S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO de Tuxtepec

Interconectividad de Redes

Trabajo**:**
Practicas

PRESENTA:

BRAVO MORALES RENE: 22350630

CARRERA:
INGENIERIA INFORMÁTICA

DOCENTE:
JULIO AGUILAR CARMONA

06/12/2025

INGENIERÍA INFORMÁTICA

INTRODUCCIÓN

El presente documento reúne el desarrollo y análisis de diversas prácticas realizadas en el simulador Cisco Packet Tracer como parte de la asignatura Interconectividad de Redes. A lo largo de este proyecto se implementaron configuraciones esenciales para el diseño, operación y administración de redes de datos, incorporando conceptos como direccionamiento estático y dinámico, enrutamiento estático y dinámico, creación de VLAN, configuración de enlaces troncales, integración de servidores DNS, DHCP y Web, así como el despliegue de redes inalámbricas con múltiples puntos de acceso y autenticación mediante RADIUS.

Cada práctica se elaboró con el objetivo de comprender el funcionamiento real de un entorno de red, aplicando configuraciones paso a paso para garantizar una comunicación eficiente, segura y escalable entre dispositivos. Este proyecto no solo permite reforzar los conocimientos teóricos adquiridos, sino que también proporciona experiencia práctica en la construcción y administración de redes, simulando escenarios que se presentan comúnmente en entornos profesionales.

MARCO TEÓRICO

1. Parámetros de configuración de red

Los parámetros de configuración de red son los elementos fundamentales que permiten que un dispositivo pueda comunicarse dentro de una red local o hacia una red externa como Internet. Entre los parámetros más importantes se encuentran la **dirección IP**, que identifica de manera lógica a cada dispositivo; la **máscara de subred**, que indica la porción de red y la porción de host dentro de la dirección; la **puerta de enlace predeterminada (gateway)**, que permite la salida de los paquetes hacia otras redes; y los **servidores DNS**, responsables de traducir nombres de dominio a direcciones IP.
Otros parámetros importantes incluyen el **DHCP**, que puede asignar estos valores automáticamente, y el **MTU**, que define el tamaño máximo de los paquetes. La correcta configuración de estos parámetros garantiza la interoperabilidad entre dispositivos y el funcionamiento adecuado de los servicios de red..

1.1 Dirección IP

Identificador lógico único en una red. En IPv4 se expresa en notación decimal punteada (ej. 192.168.1.10). Determina la dirección de origen o destino de paquetes a nivel de red.

1.2 Máscara de subred

Define qué parte de la dirección IP corresponde a la red y cuál a los hosts. Por ejemplo, 255.255.255.0 (/24) indica que los primeros 24 bits son de red. La máscara es esencial para determinar si un IP destino está en la misma red.

1.3 Puerta de enlace predeterminada (gateway)

Dirección IP del router local que recibe el tráfico con destino fuera de la red local. Si un host detecta que el destino no está en su subred, envía los paquetes al gateway.

1.4 Servidores DNS

Transforman nombres de dominio (ej. ejemplo.com) en direcciones IP. Los parámetros DNS en la configuración permiten que las aplicaciones resuelvan nombres sin conocer la IP.

1.5 DHCP (Dynamic Host Configuration Protocol)

Servicio que asigna dinámicamente parámetros de red (IP, máscara, gateway, DNS). Evita configurar manualmente cada dispositivo y simplifica la administración.

1.6 MTU (Maximum Transmission Unit)

Tamaño máximo de la carga útil de un paquete que puede transmitirse sin fragmentación. Una MTU incorrecta puede causar fragmentación y afectar rendimiento.

1.7 VLAN ID / Etiquetado

En entornos con VLANs, la configuración puede incluir el ID de VLAN y parámetros de trunking (802.1Q). Importante para segmentación lógica.

1.8 QoS (Quality of Service)

Parámetros para priorizar tráfico (por ejemplo, voz sobre IP frente a transferencias de archivos). Se configuran flags, colas y políticas en routers/switches.

2. Estrategia que utiliza el equipo de cómputo si un equipo está en la misma red o no

Un equipo de cómputo determina si otro dispositivo está en la misma red comparando su **dirección IP** con la **máscara de subred**. El proceso consiste en

aplicar una operación lógica AND entre la IP propia y la máscara, y luego repetirla con la IP destino.
Si el resultado es el mismo, significa que ambos dispositivos pertenecen a la misma red; por lo tanto, pueden comunicarse directamente mediante conmutación.
Si el resultado es diferente, el equipo reconoce que el destino está fuera de su red local y envía el tráfico al **gateway predeterminado**, que se encarga de dirigir los paquetes a otras redes.
Esta estrategia es fundamental para el funcionamiento del enrutamiento y la segmentación de redes.

2.1 Cálculo lógico (AND)

- El host realiza una operación AND entre su IP y su máscara: IP_origen AND MÁSCARA → RED_origen.
- Repite con la IP destino: IP_destino AND MÁSCARA → RED_destino.
- Si RED_origen == RED_destino entonces están en la misma subred y se intenta comunicación directa (capa 2). Si no, el paquete se envía a la puerta de enlace.

Ejemplo:
IP origen 192.168.1.10 /24 → 192.168.1.0
IP destino 192.168.2.5 /24 → 192.168.2.0 → distintas redes → enviar al gateway.

2.2 ARP (Address Resolution Protocol)

Si ambos hosts están en la misma red, el emisor necesita la MAC del destino para enviar el frame Ethernet:

- Envía una petición ARP en broadcast (“¿Quién tiene 192.168.1.20?”)
- El destino responde con su MAC.

- El emisor guarda la entrada en su ARP cache y envía el frame.

2.3 Proxy ARP y Gateway

Si la IP destino no está en la red local, se envía al gateway. En redes con Proxy ARP, un router puede responder ARP en nombre de otra subred, dando la ilusión de que la IP está en la misma red.

2.4 ICMP y pruebas de conectividad

Para verificar si el host remoto responde, se usa ping (ICMP Echo Request/Reply). Si el destino no responde, pueden intervenir firewalls, rutas inexistentes, o filtros.

3. Clasificación de direcciones IP

Las direcciones IP se dividen en dos versiones principales: **IPv4** e **IPv6**.
En IPv4, las direcciones se clasifican en cinco clases principales:

- **Clase A:** redes muy grandes, rango 0.0.0.0 a 127.255.255.255
- **Clase B:** redes medianas, rango 128.0.0.0 a 191.255.255.255
- **Clase C:** redes pequeñas, rango 192.0.0.0 a 223.255.255.255
- **Clase D:** direcciones para multicast
- **Clase E:** experimentales

Además, existen **direcciones privadas** destinadas a redes internas (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) y **direcciones públicas** utilizadas para la comunicación en Internet.
En IPv6, la clasificación cambia, adoptando tipos como **unicast**, **multicast** y **anycast**, ofreciendo un espacio de direcciones mucho más amplio y seguro.

3.1 IPv4 — clases históricas y rangos

Aunque el esquema de clases es obsoleto para diseño moderno, todavía es útil conocerlo:

- **Clase A (0.0.0.0–127.255.255.255):** /8
- **Clase B (128.0.0.0–191.255.255.255):** /16
- **Clase C (192.0.0.0–223.255.255.255):** /24
- **Clase D (224.0.0.0–239.255.255.255):** Multicast
- **Clase E (240.0.0.0–255.255.255.255):** Reservadas/experimentales

3.2 Direcciones privadas y públicas

- **Privadas (no routables en Internet):** 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.
- **Públicas:** Asignadas por RIPE/APNIC/LACNIC y routables en Internet. Para conectar redes privadas a Internet se usa NAT.

3.3 Direcciones especiales

- **Loopback:** 127.0.0.1 (pruebas locales)
- **Broadcast:** Dirección con todos los bits host en 1 (ej. 192.168.1.255 para /24)
- **Network ID:** Dirección con todos los bits host en 0 (ej. 192.168.1.0 /24)
- **APIPA:** 169.254.0.0/16 (cuando DHCP falla)

3.4 IPv6 — tipos y estructura

- **Unicast:** dirección individual de interfaz.
- **Multicast:** para grupos.
- **Anycast:** una dirección asignada a varios nodos; entrega al más cercano. IPv6 tiene prefijos globales, link-local (fe80::/10), ULA (fc00::/7) para direcciones privadas, y elimina la necesidad de NAT en muchos casos.

4. Subnetting (subneteo)

El subnetting es el proceso mediante el cual una red se divide en subredes más pequeñas. Su principal objetivo es optimizar el uso de direcciones IP, mejorar la seguridad y reducir el tráfico dentro de la red.
Para realizar subnetting se toma una red principal y se modifica la máscara de subred extendiéndola hacia los bits del host, creando así múltiples subredes con distintos tamaños.
Existen dos métodos principales:

- **Subnetting tradicional:** todas las subredes tienen el mismo tamaño.
- **VLSM (Subnetting de longitud variable):** permite crear subredes con diferentes tamaños según las necesidades.

El subnetting es esencial para el diseño de redes escalables, eficientes y ordenadas.

4.1 Conceptos básicos

- **Máscara / prefijo:** indica bits de red. Ej: /24 = 255.255.255.0.
- **Hosts por subred:** 2^(bits_host) - 2 (excepto en casos especiales).
- **Network ID y Broadcast:** identificadores importantes.

4.2 Pasos para subnetear (ejemplo práctico)

Si tienes 192.168.0.0/24 y necesitas 4 subredes:

1. Necesitas 2 bits para 4 subredes → nueva máscara /26 (24 + 2 = 26).
2. Subredes: 192.168.0.0/26 (0–63), /26 (64–127), /26 (128–191), /26 (192–255).
3. Hosts por subred: 62 (2^6 - 2).

4.3 VLSM (Variable Length Subnet Mask)

Permite máscaras de distinto tamaño en una misma red para optimizar direcciones (ej. dar /28 a subredes pequeñas y /24 a grandes).

4.4 CIDR (Classless Inter-Domain Routing)

Permite anunciar prefijos sin atarse a clases A/B/C; reduce tablas de enrutamiento mediante agregación de rutas (route summarization).

4.5 Herramientas y buenas prácticas

- Planificar subredes basado en crecimiento proyectado.
- Reservar subredes para futura expansión y para infraestructuras (servidores, gestión, VoIP).
- Documentar rangos y gateways.

5. Simulación de una red LAN

La simulación de redes LAN permite observar el funcionamiento real de una red sin necesidad de implementarla físicamente. Herramientas como Cisco Packet Tracer o GNS3 permiten recrear switches, routers, PCs, servidores y enlaces físicos.

En una simulación se pueden realizar prácticas de direccionamiento IP, configuración de VLAN, enrutamiento, DHCP, DNS y pruebas de conectividad. La simulación es útil para estudiantes y profesionales porque permite experimentar y cometer errores sin afectar una red real, facilitando el aprendizaje de conceptos complejos de interconectividad.

5.1 Topologías comunes

- **Estrella:** dispositivos conectados a un switch central (más común).
- **Bus (legacy):** todos los dispositivos en un mismo segmento (poco usado hoy).
- **Mesh:** interconexión redundante, usada en infraestructuras críticas.
- **Jerárquica:** acceso → distribución → núcleo.

5.2 Componentes básicos en la simulación

- **PCs/Servers:** endpoints.
- **Switches:** conmutación interna.
- **Routers:** inter-VLAN / acceso a otras redes.
- **Cables y medio:** cobre, fibra; en simuladores se representan por tipos (crossover, straight-through).

5.3 Diseño de direccionamiento y VLANs

- Crear plan de direccionamiento (subredes por departamento).
- Segmentar por VLANs para separar broadcast domains y mejorar seguridad.

5.4 Pruebas y métricas

- **Conectividad:** ping, traceroute.
- **Rendimiento:** throughput, latencia.
- **Simulación de fallas:** desconectar enlaces y observar convergencia.

5.5 Ventajas de simular

- Permite validar diseño, practicar comandos, probar configuraciones sin riesgo y documentar procedimientos.

6. Enrutamiento estático

El enrutamiento estático consiste en configurar manualmente las rutas que debe seguir un paquete para llegar a una red destino. El administrador define la dirección IP de la red destino, la máscara y el siguiente salto.
Es un método sencillo y seguro, ideal para redes pequeñas o topologías estables que no cambian con frecuencia. Sin embargo, requiere mantenimiento cuando hay cambios en la red, ya que no se actualiza automáticamente.
Entre sus ventajas destacan su predictibilidad, bajo consumo de recursos y control total sobre el camino de los paquetes.

6.1 Concepto y cuándo usarlo

Enrutamiento donde el administrador define rutas manualmente (ej. ip route 10.0.0.0 255.255.255.0 192.168.1.2). Adecuado para topologías pequeñas o enlaces puntuales.

6.2 Elementos de una ruta estática

- **Red destino** y **máscara**.
- **Next-hop (siguiente salto)** o interfaz de salida.

- **Administrative distance (AD):** valor que determina preferencia de una ruta (estáticas normalmente AD=1 o 0 si apunta a interfaz).

6.3 Ventajas y desventajas

- **Ventajas:** control total, bajo overhead, seguridad.
- **Desventajas:** no escala bien, requiere mantenimiento manual, propenso a errores humanos.

6.4 Ejemplo de configuración (Cisco IOS)

Router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.2

Verificación: show ip route, ping, traceroute.

6.5 Usos típicos

- Rutas hacia redes muy específicas.
- Saldos de última instancia (default route): ip route 0.0.0.0 0.0.0.0 192.168.1.1.

7. Enrutamiento dinámico

El enrutamiento dinámico utiliza protocolos especiales que permiten que los routers aprendan las rutas de forma automática. Estos protocolos intercambian información continuamente para mantener las tablas de enrutamiento actualizadas.
Algunos protocolos populares son:

- **RIP:** sencillo, basado en saltos.
- **OSPF:** basado en costo, jerárquico y eficiente para redes grandes.

- **EIGRP:** híbrido, rápido y muy flexible.

El enrutamiento dinámico permite adaptarse a cambios, fallas o ampliaciones en la red sin necesidad de configuraciones manuales constantes. Aunque consume más recursos que el estático, es indispensable en redes medianas y grandes.

7.1 Fundamento

Protocolos que permiten a los routers intercambiar información de rutas y adaptarse automáticamente a cambios de topología.

7.2 Tipos y características principales

- **RIP (Routing Information Protocol):** distancia por saltos, simple, limitado (max 15 saltos).
- **OSPF (Open Shortest Path First):** link-state, utiliza estados de enlace y algoritmo SPF (Dijkstra). Soporta áreas (reducción de LSDB), ideal para redes medianas/grandes.
- **EIGRP (Enhanced Interior Gateway Routing Protocol):** protocolo híbrido (Cisco), rápido en convergencia, métricas compuestas (retardo, ancho de banda, fiabilidad).

7.3 Conceptos clave

- **Convergencia:** tiempo que tarda la red en estabilizarse después de un cambio.
- **LSDB (Link-State Database):** en OSPF, cada router mantiene la topología.
- **Vecinos (neighbors):** routers que han establecido adyacencia para intercambiar updates.

- **Timers:** hello, dead timers controlan detección de fallos.
- **Summarization:** agregación de rutas para reducir tablas.

7.4 Ventajas y desventajas

- **Ventajas:** adaptación automática, escalabilidad, balanceo de carga (en algunos casos).
- **Desventajas:** mayor uso de recursos, configuración más compleja, posibilidad de bucles si se configuran mal.

7.5 Ejemplo conceptual (OSPF)

- Dividir en áreas (Area 0 como backbone).
- Routers comparten LSAs (Link State Advertisements).
- Cada router calcula SPF y llena su tabla de rutas.

8. VLANs (LAN Virtuales)

Las VLAN son subredes lógicas dentro de un switch que permiten segmentar la red sin necesidad de hardware adicional.
Cada VLAN actúa como una red independiente, aunque los dispositivos estén conectados al mismo switch físico. Sus beneficios principales son la mejora de la seguridad, reducción de dominio de broadcast y organización lógica por departamentos.
Las VLAN necesitan un router o un switch multicapa para permitir la comunicación entre ellas mediante técnicas como **router-on-a-stick**. Los enlaces troncales transportan múltiples VLAN a través de un solo cable utilizando protocolos como **802.1Q**.

8.1 Concepto

Las VLANs permiten segmentar una red física en múltiples dominios de broadcast lógicos.

8.2 Tipos de VLAN

- **Data VLAN:** tráfico de usuarios.
- **Voice VLAN:** tráfico VoIP, con prioridad.
- **Management VLAN:** para acceso administrativo a dispositivos (ej. VLAN 99).
- **Native VLAN:** VLAN por defecto en enlaces troncales (sin etiquetar).

8.3 Trunking y etiquetado

- **802.1Q:** estándar que inserta una etiqueta en el frame Ethernet para identificar la VLAN.
- **Trunk ports:** llevan tráfico de múltiples VLANs entre switches o hacia routers.

8.4 Inter-VLAN routing

- Para que VLANs se comuniquen entre sí se necesita un router o switch multicapa.
- **Router-on-a-stick:** una subinterfaz por VLAN en el router con 802.1Q.
- **Switch multicapa:** en switches de capa 3 se pueden crear SVIs (Switch Virtual Interfaces).

8.5 VTP (VLAN Trunking Protocol) y administración

Protocolo Cisco para propagar configuraciones VLAN entre switches; útil pero se debe usar con cuidado por riesgos de propagación de cambios no deseados.

8.6 Buenas prácticas

- Separar VLAN de gestión y VLAN de usuarios.
- Aplicar ACLs entre VLANs para controlar tráfico.
- Documentar IDs, nombres y rangos.

9. Configuración de switches

Los switches son dispositivos de capa 2 encargados de conmutar tráfico dentro de una red LAN. Su configuración permite administrar VLANs, definir puertos de acceso y troncales, habilitar protocolos de seguridad y gestionar direcciones MAC. Las configuraciones básicas incluyen:

- Asignación de VLANs
- Configuración de enlaces troncales
- Seguridad de puertos (port security)
- Spanning Tree Protocol (STP)
- Configuración de direcciones IP para administración

El correcto manejo de switches garantiza un funcionamiento eficiente y seguro de la red.

9.1 Modos y acceso

- **Modo usuario y modo privilegiado** (en Cisco IOS: enable).
- **Acceso CLI** por consola, SSH o Telnet (SSH preferible por seguridad).

9.2 Configuración básica de VLANs y puertos

- Crear VLAN: vlan 10 → name Usuarios.
- Asignar puerto a VLAN: interface fa0/1 → switchport mode access → switchport access vlan 10.
- Configurar troncal: switchport trunk encapsulation dot1q → switchport mode trunk.

9.3 Spanning Tree Protocol (STP)

Evita bucles Layer 2. Versiones: STP clásico, RSTP (802.1w) más rápido, MSTP. Importante conocer roles (root bridge, root port, designated port) y costes.

9.4 Seguridad en puertos

- **Port security:** limitar MACs por puerto, acción al violar (shutdown, restrict).
- **BPDU guard, root guard:** protecciones contra cambios de STP por dispositivos no autorizados.

9.5 Gestión y monitoreo

- **SNMP:** para recolección de métricas.
- **Syslog:** registro de eventos.
- **Telnet/SSH:** acceso remoto.
- **NetFlow/sFlow:** análisis de tráfico.

9.6 ACLs en switches de capa 3

Permiten filtrar tráfico por IP. En switches de capa 2 se usan VLAN ACLs (VACL) para filtrar tráfico dentro de VLANs.

9.7 Calidad de servicio (QoS) en switches

Clasificar tráfico por prioridad, marcar DSCP/CoS y aplicar colas para tráfico sensible (voz).

10. Redes inalámbricas (WLAN)

Las redes inalámbricas (WLAN) permiten conectar dispositivos sin cables mediante tecnología basada en el estándar **IEEE 802.11**. Utilizan puntos de acceso (AP) para distribuir la señal y pueden trabajar en bandas de frecuencia de 2.4 GHz o 5 GHz.
La seguridad es fundamental y utiliza métodos como:

- WPA2 / WPA3
- Autenticación mediante servidor RADIUS
- Filtrado MAC
- Redes invitadas

Las WLAN permiten movilidad, flexibilidad y bajo costo de instalación, siendo indispensables en entornos modernos. Su planificación requiere considerar cobertura, interferencias, canales disponibles, cantidad de usuarios y capacidad del AP.

10.1 Estándares IEEE 802.11

- **802.11a:** 5 GHz, hasta 54 Mbps.
- **802.11b:** 2.4 GHz, hasta 11 Mbps.
- **802.11g:** 2.4 GHz, hasta 54 Mbps.
- **802.11n:** MIMO, 2.4/5 GHz, mejoras en throughput.
- **802.11ac:** 5 GHz, canales más anchos, MU-MIMO.
- **802.11ax (Wi-Fi 6):** mejora eficiencia, OFDMA, mayor capacidad.

10.2 Componentes de una WLAN

- **Access Points (AP):** puntos de acceso inalámbrico.
- **Controlador WLAN (WLC):** en despliegues empresariales centraliza gestión.
- **Clientes:** laptops, smartphones, IoT.
- **RADIUS server:** autenticación central (802.1X/EAP).

10.3 Seguridad y métodos de autenticación

- **WEP (obsoleto):** inseguro.
- **WPA / WPA2 / WPA3:** mejoras sucesivas; WPA2 (AES) estándar; WPA3 mejora protección contra ataques de fuerza bruta.
- **802.1X + RADIUS (EAP):** autenticación por usuarios/credenciales (EAP-TLS, EAP-PEAP).
- **PSK (pre-shared key):** para redes domésticas o pequeñas.

10.4 Diseño y planificación de cobertura

- **Site survey:** analizar cobertura, interferencia, canales, potencia Tx.
- **Canales y coexistencia:** en 2.4 GHz pocos canales no solapados (1,6,11); en 5 GHz más opciones.
- **Densidad de usuarios:** dimensionar APs por número de clientes concurrentes.
- **Power and channel planning:** evitar co-channel interference, ajustar potencias.

10.5 Roaming y movilidad

- APs colaboran para transferir sesiones; en entornos gestionados se usan controladores y mecanismos de fast roaming (802.11r) para reducir latencia en handoffs.

10.6 MIMO, MU-MIMO y OFDMA

- **MIMO:** múltiples antenas para aumentar throughput.
- **MU-MIMO:** permite comunicarse con múltiples clientes simultáneamente.
- **OFDMA (Wi-Fi 6):** subdivide canales para servir a muchos clientes con eficiencia.

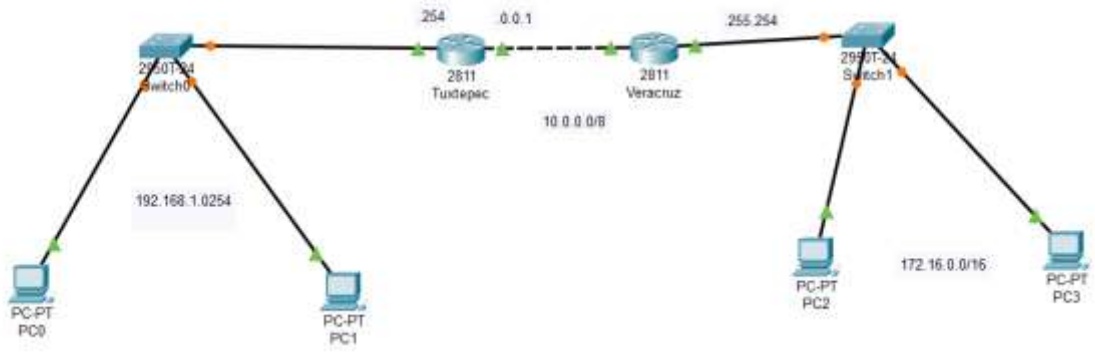
10.7 Integración con la red alámbrica

- **VLANs por SSID:** cada SSID puede mapearse a una VLAN.
- **Seguridad de gestión:** aislar administración en VLAN separada, usar SSH y ACLs.

10.8 Troubleshooting en WLAN

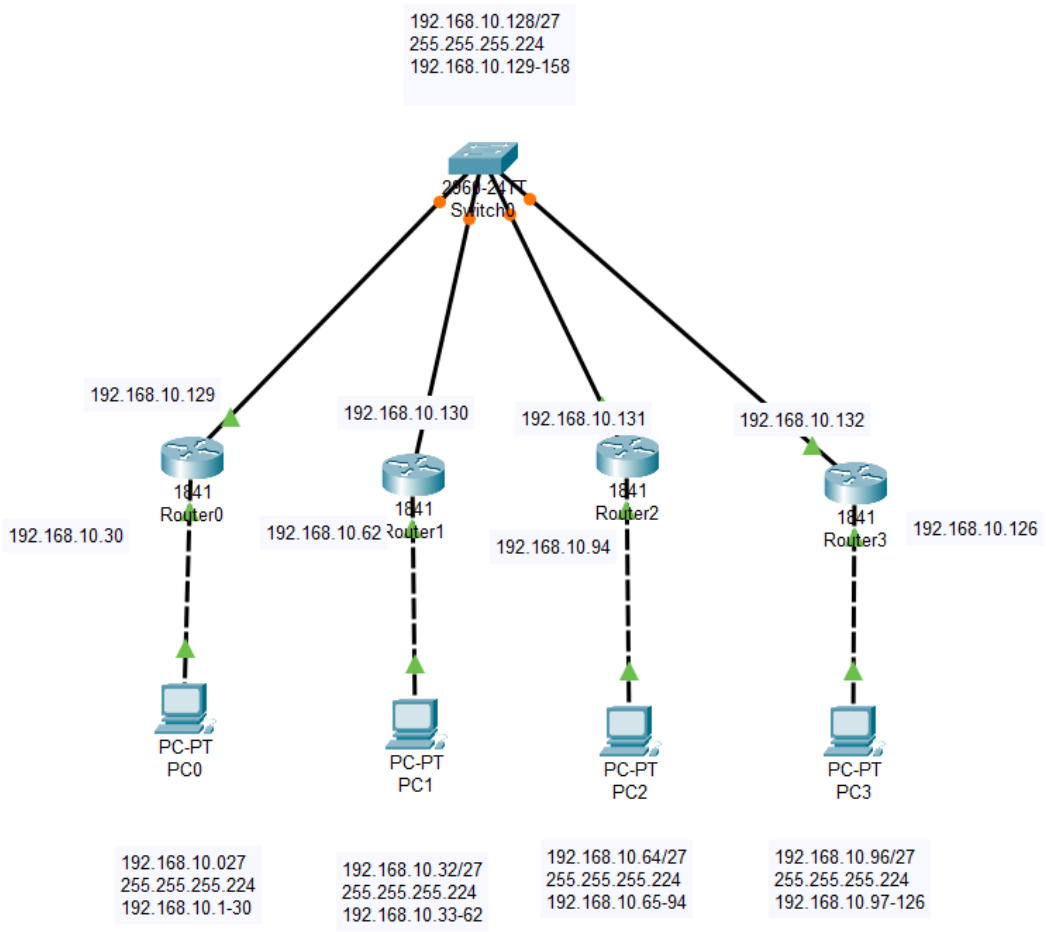
- Herramientas: análisis de espectro, logs de AP, clientes de diagnóstico. Problemas comunes: interferencia, sinal débil, configuración incorrecta de seguridad, saturación de AP.

Ruta estatica



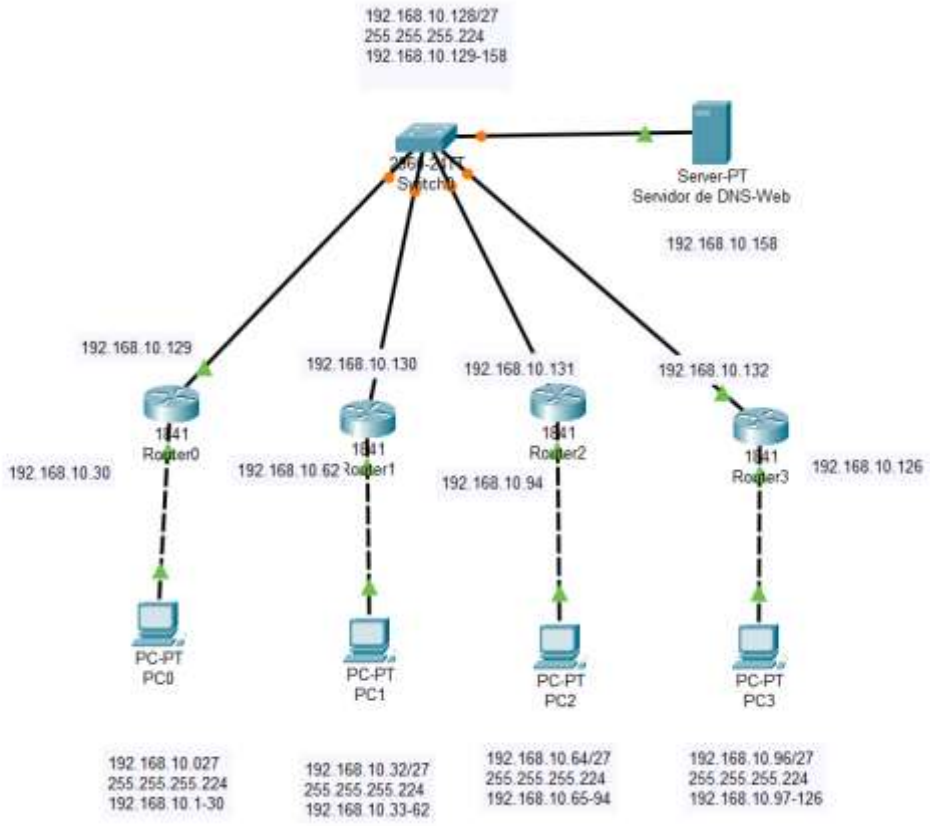
Para esta práctica configuré la comunicación entre varias redes utilizando rutas estáticas. Primero asigné direcciones IP a todas las interfaces de los routers y dispositivos finales. Posteriormente identifiqué las redes de destino y añadí manualmente las rutas estáticas con el comando ip route. Una vez configuradas, verifiqué la tabla de enrutamiento y finalmente comprobé la comunicación con *ping* y *traceroute* entre todos los segmentos de red.

Direccionamiento estatico y enrutamiento



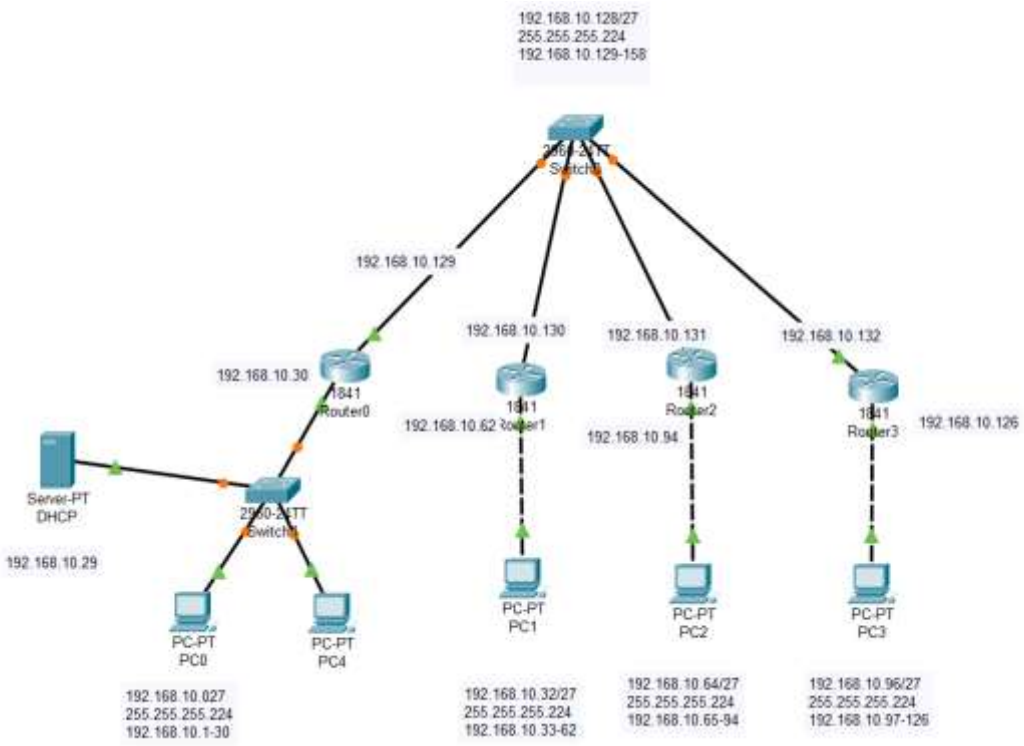
Asigné direcciones IP manualmente a cada equipo: PCs, switches y routers. Me aseguré de que el direccionamiento perteneciera a la red y máscara definidas para evitar conflictos. Después configuré las rutas necesarias dentro del router para permitir el flujo de datos entre las redes. Probé la comunicación capa por capa hasta confirmar que las PCs podían comunicarse entre sí a través del router.

Direccionamiento estatico y enrutamiento dinamico con servidor dns web



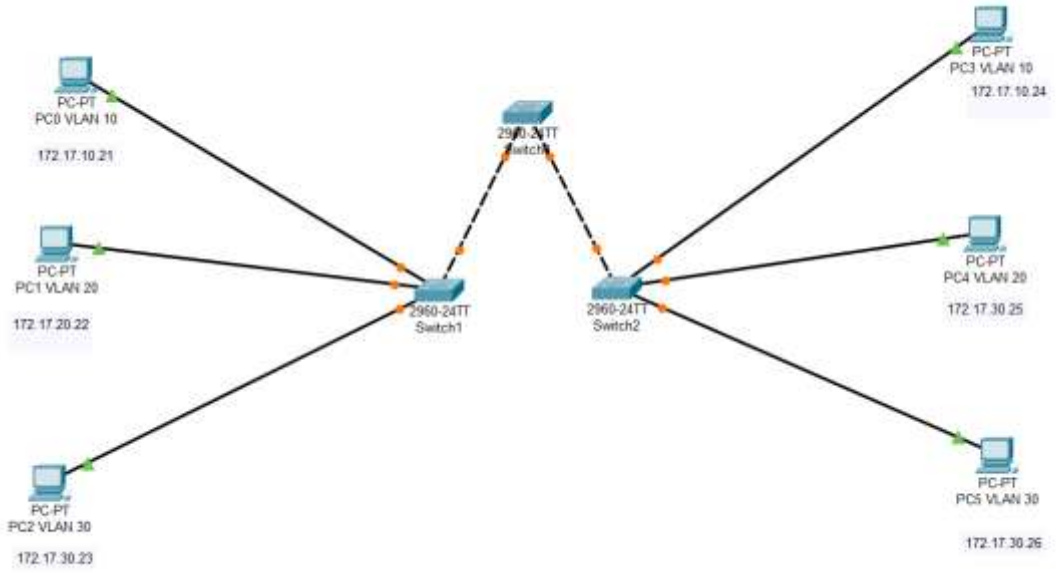
Comencé asignando direcciones IP estáticas a toda la red. Luego habilité un servidor DNS y Web, configurando el dominio en el DNS y cargando una página simple en el servicio Web. Activé en los routers un protocolo de enrutamiento dinámico como OSPF o EIGRP para que intercambiaran rutas automáticamente. Finalmente probé que desde cualquier PC se pudiera acceder al dominio configurado y a la página web.

Red con 5 direccionamiento estático con servidor



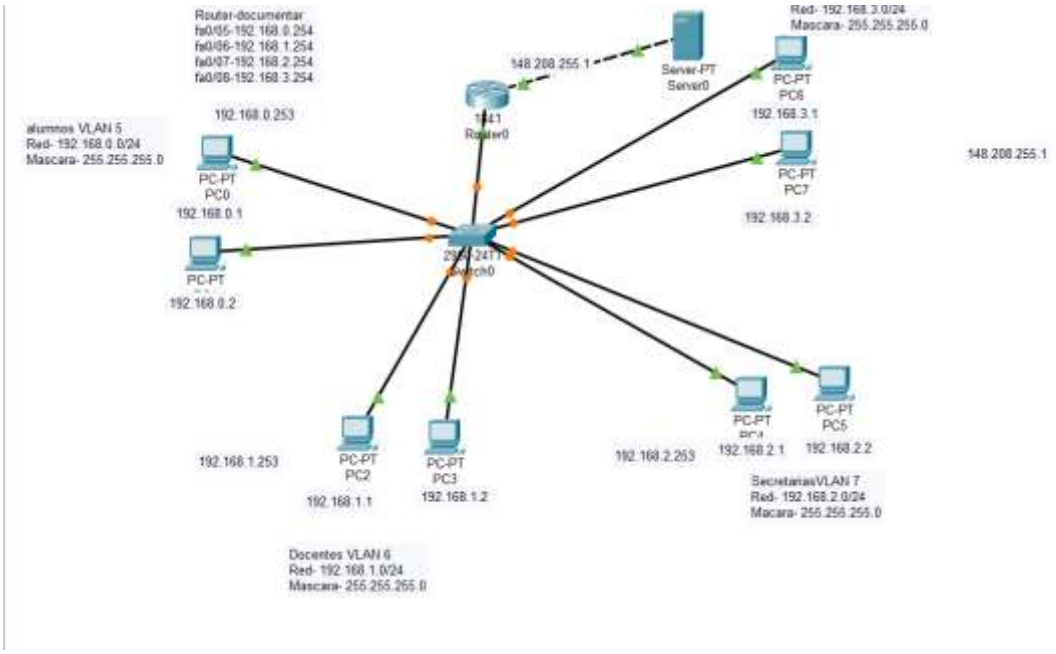
Realicé un cálculo de subnetting para crear 5 subredes con la máscara adecuada. Asigné direcciones IP a cada subred y a las interfaces del router. Configuré rutas estáticas entre todas las redes. Instalé un servidor para servicios básicos como DNS, DHCP o Web según la práctica. Verifiqué conectividad, tabla de enrutamiento y acceso al servidor desde todas las subredes.

Red con 3 VLAN y Enlace troncales



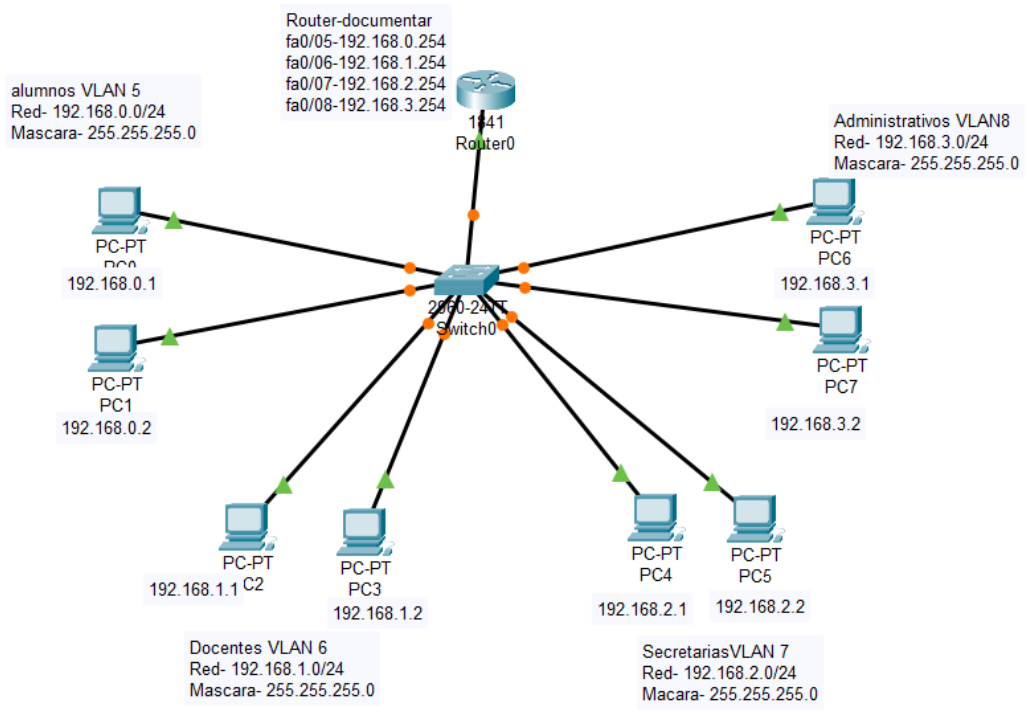
En el switch principal creé las VLAN correspondientes y asigné cada puerto a su VLAN específica. Configuré un enlace troncal usando el protocolo 802.1Q entre los switches para permitir el transporte de varias VLAN en un solo enlace. Finalmente habilité el enrutamiento entre VLAN usando un router-on-a-stick. Realicé pruebas de conectividad entre equipos de diferentes VLAN.

Red con cuatro vlan servidor DNS WEB y DHCP en el router



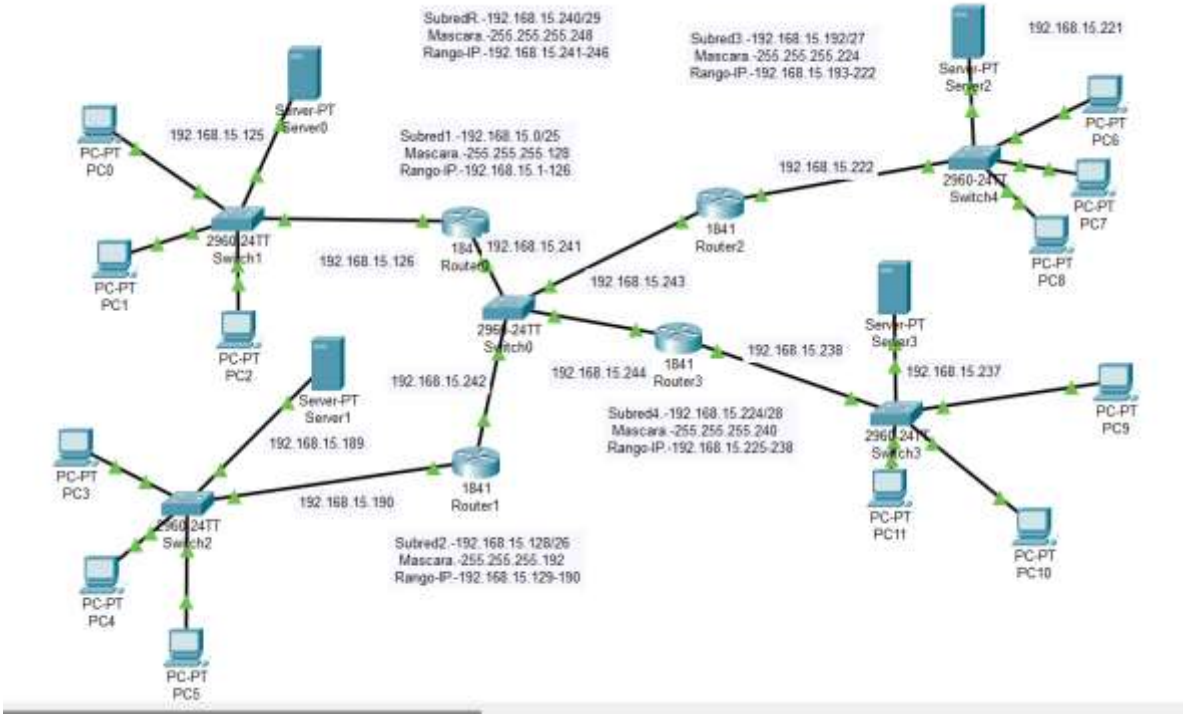
Definí cuatro VLAN en el switch y configuré subinterfaces en el router, asignando una dirección IP como gateway para cada una. Activé en el router los pools DHCP para entregar direcciones automáticamente. Configuré un servidor con servicios DNS y Web y lo conecté a una de las VLAN. Validé que cada VLAN recibiera IP, resolviera nombres y accediera al servidor sin problemas.

Red con 4 Vlan y un Router



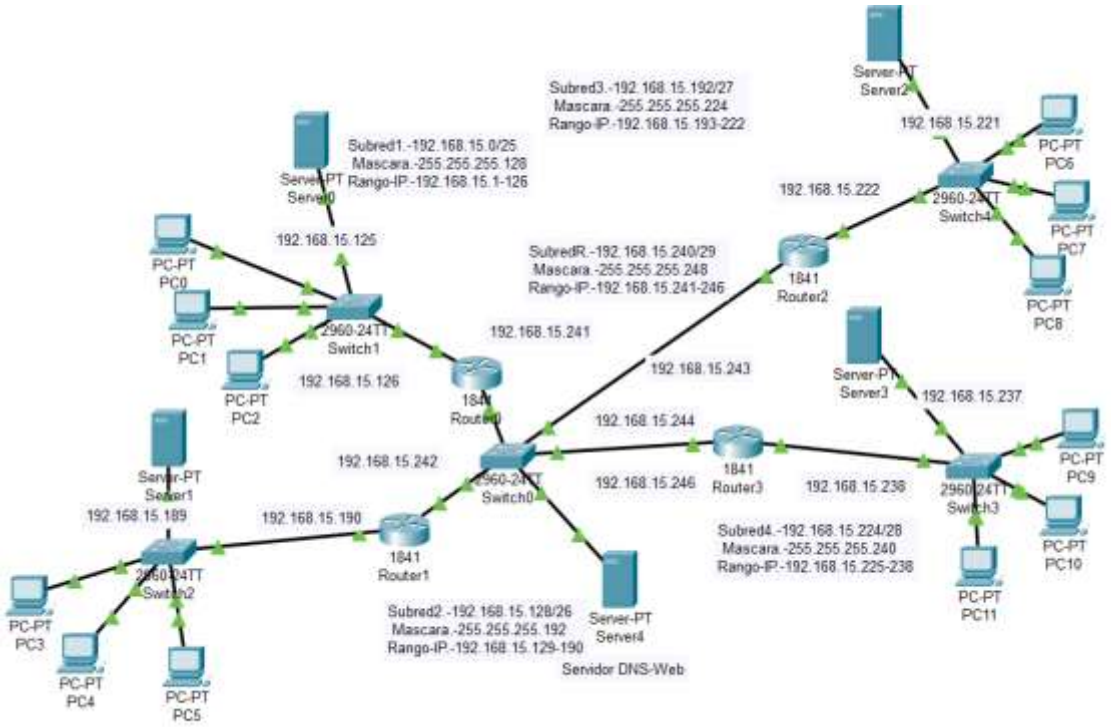
Realicé la creación de las VLAN en el switch y asignación de puertos. En el router configuré subinterfaces para cada VLAN con sus respectivas direcciones IP. Verifiqué que el router pudiera recibir y enviar tráfico etiquetado. La prueba final consistió en enviar pings entre equipos en VLAN distintas para comprobar el enrutamiento inter-VLAN.

Red con 5 subredes Con vlms direccionamiento dinamico y enrutamiento dinamico



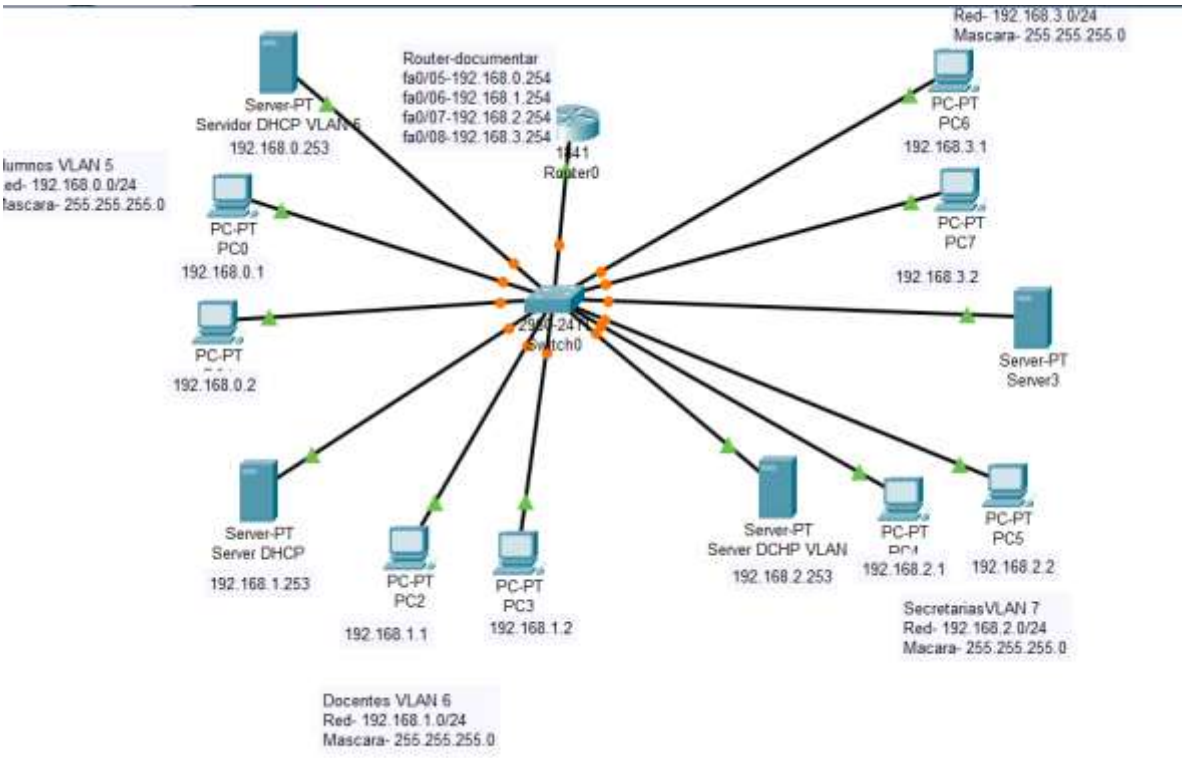
Apliqué VLSM para asignar máscaras de subred según el tamaño de cada red. Configuré los pools DHCP en el router o en un servidor para entregar direcciones de forma automática. Activé un protocolo de enrutamiento dinámico para que el router aprendiera las rutas sin ingresarlas manualmente. Realicé pruebas de conexión y verifiqué que todas las subredes recibieran IPs y se comunicaran correctamente.

Red con 5 subredes con vlms direccionamiento dinamico y enrutamiento dinamico con servidor dns web



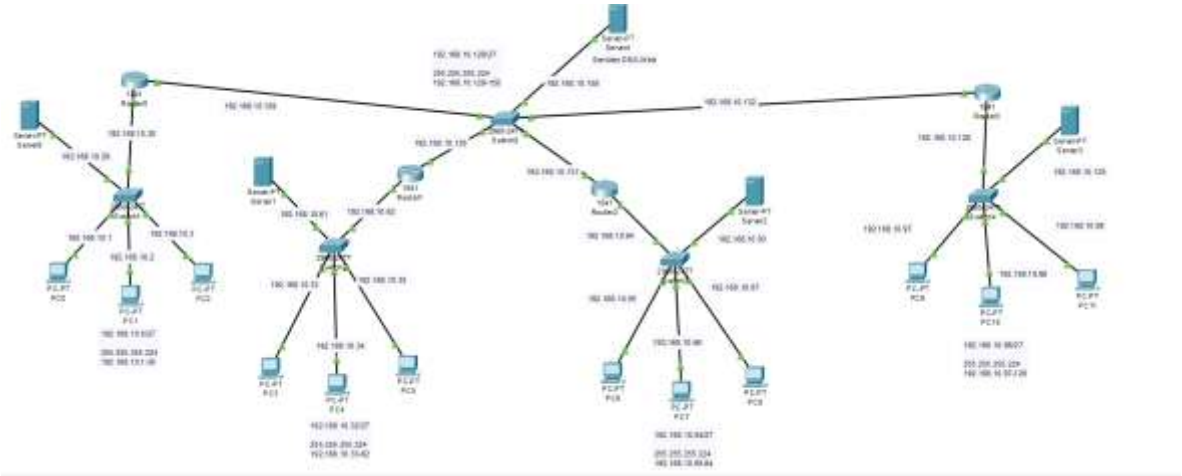
Además de implementar las subredes con VLSM y configurar DHCP, añadí un servidor que ofreciera servicios de DNS y Web. Registré un dominio en el DNS y configuré una página web de prueba. Verifiqué que cada PC obtuviera IP automáticamente, aprendiera rutas mediante enrutamiento dinámico y fuera capaz de resolver nombres y acceder a la página web.

Red Con 4 Vlan y un Router DHCP DNS en el router



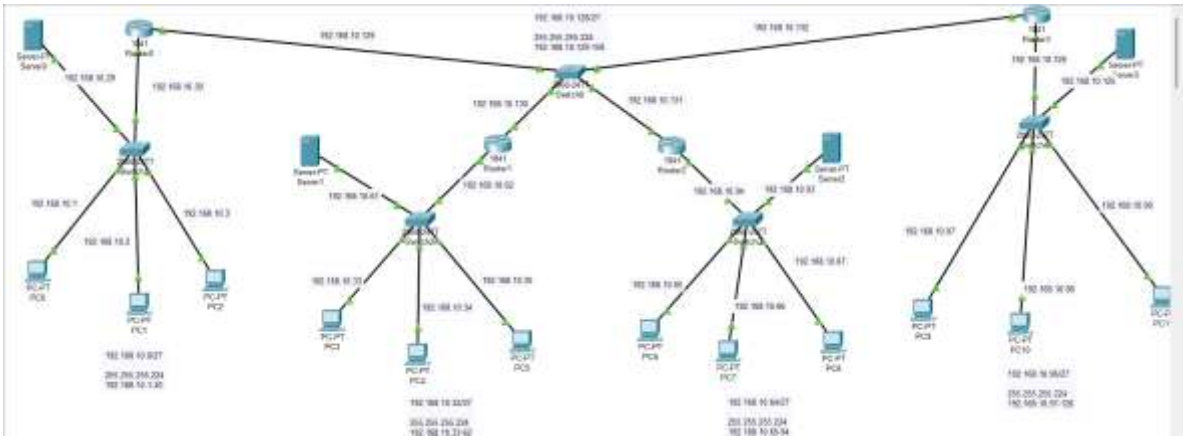
Establecí las VLAN en los switches. En el router configuré subinterfaces como gateways de cada VLAN. Configuré un servidor DHCP dentro del router para asignar direcciones IP a cada VLAN y activé el servicio DNS también desde el router. Probé conectividad mediante nombres de dominio, así como la correcta asignación de IP en todas las VLAN.

Red con subredes con direccionamiento dinamico y enrutamiento dinamico con servidor dns web



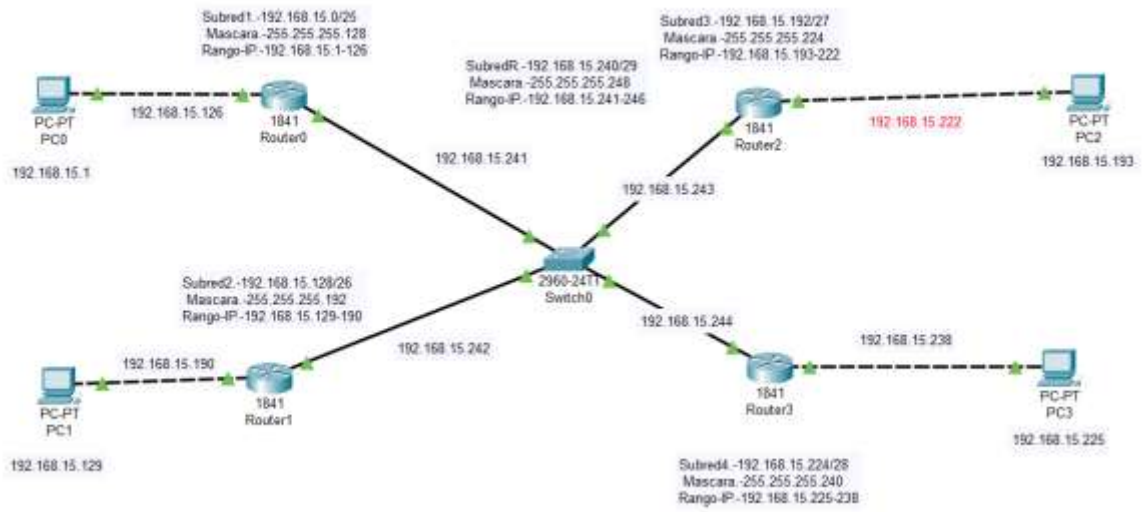
Habilité DHCP para automatizar la asignación de direcciones. Activé OSPF o EIGRP para permitir que los routers intercambiaran información de rutas. Añadí un servidor con DNS/Web y registré un dominio. Realicé pruebas de navegación, pings entre subredes y consultas DNS.

Red con 5 Subredes con direccionamiento dinamico y enrutamiento estatico



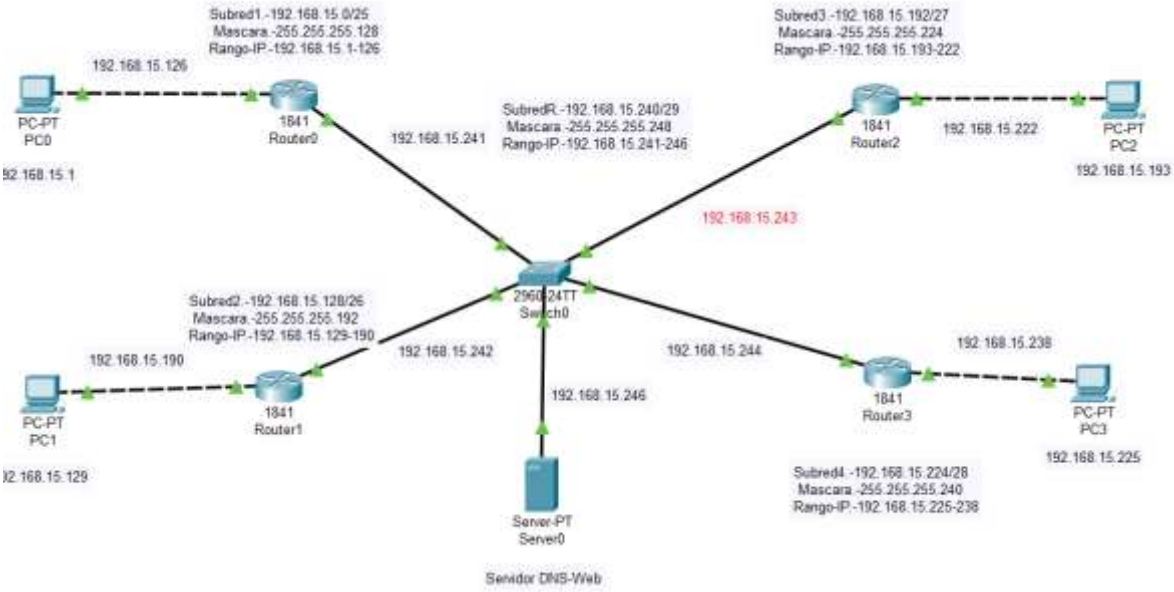
Realicé el subnetting para generar las 5 subredes necesarias. Configuré DHCP para entregar direcciones IP automáticamente a cada red. A diferencia de otras prácticas, las rutas de esta topología se ingresaron estáticamente en el router. Realicé pruebas de conectividad entre todas las redes y validé que el tráfico fluyera correctamente.

Red con 5 subredes con vlms direccionamiento estatico y enrutamiento dinamico



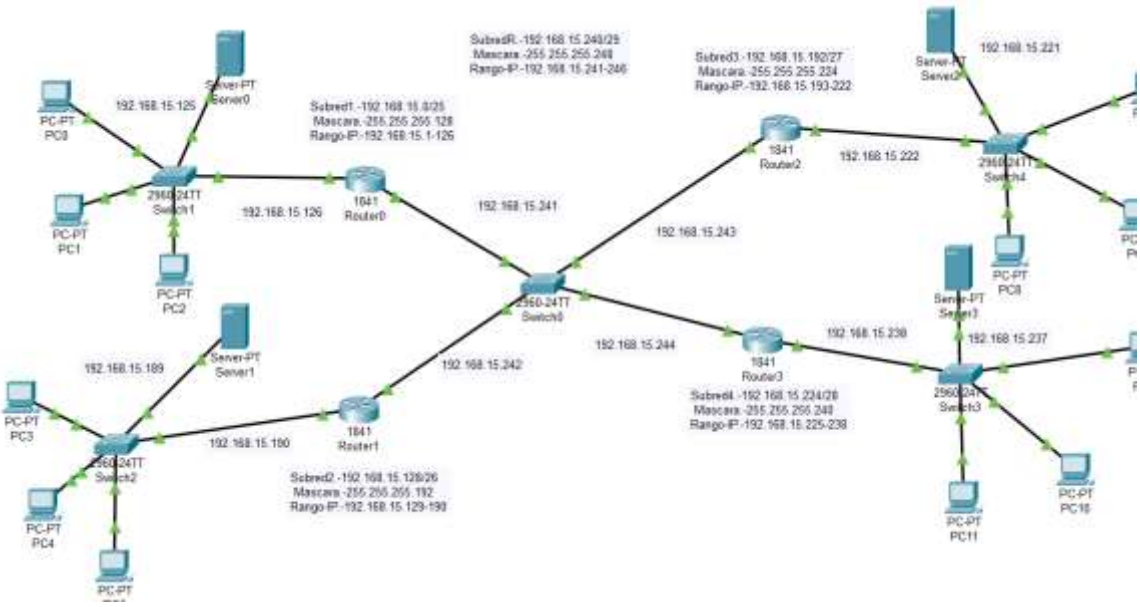
Utilicé VLSM para diseñar las subredes con la máscara adecuada para cada segmento. Asigné direcciones IP manualmente. Luego activé un protocolo dinámico para que el router aprendiera las rutas sin necesidad de ingresarlas manualmente. Realicé pruebas entre todas las subredes para confirmar la correcta comunicación.

Estatico y enrutamiento dinamico con servidor dns web



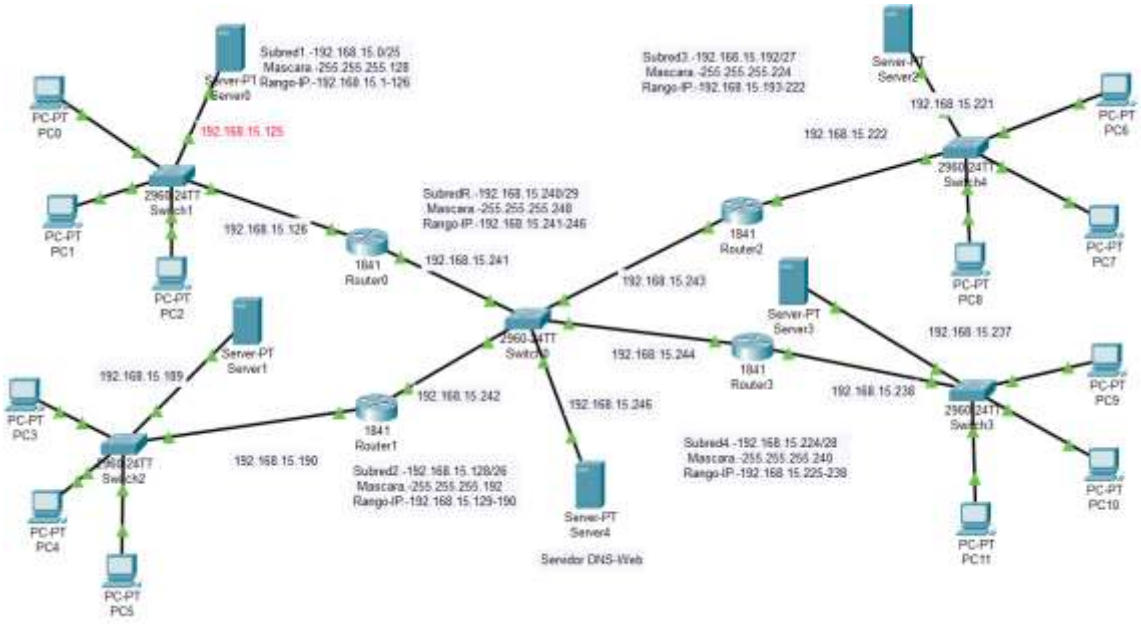
Comparé la forma de trabajo de ambos tipos de enrutamiento dentro de la misma topología. Primero configuré rutas estáticas y probé comunicación. Luego habilité enrutamiento dinámico para que el router aprendiera las rutas. Integré un servidor DNS/Web para probar accesos y resolución de nombres bajo ambos esquemas.

Red con 5 subredes con vlsm direccionamiento dinamico enrutamiento dinamico



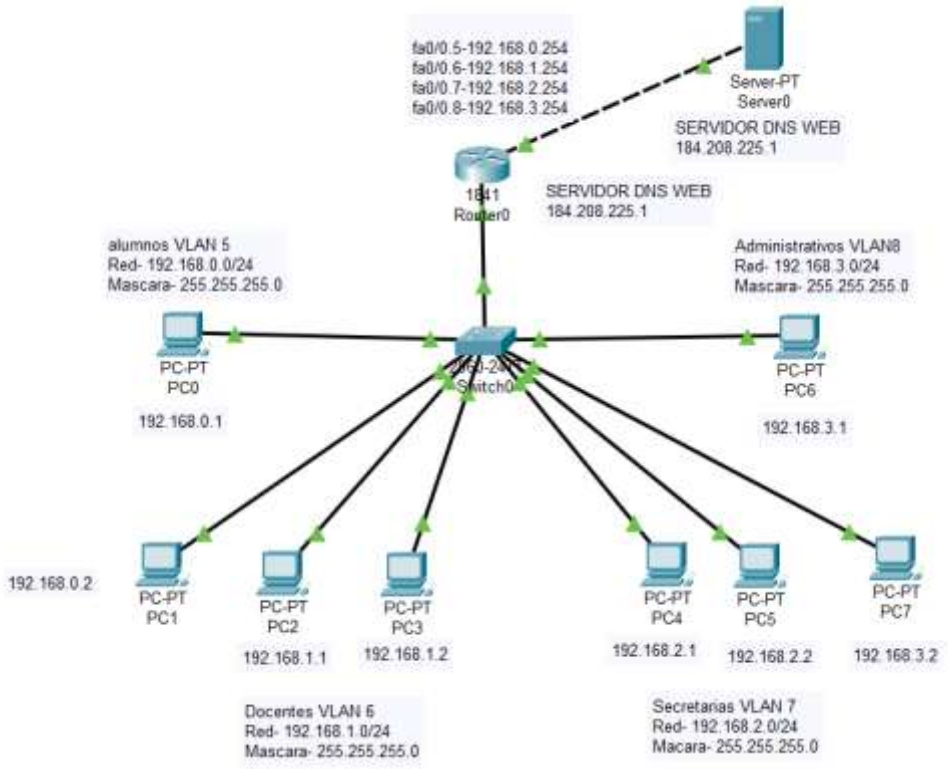
Utilicé VLSM para diseñar las subredes con la máscara adecuada para cada segmento. Asigné direcciones IP manualmente. Luego activé un protocolo dinámico para que el router aprendiera las rutas sin necesidad de ingresarlas manualmente. Realicé pruebas entre todas las subredes para confirmar la correcta comunicación.

Red con 5 subredes con vlms direccionamiento dinamico y enrutamiento dinamico con servidor dns web



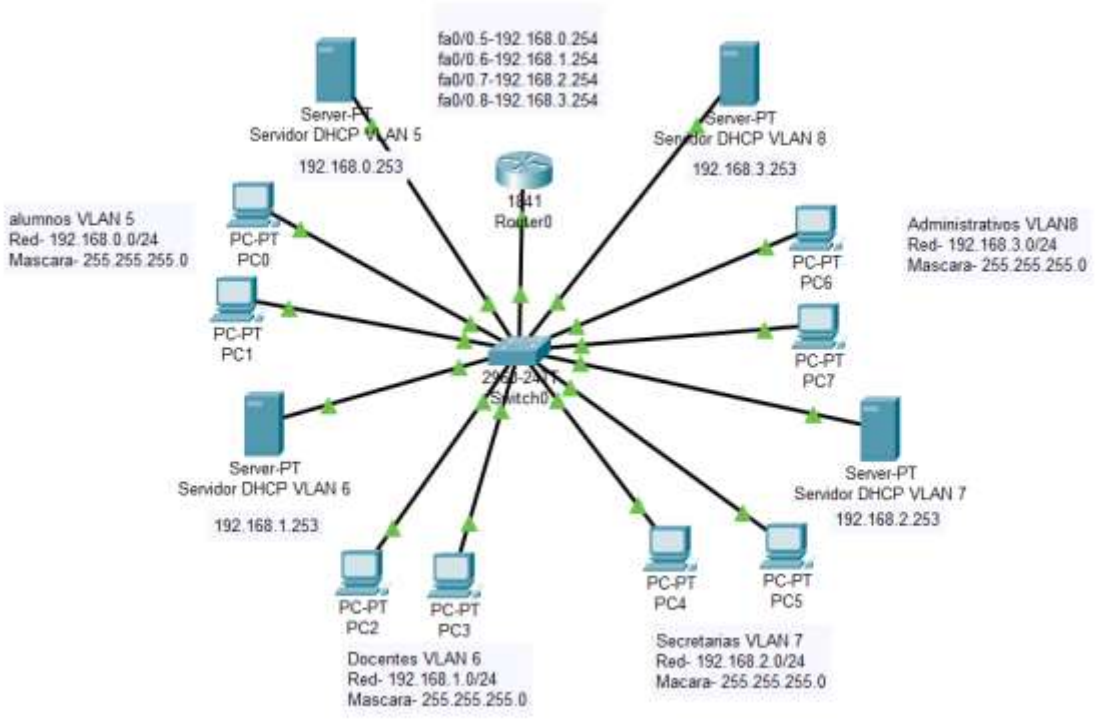
Además de implementar las subredes con VLSM y configurar DHCP, añadí un servidor que ofreciera servicios de DNS y Web. Registré un dominio en el DNS y configuré una página web de prueba. Verifiqué que cada PC obtuviera IP automáticamente, aprendiera rutas mediante enrutamiento dinámico y fuera capaz de resolver nombres y acceder a la página web.

Red con cuatro vlan y servidor dns web y dhcp en el router



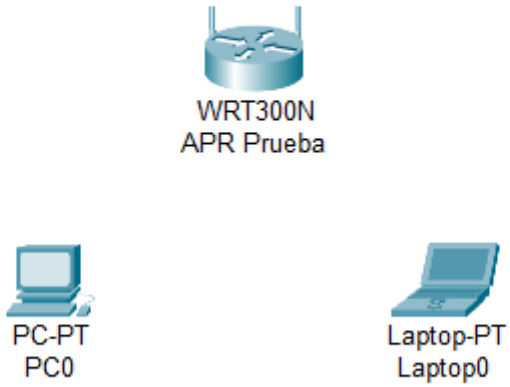
Establecí las VLAN en los switches. En el router configuré subinterfaces como gateways de cada VLAN. Configuré un servidor DHCP dentro del router para asignar direcciones IP a cada VLAN y activé el servicio DNS también desde el router. Probé conectividad mediante nombres de dominio, así como la correcta asignación de IP en todas las VLAN.

Red con cuatro vlan y servidores dhcp



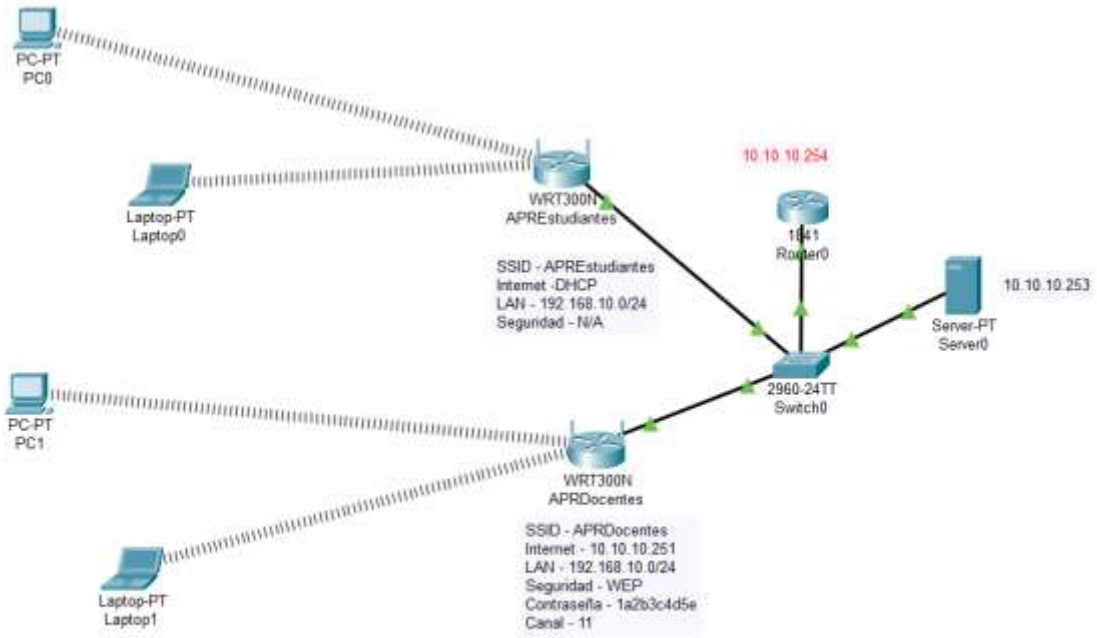
Configuré cuatro VLAN y asigné puertos en los switches. Utilicé servidores DHCP independientes (o scopes diferentes) para cada VLAN. Verifiqué que las PCs recibieran la configuración IP correcta según la VLAN donde estaban conectadas. También probé comunicación entre VLAN mediante un router-on-a-stick.

Red Vlan Con Apr y 2 equipos



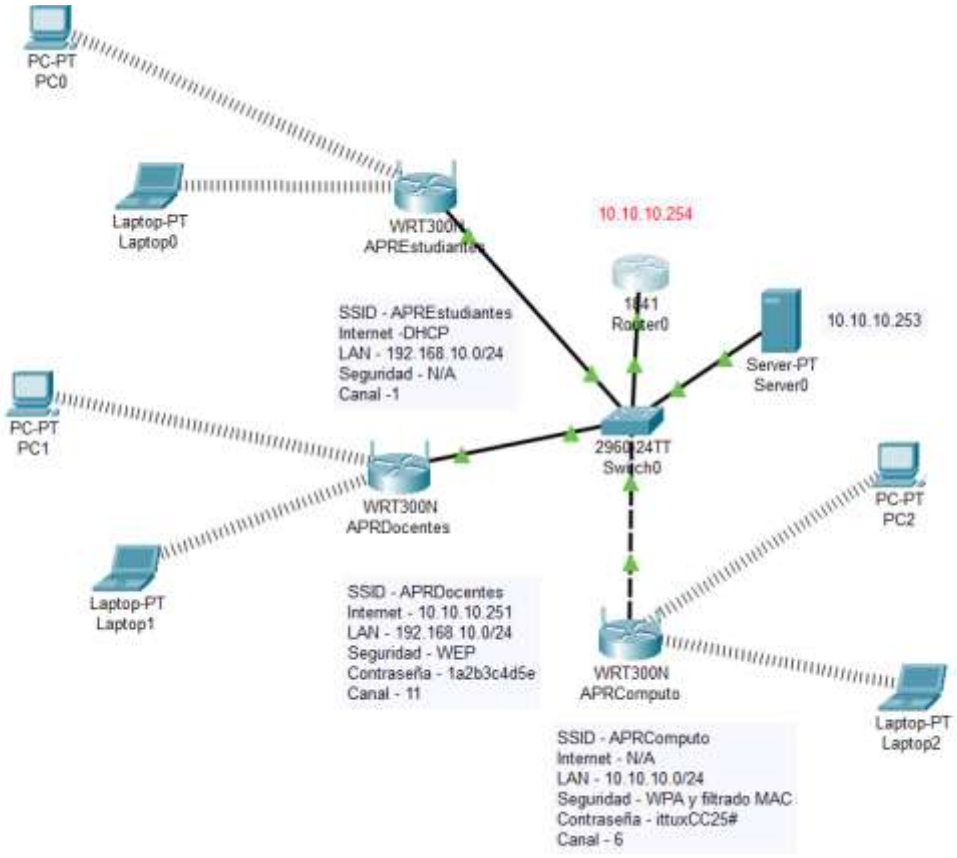
Configuré una VLAN en el switch principal y un Access Point dentro de esa VLAN. Asigné SSID, contraseña y direccionamiento. Conecté dos equipos inalámbricos y comprobé que obtuvieran IP, pertenecieran a la VLAN asignada y se comunicaran correctamente.

Red wlan con 2apr 1 router Y 1 servidor dhcp



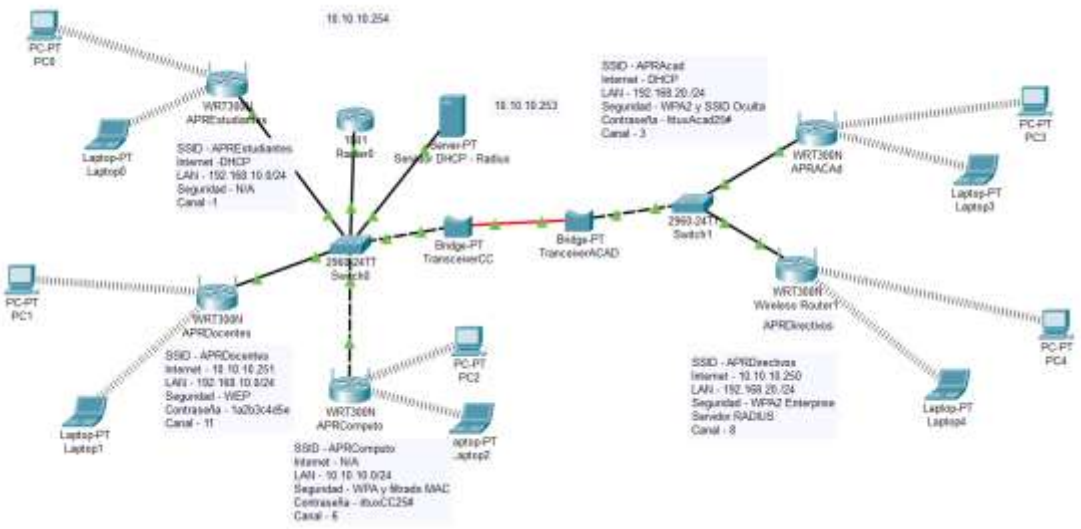
Diseñé una red inalámbrica con dos puntos de acceso. Configuré el router como gateway principal y el servidor DHCP para entregar direcciones a los dispositivos que se conectaran. Ajusté los canales de los AP para evitar interferencia y realicé pruebas de roaming entre ellos.

Red wlan con 3 apr 1router 1servidor dhcp



Extendí la red anterior agregando un tercer AP. Ajusté el rango de cobertura, repetí las configuraciones de SSID y seguridad, y mantuve un único servidor DHCP centralizado. Probé la movilidad de los dispositivos de un AP a otro sin perder conectividad.

red wlan con 5 apr, 1 router Y 1 servidor dhcp radius



Configuré un servidor RADIUS para brindar autenticación segura. Configuré cada AP para enviar credenciales al servidor RADIUS. Mantuvimos un único router como gateway y el mismo servidor como DHCP. Probé que solo los usuarios autorizados pudieran conectarse y que los dispositivos tuvieran movilidad entre APs sin perder autenticación

CONCLUSIÓN

El desarrollo de todas las prácticas en Cisco Packet Tracer permitió comprender de manera integral el funcionamiento de las redes de comunicación, desde configuraciones básicas de direccionamiento hasta la implementación de soluciones avanzadas con VLAN, enrutamiento dinámico, servicios de red y redes inalámbricas. Cada actividad contribuyó a fortalecer la capacidad de analizar, diseñar y resolver problemas de conectividad aplicando las mejores prácticas de red.

Gracias a este proyecto fue posible identificar la importancia de una correcta planificación del direccionamiento, del uso adecuado de los protocolos de enrutamiento y de la implementación de servicios esenciales como DHCP y DNS. Asimismo, se adquirió experiencia en la integración de tecnologías inalámbricas, lo cual es indispensable en redes modernas. En conjunto, estas prácticas permitieron desarrollar competencias técnicas sólidas que servirán como base para futuros proyectos y para el desempeño profesional en el área de redes e interconectividad.