S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO de Tuxtepec

INTERCONECTIVIDAD DE REDES

“REPORTE TIPO MEMORIA”

PRESENTA:

RIVERA MARTÍNEZ JESÚS

N. DE CONTROL:

22350405

DOCENTE:

JULIO AGUILAR CARMONA

CARRERA:

INGENIERIA INFORMÁTICA

SEMESTRE Y GRUPO:

7º “A”

DICIEMBRE/2025

Contenido

INTRODUCCIÓN

En el presente documento se muestran las prácticas realizadas durante el semestre en la materia de Interconectividad de Redes, donde se trabajó con el diseño de topologías, el uso de subneteo con VLSM, la configuración de direccionamiento estático y dinámico, así como la implementación de enrutamiento estático y dinámico. Además, se integraron servicios como DNS y Web, lo que permitió observar cómo los conceptos teóricos se aplican en escenarios simulados. A continuación, se presentan las evidencias de cada práctica, acompañadas de su explicación y resultados obtenidos.

OBJETIVO GENERAL

Presentar las evidencias de las prácticas realizadas a lo largo del semestre en la materia de Interconectividad de Redes, demostrando la aplicación de los conocimientos teóricos en el diseño, configuración y simulación de redes mediante herramientas como Cisco Packet Tracer.

TEMA 1. STP Y RSTP

TEORIA

1.1 QUÉ ES STP (SPANNING TREE PROTOCOL)

El **Spanning Tree Protocol (STP)** es un protocolo de capa 2 que evita bucles en redes conmutadas al crear una topología lógica en forma de árbol. Se ejecuta en switches y bridges, bloqueando enlaces redundantes y asegurando que exista un único camino activo entre dos dispositivos (CCNA desde Cero, 2020; Cisco Community, 2025).

1.2 ALGORITMO SPANNING TREE

El **Spanning Tree Algorithm (STA)** fue desarrollado en 1985 por Radia Perlman mientras trabajaba en Digital Equipment Corporation. Su objetivo es **crear una topología libre de bucles** en redes de capa 2, garantizando que exista un único camino activo entre dos dispositivos (Guru99, 2024).

El **algoritmo Spanning Tree (STA)** fue diseñado para evitar bucles en redes conmutadas de capa 2. Este algoritmo selecciona un puente raíz y calcula el camino más eficiente hacia él, bloqueando enlaces redundantes para mantener una topología libre de bucles (RedTauros, s.f.).

> “El STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al realizar un bloqueo intencional de aquellas rutas redundantes” (RedTauros, s.f.).

1.2.1 Importancia del algoritmo

- **Prevención de tormentas de broadcast:** evita que los paquetes se repliquen indefinidamente.
- **Redundancia segura:** permite enlaces alternativos sin riesgo de colapso.

- **Base para RSTP y MSTP:** el algoritmo original fue extendido para mejorar tiempos de convergencia y soportar múltiples árboles de expansión.

1.3 BPDU, ID DE PUENTE, FUNCIONES Y ESTADOS DE PUERTOS

1.3.1 BPDU (Bridge Protocol Data Units)

Las **BPDU** son tramas especiales que los switches intercambian para compartir información de la topología de red. Contienen datos como el **ID del puente raíz**, el costo del camino y el identificador del remitente.

> "Las BPDUs permiten a los switches detectar la topología de la red y decidir qué enlaces deben permanecer activos y cuáles deben bloquearse" (Studocu, s.f.).

Existen dos tipos principales:

- **Configuration BPDU:** construyen y mantienen el árbol de expansión.
- **Topology Change Notification BPDU:** notifican cambios en la topología (CCNA desde Cero, 2020).

1.3.2 Id de puente

El **Bridge ID** es un identificador único que cada switch utiliza en STP. Se compone de:

- **Prioridad del puente (Bridge Priority):** valor configurable por el administrador.
- **Dirección MAC del switch:** usada como desempate si las prioridades son iguales.

El switch con el menor Bridge ID se convierte en el **Root Bridge** (Studocu, s.f.).

1.3.3 Funciones de los puertos

Cada puerto en STP cumple una función específica:

- **Root Port:** el puerto con el mejor camino hacia el puente raíz.
- **Designated Port:** el puerto que reenvía tráfico hacia un segmento de red.
- **Alternate/Blocked Port:** puertos que permanecen inactivos para evitar bucles.

Este proceso asegura que solo exista un camino activo hacia cada destino (CCNA desde Cero, 2020).

1.3.4 Estados de los puertos

Los puertos en STP pasan por diferentes estados antes de reenviar tráfico:

1. **Blocking**: el puerto escucha BPDUs pero no reenvía tráfico.
2. **Listening:** procesa BPDUs y prepara la topología.
3. **Learning:** aprende direcciones MAC pero aún no reenvía tráfico.
4. **Forwarding:** el puerto reenvía tráfico normalmente.
5. **Disabled:** el puerto está administrativamente apagado.

Estos estados permiten que la red se estabilice antes de transmitir datos (CCNA desde Cero, 2020).

1.4 CONVERGENCIA STP

La **convergencia** es el proceso mediante el cual STP determina el puente raíz y configura los puertos en sus roles finales. Este proceso incluye tres pasos: elección del puente raíz, selección de puertos raíz y designados, y bloqueo de puertos redundantes. El tiempo de convergencia en STP clásico puede tardar entre 30 y 50 segundos, mientras que en RSTP se reduce a pocos segundos (Arias, 2014).

1.5 TOPOLOGÍAS REDUNDANTES DE CAPA 2

La redundancia en capa 2 permite tener múltiples enlaces físicos para asegurar disponibilidad. Sin embargo, esto genera riesgo de bucles. STP bloquea enlaces

redundantes y mantiene solo un camino activo, garantizando estabilidad y eficiencia (Cisco Community, 2025).

1.5.1 Problemas que generan las topologías redundantes

- **Bucles de red:** cuando existen múltiples caminos entre dos dispositivos, las tramas pueden circular indefinidamente.
- **Tormentas de broadcast:** un bucle puede replicar tramas broadcast sin control, saturando la red.
- **Inconsistencia en tablas MAC:** los switches reciben la misma dirección MAC por diferentes puertos, causando errores de reenvío.

1.6 CONFIGURACIÓN DE STP Y RSTP

1.6.1 Configuración de STP (IEEE 802.1D)

El protocolo STP clásico se configura principalmente en switches para definir cómo se selecciona el **puente raíz** y cómo se calculan los caminos hacia él.

- **Prioridad del puente:** cada switch tiene un valor de prioridad; el menor valor combinado con la dirección MAC determina el root bridge.
- **Costos de puerto:** cada enlace tiene un costo asociado según su velocidad (ejemplo: 100 Mbps = costo 19, 1 Gbps = costo 4). El algoritmo selecciona el camino con menor costo hacia el root bridge (Cisco, 2018).
- **Comandos básicos en Cisco IOS:**
    - spanning-tree vlan X priority Y → define la prioridad del switch para una VLAN.
    - spanning-tree vlan X root primary → fuerza al switch a ser root bridge.
    - show spanning-tree → verifica el estado de los puertos y el root bridge.

“La configuración de STP se basa en ajustar la prioridad del puente y los costos de enlace para controlar qué switch será el root bridge” (Cisco, 2018).

1.6.2 Configuración de RSTP (IEEE 802.1w)

El **Rapid Spanning Tree Protocol (RSTP)** es una evolución de STP que mejora los tiempos de convergencia.

- **Roles de puertos en RSTP:** además de *Root* y *Designated*, introduce *Alternate* y *Backup* para reaccionar más rápido ante fallos.
- **Estados simplificados:** RSTP reduce los estados de puerto a tres: *Discarding, Learning y Forwarding*.
- **Convergencia rápida:** permite que los puertos pasen directamente a *Forwarding* si detectan que pueden hacerlo sin riesgo de bucles (CCNA desde Cero, 2020).
- **Comandos básicos en Cisco IOS:**
    - spanning-tree mode rapid-pvst → activa RSTP en modo por VLAN.
    - show spanning-tree → muestra roles y estados de puertos bajo RSTP.

“RSTP reduce significativamente el tiempo de convergencia de la red, pasando de decenas de segundos a solo unos pocos” (CCNA desde Cero, 2020).

1.7 CONCEPTO DE BROADCAST

Un **broadcast** es un mensaje enviado a todos los dispositivos de un dominio de difusión. Cada red tiene una dirección de broadcast reservada, y los paquetes enviados a esa dirección son recibidos por todos los hosts. Aunque útil para descubrimiento, el exceso de broadcast puede saturar la red (IONOS, 2022).

TEMA 2. VLAN

TEORIA

2.1 VLAN

Una **VLAN** es una red lógica que permite segmentar una red física en múltiples dominios de broadcast independientes. Esto significa que los dispositivos dentro de una misma VLAN pueden comunicarse como si estuvieran en una red separada, aunque físicamente compartan el mismo switch (RedesZone, 2025).

> "Las VLAN permiten dividir una red física en varias redes lógicas, mejorando la seguridad y el rendimiento" (RedesInformaticas.org, 2024).

2.2TIPOS DE VLAN

- **VLAN por puerto:** asigna cada puerto del switch a una VLAN específica.
- **VLAN por MAC:** agrupa dispositivos según su dirección MAC.
- **VLAN por protocolo:** clasifica tráfico según el protocolo de capa 3.
- **VLAN por subred IP:** organiza dispositivos según su rango de direcciones IP (Guru99, 2024).

2.3 MODOS DE PUERTO DEL SWITCH (ACCESO Y TRONCAL)

Los puertos de un switch pueden configurarse en dos modos principales:

- **Acceso (Access Port):** pertenece a una sola VLAN y se conecta a dispositivos finales.
- **Troncal (Trunk Port):** transporta tráfico de múltiples VLAN a través de un solo enlace entre switches, usando etiquetas 802.1Q (Cisco, 2020).

2.4 CONTROL DE DOMINIOS DE BROADCAST

Cada VLAN constituye un **dominio de broadcast independiente**, lo que significa que las tramas de difusión solo circulan dentro de esa VLAN. Esto reduce la congestión y mejora la seguridad al aislar grupos de trabajo (RedesZone, 2025).

2.5 ENLACES TRONCALES

Los **enlaces troncales** permiten que múltiples VLAN se comuniquen entre switches. Se configuran con protocolos de encapsulación como **IEEE 802.1Q**.

> "Un enlace troncal transporta tráfico de todas las VLAN, salvo que se restrinja manualmente" (CCNA desde Cero, 2020).

2.6 CONFIGURACIÓN Y ADMINISTRACIÓN DE VLANS

La configuración básica en Cisco IOS incluye:

- **switchport mode access** → define un puerto como acceso.
- **switchport access vlan X** → asigna una VLAN a un puerto.
- **switchport mode trunk** → configura un puerto como troncal.
- **switchport trunk allowed vlan X,Y,Z** → especifica qué VLANs pasan por el troncal (Cisco, 2020).

2.7 PROTOCOLO VTP (VIRTUAL TRUNKING PROTOCOL)

El **VTP** es un protocolo propietario de Cisco que facilita la gestión de VLANs en redes grandes. Permite crear, modificar o eliminar VLANs en un switch y propagar esa información automáticamente a todos los switches del mismo dominio VTP (Cisco, 2018).

2.7.1 Modos de VTP

- **Servidor:** crea y administra VLANs, propagando la información.

- **Cliente:** recibe información de VLANs pero no puede crear ni modificar.
- **Transparente:** no participa en la propagación, pero permite configuración local.

"El protocolo VTP simplifica la administración de VLANs al centralizar su configuración en un switch" (CCNA desde Cero, 2020).

2.8 PROTOCOLO DE PUERTO DE ENLACE FRONTERIZO

El **VLAN Trunking Protocol (VTP)** es un protocolo de administración de VLAN que permite que la información de configuración de VLAN se propague automáticamente entre switches dentro de un mismo dominio VTP.

- **Función principal:** centralizar la gestión de VLANs, evitando configuraciones manuales en cada switch.
- **Modos de operación:**
    - **Servidor:** crea, modifica y elimina VLANs, propagando la información.
    - **Cliente:** recibe la información de VLANs pero no puede modificarla.
    - **Transparente:** no participa en la propagación, pero permite configuración local.
- **Beneficios:** simplifica la administración, reduce errores de configuración y asegura consistencia en redes grandes (Cisco, 2025; CCNA desde Cero, 2024).

"El protocolo VTP permite a los administradores configurar o modificar las VLAN en un solo conmutador y difundir esa información a todos los demás conmutadores de la red" (CCNA desde Cero, 2024).

2.9 CONFIGURACIÓN DE SWITCHES CON PUERTOS TRONCALES

Los **puertos troncales** son enlaces de capa 2 que transportan tráfico de múltiples VLAN entre switches. Se configuran con protocolos de encapsulación como **IEEE 802.1Q**.

2.9.1 Pasos básicos de configuración en Cisco IOS:

1. **Entrar al modo de configuración de interfaz:**

   Switch(config)# interface fastEthernet 0/1

2. **Configurar el puerto como troncal:**

   Switch(config-if)# switchport mode trunk

3. **Permitir VLANs específicas en el troncal:**

   Switch(config-if)# switchport trunk allowed vlan 10,20,30

4. **Verificar configuración:**

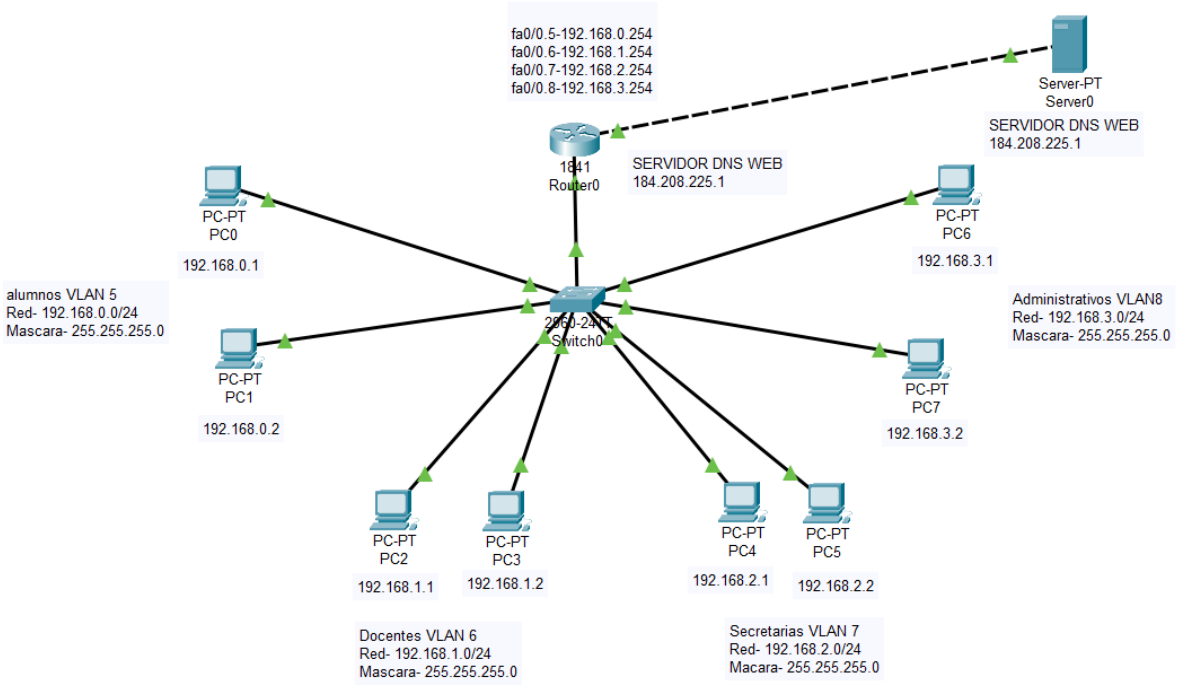
   Switch# show interfaces trunk

Consideraciones importantes:

- Los enlaces troncales transportan tráfico de todas las VLAN por defecto, salvo que se restrinja manualmente.
- Es recomendable definir un **VLAN nativa** para evitar problemas de seguridad.
- La combinación de **VTP + enlaces troncales** permite que las VLAN creadas en un switch servidor se propaguen automáticamente a través de los troncales hacia otros switches (RedesZone, 2025).

PRACTICAS

PRACTICA 1 RED CON CUATRO VLAN Y SERVIDOR DNS WEB Y DHCP EN EL ROUTER



Esta práctica consiste en configurar una red segmentada en cuatro VLANs, conectadas a un switch central y enlazadas a un router que proporciona los servicios de DHCP para todas las VLANs. Además, se incluye un servidor DNS-Web ubicado en una de las VLANs, accesible desde cualquier segmento de red. El objetivo es integrar segmentación lógica, enrutamiento inter-VLAN, asignación automática de direcciones IP y servicios de resolución de nombres y web en una infraestructura institucional.

La topología incluye un router (Router0), un switch (Switch0), ocho computadoras distribuidas en cuatro VLANs, y un servidor DNS-Web con dirección pública.

Las VLANs configuradas son:

- VLAN 5: alumnos Red: 192.168.0.0/24 Dispositivos: PC0 (192.168.0.1), PC1 (192.168.0.2)

- VLAN 6: docentes Red: 192.168.1.0/24 Dispositivos: PC2 (192.168.1.1), PC3 (192.168.1.2)
- VLAN 7: secretarias Red: 192.168.2.0/24 Dispositivos: PC4 (192.168.2.1), PC5 (192.168.2.2)
- VLAN 8: administrativos Red: 192.168.3.0/24 Dispositivos: PC6 (192.168.3.1), PC7 (192.168.3.2)

El servidor DNS-Web está ubicado en la VLAN 8 con dirección IP pública: 184.208.225.1.

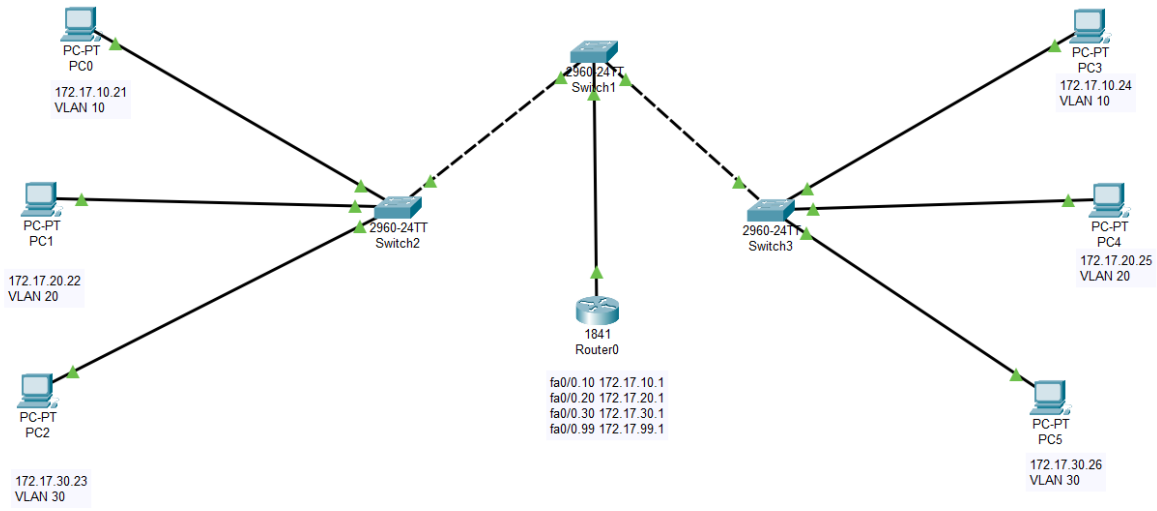
El router está configurado con subinterfaces para cada VLAN, utilizando encapsulación dot1Q, con las siguientes direcciones:

- fa0/0.5: 192.168.0.254
- fa0/0.6: 192.168.1.254
- fa0/0.7: 192.168.2.254
- fa0/0.8: 192.168.3.254

El servicio DHCP se configura directamente en el router, definiendo pools para cada VLAN, incluyendo dirección de red, máscara, puerta de enlace y servidor DNS. El switch se configura con puertos en modo acceso asignados a cada VLAN, y el enlace hacia el router se establece como troncal.

La práctica permite verificar que los dispositivos reciben su configuración IP automáticamente desde el router, que pueden resolver nombres mediante el servidor DNS, y que tienen acceso al contenido web alojado en el servidor. También se comprueba el correcto funcionamiento del enrutamiento inter-VLAN y la integración de servicios en una red institucional segmentada.

PRACTICA 2 RED CON 3 VLAN Y ENLACES TRONCALES Y ROUTER



Esta práctica consiste en configurar una red segmentada en tres VLANs distribuidas en múltiples switches, con enlaces troncales entre ellos y un router que permite la comunicación entre VLANs mediante enrutamiento inter-VLAN. El objetivo es demostrar cómo se puede mantener la segmentación lógica de usuarios y al mismo tiempo permitir la conectividad entre grupos mediante un router configurado con subinterfaces.

La topología incluye tres switches modelo 2960-24TT (Switch1, Switch2 y Switch3), un router (Router0) y seis computadoras distribuidas en tres VLANs. Los enlaces entre los switches y entre el switch principal y el router se configuran como troncales utilizando el protocolo IEEE 802.1Q.

Las VLANs configuradas son:

- VLAN 10 Red: 172.17.10.0/24 Dispositivos: PC0 (172.17.10.21), PC3 (172.17.10.24) Subinterfaz del router: fa0/0.10 – 172.17.10.1
- VLAN 20 Red: 172.17.20.0/24 Dispositivos: PC1 (172.17.20.22), PC4 (172.17.20.25) Subinterfaz del router: fa0/0.20 – 172.17.20.1
- VLAN 30 Red: 172.17.30.0/24 Dispositivos: PC2 (172.17.30.23), PC5 (172.17.30.26) Subinterfaz del router: fa0/0.30 – 172.17.30.1

Además, se configura una VLAN de administración (por ejemplo, VLAN 99) con la subinterfaz fa0/0.99 – 172.17.99.1 para gestionar los switches.

Cada puerto del switch donde se conectan los dispositivos finales se configura en modo acceso y se asigna a la VLAN correspondiente. Los enlaces entre los switches y entre el switch principal y el router se configuran en modo troncal para permitir el paso de tráfico de todas las VLANs.

La práctica permite verificar que los dispositivos de la misma VLAN pueden comunicarse entre sí, que los dispositivos de VLANs distintas pueden comunicarse a través del router, y que la segmentación lógica se mantiene. También se comprueba la correcta configuración de subinterfaces en el router, la encapsulación dot1Q y el funcionamiento del enrutamiento inter-VLAN. Esta práctica integra los conceptos de VLAN, enlaces troncales y enrutamiento en una red institucional distribuida.

TEMA 3. INTRODUCCIÓN A LAS REDES INALÁMBRICAS.

TEORIA

3.1 ESTÁNDARES APLICABLES (IEEE 802.11)

El estándar **IEEE 802.11** define las especificaciones para redes inalámbricas de área local (WLAN). Desde su primera versión en 1997, ha evolucionado en distintas variantes:

- **802.11b (1999):** opera en 2.4 GHz, con velocidades de hasta 11 Mbps.
- **802.11a (1999):** opera en 5 GHz, con velocidades de hasta 54 Mbps.
- **802.11g (2003):** combina 2.4 GHz con 54 Mbps.
- **802.11n (2009):** introduce MIMO, alcanzando hasta 600 Mbps.
- **802.11ac (2013):** opera en 5 GHz, con velocidades superiores a 1 Gbps.
- **802.11ax (Wi-Fi 6, 2019):** mejora eficiencia en entornos de alta densidad mediante OFDMA y MU-MIMO.

3.2 COMPONENTES DE INFRAESTRUCTURA INALÁMBRICA

Una WLAN requiere diversos elementos para su funcionamiento:

- **Puntos de acceso (AP):** dispositivos que permiten la conexión inalámbrica de los clientes.
- **Controladores inalámbricos:** gestionan múltiples AP en entornos empresariales.
- **Switches y routers:** proporcionan conectividad hacia la red cableada y servicios externos.
- **Clientes inalámbricos:** laptops, smartphones o IoT con tarjetas de red compatibles.

- **Antenas:** pueden ser omnidireccionales (cobertura amplia) o direccionales (cobertura focalizada).

“Los componentes de una WLAN incluyen puntos de acceso, clientes, antenas y controladores que garantizan la conectividad” (CCNA desde Cero, s.f.).

3.3 PLANEACIÓN DE UNA WLAN

La planeación de una WLAN implica analizar el entorno físico y las necesidades de los usuarios:

- **Estudio de sitio:** identificar interferencias, materiales de construcción y áreas de alta densidad.
- **Cobertura:** determinar ubicación y cantidad de AP para evitar zonas muertas.
- **Capacidad:** calcular el número de usuarios simultáneos y el tipo de aplicaciones que usarán.
- **Seguridad:** definir protocolos de autenticación y cifrado (WPA2/WPA3).
- **Escalabilidad:** prever crecimiento futuro de la red.

“La planificación Wi-Fi es el diseño de la funcionalidad WLAN para un espacio interior o exterior, con ubicación de AP y cálculo de cobertura” (EnBITCon, s.f.).

3.4 INSTALACIÓN Y CONFIGURACIÓN BÁSICA

Los pasos básicos para instalar y configurar una WLAN incluyen:

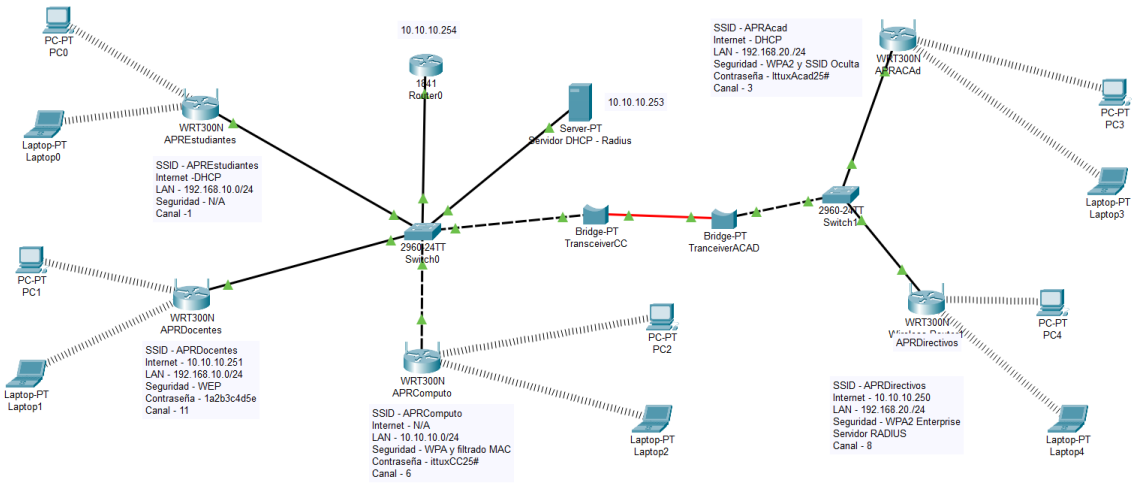
1. **Conectar el AP o router inalámbrico** a la red cableada.
2. **Definir un SSID (nombre de red)** para identificar la WLAN.
3. **Configurar seguridad:** habilitar WPA2 o WPA3 y establecer una contraseña robusta.

4. **Seleccionar canal y banda (2.4 o 5 GHz):** para minimizar interferencias.
5. **Actualizar firmware del AP/router:** para mejorar estabilidad y seguridad.
6. **Verificar conectividad:** probar acceso desde distintos dispositivos.

“La configuración básica de una WLAN incluye definir SSID, clave de acceso y parámetros de seguridad” (RedesZone, 2025).

PRACTICAS

PRACTICA 1 RED WLAN CON 5 APR 1 ROUTER 1 SERVIDOR DHCP RADIUS



Esta práctica consiste en configurar una red inalámbrica institucional compuesta por tres puntos de acceso (AP), un router, un switch central y un servidor DHCP. El objetivo es permitir la conexión de dispositivos inalámbricos distribuidos en tres redes Wi-Fi independientes, cada una con su propia configuración de seguridad, y gestionar la asignación automática de direcciones IP desde un servidor centralizado.

La topología incluye tres routers inalámbricos (modelo WRT300N), un switch (Switch0), un router (Router0), un servidor DHCP (Server0), tres laptops y tres computadoras de escritorio.

Configuración de los puntos de acceso:

- **APREestudiantes** SSID: APREestudiantes Internet: DHCP LAN: 192.168.10.0/24 Seguridad: sin cifrado Canal: 1 Dispositivos conectados: PC0, Laptop0
- **APRDocentes** SSID: APRDocentes Internet: IP estática (10.10.10.251) LAN: 192.168.10.0/24 Seguridad: WEP Contraseña: 1a2b3c4d5e Canal: 11 Dispositivos conectados: PC1, Laptop1

- **APRComputo** SSID: APRComputo Internet: sin conexión directa LAN: 10.10.10.0/24 Seguridad: WPA con filtrado MAC Contraseña: ittuxCC25# Canal: 6 Dispositivos conectados: PC2, Laptop2

Configuración del servidor DHCP:

- Server0 IP: 10.10.10.253 Servicio: DHCP Asigna direcciones IP a los dispositivos conectados a las tres redes inalámbricas

Configuración del router:

- Router0 IP: 10.10.10.254 Conectado al switch central Encargado del enrutamiento entre segmentos y salida a internet

El switch conecta los tres AP, el servidor y el router, permitiendo la comunicación entre todos los dispositivos. Los dispositivos inalámbricos se conectan a sus respectivos AP según el SSID configurado, y reciben su configuración IP automáticamente desde el servidor DHCP.

La práctica permite verificar la conectividad inalámbrica en redes con diferentes niveles de seguridad, la correcta asignación de direcciones IP, la segmentación por SSID, y el acceso a servicios de red mediante el router. También se comprueba la integración de redes inalámbricas con infraestructura cableada y la administración centralizada del direccionamiento IP en un entorno institucional.

TEMA 4. ENRUTADORES

TEORIA

4.1 COMPONENTES FÍSICOS Y LÓGICOS (CPU, MEMORIA, SO, INTERFACES)

Un router está compuesto por elementos físicos y lógicos que permiten el procesamiento y encaminamiento de paquetes:

- **CPU:** ejecuta procesos de enrutamiento y protocolos.
- **Memoria:** incluye RAM (almacena tablas de enrutamiento y configuración en ejecución), ROM (almacena el bootstrap y el sistema operativo básico), NVRAM (guarda la configuración de inicio) y Flash (almacena el IOS).
- **Sistema operativo (IOS):** software que controla el router y permite configuraciones mediante CLI.
- **Interfaces:** puertos Ethernet, FastEthernet, GigabitEthernet y seriales para conectar redes (Cisco Networking Academy, 2023).

“Los routers combinan hardware especializado y software IOS para ejecutar protocolos de enrutamiento y gestionar interfaces” (Cisco Networking Academy, 2023).

4.2 PROCESO DE ARRANQUE DEL ROUTER

El arranque de un router Cisco sigue cuatro pasos:

1. **POST (Power-On Self Test):** verifica hardware básico.
2. **Bootstrap:** cargado desde ROM, localiza y carga el IOS.
3. **Carga del IOS:** desde memoria Flash.
4. **Carga de configuración:** desde NVRAM; si no existe, inicia en modo setup (Cisco, 2020).

4.3 CONFIGURACIÓN BÁSICA MEDIANTE CLI

La configuración inicial se realiza en el **Command Line Interface (CLI)**:

- hostname Router1 → asigna nombre al dispositivo.
- enable secret clave → define contraseña de acceso privilegiado.
- interface g0/0 → accede a la interfaz.
- ip address 192.168.1.1 255.255.255.0 → asigna dirección IP.
- no shutdown → activa la interfaz.
- copy running-config startup-config → guarda configuración (Cisco, 2018).

4.4 CONSTRUCCIÓN DE TABLAS DE ENRUTAMIENTO

Las tablas de enrutamiento contienen información sobre redes conocidas y cómo alcanzarlas:

- **Redes conectadas directamente.**
- **Rutas estáticas configuradas manualmente.**
- **Rutas dinámicas aprendidas por protocolos (RIP, OSPF, EIGRP).** Cada entrada incluye destino, máscara, interfaz de salida y métrica (CCNA desde Cero, 2020).

4.5 ESTRATEGIA DE COMPARACIÓN DE IP Y MÁSCARA DE SUBRED

Un router determina si un host está en la misma red comparando la dirección IP con la **máscara de subred**. Ejemplo:

- IP: 192.168.1.10
- Máscara: 255.255.255.0 → El router identifica que pertenece a la red 192.168.1.0/24. Si la red destino difiere, el paquete se envía a otra interfaz o gateway (RedesZone, 2025).

4.6 QUÉ ES DNS (DOMAIN NAME SYSTEM)

El **DNS** traduce nombres de dominio (ej. www.google.com) en direcciones IP. Funciona como una “agenda telefónica” de Internet.

- **Servidores raíz, TLD y autoritativos** participan en la resolución.
- Mejora la usabilidad al permitir recordar nombres en lugar de números (IONOS, 2022).

4.7 CLASIFICACIÓN DE DIRECCIONES IP: PÚBLICAS Y PRIVADAS, CLASES A/B/C, IPV4 E IPV6

Direcciones públicas: asignadas por proveedores, accesibles en Internet.

Direcciones privadas: usadas en redes internas (ej. 192.168.x.x).

Clases:

- Clase A: 0.0.0.0 – 127.255.255.255
- Clase B: 128.0.0.0 – 191.255.255.255
- Clase C: 192.0.0.0 – 223.255.255.255

IPv4: 32 bits, ~4.3 mil millones de direcciones.

IPv6: 128 bits, espacio prácticamente ilimitado (Guru99, 2024).

4.8 SUBNETEO: DIVISIÓN EN SUBREDES, MÁSCARAS Y EJERCICIOS

El **subneteo (subnetting)** consiste en tomar una red principal y dividirla en subredes más pequeñas mediante el uso de **máscaras de subred**. Esto permite:

- Mejor **aprovechamiento de direcciones IP**.
- **Segmentación lógica** de departamentos o áreas.

- **Reducción de tráfico broadcast**.
- Mayor **seguridad y control** en la administración de la red (DudasyTextos, 2025).

“El subneteo es fundamental para dividir una red en segmentos más pequeños y manejables” (eClassVirtual, s.f.).

Máscaras de subred

La **máscara de subred** indica qué parte de la dirección IP corresponde a la red y qué parte a los hosts. Ejemplo:

- Dirección IP: 192.168.1.10
- Máscara: 255.255.255.0 (/24) → Red: 192.168.1.0 → Hosts disponibles: 254

Si se cambia la máscara a 255.255.255.192 (/26): → Se crean 4 subredes con 62 hosts cada una.

Fórmulas básicas

1. **Número de subredes:**

$$2^n$$

donde *n* = número de bits prestados.

2. **Número de hosts por subred:**

$$2^h - 2$$

donde *h* = número de bits para hosts.

Ejemplo:

- Red 192.168.1.0/24 → 256 direcciones totales.
- Si se subnetea con /26 → 64 direcciones por subred, 62 hosts utilizables.

Ejemplo práctico

Una empresa tiene la red 200.123.0.128/25 y necesita dividirla en subredes para tres departamentos:

- LAN A: 25 estaciones.
- LAN B: 14 estaciones.
- LAN C: 9 estaciones.

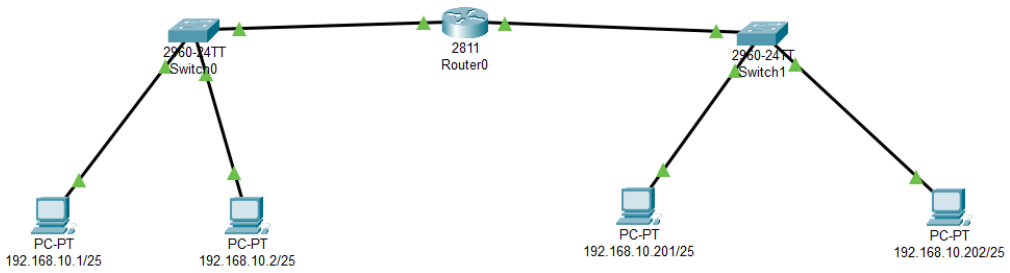
Solución (UPC, 2024):

- LAN A → máscara /27 (32 direcciones, 30 hosts).
- LAN B → máscara /28 (16 direcciones, 14 hosts).
- LAN C → máscara /28 (16 direcciones, 14 hosts).

Cada subred tiene su dirección de red, broadcast y rango de hosts asignados.

PRACTICAS

PRACTICA 1 RUTA ESTATICA CON UN 1 ROUTER



Esta práctica consiste en configurar una red segmentada en dos subredes utilizando un solo router, con direccionamiento estático en los dispositivos finales y enrutamiento estático entre interfaces. El objetivo es permitir la comunicación entre dos segmentos de red mediante rutas manuales, reforzando los conceptos de subneteo, gateway y control de tráfico.

Topología

- Router central: modelo 2811 (Router0), con dos interfaces activas.
- Switch0: conecta dos PCs con direcciones IP en la subred 192.168.10.0/25.
- Switch1: conecta dos PCs con direcciones IP en la subred 192.168.10.128/25.

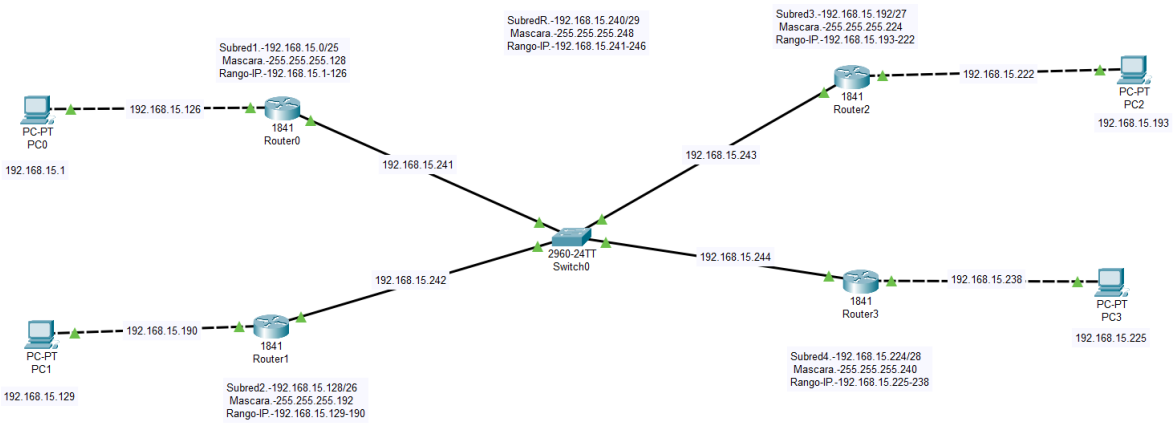
Segmentación de red

Se parte de la red base 192.168.10.0/24, dividida en dos subredes mediante VLSM:

- Subred A: 192.168.10.0/25 Rango de host: 192.168.10.1 a 192.168.10.126 Gateway: 192.168.10.126 (Router0 fa0/0) Dispositivos:
    - PC0: 192.168.10.1
    - PC1: 192.168.10.2

- Subred B: 192.168.10.128/25 Rango de host: 192.168.10.129 a 192.168.10.254 Gateway: 192.168.10.129 (Router0 fa0/1) Dispositivos:
    - PC2: 192.168.10.201
    - PC3: 192.168.10.202

PRACTICA 2 RED CON 5 SUBREDES CON VLMS DIRECCIONAMIENTO ESTATICO Y ENRUTAMIENTO ESTATICO



Esta práctica consiste en diseñar una red institucional segmentada en cinco subredes utilizando VLSM (Variable Length Subnet Masking), con asignación manual de direcciones IP y configuración de rutas estáticas en los routers. El objetivo es optimizar el uso del espacio de direcciones IP, asignando máscaras de subred según la cantidad de dispositivos por segmento, y establecer comunicación entre todas las subredes sin protocolos dinámicos.

Características principales:

- Se parte de una red base, por ejemplo: 192.168.15.0/24
- Se divide en cinco subredes con diferentes tamaños usando VLSM
- Cada subred se conecta a un router individual

- Los routers se interconectan a través de una red común y se configuran con rutas estáticas
- Las direcciones IP se asignan manualmente a cada dispositivo

Ejemplo de segmentación con VLSM:

- **Subred 1** Red: 192.168.15.0/25 Rango: 192.168.15.1–126 Router0: 192.168.15.126 PC0: 192.168.15.1 Enlace al switch: 192.168.15.241
- **Subred 2** Red: 192.168.15.128/26 Rango: 192.168.15.129–190 Router1: 192.168.15.190 PC1: 192.168.15.129 Enlace al switch: 192.168.15.242
- **Subred 3** Red: 192.168.15.192/27 Rango: 192.168.15.193–222 Router2: 192.168.15.222 PC2: 192.168.15.193 Enlace al switch: 192.168.15.243
- **Subred 4** Red: 192.168.15.224/28 Rango: 192.168.15.225–238 Router3: 192.168.15.238 PC3: 192.168.15.225 Enlace al switch: 192.168.15.244
- **Subred 5 (interconexión)** Red: 192.168.15.240/29 Rango: 192.168.15.241–247 Switch central: 2960-24TT Conecta todos los routers

Configuración de rutas estáticas (ejemplo en Router0):

ip route 192.168.15.128 255.255.255.192 192.168.15.242

ip route 192.168.15.192 255.255.255.224 192.168.15.243

ip route 192.168.15.224 255.255.255.240 192.168.15.244

Verificación:

- Cada PC debe tener como puerta de enlace la IP del router correspondiente
- Se realizan pruebas de conectividad con ping entre PCs de distintas subredes
- Se valida la tabla de enrutamiento con show ip route en cada router

TEMA 5. ENRUTAMIENTO ESTÁTICO Y DINÁMICO

TEORIA

5.1 CONFIGURACIÓN Y VERIFICACIÓN DE INTERFACES

Los **routers** requieren que sus interfaces estén configuradas con direcciones IP y máscaras de subred para poder enrutar paquetes.

- **Configuración básica en Cisco IOS:**
  - Router(config)# interface g0/0
  - Router(config-if)# ip address 192.168.1.1 255.255.255.0
  - Router(config-if)# no shutdown
- **Verificación:**
  - show ip interface brief → muestra estado de interfaces.
  - ping → prueba conectividad.
  - show running-config → confirma parámetros activos.

“La configuración de interfaces es el primer paso para habilitar la conectividad en un router” (Cisco, 2020).

5.2 PROCESO DE BÚSQUEDA EN LA TABLA DE ENRUTAMIENTO

El router utiliza la **tabla de enrutamiento** para decidir cómo enviar un paquete:

1. **Lee la dirección IP destino.**
2. **Aplica el algoritmo de longest prefix match** (prefijo más largo).
3. **Selecciona la ruta más específica.**
4. **Encamina el paquete por la interfaz de salida.** Si no encuentra coincidencia, usa la **ruta por defecto** o descarta el paquete.

“Los routers comparan la dirección IP destino con la tabla de enrutamiento y seleccionan la ruta más específica” (CCNA desde Cero, 2020).

5.3 MÉTRICAS Y DISTANCIA ADMINISTRATIVA

- **Métrica:** valor que indica la preferencia de una ruta.
    - RIP → número de saltos.
    - OSPF → costo basado en ancho de banda.
    - EIGRP → fórmula compuesta (ancho de banda, retardo, carga, confiabilidad).
- **Distancia administrativa (AD):** nivel de confianza en una ruta.
    - Conectada directamente: AD = 0
    - Estática: AD = 1
    - EIGRP: AD = 90
    - OSPF: AD = 110
    - RIP: AD = 120

“La distancia administrativa define qué protocolo se prefiere cuando existen múltiples rutas hacia el mismo destino” (Cisco Networking Academy, 2023).

5.4 ENRUTAMIENTO ESTÁTICO: RUTAS POR DEFECTO, RESUMEN, MODIFICACIÓN, VERIFICACIÓN

- **Ruta estática:** configurada manualmente.

  ip route 192.168.2.0 255.255.255.0 192.168.1.2

- **Ruta por defecto:** usada cuando no existe ruta específica.

  ip route 0.0.0.0 0.0.0.0 192.168.1.254

- **Resumen de rutas:** agrupa varias redes en una sola entrada.
- **Verificación:**
    - show ip route → muestra rutas activas.

- traceroute → verifica el camino hacia un destino.

“El enrutamiento estático es simple y confiable, pero no escala bien en redes grandes” (Cisco, 2018).

5.5 ENRUTAMIENTO DINÁMICO: RIP, EIGRP, OSPF

Los protocolos dinámicos permiten que los routers aprendan rutas automáticamente:

- **RIP (Routing Information Protocol):**
  - Métrica: número de saltos.
  - AD = 120.
  - Limitado a 15 saltos.
- **EIGRP (Enhanced Interior Gateway Routing Protocol):**
  - Protocolo híbrido de Cisco.
  - Métrica: ancho de banda y retardo.
  - AD = 90.
  - Convergencia rápida.
- **OSPF (Open Shortest Path First):**
  - Protocolo de estado de enlace.
  - Métrica: costo basado en ancho de banda.
  - AD = 110.
  - Escalable y ampliamente usado en redes empresariales.

“Los protocolos dinámicos permiten que los routers se adapten automáticamente a cambios en la topología” (CCNA desde Cero, 2020).

5.6 PROTOCOLO FTP

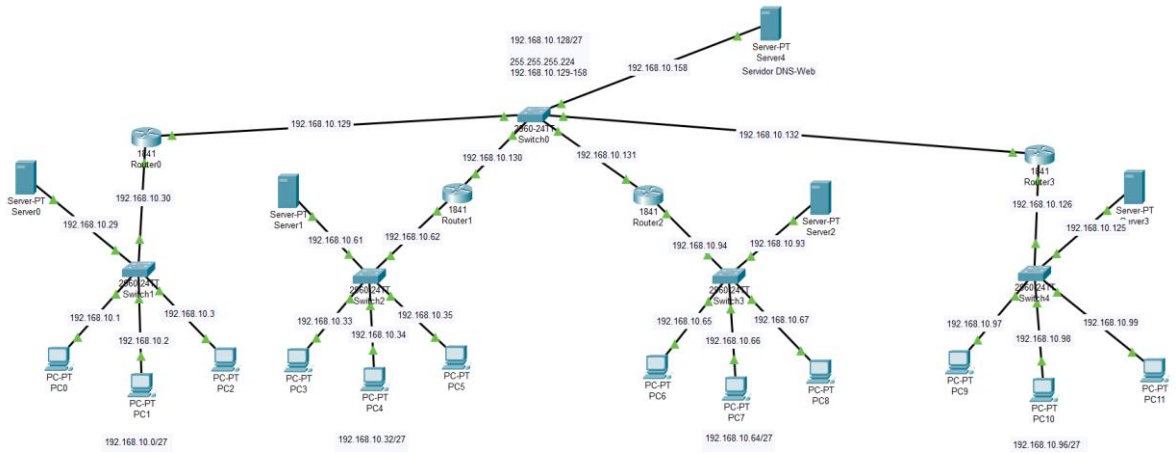
El **File Transfer Protocol (FTP)** es un protocolo de aplicación que permite la transferencia de archivos entre cliente y servidor.

- Opera sobre TCP (puertos 20 y 21).
- Modos:
    - **Activo:** el servidor inicia la conexión de datos.
    - **Pasivo:** el cliente inicia la conexión de datos (más usado en firewalls).
- Usos:
    - Subida y descarga de archivos.
    - Configuración de servidores.
    - Respaldos de configuración de routers y switches.

“FTP es uno de los protocolos más antiguos y utilizados para transferir archivos en redes TCP/IP” (IONOS, 2022).

PRACTICAS

PRACTICA 1 RED CON 5 SUBREDES CON DIRECCIONAMIENTO DINAMICO Y ENRUTAMIENTO DINAMICO CON SERVIDOR DNS WEB



Esta red está segmentada en cinco subredes mediante VLSM sobre la red 192.168.10.0/24. Cada subred tiene su propio router y servidor DHCP, con asignación automática de IPs. Los routers se interconectan a través de una red troncal y comparten rutas mediante RIP versión 2. Un servidor DNS-Web centralizado permite la resolución de nombres y servicios web internos.

Subredes configuradas:

- Subred1: 192.168.10.0/27 → PC0–PC2, Server0, DHCP en Router0
- Subred2: 192.168.10.32/27 → PC3–PC5, Server1, DHCP en Router1
- Subred3: 192.168.10.64/27 → PC6–PC8, Server2, DHCP en Router2
- Subred4: 192.168.10.96/27 → PC9–PC11, Server3, DHCP en Router3
- Subred5 (troncal): 192.168.10.128/27 → Switch0, enlaces a los cuatro routers y al servidor DNS-Web (192.168.10.158)

Configuración clave:

- DHCP configurado en cada router para su subred local
- RIP v2 activado en todos los routers (version 2, no auto-summary)

- Servidor DNS-Web con IP fija 192.168.10.158 y servicios HTTP/DNS activos
- Cada PC recibe IP automáticamente y tiene como gateway la IP LAN del router correspondiente

CONCLUSIÓN

Al finalizar las prácticas se logró comprender la importancia del subneteo y las direcciones de broadcast para organizar y delimitar la comunicación en cada subred. Se aplicaron técnicas de configuración, se utilizaron herramientas de simulación y se reforzó la relevancia de implementar protocolos de enrutamiento, tipos de seguridad y servicios de red para garantizar la conectividad y funcionalidad de la infraestructura. Estas actividades permitieron consolidar los aprendizajes del semestre y desarrollar competencias prácticas en el área de interconectividad de redes.

REFERENCIAS

Arias, V. P. (2014). *Convergencia STP*. Prezi. Recuperado de https://prezi.com/j0lckzfytraa/convergencia-stp/

CCM – Museo de Internet. (2023, septiembre 30). *IEEE 802.11: qué es, WiFi, características, para qué sirve*. Recuperado de https://es.ccm.net/aplicaciones-e-internet/museo-de-internet/enciclopedia/12004-introduccion-a-wifi-802-11-o-wifi/

CCNA desde Cero. (2020). *Enlaces troncales de VLAN*. Recuperado de https://ccnadesdecero.es/enlaces-troncales-vlan/

CCNA desde Cero. (2020). *Funcionamiento de STP*. Recuperado de https://ccnadesdecero.es/funcionamiento-stp/

CCNA desde Cero. (2020). *Protocolos de enrutamiento dinámico: RIP, EIGRP y OSPF*. Recuperado de https://ccnadesdecero.es/protocolos-enrutamiento-dinamico/

CCNA desde Cero. (2020). *Spanning Tree Protocol (STP): Qué hace y cómo funciona*. Recuperado de https://ccnadesdecero.es/spanning-tree-protocol-stp-como-funciona/

CCNA desde Cero. (2020). *Tablas de enrutamiento y búsqueda de rutas*. Recuperado de https://ccnadesdecero.es/tablas-enrutamiento-subneteo/

CCNA desde Cero. (2024). *¿Qué es VTP (VLAN Trunking Protocol)?: Comprende su función*. Recuperado de https://ccnadesdecero.es/vtp-vlan-trunking-protocol-que-es/

CCNA desde Cero. (s.f.). *Componentes de las redes WLAN*. Recuperado de https://ccnadesdecero.es/componentes-redes-wlan/

Cisco Community. (2025). *Spanning Tree Protocol Overview*. Recuperado de https://community.cisco.com/t5/blogs-routing-y-switching/spanning-tree-protocol-overview/ba-p/5242520

Cisco Networking Academy. (2023). *Introducción a routers y sus componentes*. Recuperado de https://www.netacad.com/es/courses/networking

Cisco Networking Academy. (2023). *Métricas y distancia administrativa en protocolos de enrutamiento*. Recuperado de https://www.netacad.com/es/courses/networking

Cisco. (2018). *Configuración básica de routers Cisco mediante CLI*. Recuperado de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5760-configure-stp-settings-on-a-switch-through-the-cli.html

Cisco. (2018). *Configuración de los parámetros de STP en un switch a través de la CLI*. Recuperado de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5760-configure-stp-settings-on-a-switch-through-the-cli.html

Cisco. (2018). *Configuración de rutas estáticas en routers Cisco*. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/routing/118978-config-static.html

Cisco. (2020). *Configuración de los parámetros de interfaz de puerto a VLAN en un switch a través de la CLI*. Recuperado de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5653-configure-port-to-vlan-interface-settings-on-a-switch-throug.html

Cisco. (2020). *Configuración y verificación de interfaces en routers Cisco*. Recuperado de https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-12-2-mainline/47121-router-boot.html

Cisco. (2020). *Proceso de arranque de routers Cisco*. Recuperado de https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-12-2-mainline/47121-router-boot.html

Cisco. (2025). *Explicación del protocolo troncal de VLAN (VTP)*. Recuperado de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.html

EnBITCon GmbH. (s.f.). *¿Qué es la planificación WLAN?*. Recuperado de https://www.enbitcon.es/blog/que-es-una-planificacion-wifi/

Guru99. (2024). *Direcciones IP: públicas, privadas, IPv4 e IPv6*. Recuperado de https://www.guru99.com/es/ip-address-types.html

Guru99. (2024). *Protocolo VLAN Trunking: ¿Qué es VTP en redes y beneficios?*. Recuperado de https://www.guru99.com/es/vlan-trunking-protocol.html

Guru99. (2024). *STP: explicación del protocolo de árbol de expansión*. Recuperado de https://www.guru99.com/es/stp-spanning-tree-protocol-examples.html

IONOS. (2022). *Broadcast: definición y funcionamiento de la conexión multipunto*. Recuperado de https://www.ionos.mx/digitalguide/servidores/know-how/broadcast/

RedesZone. (2025). *Cómo funciona la máscara de subred y comparación de IP*. Recuperado de https://www.redeszone.net/tutoriales/redes-cable/mascara-subred-ip/

RedesZone. (2025). *Qué es un enlace troncal o trunk y cómo configurarlo en un switch*. Recuperado de https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/

RedesZone. (2025, agosto 25). *Cómo configurar tu red doméstica y WiFi desde cero paso a paso*. Recuperado de https://www.redeszone.net/tutoriales/redes-cable/configurar-red-domestica-desde-cero/

RedTauros. (s.f.). *Spanning Tree Protocol*. Recuperado de http://www.redtauros.com/Clases/Redes_II/07_Spanning_Tree.pdf

Studocu. (s.f.). *Unidad 1 – Conmutación y enrutamiento de redes*. Recuperado de https://www.studocu.com/es-mx/document/instituto-tecnologico-latinoamericano/conmutacion-y-enrutamiento-de-redes/unidad-1/39395931