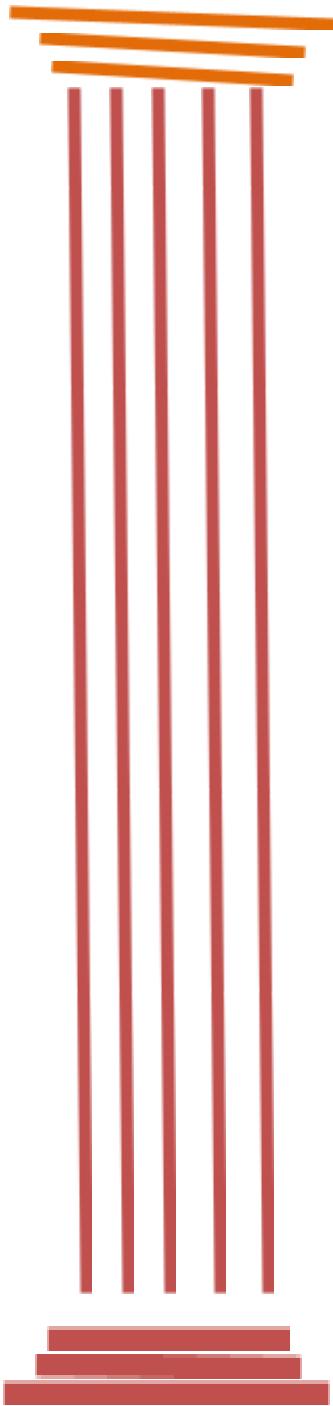




S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO de Tuxtepec



ACTIVIDAD:
Reporte

PRESENTAN:
Azamar Ortega Flor Itzel

DOCENTE:
Julio Aguilar Carmona

CARRERA:
INGENIERIA INFORMÁTICA

Diciembre 2025



Introducción

La configuración de redes constituye uno de los pilares fundamentales en el funcionamiento de cualquier infraestructura informática moderna. A través de ella se establecen parámetros esenciales como direcciones IP, máscaras de subred, gateways, servidores DNS, así como mecanismos de identificación, segmentación y comunicación entre dispositivos. Estos elementos permiten que los equipos puedan interactuar de forma eficiente, segura y organizada dentro de una red.

Además, comprender conceptos como el subnetting, el enrutamiento estático y dinámico, las VLANs y la configuración de switches es indispensable para el diseño, administración y optimización de redes tanto pequeñas como empresariales. Este documento recopila y explica de manera integral estos aspectos, así como actividades prácticas que permiten aplicar los conocimientos en entornos simulados, fortaleciendo las competencias necesarias para la gestión de redes moderna

Parametros de Configuracion de Red.

La configuración de red es el proceso de establecer las políticas, los controles y los flujos de datos que permiten que los dispositivos y sistemas se comuniquen a través de una red informática, es decir, implica asignar a cada dispositivo una dirección IP la cual puede ser estática o dinámica, una máscara de subred, un gateway predeterminado, y en ocasiones un servidor DNS u otros valores de red.

Esta configuración comprende todos los componentes físicos y virtuales de hardware y software de una red y los protocolos que dictan cómo se mueven los datos entre ellos.

Como se ha mencionado anteriormente, la configuración de red consta de distintos parámetros los cuales son:

- **Dirección IP:** Es una serie de números utilizados para identificar una interfaz de red de un equipo en una red local o Internet. En la versión de IPv4 (siendo la más utilizada) se codifica este número en 32 bits y generalmente se lo representa por 4 números separados por puntos (por ejemplo: 192.168.0.1), cada número entre 0 y 255. Mientras que en la versión IPv6 extiende este espacio de direcciones a 128 bits y las direcciones se representan generalmente por una serie de números hexadecimales separados por dos puntos (por ejemplo: 2001:0db8:13bb:0002:0000:0000:0000:0020 o su versión corta 2001:db8:13bb:2::20).
- **Máscara de Subred:** Define qué porción de una dirección IP corresponde a la red, el resto especifica el equipo.
- **Gateway:** Es la ruta por defecto que usa un dispositivo para salir de su subred y comunicarse con redes externas.
- **Servidor DNS:** Su función principal es traducir los nombres de dominio legibles por humanos en las direcciones IP numéricas que las computadoras usan para conectarse entre sí.

Todos estos parámetros en conjunto permiten que los nodos “se ubiquen” correctamente en la red, sepan cuándo un destino pertenece a su misma red o debe usarse el gateway, y puedan intercambiar información de forma ordenada.

Estrategia que usa el cómputo para identificar si está en una red.

La detección de redes es una búsqueda automática que localiza y realiza un seguimiento de todos los dispositivos, también conocidos como nodos de red, que están conectados a una red; también ayuda a visualizar que tienen acceso los dispositivos y cómo interactúan entre sí.

Este proceso suele incluirse en la primera y segunda fase de un proceso de supervisión de red. Con una herramienta de detección de redes, los administradores pueden crear inventarios de dispositivos, cambiar las políticas de acceso a los mismos y obtener visibilidad de la infraestructura de una red.

La asignación y uso de direcciones IP y direcciones MAC únicas para cada dispositivo, junto con protocolos de comunicación específicos es la estrategia principal que utiliza el cómputo para identificar si está en una red.

Clasificación de direcciones IP.

Anteriormente se ha mencionado el término “Dirección IP” el cual es una representación numérica que identifica una interfaz concreta de manera única en la red.

Estas direcciones cuentan con una clasificación que los identifica y diferencia a cada uno:

- **Clase A:** En las direcciones de clase A los primeros ocho bits de la dirección, o el primer punto decimal, son la parte de la red, mientras que la parte restante es la del host. Hay alrededor de 128 redes de clase A posibles.
- **Clase B:** En las direcciones de clase B los primeros 16 bits de la dirección son la parte de la red. Todas las redes de clase B tienen el primer bit a 1 y el segundo bit a 0. Si dividimos la dirección en octetos, nos queda que las direcciones 128.0.0.0 a 191.255.0.0 corresponden a redes de clase B. Hay 16 384 redes de clase B posibles.
- **Clase C:** En este tipo de clase los dos primeros bits están puestos a 1 y el tercero a 0. Eso hace que los primeros 24 bits de la dirección sean la parte de la red, y el resto, la del *host*. Las direcciones de red de clase C van desde 192.0.0.0 a 223.255.255.0. Hay más de 2 millones de redes de clase C posibles.

Subnetting.

El subnetting o subneteo, es el proceso de segmentar una red en partes más pequeñas, esto con la finalidad de gestionar de una mejor manera el tráfico que puede haber en una red, además de garantizar un mejor aprovechamiento de las direcciones IP que haya disponible.

Esta actividad se basa en dividir una dirección IP en dos partes siendo la primera el identificador de red esta determina a qué red pertenece la dirección. La segunda parte es el identificador de host, aquí se especifica un dispositivo dentro de la red. Para hacer subnetting, se usan máscaras de subred. Estas definen cuántos bits pertenecen a la red y cuántos a los host.

Simulación de Red LAN.

Una red de área local (LAN) es una red contenida dentro de una pequeña zona geográfica, normalmente dentro de un mismo edificio. Las redes WiFi domésticas y las redes de pequeñas empresas son algunos ejemplos comunes de LAN.

En clase elaboramos una pequeña simulación que permite validar diseño de subredes, VLANs y enrutamiento, probar topologías redundantes, practicar comandos y procedimientos sin hardware físico, y detectar errores de configuración.

Algunas de las herramientas que son utilizadas para simular este tipo de red son:

- Cisco Packet Tracer.
- GNS3.
- EVE-NG.

Enrutamiento Estático y Dinámico.

Antes de conocer cuál es la diferencia entre estos dos tipos de enrutamiento, hay que conocer qué es el enrutamiento.

Esta acción es el proceso de selección de una ruta a través de una o más redes.

En las redes de conmutación de paquetes, como Internet, el enrutamiento selecciona distintas rutas para que los paquetes del Protocolo de Internet (IP) vayan desde su origen hasta su destino. Estas decisiones de enrutamiento en Internet las llevan a cabo piezas especializadas de hardware de red conocidas como enrutadores. Esta acción se lleva a cabo a través de tablas de enrutamiento internas para tomar decisiones acerca de cómo enrutar los paquetes por las rutas de red.

Enrutamiento estático: Este tipo de enrutamiento es elaborado manualmente, es decir, aquel en el que el administrador de la red debe encargarse de configurar cada uno de los routers que forman la misma. Cuando se lleva a cabo este tipo de enrutamiento hay que acceder a cada router, configurarlo individualmente y enseñarle cada una de las rutas existentes.

Enrutamiento Dinámico: Este tipo de enrutamiento es automático, es decir se basa en la utilización o empleo de protocolos de enrutamiento con el fin de automatizar el intercambio y la actualización de las tablas de enrutamiento de cada uno de los routers. Estos protocolos comparten las tablas de enrutamiento de forma automática con los routers cercanos, lo que hace que su utilización sea recomendada para redes grandes.

VLANS.

También conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física, haciendo uso de switches gestionables que soporta VLANs para segmentar adecuadamente la red. También es muy importante que los routers que utilicemos soporten VLAN, de lo contrario, no podremos gestionarlas todas ni permitir o denegar la comunicación entre ellas.

Esto se logra agrupando dispositivos para que funcionen como si estuvieran en una red independiente, lo que mejora la seguridad, el rendimiento y la gestión de la red, y separa el tráfico entre diferentes grupos o tipos de datos.

Configuración de Switches.

Los switches son dispositivos utilizados para conectar varios equipos en la misma red. En una red diseñada correctamente, los switches LAN son responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red.

Un switch se configura para controlar, optimizar y asegurar el funcionamiento de una red local (LAN); aunque un switch puede funcionar de manera básica sin configuración, configurarlo permite aprovechar sus capacidades avanzadas. Los pasos para configurar un switch son:

- Inspección del hardware: Verificar el número de modelo del switch.
- Configuración de la IP de administración: configurar el nombre de host del switch, quizás se deba elegir una denominación más profesional y estándar. Siguiendo los lineamientos sobre nombres establecidos por la empresa y se asigna una dirección IP en la VLAN de administración.
- Verificar el número de revisión de VTP: Introducir el comando `show vtp status` para ver los números de revisión del protocolo de enlace troncal virtual (VTP).
- Configurar los puertos de acceso.
- Configurar los puertos del enlace troncal.
- Configurar los puertos de acceso.
- Configurar la línea VTY.

Compuertas Troncales.

Un puerto troncal es un tipo de puerto de conmutador de red que transporta tráfico de varias VLAN simultáneamente. A diferencia de un puerto de acceso , que solo gestiona el tráfico de una VLAN, un puerto troncal puede enviar datos desde varias VLAN a través de una sola conexión. Esto ayuda a optimizar la comunicación de red, estos funcionan mediante etiquetado VLAN, un proceso fundamental para facilitar la comunicación entre VLAN.

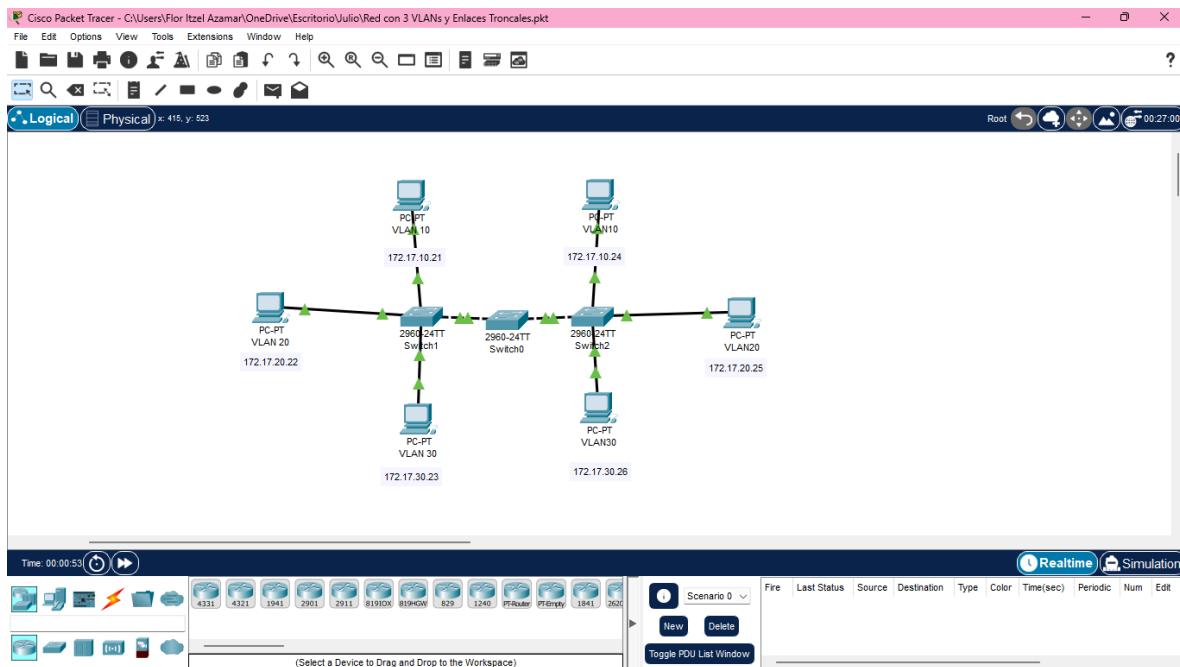
Redes inalámbricas.

Una red inalámbrica se refiere a una red informática que utiliza conexiones de radiofrecuencia (RF) entre nodos de la red, estas redes son sistemas de comunicación que conectan dispositivos sin necesidad de cables, utilizando ondas de radiofrecuencia para transmitir datos entre ellos. Facilitan la movilidad y conectividad de dispositivos como ordenadores, teléfonos y tabletas, y su funcionamiento se basa en elementos como puntos de acceso (routers) y adaptadores inalámbricos en los dispositivos. Aunque ofrecen ventajas como facilidad de instalación y movilidad, presentan desafíos como la seguridad y la susceptibilidad a interferencias.

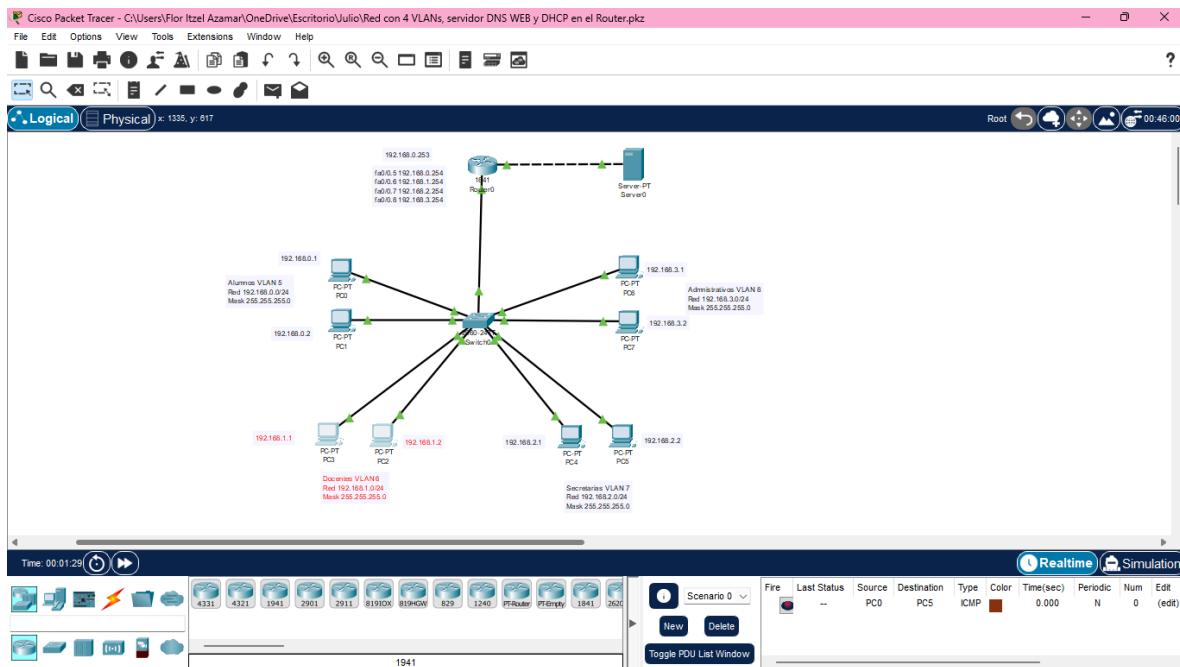
Actualmente las redes inalámbricas son una solución popular para hogares, empresas y redes de telecomunicaciones.

Anexos.

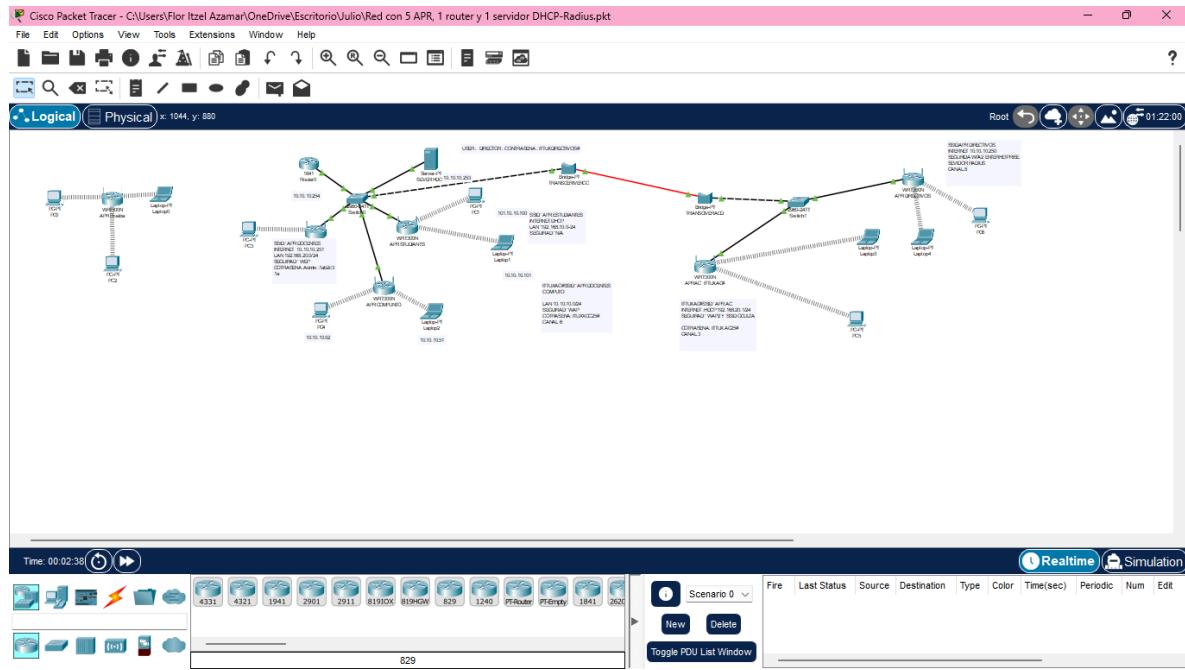
Actividad: Red con 3 VLANs y Enlaces Troncales



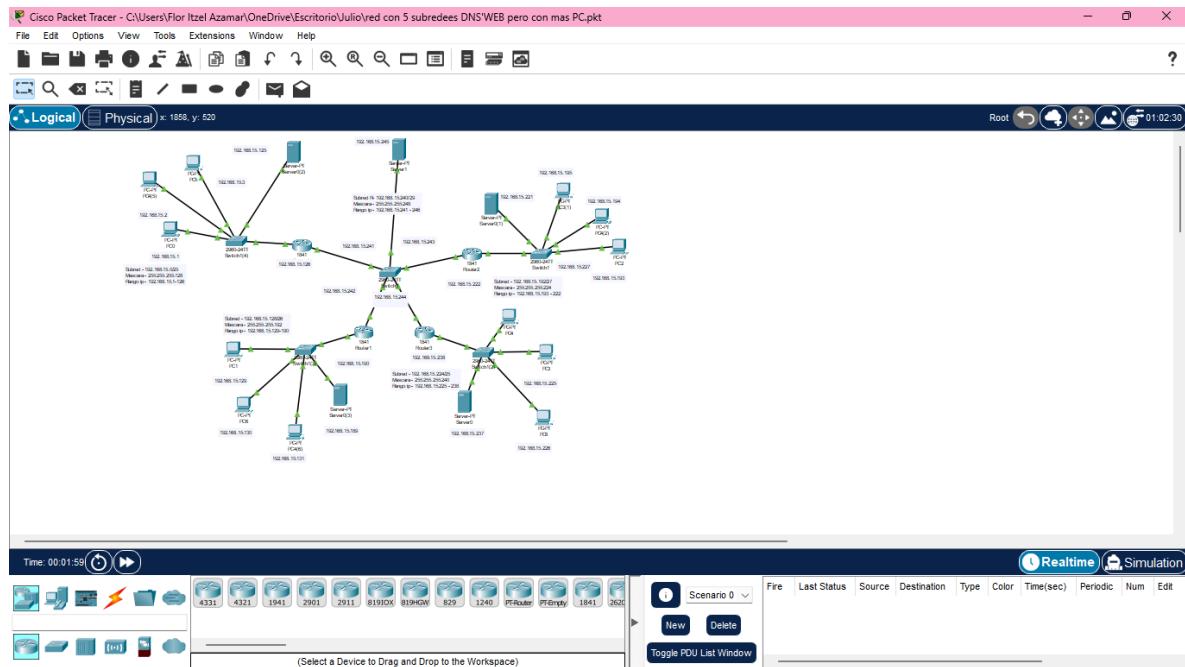
Actividad: Red con 4 VLANs, servidor DNS WEB y DHCP en el Router.



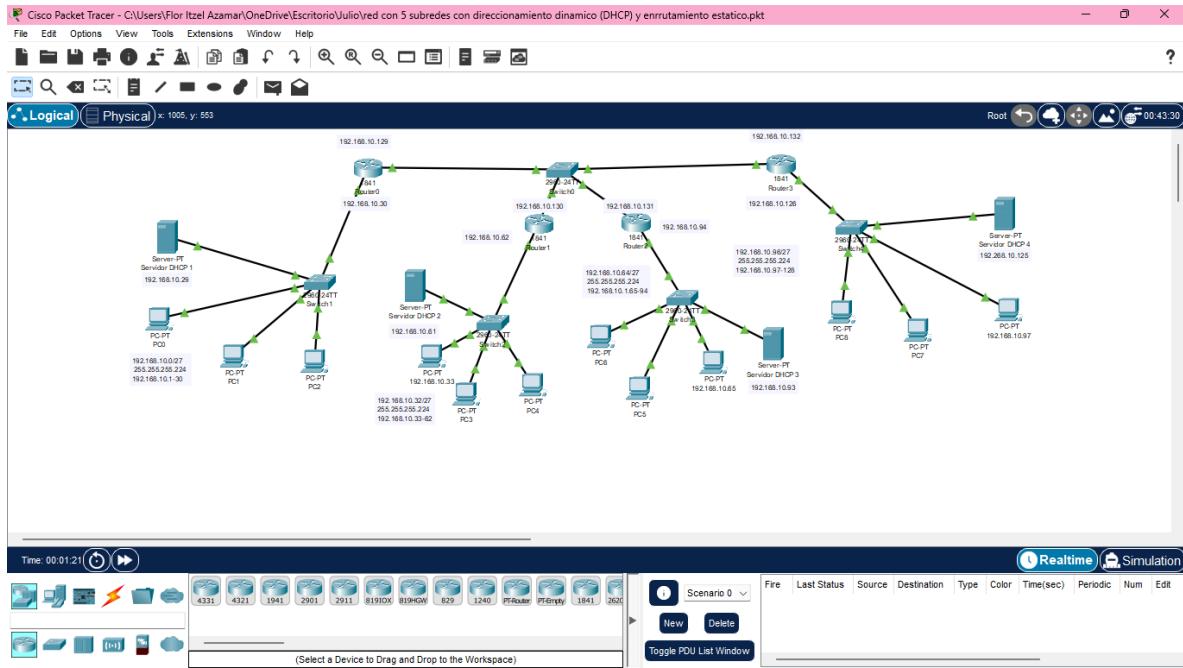
Actividad: Red con 5 APR, 1 router y 1 servidor DHCP-Radius



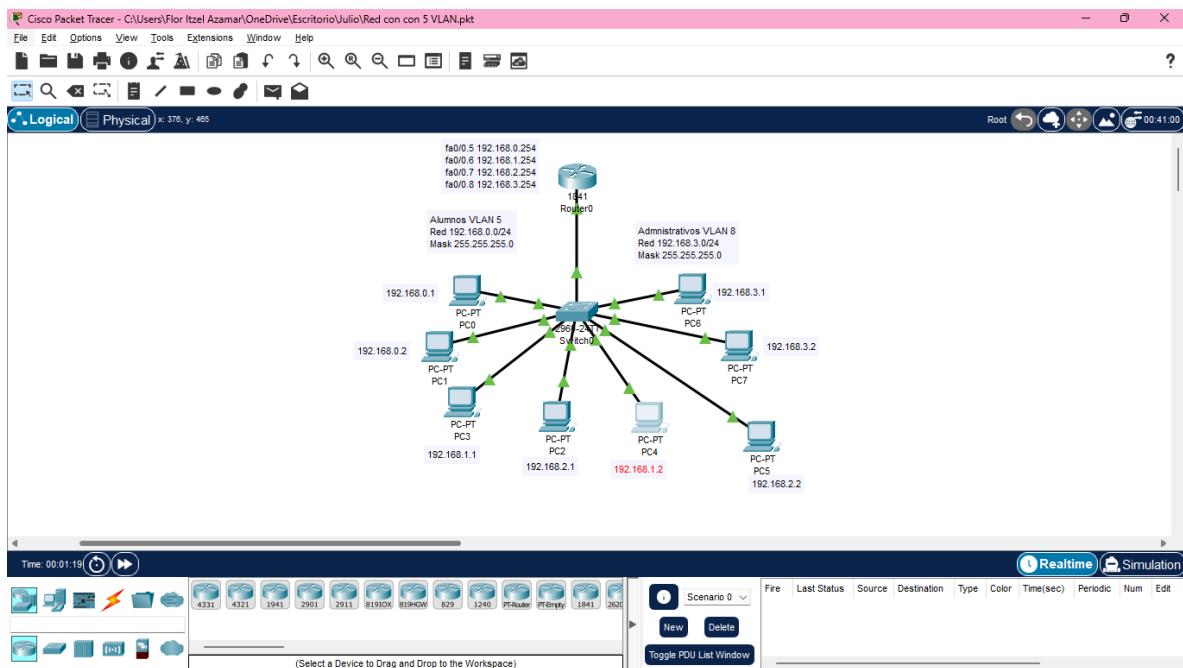
Actividad: Red con 5 subredes DNS'WEB.



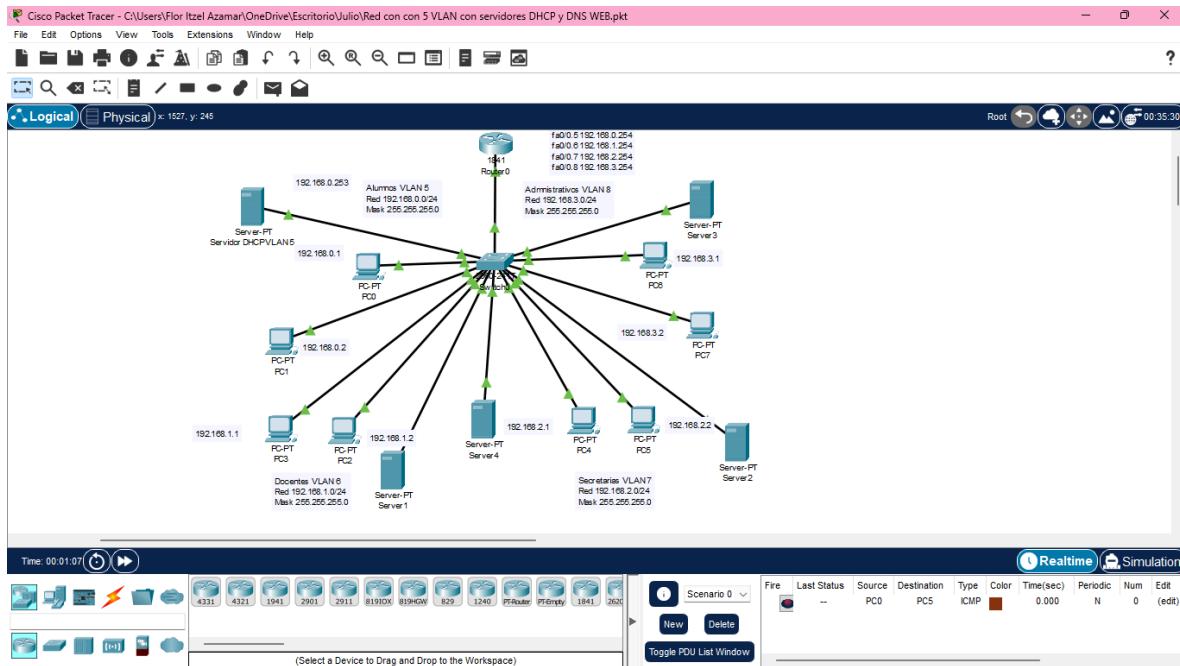
Actividad: Red con 5 subredes con direccionamiento dinamico (DHCP) y enrutamiento estatico.



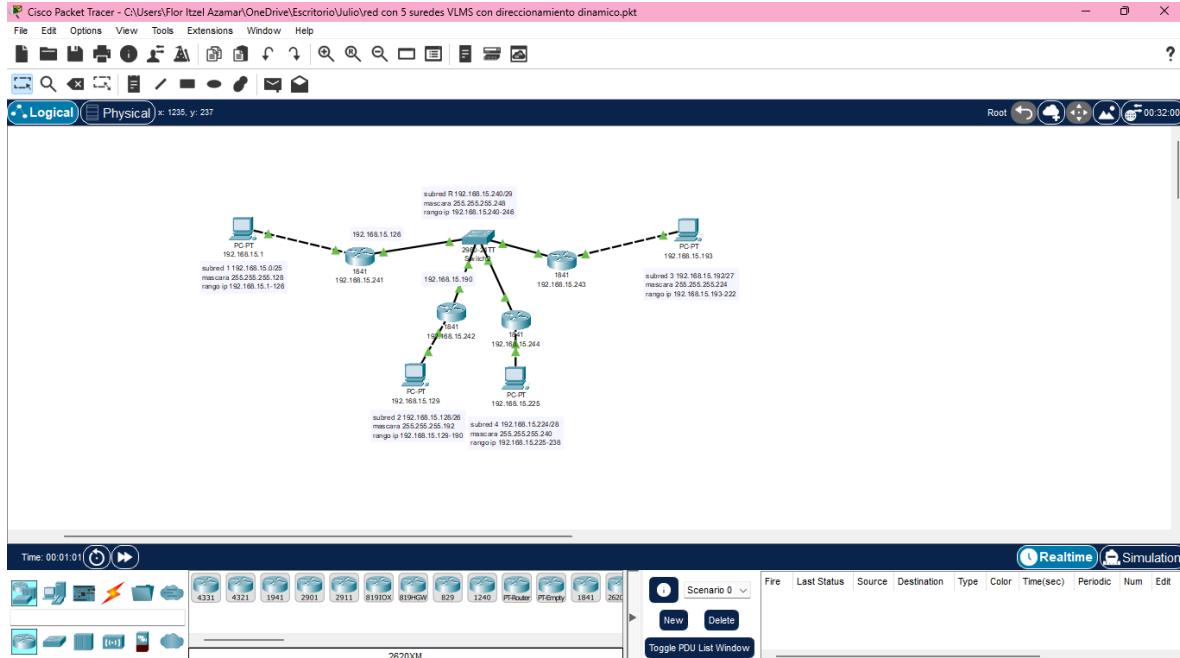
Actividad: Red con con 5 VLAN.



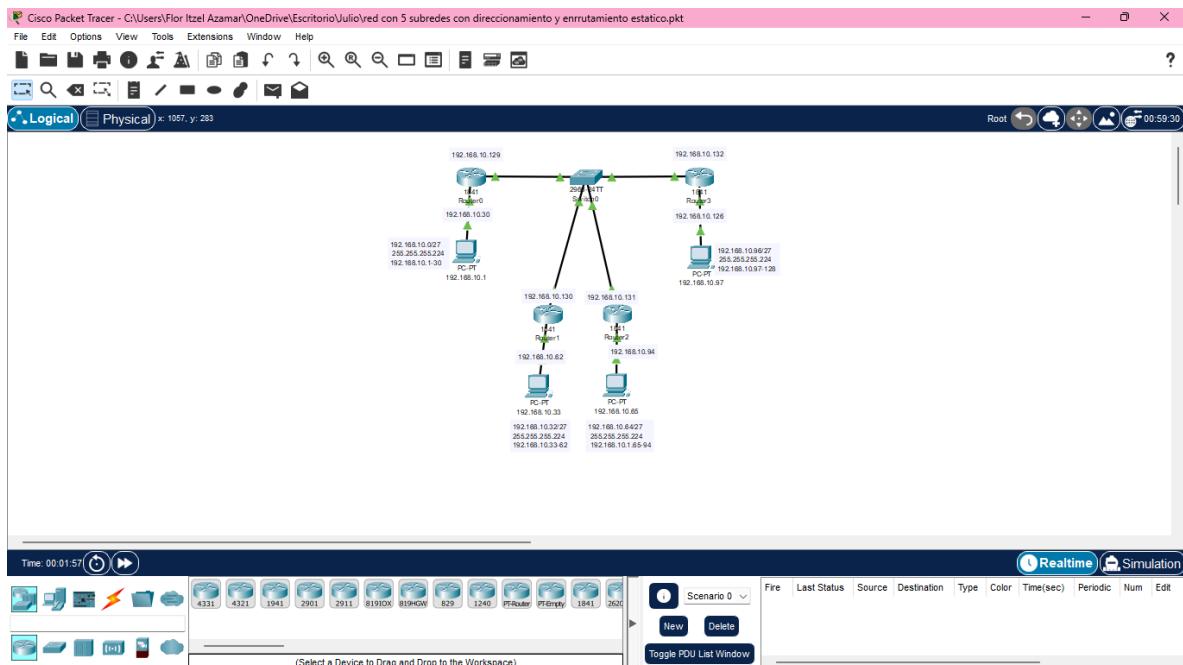
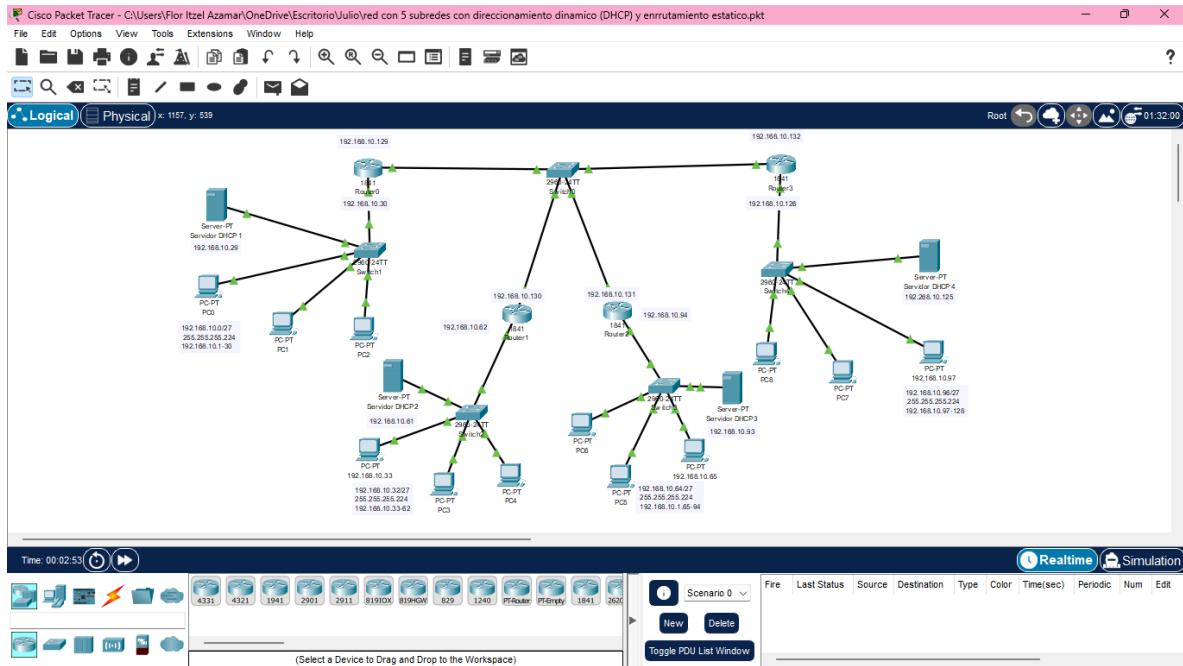
Actividad: Red con 5 VLAN con servidores DHCP y DNS WEB



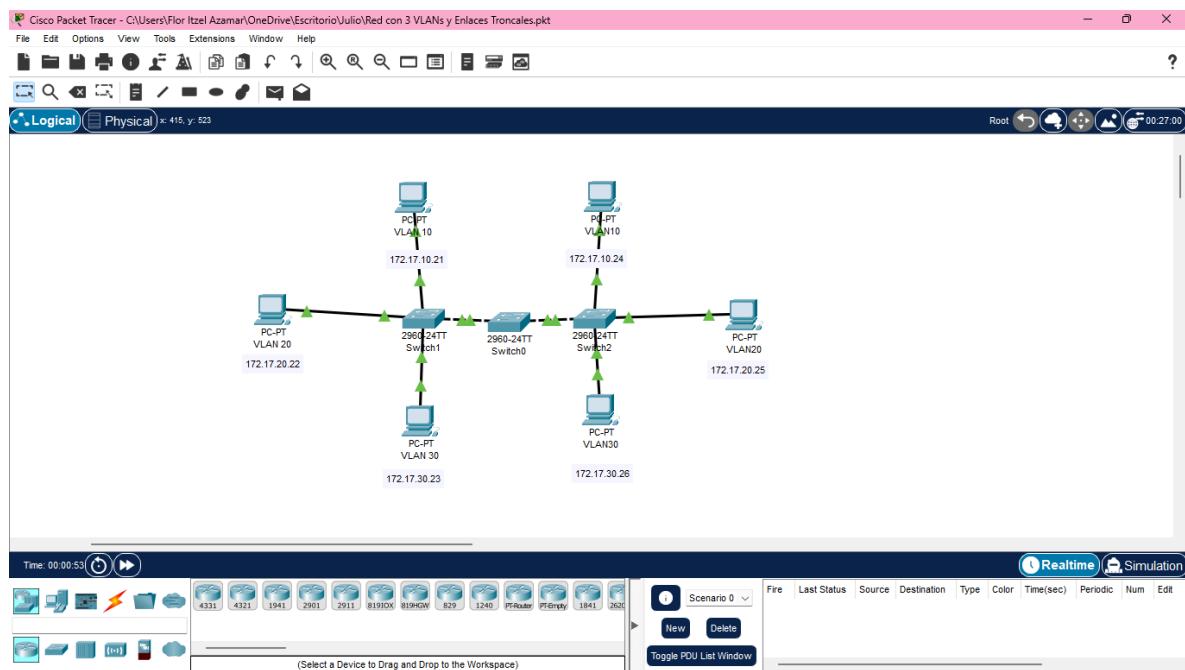
Actividad:



Actividad:



Actividad:



Conclusión

El estudio de los parámetros de configuración de red y de las tecnologías que los acompañan permite comprender cómo se estructura, administra y optimiza una red para garantizar su correcto funcionamiento. Conceptos como las direcciones IP, el subnetting, las VLANs, el enrutamiento y la configuración de switches son herramientas clave para asegurar redes eficientes, escalables y seguras.

Asimismo, las simulaciones y actividades prácticas permiten aplicar estos conocimientos en escenarios reales, favoreciendo el desarrollo de habilidades técnicas para la solución de problemas y la implementación de topologías más complejas. En conjunto, estos temas forman la base del trabajo profesional en el área de redes, indispensable para cualquier entorno informático actual.