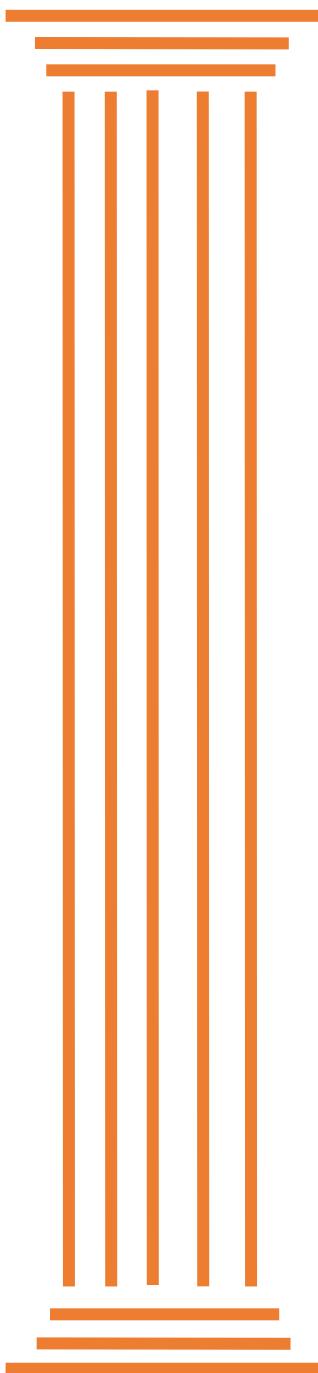




S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLOGICO de Tuxtepec



MATERIA:
INTERCONECTIVIDAD DE REDES
REPORTE

DE TODO LO

VISTO DURANTE

EL SEMESTRE

ALUMNO:
JOSE ANGEL CARVAJAL ANAYA

DOCENTE:
JULIO AGUILAR CARMONA

CARRERA:
ING. INFORMÁTICA

FECHA:
05 DE DICIEMBRE DE 2025

REPORTE TIPO MEMORIA

Contenidos vistos durante el semestre sobre redes de computadoras

1. Parámetros de configuración de red

La configuración de red es el conjunto de valores que permiten que un dispositivo pueda comunicarse con otros dentro de la misma red o a través de Internet. Entre los parámetros más importantes se encuentran:

- **Dirección IP:** Identificador único asignado a cada dispositivo.
- **Máscara de subred:** Define el tamaño de la red y determina qué parte de la dirección IP es la red y cuál es el host.
- **Puerta de enlace (Gateway):** Dirección del dispositivo encargado de conectar la red local con otras redes externas.
- **DNS (Domain Name System):** Servidores encargados de traducir nombres de dominio a direcciones IP.
- **DHCP:** Servicio que asigna automáticamente direcciones IP y otros parámetros a los dispositivos.

Estos elementos permiten que un equipo pueda integrarse adecuadamente a una infraestructura de red, interactuar con los demás dispositivos y acceder a servicios externos.

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

Para determinar si un dispositivo pertenece a una red específica, se utiliza la comparación entre:

- **Dirección IP del host**
- **Máscara de subred**

- **Dirección IP del destino**

El equipo realiza una operación lógica **AND** entre su dirección IP y la máscara de subred. Luego compara el resultado con la operación equivalente del destino. Si ambos resultados coinciden, significa que están en la **misma red**, por lo que la comunicación ocurre localmente. Si los resultados difieren, el equipo envía los paquetes a la **puerta de enlace**, que se encarga del enrutamiento hacia otras redes.

Este proceso permite al host saber si debe comunicarse de manera interna o a través de un router.

3. Clasificación de direcciones IP

Las direcciones IPv4 públicas y privadas se clasifican de acuerdo con rangos establecidos para su funcionamiento:

Clases principales

- **Clase A:**

- Rango: 0.0.0.0 – 127.255.255.255
- Máscara por defecto: 255.0.0.0
- Redes grandes con millones de hosts.

- **Clase B:**

- Rango: 128.0.0.0 – 191.255.255.255
- Máscara: 255.255.0.0
- Redes medianas.

- **Clase C:**

- Rango: 192.0.0.0 – 223.255.255.255
- Máscara: 255.255.255.0

- Redes pequeñas.

Otras clases

- **Clase D:** Multicast
- **Clase E:** Uso experimental

Direcciones privadas

- Clase A privada: 10.0.0.0/8
- Clase B privada: 172.16.0.0/12
- Clase C privada: 192.168.0.0/16

Estas direcciones se usan en redes LAN y no son enrutables en Internet.

4. Subneting

El subnetting es la técnica para **dividir una red grande en varias redes más pequeñas** (subredes). Sus beneficios son:

- Mejor administración de la red
- Más seguridad
- Menor congestión
- Aprovechamiento eficiente de direcciones IP

El proceso se basa en “pedir prestados” bits del campo de host para convertirlos en bits de red, creando así varias subredes.

Pasos generales:

1. Identificar la red base.
2. Determinar cuántas subredes o hosts se requieren.
3. Calcular cuántos bits se necesitan pedir prestados.

-
4. Obtener la nueva máscara de subred.
 5. Generar los rangos y direcciones de cada subred.
-

5. Simulación de red LAN

Durante el semestre se realizaron prácticas de simulación utilizando herramientas como **Cisco Packet Tracer** o **GNS3**, donde se recrearon:

- Topologías de red física y lógica
- Interconexión entre PCs, switches y routers
- Configuración de direccionamiento IP
- Pruebas de conectividad con *ping*, *traceroute* y tabla ARP
- Configuración de servicios como DHCP y DNS

Las simulaciones permiten replicar escenarios reales sin necesidad de hardware físico, facilitando el aprendizaje y la experimentación de fallas y soluciones.

6. Enrutamiento estático y dinámico

Enrutamiento estático

- Las rutas son configuradas manualmente por el administrador.
- Más seguro y predecible.
- Útil en redes pequeñas.
- Desventaja: No se adapta de forma automática a cambios en la red.

Ejemplo

básico:

```
ip route 192.168.10.0 255.255.255.0 192.168.1.1
```

Enrutamiento dinámico

Los routers intercambian información usando protocolos para determinar automáticamente la mejor ruta.

Ejemplos de protocolos:

- **RIP**: sencillo, limitado a 15 saltos.
- **OSPF**: rápido, jerárquico y eficiente.
- **EIGRP**: híbrido y muy robusto (propietario de Cisco).

Ventajas:

- Se adapta automáticamente a fallas.
 - Adecuado para redes medianas y grandes.
-

7. VLANs

Las **VLANs (Virtual LANs)** permiten dividir una red física en múltiples redes lógicas para mejorar:

- Seguridad
- Segmentación
- Rendimiento
- Flexibilidad administrativa

Permiten que dispositivos separados físicamente estén en la misma red lógica mientras que otros más cercanos queden aislados según configuración.

Tipos:

- VLAN de datos
- VLAN de voz
- VLAN nativa

- VLAN de administración

Comandos típicos en Cisco:

```
switch(config)# vlan 10
```

```
switch(config-vlan)# name Ventas
```

8. Configuración de switches y puertos troncales

Los switches permiten conectar múltiples dispositivos dentro de una LAN y administrarlos mediante VLANs.

Configuración de puertos de acceso (access)

Un puerto access pertenece a una sola VLAN.

```
switch(config)# interface fa0/1
```

```
switch(config-if)# switchport mode access
```

```
switch(config-if)# switchport access vlan 10
```

Puertos troncales (trunk)

Transportan múltiples VLANs entre switches o hacia routers.

```
switch(config)# interface fa0/24
```

```
switch(config-if)# switchport mode trunk
```

```
switch(config-if)# switchport trunk allowed vlan all
```

Estos enlaces son fundamentales para redes empresariales donde se manejan múltiples VLANs.

9. Redes inalámbricas

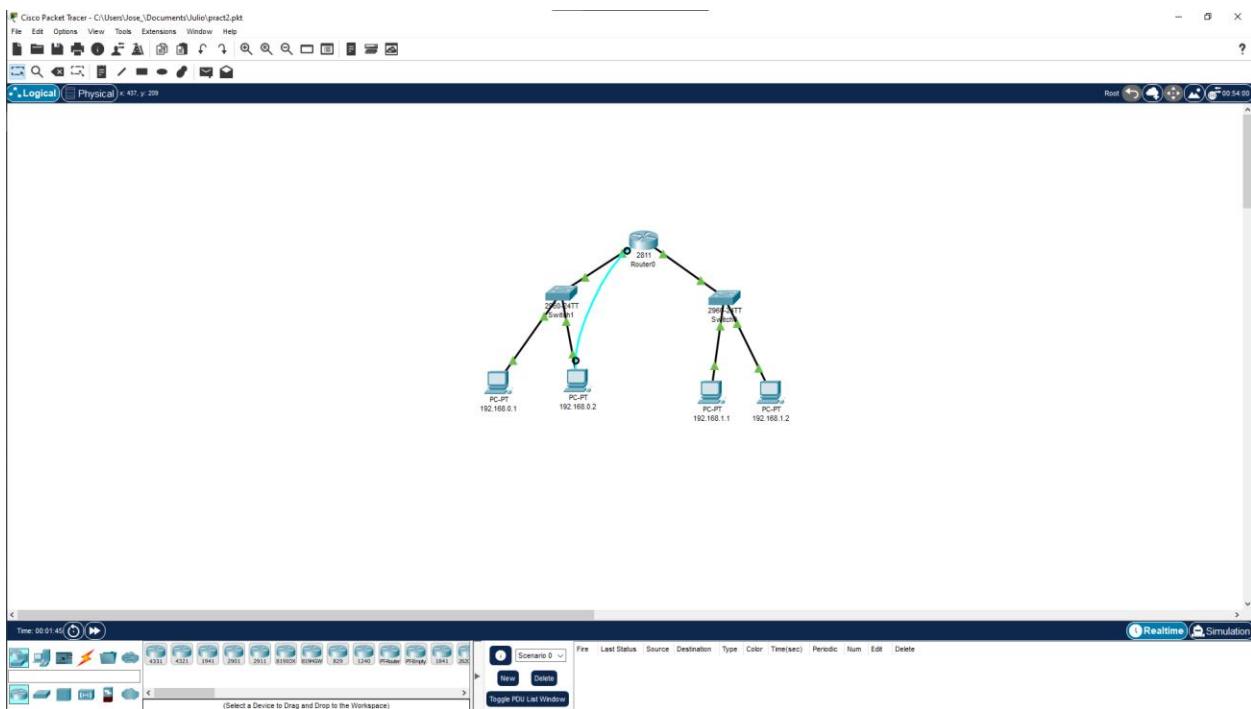
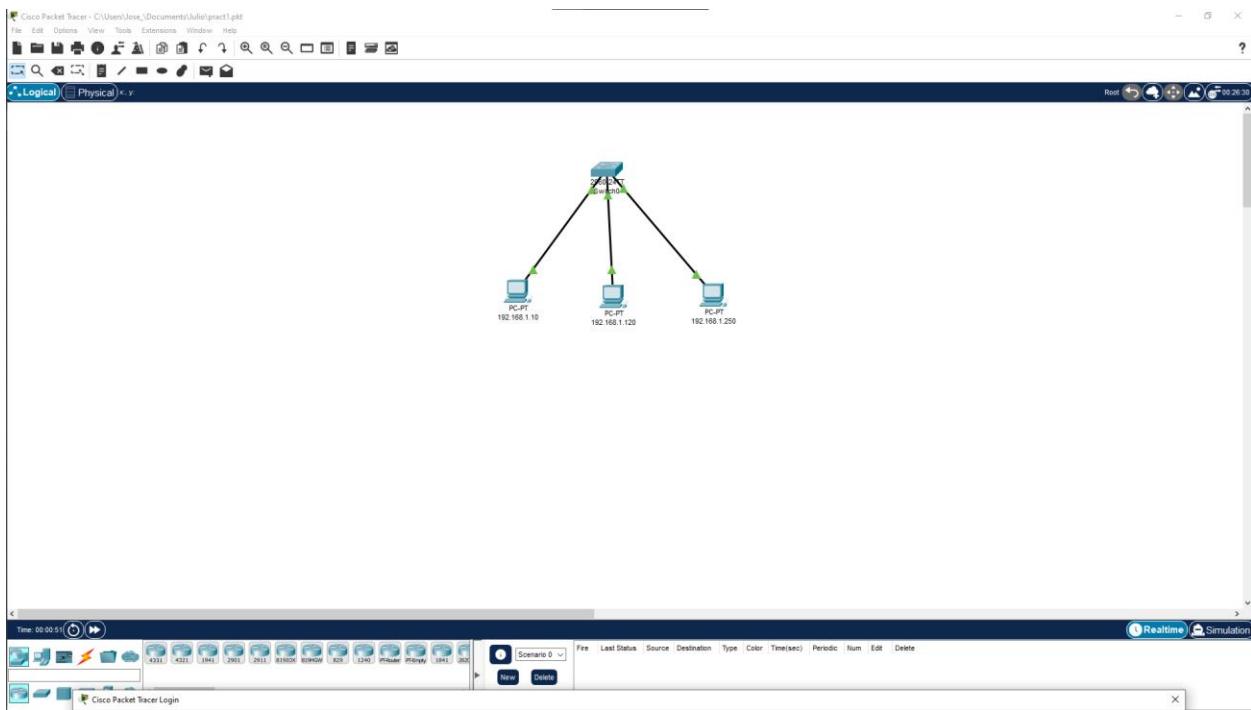
Se estudiaron los principios y configuraciones básicas del WiFi, incluyendo:

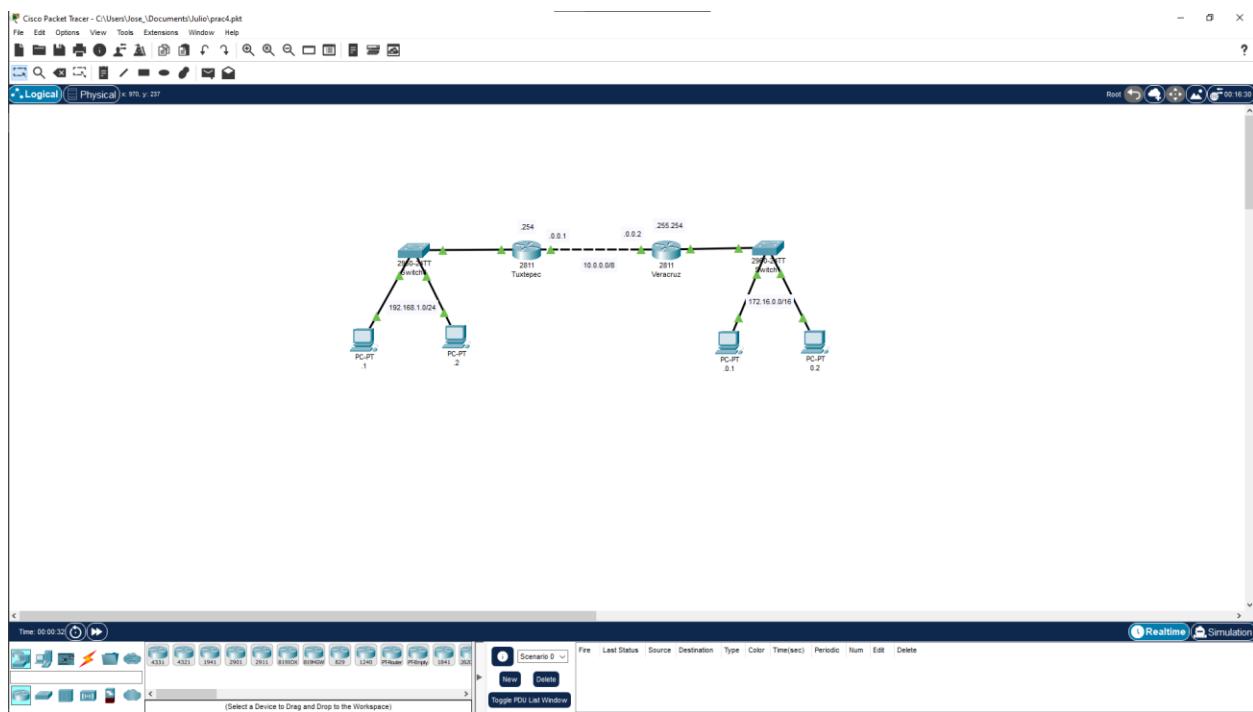
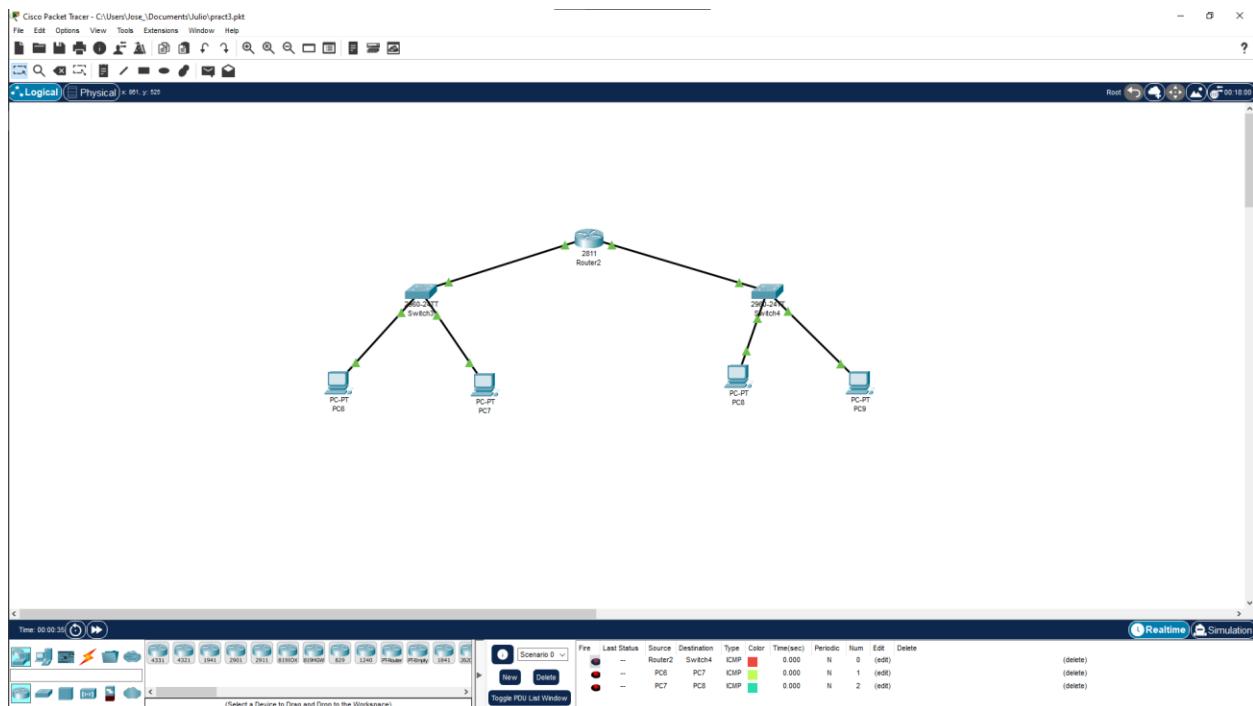
- Estándares IEEE 802.11 (a/b/g/n/ac/ax)
- SSID: nombre de la red
- Seguridad: WPA2 y WPA3
- Canales y bandas de frecuencia (2.4 GHz y 5 GHz)
- Configuración de punto de acceso
- Diferencias entre redes abiertas, personales y empresariales

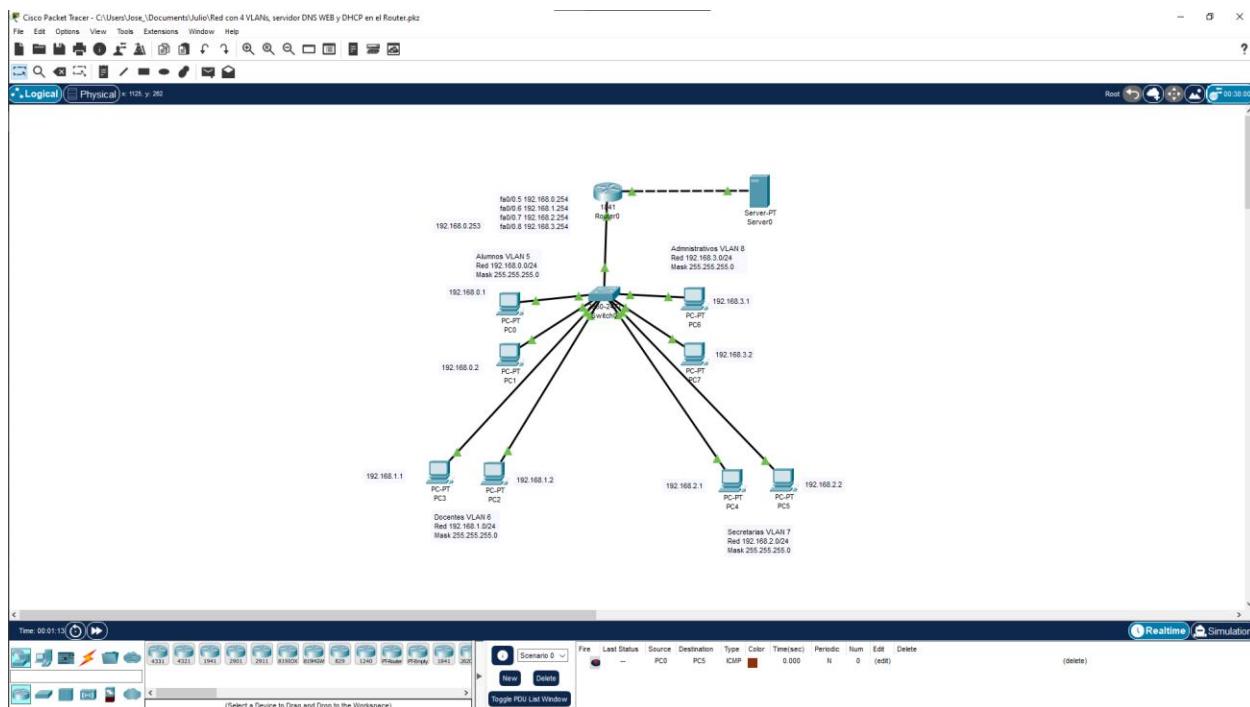
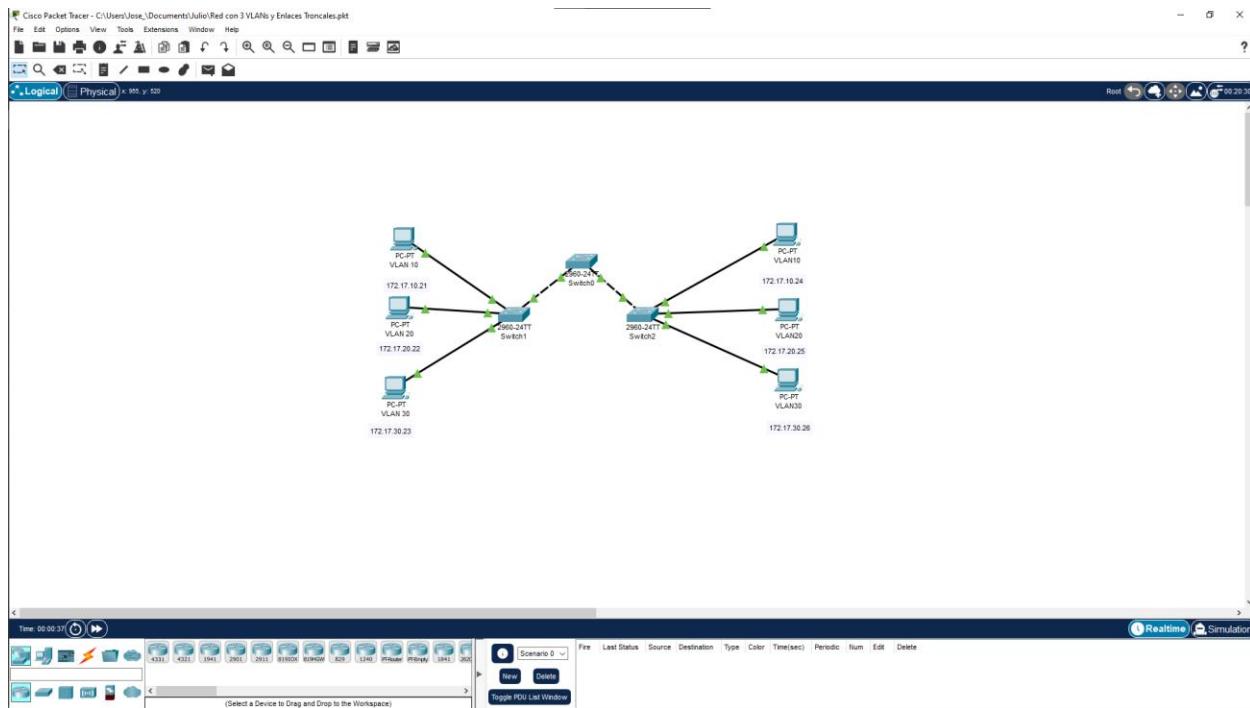
Además, se analizaron buenas prácticas como:

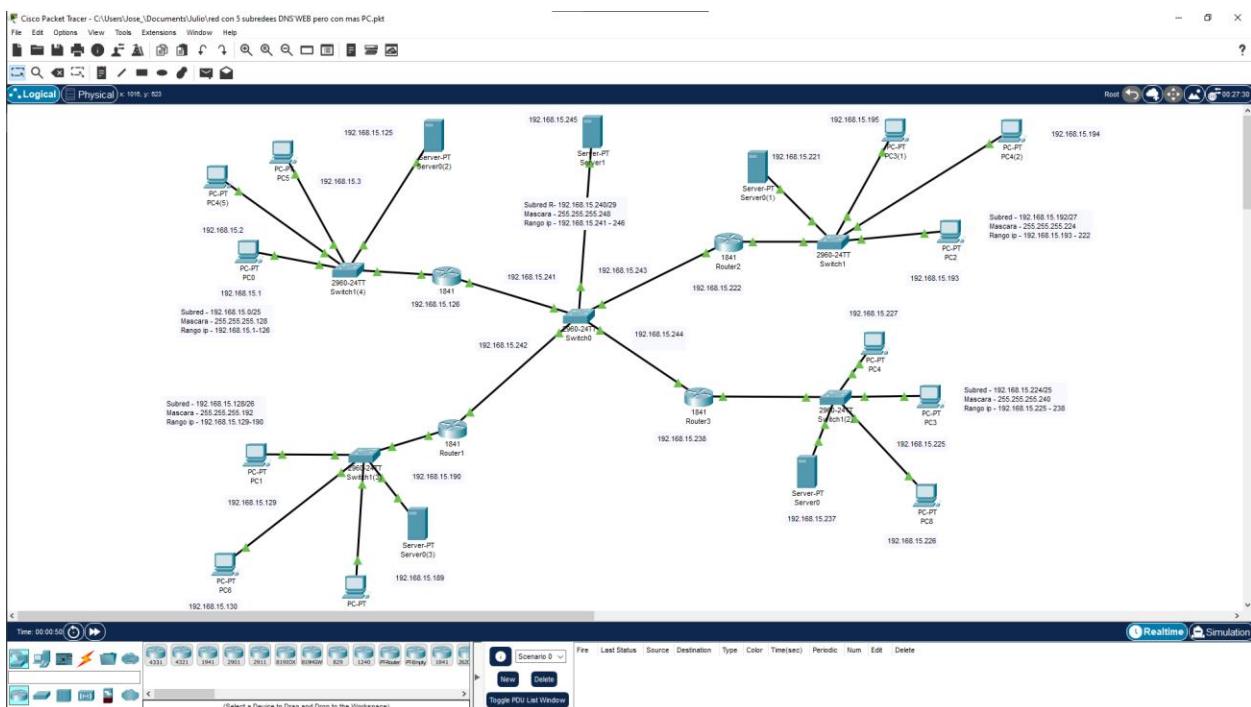
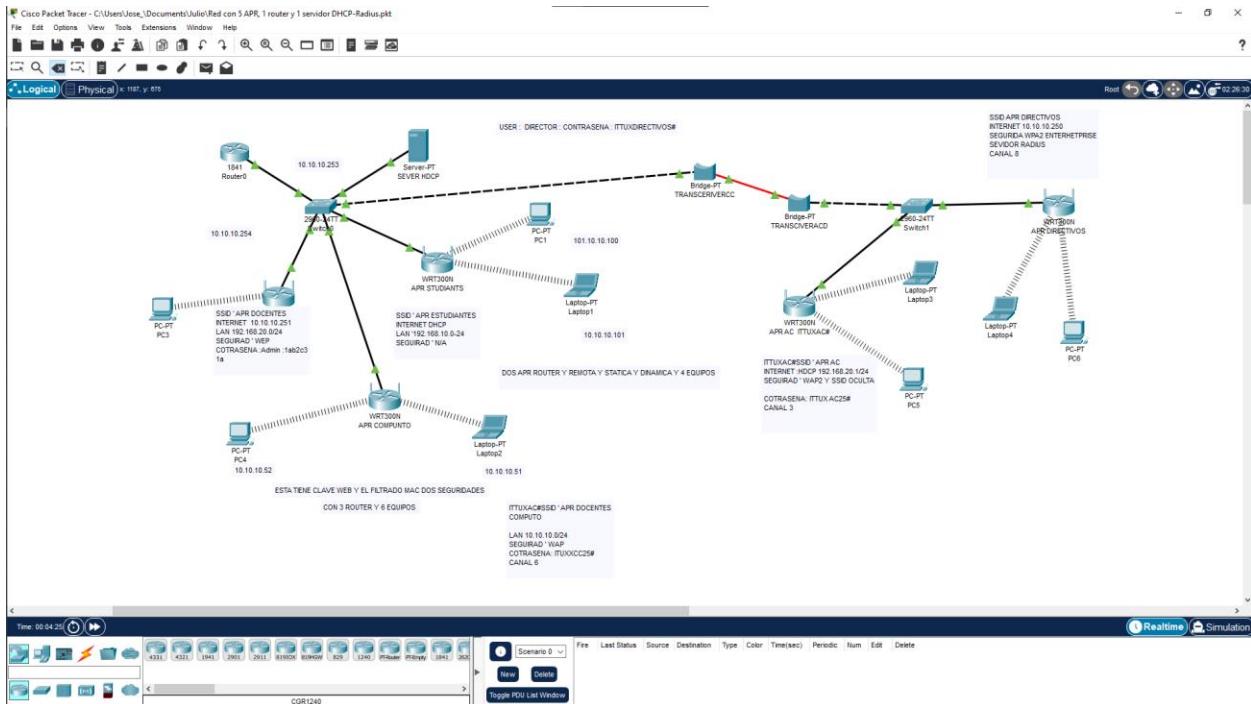
- Cambio de contraseña periódicamente
 - Ocultar SSID en entornos escolares
 - Uso de listas de control de acceso (ACL)
 - Separación de redes por VLAN para invitados y administración
-

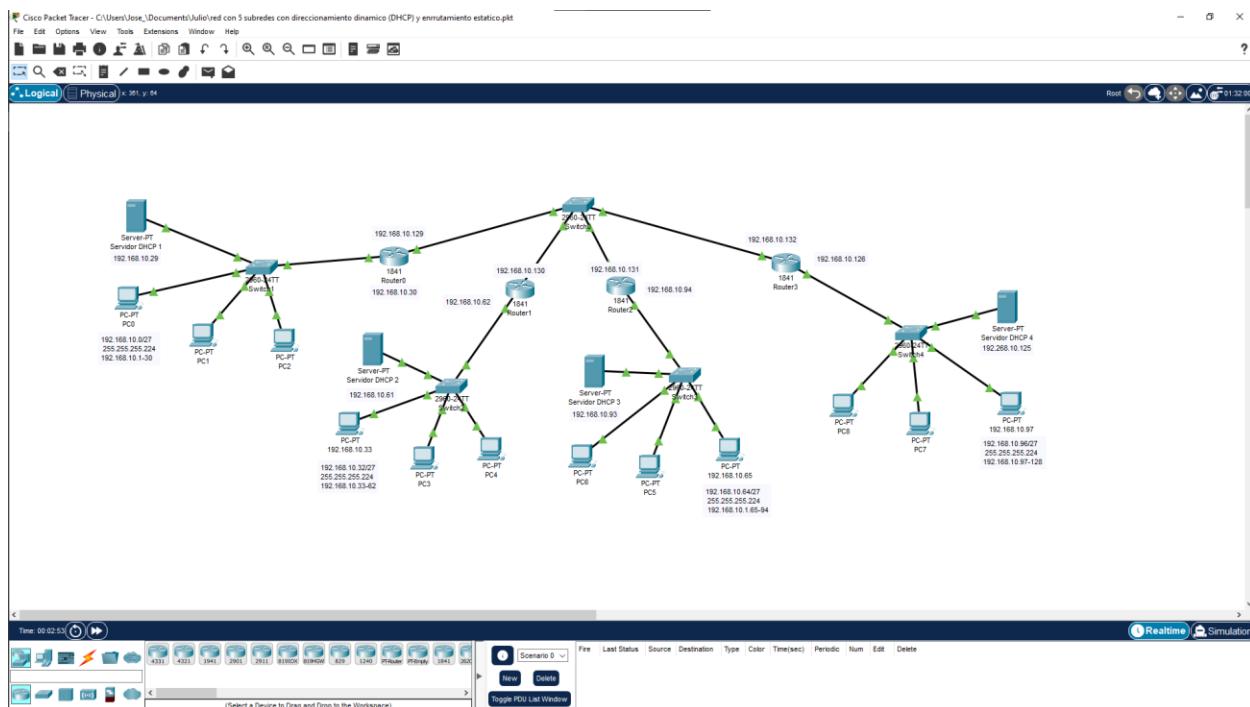
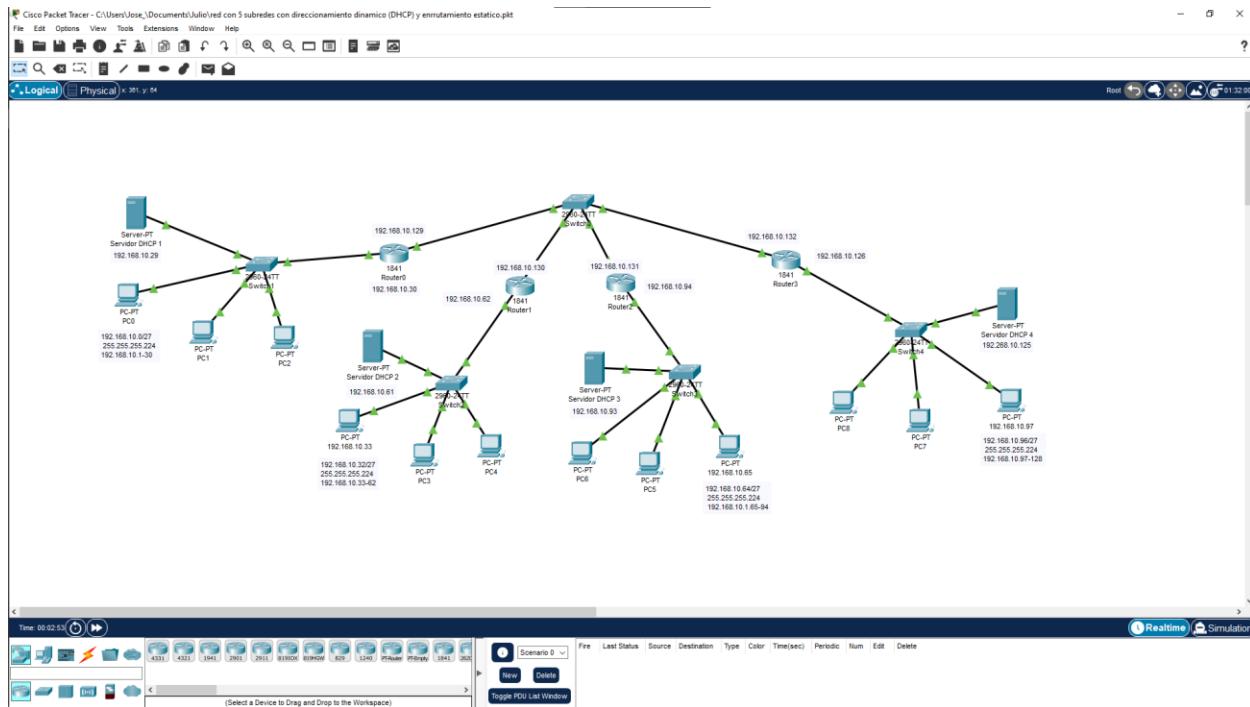
EVIDENCIAS FOTOGRAFICAS

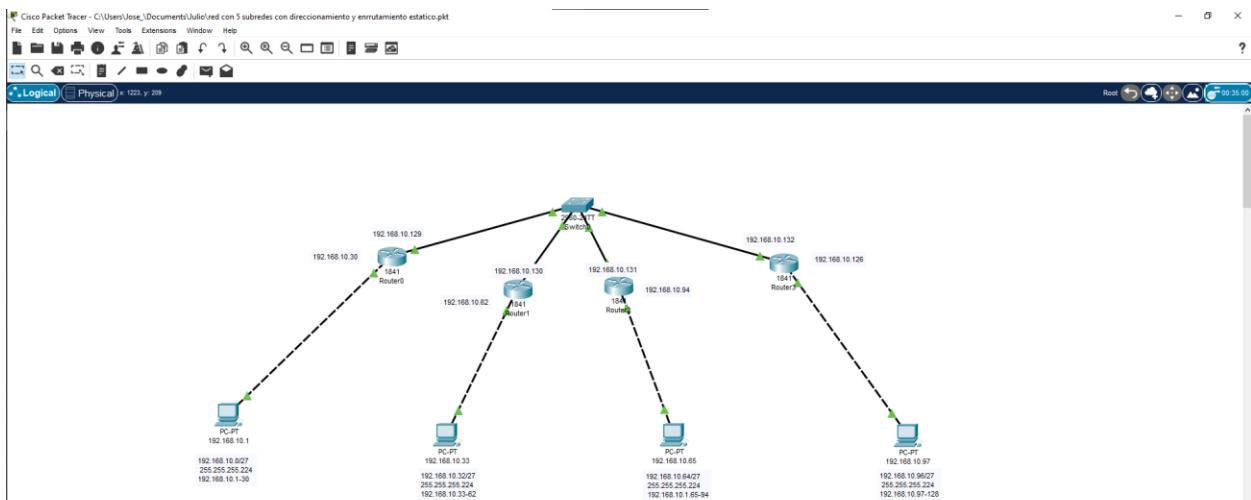
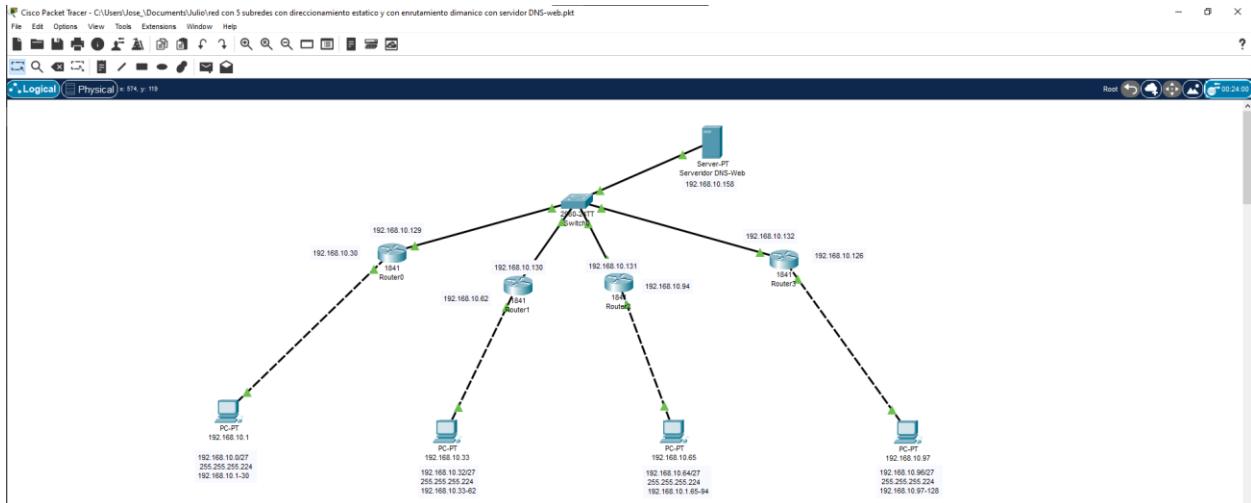


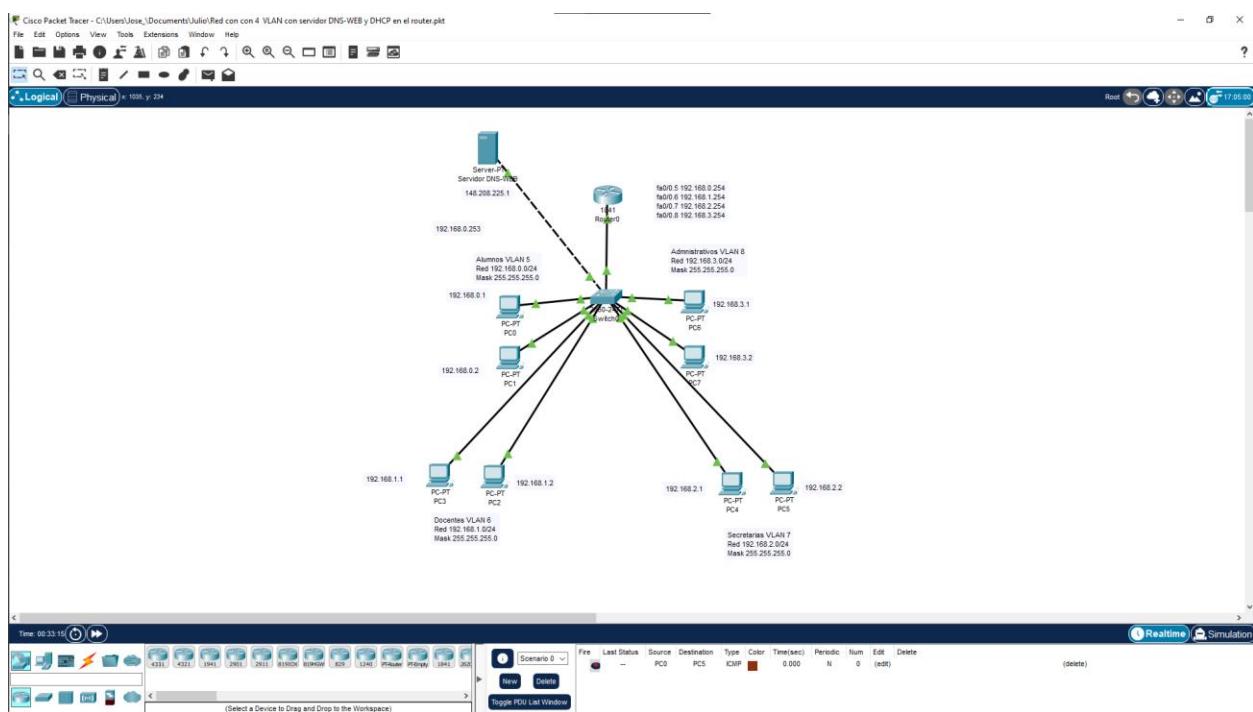
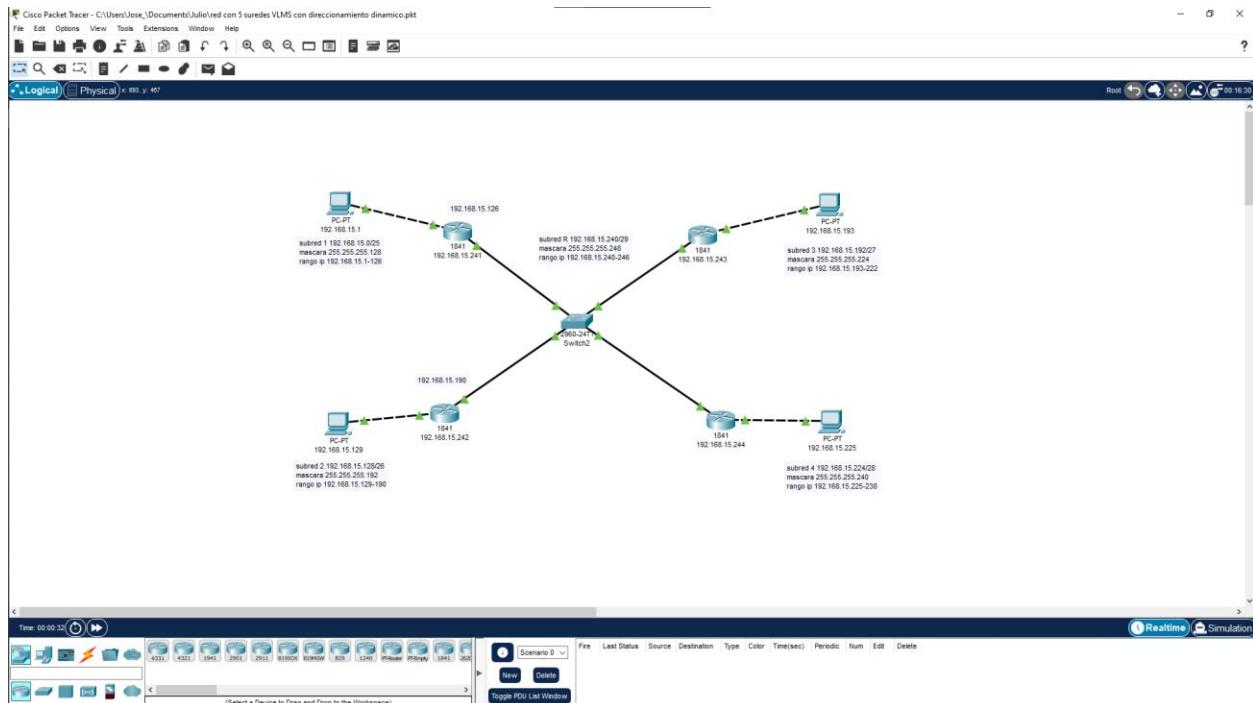


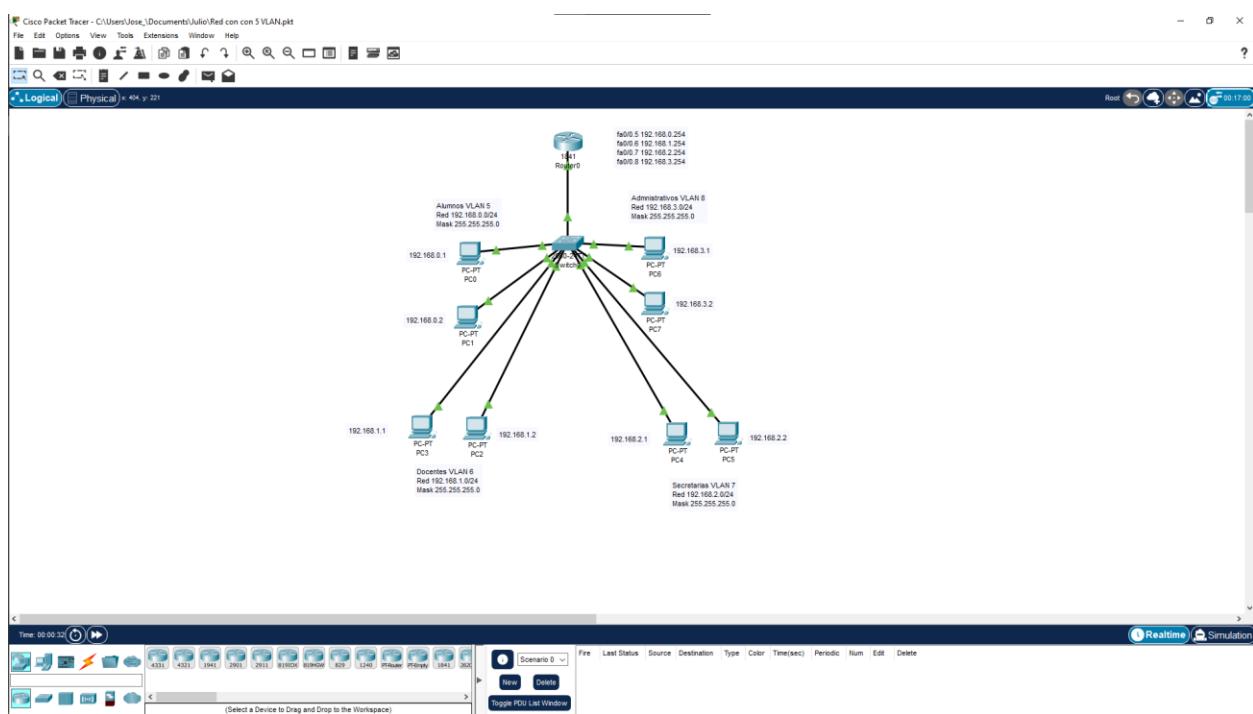
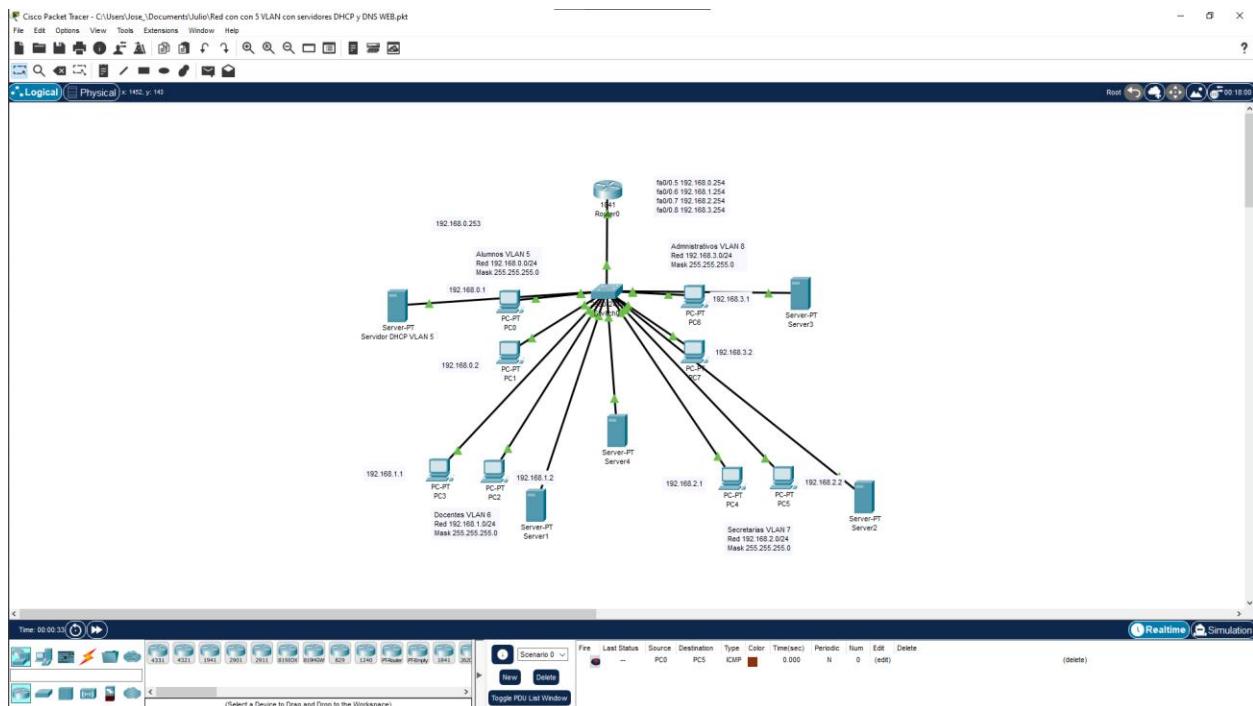


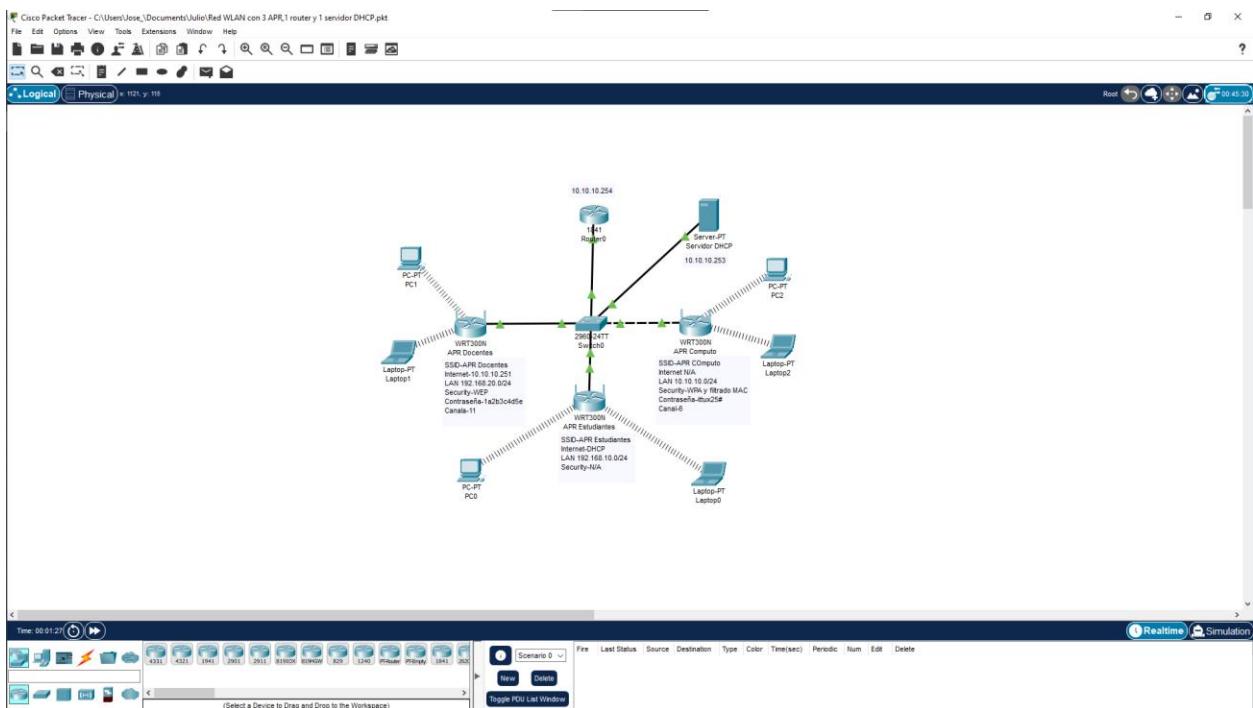
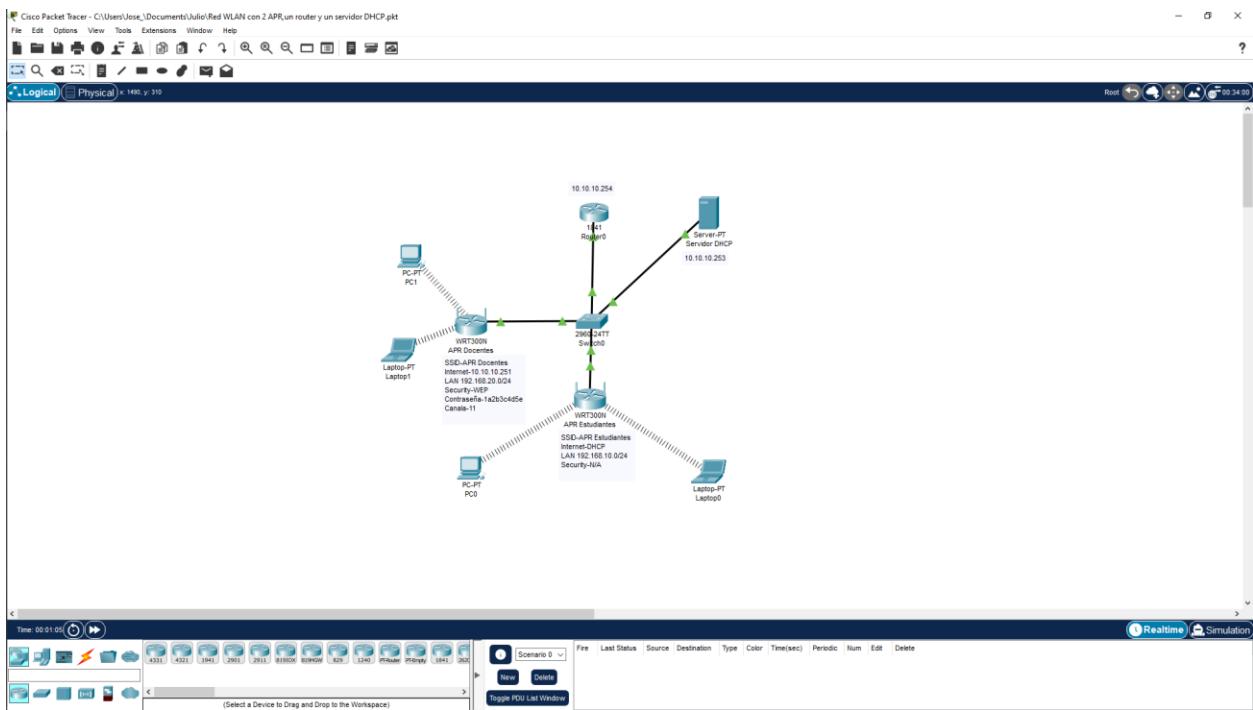


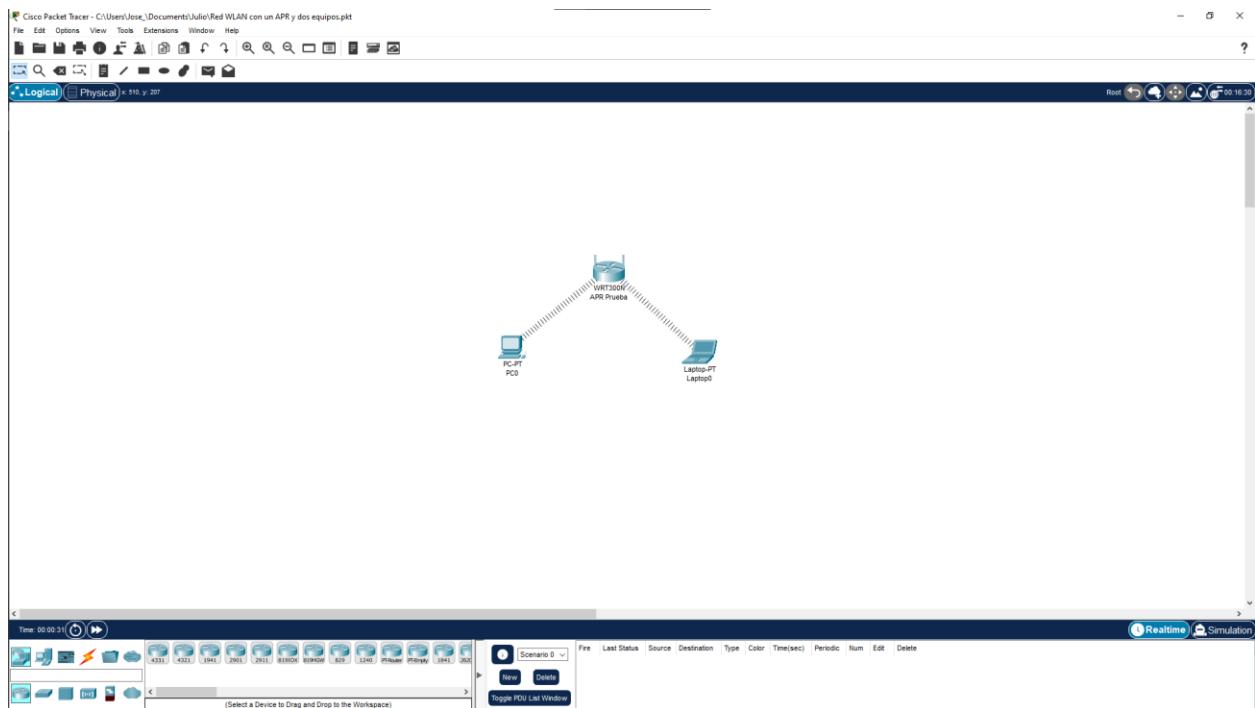












CONCLUSIONES

A lo largo del semestre se adquirieron conocimientos fundamentales para el diseño, configuración y administración de redes de computadoras. Temas como el subneteo, VLANs, enrutamiento, configuración de switches y redes inalámbricas forman la base para comprender infraestructuras reales utilizadas en entornos empresariales.

Las actividades prácticas y simulaciones permitieron reforzar conceptos clave, desarrollando habilidades para resolver problemas reales de conectividad, seguridad y optimización de redes. Este aprendizaje constituye una base sólida para cursos avanzados o para desempeñarse en el área profesional de telecomunicaciones y sistemas.