LABORATORY NO.08 – DATA LINK LAYER AND APPLICATION LAYER

ELABORADO POR:

ESTEBAN AGUILERA CONTRERAS
JUAN DAVID RODRIGUEZ RODRIGUEZ

PROFESOR(ES):

JOHN PACHON

RECO
2025-1

OBJECTIVES

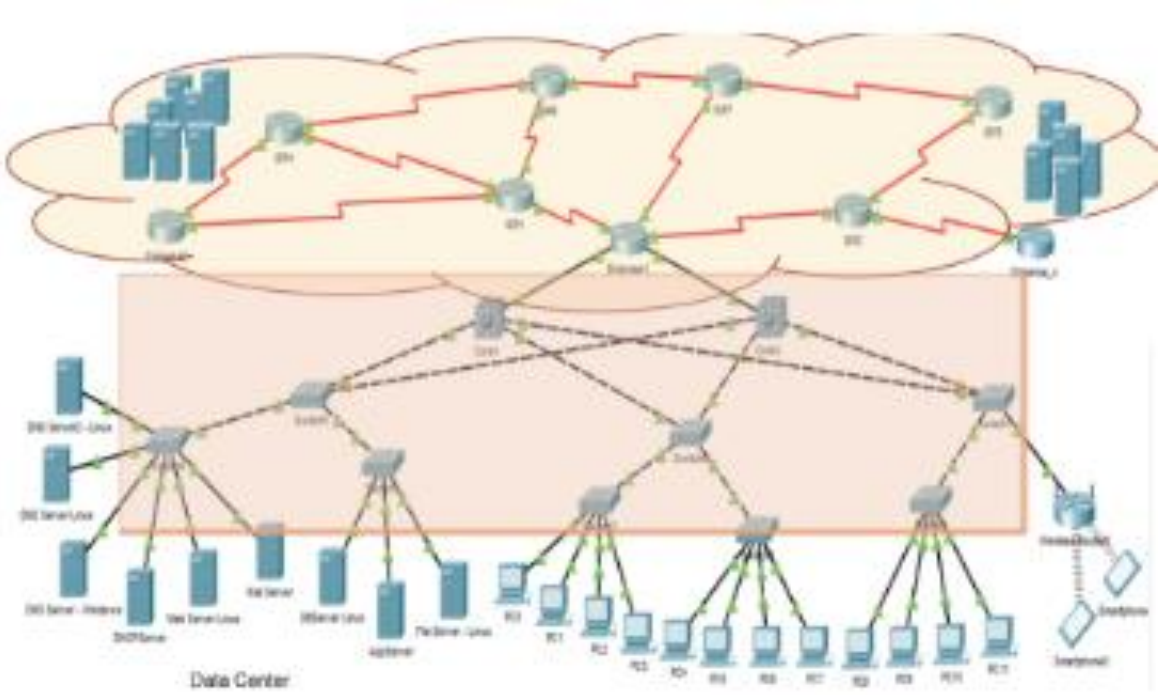
- Review the operation of Ethernet and WiFi networks.
- Review the operation of interconnection devices.
- Continue installing application layer services.

TOOLS TO BE USED

- Computers
- Virtualization software
- Internet access
- Switches
- Packet Tracer
- Wireshark

CONTEXT

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.

INTRODUCTION

Durante este laboratorio tuvimos la oportunidad de aplicar conceptos clave de redes de computadoras enfocados en la capa de enlace de datos y la capa de aplicación del modelo OSI. La actividad se desarrolló mediante la simulación de una red empresarial con dispositivos cableados e inalámbricos, switches, routers, y servidores, utilizando herramientas como Cisco Packet Tracer, Wireshark y la plataforma en la nube de AWS. Además de configurar físicamente los elementos de red, también trabajamos en la implementación de servicios de capa de aplicación como servidores web dinámicos. Este enfoque práctico nos permitió comprender no solo la teoría detrás de los protocolos y dispositivos, sino también su implementación y comportamiento real dentro de una red empresarial.

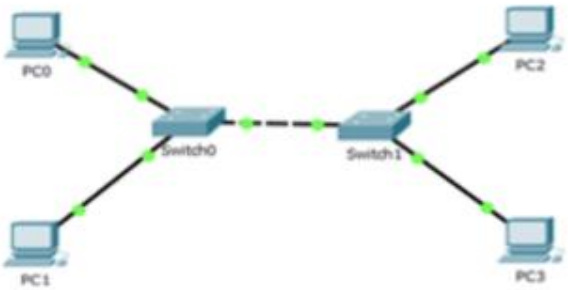
THEORICAL FRAMEWORK

- Capa de Enlace de Datos
    - La capa de enlace del modelo OSI (capa 2) se encarga del direccionamiento físico mediante direcciones MAC, del control de acceso al medio, detección de errores y la encapsulación en tramas. Tecnologías como Ethernet utilizan switches que operan en esta capa, permitiendo la transmisión eficiente de datos dentro de una red LAN.Redes WiFi
- Redes Inalámbricas (WiFi)
    - Las redes WiFi se basan en el estándar IEEE 802.11 y permiten la comunicación sin cables. Operan en bandas de 2.4 GHz y 5 GHz, y requieren configuraciones de seguridad como WPA2-PSK con cifrado AES para garantizar la protección de los datos. El uso de canales no solapados es clave para evitar interferencias.
- VLANs y Enlaces Troncales
    - Las VLANs permiten segmentar lógicamente una red física, aumentando la seguridad y reduciendo el tráfico innecesario. Los enlaces troncales (trunk links) permiten el paso de tráfico de múltiples VLANs entre switches mediante protocolos como IEEE 802.1Q.
- Spanning Tree Protocol (STP)
    - STP evita bucles en topologías con enlaces redundantes entre switches. Este protocolo bloquea los enlaces que causarían ciclos y asegura una única ruta activa entre nodos.
- Servicios en la Capa de Aplicación
    - Incluye servicios como HTTP, DNS o correo electrónico. En el laboratorio se configuró un servidor web Apache con soporte PHP y conexión a base de datos PostgreSQL, permitiendo desarrollar una aplicación web dinámica (calculadora de notas) ejecutada desde servidores Solaris y Windows Server.
- Diagnóstico y Comandos de Red
    - Se utilizaron herramientas como ifconfig, netstat, vnstat, route y ethtool para monitorear y diagnosticar el estado de la red. Estas herramientas permiten revisar interfaces, conexiones activas, tablas de enrutamiento y rendimiento de hardware.
- NAT y Direccionamiento IP
    - El uso de NAT (Network Address Translation) es esencial para permitir que dispositivos con direcciones IP privadas accedan a Internet mediante una IP pública. Fue clave para entender por qué algunos dispositivos no lograban hacer ping entre subredes sin configuración adecuada.

SETUP

1. Basic Switch Configuration

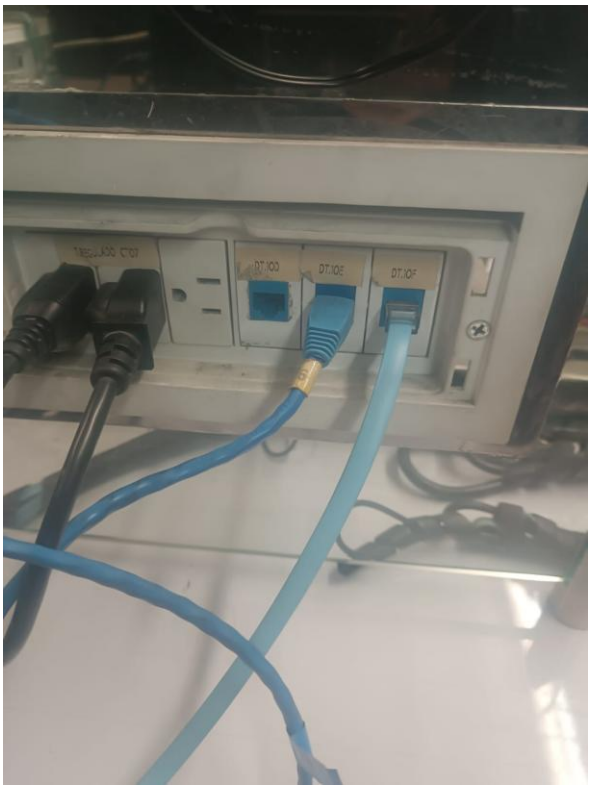
   Perform the following setup in groups. Each pair configures a switch and their 2 PCs



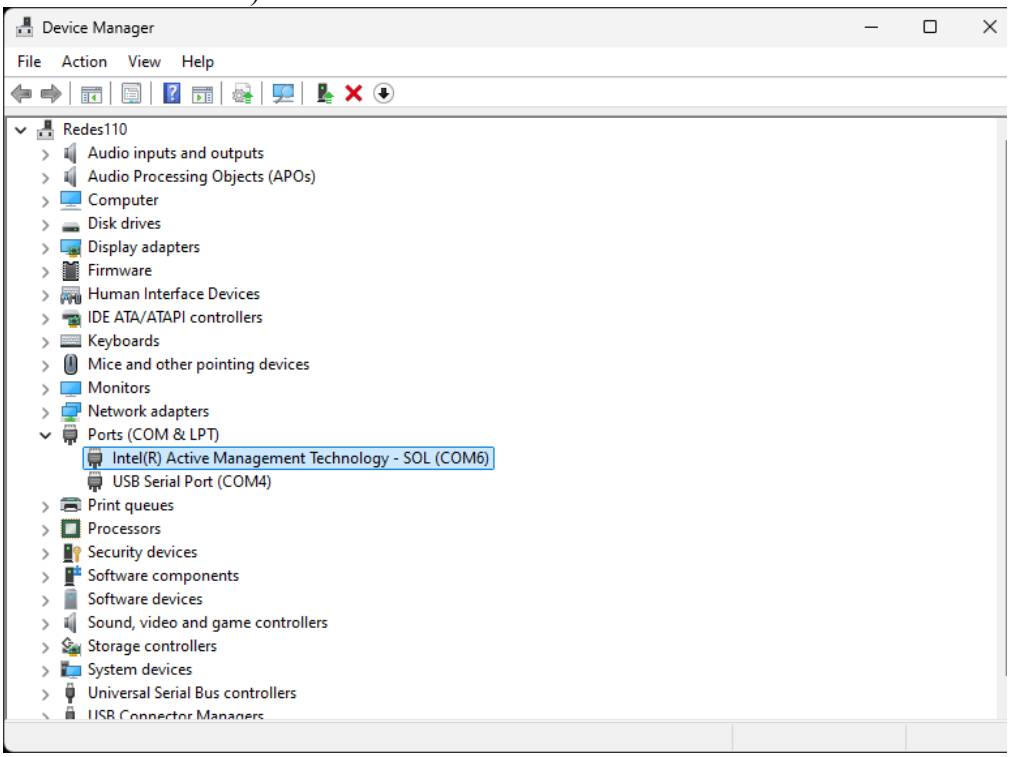
   a. Configure the devices as follows:

	PC0	PC1	PC2	PC3
Dirección IP estudiante1	183.24.30.A*	183.24.30.B*	183.24.30.C*	183.24.30.D*
Dirección IP estudiante2	183.24.50.E*	183.24.50.F*	183.24.50.G*	183.24.50.H*
Dirección IP estudiante3	183.24.70.I*	183.24.70.J*	183.24.70.K*	183.24.70.L*
Máscara	255.255.0.0 o /16			

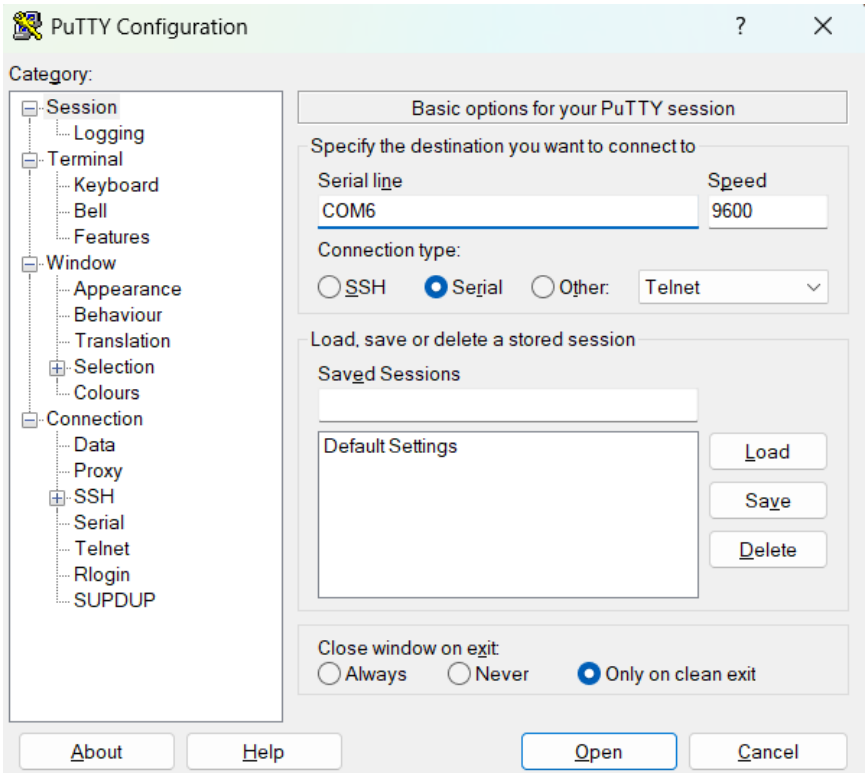
      i. Preparamos la capa fisica conectando el cable de consola del switch seleccionado (en este caso el 6) en el puerto dado en nuestra zona de trabajo, el cual es el 10f



ii. Una vez conectados los cables, verificamos el COM del cable de consola conectado a la maquina en el apartado Device Manager -> ports (En este caso es COM6)



iii. Luego ingresamos A PuTTY mediante el COM6



iv. Una vez en la consola del switch, realizamos la configuración inicial básica

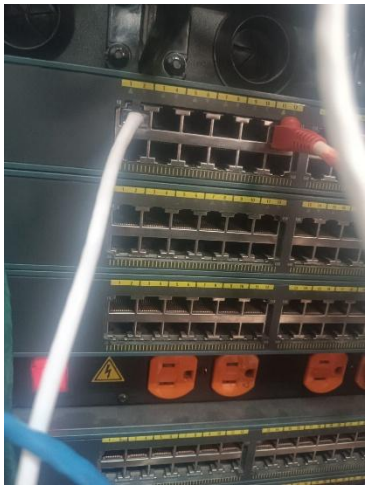
```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname tebinJuanin
tebinJuanin(config)#banner motd "Switch 6"
tebinJuanin(config)#line console 0
tebinJuanin(config-line)#logging synchronous
tebinJuanin(config-line)#password root123
tebinJuanin(config-line)#login
tebinJuanin(config-line)#exit
tebinJuanin(config)#no ip domain-lookup
tebinJuanin(config)#line vty 0 15
tebinJuanin(config-line)#loging synchronous
                         ^
% Invalid input detected at '^' marker.

tebinJuanin(config-line)#logging synchronous
tebinJuanin(config-line)#password root123
tebinJuanin(config-line)#login
tebinJuanin(config-line)#exit
tebinJuanin(config)#interface fa0/1
tebinJuanin(config-if)#description Connection with PC1
tebinJuanin(config-if)#exit
tebinJuanin(config)#interface fa0/2
tebinJuanin(config-if)#description Connection with PC2
tebinJuanin(config-if)#exit
tebinJuanin(config)#enable secret root123
tebinJuanin(config)#exit
tebinJuanin#
*Mar  1 00:41:22.658: %SYS-5-CONFIG_I: Configured from console by cons
tebinJuanin#
```

Donde:

- enable – Entra al modo privilegiado.
- configure terminal – Entra al modo de configuración global.
- hostname tebinJuanin – Cambia el nombre del switch a tebinJuanin.
- banner motd "Switch 6" – Muestra el mensaje "Switch 6" al iniciar sesión.
- line console 0 – Configura la línea de consola.
- logging synchronous – Evita que los mensajes interrumpan los comandos escritos.
- password root123 – Establece la contraseña de consola.
- login – Activa el requerimiento de contraseña en la consola.
- exit – Sale de la configuración de línea.
- no ip domain-lookup – Evita la búsqueda de nombres mal escritos como dominios.

- line vty 0 15 – Configura las líneas de acceso remoto (telnet/SSH).
- logging synchronous – Aplica sincronización de mensajes a VTY.
- password root123 – Establece la contraseña para VTY.
- login – Requiere contraseña al usar VTY.
- exit – Sale de la configuración de línea.
- interface fa0/1 – Entra a la interfaz FastEthernet 0/1.
- description Connection with PC1 – Agrega descripción a la interfaz.
- exit – Sale de la interfaz.
- interface fa0/2 – Entra a la interfaz FastEthernet 0/2.
- description Connection with PC2 – Agrega descripción a la interfaz.
- exit – Sale de la interfaz.
- enable secret root123 – Establece contraseña secreta para el modo privilegiado.
- exit – Sale al modo privilegiado.

v. Con la configuración inicial básica realizada, conectamos los cables de FastEthernet al Switch mediante los puertos mostrados anteriormente



vi. Ahora para realizar la conexión hacia el switch de nuestros compañeros de la mesa de trabajo, conectamos mediante el puerto GigabitEthernet los dos switches

vii. Una vez conectados, configuramos la interfaz en la consola al igual que realizamos las de FastEthernet

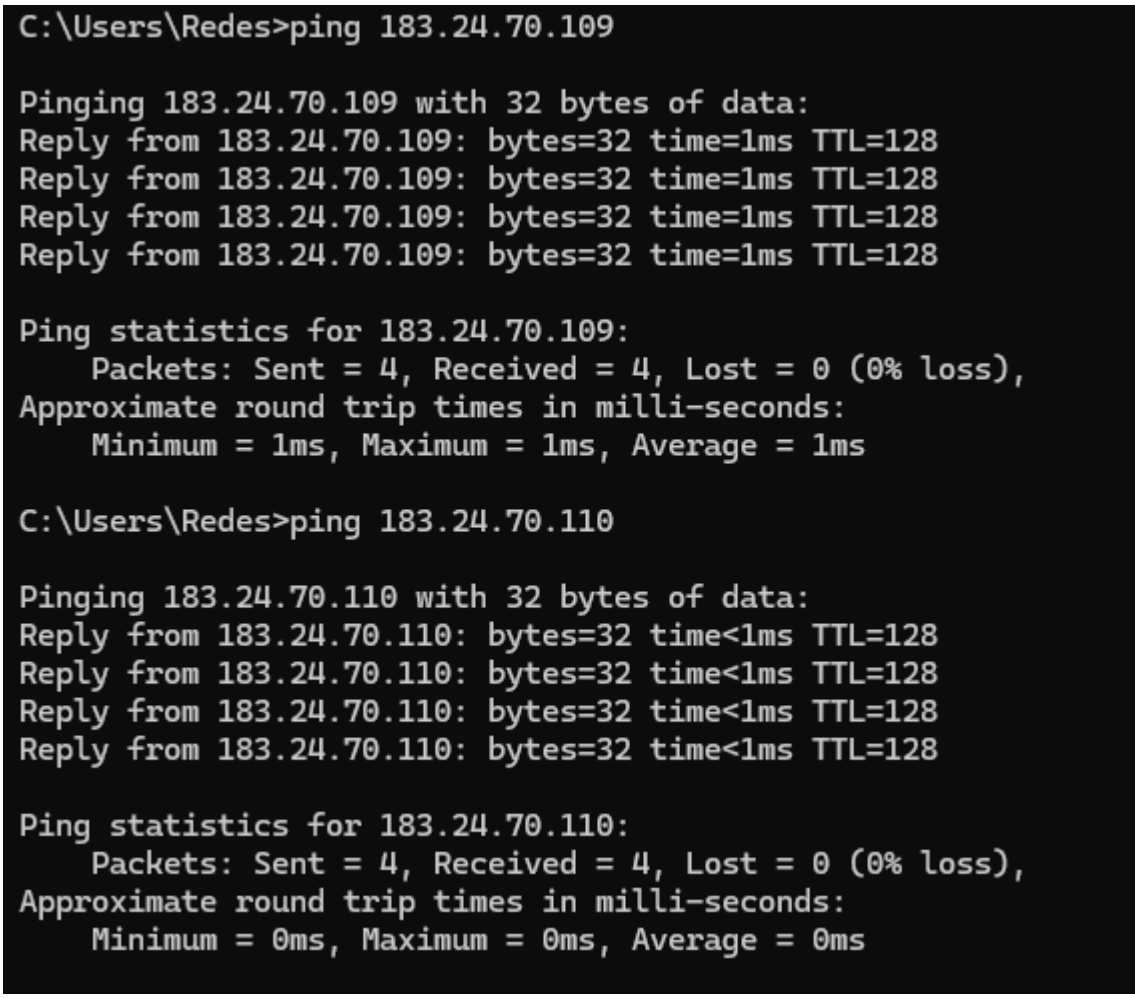
```
tebinJuanin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
tebinJuanin(config)#interface GigabitEthernet0/2
tebinJuanin(config-if)#description "Connection with switch 3"
tebinJuanin(config-if)#exit
tebinJuanin(config)#exit
tebinJuanin#wri
*Mar  1 01:21:51.513: %SYS-5-CONFIG_I: Configured from console by conso
tebinJuanin#write memory
Building configuration...
[OK]
tebinJuanin#
```

viii. Verificamos que tanto como los FastEthernet y el Gigabit que configuramos tengan los protoclos arriba con el comando show ip interface brief

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

ix.

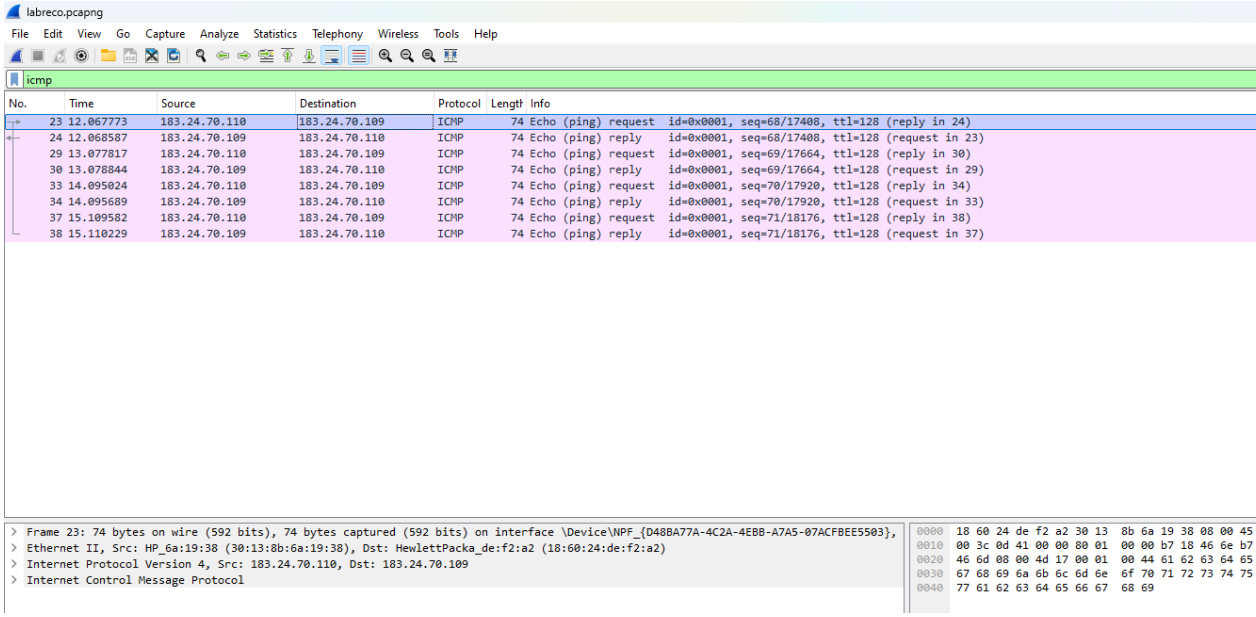
b. Verify the connectivity between the computers using the ping command.
   i. Agregamos las ip de los rangos dados (para nuestro caso son 183.24.70.109 y 110) en los dos equipos y tratamos de hacer ping entre ellos (el firewall de los equipos debe estar abajo)



ii. Ahora probamos la conexión con las maquinas de los compañeros de nuestra mesa de trabajo

```
C:\Users\Redes>ping 183.24.70.111

Pinging 183.24.70.111 with 32 bytes of data:
Reply from 183.24.70.111: bytes=32 time=75ms TTL=128
Reply from 183.24.70.111: bytes=32 time=1ms TTL=128
Reply from 183.24.70.111: bytes=32 time=1ms TTL=128
Reply from 183.24.70.111: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.70.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 75ms, Average = 19ms

C:\Users\Redes>ping 183.24.70.112

Pinging 183.24.70.112 with 32 bytes of data:
Reply from 183.24.70.112: bytes=32 time=137ms TTL=128
Reply from 183.24.70.112: bytes=32 time<1ms TTL=128
Reply from 183.24.70.112: bytes=32 time<1ms TTL=128
Reply from 183.24.70.112: bytes=32 time<1ms TTL=128

Ping statistics for 183.24.70.112:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 137ms, Average = 34ms

C:\Users\Redes>
```

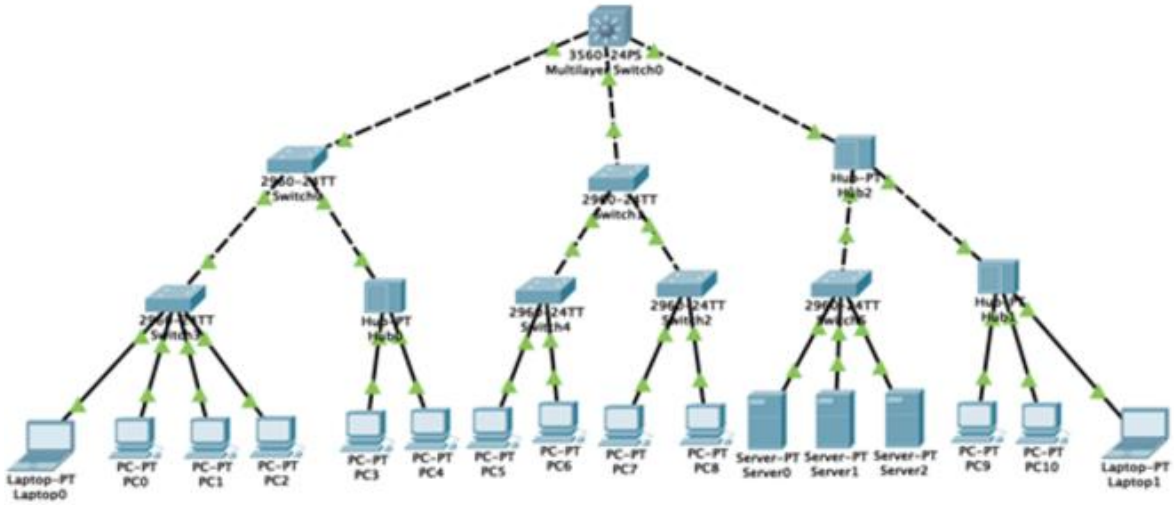
c. Use Wireshark to capture a packet and examine the Ethernet frame. Verify the frame structure, MAC addresses, error control, etc.



- Estructura de la Trama Ethernet
    - Tipo de trama: Ethernet II
    - Tipo de protocolo: 0x0800 (IPv4)
    - Encapsulamiento superior: Protocolo IP que contiene un mensaje ICMP
- 2. Direcciones MAC
    - Dirección MAC de origen: 98:da:c4:0e:f2:b3
    - Dirección MAC de destino: 3c:2c:30:d6:cf:6b
      Estas direcciones identifican los dispositivos de red físico que participan en la comunicación.
- Control de Errores
    - El campo FCS (Frame Check Sequence), responsable de la detección de errores en la trama Ethernet, no se muestra en la interfaz de Wireshark ya que es procesado y eliminado por la tarjeta de red (NIC) antes de que el paquete sea capturado.
    - La correcta visualización del paquete indica que no hubo errores detectados en la transmisión.
- Protocolo de Red y Capa de Aplicación
    - Protocolo IP (versión 4): Transporta un mensaje ICMP.
    - Protocolo ICMP: Se identifican paquetes de tipo "Echo (ping) request" y "Echo (ping) reply", lo que confirma conectividad entre los dispositivos.
    - Los identificadores de secuencia y TTL son visibles, lo que permite verificar el tiempo de vida de los paquetes y la correlación entre solicitudes y respuestas.

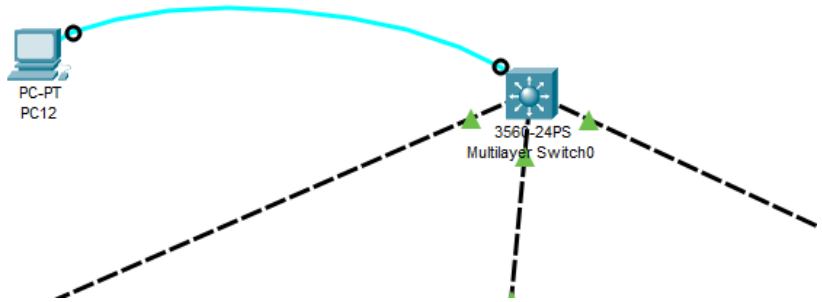
2. Larger Switch Networks

Using Cisco Packet Tracer, set up the following network. Each student must create their own Packet Tracer project.

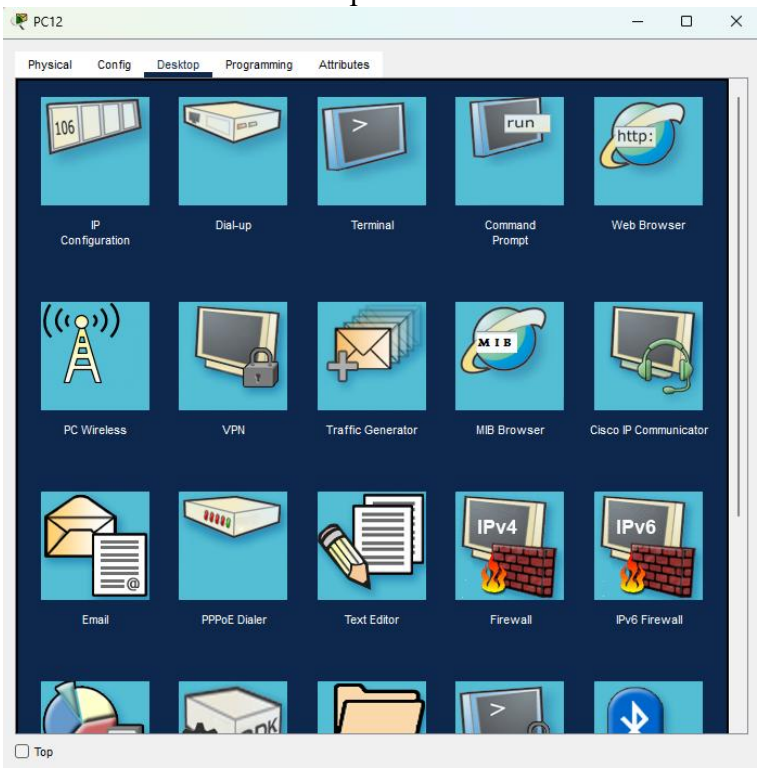


a. Perform the basic configuration on ALL switches.

i. Para realizar la configuración en los switches, agregamos una maquina adicional y lo conectamos mediante un cable de consola al switch que queramos configurar. Iniciamos con el multiplayer switch0



ii. Entramos a la terminal del pc 12

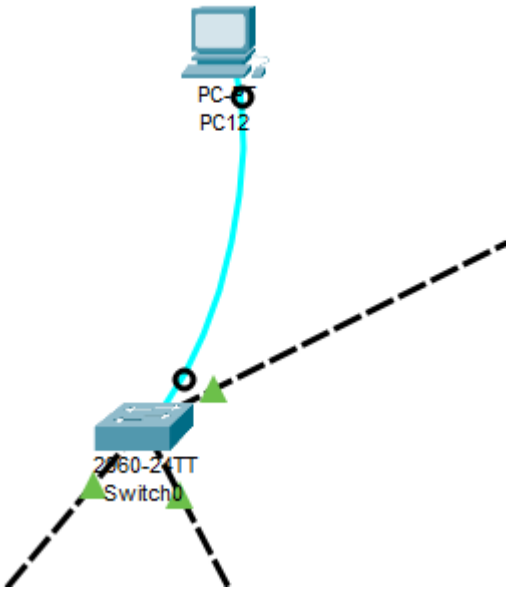


iii. Realizamos la configuración inicial del switch configuración el hostname, , login e interfaces de red con su respectiva descripción del equipo al cual se conecta.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname multiplayerSwitch
multiplayerSwitch(config)#banner motd "Lab 08 / Multiplayer switch"
multiplayerSwitch(config)#line console 0
multiplayerSwitch(config-line)#logging synchronous
multiplayerSwitch(config-line)#exit
multiplayerSwitch(config)#interface fastEthernet 0/1
multiplayerSwitch(config-if)#description connection to switch0
multiplayerSwitch(config-if)#exit
multiplayerSwitch(config)#interface fastEthernet 0/2
multiplayerSwitch(config-if)#description
% Incomplete command.
multiplayerSwitch(config-if)#description connection to switch 1
multiplayerSwitch(config-if)#exit
multiplayerSwitch(config)#interface fastEthernet 0/3
multiplayerSwitch(config-if)#description connection to hub2
multiplayerSwitch(config-if)#exit
multiplayerSwitch(config)#write memory
                         ^
% Invalid input detected at '^' marker.

multiplayerSwitch(config)#exit
multiplayerSwitch#
%SYS-5-CONFIG_I: Configured from console by console

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

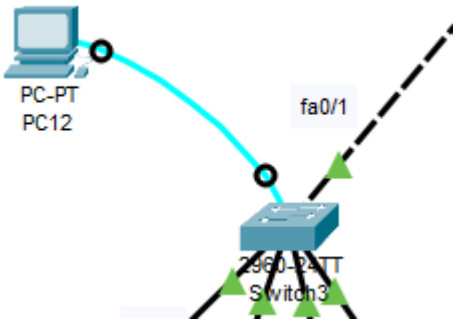
iv. Ahora repetimos el mismo proceso para los demás switches (conectar cable de consola y realizar configuración básica de switch)

v. Switch 0



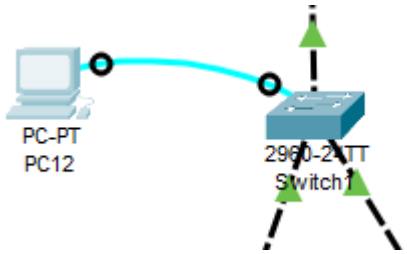
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch0
switch0(config)#banner motd "Lab 08 / Switch0"
switch0(config)#line console 0
switch0(config-line)#logging synchronous
switch0(config-line)#exit
switch0(config)#interface fastEthernet 0/1
switch0(config-if)#description connection to multiplayer switch 0
switch0(config-if)#exit
switch0(config)#interface fastEthernet 0/2
switch0(config-if)#description connection to switch 3
switch0(config-if)#exit
switch0(config)#interface fastEthernet 0/3
switch0(config-if)#description connection to hub 0
switch0(config-if)#exit
switch0(config)#exit
switch0#
%SYS-5-CONFIG_I: Configured from console by console

switch0#write memory
Building configuration...
[OK]
switch0#
```

vi. Switch 3



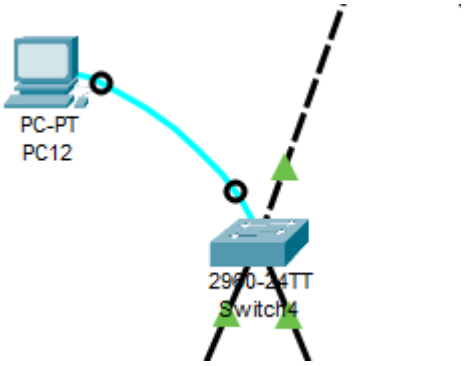
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch 3
                           ^
% Invalid input detected at '^' marker.

Switch(config)#hostname switch3
switch3(config)#banner motd "Lab 08 / Switch3"
switch3(config)#line console 0
switch3(config-line)#logging synchronous
switch3(config-line)#exit
switch3(config)#interface fastEthernet 0/1
switch3(config-if)#description connection to switch0
switch3(config-if)#exit
switch3(config)#interface fastEthernet 0/2
switch3(config-if)#description connection to laptop 0
switch3(config-if)#exit
switch3(config)#interface fastEthernet 0/3
switch3(config-if)#description connection to pc0
switch3(config-if)#exit
switch3(config)#interface fastEthernet 0/4
switch3(config-if)#description connection to pc1
switch3(config-if)#exit
switch3(config)#interface fastEthernet 0/5
switch3(config-if)#description connection to pc2
switch3(config-if)#exit
switch3(config)#exit
switch3#
%SYS-5-CONFIG_I: Configured from console by console

switch3#write memory
Building configuration...
[OK]
switch3#
```

vii. Switch 1



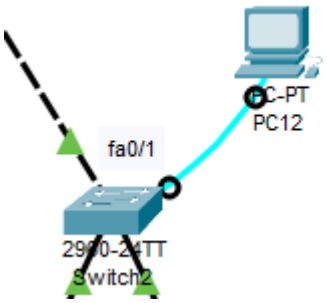
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#banner motd "Lab08 / switch1"
Switch(config)#line console
% Incomplete command.
Switch(config)#logging synchronous
                      ^
% Invalid input detected at '^' marker.

Switch(config)#logging synchronous
                      ^
% Invalid input detected at '^' marker.

Switch(config)#line console 0
Switch(config-line)#logging synchronous
Switch(config-line)#exit
Switch(config)#interface fastEthernet0/1
Switch(config-if)#description connection to multiplayer Switch0
Switch(config-if)#exit
Switch(config)#interface fastEthernet0/2
Switch(config-if)#description connection to switch4
Switch(config-if)#exit
Switch(config)#interface fastEthernet0/3
Switch(config-if)#description connection to switch2
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

viii. Switch 4



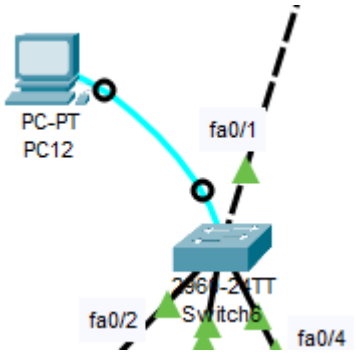
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch 4
                               ^
% Invalid input detected at '^' marker.

Switch(config)#hostname switch4
switch4(config)#bannermotd "Lab08 /switch4"
                       ^
% Invalid input detected at '^' marker.

switch4(config)#banner motd "Lab08 /switch4"
switch4(config)#line console 0
switch4(config-line)#logging synchronous
switch4(config-line)#exit
switch4(config)#interface fastEthernet 0/1
switch4(config-if)#description connection to switch 1
switch4(config-if)#exit
switch4(config)#interface fastEthernet 0/2
switch4(config-if)#description connection to pc5
switch4(config-if)#exit
switch4(config)#interface fastEthernet 0/3
switch4(config-if)#description connection to pc6
switch4(config-if)#exit
switch4(config)#exit
switch4#
%SYS-5-CONFIG_I: Configured from console by console

switch4#write memory
Building configuration...
[OK]
switch4#
```

ix. Switch 2



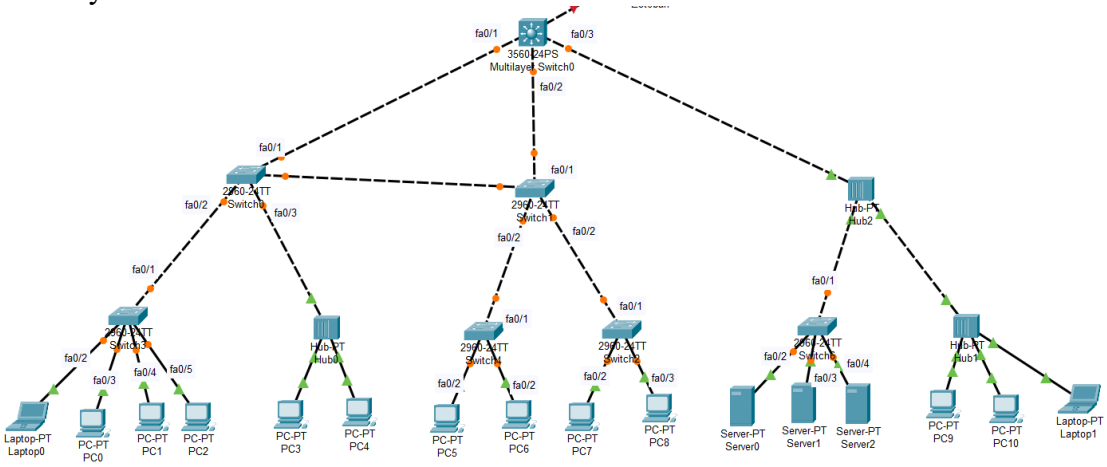
```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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

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

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

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


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch2
switch2(config)#banner motd "Lab08 / switch2"
switch2(config)#line console 0
switch2(config-line)#logging synchronous
switch2(config-line)#exit
switch2(config)#interface fastEthernet0/1
switch2(config-if)#description connection to switch 1
switch2(config-if)#exit
switch2(config)#interface fastEthernet0/2
switch2(config-if)#description connection to pc7
switch2(config-if)#exit
switch2(config)#interface fastEthernet0/3
switch2(config-if)#description connection to pc8
switch2(config-if)#exit
switch2(config)#exit
switch2#
%SYS-5-CONFIG_I: Configured from console by console

switch2#write memory
Building configuration...
[OK]
switch2#
```

x. Switch 6



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

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

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


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch6
switch6(config)#banner motd "Lab08 / switch6"
switch6(config)#line console 0
switch6(config-line)#logging synchronous
switch6(config-line)#exit
switch6(config)#interface fastEthernet0/1
switch6(config-if)#connection to hub2
                   ^
% Invalid input detected at '^' marker.

switch6(config-if)#description connection to hub2
switch6(config-if)#exit
switch6(config)#interface fastEthernet0/2
switch6(config-if)#description connection to server0
switch6(config-if)#exit
switch6(config)#interface fastEthernet0/3
switch6(config-if)#description connection to server1
switch6(config-if)#exit
switch6(config)#interface fastEthernet0/4
switch6(config-if)#description connection to server2
switch6(config-if)#exit
switch6(config)#exit
switch6#
%SYS-5-CONFIG_I: Configured from console by console

switch6#write memory
Building configuration...
[OK]
switch6#
```

xi. Agregamos comentarios de las interfaces de la configuración realizada para mayor claridad en la interfaz

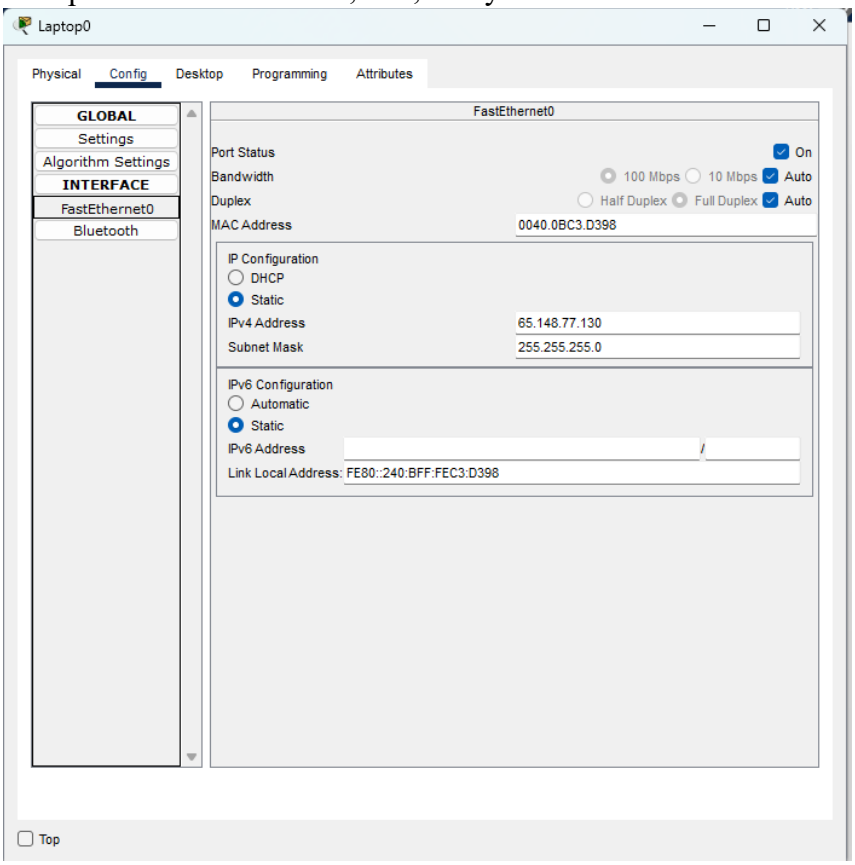


b. Configure the computers and servers with the information provided below:

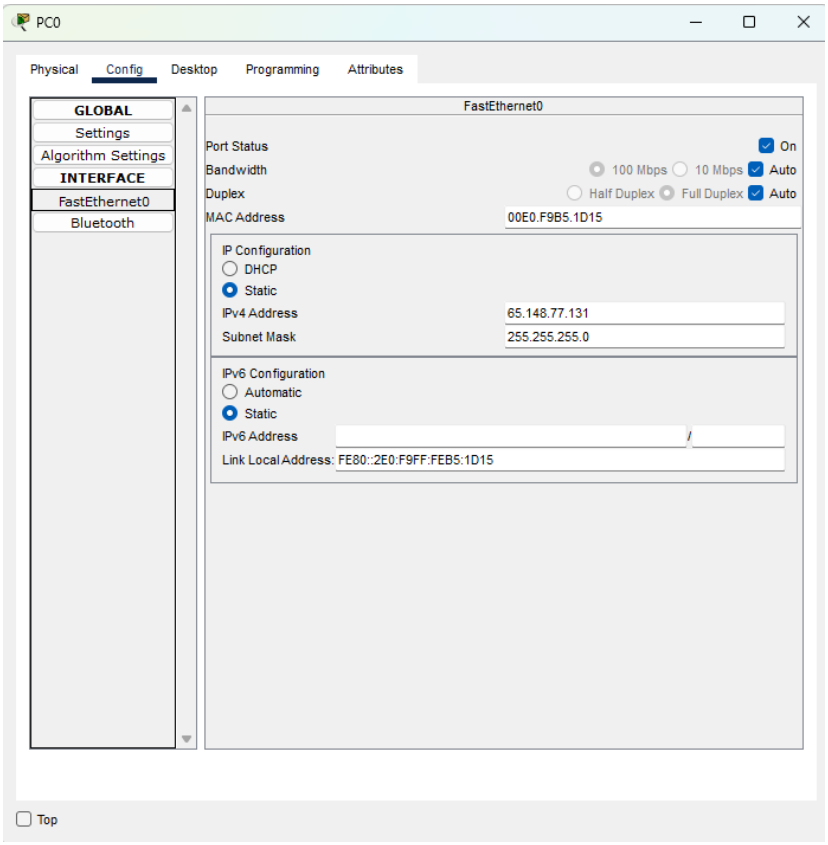
Estudiante1	Estudiante 2	Estudiante 3
IP: 65.148.77.x (x= número secuencial de 100 a 120) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1	IP: 65.148.77.x (x= número secuencial de 130 a 150) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1	IP: 65.148.77.x (x= número secuencial de 160 a 190) Máscara: 255.255.255.0;/24 Gateway: 65.148.77.1

i. Realizamos la configuración de los computadores en el apartado de la interfaz de red. (Para esta configuración usamos el estudiante 2 EstebanPacketTracerPunto3, Juanito tiene Estudiante 1)

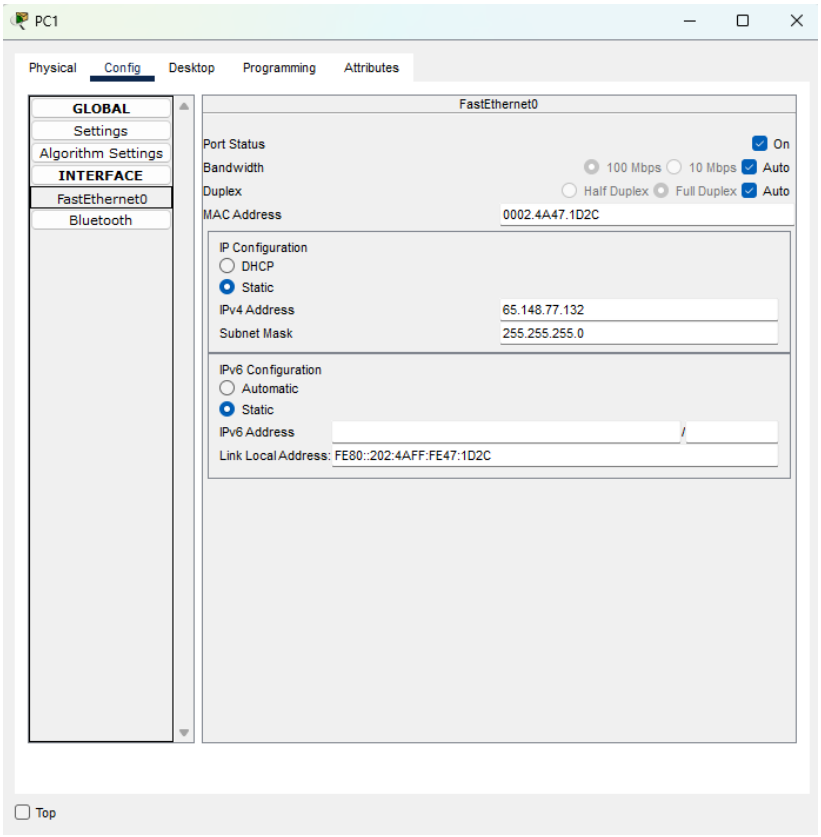
ii. Iniciamos con la laptop0 y repetimos el proceso para las demás maquinas reemplazando la x con 130, 131, 132 y así sucesivamente …



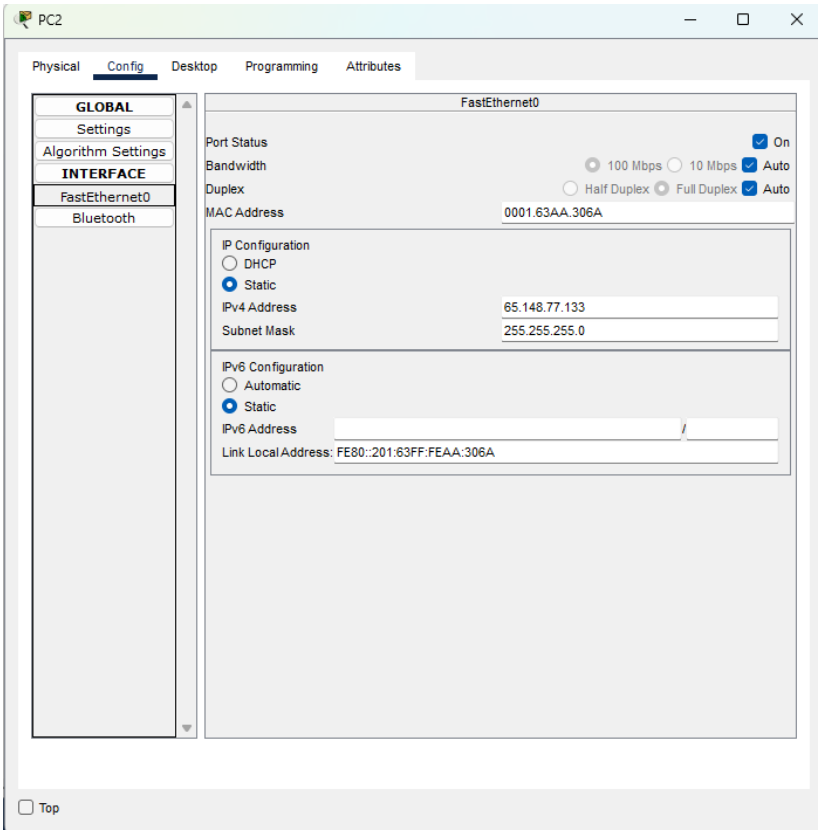
iii. Pc0


PC0
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F9B5.1D15
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.131
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::2E0:F9FF:FEB5:1D15
Top

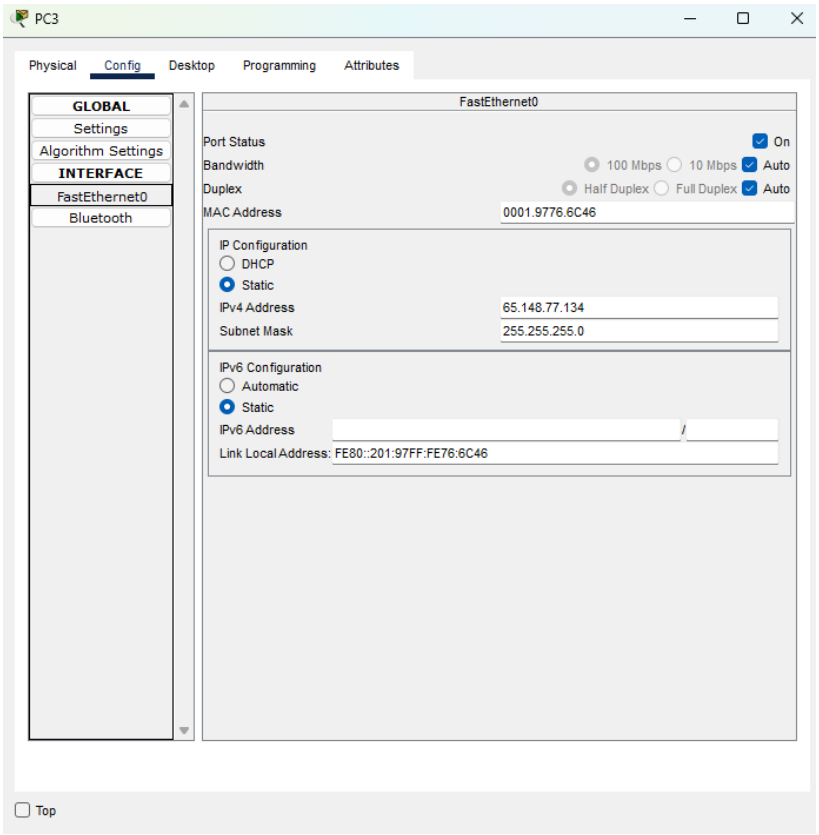
iv. Pc1


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.4A47.1D2C
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.132
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::202:4AFF:FE47:1D2C
Top

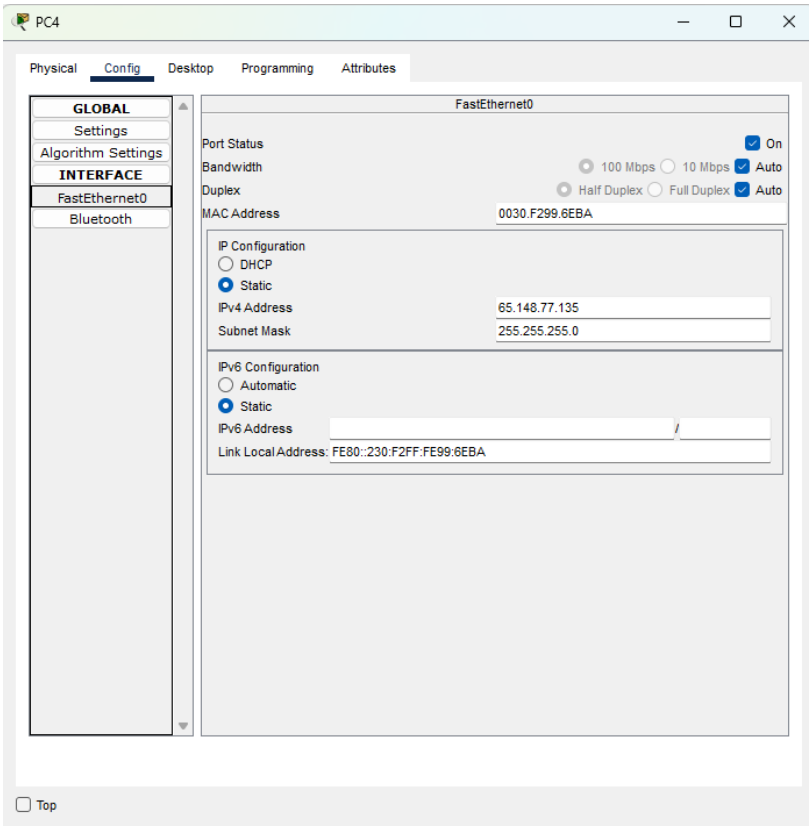
v. Pc2


PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.63AA.306A
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.133
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::201:63FF:FEAA:306A
Top

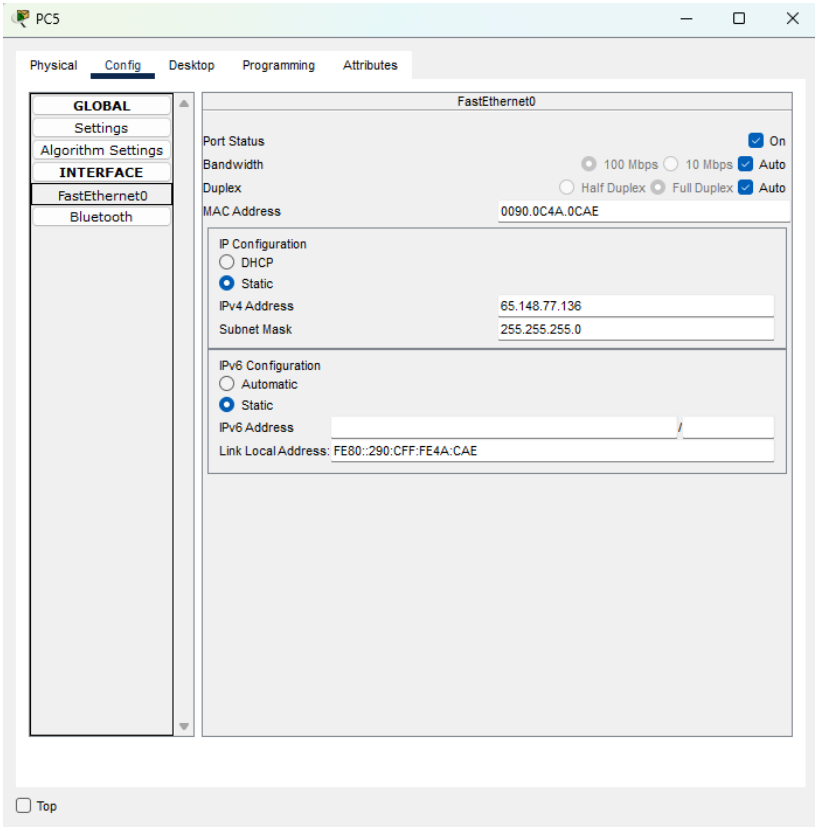
vi. Pc3


PC3
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.9776.6C46
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.134
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::201:97FF:FE76:6C46
Top

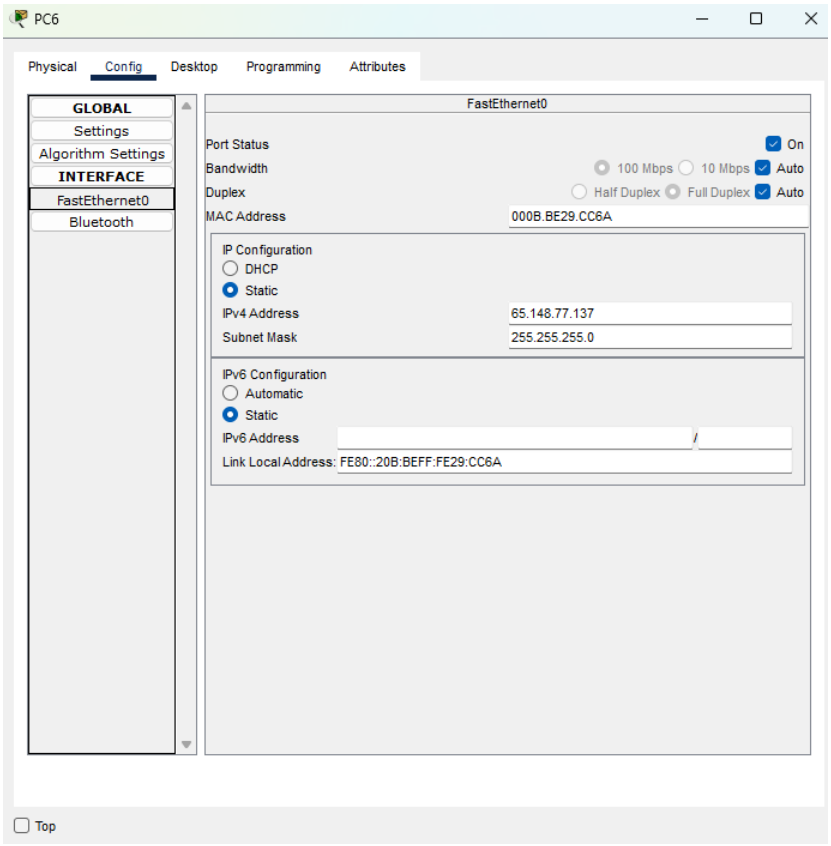
vii. Pc4



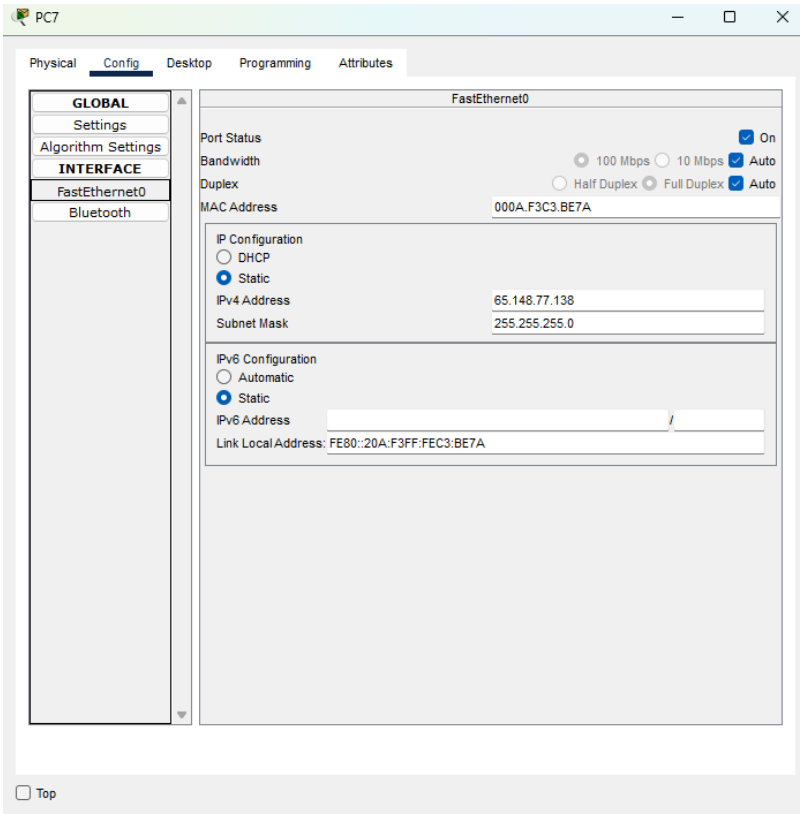
viii. Pc5



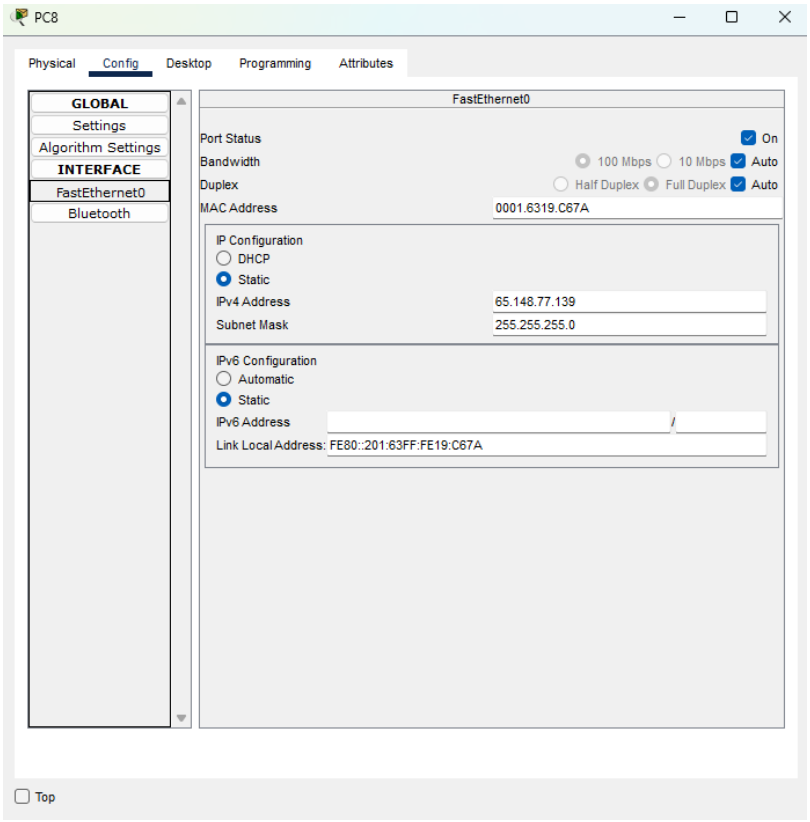
ix. Pc6


PC6
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000B.BE29.CC6A
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.137
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::20B:BEFF:FE29:CC6A
Top

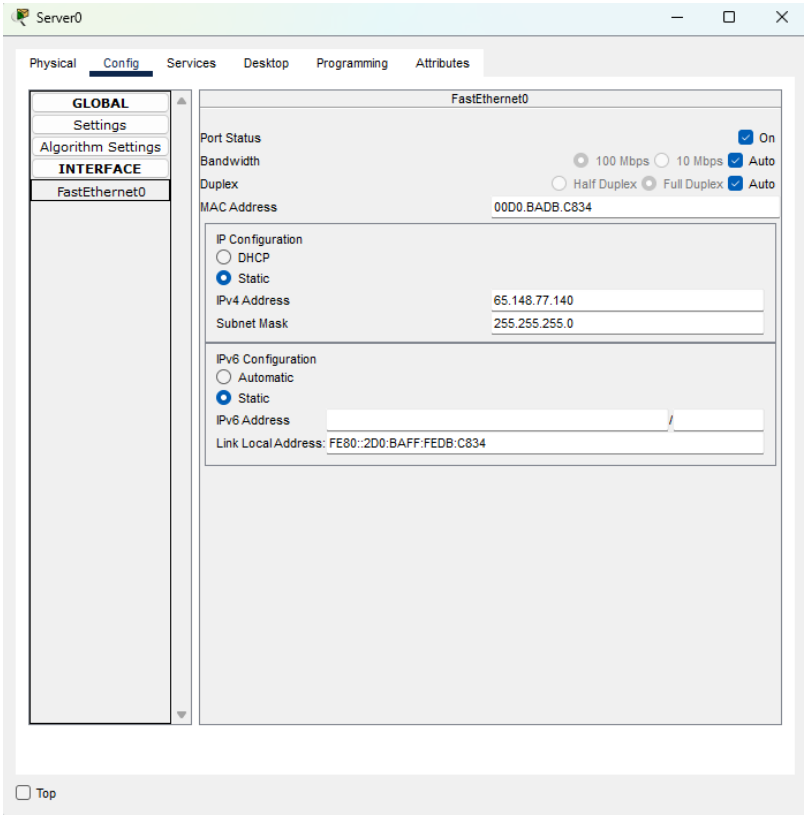
x. Pc7


PC7
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000A.F3C3.BE7A
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.138
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::20A:F3FF:FEC3:BE7A
Top

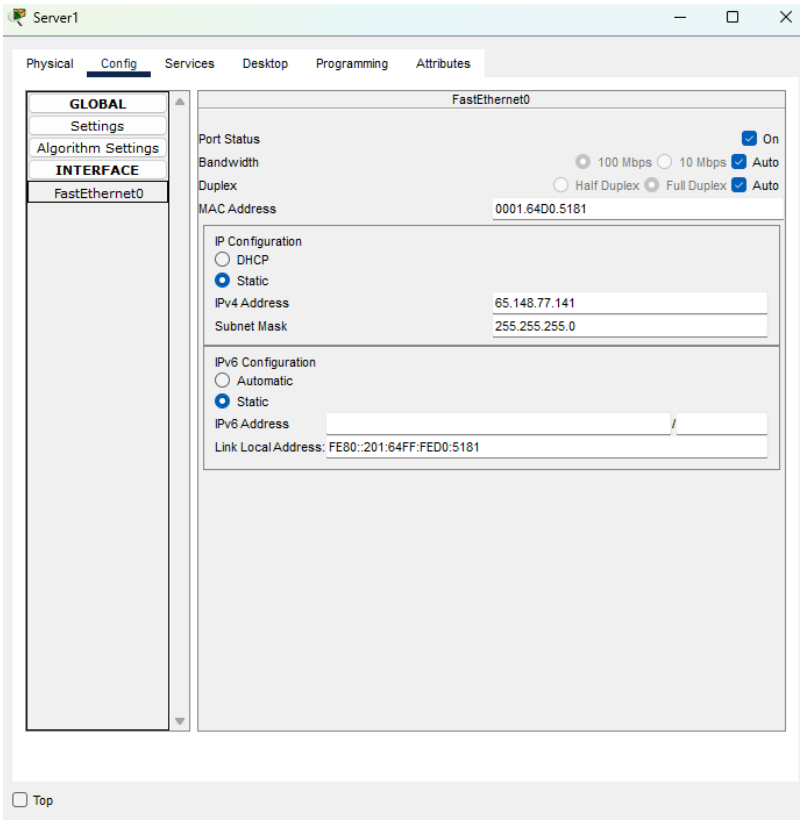
xi. Pc8



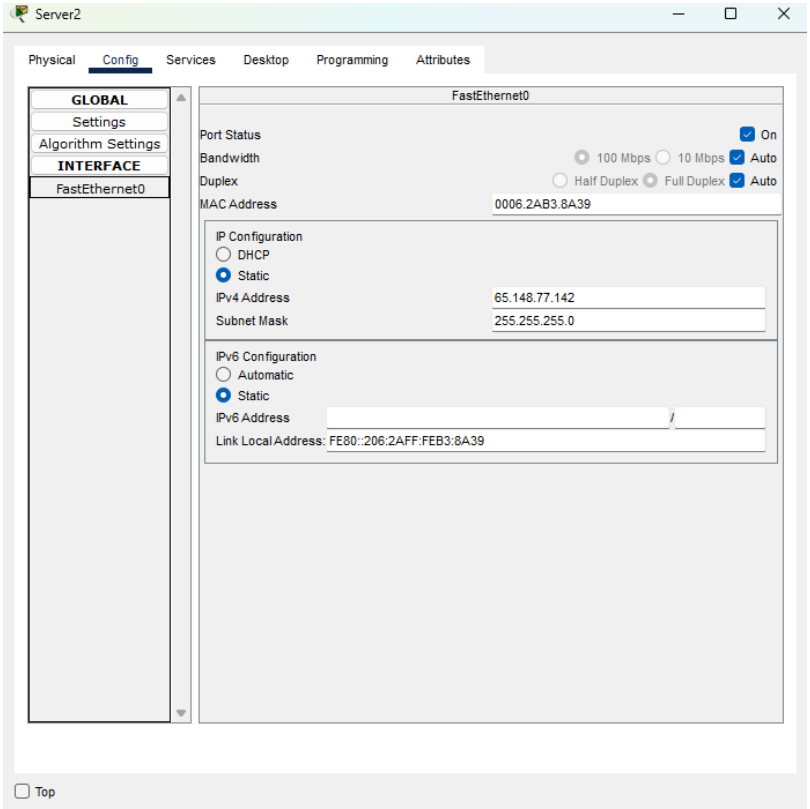
xii. Server0



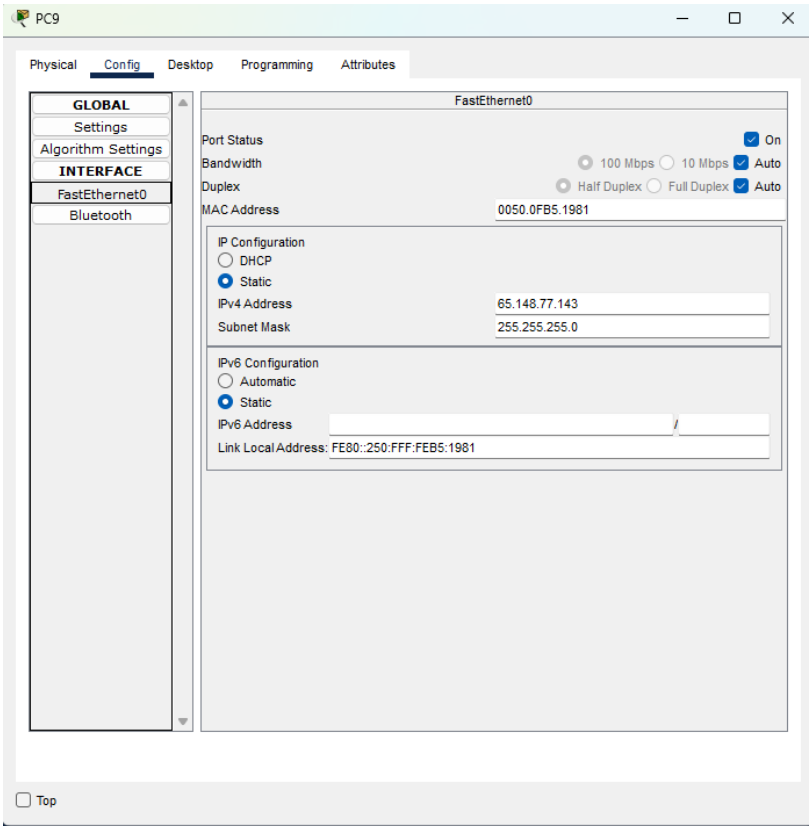
xiii. Server1



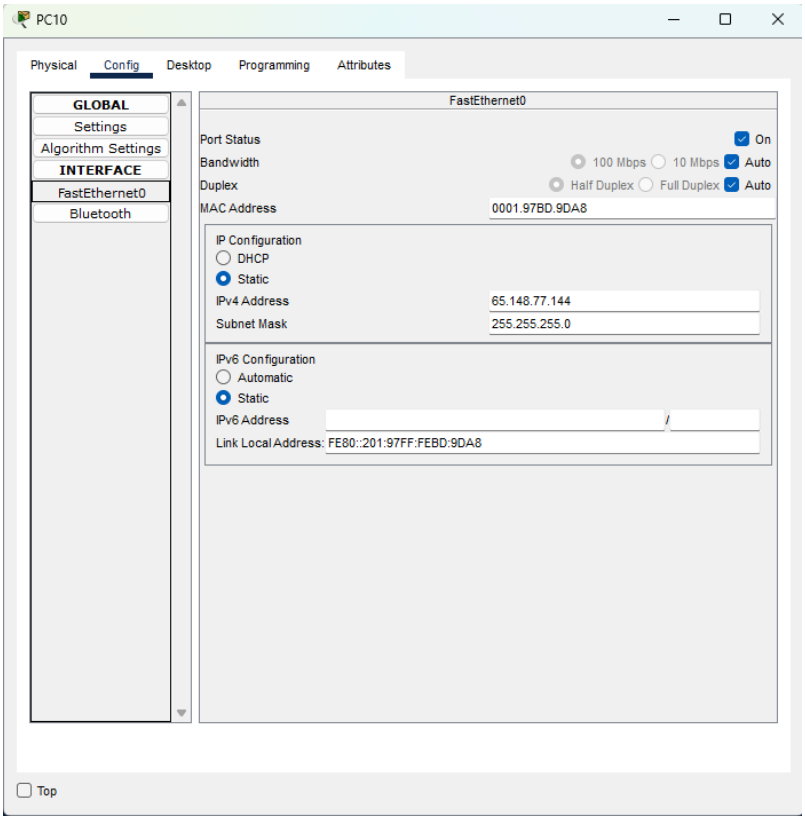
xiv. Server2



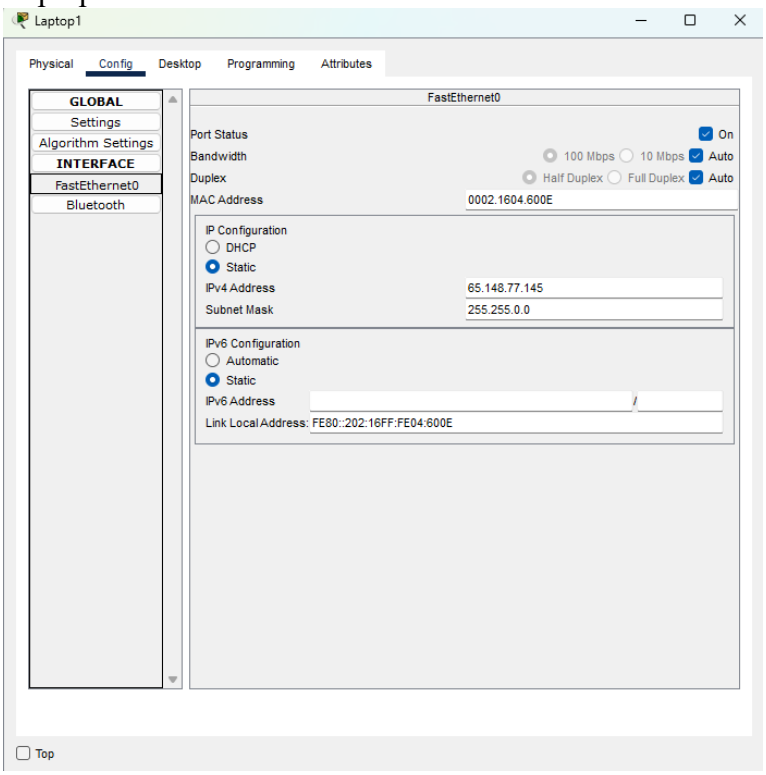
xv. Pc9



xvi. Pc10

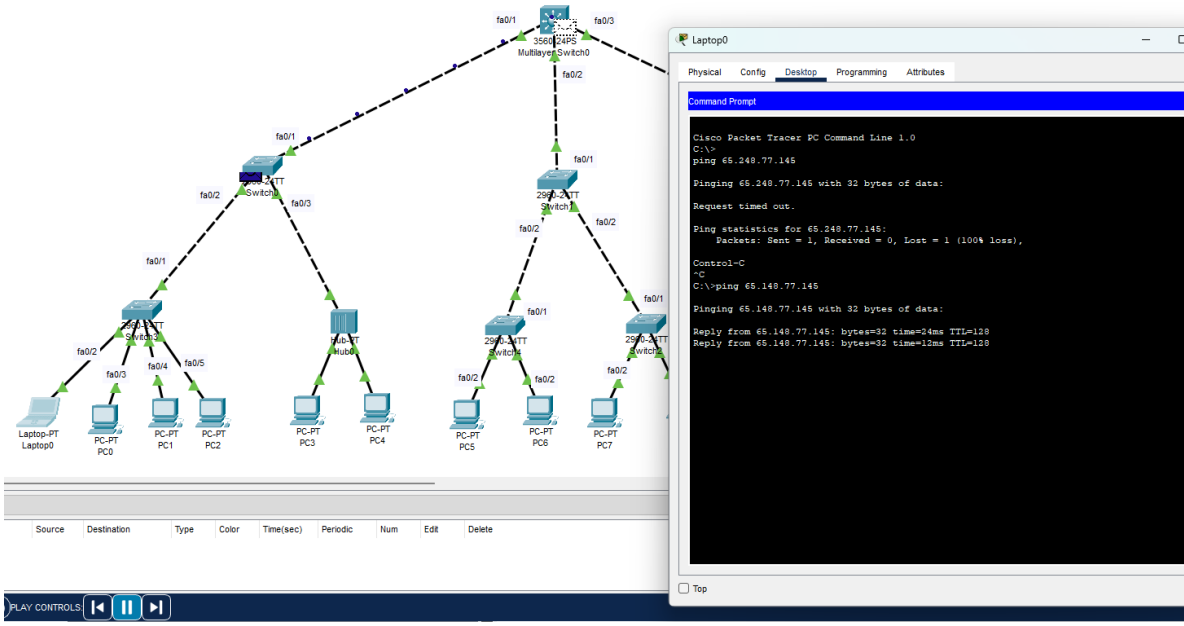


xvii. Laptop1



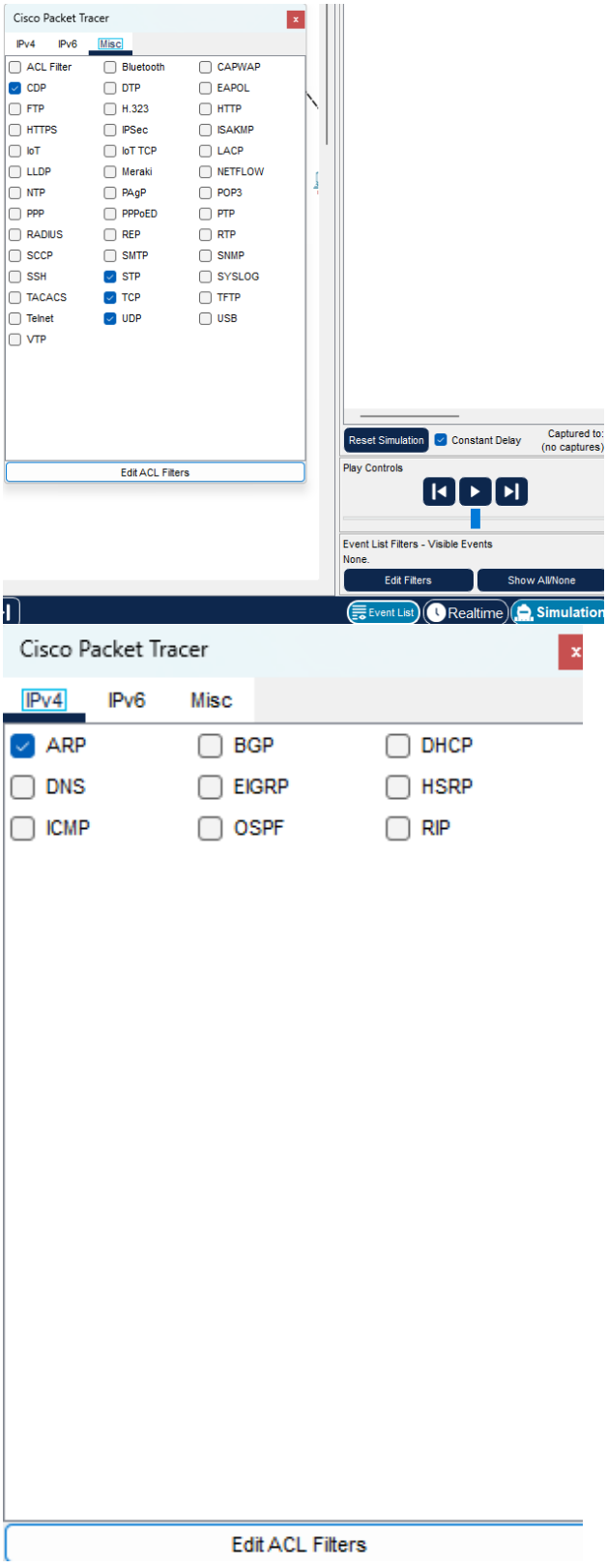
c. Check the connectivity between the devices.

i. Verificamos la conexión entre los dispositivos realizando una prueba desde la laptop 0 hasta la ultima maquina configurada la cual es la .145



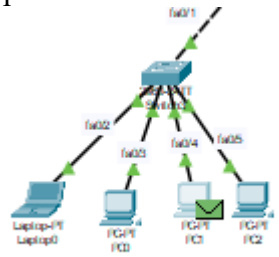
d. Using simulation mode, analyze the network behavior and the format of an Ethernet frame by sending the following frames. Identify the switches' behavior and their forwarding tables.

i. Para verificar la comunicación entre switches y maquinas solo dejamos seleccionados los protocolos necesarios. En este caso son CDP, STP, TCP, UDP, ARP

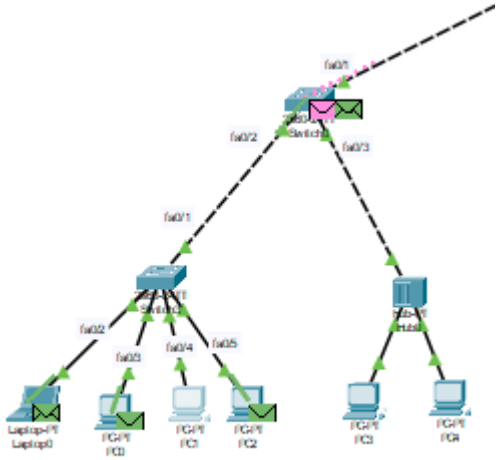


ii. From PC1 to PC7.

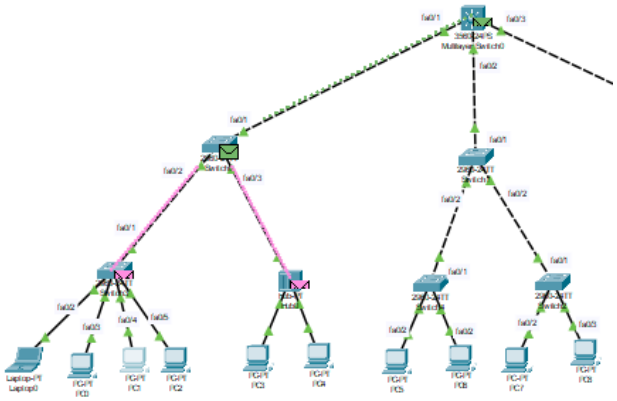
1. PC1 ejecuta el comando ping dirigido a la dirección IP de PC7. El mensaje ICMP se envía desde PC1 hacia el switch, ingresando por el puerto fa0/4.



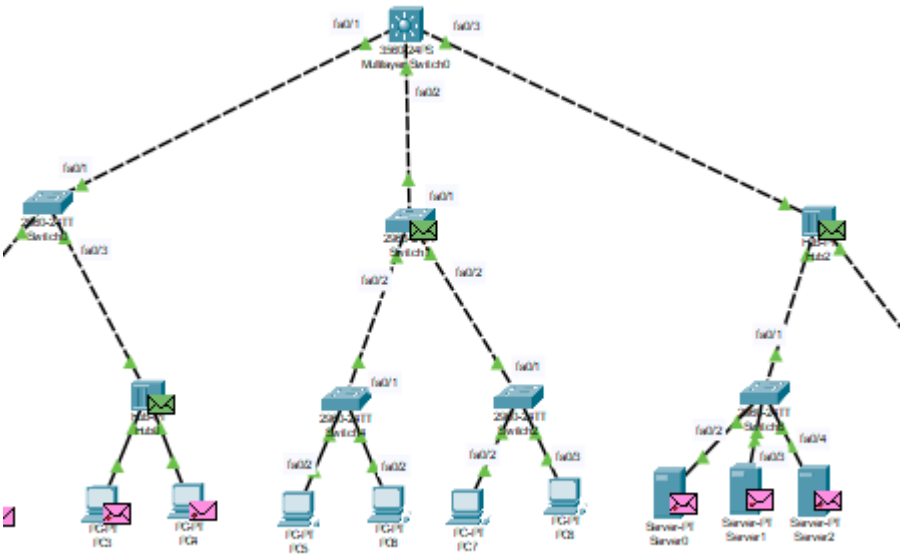
2. El switch recibe el mensaje y, al no conocer aún la dirección MAC de PC7, realiza un broadcast ARP para buscar el dispositivo correspondiente a esa IP. Todos los dispositivos que reciban este mensaje y no sean PC7 lo rechazarán.



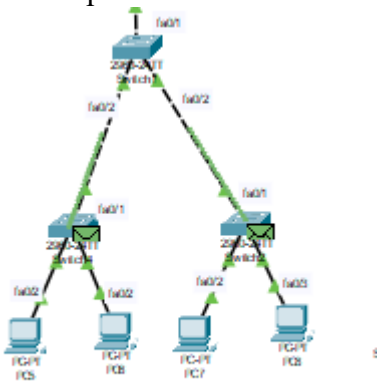
3. Si el mensaje llega a otro switch, este también realizará un broadcast para intentar encontrar al dispositivo con la IP de PC7.

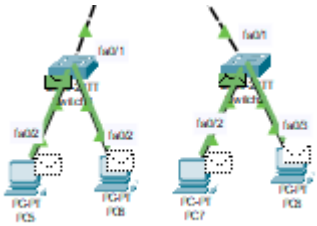


4. El mismo procedimiento se repite entre los switches a los que les llegue el broadcast, propagando la solicitud hasta cubrir toda la red.

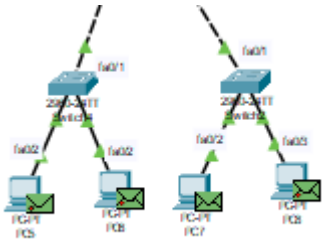


5. Los switches continúan reenviando el broadcast a todos sus puertos (excepto por donde llegó), hasta que el mensaje llega a todos los extremos posibles.



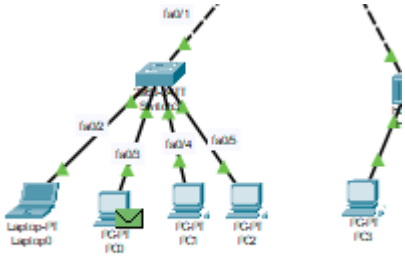


6. Finalmente, el mensaje llega a las máquinas conectadas. Las otras tres PCs rechazan el mensaje, mientras que PC7 lo acepta, responde con su dirección MAC, y se completa la comunicación. PC1 ahora puede enviar paquetes directamente a PC7 sin necesidad de broadcast.

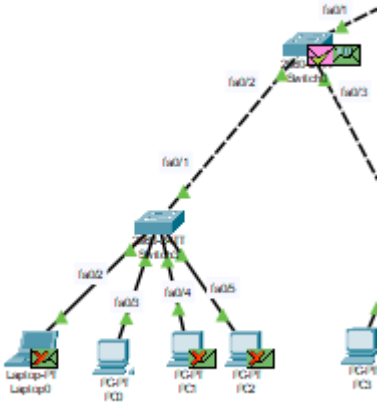


iii. From PC0 to PC9.

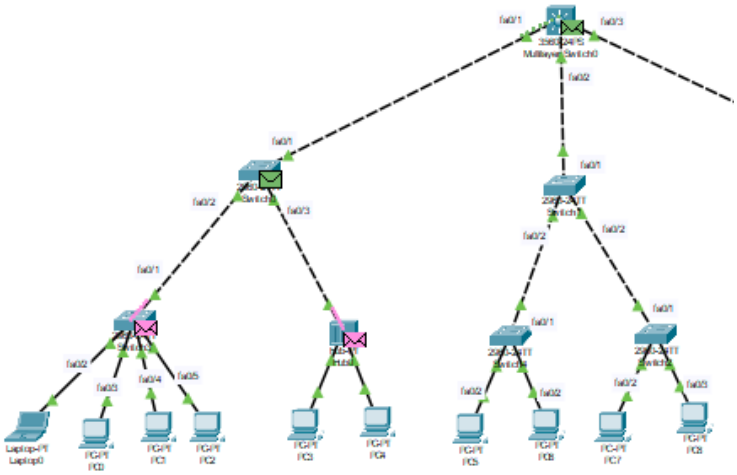
1. PC0 ejecuta el comando ping dirigido a la dirección IP de PC9. El mensaje ICMP se envía desde PC0 hacia el switch, ingresando por el puerto fa0/4.



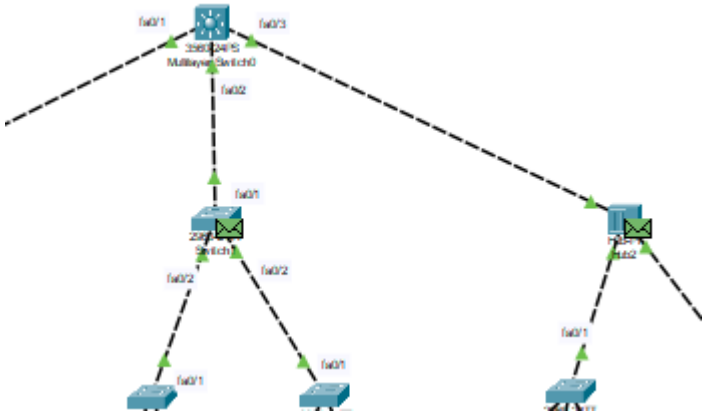
2. El switch recibe el mensaje y, al no conocer aún la dirección MAC de PC9, realiza un broadcast ARP para buscar el dispositivo correspondiente a esa IP. Todos los dispositivos que reciban este mensaje y no sean PC9 lo rechazarán.



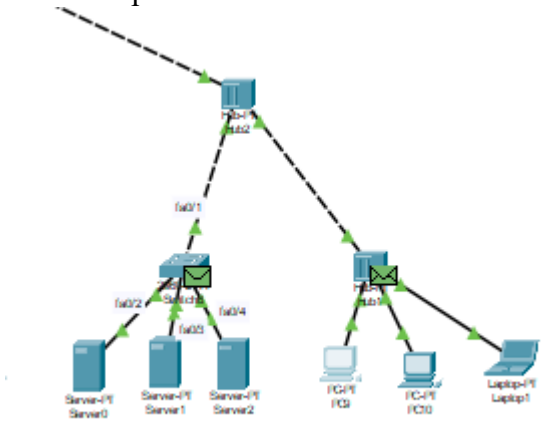
3. Si el mensaje llega a otro switch, este también realizará un broadcast para intentar encontrar al dispositivo con la IP de PC7.



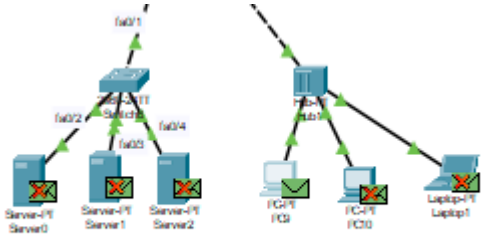
4. El mismo procedimiento se repite entre los switches a los que les llegue el broadcast, propagando la solicitud hasta cubrir toda la red.



5. Los switches continúan reenviando el broadcast a todos sus puertos (excepto por donde llegó), hasta que el mensaje llega a todos los extremos posibles.



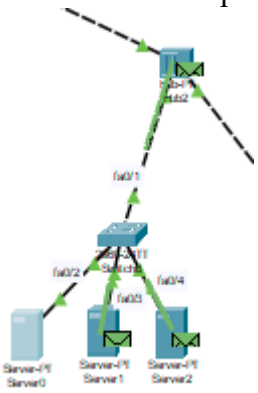
6. Finalmente, el mensaje llega a las máquinas conectadas. Las otras PCs rechazan el mensaje, mientras que PC9 lo acepta, responde con su dirección MAC, y se completa la comunicación. PC0 ahora puede enviar paquetes directamente a PC9 sin necesidad de broadcast.



iv. From Server0 to Server1

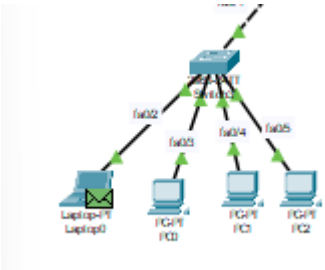
1. El Servidor 0 envía un mensaje ping dirigido al Servidor 1.

2. Al llegar el mensaje al hub, este no identifica direcciones, por lo que simplemente realiza un broadcast, enviando el mensaje a todos los dispositivos conectados a él. Todos los dispositivos reciben el mensaje, pero solamente el Servidor 1 lo reconoce como destinado a él. Este responde al Servidor 0, indicando que recibió correctamente el ping

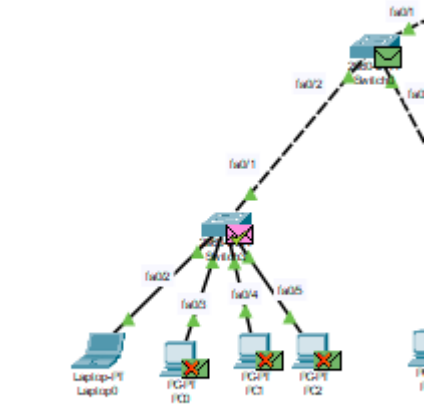


v. From Laptop0 to Laptop1.

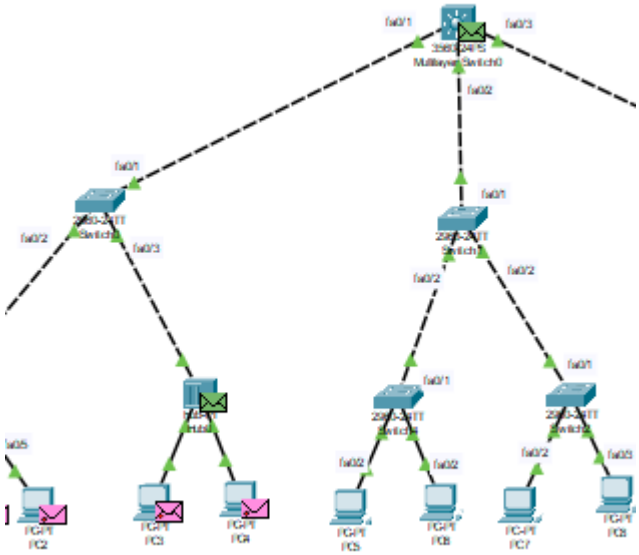
1. Laptop0 ejecuta el comando ping dirigido a la dirección IP de Laptop1. El mensaje ICMP se envía desde Laptop0 hacia el switch, ingresando por el puerto fa0/4.



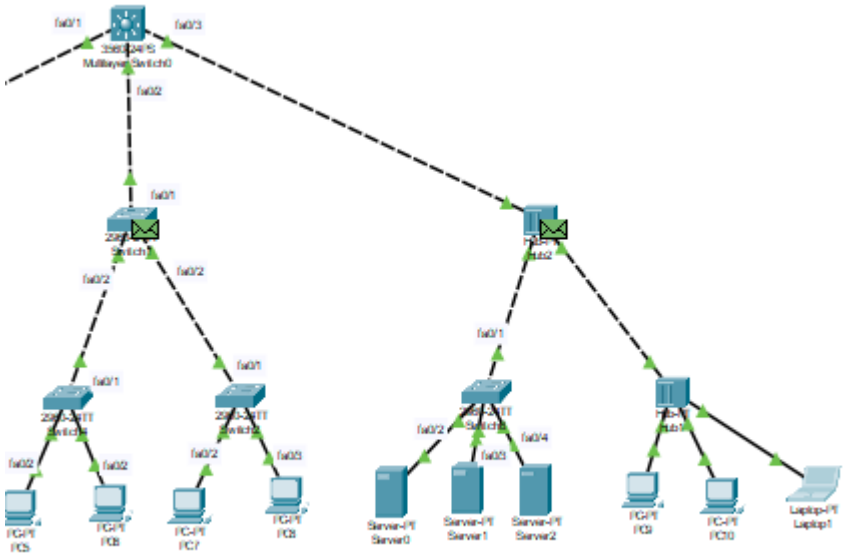
2. El switch recibe el mensaje y, al no conocer aún la dirección MAC de laptop1, realiza un broadcast ARP para buscar el dispositivo correspondiente a esa IP. Todos los dispositivos que reciban este mensaje y no sean laptop1 lo rechazarán.



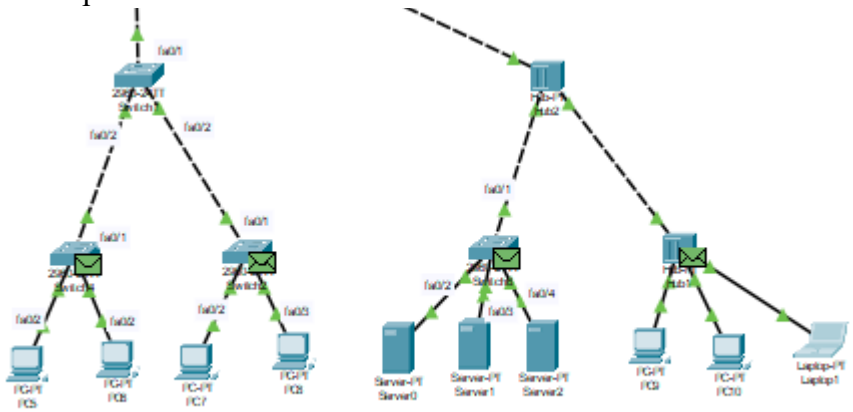
3. Si el mensaje llega a otro switch, este también realizará un broadcast para intentar encontrar al dispositivo con la IP de laptop1



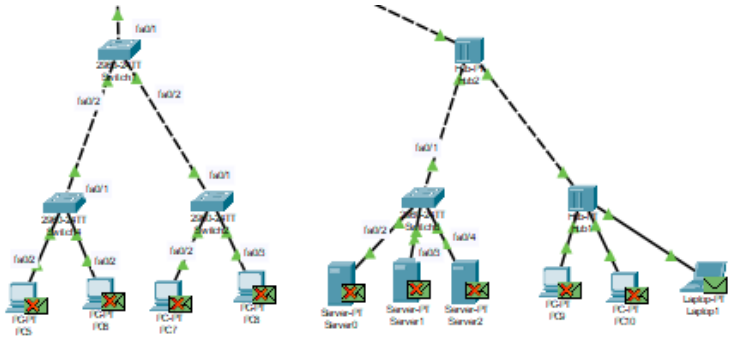
4. El mismo procedimiento se repite entre los switches a los que les llegue el broadcast, propagando la solicitud hasta cubrir toda la red.



5. Los switches continúan reenviando el broadcast a todos sus puertos (excepto por donde llegó), hasta que el mensaje llega a todos los extremos posibles.

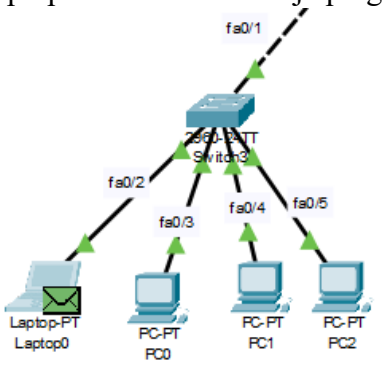


6. Finalmente, el mensaje llega a las máquinas conectadas. Las otras PCs rechazan el mensaje, mientras que laptop1 lo acepta, responde con su dirección MAC, y se completa la comunicación. laptop0 ahora puede enviar paquetes directamente a laptop1 sin necesidad de broadcast.

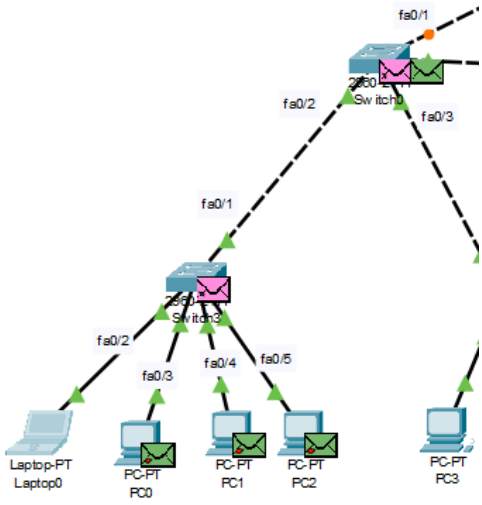


e. Examine the operation of the spanning tree algorithm. To do this, interconnect switches 0 and 1 and observe the link behavior.

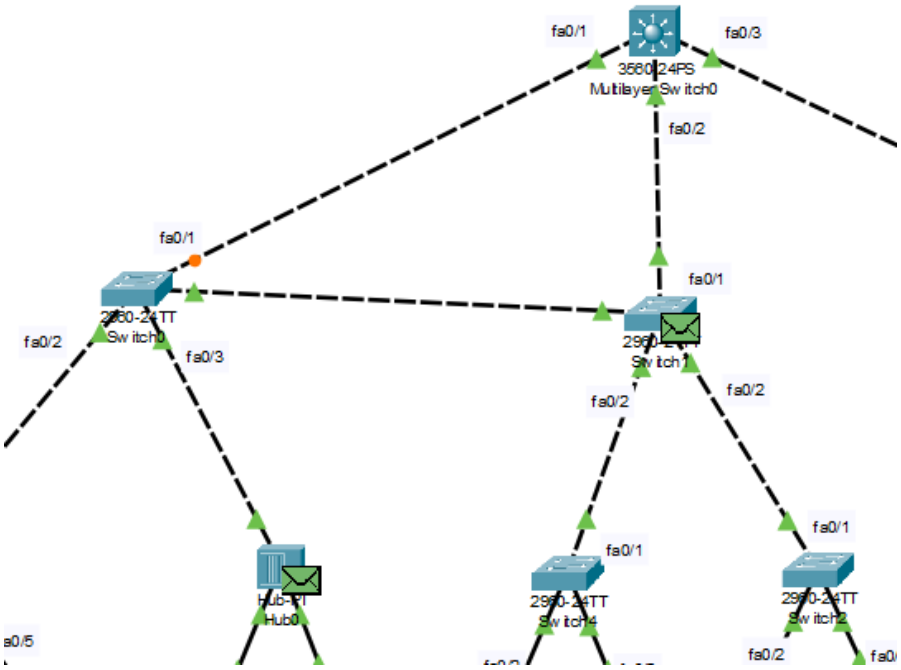
i. La laptop0 envía un mensaje ping dirigido al PC8.



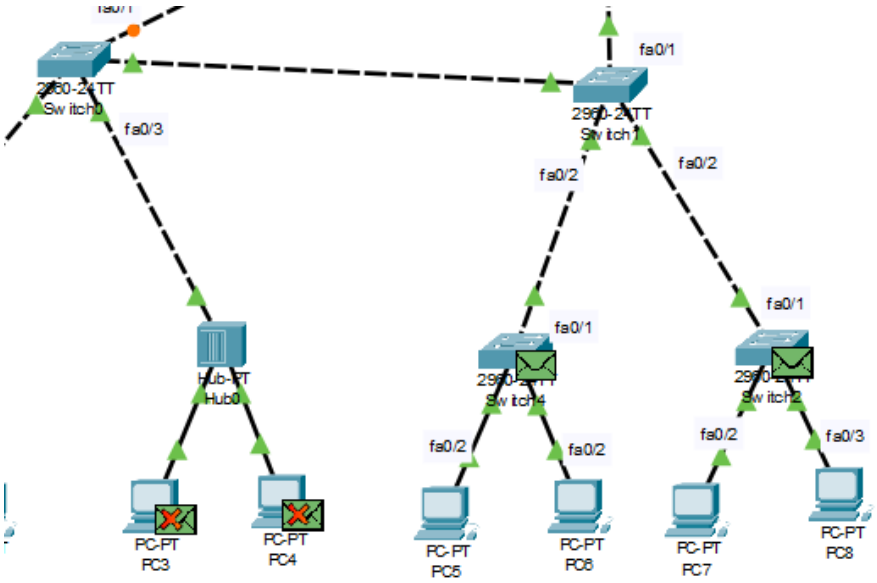
ii. El switch recibe el mensaje y, al no conocer aún la dirección MAC de PC8, realiza un broadcast ARP para buscar el dispositivo correspondiente a esa IP. Todos los dispositivos que reciban este mensaje y no sean laptop1 lo rechazarán.



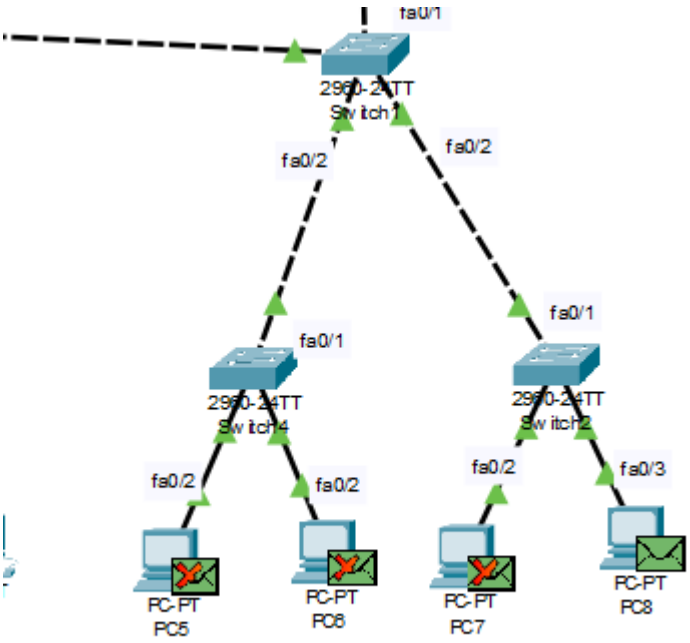
iii. Al haber dos caminos posibles para reenviar el mensaje, el switch aplica el protocolo Spanning Tree, cerrando uno de los caminos para evitar bucles en la red.



iv. Los switches continúan reenviando el broadcast a todos sus puertos (excepto por donde llegó), hasta que el mensaje llega a todos los extremos posibles.

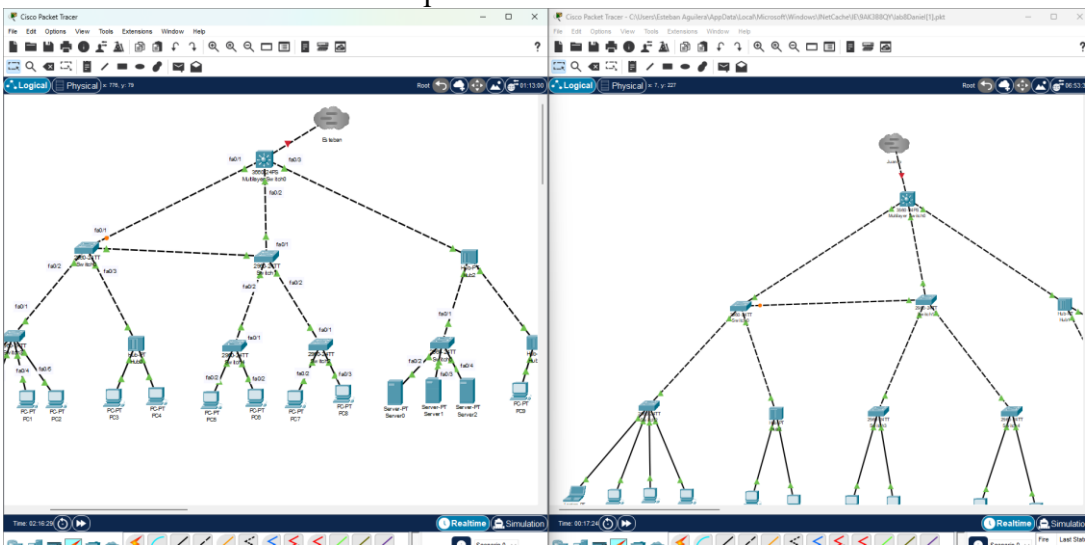


v. Finalmente, el mensaje llega a las máquinas conectadas. Las otras PCs rechazan el mensaje, mientras que PC8 lo acepta, responde con su dirección MAC, y se completa la comunicación. laptop0 ahora puede enviar paquetes directamente a PC8 sin necesidad de broadcast.



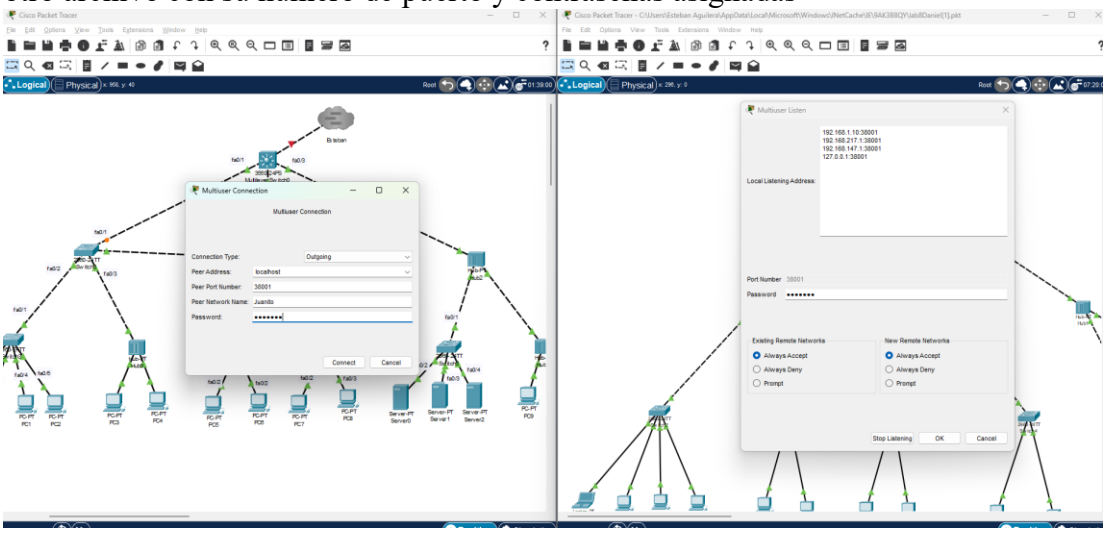
f. Merge the project files of the team members. For groups with one student, request a project file from a group of classmates, merge their project with yours, and indicate who provided the file.

i. Para realizar la conexión de los dos archivos, agregamos el objeto multiuser en los dos archivos de packet tracer

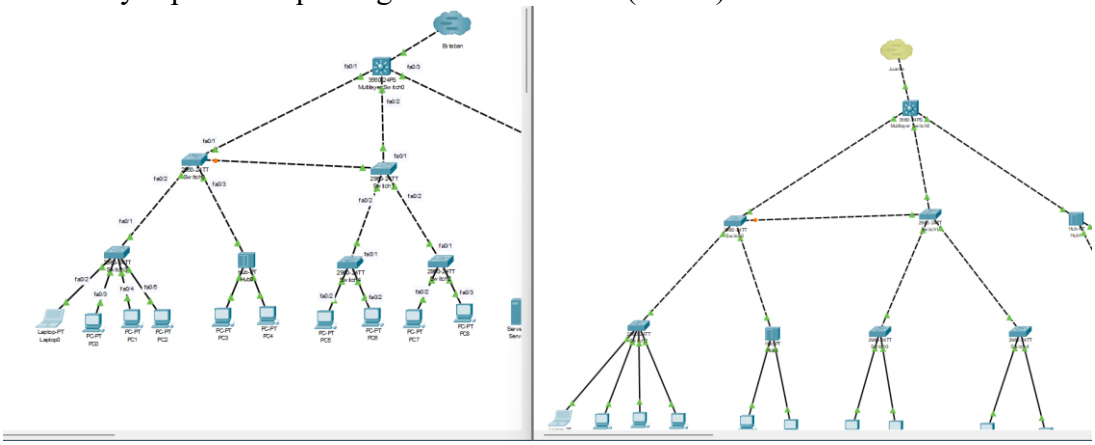


ii. Una vez agregados, en un archivo agregamos la contraseña y activamos las opciones always accept en ambos apartados mientras que en el otro

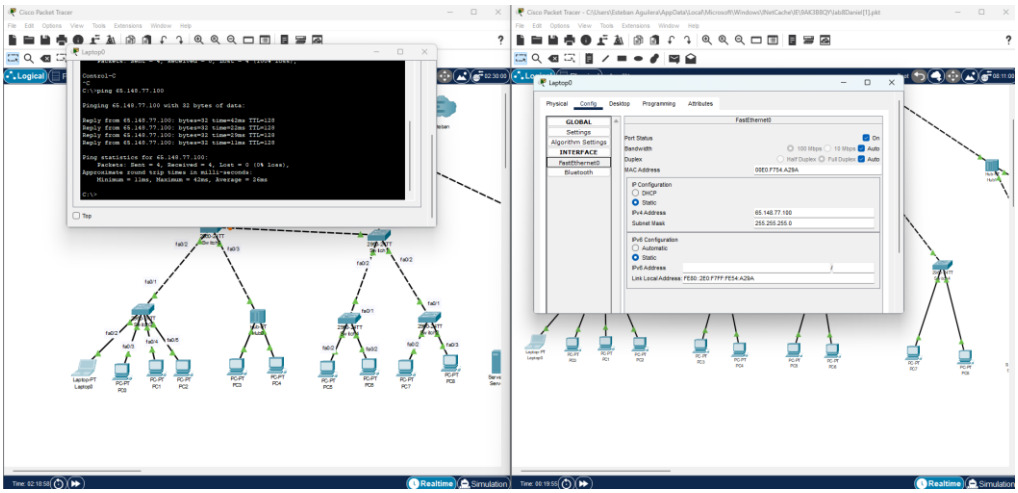
activamos la función incoming, colocamos el nombre de la multiuser del otro archivo con su numero de puerto y contraseñas asignadas



iii. Luego a esto generamos el link entre el multiplayer switch en ambos archivos y esperamos que se genere la conexión (verde)

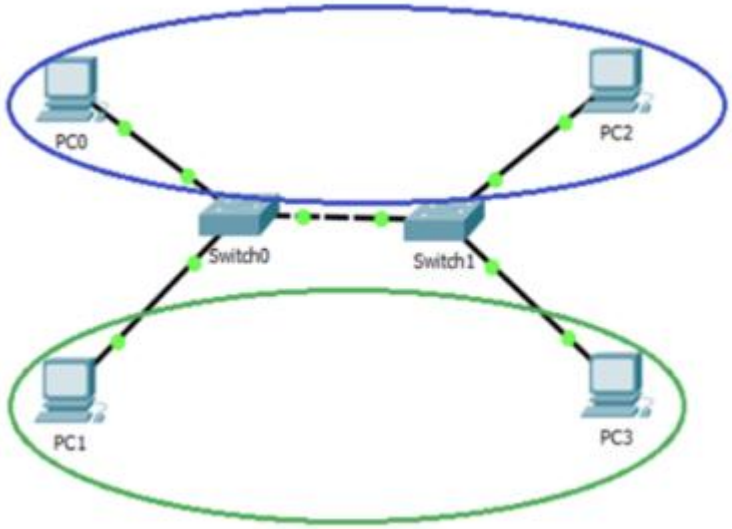


iv. Probamos un comando de ping desde el laptop 0 de un archivo hacia laptop 0 del otro para probar que la conexión sea correcta



3. VLAN Configuration

Using the configuration from points 1 and 2 as a base, in the small groups (disconnect the connections between the entire lab group and only keep the connections for the small groups), create two VLANs as shown in the diagram.



a. Enter configuration mode.
b. Configure two VLANs
    i. *systems → VLAN ID 50 (blue circular frame).*
    ii. *others → VLAN ID 55 (green circular frame).*
    iii. Creamos las vlan con los id y nombres asignados anteriormente

```
tebinJuanin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
tebinJuanin(config)#vlan 50
tebinJuanin(config-vlan)#name systems
tebinJuanin(config-vlan)#exit
tebinJuanin(config)#vlan 55
tebinJuanin(config-vlan)#name others
tebinJuanin(config-vlan)#exit
tebinJuanin(config)#
```

c. Assign computers PC1 and PC3 to the ”systems” VLAN. Assign computers PC2 and PC0 to the ”others” VLAN.
    i. Ingresamos a las interfaces de red configuradas anteriormente y agregamos las vlan correspondientes(Fa0/1 será la vlan 50 y fa0/2 sera la vlan 55) y Fa0/2 mediante los comandos :

```
tebinJuanin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
tebinJuanin(config)#interface fa0/1
tebinJuanin(config-if)#switchport mode access
tebinJuanin(config-if)#switchport access vlan 50
tebinJuanin(config-if)#exit
tebinJuanin(config)#interface fa0/2
tebinJuanin(config-if)#switchport mode access
tebinJuanin(config-if)#switchport access vlan 55
tebinJuanin(config-if)#exit
tebinJuanin(config)#exit
tebinJuanin#wi
*Mar  1 01:59:26.807: %SYS-5-CONFIG_I: Configured from console by cons
tebinJuanin#write memory
Building configuration...
[OK]
tebinJuanin#
```

Donde:

- configure terminal – Entra al modo de configuración global.
- interface fa0/1 – Entra a la interfaz FastEthernet 0/1.
- switchport mode access – Configura el puerto como acceso (para una sola VLAN).
- switchport access vlan 50 – Asigna la interfaz a la VLAN 50.
- exit – Sale de la configuración de la interfaz.
- interface fa0/2 – Entra a la interfaz FastEthernet 0/2.
- switchport mode access – Configura el puerto como acceso.
- switchport access vlan 55 – Asigna la interfaz a la VLAN 55.
- exit – Sale de la interfaz.
- write memory – Guarda la configuración para que se mantenga tras reiniciar el switch.

ii. Verificamos que las vlans estén asignadas a las interfaces correctas con el comando show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, 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
50   systems                           active    Fa0/1
55   others                            active    Fa0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
tebinJuanin#
```

d. Configure the link between the switches to allow VLAN connections. Hint: What are trunk links? What are they used for?

i. Para poder comunicarnos entre dispositivos que están en diferentes switches pero dentro de la misma VLAN, es necesario configurar una troncal.

ii. Una troncal es básicamente un enlace especial entre switches que permite que pasen varias VLAN por un solo cable. Configuramos esta troncal en la interfaz Gigabit (que es la que se conecta a otros switches) usando los siguientes comandos:

```
tebinJuanin(config)#interface GigabitEthernet0/2
tebinJuanin(config-if)#switchport mode trunk
tebinJuanin(config-if)#swit
*Mar  1 02:10:37.878: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEtherne
*Mar  1 02:10:37.878: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
tebinJuanin(config-if)#switchport t
*Mar  1 02:10:40.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEtherne
tebinJuanin(config-if)#switchport trunk allowed vlan 50,55
tebinJuanin(config-if)#exit
tebinJuanin(config)#exit
tebinJuanin#wirt
*Mar  1 02:11:08.866: %SYS-5-CONFIG_I: Configured from console by console
tebinJuanin#write memory
Building configuration...
[OK]
```

Donde:

- interface GigabitEthernet0/2 – Entra a la interfaz GigabitEthernet 0/2.
- switchport mode trunk – Cambia el modo de la interfaz a trunk (para permitir varias VLANs).
- exit – Sale de la interfaz.
- interface GigabitEthernet0/2 – Vuelve a entrar a la interfaz (para seguir configurando).
- switchport trunk allowed vlan 50,55 – Permite únicamente las VLANs 50 y 55 en el trunk.
- exit – Sale al modo privilegiado.
- write memory – Guarda la configuración activa para que persista tras reinicio.

iii. Verificamos que la troncal haya quedado configurada correctamente con el comando show nombre_interfaz switchport

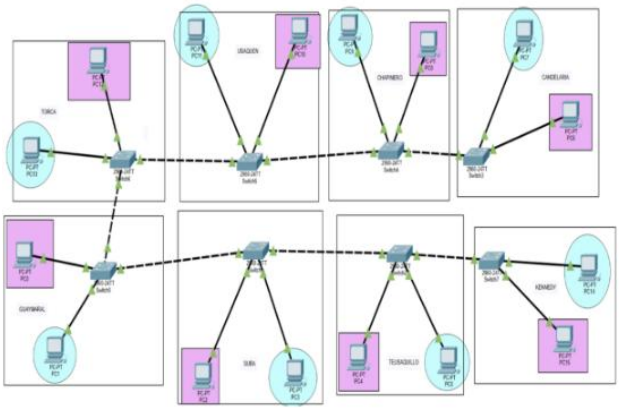
```
tebinJuanin#show interface GigabitEthernet0/2 switchport
Name: Gi0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 50,55
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
 --More--
```

e. Verify connectivity.

i. Realizamos pings desde la fa0/1 hacia las maquinas de nuestra mesa de trabajo. Un ping debe fallar ya que es la vlan 55 y el otro si debe funcionar ya que las maquinas están en la misma vlan que es la 50

```
C:\Users\Redes>ping 183.24.70.111

Pinging 183.24.70.111 with 32 bytes of data:
Reply from 183.24.70.111: bytes=32 time<1ms TTL=128
Reply from 183.24.70.111: bytes=32 time<1ms TTL=128

Ping statistics for 183.24.70.111:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Redes>ping 183.24.70.112

Pinging 183.24.70.112 with 32 bytes of data:
Control-C
^C
C:\Users\Redes>
```

f. Now, interconnect all setups from the entire group and verify their operation. It should look some- thing like this:



i. Luego del trabajo en equipo conectando los switches entre todos, realizamos varias pruebas de ping a varias redes para ver que todo este funcionando correctamente

1. 183.24.70.111 – 183.24.70.112

```
C:\Users\Redes>ping 183.24.70.111

Pinging 183.24.70.111 with 32 bytes of data:
Reply from 183.24.70.111: bytes=32 time<1ms TTL=128
Reply from 183.24.70.111: bytes=32 time<1ms TTL=128

Ping statistics for 183.24.70.111:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Redes>ping 183.24.70.112

Pinging 183.24.70.112 with 32 bytes of data:
Control-C
^C
C:\Users\Redes>
```

2. 183.24.30.101, 183.24.30.102

```
C:\Users\Redes>ping 183.24.30.101

Pinging 183.24.30.101 with 32 bytes of data:
Reply from 183.24.30.101: bytes=32 time<1ms TTL=128
Reply from 183.24.30.101: bytes=32 time<1ms TTL=128
Reply from 183.24.30.101: bytes=32 time<1ms TTL=128
Reply from 183.24.30.101: bytes=32 time<1ms TTL=128

Ping statistics for 183.24.30.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Redes>ping 183.24.30.102

Pinging 183.24.30.102 with 32 bytes of data:
Reply from 183.24.70.110: Destination host unreachable.
```

3. 183.24.30.103- 183.24.30.104

```
C:\Users\Redes>ping 183.24.30.103

Pinging 183.24.30.103 with 32 bytes of data:
Reply from 183.24.30.103: bytes=32 time=1ms TTL=128
Reply from 183.24.30.103: bytes=32 time<1ms TTL=128
Reply from 183.24.30.103: bytes=32 time=1ms TTL=128
Reply from 183.24.30.103: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.30.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Redes>ping 183.24.30.104

Pinging 183.24.30.104 with 32 bytes of data:
Reply from 183.24.70.110: Destination host unreachable.
```

4. 183.24.80.113-183.24.80.114

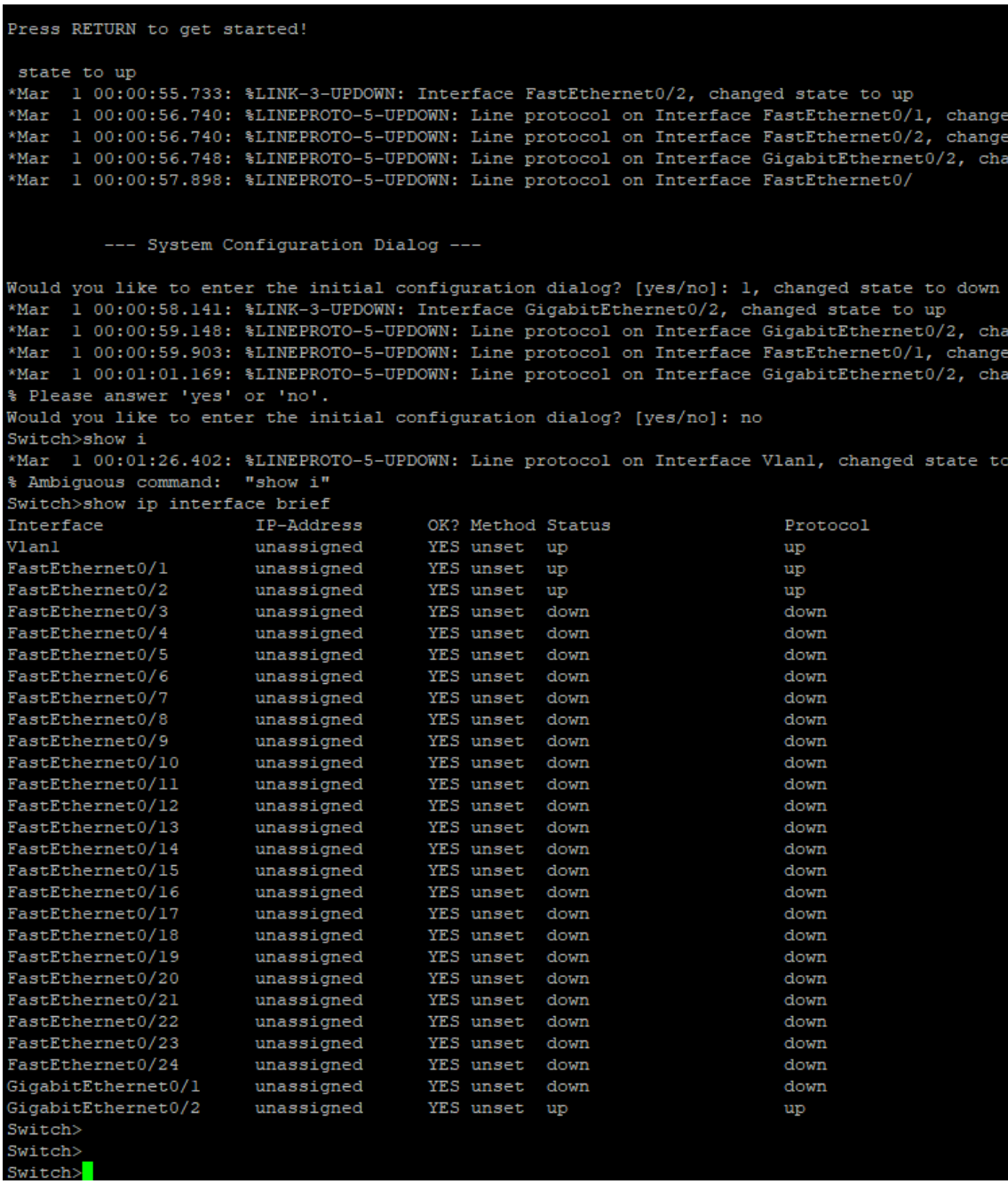
```
C:\Users\Redes>ping 183.24.90.113

Pinging 183.24.90.113 with 32 bytes of data:
Reply from 183.24.70.110: Destination host unreachable.

Ping statistics for 183.24.90.113:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Control-C
^C
C:\Users\Redes>ping 183.24.90.114

Pinging 183.24.90.114 with 32 bytes of data:
Reply from 183.24.90.114: bytes=32 time=445ms TTL=128
Reply from 183.24.90.114: bytes=32 time<1ms TTL=128
Reply from 183.24.90.114: bytes=32 time<1ms TTL=128
Reply from 183.24.90.114: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.90.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 445ms, Average = 111ms

C:\Users\Redes>
```

g. Disconnect the devices, leave the computers connected to the D ports of the structured cabling, and remove the configuration made on the switches.

i. Eliminamos la configuración de los switches con el comando erase startup-config y posteriormente reiniciamos con el comando reload

```
tebinJuanin#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confi
[OK]
Erase of nvram: complete
tebinJuanin#
*Mar  1 02:35:09.559: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
tebinJuanin#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

*Mar  1 02:35:20.112: %SYS-5-RELOAD: Reload requested by console. Reload Reason: R
```

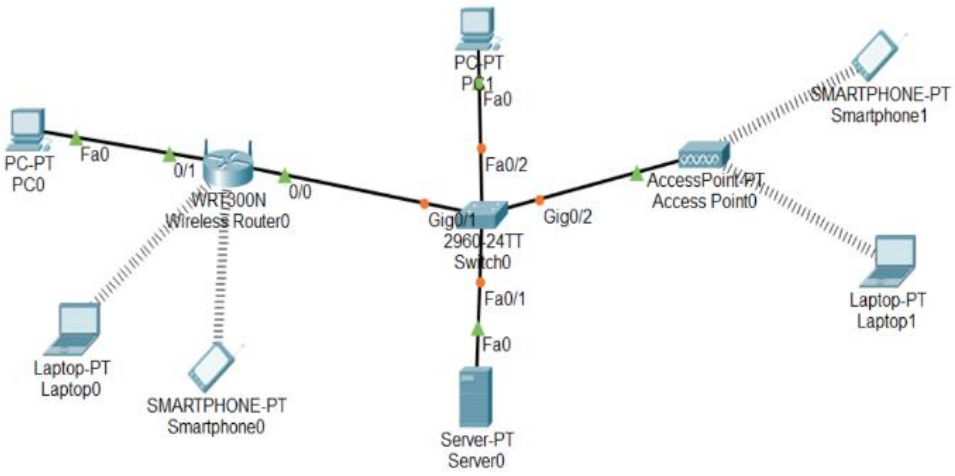
ii. Una vez reiniciada la consola y la configuración, verificamos nuevamente que todo este borrado con el comando show ip interface brief .



iii. Notamos que los protocolos están up por lo que desconectamos los cables del switch (consola, fast y gigabit Ethernet) así bajando los protocolos.

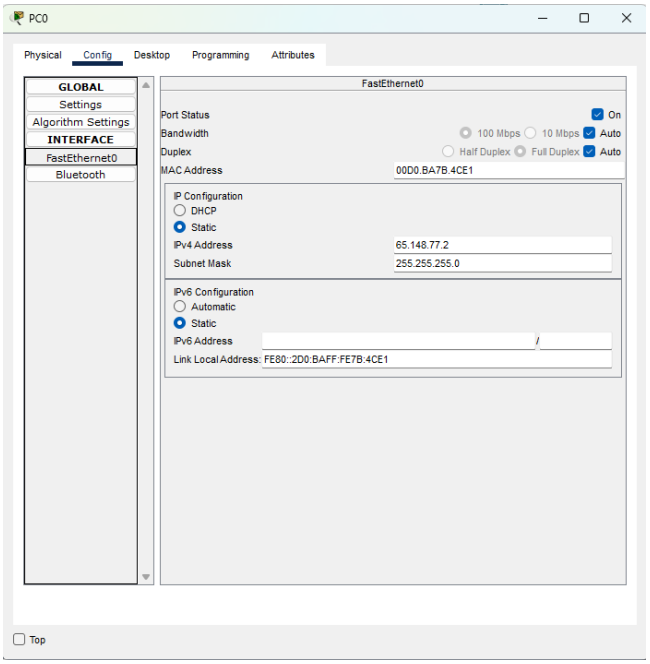
4. Basic WiFi Configuration

Perform the following setup in Cisco Packet Tracer. Each student must complete it individually.

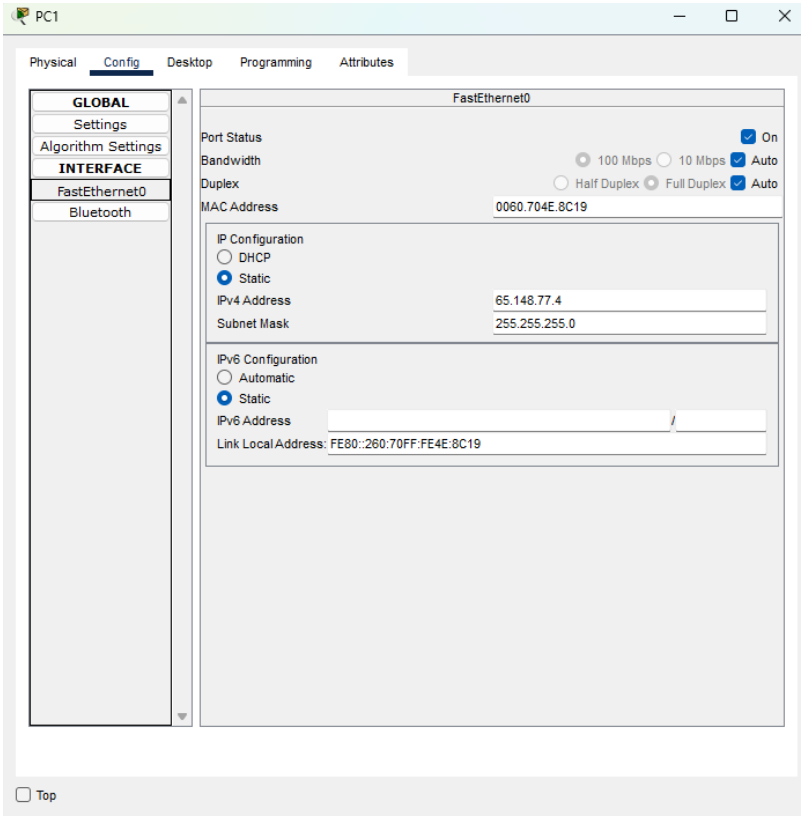


The wired LAN portion (Server0, PC1, and the router's Internet interfaces) belongs to the range 65.148.77.1 to 65.148.77.20 with a subnet mask of 255.255.255.0. This range will also include Smartphone1 and Lap-top1.

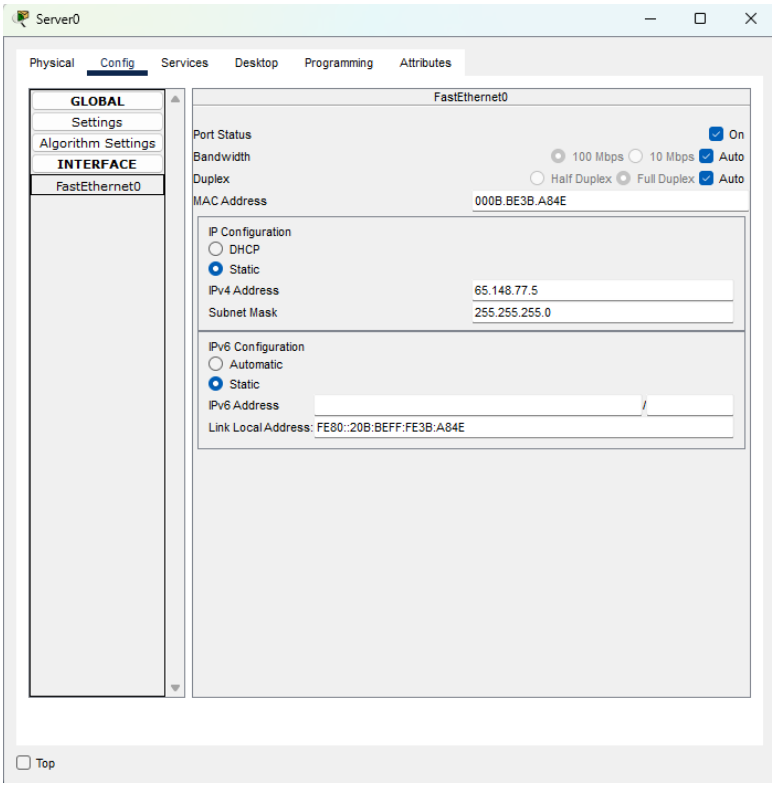
- En primera parte , agregamos las ips y mascaras de las maquinas pc0, server 0, pc1
- Pc0



- Pc1

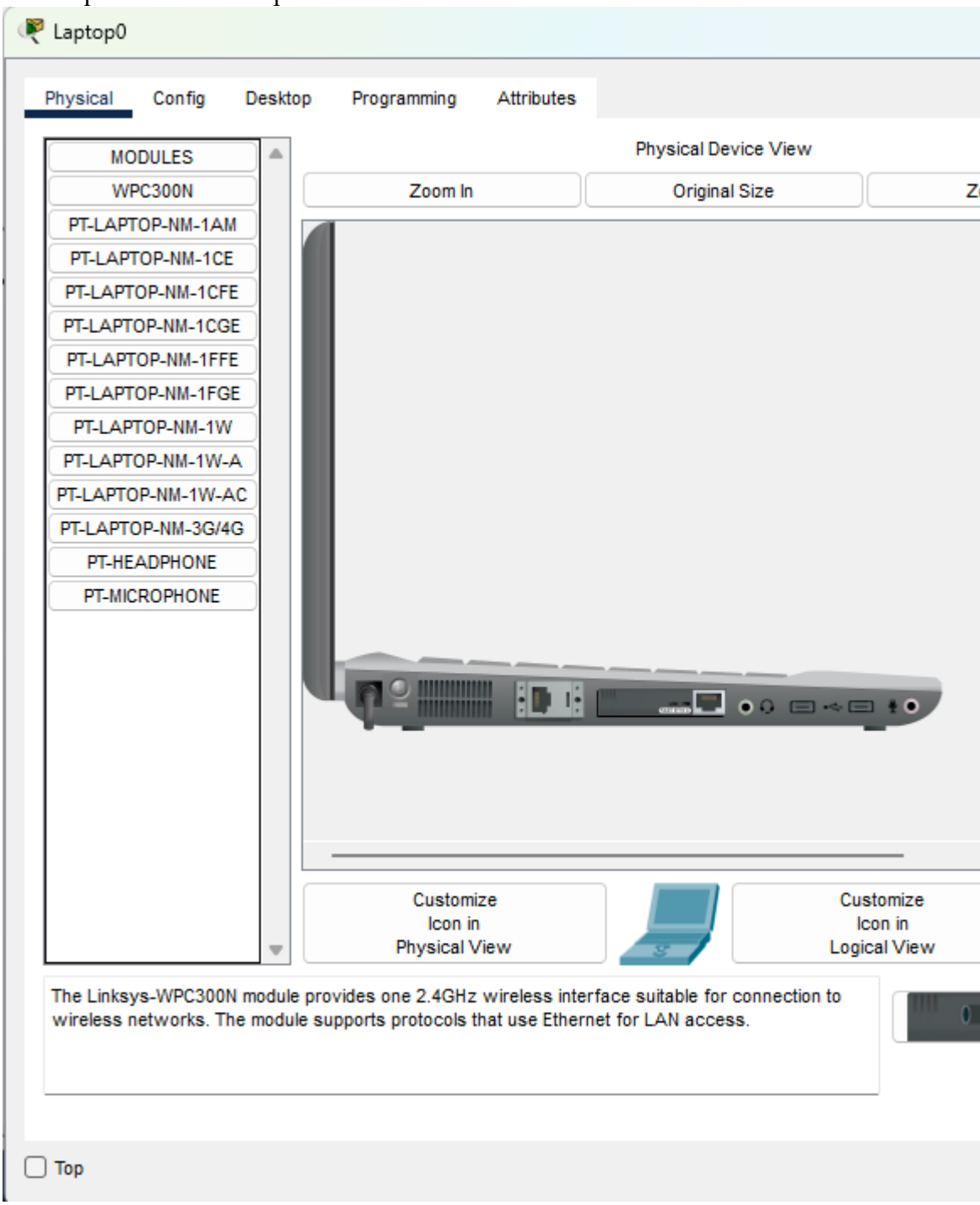

PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.704E.8C19
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.4
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::260:70FF:FE4E:8C19
Top

- Server 0

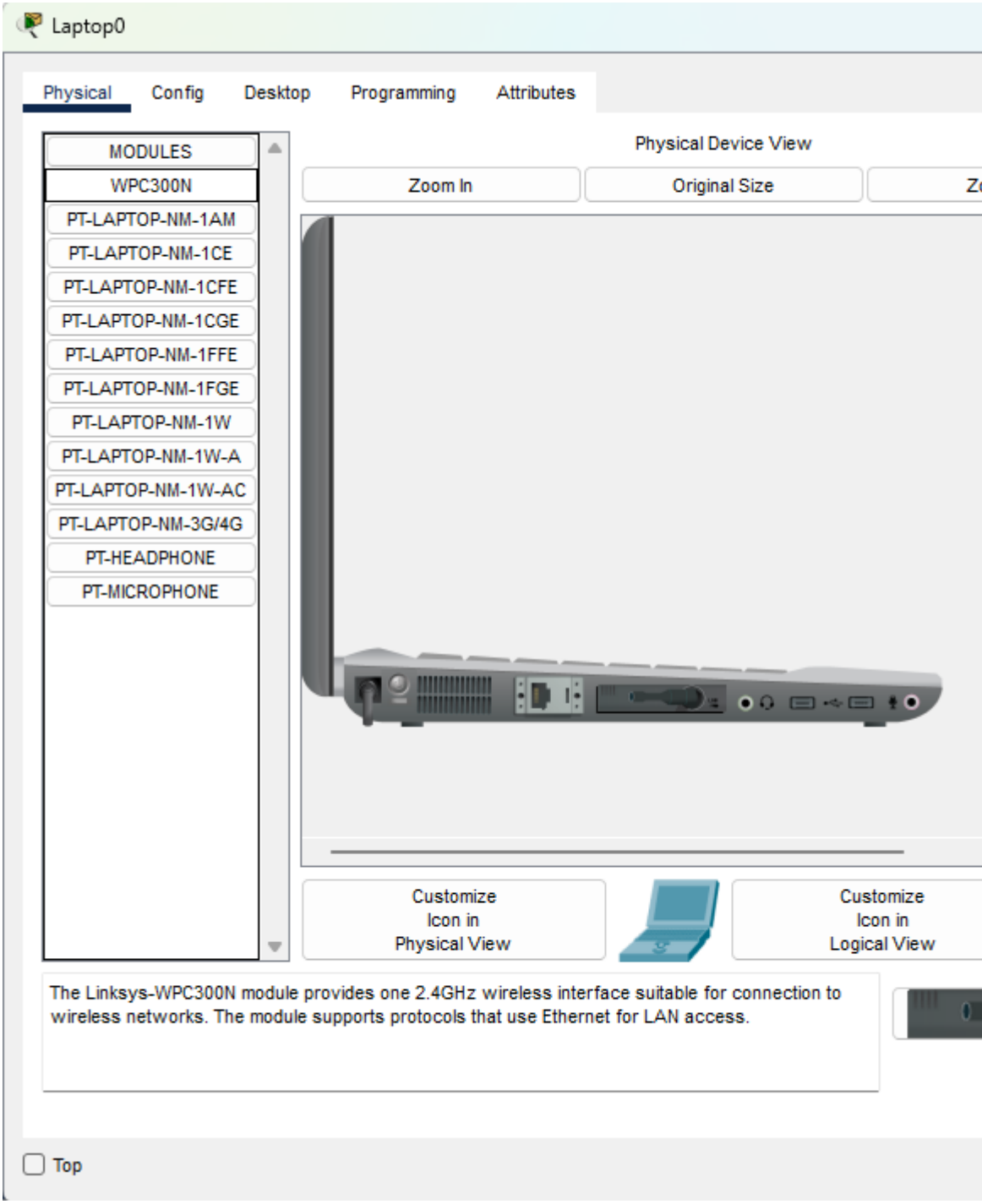

Server0
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000B.BE3B.A84E
IP Configuration
DHCP
Static
IPv4 Address
65.148.77.5
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::20B:BEFF:FE3B:A84E
Top

Use a laptop to configure the wireless router. Username and password: admin/admin. (The router is configured via a web interface. For more information, consult the router manual online.

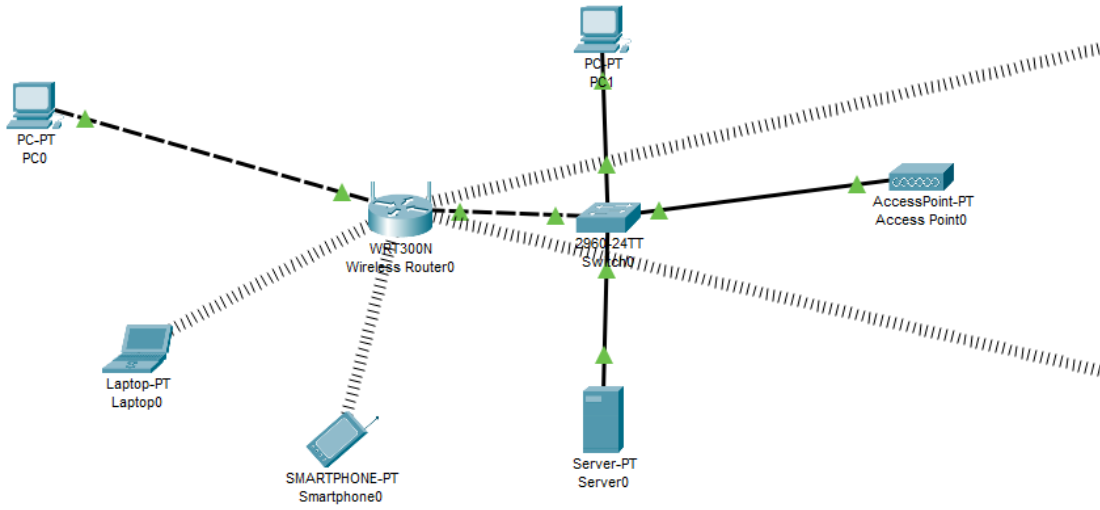
- Ahora , para configurar el router, apagamos el equipo y quitamos el modulo de red que esta instalada por defecto



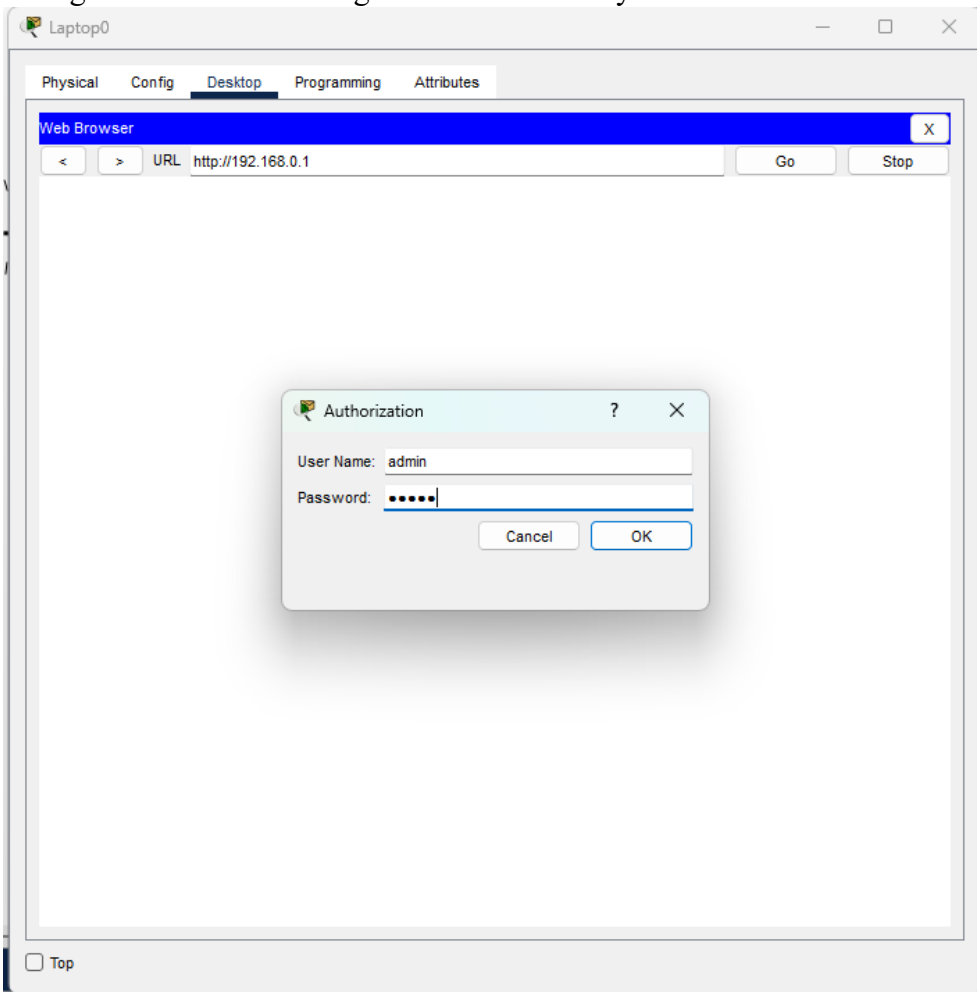
- Luego agregamos la interfaz Wpc300n y prendemos el equipo nuevamente



- Ahora nuestra laptop0 tiene conexión Wireless como se puede ver en la imagen con líneas continuas paralelas

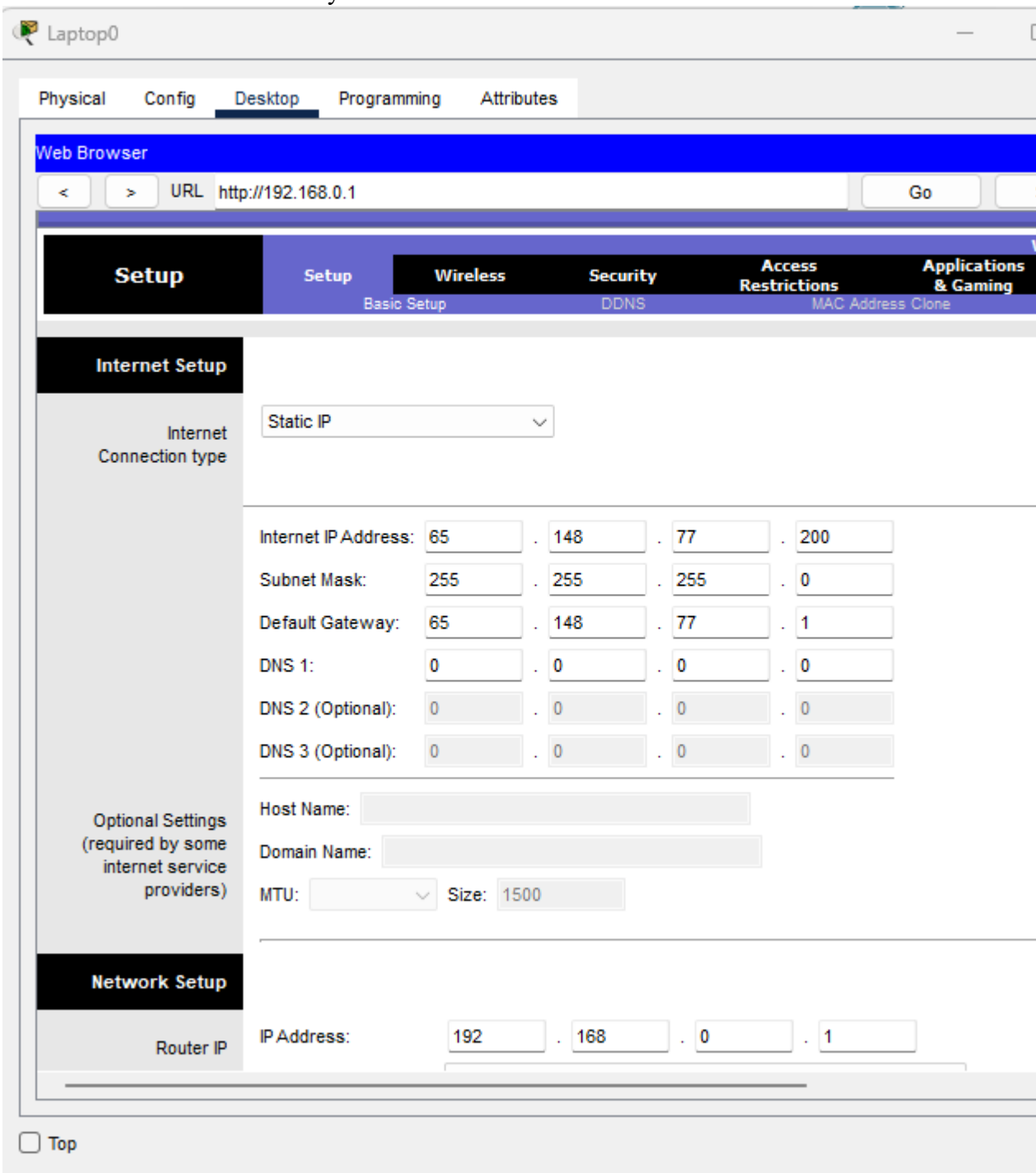


- Una vez con el modulo de conexión Wireless, en la laptop 0 iniciamos un navegador web y buscamos la dirección http://192.168.0.1 para abrir la configuración del router. Ingresamos el usuario y la contraseña admin



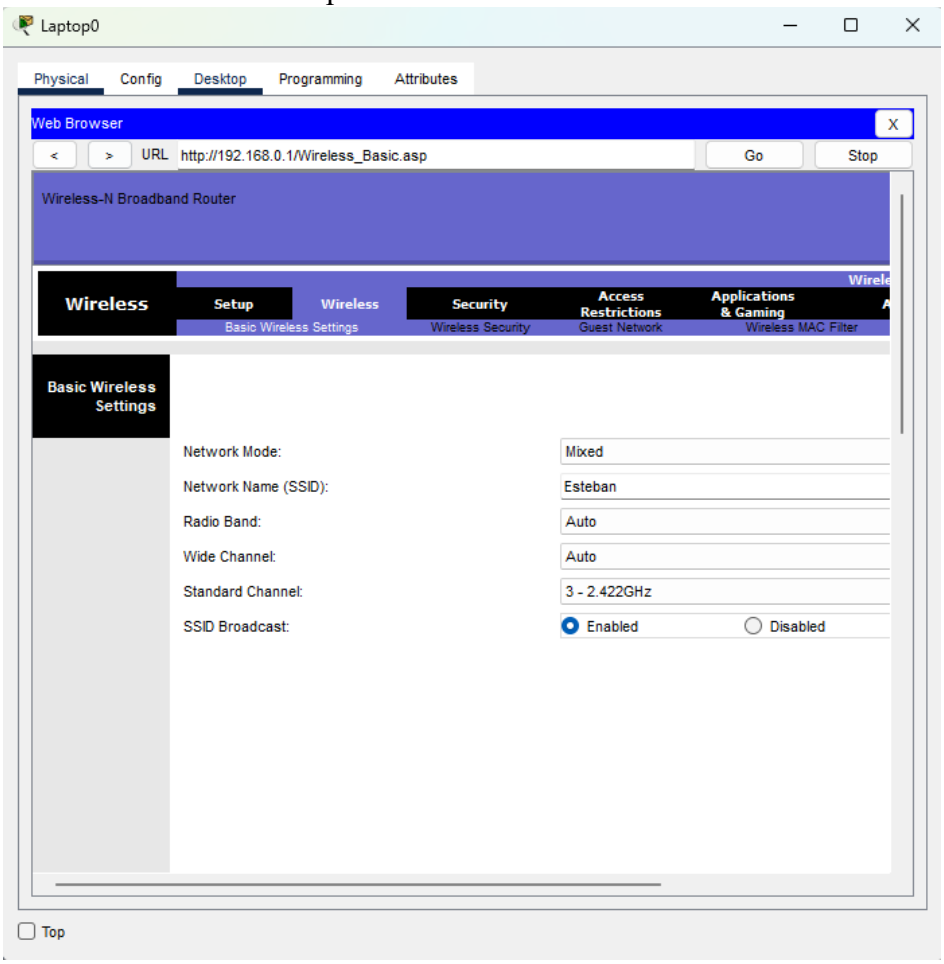
The IP address of the wireless router towards the wired LAN should be 65.148.77.200 with a subnet mask of 255.255.255.0.

- Una vez en la configuración del router. Agregamos:
  - Internet Ip Address : 65.148.77.200
  - Subnet mask : 255.255.255.0
  - Default Gateway: 65.148.77.1

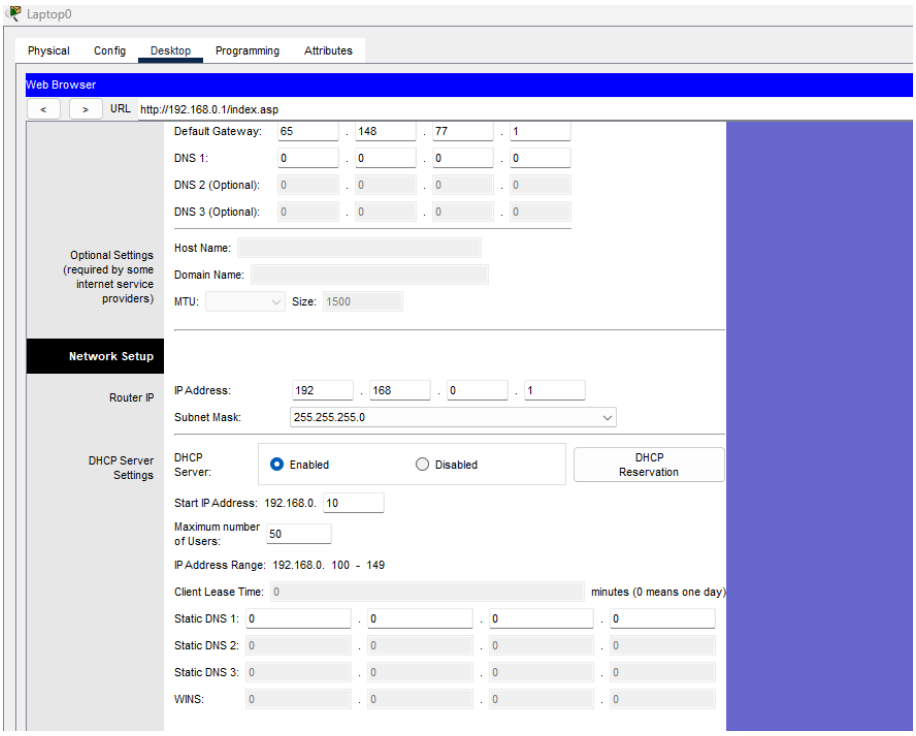


For the wireless network, use the following information

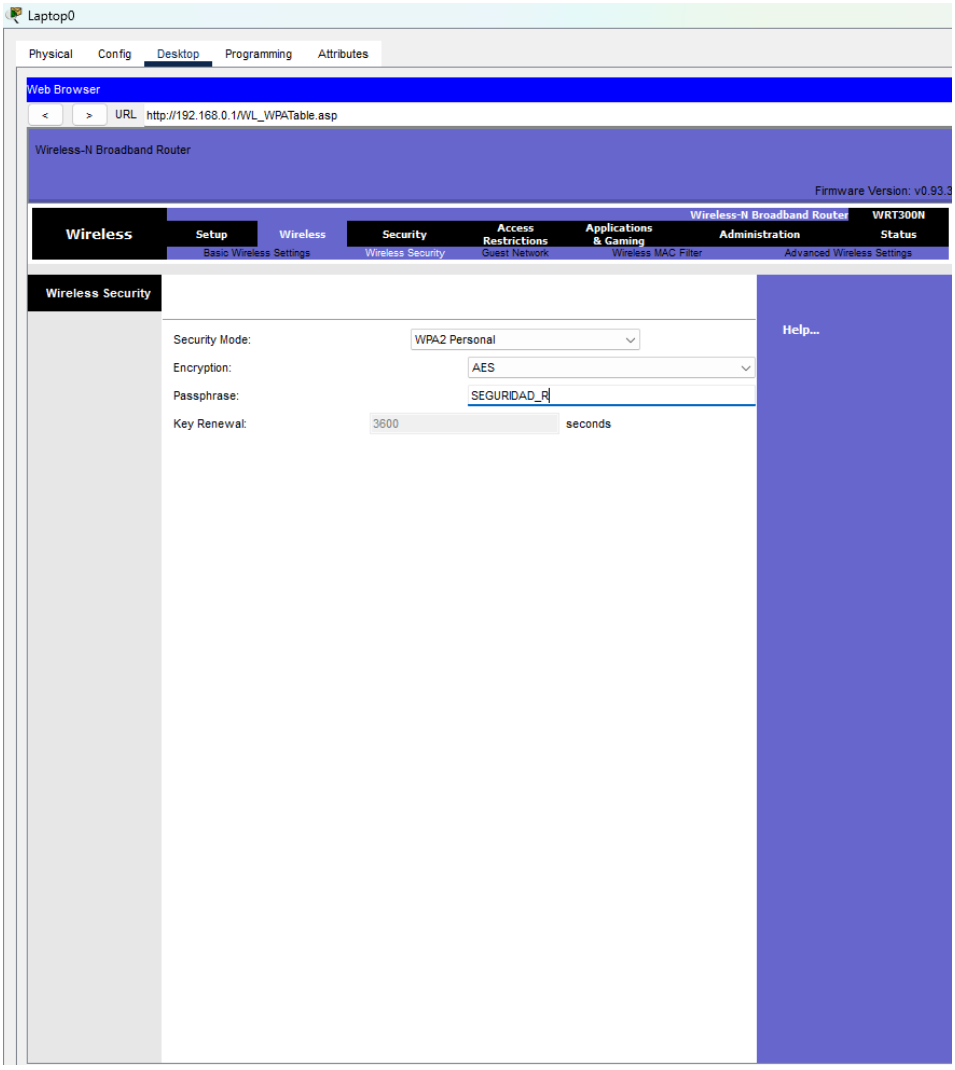
a. Wireless network identifier - SSID: student name
    i. Ahora agregamos el SSID por el cual el resto de maquinas van a reconocer el dispositivo. En este caso lo llamaremos Esteban



b. Wireless network IP: 192.168.0.0/24
c. Wireless router IP address (wireless interface): 192.168.0.1
d. IP address range for mobile devices (DHCP): 192.168.0.X to 192.168.0.Y, where X and Y correspond to an IP range:
    i. Student 1: 10 to 50
    ii. Student 2: 60 to 100
    iii. Student 3: 110 to 150



e. Access mechanism for wireless clients: WPA2-PSK with AES
f. Router access password for mobile devices: SECURITY R
    i. Para este caso vamos a usar el Student 1 por lo que ingresamos en start ip address 10 y en maximun number of user 50 asi estableciendo el rango de las ips. (Juan usara el Studen2 en su respectivo archivo de packet tracer)



ii. Luego de esto guardamos cambios y cerramos el navegador web.

g. Configure a specific channel. What channel options can be configured on each wireless router?

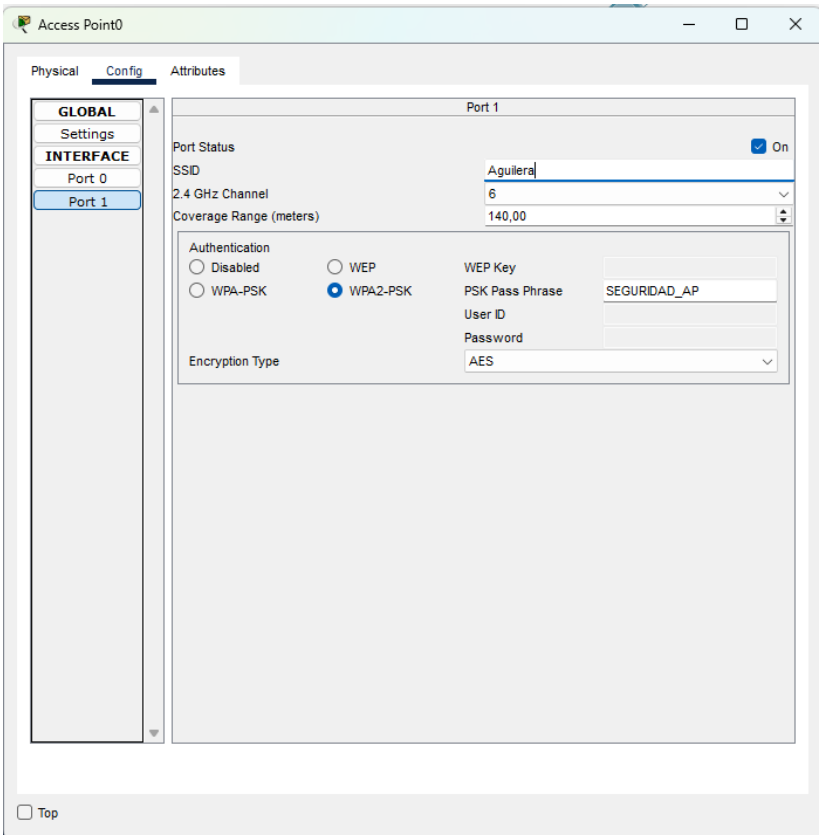
i. En los routers inalámbricos se pueden configurar los siguientes canales, dependiendo de la banda:

1. Banda de 2.4 GHz: Canales del 1 al 11 (en este lab se uso el 3 anteriormente.
2. Banda de 5 GHz: Canales como 36, 40, 44, 48, 149, 153, 157, 161, 165 (según país y modelo).
3. Banda de 6 GHz (Wi-Fi 6E): Canales entre el 1 y el 233 (solo en routers compatibles).

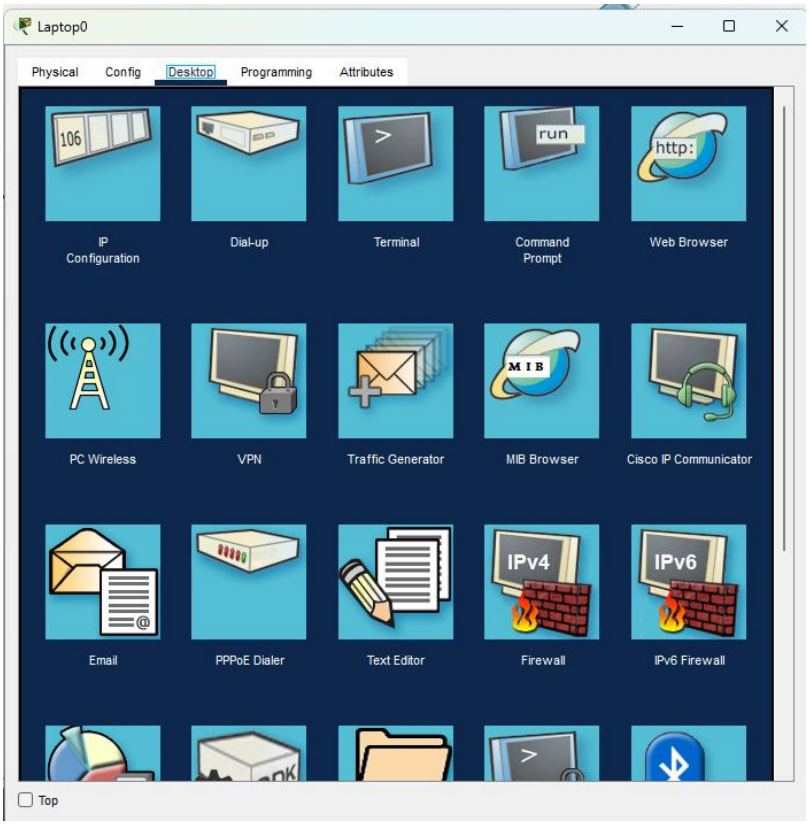
ii. Estos canales se eligen para evitar interferencias con otras redes y mejorar el rendimiento del Wi-Fi.

For the Access Point, review the available configurations. The SSID will be Lastname Student, and the password will be SECURITY AP.

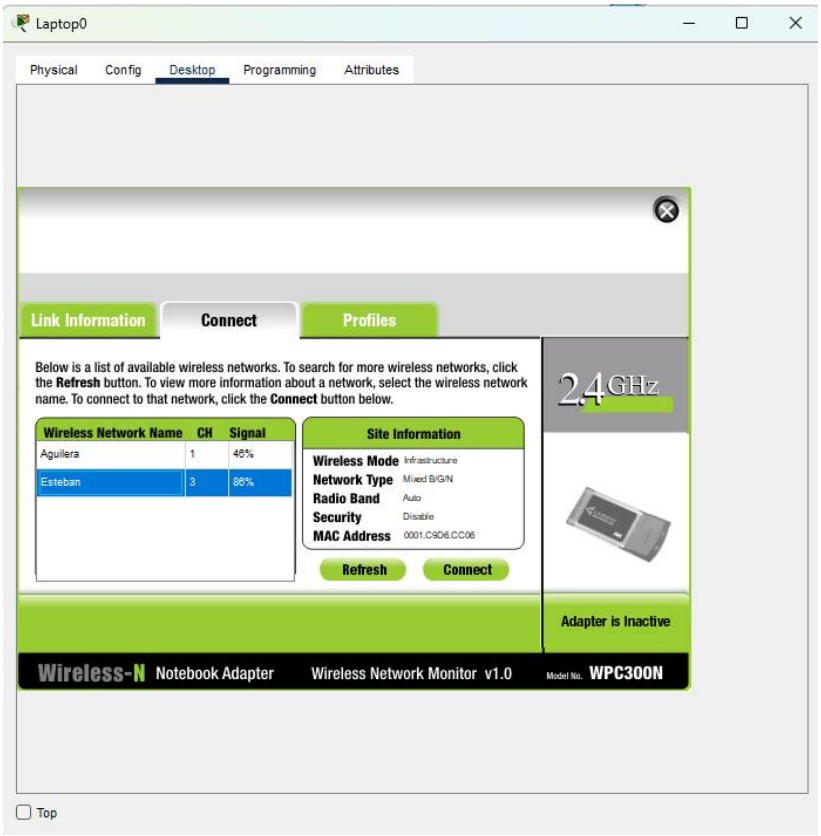
- Ahora configuramos el access point agregando el SSID, y el tipo de autenticación el cual será WAP2-PSK con contraseña SEGURIDAD_AP



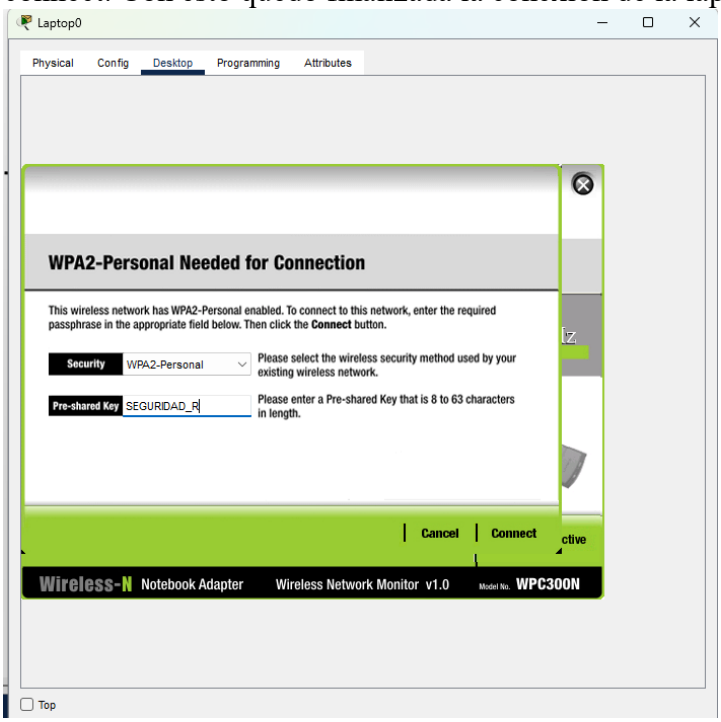
h. Configure the devices to connect to the wireless router and the AP as shown in the diagram.
i. For wireless devices connected to the AP, assign IP addresses in the range 65.148.77.100 to 65.148.77.120 with a subnet mask of 255.255.255.0.
    i. Ya configurado el router y el Access point ahora solo queda permitir la conexión en las maquinas
    ii. Ingresamos en el PC0 en el apartado wireless



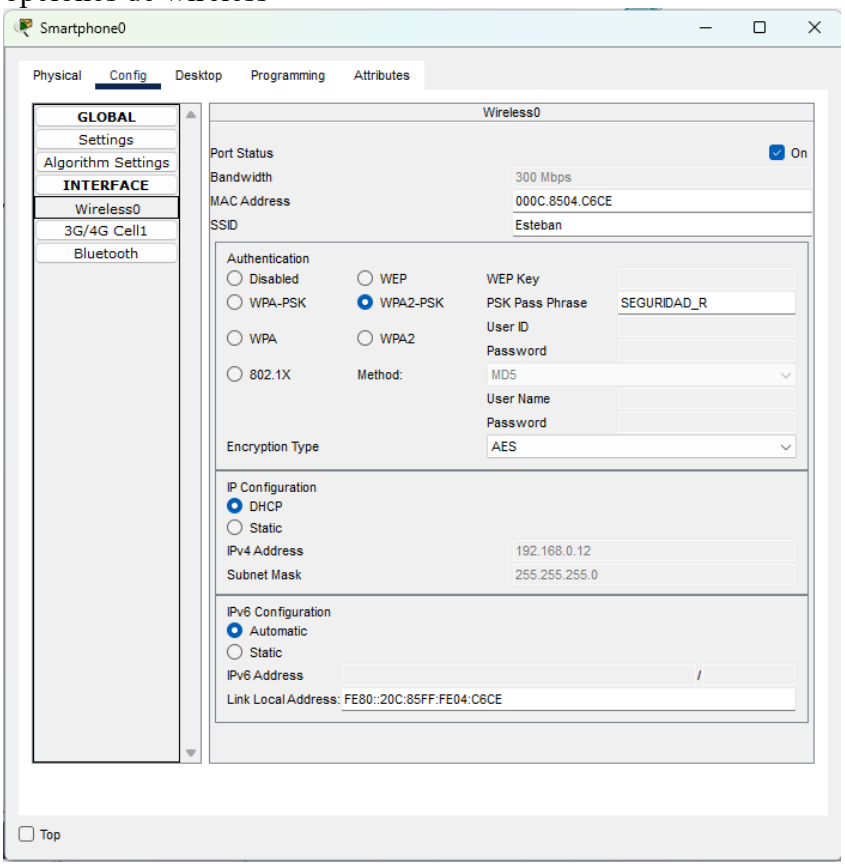
iii. Seleccionamos Esteban el cual es el SSID del router configurado anteriormente . Presionamos connect



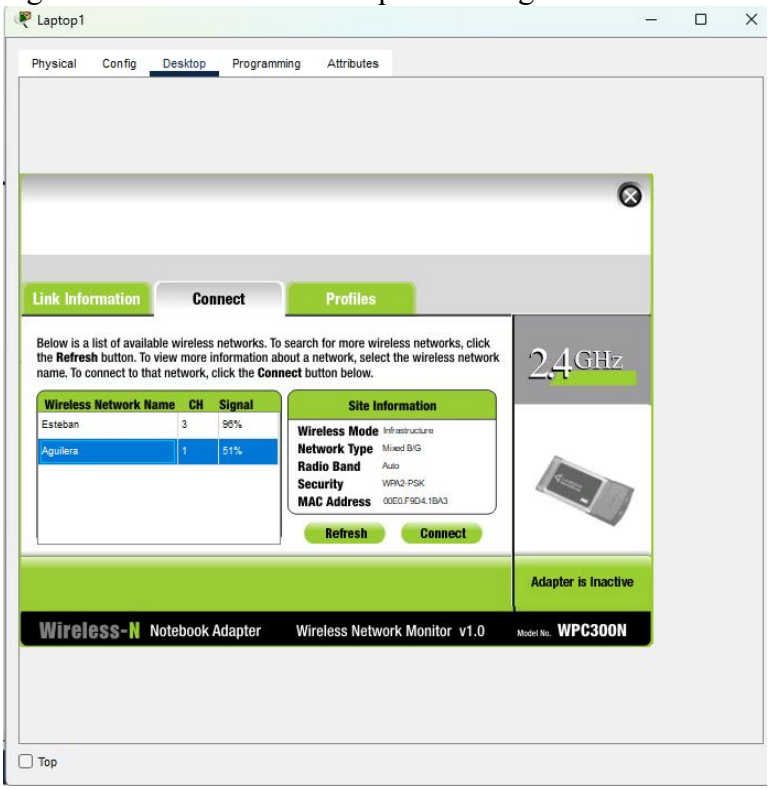
iv. Digitamos la contraseña configurada anteriormente y presionamos connect. Con esto quedo finalizada la conexión de la laptop 1



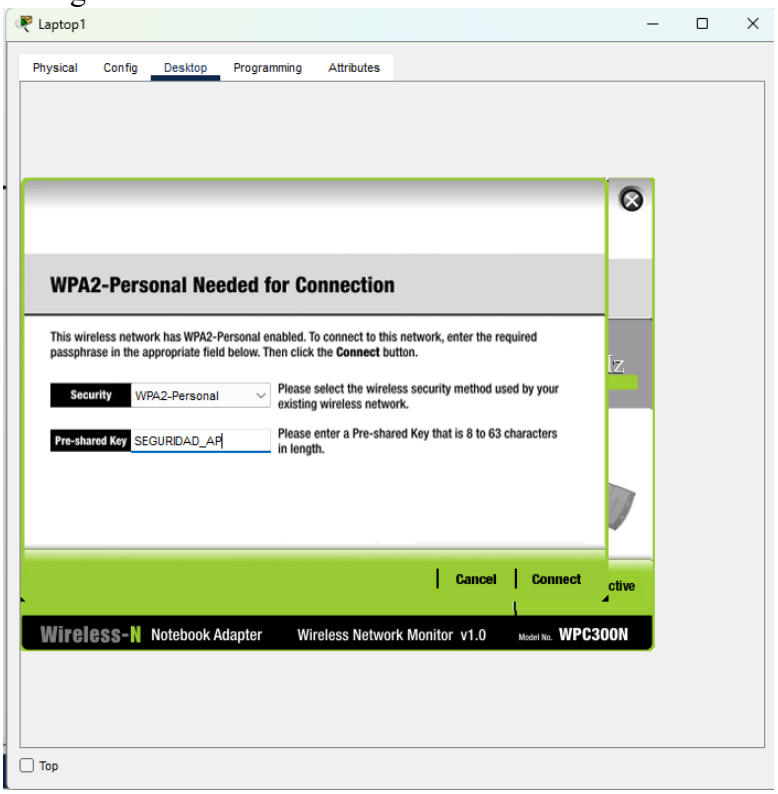
v. Ahora , agregamos la contraseña y el SSID del smarthpone en las opciones de wireless



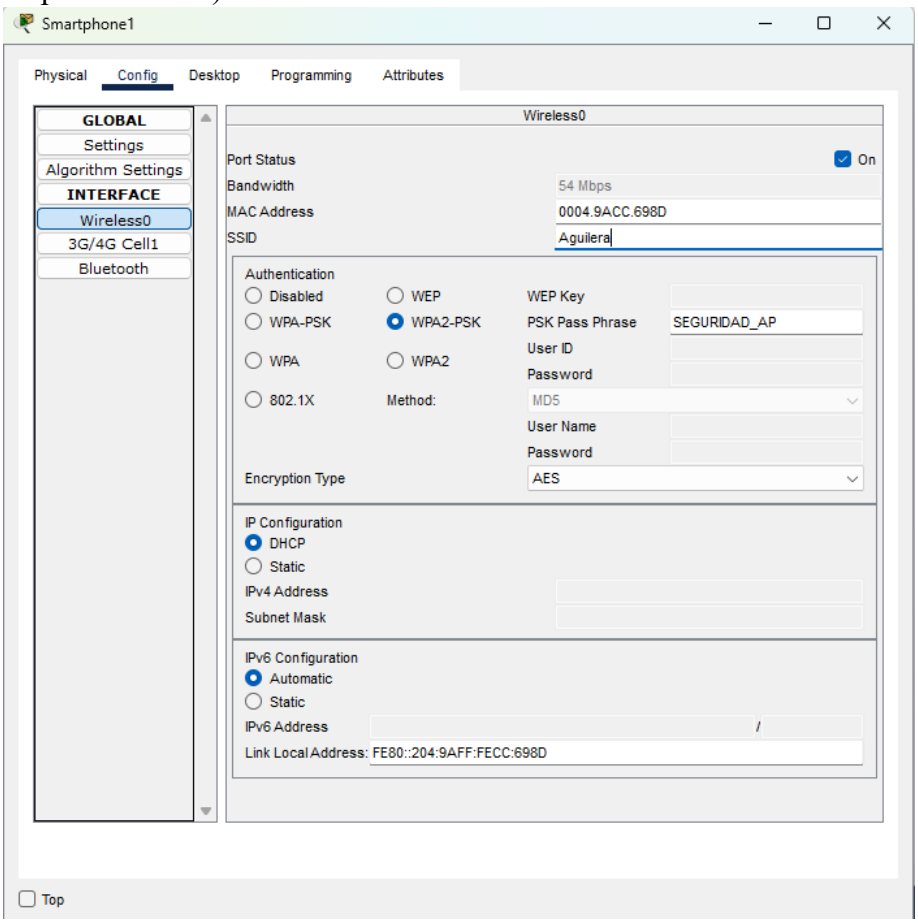
vi. Repetimos el mismo proceso para la laptop 1 pero ahora seleccionamos Aguilera el cual es el Access point configurado anteriormente



vii. Nos conectamos con la contraseña SEGURIDAD_AP la cual fue configurada anteriormente

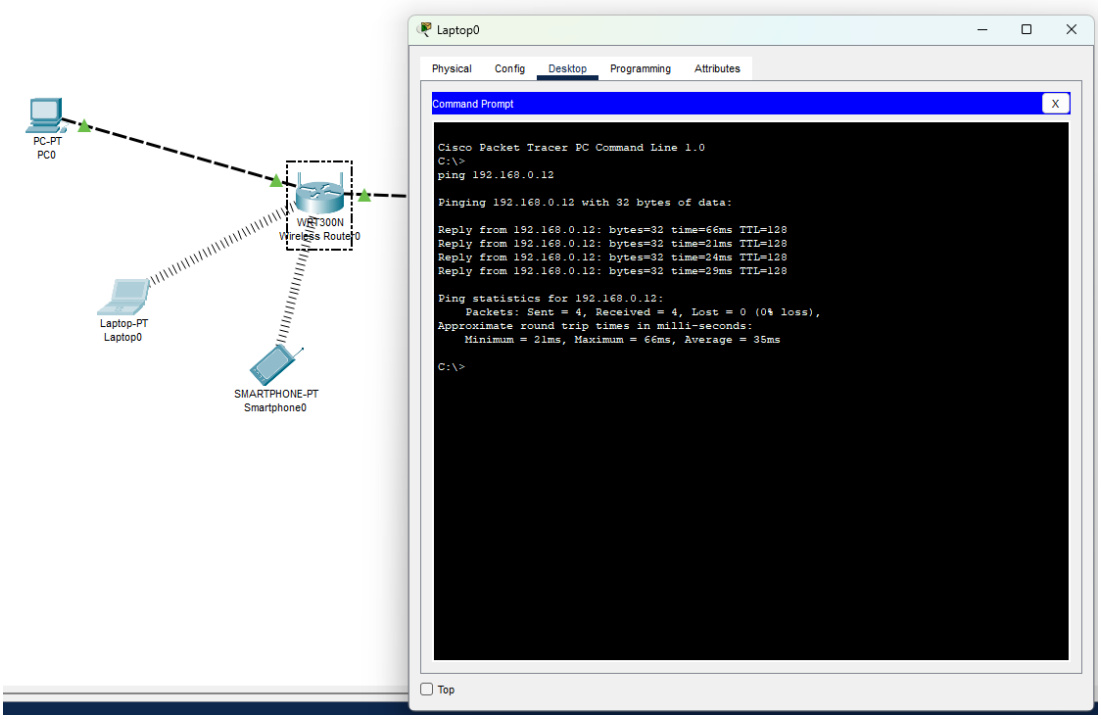


viii. Ahora repetimos el mismo proceso del smartphone1 pero ahora el SSID y la contraseña son del Access point (Aguilera y SEGURIDAD_AP respectivamente)

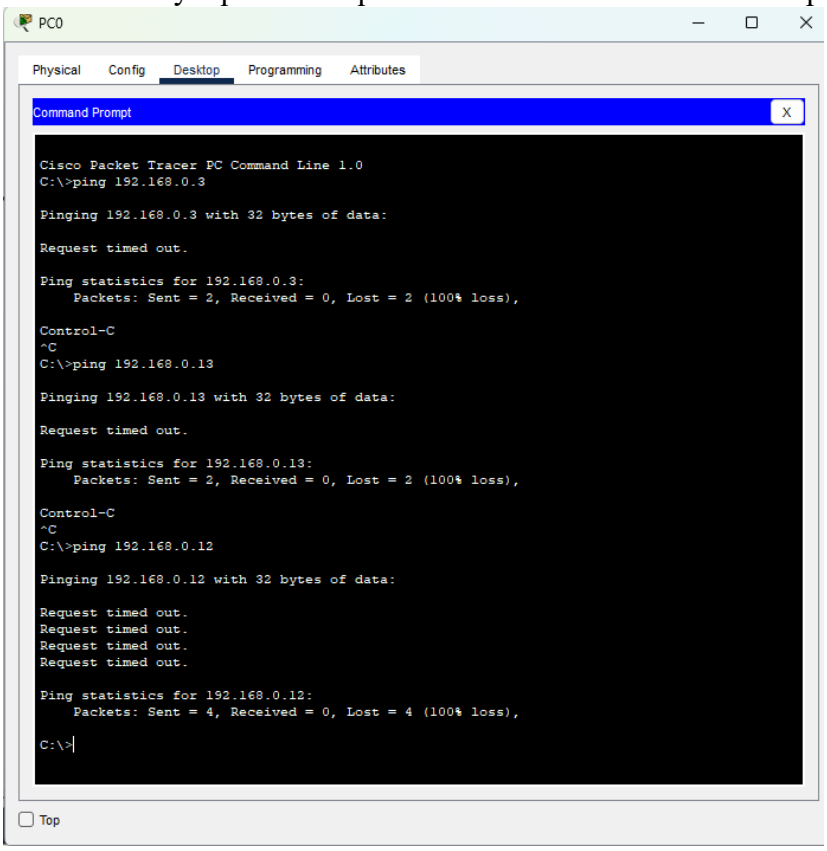


j. Verify connectivity between the devices. Which devices can ping each other, and why?

i. Verificamos la conexión realizando ping entre dos máquinas con ip estáticas

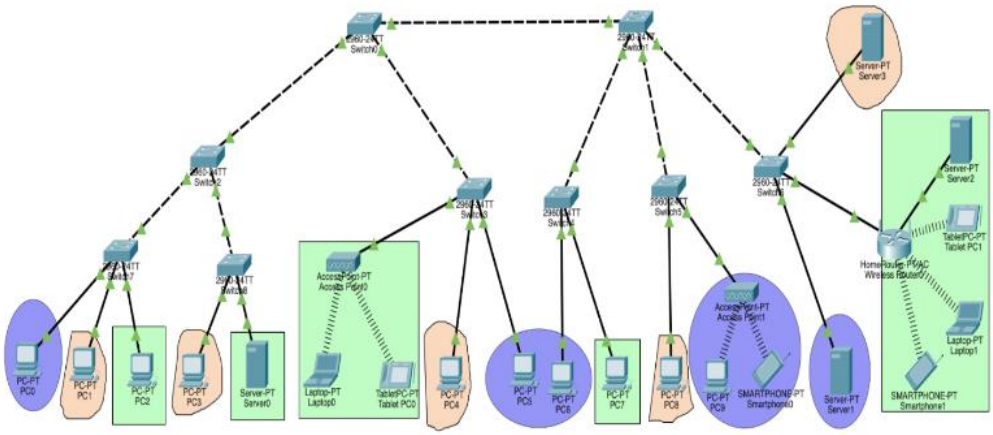


ii. Al momento de realizar un ping hacia una maquina con Wireless genera un timed out ya que las maquinas Wireless tienen direcciones ip privadas.

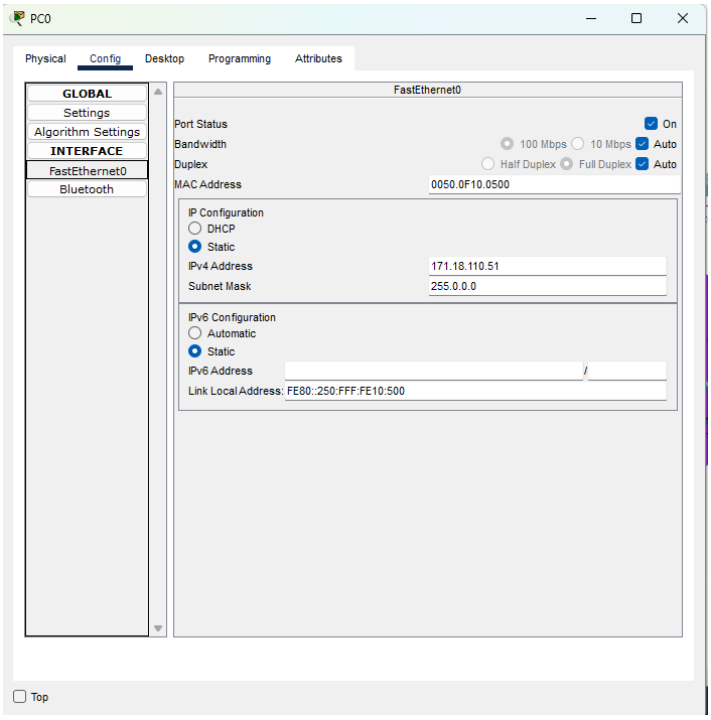


5. Configuration of Wired and Wireless LAN

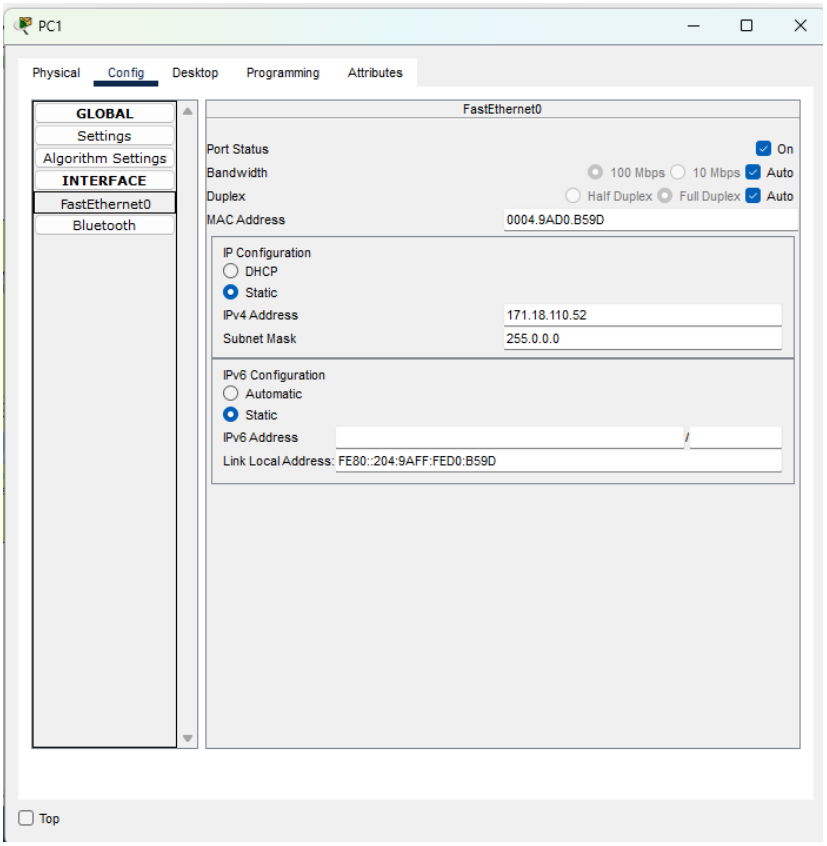
Create a setup in Packet Tracer as shown in the diagram (include the frames and colors presented in the diagram). Initially, VLANs are not configured. Each student must complete the setup individually



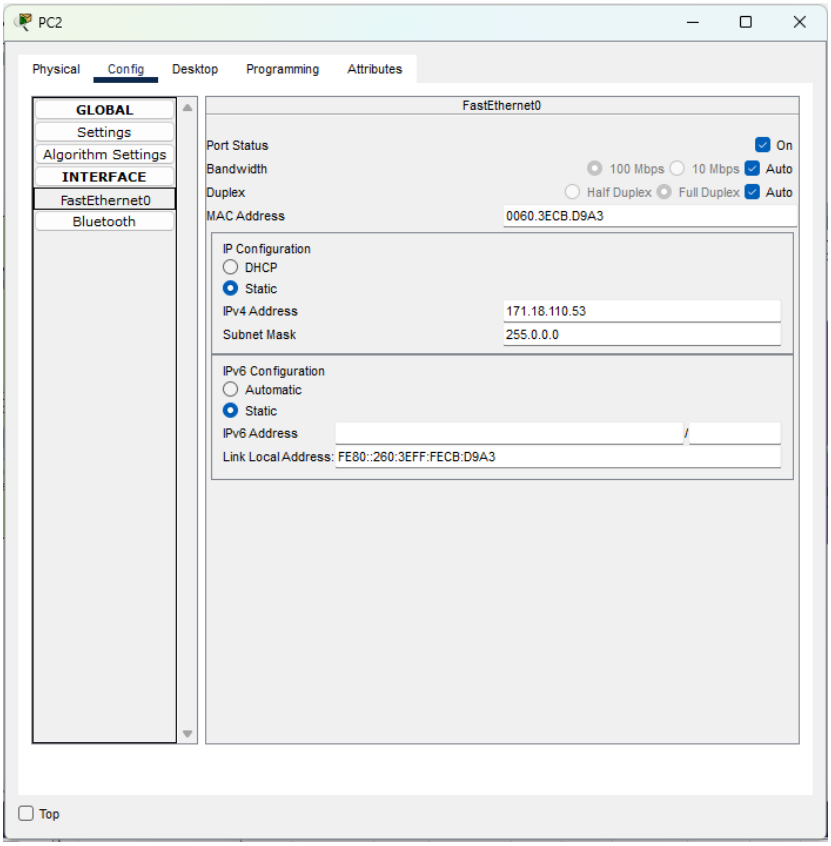
a. Configure all wired devices with the following IP addresses:
   i. *Student 1: 171.18.100.50 to 171.18.100.80. Subnet mask 255.0.0.0*
   ii. *Student 2: 171.18.110.50 to 171.18.110.80. Subnet mask 255.0.0.0*
   iii. *Student 3: 171.18.120.50 to 171.18.120.80. Subnet mask 255.0.0.0*
   iv. Agregamos las ip de las maquinas desde la 50 , 51, 52 y así sucesivamente hasta configurar todos los equipos
   v. PC0



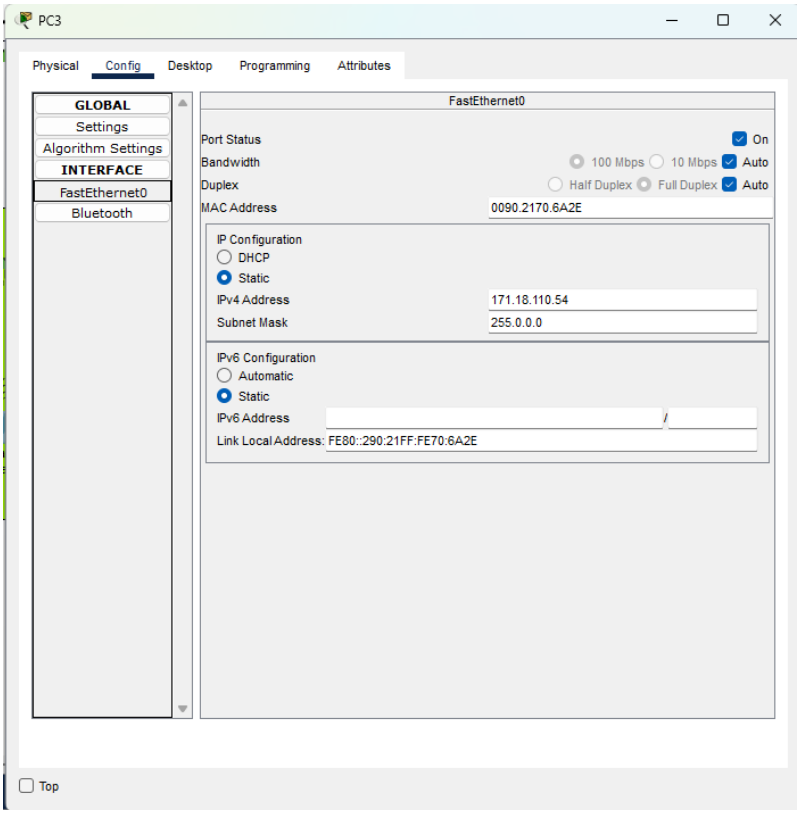
   vi. PC1


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0004.9AD0.B59D
IP Configuration
DHCP
Static
IPv4 Address
171.18.110.52
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::204:9AFF:FED0:B59D
Top

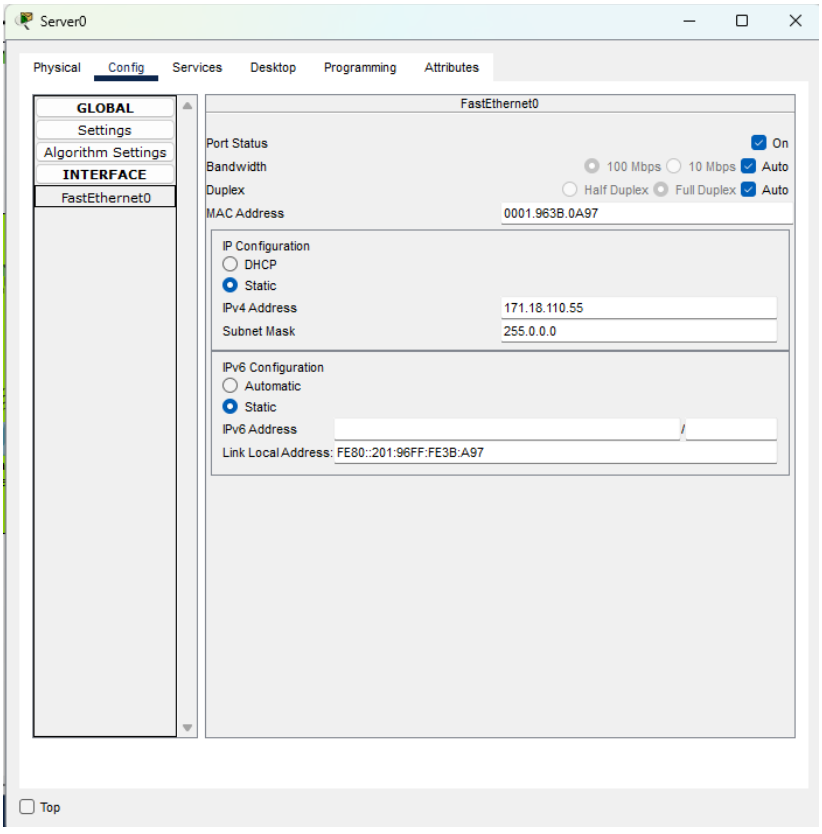
vii. PC2


PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.3ECB.D9A3
IP Configuration
DHCP
Static
IPv4 Address
171.18.110.53
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::260:3EFF:FECB:D9A3
Top

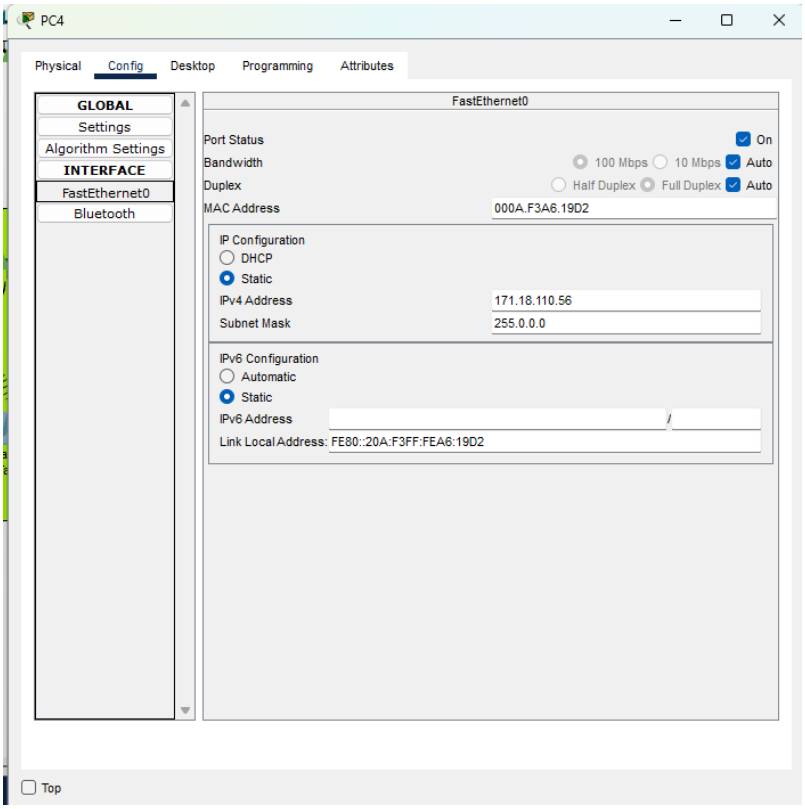
viii. PC3



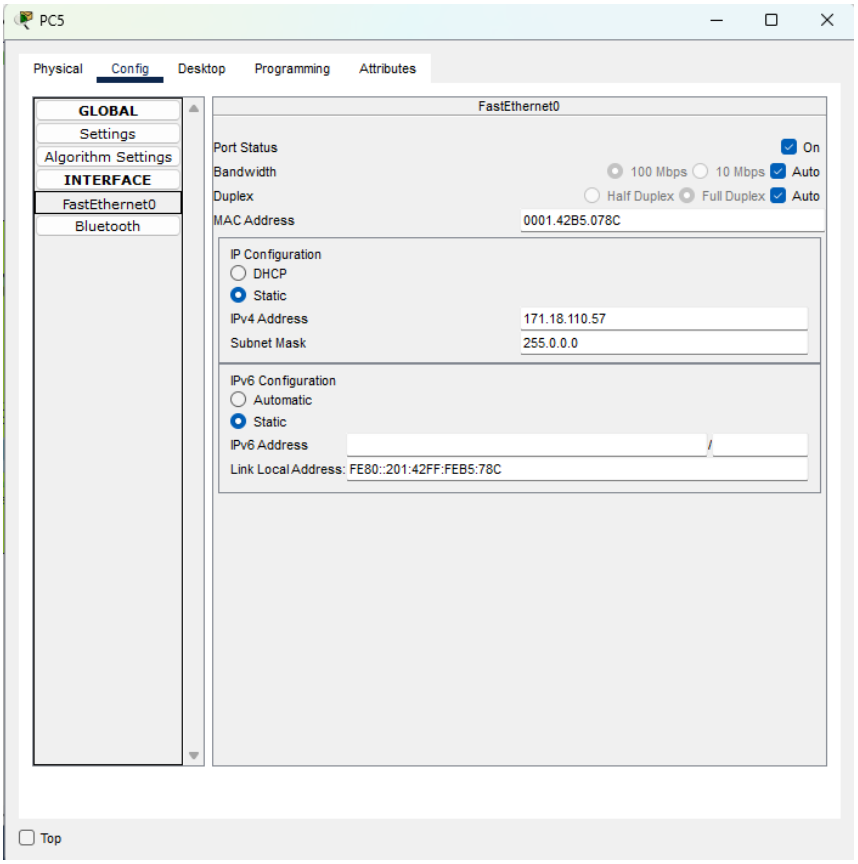
ix. Server0



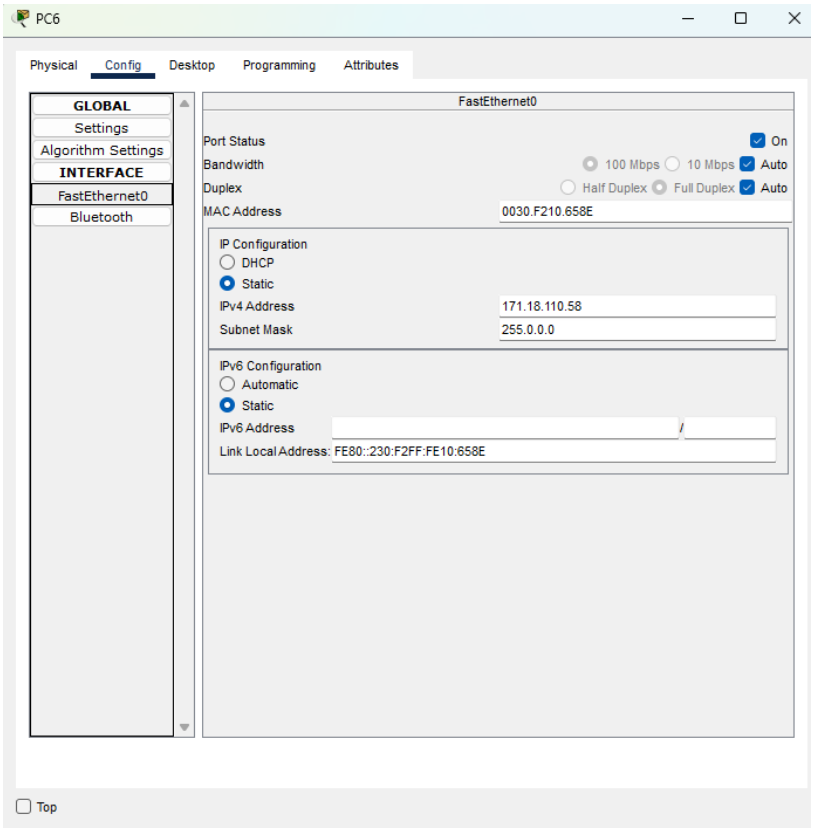
x. Pc4


PC4
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000A.F3A6.19D2
IP Configuration
DHCP
Static
IPv4 Address
171.18.110.56
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20A:F3FF:FEA6:19D2
Top

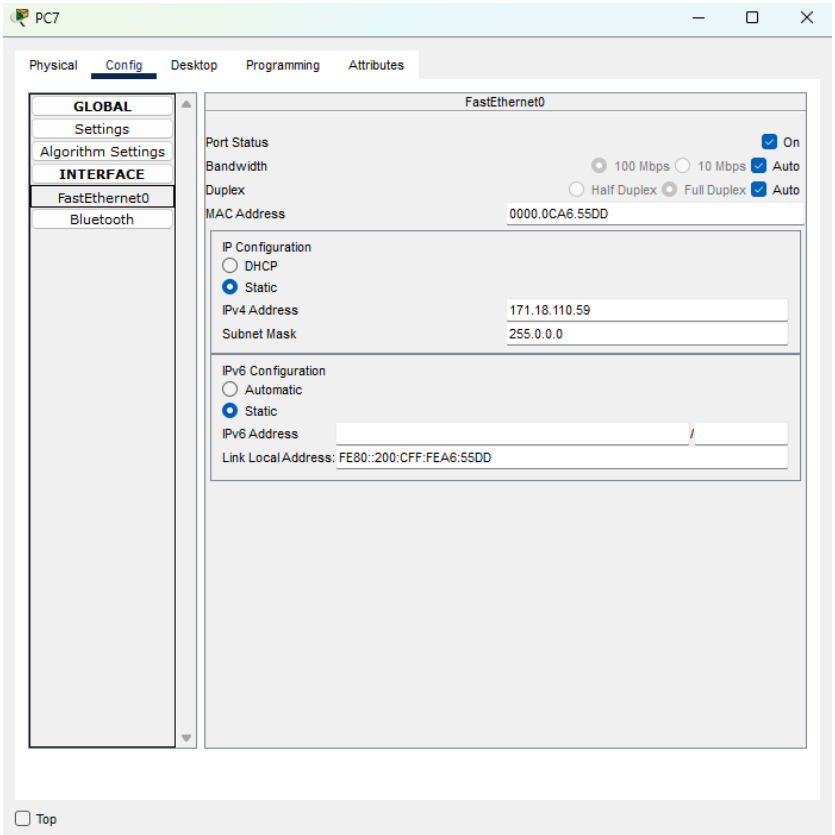
xi. Pc5


PC5
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.42B5.078C
IP Configuration
DHCP
Static
IPv4 Address
171.18.110.57
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:42FF:FEB5:78C
Top

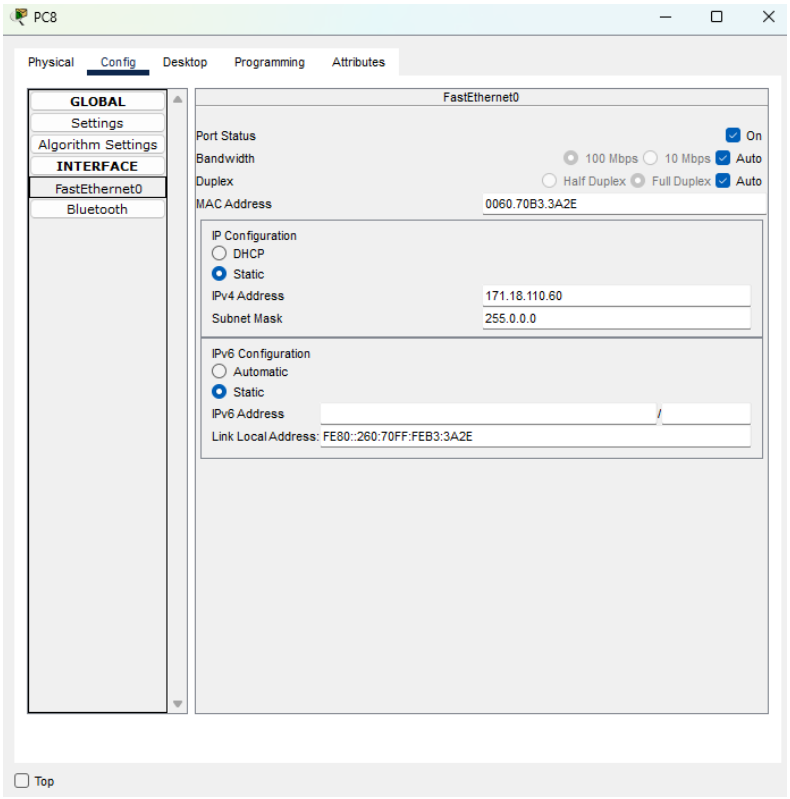
xii. Pc6



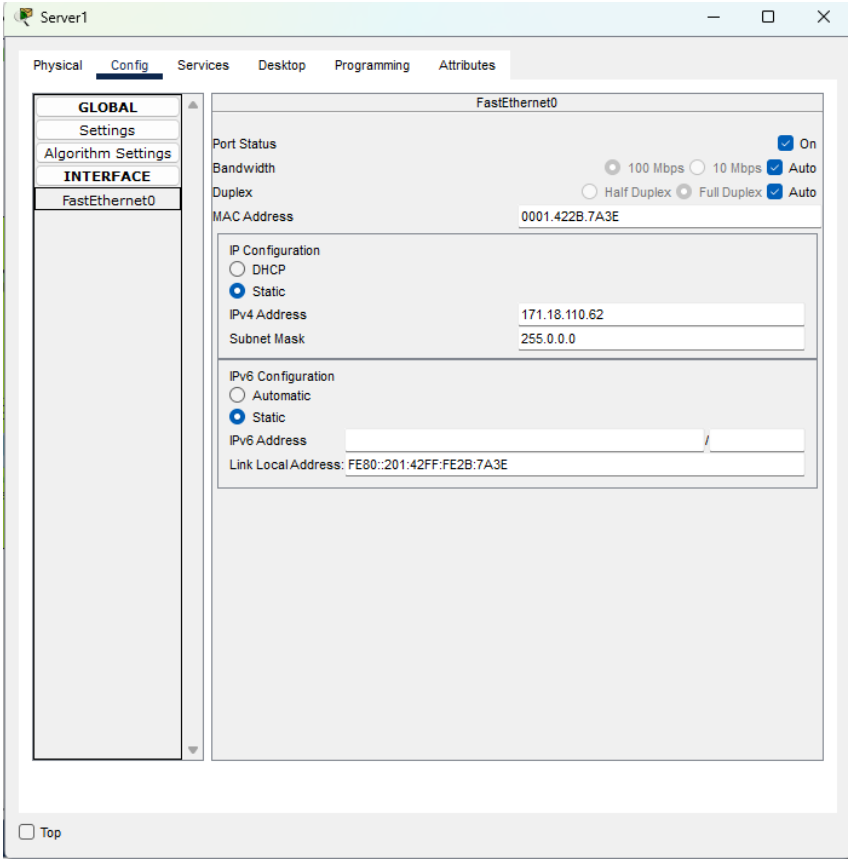
xiii. Pc7



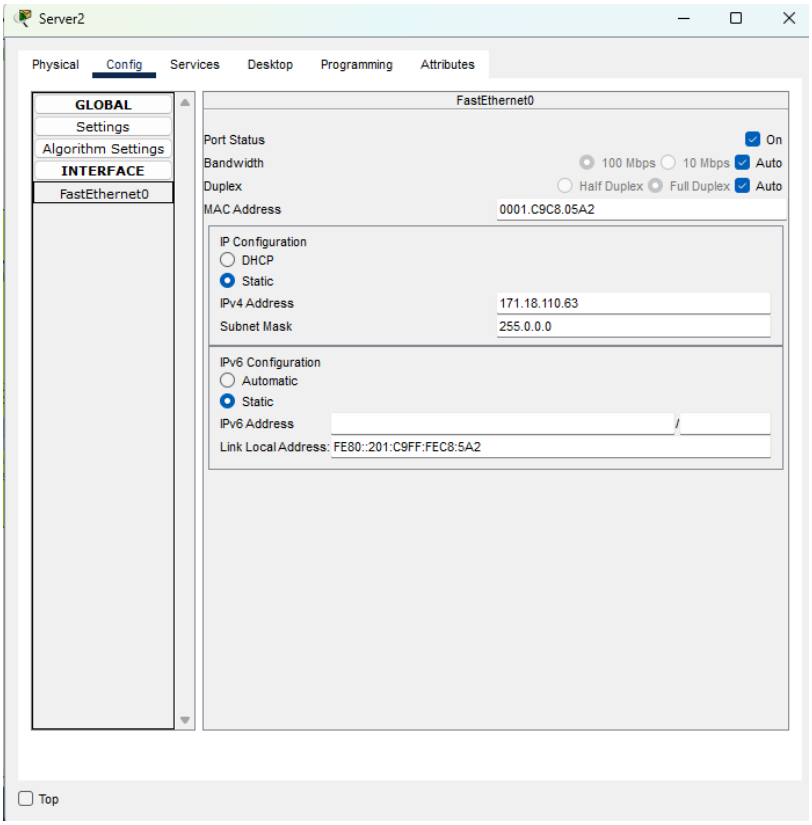
xiv. Pc8



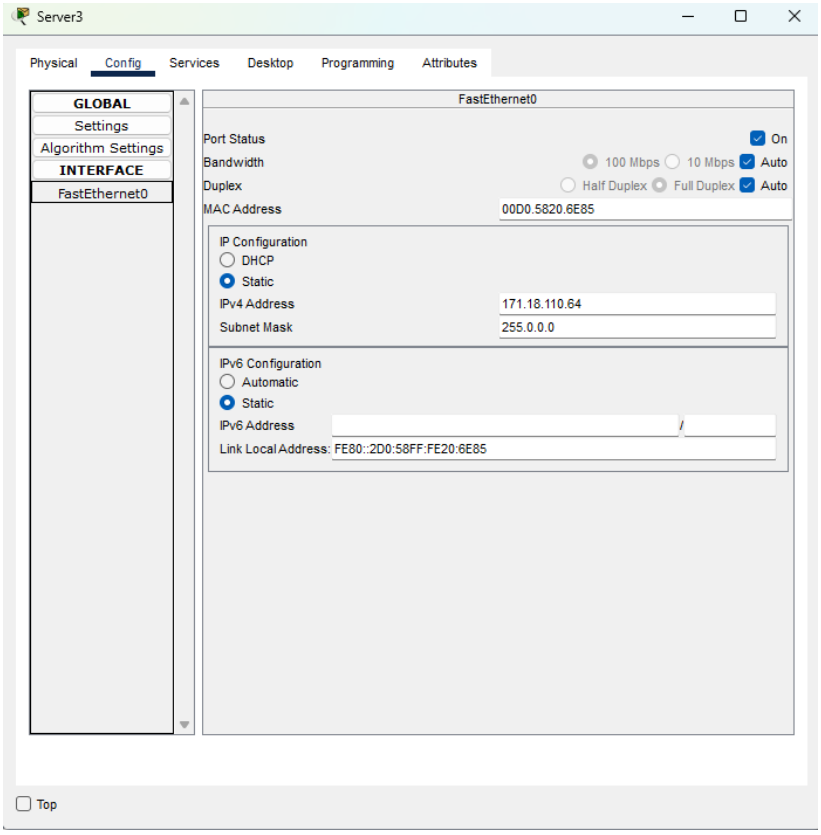
xv. Server1



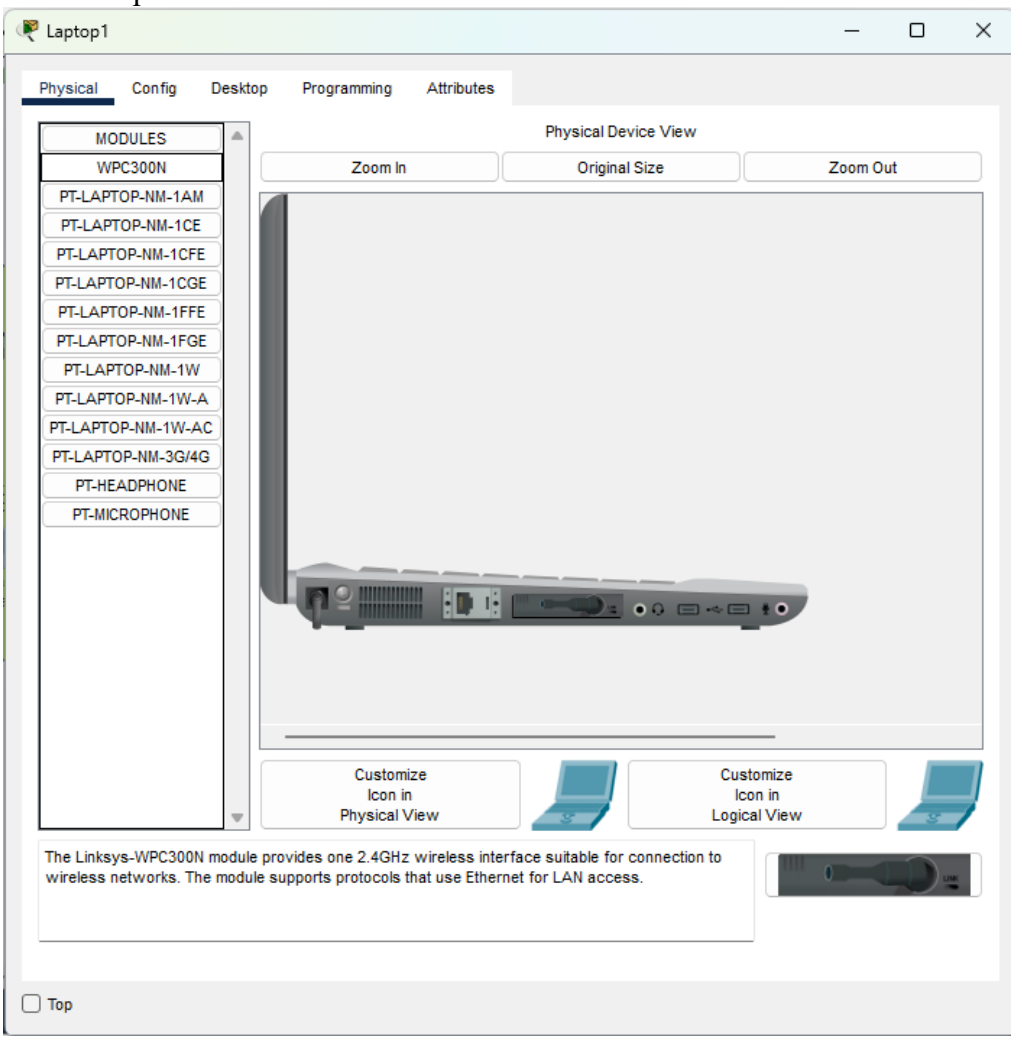
xvi. Server2



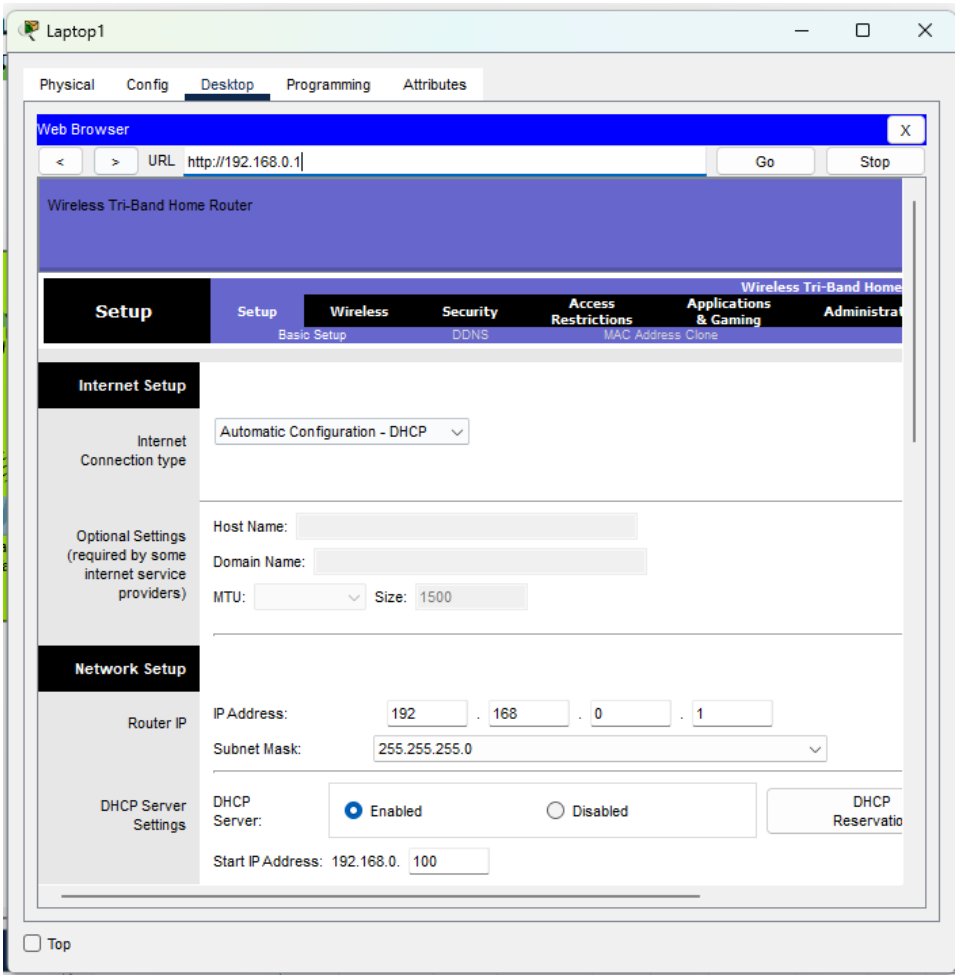
xvii. Server3



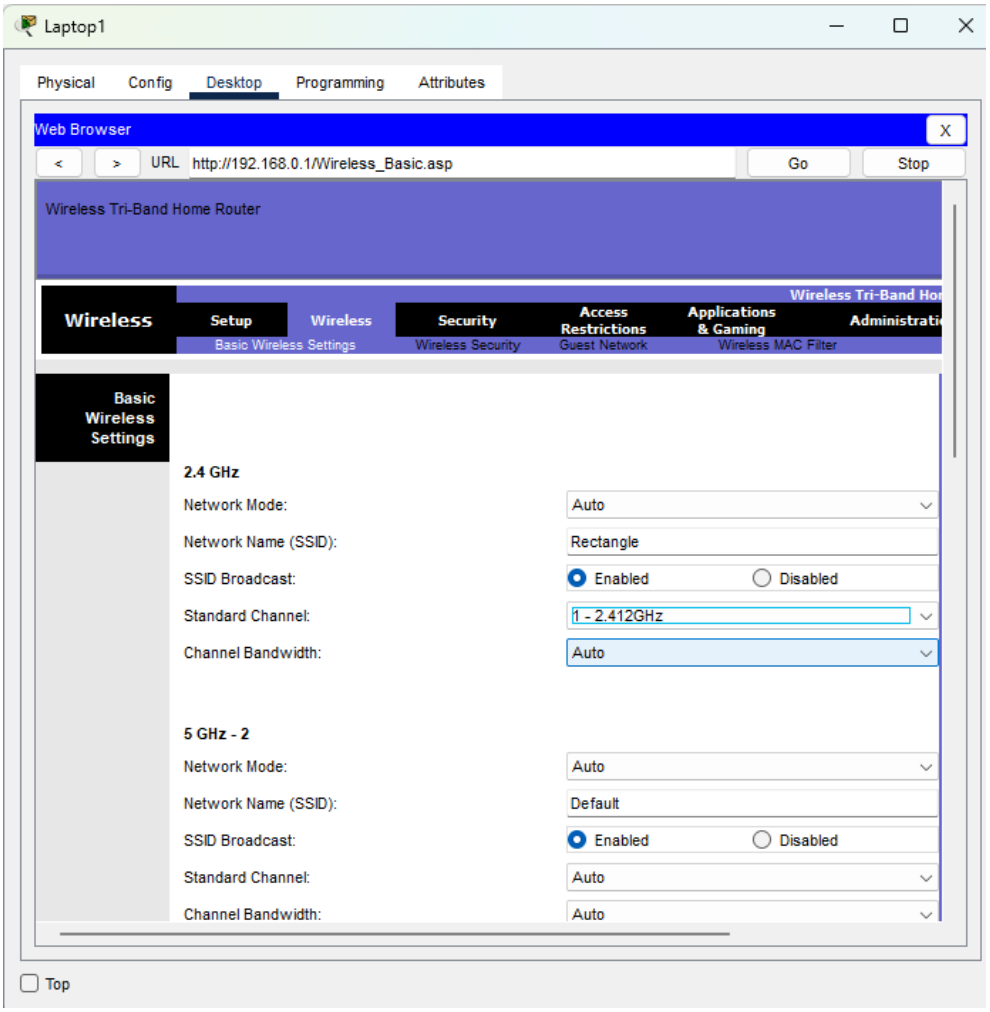
b. For the wireless network configuration, consider the following:
    i. Green Wireless Network (Rectangles)
        1. Para permitir la conexión del router a la laptop agregamos el modulo wpc300n



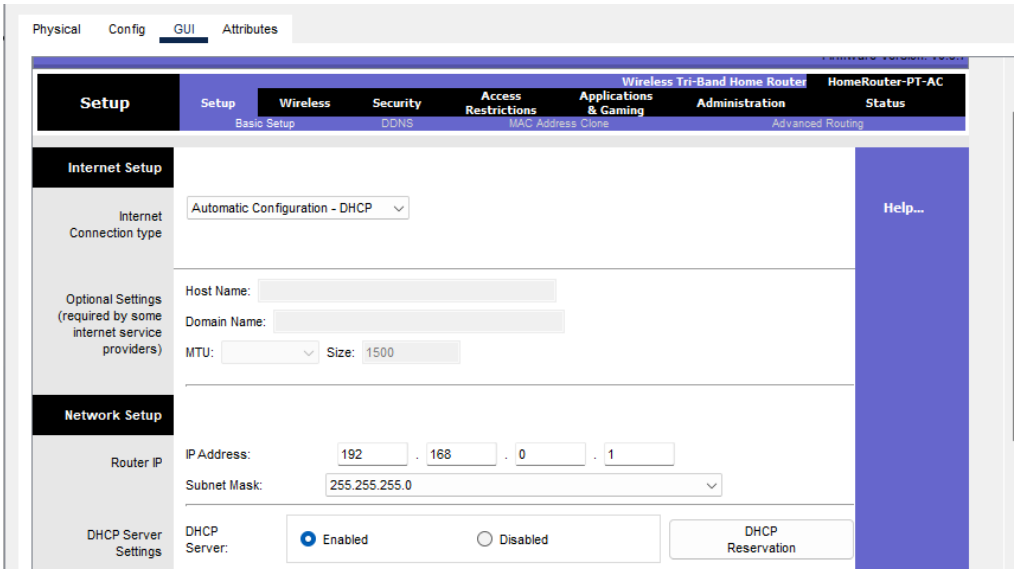
        2. Ingresamos en el navegador web con la dirección http://192.168.0.1 para ingresar a la configuración el router



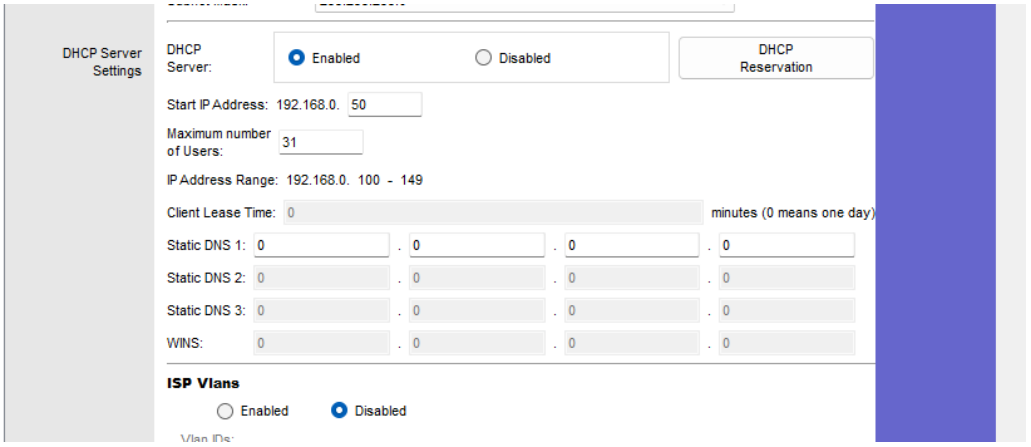
3. Wireless network identifier - SSID: Rectangle
    a. Agregamos el SSID del router el cual será Rectangle mediante el canal 1 .



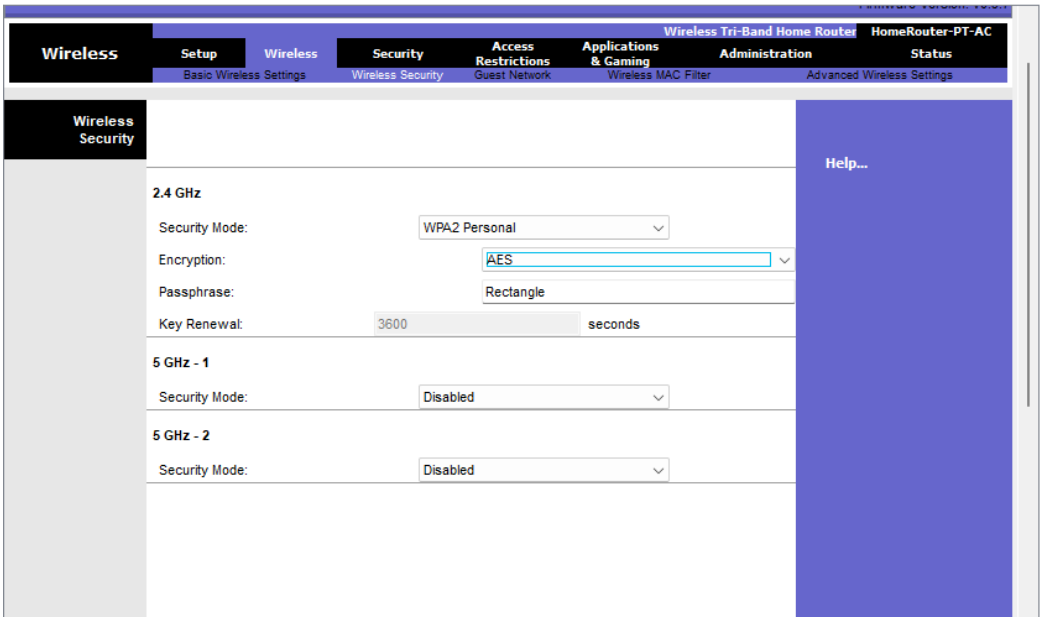
4. Wireless network IP: 192.168.0.0/24
5. Wireless router IP address (wireless interface): 192.168.0.
    a. Ahora agregamos la ip de la red la cual es 192.168.0.1 con la mascara 255.255.255.0



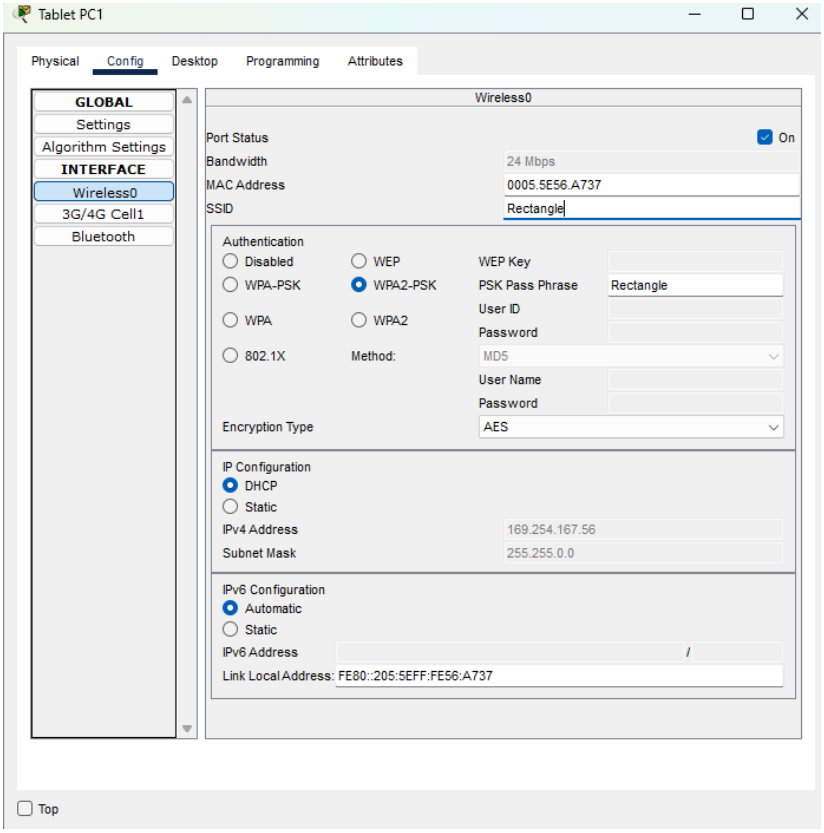
6. IP address range for mobile devices: 192.168.0.x to 192.168.0.y. Use the same ranges from the previous setup
    a. Agregamos los rangos de la red los cuales van de la 192.168.0.50-192.168.0.80 .



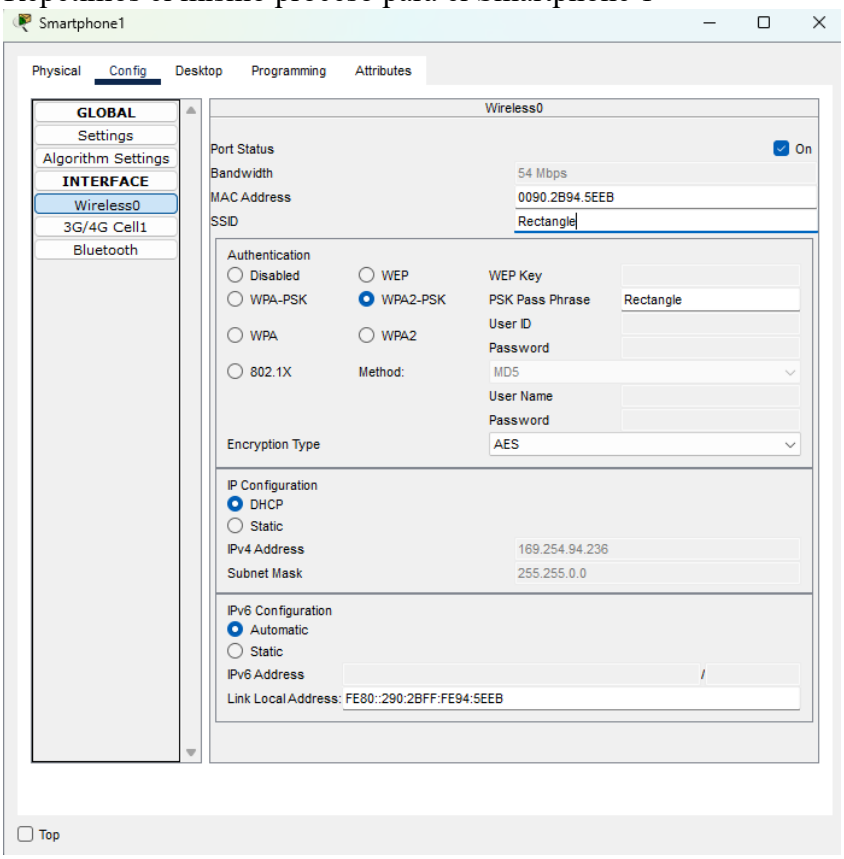
7. Access mechanism for wireless clients: WPA2-PSK with AES
    a. Agregamos la autenticación mediante la encripción AES y la contraseña Rectangle



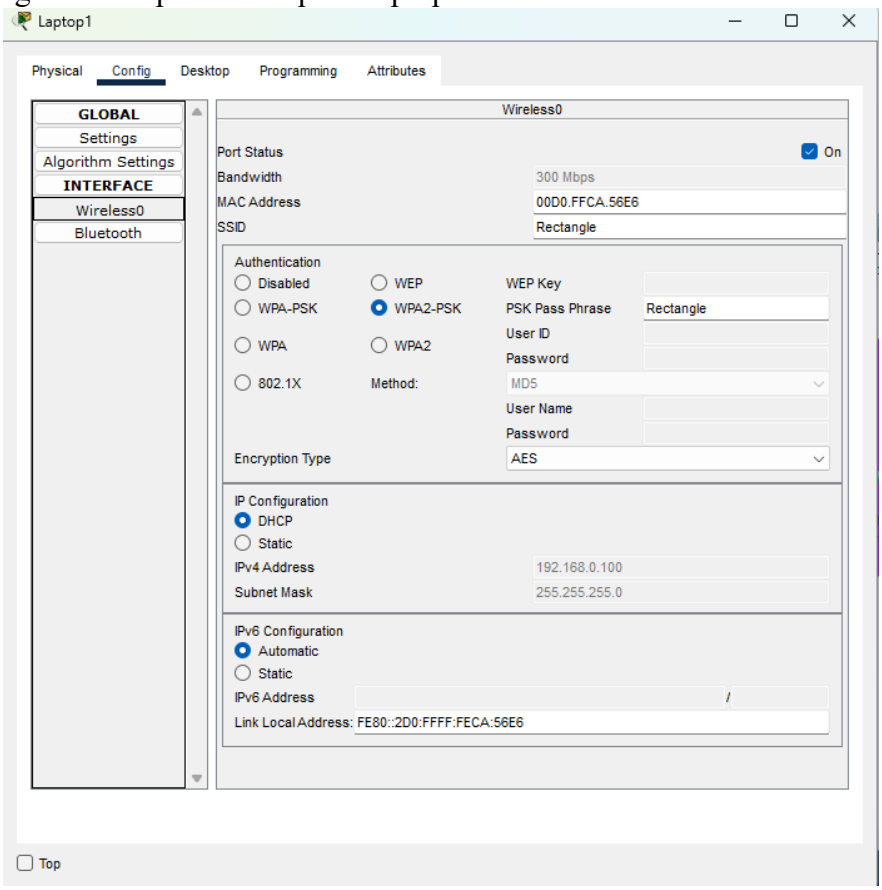
8. Una vez configurado el router y guardado los cambios, procedemos a configurar las maquinas permitiendo la conexión
9. Ingresamos a la Tablet Pc1 y agregamos el SSID y la contraseña configurada anteriormente (Rectangle – Rectangle)



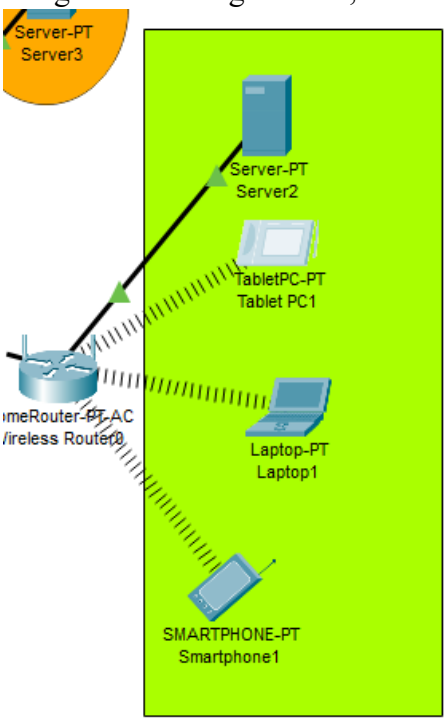
10. Repetimos el mismo proceso para el Smartphone 1



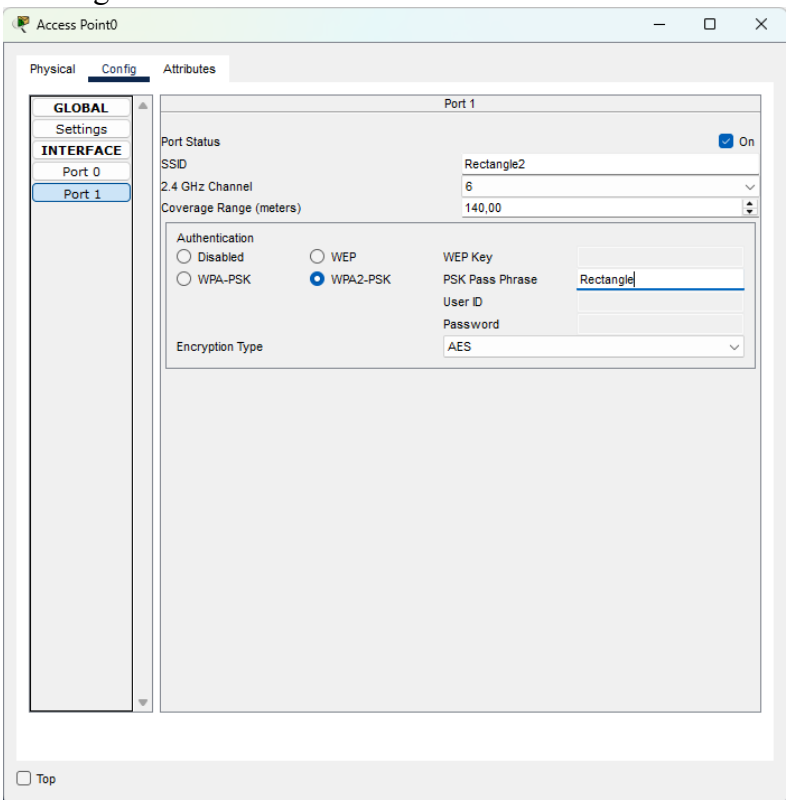
11. Igualmente para la maquina laptop1



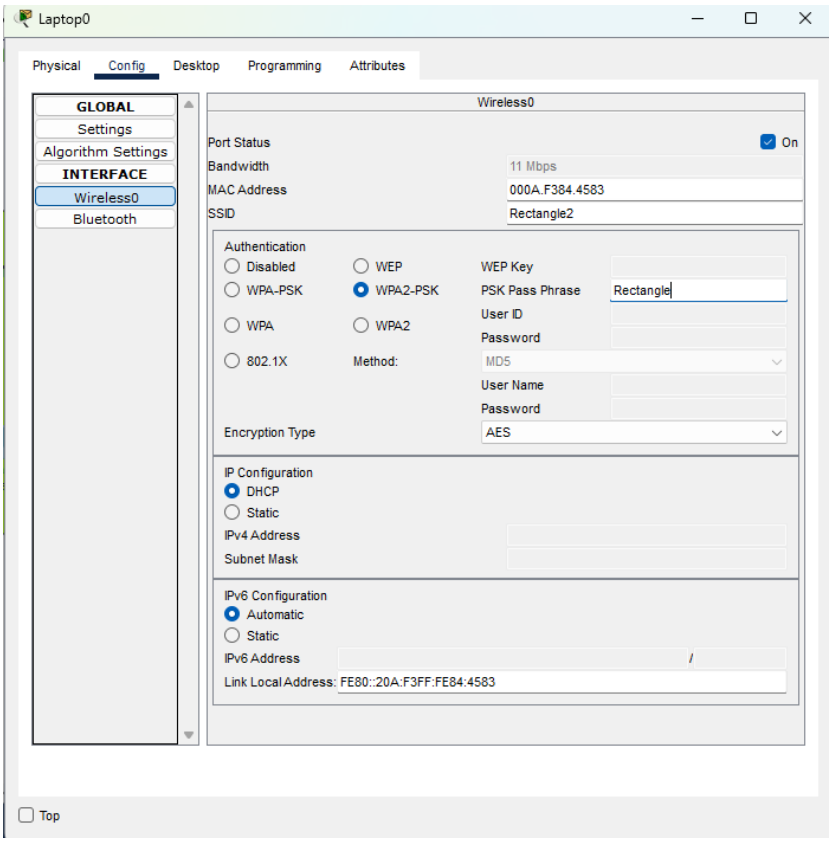
12. Luego de la configuración , se tendrá que ver así:



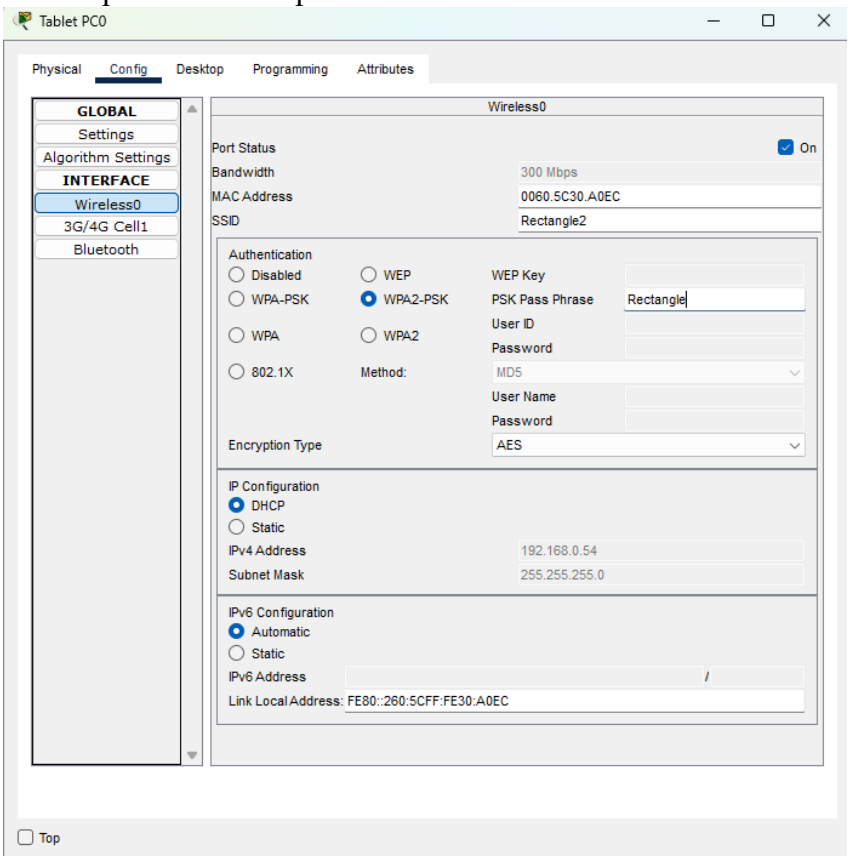
13. Ahora configuramos la otra zona verde la cual tiene el Access point
14. En este caso le daremos el SSID Rectangle 2 con contraseña Rectangle



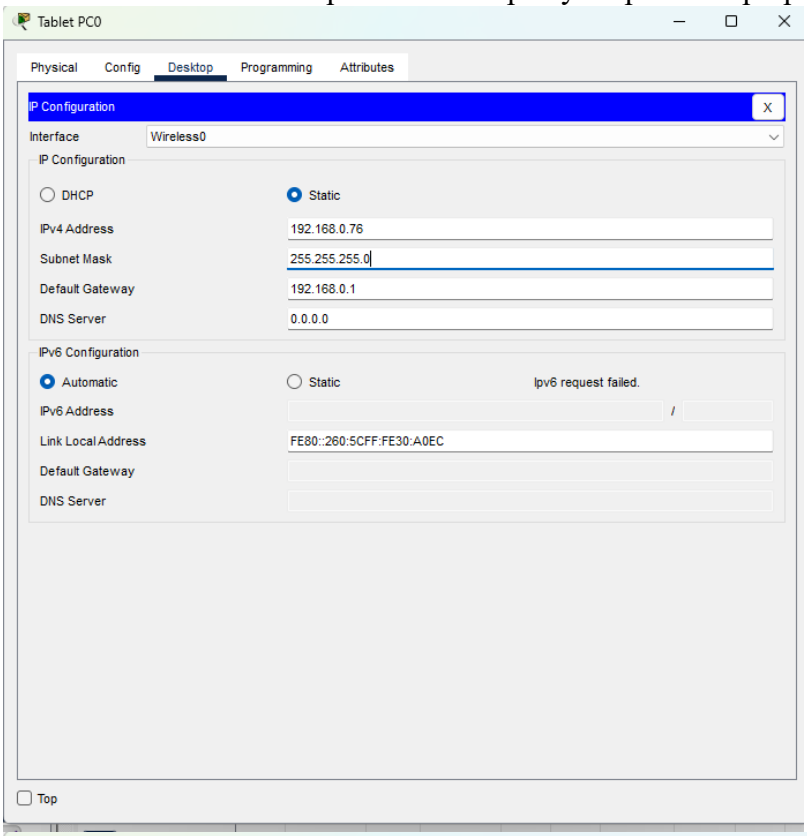
15. Igual que en los pasos anteriores, ingresamos en la laptop0 y colocamos el SSID de Rectangle 2 y contraseña Rectangle

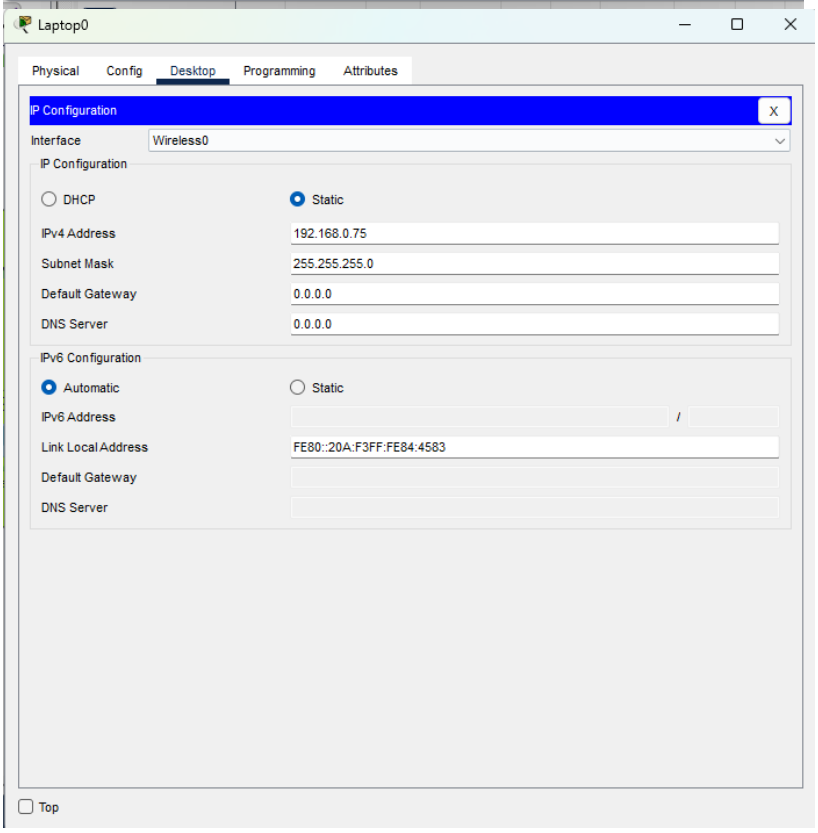


16. Mismo procedimiento para tablet PC0

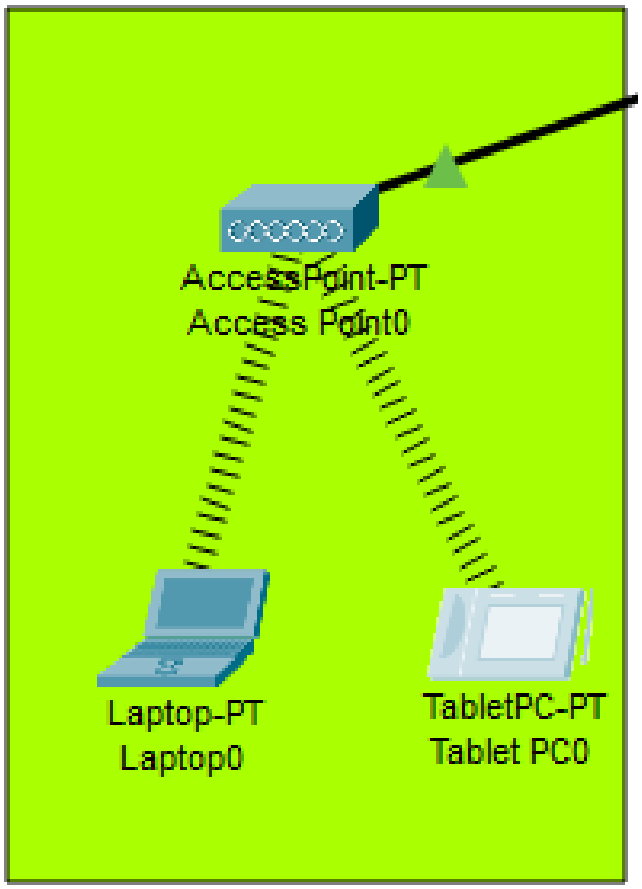


17. Configuramos las ip manualmente teniendo el cuenta el rango, en este caso usaremos la 76 para la Tablet pc0 y 77 para la laptop0



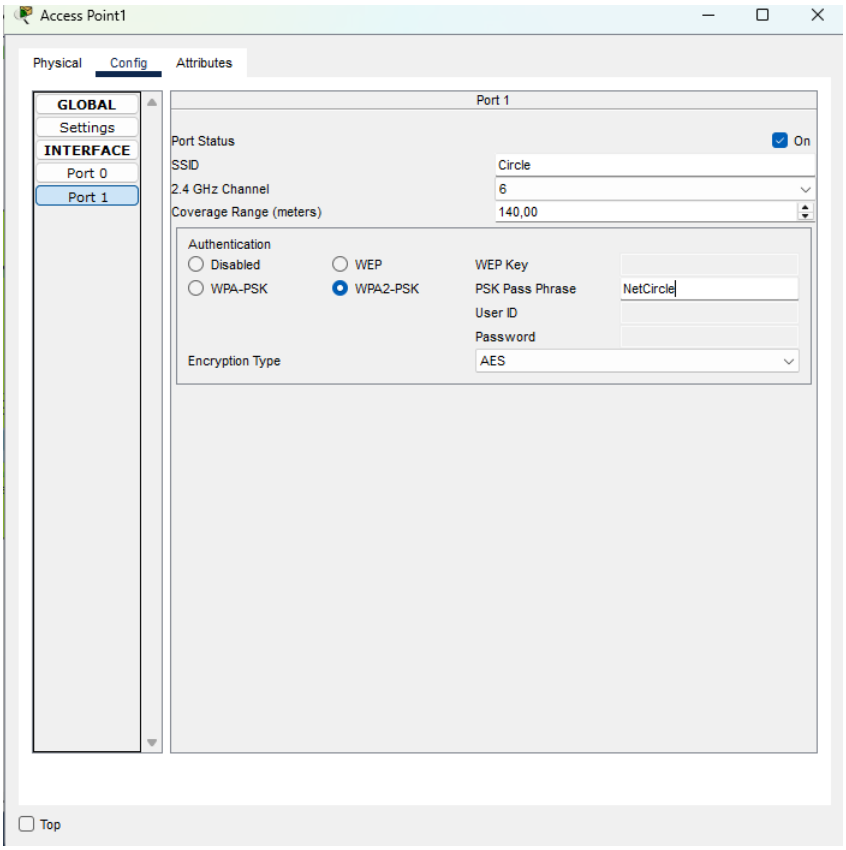


18. Una vez configurado se tendrá que ver así:

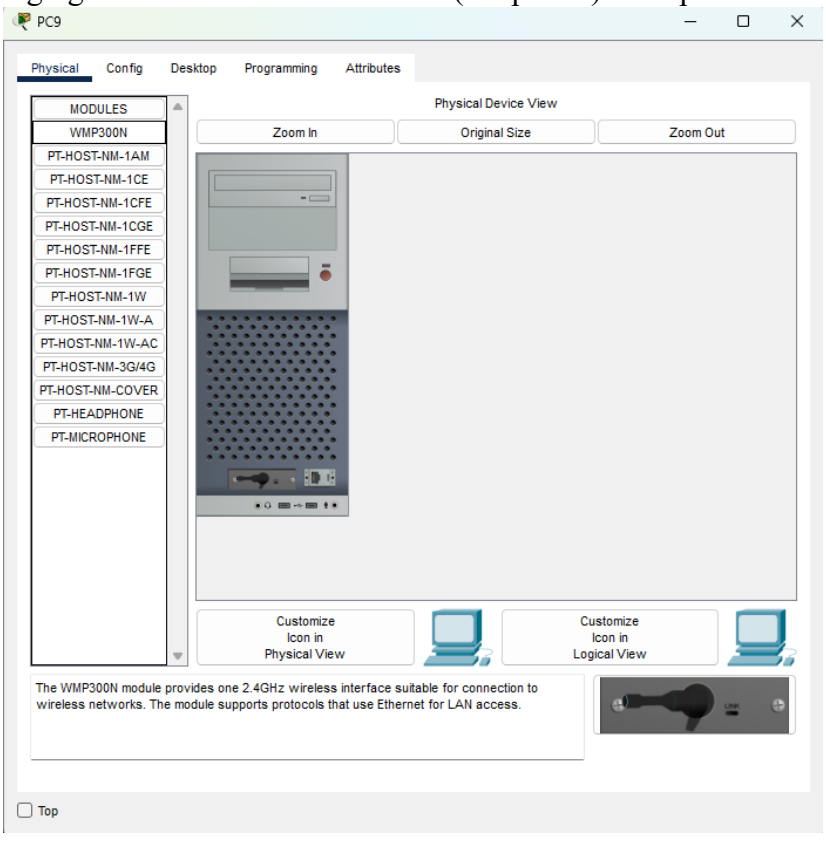


ii. Purple Wireless Network (Circles)

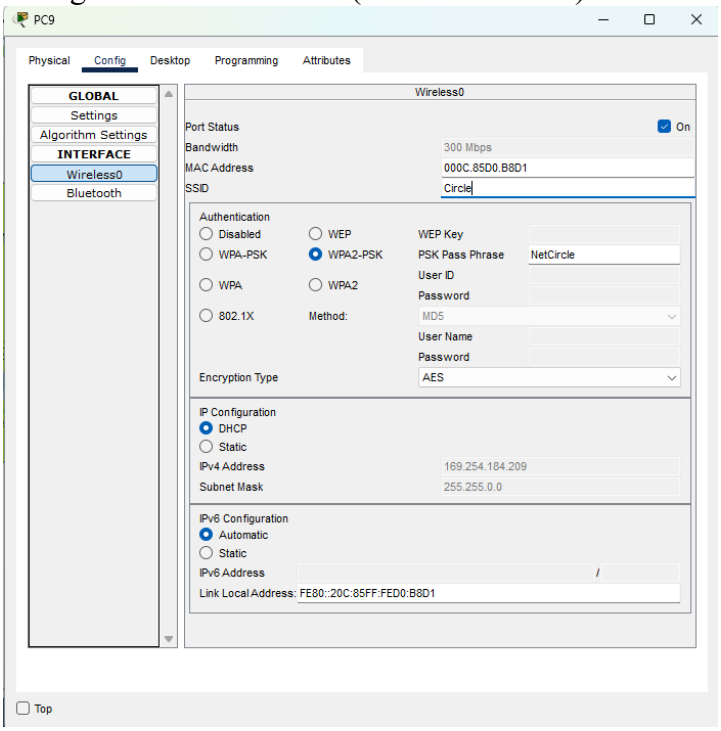
1. Wireless network identifier - SSID: Circle
2. Access mechanism for wireless clients: WPA2-PSK with AES
3. Access Point password for mobile devices: Circle
4. Repetimos el mismo proceso anterior del Access point pero ahora el SSID y la contraseña es Circle y NetCircle respectivamente



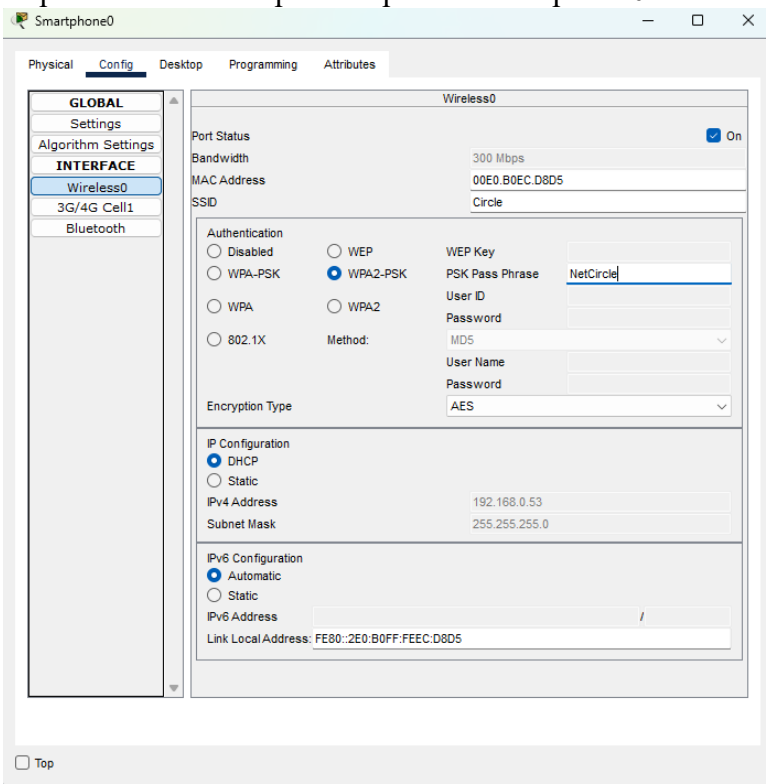
5. Agregamos el módulo de Wireless (wmp300n) en el pc9



6. Una vez agregado el módulo, agregamos el SSID y contraseña configurada anteriormente (Circle-NetCircle)

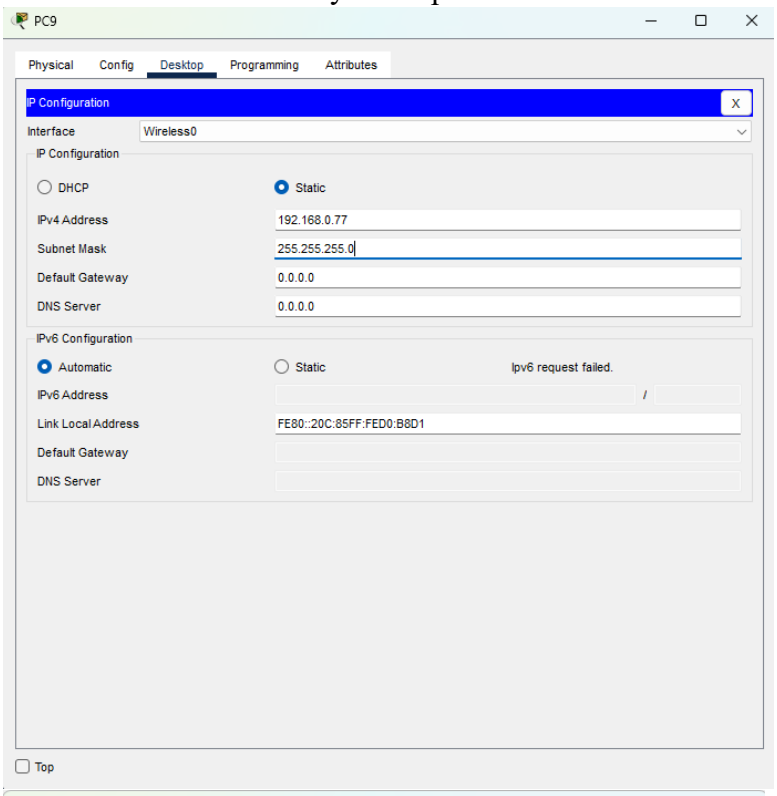


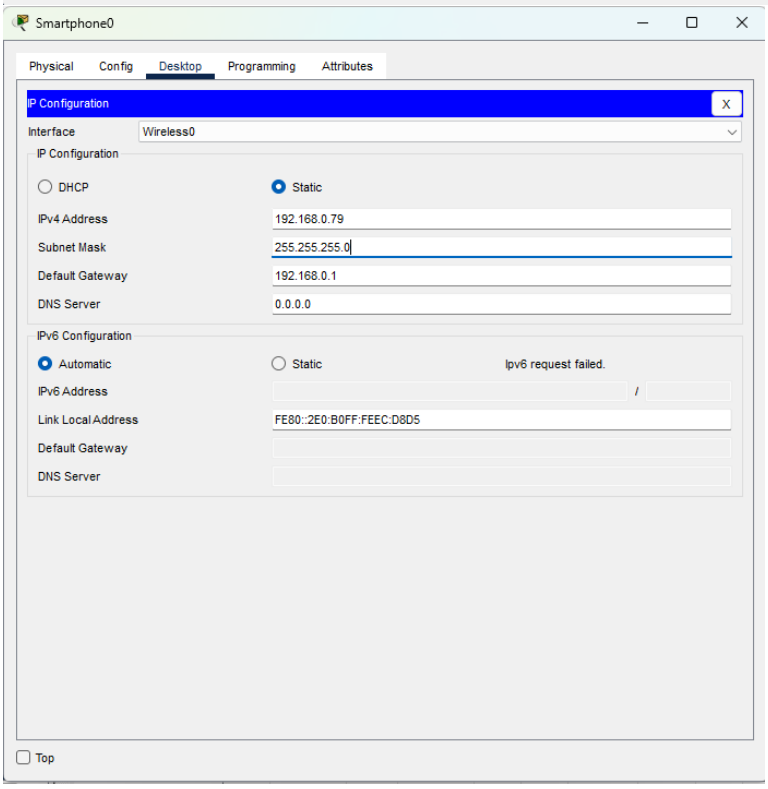
7. Repetimos el mismo proceso para el Smartphone0



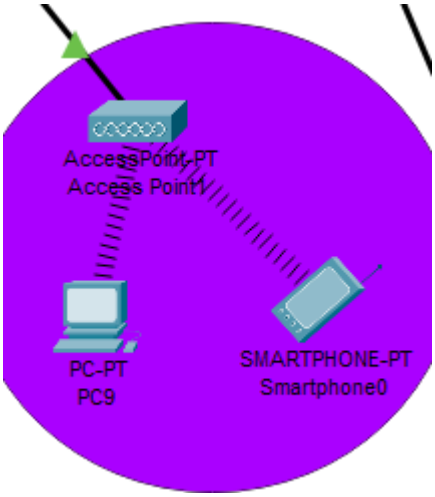
8. Assign IP addresses to computers connected to this network based on the range used in the wired network.

a. Ahora agregamos las ip de manera estática las cuales las tomamos del rango asignado inicialmente. En este caso tomaremos 192.168.0.77 y 78 respectivamente

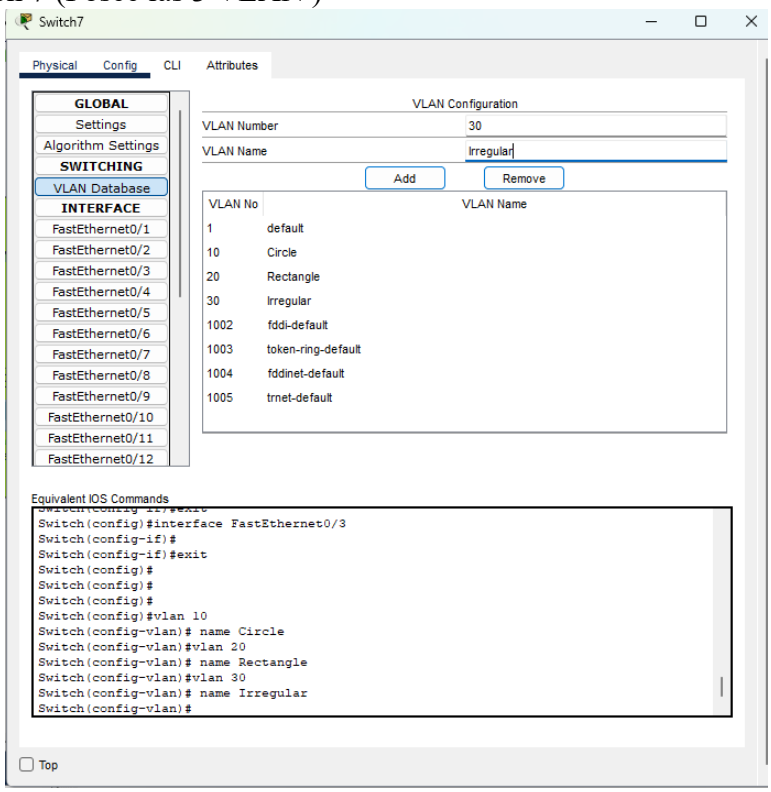




9. Una vez configurado todo se verá así:

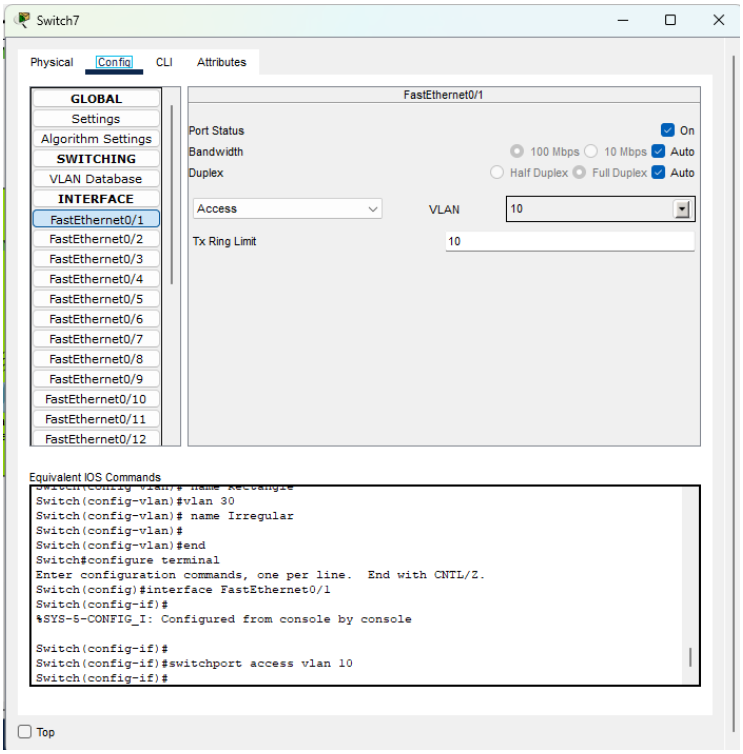


c. Verify connectivity between all devices. What can and cannot be done?
    i. Todavia no permite la conexión entre dispositivos ya que no están configuradas las interfaces de red de los switches
d. Configure the VLANs based on the colors in the diagram
    i. Ahora, para configurar las vlan, ingresamos en cada switch y agregamos los nombres que asignamos anteriormente en los routers y Access Point
    ii. Para Circle usaremos 10, para rectangle 20 e irregular 30 (son los pc que no realizamos ninguna configuración adicional)
    iii. Switch 7 (Posee las 3 VLAN)

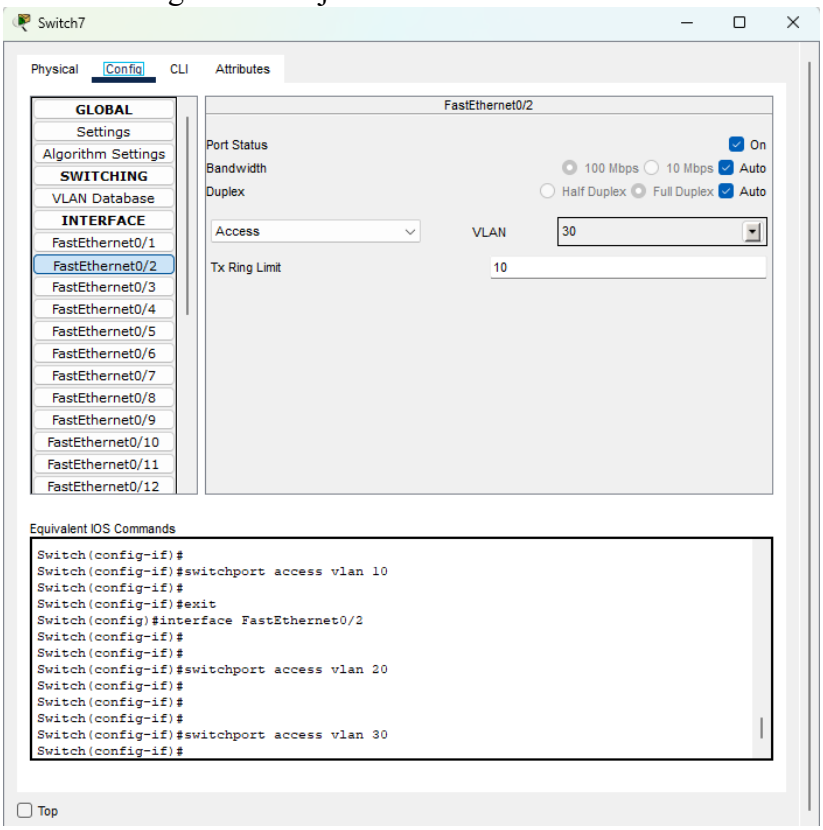


1. Ahora configuramos las interfaces de red dependiendo de la conexión del cable del switch y a la vlan que pertenece.

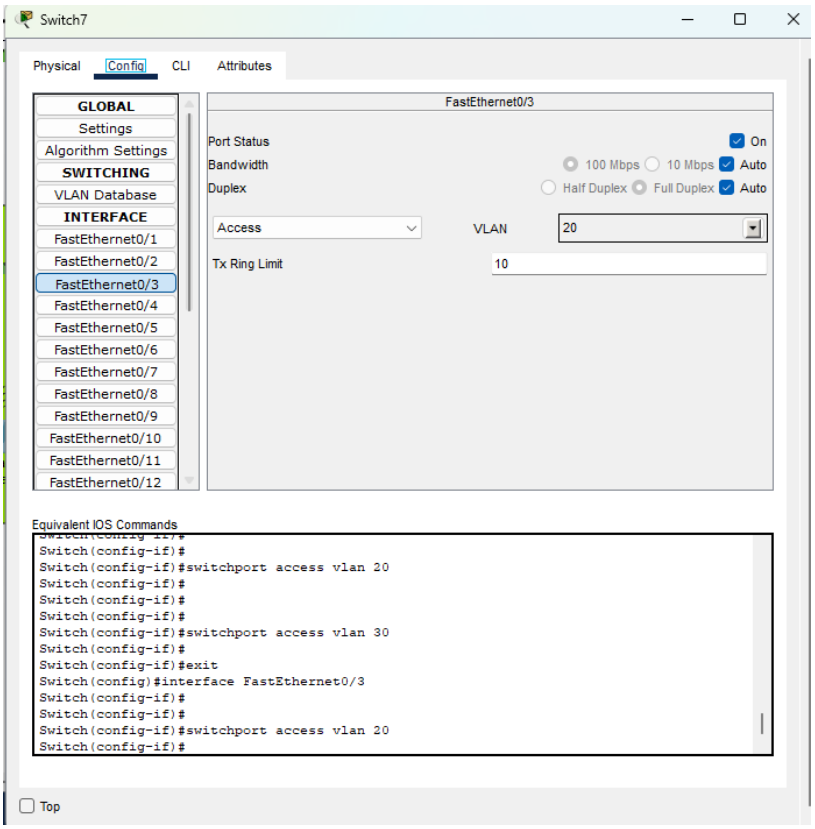
2. Fa0/1 Circle -> Morado



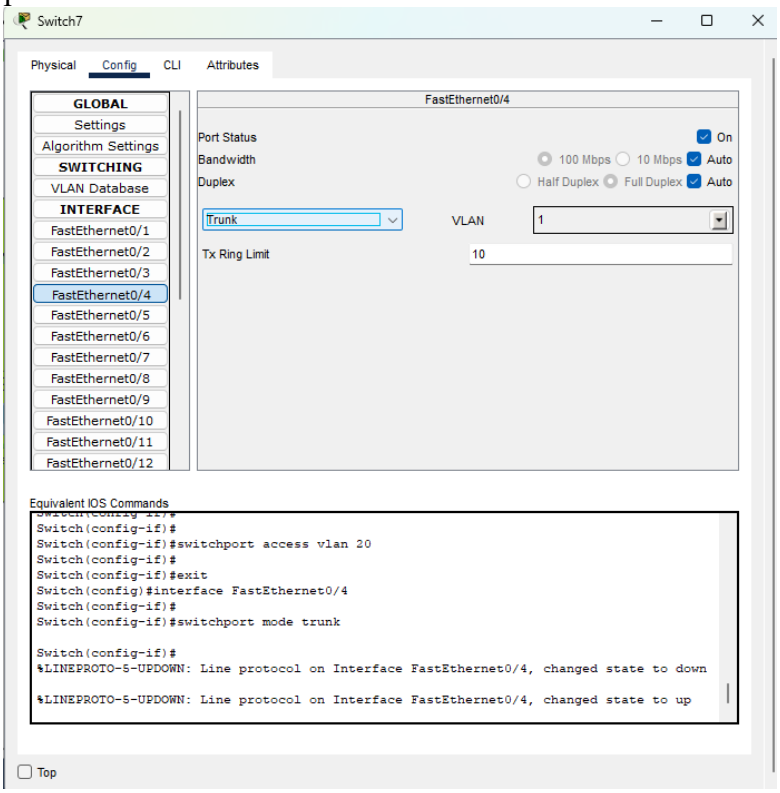
3. Fa0/2 -> Irregular Naranja



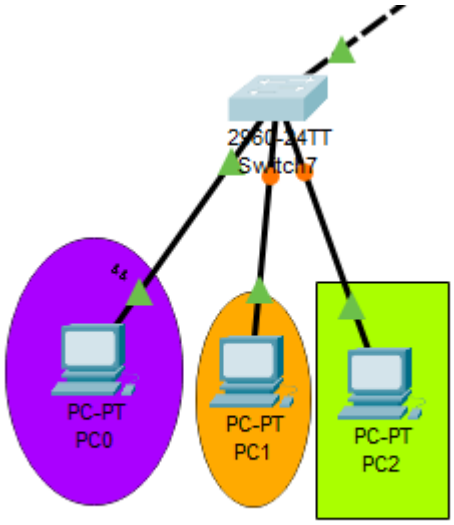
4. Fa0/3 Rectangle-> verde



5. Para la conexión entre switches usamos trunk el cual permite el paso de todas la vlans mediante el switch .



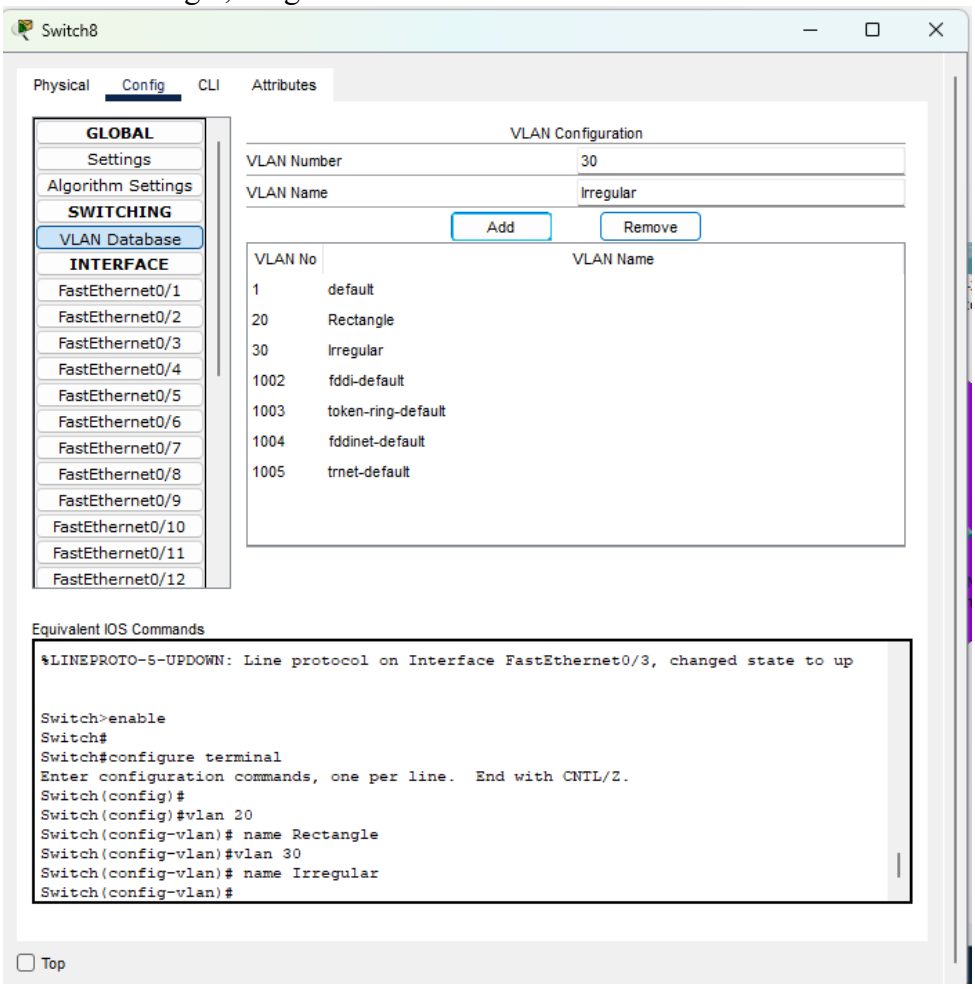
6. La configuración se realize en base a las conexiones



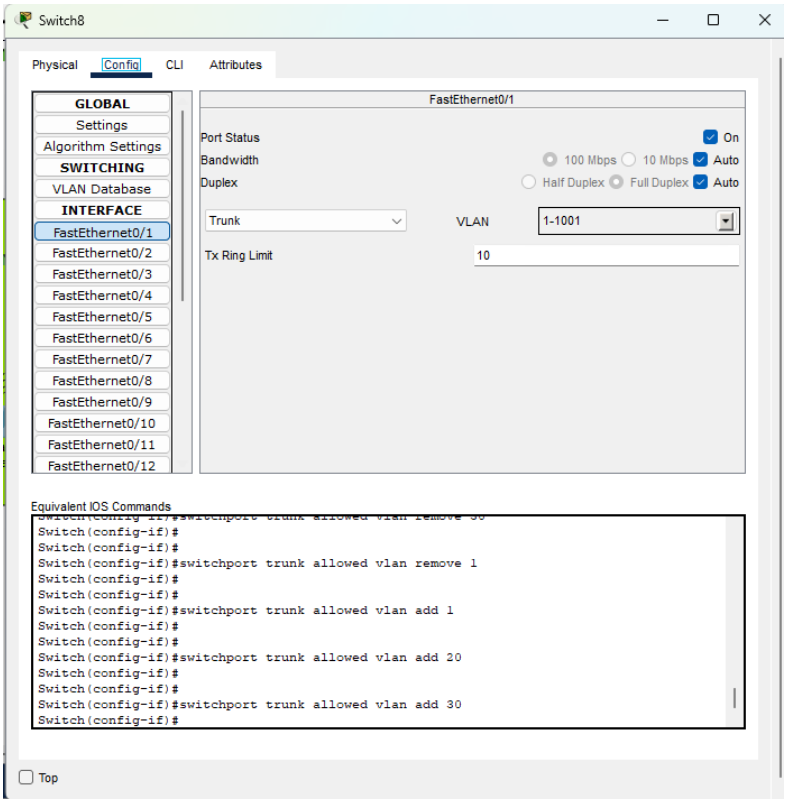
iv. Repetimos el mismo proceso para los siguientes switches

v. Switch 8

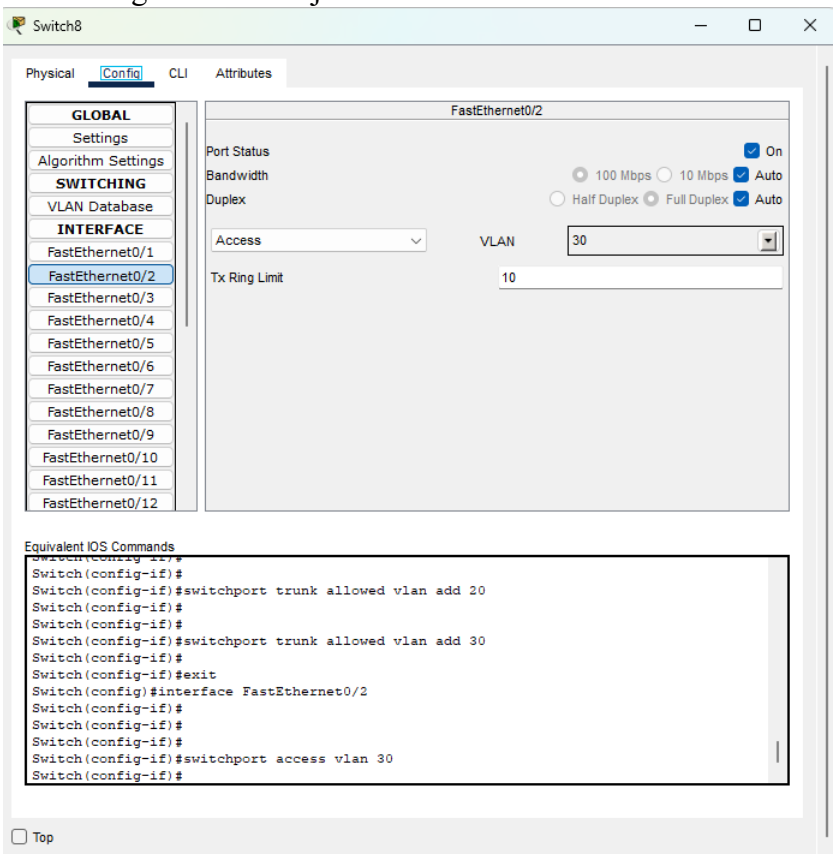
1. Vlans: Rectangle, irregular



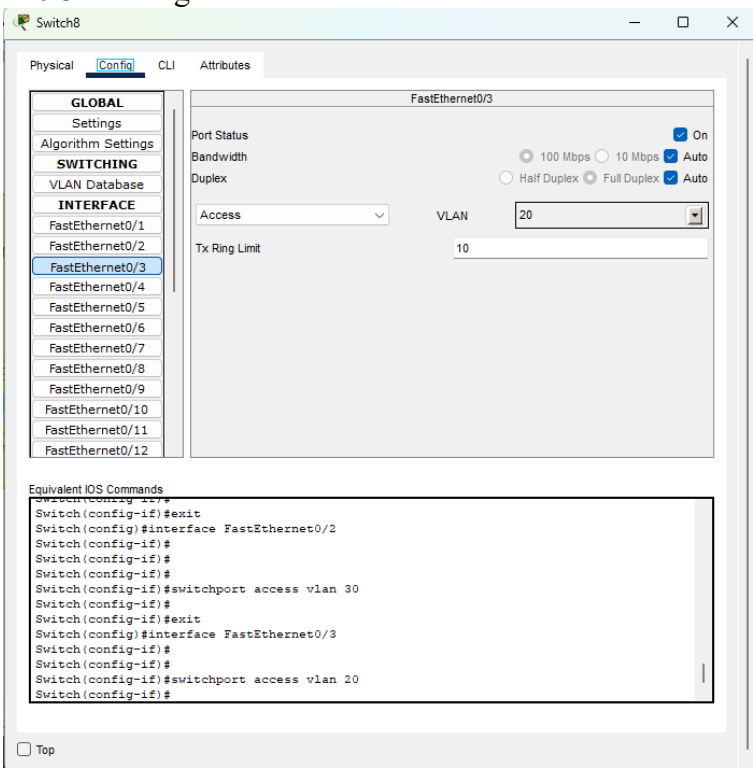
2. Fa0/1 Circle -> morado



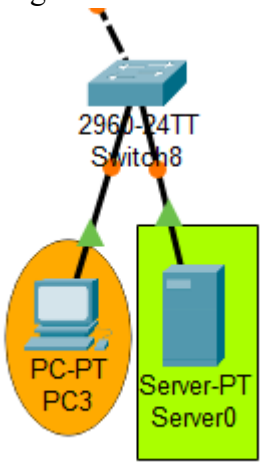
3. Fa0/2 Irregular -> naranja



4. Fa0/3 Rectangle->verde

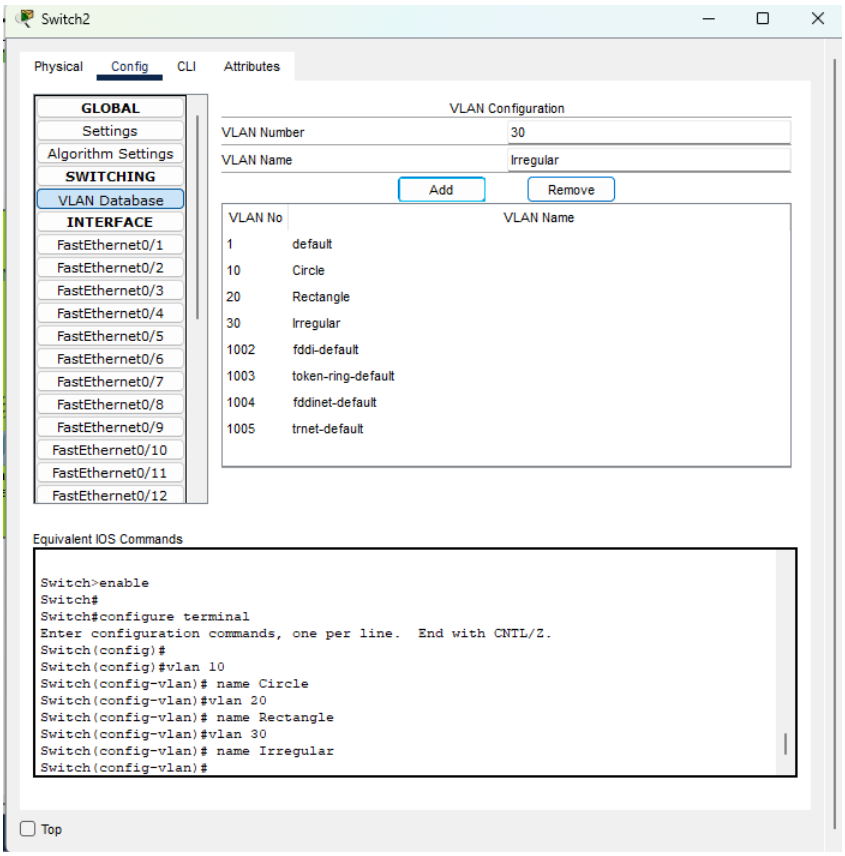


5. Configuración realizada:

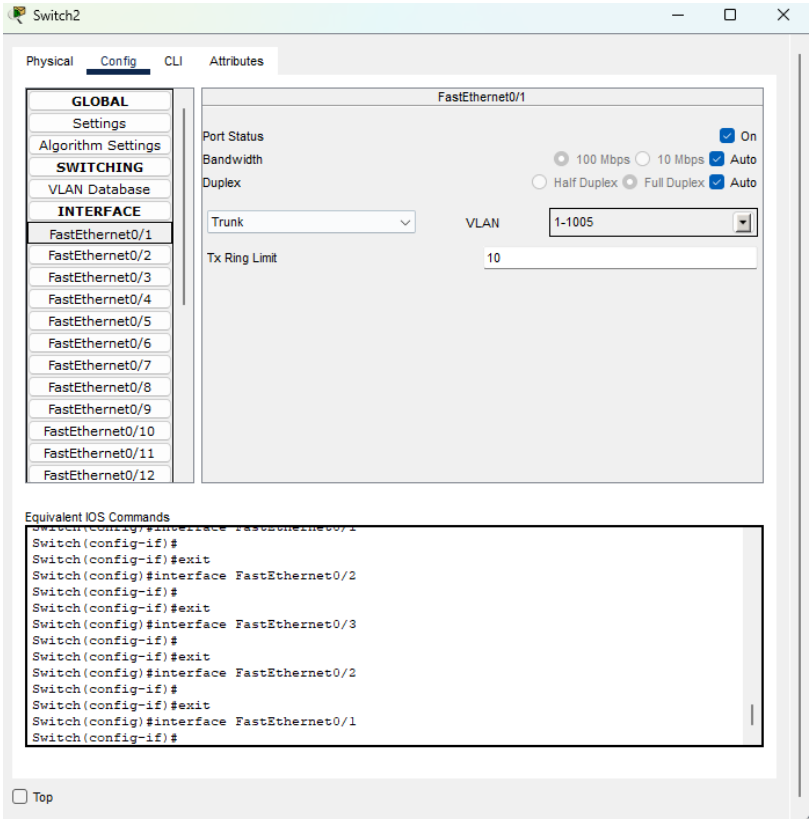


vi. Switch 2

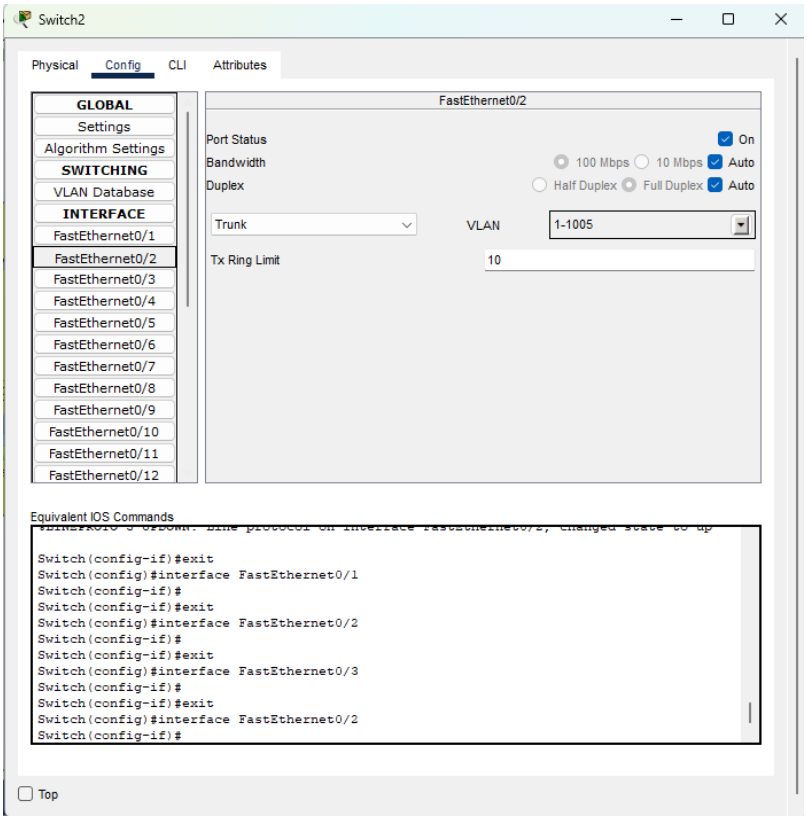
1. Vlans: Circle, rectangle , irregular



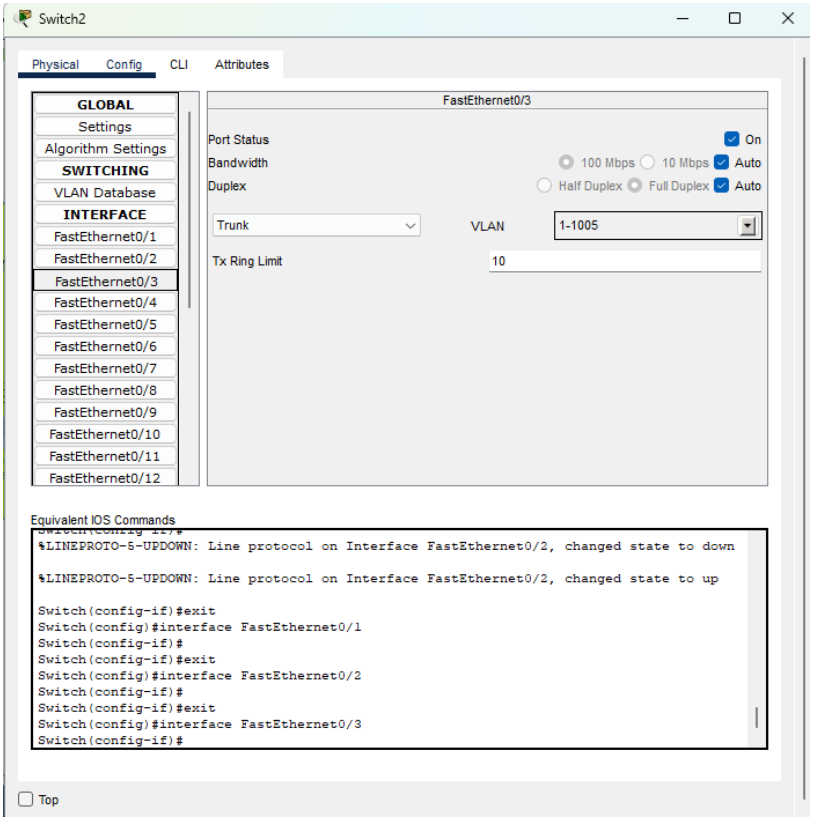
2. Fa0/1 Conexión switch



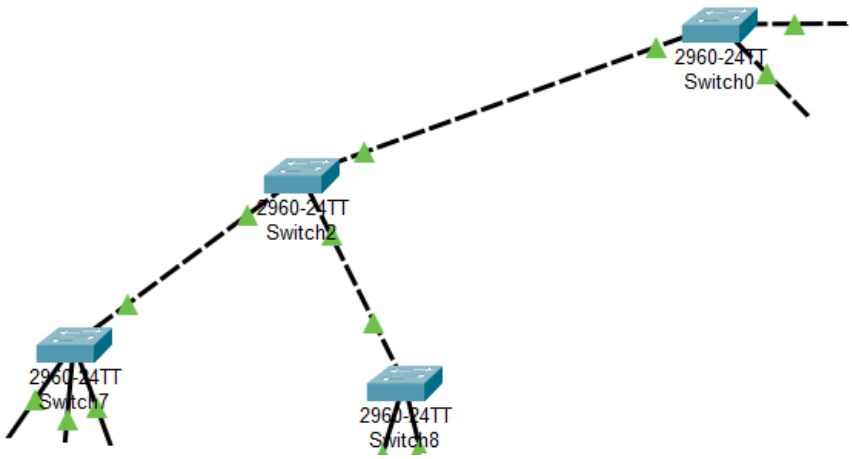
3. Fa0/2 Conexión switch



4. Fa0/3 conexión switch

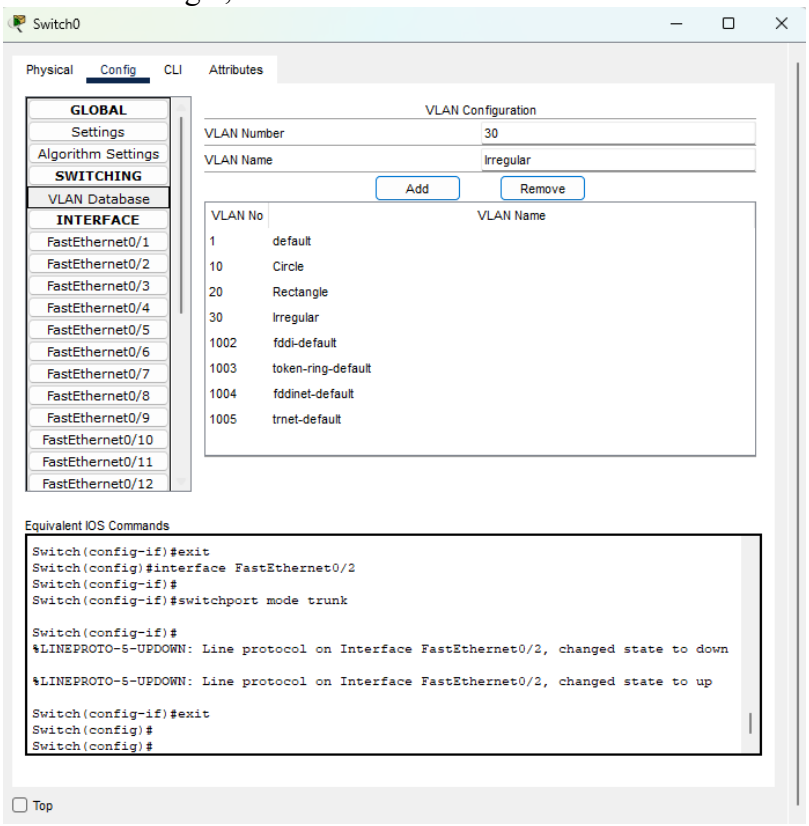


5. Configuración realizada:

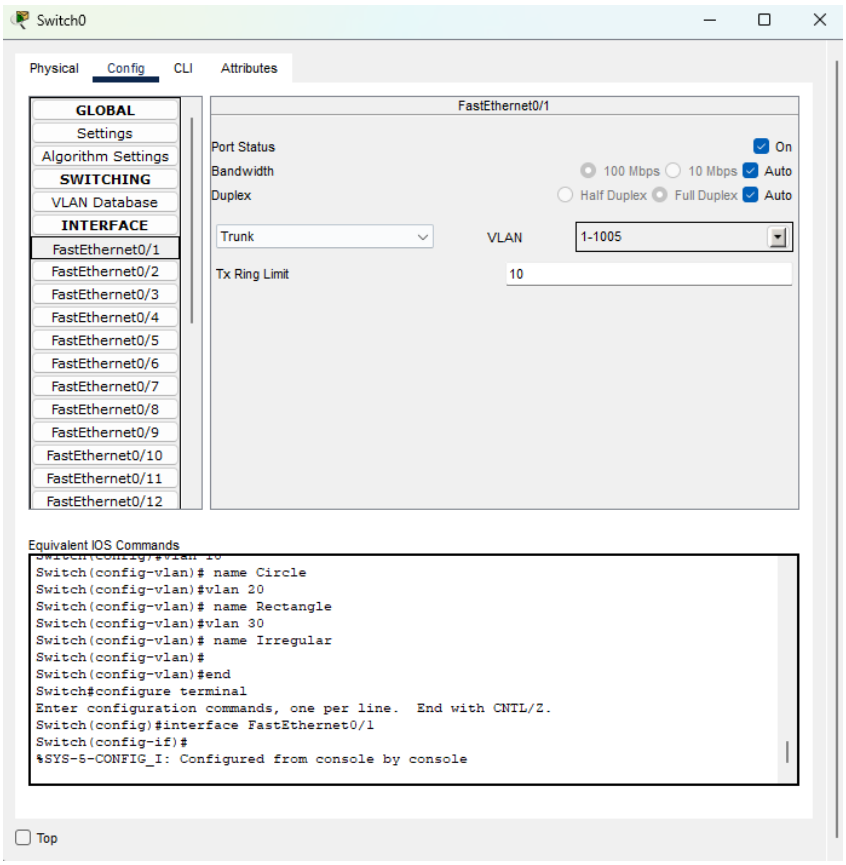


vii. Switch 0

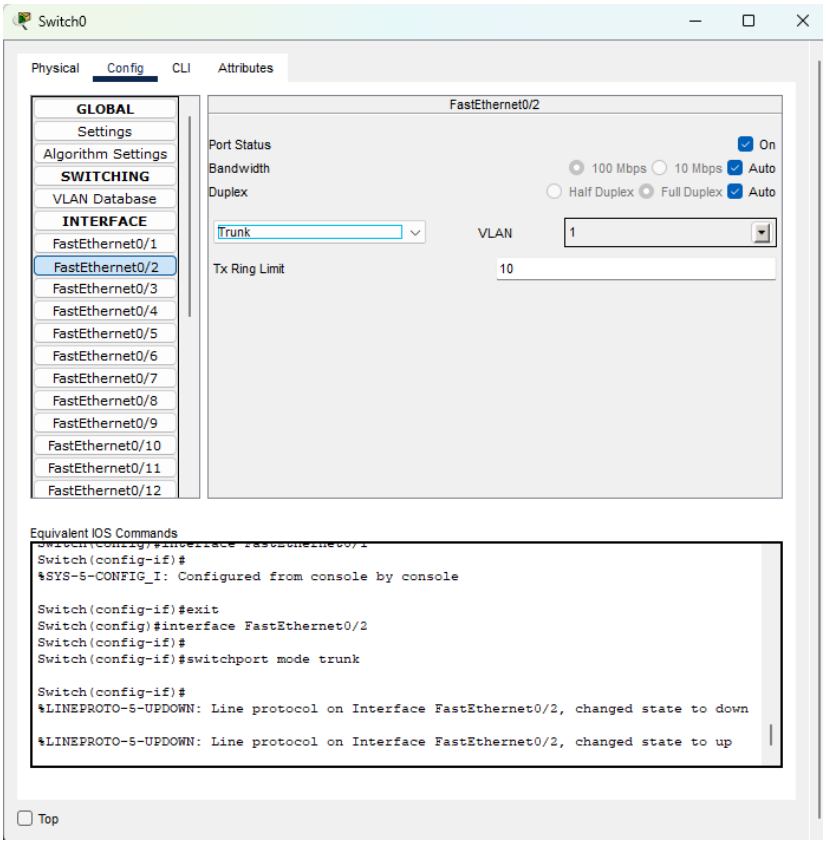
1. Vlans: Rectangle, circle



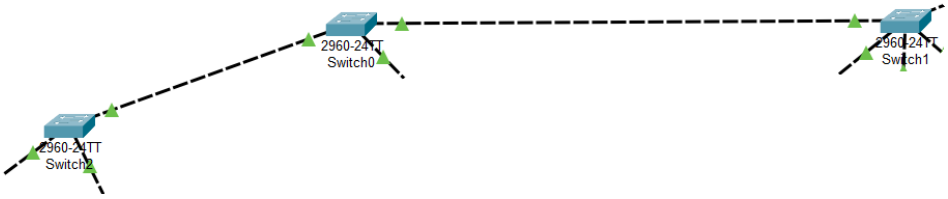
2. Fa0/1 Conexión switch



3. Fa0/2 Conexión switch

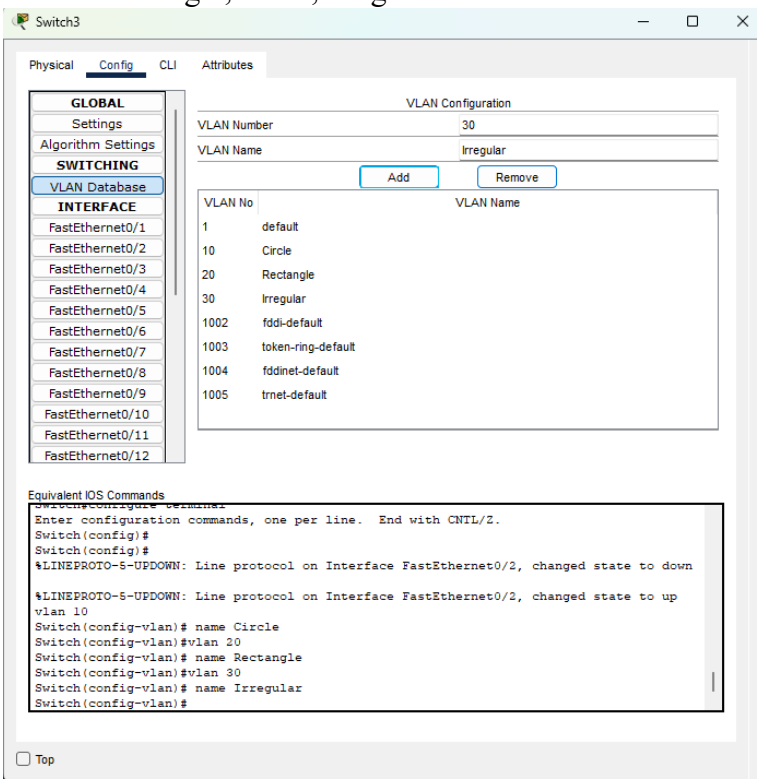


4. Configuración realizada

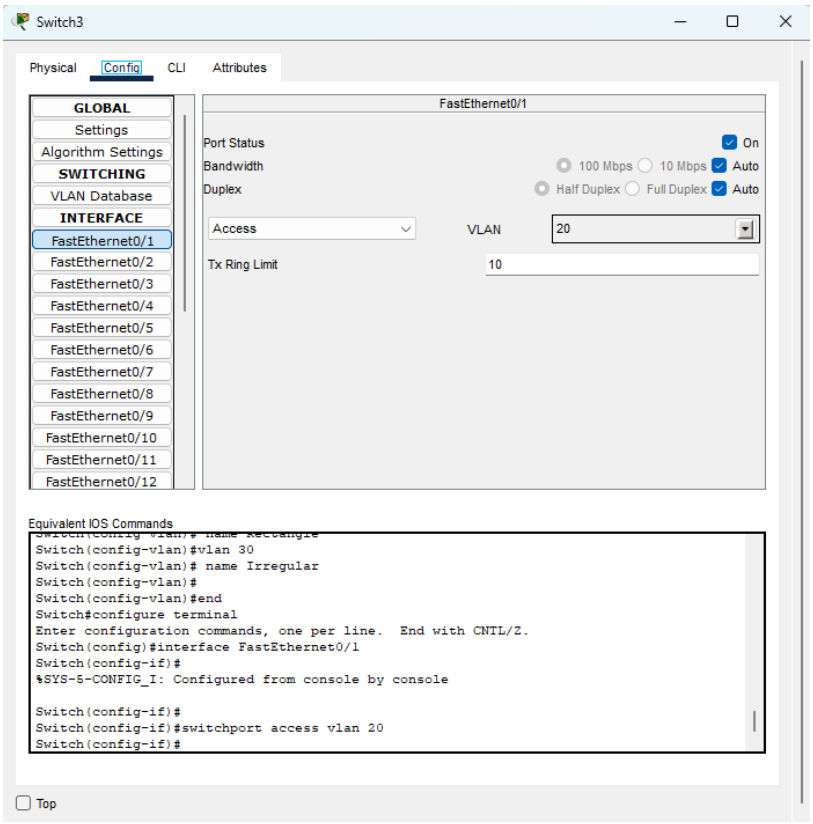


viii. Switch 3

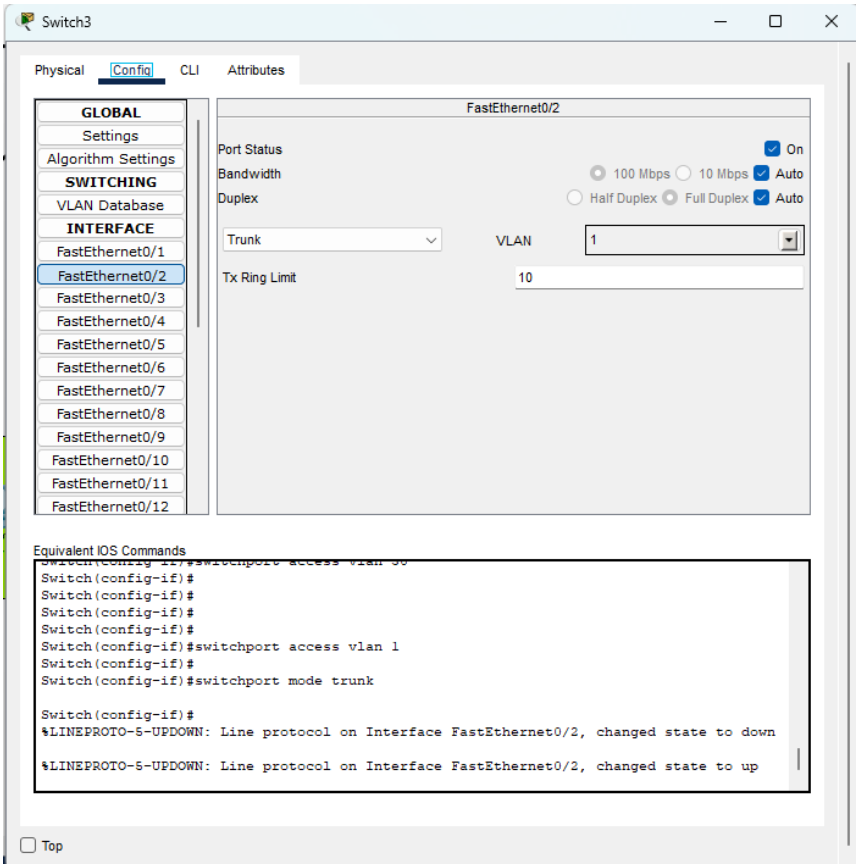
1. Vlans: Rectangle, circle, irregular



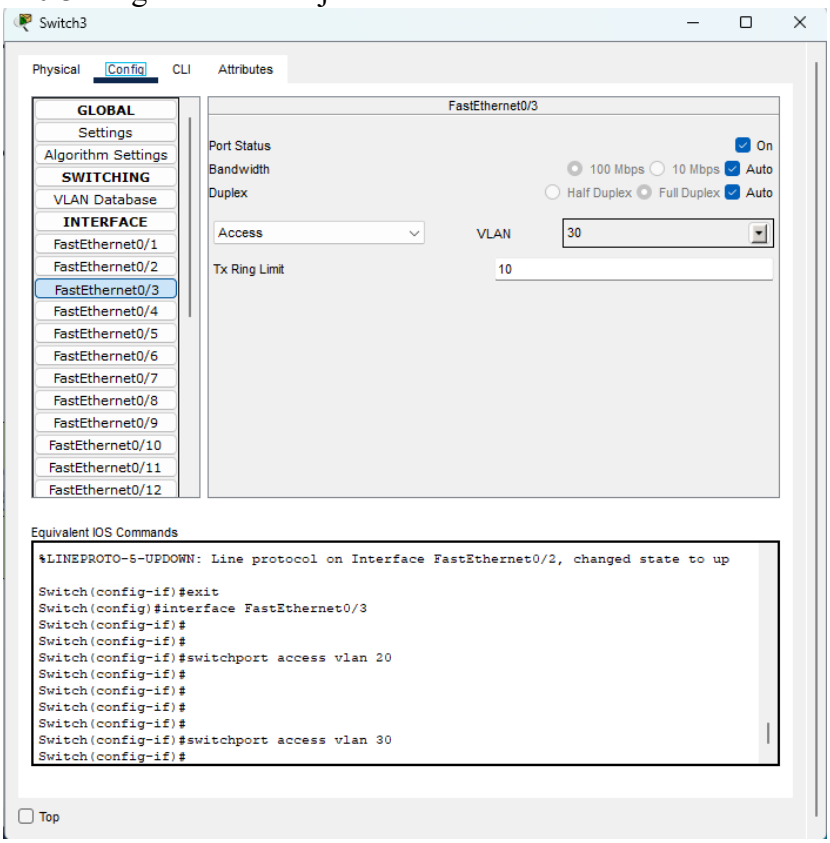
2. Fa0/1 Rectangle -> Verde



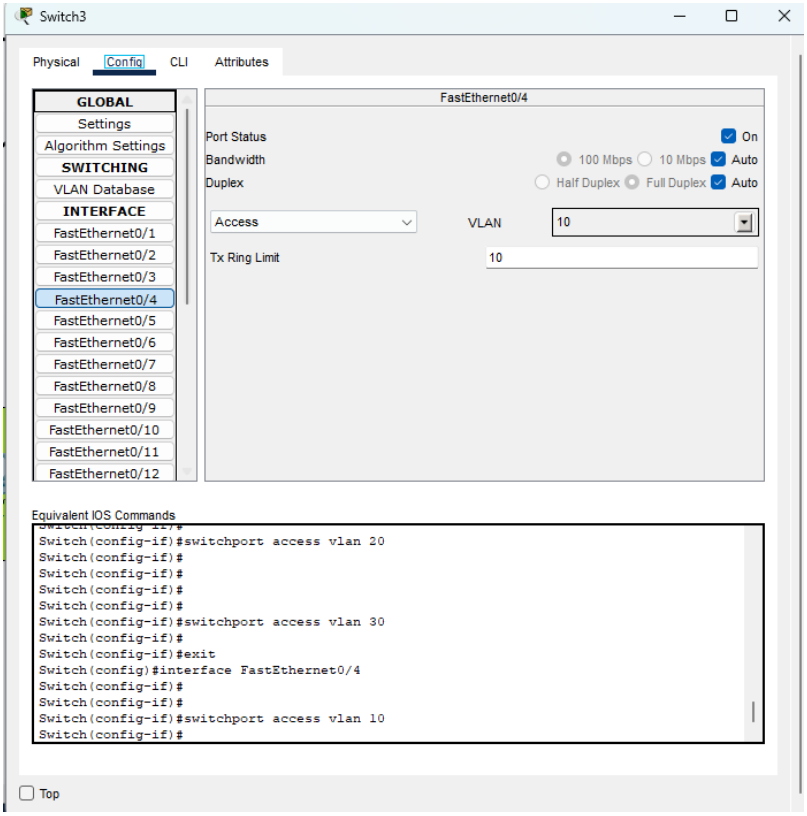
3. Fa0/2 Conexión switch



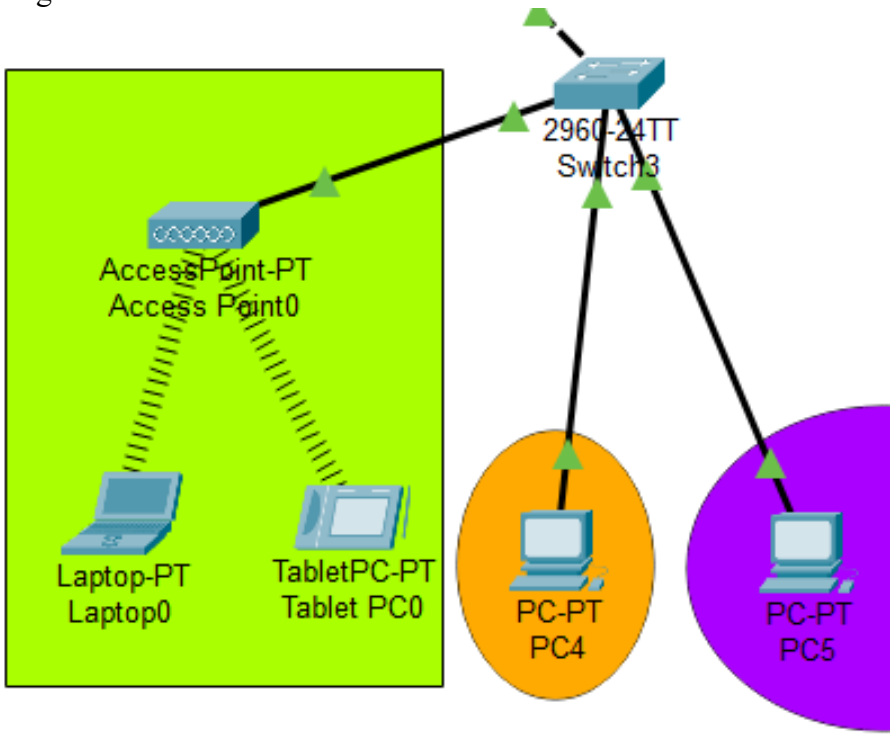
4. Fa0/3 Irregular -> Naranja



5. Fa0/4 Circle -> morado

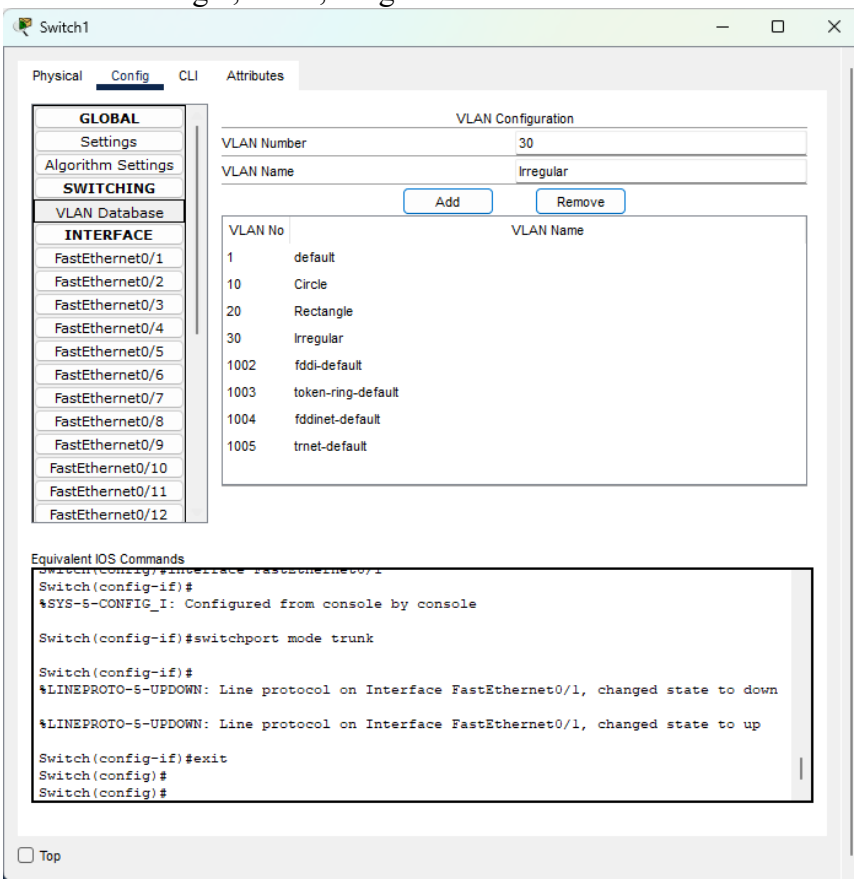


6. Configuración realizada:

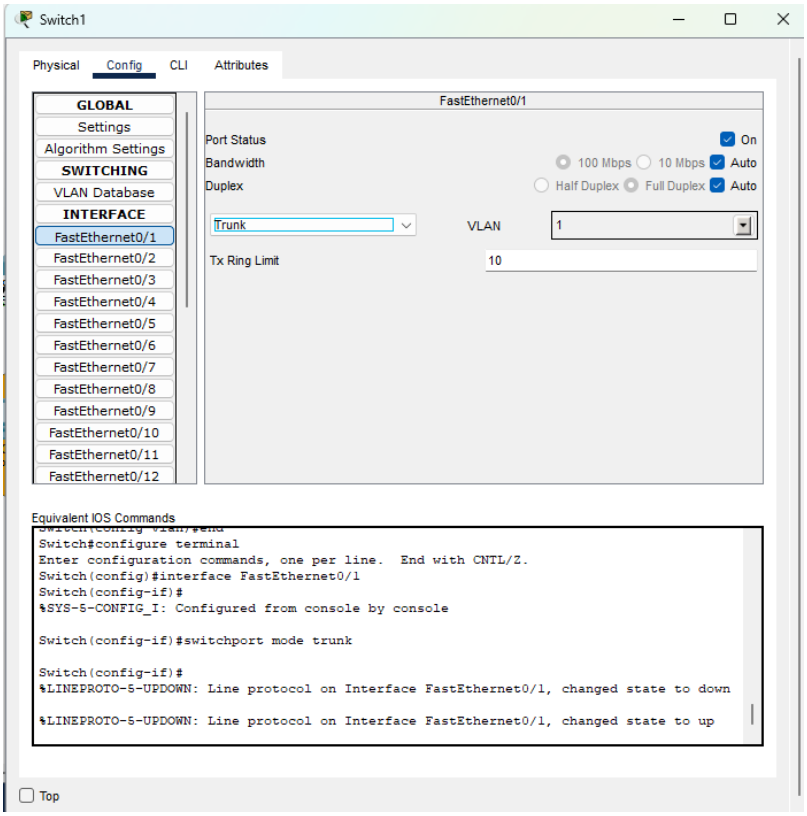


ix. Switch 1

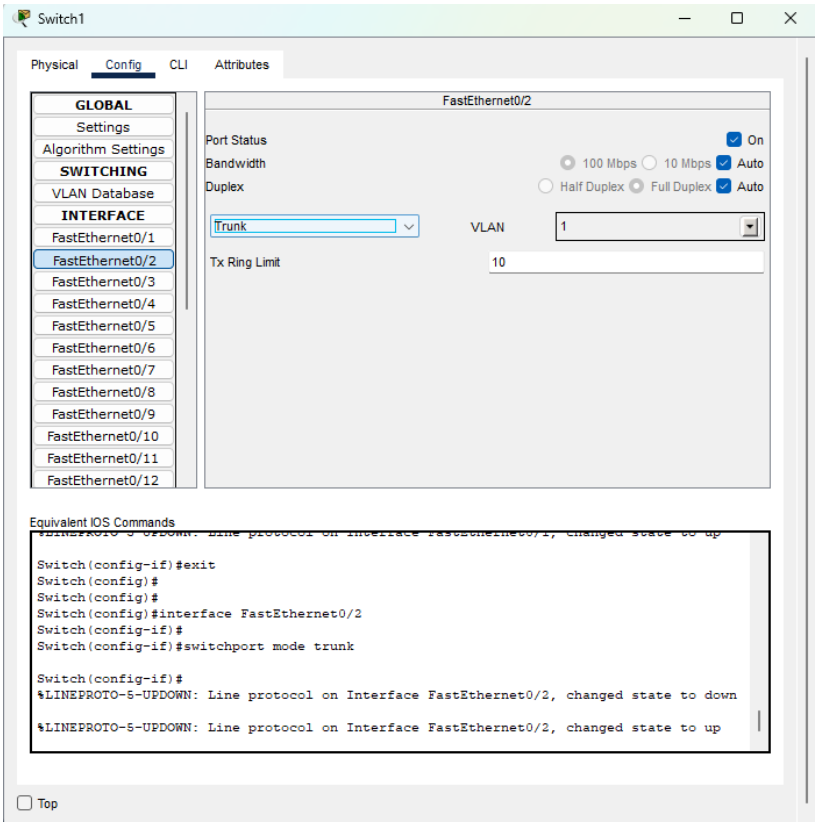
1. Vlans : Rectangle, circle, irregular



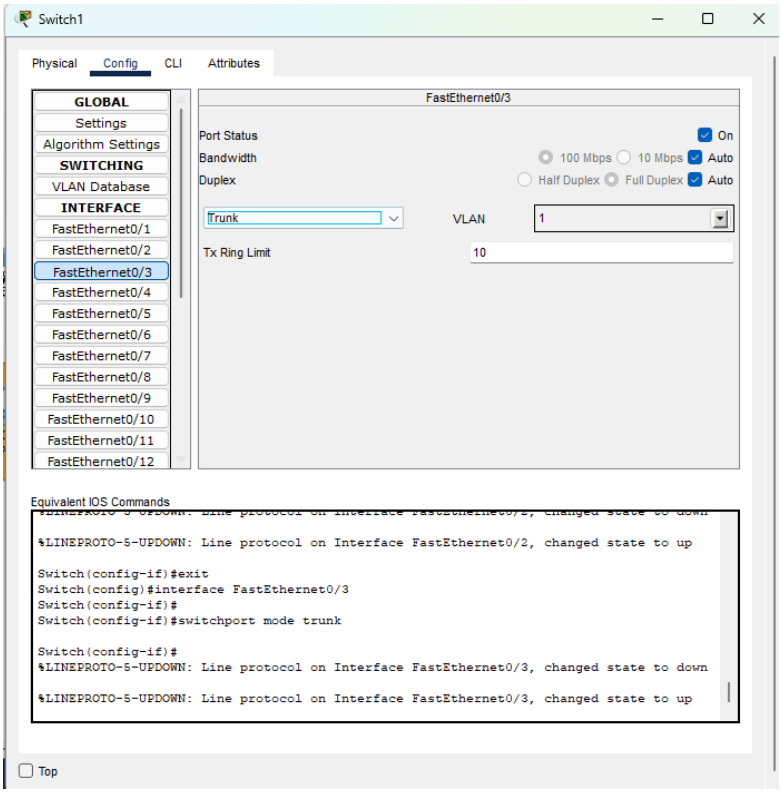
2. Fa0/1 Conexión switch



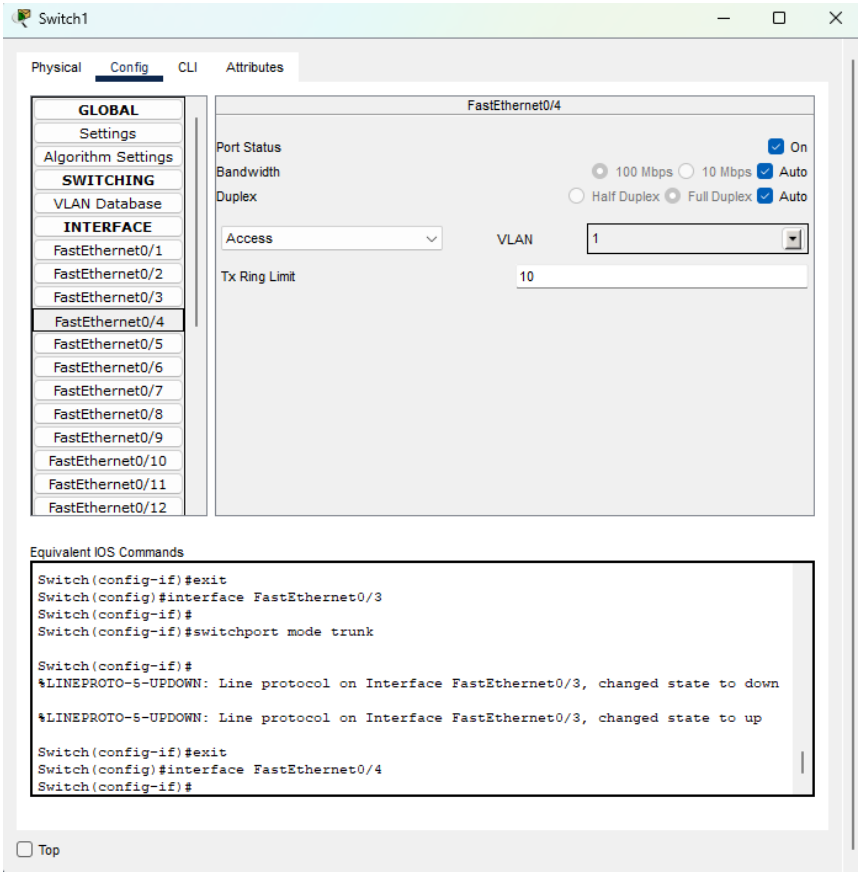
3. Fa0/2 conexión switch



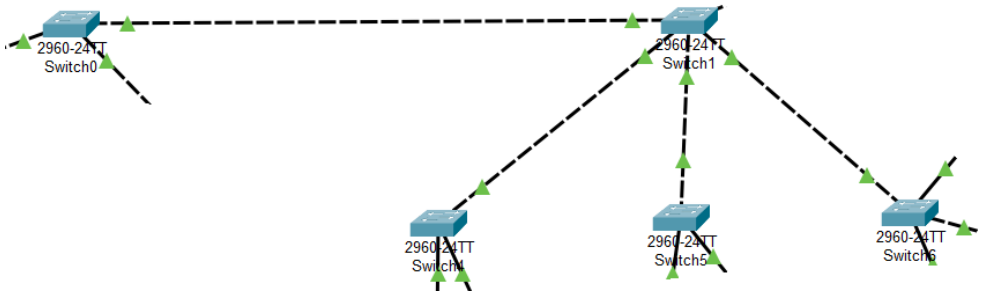
4. Fa0/3 conexión switch



5. Fa0/4 conexión switch

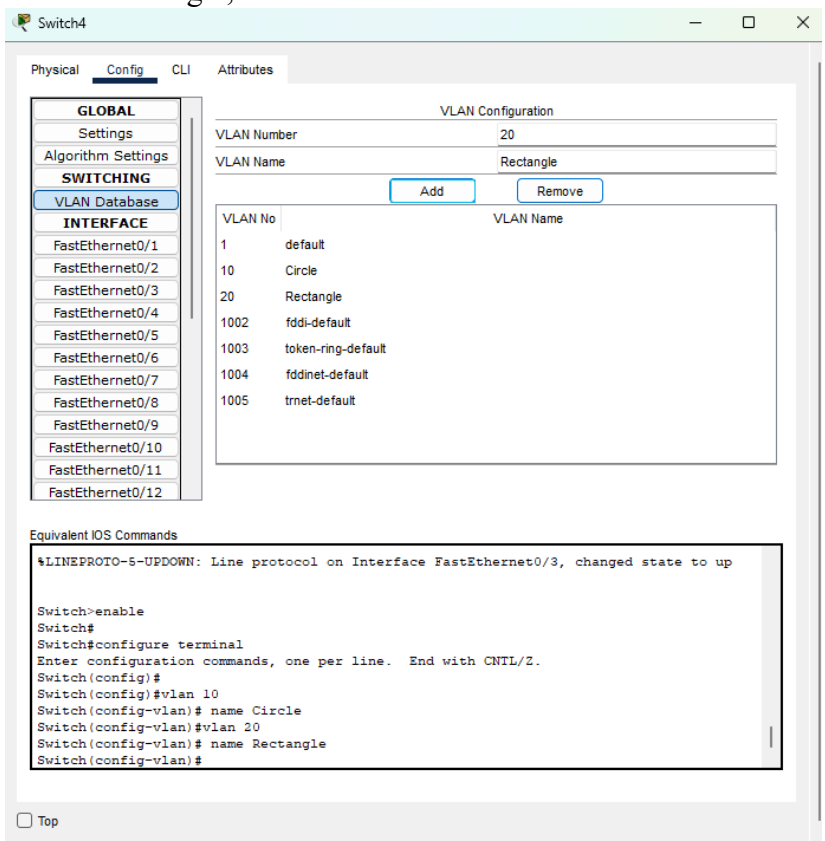


6. Configuración realizada

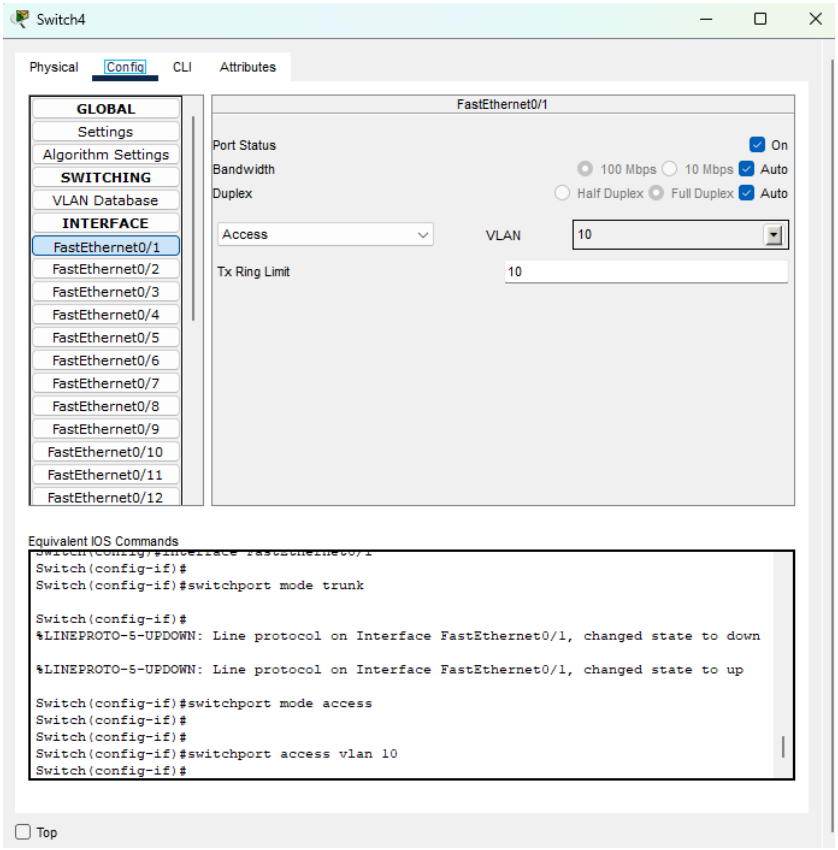


x. Switch 4

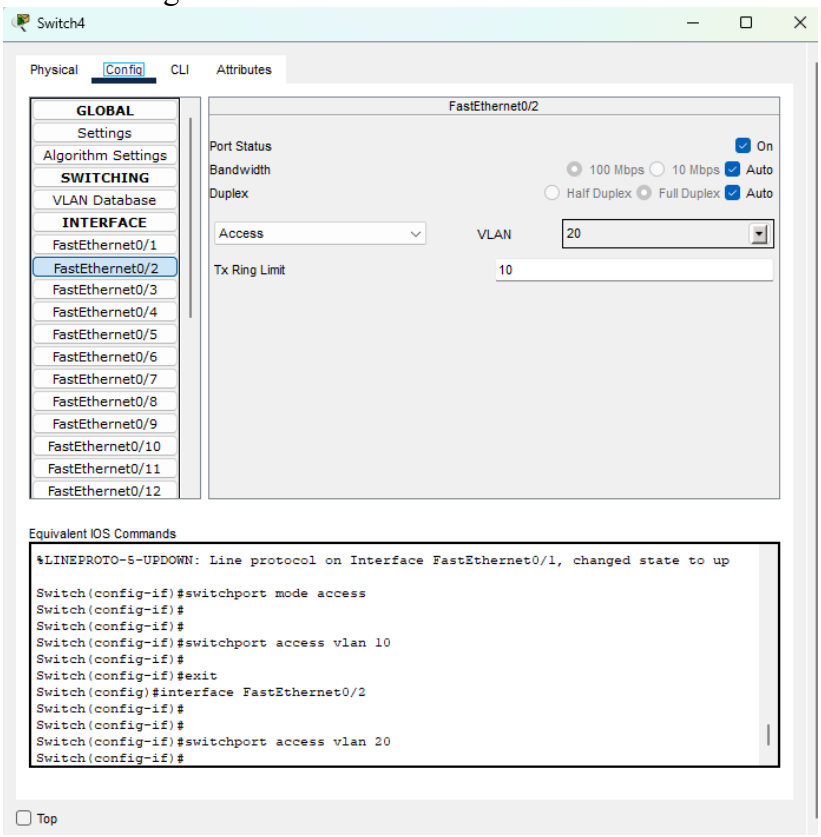
1. Vlans: Rectangle, circle



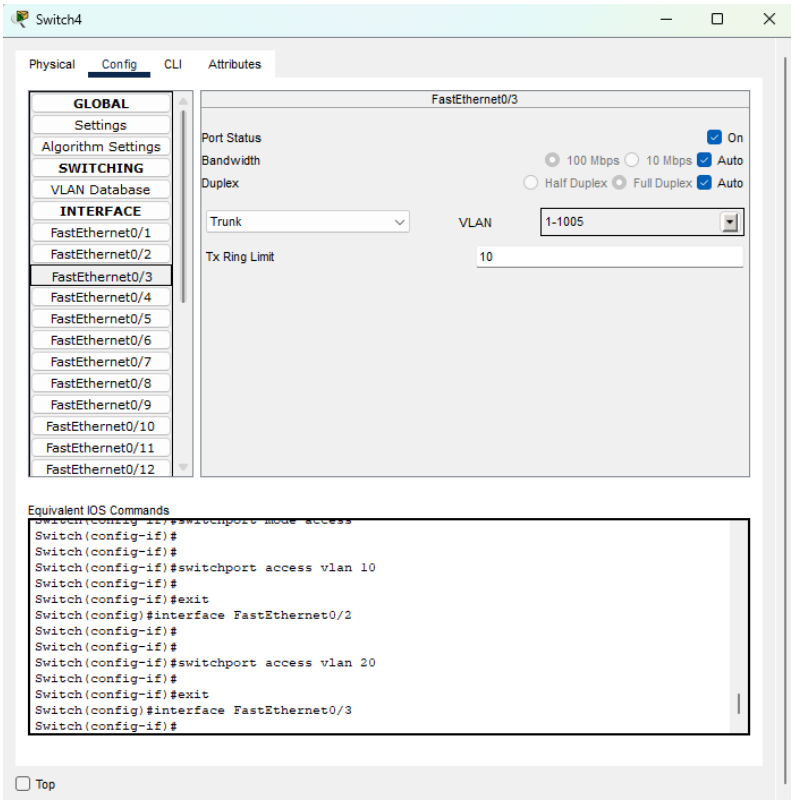
2. Fa0/1 Circle-> morado



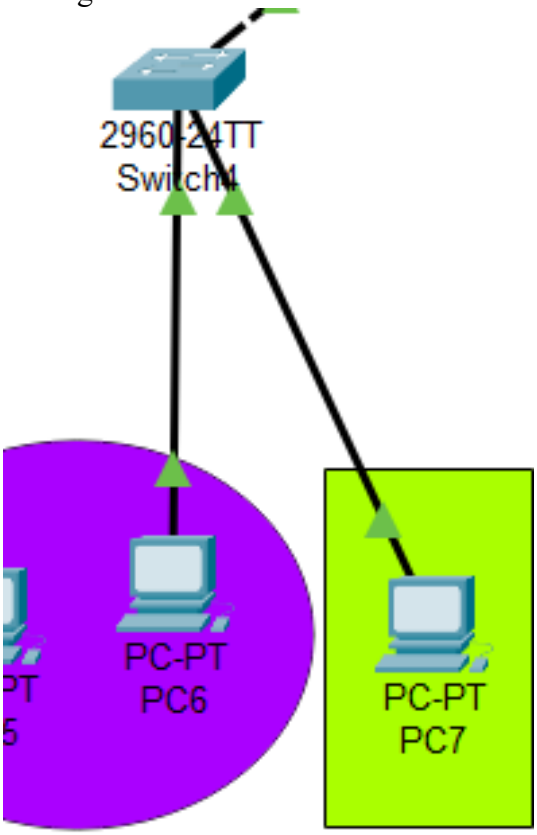
3. Fa0/2 rectangle-> verde



4. Fa0/3 conexión switch

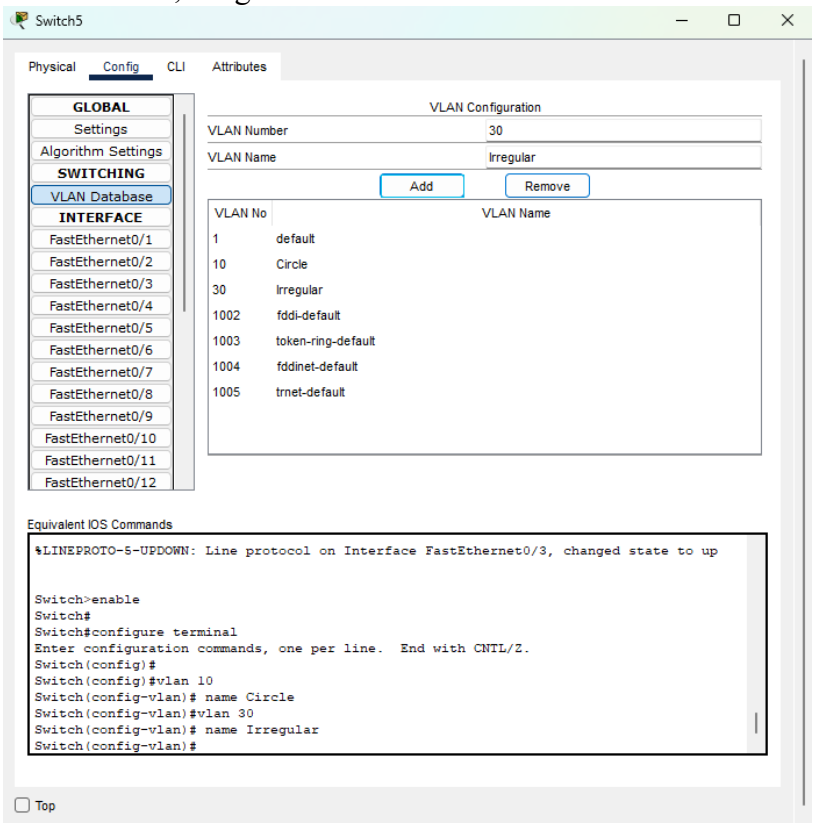


5. Configuración realizada:

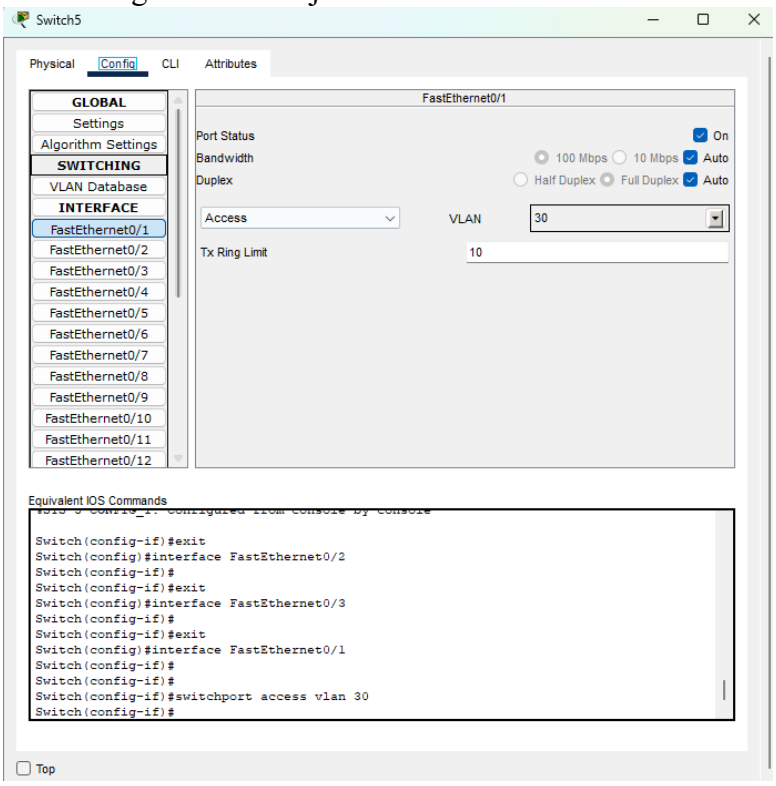


xi. Switch 5

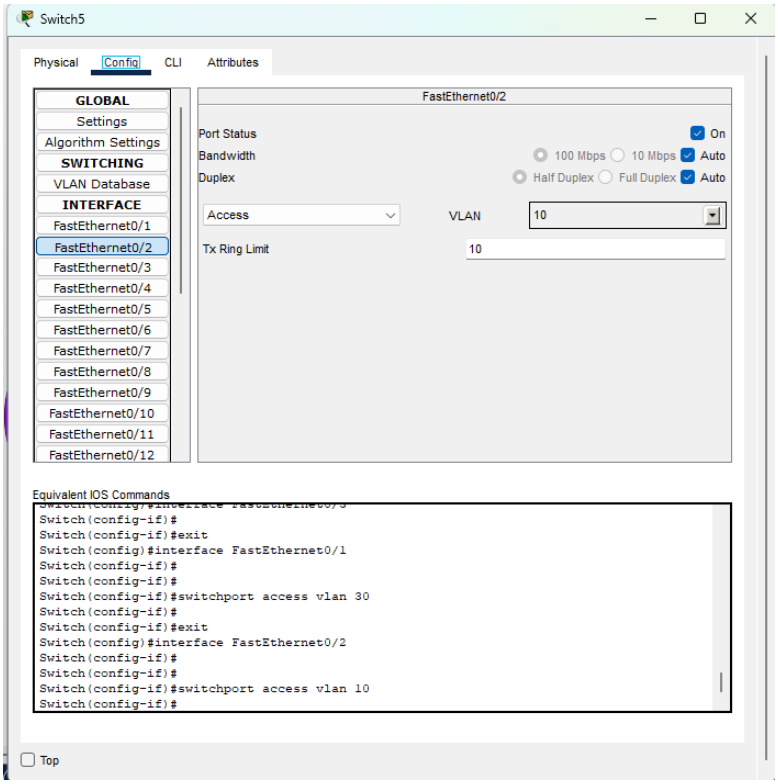
1. Vlans: Circle, irregular



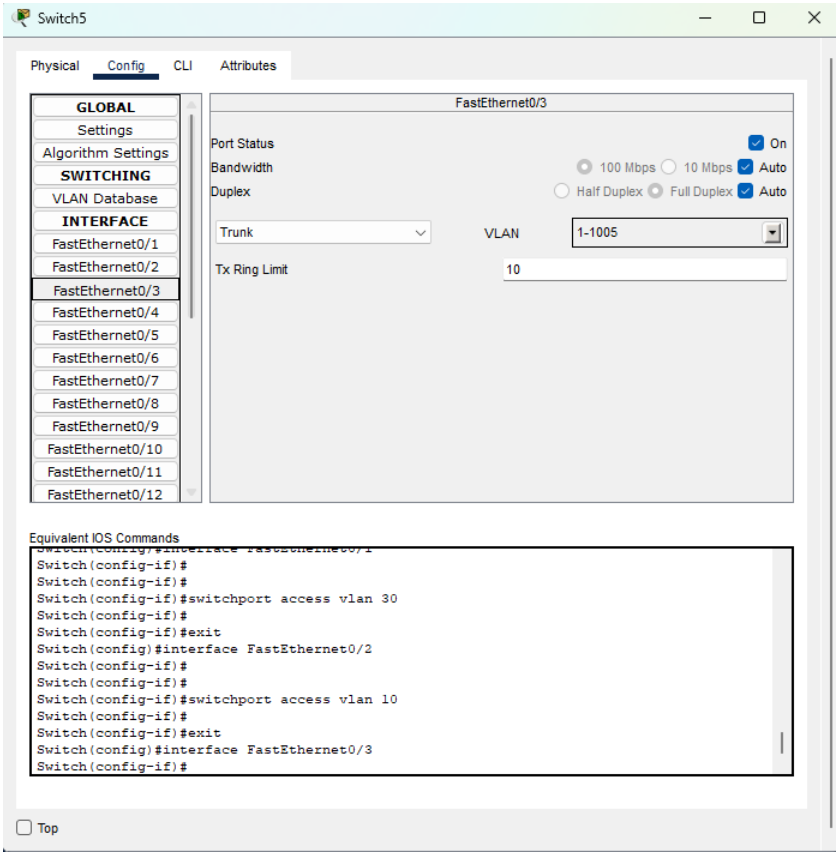
2. Fa0/1 Irregular-> Naranja



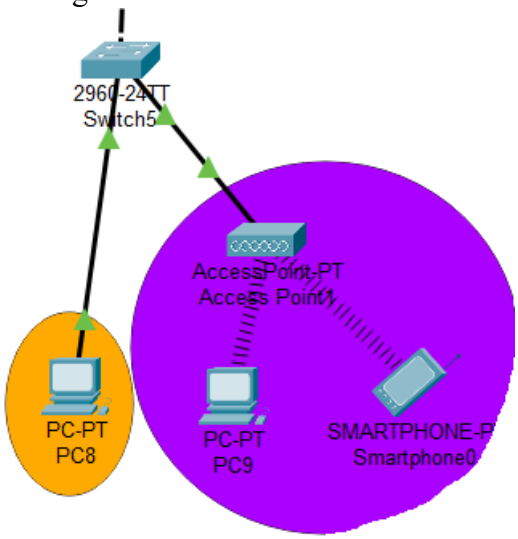
3. Fa0/2 Circle-> morado



4. Fa0/3 Conexión switch

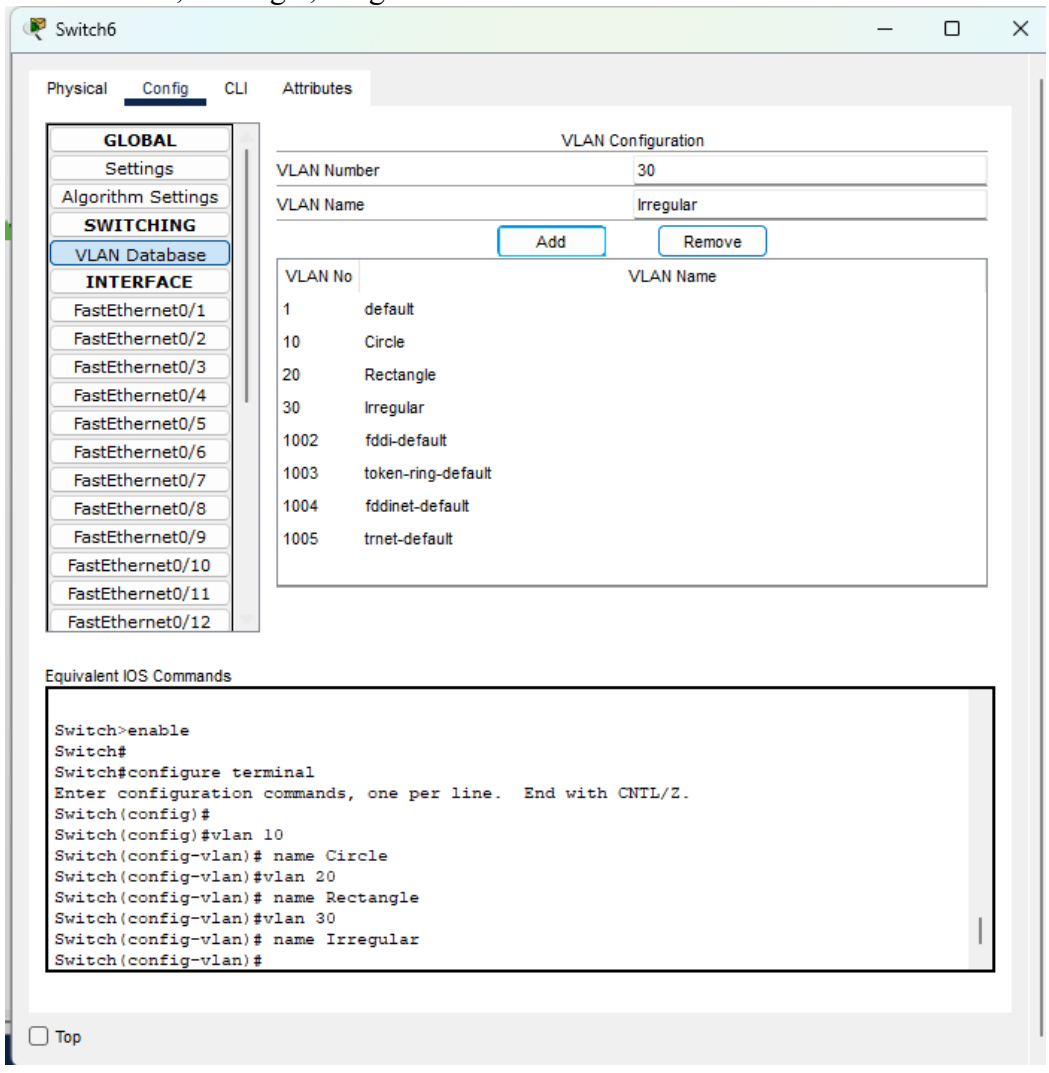


5. Configuración realizada

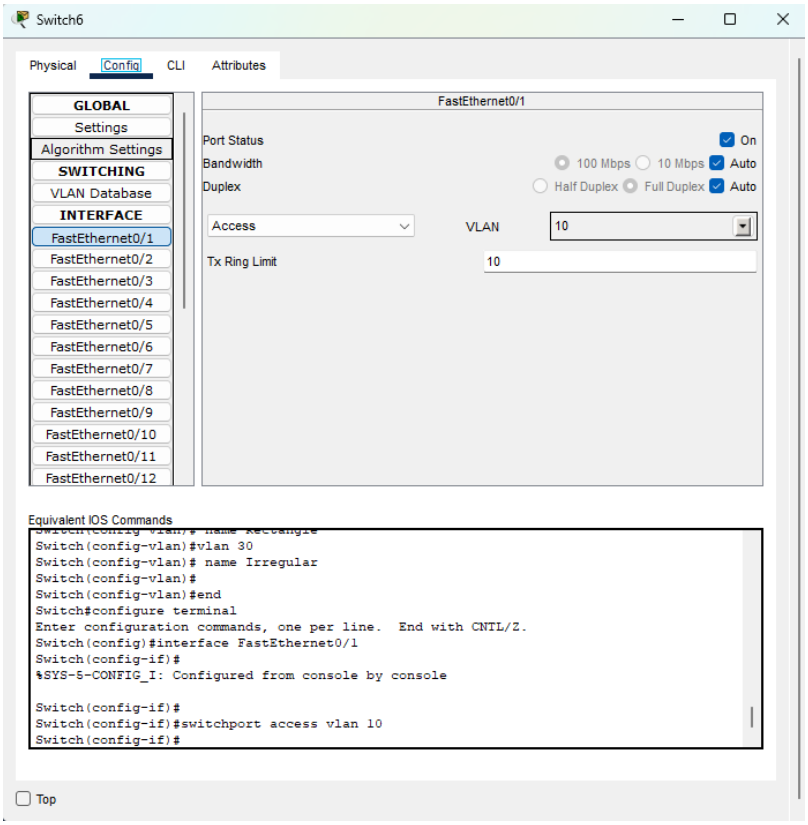


xii. Switch 6

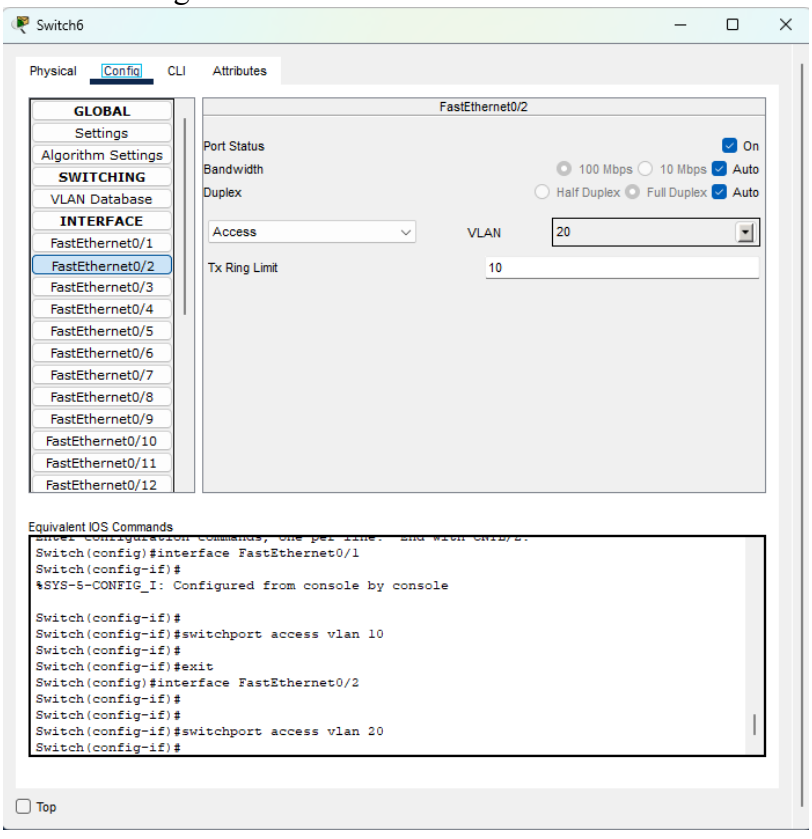
1. Vlans: Circle, rectangle, irregular



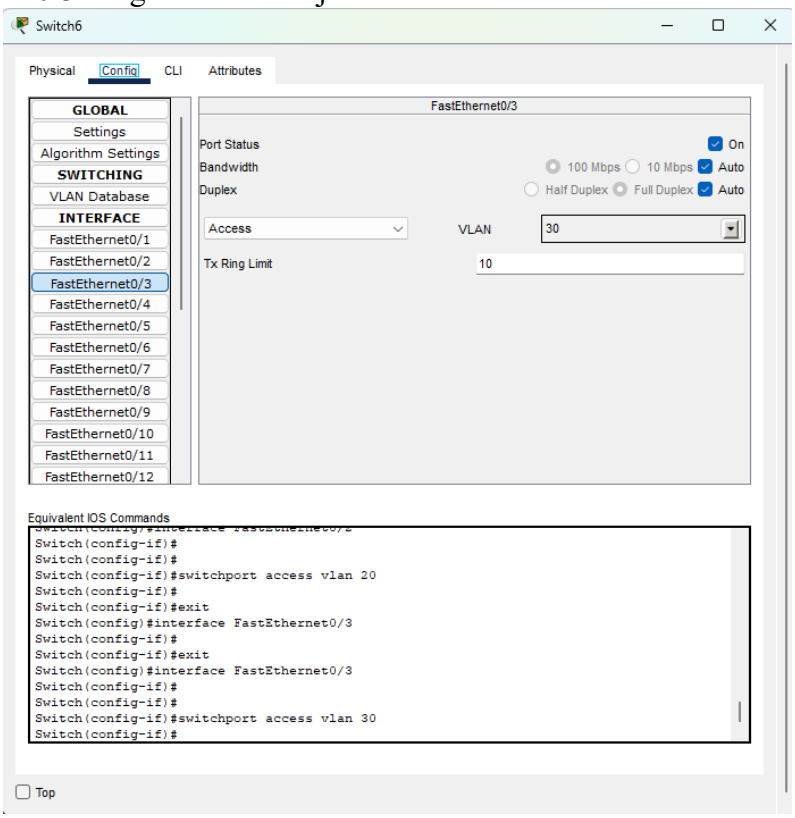
2. Fa0/1 Circle -> morado



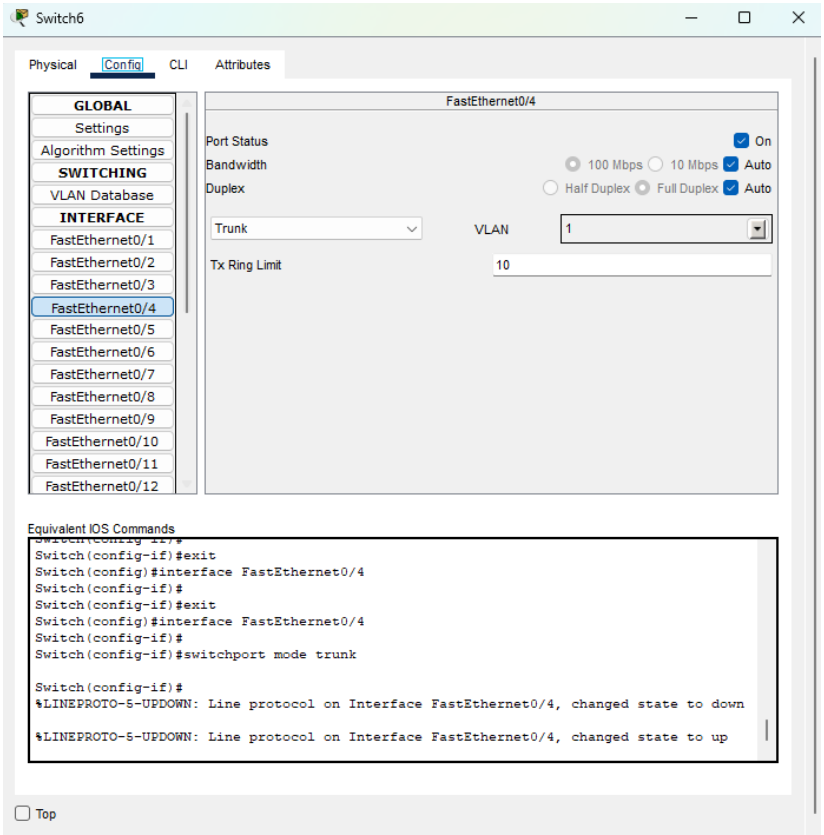
3. Fa0/2 Rectangle-> verde



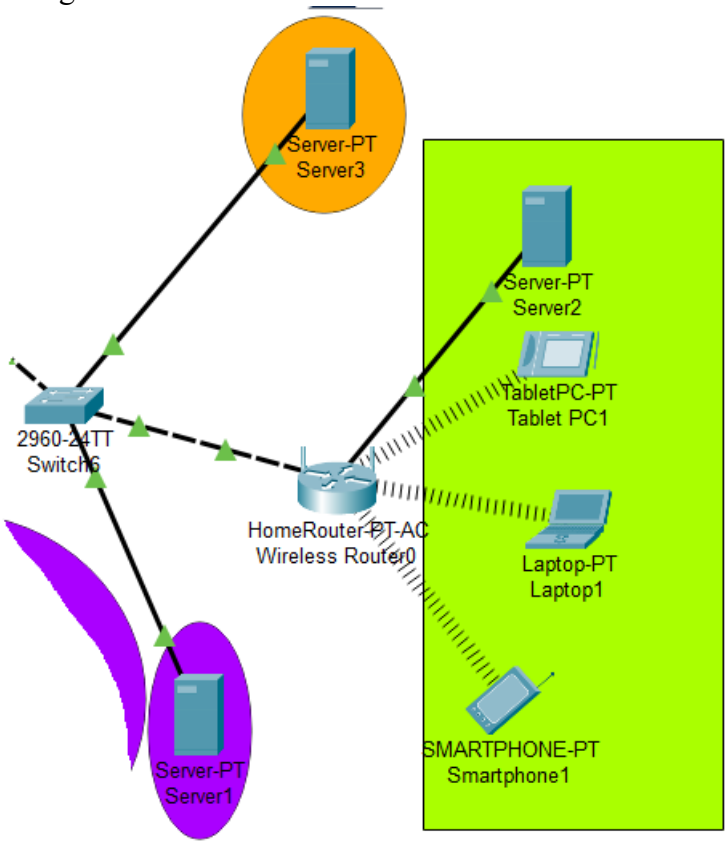
4. Fa0/3 irregular -> Naranja



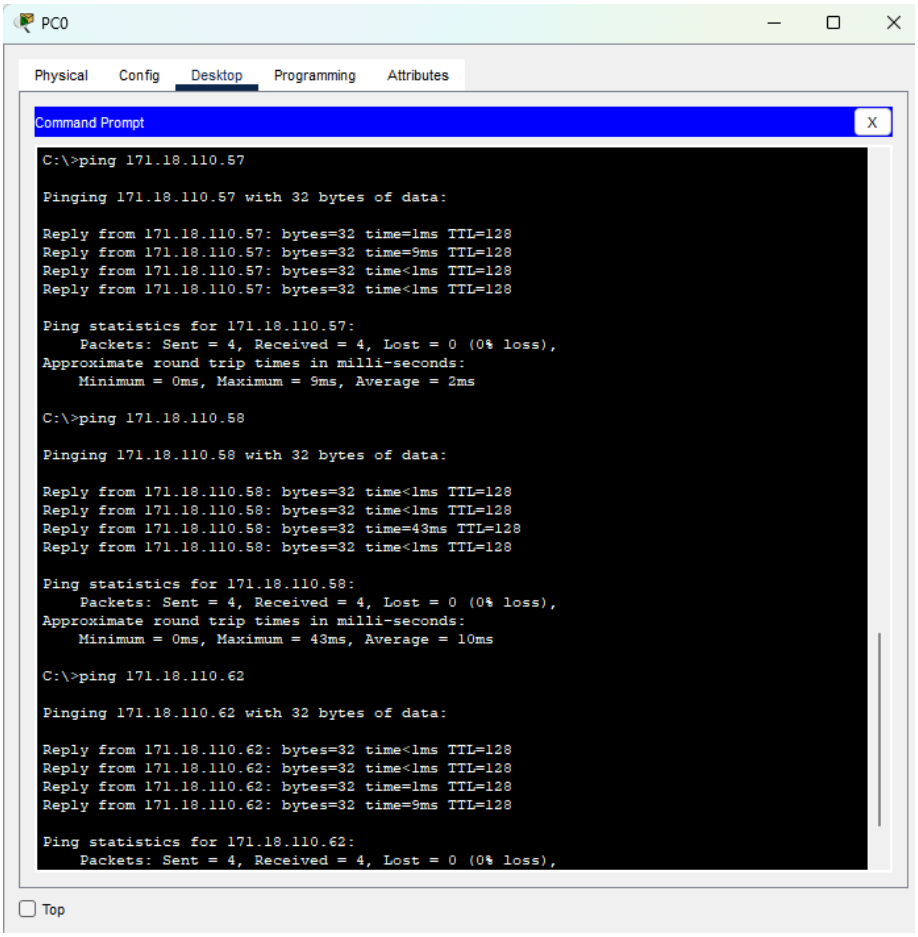
5. Fa0/4 conexión switch



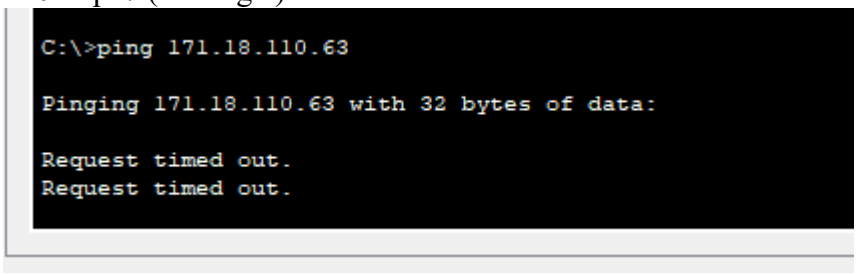
6. Configuración realizada



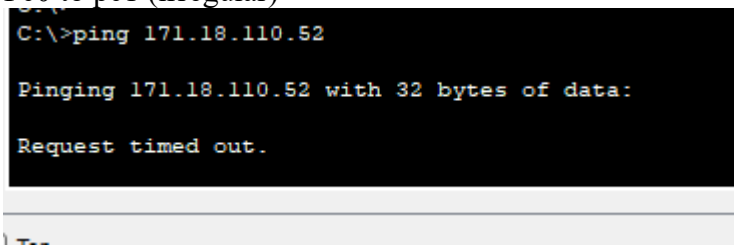
e. Verify that the network operates as expected according to the configured VLANs.
   i. Ahora realizamos pruebas de conectividad utilizando el comando ping desde cada VLAN. La primera prueba consiste en hacer ping a dispositivos que están dentro de la misma VLAN.
   ii. Las pruebas 2 y 3 se realizan hacia dispositivos que pertenecen a VLANs diferentes, y generan un "Request timed out", ya que por defecto, las VLANs no permiten comunicación entre sí sin la configuración de un router o un dispositivo capa 3.
   iii. Circle
      1. Pc0 to pc5, pc6, server 1 (circle)



2. Pc0 to pc7 (rectangle)

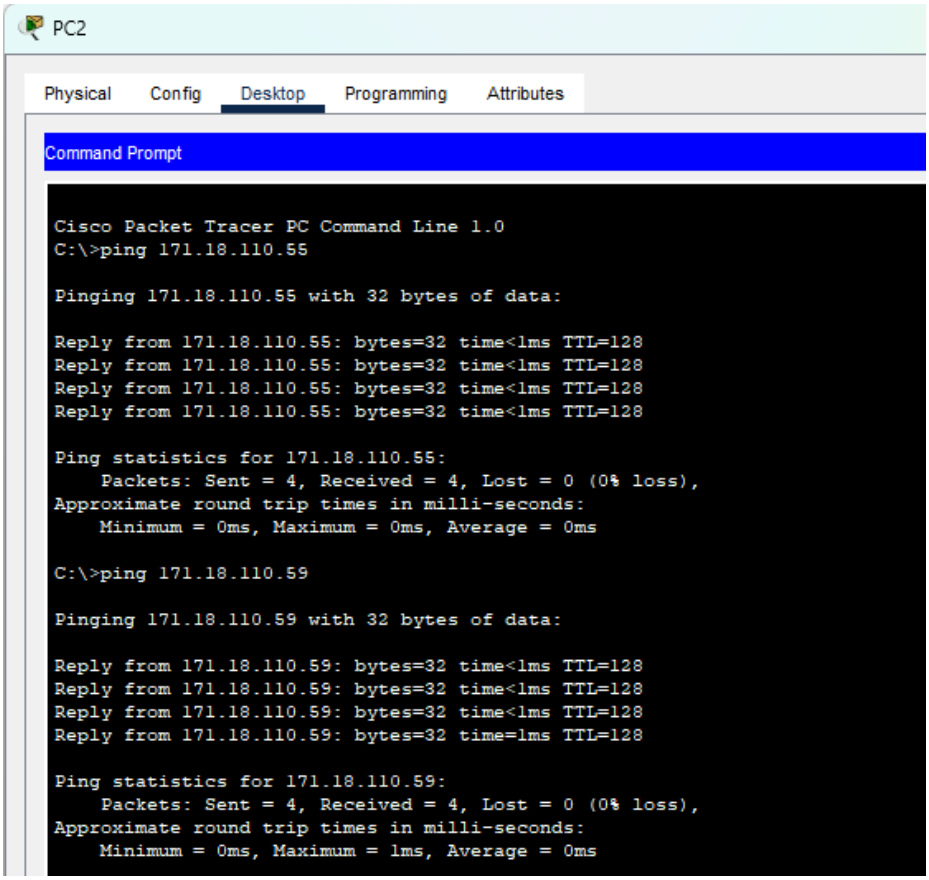


3. Pc0 to pc1 (irregular)



iv. Rectangle

1. Pc2 to server 0, pc7 (rectangle)



2. Pc2 to pc1 (irregular)

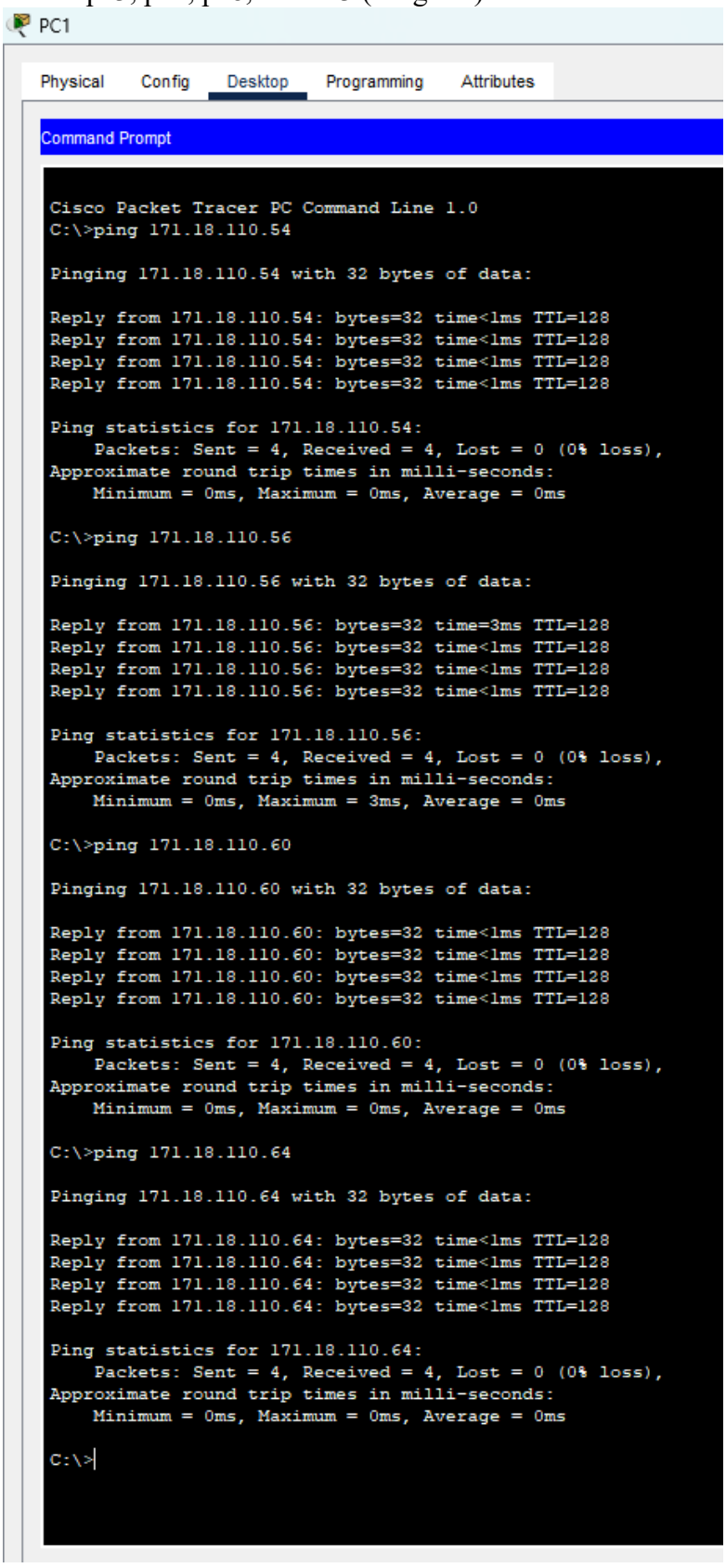
```
C:\>ping 171.18.110.51

Pinging 171.18.110.51 with 32 bytes of data:

Request timed out.

Ping statistics for 171.18.110.51:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
```

3. Pc2 to pc0 (circle)

```
C:\>ping 171.18.110.50

Pinging 171.18.110.50 with 32 bytes of data:

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

Ping statistics for 171.18.110.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
```

v. Irregular

1. Pc1 to pc3, pc4, pc8, server 3 (irregular)



2. Pc1 to pc2 (rectangle)

```
C:\>ping 171.18.110.53

Pinging 171.18.110.53 with 32 bytes of data:

Request timed out.
```

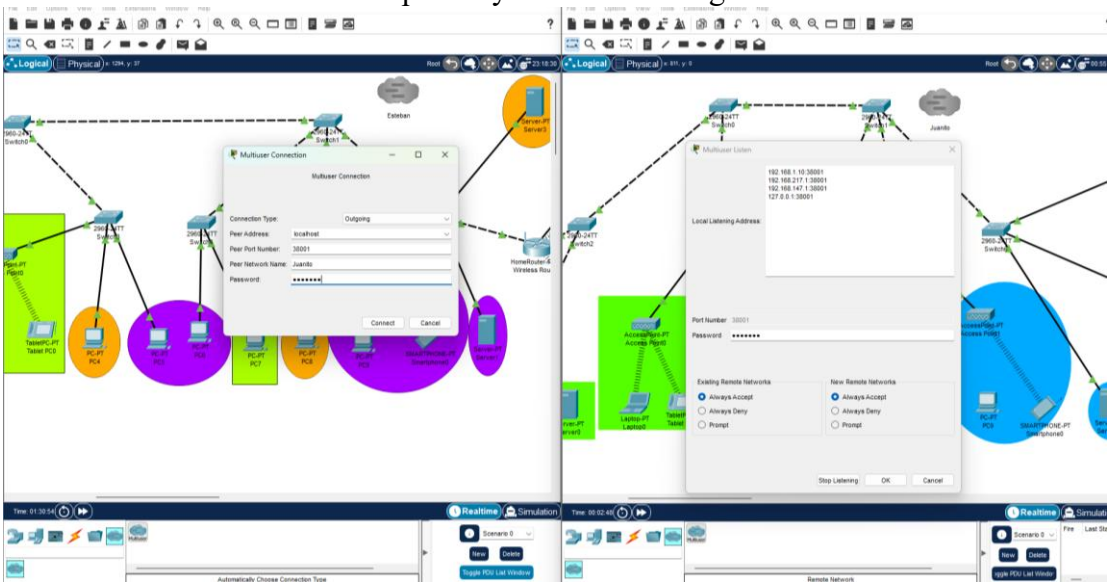
3. Pc1 to pc0 (circle)

```
C:\>ping 171.18.110.51

Pinging 171.18.110.51 with 32 bytes of data:

Request timed out.

Ping statistics for 171.18.110.51:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
```

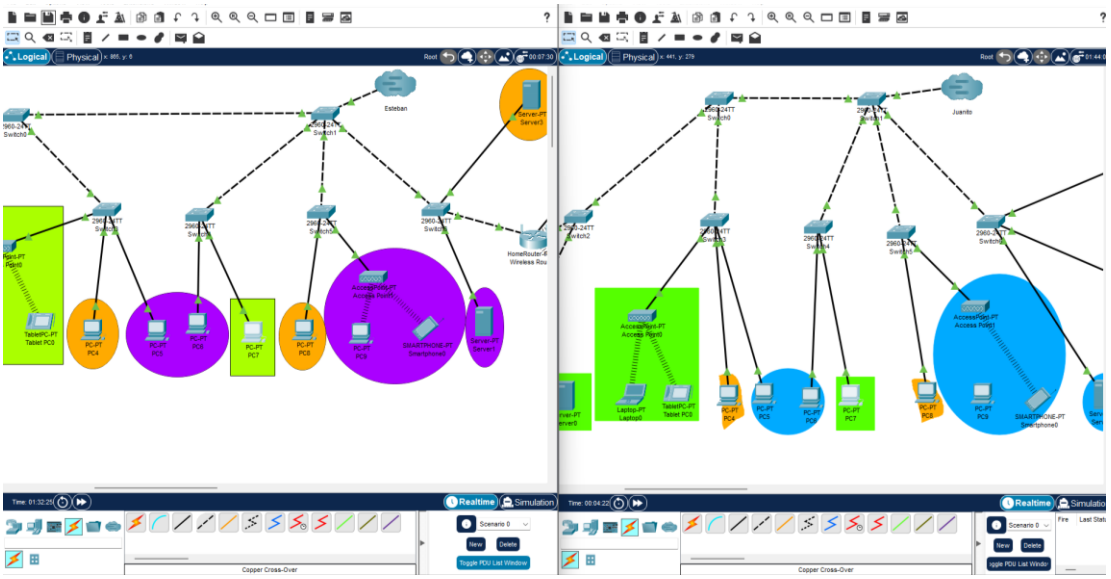
f. Merge the project files with team members. For groups of 1 student, request a project file from another group member (e.g., Student2 or Student3) and interconnect their setup with yours. Indicate who provided the project file

i. Conectamos los archivos del Student 1 (Esteban) con el Student 2 (Juanito) mediante la opción multiuser en ambos archivos.

ii. Una vez agregados, en un archivo agregamos la contraseña y activamos las opciones always accept en ambos apartados mientras que en el otro activamos la función incoming, colocamos el nombre de la multiuser del otro archivo con su numero de puerto y contraseñas asignadas



iii. Agregamos los links a las nubes y esperamos que se genere la conexión (verde)



6. WiFi

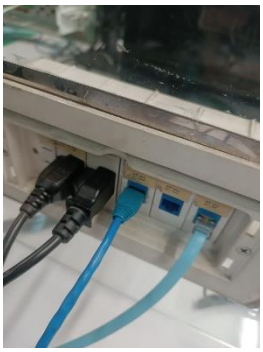
In the same groups, complete the following setup.

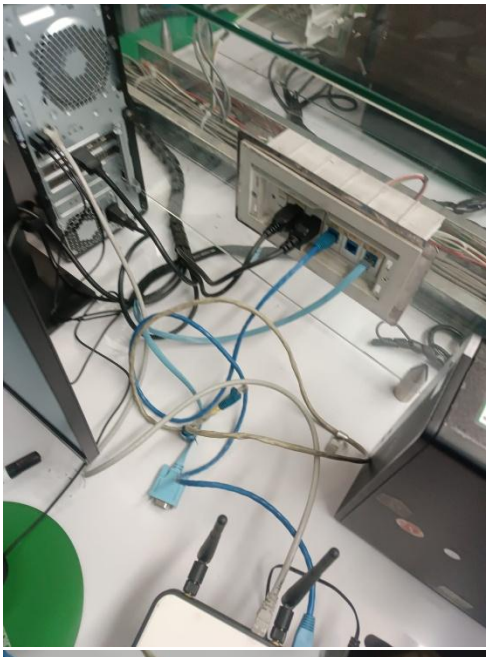
Each group must configure a wireless router using the computers that were disconnected. The routers will be configured via web; refer to the router manual online for instructions on how to connect and configure it

Use the IP configuration of the computer you disconnected to configure the Internet port of each wireless router. This will allow all devices connected to the wireless routers to have internet access.

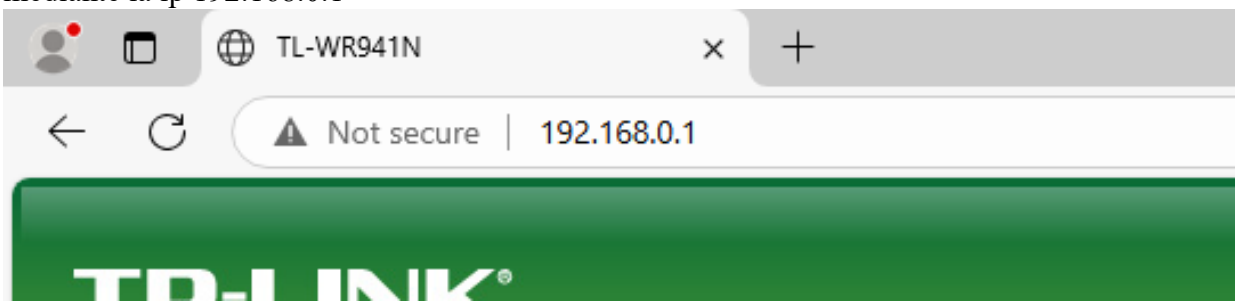
- Conectamos el router y la maquina con la cual lo vamos a configurar (parte física)
- Debe haber dos conexiones.
    - Router en el puerto Ethernet hacia el puerto de internet de la universidad (cable azul)

    - Router en cualquier puerto FastEthernet hacia la maquina



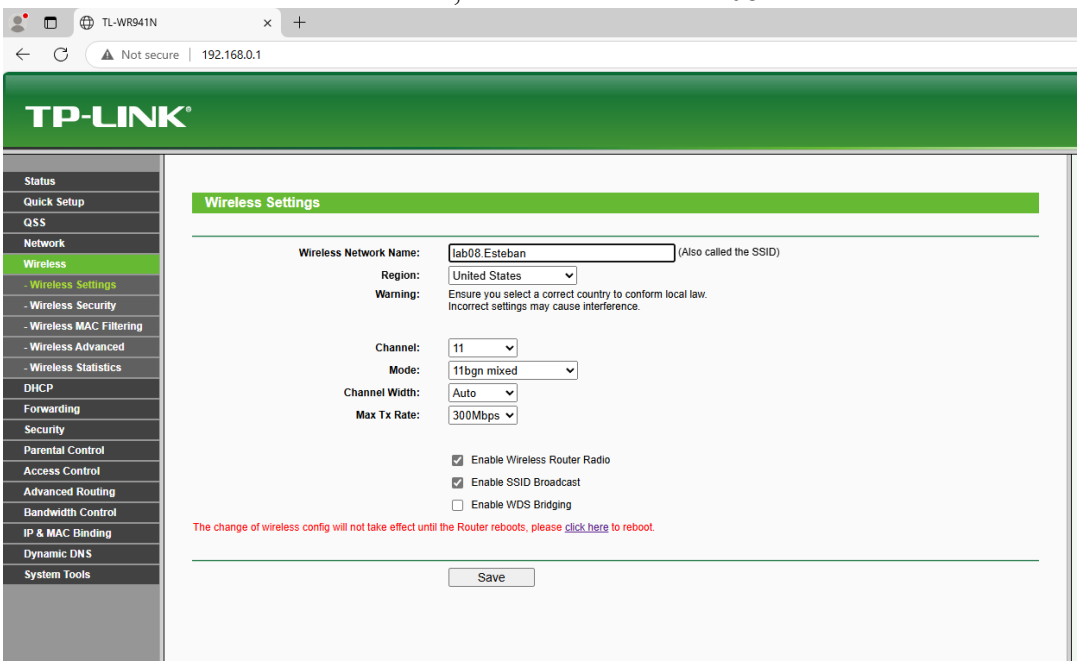


- Ya conectado el router accedemos a la configuración de este a través de un navegador mediante la ip 192.168.0.1

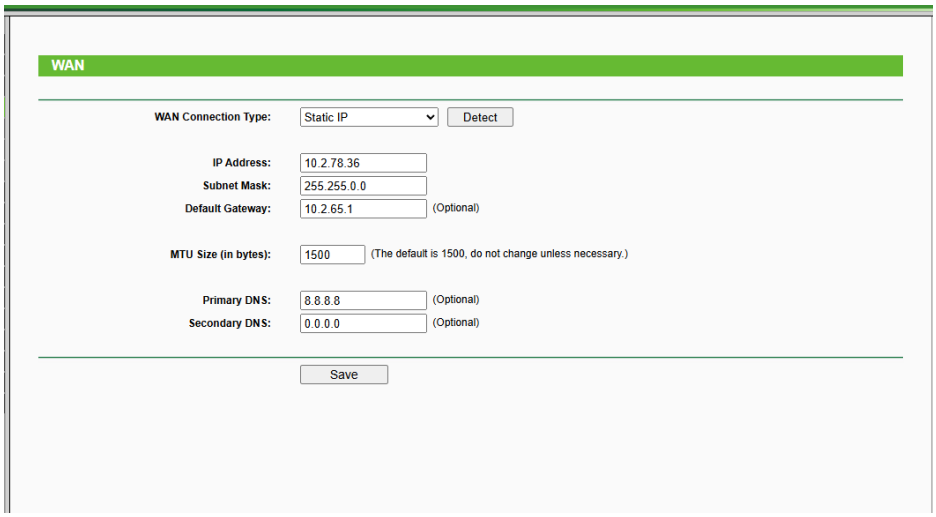


Configure the wireless network as follows:

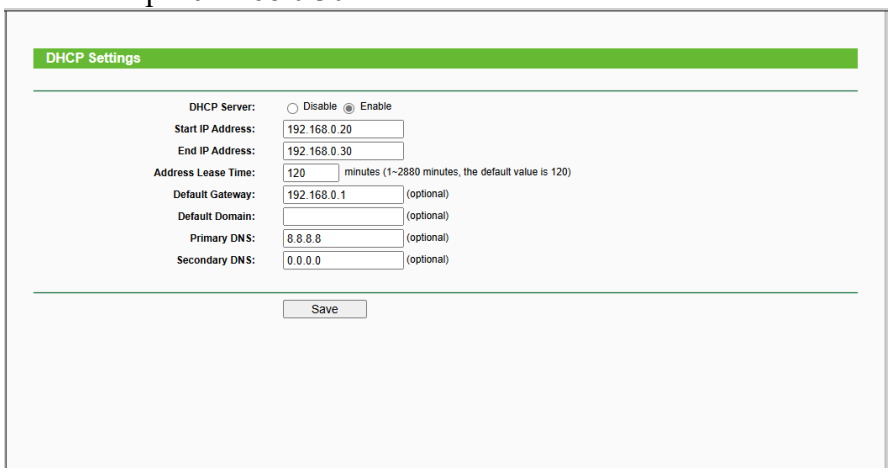
a. Wireless network identifier - SSID: Lab8 ape (where ape is the last name of one of the group members).
   i. Ingresamos en el apartado de Wireless Network y en la sección Wireless Network Name colocamos el SSID, en este caso será lab08.esteban



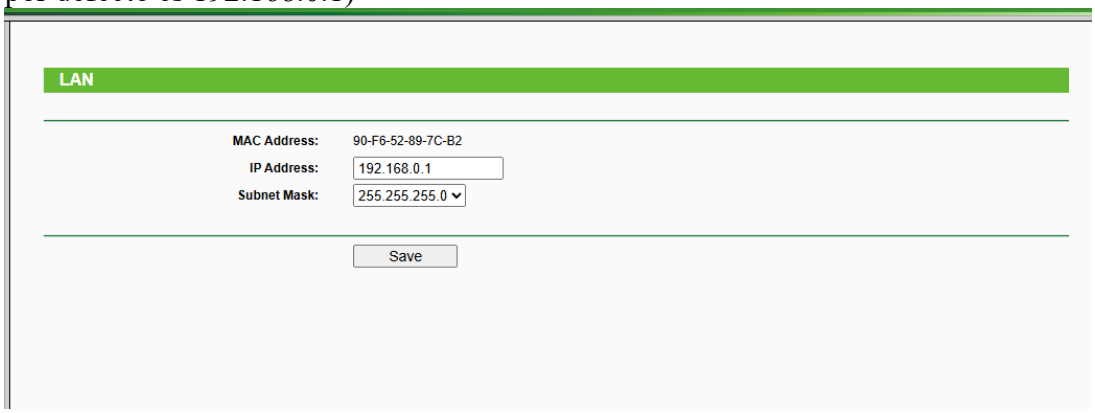
b. Wireless router IP address (wireless interface): 192.168.0.1
   i. Ya que el router no detecta automáticamente la ip de la cual debe tomar la red, configuramos una ip estática
   ii. La ip estática tendrá una de las direcciones asignadas al inicio del semestre (en este caso tomaremos 10.2.78.36) para que posteriormente el router tome esta red y la reparta entre los diferentes dispositivos conectados a este



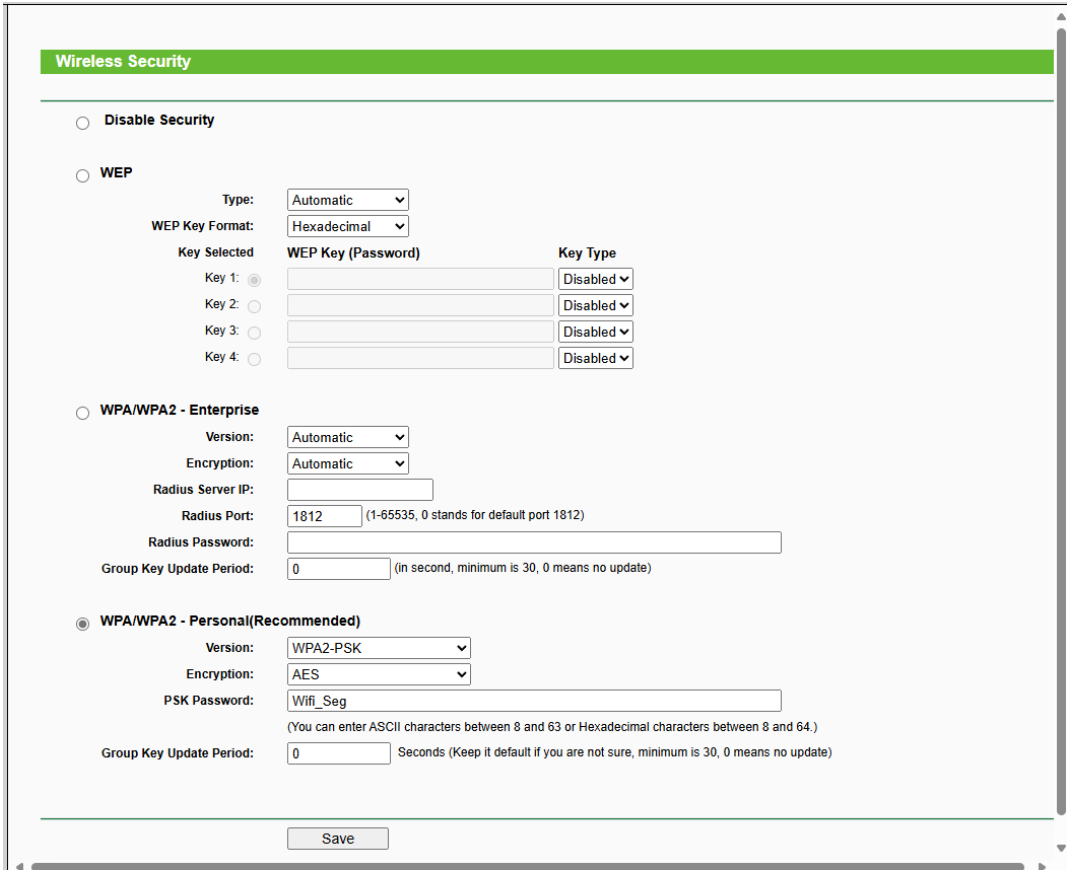
c. IP address range for mobile devices (DHCP): 192.168.0.20 to 192.168.0.30
    i. En el apartado DHCP ingresamos los rangos de las IP
        1. Start ip : 192.168.0.20
        2. End ip: 192.168.0.30



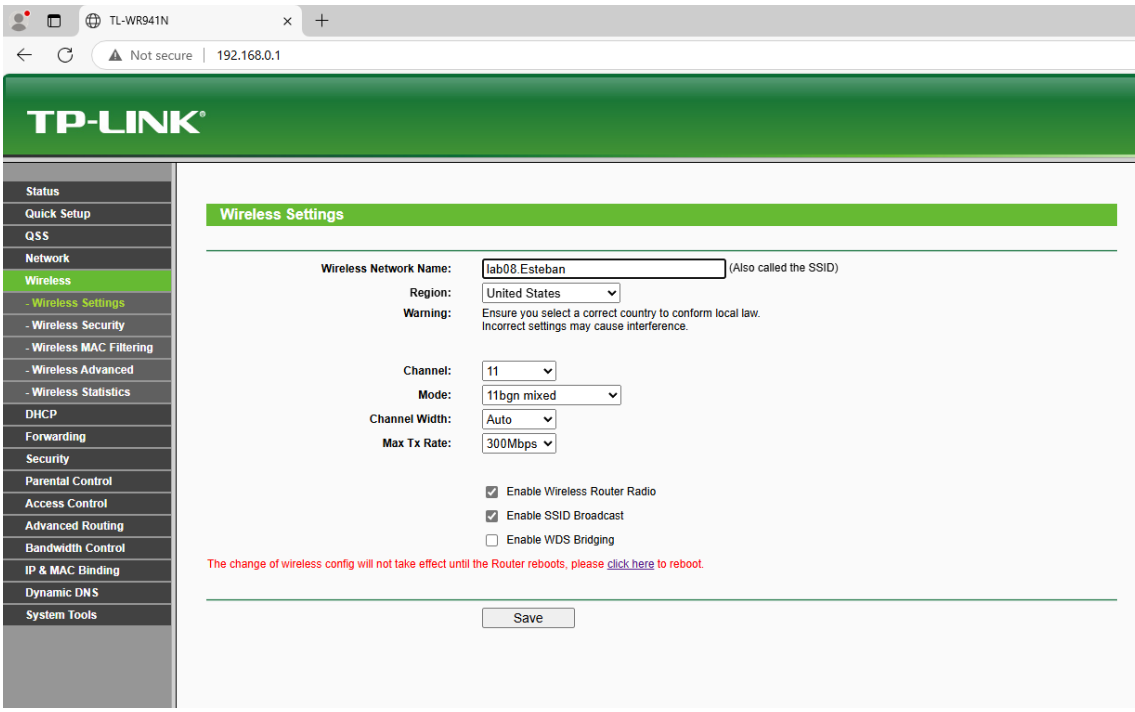
d. Towards the wired LAN: Use the IP address of the computer you disconnected to connect the wireless router.
    i. Ahora ingresamos en el apartado de lan e ingresamos la ip de nuestro computador (la ip por defecto es 192.168.0.1)



e. Access mechanism for wireless clients: WPA2-PSK with AES.
f. Router access password for mobile devices: WiFi Seg.
    i. En el apartado de Wireless Security seleccionamos la opción WPA2 - Personal donde agregamos la versión WPA2-PSK, encriptado AES y contraseña Wifi_Seg



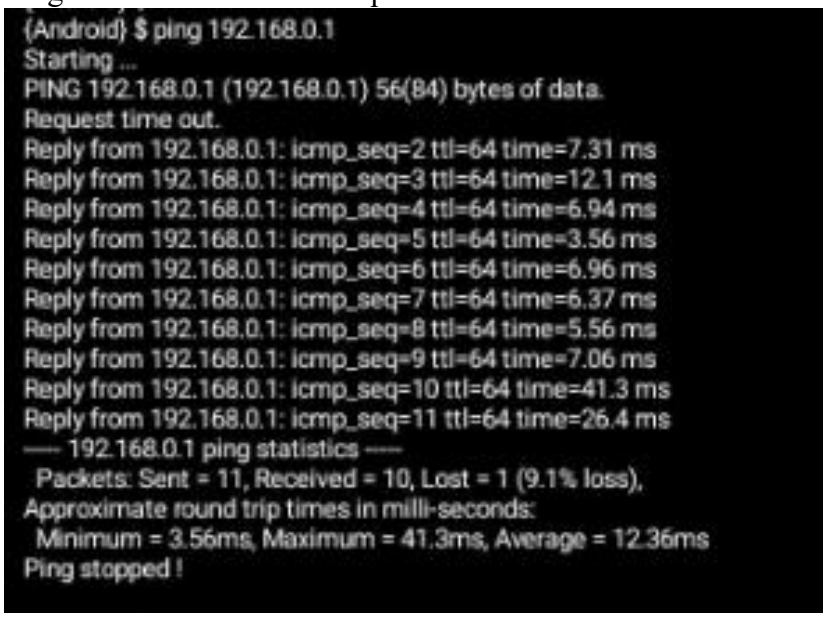
g. Change the default channel and assign a different one. Ensure that both devices do not use the same channel.
    i. En el momento que configuramos el SSID se eligió el canal 11



h. What channel options can be configured on each wireless router?
    i. Los canales que pueden ser configurados van del 1 al 11

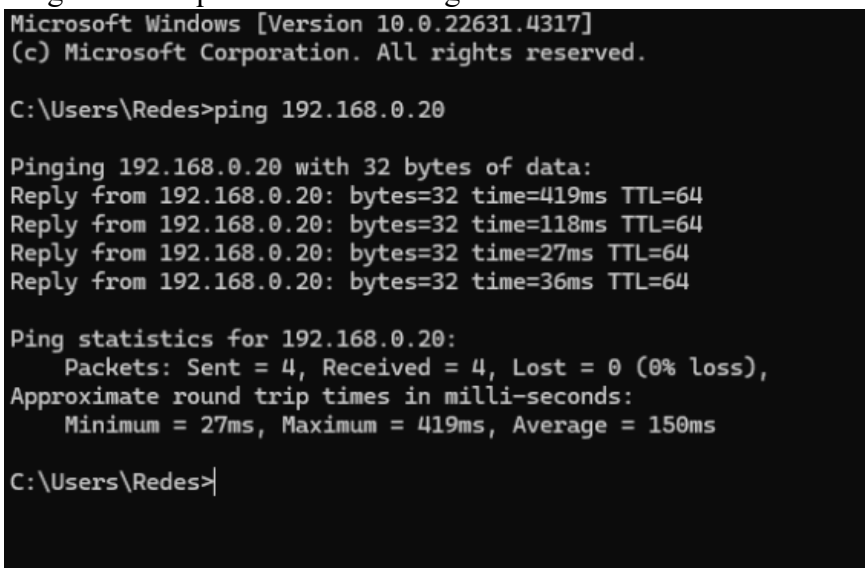
i. Perform the following test using a smartphone:
    i. Disable your mobile data plan and enable WiFi
    ii. Connect the smartphone to the wireless router you just configured.
    iii. Browse the internet using the smartphone.
    iv. Install an app that allows you to execute the ping command and perform operation tests

j. Test the connection between devices in the diagram and devices on the internet. Use the ping command between devices.
    i. Ping al router desde el smartphone



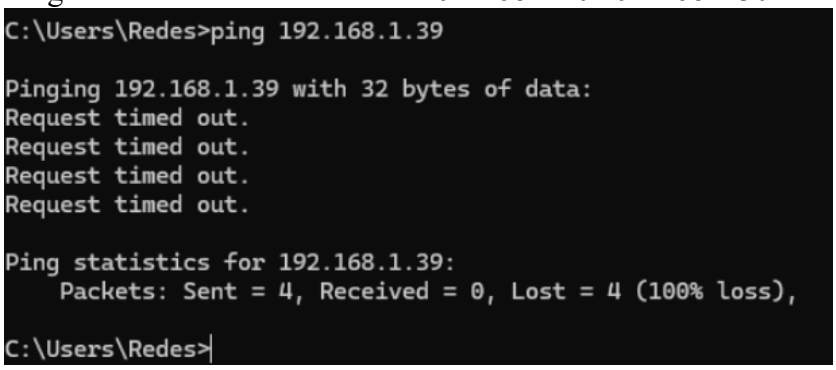
ii. Ping a google desde el smartphone

iii. Ping a una maquina dentro del rango



k. Report which pings are successful and which are not.

i. Pings hacia otra red afuera de la 192.168.1.20-192.168.1.30

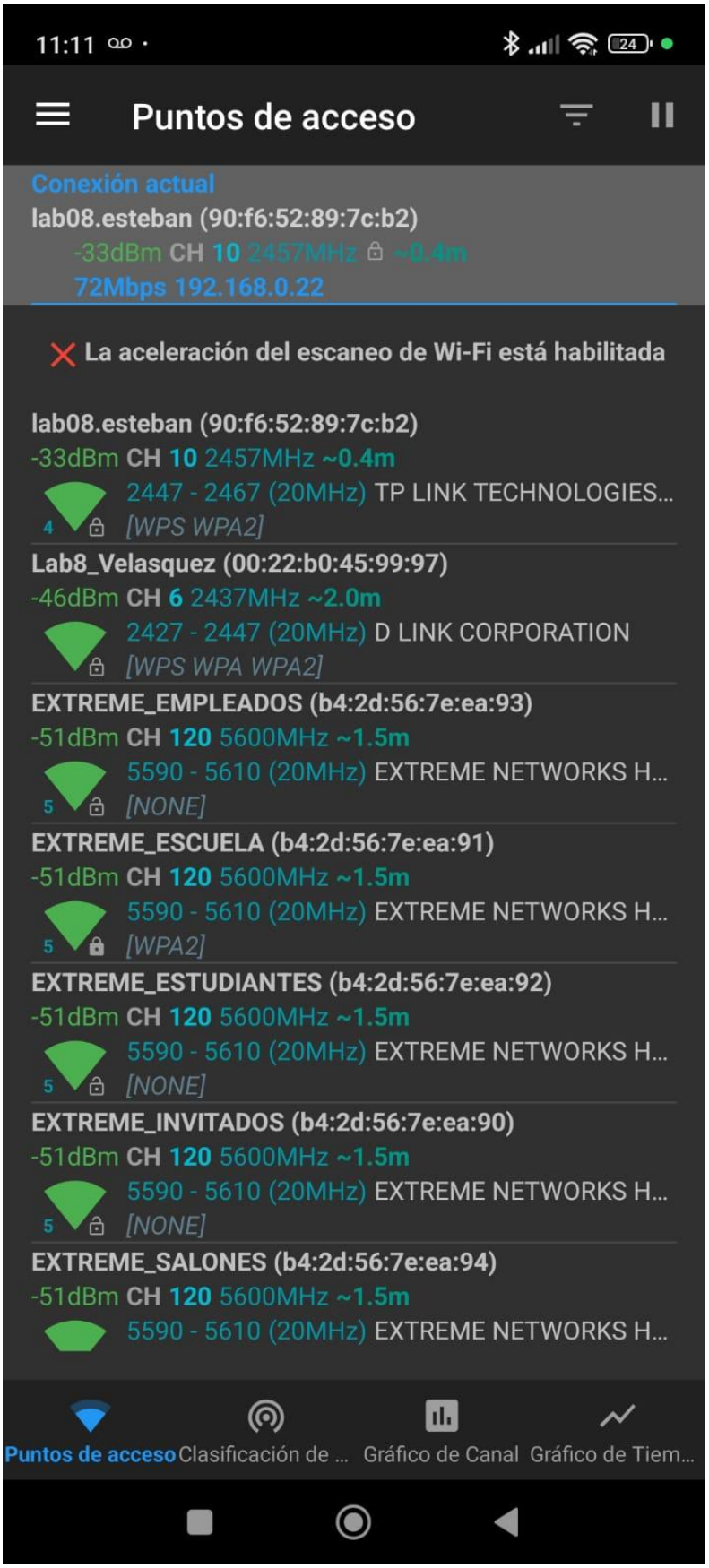


l. If not all pings are successful, explain why. (Hint: What is NAT?)

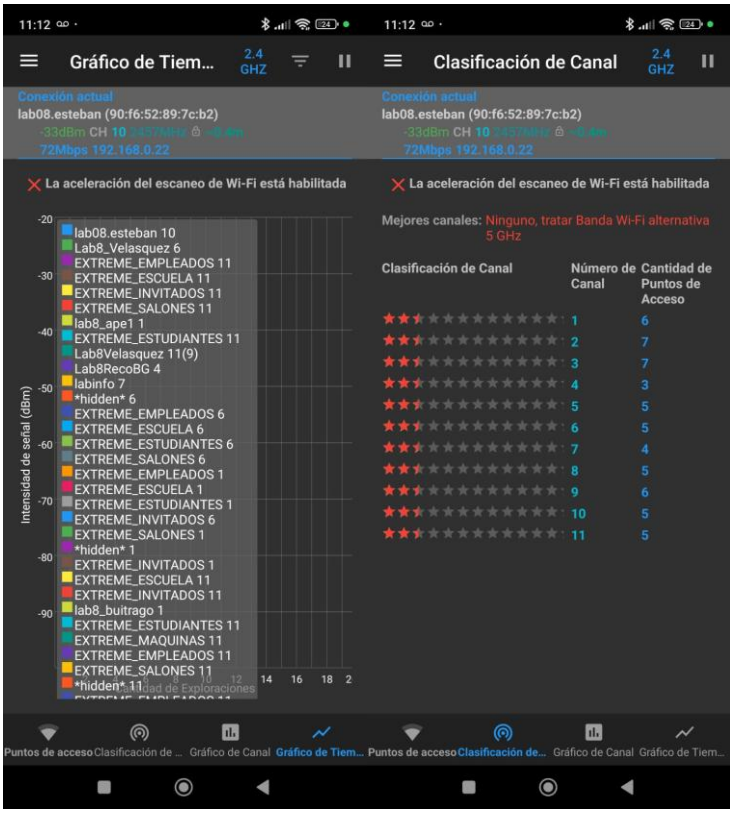
i. Some devices did not respond to ping due to the lack of NAT configuration. This allows devices within a

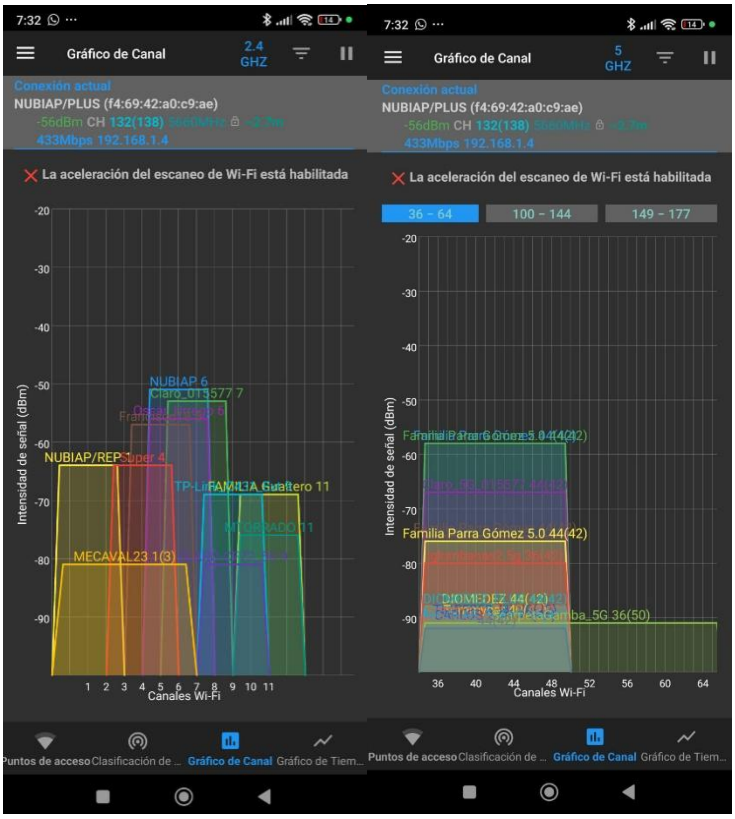
ii. private network (LAN) to communicate with devices on the Internet using a single public IP address assigned to the router

m. Using the smartphone, review active networks nearby using an app to monitor wireless traffic, such as WiFi Analyzer for Android. Discover wireless networks in the lab area, including your own and your classmates' networks. Also, check the channels they are using.
    i. We use WiFi Analyzer to capture the traffic of nearby Wi-Fi networks. We can observe our wireless network and the university's networks

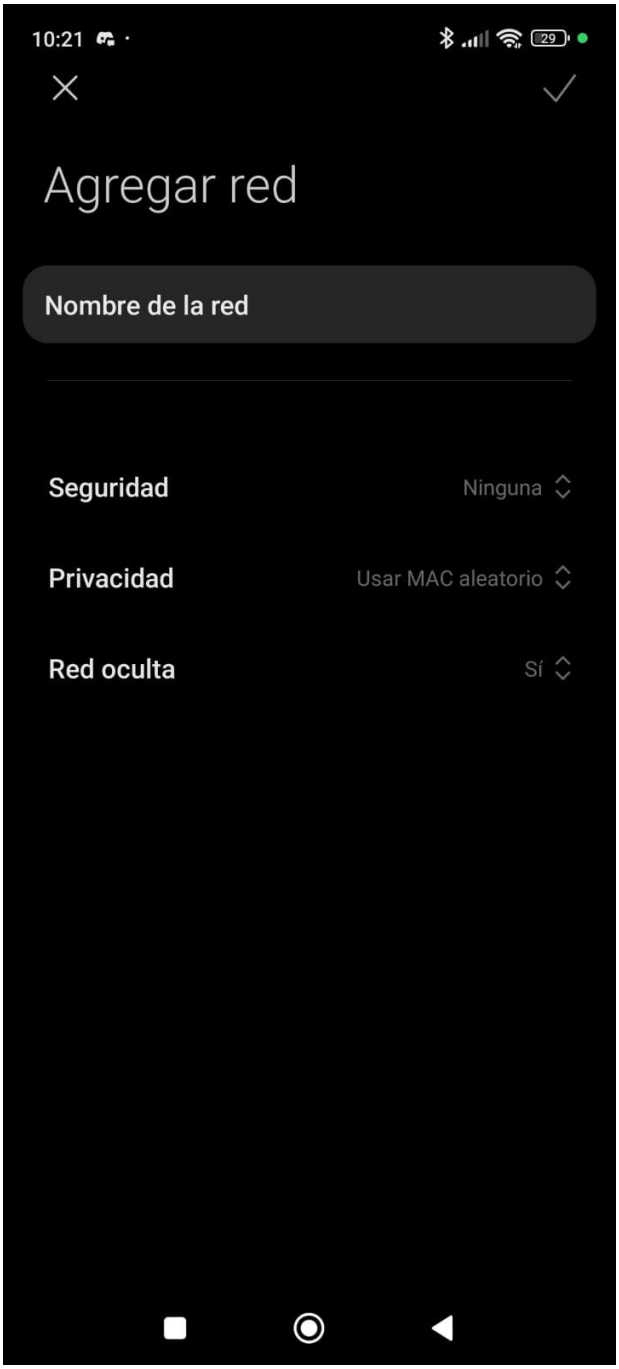

11:11
Puntos de acceso
Conexión actual
lab08.esteban (90:f6:52:89:7c:b2)
-33dBm CH 10 2457MHz ~0.4m
72Mbps 192.168.0.22
La aceleración del escaneo de Wi-Fi está habilitada
lab08.esteban (90:f6:52:89:7c:b2)
-33dBm CH 10 2457MHz ~0.4m
2447 - 2467 (20MHz) TP LINK TECHNOLOGIES...
[WPS WPA2]
Lab8_Velasquez (00:22:b0:45:99:97)
-46dBm CH 6 2437MHz ~2.0m
2427 - 2447 (20MHz) D LINK CORPORATION
[WPS WPA WPA2]
EXTREME_EMPLEADOS (b4:2d:56:7e:ea:93)
-51dBm CH 120 5600MHz ~1.5m
5590 - 5610 (20MHz) EXTREME NETWORKS H...
[NONE]
EXTREME_ESCUELA (b4:2d:56:7e:ea:91)
-51dBm CH 120 5600MHz ~1.5m
5590 - 5610 (20MHz) EXTREME NETWORKS H...
[WPA2]
EXTREME_ESTUDIANTES (b4:2d:56:7e:ea:92)
-51dBm CH 120 5600MHz ~1.5m
5590 - 5610 (20MHz) EXTREME NETWORKS H...
[NONE]
EXTREME_INVITADOS (b4:2d:56:7e:ea:90)
-51dBm CH 120 5600MHz ~1.5m
5590 - 5610 (20MHz) EXTREME NETWORKS H...
[NONE]
EXTREME_SALONES (b4:2d:56:7e:ea:94)
-51dBm CH 120 5600MHz ~1.5m
5590 - 5610 (20MHz) EXTREME NETWORKS H...
Puntos de acceso
Clasificación de ...
Gráfico de Canal
Gráfico de Tiem...

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



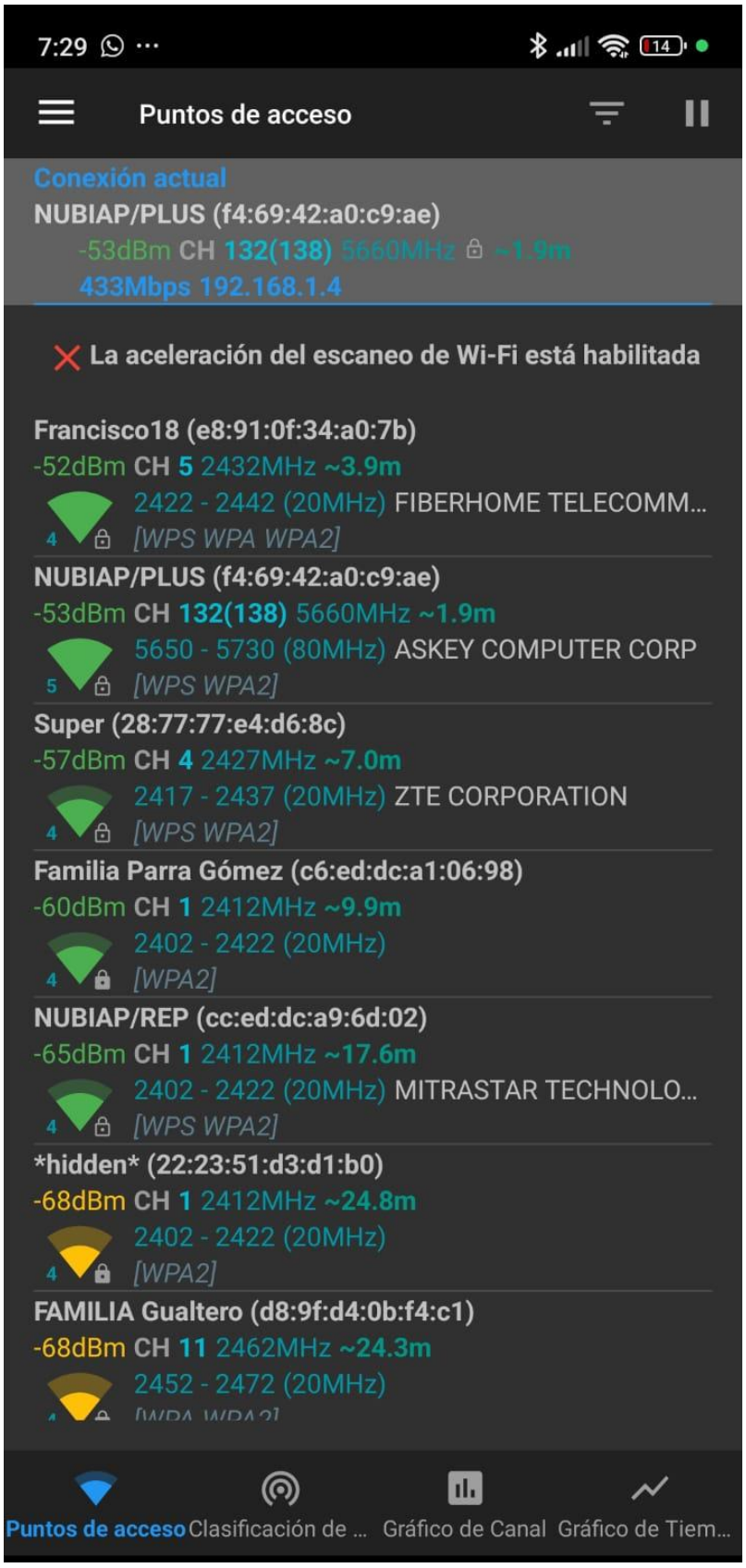


n. Test disabling the beacon frame and connecting to the network without accessing it via your smart phone
o. Use WiFi Analyzer again to see if your network is still visible
    i. Si se desactiva el beacon frame la red no aparece para conectarse en la configuración del wifi.
    ii. Se debe colocar de manera manual añadiendo la red con el nombre del SSID

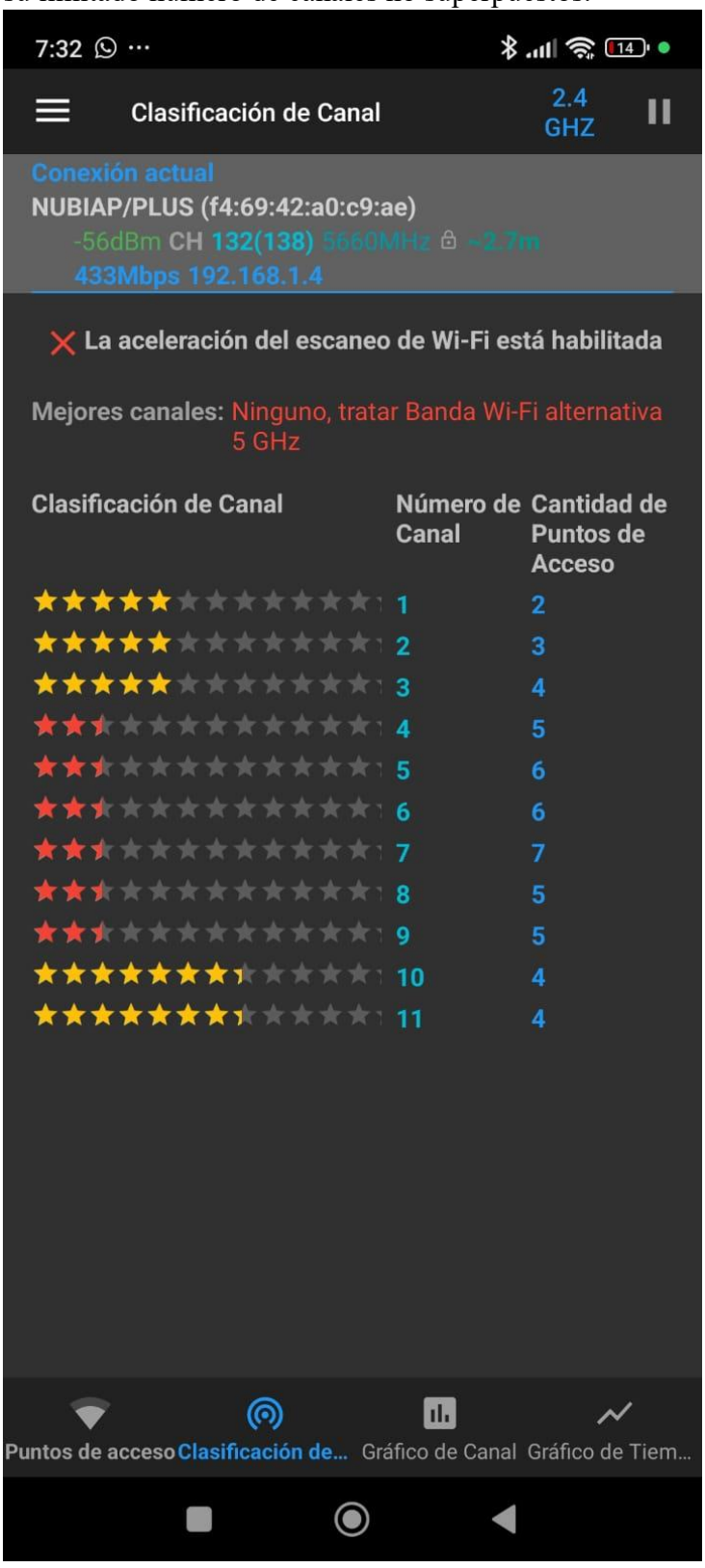


7. Reviewing WiFi Networks Near Your Home

a. Using a wireless traffic monitoring app, such as WiFi Analyzer for Android, discover wireless network near your home, including your own. Document the networks found, the bands, and the channels they operate on.
    i. Para esta actividad, se utilizó la aplicación WiFi Analyzer en un dispositivo Android para escanear las redes inalámbricas disponibles en los alrededores de mi hogar. A continuación se presenta el análisis y evidencia fotográfica obtenida:
    ii. Se identificaron múltiples redes WiFi activas, con información detallada sobre cada una, incluyendo:
        1. SSID (nombre de red)
        2. Banda de operación (2.4 GHz o 5 GHz)
        3. Canal en uso
        4. Seguridad (WPA/WPA2)
        5. Intensidad de señal (dBm)


7:29
Puntos de acceso
Conexión actual
NUBIAP/PLUS (f4:69:42:a0:c9:ae)
-53dBm CH 132(138) 5660MHz ~1.9m
433Mbps 192.168.1.4
La aceleración del escaneo de Wi-Fi está habilitada
Francisco18 (e8:91:0f:34:a0:7b)
-52dBm CH 5 2432MHz ~3.9m
2422 - 2442 (20MHz) FIBERHOME TELECOMM...
[WPS WPA WPA2]
NUBIAP/PLUS (f4:69:42:a0:c9:ae)
-53dBm CH 132(138) 5660MHz ~1.9m
5650 - 5730 (80MHz) ASKEY COMPUTER CORP
[WPS WPA2]
Super (28:77:77:e4:d6:8c)
-57dBm CH 4 2427MHz ~7.0m
2417 - 2437 (20MHz) ZTE CORPORATION
[WPS WPA2]
Familia Parra Gómez (c6:ed:dc:a1:06:98)
-60dBm CH 1 2412MHz ~9.9m
2402 - 2422 (20MHz)
[WPA2]
NUBIAP/REP (cc:ed:dc:a9:6d:02)
-65dBm CH 1 2412MHz ~17.6m
2402 - 2422 (20MHz) MITRASTAR TECHNOLO...
[WPS WPA2]
hidden (22:23:51:d3:d1:b0)
-68dBm CH 1 2412MHz ~24.8m
2402 - 2422 (20MHz)
[WPA2]
FAMILIA Gualtero (d8:9f:d4:0b:f4:c1)
-68dBm CH 11 2462MHz ~24.3m
2452 - 2472 (20MHz)
Puntos de acceso
Clasificación de ...
Gráfico de Canal
Gráfico de Tiem...

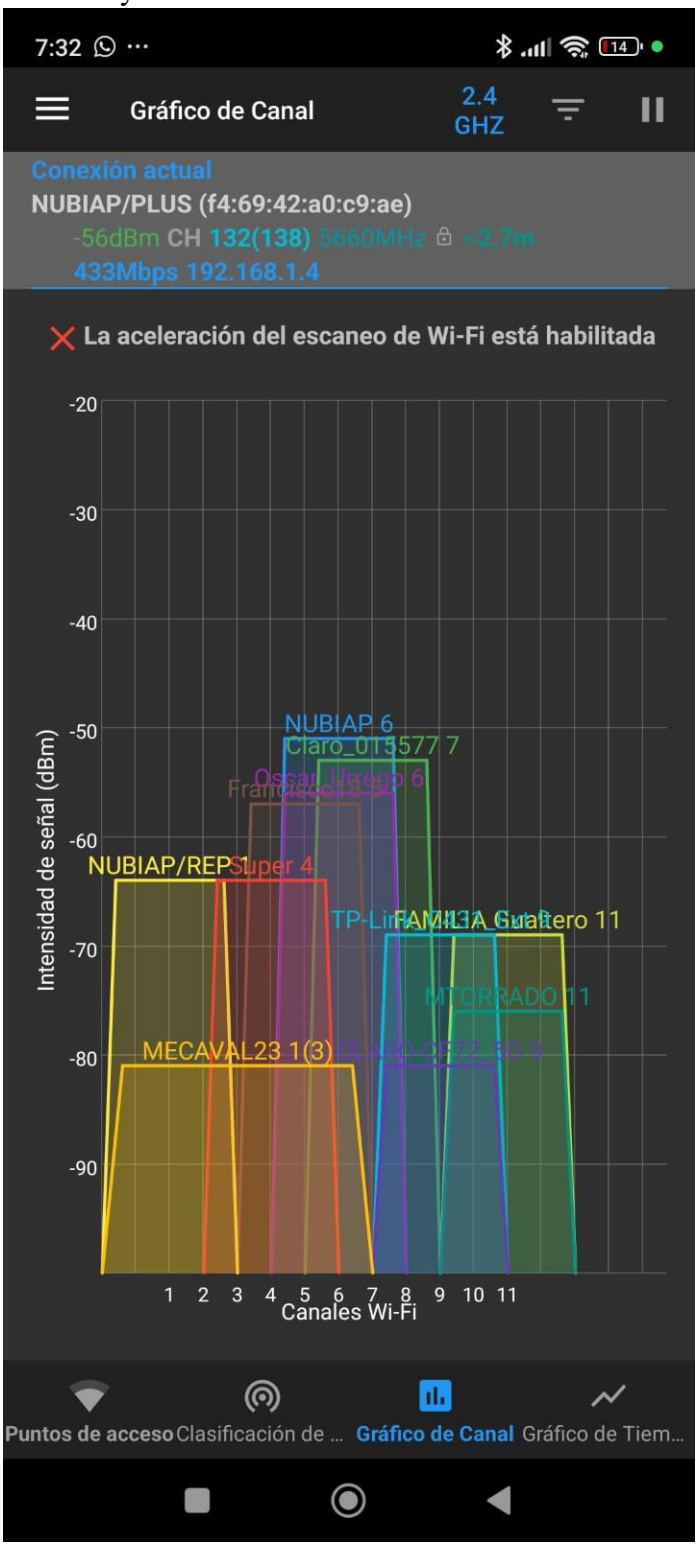
iii. La visualización muestra múltiples redes superpuestas, principalmente en los canales 4, 5 ,6,7,8,9 . Esta banda presenta mayor congestión debido a su limitado número de canales no superpuestos.

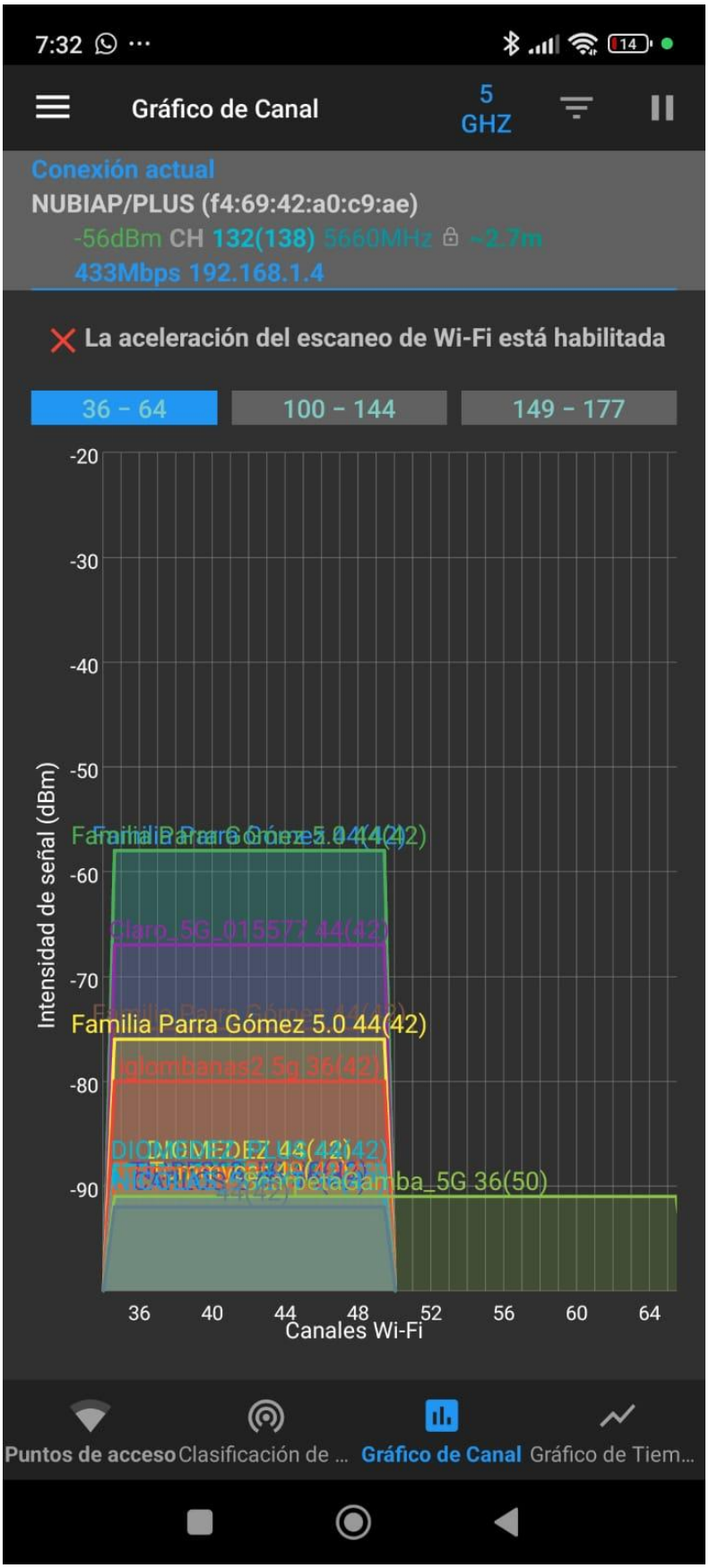


iv. Se observa una distribución más dispersa de redes, utilizando canales como 48,52,56,60, correspondientes al sub-bloque de 5.7 GHz. Esta banda permite mayor rendimiento y menor interferencia.

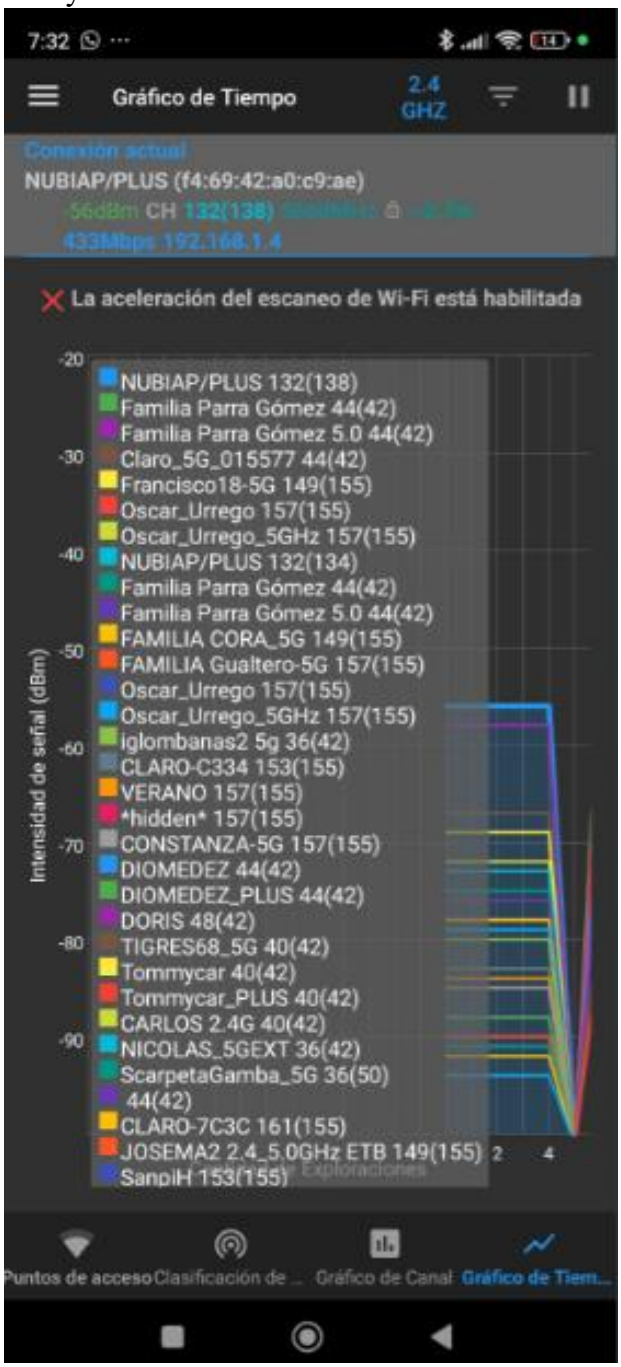
v. Se verifica que no hay redes activas en la banda de 6 GHz ni 60 GHz. Esto se comprueba con el mensaje:
   1. “La aceleración del escaneo de Wi-Fi está habilitada”
   2. “6 GHz – 0 puntos de acceso”

vi. Se capturaron nuevas redes operando en ambos rangos. Algunas redes nuevas usan canales como el 11 (2.4 GHz) y 157 (5 GHz), lo cual confirma la coexistencia de ambas bandas. Aquí se comparan todas las redes disponibles según su canal y banda. Se reafirma la saturación en 2.4 GHz y el uso selectivo de 5 GHz.




7:32
Gráfico de Canal
5 GHZ
Conexión actual
NUBIAP/PLUS (f4:69:42:a0:c9:ae)
-56dBm CH 132(138) 5660MHz ~2.7m
433Mbps 192.168.1.4
La aceleración del escaneo de Wi-Fi está habilitada
36 – 64
100 – 144
149 – 177
Intensidad de señal (dBm)
-20
-30
-40
-50
-60
-70
-80
-90
Familia Parra Gómez 5.0 44(42)
Claro_5G_015577 44(42)
Familia Parra Gómez 5.0 44(42)
iglombanas2 5g 36(42)
DIOMEDEZ 44(42)
CasaCarpetaGamba_5G 36(50)
36
40
44
48
52
56
60
64
Canales Wi-Fi
Puntos de acceso
Clasificación de ...
Gráfico de Canal
Gráfico de Tiem...

vii. Por ultimo se muestra un gráfico donde se observa la variación de la intensidad de señal (dBm) a lo largo del tiempo para múltiples redes, tanto en la banda de 2.4 GHz como 5 GHz. La señal más estable y fuerte corresponde a NUBIAP/PLUS (la red a la cual esta conectada el celular), operando en 5 GHz. Las redes con menor potencia, como "Oscar_Urrego_5GHz" y "Claro_5G_015577", presentan valores más cercanos a -80 dBm, indicando una señal más débil. Este tipo de gráfico es útil para identificar la estabilidad y potencia real de cada red, lo cual influye en la calidad de conexión del usuario.

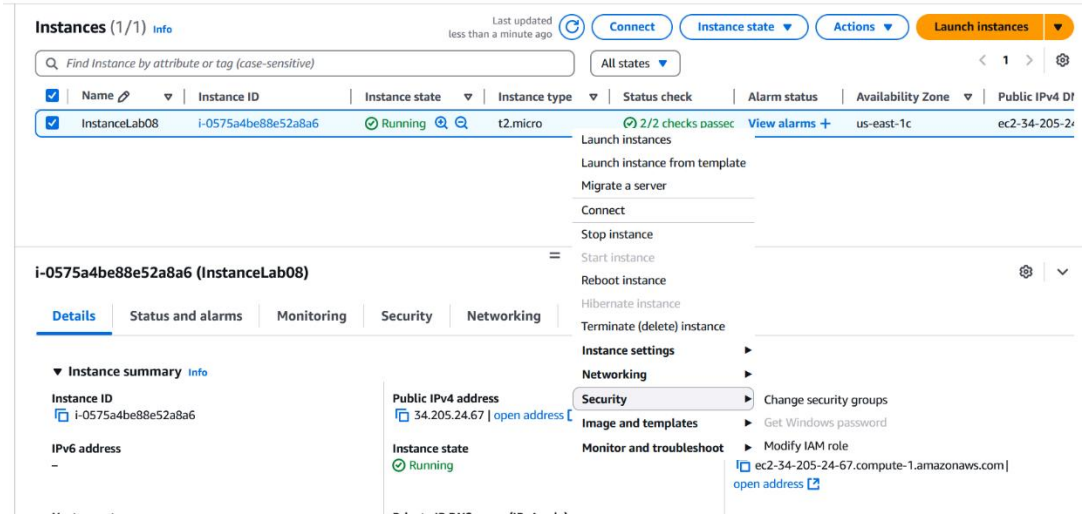


b. Are there networks operating on the 2.4 GHz, 5.7 GHz, and 60 GHz bands?
    i. Según los datos obtenidos mediante el escaneo, se concluye lo siguiente:
        1. 2.4 GHz: Sí hay múltiples redes activas en esta banda, visibles en los canales 1, 6 y 11.
        2. 5.7 GHz: También se detectaron redes utilizando canales como 149, 153 y 157, que pertenecen al sub-bloque de 5.7 GHz dentro del espectro de 5 GHz.
        3. 60 GHz: No se detectaron redes operando en esta banda. Esta ausencia es común, ya que el uso de 60 GHz está limitado a dispositivos muy específicos como routers WiGig o estaciones mmWave, los cuales no son comunes en ambientes residenciales.

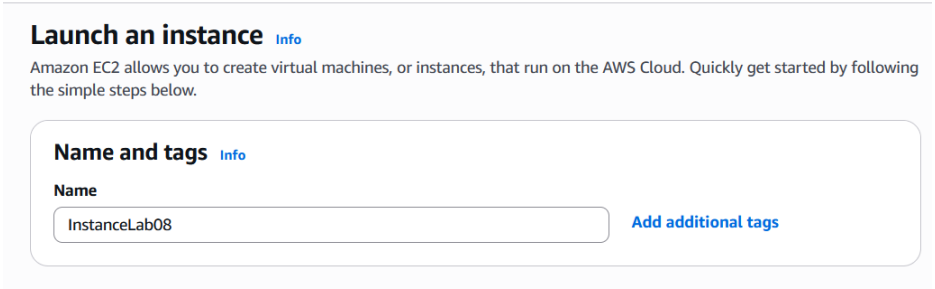
BASE SOFTWARE INSTALLATION

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

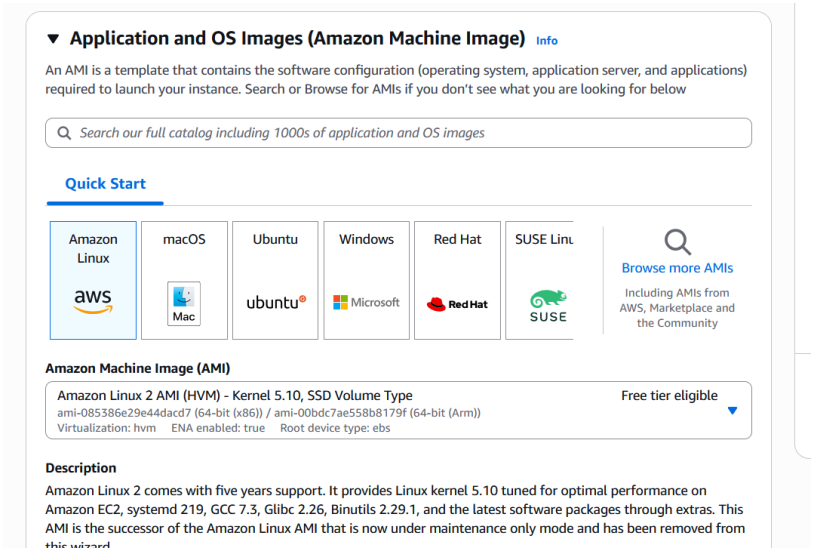
1. Dynamic Web Service
    a. Using the cloud lab on the AWS platform as a base, write a web application to be deployed on Apache. This application should display a webpage that functions as a basic grade calculator for courses in the School. It must request the student's name and the final grades for each third of the semester and cal-culate the final semester grade (30%, 30%, and 40%). Configure it dynamically to interpret PHP code. Additionally, it must save these records in a relational database (e.g., PostgreSQL)
        i. Nos dirigimos a la plataforma de AWS y creamos una nueva instancia



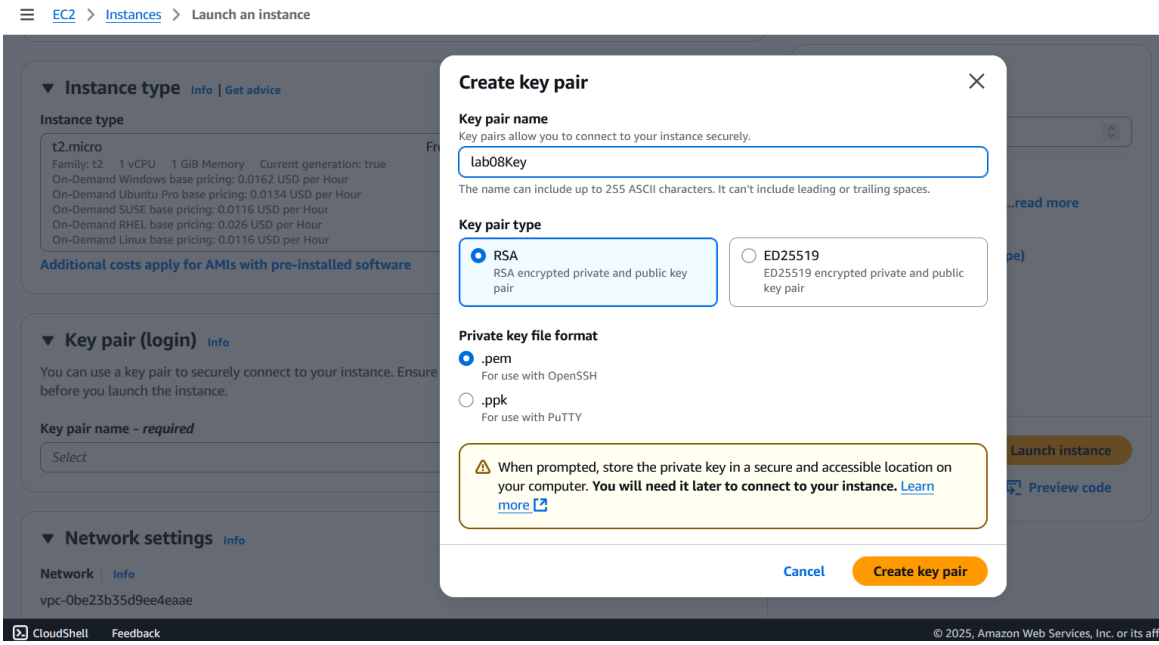
        ii. Asignamos un nombre a la instancia, en este caso será instancelab08



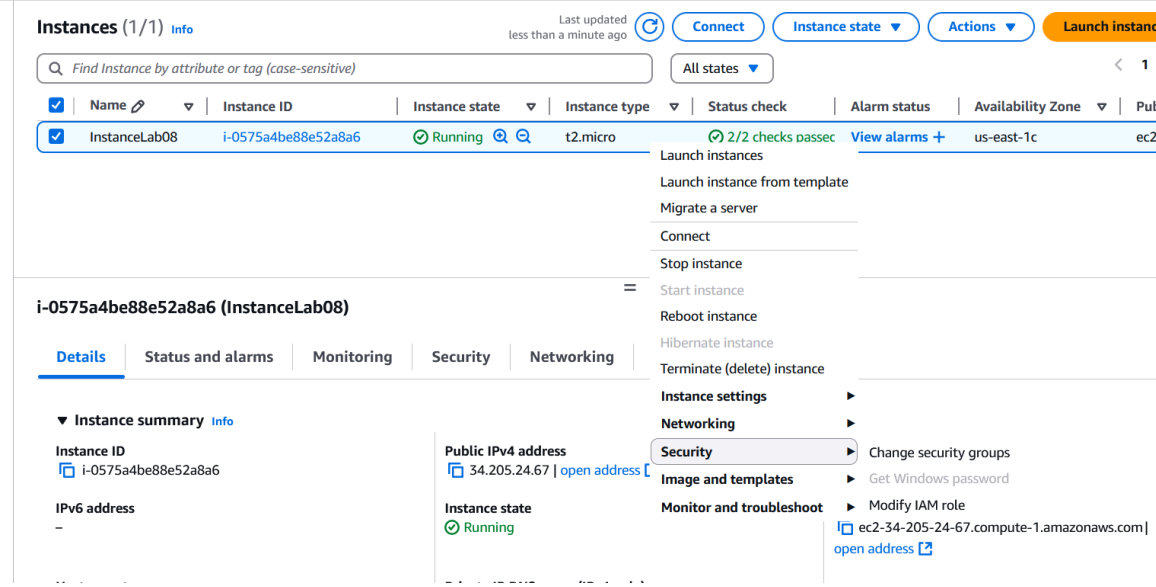
        iii. Escogemos Amazon linus en el apartado de quick start
        iv. Además seleccionamos el tipo de imagin a "Amazon Linux 2 AMI"



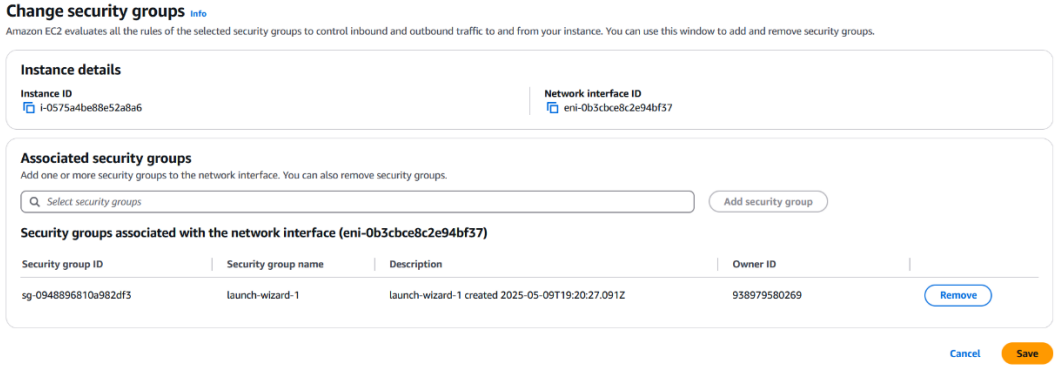
v. Creamos una nueva key y la asignamos a la instancia



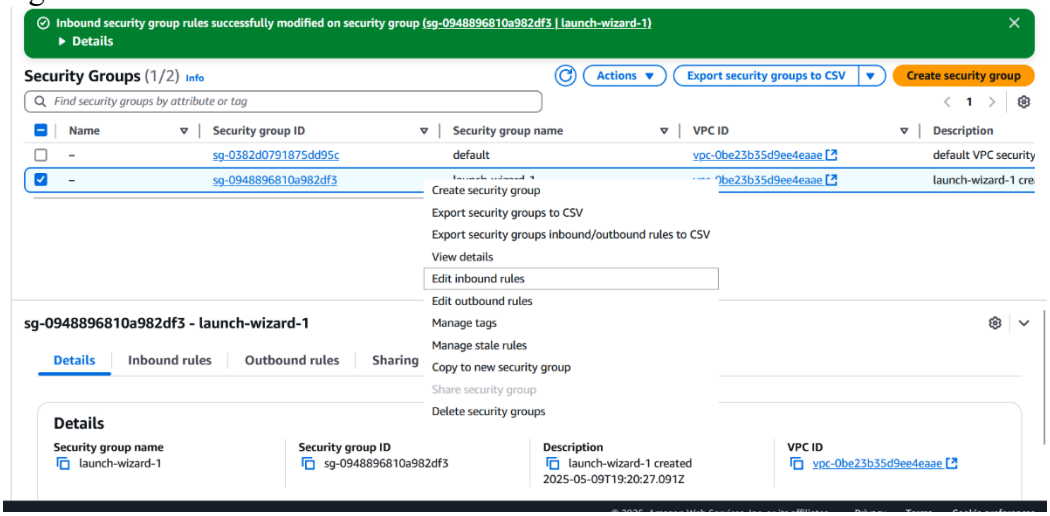
vi. Posterior a esto, accedemos a los grupos de seguridad de la instancia



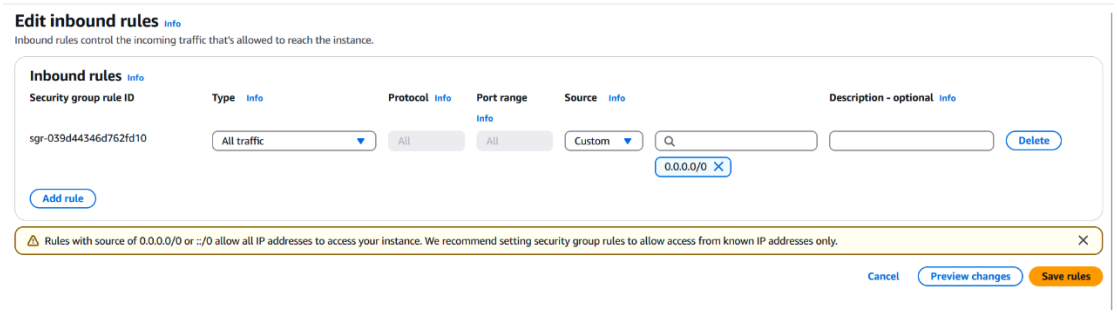
vii. Miramos con que grupo de seguridad quedo configurada, en este caso es launch-wizard



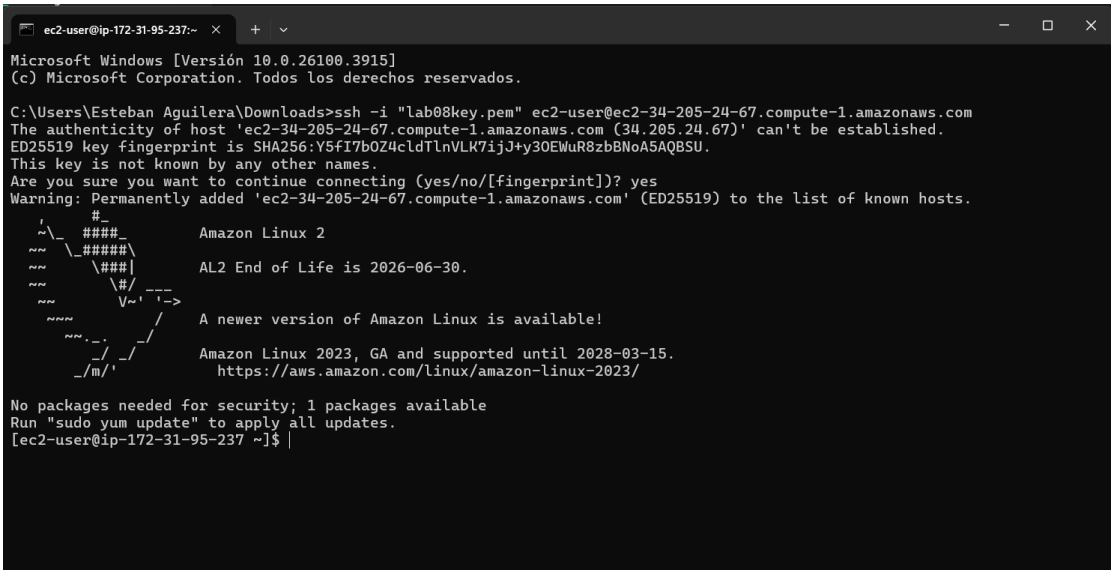
viii. Una vez identificado el nombre nos dirigimos al grupo de seguridad en las reglas de entrada



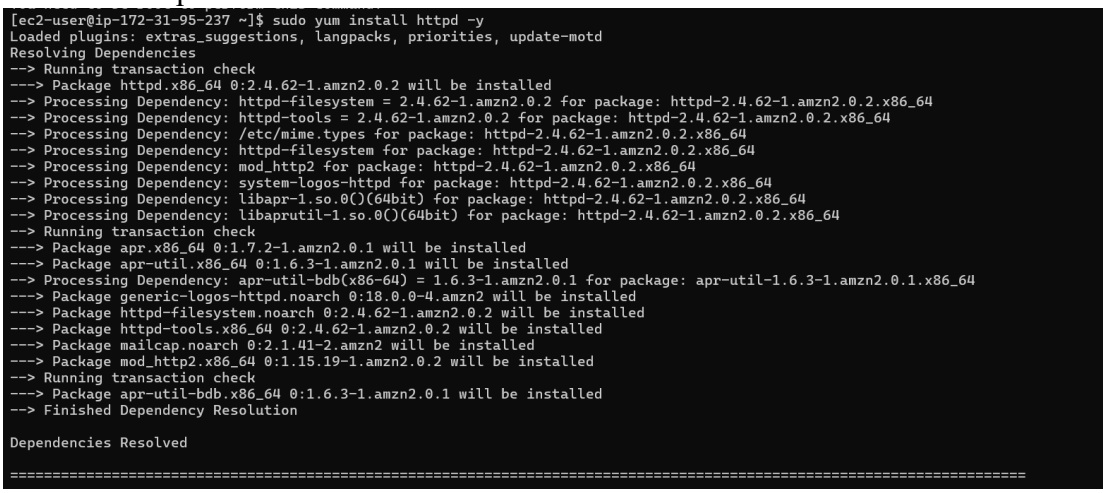
ix. Agregamos una nueva regla que permita todo el trafico en cualquier dirección ip



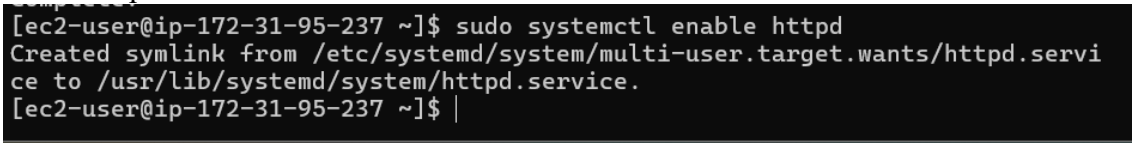
x. Ya con todo configurado creamos la instancia y accedemos a ella con cmd mediante el comando shh -i “nombreInstancia” linkInstancia



xi. Ahora ejecutamos el comando sudo yum install httpd -v para instalar el servidor de Apache



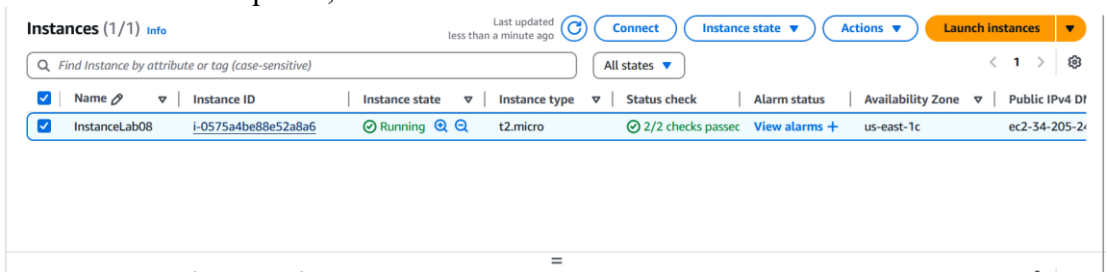
xii. Una ves intalado, habilitamos el servicio con el comando sudo systemctl enable httpd



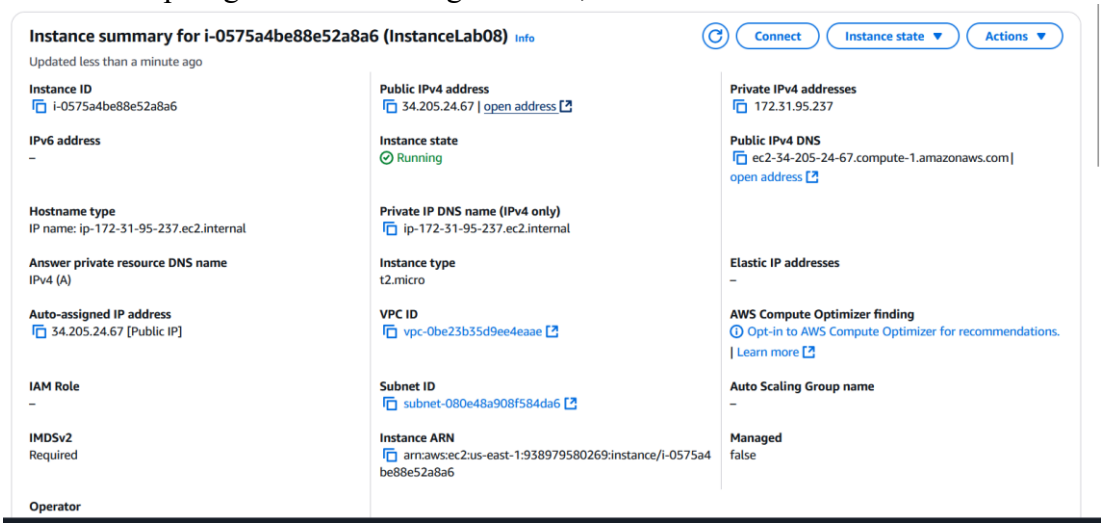
xiii. Posterior a esto, iniciamos el servicio con el comando sudo systemctl start httpd y verificamos que el estado con el comando sudo systemctl status httpd. Nos deberá aparecer que el servicio de apache esta Active (verde)

```
[ec2-user@ip-172-31-95-237 ~]$ sudo systemctl start httpd
[ec2-user@ip-172-31-95-237 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pr
eset: disabled)
   Active: active (running) since Fri 2025-05-09 19:26:39 UTC; 4s ago
     Docs: man:httpd.service(8)
 Main PID: 3442 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─3442 /usr/sbin/httpd -DFOREGROUND
           ├─3443 /usr/sbin/httpd -DFOREGROUND
           ├─3444 /usr/sbin/httpd -DFOREGROUND
           ├─3445 /usr/sbin/httpd -DFOREGROUND
           ├─3446 /usr/sbin/httpd -DFOREGROUND
           └─3447 /usr/sbin/httpd -DFOREGROUND

May 09 19:26:39 ip-172-31-95-237.ec2.internal systemd[1]: Starting The Ap...
May 09 19:26:39 ip-172-31-95-237.ec2.internal systemd[1]: Started The Apa...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-172-31-95-237 ~]$
```

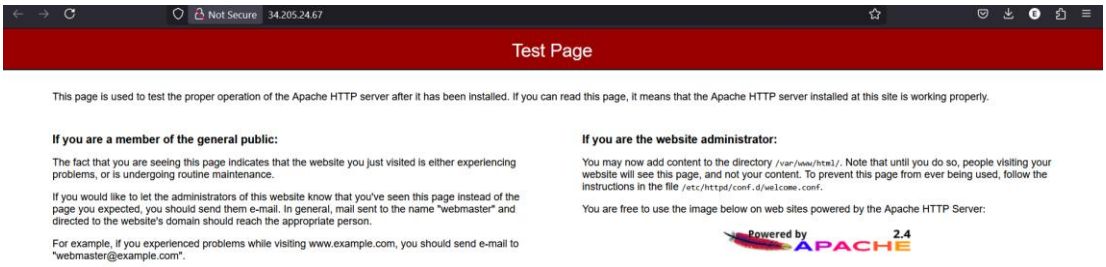
xiv. Una vez instalado apache, accedemos a la instancia nuevamente



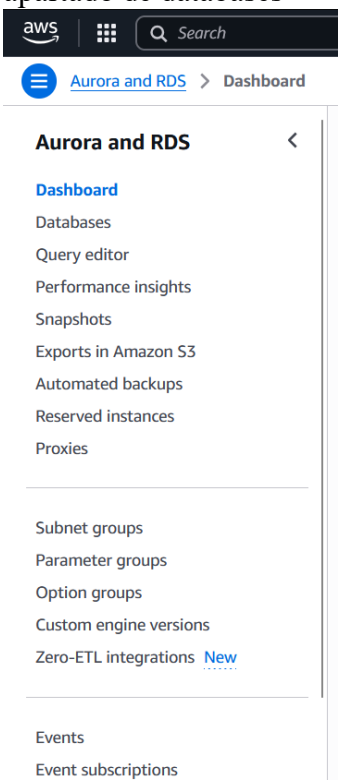
xv. Abrimos la ip asignada en un navegador web, en este caso 34.205.24.67



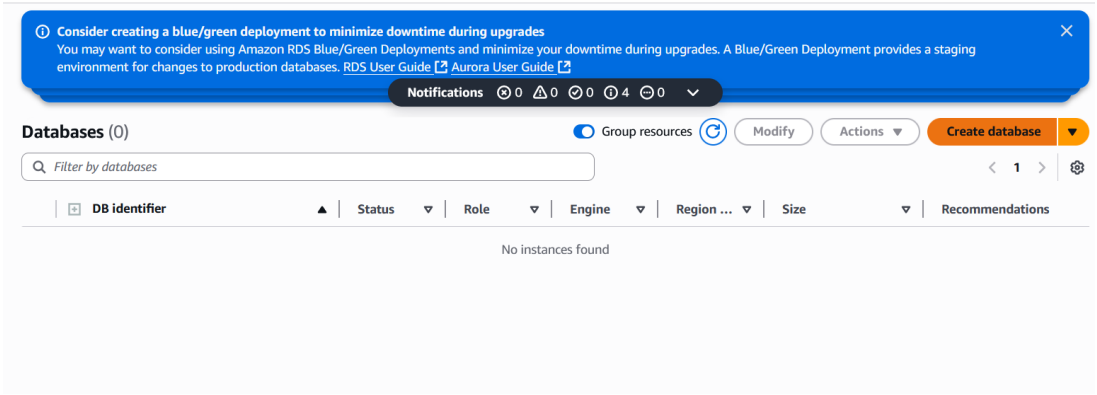
xvi. Si todo esta bien instalado, nos abre la web page por defecto de Apache



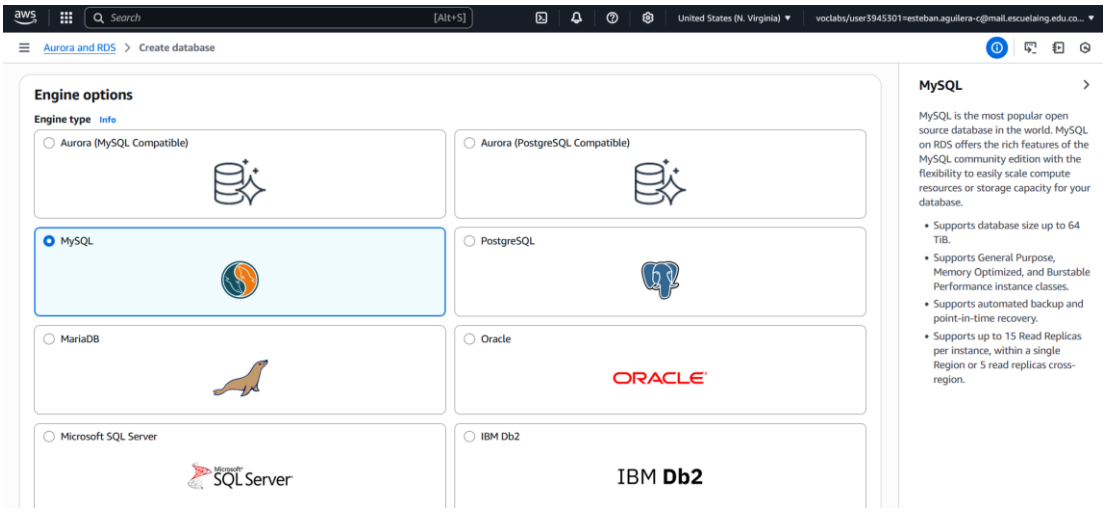
xvii. Ahora, vamos a configurar la base de datos. Para eso accedemos al apartado de databases



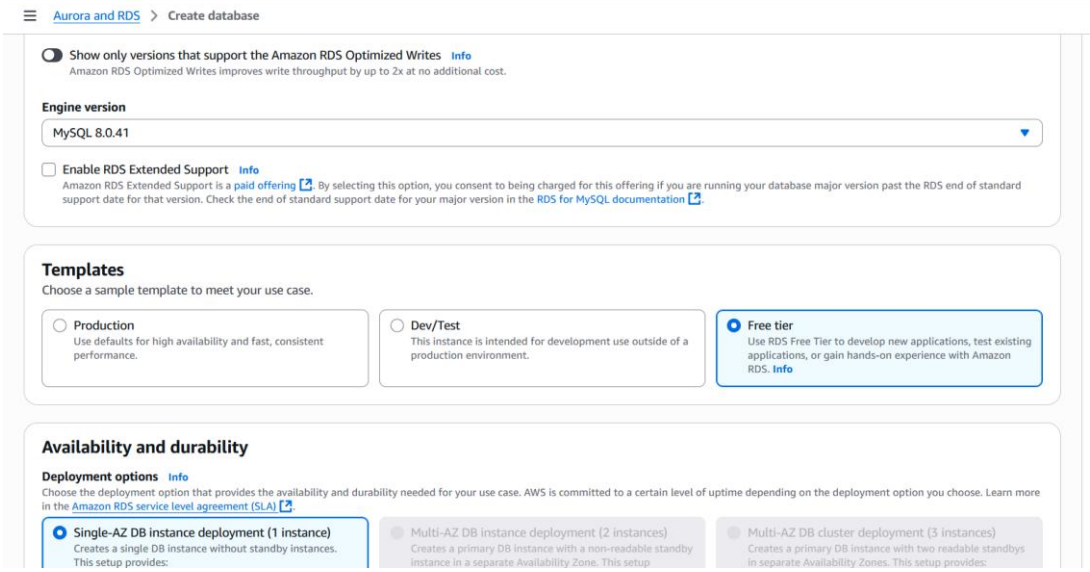
xviii. Seleccionamos “Create database”



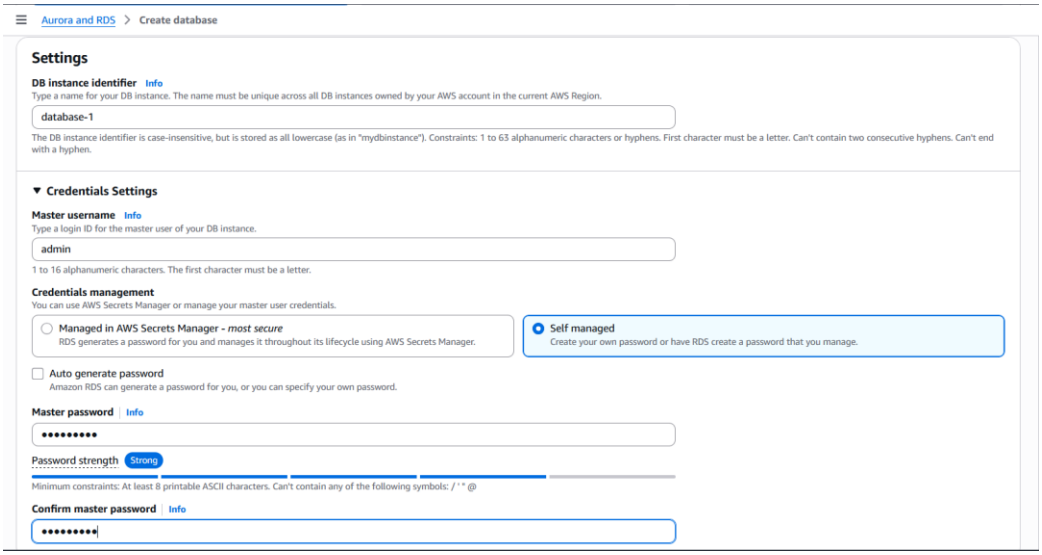
xix. En este caso, vamos a trabajar con MySql



xx. Seleccionamos la opción Free tier en el apartado de Templates

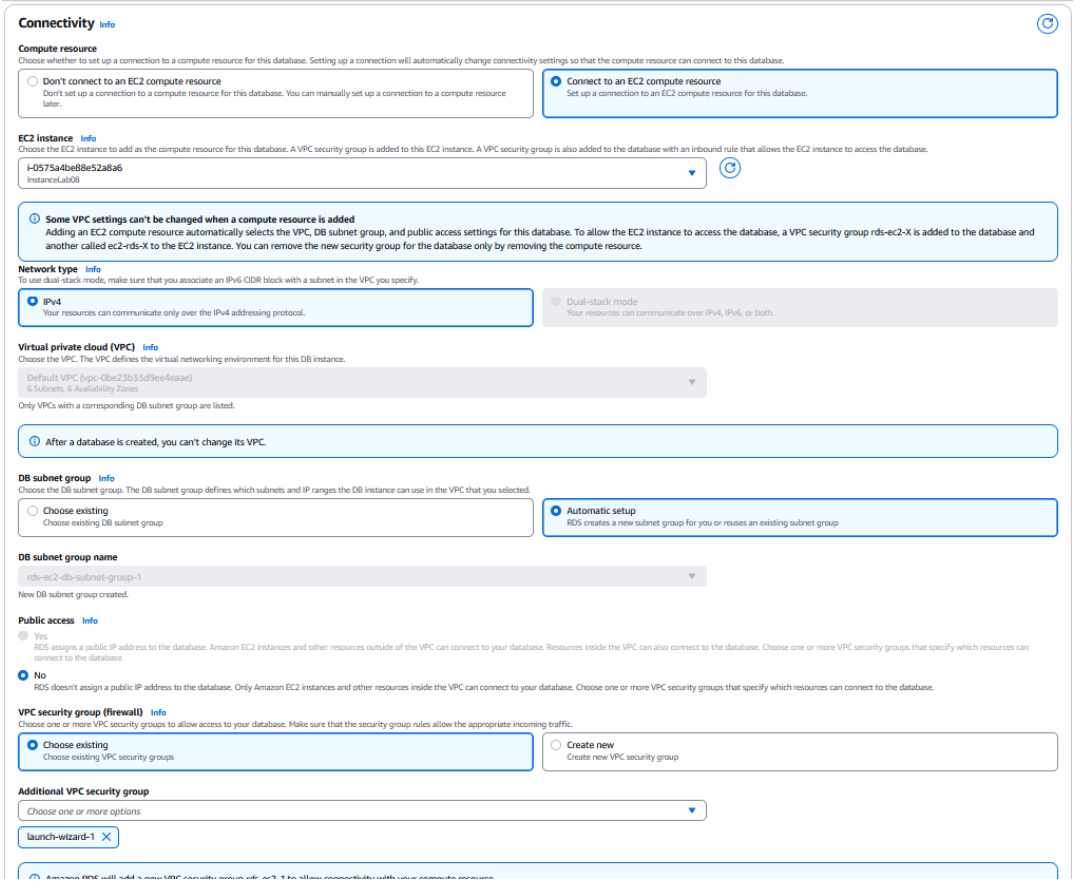


xxi. Ahora asignamos una contraseña en el apartado de Credential Settings, en este caso será : root123A-



xxii. Ahora seleccionamos En el apartado EC2 Instance el id de la instancia creada anteriormente. Mismo procedimiento para el VPC Security Group (launch-wizard)

xxiii. Finalmente creamos la base de datos



xxiv. Una vez creada la base de datos, ingresamos en la instancia de nuevo a través del cmd e instalamos las dependencias de mysql con el comando sudo yum install –nogpgcheck mysql mysql-client

```
[ec2-user@ip-172-31-95-237 ~]$ sudo yum install --nogpgcheck mysql mysql-client
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                               | 3.6 kB     00:00
No package mysql-client available.
Resolving Dependencies
--> Running transaction check
---> Package mariadb.x86_64 1:5.5.68-1.amzn2.0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package      Arch        Version                     Repository       Size
================================================================================
Installing:
 mariadb      x86_64      1:5.5.68-1.amzn2.0.1        amzn2-core      8.8 M

Transaction Summary
================================================================================
Install  1 Package

Total download size: 8.8 M
Installed size: 49 M
Is this ok [y/d/N]: y
Downloading packages:
mariadb-5.5.68-1.amzn2.0.1.x86_64.rpm                    | 8.8 MB   00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                         1/1
  Verifying  : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                         1/1

Installed:
```

xxv. Con las dependencias instaladas, ingresamos a la base de datos con el comando mysql -h “Link del alojamiento de la base de datos “ -u admin -p. Nos pedirá la contraseña una vez ejecutemos el comando, en este caso es root123A-

```
[ec2-user@ip-172-31-95-237 ~]$ mysql -h database-1.ctj22cnkyjyl.us-east-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 25
Server version: 8.0.41 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

xxvi. Posterior a esto, creamos la base de datos , en este caso se llamara “school”

```
MySQL [(none)]> CREATE DATABASE school;
Query OK, 1 row affected (0.01 sec)
```

xxvii. Ingresamos a la base de datos con el comando use “nombre_base_de_datos”

```
MySQL [(none)]> USE school
Database changed
```

xxviii. Creamos la table que nos va permitir guardar las notas de los estudiantes con los atributos mostrados a continuación

```
MySQL [school]> CREATE TABLE grades (
    ->     id INT AUTO_INCREMENT PRIMARY KEY,
    ->     student_name VARCHAR(100),
    ->     grade1 DECIMAL(5,2),
    ->     grade2 DECIMAL(5,2),
    ->     grade3 DECIMAL(5,2),
    ->     final_grade DECIMAL(5,2),
    ->     created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
    -> );
Query OK, 0 rows affected (0.03 sec)
```

xxix. Salimos de la base de datos con el comando exit

```
MySQL [school]> exit
Bye
```

xxx. Ya con la estructura de la base de datos ahora vamos a generar el comando php para calcular las notas . Para esto primero accedemos a la ruta /var/www/hml y creamos el archivo que nos va permitir la conexión con la base de datos con el comando sudo nano connectionDb.php

```
[ec2-user@ip-172-31-95-237 /]$ cd /var/www/html
[ec2-user@ip-172-31-95-237 html]$ sudo nano connectionDb.php
```

xxxi. Ahora, creamos un script php que nos permita el acceso a la base de datos .

xxxii. El script connectionDb.php contiene las credenciales necesarias y utiliza la clase PDO para establecer la conexión con la base de datos MySQL. Además, se implementa una estructura try-catch para capturar posibles errores de conexión y mostrar un mensaje descriptivo en caso de fallo.

```
 GNU nano 2.9.8                                                connectionDb.php

<?php
$host = "database-1.ctj22cnkyjyl.us-east-1.rds.amazonaws.com";
$dbname = "school";
$username = "admin";
$password = "root123A-";

try {
    $pdo = new PDO("mysql:host=$host;dbname=$dbname", $username, $password);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Error al conectar a la base de datos: " . $e->getMessage();
}
?>
```

Donde:

- Se abre el bloque de código PHP.
- Se definen cuatro variables con los datos necesarios para conectarse a la base de datos:
  - Dirección del servidor de base de datos (host).
  - Nombre de la base de datos.
  - Nombre de usuario.
  - Contraseña.

- Se utiliza un bloque try para intentar establecer la conexión con la base de datos mediante la clase PDO (PHP Data Objects).
- Dentro del try, se crea un nuevo objeto PDO utilizando los datos de conexión definidos anteriormente.
- Se configura el objeto PDO para que muestre excepciones cuando ocurra un error (modo de error: excepciones).
- Si ocurre algún problema durante la conexión, el bloque catch captura la excepción lanzada por PDO.
- En caso de error, se muestra un mensaje indicando que no se pudo conectar, junto con el detalle del error.
- Se cierra el bloque de código PHP.

xxxiii. Luego creamos el archive que va realizar el calculo de notas con el comando sudo nano index.php

xxxiv. Ahora, desarrollamos un script PHP que permite calcular la nota final de un estudiante y almacenarla en la base de datos. El formulario permite ingresar el nombre del estudiante y tres notas. El sistema valida que estén entre 0 y 50, calcula la nota final según un promedio ponderado, guarda los datos y muestra los registros almacenados en una tabla.

```php
<?php include 'connectionDb.php'; ?>

<!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>
</head>
<body>
    <h2>Calculadora de Nota Final</h2>

    <?php
    if ($_SERVER["REQUEST_METHOD"] == "POST") {
        $name = $_POST["student_name"];
        $grade1 = floatval($_POST["grade1"]);
        $grade2 = floatval($_POST["grade2"]);
        $grade3 = floatval($_POST["grade3"]);

        // Validación de rango: entre 0 y 50
        if (
            $grade1 < 0 || $grade1 > 50 ||
            $grade2 < 0 || $grade2 > 50 ||
            $grade3 < 0 || $grade3 > 50
        ) {
            echo "<p style='color:red'><strong>❌ Las notas deben estar entre 0 y 50.</strong></p>";
        } else {
            $final = $grade1 * 0.3 + $grade2 * 0.3 + $grade3 * 0.4;

            $stmt = $pdo->prepare("INSERT INTO grades (student_name, grade1, grade2, grade3, final_grade)
                                   VALUES (?, ?, ?, ?, ?)");
            $stmt->execute([$name, $grade1, $grade2, $grade3, $final]);

            echo "<p><strong>$name tiene una nota final de: " . number_format($final, 2) . "</strong></p>";
        }
    }
    ?>

    <form method="post" action="">
        <label>Nombre del estudiante: <input type="text" name="student_name" required></label><br><br>
        <label>Nota 1 (30%): <input type="number" step="0.01" name="grade1" min="0" max="50" required></label><br><br>
        <label>Nota 2 (30%): <input type="number" step="0.01" name="grade2" min="0" max="50" required></label><br><br>
        <label>Nota 3 (40%): <input type="number" step="0.01" name="grade3" min="0" max="50" required></label><br><br>
        <button type="submit">Calcular</button>
    </form>

    <h2>Notas Registradas</h2>
    <table border="1" cellpadding="5">
        <tr>
            <th>Estudiante</th>
            <th>Nota 1</th>
            <th>Nota 2</th>
            <th>Nota 3</th>
            <th>Nota Final</th>
        </tr>
        <?php
        $stmt = $pdo->query("SELECT student_name, grade1, grade2, grade3, final_grade FROM grades");
        while ($row = $stmt->fetch()) {
            echo "<tr>";
            echo "<td>" . htmlspecialchars($row["student_name"]) . "</td>";
            echo "<td>" . $row["grade1"] . "</td>";
            echo "<td>" . $row["grade2"] . "</td>";
            echo "<td>" . $row["grade3"] . "</td>";
            echo "<td>" . number_format($row["final_grade"], 2) . "</td>";
            echo "</tr>";
        }
        ?>
    </table>
</body>
</html>
```

Donde

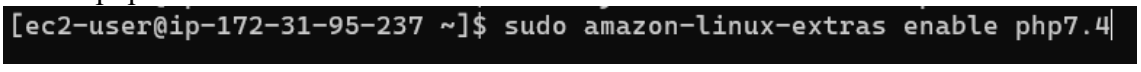
- Se incluye el archivo connectionDb.php para establecer la conexión con la base de datos.
- Se define una estructura HTML con un formulario y una tabla para mostrar los datos registrados.
- Dentro del bloque PHP:
    - Se verifica si el formulario fue enviado usando el método POST.

        - Se capturan los valores ingresados: el nombre del estudiante y tres notas numéricas.
    - Se realiza una validación para asegurar que las tres notas estén en el rango permitido (entre 0 y 50).
    - Si alguna nota está fuera del rango, se muestra un mensaje de advertencia en rojo indicando que las notas deben estar entre 0 y 50.
    - Si las notas son válidas, se calcula la nota final usando un promedio ponderado:
        - Nota 1 tiene un peso del 30%.
        - Nota 2 tiene un peso del 30%.
        - Nota 3 tiene un peso del 40%.
    - Se prepara y ejecuta una consulta SQL para insertar los datos del estudiante y sus notas en la tabla grades.
    - Se muestra en pantalla el nombre del estudiante junto con su nota final formateada con dos decimales.
    - En la parte inferior de la página, se realiza una consulta a la base de datos para obtener todos los registros existentes en la tabla grades.
    - Los datos recuperados se muestran en una tabla HTML con las siguientes columnas:
    - Nombre del estudiante.
        - Nota 1.
        - Nota 2.
        - Nota 3.
        - Nota final (formateada con dos decimales).

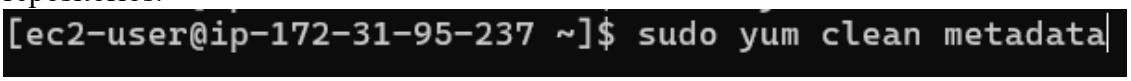
xxxv. Por ultimo accedemos al archivo con el comando sudo nano /var/www/html/.htaccess

xxxvi. Se agrega la línea DirectoryIndex index.php index.html para definir que al acceder a la IP del servidor en AWS, se cargue automáticamente el archivo index.php como página principal por defecto.

xxxvii. Ahora , habilitamos las dependencias de php con sudo amazon-linux-extras enable php7.4



xxxviii. Se ejecuta el comando sudo yum clean metadata para borrar la caché de información sobre los paquetes disponibles y forzar la actualización de los repositorios.

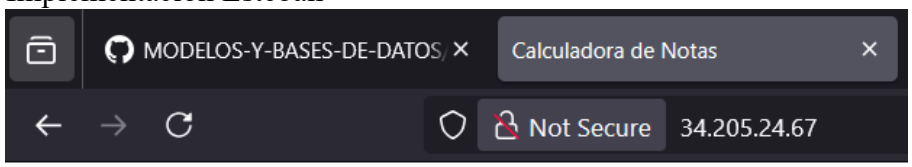


xxxix. Ahora instalamos la dependencia de php con el comando sudo yum install php php-mysqlnd

```
[ec2-user@ip-172-31-95-237 html]$ sudo yum install php php-mysqlnd
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Running transaction check
---> Package php.x86_64 0:5.4.16-46.amzn2.0.6 will be installed
--> Processing Dependency: php-common(x86-64) = 5.4.16-46.amzn2.0.6 for package: php-5.4.16-46.amzn2.0.6.x86_64
--> Processing Dependency: php-cli(x86-64) = 5.4.16-46.amzn2.0.6 for package: php-5.4.16-46.amzn2.0.6.x86_64
---> Package php-mysqlnd.x86_64 0:5.4.16-46.amzn2.0.6 will be installed
--> Processing Dependency: php-pdo(x86-64) = 5.4.16-46.amzn2.0.6 for package: php-mysqlnd-5.4.16-46.amzn2.0.6.x86_64
--> Running transaction check
---> Package php-cli.x86_64 0:5.4.16-46.amzn2.0.6 will be installed
---> Package php-common.x86_64 0:5.4.16-46.amzn2.0.6 will be installed
--> Processing Dependency: libzip.so.2()(64bit) for package: php-common-5.4.16-46.amzn2.0.6.x86_64
---> Package php-pdo.x86_64 0:5.4.16-46.amzn2.0.6 will be installed
--> Running transaction check
---> Package libzip010-compat.x86_64 0:0.10.1-9.amzn2.0.5 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                                Arch                           Version
================================================================================================================================
Installing:
 php                                    x86_64                         5.4.16-46.amzn2.0.6
 php-mysqlnd                            x86_64                         5.4.16-46.amzn2.0.6
Installing for dependencies:
 libzip010-compat                       x86_64                         0.10.1-9.amzn2.0.5
 php-cli                                x86_64                         5.4.16-46.amzn2.0.6
 php-common                             x86_64                         5.4.16-46.amzn2.0.6
 php-pdo                                x86_64                         5.4.16-46.amzn2.0.6
```

xl. Accedemos a la página web de nuevo y podemos ver la lógica implementada anteriormente del cálculo de notas.

1. Implementación Esteban



Calculadora de Nota Final

Nombre del estudiante:

Nota 1 (30%):

Nota 2 (30%):

Nota 3 (40%):

Calcular

Notas Registradas

Estudiante	Nota 1	Nota 2	Nota 3	Nota Final

2. Implementación Juan (es la misma lógica pero cambia el diseño)

2. Other Useful Commands
    a. Study the functionality of network information commands, such as ifconfig, netstat, vnstat, route, and ethtool (or similar) for Slackware, NetBSD, and Windows Server systems. Examine the various parame-ters that can be used and create a Shell program that utilizes them (create a menu with at least 5 options to show different executions of these commands). Students must be able to understand the output of the commands and present it in a user-friendly manner

    NETBSD

    - Primero, creamos nuestro script de shell y diseñamos un menú con las opciones mostradas en la imagen. Usamos netstat para mostrar información de red como puertos, servicios, estadísticas y conexiones UDP y TCP. También usamos route para ver la tabla de enrutamiento y ethtool para verificar la información de las interfaces de red.

```
 GNU nano 8.3                    Shell1.8.sh
#!/bin/sh

while :; do
    echo ""
    echo "========= Red - Opciones ========="
    echo "1) Conexiones activas y puertos en escucha"
    echo "2) Estadasticas de red"
    echo "3) Tabla de rutas"
    echo "4) Detalles de interfaces"
    echo "5) Filtrar por protocolo"
    echo "6) Salir"
    echo "Seleccione una opcion:"
    read -r respuesta

    case $respuesta in
        1)
            echo ""
            echo ">> Conexiones y puertos en escucha:"
            sockstat -4 -l
            ;;
        2)
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
 GNU nano 8.3                          Shell1.8.sh
        2)
            echo ""
            echo ">> Estadisticas de uso de red:"
            netstat -i
            ;;
        3)
            echo ""
            echo ">> Mostrando tabla de rutas:"
            netstat -r
            ;;
        4)
            echo ""
            echo ">> Informacion de interfaces de red:"
            ifconfig -a
            ;;
        5)
            echo ""
            echo "Seleccione protocolo a visualizar:"
            echo "1 - TCP"
            echo "2 - UDP"
            read -r tipo

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
 GNU nano 8.3                          Shell1.8.sh
                    sockstat -4 -P tcp
                    ;;
                2)
                    echo ""
                    echo ">> Conexiones UDP:"
                    sockstat -4 -P udp
                    ;;
                *)
                    echo ">> OpciA3n invAilida de protocolo."
                    ;;
            esac
            ;;
        6)
            echo ">> Cerrando el programa."
            exit 0
            ;;
        *)
            echo ">> OpciA3n no reconocida. Intente de nuevo."
            ;;
    esac
done

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

- Probamos la opción 1 del menú (Conexiones de red y puertos en escucha). Como podemos ver, se muestran los protocolos de la capa de transporte con los puertos en los que están escuchando, junto con las direcciones IP permitidas.

```
1
Mostrando puertos en escucha y servicios:
tcp        0      0  *.80                   *.*                    LISTEN
tcp        0      0  *.5666                 *.*                    LISTEN
tcp        0      0  *.139                  *.*                    LISTEN
tcp        0      0  *.445                  *.*                    LISTEN
tcp        0      0  127.0.0.1.953          *.*                    LISTEN
tcp        0      0  127.0.0.1.53           *.*                    LISTEN
tcp        0      0  10.2.78.35.53          *.*                    LISTEN
tcp6       0      0  *.5666                 *.*                    LISTEN
tcp6       0      0  *.139                  *.*                    LISTEN
tcp6       0      0  *.445                  *.*                    LISTEN
tcp6       0      0  ::1.953                *.*                    LISTEN
tcp6       0      0  fe80::1%lo0.53         *.*                    LISTEN
tcp6       0      0  ::1.53                 *.*                    LISTEN
tcp6       0      0  fe80::20c:29ff:f.53    *.*                    LISTEN
```

- Probamos la opción 2 en el menú (Uso de red). Podemos ver información sobre eth1 (Interfaz de red) y lo (Bucle de retorno).

```
Estadisticas de red:
Name  Mtu   Network       Address              Ipkts Ierrs    Opkts Oerrs Colls
wm0   1500  <Link>        00:0c:29:cf:c8:84      751     0      132     0     0
wm0   1500  fe80::/64     fe80::20c:29ff:fe      751     0      132     0     0
wm0   1500  10.2/16       Juanito.is.escuel      751     0      132     0     0
lo0   33624 <Link>                              52     0       52     0     0
lo0   33624 127/8         localhost              52     0       52     0     0
lo0   33624 localhost/128 ::1                    52     0       52     0     0
lo0   33624 fe80::/64     fe80::1                52     0       52     0     0
```

- Probamos la opción 3 en el menú (Tabla de enrutamiento). Podemos ver las rutas en la tabla de enrutamiento.

```
fe80::%wm0/64                     link#1                         UC
   -        -      -  wm0
fe80::20c:29ff:fecf:c884          link#1                         UHl
   -        -      -  lo0
fe80::%lo0/64                     fe80::1                        U
   -        -      -  lo0
fe80::1                           lo0                            UHl
   -        -      -  lo0
ff01:1::/32                       link#1                         UC
   -        -      -  wm0
ff01:2::/32                       ::1                            UC
   -        -  33624  lo0
ff02::%wm0/32                     link#1                         UC
   -        -      -  wm0
ff02::%lo0/32                     ::1                            UC
   -        -  33624  lo0
```

- Probamos la opción 4 en el menú (Detalles de la interfaz de red). Podemos ver los detalles de eth1.

```
4
Detalles de interfaces de red:
Ingrese el nombre de la interfaz (ej: wm0, vio0):
wm0
wm0: flags=0x8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        capabilities=0x2bf80<TSO4,IP4CSUM_Rx,IP4CSUM_Tx,TCP4CSUM_Rx>
        capabilities=0x2bf80<TCP4CSUM_Tx,UDP4CSUM_Rx,UDP4CSUM_Tx,TCP6CSUM_Tx>
        capabilities=0x2bf80<UDP6CSUM_Tx>
        enabled=0
        ec_capabilities=0x7<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU>
        ec_enabled=0x2<VLAN_HWTAGGING>
        address: 00:0c:29:cf:c8:84
        media: Ethernet autoselect (1000baseT full-duplex,master)
        status: active
        inet6 fe80::20c:29ff:fecf:c884%wm0/64 flags 0 scopeid 0x1
        inet 10.2.78.35/16 broadcast 10.2.255.255 flags 0
```

- Probamos la opción 5 en el menú (Conexiones UDP y conexiones TCP).

```
Conexiones UDP:
udp:
        95 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        28 dropped due to no socket
        18 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        49 delivered
        74 PCB hash misses
        475 datagrams output
```

WINDOWS

```
function Show-IPConfig {
    Write-Host "`n==== IP CONFIGURATION ====" -ForegroundColor Cyan
    ipconfig /all
}

function Show-NetStat {
    Write-Host "`n==== ACTIVE CONNECTIONS ====" -ForegroundColor Cyan
    netstat -ano
}

function Show-Routes {
    Write-Host "`n==== ROUTING TABLE ====" -ForegroundColor Cyan
    route print
}

function Show-NetworkStats {
    Write-Host "`n==== INTERFACE STATISTICS ====" -ForegroundColor Cyan
    netstat -e
}

function Show-AdapterDetails {
    Write-Host "`n==== NETWORK ADAPTERS (Detailed) ====" -ForegroundColor Cyan
    Get-NetAdapter | Format-List
}

do {
    Clear-Host
    Write-Host "====== NETWORK INFORMATION MENU ======" -ForegroundColor Yellow
    Write-Host "1. Show IP configuration (ipconfig)"
    Write-Host "2. Show active connections (netstat)"
    Write-Host "3. Show routing table (route print)"
    Write-Host "4. Show network interface statistics (netstat -e)"
    Write-Host "5. Show adapter details (Get-NetAdapter)"
    Write-Host "0. Exit"
    $choice = Read-Host "Select an option (0-5)"

    switch ($choice) {
        "1" { Show-IPConfig; Pause }
        "2" { Show-NetStat; Pause }
        "3" { Show-Routes; Pause }
        "4" { Show-NetworkStats; Pause }
        "5" { Show-AdapterDetails; Pause }
        "0" { Write-Host "Exiting..." -ForegroundColor Green }
        default { Write-Host "Invalid option, try again." -ForegroundColor Red; Pause }
    }
} while ($choice -ne "0")
```

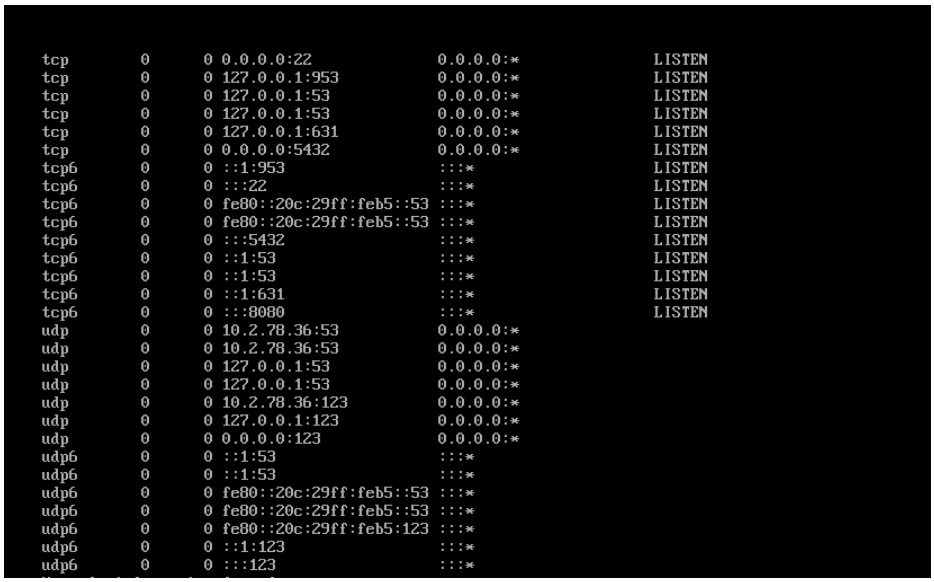
SLACKWARE

- Utilizamos netstat para mostrar información de red como puertos, servicios, estadísticas y conexiones UDP y TCP. También usamos route para ver la tabla de enrutamiento y ethtool para verificar la información de las interfaces de red.

```
 GNU nano 6.0                                Shell1.8.sh
#!/bin/bash
while true;do
        echo "Menu de informacion de red"
        echo "1) Mostrar conexiones de red y puertos en escucha"
        echo "2) Mostrar uso de red"
        echo "3) Mostar tabla de enrutamiento"
        echo "4) Mostrar detalles de la interfax de red"
        echo "5) Mostrar conexiones con un protocolo especificos"
        echo "6) Salir"


        read option

        case $option in
        1)
                echo "Mostrando puertos en escucha y servicios:"
                netstat -tunl
        ;;
        2)
                echo "Estadisticas de red"
                netstat -i
        ;;
        3)
                echo "Tabla de enrutamiento"
                route -n
        ;;
        4)
                echo "Deatlles de la interfaz de red"
                ethtool eth1
        ;;
        5)
                echo "Seleccione el protocolo:"
                echo "1. UDP"
```

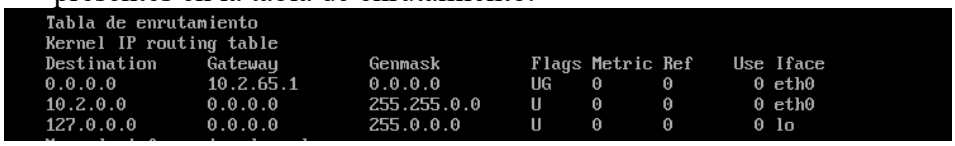
```
          ;;
          5)
                  echo "Seleccione el protocolo:"
                  echo "1. UDP"
                  echo "2. TCO"
                  read protocol
                  case $protocol in
                          1)
                                  echo "Conexiones TCP"
                                  netstat -tan
                          ;;
                          2)
                                  echo "Conexiones UDP"
                                  netstat -uan
                          ;;
                          *)
                                  echo "Opcion invalida de protocolo"
                          ;;
                  esac
          ;;
          6)
                  echo "cerrando programa"
                  break
          ;;
          *)
                  echo "Opcion Invalida"
          ;;
    esac
    done
```

- Probamos la opción 1 del menú (Conexiones de red y puertos en escucha). Como podemos ver, se muestran los protocolos de la capa de transporte junto con los puertos en los que están escuchando, además de las direcciones IP permitidas.

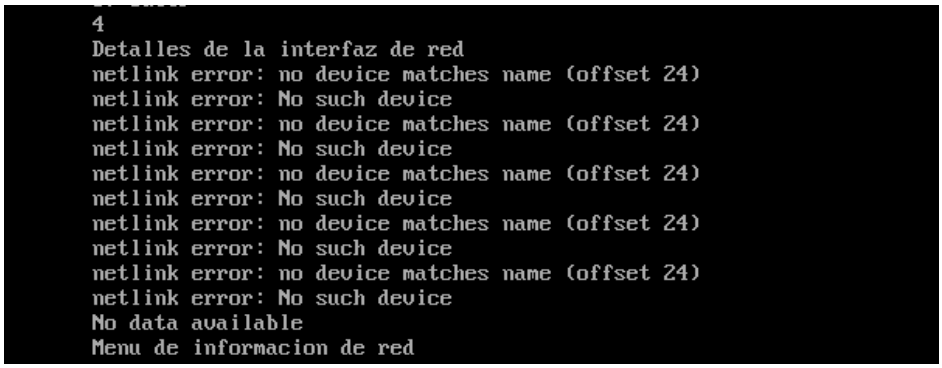


- Probamos la opción 2 del menú (Uso de la red). Podemos ver información sobre eth1 (interfaz de red) y lo (loopback o interfaz de bucle local).

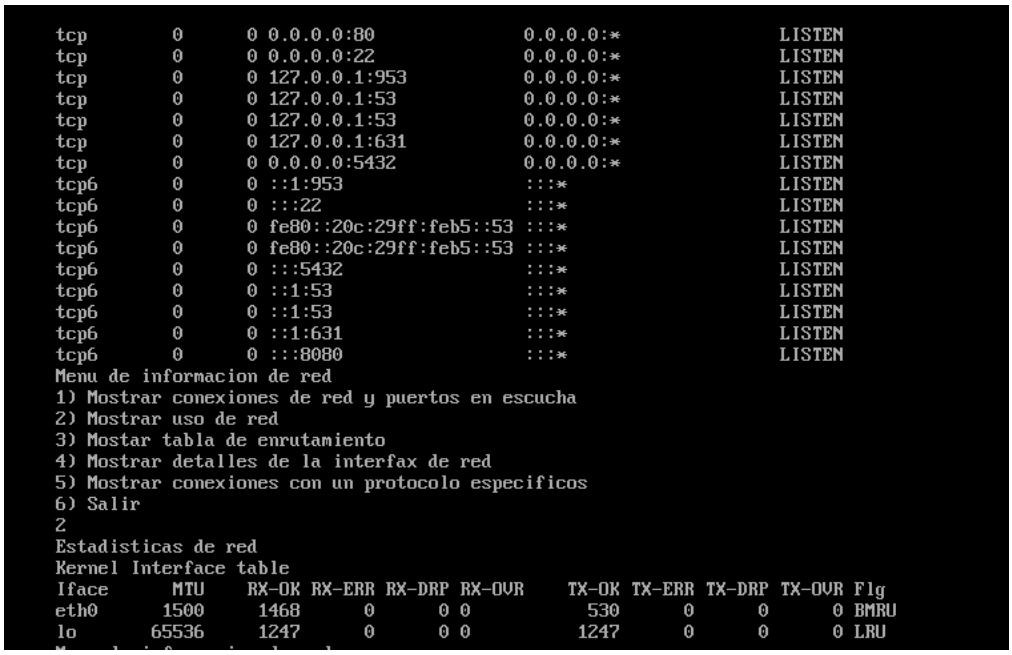
- Probamos la opción 3 del menú (Tabla de enrutamiento). Podemos ver las rutas presentes en la tabla de enrutamiento.



- Probamos la opción 4 del menú (Detalles de la interfaz de red). Podemos ver los detalles de eth1.



- Probamos la opción 5 del menú (Conexiones UDP y conexiones TCP).


tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:5432 0.0.0.0:* LISTEN
tcp6 0 0 ::1:953 :::* LISTEN
tcp6 0 0 :::22 :::* LISTEN
tcp6 0 0 fe80::20c:29ff:feb5::53 :::* LISTEN
tcp6 0 0 fe80::20c:29ff:feb5::53 :::* LISTEN
tcp6 0 0 :::5432 :::* LISTEN
tcp6 0 0 ::1:53 :::* LISTEN
tcp6 0 0 ::1:53 :::* LISTEN
tcp6 0 0 ::1:631 :::* LISTEN
tcp6 0 0 :::8080 :::* LISTEN
Menu de informacion de red
1) Mostrar conexiones de red y puertos en escucha
2) Mostrar uso de red
3) Mostar tabla de enrutamiento
4) Mostrar detalles de la interfax de red
5) Mostrar conexiones con un protocolo especificos
6) Salir
2
Estadisticas de red
Kernel Interface table
Iface MTU RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1500 1468 0 0 0 530 0 0 0 BMRU
lo 65536 1247 0 0 0 1247 0 0 0 LRU

CONCLUTIONS

A partir del desarrollo del laboratorio, se obtuvieron las siguientes conclusiones:

1. **Aplicación práctica de conceptos OSI**: La implementación de redes LAN y WLAN permitió comprender cómo interactúan las capas del modelo OSI, especialmente la capa 2 y la capa 7.
2. **Importancia de las VLANs**: La segmentación de red mediante VLANs mejora la seguridad, organiza el tráfico y permite una administración más efectiva de la red.
3. **Análisis con Wireshark**: El análisis de tramas Ethernet y paquetes ICMP evidenció cómo se estructura la información en la red, reforzando el aprendizaje sobre protocolos como ARP e ICMP.
4. **Configuración inalámbrica segura**: Establecer redes WiFi con WPA2-PSK y canales específicos mostró la relevancia de una planificación adecuada en entornos saturados.
5. **Integración de servicios web**: El despliegue de una aplicación web dinámica sobre Apache/PHP evidenció la conexión entre servicios de red y desarrollo backend.
6. **Conectividad en entornos mixtos**: La combinación de dispositivos cableados e inalámbricos exigió comprender direccionamiento IP, subredes y uso de NAT.
7. **Uso de herramientas CLI**: Dominar comandos como ifconfig, netstat, y route permite al administrador diagnosticar y resolver problemas de red de forma efectiva.
8. **Interoperabilidad de plataformas**: Trabajar con Solaris, Windows Server y sistemas Linux evidenció la necesidad de habilidades multiplataforma.
9. **Simulación y diseño previo**: Packet Tracer fue clave para planear topologías antes de ejecutarlas en el entorno físico o virtual.
10. **Preparación para escenarios reales**: Este laboratorio simula condiciones reales de una red empresarial, preparando al estudiante para retos laborales concretos.

BIBLIOGRAPHY

- Cisco Systems. (2020). *VLANs and Trunks Configuration Guide*. Cisco Networking Academy. https://www.netacad.com/
- Cisco Systems. (s.f.). *Configuring VLANs*. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-3s/ls-xe-3s-book/ls-vlan.html
- IEEE. (2018). *IEEE 802.1Q - VLAN Tagging Standard*. https://ieeexplore.ieee.org/document/8403927
- Wireshark Foundation. (s.f.). *Wireshark User Guide*. https://www.wireshark.org/docs/wsug_html_chunked/
- DigitalOcean. (2023). *How To Use Netstat on Linux*. https://www.digitalocean.com/community/tutorials/how-to-use-netstat-on-linux
- Apache Software Foundation. (s.f.). *Apache HTTP Server Documentation*. https://httpd.apache.org/docs/