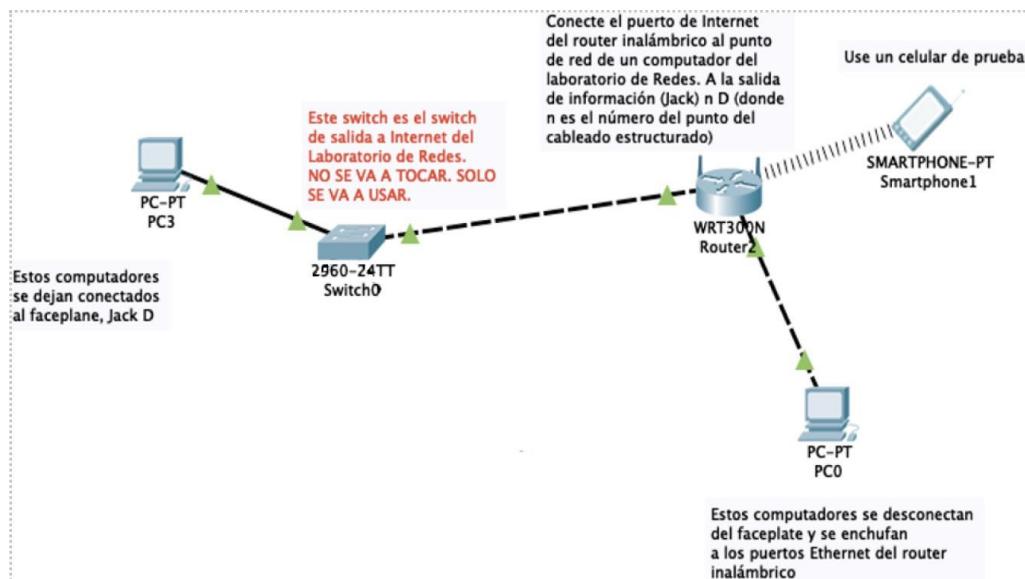
Reply from 171.18.100.51: bytes=32 time<1ms TTL=128
Reply from 171.18.100.51: bytes=32 time=5ms TTL=128
Reply from 171.18.100.51: bytes=32 time<1ms TTL=128
Reply from 171.18.100.51: bytes=32 time=4ms TTL=128

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)

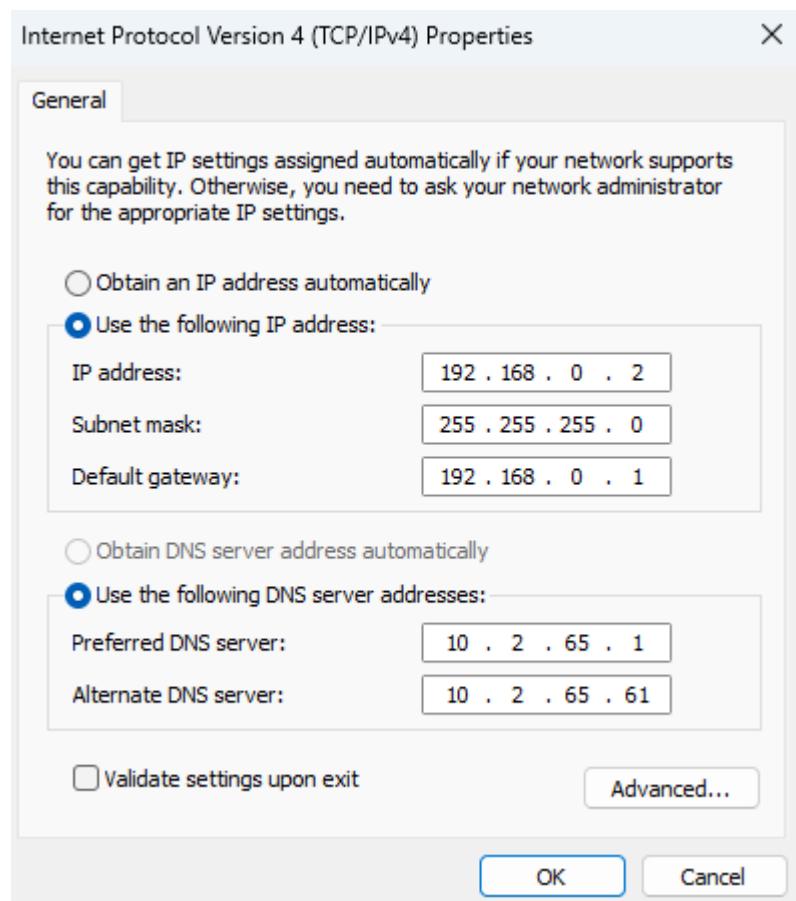


Figure 58. Configuring IP and Subnet Mask on the Computer ("PC0")

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

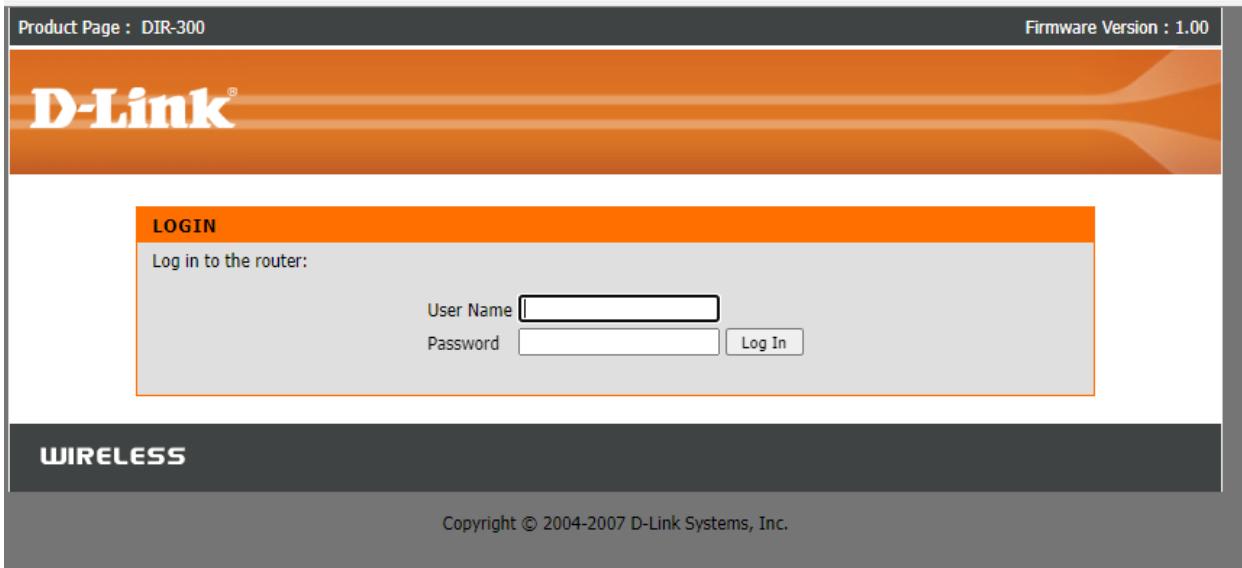


Figure 59. Authenticating to Configure the Wireless Router

- We go to Wireless Setup

Figure 60. Main Menu of the Wireless Router Configuration

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

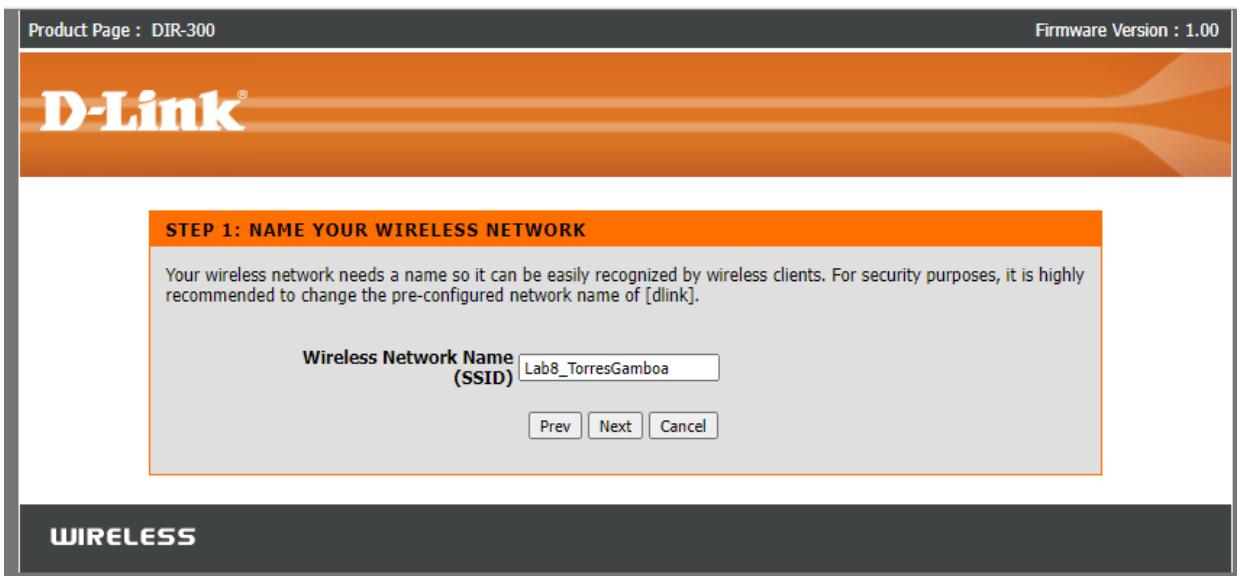


Figure 61. Assigning a Name to the Wireless Network

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

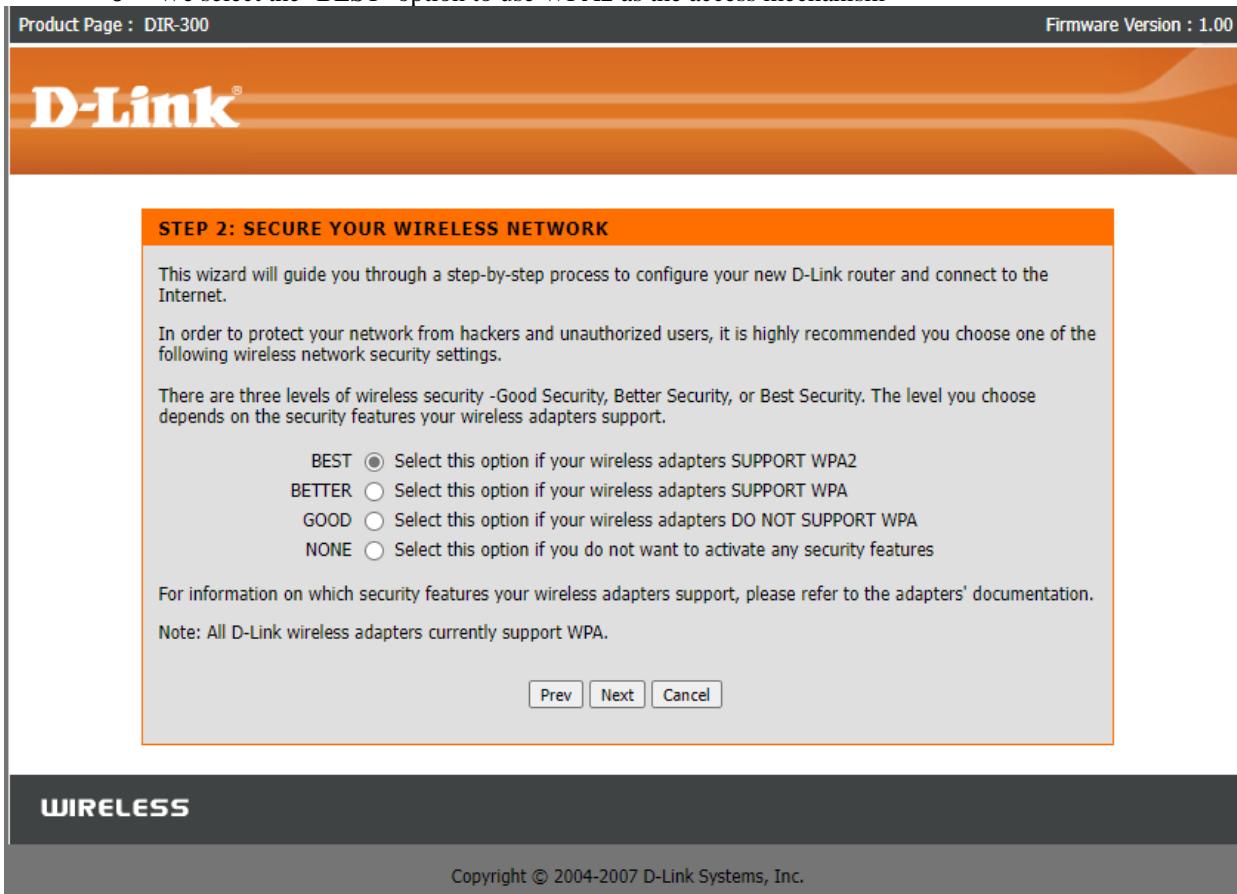


Figure 62. Assigning Access Mechanism to Wireless Clients: WPA2-PSK with AES

- We create the router's access key

Product Page : DIR-300      Firmware Version : 1.00

# D-Link®

**STEP 3: SET YOUR WIRELESS SECURITY PASSWORD**

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password:  (2 to 20 characters)

Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

[Prev](#) [Next](#) [Cancel](#)

**WIRELESS**

Copyright © 2004-2007 D-Link Systems, Inc.

*Figure 63. Assigning a Wireless Security Password*

- We verify the changes and save them

Product Page : DIR-300      Firmware Version : 1.00

# D-Link®

**SETUP COMPLETE!**

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : Lab8\_TorresGamboa

[Prev](#) [Save](#) [Cancel](#)

**WIRELESS**

Copyright © 2004-2007 D-Link Systems, Inc.

*Figure 64. Saving Changes to the Wireless Setup*

- Now, we go to the Internet Connection Wizard

Product Page : DIR-300      Firmware Version : 1.00

# D-Link®

<b>DIR-300 //</b>	<b>SETUP</b>	<b>ADVANCED</b>	<b>MAINTENANCE</b>	<b>STATUS</b>	<b>HELP</b>
<a href="#">Internet Setup</a> <a href="#">Wireless Setup</a> <a href="#">LAN Setup</a> <a href="#">Time and Date</a> <a href="#">Parental Control</a> <a href="#">Logout</a>   <a href="#">Internet Offline</a>  <a href="#">Reboot</a>	<b>INTERNET CONNECTION</b> <p>If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.</p> <b>INTERNET CONNECTION SETUP WIZARD</b> <p>If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.</p> <p style="text-align: center;"><a href="#">Internet Connection Setup Wizard</a></p> <p><b>Note:</b> Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.</p> <b>MANUAL INTERNET CONNECTION OPTIONS</b> <p>If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.</p> <p style="text-align: center;"><a href="#">Manual Internet Connection Setup</a></p>				<b>Helpful Hints..</b> <ul style="list-style-type: none"> <li>• If you are new to networking and have never configured a router before, click on <b>Internet Connection Setup Wizard</b> and the router will guide you through a few simple steps to get your network up and running.</li> <li>• If you consider yourself an advanced user and have configured a router before, click <b>Manual Internet Connection Setup</b> to input all the settings manually.</li> </ul>

Figure 65. Accessing to Internet Connection Setup Wizard

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

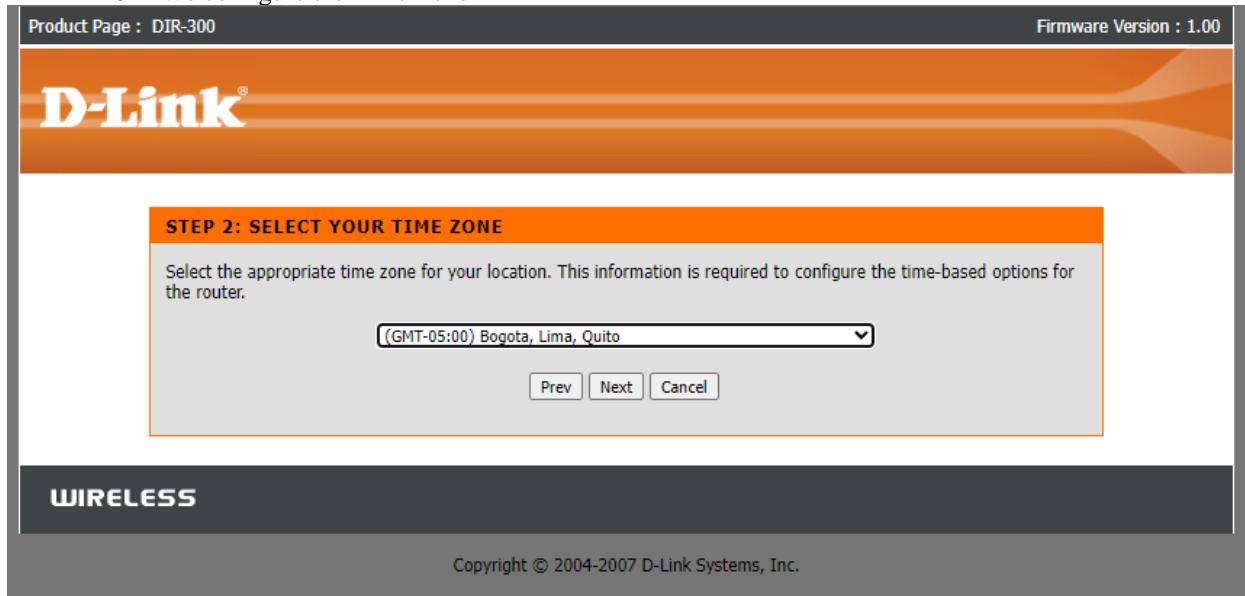
Product Page : DIR-300      Firmware Version : 1.00

# D-Link®

<b>STEP 1: SET YOUR PASSWORD</b> <p>By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:</p> <p>Password : <input type="password"/> Verify Password : <input type="password"/></p> <p style="text-align: center;"><a href="#">Prev</a> <a href="#">Next</a> <a href="#">Cancel</a></p>	
<b>WIRELESS</b> <p>Copyright © 2004-2007 D-Link Systems, Inc.</p>	

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

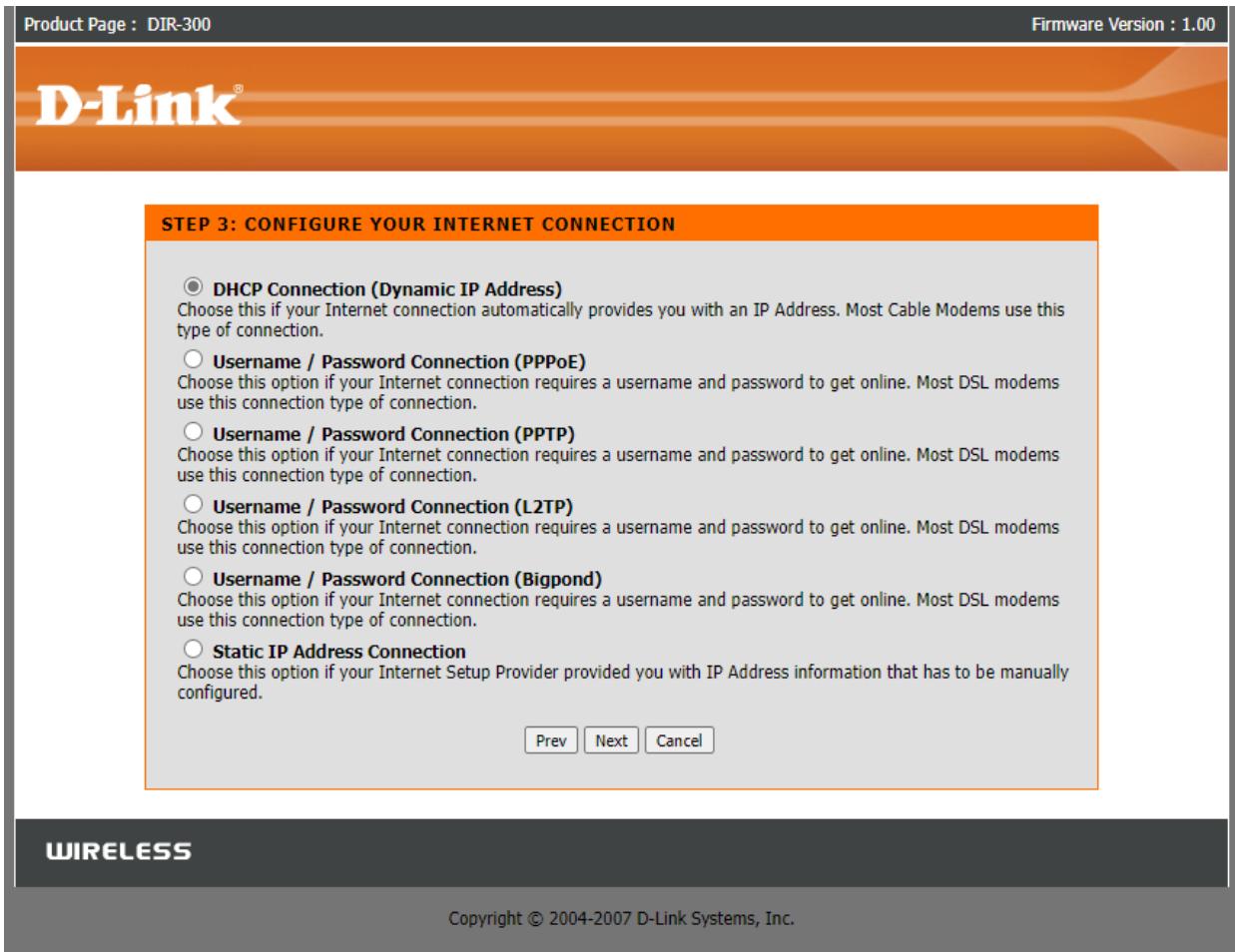


Figure 68. Configuring Internet Connection

- We leave the default option and click Next

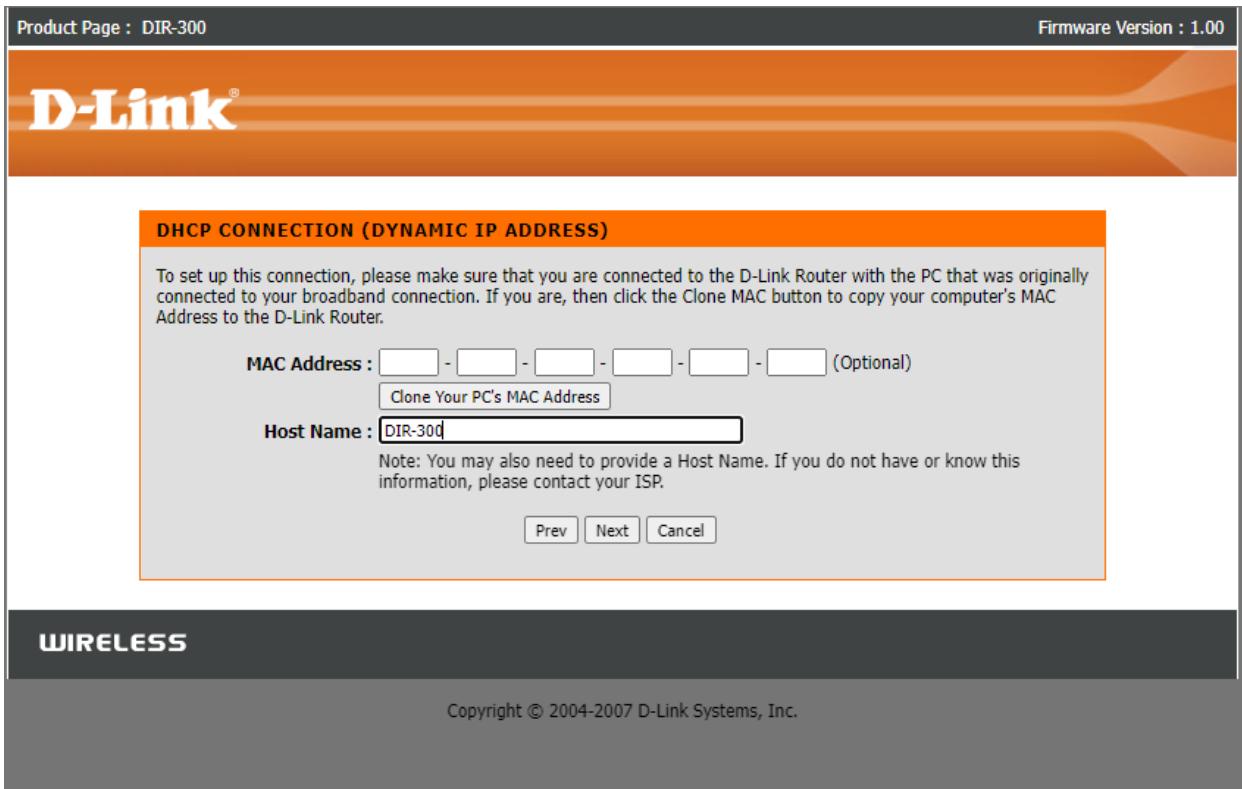
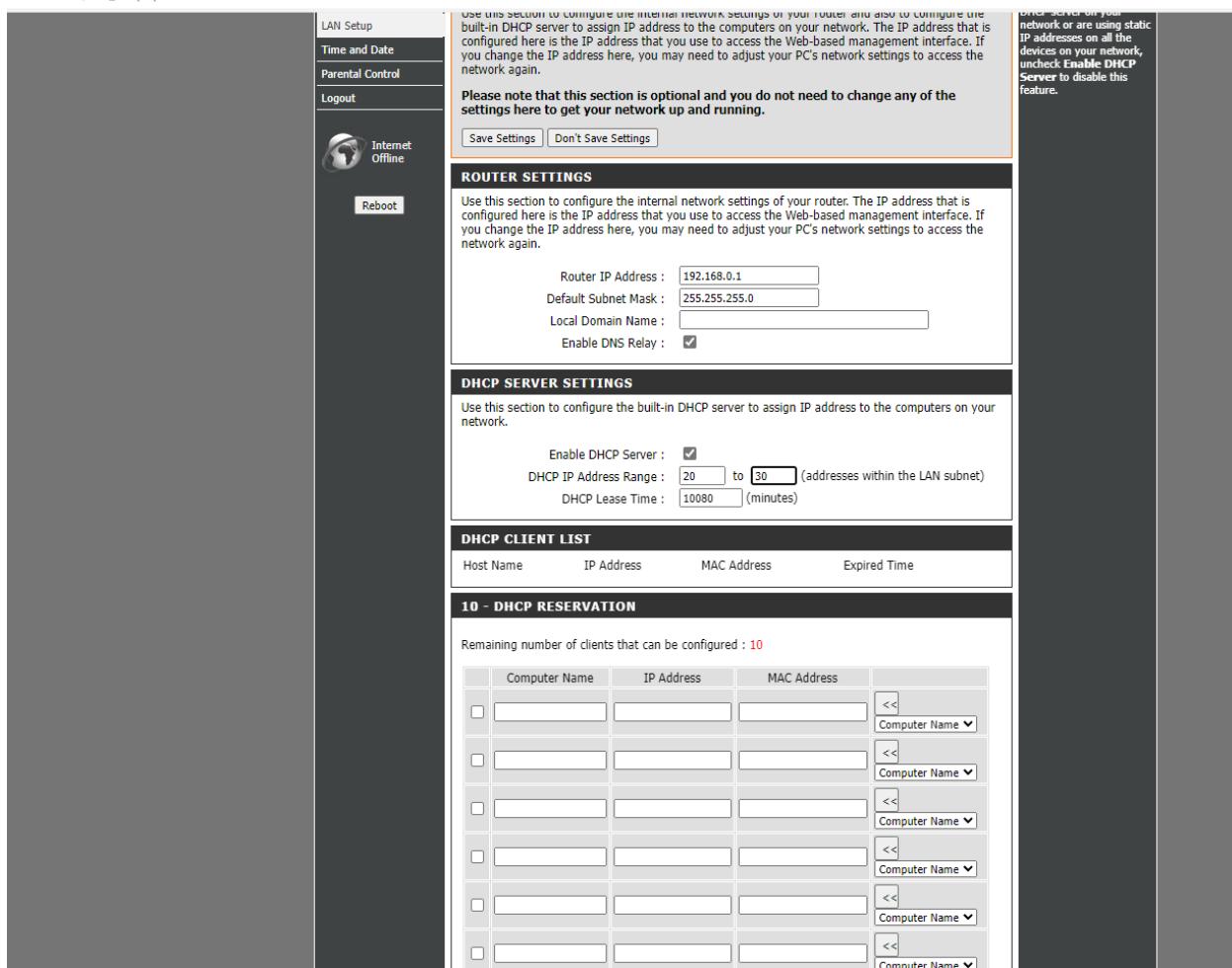


Figure 69. Default Value for the DHCP Connection Section

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

192.168.0.1/bsc\_lan.php



The screenshot shows the router's configuration interface at [192.168.0.1/bsc\\_lan.php](http://192.168.0.1/bsc_lan.php). The left sidebar includes links for LAN Setup, Time and Date, Parental Control, Logout, Internet Offline, and Reboot. The main content area has a header: "Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP address to the computers on your network. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again." Below this, a note says: "Please note that this section is optional and you do not need to change any of the settings here to get your network up and running." There are "Save Settings" and "Don't Save Settings" buttons. The "ROUTER SETTINGS" section follows, with a note: "Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again." It contains fields for Router IP Address (192.168.0.1), Default Subnet Mask (255.255.255.0), Local Domain Name, and Enable DNS Relay (checked). The "DHCP SERVER SETTINGS" section follows, with a note: "Use this section to configure the built-in DHCP server to assign IP address to the computers on your network." It contains fields for Enable DHCP Server (checked), DHCP IP Address Range (20 to 30), and DHCP Lease Time (10080 minutes). The "DHCP CLIENT LIST" section shows a table with columns Host Name, IP Address, MAC Address, and Expired Time. The "10 - DHCP RESERVATION" section shows a table for configuring clients, with columns Computer Name, IP Address, MAC Address, and a dropdown menu for Computer Name.

Figure 70. Configuring IP Address Range on the Wireless Router

- Now, we go to Manual Internet Connection Setup

Product Page : DIR-300

Firmware Version : 1.00

# D-Link®

DIR-300 //	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
<a href="#">Internet Setup</a> <a href="#">Wireless Setup</a> <a href="#">LAN Setup</a> <a href="#">Time and Date</a> <a href="#">Parental Control</a> <a href="#">Logout</a>   <a href="#">Internet Offline</a>  <a href="#">Reboot</a>	<b>INTERNET CONNECTION</b> <p>If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.</p> <b>INTERNET CONNECTION SETUP WIZARD</b> <p>If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.</p> <p style="text-align: center;"><a href="#">Internet Connection Setup Wizard</a></p> <p><b>Note:</b> Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.</p> <b>MANUAL INTERNET CONNECTION OPTIONS</b> <p>If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.</p> <p style="text-align: center;"><a href="#">Manual Internet Connection Setup</a></p>				
	<b>Helpful Hints..</b> <ul style="list-style-type: none"> <li>• If you are new to networking and have never configured a router before, click on <b>Internet Connection Setup Wizard</b> and the router will guide you through a few simple steps to get your network up and running.</li> <li>• If you consider yourself an advanced user and have configured a router before, click <b>Manual Internet Connection Setup</b> to input all the settings manually.</li> </ul>				

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

<b>DIR-300 //</b>	<b>SETUP</b>	<b>ADVANCED</b>	<b>MAINTENANCE</b>	<b>STATUS</b>	<b>HELP</b>																					
<a href="#">Internet Setup</a> <a href="#">Wireless Setup</a> <a href="#">LAN Setup</a> <a href="#">Time and Date</a> <a href="#">Parental Control</a> <a href="#">Logout</a>	<div style="background-color: #FF9900; color: white; padding: 5px;"> <b>INTERNET CONNECTION</b> </div> <p>Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.</p> <p><b>Note:</b> If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.</p> <p><input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/></p> <hr/> <div style="background-color: #333333; color: white; padding: 2px;"> <b>ACCESS POINT MODE</b> </div> <p>Use this to disable NAT on the router and turn it into an Access Point.</p> <p><input type="checkbox"/> Enable Access Point Mode</p> <hr/> <div style="background-color: #333333; color: white; padding: 2px;"> <b>INTERNET CONNECTION TYPE</b> </div> <p>Choose the mode to be used by the router to connect to the Internet.</p> <p>My Internet Connection is : <input type="button" value="Static IP"/></p> <hr/> <div style="background-color: #333333; color: white; padding: 2px;"> <b>STATIC IP ADDRESS INTERNET CONNECTION TYPE</b> </div> <p>Enter the static address information provided by your Internet Service Provider (ISP).</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">IP Address :</td> <td><input type="text" value="10.2.67.105"/></td> <td>(assigned by your ISP)</td> </tr> <tr> <td>Subnet Mask :</td> <td><input type="text" value="255.255.0.0"/></td> <td></td> </tr> <tr> <td>ISP Gateway Address :</td> <td><input type="text" value="10.2.65.1"/></td> <td></td> </tr> <tr> <td>MAC Address :</td> <td><input type="text" value=""/> - <input type="text" value=""/></td> <td>(optional) <input type="button" value="Clone MAC Address"/></td> </tr> <tr> <td>Primary DNS Address :</td> <td colspan="2"><input type="text" value="10.2.65.2"/></td> </tr> <tr> <td>Secondary DNS Address :</td> <td colspan="2"><input type="text" value=""/> (optional)</td> </tr> <tr> <td>MTU :</td> <td colspan="2"><input type="text" value="1500"/></td> </tr> </table> <p><input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/></p>					IP Address :	<input type="text" value="10.2.67.105"/>	(assigned by your ISP)	Subnet Mask :	<input type="text" value="255.255.0.0"/>		ISP Gateway Address :	<input type="text" value="10.2.65.1"/>		MAC Address :	<input type="text" value=""/> - <input type="text" value=""/>	(optional) <input type="button" value="Clone MAC Address"/>	Primary DNS Address :	<input type="text" value="10.2.65.2"/>		Secondary DNS Address :	<input type="text" value=""/> (optional)		MTU :	<input type="text" value="1500"/>	
IP Address :	<input type="text" value="10.2.67.105"/>	(assigned by your ISP)																								
Subnet Mask :	<input type="text" value="255.255.0.0"/>																									
ISP Gateway Address :	<input type="text" value="10.2.65.1"/>																									
MAC Address :	<input type="text" value=""/> - <input type="text" value=""/>	(optional) <input type="button" value="Clone MAC Address"/>																								
Primary DNS Address :	<input type="text" value="10.2.65.2"/>																									
Secondary DNS Address :	<input type="text" value=""/> (optional)																									
MTU :	<input type="text" value="1500"/>																									
	<b>Helpful Hints..</b> <ul style="list-style-type: none"> <li>• <b>Internet Connection:</b> When configuring the router to access the Internet, be sure to choose the correct <b>Internet Connection Type</b> from the drop down menu. If you are unsure of which option to choose, please contact your <b>Internet Service Provider (ISP)</b>.</li> <li>• <b>Support:</b> If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.</li> </ul>																									

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

## WIRELESS NETWORK SETTINGS

Enable Wireless :

Wireless Network Name :  (Also called the SSID)

Wireless Channel :  (Mbit/s)  
1 automatic  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11

Enable Auto Channel Selection :

Transmission Rate :  (Mbit/s)

WMM Enable :

Enable Hidden Wireless :

---

## WIRELESS SECURITY MODE

Security Mode :

---

## WPA2 ONLY

WPA2 Only requires stations to use high g

Cipher Type :

PSK / EAP :

Network Key :  (8~63 ASCII or 64 HEX)

Figure 73. Available Channels of the Wireless Router

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

The screenshot shows the configuration interface of a D-Link wireless router. On the left sidebar, there are links for Internet Setup, Wireless Setup, LAN Setup, Time and Date, Parental Control, and Logout. Below these are icons for Internet Online and Reboot.

**WIRELESS NETWORK**

Use this section to configure the wireless settings for your D-Link router. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

**WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)**

Enable :   
 Current PIN : **07477836**  
   
 Wi-Fi Protected Status : Enabled / Configured

**WIRELESS NETWORK SETTINGS**

Enable Wireless :   
 Wireless Network Name : **Lab8\_TorresGamboa** (Also called the SSID)  
 Wireless Channel : **5**  
 Enable Auto Channel Selection :   
 Transmission Rate : **Best (automatic)** (Mbit/s)  
 WMM Enable :  (Wireless QoS)  
 Enable Hidden Wireless :  (Also called the SSID Broadcast)

**WIRELESS SECURITY MODE**

Security Mode : **Enable WPA2 Only Wireless Security (enhanced)**

**WPA2 ONLY**

WPA2 Only requires stations to use high grade encryption and authentication.

Cipher Type : **AES**  
 PSK / EAP : **PSK**  
 Network Key : **WiFi\_Seg** (8~63 ASCII or 64 HEX)

**Helpful Hints..**

- Wi-Fi Protected Setup provides a more intuitive way of setting up wireless security between the router and the wireless client. Make sure the wireless card supports such feature or uses a certified Windows Vista driver in order to take advantage of this feature.
- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

**Save Settings** **Don't Save Settings**

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

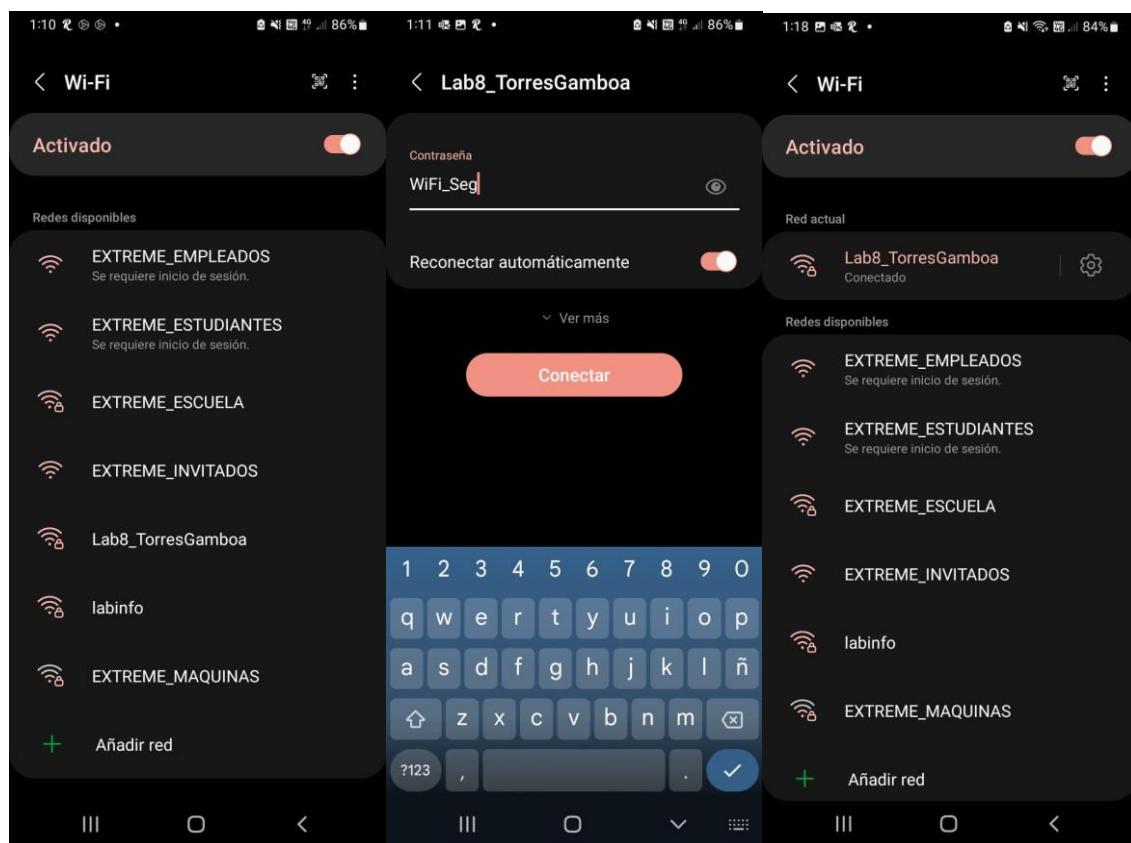


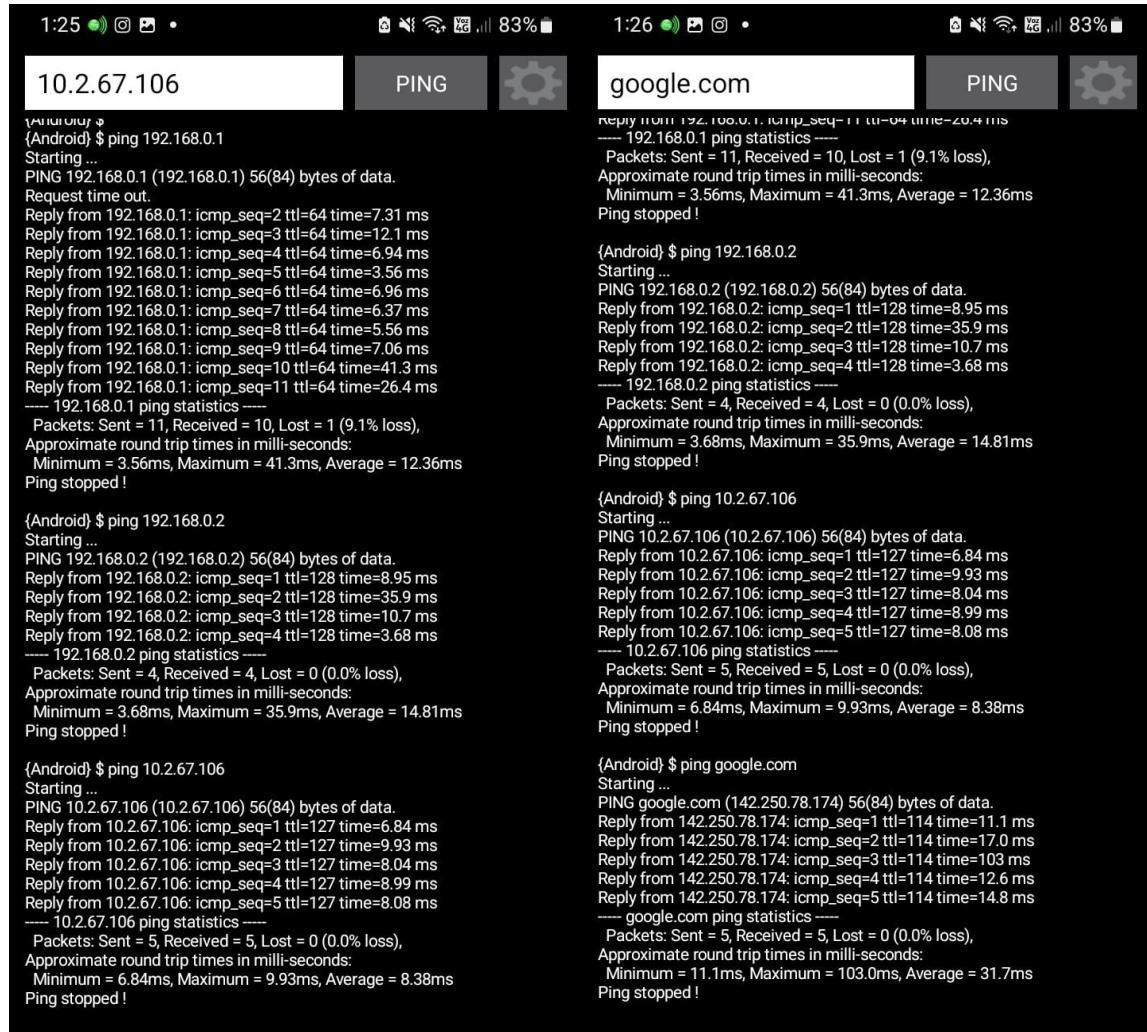
Figure 75. Authenticating and Connecting to the Wireless Network from the Mobile

- 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

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)

```
C:\Users\Redes>ping 10.2.67.107

Pinging 10.2.67.107 with 32 bytes of data:
Reply from 10.2.67.107: bytes=32 time=3ms TTL=127
Reply from 10.2.67.107: bytes=32 time=4ms TTL=127
Reply from 10.2.67.107: bytes=32 time=2ms TTL=127
Reply from 10.2.67.107: bytes=32 time=3ms TTL=127

Ping statistics for 10.2.67.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\Users\Redes>
```

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

```
C:\Users\Redes>ping 192.168.1.39

Pinging 192.168.1.39 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.39:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Redes>
```

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

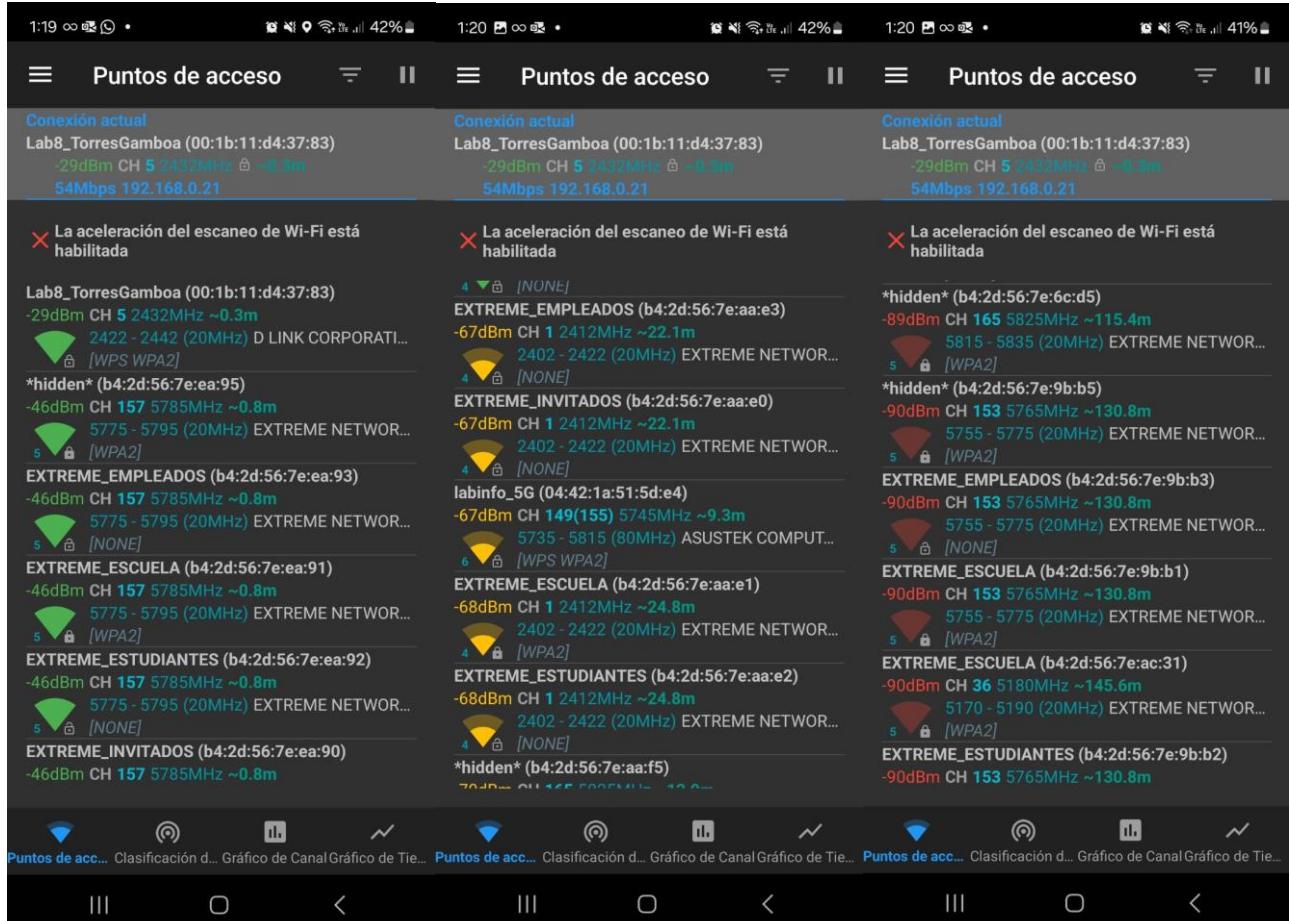


Figure 84. Obtaining Wireless Traffic from Active Networks Nearby Using Wi-Fi Analyzer

- 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)

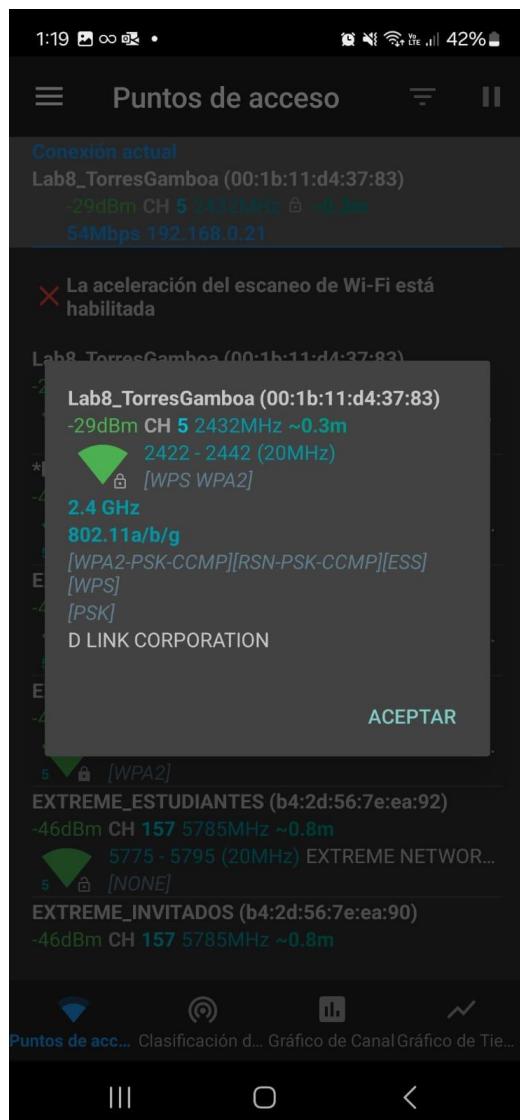


Figure 85. Information from the Wireless Network Capture

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

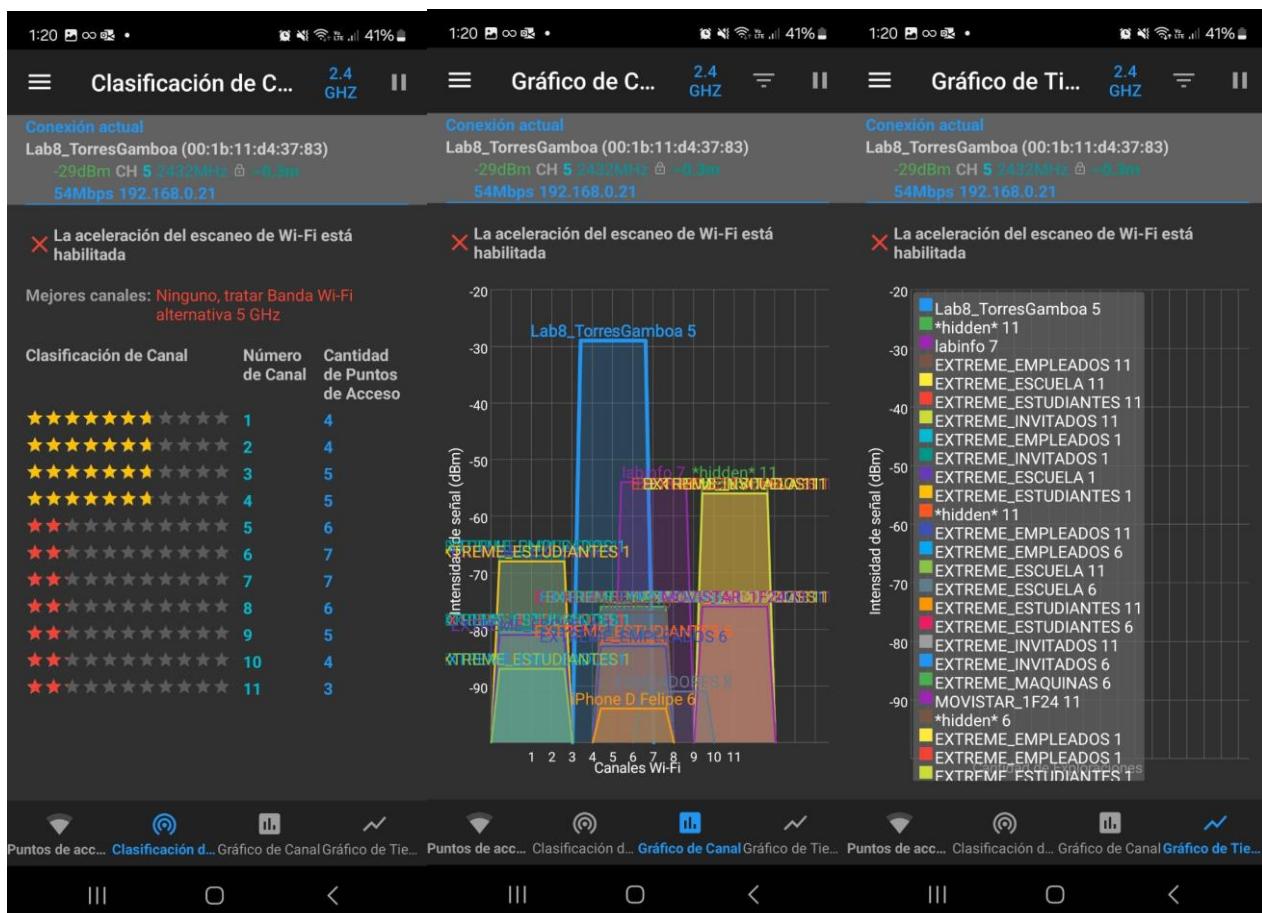


Figure 86. Information on Router Channels

### 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

<b>DIR-300 //</b>	<b>SETUP</b>	<b>ADVANCED</b>	<b>MAINTENANCE</b>	<b>STATUS</b>	<b>HELP</b>
<a href="#">Internet Setup</a> <a href="#">Wireless Setup</a> <a href="#">LAN Setup</a> <a href="#">Time and Date</a> <a href="#">Parental Control</a> <a href="#">Logout</a>	<h3>WIRELESS NETWORK</h3> <p>Use this section to configure the wireless settings for your D-Link router. Please note that changes made on this section may also need to be duplicated on your wireless client.</p> <p>To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.</p> <p><input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/></p>				
 <input type="button" value="Reboot"/>	<h3>WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)</h3> <p>Enable : <input checked="" type="checkbox"/>      Current PIN : <b>07477836</b>  <input type="button" value="Generate New PIN"/> <input type="button" value="Reset PIN to Default"/></p> <p>Wi-Fi Protected Status : Enabled / Configured  <input type="button" value="Reset to Unconfigured"/>  <input type="button" value="Add Wireless Device with WPS"/></p>				
	<h3>WIRELESS NETWORK SETTINGS</h3> <p>Enable Wireless : <input checked="" type="checkbox"/>      Wireless Network Name : <b>Lab8_TorresGamboa</b> (Also called the SSID)      Wireless Channel : <b>5</b>      Enable Auto Channel Selection : <input type="checkbox"/>      Transmission Rate : <b>Best (automatic)</b> (Mbit/s)      WMM Enable : <input type="checkbox"/> (Wireless QoS)      Enable Hidden Wireless : <input type="checkbox"/> (Also called the SSID Broadcast)</p>				
	<h3>WIRELESS SECURITY MODE</h3> <p>Security Mode : <b>Enable WPA2 Only Wireless Security (enhanced)</b></p>				
	<h3>WPA2 ONLY</h3> <p>WPA2 Only requires stations to use high grade encryption and authentication.</p> <p>Cipher Type : <b>AES</b>      PSK / EAP : <b>PSK</b>      Network Key : <b>WiFi_Seg</b> (8~63 ASCII or 64 HEX)</p>				
	<p><input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/></p>				

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

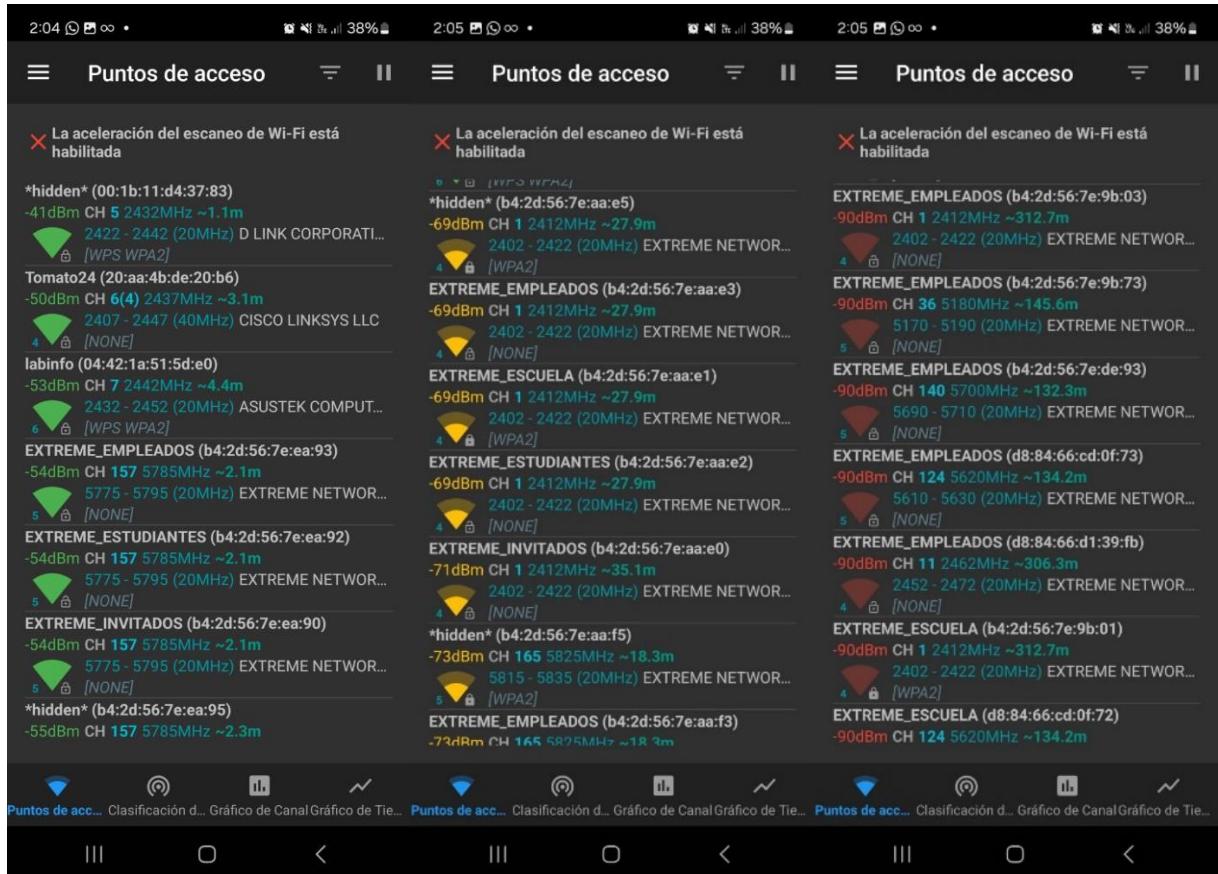


Figure 88. Verifying the Wireless Network with Beacon Frame Disabled in WiFi Analyzer

## 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.

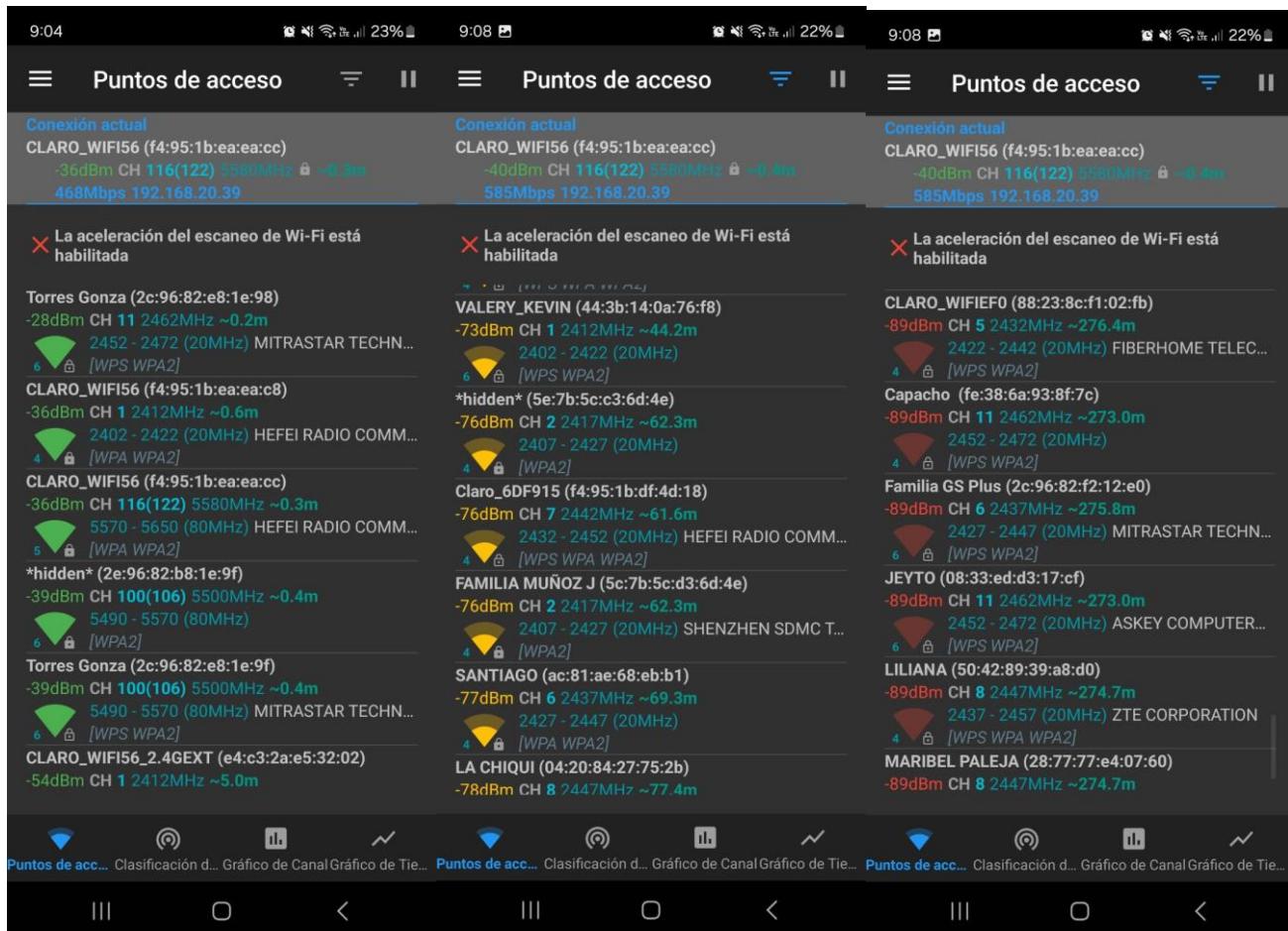


Figure 89. Obtaining Wireless Traffic from Active Networks Near the House with Wi-Fi Analyzer

- 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

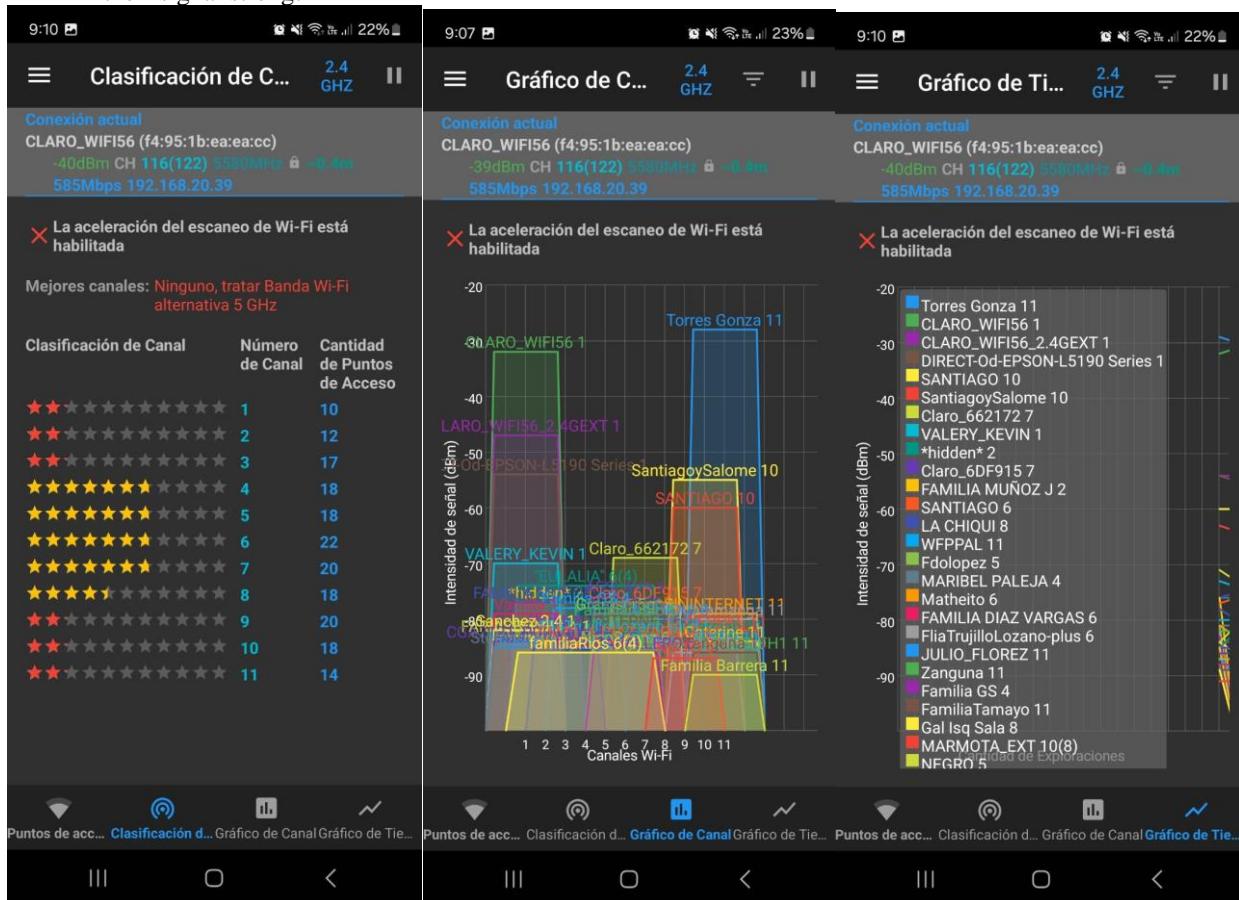


Figure 91. Information on Router Channels and Time Graph

## 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-httpd-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.^N Reemplazar^U Pegar txt ^T Ortografía^_ Ir a lÃnea
```

Figure 93. Adding 'LoadModule php5\_module libexec/libphp5.so' into httpd.conf

```
#  
# AddEncoding allows you to have certain browsers uncompress  
# information on the fly. Note: Not all browsers support this.  
#  
#AddEncoding x-compress .Z  
#AddEncoding x-gzip .gz .tgz  
#  
# If the AddEncoding directives above are commented-out, then you  
# probably should define those extensions to indicate media types:  
#  
AddType application/x-compress .Z  
AddType application/x-gzip .gz .tgz  
AddType application/x-httpd-php .php  
#  
# AddHandler allows you to map certain file extensions to "handlers":  
# actions unrelated to filetype. These can be either built into the server  
# or added with the Action directive (see below)  
#  
# To use CGI scripts outside of ScriptAliased directories:  
# (You will also need to add "ExecCGI" to the "Options" directive.)  
#  
AddHandler cgi-script .cgi  
  
# For type maps (negotiated resources):  
#AddHandler type-map var  
  
#  
# Filters allow you to process content before it is sent to the client.  
#  
^G Ver ayuda ^O Guardar ^W  
^X Salir ^R Leer fich.^V Reemplazar^U Pegar txt ^T OrtografÃ-a^L Ir a lÃnea
```

Figure 94. Adding 'AddType application/x-httpd-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:

```

#Order allow,deny
#Allow from all
AuthType Basic
AuthName "Nagios Access"
AuthUserFile /usr/local/nagios/etc/htpasswd.users
Require valid-user

</Directory>
<Directory "/usr/local/nagios/share/">
    Options None
    AllowOverride None
    #Order allow,deny
    #Allow from all
    Require all granted
    DirectoryIndex index.php index.html
    AuthType Basic
    AuthName "Nagios Access"
    AuthUserFile /usr/local/nagios/etc/htpasswd.users
    Require valid-user
</Directory>
Alias /calculadora "/var/apache2/2.4/htdocs/calculadora"
<Directory "/var/apache2/2.4/htdocs/calculadora">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    DirectoryIndex index.php index.html
</Directory>

```

**[ ]** Ver ayuda **[ ]** Guardar **[ ]** **[ ]**  
**[ ]** Salir **[ ]** Leer fich. **[ ]** Reemplazar **[ ]** Pegar txt **[ ]** Ortografía-a **[ ]** Ir a lÃnea

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@solari:/var/apache2/2.4/htdocs/calculadora# ls
index.php
root@solari:/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: none; }
        .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="1" required>

        <label for="tercio2">Nota Segundo Tercio (30%):</label>
        <input type="number" id="tercio2" name="tercio2" min="0" max="100" step="1" required>

        <label for="tercio3">Nota Tercer Tercio (40%):</label>
        <input type="number" id="tercio3" name="tercio3" min="0" max="100" step="1" required>
    <^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 lÃnea
```

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

192.168.20.101/calculadora/

## Calculadora de Notas del Semestre

**Nombre del Estudiante:**

Camila Torres

**Nota Primer Tercio (30%):**

45

**Nota Segundo Tercio (30%):**

42

**Nota Tercer Tercio (40%):**

40

**Calcular Nota Final**

### Resultados:

**Estudiante:** Camila Torres

**Nota Final:** 42.10

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

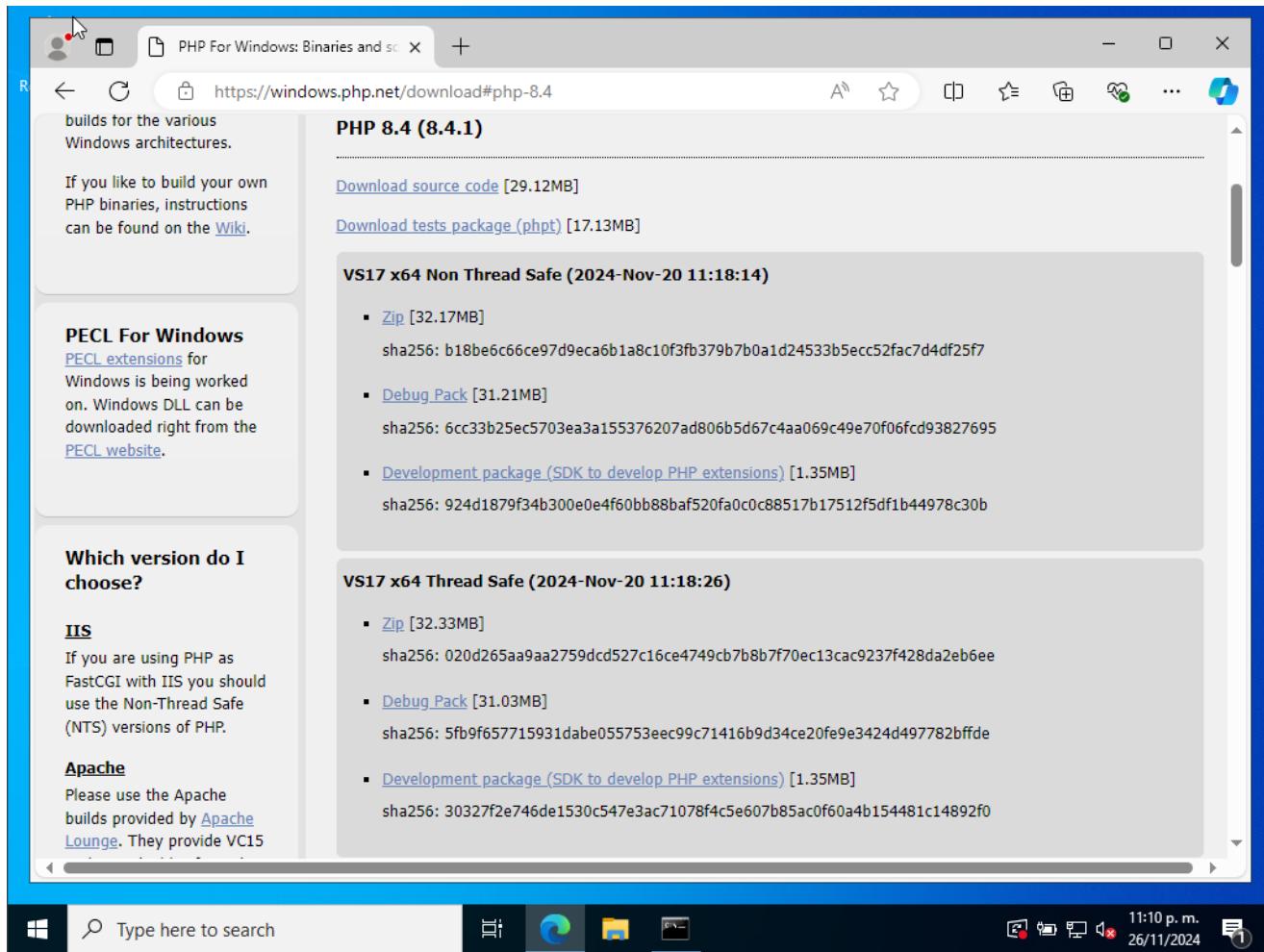


Figure 101. Downloading PHP 8.4.1

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

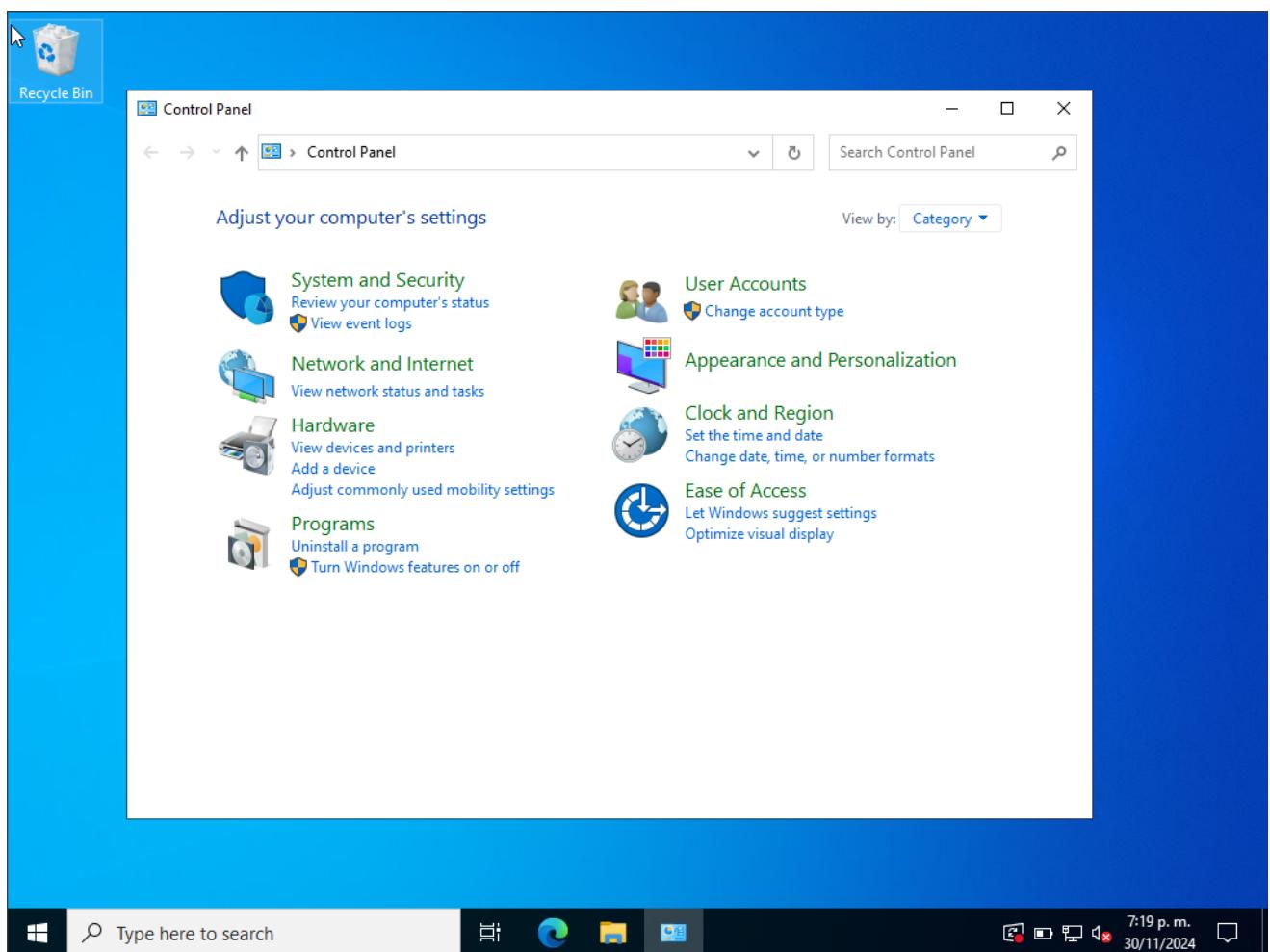


Figure 102. Control Panel in Windows Server

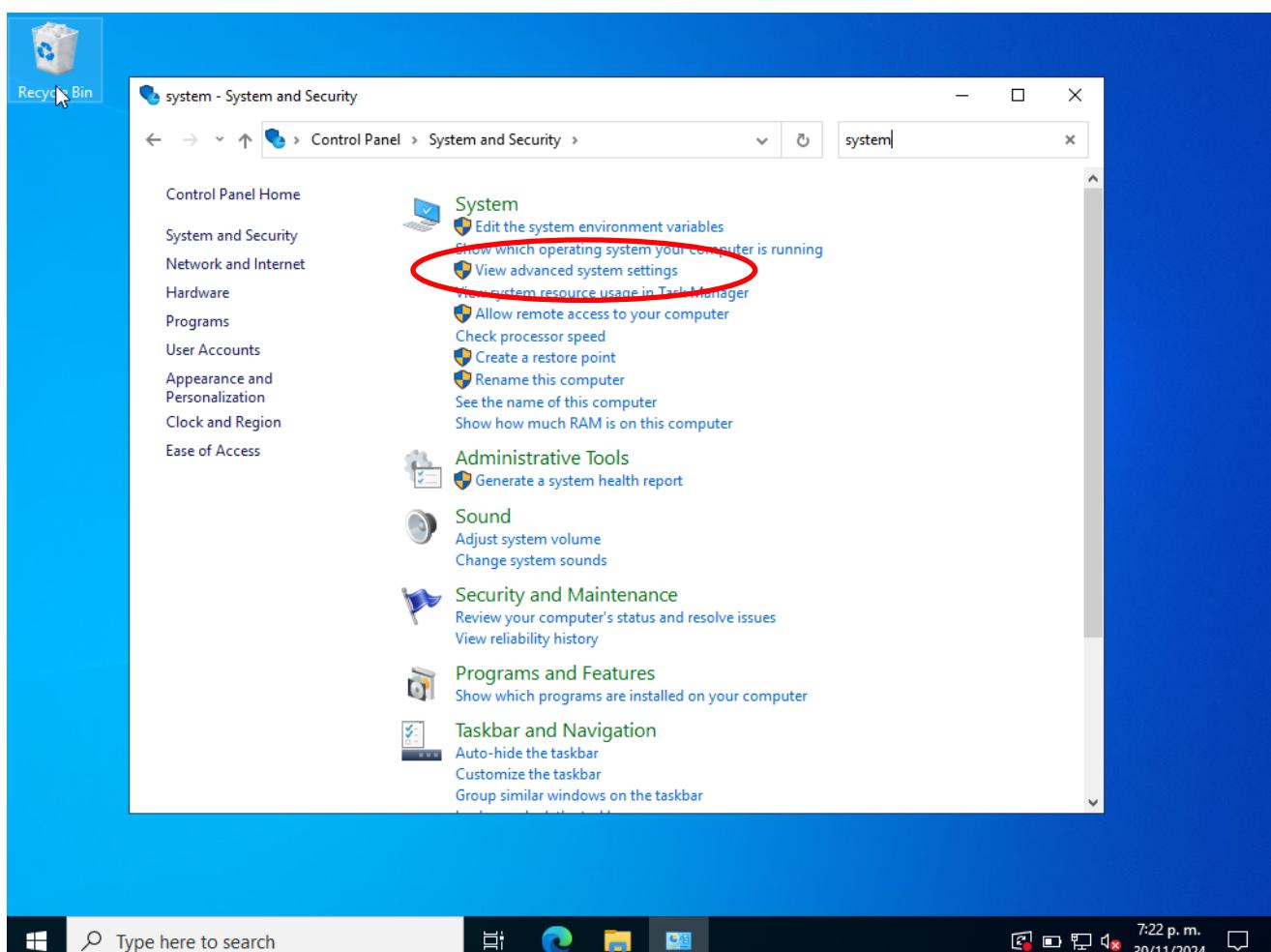


Figure 103. System Settings

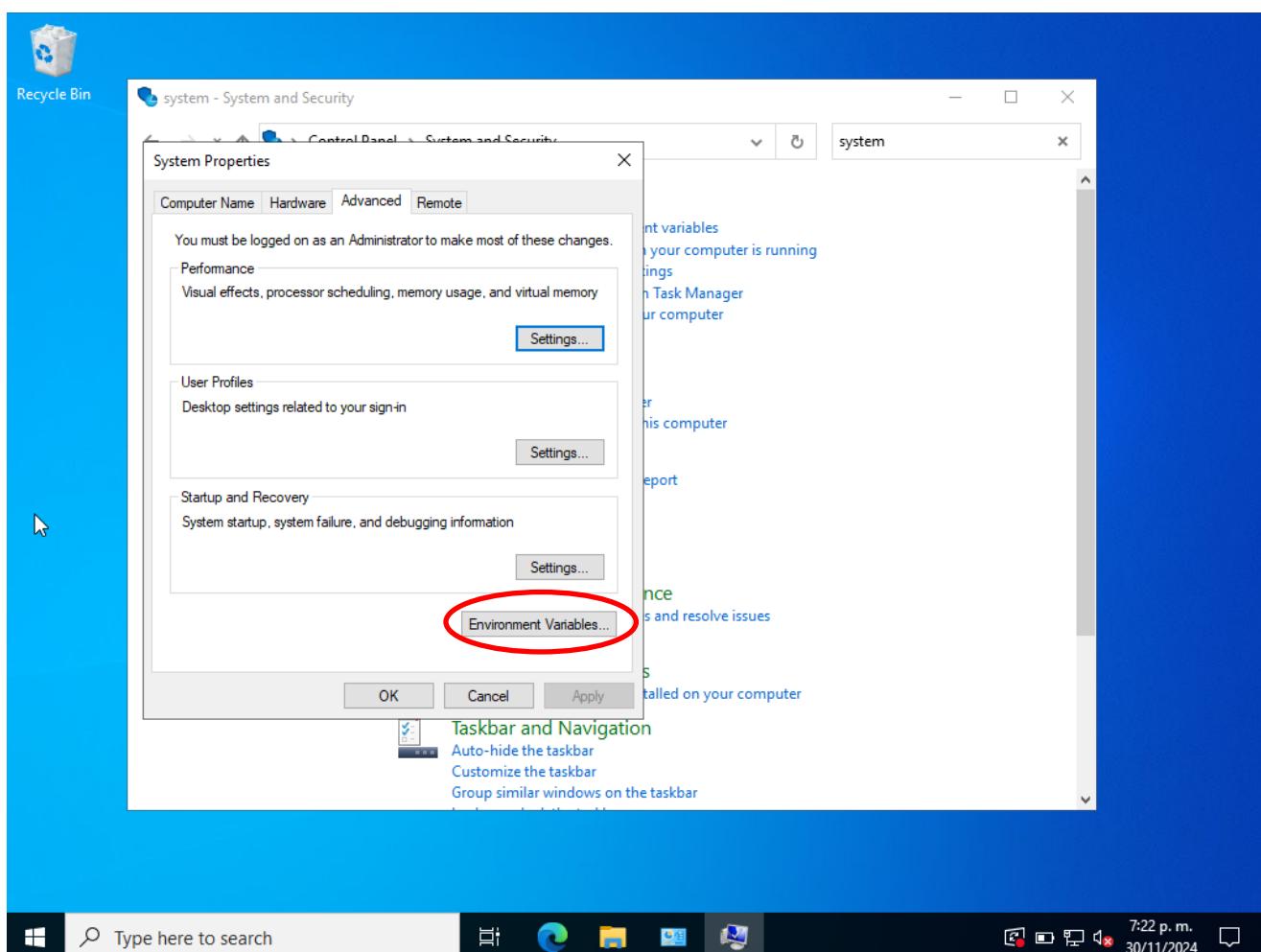


Figure 104. Opening Environment Variables in Windows Server

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

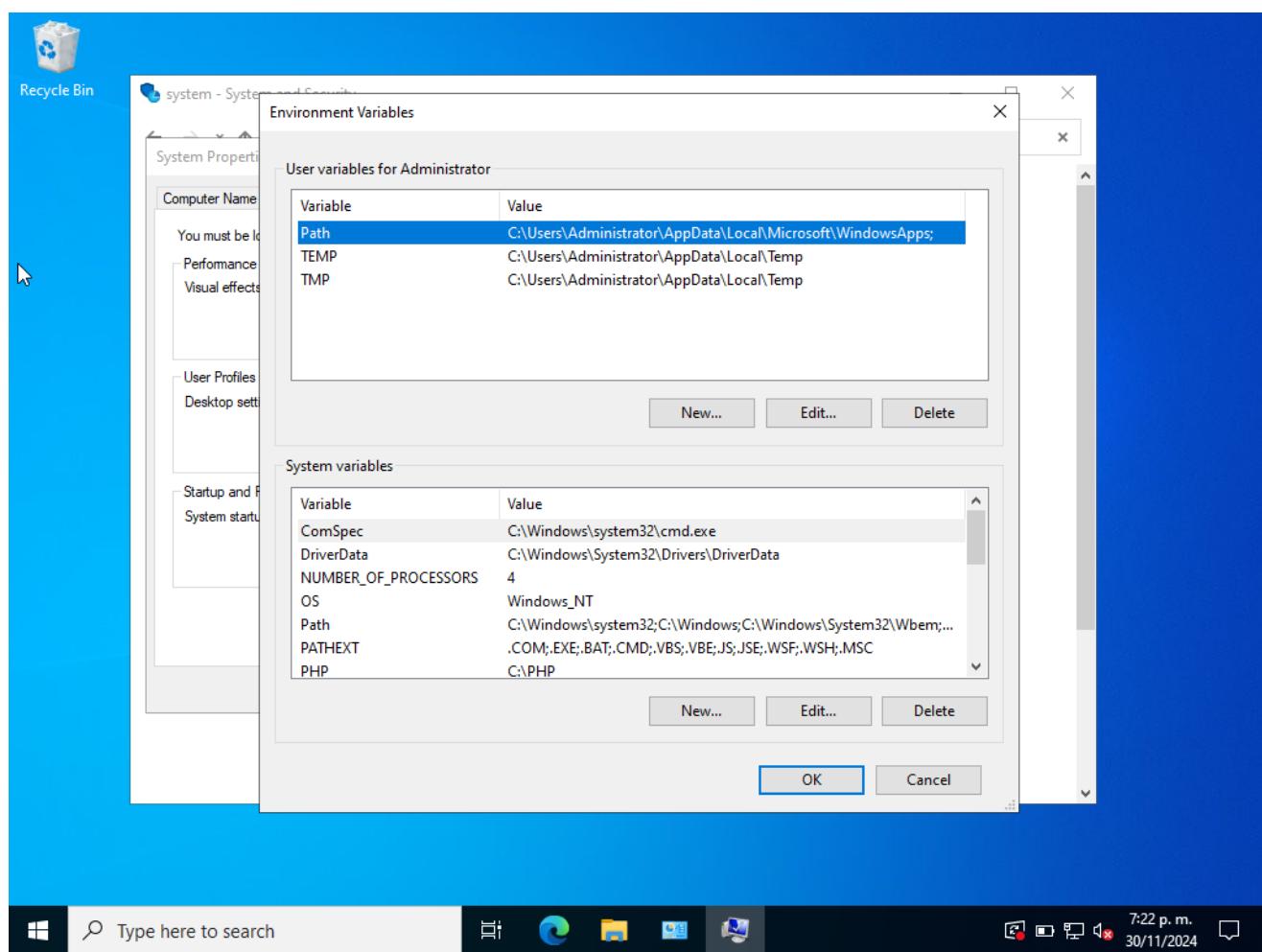


Figure 105. Editing System Variables

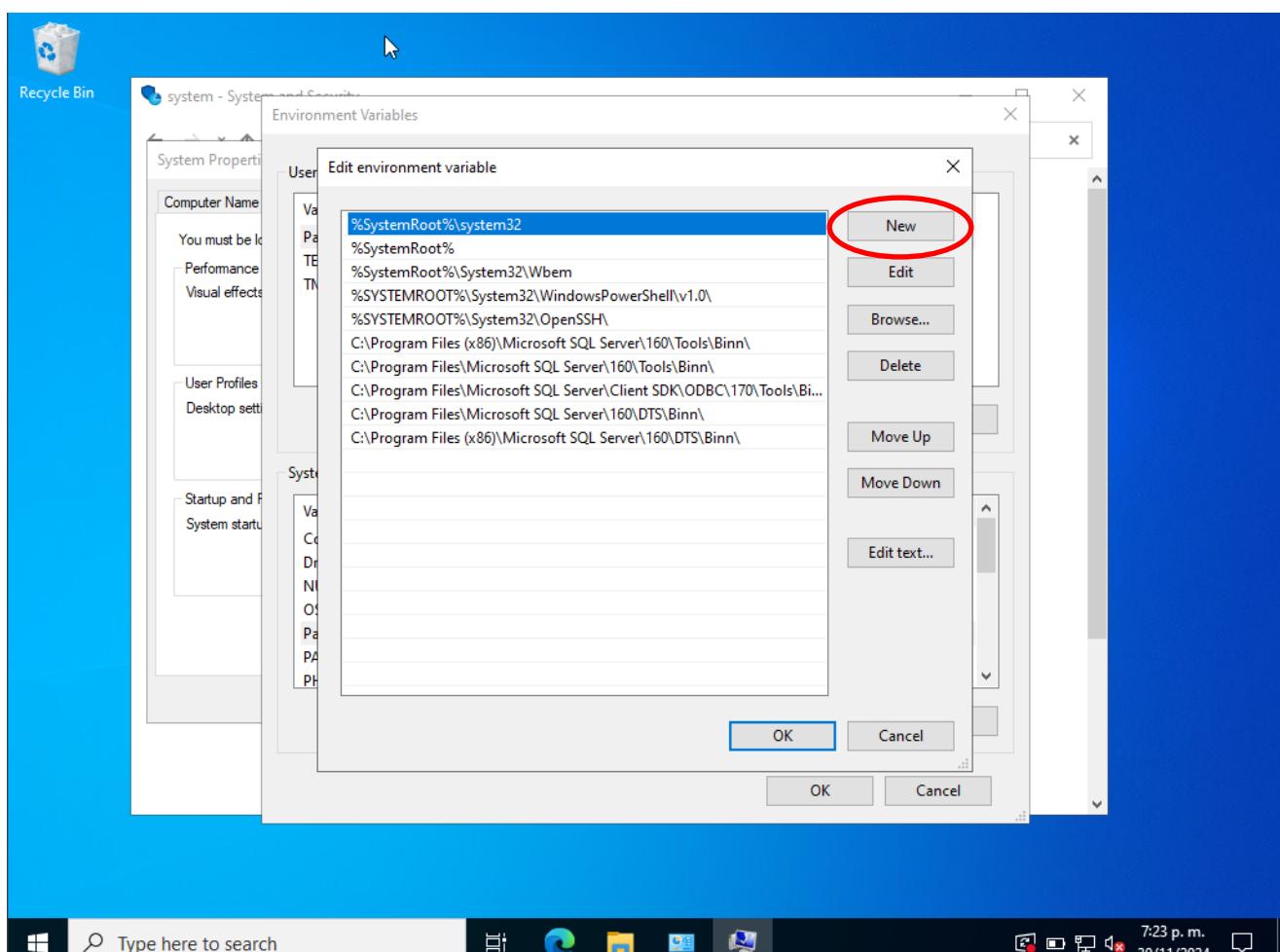


Figure 106. Adding a new path

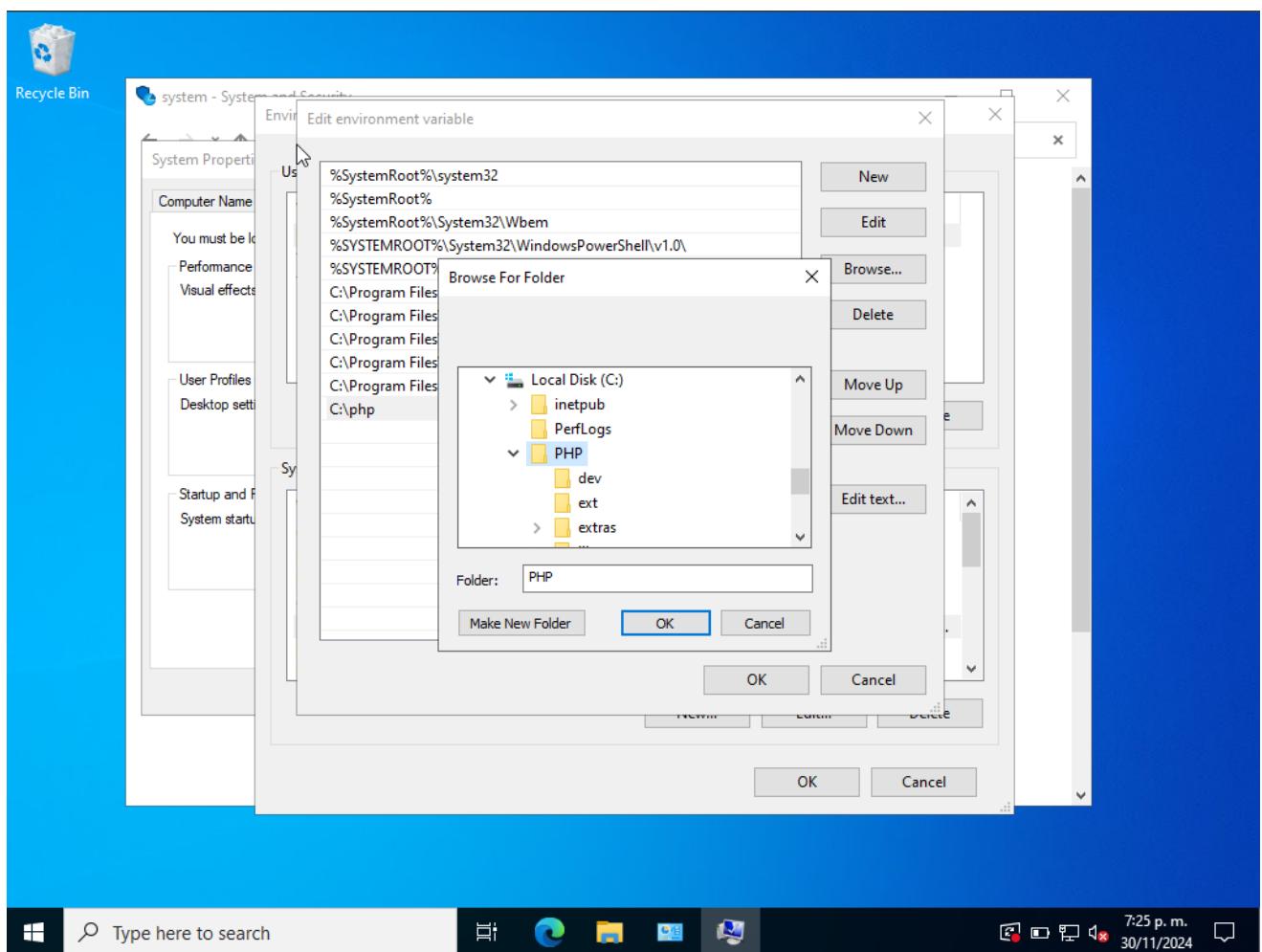


Figure 107. Adding the PHP path in the environment variable configuration

- 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

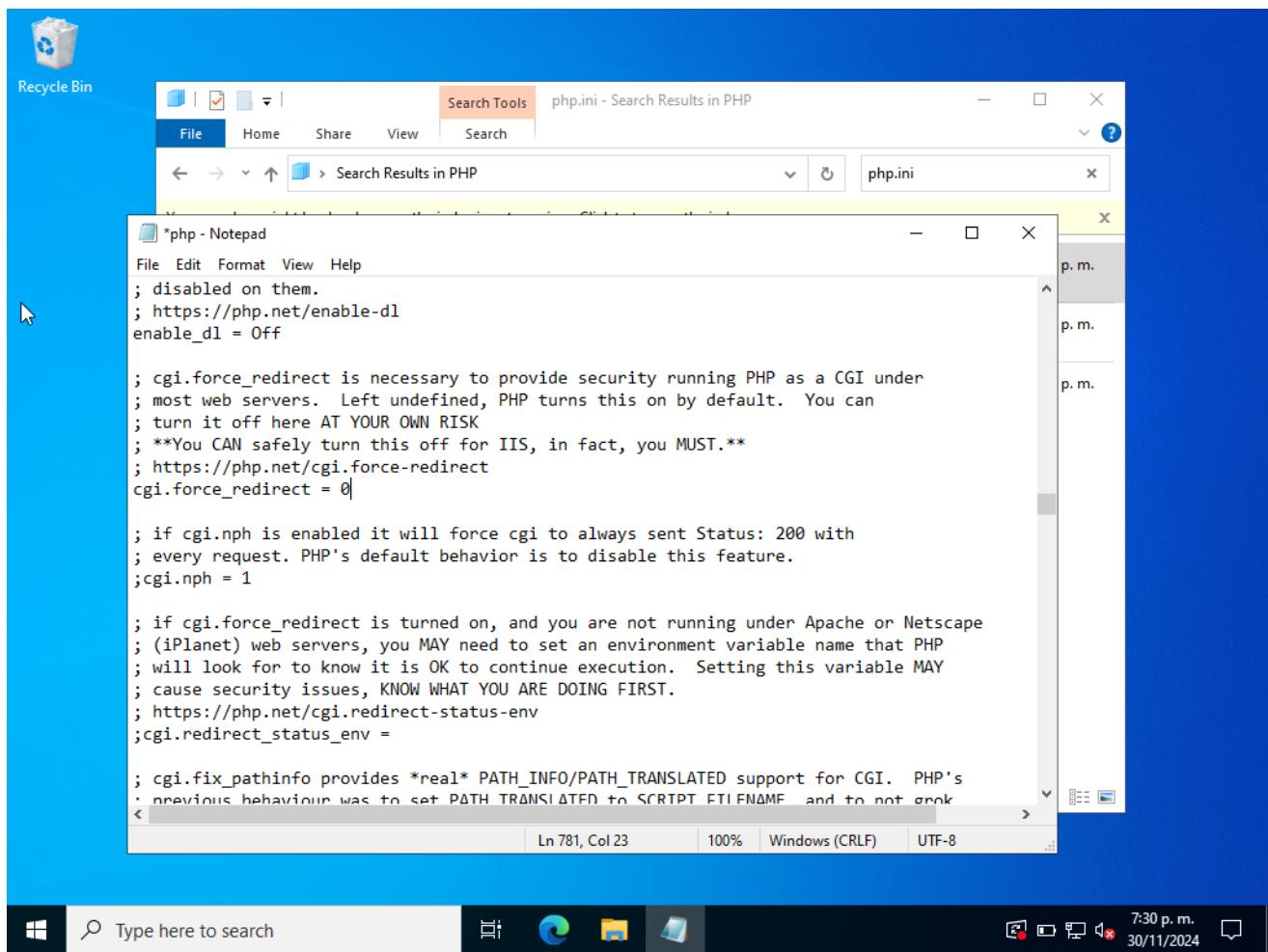


Figure 108. Editing the php.ini file

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

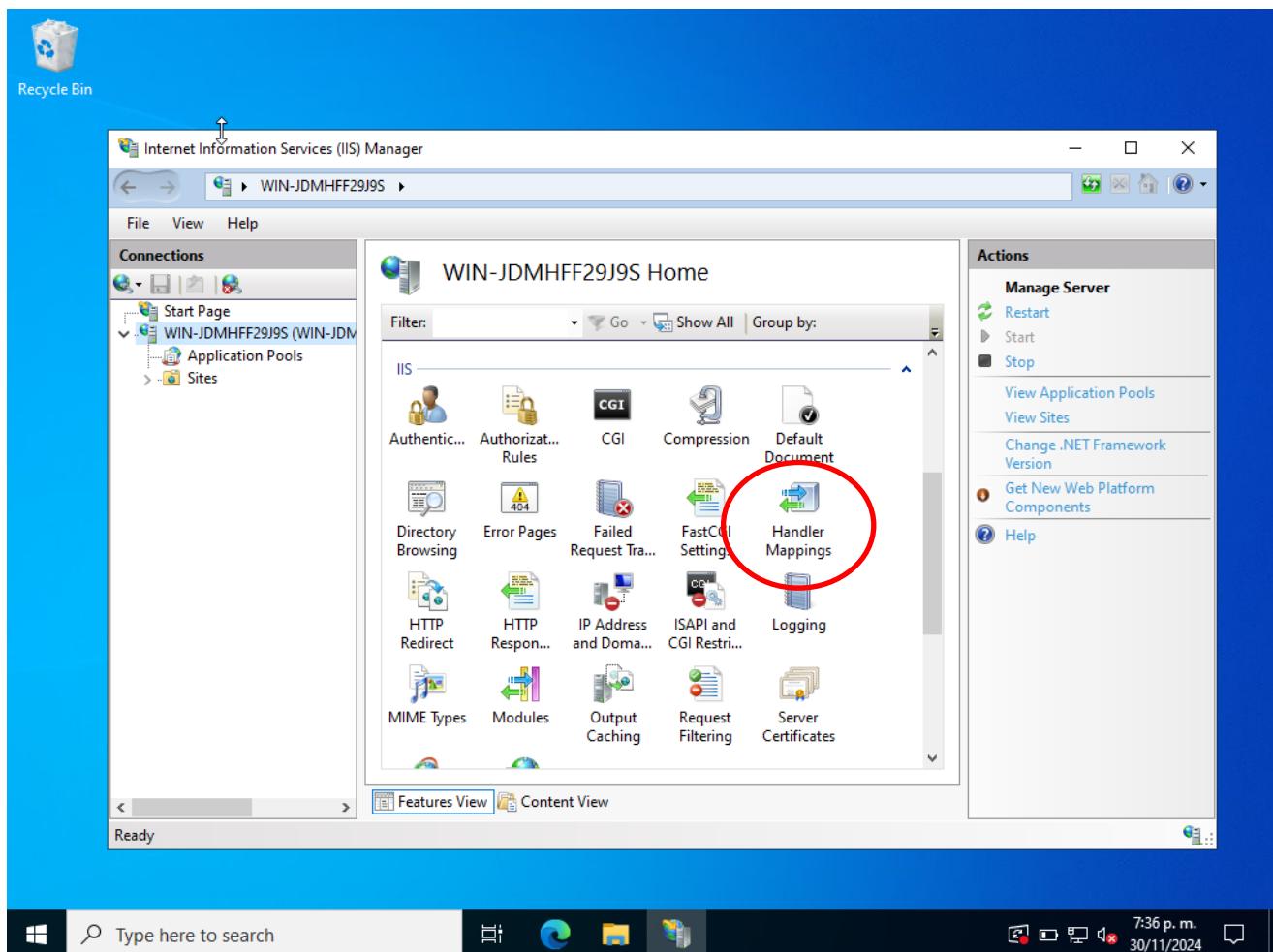


Figure 109. IIS Manager Menu

- Click on **Add Script Map**

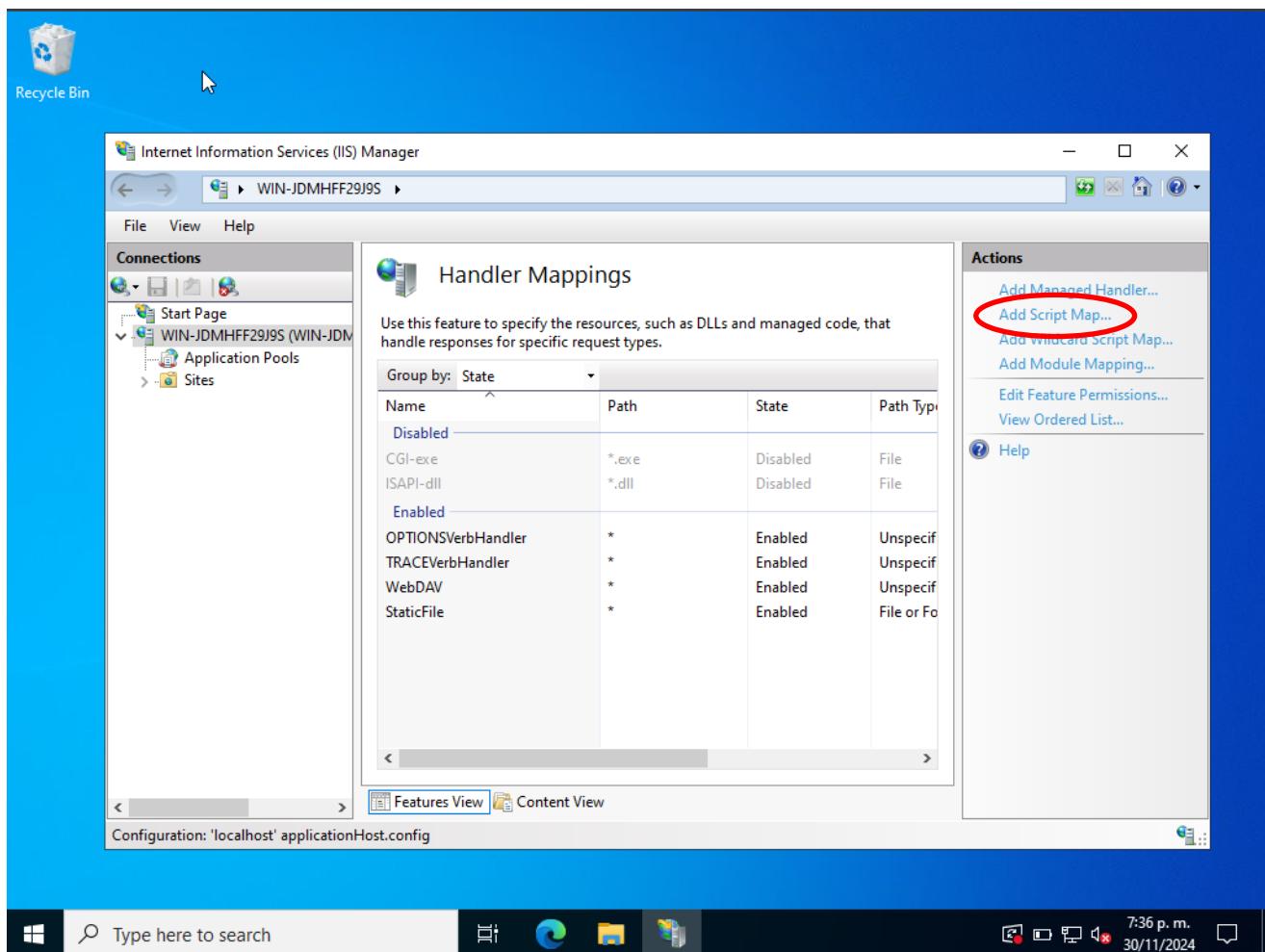


Figure 110. Handler Mappings Section

- We configure the following:

Request Path: \*.php

Module: FastCGIModule

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

Name: PHP\_via\_FastCGI

Finally, we click OK

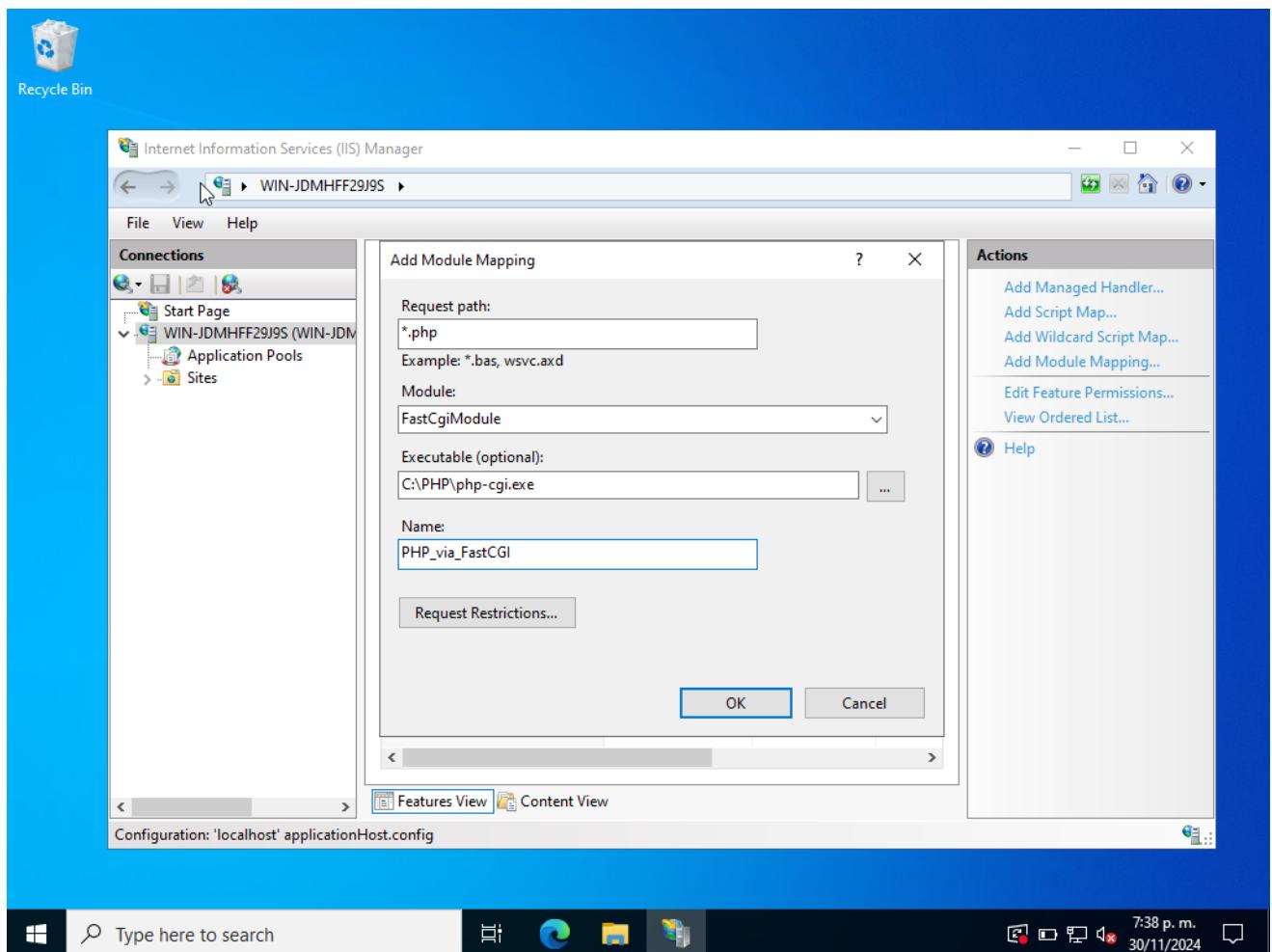


Figure 111. Configuring Module Mapping for PHP

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

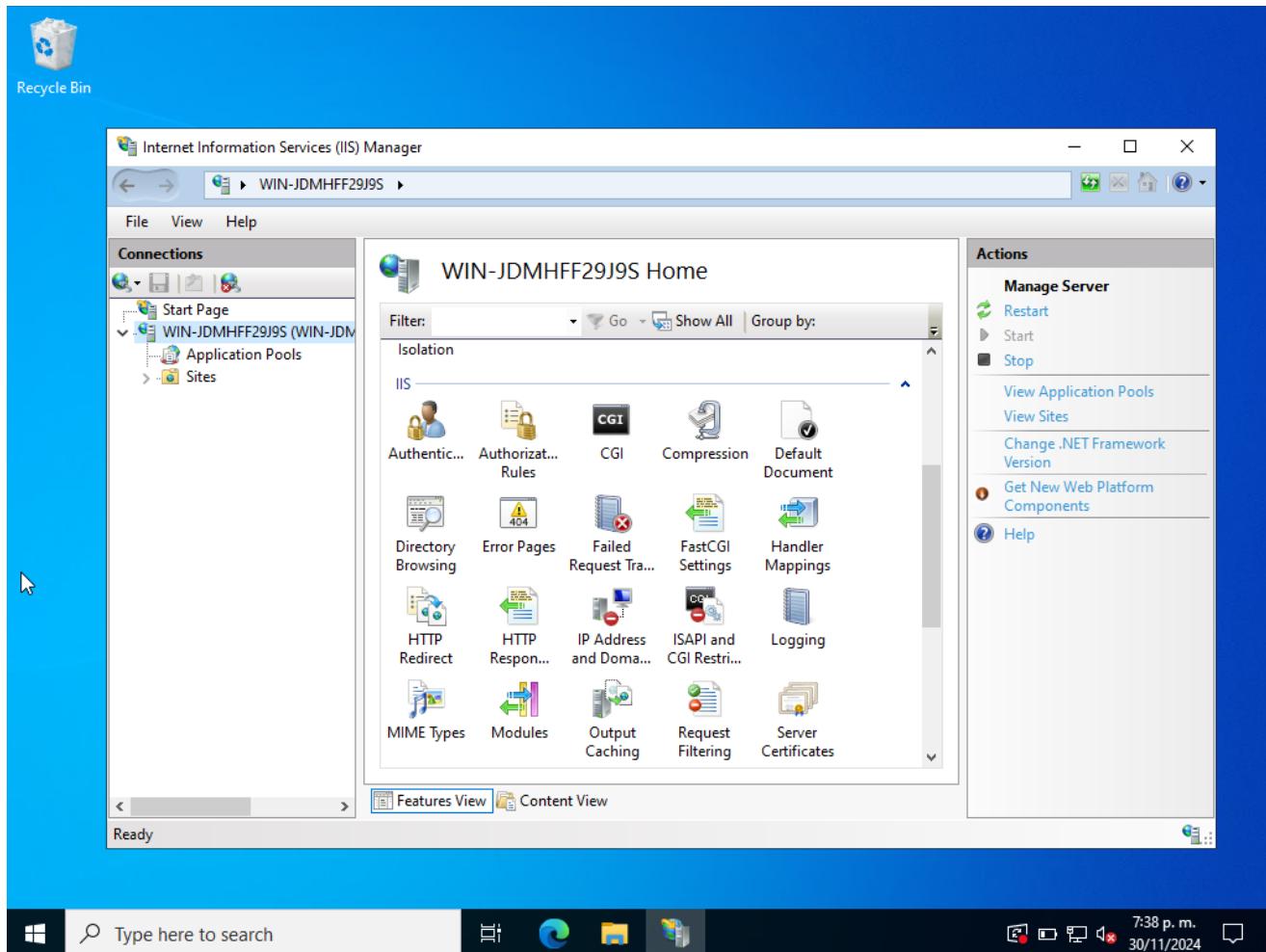


Figure 112. Navigating to FastCGI Settings

- 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.

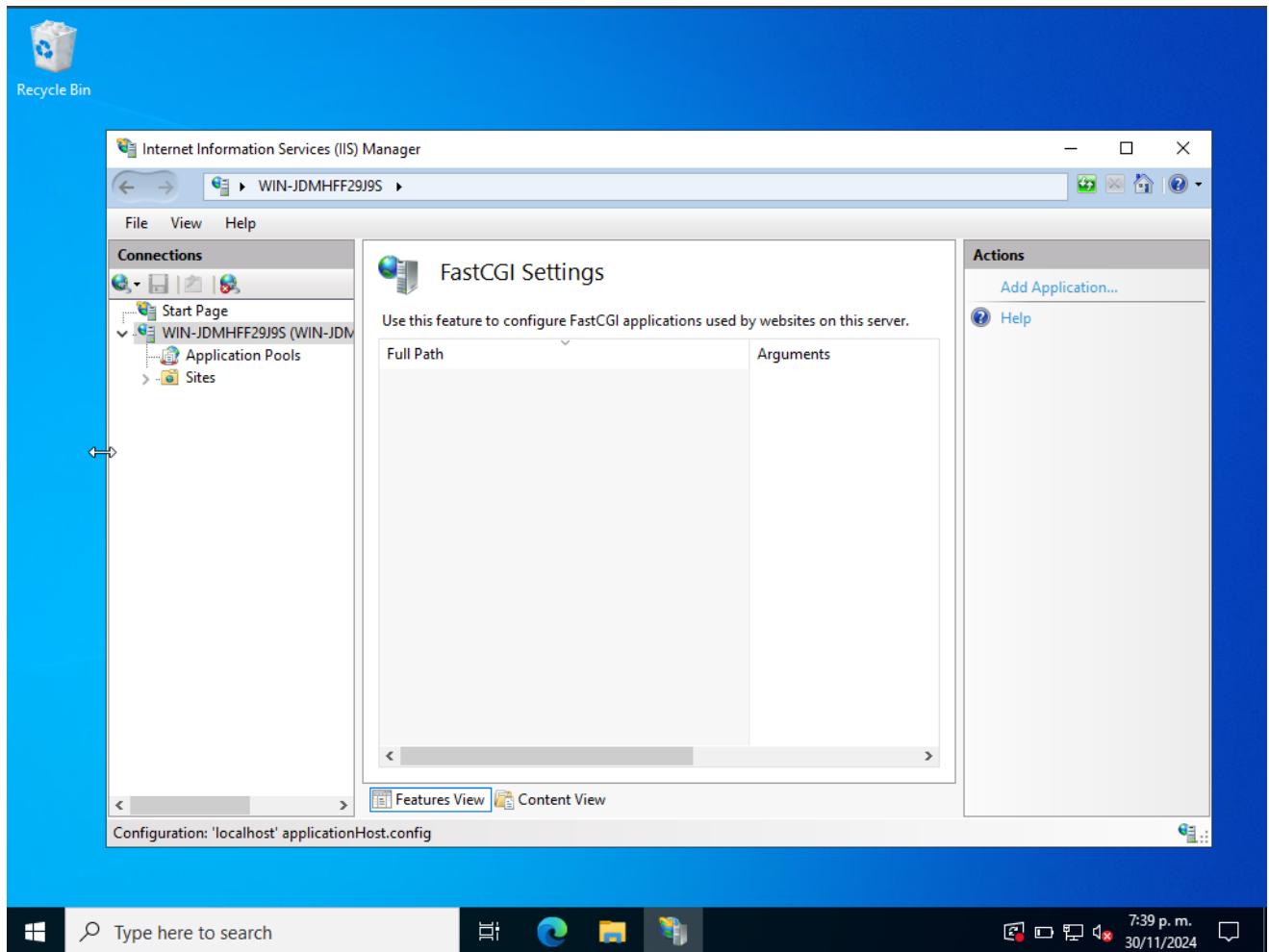


Figure 113. FastCGI Settings section

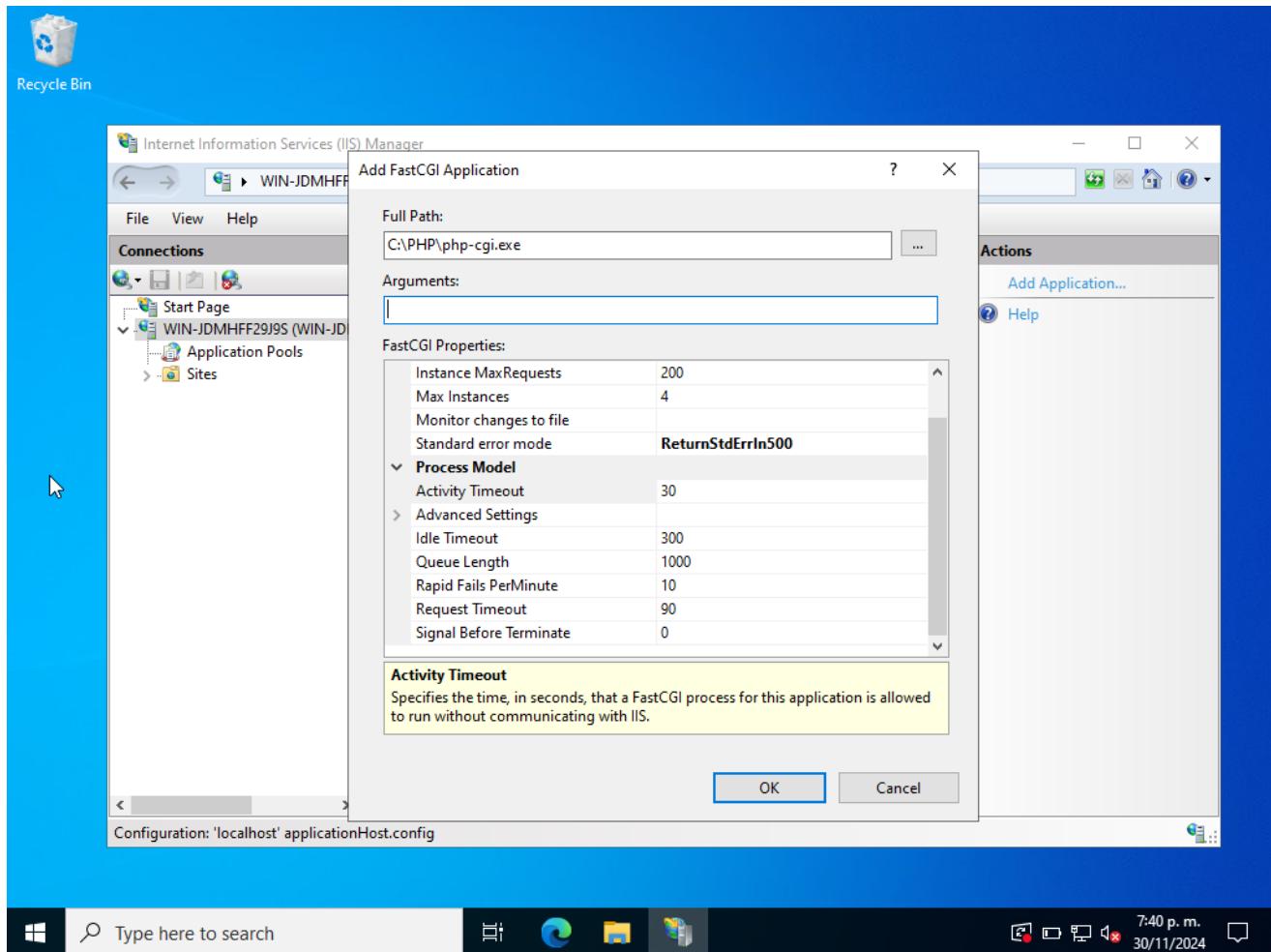


Figure 114. Adding FastCGI Application

- 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

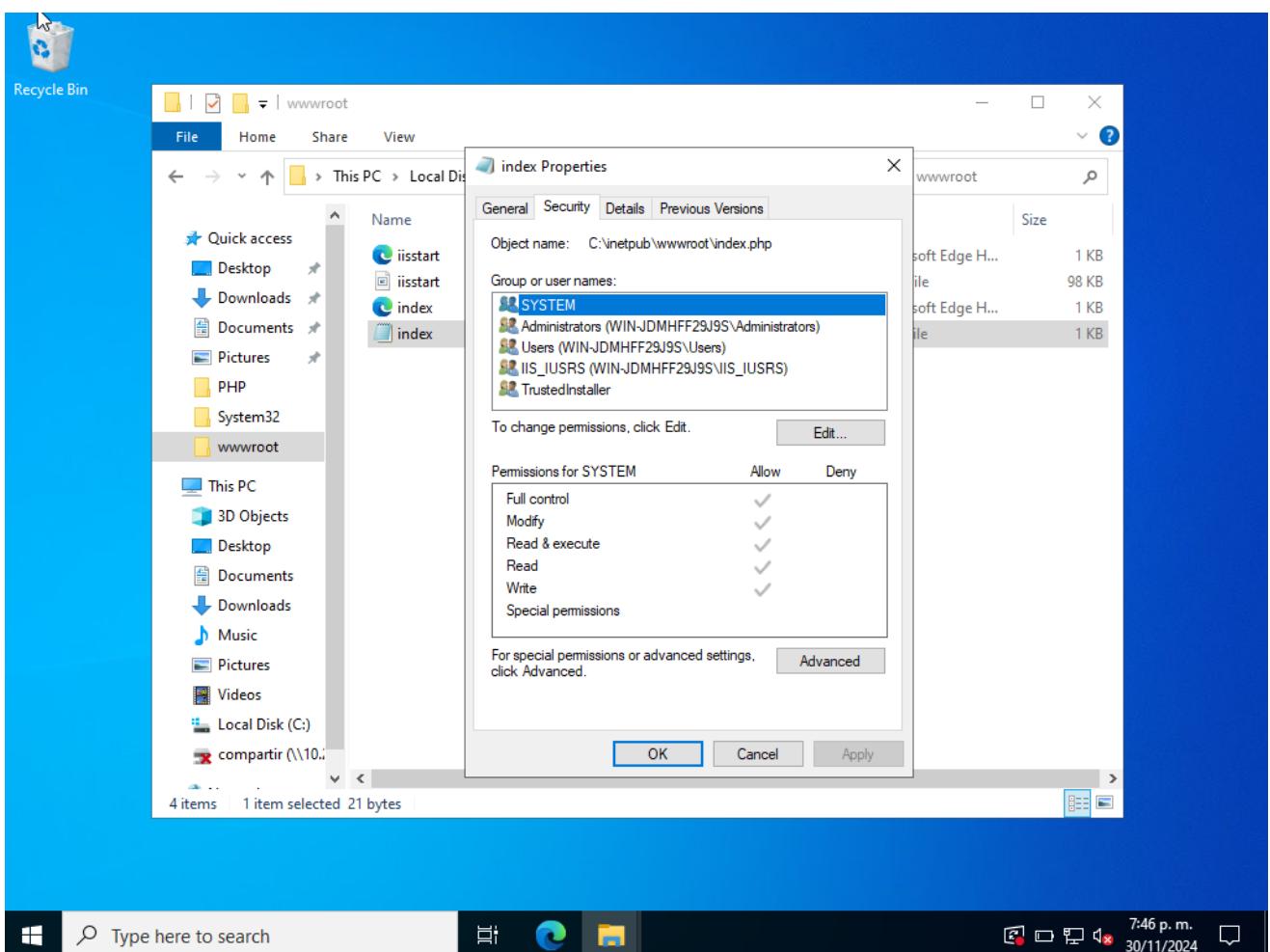


Figure 115. Verifying that the IIS user has the correct permissions for index.php

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

 No es seguro 192.168.20.160/index.php

## Calculadora de Notas del Semestre

Nombre del Estudiante:

Nota Primer Tercio (30%):

Nota Segundo Tercio (30%):

Nota Tercer Tercio (40%):

Calcular Nota Final

### Resultados:

Estudiante: Camila Torres

Nota Final: 3.40

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
    esac
}

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

Figure 117. Shell program part 1

```
GNU nano 6.0                                     network_info.sh
 1) echo -e "\n*** Network Statistics ***"
 2) netstat -i
 3) echo -e "\n*** Bandwidth Usage ***"
    read -p "Enter the interface" interface
    iftop -i $interface
 4) echo -e "\n*** Routing Table ***"
    if command -v route &>/dev/null; then
      route -n
    else
      ip route show
    fi
 5) echo -e "\n*** Ethernet Information ***"
    if command -v ethtool &>/dev/null; then
      ethtool "$(ip route | grep default | awk '{print $5}')"
    else
      ip link show
    fi
 6) echo "Exiting..."
  exit 0
*)
echo "Invalid option. Please try again."

```

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

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
-
```

**Keyboard Shortcuts:**

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

```
*** Network Interfaces ***
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.20.48 netmask 255.255.255.0 broadcast 192.168.20.255
        inet6 fe80::a00:27ff:fe98:cd53 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:98:cd:53 txqueuelen 1000 (Ethernet)
            RX packets 1397 bytes 508929 (497.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1650 bytes 107960 (105.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 613 bytes 53800 (52.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 613 bytes 53800 (52.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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):
```

Figure 121. Network interfaces information (ifconfig command)

```
*** Network Statistics ***
Kernel Interface table
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR     TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1      1500    1403     0     0 0    1660     0     0     0 BMRU
lo       65536    619     0     0 0    619     0     0     0 LRU
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): _
```

Figure 122. Network Statistics (netstat command)

```
*** Bandwidth Usage ***
Enter the interface: eth1
```

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

	12.5Kb	25.0Kb	37.5Kb	50.0Kb	62.5Kb
192.168.20.255		=> 192.168.20.26		0b	0b
		<=		0b	236b
192.168.20.48		=> dns.google		0b	0b
		<=		0b	214b
255.255.255.255		=> 192.168.20.91		0b	260b
		<=		0b	0b
				0b	63b
TX:	cum:	429B	peak:	1.67Kb	rates:
RX:		1.21KB		3.19Kb	0b      236b      214b
TOTAL:		1.63KB		4.86Kb	0b      236b      618b
					0b      236b      833b

Figure 124. Traffic monitoring of eth1 (iftop command)

```
*** Routing Table ***
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          192.168.20.1   0.0.0.0        UG    0      0        0 eth1
127.0.0.0         0.0.0.0       255.0.0.0     U      0      0        0 lo
192.168.20.0     0.0.0.0       255.255.255.0  U      0      0        0 eth1
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): _
```

Figure 125. Routing table information (route command)

```
*** Ethernet Information ***
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:98:cd:53 brd ff:ff:ff:ff:ff:ff
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):
```

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](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/nes5500/l2vpn/l2vpn-l2config/b-l2vpn-l2config-book/b-l2vpn-l2config\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/iosxr/nes5500/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](https://en.wikipedia.org/wiki/IEEE_802.1Q)

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