S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO de Tuxtepec

INTERCONECTIVIDAD DE REDES

REPORTE TIPO MEMORIA “TEORÍA Y PRÁCTICAS DE INTERCONECTIVIDAD DE REDES”

PRESENTA:

Ortega Tomás Nelly Johana

NÚMERO DE CONTROL:

22350403

DOCENTE:

Dr. Julio Aguilar Carmona

GRADO Y GRUPO:

7° “A”

CARRERA:

INGENIERIA INFORMÁTICA

San Juan Bautista Tuxtepec, Oaxaca, México

DICIEMBRE 2025

ÍNDICE

INTRODUCCIÓN 3
OBJETIVO 4
DESARROLLO 5
TEORÍA 5
1. Spanning Tree Protocol (STP) 5
2. Clasificaciones de las direcciones IP 6
3. Subneteo (Subnetting) 7
4. Simulación de una red LAN en Cisco Packet Tracer 9
5. Enrutamiento Estático 10
6. Enrutamiento Dinámico 11
7. Métricas y distancia administrativa 12
8. VLAN (Virtual Local Area Network) 12
9. WLAN (Redes inalámbricas) 14
10. Protocolo de puerto de enlace fronterizo (BGP o VTP) 15
11. Protocolo FTP (File Transfer Protocol) 16
12. Protocolo OSPF (Open Shortest Path First) 16
PRÁCTICAS 17
PRÁCTICA 1: Red con cuatro VLAN, servidor DNS-Web y DHCP en el router 17
PRÁCTICA 2: Red con 3 VLAN, enlaces troncales y router 19
PRÁCTICA 3: Red WLAN con 3 AP, 1 router y 1 servidor DHCP 20
PRÁCTICA 4: Red con 5 subredes usando VLSM, direccionamiento estático y enrutamiento estático 21
CONCLUSIÓN 22
REFERENCIAS 23

INTRODUCCIÓN

El presente reporte tiene como finalidad documentar de manera teórica y práctica los principales conceptos relacionados con el diseño, configuración y administración de interconectividad de redes, a lo largo del desarrollo se abordan fundamentos como el direccionamiento IP, subneteo, VLAN, enrutamiento estático y dinámico, así como tecnologías inalámbricas y protocolos utilizados en redes locales y de mayor escala.

Asimismo, se integran prácticas realizadas en un entorno de simulación utilizando Cisco Packet Tracer, lo que permitió aplicar los conocimientos teóricos en escenarios controlados que representan situaciones reales de configuración de redes, estas prácticas incluyen la segmentación lógica mediante VLAN, el uso de enlaces troncales, la implementación de servicios como DHCP y DNS, la configuración de redes inalámbricas y el uso de VLSM para un aprovechamiento eficiente del direccionamiento IP.

Este trabajo se presenta como una memoria técnica que evidencia el proceso de aprendizaje, comprensión y aplicación de los conceptos fundamentales de redes, reforzando la relación entre la teoría y su implementación práctica.

OBJETIVO

Analizar y aplicar los principios fundamentales de la interconectividad de redes mediante el estudio teórico y la implementación práctica de configuraciones de red, con el fin de comprender el funcionamiento, la segmentación, el direccionamiento y el enrutamiento en diferentes escenarios.

DESARROLLO

TEORÍA

1. Spanning Tree Protocol (STP)

Definición y propósito

El Spanning Tree Protocol (STP) es un protocolo de la capa de enlace de datos diseñado para prevenir bucles en redes Ethernet que cuentan con enlaces redundantes. Fue creado por Radia Perlman y estandarizado en IEEE 802.1D. Su función principal es garantizar que exista una única ruta lógica entre dispositivos de red, evitando la duplicación de tramas y las tormentas de broadcast que pueden saturar la red.

Problema de los bucles en Ethernet

En redes con múltiples caminos de conexión, los bucles generan un flujo infinito de tramas que afectan la estabilidad y disponibilidad del servicio. STP resuelve este problema al bloquear dinámicamente los enlaces redundantes, manteniendo una topología libre de bucles.

Funcionamiento básico

El protocolo selecciona un switch raíz (root bridge) como referencia central. A partir de este, los demás switches calculan la mejor ruta hacia el nodo raíz. Los enlaces que podrían provocar bucles se colocan en estado bloqueado, mientras que los enlaces activos permanecen en estado de reenvío. En caso de falla, STP reactiva un enlace previamente bloqueado para asegurar la continuidad del servicio.

Estados de los puertos

- Los puertos de los switches atraviesan diferentes estados:
- Blocking: evita el reenvío de tramas para prevenir bucles.
- Listening: analiza mensajes BPDU para determinar su rol.
- Learning: registra direcciones MAC sin reenviar tráfico.
- Forwarding: permite el paso normal de tramas.
- Disabled: permanece inactivo por configuración o error.

Variantes del protocolo

Con el tiempo surgieron mejoras como el Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w), que ofrece una convergencia más rápida, y el Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s), que permite gestionar múltiples árboles de expansión en redes con VLANs.

2. Clasificaciones de las direcciones IP

Direcciones públicas y privadas

Las direcciones IP públicas son aquellas asignadas por los proveedores de servicios de Internet (ISP) y permiten la comunicación directa en la red global. En contraste, las direcciones privadas se utilizan dentro de redes locales (LAN) y no son enrutables en Internet. Estas últimas están definidas en rangos específicos por la RFC 1918, como 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

Clases A, B y C

El sistema de clases de direcciones IP fue uno de los primeros métodos de organización de direcciones IPv4.

- Clase A: direcciones desde 0.0.0.0 a 127.255.255.255, con una gran cantidad de hosts por red.
- Clase B: direcciones desde 128.0.0.0 a 191.255.255.255, con un balance entre número de redes y hosts.
- Clase C: direcciones desde 192.0.0.0 a 223.255.255.255, con muchas redes, pero pocos hosts por cada una. Aunque este esquema ya no se utiliza en la práctica moderna (fue reemplazado por CIDR), sigue siendo importante para comprender la evolución del direccionamiento IP.

IPv4 e IPv6

- IPv4: utiliza direcciones de 32 bits, expresadas en formato decimal con cuatro octetos (ejemplo: 192.168.1.1). Su espacio de direcciones es limitado (aproximadamente 4.3 mil millones de direcciones).
- IPv6: emplea direcciones de 128 bits, expresadas en formato hexadecimal (ejemplo: 2001:0db8:85a3::8a2e:0370:7334). Fue diseñado para superar las limitaciones de IPv4, ofreciendo un espacio prácticamente ilimitado de direcciones y mejoras en seguridad y eficiencia en el enrutamiento.

3. Subneteo (Subnetting)

División de redes en subredes

El subneteo es el proceso de dividir una red IP en múltiples subredes más pequeñas. Esta técnica permite un mejor aprovechamiento de las direcciones disponibles, mejora la administración de la red y aumenta la seguridad al segmentar el tráfico.

Cada subred funciona como una red independiente, pero todas forman parte de la misma red principal.

Máscaras de subred

La máscara de subred es un valor binario que determina qué parte de la dirección IP corresponde a la red y cuál a los hosts. Se representa en formato decimal con cuatro octetos (ejemplo: 255.255.255.0) o en notación CIDR (ejemplo: /24).

- Una máscara más grande (ejemplo: /28) significa más subredes pero menos hosts por cada una.
- Una máscara más pequeña (ejemplo: /16) significa menos subredes pero más hosts disponibles.

Ejercicios con máscara

Un ejemplo práctico:

- Dirección IP: 192.168.1.0/24
- Máscara: 255.255.255.0
- Resultado: 1 red con 254 hosts disponibles.

Si se aplica subneteo con /26:

- Cada subred tiene 64 direcciones (62 hosts utilizables).
- Se generan 4 subredes dentro de la red original.

Este tipo de ejercicios permite calcular el número de subredes y hosts disponibles según la máscara aplicada, siendo una práctica esencial en la administración de redes.

4. Simulación de una red LAN en Cisco Packet Tracer

Configuración de switches

Los switches son dispositivos de capa 2 que permiten la interconexión de múltiples equipos dentro de una red local. En Cisco Packet Tracer, la configuración básica incluye:

- Asignación de nombre al dispositivo.
- Configuración de VLANs para segmentar el tráfico.
- Activación de puertos y verificación de conectividad mediante comandos como ping.
- Opcionalmente, se pueden configurar protocolos como STP para evitar bucles en redes con enlaces redundantes.

Configuración de PCs

Las computadoras dentro de la simulación requieren parámetros básicos para integrarse a la red:

- Asignación de dirección IP y máscara de subred.
- Configuración de puerta de enlace predeterminada para comunicación fuera de la subred.
- Pruebas de conectividad con otros dispositivos mediante comandos como ping o tracert.

Configuración de routers

Los routers operan en la capa 3 y permiten la interconexión entre diferentes redes o subredes. En Cisco Packet Tracer, la configuración incluye:

- Asignación de direcciones IP a las interfaces.
- Configuración de rutas estáticas o dinámicas (ejemplo: RIP, OSPF).

- Activación de servicios como DHCP para asignación automática de direcciones IP.
- Verificación de conectividad entre redes mediante pruebas de comunicación entre hosts.

5. Enrutamiento Estático

Configuración manual de rutas

El enrutamiento estático consiste en la configuración manual de rutas en un router. El administrador de red define explícitamente la dirección de destino, la máscara de subred y la interfaz de salida o el siguiente salto. Este método es sencillo y ofrece control total sobre el tráfico, pero requiere mayor esfuerzo de administración en redes grandes.

Tabla de enrutamiento

Las rutas configuradas manualmente se almacenan en la tabla de enrutamiento del router. Esta tabla contiene información sobre las redes conocidas, la máscara de subred correspondiente y el camino que debe seguir cada paquete. En el caso del enrutamiento estático, las entradas permanecen fijas hasta que el administrador las modifique.

Interfaces de salida

Cada ruta estática debe especificar una interfaz de salida o un siguiente salto. La interfaz de salida indica por dónde debe enviarse el paquete hacia la red de destino. Si la interfaz falla, el tráfico no podrá ser redirigido automáticamente, lo que representa una limitación frente a los protocolos dinámicos.

6. Enrutamiento Dinámico

Definición

El enrutamiento dinámico utiliza protocolos que permiten a los routers intercambiar información de manera automática para determinar las mejores rutas disponibles. A diferencia del enrutamiento estático, las rutas se actualizan de forma continua según los cambios en la topología de la red.

Protocolos de enrutamiento dinámico

Existen diferentes protocolos que implementan enrutamiento dinámico:

- RIP (Routing Information Protocol): basado en el conteo de saltos.
- OSPF (Open Shortest Path First): utiliza el algoritmo de Dijkstra para calcular la ruta más corta.
- EIGRP (Enhanced Interior Gateway Routing Protocol): protocolo híbrido desarrollado por Cisco.
- BGP (Border Gateway Protocol): utilizado para el enrutamiento entre sistemas autónomos en Internet.

Ventajas

- Adaptación automática a cambios en la red.
- Escalabilidad en redes grandes.
- Reducción de la carga administrativa.

Desventajas

- Mayor consumo de recursos (CPU y memoria).
- Complejidad en la configuración inicial.

7. Métricas y distancia administrativa

Métricas en enrutamiento

Las métricas son valores numéricos que los protocolos de enrutamiento utilizan para determinar la mejor ruta hacia un destino. Cada protocolo emplea diferentes criterios:

- RIP: número de saltos (hop count).
- OSPF: costo basado en el ancho de banda.
- EIGRP: combinación de ancho de banda, retardo, confiabilidad y carga. Las métricas permiten comparar rutas y seleccionar la más eficiente.

Distancia administrativa

La distancia administrativa (AD) es un valor que indica la confiabilidad de una fuente de enrutamiento. Los routers utilizan la AD para decidir entre múltiples rutas hacia el mismo destino.

- AD de rutas conectadas directamente: 0 (máxima confiabilidad).
- AD de rutas estáticas: 1.
- AD de protocolos dinámicos: varía (ejemplo: OSPF = 110, RIP = 120, EIGRP = 90). Este mecanismo asegura que el router elija la ruta más confiable cuando existen múltiples opciones.

8. VLAN (Virtual Local Area Network)

Tipos de VLAN

Las VLAN permiten segmentar una red física en múltiples redes lógicas. Los principales tipos son:

- VLAN de datos: separan el tráfico de usuarios.
- VLAN de voz: optimizadas para telefonía IP.
- VLAN nativas: utilizadas para tráfico no etiquetado en enlaces troncales.
- VLAN de administración: reservadas para la gestión de dispositivos de red.

Modos de puerto del switch

Los switches manejan dos modos principales de puerto:

- Acceso: asignado a una única VLAN, utilizado para conectar dispositivos finales (PCs, impresoras).
- Troncal (trunk): transporta múltiples VLANs mediante etiquetado (802.1Q), utilizado para interconectar switches o switches con routers.

Control de dominios de broadcast

Las VLAN dividen la red en dominios de broadcast más pequeños. Esto significa que las tramas de difusión se limitan a la VLAN correspondiente, reduciendo la congestión y mejorando la seguridad.

Configuración de switches con puertos troncales

La configuración básica en Cisco IOS incluye:

- Definir VLANs con el comando vlan [ID].
- Asignar puertos de acceso con switchport mode access y switchport access vlan [ID].
- Configurar puertos troncales con switchport mode trunk y permitir VLANs específicas con switchport trunk allowed vlan [IDs]. Esto asegura que las VLAN funcionen correctamente entre múltiples dispositivos.

9. WLAN (Redes inalámbricas)

Componentes de infraestructura inalámbrica

Una WLAN (Wireless Local Area Network) es una red local que utiliza ondas de radio para conectar dispositivos sin necesidad de cables físicos. Sus principales componentes son:

- Puntos de acceso (Access Points, APs): dispositivos que permiten la conexión inalámbrica de los clientes a la red.
- Clientes inalámbricos: laptops, smartphones, tablets y otros dispositivos con tarjetas de red Wi-Fi.
- Controladores inalámbricos: gestionan múltiples puntos de acceso en redes empresariales, centralizando la administración.
- Antenas: internas o externas, que amplifican la señal y mejoran la cobertura.
- Switches y routers: integran la WLAN con la red cableada y permiten la salida hacia Internet.

Instalación y configuración básica

La instalación de una WLAN requiere la planificación de cobertura y seguridad. Los pasos básicos incluyen:

- Ubicación de puntos de acceso: se colocan estratégicamente para garantizar cobertura uniforme y evitar zonas muertas.
- Configuración de SSID (Service Set Identifier): nombre de la red que permite a los usuarios identificarla.
- Asignación de direcciones IP: mediante DHCP o configuración manual.
- Seguridad inalámbrica: se recomienda el uso de WPA2 o WPA3 para proteger la red contra accesos no autorizados.
- Pruebas de conectividad: verificar que los dispositivos puedan acceder a la red y navegar en Internet.

En entornos empresariales, la configuración puede incluir VLANs para segmentar el tráfico, autenticación mediante servidores RADIUS y monitoreo de rendimiento con controladores inalámbricos.

10. Protocolo de puerto de enlace fronterizo (BGP o VTP)

BGP (Border Gateway Protocol):

El Border Gateway Protocol (BGP) es un protocolo de enrutamiento dinámico utilizado para el intercambio de información entre sistemas autónomos en Internet. Es fundamental para determinar las rutas más eficientes entre diferentes proveedores de servicios y redes globales.

- Tipo: protocolo de enrutamiento de exterior (EGP).
- Característica principal: selecciona rutas basadas en políticas y atributos, no únicamente en métricas técnicas.
- Uso: es el protocolo que mantiene la estructura jerárquica de Internet.

VTP (VLAN Trunking Protocol):

El VLAN Trunking Protocol (VTP) es un protocolo propietario de Cisco que administra la creación y propagación de VLANs en una red de switches.

- Permite que un switch actúe como servidor y distribuya información de VLANs a otros switches.
- Facilita la administración centralizada de VLANs en redes grandes.
- Funciona sobre enlaces troncales configurados con 802.1Q o ISL.

11. Protocolo FTP (File Transfer Protocol)

El File Transfer Protocol (FTP) es un protocolo de aplicación que permite la transferencia de archivos entre sistemas a través de una red TCP/IP.

Funcionamiento

- Utiliza el puerto 21 para el control de la conexión.
- Puede operar en modo activo o pasivo.
- Requiere autenticación mediante usuario y contraseña, aunque existen implementaciones de acceso anónimo.

Usos

- Publicación y descarga de archivos en servidores web.
- Intercambio de datos en entornos empresariales.
- Administración remota de archivos.

12. Protocolo OSPF (Open Shortest Path First)

El Open Shortest Path First (OSPF) es un protocolo de enrutamiento dinámico de interior (IGP) basado en el algoritmo de Dijkstra.

Características

- Utiliza métricas de costo basadas en el ancho de banda.
- Divide la red en áreas para mejorar la escalabilidad.
- Garantiza convergencia rápida y eficiente en redes grandes.

Ventajas

- Escalabilidad en redes empresariales.
- Soporte para VLSM (Variable Length Subnet Mask).
- Menor consumo de ancho de banda en comparación con protocolos como RIP.

PRÁCTICAS

PRÁCTICA 1: Red con cuatro VLAN, servidor DNS-Web y DHCP en el router

En esta práctica realicé la configuración de una red con cuatro VLAN, utilizando un switch y un router. Cada VLAN representa un grupo distinto de usuarios y cuenta con su propia red IP. El router se encarga de realizar el enrutamiento entre VLAN y también de proporcionar el servicio de DHCP, para que las computadoras obtengan su dirección IP de manera automática.

La red está formada por un router, un switch, ocho computadoras y un servidor DNS-Web. Las computadoras se distribuyeron en las cuatro VLAN, dos equipos por cada una. El servidor DNS-Web se colocó en una de las VLAN para que pudiera ser accesible desde las demás.

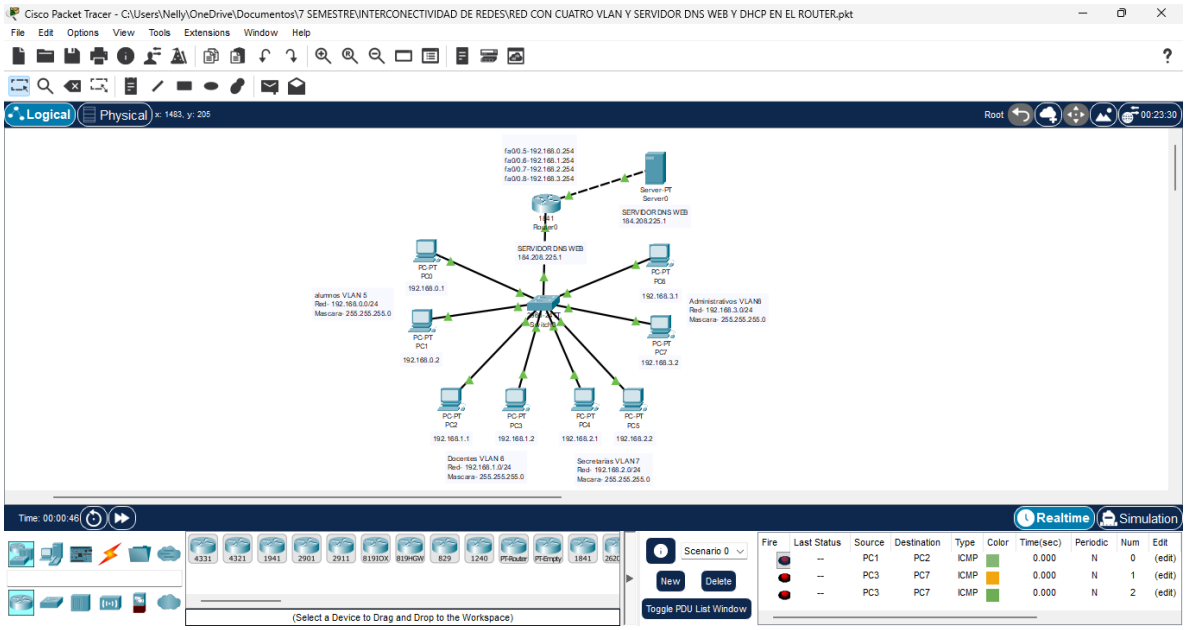
Las VLAN configuradas fueron las siguientes:

- VLAN 5 (alumnos)
- Red: 192.168.0.0/24
- Equipos: PC0 y PC1

- VLAN 6 (docentes)
- Red: 192.168.1.0/24
- Equipos: PC2 y PC3

- VLAN 7 (secretarias)
- Red: 192.168.2.0/24
- Equipos: PC4 y PC5

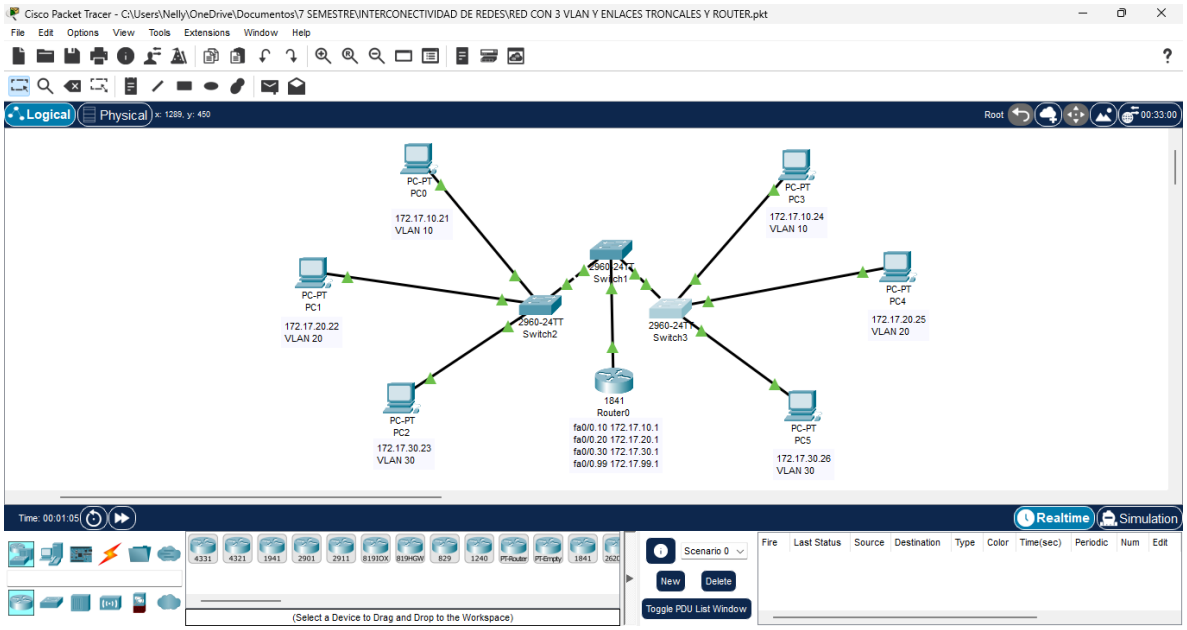
- VLAN 8 (administrativos)
- Red: 192.168.3.0/24
- Equipos: PC6 y PC7



PRÁCTICA 2: Red con 3 VLAN, enlaces troncales y router

En esta práctica configuré una red con tres VLAN, utilizando varios switches conectados entre sí mediante enlaces troncales y un router para permitir la comunicación entre las VLAN mediante enrutamiento inter-VLAN. El propósito de la práctica fue comprobar que es posible mantener separadas las VLAN y, al mismo tiempo, permitir que los equipos de distintas VLAN se comuniquen a través del router.

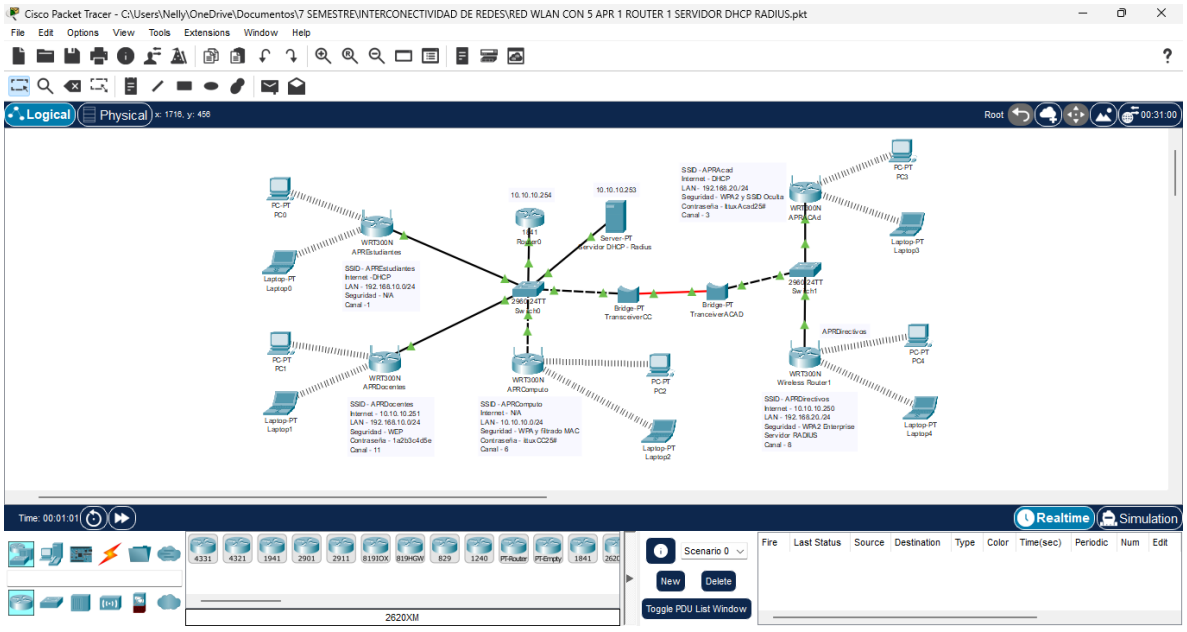
La topología está formada por tres switches Cisco 2960-24TT (Switch1, Switch2 y Switch3), un router (Router0) y seis computadoras, distribuidas en las tres VLAN. Los enlaces entre los switches y el enlace entre el switch principal y el router se configuraron en modo troncal, utilizando encapsulación IEEE 802.1Q, para permitir el tráfico de todas las VLAN.



PRÁCTICA 3: Red WLAN con 3 AP, 1 router y 1 servidor DHCP

En esta práctica configuré una red inalámbrica (WLAN) formada por tres puntos de acceso, un router, un switch central y un servidor DHCP, con el objetivo de permitir la conexión de dispositivos inalámbricos distribuidos en tres redes Wi-Fi distintas, cada una con su propia configuración de seguridad. Además, se buscó centralizar la asignación de direcciones IP mediante un servidor DHCP.

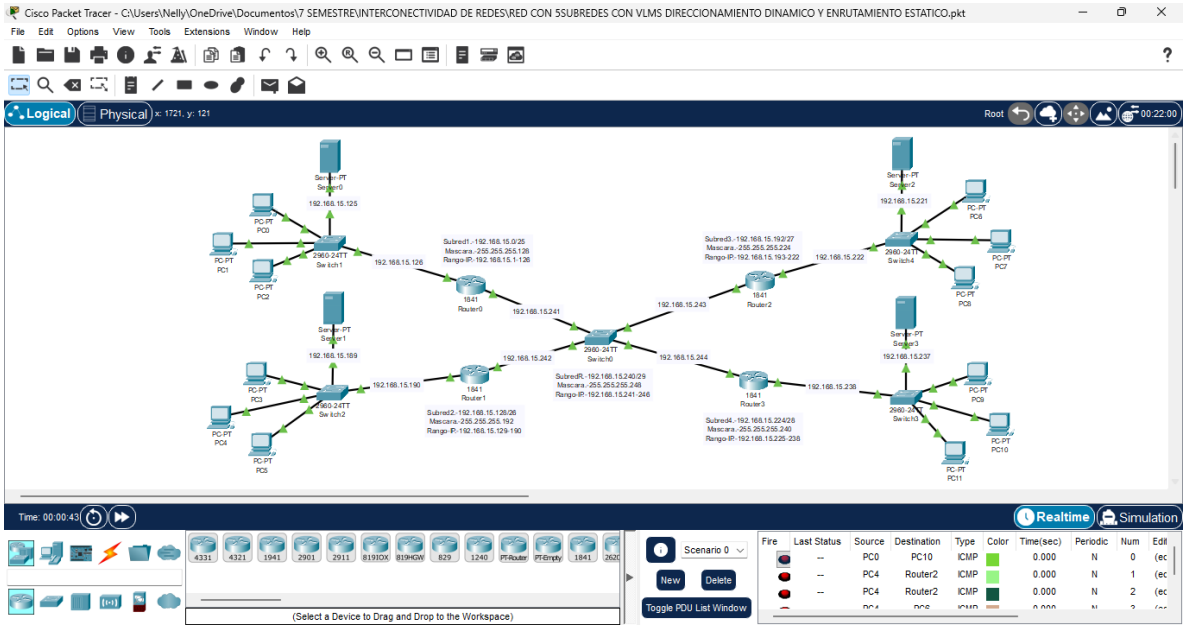
La topología está compuesta por tres routers inalámbricos modelo WRT300N, un switch (Switch0), un router (Router0), un servidor (Server0), tres laptops y tres computadoras de escritorio. Todos los dispositivos cableados se conectan al switch central, el cual permite la comunicación entre los puntos de acceso, el servidor y el router.



PRÁCTICA 4: Red con 5 subredes usando VLSM, direccionamiento estático y enrutamiento estático

En esta práctica diseñé y configuré una red dividida en cinco subredes, utilizando el método de VLSM (Variable Length Subnet Masking) para optimizar el uso de las direcciones IP. Todas las direcciones fueron asignadas de forma manual, y la comunicación entre las subredes se logró mediante enrutamiento estático, sin utilizar protocolos de enrutamiento dinámico.

El propósito principal de la práctica fue aplicar el cálculo de subredes con diferentes máscaras, asignar direcciones IP de acuerdo con las necesidades de cada segmento y configurar rutas estáticas para permitir la comunicación entre todos los dispositivos de la red.



CONCLUSIÓN

A través del desarrollo de este reporte fue posible reforzar los conocimientos teóricos y prácticos relacionados con la interconectividad de redes, comprendiendo la importancia de una correcta planeación y configuración de la infraestructura de red, el estudio de protocolos como STP, OSPF y FTP permitió entender cómo se garantiza la estabilidad, eficiencia y seguridad en la transmisión de datos.

Las prácticas realizadas demostraron la relevancia de la segmentación de redes mediante VLAN, el uso de enlaces troncales, asimismo, el uso de VLSM permitió optimizar el direccionamiento IP, evitando el desperdicio de direcciones y facilitando la administración de la red.

Finalmente, la simulación de redes cableadas e inalámbricas en Cisco Packet Tracer permitió aplicar los conceptos aprendidos en escenarios cercanos a la realidad, fortaleciendo habilidades técnicas fundamentales para el diseño y administración de redes, este trabajo contribuye significativamente a la formación profesional, al integrar teoría y práctica de manera estructurada y coherente.

REFERENCIAS

CCNA desde Cero. (s.f.). Spanning Tree Protocol (STP): Qué hace y cómo funciona. Recuperado de https://ccnadesdecero.es/spanning-tree-protocol-stp-como-funciona/

Profesor Iván Anguiano. (2023, diciembre 4). STP Spanning Tree Protocol. Universidad Autónoma de Baja California. Recuperado de https://sites.google.com/uabc.edu.mx/profesor-ivan-anguiano/modelo-osi-y-tcpip/OSICapa2/stp-spanning-tree-protocol

Wikipedia. (s.f.). Spanning Tree Protocol. En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Spanning_Tree_Protocol

IEEE. (s.f.). IEEE 802.1D. En Wikipedia. Recuperado de https://en.wikipedia.org/wiki/IEEE_802.1D

Cisco Systems, Inc. (2023, febrero 9). Explicación del Protocolo de árbol de expansión rápida (802.1w). Recuperado de https://www.cisco.com/c/es_mx/support/docs/lan-switching/spanning-tree-protocol/24062-146.html

Cisco Networking Academy. (s.f.). Direcciones IP públicas y privadas. Recuperado de https://www.netacad.com/es/courses/networking/ip-addresses

RFC 1918. (1996). Address Allocation for Private Internets. Internet Engineering Task Force (IETF). Recuperado de https://datatracker.ietf.org/doc/html/rfc1918

Wikipedia. (s.f.). Classful network. En Wikipedia. Recuperado de https://en.wikipedia.org/wiki/Classful_network

Wikipedia. (s.f.). IPv4. En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/IPv4

Wikipedia. (s.f.). IPv6. En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/IPv6

Cisco Networking Academy. (s.f.). Subnetting. Recuperado de https://www.netacad.com/courses/networking/subnetting

RFC 950. (1985). Internet Standard Subnetting Procedure. Internet Engineering Task Force (IETF). Recuperado de https://datatracker.ietf.org/doc/html/rfc950

Wikipedia. (s.f.). Subnetting. En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Subnetting

GeeksforGeeks. (2023). Subnetting in Computer Network. Recuperado de https://www.geeksforgeeks.org/subnetting-in-computer-network/

Tutorialspoint. (s.f.). Subnetting. Recuperado de https://www.tutorialspoint.com/subnetting/index.htm

Cisco Networking Academy. (s.f.). Packet Tracer: A network simulation tool. Recuperado de https://www.netacad.com/courses/packet-tracer

Tutorialspoint. (s.f.). Cisco Packet Tracer. Recuperado de https://www.tutorialspoint.com/cisco-packet-tracer/index.htm

GeeksforGeeks. (2023). Introduction to Cisco Packet Tracer. Recuperado de https://www.geeksforgeeks.org/introduction-to-cisco-packet-tracer/

Wikipedia. (s.f.). Cisco Packet Tracer. En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Cisco_Packet_Tracer

RFC 1812. (1995). Requirements for IP Version 4 Routers. Internet Engineering Task Force (IETF). Recuperado de https://datatracker.ietf.org/doc/html/rfc1812

Cisco Networking Academy. (s.f.). Wireless LANs. Recuperado de https://www.netacad.com/courses/networking/wireless-lans

IEEE. (s.f.). IEEE 802.11 Wireless LAN Standards. En IEEE Standards Association. Recuperado de https://standards.ieee.org/802/802.11/

Wikipedia. (s.f.). Wireless LAN. En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Wireless_LAN

GeeksforGeeks. (2023). Wireless LAN (WLAN) in Computer Network. Recuperado de https://www.geeksforgeeks.org/wireless-lan-wlan-in-computer-network/

Tutorialspoint. (s.f.). Wireless LAN Configuration. Recuperado de https://www.tutorialspoint.com/wireless-lan-configuration