Universidad San Carlos de Guatemala
Facultad de ingeniería.
Ingeniería en ciencias y sistemas

Proyecto 2:
NetUSAC: Proyecto de Interconexión

PONDERACIÓN: 34

Horas Aproximadas: 35

Índice

Contenido

1. Resumen Ejecutivo

Este proyecto tiene como objetivo central el diseño, configuración y simulación de una infraestructura de red interedificios para el campus central, enfocada en segmentación, seguridad, redundancia y enrutamiento avanzado.

La solución técnica se desarrolla a través de la interconexión de cinco edificios clave: Biblioteca Central, Edificio T4, Edificio S11, Edificio S12 y DIGA. Cada uno cuenta con una red local segmentada mediante VLANs específicas (Estudiantes, Docentes, Administración, Videovigilancia y Biblioteca), implementadas con su correspondiente asignación de subredes usando técnicas de VLSM y FLSM, optimizando el uso de direcciones IP.

La comunicación entre VLANs se gestiona mediante la técnica de Router-on-a-Stick, configurando subinterfaces con puertas de enlace virtuales. Se incorporan medidas de seguridad como ACLs en dispositivos firewall para evitar tráfico entre VLANs distintas, permitiendo únicamente comunicación dentro de la misma VLAN, sin importar el edificio.

El diseño considera alta disponibilidad mediante protocolos de redundancia (HSRP y VRRP), y la integración de protocolos de enrutamiento estático y dinámico (RIP, OSPF, EIGRP), además de redistribución de rutas en puntos de interconexión clave. Todo el proyecto se implementa y verifica en Cisco Packet Tracer, complementado con una fase de prueba física con laptops reales, replicando parte del entorno simulado.

Este proyecto permite que el estudiante demuestre de forma práctica el dominio de conceptos clave de redes, aplicando un enfoque estructurado, seguro y escalable en una red institucional realista.

2. Competencia que desarrollaremos

- Diseñar topologías de red estructuradas y escalables, utilizando segmentación lógica mediante VLANs.
- Aplicar técnicas de subneteo eficientes (VLSM y FLSM) para la asignación de direcciones IP según requerimientos específicos.
- Configurar ruteo inter-VLAN mediante la técnica de Router-on-a-Stick y el uso de subinterfaces.
- Implementar protocolos de enrutamiento estático y dinámico (RIP, OSPF, EIGRP), incluyendo la redistribución de rutas.
- Establecer mecanismos de redundancia y alta disponibilidad utilizando protocolos como HSRP y VRRP.
- Aplicar políticas de seguridad mediante listas de control de acceso (ACLs) para restringir el tráfico entre VLANs.

- Configurar dispositivos de red mediante CLI (Command Line Interface), reforzando la precisión y comprensión técnica.

- Ejecutar pruebas físicas que repliquen la simulación virtual, identificando errores y validando conectividad entre dispositivos reales.

3. Objetivos del Aprendizaje

3.1 Objetivo General

Desarrollar en el estudiante la capacidad de diseñar, implementar, documentar y evaluar una red de datos interedificios que integre conceptos avanzados de segmentación mediante VLANs, asignación eficiente de direcciones IP, enrutamiento estático y dinámico, y políticas de seguridad, utilizando simuladores de red y entornos físicos controlados, con el fin de fortalecer su comprensión práctica y teórica sobre la administración de redes informáticas en contextos reales.

3.2 Objetivos Específicos

1. Diseñar e implementar una red interedificios segmentada mediante VLANs, aplicando criterios de organización lógica por áreas funcionales para optimizar el tráfico y la seguridad en la red.

2. Configurar el enrutamiento inter-VLAN utilizando la técnica de Router-on-a-Stick, junto con protocolos de enrutamiento estático y dinámico (RIP, OSPF, EIGRP), asegurando la conectividad entre los distintos edificios.

3. Aplicar técnicas de subneteo con VLSM y FLSM para distribuir eficientemente las direcciones IP, y establecer políticas de seguridad mediante ACLs que restrinjan la comunicación entre VLANs no autorizadas.

4. Enunciado del Proyecto

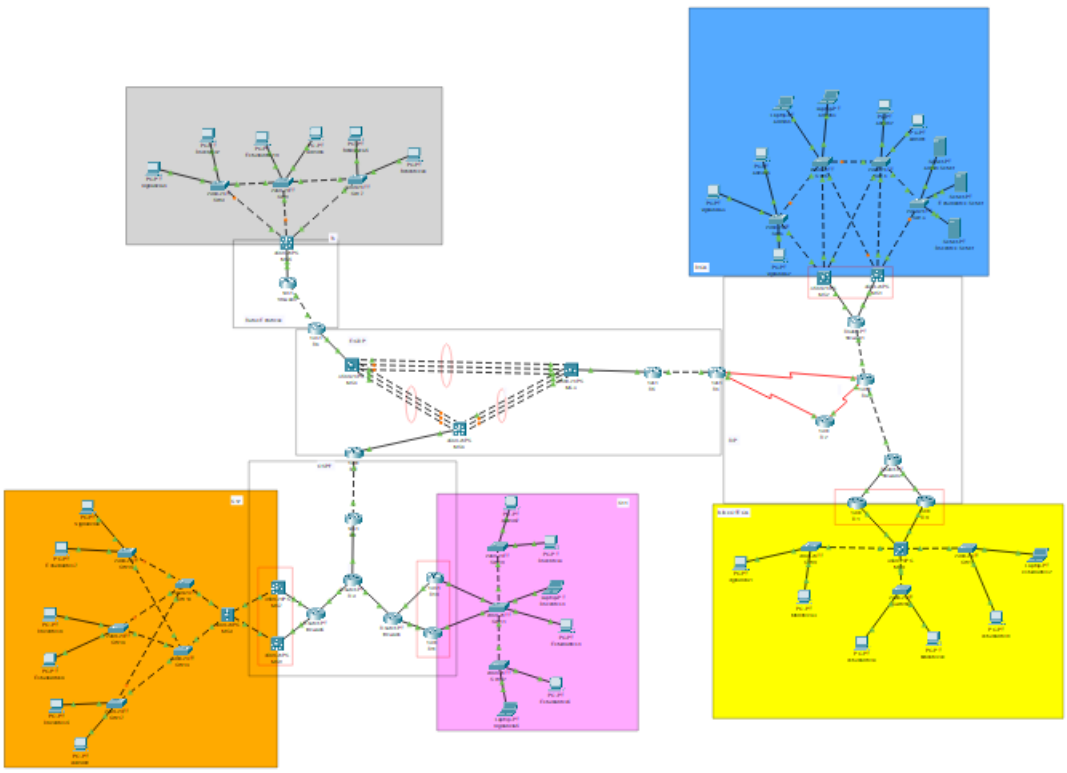
En el marco de un proceso de modernización tecnológica, la Universidad de San Carlos de Guatemala (USAC) ha lanzado un proyecto piloto para fortalecer la conectividad, seguridad y gestión de redes en su campus central. Este proyecto, liderado por la Dirección General de Tecnologías de la Información y la Comunicación (DGTIC), tiene como objetivo principal el diseño e implementación de una red Inter edificios estructurada, segmentada y gestionada mediante protocolos de enrutamiento dinámico.

El proyecto abarca cinco edificios clave del campus central: Biblioteca Central, Edificio T4, Edificio S11, Edificio S12 y DIGA. En cada uno de estos edificios se identificaron necesidades específicas de conectividad para distintas unidades funcionales: personal administrativo, docentes, estudiantes, dispositivos de videovigilancia y terminales bibliotecarios.

El proyecto incluirá la segmentación de la red mediante la creación de VLANs para distintas áreas de la universidad, como Admon, Estudiantes, Docentes, Biblioteca, y Videovigilancia. Además, se implementará el ruteo inter-VLAN utilizando la técnica de Router on a Stick y configurando interfaces virtuales. El estudiante también deberá aplicar VLSM y FLSM para la asignación eficiente de direcciones IP, y configurar el ruteo estático, dinámico y aplicar políticas de seguridad para asegurar la conectividad entre los edificios.

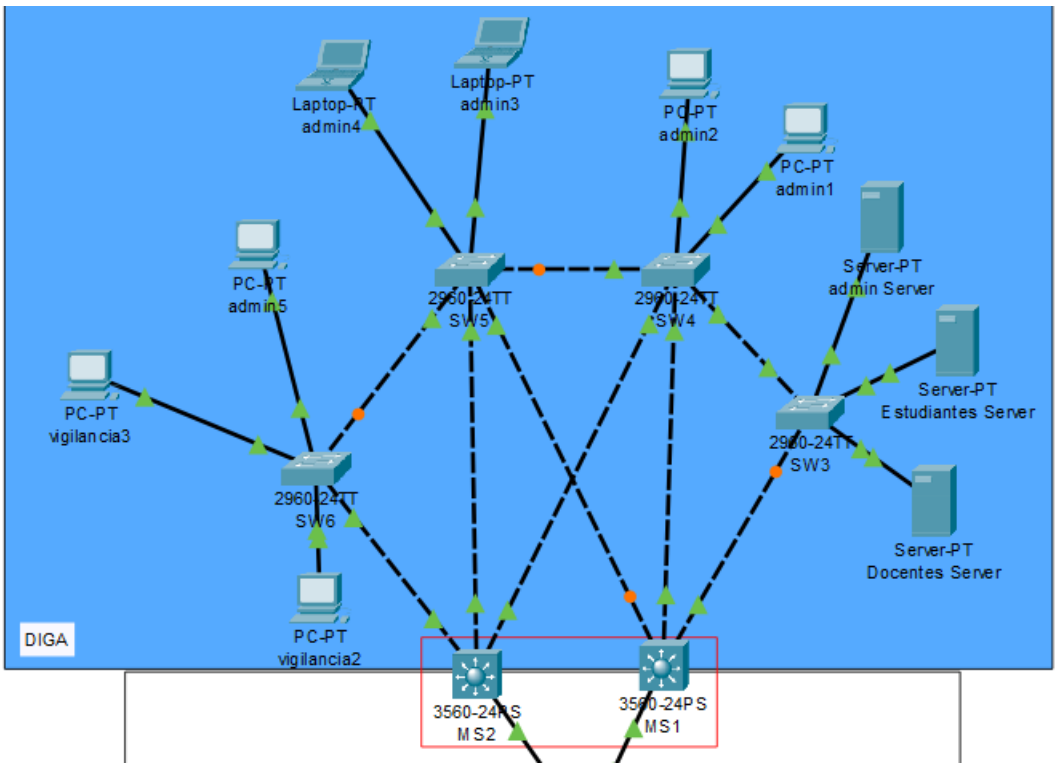
4.1 Simulación

Topología Completa



Como se mencionó anteriormente, la topología propuesta cuenta con 5 edificios los cuales se detallan a continuación y que están conectadas por medio de un Core/Backbone.

4.1.1 DIGA



La red del edificio DIGA se diseñará utilizando 4 VLANs. Cada VLAN tendrá su propio ID de red, el cual se calculará utilizando VLSM. El ID de red base otorgado para realizar el VLSM será 192.168.XX.0 /24, donde XX serán los últimos dos dígitos de su carnet.

Los requisitos de cada VLAN serán los siguientes:

VLAN	ID de VLAN	Equipos
Estudiantes	1Y	5
Docentes	2Y	5
Vigilancia	3Y	20
Admin	4Y	120

Para determinar el valor de Y en cada ID de VLAN:

- Se deben sumar los últimos 2 dígitos de su carnet.
- Si el resultado es mayor a 9, se toma únicamente el último dígito del resultado.
- Se sustituye Y por el valor obtenido.

Ejemplo:

Para el carnet 20198774:
Últimos dígitos: 7 + 4 = 11
IDs de VLAN resultantes: 11, 21, 31, 41 respectivamente.

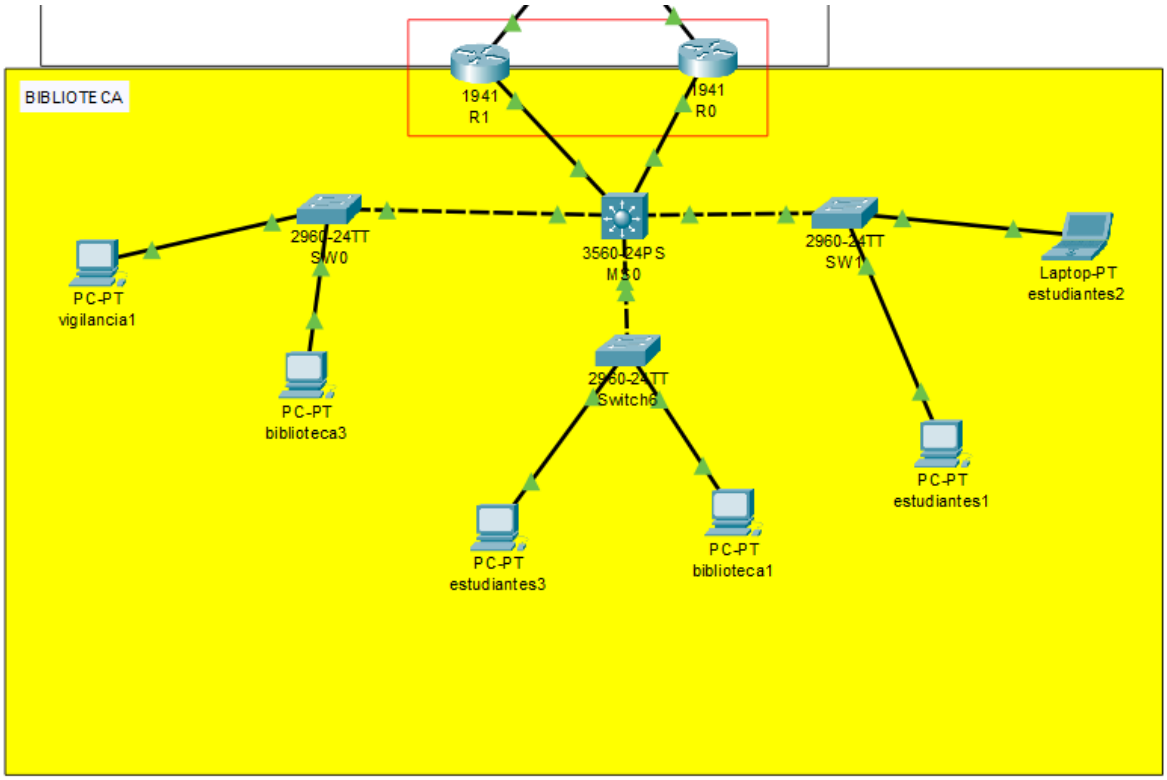
La salida de la red interna del DIGA estará a cargo de dos switches multicapa (MS1 y MS2), configurados para proveer redundancia mediante el protocolo HSRP. Estos dispositivos ofrecerán interfaces virtuales que funcionarán como puertas de enlace predeterminadas para todas las VLANs de la red.

Se configurarán ACLs extendidas para permitir tráfico únicamente entre dispositivos de la misma VLAN en el dispositivo firewall 1.

También se debe configurar el protocolo VTP para la propagación de VLANS dentro de la red. Los parámetros serán:

- Dominio: #Carnet
- Password: usac2025
- Modo: Server (SW5), Cliente (el resto de switches de esta red).

4.1.2 Biblioteca



La red de la biblioteca central está diseñada para dividir y usar 3 VLANs para diferentes áreas y para ello le solicitan que realice el subnetting correspondiente, por lo que se le asigna un ID de red base: 192.158.XX.0 /24; con el ID proporcionado deberá usar el método de VLSM.

Nota: Las XX corresponden a los últimos dos dígitos de su carnet

Requisitos de cada VLAN:

VLAN	ID de VLAN	Equipos
Estudiantes	1Y	75
Vigilancia	3Y	30
Biblioteca	5Y	25

Para determinar el valor de Y en cada ID de VLAN:

- Se deben sumar los últimos 2 dígitos de su carnet.
- Si el resultado es mayor a 9, se toma únicamente el último dígito del resultado.
- Se sustituye Y por el valor obtenido.

Ejemplo:

Para el carnet 20198744:
Últimos dígitos: 4 + 4 = 8
IDs de VLAN resultantes: 18, 28, 38, 48 respectivamente.

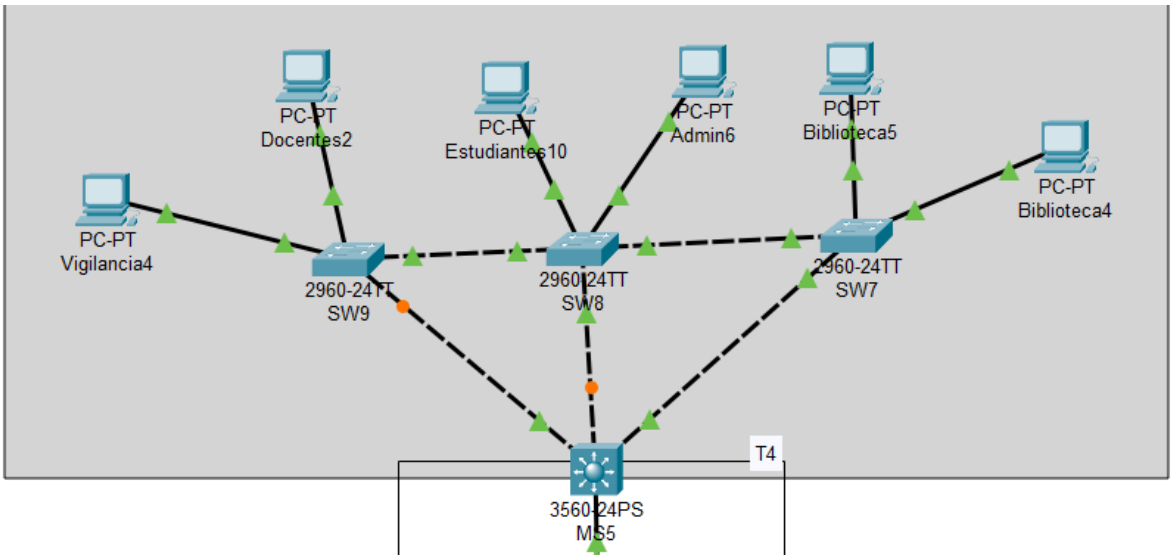
Se debe configurar el protocolo VRRP (HSRP en cisco) entre los routers R1 y R0 para proporcionar redundancia cuando un dispositivo de enrutamiento sea comprometido o deje de funcionar. Se deben configurar subinterfaces en los routers para las puertas de enlace predeterminadas de las VLANS en los routers correspondientes.

Se configurarán ACLs extendidas para permitir tráfico únicamente entre dispositivos de la misma VLAN en el dispositivo firewall 2.

Adicional a eso deberán configurar lo que es el protocolo de VTP para la propagación de las vlans en los swtiches, los parámetros que deben seguir son los siguientes:

- Dominio: #Carnet
- Password: usac2025
- Modo: Server (MS0), Cliente(el resto de switches de esta red).

4.1.3 Edificio T4



La red del edificio T4 se implementará con 5 VLANs, asignadas a áreas clave. Cada VLAN tendrá un ID de red único, calculado mediante VLSM (Variable Length Subnet Masking). La red base para realizar el subneting será 172.16.XX.0 /24, donde XX serán los últimos 2 dígitos de su carnet.

Los requisitos de cada VLAN serán los siguientes:

VLAN	ID de VLAN	Equipos
Estudiantes	1Y	60
Docentes	2Y	10
Vigilancia	3Y	15
Admin	4Y	75
Biblioteca	5Y	12

Para determinar el valor de Y en cada ID de VLAN:

- Se deben sumar los últimos 2 dígitos de su carnet.
- Si el resultado es mayor a 9, se toma únicamente el último dígito del resultado.
- Se sustituye Y por el valor obtenido.

Ejemplo:

> Para el carnet 20198774:
> Últimos dígitos: 7 + 4 = 11
> IDs de VLAN resultantes: 11, 21, 31, 41 respectivamente.

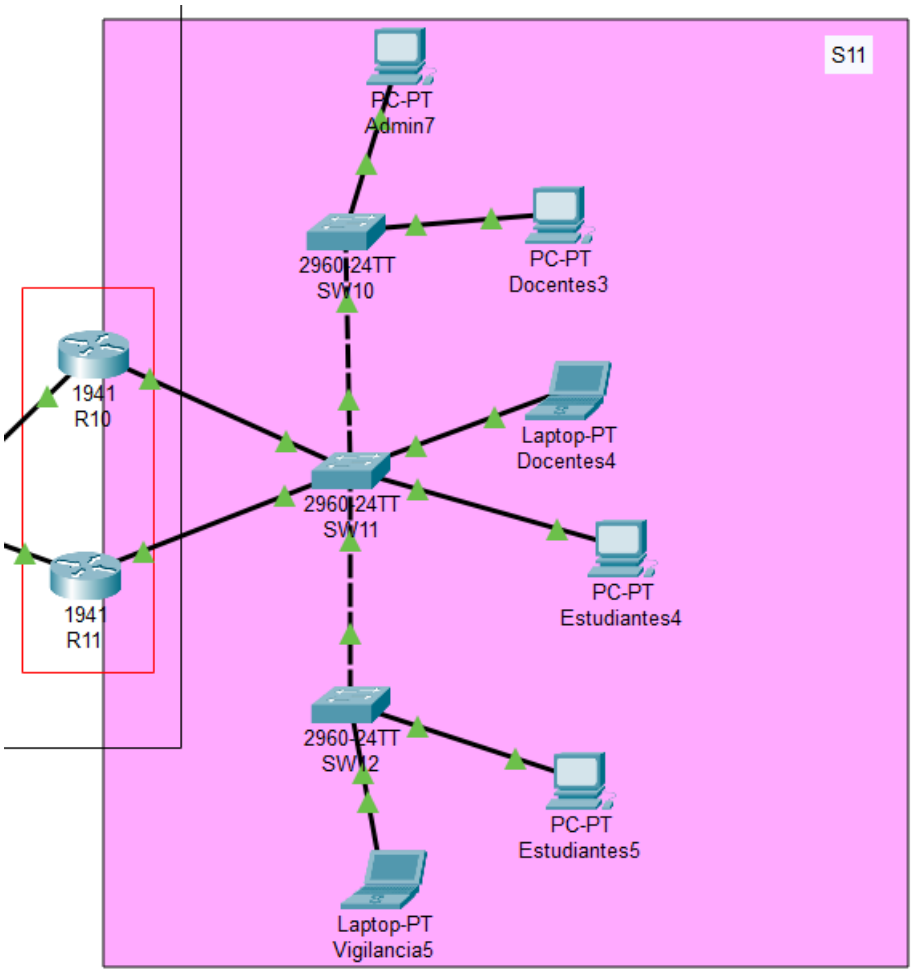
La salida de la red de este edificio estará a cargo del switch MS5, se deben configurar las respectivas interfaces virtuales para configurar puertas de enlace predeterminadas para cada VLAN de la red.

Se configurarán ACLs extendidas para permitir tráfico únicamente entre dispositivos de la misma VLAN en el dispositivo firewall 3.

También se debe configurar el protocolo VTP para la propagación de VLANS dentro de la red. Los parámetros serán:

- Dominio: #Carnet.
- Password: usac2025
- Modo: Server (SW8), Cliente(el resto de switches de esta red).

4.1.4 Edificio S11



La red del edificio S11 se diseñará utilizando 4 VLANs. Cada VLAN tendrá su propio ID de red, el cual se calculará utilizando VLSM. El ID de red base otorgado para realizar el VLSM será 172.148.XX.0 /24, donde XX serán los últimos 2 dígitos de su carnet.

Los requisitos de cada VLAN serán los siguientes:

VLAN	ID de VLAN	Equipos
Estudiantes	1Y	100
Docentes	2Y	15
Vigilancia	3Y	10
Admin	4Y	55

Para determinar el valor de Y en cada ID de VLAN:

- Se deben sumar los últimos 2 dígitos de su carnet.
- Si el resultado es mayor a 9, se toma únicamente el último dígito del resultado.
- Se sustituye Y por el valor obtenido.

Ejemplo:

Para el carnet 20200554:
Últimos dígitos: 5 + 4 = 9
IDs de VLAN resultantes: 19, 29, 39, 49 respectivamente.

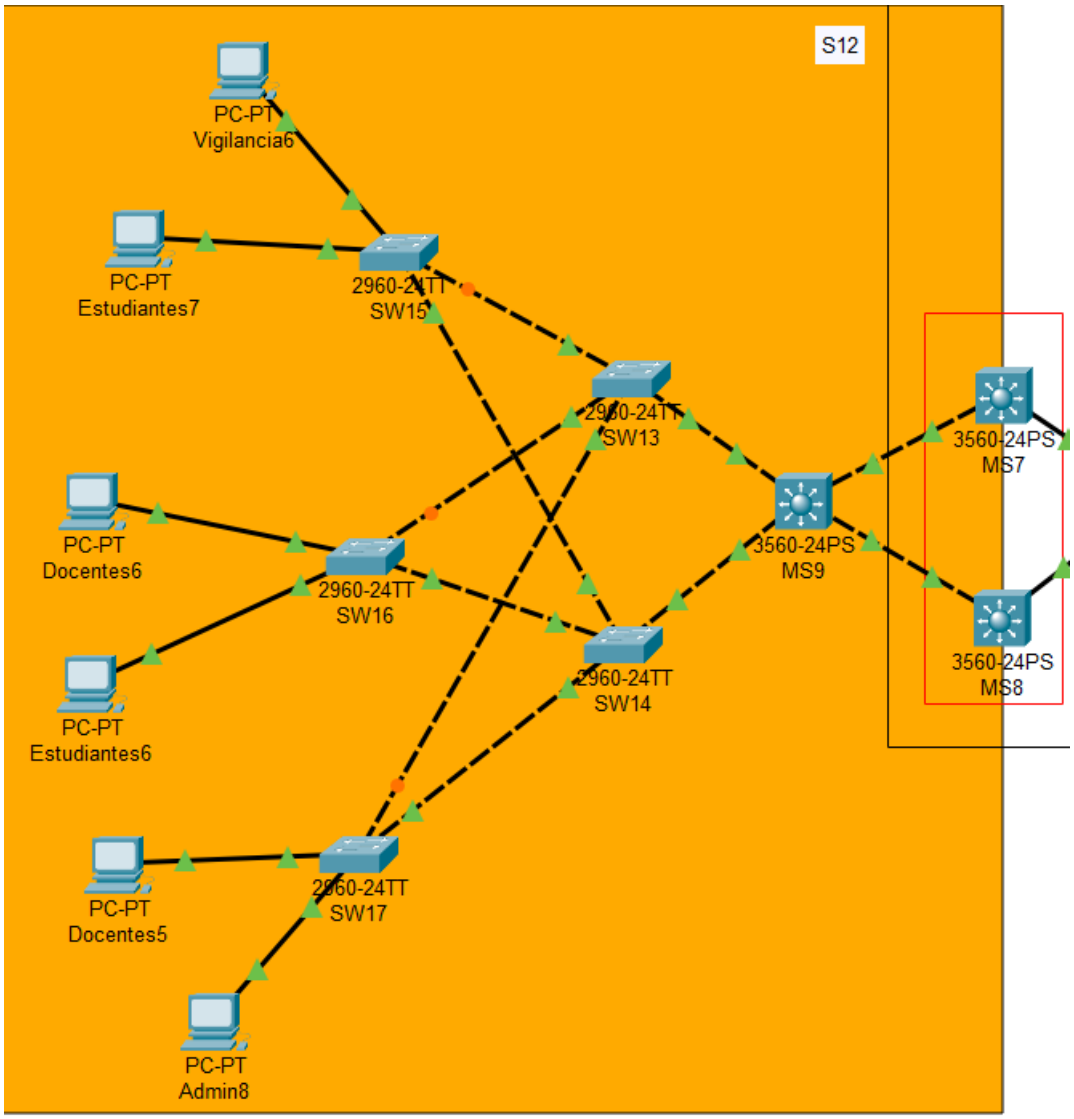
Se debe configurar el protocolo VRRP (HSRP en cisco) entre los routers R10 y R11 para proporcionar redundancia cuando un dispositivo de enrutamiento sea comprometido o deje de funcionar. Se deben configurar subinterfaces en los routers para las puertas de enlace predeterminadas de las VLANS en los routers correspondientes.

Se configurarán ACLs extendidas para permitir tráfico únicamente entre dispositivos de la misma VLAN en el dispositivo firewall 4.

También se debe configurar el protocolo VTP para la propagación de VLANS dentro de la red. Los parámetros serán:

- Dominio: #Carnet
- Password: usac2025
- Modo: Server (SW11), Cliente(el resto de switches de esta red).

4.1.5 Edificio S12



La red del edificio S12 se diseñará utilizando 4 VLANs. Cada VLAN tendrá su propio ID de red, el cual se calculará utilizando VLSM. El ID de red base otorgado para realizar el VLSM será 192.128.XX.0 /24, donde XX serán los últimos 2 dígitos de su carnet.

Los requisitos de cada VLAN serán los siguientes:

VLAN	ID de VLAN	Equipos
Estudiantes	1Y	125
Docentes	2Y	35
Vigilancia	3Y	20
Admin	4Y	25

Para determinar el valor de Y en cada ID de VLAN:

- Se deben sumar los últimos 2 dígitos de su carnet.
- Si el resultado es mayor a 9, se toma únicamente el último dígito del resultado.
- Se sustituye Y por el valor obtenido.

Ejemplo:
Para el carnet 201903944:
Últimos dígitos: 4 + 4 = 8
IDs de VLAN resultantes: 18, 28, 38, 48 respectivamente.

La salida de la red interna del S12 estará a cargo de dos switches multicapa (MS7 y MS8), configurados para proveer redundancia mediante el protocolo HSRP. Estos dispositivos ofrecerán interfaces virtuales que funcionarán como puertas de enlace predeterminadas para todas las VLANs de la red.

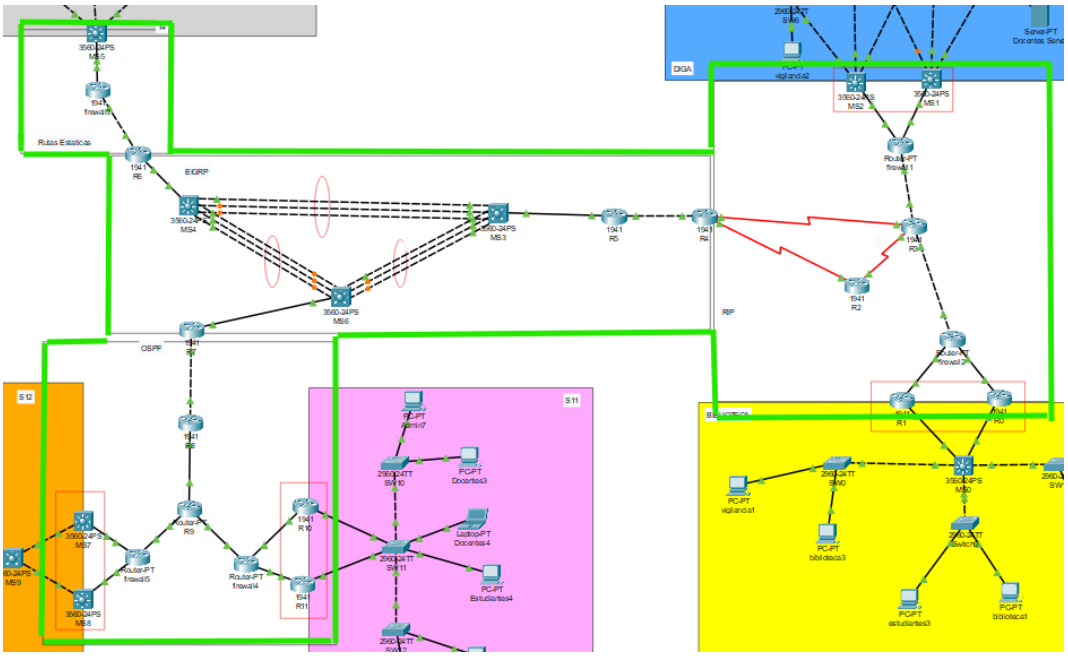
Se configurarán ACLs extendidas para permitir tráfico únicamente entre dispositivos de la misma VLAN en el dispositivo firewall 5.

También se debe configurar el protocolo VTP para la propagación de VLANS dentro de la red. Los parámetros serán:

●Dominio: #Carnet
●Password: usac2025
●Modo: Server (MS9), Cliente(el resto de switches de esta red).

4.1.6 CORE/BACKBONE

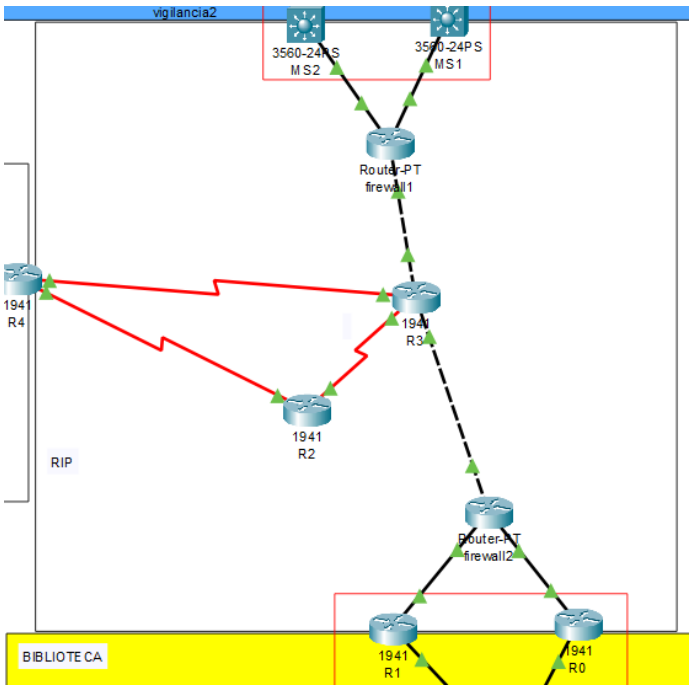
El backbone es la parte de la infraestructura de red que se encargará de las interconexiones/enrutamiento de los distintos edificios.



Esta infraestructura está segmentada por distintos protocolos de enrutamiento. Se utilizará el ID de red: 10.0.0.0 /24 implementando FLSM según sea necesario.

Segmentación según los protocolos de enrutamiento:

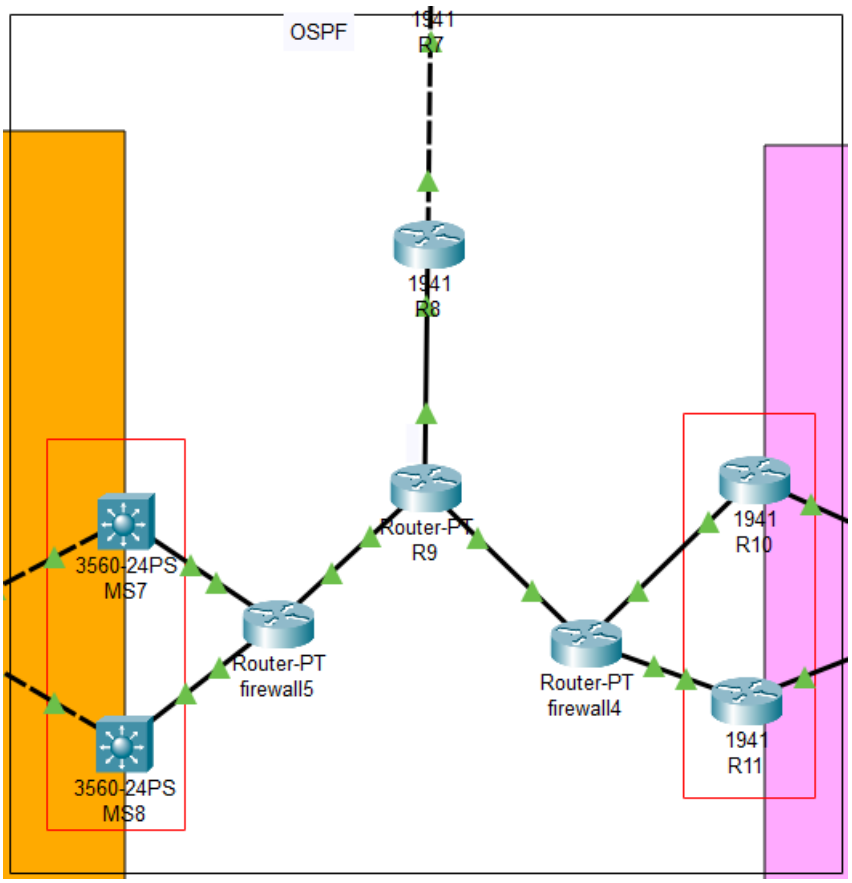
4.1.6.1 RIP(Routing Information Protocol):



Se estará usando el protocolo RIP en el segmento entre DIGA y Biblioteca Central. En el router R4, que actúa como punto de interconexión con el segmento que opera bajo EIGRP, se deberá realizar la redistribución de rutas (redistribute) correspondiente. Esto permitirá que ambos protocolos compartan información de enrutamiento, asegurando la conectividad entre las diferentes áreas de la red y evitando la pérdida de paquetes debido a rutas no conocidas. Los dispositivos que participarán en este protocolo de enrutamiento serán:

- MS1, MS2, R1, R0, R2, R3, R4,firewall 1, firewall2.

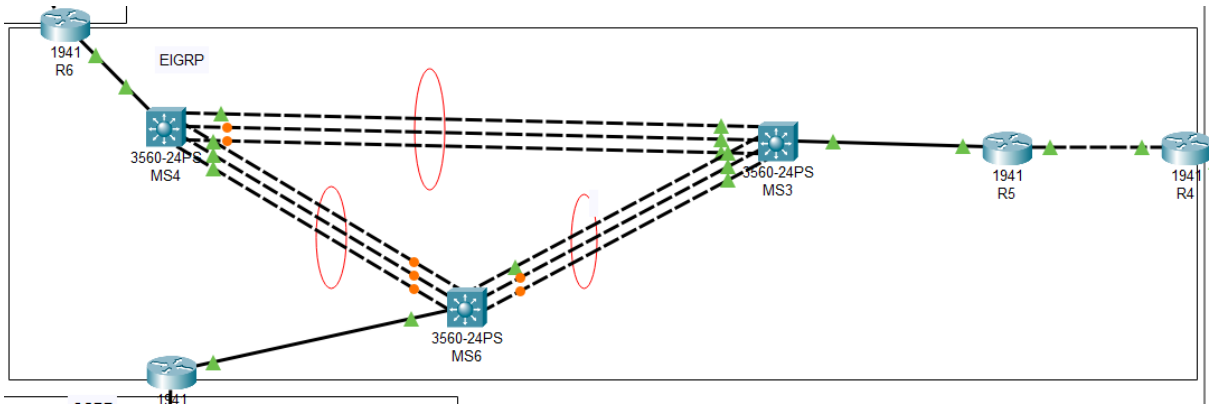
4.1.6.2 OSPF (Open Shortest Path First):



El protocolo de OSPF será implementado entre el edificio S11 y S12, proporcionando una convergencia rápida y optimización del tráfico de la red. El router R7 actuará como punto de interconexión con el segmento que opera con EIGRP por lo tanto se deberá de realizar la redistribución de las rutas correspondientes en este dispositivo. Los dispositivos que participarán en este protocolo de enrutamiento serán:

- R7, R8, R9, R10, R11, MS7, MS8, firewall 4 y firewall 5.

4.1.6.3 EIGRP (Enhanced Interior Gateway Routing Protocol):



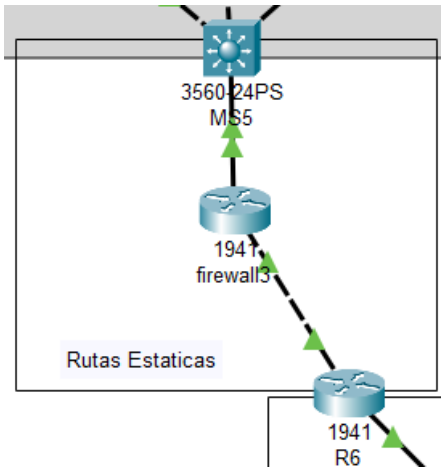
Este protocolo será aplicado al segmento de la red para interconectar todos los edificios ofreciendo un balance de la carga y una estabilidad en la transmisión de los datos. Los routers R4, R6 y R7 trabajarán como punto de conexión con las áreas RIP, OSPF y la de rutas estáticas, por lo tanto, en estos dispositivos se deberá configurar la redistribución de rutas correspondiente.

Los dispositivos que participarán en este protocolo de enrutamiento serán:

- R4, R5, R6, R7, MS3, MS4, MS6.

Se debe configurar etherchannel entre los Switches MS3, MS4 y MS6 .

4.1.6.4 Rutas Estáticas:



Finalmente, para la conexión entre el router R6 y el edificio T4 se deben configurar rutas estáticas. En el router R6 se deberá realizar la redistribución de rutas para que el proceso EIGRP enrute tráfico hacia los otros edificios.

4.2 Seguridad

Por motivos de seguridad y segmentación lógica, se establece que la comunicación entre dispositivos estará restringida exclusivamente a aquellos que pertenezcan a la misma VLAN, independientemente del edificio en el que se encuentren ubicados, mediante la implementación de listas de control de acceso (ACLs) en los firewalls indicados.

Esto implica que:

Los dispositivos asociados a una VLAN determinada (por ejemplo, VLAN ESTUDIANTES) podrán comunicarse entre sí aun si se encuentran distribuidos en distintos edificios (T4, S11, S12, DIGA, Biblioteca Central).

No se permitirá el tráfico entre VLANs distintas.

Esta medida busca reducir el riesgo de accesos no autorizados, mitigar la propagación de amenazas entre segmentos de red y mantener un entorno de red ordenado y seguro, especialmente en un entorno académico de alta concurrencia como el de la Universidad de San Carlos de Guatemala.

4.3 Parte Física

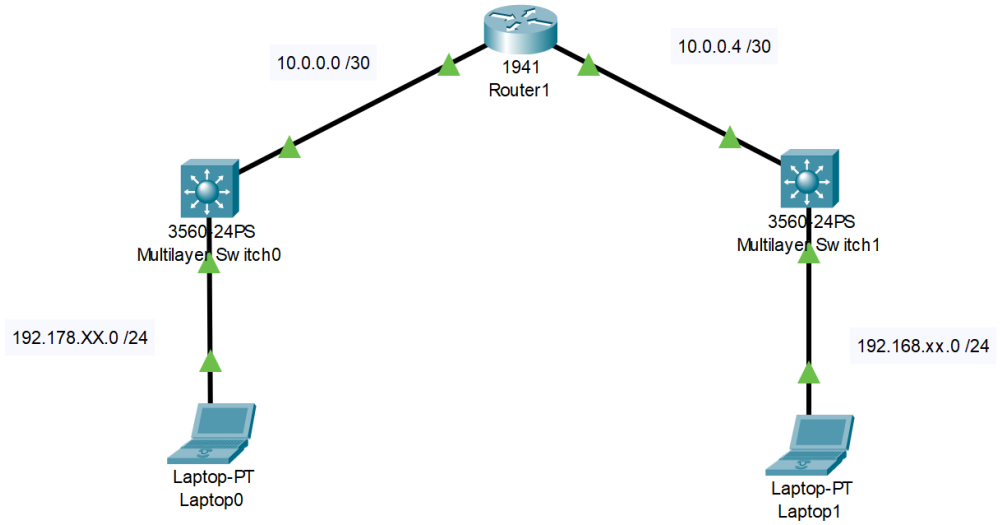
El proyecto requiere realizar una topología física donde se implementan dos
Switches multicapa y un router, estableciendo la funcionalidad y roles específicos de cada dispositivo en la red.
La configuración debe incluir la creación de VLANs (Virtual LANs) en ambos switches. Estas VLANs deben coincidir con las que se configuraron previamente en la simulación.

Dispositivos:

Cada integrante del equipo debe llevar una laptop (2 por grupo). Estas laptops se utilizarán para verificar la comunicación en cada VLAN.

Se utilizarán los mismos rangos de red que se implementaron en el Packet Tracer 192. 168.XX.0/24 para lado derecho, 192.178.XX.0/24 para lado izquierdo y 10.0.0.0 /30 para el enlace entre routers.

Referencia de implementación física:



4.4 Entregables

Se debe de entregar un enlace a su repositorio privado de GitHub, el cual debe contener:

Tipo	Descripción
Documentación Técnica	El manual técnico debe ser un archivo de tipo markdown, y debe contener capturas de la implementación de las topologías, detalle de todas configuraciones de cada dispositivo, IP´s asignadas, vlans, puertos, etc.
Archivo PKT	Archivo .pkt de la topología de Packet Tracer

Se debe agregar al auxiliar al repositorio como colaborador. Usuarios de github:

Sección A:

Tutor 1: Tiwue – Steven González

Tutor 2: fsquijada – Fredy Quijada

Sección N:

Tutor 1: JoseLacan – Jose Lacan

Tutor 2:allangomez72 – Allan Gomez

Fecha y hora límite de entrega: viernes 24 de octubre de 2025, antes de las 23:59.

5. Calificación

5.1 Resumen de Puntuaciones

Descripción de Ponderación	Valor
Configuración de la Red Simulada	**65**
DIGA	**8**
Subnetting correcto	1
VTP correcto	1
Ruteo InterVLAN correcto	1,5
Redundancia de routers correcta (HSRP)	2
RIP correcto	1,5
ACLs correctas	1
Biblioteca	**8**
Subnetting correcto	1
VTP correcto	1
Ruteo InterVLAN correcto	1,5
Redundancia de routers correcta (HSRP)	2
RIP correcto	1,5
ACLs correctas	1
T4	**7,5**
Subnetting correcto	1
VTP correcto	1
Ruteo InterVLAN correcto	1,5
Rutas estáticas correctas	3
ACLs correctas	1
S11	**8**
Subnetting correcto	1
VTP correcto	1
Ruteo InterVLAN correcto	1,5
Redundancia de routers correcta (HSRP)	2
OSPF correcto	1,5
ACLs correctas	1

S12	**8**
Subnetting correcto	1
VTP correcto	1
Ruteo InterVLAN correcto	1,5
OSPF correcto	1,5
Redundancia de routers correcta (HSRP)	2
ACLs correctas	1
Core	**15,5**
Subnetting correcto	1
RIP correcto	3
OSPF correcto	3
EIGRP correcto	3
Rutas estáticas correctas	2
Redistribuciones de rutas correctas	2
Etherchannel correcto	1,5
Conectividad	**10**
No conectividad entre distintas vlans	5
Conectividad entre misma vlans	5
Parte Física	**30**
Configuracion correcta	10
Ruteo dinámico/estático	10
Pings entre computadoras	10
Aspectos no funcionales	**5**
Pregunta 1	1.5
Pregunta 2	1.5
Manual Técnico	2
Penalizaciones	**0%**
Entrada tarde a la calificacion	-10%
No tener el proyecto listo para presentar	-10%
No realiza la parte física del proyecto	-100%
No se tiene al tutor agregado en el repositorio	-50%
No se usa el dominio y contraseña vtp correcto	-100%
No se sigue el esquema de id de vlans usando sus carnets	-100%

No se utilizó la topología del enunciado	-100%
Entrega o commit fuera de fecha	-100%
No uso FLSM ni VLSM para el subnetting de la red	-20%
No implementar los protocolos de enrutamiento de la manera indicada	-30%
TOTAL	**100**

5.2 Restricciones

- La parte simulada se desarrollará de manera INDIVIDUAL.
- La parte física se realizará en parejas.
- En el mismo repositorio creado para la práctica y proyecto 1 debe crearse una carpeta con nombre “Proyecto 2” en la cual se irá actualizando el desarrollo del proyecto.
- Entregas por otro medio que no sea **UEDI o Classroom** tendrán automáticamente una nota de 0 puntos.
- **Las entregas tarde tendrán automáticamente una nota de 0 puntos.**
- **Cualquier copia (PARCIAL O TOTAL)** tendrá una nota de 0 puntos y los responsables serán reportados a la Escuela de Ciencias y Sistemas.
- Las configuraciones deben realizarlas desde la CLI.
- El manual técnico debe ser un archivo de tipo markdown, y debe contener un manual de configuración con todos los detalles técnicos de la topología, configuración de cada dispositivo, IP´s asignadas, vlans, puertos, etc.
- La implementación de la red debe realizarse en Cisco Packet Tracer y el nombre del archivo debe ser Proyecto_2_#carnet.pkt
- Si durante la calificación se les pide realizar una instrucción o mostrar una configuración y el estudiante tarda en hacerla, tendrá una nota de 0 puntos en este apartado.