



S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO de Tuxtepec

REPORTE

MATERIA:
INTERCONECTIVIDAD DE REDES

ALUMNO:
JUAN DE JESÚS BAUTISTA GARCÍA
23350591

DOCENTE:
JULIO AGUILAR CARMONA

CARRERA:
INGENIERIA INFORMÁTICA



INDICE

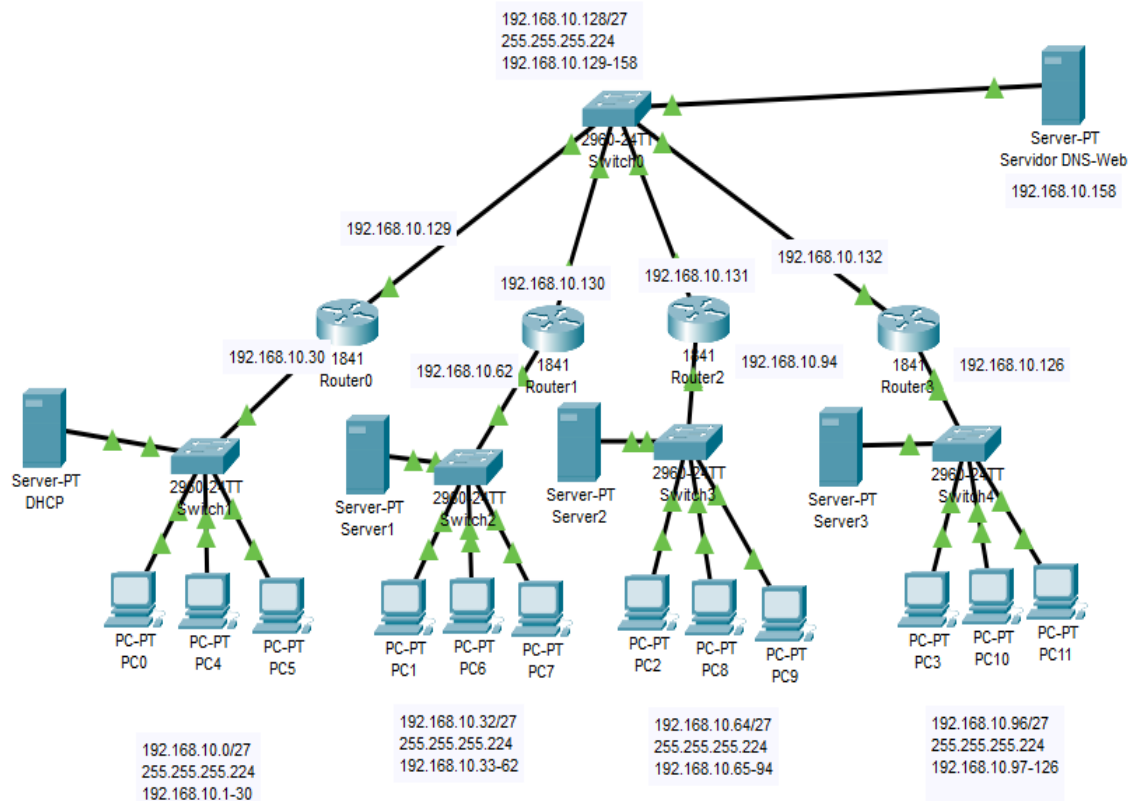
Introducción.....	2
Parámetros de configuración de red.....	3
Estrategia que usa el computo para identificar si está en una red.....	5
Clasificación de direcciones IP	8
Subnetting.....	1
Simulación de red LAN	3
Enrutamiento estático	4
Enrutamiento dinámico	6
VLANs.....	8
Configuración de switches con puerto troncal	10
Redes inalámbricas	12
Conclusión.....	13

INTRODUCCIÓN

Durante el presente semestre, en la materia de Interconectividad de Redes, adquirí conocimientos teóricos y prácticos fundamentales sobre el funcionamiento, la configuración y la administración de redes de computadoras. A lo largo del curso, comprendí la importancia que tienen las redes en el ámbito tecnológico actual, así como su aplicación en distintos entornos, tanto educativos como laborales. Entre los principales temas abordados se encuentran los parámetros de configuración de red, la estrategia que utiliza el cómputo para identificar si un dispositivo se encuentra dentro de una red, la clasificación de las direcciones IP, el subnetting, la simulación de redes LAN, el enrutamiento estático y dinámico, así como la implementación de VLANs. Realicé diversas actividades prácticas utilizando el software Cisco Packet Tracer, en el cual pude simular diferentes escenarios de red, configurar dispositivos de red y comprobar el correcto funcionamiento de las conexiones.



Parámetros de configuración de red



Aprendí a aplicar los parámetros básicos de configuración de red necesarios para que cada dispositivo pueda comunicarse correctamente dentro de su subred y también con otras redes.

Lo primero que realicé fue la asignación de direcciones IP, máscaras de subred y gateways predeterminados a cada PC.

- La subred 192.168.10.0/27 para PCs conectadas al Router0.
- La subred 192.168.10.32/27 para los dispositivos del Router1.
- La subred 192.168.10.64/27 para los conectados al Router2.
- La subred 192.168.10.96/27 para los del Router3.

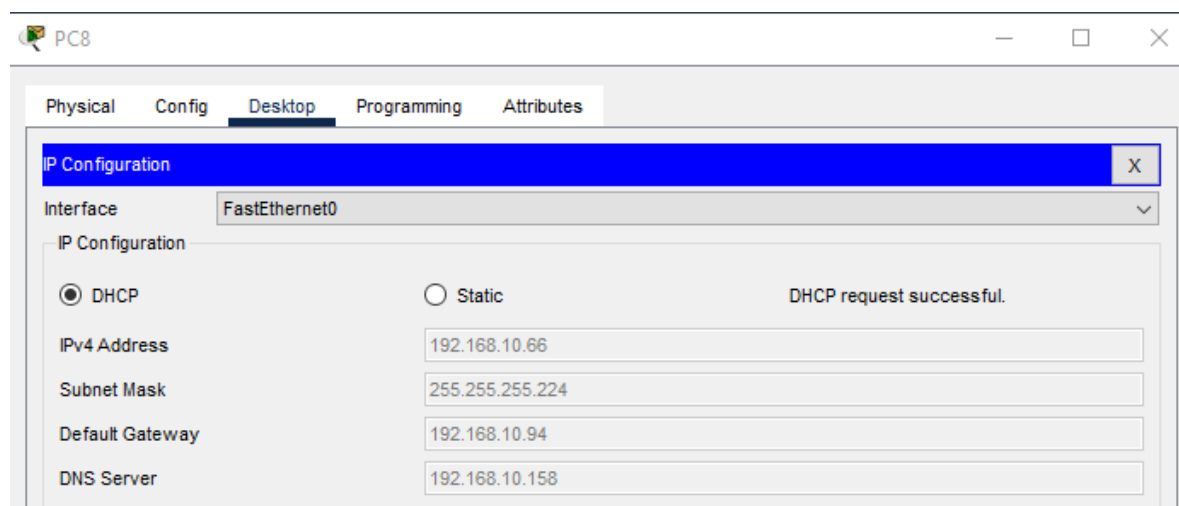
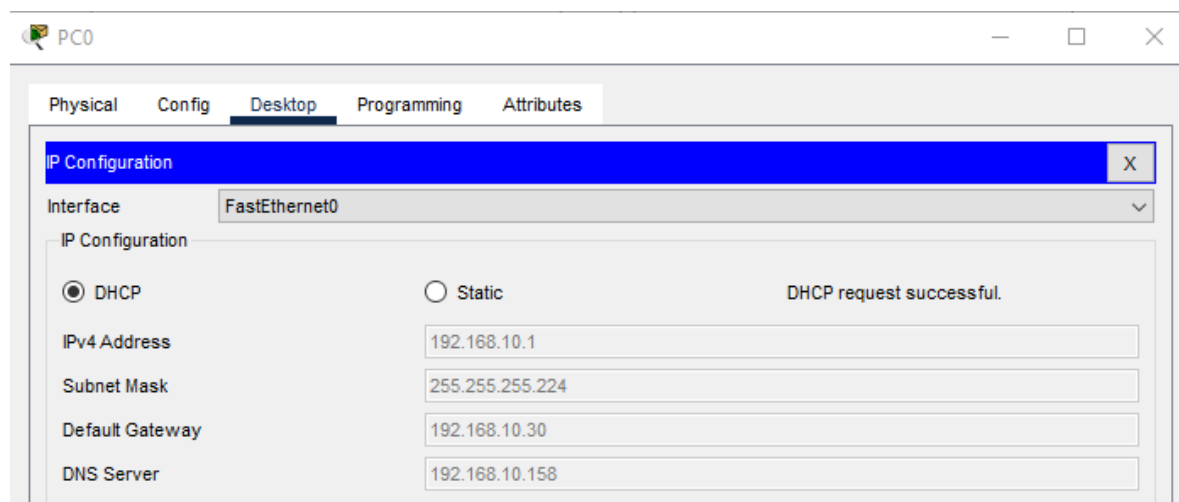
En cada dispositivo ingresé a la configuración de la NIC y establecí los parámetros correspondientes, asegurándome de que la IP, la máscara y el gateway coincidieran exactamente con los valores definidos.

Para un PC de la primera subred configuré:

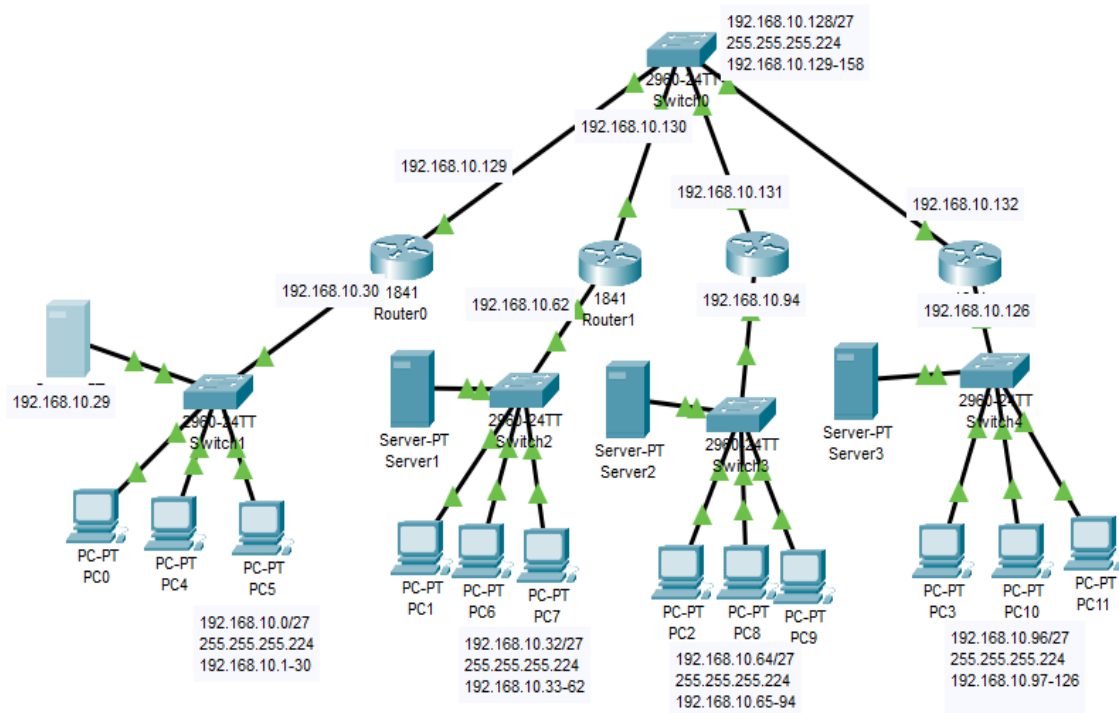
- IP: 192.168.10.1
- Máscara: 255.255.255.224
- Gateway: 192.168.10.30

Además de los hosts, asigné las direcciones IP de las interfaces de cada router. Esto incluyó la configuración de las interfaces que se conectaban al switch central y también de las interfaces que conectaban los routers a las subredes de PCs.

Finalmente configuré también la dirección del servidor DNS-WEB, que en este caso fue 192.168.10.158, asegurando que todas las redes pudieran alcanzarlo.



Estrategia que usa el computo para identificar si está en una red



En la topología configuramos un servidor DHCP, encargado de asignar direcciones IP, máscara, gateway y DNS a las computadoras.

Cuando una computadora estaba configurada en DHCP, realizó el siguiente proceso automáticamente:

1. Envío de un mensaje DHCP: La PC envía un mensaje buscando algún servidor DHCP en la red local.
2. Servidor responde con DHCP: El servidor DHCP propone una dirección IP dentro del rango asignado a su subred, según la tabla de direccionamiento.
3. La PC acepta la oferta.
4. El servidor finaliza la asignación.

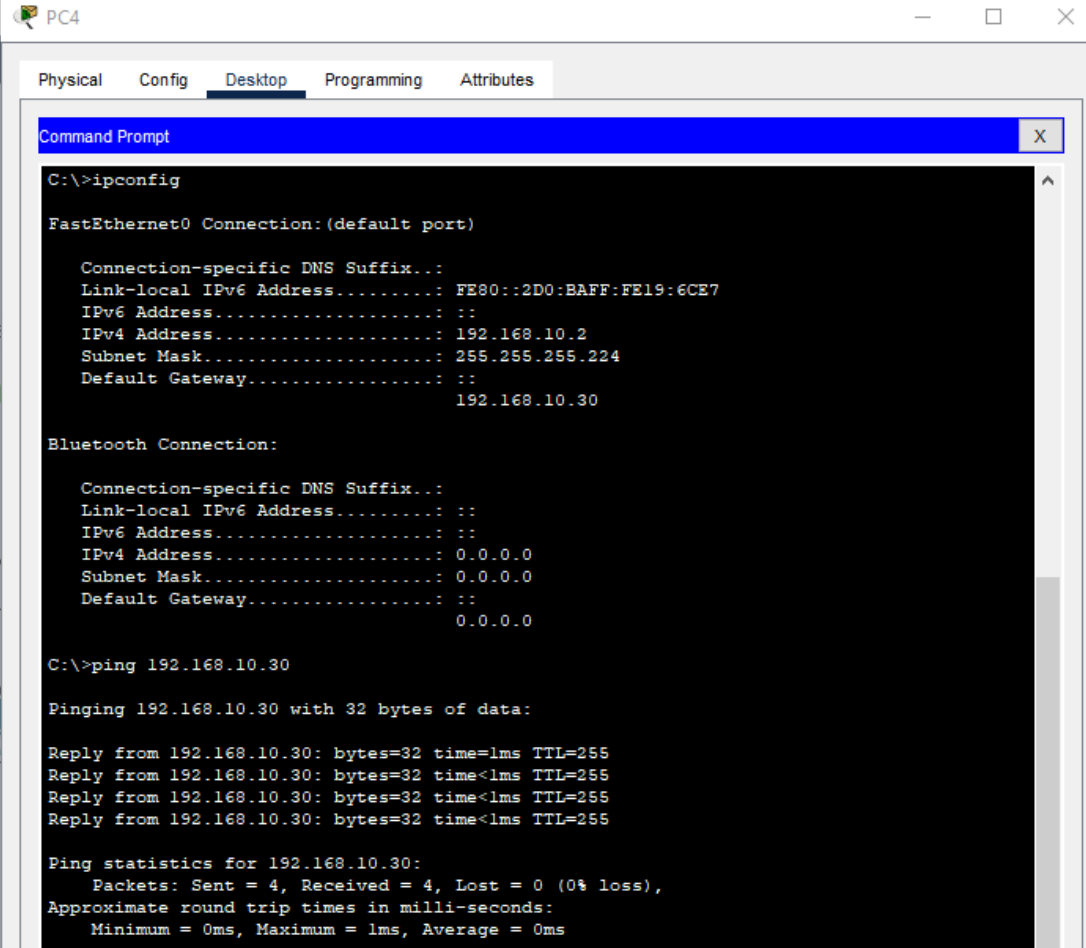
Con esto, cada computadora obtuvo automáticamente:

- Una IP válida dentro de su subred.
- Una máscara correcta.
- Puerta de enlace.

Después de asignar correctamente la IP, verificamos que cada computadora pudiera comunicarse dentro de su red y hacia otras redes.

Las pruebas realizadas:

Ping al Gateway



The screenshot shows a window titled "PC4" with a tabbed interface. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the output of the "ipconfig" command, detailing network settings for "FastEthernet0" and "Bluetooth". It then shows the output of a "ping 192.168.10.30" command, indicating successful connectivity with 0% loss.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:BAFF:FE19:6CE7
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.10.2
    Subnet Mask . . . . .: 255.255.255.224
    Default Gateway . . . . .: ::
                                   192.168.10.30

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

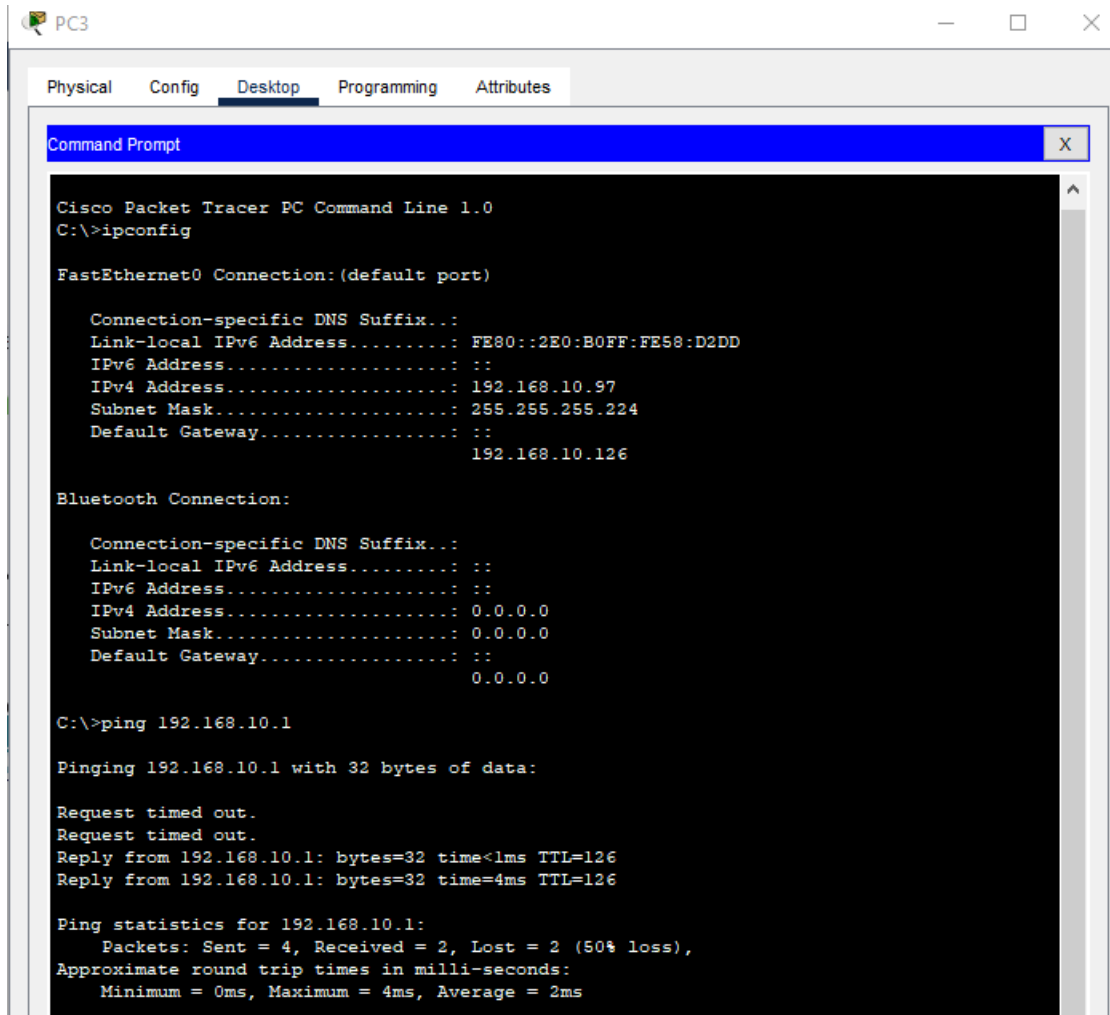
C:\>ping 192.168.10.30

Pinging 192.168.10.30 with 32 bytes of data:

Reply from 192.168.10.30: bytes=32 time=1ms TTL=255
Reply from 192.168.10.30: bytes=32 time<1ms TTL=255
Reply from 192.168.10.30: bytes=32 time<1ms TTL=255
Reply from 192.168.10.30: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping entre dispositivos de diferentes redes



```
PC3
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::2E0:B0FF:FE58:D2DD
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.10.97
    Subnet Mask . . . . .: 255.255.255.224
    Default Gateway . . . . .: ::
                                192.168.10.126

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 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

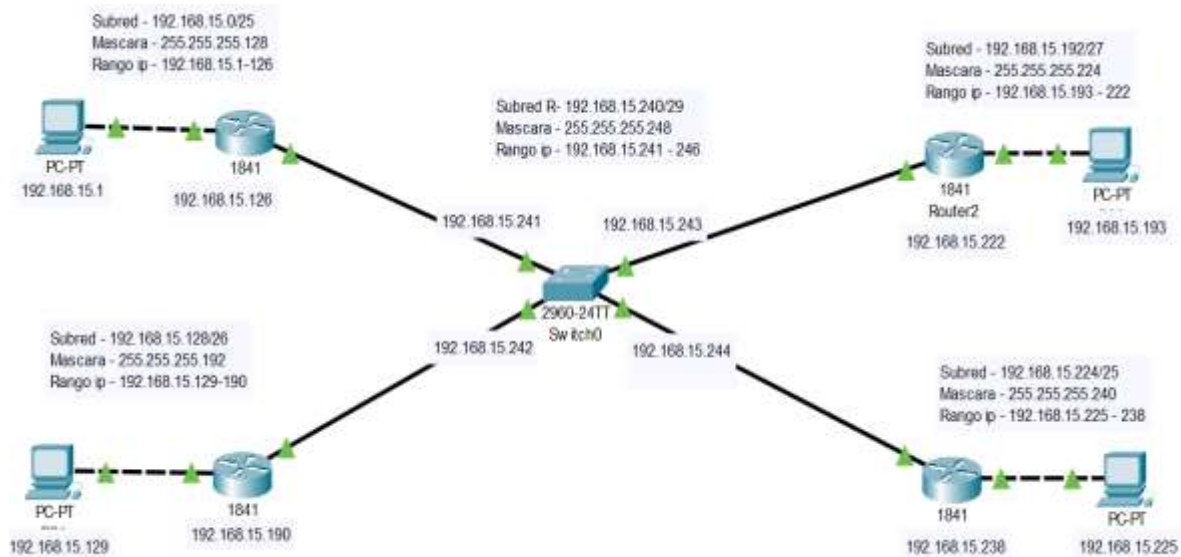
Request timed out.
Request timed out.
Reply from 192.168.10.1: bytes=32 time<1ms TTL=126
Reply from 192.168.10.1: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 2ms
```

Cuando algo estaba mal configurado:

- El DHCP no asignaba IP → la PC no podía identificar su red.
- El ping al gateway fallaba → había un problema en la configuración de IP o de máscara.
- El ping a otras redes no respondía → había un error de enrutamiento.

Clasificación de direcciones IP



En la práctica realizada trabajamos con clasificación y organización de direcciones IP mediante VLSM (Variable Length Subnet Mask). El objetivo fue dividir una red principal en 5 subredes, cada una con tamaños diferentes según la cantidad de hosts necesarios, y luego aplicar direccionamiento estático y enrutamiento dinámico para permitir la comunicación entre todas ellas.

Partimos del bloque de red 192.168.15.0, perteneciente a la Clase C según la clasificación tradicional de direcciones IP:

Clase C Rango por defecto: 192.0.0.0 – 223.255.255.255 Máscara por defecto: /24 (255.255.255.0)

Subred 1 – /25

- Red: 192.168.15.0/25
- Máscara: 255.255.255.128
- Rango de hosts: 192.168.15.1 – 192.168.15.126
- Uso: PC de la parte izquierda
- IP usada: 192.168.15.1 (PC), 192.168.15.126 (Router)

Subred 2 – /26

- Red: 192.168.15.128/26
- Máscara: 255.255.255.192
- Rango de hosts: 192.168.15.129 – 192.168.15.190
- Uso: PC inferior izquierda
- IP usada: 192.168.15.129 (PC), 192.168.15.190 (Router)

Subred R (de routers) – /29

- Red: 192.168.15.240/29
- Máscara: 255.255.255.248
- Rango de hosts:
192.168.15.241 –
192.168.15.246
- Uso: Conexión entre routers y switch central
- IPs usadas: 192.168.15.241,
192.168.15.242,
192.168.15.243,
192.168.15.244

Subred 3 – /27

- Red: 192.168.15.192/27
- Máscara: 255.255.255.224

- Rango de hosts:
192.168.15.193 –
192.168.15.222
- Uso: PC en la parte superior derecha
- IP usada: 192.168.15.193 (PC), 192.168.15.222 (Router)

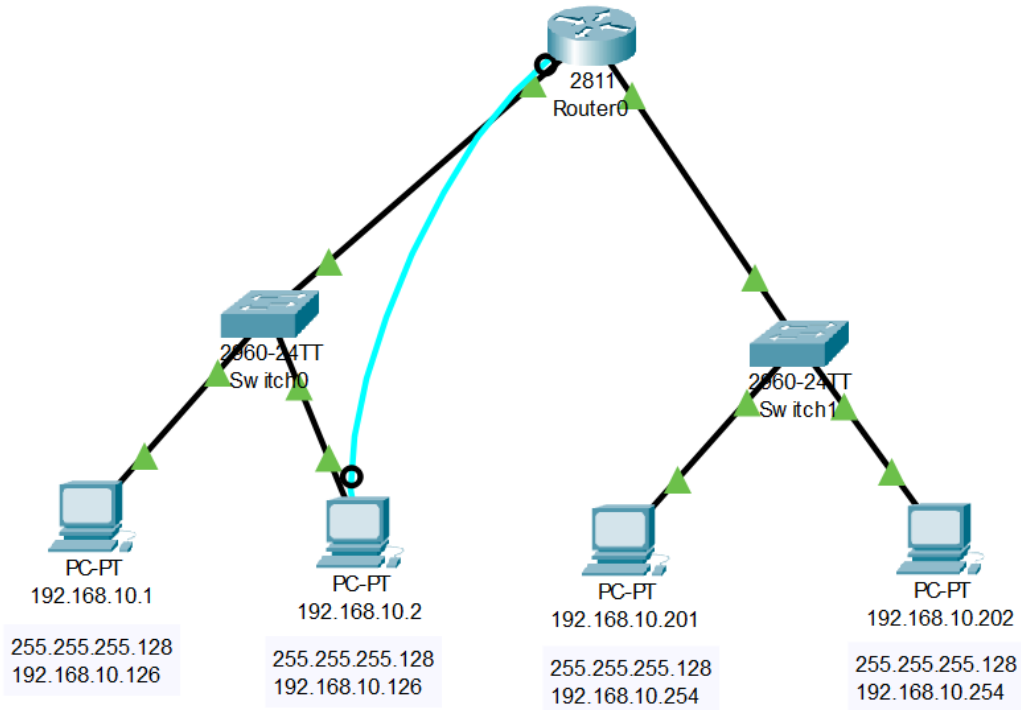
Subred 4 – /25

- Red: 192.168.15.224/25
- Máscara: 255.255.255.240
- Rango de hosts:
192.168.15.225 –
192.168.15.238
- Uso: PC inferior derecha
- IP usada: 192.168.15.225 (PC), 192.168.15.238 (Router)

Cómo usamos esta clasificación en el diseño

1. Dividimos la red principal en subredes con diferentes tamaños usando VLSM.
2. Asignamos direcciones IP a PCs, interfaces de routers y enlaces troncales según la subred correspondiente.
3. Aplicamos enrutamiento estático y dinámico para permitir que todas las subredes se comuniquen:
 - Cada router conocía su propia subred directamente conectada.
 - Las rutas hacia otras subredes se aprendieron mediante RIP.

Subnetting



En la práctica realizada aplicamos el proceso de subnetting para dividir una red mayor en subredes más pequeñas. El objetivo principal es organizar los equipos en diferentes segmentos de red y asignar direcciones IP válidas a cada dispositivo, asegurando que cada subred pudiera comunicarse correctamente a través del router.

Partimos de la red principal:

- 192.168.10.0
- Máscara: 255.255.255.128 (/25)

Con la máscara /25, obtenemos:

Subred 1

- Rango: 192.168.10.0 - 192.168.10.127
- Máscara: 255.255.255.128
- Gateway: 192.168.10.126

Subred 2

- Rango: 192.168.10.128 – 192.168.10.255
- Máscara: 255.255.255.128
- Gateway: 192.168.10.254

Asignación de direcciones IP a los dispositivos:

Subred 1 (192.168.10.0/25)

Se conectaron PC a través del Switch0:

- PC1 → 192.168.10.1
- PC2 → 192.168.10.2
- Máscara: 255.255.255.128
- Gateway: 192.168.10.126

Subred 2 (192.168.10.128/25)

Conectada al Switch1:

- PC3 → 192.168.10.201
- PC4 → 192.168.10.202
- Máscara: 255.255.255.128
- Gateway: 192.168.10.254

El router 2811 actúa como el dispositivo que permite la comunicación entre las subredes.

Cada interfaz del router se configuró con la dirección gateway correspondiente:

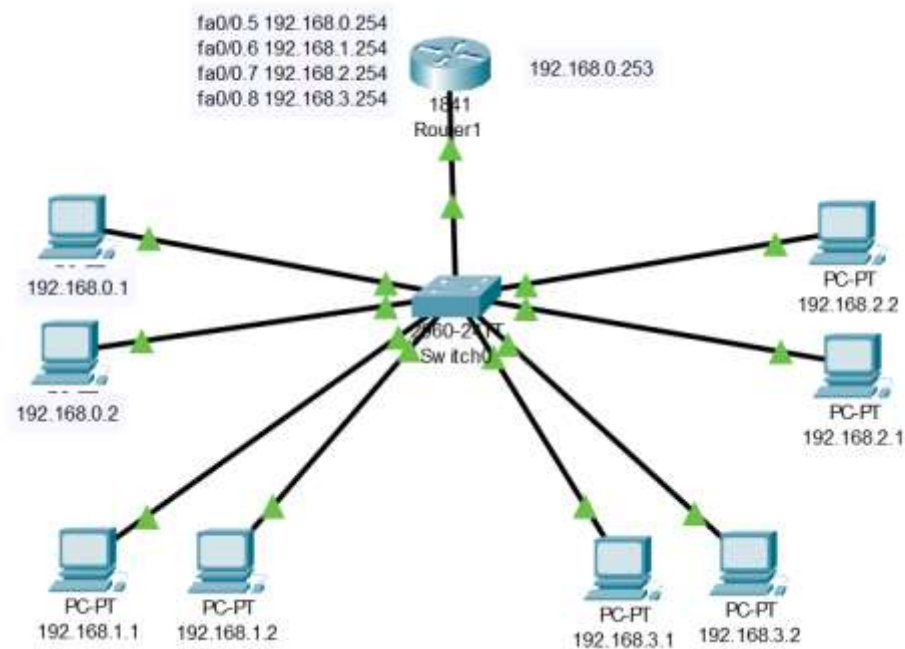
- 192.168.10.126 para la subred 1
- 192.168.10.254 para la subred 2

De esta forma, todas las PCs de ambas subredes pueden enviar paquetes hacia el router para comunicarse entre sí. 5. Verificación de conectividad

Después de configurar las IP y los gateways:

- Se realizaron pings entre PCs de la misma subred → respuesta exitosa.
- Se realizaron pings entre PCs de subredes distintas → comunicación correcta gracias al router.

Simulación de red LAN



En esta actividad utilizamos Cisco Packet Tracer para simular una Red de Área Local (LAN) y comprender cómo se comunican múltiples dispositivos dentro de una misma red física a través de un switch y un router.

Creamos una red compuesta por:

- Un switch 2960 al centro de la topología. Varias
- PCs conectadas directamente al switch.
- Un router 1841 conectado al switch para permitir la comunicación entre las distintas subredes

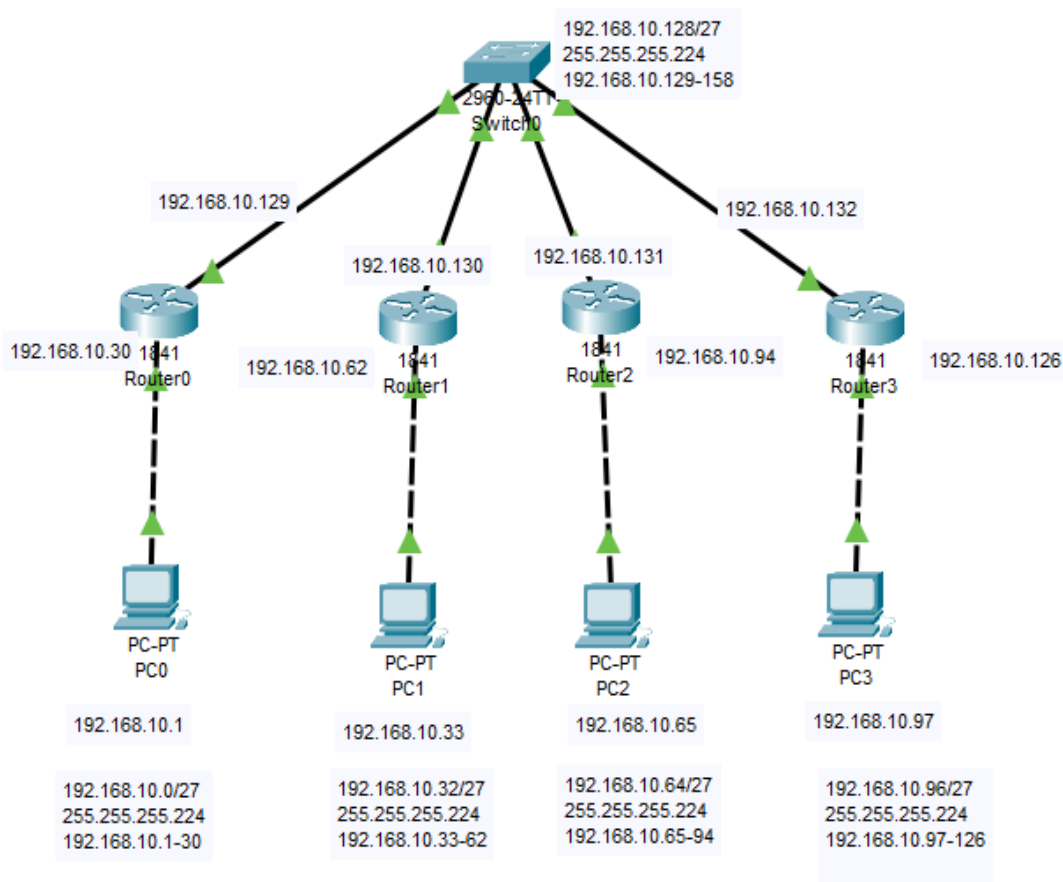
Cada dispositivo fue conectado mediante cables correctos:

- Cobre directo para PC ↔ Switch
- Cobre directo o cruzado para Switch ↔ Router

Cada PC recibió:

- Su dirección IP
- Su máscara
- Su Gateway

Enrutamiento estático



Durante la práctica de enrutamiento estático en Cisco Packet Tracer, configuré una red formada por cuatro routers conectados a un switch central, y cada router daba servicio a una subred diferente. Para comenzar, asigné las direcciones IP correspondientes tanto a los routers como a las PC. Cada subred tenía un segmento distinto:

- Router0 – Red 192.168.10.0/27 PC conectada: 192.168.10.1
- Router1 – Red 192.168.10.32/27 PC conectada: 192.168.10.33
- Router2 – Red 192.168.10.64/27 PC conectada: 192.168.10.65
- Router3 – Red 192.168.10.96/27 PC conectada: 192.168.10.97

Además, el switch central usaba la red 192.168.10.128/27, donde cada router tenía una interfaz con su propia IP:

- Router0 → 192.168.10.129
- Router1 → 192.168.10.130
- Router2 → 192.168.10.131
- Router3 → 192.168.10.132

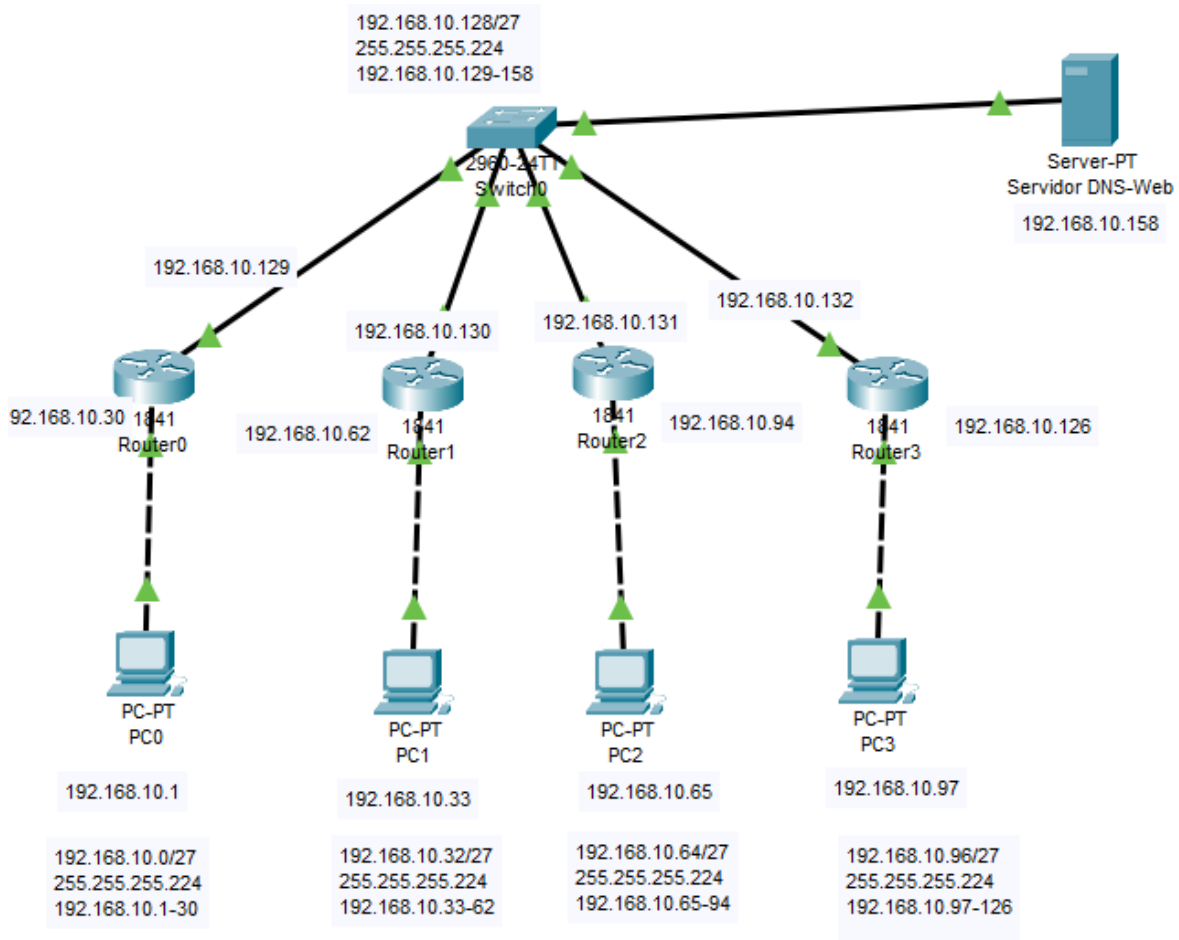
Una vez configuradas todas las IP, procedí a crear las rutas estáticas. El propósito de estas rutas era permitir que cada router supiera hacia dónde enviar los paquetes destinados a redes diferentes a la propia. Para esto, en cada router agregué rutas que apuntaban a las demás subredes, usando como siguiente salto la dirección IP del router correspondiente dentro de la red del switch.

En el Router0 configuré rutas estáticas para llegar a las redes:

- 192.168.10.32/27 → vía 192.168.10.130
- 192.168.10.64/27 → vía 192.168.10.131
- 192.168.10.96/27 → vía 192.168.10.132

Realicé un proceso similar en cada uno de los routers, agregando todas las rutas necesarias para que las cuatro subredes pudieran comunicarse entre sí. Esto me permitió observar cómo funciona el enrutamiento estático: cada router necesita que uno mismo le indique de forma manual a qué dirección enviar los paquetes para llegar a redes remotas.

Enrutamiento dinámico



En esta práctica configuramos una red compuesta por varias subredes, cada una conectada a un router diferente, y todas unidas a un switch central.

Primero, utilizamos una red principal del segmento 192.168.10.0/24, la cual fue subdividida mediante subneteo con máscara /27 (255.255.255.224).

Esto generó varias subredes más pequeñas, cada una asignada a un router distinto:

- Router0 → 192.168.10.0/27
- Router1 → 192.168.10.32/27
- Router2 → 192.168.10.64/27
- Router3 → 192.168.10.96/27

Cada router se conectó al 2960-24TT Switch0, usando una IP de enlace distinta:

- Router0: 192.168.10.129
- Router1: 192.168.10.130
- Router2: 192.168.10.131
- Router3: 192.168.10.132

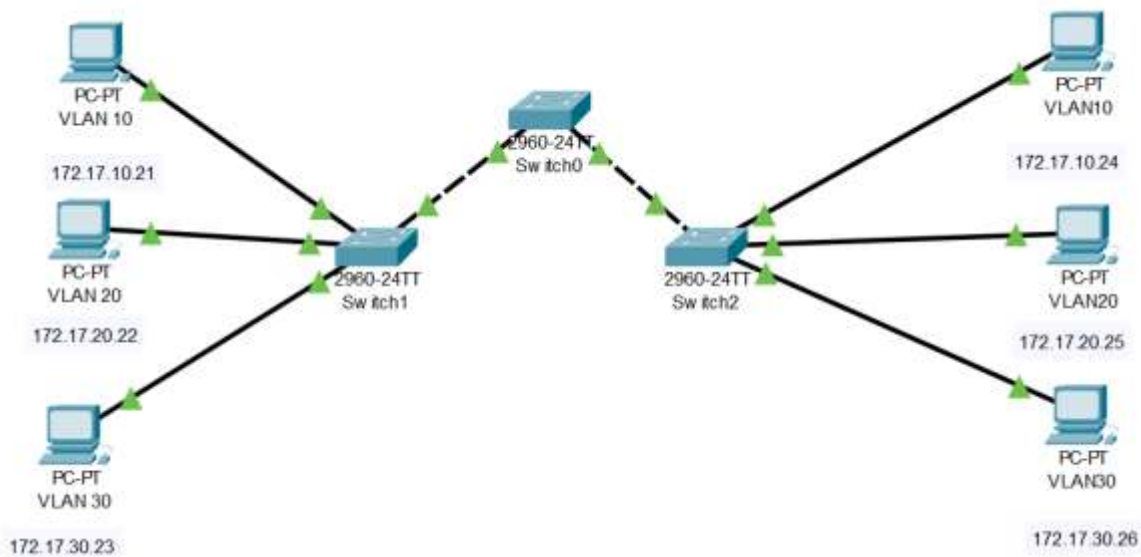
El servidor DNS–Web fue conectado al switch principal con la IP: 192.168.10.158 Dentro de la misma red /27 de interconexión. El servidor fue configurado para: Resolver nombres de dominio (DNS) Servir páginas Web a las PCs de todas las subredes

En cada router activamos un protocolo de enrutamiento dinámico RIP, Lo que hicimos fue:

1. Habilitar RIP
2. Ingresar las redes a las que pertenece cada router
3. En cada router anunciamos su subred local y la red de interconexión
4. Permitimos que los routers intercambien rutas automáticamente

Finalmente, verificamos que todas las PCs podían comunicarse con otras subredes gracias al enrutamiento dinámico, verificar si podían acceder al servidor DNS y Web.

VLANs



En esta práctica realicé la configuración de VLANs con el objetivo de segmentar la red en diferentes áreas lógicas, aun cuando todos los equipos estaban conectados a switches físicamente. Para ello, utilicé tres switches, en los cuales se crearon distintas VLAN para organizar el tráfico de la red de forma segura y eficiente.

Primero, configuré las siguientes VLANs:

- VLAN 10 – Faculty/Staff
- VLAN 20 – Students
- VLAN 30 – Guest
- VLAN 99 – Management y Nativa

Después, asigné manualmente los puertos de los switches a cada VLAN:

- Los puertos Fa0/1 a Fa0/5 fueron asignados a la VLAN 99 para la administración.
- Los puertos Fa0/6 a Fa0/10 fueron asignados a la VLAN 30 (Guest).
- Los puertos Fa0/11 a Fa0/17 fueron asignados a la VLAN 10 (Faculty/Staff).
- Los puertos Fa0/18 a Fa0/24 fueron asignados a la VLAN 20 (Students).

Posteriormente, configuré las direcciones IP de cada equipo con base en la tabla de direccionamiento, asignando una red diferente para cada VLAN:

- Los equipos de la VLAN 10 recibieron direcciones como 172.17.10.21 y 172.17.10.24, con máscara 255.255.255.0 y puerta de enlace 172.17.10.1.
- Los equipos de la VLAN 20 recibieron direcciones como 172.17.20.22 y 172.17.20.25, con gateway 172.17.20.1.
- Los equipos de la VLAN 30 recibieron direcciones como 172.17.30.23 y 172.17.30.26, con gateway 172.17.30.1.

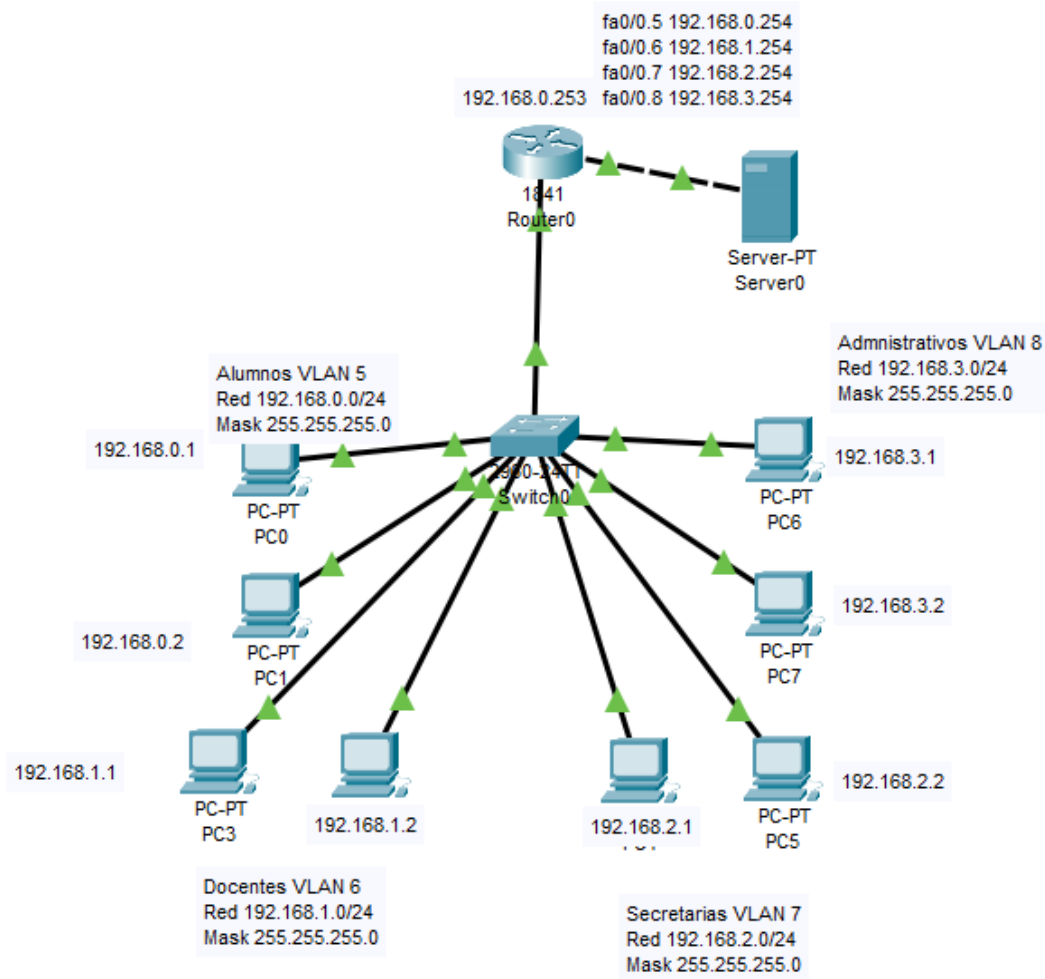
También configuré las direcciones IP de administración en los switches, todas dentro de la VLAN 99, utilizando:

- 172.17.99.11 para S1
- 172.17.99.12 para S2
- 172.17.99.13 para S3

Finalmente, verifiqué el correcto funcionamiento de las VLAN comprobando que los equipos solo se comunicaran correctamente con los dispositivos de su misma VLAN.

Puertos	VLAN	Descripción	Red
Fa0/1 – Fa0/5	VLAN 99	Management / Nativa	172.17.99.0/24
Fa0/6 – Fa0/10	VLAN 30	Guest (Invitados)	172.17.30.0/24
Fa0/11 – Fa0/17	VLAN 10	Faculty / Staff	172.17.10.0/24
Fa0/18 – Fa0/24	VLAN 20	Students (Estudiantes)	172.17.20.0/24

Configuración de switches con puerto troncal



En esta práctica realicé la configuración de un switch con puerto troncal para permitir la comunicación entre varias VLANs mediante un solo enlace hacia el router. El objetivo fue interconectar diferentes áreas de la red, separadas lógicamente por VLANs, pero manteniendo la comunicación entre ellas.

Primero, creé las VLANs en el switch, asignando:

- VLAN 5 para Alumnos (Red 192.168.0.0/24),
- VLAN 6 para Docentes (Red 192.168.1.0/24),
- VLAN 7 para Secretarías (Red 192.168.2.0/24),
- VLAN 8 para Administrativos (Red 192.168.3.0/24).

Después, configuré cada puerto del switch en modo access, asignándolo a su VLAN correspondiente, de acuerdo con el equipo conectado. A cada computadora se le asignó una dirección IP dentro de su red, junto con su respectiva máscara de subred y puerta de enlace.

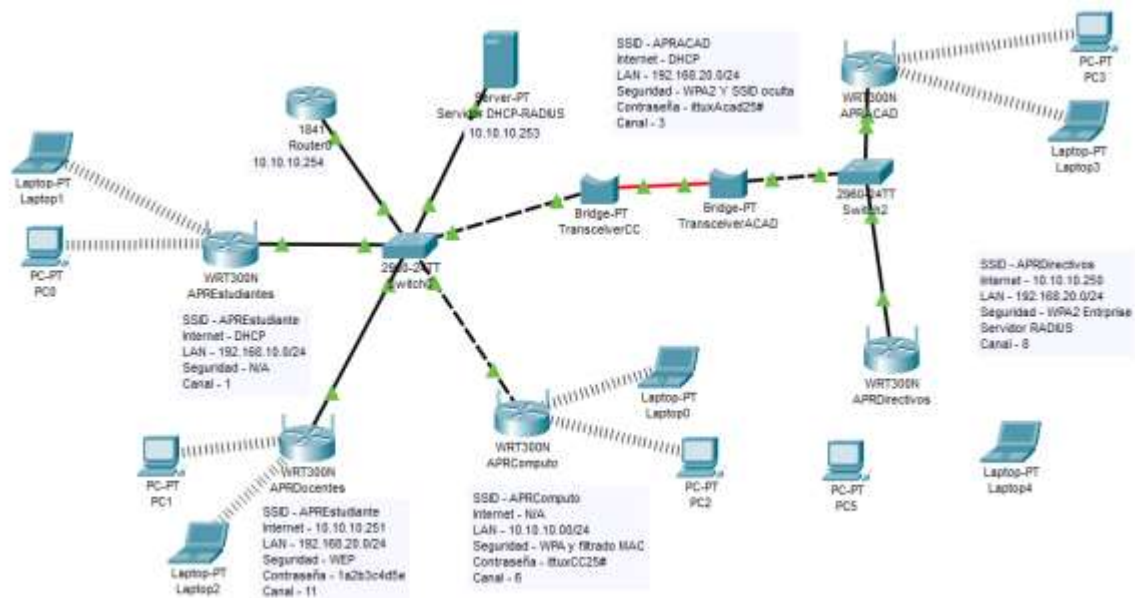
Posteriormente, configuré el puerto del switch que se conecta al router en modo trunk, permitiendo así el paso del tráfico de todas las VLANs por un solo enlace físico.

En el router, realicé la creación de subinterfaces, una por cada VLAN, asignando direcciones IP que funcionaron como puerta de enlace para cada red:

- 192.168.0.254 para VLAN 5,
- 192.168.1.254 para VLAN 6,
- 192.168.2.254 para VLAN 7,
- 192.168.3.254 para VLAN 8.

Finalmente, verifiqué la conectividad realizando pruebas de comunicación entre equipos de distintas VLANs, comprobando que el tráfico pasara correctamente por el enlace troncal y que el enrutamiento entre VLANs funcionara de manera correcta.

Redes inalámbricas



Configuré el router principal que proporcionaba la conexión a internet y asignaba direcciones IP mediante DHCP. Este router se conectó a un switch central, desde el cual se distribuyó la red hacia los demás dispositivos.

Posteriormente, configuré varios routers inalámbricos WRT300N, cada uno con un nombre de red (SSID) diferente:

- APREstudiantes, con seguridad abierta y asignación de IP por DHCP.
- APRDocentes, con seguridad WEP y una contraseña establecida.
- APRComputo, con seguridad WPA y filtrado por dirección MAC.
- APRACAD, con seguridad WPA2, ocultamiento de SSID y contraseña.
- APRDirectivos, con seguridad WPA2 Enterprise, autenticada mediante el servidor RADIUS.

A cada punto de acceso inalámbrico se le asignó una dirección de red diferente, así como un canal específico, con el fin de evitar interferencias entre las señales. Además, se configuraron varios dispositivos como laptops y computadoras, los cuales se conectaron de manera inalámbrica a su respectiva red verificando que recibieran correctamente su dirección IP y acceso a la red.

CONCLUSIÓN

La materia de Interconectividad de Redes me permitió adquirir conocimientos esenciales sobre el funcionamiento y la estructura de las redes de computadoras, así como desarrollar habilidades prácticas importantes para mi formación académica y profesional. Cada uno de los temas abordados contribuyó a que comprendiera mejor cómo se comunican los dispositivos, cómo se organizan las redes y cómo se pueden administrar de manera eficiente. El estudio de los parámetros de configuración de red, la identificación de dispositivos dentro de una red, la clasificación de direcciones IP, el subnetting, el enrutamiento estático y dinámico, las VLANs, la configuración de switches con puertos trunk y las redes inalámbricas fortaleció mis conocimientos técnicos y me permitió entender procesos que antes solo conocía de forma teórica. Además, el uso de Cisco Packet Tracer fue una herramienta fundamental, ya que me ayudó a simular escenarios reales, comprobar configuraciones y resolver problemas de red de manera práctica.

