

**Integración y Operación de Infraestructuras LAN/WLAN y Servicios de Capa de
Aplicación**

Santiago Botero García

Laura Natalia Perilla Quintero

Escuela Colombiana de Ingeniería Julio Garavito

AYSR-1L: Arquitectura y Servicios de Red

Ing. Jhon Alexander Pachón Pinzón

Noviembre 22, 2025

Resumen

El trabajo realizado permitió afianzar una comprensión global del funcionamiento de las redes modernas, desde la capa de enlace hasta la de aplicación. A lo largo del proceso se configuraron equipos de red, se analizó tráfico, se implementaron VLANs, se desplegaron redes WiFi y se configuraron servicios en servidores, integrando conceptos teóricos con prácticas reales.

En las primeras actividades se estudió el comportamiento de redes Ethernet y WiFi mediante configuraciones básicas de switches y el uso de herramientas como Wireshark. Esto permitió entender el rol de las MAC addresses, el aprendizaje de tablas de conmutación y el funcionamiento de tramas y broadcasts. También se experimentó con el protocolo Spanning Tree, observando cómo evita bucles y determina enlaces activos.

La segmentación mediante VLANs fue clave para organizar y asegurar la red. La creación de VLANs y enlaces troncales mostró cómo separar tráfico, mejorar el rendimiento y facilitar la administración, reforzando la importancia de una adecuada gestión y documentación de los equipos.

En el ámbito inalámbrico se configuraron routers y Access Points aplicando estándares de seguridad, planificación de canales y análisis de espectro. Esto permitió identificar interferencias, evaluar el funcionamiento del beacon frame y comprender las diferencias entre bandas de frecuencia y el impacto de mecanismos como NAT.

Finalmente, en la capa de aplicación se desplegó un servicio web dinámico con Apache, PHP y una base de datos, entendiendo la integración entre servidores, scripting y

almacenamiento. Complementariamente, se utilizaron herramientas de administración y monitoreo en distintos sistemas operativos, incluyendo SNMP y scripts en Shell.

Palabras clave. Ethernet, WiFi, VLAN, Tramas Ethernet, Spanning Tree Protocol (STP), Switches L2/L3, Trunking, WPA2-PSK, NAT, Análisis de tráfico, Wireshark, Apache, PHP, Base de datos relacional, SNMP, Monitoreo de red, Automatización en Shell, Arquitectura de red, Subnetting, Packet Tracer

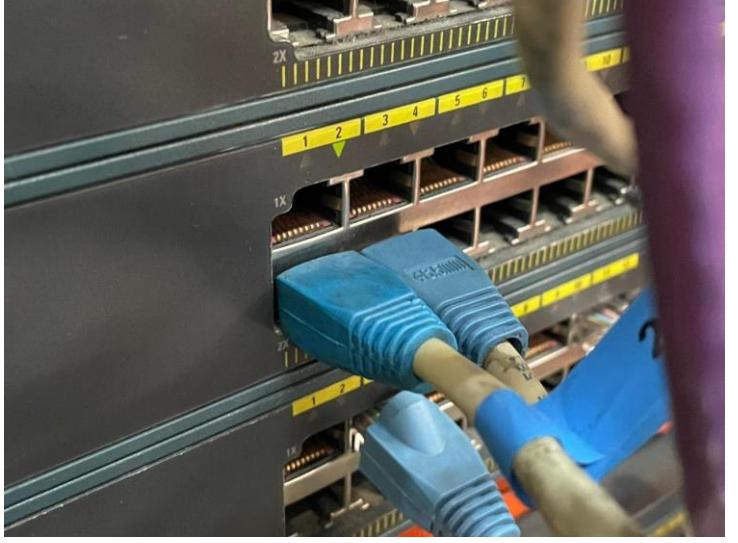
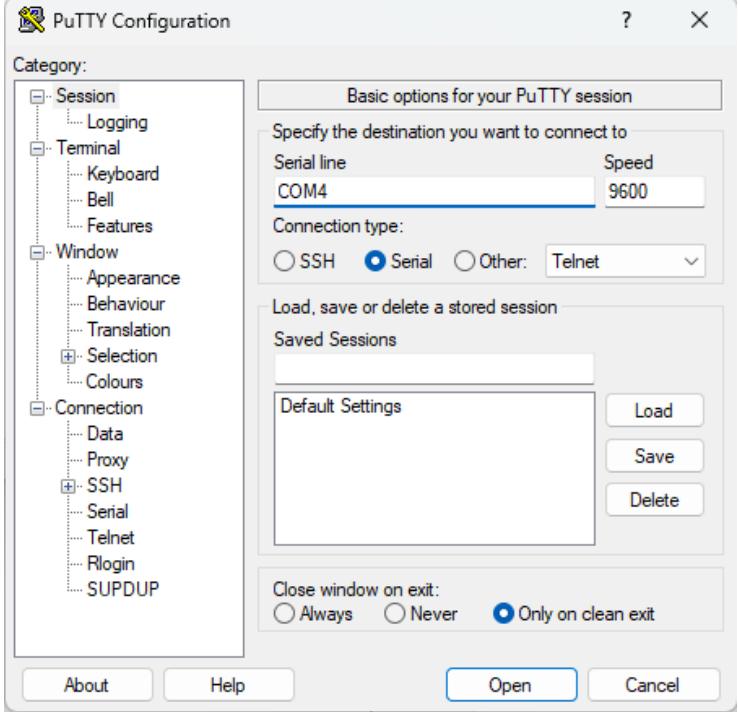
Contenido

Resumen.....	2
Configuración y Seguridad de Switches con VLAN en LAN	5
Redes de comutadores de red más grandes	20
Implementación de Santiago.....	20
Implementación de Natalia	25
Interconexión entre Proyectos	30
Configuración WiFi-básica.....	33
Implementación de Santiago.....	34
Implementación de Natalia	42
Configuración de LAN cableada e inalámbrica.....	47
Implementación de Santiago.....	47
Implementación de Natalia	55
Revisando las redes WiFi-cercanas	59
Redes en banda 2.4 GHz.....	61
Redes en banda 5 GHz.....	61
Instalación del software básico	63
Servicio web dinámico.....	63
Otros comandos útiles.....	68
Módulo de Monitoreo y Diagnóstico de Red.....	68
Mecanismo de Detección de Puertos	71
Gestión de red	73
Conclusiones	76

Configuración y Seguridad de Switches con VLAN en LAN

En este apartado se describe el proceso completo de configuración inicial de switches Cisco dentro de una red LAN, abarcando desde la preparación básica de los dispositivos hasta la implementación de medidas de seguridad y la segmentación de la red mediante VLANs. Se detallan las configuraciones esenciales de identificación del switch, mensajes administrativos, contraseñas de acceso, parámetros de consola y organización de interfaces. Además, se realiza la creación y asignación de VLANs, así como la configuración de enlaces troncales entre switches para permitir la comunicación inter-VLAN. Finalmente, se verifican las conexiones mediante pruebas de conectividad y análisis de tramas, asegurando el correcto funcionamiento de toda la topología implementada.

Acción Realizada	Evidencia Visual
Se estableció la conexión inicial mediante serial enlazado entre un switch Cisco Catalyst 2960 Series y el puerto correspondiente del equipo destinado a su configuración, permitiendo así el acceso a la consola del dispositivo para realizar los ajustes necesarios.	

<p>Cada switch fue conectado a dos computadores utilizando cables directos, estableciendo el enlace desde los puertos de red de cada equipo hacia los puertos FastEthernet0/2 y FastEthernet0/4 del switch, garantizando así la comunicación física.</p>	
<p>Para realizar la conexión por consola al switch, se utilizó el software PuTTY desde el equipo conectado mediante un adaptador de RJ45 a USB, el cual fue enlazado al puerto correspondiente del computador. Posteriormente, a través del Device Manager se identificó el puerto serial asignado por el sistema operativo al adaptador (en este caso, COM4) y se configuró la sesión de PUTTY manteniendo la velocidad predeterminada de 9600 bps.</p>	
<p>Una vez establecida la comunicación por consola, se inició la configuración básica del switch con Cisco IOS. Se asignó un nombre de host, se configuró un mensaje MOTD y se habilitó la sincronización de pantalla en la consola y luego en las líneas VTY. Finalmente, se deshabilitó la búsqueda DNS.</p>	<pre>Would you like to enter the initial configuration dialog? [yes/no]: no Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname boteroperilla boteroperilla(config)#banner motd #Exclusive use for AYSR students# boteroperilla(config)#line console 0 boteroperilla(config-line)#logging synchronous boteroperilla(config-line)#exit boteroperilla(config)#no ip domain-lookup boteroperilla(config)#</pre>

Se asignaron descripciones a las interfaces FastEthernet0/2 y 0/4, indicando su conexión a PC1 y PC2.	<pre>boteroperilla(config)#interface FastEthernet0/2 boteroperilla(config-if)#description connected to PC2 boteroperilla(config-if)#exit boteroperilla(config)#interface FastEthernet0/4 boteroperilla(config-if)#description connected to PC3 boteroperilla(config-if)#exit boteroperilla(config)#[</pre>
Se configuraron contraseñas para el switch: “E” en modo privilegiado, “C” en la consola local y “T” en las líneas VTY, asegurando seguridad y control de acceso.	<pre>boteroperilla(config)#enable secret E boteroperilla(config)#line console 0 boteroperilla(config-line)#password C boteroperilla(config-line)#login boteroperilla(config-line)#logging synchronous boteroperilla(config-line)#exit boteroperilla(config)#line vty 0 4 boteroperilla(config-line)#password T boteroperilla(config-line)#login boteroperilla(config-line)#logging synchronous boteroperilla(config-line)#exit boteroperilla(config)#[</pre>
Se verificó la configuración en ejecución del switch, confirmando que nombre, MOTD, descripciones de interfaces y contraseñas estaban correctamente aplicados.	<pre>boteroperilla#show running-config Building configuration... ! Current configuration : 3199 bytes ! version 12.2 no service pad service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname boteroperilla ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$RwHJ\$gN2N4NwpfvltDtKK50K5v. !</pre>
Una vez verificadas las configuraciones, se guardaron los cambios en la memoria de arranque con copy running-config startup-config. Alternativamente, podrían usarse write memory o copy run start.	<pre>boteroperilla#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] boteroperilla#[</pre>

Antes de proceder con la configuración de VLAN, se realizó un ajuste en la dirección IP del equipo conectado al switch a través de la interfaz FastEthernet0/2. Desde las configuraciones de Windows, se asignó la dirección IPv4 183.24.50.105, con máscara de subred 255.255.0.0, puerta de enlace 183.24.50.1 y servidor DNS preferido 183.24.50.1.

Edit IP settings

Manual

IPv4

On

IP address

183.24.50.105

Subnet mask

255.255.0.0

Gateway

183.24.50.1

Preferred DNS

183.24.50.1

x

DNS over HTTPS

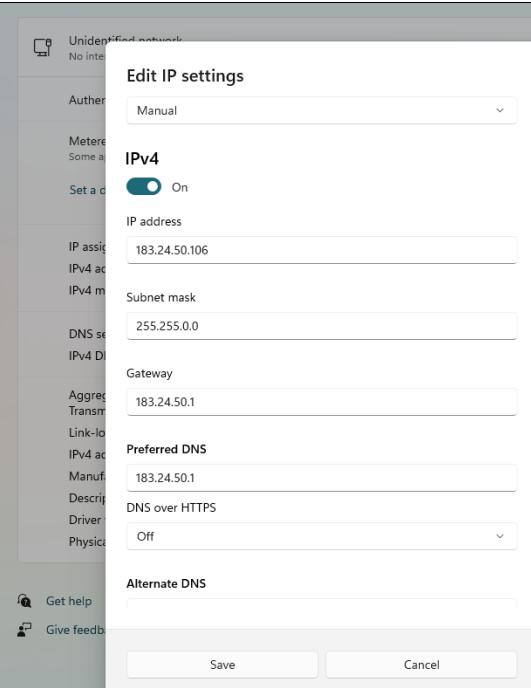
Off

Alternate DNS

Save

Cancel

De manera similar, al segundo equipo conectado al puerto FastEthernet0/4 se le configuró la dirección IPv4 183.24.50.106, con máscara de subred 255.255.0.0, puerta de enlace 183.24.50.1 y servidor DNS preferido 183.25.50.1.



Con la configuración de direcciones IP completada, se verificó la conectividad entre los dos equipos mediante el comando ping. Desde la máquina con IP 183.24.50.105 se envió un ping a la máquina con IP 183.24.50.106, obteniendo como resultado la recepción de los cuatro paquetes enviados, con 0% de pérdida y un promedio de latencia de 1 ms.

```
Microsoft Windows [Version 10.0.22631.5624]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Redes>ping 183.24.50.106

Pinging 183.24.50.106 with 32 bytes of data:
Reply from 183.24.50.106: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.50.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Redes>
```

Para confirmar de manera completa la conectividad bidireccional, se realizó un ping desde la máquina con IP 183.24.50.106 hacia la máquina 183.24.50.105. Los resultados mostraron que se enviaron y recibieron 4 paquetes, con 0% de pérdida, y un promedio de latencia de 629 ms.

```
Microsoft Windows [Version 10.0.26100.4770]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Redes>ping 183.24.50.105

Pinging 183.24.50.105 with 32 bytes of data:
Reply from 183.24.50.105: bytes=32 time=2517ms TTL=128
Reply from 183.24.50.105: bytes=32 time<1ms TTL=128
Reply from 183.24.50.105: bytes=32 time<1ms TTL=128
Reply from 183.24.50.105: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.50.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2517ms, Average = 629ms

C:\Users\Redes>
```

Durante la verificación de conectividad se capturaron 30 paquetes con Wireshark, incluyendo solicitudes y respuestas ARP, paquetes ICMP de ping y tramas STP del switch. Esto permitió confirmar la comunicación entre equipos, la resolución de direcciones MAC y la correcta operación del control de bucles, verificando la estabilidad y confiabilidad de la red.

Figura 1

Packet List de la captura de red

No.	Time	Source	Destination	Protocol	Length Info
1 0.000000	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
2 0.028070	HP_6a:19:17		Broadcast	ARP	60 Who has 183.24.50.1? Tell 183.24.50.106
3 0.302801	Cisco_0d:c9:82		Nearest-Customer-Brm... STP		60 Conf. Root = 32768/1/fc:fb:0d:c9:80 Cc
4 0.581056	HP_6a:19:17		Broadcast	ARP	60 Who has 183.24.50.1? Tell 183.24.50.106
5 0.994087	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
6 1.552699	183.24.50.105		183.24.50.106	ICMP	74 Echo (ping) request id=0x0001, seq=7/1792
7 1.554025	183.24.50.105		183.24.50.105	ICMP	74 Echo (ping) reply id=0x0001, seq=7/1792
8 1.580014	HP_6a:19:17		Broadcast	ARP	60 Who has 183.24.50.1? Tell 183.24.50.106
9 2.307599	Cisco_0d:c9:82		Nearest-Customer-Brm... STP		60 Conf. Root = 32768/1/fc:fb:0d:c9:80 Cc
10 2.557118	183.24.50.105		183.24.50.106	ICMP	74 Echo (ping) request id=0x0001, seq=8/2048
11 2.558197	183.24.50.105		183.24.50.105	ICMP	74 Echo (ping) reply id=0x0001, seq=8/2048
12 2.870458	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
13 3.494908	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
14 3.573345	183.24.50.105		183.24.50.106	ICMP	74 Echo (ping) request id=0x0001, seq=9/2304
15 3.574553	183.24.50.105		183.24.50.105	ICMP	74 Echo (ping) reply id=0x0001, seq=9/2304
16 3.689102	HP_6a:19:17		Broadcast	ARP	60 Who has 183.24.50.1? Tell 183.24.50.106
17 4.312480	Cisco_0d:c9:82		Nearest-Customer-Brm... STP		60 Conf. Root = 32768/1/fc:fb:0d:c9:80 Cc
18 4.496263	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
19 4.547330	Cisco_0d:c9:82		Cisco_0d:c9:82	LOOP	60 Reply
20 4.574044	HP_6a:19:17		Broadcast	ARP	60 Who has 183.24.50.1? Tell 183.24.50.106
21 4.590200	183.24.50.105		183.24.50.106	ICMP	74 Echo (ping) request id=0x0001, seq=10/256
22 4.591492	183.24.50.106		183.24.50.105	ICMP	74 Echo (ping) reply id=0x0001, seq=10/256
23 5.579788	HP_6a:19:17		Broadcast	ARP	60 Who has 183.24.50.1? Tell 183.24.50.106
24 5.903875	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
25 6.080441	HP_6a:19:17	HP_6a:19:46		ARP	60 Who has 183.24.50.105? Tell 183.24.50.106
26 6.080459	HP_6a:19:46	HP_6a:19:17		ARP	42 183.24.50.105 is at 30:13:8b:6a:19:46
27 6.321206	Cisco_0d:c9:82		Nearest-Customer-Brm... STP		60 Conf. Root = 32768/1/fc:fb:0d:c9:80 Cc
28 6.497250	HP_6a:19:46	HP_6a:19:17		ARP	42 Who has 183.24.50.106? Tell 183.24.50.105
29 6.497265	HP_6a:19:46		Broadcast	ARP	42 Who has 183.24.50.1? Tell 183.24.50.105
30 6.498238	HP_6a:19:17	HP_6a:19:46		ARP	60 183.24.50.106 is at 30:13:8b:6a:19:17

Nota. La figura muestra la vista general de los paquetes capturados en Wireshark, incluyendo número de paquete, timestamp, direcciones de origen y destino, protocolo, longitud e información rápida. Esta vista permite observar patrones de tráfico, como ARP broadcast, ICMP ping y mensajes STP, proporcionando un panorama completo de la comunicación en la red.

En la vista de lista de paquetes (Packet List) se pueden observar todos los paquetes capturados con información de tiempo, dirección de origen y destino, protocolo, longitud del paquete y detalles rápidos de cada mensaje. Esta vista permite identificar patrones de tráfico, como los paquetes broadcast de ARP y los mensajes ICMP de ping, así como la presencia de mensajes de control de switches mediante STP.

Figura 2

Paquete ARP broadcast para resolución de dirección IP

```

Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D48BA77A-4C2A-4EBB-A7A5-07ACF1
  Section number: 1
  Interface id: 0 (\Device\NPF_{D48BA77A-4C2A-4EBB-A7A5-07ACF1)
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 15, 2025 09:29:37.413374000 SA Pacific Standard Time
  UTC Arrival Time: Nov 15, 2025 14:29:37.413374000 UTC
  Epoch Arrival Time: 1763216977.413374000
  [Time shift for this packet: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 42 bytes (336 bits)
  Capture Length: 42 bytes (336 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
    Character encoding: ASCII (0)
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
  Ethernet II, Src: HP_6a:19:46 (30:13:8b:6a:19:46), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: HP_6a:19:46 (30:13:8b:6a:19:46)
    Type: ARP (0x0806)
    [Stream index: 0]
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HP_6a:19:46 (30:13:8b:6a:19:46)
    Sender IP address: 183.24.50.105
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 183.24.50.1
0000 ff ff ff ff ff 30 13 8b 6a 19 46 08 06 00 01 .. j F ...
0010 08 00 06 04 00 01 30 13 8b 6a 19 46 b7 18 32 69 .. 0.. j F .. 2i
0020 00 00 00 00 00 00 b7 18 32 01 .. 2.

```

Nota. La figura ilustra un paquete ARP tipo request, enviado como broadcast para resolver la dirección IP 183.24.50.1 a su correspondiente dirección MAC. El paquete muestra la dirección MAC de origen, la dirección de destino broadcast (FF:FF:FF:FF:FF:FF) y el contenido de la solicitud. Esta captura permite analizar cómo los dispositivos resuelven direcciones IP en la red local.

Los paquetes ARP se capturaron principalmente como solicitudes y respuestas para la resolución de direcciones IP a direcciones MAC. Los paquetes de tipo ARP request se envían como broadcast, con destino FF:FF:FF:FF:FF:FF, mientras que las respuestas son unicast. Por ejemplo, el paquete “Who has 183.24.50.1? Tell 183.24.50.105” representa una solicitud ARP broadcast, y “183.24.50.105 is at 30:13:8b:6a:19:46” es la respuesta unicast correspondiente. Este análisis permite relacionar direcciones IP con MAC y observar la dinámica de resolución de direcciones dentro de la red.

Figura 3

Paquete ICMP ping request y reply

```

▼ Frame 6: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D48BA77A-4C2A-4EBB-A7A5-07ACFBEE5503}
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{D48BA77A-4C2A-4EBB-A7A5-07ACFBEE5503})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 15, 2025 09:29:38.966073000 SA Pacific Standard Time
    UTC Arrival Time: Nov 15, 2025 14:29:38.966073000 UTC
    Epoch Arrival Time: 1763216978.966073000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 558.612000 milliseconds]
    [Time delta from previous displayed frame: 558.612000 milliseconds]
    [Time since reference or first frame: 1.552699000 seconds]
    Frame Number: 6
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ether:type:ip:icmp:data]
    Character encoding: ASCII (8)
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
  ▶ Ethernet II, Src: HP_6a:19:46 (30:13:8b:6a:19:46), Dst: HP_6a:19:17 (30:13:8b:6a:19:17)
    ▶ Destination: HP_6a:19:17 (30:13:8b:6a:19:17)
    ▶ Source: HP_6a:19:46 (30:13:8b:6a:19:46)
      Type: IPv4 (0x0800)
      [Stream index: 3]
  ▶ Internet Protocol Version 4, Src: 183.24.50.105, Dst: 183.24.50.106
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x54bc (21692)
    ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 183.24.50.105
    Destination Address: 183.24.50.106
    [Stream index: 0]
  ▶ Internet Control Message Protocol
    Type: Echo (ping) request (8)
    Code: 0
    Checksum: 0x4d54 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 7 (0x0007)
    Sequence Number (LE): 1792 (0x0700)
    [Response Frame: 7]
  ▶ Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
    [Length: 32]

```

Nota. La figura presenta un par de paquetes ICMP, consistentes en un ping request y su correspondiente reply entre los hosts 183.24.50.105 y 183.24.50.106. Se pueden observar los campos de identificador, número de secuencia y TTL, así como la correspondencia entre solicitud y respuesta. Esta captura demuestra la conectividad entre los dispositivos y permite calcular tiempos de respuesta.

Los paquetes ICMP capturados corresponden a solicitudes y respuestas de ping entre las direcciones IP 183.24.50.105 y 183.24.50.106. Cada paquete ICMP contiene información de identificador, número de secuencia y TTL. Al comparar solicitudes y respuestas se puede verificar la correspondencia entre ellas, calcular el tiempo de respuesta (RTT) y detectar posibles

pérdidas de paquetes. Este análisis confirma la conectividad entre los dispositivos y permite relacionar las direcciones IP con las direcciones MAC previamente obtenidas mediante ARP.

Figura 4

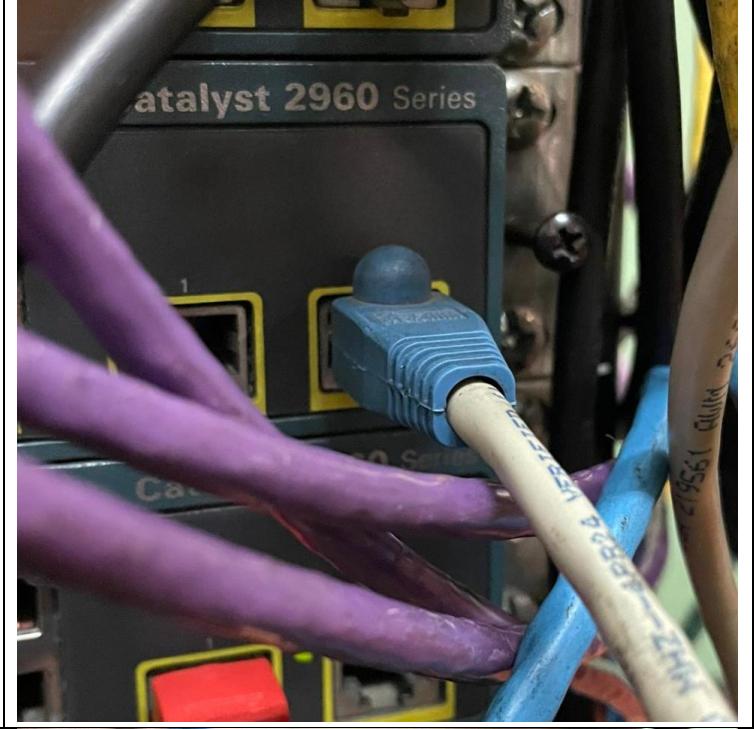
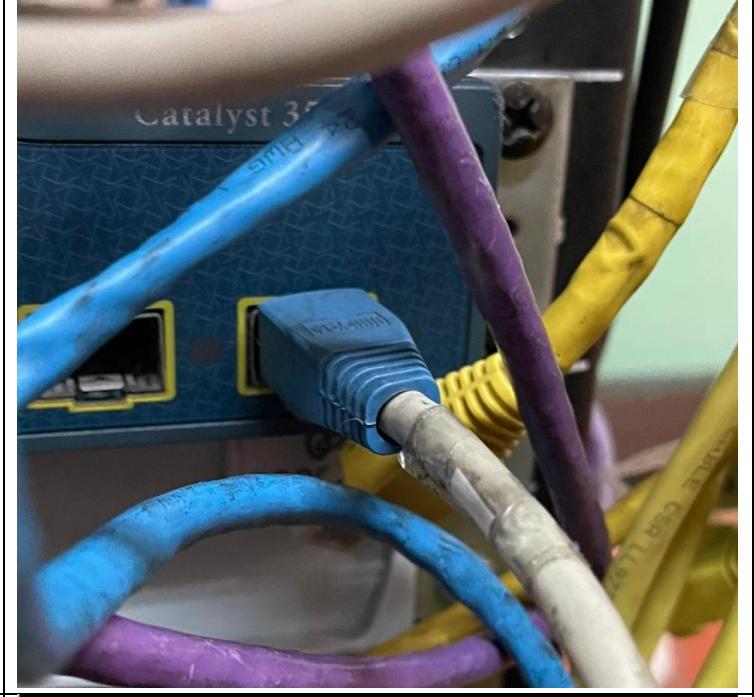
Paquete STP (Spanning Tree Protocol) de un switch Cisco

Nota. La figura muestra un paquete STP enviado por el switch Cisco_0d:c9:82. Se observan campos relevantes para la topología de la red, como Root Bridge ID, costo de camino y puerto. Esta captura permite analizar cómo los switches controlan la estructura de la red, previenen bucles y determinan la ruta óptima entre dispositivos.

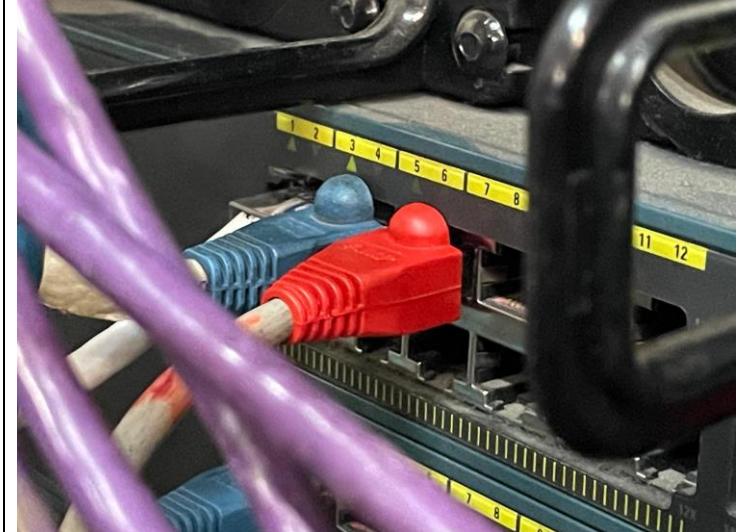
Los paquetes de tipo STP (Spanning Tree Protocol) provienen del switch Cisco (Cisco_0d:c9:82) y contienen información sobre la topología de la red, como el Root Bridge ID, el costo de camino y el puerto. Estos mensajes no transportan datos de usuario, sino que sirven para controlar la estructura de la red, evitando bucles y estableciendo la ruta óptima entre switches. El análisis de STP permite entender cómo se determina la topología y cómo se elige el root bridge.

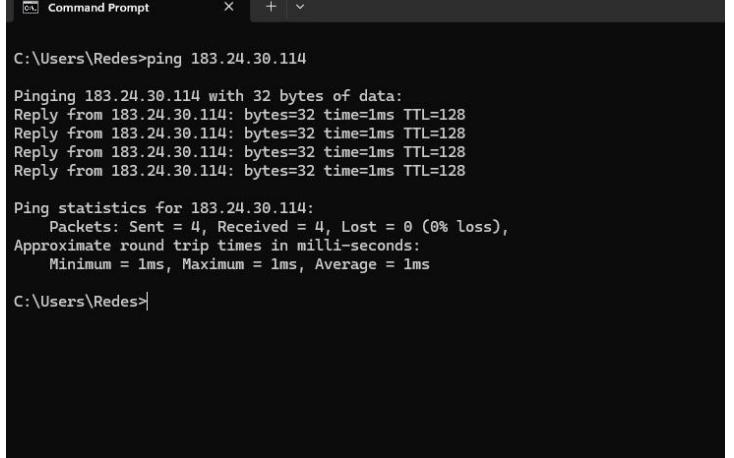
Cada paquete capturado puede analizarse en detalle mostrando la trama Ethernet, donde se distinguen los siguientes elementos: dirección MAC de destino (unicast o broadcast), dirección MAC de origen, tipo de protocolo (ARP, IP, STP, etc.), payload (datos transportados) y control de errores mediante FCS (Frame Check Sequence). La vista de bytes permite observar la representación hexadecimal de la trama completa y verificar la integridad de los paquetes.

Acción Realizada	Evidencia Visual
Para iniciar la segmentación de la red, se ingresó al modo de configuración global del switch para crear las VLAN necesarias. Se configuraron dos VLANs: la VLAN 50, denominada “systems”, y la VLAN 55, denominada “others”	<pre>boteroperilla(config)#vlan 50 boteroperilla(config-vlan)#name systems boteroperilla(config-vlan)#exit boteroperilla(config)#vlan 55 boteroperilla(config-vlan)#name others boteroperilla(config-vlan)#exit boteroperilla(config)#[REDACTED]</pre>
A continuación, se procedió a asignar los puertos del switch a las VLAN correspondientes, de acuerdo con la segmentación definida previamente. En este caso, el equipo conectado al puerto FastEthernet0/2 fue asignado a la VLAN 50 (systems), mientras que el equipo en FastEthernet0/4 quedó en la VLAN 55 (others).	<pre>boteroperilla(config)#interface FastEthernet0/2 boteroperilla(config-if)#switchport mode access boteroperilla(config-if)#switchport access vlan 50 boteroperilla(config-if)#exit boteroperilla(config)#interface FastEthernet0/4 boteroperilla(config-if)#switchport mode access boteroperilla(config-if)#switchport access vlan 55</pre>

<p>Para establecer la interconexión física entre los switches, se conectó un cable cruzado desde el puerto GigabitEthernet0/2 del Cisco Catalyst 2960 Series hacia el puerto GigabitEthernet0/2 del switch Cisco Catalyst 3500 Series de nuestros compañeros.</p>	
<p>Es importante aclarar que durante la conexión hacia el Catalyst 3500 corresponde a la interconexión con los equipos de otro grupo. Dichos equipos realizaron su propia configuración de red, asignando direcciones IP dentro del rango 183.24.50.0/16, y configurando sus respectivas VLANs.</p>	
<p>Para permitir la comunicación entre VLANs de diferentes switches, se configuró un enlace trunk en la interfaz que conecta ambos dispositivos. En nuestro caso, el enlace correspondía a GigabitEthernet0/2. Se estableció el</p>	<pre>boterooperilla(config)#interface GigabitEthernet0/2 boterooperilla(config-if)#switchport mode trunk boterooperilla(config-if)#switchport trunk allowed vlan 50,55 boterooperilla(config-if)#exit boterooperilla(config)#[</pre>

<p>modo trunk y se especificaron las VLANs permitidas, 50 y 55.</p>	<p>Para verificar la correcta creación y asignación de las VLANs en el switch, se utilizó el comando show vlan brief, el cual permitió revisar el estado de las VLANs, mostrando cuáles estaban activas, sus identificadores (IDs), los nombres asignados y los puertos asociados a cada VLAN. La salida del comando confirmó que la VLAN 50 (systems) y la VLAN 55 (others) se encontraban correctamente configuradas y que los puertos correspondientes a los equipos del grupo estaban asignados a sus VLANs respectivas</p> <pre>botoperilla#show vlan brief VLAN Name Status Ports ----- ----- 1 default active Fa0/1, Fa0/3, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2 10 Valexa active 20 Bonyurt active 35 PRIVADA active 50 systems active Fa0/2 55 others active Fa0/4 1002 fddi-default act/unsup 1003 token-ring-default act/unsup 1004 fddinet-default act/unsup 1005 trnet-default act/unsup botoperilla#</pre>
<p>Para comprobar que el enlace trunk entre los switches estaba correctamente configurado, se utilizó el comando show interfaces trunk. Este comando permitió verificar qué interfaces del switch estaban operando en modo trunk, qué VLANs estaban permitidas a través del enlace y el estado de cada VLAN en el trunk. La salida confirmó que la interfaz GigabitEthernet0/2 estaba activa como trunk y que las VLANs 50 y 55 podían comunicarse correctamente entre los switches.</p>	<pre>botoperilla#show interfaces trunk Port Mode Encapsulation Status Native vlan GigabitEthernet0/2 on 802.1q trunking 1 Port Vlans allowed on trunk GigabitEthernet0/2 50,55 Port Vlans allowed and active in management domain GigabitEthernet0/2 50,55 Port Vlans in spanning tree forwarding state and not pruned GigabitEthernet0/2 50,55 botoperilla#</pre>
<p>Para verificar el correcto funcionamiento del enlace trunk y la comunicación entre VLANs de diferentes switches, se realizó un ping desde el PC con dirección IP 183.24.50.106 hacia el equipo con IP 183.24.50.107, correspondiente a</p>	<pre>C:\Users\Redes>ping 183.24.50.107 Pinging 183.24.50.107 with 32 bytes of data: Reply from 183.24.50.107: bytes=32 time<1ms TTL=128 Ping statistics for 183.24.50.107: 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></pre>

<p>la VLAN 50 del otro grupo. La prueba arrojó que se enviaron y recibieron 4 paquetes, con 0% de pérdida y un promedio de latencia de 0 ms.</p>	
<p>De manera similar, para comprobar la comunicación entre la VLAN 55 de nuestro grupo y la correspondiente del otro grupo, se realizó un ping desde el PC con IP 183.24.50.105 hacia el equipo con IP 183.24.50.108. La prueba mostró que se enviaron y recibieron 4 paquetes, con 0% de pérdida y una latencia promedio de 0 ms, confirmando nuevamente que la interconexión entre VLANs a través del enlace trunk funcionaba correctamente.</p>	<pre>C:\Users\Redes>ping 183.24.50.108 Pinging 183.24.50.108 with 32 bytes of data: Reply from 183.24.50.108: bytes=32 time=1ms TTL=128 Reply from 183.24.50.108: bytes=32 time=1ms TTL=128 Reply from 183.24.50.108: bytes=32 time=1ms TTL=128 Reply from 183.24.50.108: bytes=32 time<1ms TTL=128 Ping statistics for 183.24.50.108: 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></pre>
<p>En la imagen se observa la conexión física en la switch utilizada para interconectar las configuraciones de todo el grupo. El puerto FastEthernet0/1 está asignado a la VLAN 50 denominada systems, mientras que el puerto FastEthernet0/3 pertenece a la VLAN 55 denominada others. Además, se habilitó el puerto FastEthernet0/5 para establecer un enlace hacia otro switch, configurado como trunk, lo que permite el transporte de tráfico de ambas VLAN a través de un único enlace. Esta configuración asegura la comunicación entre los diferentes segmentos de la red, manteniendo la separación lógica de las VLAN y garantizando la interoperabilidad entre los equipos del grupo.</p>	

<p>En esta captura se muestra la configuración realizada en el switch para habilitar el enlace troncal en el puerto FastEthernet0/5. Se aplicó el comando switchport mode trunk para permitir el transporte de múltiples VLAN por el mismo enlace físico, y posteriormente se especificaron las VLAN permitidas (50 y 55) mediante switchport trunk allowed vlan 50,55.</p>	<pre>boteroperilla(config)#interface FastEthernet0/5 boteroperilla(config-if)#switchport mode trunk boteroperilla(config-if)#switchport trunk allowed vlan 50,55 *Mar 1 18:36:29.550: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down boteroperilla(config-if)#switchport modetrunk *Mar 1 18:36:32.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up boteroperilla(config-if)#switchport trunk allowed vlan 50,55 boteroperilla(config-if)#exit boteroperilla(config)#</pre>
<p>La segunda captura evidencia la verificación de la conectividad entre equipos pertenecientes a diferentes switches del grupo. Se realizó un ping hacia la dirección IP 183.24.30.113, obteniendo respuestas exitosas con un tiempo mínimo de 1 ms y sin pérdida de paquetes.</p>	<pre>C:\Users\Redes>ping 183.24.30.113 Pinging 183.24.30.113 with 32 bytes of data: Reply from 183.24.30.113: bytes=32 time=1ms TTL=128 Ping statistics for 183.24.30.113: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms</pre>
<p>En esta captura se muestra la segunda prueba de conectividad, esta vez hacia la dirección IP 183.24.30.114, correspondiente a un equipo conectado al switch de otro compañero del grupo.</p>	 <pre>Command Prompt C:\Users\Redes>ping 183.24.30.114 Pinging 183.24.30.114 with 32 bytes of data: Reply from 183.24.30.114: bytes=32 time=1ms TTL=128 Ping statistics for 183.24.30.114: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms C:\Users\Redes></pre>

En esta prueba se realizó un ping hacia la dirección IP 183.24.30.116, correspondiente a un equipo conectado en otro switch dentro de la topología completa del grupo. El resultado muestra respuestas exitosas con tiempos de 1 a 3 ms y sin pérdida de paquetes, lo que confirma que la interconexión entre todos los switches mediante enlaces troncales funciona correctamente.

```
C:\Users\Redes>ping 183.24.30.116

Pinging 183.24.30.116 with 32 bytes of data:
Reply from 183.24.30.116: bytes=32 time=3ms TTL=128
Reply from 183.24.30.116: bytes=32 time=2ms TTL=128
Reply from 183.24.30.116: bytes=32 time=1ms TTL=128
Reply from 183.24.30.116: bytes=32 time=2ms TTL=128

Ping statistics for 183.24.30.116:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

C:\Users\Redes>
```

Finalmente, para dejar los switches en su estado de fábrica y limpiar todas las configuraciones realizadas durante la práctica, se procedió a borrar la configuración de inicio utilizando el comando erase startup-config seguido de reload.

```
boteroperilla#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
boteroperilla#
*Mar 1 01:43:01.195: $SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
boteroperilla#
```

Redes de conmutadores de red más grandes

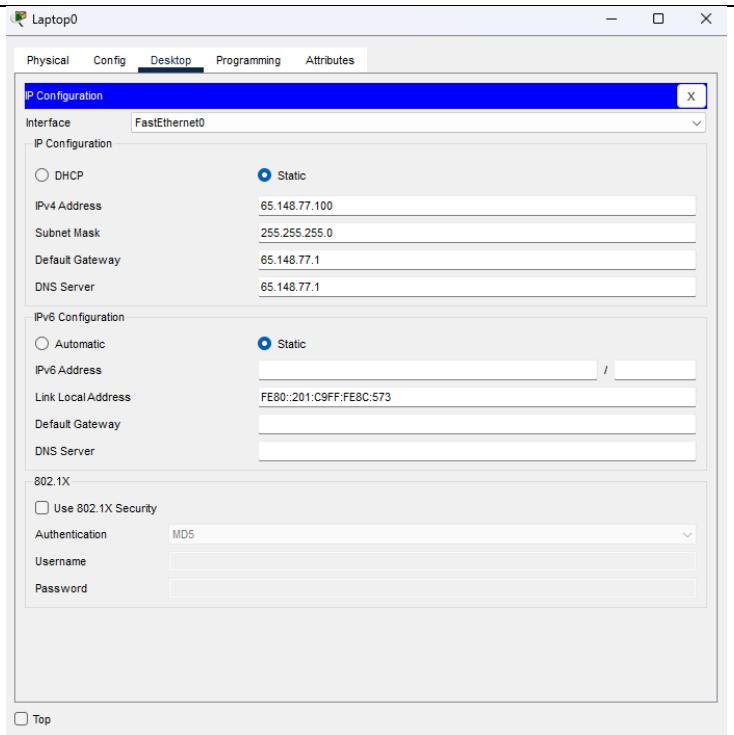
En esta sección se abordará la implementación de redes con múltiples switches utilizando Cisco Packet Tracer. Cada implementación incluye la configuración básica de todos los switches, la asignación de direcciones a computadoras y servidores, la verificación de conectividad entre los dispositivos, y el análisis del comportamiento de la red en modo simulación, observando la transmisión de tramas Ethernet y la tabla de reenvío de los switches. Además, se explorará el funcionamiento del algoritmo Spanning Tree para prevenir bucles en la red. Finalmente, se realizará la fusión de los proyectos individuales para presentar un entorno de red interconectado completo.

Implementación de Santiago

Acción Realizada	Captura de pantalla
Se diseñó la siguiente topología de red, que incluye un total de 5 switches, 1 switch multilayer, 3 hubs, 2 laptops, 3 servidores y 11 computadoras.	

Se configura el siguiente esquema de red, que utiliza la red 65.148.77.0/24 con máscara 255.255.255.0 y como gateway el 65.148.77.1, asignando el rango 65.148.77.100–65.148.77.120 a los dispositivos, los cuales permanecen todos dentro de la misma red cambiando únicamente el host ID; así, las IP quedan organizadas de la siguiente manera: PC0 65.148.77.100, PC1 65.148.77.101, PC2 65.148.77.102, Laptop0 65.148.77.103, PC3 65.148.77.104, PC4 65.148.77.105, PC5 65.148.77.106, PC6 65.148.77.107, PC7 65.148.77.108, PC8 65.148.77.109, Server0 65.148.77.110, Server1 65.148.77.111, Server2 65.148.77.112, PC9 65.148.77.113, PC10 65.148.77.114, y Laptop1 con dirección 65.148.77.115.

Para cada switch se debe realizar la misma configuración básica, comenzando con enable y configure terminal, asignando un nombre con hostname Switch, deshabilitando la resolución de dominios mediante no ip domain-lookup, activando spanning-tree mode pvst y spanning-tree portfast default, habilitando el cifrado de contraseñas con service password-encryption, configurando el banner de acceso mediante banner motd estableciendo la contraseña privilegiada con enable secret class, y configurando el acceso por consola con line console 0,

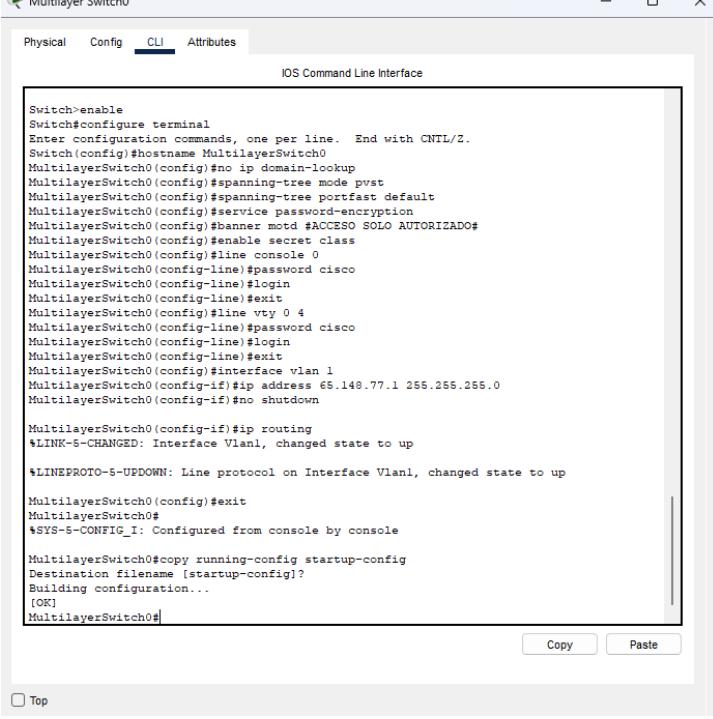


```

*LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
*LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch1
Switch1(config)#no ip domain-lookup
Switch1(config)#spanning-tree mode pvst
Switch1(config)#spanning-tree portfast default
Switch1(config)#service password-encryption
Switch1(config)#banner motd #ACCESO SOLO AUTORIZADO#
Switch1(config)#enable secret class
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#exit
Switch1(config)#line vty 0 4
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#exit
Switch1(config)#exit
Switch1#*SYS-5-CONFIG_I: Configured from console by console
Switch1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch1#

```

<p>password cisco, login, seguido de la configuración de las líneas virtuales VTY mediante line vty 0 4, password cisco y login.</p>	
<p>En el multilayer switch se aplicó una configuración completa iniciando con enable y configure terminal, asignándole el nombre MultilayerSwitch0 y deshabilitando la resolución de dominios mediante no ip domain-lookup. Se habilitó spanning-tree mode pvst junto con spanning-tree portfast default, se activó el cifrado de contraseñas con service password-encryption y se configuró el banner de acceso usando banner motd. También se estableció la contraseña privilegiada con enable secret class, se configuró el acceso por consola con line console 0, password cisco y login, y luego las líneas VTY mediante line vty 0 4, password cisco y login. Posteriormente, se configuró la interfaz VLAN 1 asignando la dirección 65.148.77.1 con máscara 255.255.255.0, se activó con no shutdown y se habilitó el enrutamiento con ip routing. Finalmente, se guardaron los cambios usando copy running-config startup-config.</p>	 <pre> Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname MultilayerSwitch0 MultilayerSwitch0(config)#no ip domain-lookup MultilayerSwitch0(config)#spanning-tree mode pvst MultilayerSwitch0(config)#spanning-tree portfast default MultilayerSwitch0(config)#service password-encryption MultilayerSwitch0(config)#banner motd #ACCESO SOLO AUTORIZADO# MultilayerSwitch0(config)#enable secret class MultilayerSwitch0(config)#line console 0 MultilayerSwitch0(config-line)#password cisco MultilayerSwitch0(config-line)#login MultilayerSwitch0(config-line)#exit MultilayerSwitch0(config)#line vty 0 4 MultilayerSwitch0(config-line)#password cisco MultilayerSwitch0(config-line)#login MultilayerSwitch0(config-line)#exit MultilayerSwitch0(config)#interface vlan 1 MultilayerSwitch0(config-if)#ip address 65.148.77.1 255.255.255.0 MultilayerSwitch0(config-if)#no shutdown MultilayerSwitch0(config-if)#ip routing *LINK-5-CHANGED: Interface Vlan1, changed state to up *LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up MultilayerSwitch0(config)#exit MultilayerSwitch0# *SYS-5-CONFIG_I: Configured from console by console MultilayerSwitch0#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] MultilayerSwitch0# </pre>

Desde la PC2, con IP 65.148.77.102, se realizó un ping a la máquina PC3, con IP 65.148.77.104, obteniendo como resultado el envío de 4 paquetes, sin pérdida de paquetes (0%) y un tiempo de respuesta promedio de 1 ms.

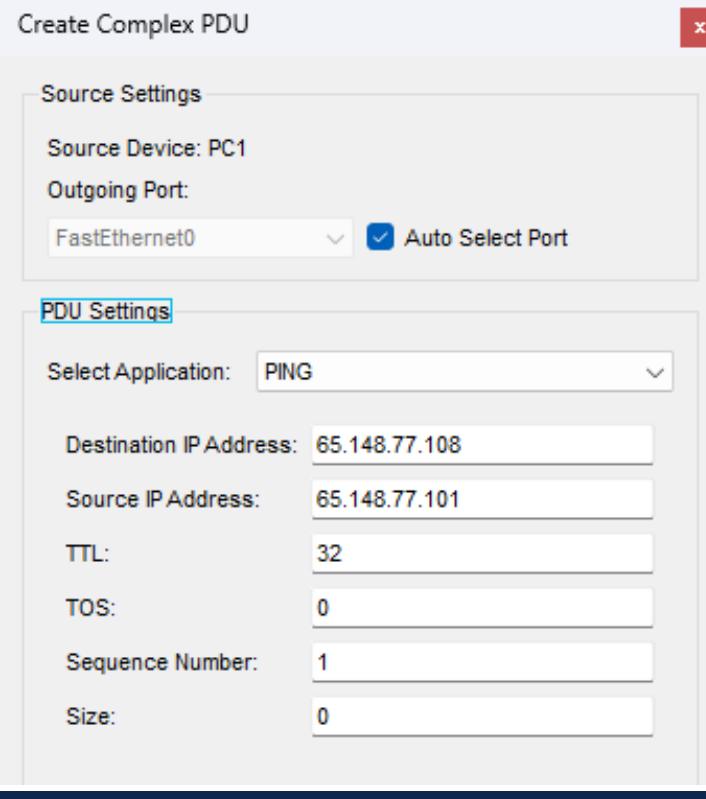
```
Cisco Packet Tracer PC Command Line 1.0
C:\ping 65.148.77.104

Pinging 65.148.77.104 with 32 bytes of data:
Reply from 65.148.77.104: bytes=32 time<1ms TTL=128
Reply from 65.148.77.104: bytes=32 time=1ms TTL=128
Reply from 65.148.77.104: bytes=32 time<1ms TTL=128
Reply from 65.148.77.104: bytes=32 time<1ms TTL=128

Ping statistics for 65.148.77.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\|
```

Para realizar las pruebas, se crearon 4 complex PDU con las siguientes configuraciones: desde PC1 a PC7, desde PC0 a PC9, desde Server0 a Server1 y desde Laptop0 a Laptop1, todas con TTL 32, TOS 0, Sequence number 1, Size 0 y Time 0.



El resultado de todas las pruebas fue exitoso, ya que cada uno de los complex PDU enviados entre los dispositivos, ya sea desde PC1 a

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC1	65.148.77.108	ICMP	■	0.000	N	0	(edit)	
●	Successful	PC0	65.148.77.113	ICMP	■	0.000	N	1	(edit)	
●	Successful	Server0	65.148.77.111	ICMP	■	0.000	N	2	(edit)	
●	Successful	Laptop0	65.148.77.115	ICMP	■	0.000	N	3	(edit)	

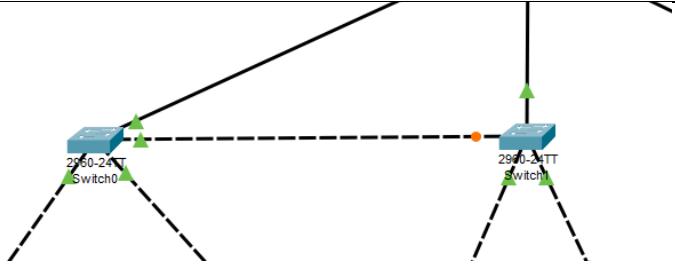
PC7, desde PC0 a PC9, desde Server0 a Server1, o desde Laptop0 a Laptop1, se completó correctamente y se obtuvo un status successful en todos los casos.

Al principio, las transmisiones son de tipo broadcast debido al uso de ARP para resolver direcciones MAC a partir de direcciones IP. Luego, STP comienza a funcionar para evitar bucles de red y establecer el camino más eficiente entre los switches. Despues, el protocolo CDP permite que los dispositivos Cisco descubran y comparten información sobre la topología de la red. Finalmente, DTP negocia dinámicamente los enlaces troncales entre los switches, asegurando que la comunicación entre ellos se realice correctamente y sin conflictos.

Al conectar Switch0 y Switch1 con un cable cruzado (crossover), PVST permite que STP funcione por cada VLAN, evitando bucles. PortFast se usa en puertos de PCs para evitar esperas, pero no en enlaces entre switches, donde STP bloquea un puerto si hay múltiples enlaces para evitar loops.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.000	--	PC1	ARP
	0.001	PC1	Switch2	ARP
	0.002	Switch2	Laptop0	ARP
	0.002	Switch2	PC0	ARP
	0.002	Switch2	PC2	ARP
	0.002	Switch2	Switch0	ARP
	0.003	Switch0	Multilayer Switch0	ARP
	0.003	Switch0	Hub0	ARP
	0.004	Multilayer Switch0	Switch1	ARP
	0.004	Multilayer Switch0	Hub1	ARP
	0.004	Hub0	PC3	ARP
	0.004	Hub0	PC4	ARP
	0.005	Switch1	Switch3	ARP
	0.005	Switch1	Switch4	ARP
	0.005	Hub1	Switch5	ARP
	0.005	Hub1	Hub2	ARP
	0.006	Switch3	PC5	ARP
	0.006	Switch3	PC6	ARP
	0.006	Switch4	PC7	ARP
	0.006	Switch4	PC8	ARP
	0.006	Switch5	Server0	ARP
	0.006	Switch5	Server1	ARP

Reset Simulation Constant Delay Captured to: 11.155 s



Para probar STP, espera unos segundos y luego ejecuta show spanning-tree en cualquier switch. El resultado mostrará el estado de los puertos, indicando cuál es el puerto root (Fa0/1), el alternativo bloqueado (Fa0/2), y los puertos designados (Gi0/1 y Gi0/2) en estado forwarding.

```

Switch1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority 32769
            Address 0001.43AE.16AD
            Cost 19
            Port  1(FastEthernet0/1)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
            Address 00D0.FF33.6B85
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
----- ---- -- -- -----
Fa0/2  Altn BLK 19 128.2 P2p
Fa0/1  Root FWD 19 128.1 P2p
Gi0/1  Desg FWD 4 128.25 P2p
Gi0/2  Desg FWD 4 128.26 P2p

Switch1>

```

Implementación de Natalia

Acción Realizada	Captura de pantalla
El objetivo de esta configuración es verificar la conectividad entre todos los dispositivos, analizar el comportamiento de los switches mediante la tabla de direcciones MAC y observar cómo se optimiza el tráfico después del proceso de aprendizaje.	

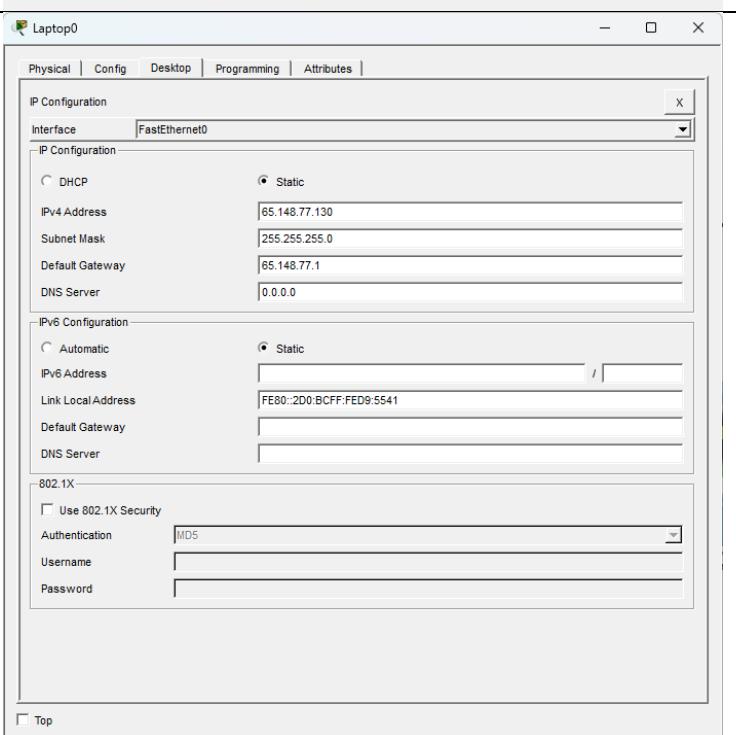
Esta configuración asegura la seguridad básica del equipo, facilita la administración y cumple con las buenas prácticas de identificación y documentación en redes.

```

$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
$LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
$LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch0
Switch(config)#banner motd # Uso exclusivo para estudiantes de AYSR #
Switch0(config)#no ip domain-lookup
Switch0(config)#enable secret Clave_E
Switch0(config)#line console 0
Switch(config-line)#logging synchronous
Switch(config-line)#password Clave_C
Switch0(config-line)#login
Switch0(config-line)#exit
Switch0(config)#line vty 0 15
Switch0(config-line)#logging synchronous
Switch0(config-line)#password Clave_T
Switch0(config-line)#login
Switch0(config-line)#exit
Switch0(config)#interface FastEthernet0/1
Switch0(config-if)#description "Conexion con Multilayer Switch0"
Switch0(config-if)#exit
Switch0(config-if)#description "Conexion con Switch2"
Switch0(config-if)#exit
Switch0(config-if)#description "Conexion con Hub0"
Switch0(config-if)#exit
Switch0(config)#end

```



En esta imagen se muestra la verificación de conectividad entre los dispositivos de la red mediante el comando ping ejecutado en la línea de comandos

```
C:\>ping 65.148.77.141
Pinging 65.148.77.141 with 32 bytes of data:
Reply from 65.148.77.141: bytes=32 time<1ms TTL=128
Reply from 65.148.77.141: bytes=32 time<1ms TTL=128
Reply from 65.148.77.141: bytes=32 time<1ms TTL=128
Reply from 65.148.77.141: bytes=32 time=<1ms TTL=128

Ping statistics for 65.148.77.141:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 65.148.77.142
Pinging 65.148.77.142 with 32 bytes of data:
Reply from 65.148.77.142: bytes=32 time=1ms TTL=128
Reply from 65.148.77.142: bytes=32 time<1ms TTL=128
Reply from 65.148.77.142: bytes=32 time=4ms TTL=128
Reply from 65.148.77.142: bytes=32 time<1ms TTL=128

Ping statistics for 65.148.77.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

El resultado indica “No ARP Entries Found”, lo que significa que en ese momento no existen direcciones IP asociadas a direcciones MAC en la caché ARP del equipo.

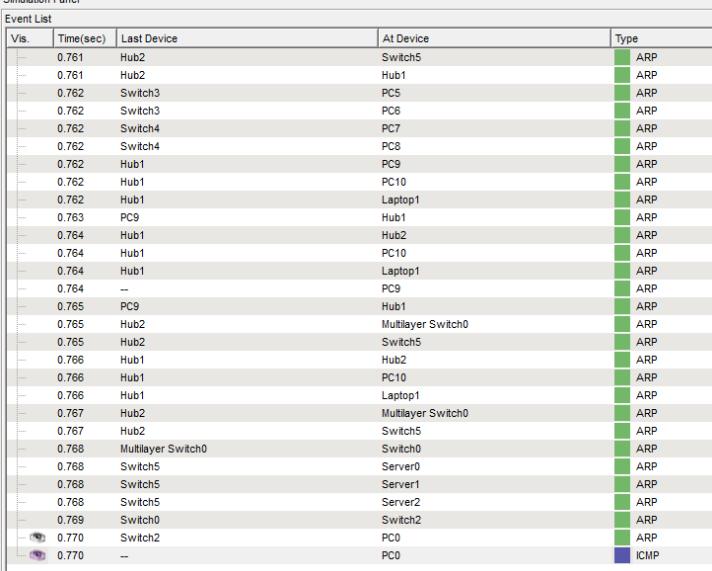
Se observa una lista de tramas ARP enviadas entre diferentes dispositivos, como switches, hubs, PCs y servidores, lo que indica que la red está realizando el proceso de resolución de direcciones IP a direcciones MAC para establecer la comunicación. Este comportamiento corresponde a la fase inicial de transmisión en modo broadcast, donde los switches aún no han aprendido las direcciones MAC y difunden las solicitudes ARP a todos los puertos. Posteriormente, se aprecia un evento ICMP, que corresponde a la ejecución del comando ping, utilizado para verificar la conectividad entre dos dispositivos.

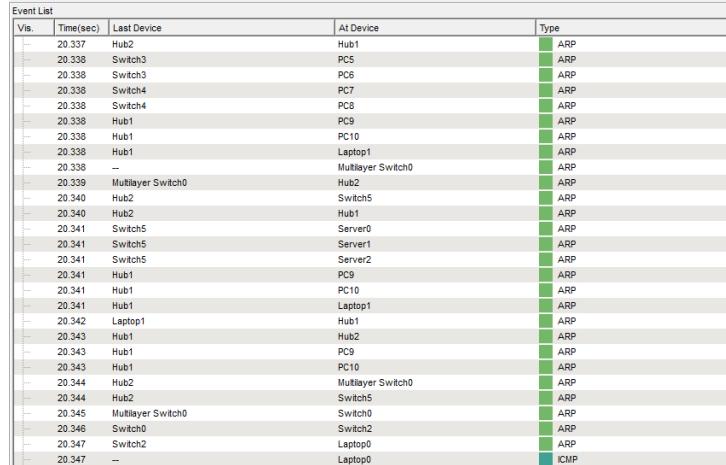
Se muestra nuevamente el uso del comando arp -a, pero en este caso después de haber realizado la comunicación entre PC1 y PC7 mediante la simulación en Cisco Packet Tracer. El resultado indica que ahora existe una entrada en la tabla ARP, donde se asocia la dirección IP 65.148.77.138 con la dirección física (MAC)

```
C:\>arp -a
No ARP Entries Found
```

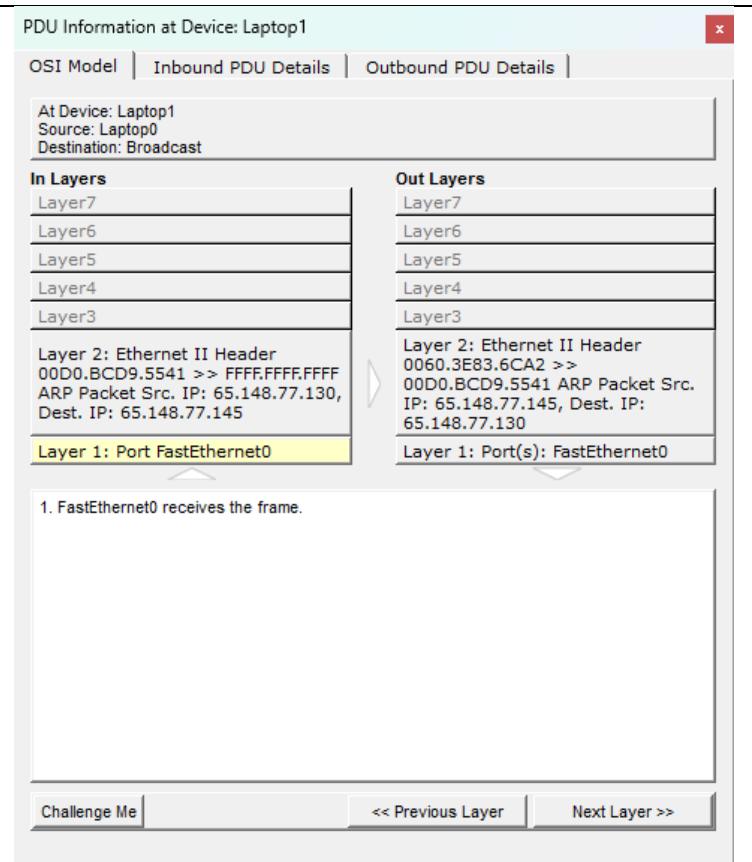
Simulation Panel					
Event List	Vis.	Time(sec)	Last Device	At Device	Type
-	29.847	--		Switch2	ARP
-	29.848		Switch2	PC0	ARP
-	29.848		Switch0	Multilayer Switch0	ARP
-	29.848		Switch0	Hub0	ARP
-	29.849		Multilayer Switch0	Switch1	ARP
-	29.849		Multilayer Switch0	Hub2	ARP
-	29.849		Hub0	PC3	ARP
-	29.849		Hub0	PC4	ARP
-	29.850		Switch1	Switch3	ARP
-	29.850		Switch1	Switch4	ARP
-	29.850		Hub2	Switch5	ARP
-	29.850		Hub2	Hub1	ARP
-	29.851		Switch3	PC5	ARP
-	29.851		Switch3	PC6	ARP
-	29.851		Switch4	PC7	ARP
-	29.851		Switch4	PC8	ARP
-	29.851		Switch5	Server0	ARP
-	29.851		Switch5	Server1	ARP
-	29.851		Switch5	Server2	ARP
-	29.851		Hub1	PC9	ARP
-	29.851		Hub1	PC10	ARP
-	29.851		Hub1	Laptop1	ARP
-	29.852		PC7	Switch4	ARP
-	29.853		Switch4	Switch1	ARP
-	29.854		Switch1	Multilayer Switch0	ARP
-	29.855		Multilayer Switch0	Switch0	ARP
-	29.856		Switch0	Switch2	ARP
-	29.857		Switch2	PC1	ARP
-	29.857	--		PC1	ICMP

```
C:\>arp -a
Internet Address      Physical Address      Type
65.148.77.138          0090.0cc8.cabb      dynamic
c:\>
```

<p>0090.0cc8.cdbb, y el tipo de registro es dynamic, lo que significa que fue aprendido automáticamente durante el intercambio de tramas ARP.</p>	 <table border="1"> <thead> <tr> <th>Vis.</th> <th>Time(sec)</th> <th>Last Device</th> <th>At Device</th> <th>Type</th> </tr> </thead> <tbody> <tr><td>-</td><td>0.761</td><td>Hub2</td><td>Switch5</td><td>ARP</td></tr> <tr><td>-</td><td>0.761</td><td>Hub2</td><td>Hub1</td><td>ARP</td></tr> <tr><td>-</td><td>0.762</td><td>Switch3</td><td>PC5</td><td>ARP</td></tr> <tr><td>-</td><td>0.762</td><td>Switch4</td><td>PC7</td><td>ARP</td></tr> <tr><td>-</td><td>0.762</td><td>Switch4</td><td>PC8</td><td>ARP</td></tr> <tr><td>-</td><td>0.762</td><td>Hub1</td><td>PC9</td><td>ARP</td></tr> <tr><td>-</td><td>0.762</td><td>Hub1</td><td>PC10</td><td>ARP</td></tr> <tr><td>-</td><td>0.762</td><td>Hub1</td><td>Laptop1</td><td>ARP</td></tr> <tr><td>-</td><td>0.763</td><td>PC9</td><td>Hub1</td><td>ARP</td></tr> <tr><td>-</td><td>0.764</td><td>Hub1</td><td>Hub2</td><td>ARP</td></tr> <tr><td>-</td><td>0.764</td><td>Hub1</td><td>PC10</td><td>ARP</td></tr> <tr><td>-</td><td>0.764</td><td>Hub1</td><td>Laptop1</td><td>ARP</td></tr> <tr><td>-</td><td>0.764</td><td>--</td><td>PC9</td><td>ARP</td></tr> <tr><td>-</td><td>0.765</td><td>PC9</td><td>Hub1</td><td>ARP</td></tr> <tr><td>-</td><td>0.765</td><td>Hub2</td><td>Multilayer Switch0</td><td>ARP</td></tr> <tr><td>-</td><td>0.765</td><td>Hub2</td><td>Switch5</td><td>ARP</td></tr> <tr><td>-</td><td>0.766</td><td>Hub1</td><td>Hub2</td><td>ARP</td></tr> <tr><td>-</td><td>0.766</td><td>Hub1</td><td>PC10</td><td>ARP</td></tr> <tr><td>-</td><td>0.766</td><td>Hub1</td><td>Laptop1</td><td>ARP</td></tr> <tr><td>-</td><td>0.767</td><td>Hub2</td><td>Multilayer Switch0</td><td>ARP</td></tr> <tr><td>-</td><td>0.767</td><td>Hub2</td><td>Switch5</td><td>ARP</td></tr> <tr><td>-</td><td>0.768</td><td>Multilayer Switch0</td><td>Switch0</td><td>ARP</td></tr> <tr><td>-</td><td>0.768</td><td>Switch5</td><td>Server0</td><td>ARP</td></tr> <tr><td>-</td><td>0.768</td><td>Switch5</td><td>Server1</td><td>ARP</td></tr> <tr><td>-</td><td>0.768</td><td>Switch5</td><td>Server2</td><td>ARP</td></tr> <tr><td>-</td><td>0.769</td><td>Switch0</td><td>Switch2</td><td>ARP</td></tr> <tr><td>-</td><td>0.770</td><td>Switch2</td><td>PC0</td><td>ARP</td></tr> <tr><td>-</td><td>0.770</td><td>--</td><td>PC0</td><td>ICMP</td></tr> </tbody> </table>	Vis.	Time(sec)	Last Device	At Device	Type	-	0.761	Hub2	Switch5	ARP	-	0.761	Hub2	Hub1	ARP	-	0.762	Switch3	PC5	ARP	-	0.762	Switch4	PC7	ARP	-	0.762	Switch4	PC8	ARP	-	0.762	Hub1	PC9	ARP	-	0.762	Hub1	PC10	ARP	-	0.762	Hub1	Laptop1	ARP	-	0.763	PC9	Hub1	ARP	-	0.764	Hub1	Hub2	ARP	-	0.764	Hub1	PC10	ARP	-	0.764	Hub1	Laptop1	ARP	-	0.764	--	PC9	ARP	-	0.765	PC9	Hub1	ARP	-	0.765	Hub2	Multilayer Switch0	ARP	-	0.765	Hub2	Switch5	ARP	-	0.766	Hub1	Hub2	ARP	-	0.766	Hub1	PC10	ARP	-	0.766	Hub1	Laptop1	ARP	-	0.767	Hub2	Multilayer Switch0	ARP	-	0.767	Hub2	Switch5	ARP	-	0.768	Multilayer Switch0	Switch0	ARP	-	0.768	Switch5	Server0	ARP	-	0.768	Switch5	Server1	ARP	-	0.768	Switch5	Server2	ARP	-	0.769	Switch0	Switch2	ARP	-	0.770	Switch2	PC0	ARP	-	0.770	--	PC0	ICMP
Vis.	Time(sec)	Last Device	At Device	Type																																																																																																																																														
-	0.761	Hub2	Switch5	ARP																																																																																																																																														
-	0.761	Hub2	Hub1	ARP																																																																																																																																														
-	0.762	Switch3	PC5	ARP																																																																																																																																														
-	0.762	Switch4	PC7	ARP																																																																																																																																														
-	0.762	Switch4	PC8	ARP																																																																																																																																														
-	0.762	Hub1	PC9	ARP																																																																																																																																														
-	0.762	Hub1	PC10	ARP																																																																																																																																														
-	0.762	Hub1	Laptop1	ARP																																																																																																																																														
-	0.763	PC9	Hub1	ARP																																																																																																																																														
-	0.764	Hub1	Hub2	ARP																																																																																																																																														
-	0.764	Hub1	PC10	ARP																																																																																																																																														
-	0.764	Hub1	Laptop1	ARP																																																																																																																																														
-	0.764	--	PC9	ARP																																																																																																																																														
-	0.765	PC9	Hub1	ARP																																																																																																																																														
-	0.765	Hub2	Multilayer Switch0	ARP																																																																																																																																														
-	0.765	Hub2	Switch5	ARP																																																																																																																																														
-	0.766	Hub1	Hub2	ARP																																																																																																																																														
-	0.766	Hub1	PC10	ARP																																																																																																																																														
-	0.766	Hub1	Laptop1	ARP																																																																																																																																														
-	0.767	Hub2	Multilayer Switch0	ARP																																																																																																																																														
-	0.767	Hub2	Switch5	ARP																																																																																																																																														
-	0.768	Multilayer Switch0	Switch0	ARP																																																																																																																																														
-	0.768	Switch5	Server0	ARP																																																																																																																																														
-	0.768	Switch5	Server1	ARP																																																																																																																																														
-	0.768	Switch5	Server2	ARP																																																																																																																																														
-	0.769	Switch0	Switch2	ARP																																																																																																																																														
-	0.770	Switch2	PC0	ARP																																																																																																																																														
-	0.770	--	PC0	ICMP																																																																																																																																														
<p>Se muestra el resultado del comando arp -a ejecutado después de la comunicación entre PC0 y PC9 en la simulación. Ahora la tabla ARP contiene una entrada que asocia la dirección IP 65.148.77.143 con la dirección física (MAC) 0090.21d7.050c, registrada como dynamic, lo que indica que fue aprendida automáticamente durante el intercambio de tramas ARP.</p>	 <pre>C:\>arp -a Internet Address Physical Address Type 65.148.77.143 0090.21d7.050c dynamic C:\></pre>																																																																																																																																																	
<p>En esta imagen se observa el Simulation Panel durante la simulación de comunicación entre Server0 y Server1.</p>	 <table border="1"> <thead> <tr> <th>Vis.</th> <th>Time(sec)</th> <th>Last Device</th> <th>At Device</th> <th>Type</th> </tr> </thead> <tbody> <tr><td>110.916</td><td>Hub2</td><td>Multilayer Switch0</td><td>DTP</td></tr> <tr><td>110.916</td><td>Hub2</td><td>Switch5</td><td>DTP</td></tr> <tr><td>110.916</td><td>Hub2</td><td>Hub1</td><td>DTP</td></tr> <tr><td>110.916</td><td>--</td><td>Server0</td><td>ICMP</td></tr> <tr><td>110.916</td><td>--</td><td>Server0</td><td>ARP</td></tr> <tr><td>110.917</td><td>Hub1</td><td>PC9</td><td>DTP</td></tr> <tr><td>110.917</td><td>Hub1</td><td>PC10</td><td>DTP</td></tr> <tr><td>110.917</td><td>Hub1</td><td>Laptop1</td><td>DTP</td></tr> <tr><td>110.917</td><td>Hub1</td><td>Switch5</td><td>ARP</td></tr> <tr><td>110.918</td><td>Switch5</td><td>Server2</td><td>ARP</td></tr> <tr><td>110.918</td><td>Switch5</td><td>Server5</td><td>ARP</td></tr> <tr><td>110.918</td><td>--</td><td>Switch5</td><td>ARP</td></tr> <tr><td>110.919</td><td>Switch5</td><td>Server1</td><td>ARP</td></tr> <tr><td>110.920</td><td>Server1</td><td>Switch5</td><td>ARP</td></tr> <tr><td>110.921</td><td>--</td><td>Switch5</td><td>ARP</td></tr> <tr><td>110.921</td><td>Switch5</td><td>Server0</td><td>ARP</td></tr> <tr><td>110.921</td><td>Switch5</td><td>Hub2</td><td>ARP</td></tr> <tr><td>110.921</td><td>--</td><td>Server0</td><td>ICMP</td></tr> <tr><td>110.922</td><td>Hub2</td><td>Multilayer Switch0</td><td>DTP</td></tr> <tr><td>110.922</td><td>Hub2</td><td>Switch5</td><td>DTP</td></tr> <tr><td>110.922</td><td>Hub2</td><td>Hub1</td><td>DTP</td></tr> <tr><td>110.922</td><td>Server0</td><td>Switch5</td><td>ICMP</td></tr> <tr><td>110.923</td><td>Hub1</td><td>PC9</td><td>DTP</td></tr> <tr><td>110.923</td><td>Hub1</td><td>PC10</td><td>DTP</td></tr> <tr><td>110.923</td><td>Hub1</td><td>Laptop1</td><td>DTP</td></tr> <tr><td>110.923</td><td>Hub1</td><td>Switch5</td><td>ARP</td></tr> <tr><td>110.923</td><td>Switch5</td><td>Server1</td><td>ARP</td></tr> <tr><td>110.924</td><td>Server1</td><td>Switch5</td><td>ARP</td></tr> </tbody> </table>	Vis.	Time(sec)	Last Device	At Device	Type	110.916	Hub2	Multilayer Switch0	DTP	110.916	Hub2	Switch5	DTP	110.916	Hub2	Hub1	DTP	110.916	--	Server0	ICMP	110.916	--	Server0	ARP	110.917	Hub1	PC9	DTP	110.917	Hub1	PC10	DTP	110.917	Hub1	Laptop1	DTP	110.917	Hub1	Switch5	ARP	110.918	Switch5	Server2	ARP	110.918	Switch5	Server5	ARP	110.918	--	Switch5	ARP	110.919	Switch5	Server1	ARP	110.920	Server1	Switch5	ARP	110.921	--	Switch5	ARP	110.921	Switch5	Server0	ARP	110.921	Switch5	Hub2	ARP	110.921	--	Server0	ICMP	110.922	Hub2	Multilayer Switch0	DTP	110.922	Hub2	Switch5	DTP	110.922	Hub2	Hub1	DTP	110.922	Server0	Switch5	ICMP	110.923	Hub1	PC9	DTP	110.923	Hub1	PC10	DTP	110.923	Hub1	Laptop1	DTP	110.923	Hub1	Switch5	ARP	110.923	Switch5	Server1	ARP	110.924	Server1	Switch5	ARP																												
Vis.	Time(sec)	Last Device	At Device	Type																																																																																																																																														
110.916	Hub2	Multilayer Switch0	DTP																																																																																																																																															
110.916	Hub2	Switch5	DTP																																																																																																																																															
110.916	Hub2	Hub1	DTP																																																																																																																																															
110.916	--	Server0	ICMP																																																																																																																																															
110.916	--	Server0	ARP																																																																																																																																															
110.917	Hub1	PC9	DTP																																																																																																																																															
110.917	Hub1	PC10	DTP																																																																																																																																															
110.917	Hub1	Laptop1	DTP																																																																																																																																															
110.917	Hub1	Switch5	ARP																																																																																																																																															
110.918	Switch5	Server2	ARP																																																																																																																																															
110.918	Switch5	Server5	ARP																																																																																																																																															
110.918	--	Switch5	ARP																																																																																																																																															
110.919	Switch5	Server1	ARP																																																																																																																																															
110.920	Server1	Switch5	ARP																																																																																																																																															
110.921	--	Switch5	ARP																																																																																																																																															
110.921	Switch5	Server0	ARP																																																																																																																																															
110.921	Switch5	Hub2	ARP																																																																																																																																															
110.921	--	Server0	ICMP																																																																																																																																															
110.922	Hub2	Multilayer Switch0	DTP																																																																																																																																															
110.922	Hub2	Switch5	DTP																																																																																																																																															
110.922	Hub2	Hub1	DTP																																																																																																																																															
110.922	Server0	Switch5	ICMP																																																																																																																																															
110.923	Hub1	PC9	DTP																																																																																																																																															
110.923	Hub1	PC10	DTP																																																																																																																																															
110.923	Hub1	Laptop1	DTP																																																																																																																																															
110.923	Hub1	Switch5	ARP																																																																																																																																															
110.923	Switch5	Server1	ARP																																																																																																																																															
110.924	Server1	Switch5	ARP																																																																																																																																															
<p>La tabla ARP ahora contiene una entrada que asocia la dirección IP 65.148.77.141 con la dirección</p>	 <pre>C:\>arp -a Internet Address Physical Address Type 65.148.77.141 0060.bcd6.99a9 dynamic C:\></pre>																																																																																																																																																	

<p>física (MAC) 000d.bcde.99a9, registrada como dynamic, lo que indica que fue aprendida automáticamente durante el intercambio de tramas ARP.</p>																																																																																																																																																		
<p>En esta imagen se muestra el Simulation Panel durante la simulación de comunicación entre Laptop0 y Laptop1.</p>	 <p>The Simulation Panel displays the Event List for the network simulation. The events show various devices sending ARP requests and responses, indicating the discovery of each other's MAC addresses. The list includes entries for Hub2, Switch3, PC5, PC6, PC7, PC8, PC9, PC10, Laptop1, Multilayer Switch0, Hub1, and Server0, Server1, Server2, PC9, PC10, Laptop1, Hub1, Laptop0, and Multilayer Switch0.</p> <table border="1"> <thead> <tr> <th>Vis.</th> <th>Time(sec)</th> <th>Last Device</th> <th>At Device</th> <th>Type</th> </tr> </thead> <tbody> <tr><td>20.337</td><td></td><td>Hub2</td><td>Hub1</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Switch3</td><td>PC5</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Switch3</td><td>PC6</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Switch4</td><td>PC7</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Switch4</td><td>PC8</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Hub1</td><td>PC9</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Hub1</td><td>PC10</td><td>ARP</td></tr> <tr><td>20.338</td><td></td><td>Hub1</td><td>Laptop1</td><td>ARP</td></tr> <tr><td>20.338</td><td>--</td><td></td><td>Multilayer Switch0</td><td>ARP</td></tr> <tr><td>20.339</td><td></td><td>Multilayer Switch0</td><td>Hub2</td><td>ARP</td></tr> <tr><td>20.340</td><td></td><td>Hub2</td><td>Switch5</td><td>ARP</td></tr> <tr><td>20.340</td><td></td><td>Hub2</td><td>Hub1</td><td>ARP</td></tr> <tr><td>20.341</td><td></td><td>Switch5</td><td>Server0</td><td>ARP</td></tr> <tr><td>20.341</td><td></td><td>Switch5</td><td>Server1</td><td>ARP</td></tr> <tr><td>20.341</td><td></td><td>Switch5</td><td>Server2</td><td>ARP</td></tr> <tr><td>20.341</td><td></td><td>Hub1</td><td>PC9</td><td>ARP</td></tr> <tr><td>20.341</td><td></td><td>Hub1</td><td>PC10</td><td>ARP</td></tr> <tr><td>20.341</td><td></td><td>Hub1</td><td>Laptop1</td><td>ARP</td></tr> <tr><td>20.342</td><td></td><td>Laptop1</td><td>Hub1</td><td>ARP</td></tr> <tr><td>20.343</td><td></td><td>Hub1</td><td>Hub2</td><td>ARP</td></tr> <tr><td>20.343</td><td></td><td>Hub1</td><td>PC9</td><td>ARP</td></tr> <tr><td>20.343</td><td></td><td>Hub1</td><td>PC10</td><td>ARP</td></tr> <tr><td>20.344</td><td></td><td>Hub2</td><td>Multilayer Switch0</td><td>ARP</td></tr> <tr><td>20.344</td><td></td><td>Hub2</td><td>Switch5</td><td>ARP</td></tr> <tr><td>20.345</td><td></td><td>Multilayer Switch0</td><td>Switch0</td><td>ARP</td></tr> <tr><td>20.346</td><td></td><td>Switch0</td><td>Switch2</td><td>ARP</td></tr> <tr><td>20.347</td><td></td><td>Switch2</td><td>Laptop0</td><td>ARP</td></tr> <tr><td>20.347</td><td>--</td><td></td><td>Laptop0</td><td>ICMP</td></tr> </tbody> </table>	Vis.	Time(sec)	Last Device	At Device	Type	20.337		Hub2	Hub1	ARP	20.338		Switch3	PC5	ARP	20.338		Switch3	PC6	ARP	20.338		Switch4	PC7	ARP	20.338		Switch4	PC8	ARP	20.338		Hub1	PC9	ARP	20.338		Hub1	PC10	ARP	20.338		Hub1	Laptop1	ARP	20.338	--		Multilayer Switch0	ARP	20.339		Multilayer Switch0	Hub2	ARP	20.340		Hub2	Switch5	ARP	20.340		Hub2	Hub1	ARP	20.341		Switch5	Server0	ARP	20.341		Switch5	Server1	ARP	20.341		Switch5	Server2	ARP	20.341		Hub1	PC9	ARP	20.341		Hub1	PC10	ARP	20.341		Hub1	Laptop1	ARP	20.342		Laptop1	Hub1	ARP	20.343		Hub1	Hub2	ARP	20.343		Hub1	PC9	ARP	20.343		Hub1	PC10	ARP	20.344		Hub2	Multilayer Switch0	ARP	20.344		Hub2	Switch5	ARP	20.345		Multilayer Switch0	Switch0	ARP	20.346		Switch0	Switch2	ARP	20.347		Switch2	Laptop0	ARP	20.347	--		Laptop0	ICMP
Vis.	Time(sec)	Last Device	At Device	Type																																																																																																																																														
20.337		Hub2	Hub1	ARP																																																																																																																																														
20.338		Switch3	PC5	ARP																																																																																																																																														
20.338		Switch3	PC6	ARP																																																																																																																																														
20.338		Switch4	PC7	ARP																																																																																																																																														
20.338		Switch4	PC8	ARP																																																																																																																																														
20.338		Hub1	PC9	ARP																																																																																																																																														
20.338		Hub1	PC10	ARP																																																																																																																																														
20.338		Hub1	Laptop1	ARP																																																																																																																																														
20.338	--		Multilayer Switch0	ARP																																																																																																																																														
20.339		Multilayer Switch0	Hub2	ARP																																																																																																																																														
20.340		Hub2	Switch5	ARP																																																																																																																																														
20.340		Hub2	Hub1	ARP																																																																																																																																														
20.341		Switch5	Server0	ARP																																																																																																																																														
20.341		Switch5	Server1	ARP																																																																																																																																														
20.341		Switch5	Server2	ARP																																																																																																																																														
20.341		Hub1	PC9	ARP																																																																																																																																														
20.341		Hub1	PC10	ARP																																																																																																																																														
20.341		Hub1	Laptop1	ARP																																																																																																																																														
20.342		Laptop1	Hub1	ARP																																																																																																																																														
20.343		Hub1	Hub2	ARP																																																																																																																																														
20.343		Hub1	PC9	ARP																																																																																																																																														
20.343		Hub1	PC10	ARP																																																																																																																																														
20.344		Hub2	Multilayer Switch0	ARP																																																																																																																																														
20.344		Hub2	Switch5	ARP																																																																																																																																														
20.345		Multilayer Switch0	Switch0	ARP																																																																																																																																														
20.346		Switch0	Switch2	ARP																																																																																																																																														
20.347		Switch2	Laptop0	ARP																																																																																																																																														
20.347	--		Laptop0	ICMP																																																																																																																																														
<p>En esta imagen se muestra el resultado del comando arp -a después de la comunicación entre Laptop0 y Laptop1. La tabla ARP ahora contiene dos entradas dinámicas: la primera asocia la dirección IP 65.148.77.139 con la dirección física (MAC) 00d0.d3dd.eea1, y la segunda corresponde a la IP 65.148.77.145 con la MAC 0060.3e83.6ca2.</p>	<pre>C:\>arp -a Internet Address Physical Address Type 65.148.77.139 00d0.d3dd.eea1 dynamic 65.148.77.145 0060.3e83.6ca2 dynamic</pre>																																																																																																																																																	

Este análisis permite comprender cómo se encapsulan los datos en la capa de enlace y cómo se realiza la resolución de direcciones antes de establecer la comunicación directa entre dispositivos.

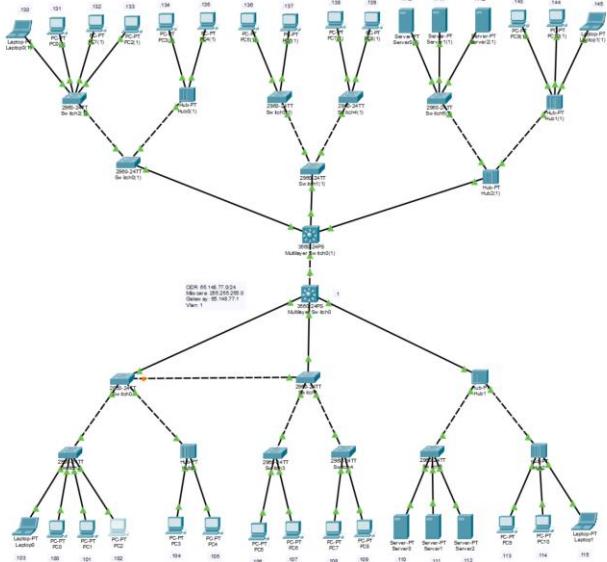


Interconexión entre Proyectos

En esta etapa, fusionamos los archivos del proyecto de cada miembro del grupo. Primero, se conecta ambos multilayer switches mediante un cable cruzado (crossover). Este tipo de cable es necesario cuando se establece una conexión directa entre dos switches. Con esta conexión, los switches pueden intercambiar información y permitir que los dispositivos en las distintas topologías se comuniquen de manera efectiva. El uso del cable de cobre cruzado garantiza que los puertos de cada switch puedan detectar la señal y establecer la comunicación sin problemas.

Figura 5

Topología completa con conexión de multilayer switches mediante cable cruzado

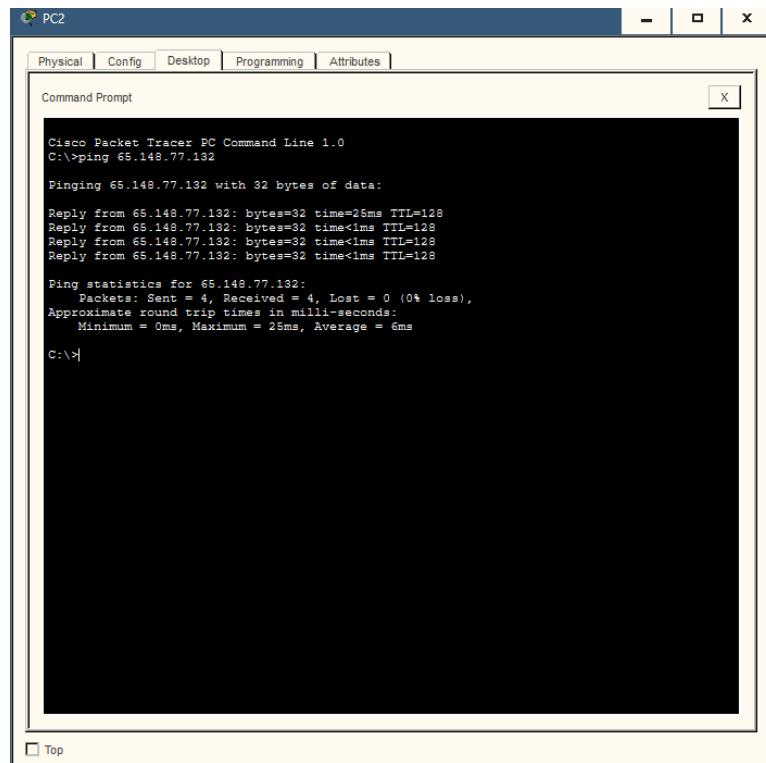


Nota. En esta imagen se muestra la interconexión entre los switches utilizando un cable de cobre cruzado, que es necesario para la conexión directa entre switches.

Después, se realiza un ping desde el PC2 de la topología de Santiago (con dirección IP 65.148.77.102) hacia el PC1 de la topología de Natalia (con dirección IP 65.148.77.132). Durante la prueba, se enviaron 4 paquetes y se obtuvo un 0% de pérdida de paquetes, lo que indica que todos los paquetes enviados llegaron correctamente a su destino. El tiempo promedio de respuesta fue de 6 ms, con la primera solicitud de eco (echo request) tardando 25 ms debido a la necesidad de resolver la dirección MAC de la IP destino a través de ARP. Sin embargo, una vez resuelta la dirección, los siguientes paquetes fueron respondidos en menos de 1 ms, lo que muestra que la comunicación se estabilizó rápidamente.

Figura 6

Ping entre PC2 (Santiago) y PC1 (Natalia) con resultados de 4 paquetes enviados



The screenshot shows a window titled "PC2" with a tab bar at the top containing "Physical", "Config", "Desktop", "Programming", and "Attributes". Below the tabs is a "Command Prompt" window with the title "Cisco Packet Tracer PC Command Line 1.0". The command entered was "C:\>ping 65.148.77.132". The output shows four successful replies from the target IP address, followed by ping statistics and a prompt "C:\>".

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 65.148.77.132

Pinging 65.148.77.132 with 32 bytes of data:
Reply from 65.148.77.132: bytes=32 time=25ms TTL=128
Reply from 65.148.77.132: bytes=32 time<1ms TTL=128
Reply from 65.148.77.132: bytes=32 time<1ms TTL=128
Reply from 65.148.77.132: bytes=32 time<1ms TTL=128

Ping statistics for 65.148.77.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 25ms, Average = 6ms

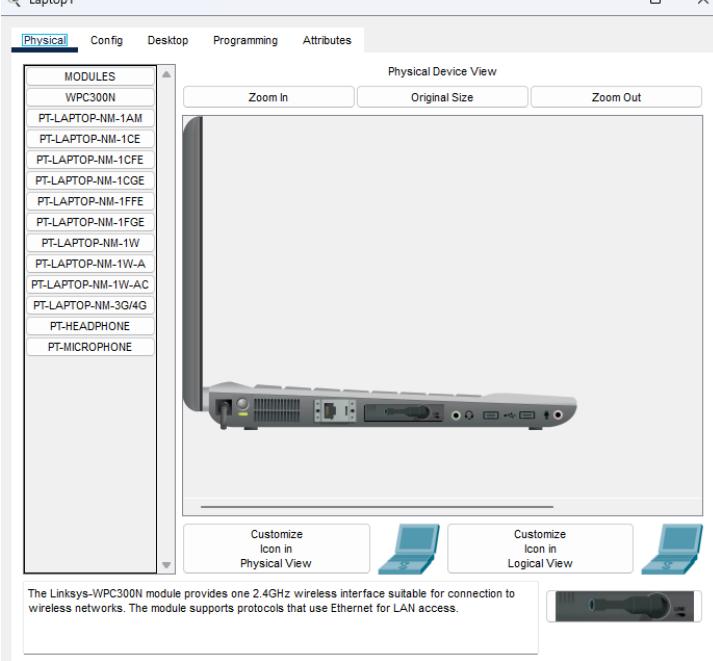
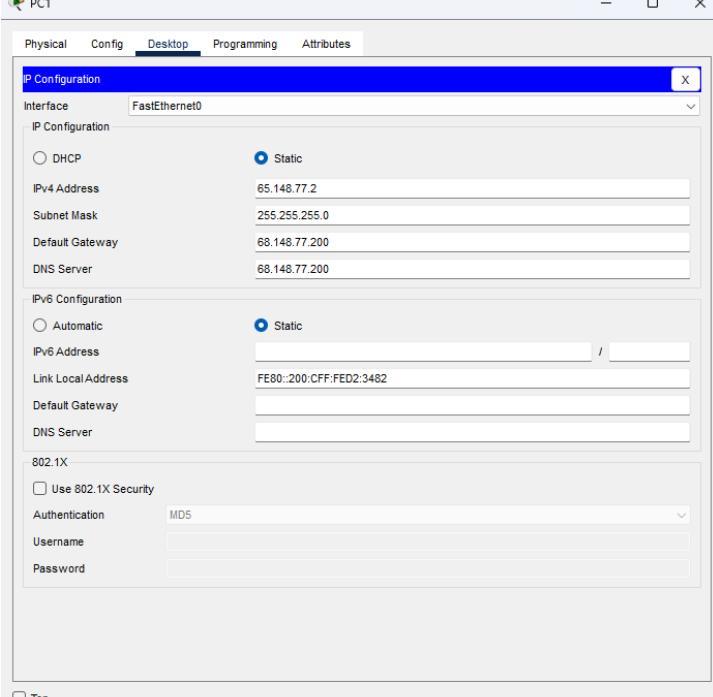
C:\>
```

Nota. El ping entre los dispositivos mostró un tiempo promedio de respuesta de 6 ms, con una ligera demora en la primera solicitud debido a la resolución ARP.

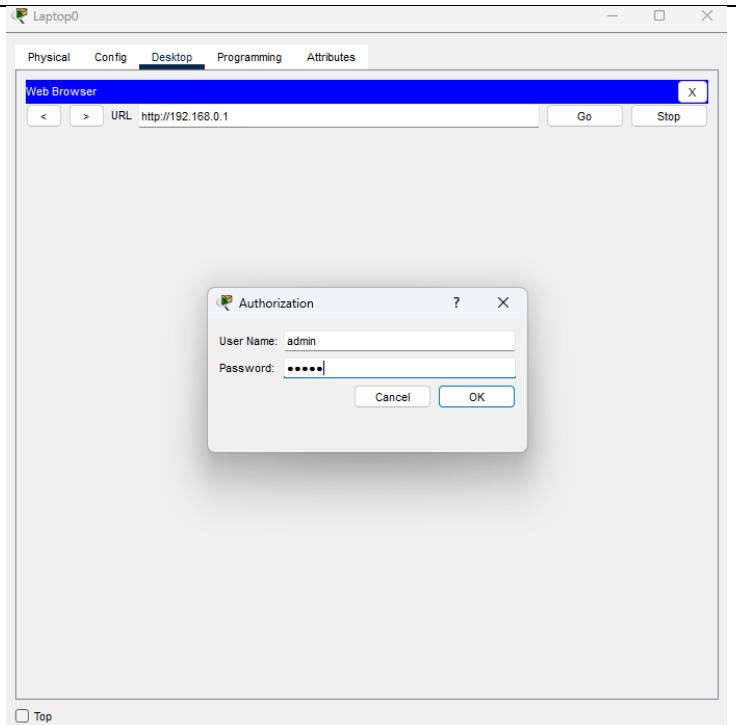
Configuración WiFi-básica

En esta sección, se llevará a cabo la configuración de una red híbrida que involucra tanto conexiones cableadas como inalámbricas utilizando Cisco Packet Tracer. Cada implementación incluye la configuración de manera individual. El segmento de la LAN cableada incluirá dispositivos como Server0, PC1, y las interfaces de Internet del router, todas dentro del rango de IPs 65.148.77.1 a 65.148.77.20 con una máscara de subred 255.255.255.0. Además, se configurará un router inalámbrico para gestionar el acceso a la red inalámbrica, asignando direcciones IP dentro del rango 192.168.0.0/24 para los dispositivos móviles conectados por WiFi. Se utilizará un laptop para configurar el router inalámbrico mediante su interfaz web, especificando el SSID y configurando la seguridad con WPA2-PSK. Posteriormente, se verificará la conectividad entre los dispositivos, configurando correctamente las direcciones IP, el rango DHCP y los parámetros de seguridad para los dispositivos móviles y las conexiones inalámbricas. Se analizará qué dispositivos pueden hacer ping entre sí y se investigarán las razones detrás de estas interacciones.

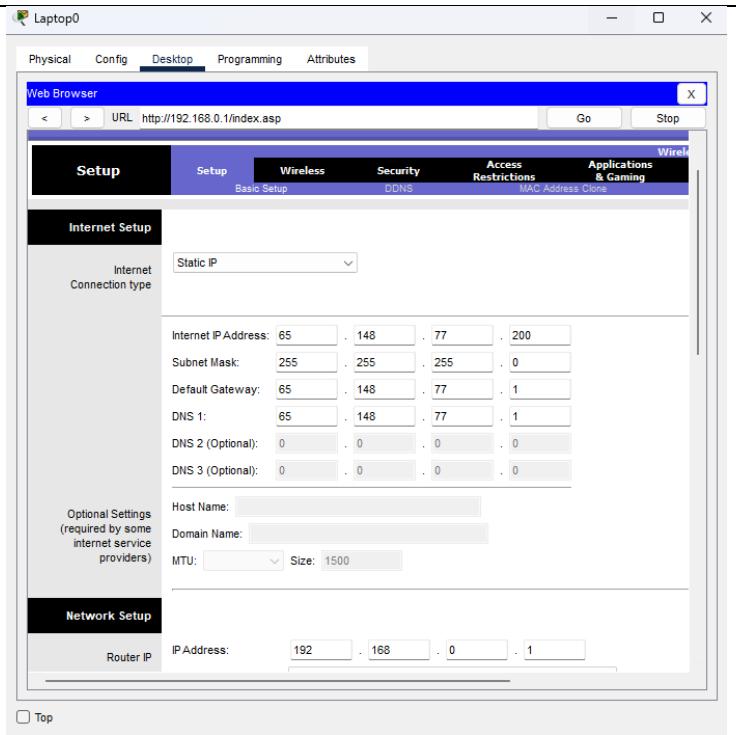
Implementación de Santiago

Acción Realizada	Captura de pantalla
<p>Se agregarán los siguientes dispositivos a la topología: 2 laptops, 2 PCs, 2 smartphones, 1 switch, 1 servidor, 1 router inalámbrico WRT300N y 1 punto de acceso. Al principio, no todas las conexiones estarán operativas, por lo que, inicialmente, se les instalará un módulo WPC300N a las laptops para habilitar su conexión inalámbrica.</p>	 <p>The Linksys-WPC300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.</p>
<p>Se configuró PC1 con la dirección IP 65.148.77.2, máscara de subred 255.255.255.0 y gateway 65.148.77.200, mientras que Server0 se configuró con la dirección IP 65.148.77.3, máscara de subred 255.255.255.0 y gateway 65.148.77.200, asegurando que ambos dispositivos estuvieran dentro del mismo rango de red para permitir su comunicación.</p>	

Desde Laptop0, se accedió a la dirección <https://192.168.0.1>, correspondiente a la red LAN del wireless router. En el navegador web, se ingresó el nombre de usuario y la contraseña como admin para acceder a la interfaz de configuración del router.

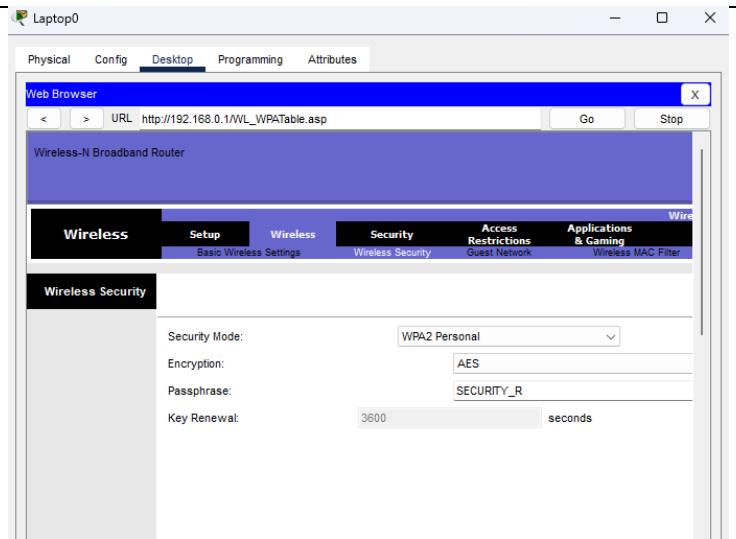
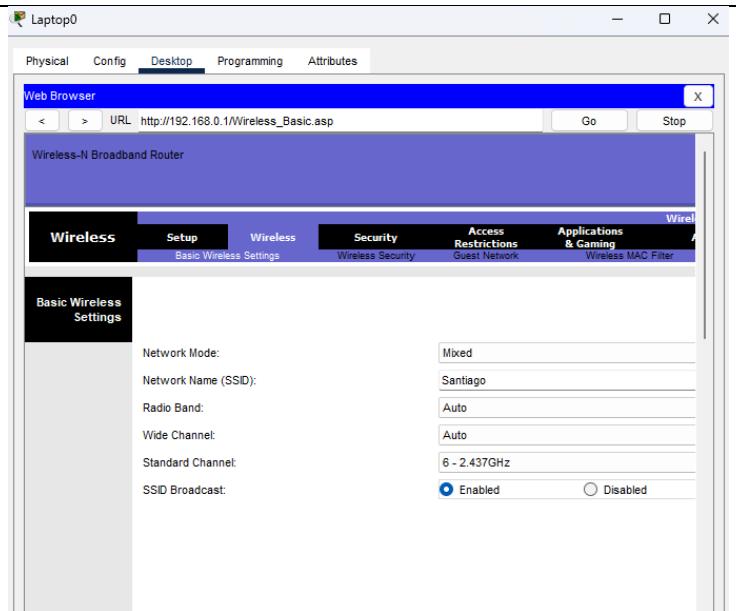


En el setup básico del router, se configuró la red expuesta hacia Internet con la dirección IP 65.148.77.200, máscara de subred 255.255.255.0, gateway 65.148.77.1 y DNS 65.148.77.1, asegurando la conectividad adecuada entre la red interna y la red externa.

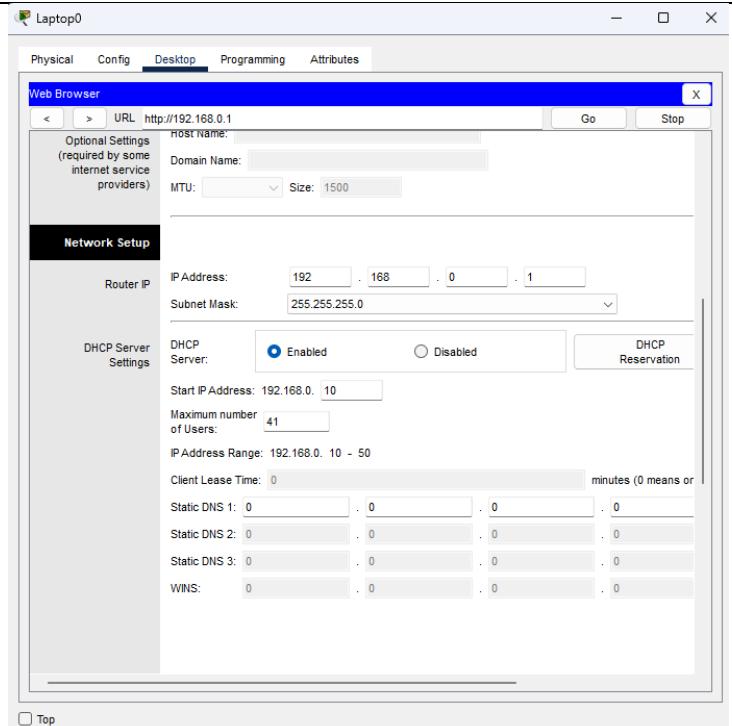


En la configuración de Internet Wireless del router, se activó el modo Mixed para permitir la compatibilidad con dispositivos de diferentes estándares inalámbricos. Se asignó el SSID Santiago, con radio band en modo automático, ancho de canal automático, y se configuró el canal estándar 6 en la frecuencia de 2.437 GHz. Además, se habilitó el broadcast del SSID para que los dispositivos inalámbricos pudieran detectar y conectarse a la red de manera sencilla.

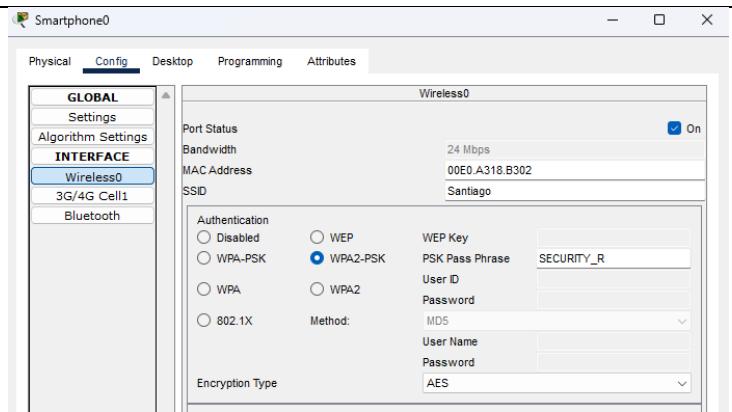
En la configuración de seguridad Wireless, se activó el modo WPA2 Personal con encripción AES para garantizar una conexión segura. Además, se estableció la passphrase SECURITY_R, que es la clave que los dispositivos deben ingresar para conectarse a la red inalámbrica de forma segura.



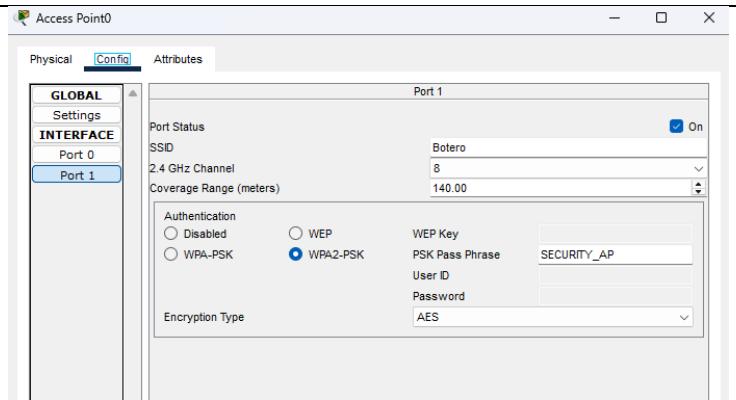
Finalmente, se activó la configuración DHCP en el router para asignar automáticamente direcciones IP a los dispositivos inalámbricos. Se estableció un rango de direcciones IP de 192.168.0.10 a 192.168.0.50, asegurando que los dispositivos conectados a la red inalámbrica recibieran direcciones dentro de este rango sin necesidad de configuración manual.



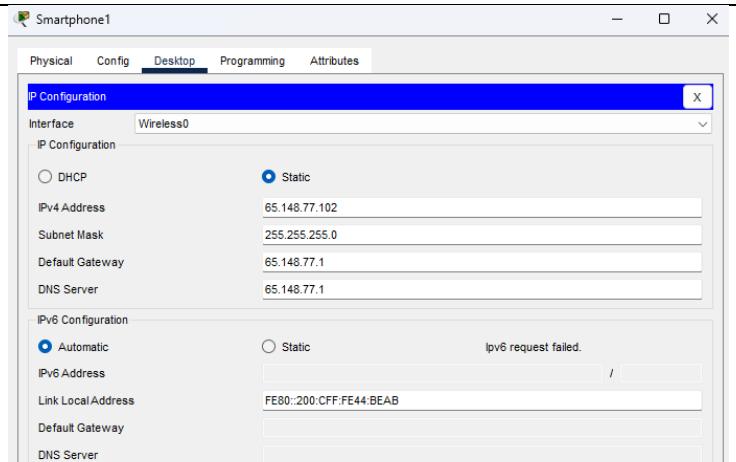
Se configuró Smartphone0 y Laptop0 para que se conectaran al router Santiago, asegurándose de que ambos tuvieran activada la opción DHCP para recibir una dirección IP automáticamente. En el caso del Smartphone0, se utilizó la interfaz wireless0 para ingresar manualmente la passphrase SECURITY_R, el SSID Santiago y la configuración de WPA2-PSK. Por otro lado, para Laptop0, se usó la interfaz WPC300N para establecer la conexión inalámbrica, manteniendo la configuración de seguridad y SSID de manera automática a través de esta interfaz.



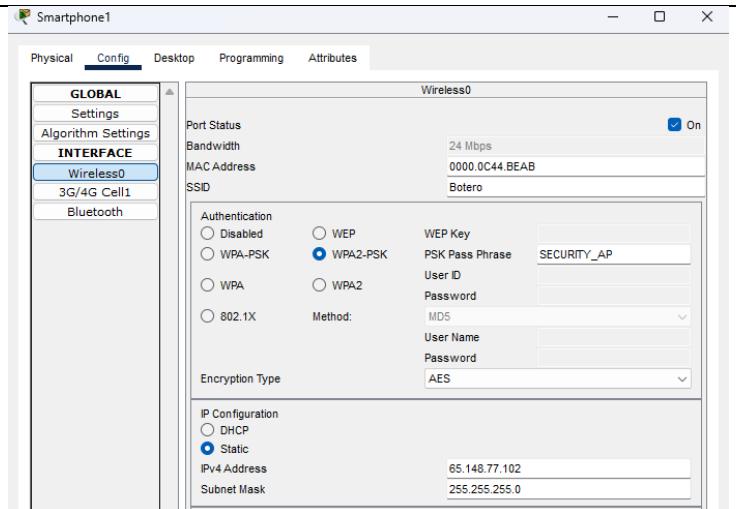
Para la configuración del punto de acceso, se estableció el SSID Botero en el canal 8 para evitar interferencias con el canal 6 utilizado por el router. El rango de cobertura se configuró en 140 metros para garantizar una buena señal en el área deseada. Se activó el modo de autenticación WPA2-PSK con la passphrase SECURITY_AP y se habilitó la encriptación AES para asegurar la conexión inalámbrica.



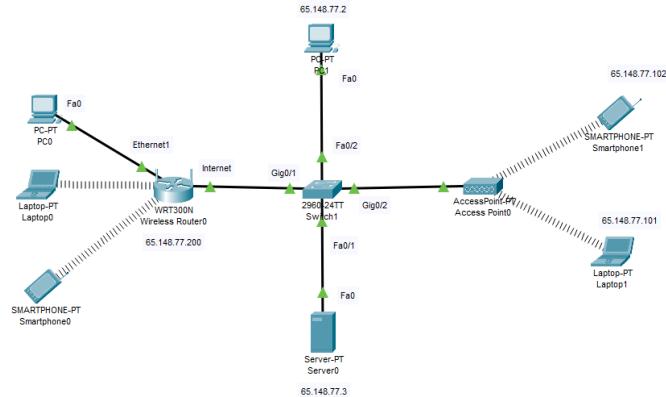
La conexión de los dispositivos con el Access Point se configuró de manera estática. Para ello, se asignaron las direcciones IP 65.148.77.102 al Smartphone1 y 65.148.77.101 a la Laptop1, asegurando que ambos dispositivos tuvieran direcciones fijas dentro del rango de la red para una comunicación estable y sin conflictos.



Adicionalmente, para garantizar la conexión con el Access Point, se accedió a la interfaz wireless0 en Smartphone1 y se configuró la conexión con el Access Point Botero. Por otro lado, en Laptop1, se utilizó la interfaz WPC300N para establecer la conexión con el mismo punto de acceso, asegurando que ambos dispositivos se conectaran correctamente a la red inalámbrica.



Con estas configuraciones, la topología de red quedaría completamente operativa, con dispositivos conectados tanto de manera cableada como inalámbrica.



Para garantizar el correcto funcionamiento de la red, se establecieron tres pruebas de conectividad. En la primera prueba, desde PC0, con dirección IP privada 192.168.0.12, se realizó un ping hacia Server3, que tiene la dirección IP pública 65.148.77.3. Durante esta prueba, se enviaron 4 paquetes, de los cuales el primero se perdió debido a la resolución inicial de la dirección, pero los otros tres paquetes llegaron correctamente. El tiempo promedio de respuesta fue de 2 ms, lo que indica una comunicación eficiente y estable después de la primera solicitud.

```

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

Pinging 65.148.77.3 with 32 bytes of data:
Request timed out.
Reply from 65.148.77.3: bytes=32 time<1ms TTL=127
Reply from 65.148.77.3: bytes=32 time<1ms TTL=127
Reply from 65.148.77.3: bytes=32 time=7ms TTL=127

Ping statistics for 65.148.77.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...: FE80::240:BFF:FE89:59A
    Link-local IPv6 Address....: FE80::240:BFF:FE89:59A
    IPv6 Address.....: ::1
    IPv4 Address.....: 192.168.0.12
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address....: ::1
    IPv6 Address.....: ::1
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0

C:\>

```

Como segunda prueba, desde Smartphone1, con dirección IP pública 65.148.77.102, se realizó un ping hacia Laptop1, que tiene la dirección IP privada 192.168.0.11. Durante la prueba, se enviaron 4 paquetes, pero todos los paquetes se perdieron. Este comportamiento es adecuado, ya que, según la configuración de la red, los dispositivos con direcciones IP privadas no pueden comunicarse directamente con otros dispositivos fuera de su red sin pasar a través de un router que realice la traducción de direcciones (NAT). La pérdida de los paquetes indica que la comunicación entre una IP pública y una IP privada está correctamente gestionada por las reglas de NAT del router.

```

Smartphone1
Physical Config Desktop Programming Attributes
Command Prompt X
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

Wireless0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::200:CFF:FE44:BEAB
IPv6 Address.....: ::1
IPv4 Address.....: 65.148.77.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
                                         65.148.77.1

3G/4G Cell Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20C:FFFF:FE6B:2026
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
                                         0.0.0.0

Bluetooth Connection:
--More--
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
                                         0.0.0.0

C:\>ping 192.168.0.11
Pinging 192.168.0.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

```

 Top

Finalmente, en la tercera prueba, desde Smartphone0, con dirección IP privada 192.168.0.14, se realizó un ping hacia Laptop1, que tiene la dirección IP privada 192.168.0.11. Se enviaron 4 paquetes, y no se perdió ninguno, lo que resultó en un 0% de pérdida. El tiempo de respuesta promedio fue de 20 ms, lo que indica que la comunicación entre los dispositivos dentro de la misma red privada se realizó de manera exitosa y eficiente, sin ninguna interferencia ni problemas de conectividad.

The screenshot shows a Windows Command Prompt window titled "Smartphone0". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Below the tabs is a title bar "Command Prompt" with a close button "X". The main area of the window displays network configuration details for three connections:

- Wireless0 Connection: (default port)**
 - Connection-specific DNS Suffix..: FE80::2E0:A3FF:FE18:B302
 - Link-local IPv6 Address.....: ::
 - IPv6 Address.....: 192.168.0.14
 - IPv4 Address.....: 0.0.0.0
 - Subnet Mask.....: 255.255.255.0
 - Default Gateway.....: :: 192.168.0.1
- 3G/4G Cell Connection:**
 - Connection-specific DNS Suffix..: FE80::2E0:70FF:FEBC:5093
 - Link-local IPv6 Address.....: ::
 - IPv6 Address.....: 0.0.0.0
 - IPv4 Address.....: 0.0.0.0
 - Subnet Mask.....: 0.0.0.0
 - Default Gateway.....: 0.0.0.0
- Bluetooth Connection:**
 - More--
 - Connection-specific DNS Suffix..: ::
 - Link-local IPv6 Address.....: ::
 - IPv6 Address.....: ::
 - IPv4 Address.....: 0.0.0.0
 - Subnet Mask.....: 0.0.0.0
 - Default Gateway.....: 0.0.0.0

At the bottom of the window, the command "C:\>ping 192.168.0.11" is entered, followed by its output:

```
C:\>ping 192.168.0.11

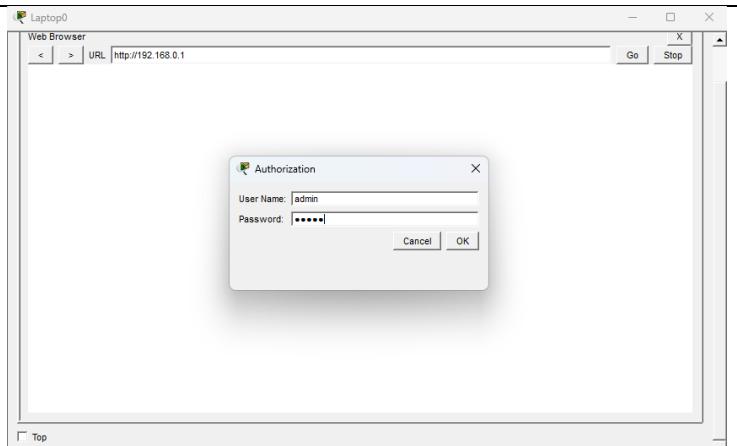
Pinging 192.168.0.11 with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time=24ms TTL=128
Reply from 192.168.0.11: bytes=32 time=22ms TTL=128
Reply from 192.168.0.11: bytes=32 time=20ms TTL=128
Reply from 192.168.0.11: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 24ms, Average = 20ms
```

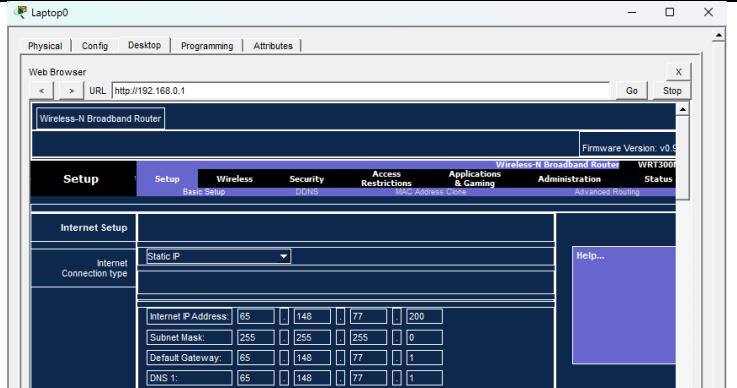
Implementación de Natalia

Acción Realizada	Captura de pantalla
En esta imagen se muestra la topología diseñada en Cisco Packet Tracer para integrar una red cableada con una red inalámbrica.	
En esta imagen se muestra la configuración manual de la dirección IP en Server0 dentro de Cisco Packet Tracer.	
En esta imagen se muestra la configuración manual de la dirección IP en PC1 dentro de Cisco Packet Tracer.	

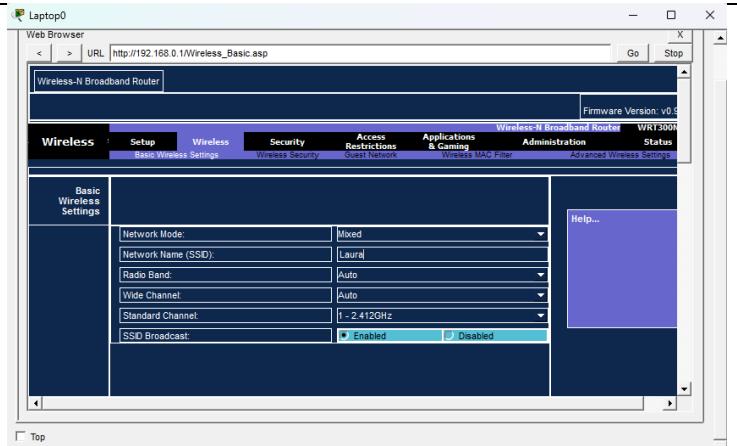
En esta imagen se muestra el proceso de acceso a la interfaz web del Wireless Router desde Laptop0. Para ello, se ha ingresado la dirección IP 192.168.0.1 en el navegador, que corresponde a la interfaz inalámbrica del router.



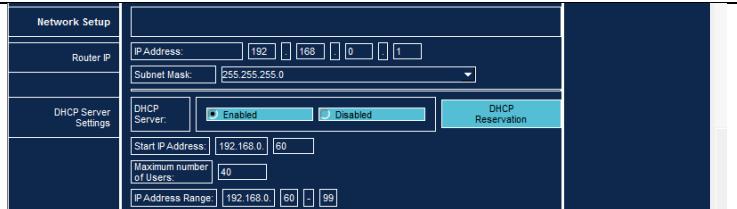
En esta imagen se muestra la interfaz de configuración del Wireless Router accedida desde Laptop0 mediante la dirección 192.168.0.1.

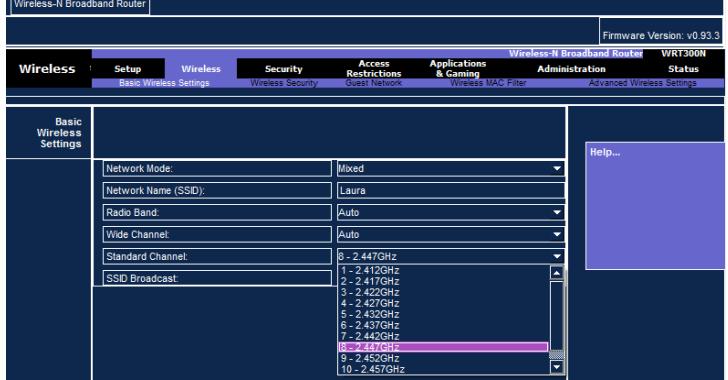


En esta imagen se muestra la sección Basic Wireless Settings del Wireless Router en la interfaz web. Aquí se ha configurado el SSID con el nombre "Laura", que identifica la red inalámbrica para los dispositivos que se conectarán.



En esta imagen se muestra la configuración del servidor DHCP en el Wireless Router. Se ha habilitado la opción DHCP Server, lo que permite asignar direcciones IP automáticamente a los dispositivos inalámbricos conectados. El rango definido para la asignación es desde 192.168.0.60 hasta 192.168.0.99, cumpliendo con las instrucciones del



<p>laboratorio para el estudiante correspondiente.</p>	<p>En esta imagen se muestra la configuración del servidor DHCP en el Wireless Router. Se ha habilitado la opción DHCP Server, lo que permite asignar direcciones IP automáticamente a los dispositivos inalámbricos conectados. El rango definido para la asignación es desde 192.168.0.60 hasta 192.168.0.99, cumpliendo con las instrucciones del laboratorio para el estudiante correspondiente.</p> 
<p>En esta imagen se muestra nuevamente la sección Basic Wireless Settings del Wireless Router, enfocada en la selección del canal de operación. El SSID configurado sigue siendo “Laura”, y se observa el menú desplegable para elegir el Standard Channel, donde se ha seleccionado el canal 8 (2.447 GHz).</p>	
<p>En esta imagen se muestra la interfaz del Wireless Network Monitor en Cisco Packet Tracer, donde se visualizan las redes inalámbricas disponibles para conexión. Se observan dos SSID: “Default” en el canal 1 con señal al 100%, y “Laura” en el canal 8 con señal al 80%, que corresponde a la red configurada previamente en el router.</p>	

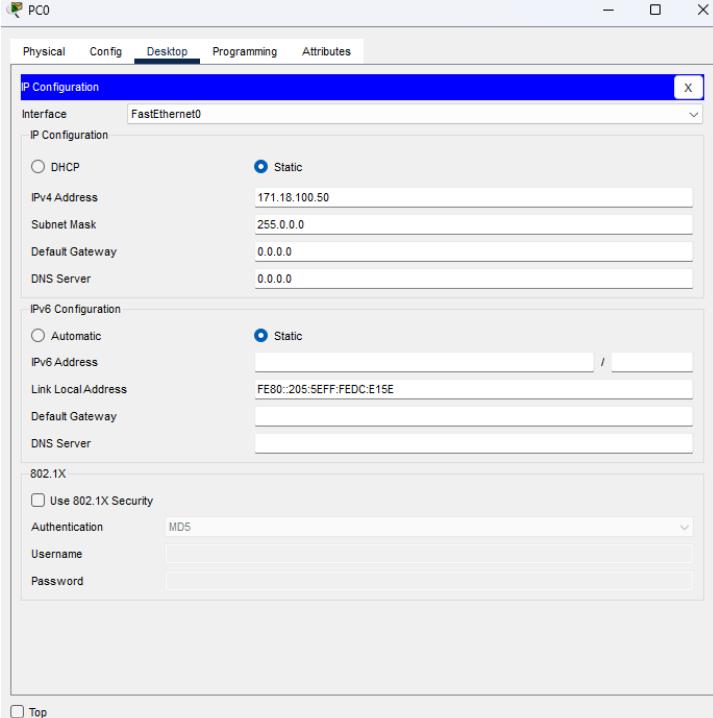
<p>En esta imagen se muestra la configuración de la conexión inalámbrica en Smartphone0 dentro de Cisco Packet Tracer. Se observa que el dispositivo está conectado a la interfaz Wireless0, con el SSID configurado como “Laura”, correspondiente a la red creada previamente en el router.</p>	
<p>En esta imagen se muestra la configuración del Access Point (AP) en Cisco Packet Tracer. Se ha definido el SSID “Perilla”, que identifica la red inalámbrica gestionada por este dispositivo, y se ha seleccionado el canal 6 en la banda de 2.4 GHz para evitar interferencias con el router principal, que opera en otro canal.</p>	
<p>Se muestra la configuración manual de la dirección IP en Smartphone1 dentro de Cisco Packet Tracer.</p>	
<p>Se muestra la configuración manual de la dirección IP en Laptop1 dentro de Cisco Packet Tracer.</p>	
<p>Los resultados muestran respuestas exitosas al direccionar paquetes hacia la IP 65.148.77.102 y hacia 65.148.77.1 sin pérdida de paquetes.</p>	

Desde PC0 se realizaron pings hacia 65.148.77.200 (Wireless Router), 65.148.77.102 (dispositivo del AP) y 65.148.77.101 (otro dispositivo en la misma subred).

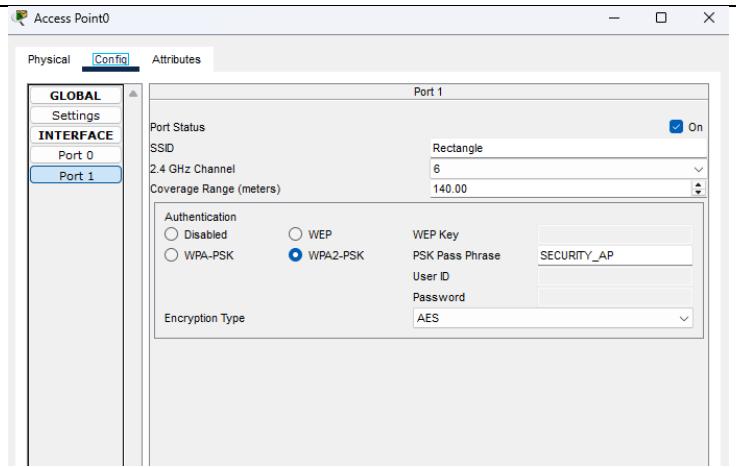
```
PC0
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms
C:\>ping 65.148.77.200
Pinging 65.148.77.200 with 32 bytes of data:
Reply from 65.148.77.200: bytes=32 time=1ms TTL=255
Ping statistics for 65.148.77.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 9ms, Average = 9ms
C:\>ping 65.148.77.102
Pinging 65.148.77.102 with 32 bytes of data:
Reply from 65.148.77.102: bytes=32 time=8ms TTL=127
Ping statistics for 65.148.77.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
C:\>ping 65.148.77.101
```

Configuración de LAN cableada e inalámbrica

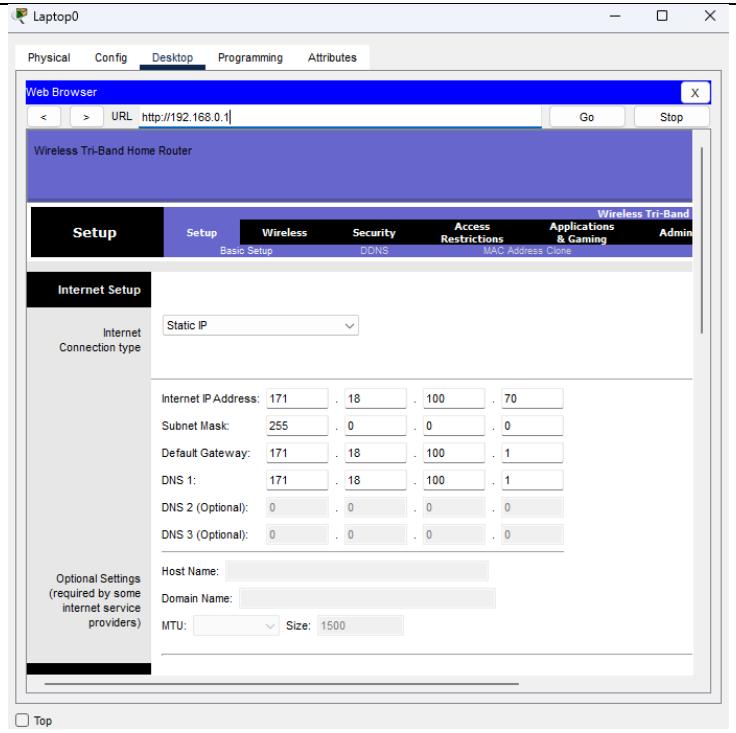
Implementación de Santiago

Acción Realizada	Captura de pantalla
<p>Como paso inicial, se replicaron los switches 2960 y los seis grupos de dispositivos separados por colores, sin implementar VLANs, por lo que toda la red funciona como una única LAN. Los grupos de dispositivos se organizaron en tres categorías de red inalámbrica: Naranja (Wireless - SSID Irregular), Verde (Wireless - SSID Rectangle) y Morado (Wireless - SSID Circle), además de los PCs y servidores cableados. El rango de direcciones IP utilizado por el estudiante 1 fue de 171.18.100.50 a 171.18.100.80 con máscara de subred 255.0.0.0. Todos los dispositivos cableados, como PC0, PC1, PC2, PC3, Server0, Server1, Server2, Server3, PC4, PC5, PC6, PC7, PC8 y PC9, fueron configurados con direcciones IP dentro de este rango, sin configurar un gateway, ya que aún no se está utilizando ningún router ni se ha segmentado la red en subredes.</p>	

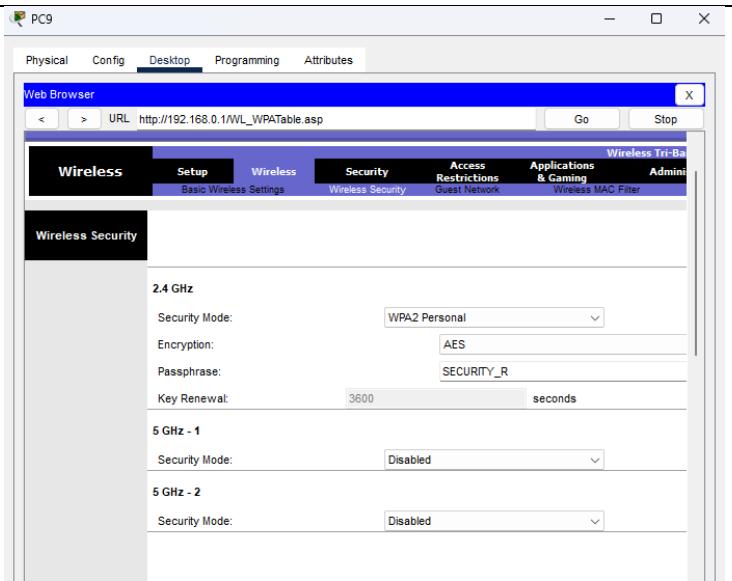
Se configuró el Access Point 0 con el SSID Rectangle, utilizando el canal 2.4 GHz, canal 6, con un rango de cobertura de 140 metros. La seguridad se estableció en WPA2-PSK con la passphrase SECURITY_AP y encriptación AES.



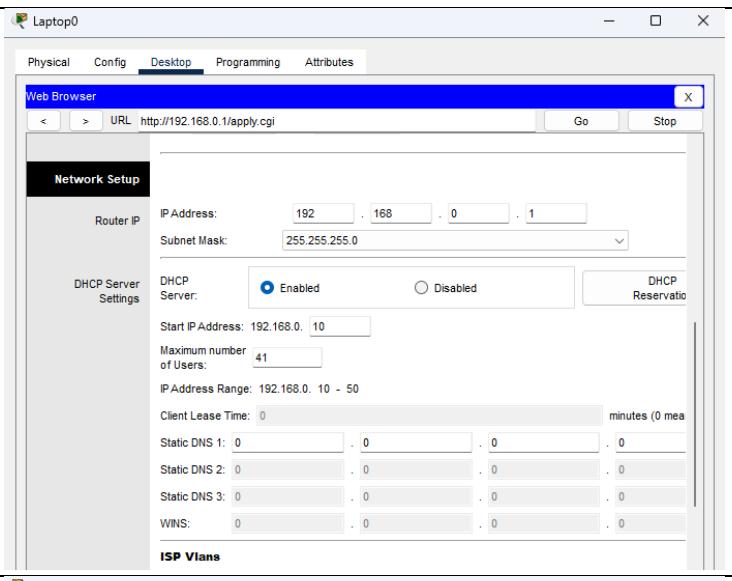
Desde Laptop0, con username y password configurados como admin, se configuró el Wireless Router con los siguientes parámetros: IP 171.18.100.70, máscara 255.0.0.0, gateway 171.18.10.1 y DNS 171.18.10.1.



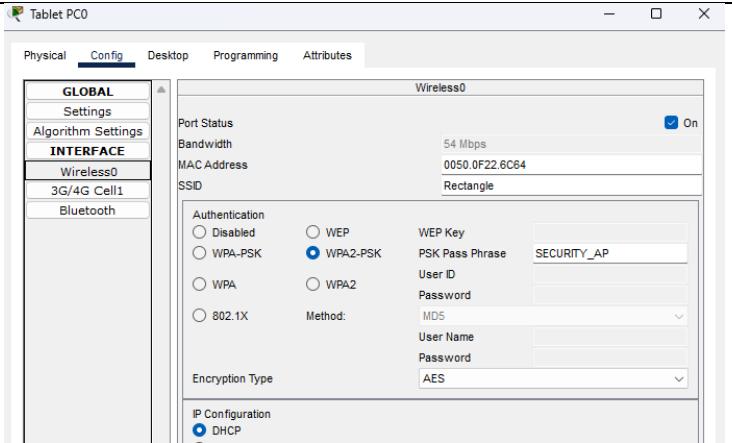
Se configuró la seguridad inalámbrica del router, asignándole WPA2 Personal en la banda de 2.4 GHz con encriptación AES y la passphrase SECURITY_R.



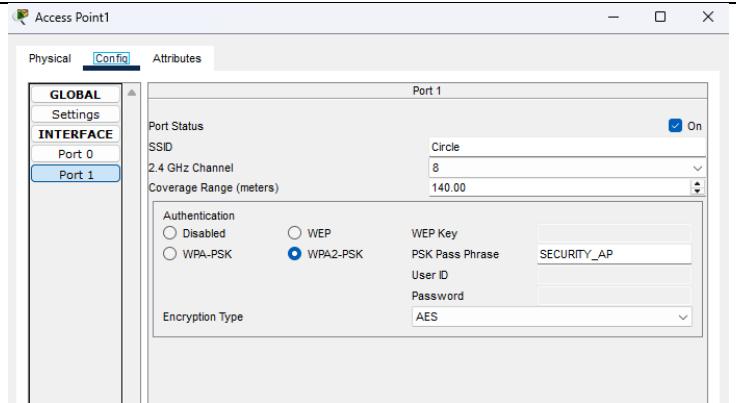
Adicionalmente, se activó la configuración DHCP en el router para asignar automáticamente direcciones IP a los dispositivos inalámbricos. Se estableció un rango de direcciones IP de 192.168.0.10 a 192.168.0.50, asegurando que los dispositivos conectados a la red inalámbrica recibieran direcciones dentro de este rango sin necesidad de configuración manual.



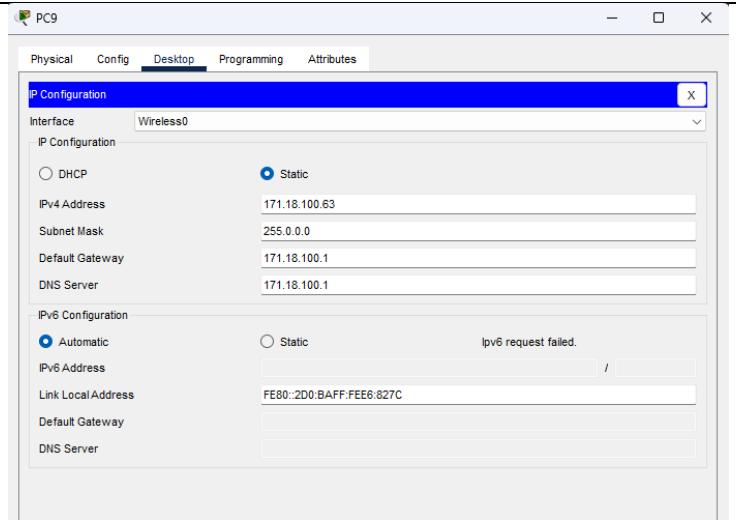
Los equipos inalámbricos que debían conectarse al Access Point 0 fueron correctamente conectados, estableciendo comunicación inalámbrica con la red configurada.



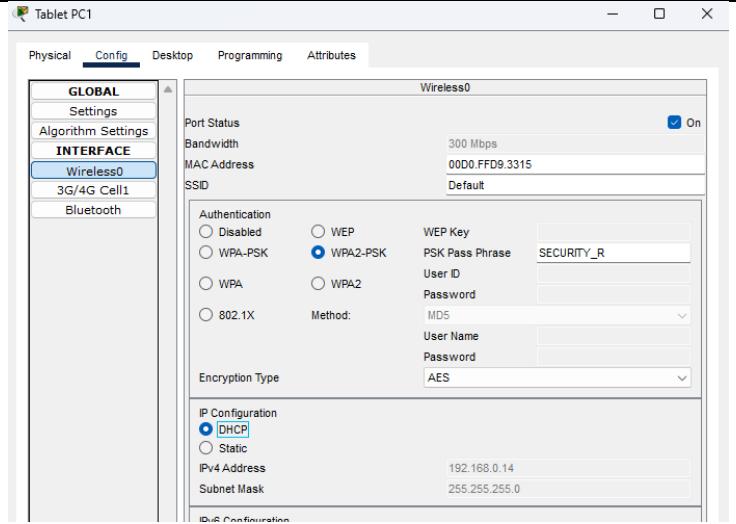
Se configuró el Access Point 1 con el SSID Circle, utilizando el canal 2.4 GHz, canal 8, con un rango de cobertura de 140 metros. La seguridad se estableció en WPA2-PSK con la clave SECURITY_AP y encriptación AES.



Los dispositivos inalámbricos se conectaron a la red del Access Point 1, pero, a diferencia de la configuración predeterminada por DHCP, se asignaron manualmente direcciones IP públicas dentro del CIDR completo de la topología en lugar de usar las IPs privadas. Esto garantizó que los dispositivos tuvieran una dirección IP pública adecuada para la red.

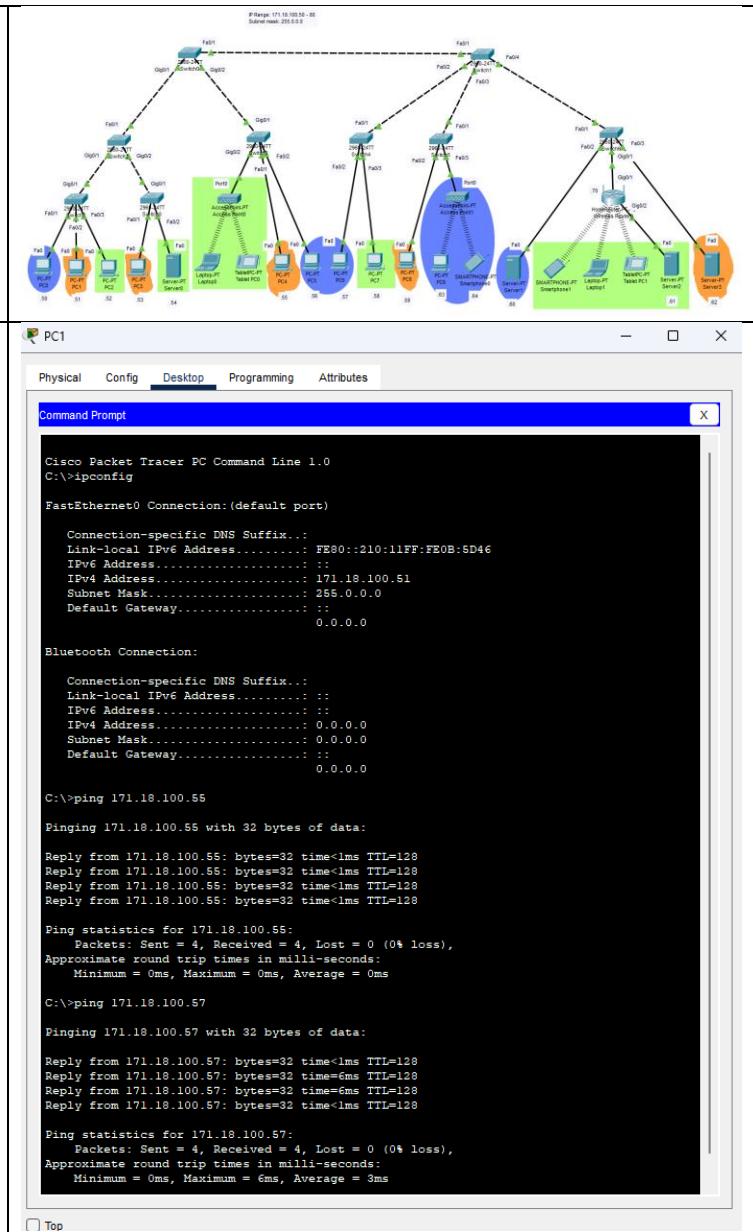


Finalmente, se estableció la conexión con el router para los dispositivos que aún faltaban por conectar.



De esta manera, la topología completa quedó configurada sin implementar VLANs, funcionando como una red única en la que todos los dispositivos.

Para probar el funcionamiento de la red, se utilizó PC1 con dirección IP 171.18.100.51 y se realizó un ping a las máquinas con IP 171.18.100.51 y 171.18.100.57. En el primer caso, al hacer ping a 171.18.100.51, se enviaron 4 paquetes con 0% de pérdida y un tiempo promedio de 0 ms. En el segundo caso, al hacer ping a 171.18.100.57, también se enviaron 4 paquetes, con 0% de pérdida y un tiempo promedio de 3 ms, lo que indica una conectividad estable y rápida entre los dispositivos dentro de la misma red.



La configuración de las VLANs se realizó en todos los switches, incluyendo los intermedios, para segmentar la red y garantizar que el tráfico se dirigiera adecuadamente a cada grupo de dispositivos. Primero, se crearon tres VLANs: VLAN 10 para la red Rectangle, VLAN 20 para la red Circle, y VLAN 30 para la red Irregular. Luego, se asignaron las interfaces correspondientes a cada VLAN en los switches. Una vez configuradas las VLANs y asignadas las interfaces a cada una, se configuraron los puertos de trunk para permitir que el tráfico de todas las VLANs (10, 20 y 30) pudiera atravesar los switches intermedios sin problemas. Finalmente, se guardó la configuración para que se mantuviera después de un reinicio, y se verificó que el tráfico entre las diferentes VLANs y dispositivos estuviera correctamente segmentado y gestionado a través de los switches.

```

Switch>enable
Switch>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Rectangle
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Irregular
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,30
Switch(config-if)#exit
Switch(config)#exit
Switch# 
SYS-5-CONFIG_I: Configured from console by console

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

```

Inicialmente, se realizó una prueba de conectividad entre dos dispositivos que pertenecen a diferentes VLANs dentro de la misma red. Se intentó hacer un ping desde 171.18.100.50 a 171.18.100.51, pero se obtuvo el mensaje de request timed out, lo que resultó en un 100% de pérdida de paquetes.

```

PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::205:SEFF:FE0E:B16E
IPv6 Address.....: :::
IPv4 Address.....: 171.18.100.50
Subnet Mask.....: 255.0.0.0
Default Gateway.....: :::
0.0.0.0

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0

C:\>ping 171.18.100.51

Pinging 171.18.100.51 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 171.18.100.51:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

```

La siguiente prueba se realizó dentro de la misma red y la misma VLAN, utilizando direcciones IP privadas. En esta prueba, se hizo un ping desde 192.168.0.10 a 192.168.0.11 a través del Access Point 0, que estaba configurado en VLAN 10. Se enviaron 4 paquetes, todos los cuales fueron recibidos correctamente, resultando en 0% de pérdida de paquetes. El tiempo promedio de respuesta fue de 22 ms.

```

Laptop
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>

ipconfig

Bluetooth Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0

Wireless0 Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:97FF:FE68:15DD
IPv6 Address.....: :::
IPv4 Address.....: 192.168.0.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
192.168.0.1

C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time=40ms TTL=128
Reply from 192.168.0.11: bytes=32 time=15ms TTL=128
Reply from 192.168.0.11: bytes=32 time=15ms TTL=128
Reply from 192.168.0.11: bytes=32 time=14ms TTL=128

Ping statistics for 192.168.0.11:
Packets: Sent = 4, Received = 4 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 40ms, Average = 22ms
C:\>

```

En la siguiente prueba, se intentó hacer un ping desde 171.18.100.52 a 171.18.100.56, que pertenecen a diferentes redes y diferentes VLANs. Como resultado, se obtuvo el mensaje request timed out, con 100% de pérdida de paquetes.

```

PC2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::207:ECFF:FE00:5278
IPv6 Address.....: ::1
IPv4 Address.....: 171.18.100.52
Subnet Mask.....: 255.0.0.0
Default Gateway.....: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ping 171.18.100.56

Pinging 171.18.100.56 with 32 bytes of data:

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

Ping statistics for 171.18.100.56:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

```

En esta prueba, se realizó un ping desde 171.18.100.51 a 171.18.100.53, que, aunque pertenecen a diferentes redes, están en la misma VLAN. Se enviaron 4 paquetes, todos los cuales fueron recibidos correctamente, con un resultado de 0% de pérdida y un tiempo promedio de respuesta de 1 ms.

```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::210:11FF:FE0B:5D46
IPv6 Address.....: ::1
IPv4 Address.....: 171.18.100.51
Subnet Mask.....: 255.0.0.0
Default Gateway.....: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ping 171.18.100.53

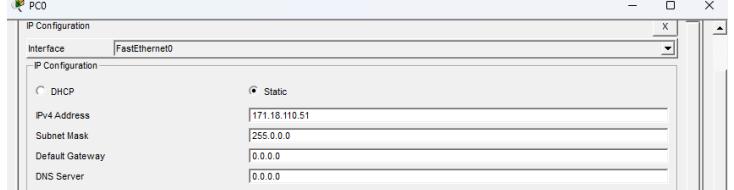
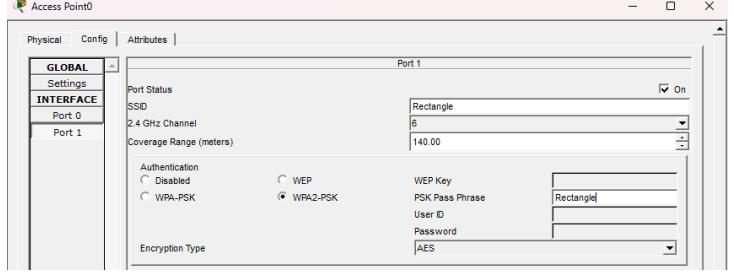
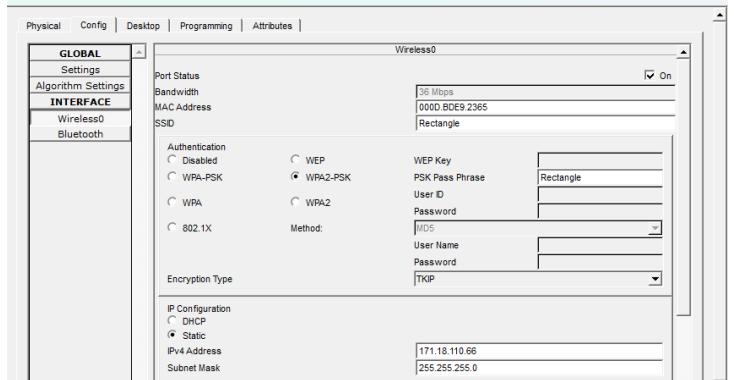
Pinging 171.18.100.53 with 32 bytes of data:

Reply from 171.18.100.53: bytes=32 time<1ms TTL=128
Reply from 171.18.100.53: bytes=32 time=5ms TTL=128
Reply from 171.18.100.53: bytes=32 time<1ms TTL=128
Reply from 171.18.100.53: bytes=32 time<1ms TTL=128

Ping statistics for 171.18.100.53:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 5ms, Average = 1ms
C:\>

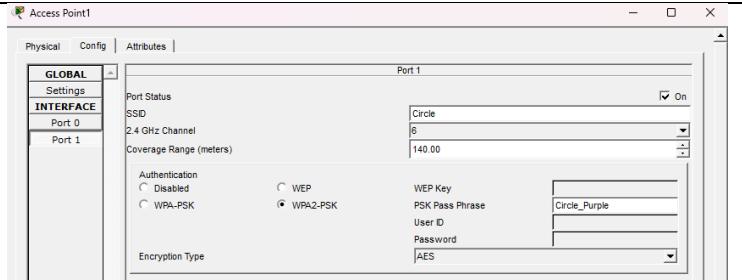
```

Implementación de Natalia

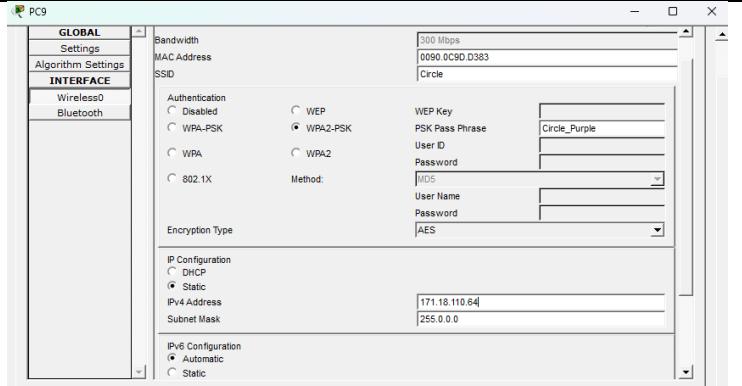
Acción Realizada	Captura de pantalla
<p>En esta primera imagen se muestra la configuración manual de la dirección IP en PC0 dentro de Cisco Packet Tracer.</p>	
<p>Se muestra la configuración del Access Point para la red inalámbrica verde, identificada como Rectangle. Esta configuración garantiza que los dispositivos móviles puedan conectarse de forma segura a la red verde, cumpliendo con los parámetros solicitados en el enunciado y asegurando la autenticación mediante un estándar robusto.</p>	
<p>Se muestra la configuración de Laptop0 para conectarse a la red inalámbrica verde con SSID Rectangle. Esta configuración asegura que el equipo pueda conectarse de forma segura al Access Point y participar en la comunicación dentro de la topología definida.</p>	
<p>Se muestra la configuración básica del Wireless Router para la red verde con SSID Rectangle. Esta configuración es fundamental para garantizar que la red inalámbrica esté visible y operativa, permitiendo la conexión segura de los dispositivos previamente configurados.</p>	

<p>Se muestra la configuración del DHCP Server en el Wireless Router para la red verde. Esta configuración permite que los dispositivos conectados al SSID Rectangle obtengan su dirección IP sin necesidad de configuración manual, facilitando la administración y garantizando la conectividad dentro de la red verde.</p>	
<p>Se muestra la configuración de seguridad inalámbrica del Wireless Router para la red verde. Esta configuración es fundamental para asegurar la integridad y confidencialidad de la red inalámbrica, evitando vulnerabilidades y cumpliendo con el estándar WPA2-PSK.</p>	
<p>Se muestra la configuración de la interfaz WAN del Wireless Router para conectarlo a la red cableada. Esta configuración permite que el router actúe como puente entre la red inalámbrica (192.168.0.x) y la red cableada (171.18.110.x), garantizando la comunicación entre dispositivos de ambas redes.</p>	
<p>Se muestra la configuración de Tablet PC1 para conectarse a la red inalámbrica verde con SSID Rectangle. Esta configuración permite que la tablet se conecte de forma segura al Access Point.</p>	

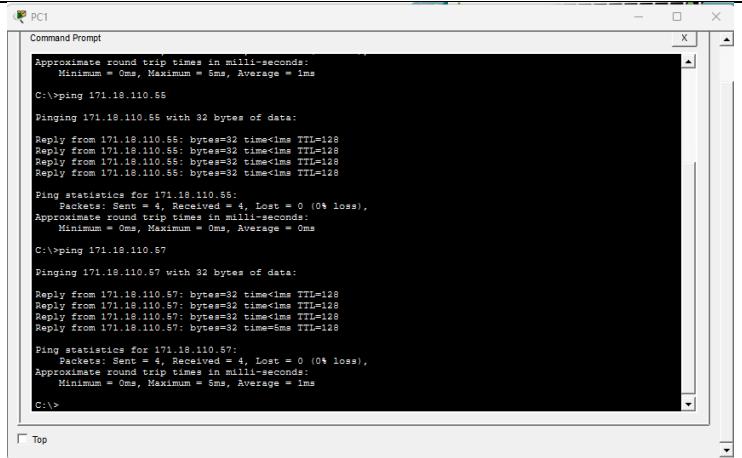
Se muestra la configuración del Access Point para la red inalámbrica morada, identificada como Circle. Esta configuración garantiza que los dispositivos que se conecten a esta red lo hagan de manera segura, cumpliendo con los parámetros solicitados para la red morada en el enunciado.



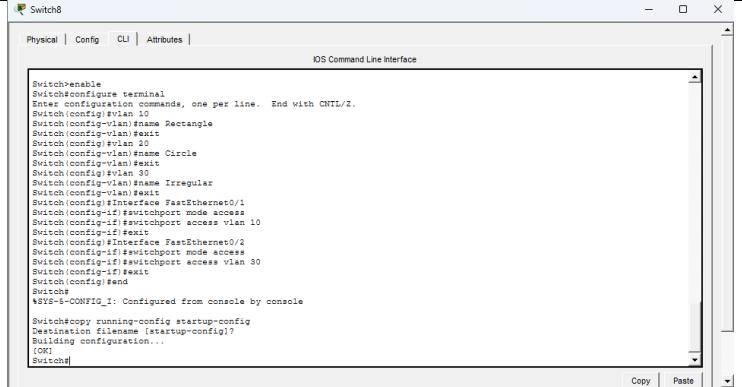
Se muestra la configuración de PC9 para conectarse a la red inalámbrica morada con SSID Circle. Esta configuración asegura conectividad segura y coherente dentro de la topología morada.



En esta fase, antes de configurar las VLAN, se está realizando una verificación de conectividad lógica mediante el comando ping entre dispositivos que pertenecen a diferentes rangos IP dentro de la misma red física. El objetivo es confirmar que todos los equipos pueden comunicarse entre sí sin restricciones, ya que actualmente no hay segmentación por VLAN.



En esta etapa se realiza la segmentación lógica de la red mediante la creación y asignación de VLANs en el switch. Cada VLAN corresponde a un grupo de dispositivos según el diseño del proyecto, lo que permite aislar el tráfico entre ellas para mejorar la seguridad y el control de la red.



En esta etapa, después de configurar las VLAN, se observa que al intentar hacer ping a una máquina ubicada en otra VLAN, todas las solicitudes terminan en “Request timed out” y el resultado indica 100% de pérdida de paquetes. Esto ocurre porque la segmentación lógica aplicada mediante VLANs impide la comunicación directa entre dispositivos que pertenecen a diferentes dominios de broadcast.

```
Pinging 171.18.110.52 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 171.18.110.52:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Revisando las redes WiFi-cercanas

Se realizó un análisis de las redes WiFi-cercanas utilizando la aplicación WiFi Analyzer.

El objetivo fue identificar las redes disponibles, las bandas de frecuencia en las que operan y los canales utilizados. Además, se verificó la presencia de redes en las bandas de 2.4 GHz, 5 GHz, 6 GHz y 60 GHz.

Figura 7

Lista de puntos de acceso Wi-Fi detectados en la banda de 2.4 GHz.



Nota. La imagen presenta diferentes redes inalámbricas disponibles, con detalles como dirección MAC, cifrado WPA2-PSK y canales utilizados, lo que permite analizar la distribución y seguridad de las redes en el entorno.

Figura 8

Lista de puntos de acceso Wi-Fi detectados en la banda de 5 GHz.



Nota. La imagen presenta diferentes redes inalámbricas disponibles en la banda de 5 GHz, con detalles como dirección MAC, cifrado WPA2-PSK y canales utilizados, lo que permite analizar la distribución y seguridad de las redes en el entorno.

Figura 9

Lista de puntos de acceso Wi-Fi detectados en la banda de 6 GHz.



Nota. La imagen muestra la ausencia de redes disponibles en el área en ese momento, lo que indica que no hay dispositivos emitiendo señal en la frecuencia analizada.

Redes en banda 2.4 GHz

Nombre de Red	Frecuencia	Canal
46190A	2412 MHz	CH 1
WG_FAMILIA_MALAVER	2432 MHz	CH 5
FILIA DIAMOND	2462 MHz	CH 11
sc-f650	2412 MHz	CH 1
CLARO-B4F8	2452 MHz	CH 9
FAMILIA ROMERO 2.4	2422 MHz	CH 3

Redes en banda 5 GHz

Nombre de Red	Frecuencia	Canal
46190A	5180 MHz	CH 36
HiddenSSID	5260 MHz	CH 52
Maria_Cortes	5660 MHz	CH 132
sc-f650	5520 MHz	CH 104
Claro_5G_67F0DB	5220 MHz	CH 44

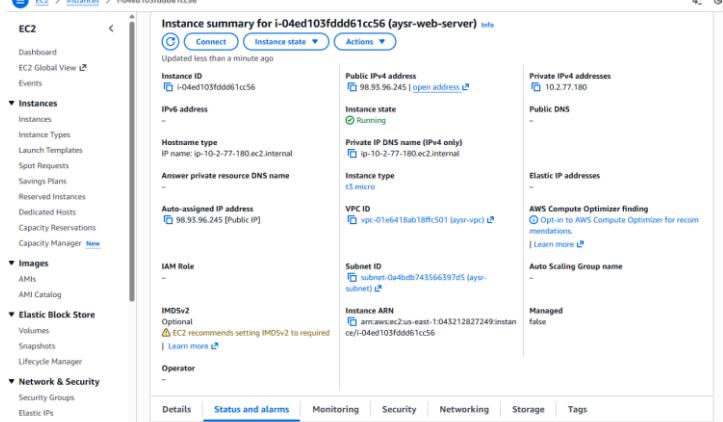
Se detectaron redes en las bandas de 2.4 GHz y 5 GHz. No se encontraron redes en la banda de 6 GHz ni en la banda de 60 GHz. Esto indica que en el entorno analizado no hay dispositivos que soporten WiFi 6E (6 GHz) ni tecnologías WiGig (60 GHz).

Sí hay redes en las bandas de 2.4 GHz y 5 GHz. No hay redes en las bandas de 6 GHz ni 60 GHz. La mayoría de las redes domésticas utilizan 2.4 GHz por su mayor alcance, mientras que 5 GHz ofrece mayor velocidad, pero menor cobertura.

Instalación del software básico

Servicio web dinámico

En esta sección, se desarrollará una aplicación web que se desplegará en un servidor Apache, utilizando como base el laboratorio en la plataforma AWS Cloud. La aplicación funcionará como una calculadora básica de calificaciones para estudiantes, solicitando el nombre del estudiante y las calificaciones finales de cada tercio del semestre. Luego, calculará la calificación final del semestre con un esquema de ponderación (30%, 30%, y 40%). La aplicación estará configurada para interpretar código PHP de forma dinámica, permitiendo realizar los cálculos en tiempo real. Además, los registros de los estudiantes, que incluirán sus nombres y calificaciones calculadas, se almacenarán en una base de datos relacional, como PostgreSQL, para su consulta y almacenamiento a largo plazo.

Acción Realizada	Captura de pantalla
Se utilizó la instancia EC2 previamente creada para configurar el servidor Apache.	 <p>The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like Dashboard, EC2 Global View, Events, Instances, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, and Placement Groups. The main panel displays the instance summary for 'i-04ed103fddd61cc56 (aysr-web-server)'. It shows the instance ID, Public IP address (98.93.96.245), Private IP address (10.2.77.180), Instance state (Running), and VPC ID (vpc-01e6418ab18fffc501). The instance is associated with a subnet (subnet-0a4bdb743566397d5) and an Auto Scaling group (aysr-subnet).</p>

Se actualizó el sistema con el comando sudo yum update -y para asegurar que todos los paquetes estuvieran al día. Luego, se instalaron Apache, el módulo SSL para conexiones seguras, PHP y el controlador php-mysqlnd utilizando sudo yum install httpd mod_ssl php php-mysqlnd -y. Después, se inició el servicio de Apache con sudo systemctl start httpd y se verificó su estado con sudo systemctl status httpd, confirmando que el servicio estaba activo. A continuación, se habilitó Apache para que se inicie automáticamente en el arranque con sudo systemctl enable httpd. Para probar la instalación de PHP, se creó un archivo de prueba info.php en /var/www/html con sudo nano /var/www/html/info.php.

Finalmente, se reinició Apache con sudo systemctl restart httpd para asegurarse de que todos los cambios y configuraciones fueran aplicados correctamente.

```
ec2-user@ip-10-2-77-180:~ + - 
mod_ssl.x86_64 1:2.4.65-1.amzn2.0.2      php.x86_64 0:5.4.16-46.amzn2.0.6      php-mysqlnd.x8
Dependency Installed:
liblalloc.x86_64 0:2.1.16-1.amzn2
php-cli.x86_64 0:5.4.16-46.amzn2.0.6
php-pdo.x86_64 0:5.4.16-46.amzn2.0.6
libzip010-compat.x86_64 0:0.10.1-9
php-common.x86_64 0:5.4.16-46.amzn2.0.1
sscg.x86_64 0:2.3.3-2.amzn2.0.1

Complete!
[ec2-user@ip-10-2-77-180 ~]$ sudo systemctl start httpd
[ec2-user@ip-10-2-77-180 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
    Active: active (running) since Sat 2025-11-22 03:29:46 UTC; 21min ago
      Docs: man:httpd.service(8)
 Main PID: 2028 (httpd)
   Status: "Total requests: 5; Idle/Busy workers 100/0;Requests/sec: 0.00385; Bytes served/
 CGroup: /system.slice/httpd.service
         ├─2028 /usr/sbin/httpd -DFOREGROUND
         ├─2062 /usr/sbin/httpd -DFOREGROUND
         ├─2063 /usr/sbin/httpd -DFOREGROUND
         ├─2064 /usr/sbin/httpd -DFOREGROUND
         ├─2065 /usr/sbin/httpd -DFOREGROUND
         ├─2066 /usr/sbin/httpd -DFOREGROUND
         ├─2318 /usr/sbin/httpd -DFOREGROUND

Nov 22 03:29:46 ip-10-2-77-180.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Nov 22 03:29:46 ip-10-2-77-180.ec2.internal systemd[1]: Started The Apache HTTP Server.
[ec2-user@ip-10-2-77-180 ~]$ sudo systemctl enable httpd
[ec2-user@ip-10-2-77-180 ~]$ sudo nano /var/www/html/info.php
[ec2-user@ip-10-2-77-180 ~]$ |
```

Se abrió la dirección IP pública del servidor, que en ese momento era <http://98.93.96.245/info.php>, y se verificó que la instalación de Apache y PHP se realizó correctamente. Al acceder a esta página de prueba, se confirmó que PHP estaba funcionando correctamente y se mostró la información detallada de la configuración de PHP. Además, se verificó que el plugin de MySQL estaba instalado y configurado correctamente, lo que indica que el servidor estaba listo para interactuar con bases de datos.

The screenshot shows the output of the PHP info page. Key details include:

- System:** Linux ip-10-2-77-180 ec2.internal 4.14.355-280.698.amzn2.x86_64 #1 SMP Mon Oct 18:10:46 UTC 2025
- Build Date:** Apr 7 2025 16:22:56
- Server API:** Apache 2.0 Handler
- Virtual Directory Support:** disabled
- Configuration File (php.ini) Path:** /etc
- Loaded Configuration File:** /etc/php.ini
- Scan this dir for additional .ini files:** /etc/php.d
- Additional .ini files parsed:** /etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/mysqlind.ini, /etc/php.d/mysqlnd.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqldnd.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysqlnd.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/sqlite3.ini, /etc/php.d/zip.ini
- PHP API:** 20100412
- PHP Extension:** 20100525
- Zend Extension:** 220100525
- Zend Extension Build:** API20100525.NTS
- PHP Extension Build:** API20100525.NTS
- Debug Build:** no
- Thread Safety:** disabled
- Zend Signal Handling:** disabled
- Zend Memory Manager:** enabled
- Zend Multibyte Support:** disabled
- IPv6 Support:** enabled
- DTrace Support:** disabled
- Registered PHP Streams:** https, ftps, compress,zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
- Registered Stream Socket Transports:** tcp, udp, unix, udg, ssl, sslv3, tls
- Registered Stream Filters:** zlib*, bzip2*, convert.iconv*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert*, consumed, dechunk

Powered By Zend Engine 2

Se instaló MariaDB utilizando el comando sudo yum install -y mariadb-server, lo que permitió la instalación del servidor de bases de datos. Luego, se verificó la versión de MariaDB instalada con mysql --version para asegurar que la instalación fuera exitosa. A continuación, se inició el servicio de MariaDB con sudo systemctl start mariadb y se habilitó para que se inicie automáticamente al arrancar el sistema con sudo systemctl enable mariadb. Finalmente, se ejecutó sudo mysql_secure_installation para asegurar y configurar MariaDB, lo que incluye establecer una contraseña de root, eliminar usuarios y bases de datos innecesarias y mejorar la seguridad general de la instalación.

```
[ec2-user@ip-10-2-77-180:~]$ mysql --version
mysql  Ver 15.1 Distrib 5.5.68-MariaDB, for Linux (x86_64) using readline 5.1
[ec2-user@ip-10-2-77-180:~]$ sudo systemctl start mariadb
[ec2-user@ip-10-2-77-180:~]$ sudo systemctl enable mariadb
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.
[ec2-user@ip-10-2-77-180:~]$ |
```

Primero, se ingresó a MariaDB como usuario root con el comando mysql -u root -p. Luego, se creó la base de datos school_grades_db con el comando CREATE DATABASE school_grades_db;. A continuación, se creó un nuevo usuario llamado 'santiago' con el comando CREATE USER 'santiago'@'localhost' IDENTIFIED BY 'peanut123';, asignándole la contraseña 'peanut123'. Se le otorgaron todos los privilegios sobre la base de datos school_grades_db con el comando GRANT ALL PRIVILEGES ON school_grades_db.* TO 'santiago'@'localhost'. Finalmente, se ejecutó FLUSH PRIVILEGES; para aplicar los cambios.

```
ec2-user@ip-10-2-77-180:~ % mysql -u root -p
Cleaning up...
All done! If you've completed all of the above steps, your MariaDB installation should now be secure.

Thanks for using MariaDB!
[ec2-user@ip-10-2-77-180 ~]$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 5.5.68-MariaDB MariaDB Server

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

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

MariaDB [(none)]> CREATE DATABASE school_grades_db;
Query OK, 1 row affected (0.00 sec)

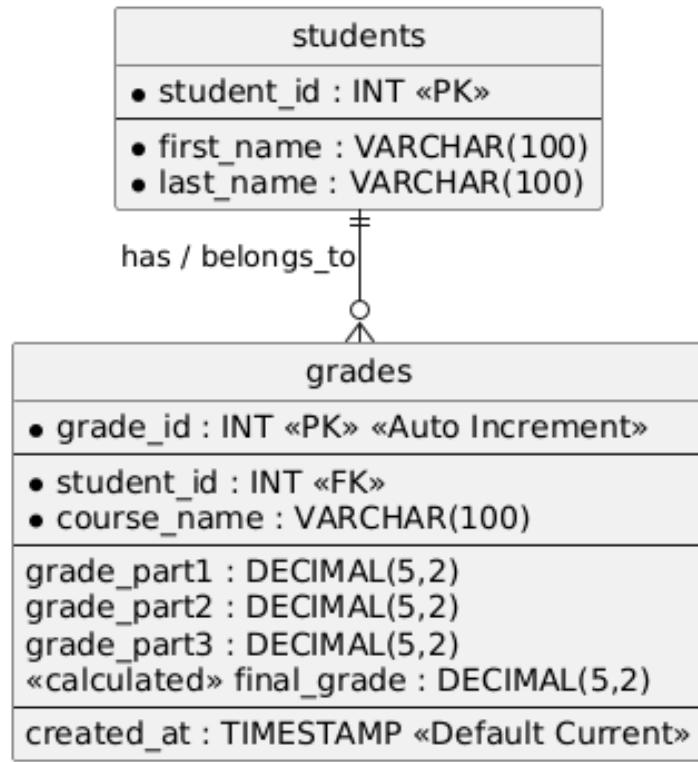
MariaDB [(none)]> CREATE USER 'santiago'@'localhost' IDENTIFIED BY 'peanut123';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON school_grades_db.* TO 'santiago'@'localhost';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]>
```

Se desarrolló un diagrama entidad-relación (ER) simplificado para la base de datos school_grades_db, que incluye dos entidades principales: Students (Estudiantes) y Grades (Calificaciones).



Se utilizó el comando USE school_grades_db; para seleccionar la base de datos school_grades_db en el entorno de MariaDB. A continuación, se ejecutaron las consultas SQL necesarias para crear las tablas y establecer la estructura de la base de datos.

```
ec2-user@ip-10-2-77-180:~ % + v
MariaDB [school_grades_db]> CREATE VIEW student_final_grades AS SELECT grade_id, student_id, course_name, grade_part1, grade_part2, grade_part3, (grade_part1 * 0.3 + grade_part2 * 0.3 + grade_part3 * 0.4) AS final_grade, created_at FROM grades;
Query OK, 0 rows affected (0.00 sec)

MariaDB [school_grades_db]> SHOW TABLES;
+ Tables_in_school_grades_db +
| grades      |
| student_final_grades |
| students    |
+-----+
3 rows in set (0.00 sec)

MariaDB [school_grades_db]> DESCRIBE grades;
+-----+-----+-----+-----+-----+
| Field | Type   | Null | Key | Default | Extra       |
+-----+-----+-----+-----+-----+
| grade_id | int(11) | NO  | PRI | NULL    | auto_increment |
| student_id | int(11) | NO  | MUL | NULL    |                |
| course_name | varchar(100) | NO  |     | NULL    |                |
| grade_part1 | decimal(5,2) | YES |     | NULL    |                |
| grade_part2 | decimal(5,2) | YES |     | NULL    |                |
| grade_part3 | decimal(5,2) | YES |     | NULL    |                |
| created_at | timestamp | NO  |     | CURRENT_TIMESTAMP |                |
+-----+-----+-----+-----+-----+
7 rows in set (0.00 sec)

MariaDB [school_grades_db]>
```

Se creó el archivo index.php para manejar la lógica de la aplicación y capturar las calificaciones de los estudiantes, y el archivo styles.css para definir el diseño y los estilos visuales de la página.

```
MariaDB [school_grades_db]> EXIT;
Bye
[ec2-user@ip-10-2-77-180 ~]$ nano /var/www/html/index.html
[ec2-user@ip-10-2-77-180 ~]$ sudo nano /var/www/html/index.php
[ec2-user@ip-10-2-77-180 ~]$ sudo nano /var/www/html/styles.css
[ec2-user@ip-10-2-77-180 ~]$ |
```

La siguiente captura muestra la página desplegada correctamente en el navegador, con la interfaz funcional y los estilos aplicados, confirmando que la aplicación web está funcionando según lo esperado.

La siguiente captura muestra la inserción correcta de los datos en la base de datos, donde se agregaron las calificaciones del estudiante Santiago para la materia AYSR. Las calificaciones fueron: primer tercio con 3.0, segundo tercio con 4.0, y tercer tercio con 3.8. La aplicación calculó correctamente la nota ponderada de 3.6, según el esquema de ponderación (30%, 30%, 40%). Además, la información se reflejó correctamente en la base de datos, incluyendo la asignatura como atributo asociado a las calificaciones.

The screenshot shows a web-based application titled "School Grades Management". At the top, it says "Enter student grades for a course" and "Grades saved successfully for **Santiago**". Below this, there are four input fields: "Student Name" (Santiago), "Course Name" (AYSR), "Grade Part 1" (3.0), "Grade Part 2" (4.0), and "Grade Part 3" (3.8). A blue "Save Grades" button is visible. Below the form is a table titled "All Student Grades" with one row:

Student Name	Course	Grade 1	Grade 2	Grade 3	Average
Santiago	AYSR	3.00	4.00	3.80	3.60

Otros comandos útiles

Módulo de Monitoreo y Diagnóstico de Red

El script network_info_menu.sh implementa un menú interactivo para la consulta de información de red en sistemas Unix/Linux. Está diseñado para ser portable, funcionando tanto en Linux como en Solaris, BSD u otros sistemas UNIX, y adaptándose dinámicamente a los comandos disponibles en cada entorno. Entre sus funcionalidades destacan la visualización de interfaces de red y sus direcciones IP, la consulta de la tabla de ruteo, el listado de conexiones activas (TCP/UDP), estadísticas detalladas por interfaz y un reporte consolidado del estado general de la red. Además, integra mecanismos de manejo de errores, verificación de comandos, trazas de tiempo y un menú interactivo limpio con refresco de pantalla, mejorando la experiencia del operador y la seguridad del monitoreo.

La estrategia de desarrollo se basó en tres principios fundamentales: portabilidad multiplataforma, diseño modular e interfaz interactiva controlada. Para garantizar la portabilidad,

el script identifica automáticamente el sistema operativo mediante uname -s y selecciona los comandos apropiados según la disponibilidad: ip como preferencia en Linux, ifconfig como fallback en Unix, route o netstat cuando no existen alternativas modernas, y herramientas como ethtool o vnstat para estadísticas avanzadas según disponibilidad. Esto asegura que el script funcione correctamente en distribuciones modernas de Linux, Solaris, BSD y otros sistemas antiguos que no cuenten con herramientas recientes.

El diseño modular del script encapsula cada funcionalidad en funciones independientes (show_interfaces, show_routes, show_connections, show_statistics y show_summary), lo que facilita su mantenimiento, depuración y ampliación. Cualquier cambio futuro puede aplicarse a funciones específicas sin afectar el resto del flujo. Por otro lado, la interfaz interactiva incluye un menú persistente, limpieza de pantalla mediante secuencias ANSI, mensajes de log con timestamp y control de errores mediante set -e y trap ERR. Esto garantiza que ante fallos inesperados el script informe al operador de manera clara y finalice ordenadamente, evitando procesos huérfanos o estados inconsistentes.

Figura 10

Tabla de rutas y rutas IPv4/IPv6 en Solaris mediante la opción 2 del script.

```

Network Information Menu:
1) Show interfaces and IP addresses
2) Show routing table
3) Show active network connections
4) Show interface statistics
5) Show summarized network report
6) Exit
Select an option [1-6]: 2

Routing Table: IPv4
Destination          Gateway          Flags Ref   Use      Interface
-----              -----          -----  ---  ---  -----
default             10.2.65.1        UG     4      1237
10.2.0.0            10.2.77.180       U      5      4002 net0
127.0.0.1           127.0.0.1        UH     2      256 1lo0

Routing Table: IPv6
Destination/Mask    Gateway          Flags Ref   Use      If
-----              -----          -----  ---  ---  -----
::1                ::1              UH     2      566 1lo0
2800:484:1373:a500:643f:67dd:202e:884f 2800:484:1373:a500:643f:67dd:202e:884f UH
2                  0 net0          fe80::20c:29ff:feee:c12c   U      2      0 net0

Press Enter to continue...

```

Nota. La captura muestra que el script detecta correctamente las rutas activas en Solaris, listando tanto direcciones IPv4 como IPv6, lo que permite verificar la conectividad y la configuración de la red en este sistema operativo.

Figura 11

Resumen general de la red en Slackware mediante la opción 5 del script.

```

Network Information Menu:
1) Show interfaces and IP addresses
2) Show routing table
3) Show active network connections
4) Show interface statistics
5) Show summarized network report
6) Exit
Select an option [1-6]: 5
2025-11-22 03:40:29 - Generating summarized network report...
Hostname: darkstar
Uptime: 03:40:29 up 2:48
Default Gateway: 10.2.65.1
Active Interfaces and IP Addresses:
lo: 127.0.0.1/8
eth0: 10.2.77.182/16

Press Enter to continue...

```

Nota. La captura presenta el reporte consolidado generado por el script, incluyendo uptime, hostname, gateway e interfaces de red, demostrando que el script funciona correctamente en sistemas Linux antiguos y proporciona información resumida del estado de la red.

Mecanismo de Detección de Puertos

El script desarrollado tiene como objetivo verificar si un puerto específico está abierto en el host local y, si es así, identificar el servicio asociado a dicho puerto según el archivo de servicios del sistema, ya sea /etc/services o /etc/inet/services. Para lograrlo, el script primero intenta usar nc (netcat) para la verificación de puertos, y si no está disponible, recurre de manera secuencial a nmap, telnet, y netstat, según lo que esté disponible en el sistema. Una vez determinado el estado del puerto, el script consulta el archivo de servicios utilizando awk, que analiza línea por línea el archivo de configuración del sistema, identificando el puerto y el protocolo, y extrae el nombre del servicio correspondiente. Esto garantiza que el script funcione en entornos antiguos y actuales, incluso cuando se presentan variaciones en el formato del archivo de servicios.

La estrategia de desarrollo del script se centró en asegurar la compatibilidad, precisión y robustez en la detección de puertos abiertos y en la identificación de los servicios correspondientes. Debido a la falta de soporte para versiones modernas de grep y awk en la distribución utilizada, se diseñó el script para ser completamente compatible con versiones más antiguas de estas herramientas. Para la identificación del servicio, se evitó el uso de expresiones regulares avanzadas y se implementó un parser manual en awk que analiza línea por línea el archivo de servicios, garantizando que incluso los puertos con espacios irregulares, comentarios u otros formatos específicos de distribuciones como Solaris o BSD puedan ser procesados correctamente. Además, la detección de puertos abiertos se realiza de manera escalonada, utilizando las herramientas disponibles en el sistema, lo que asegura que el script funcione en una amplia variedad de entornos, desde sistemas actuales hasta configuraciones más antiguas o mínimas.

Figura 12

Resultado del script en Slackware identificando el puerto 22 abierto.

```
root@darkstar:~# ss -tuinp
Netid State Recv-Q Send-Q Local Address:Port    Peer Address:Port Process
tcp   LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users:(("sshd",pid=991,fd=3))
tcp   LISTEN 0      128          [::]:22        [::]:*      users:(("sshd",pid=991,fd=4))
root@darkstar:~# bash /mnt/solaris_share/port_check.sh 22
Port 22 is OPEN. Service: **ssh**
root@darkstar:~#
```

Nota. La captura muestra que el script detecta correctamente que únicamente el puerto 22 (SSH) está abierto en el sistema Slackware, demostrando su capacidad de verificación de puertos en entornos Linux antiguos.

Figura 13

Resultado del script en Solaris identificando los puertos 22 y 139 abiertos.

```
aurora@solaris:~$ netstat -an | grep LISTEN
127.0.0.1.5999      *.*                  0      0 256000      0 LISTEN
      *.22             *.*                  0      0 256000      0 LISTEN
127.0.0.1.4999      *.*                  0      0 256000      0 LISTEN
127.0.0.1.631       *.*                  0      0 256000      0 LISTEN
      *.111            *.*                  0      0 256000      0 LISTEN
      *.111            *.*                  0      0 256000      0 LISTEN
      *.515            *.*                  0      0 256000      0 LISTEN
      *.445            *.*                  0      0 256000      0 LISTEN
      *.139            *.*                  0      0 256000      0 LISTEN
      *.6787           *.*                  0      0 256000      0 LISTEN
      ::1.5999          *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      *.22              *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      ::1.631           *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      *.111            *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      *.515            *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      *.445            *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      *.139            *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
      *.6787           *.*                  0      0 256000      0 LISTEN
      0 256000          0 LISTEN
aurora@solaris:~$ bash /path/to/shared/directory/port_check.sh 22
Port 22 is OPEN. Service: **ssh**
aurora@solaris:~$ bash /path/to/shared/directory/port_check.sh 139
Port 139 is OPEN. Service: **netbios-ssn**
aurora@solaris:~$
```

Nota. La captura muestra que el script detecta correctamente los puertos 22 (SSH) y 139 (NetBIOS-SSN) en Solaris, confirmando su funcionamiento en sistemas Unix y la correcta identificación de los servicios asociados.

Gestión de red

Acción Realizada	Captura de pantalla
Este paso corresponde a la instalación del paquete Net-SNMP, en Solaris que implementa el protocolo SNMP.	<pre>root@solaris:~# pkg install net-snmp No hay actualizaciones para esta imagen. root@solaris:~# </pre>
Este comando crea el directorio /etc/snmp, que se utilizará para almacenar los archivos de configuración del servicio SNMP en Solaris.	<pre>root@solaris:~# mkdir -p /etc/snmp root@solaris:~# </pre>
Se muestra la edición del archivo /etc/snmp/snmpd.conf utilizando el editor nano. Aquí se está configurando el servicio SNMP en Solaris para definir parámetros básicos de monitorización	<pre>GNU nano 2.9.3 /etc/snmp/snmpd.conf ``'s Basic SNMP configuration for Solaris # Solo lectura con comunidad 'public' rocommunity public default # Información del sistema syslocation "Solaris VM" syscontact "admin@empresa.local" # Monitoreo básico de recursos disk / 10% load 12 10 5</pre>
El primer comando habilita el servicio net-snmp, permitiendo que el agente SNMP escuche solicitudes. El segundo comando verifica su estado: net-snmp:default aparece activo y snmp-notify deshabilitado. Esto confirma que el agente SNMP está funcionando y listo para responder consultas de monitoreo remoto.	<pre>root@solaris:~# svcadm enable svc:/application/management/net-snmp:default root@solaris:~# svcs -a grep snmp disabled 8:46:05 svc:/system/fm/snmp-notify:default online 9:25:39 svc:/application/management/net-snmp:default root@solaris:~# </pre>
Este comando se utiliza para verificar si el puerto 161/UDP, que es el puerto estándar para el protocolo SNMP, está activo y escuchando en el sistema.	<pre>root@solaris:~# netstat -an grep 161 * 161 Idle 57344 0 57344 0 root@solaris:~# </pre>

<p>El comando <code>snmpwalk -v2c -c public localhost</code> realiza una consulta SNMP al agente local utilizando la versión 2c del protocolo y la comunidad public, este paso es clave porque confirma que el agente SNMP está funcionando correctamente y que las métricas del sistema pueden ser consultadas por herramientas de monitorización remota.</p>	<pre>root@solaris:~# netstat -an grep 161 *.161 Idle 57344 0 57344 0 root@solaris:~# snmpwalk -v2c -c public localhost SNMPv2-MIB::sysDescr.0 = STRING: SunOS solaris 5.11 11.4.0.15.0 186pc SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOids.3 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53017) 0:08:56.17 SNMPv2-MIB::sysContact.0 = STRING: "\System administrator\"" SNMPv2-MIB::sysName.0 = STRING: solaris SNMPv2-MIB::sysLocation.0 = STRING: "(\"System administrators office\")" SNMPv2-MIB::sysServices.0 = INTEGER: 72 SNMPv2-MIB::sysORLastChange.0 = Timeticks: (400) 0:00:04.00 SNMPv2-MIB::sysOID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance SNMPv2-MIB::sysOID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance SNMPv2-MIB::sysOID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance SNMPv2-MIB::sysOID.4 = OID: SNMPv2-MIB::snmpMIB SNMPv2-MIB::sysOID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup SNMPv2-MIB::sysOID.6 = OID: TCP-MIB::tcpMIB SNMPv2-MIB::sysOID.7 = OID: IP-MIB::ip SNMPv2-MIB::sysOID.8 = OID: UDP-MIB::udpMIB SNMPv2-MIB::sysOID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance SNMPv2-MIB::sysOID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching. SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP User-based Security Model. SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB. SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP. SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing TCP implementations SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing IP and ICMP implementations SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing UDP implementations SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering. SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications. SNMPv2-MIB::sysORUpTime.1 = Timeticks: (400) 0:00:04.00 SNMPv2-MIB::sysORUpTime.2 = Timeticks: (400) 0:00:04.00 SNMPv2-MIB::sysORUpTime.3 = Timeticks: (400) 0:00:04.00 SNMPv2-MIB::sysORUpTime.4 = Timeticks: (400) 0:00:04.00 SNMPv2-MIB::sysORUpTime.5 = Timeticks: (400) 0:00:04.00</pre>
<p>Se realizó una modificación en el archivo <code>/etc/snmp/snmpd.conf</code> por <code>rocommunity public 10.2.0.0/16</code>, este ajuste es importante porque refuerza la seguridad del servicio SNMP, evitando accesos desde redes externas y asegurando que solo dispositivos autorizados puedan consultar métricas del sistema.</p>	 <pre>rocommunity public 10.2.0.0/16 syslocation "Solaris VM" syscontact "admin@empresa.local" disk / 10% load 12 10 5</pre>
<p>Este comando reinicia el servicio <code>net-snmp</code> en Solaris para aplicar los cambios realizados en el archivo de configuración <code>snmpd.conf</code>.</p>	<pre>root@solaris:~# svcadm restart svc:/application/management/net-snmp:default root@solaris:~ </pre>
<p>Esta captura corresponde a la instalación del paquete <code>net-snmp</code> en Slackware desde el medio de instalación. Este paso es fundamental porque proporciona el agente SNMP y las utilidades necesarias para habilitar la monitorización en Slackware, permitiendo consultas y gestión remota mediante el protocolo SNMP.</p>	<pre>root@natalia:/mnt/cdrom/slackware64/n# ls grep snmp net-snmp-5.9.1-x86_64-4.txt net-snmp-5.9.1-x86_64-4.txz net-snmp-5.9.1-x86_64-4.txz.asc root@natalia:/mnt/cdrom/slackware64/n# installpkg net-snmp-5.9.1-x86_64-4.txz Verifying package net-snmp-5.9.1-x86_64-4.txz. Installing package net-snmp-5.9.1-x86_64-4.txz [REC]: PACKAGE DESCRIPTION: # net-snmp (Simple Network Management Protocol tools) # # Various tools relating to the Simple Network Management Protocol: # # An extensible agent # An SNMP library # Tools to request or set information from SNMP agents # Tools to generate and handle SNMP traps # A version of the UNIX 'netstat' command using SNMP # A graphical Perl/Tk/SNMP based mib browser # Executing install script for net-snmp-5.9.1-x86_64-4.txz. Package net-snmp-5.9.1-x86_64-4.txz installed. root@natalia:/mnt/cdrom/slackware64/n# which snmpd /usr/sbin/snmpd root@natalia:/mnt/cdrom/slackware64/n# snmpd --version NET-SNMP version: 5.9.1 Web: http://www.net-snmp.org/ Email: net-snmp-coders@lists.sourceforge.net root@natalia:/mnt/cdrom/slackware64/n# </pre>

Se muestra la edición del archivo /etc/snmp/snmpd.conf en Slackware para configurar el agente SNMP.

```
rocommunity public 10.2.0.0/16
#####
# System contact information
#
# It is also possible to set the sysContact and sysLocation system
# variables through the snmpd.conf file:
syslocation "Slackware Monitoring Server"
syscontact "Admin <admin@ysr.local>"
syslocation Unknown (edit /etc/snmp/snmpd.conf)
syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf)

view      systemview     included    .1.3.6.1.2.1.1
view      systemview     included    .1.3.6.1.2.1.25.1.1
access   notConfigGroup  ""        any       noauth      exact      systemview none none
root@natalia:/# chmod +x /etc/rc.d/rc.snmpd
root@natalia:/# /etc/rc.d/rc.snmpd start
Starting snmpd: /usr/sbin/snmpd -A -p /var/run/snmpd -a -c /etc/snmp/snmpd.conf
root@natalia:/# netstat -ulpn | grep 161
udp        0      0      0.0.0.0:161          0.0.0.0:*
                                         1301/snmpd
udp6       0      0      ::1:161             ::*:*
                                         1327/snmpd
```

Este procedimiento confirma que el agente SNMP está activo y listo para recibir solicitudes de monitoreo desde herramientas externas, cumpliendo con el objetivo de supervisar recursos del sistema en tiempo real.

Se ejecuta el comando snmpwalk -v2c -c public localhost en Slackware, que realiza una consulta SNMP al agente local usando la versión 2c del protocolo y la comunidad public. El resultado confirma que el servicio SNMP está activo y responde correctamente

```
root@natalia:/mnt/cdrom/slackware64/n# snmpwalk -v2c -c public localhost
SNMPv2-MIB::sysDescr.0 = STRING: Linux natalia.local 5.15.19 #1 SMP PREEMPT Wed Feb 2 01:50:51 CST 202
2 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (15614) 0:02:36.14
SNMPv2-MIB::sysName.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysContact.0 = STRING: natalia.local
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORDID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORDID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORDID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORDID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORDID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORDID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORDID.8 = OID: IP-MIB::ip
SNMPv2-MIB::sysORDID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORDID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysRUpTime.1 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.2 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.3 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.4 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.5 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.6 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.7 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.8 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.9 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.10 = Timeticks: (0) 0:00:00
HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (133375) 0:22:13.75
HOST-RESOURCES-MIB::hrSystemUptime.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
root@natalia:/mnt/cdrom/slackware64/n#
```

Se ejecuta el comando snmpwalk -v2c -c public 10.2.77.185 que realiza una consulta SNMP desde Solaris hacia la máquina Slackware en la IP 10.2.77.185, utilizando la comunidad public y la versión 2c del protocolo. El resultado confirma que la comunicación entre ambos sistemas funciona correctamente, mostrando información del agente remoto como descripción del sistema, tiempo de actividad, módulos SNMP y objetos MIB disponibles.

```
root@solaris:# snmpwalk -v2c -c public 10.2.77.185
SNMPv2-MIB::sysDescr.0 = STRING: Linux natalia.local 5.15.19 #1 SMP PREEMPT Wed Feb 2 01:50:51 CST 2022 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (352592) 0:58:45.92
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysRUpLastChange.0 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysORDID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORDID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORDID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORDID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORDID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORDID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORDID.8 = OID: IP-MIB::ip
SNMPv2-MIB::sysORDID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORDID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysRUpTime.2 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.3 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.4 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.5 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.6 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.7 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.8 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.9 = Timeticks: (0) 0:00:00
SNMPv2-MIB::sysRUpTime.10 = Timeticks: (0) 0:00:00
HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (470353) 1:18:23.53
HOST-RESOURCES-MIB::hrSystemUptime.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
root@solaris:~#
```

Conclusiones

A lo largo de este laboratorio se consolidaron conocimientos esenciales sobre el funcionamiento de las redes de área local, la arquitectura Ethernet, los mecanismos de switching y diversos servicios de capa de aplicación. Se realizaron configuraciones básicas y avanzadas en switches, incluyendo asignación de nombres, contraseñas, mensajes de día, descripciones de interfaces y almacenamiento de configuraciones, lo cual permitió comprender el proceso real de preparación de un dispositivo de red en un entorno profesional.

La interconexión de equipos y switches evidenció el proceso de aprendizaje de direcciones MAC, la construcción de tablas de conmutación y el comportamiento inicial de broadcast típico de las redes Ethernet. Además, se analizó la operación del algoritmo Spanning Tree, observando cómo evita bucles en topologías con enlaces redundantes.

La implementación de VLANs permitió dividir la red física en dominios lógicos independientes, comprobando el impacto del etiquetado de tramas, la función de los enlaces troncales y el aislamiento del tráfico según el diseño planteado. Asimismo, se construyeron topologías más amplias en Packet Tracer, integrando servidores, computadoras y diversos segmentos de red, verificando su conectividad y funcionamiento.

En la capa de aplicación, se configuró un servicio web dinámico que integra PHP y una base de datos relacional, demostrando el flujo completo de una aplicación que procesa información del usuario y la almacena de forma persistente. Finalmente, se exploraron comandos fundamentales para la administración de red y se desarrolló un script que facilita su ejecución, mejorando la comprensión del estado y rendimiento de los dispositivos. También se instaló y configuró un sistema de monitoreo mediante SNMP, permitiendo visualizar métricas críticas de las máquinas virtuales en tiempo real.

En conjunto, el laboratorio permitió aplicar conceptos teóricos en escenarios prácticos, reforzando competencias en configuración de redes, administración de switches, virtualización, servicios web y monitoreo.