Anexos

Anexo A Ingeniería de requerimientos

A.1 Propósito

Contribuir al mejoramiento de la red de datos de la cooperativa Cosaalt R.L., para evitar gastos y tiempo innecesario en resolver los problemas generados por esta red poco eficiente.

A.2 Alcance

Este proyecto comenzará desde el análisis de la red de datos con la que cuenta la cooperativa, hasta la reestructuración de la red de datos, para la cual se utilizará todos los datos y resultados del análisis de la red de datos actual.

A.3 Definición, acrónimos y abreviaturas

UPS – Sistema de Alimentación Ininterrumpida

IEEE – Instituto de Ingenieros Eléctricos y Electrónicos

MDF – Main Distribution Frame (marco de distribución principal).

IDF – Cuadro intermedio de distribución.

ISO – Organización internaciones de normalización

Red de datos – Infraestructura creada con el propósito de transmitir información de cualquier naturaleza desde un punto a otro a través del intercambio de datos.

VPN – Virtual Private Network, o red privada virtual, permite crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet, y puede por ejemplo estar conectados de una punta del mundo a la otra.

Rack – base, estructura metálica o soporte cuya misión es alojar sistemas informáticos y redes de telecomunicaciones.

DNS – Sistema de nombres de dominio, es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes.

GNS3 – Graphical Network Simulator-3, es un simulador de redes de computadoras que permite a los usuarios diseñar, construir y simular redes complejas. Es una herramienta de software libre que se utiliza para simular redes de computadoras en un ambiente de laboratorio virtual.

Packet Tracer es un software desarrollado por Cisco Systems que permite a los usuarios crear y simular redes de computadoras.

A.4 Referencias

Referencia	Título	Ruta	Fecha	Autor
	Que es el FortiGate y cómo te ayuda a proteger tus dispositivos corporativos	https://cerounosoftware.com.mx/2022/04/22/que-es-fortigate-fortinet/#:~:text=%C2%BFPara%20que%20sirve%20Fortigate%3F,y%20bloqueando%20accesos%20no%20autorizados.	20/04/2023	Cero uno
2	Interfaces de red TCP/IP	https://www.ibm.com/docs/es/aix/7.1?topic=protocol-tcpip-network-interfaces	25/04/2023	

3	Estándares, modelos y normas internaciones de redes	https://es.slideshare.net/joseaortiz547/estndares-modelos-y-normas-internacionales-de-redes	08/05/2023	Jose Adalberto Cardona Ortiz
4	IEEE 802.3	https://standards.ieee.org/ieee/802.3/6003/	08/05/2023	IEEE S.A
5	Mantenimiento de redes de cableado: tipos, consideraciones y medidas	https://blog.conzultek.com/mantenimiento-de-redes	10/05/2023	Conzultek
6	Porque es necesario actualizar los servicios de TI en su empresa	https://www.clasesordenador.com/porque-es-necesario-actualizar-los-servicios-ti-de-su-empresa/	10/05/2023	Clasesordenador.com
7	Que es una conexión VPN, para qué sirve y qué ventajas tiene	https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene	21/05/2023	Iván Ramírez de Xataka Basics.
8	Sistema de nombres de dominio	https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio	22/05/2023	Wikipedia

Tabla 1: Tabla de referencias
Fuente: Elaboración propia

A.5 Resumen

El documento está organizado de acuerdo al formato establecido por la IEEE 802.3, exponiendo la reestructuración de una red de datos para la cooperativa Cosaalt R.L., el proyecto está

dividido por puntos. Para empezar, se describe la red y su contexto, los requisitos de la red y los apéndices o anexos.

A.6 Perspectiva del producto

La red es independiente y no tiene relación con ningún otro sistema.

A.7 Funcionalidad del producto

1. Compartir información y recursos

Hace referencia a que múltiples dispositivos compartan información y recursos, como archivos, impresoras y dispositivos de almacenamiento.

2. Comunicación

Un dispositivo puede conectarse a otro, ya sea a través de mensajes de texto, correo electrónico, voz, video o conferencias en línea. Además, mejora la productividad y la colaboración.

3. Accesibilidad de recursos compartidos

Los trabajadores pueden acceder a archivos y aplicaciones en servidores centralizados, lo que puede facilitar la administración y el mantenimiento de los sistemas de TI.

4. Seguridad

Se refiere a que los responsables de brindar seguridad a la red son los firewalls y el sistema de detección de intrusos, que ayudan a proteger los datos y la información de la empresa de amenazas externas e internas.

5. Monitoreo y gestión

Se refiere a la administración de la red, detectando problemas, diagnosticando fallo y realizando tareas de mantenimiento.

A.8 Restricciones

La red de datos debe cumplir con las restricciones, requerimientos, presupuesto y normas de la cooperativa “Cosaalt R.L.”, y de la mayoría de los estándares internaciones para garantizar el buen funcionamiento de la red.

A.9 Suposiciones y dependencias

Se supone que se contara con una disposición de los trabajadores para el desarrollo de los requerimientos de su labor diaria, y que se contara con el material necesario para la reestructuración de la red, se supone que la disponibilidad del ancho de banda será adecuado para satisfacer las demandas futuras, que la red es inherentemente segura sin implementar medidas de seguridad adecuadas, que la red actual puede escalar indefinidamente sin cambios en la arquitectura, se supone que la red siempre estará disponible sin interrupciones. También se depende de la aprobación del POA para el presupuesto de la implementación de la red, de una única conexión exclusiva a internet para la conectividad y de una tecnología de red específica como los protocolos de enrutamiento.

A.10 Evolución previsible del sistema

En un futuro, la red de datos debe ser actualizada nuevamente con la tecnología emergente y las demandas cambiantes para mantener una red eficiente y segura. Se deberá reestructurar la red tomando en cuenta el ancho de banda, tecnologías inalámbricas, probablemente una adopción de IPv6 para abordar la limitación de direcciones IP en IPv4, si es el caso, entre muchos otros requisitos que se consideren necesarios.

Anexo B: Planos a escala

B.1 Plano de la planta baja

Estos planos se encuentran en escala 1:100

Figura B.1.1: Plano a escala de la planta baja
Fuente: COSAALT

B.2 Plano del primer piso

Figura B.2.1: Plano a escala del primer piso
Fuente: COSAALT

B.3 Plano del segundo piso

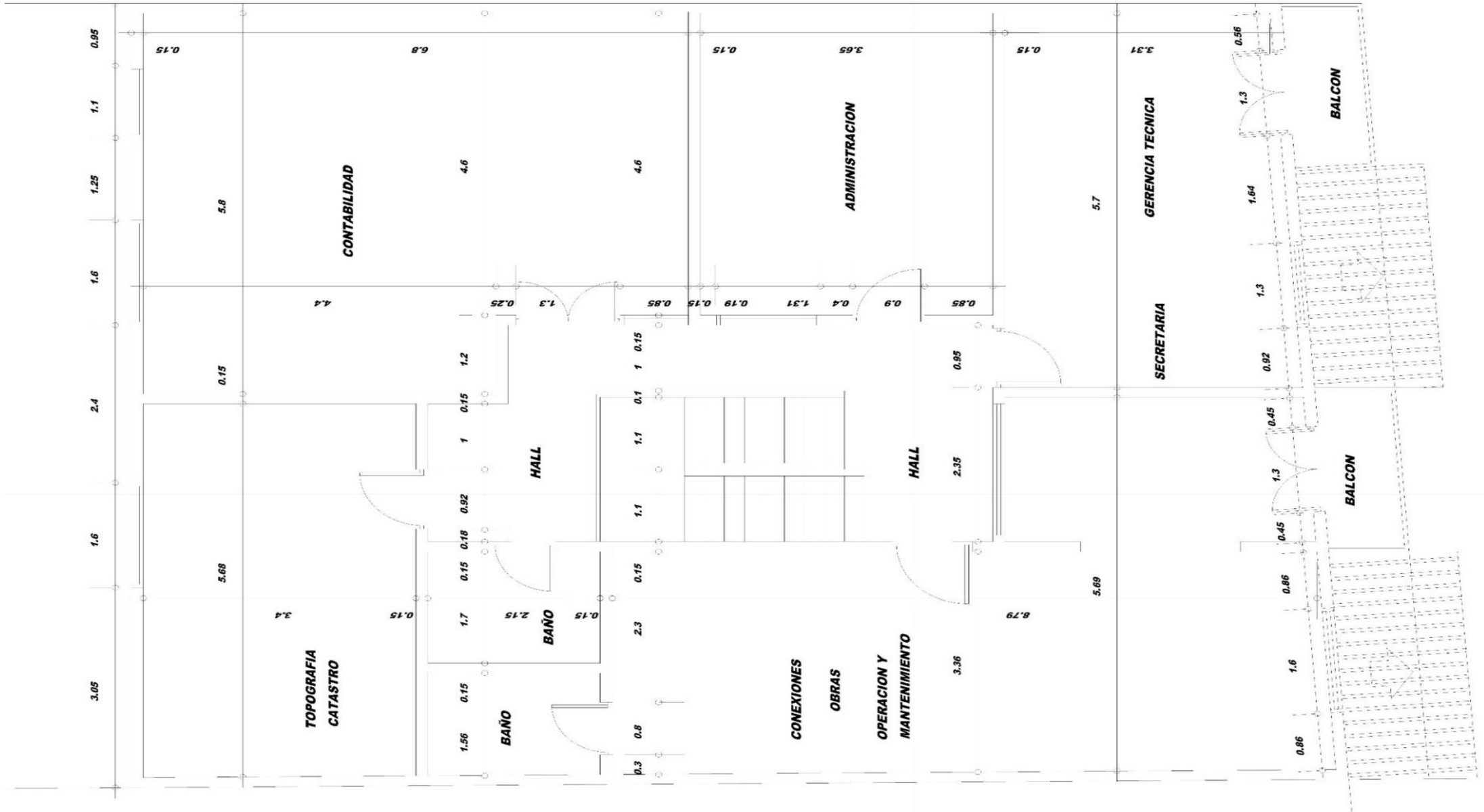


Figura B.3.1: Plano a escala de la planta baja
Fuente: COSAALT

B.4 Plano del tercer piso

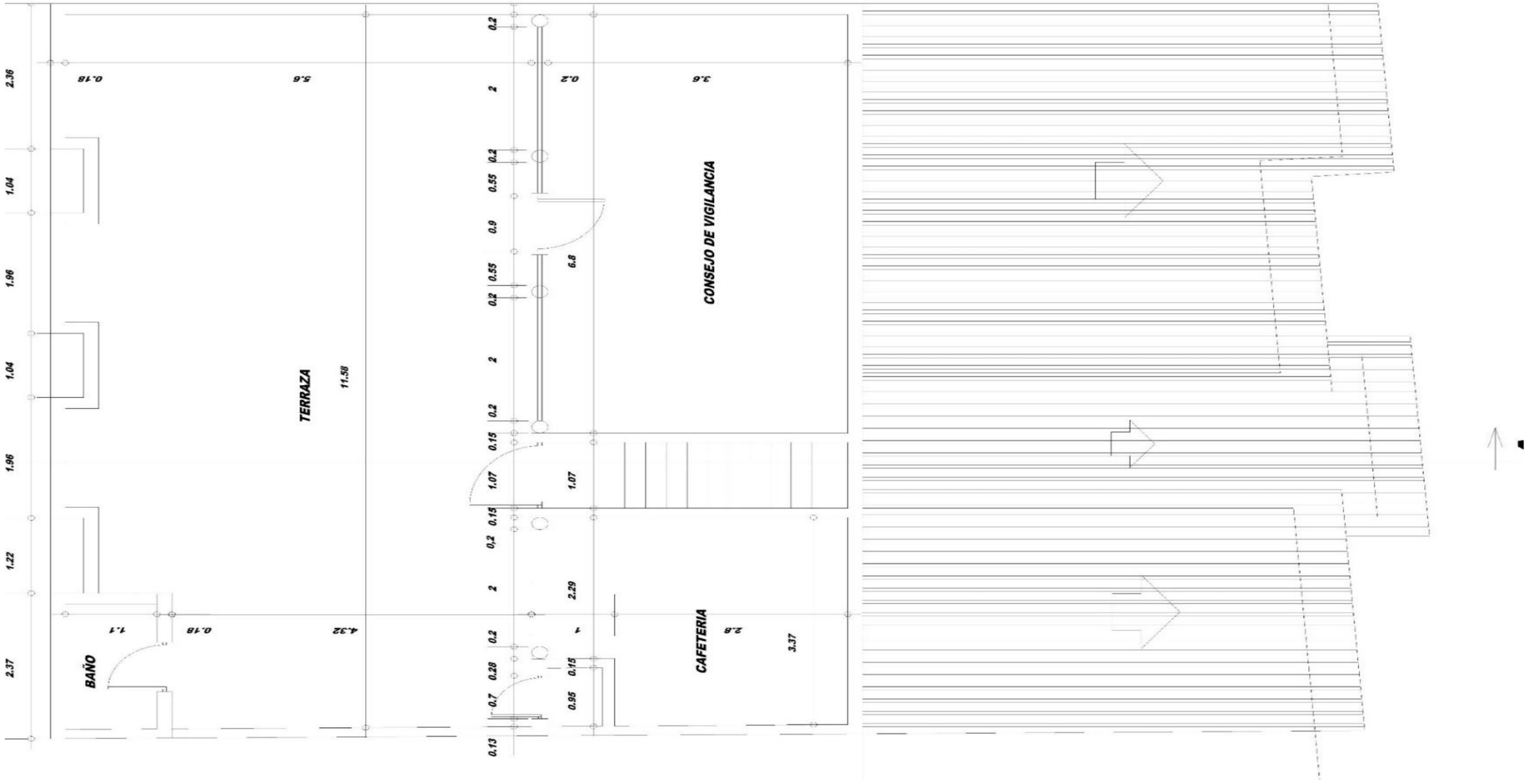


Figura B.4.1: Plano a escala de la planta baja
Fuente: COSAALT

Anexo C: Cartas de conformidad

C.1 Documentos de confirmación de colaboración con Cosaalt.

UNIVERSIDAD AUTÓNOMA
"JUAN MISAEL SARACHO"
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE INFORMATICA Y SISTEMAS
"Con Ética y Responsabilidad Social"

i-S Departamento de Informática y Sistemas

RECIBIDO
05 JUN. 2023
ATRIA. GERENCIA GENERAL
COSAALT R.L.
10:20
3803

As. Legal
12-06-23

Tarija, 01 de junio de 2023
FAC. CS.Y TEC, DPTO. INF. Y SIST, OF. Nº 168/23

Señor
Lic. José Luis Patiño
GERENTE GENERAL DE COSAALT R.L.
Presente.-

De mi mayor consideración:

A tiempo de saludarle y desearle éxitos en las delicadas funciones que desempeña diariamente, me dirijo a su autoridad a objeto de informarle que la estudiante **MARIA ISABEL SOSA RAMOS** con C.I. 7205030 Tja., cursa la materia de profesionalización **INF501 TALLER III** del Plan de Estudios de la carrera de Ingeniería Informática; actualmente se encuentra elaborando el proyecto intitulado "RESTRUCTURACION DE LA RED DE DATOS EN LA COOPERATIVA DE SERVICIOS PUBLICOS DE AGUA POTABLE Y ALCANTARILLADO SANITARIO TARIJA COSAALT R.L.". A tal efecto, agradeceré a su persona su colaboración a la mencionada estudiante y solicitamos a su autoridad pueda autorizar a los funcionarios de su institución proporcionar la información requerida para el desarrollo de su proyecto.

Agradeciendo de antemano su gentil deferencia, aprovecho la oportunidad para saludarle.

Atentamente,

UNIVERSIDAD AUTÓNOMA JUAN MISAEL SARACHO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
Tarija-Bolivia

M.Sc. Lic. Deysi Beatriz Arancibia Marquez
DIRECTORA a.i. DPTO. DE INFORMÁTICA Y SISTEMAS
FACULTAD DE CIENCIAS Y TECNOLOGIA

cc/Arch

Campus Universitario "El Tejar" - Tel. Fax. 591-6640265 - Casilla 51
Email. dis@uajms.edu.bo Web. dis.uajms.edu.bo
Tarija – Bolivia

Tarija, 28 de Agosto 2023

Señora

Lic. Deysi Arancibia

JEFE DEPARTAMENTO INFORMATICA Y SISTEMAS

UNIVERSIDAD AUTÓNOMA JUAN MISAEL SARACHO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE INFORMÁTICA
Fecha: 31 / Agosto /2023 Hora: 16:10
FIRMA

REF: Carta de Conformidad

Presente:

Reciba usted un cordial saludo.

Por medio dela presente,me dirijo a usted para informarle que el estudiante MARIA ISABEL SOSA RAMOS, nos ha hecho llegar su propuesta, para proponer un re diseño de la red de datos en el edificio de la cooperativa

Sin otro particular, agradecemos su colaboración prestada a nuestra Institución

Atentamente.

M.Sc. Lic. José Luis Patiño Ahazgo
GERENTE GENERAL
COSAALT R.L.

M.Sc. Lic. Deysi Beatriz Arancibia Marquez
DIRECTORA a.i. DPTO. INFORMÁTICA Y SISTEMAS
FACULTAD DE CIENCIAS Y TECNOLOGÍA
U.A.J.M.S.

C.2 Documento formal de aprobación de la propuesta de red por la Gerencia de COSAALT.

Cooperativa de Servicios Públicos de Agua Potable y Alcantarillado Sanitario Tarija
TARIJA - BOLIVIA

ES AGUA A TU SERVICIO
TARIJA - BOLIVIA

Tarija, Julio 23 de 2024
CITE OF. G. G. N° 504/2024

Señor
Ing. Fernando Cortez
DIRECTOR a. i. DEPARTAMENTO DE INFORMATICA Y SISTEMAS
Presente. -

De mi mayor Consideración:

Por intermedio de la presente, deseo que he revisado y comprendido la propuesta de re diseño de la red presentada por Sosa Ramos María Isabel, en el contexto de su tesis titulada: **"Diseño y simulación de una infraestructura de red escalable en la Cooperativa de Servicios Públicos de Agua Potable y Alcantarillado Sanitario Tarija COSAALT R.L."(edificio principal).** La propuesta ha sido analizada y discutida y estamos convencidos que las mejores sugerencias aportaran significativos beneficios a nuestra infraestructura tecnológica.

A través de la explicación de la propuesta presentada por la estudiante, hemos comprendido el estudio completo de su tesis y los beneficios que traerá el rediseño de la red en términos de:

- Seguridad
- Escalabilidad
- Estabilidad

Expresamos nuestra conformidad e interés en el rediseño de la red, reconociendo el impacto positivo que tendrá en la eficiencia operativa, la seguridad y la capacidad de crecimiento de COSAALT R.L. Valoramos el trabajo y la dedicación de Sosa Ramos María Isabel en la elaboración de esta propuesta.

Sin otro particular, agradecemos su colaboración prestada a nuestra institución.

Atentamente.

MSc. Lic. José Luis Patiño Anazgo
GERENTE GENERAL
COSAALT R.L

COOPERATIVA DE SERVICIOS DE AGUA Y ALCANTARILLADO
GERENCIA GENERAL
COSAALT R.L
TARIJA

c. Arch.

Ingavi esq. O'Connor N° 675
cosaalt-rl@cosaalt.org.bo
N° Piloto: 66 30595
Odeco: 66 42828
Líneas Gratuitas: 800109292
Emergencias: 178

C.3 Carta de aprobación por parte del docente.

Tarija 27 de noviembre de 2024

Señor: José Luis Patiño Añasgo

Gerente General de COSAALT

Presente.

Certificación

Por intermedio de la presente se certifica que la estudiante Maria Isabel Sosa Ramos a desarollado el proyecto "**Diseño y Simulación de una infraestructura de Red Escalable en la Cooperativa de Servicios públicos de agua potable y alcantarillado sanitario de Tarija COSAALT"**, dicho proyecto cumple con los requerimientos funcionales que fueron especificados en la norma.

Su proyecto, basado en la metodología **Top-Down**, contempla el desarrollo de una infraestructura de red con características de escalabilidad, seguridad y redundancia, aspectos que resultan esenciales para la solución planteada. La inclusión de tecnologías como **VLANs, HSRP, ACLs y QoS**, así como la integración de simuladores como **Cisco Packet Tracer, GNS3 y Sketchup**, refuerza la viabilidad técnica y educativa de su propuesta.

Sin otro particular, saluda a usted muy atentamente.

Elizabet Castro Figueroa

Docente de la asignatura DIS taller III

C.4 Cuestionario realizado a los encargados de TI para el análisis de la red

Entrevista al encargado de TI

¿Cuenta con un diseño lógico y una topología de red actual?

R.- Se cuenta con un diseño lógico y con una topologia mixta, estrella y lineal

¿Cómo está estructurada la topología de red (centralizada, distribuida, etc)?

R.- Centralizada

¿Qué tipos de dispositivos utilizan en la red actual?

R.- Router, switches administrables y no administrables, acces point, servidores (Web, QoS, BD) y Firewall

¿Cuántos dispositivos de red tiene la empresa, donde están ubicados?

R.- 220 dispositivos entre los que se encuentran 66 computadoras, 6 table 3 servidores, 1 router, 4 switches, 2 Firewalls, 54 impresoras

¿Cuál es la marca y modelo de los principales dispositivos de red?

R.- Servidor Dell EMC, powerEdge R740 server, Servidor IBM system x3650 m4,

¿Qué capacidad tienen los equipos de red en términos de rendimiento y escalabilidad?

R.- Capacidad media

¿Cómo se gestiona el rendimiento de la red? ¿Existen herramientas de monitoreo utilizadas regularmente?

R.- Se utiliza routerOs de Microtik para monitorear la red

¿La red está dividida en segmentos o subredes?

R.- En subredes (192.25.3.0 para equipos de computo alambrica inalambricos, 192.25.4.0 moviles, 192.25.1.0 impresoras, 192.25.2 dispositivos inalambricos).

¿Cuáles son las políticas de seguridad de la red?

R.- Se tienen politicas de acceso a la red alambrica, inalambrica, a servidores corporativos o de gestión, a la internet.

¿Que medidas de seguridad se han implementado para proteger la red contra amenazas externas?

R.- Politicas de Firewall

¿Como están asignadas las direcciones IP en la red?

R.- Se tiene asignación estática

¿Cuál es la capacidad de ancho de banda de la red?

R.- Se tienen 2 capacidades: 10/100 Mbps y 10/100/1000 Mbps

velocidad 60 mbps

proveedor tigo

¿Cuáles son los problemas más comunes que enfrenta la red?

R.- El cableado

¿Cómo se gestionan y resuelven estos problemas?

R.- De acuerdo a la necesidad. No se cuenta con procedimientos establecidos para la atención

¿Existen áreas de la red que necesiten mejoras urgentes o actualizaciones?

R.- el área de computo

¿Hay planes futuros para actualiza o expandir la red?

R.- no

¿Qué cambios están considerando?

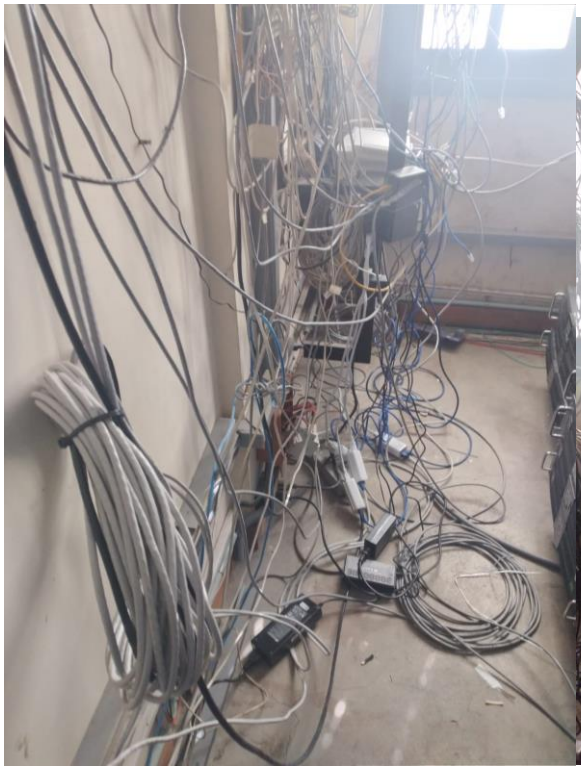
R.- el cableado

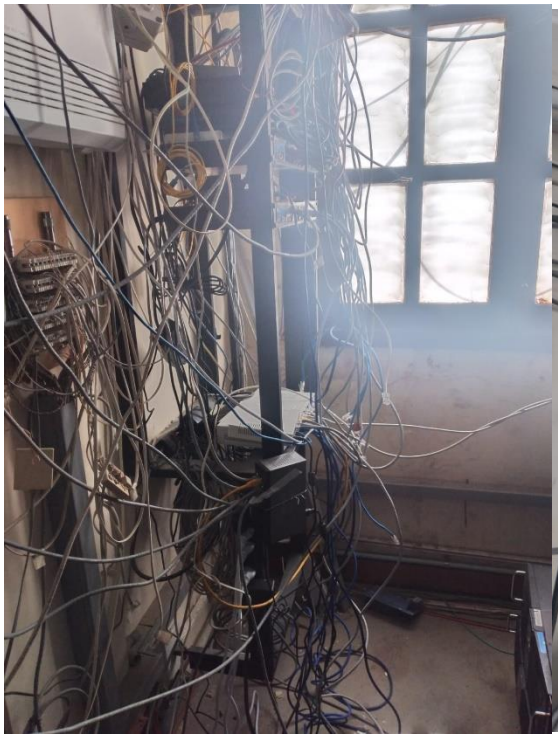
¿Qué áreas de trabajo requieren prioridad para su funcionamiento?

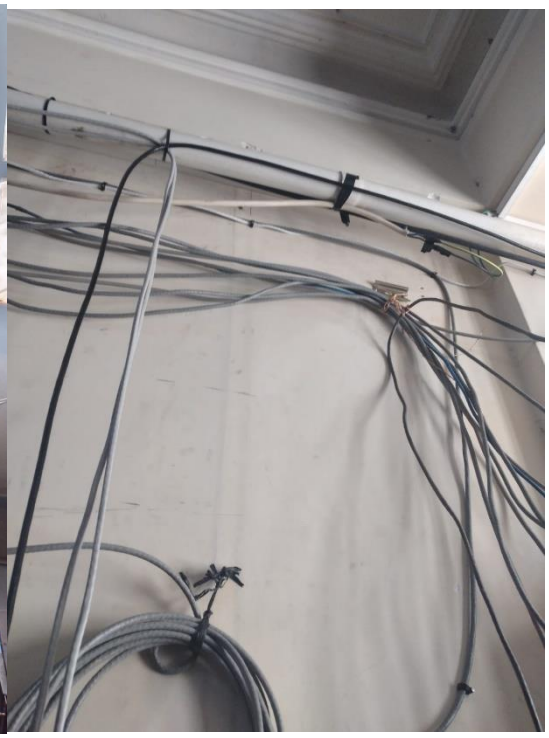
R.- Centro de cómputo, cajas, atención al cliente, archivos

Lic. Iván Ríos Orellano
ENC. DESARROLLO Y MTTO. DE SIST. COMPUTARIZADOS a.i.
COSAALT R.L.

C.5 Imágenes de referencia para probar el estado de la red física








IBM


IBM

Anexo D: Manual de configuración

D.1 Introducción

Este manual se centra en la simulación de una red empresarial diseñada para una empresa mediana, utilizando Cisco Packet Tracer como herramienta principal. Su objetivo es proporcionar una guía clara y detallada de la configuración, destacando los principios teóricos detrás de cada paso implementado.

La red se diseñó para soportar las operaciones diarias de la empresa, con enfoque en escalabilidad, redundancia y segmentación. Se usaron VLANs para segmentar departamentos, HSRP para redundancia de gateway y OSPF para enrutamiento dinámico. Aunque no se implementa físicamente, la simulación busca reflejar un diseño listo para producción.

La empresa en cuestión opera en un edificio de tres pisos, con diversas áreas administrativas, técnicas y operativas. Dado el crecimiento esperado, se diseñó una red con suficiente capacidad de expansión.

El diseño incluye:

- **Segmentación de la red:** Se implementaron VLANs para aislar departamentos y mejorar la eficiencia y seguridad.
- **Redundancia:** Se emplearon protocolos como HSRP para garantizar continuidad de servicio en caso de fallos.
- **Enrutamiento dinámico:** Se configuró OSPF para optimizar la comunicación entre redes internas y el ISP.

Este manual también sirve como guía para futuros administradores, proporcionando una base sólida para el mantenimiento y escalabilidad de la red.

D.2 Diseño de la red

La red utiliza una **topología jerárquica**, donde los switches principales (MDF) conectan con los secundarios (IDF) en cada piso. Esta topología es ideal para empresas medianas, ya que:

- Mejora la gestión del tráfico.
- Facilita la localización de fallos.
- Ofrece un camino claro para la escalabilidad.

D.2.1 Segmentación de la Red

Se implementaron VLANs para dividir el tráfico según las funciones de cada departamento. Esto reduce el dominio de colisión y proporciona mayor control sobre el flujo de datos.

Estructura de la red

La red consta de los siguientes componentes principales:

- **Routers:** Actúan como el gateway de la red interna y conectan al ISP.
- **Switches MDF:** Distribuyen el tráfico hacia los switches IDF y otros dispositivos principales.
- **Switches IDF:** Conectan a los dispositivos finales en cada piso.
- **Servidores:** Proporcionan servicios esenciales como DNS, y QoS.

N°	VLAN	Cantidad de Equipos Actual	Máscara	Rango de IPs	IP del Gateway	Rango Futuro Aprox.
10	Comercial y Atención al Cliente	38	255.255.255.192	192.25.3.1 - 192.25.3.62	192.25.3.1	Hasta 62 dispositivos
20	Administrativa y Financiera	21	255.255.255.224	192.25.3.65 - 192.25.3.94	192.25.3.65	Hasta 30 dispositivos
30	Técnica y Operativa	13	255.255.255.224	192.25.3.97 - 192.25.3.126	192.25.3.97	Hasta 30 dispositivos
40	Directiva y Supervisión	13	255.255.255.224	192.25.3.129 - 192.25.3.158	192.25.3.129	Hasta 30 dispositivos
50	Sistemas de Cómputo	3	255.255.255.240	192.25.3.161 - 192.25.3.174	192.25.3.161	Hasta 14 dispositivos
80	Impresoras	56	255.255.255.192	192.25.1.1 - 192.25.1.62	192.25.1.1	Hasta 62 dispositivos

60	Access Point	8	255.255.255.240	192.25.3.241 - 192.25.3.254	192.25.3.241	Hasta 14 dispositivos
70	Routers y Servidores	N/A	255.255.255.248	192.25.4.1 - 192.25.3.254	192.25.4.1	Hasta 6 dispositivos

Tabla 2: Segmentación de la red
Fuente: Elaboración propia

D.2.2 Diagrama de la red

Diagrama físico

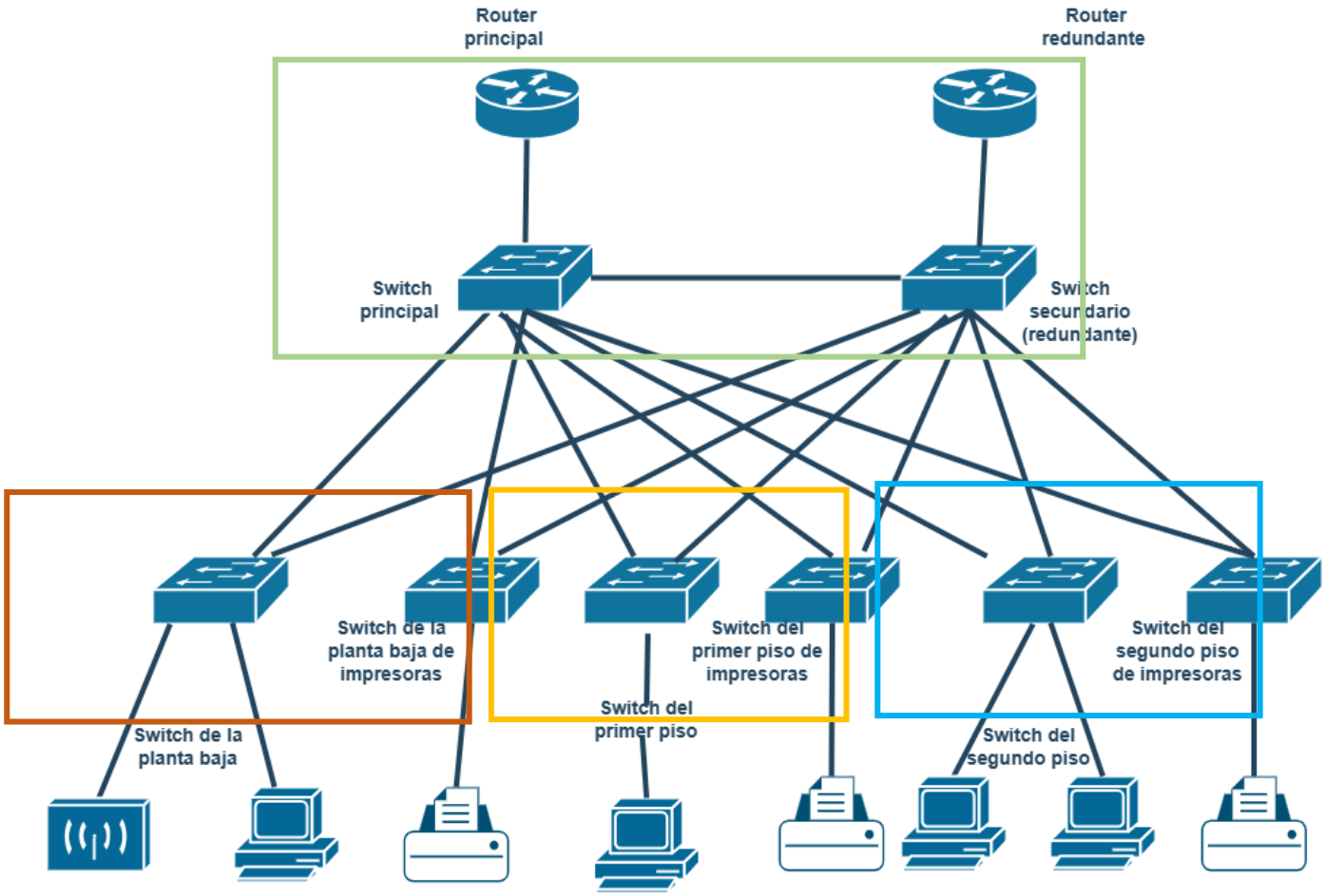


Figura D.2.1: diagrama de red
Fuente: Elaboración propia

Cuarto de MDF

Rack IDF de la planta baja

Rack IDF de la primera planta

Rack IDF de la segunda planta

Diagrama lógico

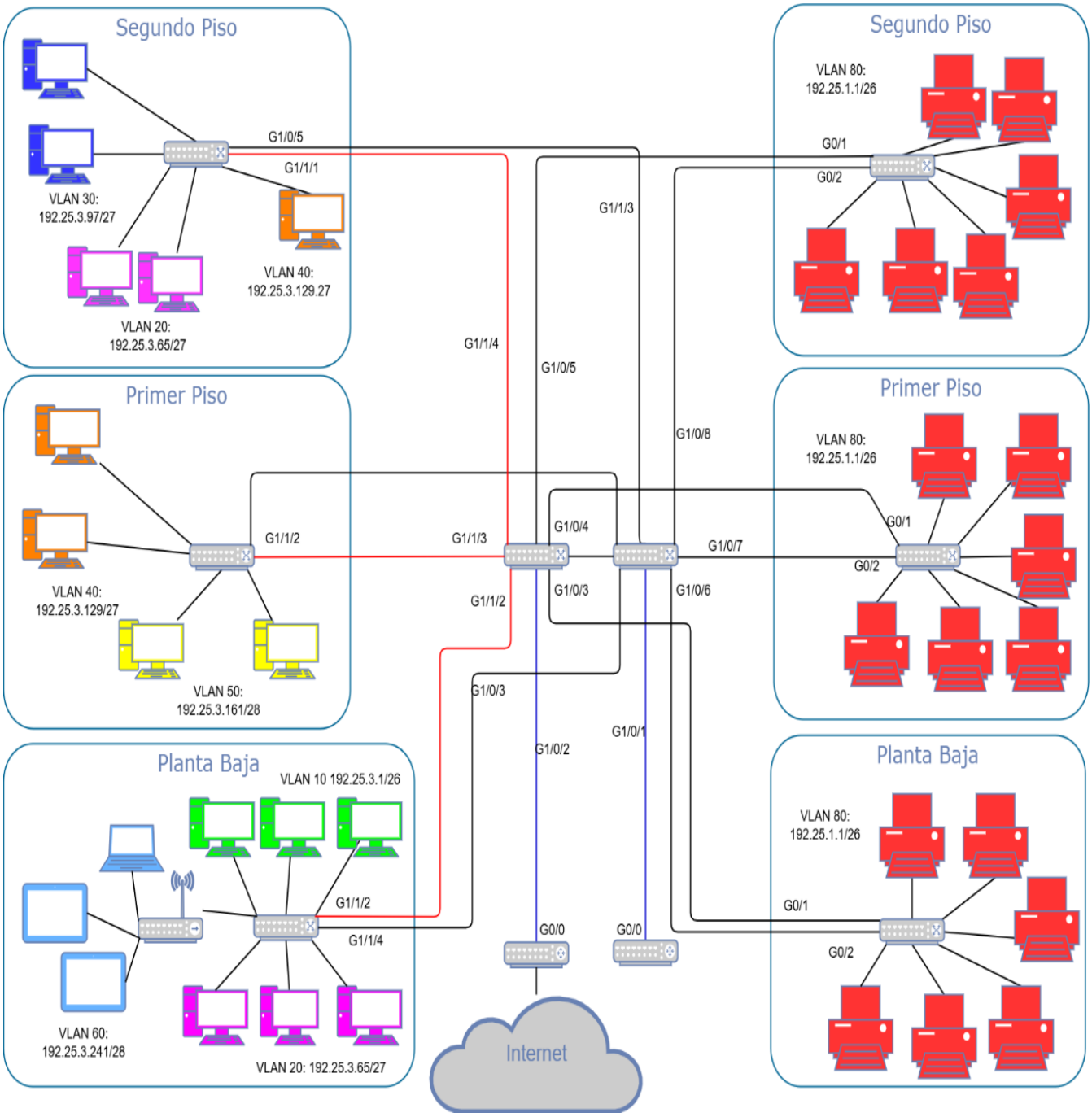


Figura D.2.2: diagrama logico
Fuente: Elaboración propia

D.3 Lista de equipos

D.3.1 Routers

Dispositivo	Modelo	Funciones
Router Principal (R1)	Cisco 2911	Interconexión de VLANs, NAT, HSRP, OSPF, Servidor DHCP.
Router de Respaldo (R2)	Cisco 2911	Redundancia (HSRP), respaldo para NAT, OSPF, y DHCP en caso de falla de R1.

Tabla 3: Lista de Routers utilizados en el diseño
Fuente: Elaboración propia

D.3.2 Switches

Dispositivo	Modelo	Ubicación	Funciones
Switch MDF1 (Principal)	Cisco 2960-24TT	Sala de Servidores	Distribución de VLANs, EtherChannel, enlace a routers y switches de piso.
Switch MDF2 (Respaldo)	Cisco 2960-24TT	Sala de Servidores	Redundancia en el tráfico de red, EtherChannel, enlace a switches de piso.
Switch IDF1 (Piso 1)	Cisco 2960-24TT	Piso 1	Conexión de dispositivos VLAN 10, 20 y 70.
Switch IDF2 (Piso 2)	Cisco 2960-24TT	Piso 2	Conexión de dispositivos VLAN 40 y 50.
Switch IDF3 (Piso 3)	Cisco 2960-24TT	Piso 3	Conexión de dispositivos VLAN 30, 20 y 40.

Tabla 4: Lista de Switches utilizados en el diseño
Fuente: Elaboración propia

D.3.3 Servidores

Servidor	Características	Funciones
Servidor Web	1 NIC, IP estática asignada	Alojar página web de la empresa.
Servidor Base de Datos	1 NIC, IP estática asignada	Gestión de información empresarial.
Servidor de QoS	1 NIC, IP estática asignada	Priorización de tráfico para aplicaciones críticas.

Tabla 5: Lista de Servidores utilizados en el diseño
Fuente: Elaboración propia

D.3.4 Dispositivos Finales

Tipo de Dispositivo	Cantidad	Ubicación/Conexión
Computadoras de Escritorio	100	Distribuidas en todas las VLANs.
Impresoras	56	VLAN 70 (Red de Impresoras).
Access Points	8	VLAN 60 (Red Inalámbrica).

Tabla 6: Lista de dispositivos finales utilizados en el diseño
Fuente: Elaboración propia

D.3.5 Otros Equipos y Materiales

Equipo/Material	Cantidad	Propósito
Cables Ethernet (Cat6)	120	Conexión de dispositivos finales y switches.

Cables de Fibra Óptica	6	Enlaces troncales entre routers y switches MDF.
Módulos SFP	6	Extensión de enlaces de fibra para los routers y switches principales.

Tabla 7: Lista de materiales de conexión utilizados en el diseño
Fuente: Elaboración propia

D.4 Configuración detallada

D.4.1 Configuración de R1- Router Principal

R1 actua como el router principal de la red, con configuraciones de HSRP, OSPF, RIP y DHCP. También se definieron las subinterfaces para cada VLAN

Paso 1: Configuración de Hostname

```
R1> enable

R1# configure terminal

R1(config)# hostname R1
```

Paso 2: Configuración de Interfaces para las VLANs

Conectaremos el router a un switch en el MDF mediante interfaces subinterfaces para cada VLAN en el enlace troncal.

1. Habilitar el enlace troncal en la interface GigabitEthernet0/0

```
R1(config)# interface gigabitEthernet 0/0

R1(config-if)# no shutdown
```

2. **Crear Subinterfaces** para cada VLAN en la interfaz troncal **GigabitEthernet0/0** y asignar IPs de gateway de acuerdo con las VLANs:

// VLAN Comercial y Atención al Cliente

```
R1(config)# interface gigabitEthernet 0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.25.3.1 255.255.255.192
```

// VLAN Administrativa y Financiera

```
R1(config)# interface gigabitEthernet 0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.25.3.65 255.255.255.224
```

// VLAN Técnica y Operativa

```
R1(config)# interface gigabitEthernet 0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.25.3.97 255.255.255.224
```

// VLAN Directiva y Supervisión

```
R1(config)# interface gigabitEthernet 0/0.40
R1(config-subif)# encapsulation dot1Q 40
R1(config-subif)# ip address 192.25.3.129 255.255.255.224
```

// VLAN Sistemas de Cómputo

```
R1(config)# interface gigabitEthernet 0/0.50
```

```
R1(config-subif)# encapsulation dot1Q 50

R1(config-subif)# ip address 192.25.3.161 255.255.255.240
```

// VLAN Access Point

```
R1(config)# interface gigabitEthernet 0/0.60

R1(config-subif)# encapsulation dot1Q 60

R1(config-subif)# ip address 192.25.3.241 255.255.255.240
```

// VLAN Routers y Servidores

```
R1(config)# interface gigabitEthernet 0/0.70

R1(config-subif)# encapsulation dot1Q 70

R1(config-subif)# ip address 192.25.4.1 255.255.255.248
```

// VLAN Impresoras

```
R2(config)# interface gigabitEthernet 0/0.80

R2(config-subif)# encapsulation dot1Q 80

R2(config-subif)# ip address 192.25.1.2 255.255.255.192
```

Paso 3: Configuración del Enrutamiento entre VLANs

Para interconectar las VLANs y permitir que se comuniquen entre sí, configuraremos **RIP versión 2** en ambos routers. Esta versión de RIP permite enrutar subredes dentro de la misma red de clase y es compatible con Cisco Packet Tracer.

```
R1(config)# router rip

R1(config-router)# version 2
```

```
R1(config-router)# no auto-summary
```

// Anunciamos las redes conectadas al R1

```
R1(config-router)# network 192.25.3.0

R1(config-router)# network 192.25.4.0

R1(config-router)# network 192.25.1.0
```

Paso 4: Configuración de la Ruta de Salida al ISP

Para permitir la comunicación con redes externas a través del ISP, configuramos una ruta estática en R1:

```
R1(config)# ip route 0.0.0.0 0.0. 0.0 192.25.3.254
```

Paso 5: Configuracion de HSRP para Cada VLAN

// VLAN 10: Comercial y Atención al Cliente

```
R1(config)# interface gigabitEthernet 0/0.10

R1(config-if)# standby 10 ip 192.25.3.1

R1(config-if)# standby 10 priority 110

R1(config-if)# standby 10 preempt
```

// VLAN 20: Administrativa y Financiera

```
R1(config)# interface gigabitEthernet 0/0.20

R1(config-if)# standby 20 ip 192.25.3.65

R1(config-if)# standby 20 priority 110

R1(config-if)# standby 20 preempt
```

// VLAN 30: Técnica y Operativa

```
R1(config)# interface gigabitEthernet 0/0.30

R1(config-if)# standby 30 ip 192.25.3.97

R1(config-if)# standby 30 priority 110

R1(config-if)# standby 30 preempt
```

// VLAN 40: Directiva y Supervisión

```
R1(config)# interface gigabitEthernet 0/0.40

R1(config-if)# standby 40 ip 192.25.3.129

R1(config-if)# standby 40 priority 110

R1(config-if)# standby 40 preempt
```

// VLAN 50: Sistemas de Cómputo

```
R1(config)# interface gigabitEthernet 0/0.50

R1(config-if)# standby 50 ip 192.25.3.161

R1(config-if)# standby 50 priority 110

R1(config-if)# standby 50 preempt
```

// VLAN 60: Access Point

```
R1(config)# interface gigabitEthernet 0/0.60

R1(config-if)# standby 60 ip 192.25.3.241

R1(config-if)# standby 60 priority 110

R1(config-if)# standby 60 preempt
```

// VLAN 80: Impresoras

```
R1(config)# interface gigabitEthernet 0/0.80
R1(config-if)# standby 80 ip 192.25.1.1
R1(config-if)# standby 80 priority 110
R1(config-if)# standby 80 preempt
```

// VLAN 70: Routers y Servidores

```
R1(config)# interface gigabitEthernet 0/0.70
R1(config-if)# standby 70 ip 192.25.4.1
R1(config-if)# standby 70 priority 110
R1(config-if)# standby 70 preempt
```

Paso 6: Configuracion de OSPF

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.25.3.0 0.0.0.255 area 0
R1(config-router)# network 192.25.1.0 0.0.0.63 area 0
R1(config-router)# network 192.25.4.0 0.0.0.7 area 0
```

Paso 7: Configuracionde DHCP

//VLAN 10 (Comercial y Atención al Cliente)

```
ip dhcp pool VLAN10
 network 192.25.3.0 255.255.255.192
```

```
 default-router 192.25.3.1

 dns-server 8.8.8.8

 lease 7
```

// VLAN 20 (Administrativa y Financiera)

```
ip dhcp pool VLAN20

 network 192.25.3.64 255.255.255.224

 default-router 192.25.3.65

 dns-server 8.8.8.8

 lease 7
```

// VLAN 30 (Técnica y Operativa)

```
ip dhcp pool VLAN30

 network 192.25.3.96 255.255.255.240

 default-router 192.25.3.97

 dns-server 8.8.8.8

 lease 7
```

//VLAN 40 (Directiva y Supervisión)

```
ip dhcp pool VLAN40

 network 192.25.3.129 255.255.255.224

 default-router 192.25.3.130

 dns-server 8.8.8.8
```

```
lease 7
```

//VLAN 50 (Sistemas de Cómputo)

```
ip dhcp pool VLAN50
 network 192.25.3.161 255.255.255.240
 default-router 192.25.3.162
 dns-server 8.8.8.8
 lease 7
```

//VLAN 60 (Access Point)

```
ip dhcp pool VLAN60
 network 192.25.3.241 255.255.255.240
 default-router 192.25.3.242
 dns-server 8.8.8.8
 lease 7
```

//VLAN 80 (Impresoras en la red 192.25.1.0/29)

```
ip dhcp pool VLAN80
 network 192.25.1.1 255.255.255.192
 default-router 192.25.1.2
 dns-server 8.8.8.8
 lease 7
```

D.4.2 Configuración del r2(router de respaldo)

R2 es el router secundario con configuración HSRP, RIP para redundancia y como respaldo en caso de falla de R1

Paso 1: Configuración de Hostname

```
R2> enable

R2# configure terminal

R2(config)# hostname R2
```

Paso 2: Configuración de las Subinterfaces y VLAN de Impresoras

Configuramos las subinterfaces de las VLAN que estarán respaldadas en R2, incluyendo la VLAN de impresoras.

// Interface principal para troncal en gigabitEthernet 0/0

```
R2(config)# interface gigabitEthernet 0/0

R2(config-if)# no shutdown
```

// VLAN de Impresoras

```
R2(config)# interface gigabitEthernet 0/0.80

R2(config-subif)# encapsulation dot1Q 80

R2(config-subif)# ip address 192.25.1.2 255.255.255.192
```

Paso 3: Configuración del Enrutamiento RIP en R2

Para habilitar la comunicación de todas las VLANs, configuramos RIP en R2.

```
R2(config)# router rip
```

```
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

// Anunciamos las redes conectadas al R2

```
R2(config-router)# network 192.25.3.0
R2(config-router)# network 192.25.1.0
R2(config-router)# network 192.25.4.0
```

Paso 4: Configuracion de HSRP para Cada VLAN

// VLAN 10: Comercial y Atención al Cliente

```
R2(config)# interface gigabitEthernet 0/0.10
R2(config-if)# standby 10 ip 192.25.3.1
R2(config-if)# standby 10 priority 100
R2(config-if)# standby 10 preempt
```

// VLAN 20: Administrativa y Financiera

```
R2(config)# interface gigabitEthernet 0/0.20
R2(config-if)# standby 20 ip 192.25.3.65
R2(config-if)# standby 20 priority 100
R2(config-if)# standby 20 preempt
```

// VLAN 30: Técnica y Operativa

```
R2(config)# interface gigabitEthernet 0/0.30
R2(config-if)# standby 30 ip 192.25.3.97
```

```
R2(config-if)# standby 30 priority 100
R2(config-if)# standby 30 preempt
```

// VLAN 40: Directiva y Supervisión

```
R2(config)# interface gigabitEthernet 0/0.40
R2(config-if)# standby 40 ip 192.25.3.129
R2(config-if)# standby 40 priority 100
R2(config-if)# standby 40 preempt
```

// VLAN 50: Sistemas de Cómputo

```
R2(config)# interface gigabitEthernet 0/0.50
R2(config-if)# standby 50 ip 192.25.3.161
R2(config-if)# standby 50 priority 100
R2(config-if)# standby 50 preempt
```

// VLAN 60: Access Point

```
R2(config)# interface gigabitEthernet 0/0.60
R2(config-if)# standby 60 ip 192.25.3.241
R2(config-if)# standby 60 priority 100
R2(config-if)# standby 60 preempt
```

// VLAN 80: Impresoras

```
R2(config)# interface gigabitEthernet 0/0.80
R2(config-if)# standby 80 ip 192.25.1.1
```

```
R2(config-if)# standby 80 priority 100

R2(config-if)# standby 80 preempt
```

// VLAN 70: Routers y Servidores

```
R2(config)# interface gigabitEthernet 0/0.70

R2(config-if)# standby 70 ip 192.25.4.1

R2(config-if)# standby 70 priority 100

R2(config-if)# standby 70 preempt
```

Paso 5: Configuracion de OSPF

```
R2(config)# router ospf 1

R2(config-router)# router-id 2.2.2.2

R2(config-router)# network 192.25.3.0 0.0.0.255 area 0

R2(config-router)# network 192.25.1.0 0.0.0.63 area 0

R2(config-router)# network 192.25.4.0 0.0.0.7 area 0
```

D.4.3 Configuracion del main switch1

Paso 1: configuración de VLANS

```
Switch(config)# vlan 10

Switch(config-vlan)# name Comercial_Atencion

Switch(config-vlan)# exit
```

```
Switch(config)# vlan 20
```

```
Switch(config-vlan)# name Administrativa_Financiera

Switch(config-vlan)# exit
```

```
Switch(config)# vlan 30

Switch(config-vlan)# name Tecnica_Operativa

Switch(config-vlan)# exit
```

```
Switch(config)# vlan 40

Switch(config-vlan)# name Directiva_Supervision

Switch(config-vlan)# exit
```

```
Switch(config)# vlan 50

Switch(config-vlan)# name Sistemas_Computo

Switch(config-vlan)# exit
```

```
Switch(config)# vlan 60

Switch(config-vlan)# name Access_Point

Switch(config-vlan)# exit
```

```
Switch(config)# vlan 80
```

```
Switch(config-vlan)# name Impresoras

Switch(config-vlan)# exit
```

Paso 2: configuracion de interfaces troncolas

Conexión al router R1

```
Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80

Switch(config-if)# exit
```

Conexion al switch de la planta baja

```
Switch(config)# interface gigabitEthernet 1/1/2

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,70

Switch(config-if)# exit
```

Conexion al switch del primer piso

```
Switch(config)# interface gigabitEthernet 1/1/3

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 40,50

Switch(config-if)# exit
```

Conexion al switch del segundo piso

```
Switch(config)# interface gigabitEthernet 1/1/4
```

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

Switch(config-if)# switchport trunk allowed vlan 30,20,40

Switch(config-if)# exit
```

Conexión a los switches de impresoras

```
Switch(config)# interface range gigabitEthernet 1/0/3- gigabitEthernet 1/0/5

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 80

Switch(config-if)# exit
```

D.4.4 Conexión al switch main-switch2

```
interface range GigabitEthernet1/0/23 – 1/0/24

 switchport mode trunk

 channel-group 1 mode active

 no shutdown
```

```
interface Port-channel1

 switchport mode trunk
```

configuracion de STP

```
spanning-tree vlan 1,3,5,7 priority 4096
```

D.4.5 Configuración del main switch2

Paso 1: configuración de VLANS

```
Switch(config)# vlan 10
Switch(config-vlan)# name Comercial_Atencion
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 20
Switch(config-vlan)# name Administrativa_Financiera
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 30
Switch(config-vlan)# name Tecnica_Operativa
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 40
Switch(config-vlan)# name Directiva_Supervision
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 50
Switch(config-vlan)# name Sistemas_Computo
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 60
Switch(config-vlan)# name Access_Point
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 80
Switch(config-vlan)# name Impresoras
Switch(config-vlan)# exit
```

Paso 2: configuracion de interfaces troncolas

Conexión al router R2

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80
Switch(config-if)# exit
```

Conexión al switch de la planta baja

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,60
Switch(config-if)# exit
```

Conexión al switch del primer piso

```
Switch(config)# interface gigabitEthernet 1/0/4
```

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

Switch(config-if)# switchport trunk allowed vlan 40,50

Switch(config-if)# exit
```

Conexión al switch del segundo piso

```
Switch(config)# interface gigabitEthernet 1/0/5

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 30,20,40

Switch(config-if)# exit
```

Conexión a los switches de impresoras

```
Switch(config)# interface range gigabitEthernet 1/0/6- gigabitEthernet 1/0/8

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 80

Switch(config-if)# exit
```

D.4.6 Conexion al switch MAIN-SWITCH1

```
interface range GigabitEthernet1/0/23 – 1/0/24

 switchport mode trunk

 channel-group 1 mode active

 no shutdown
```

```
interface Port-channel1
```

```
switchport mode trunk
```

Configuracion de STP

```
spanning-tree vlan 2,4,6,8 priority 4096
```

D.4.7 Configuración del switch de la planta baja

Paso 1: configuración de la interfaz de conexión al switch Main-Switch1 como troncal

```
Switch(config)# interface gigabitEthernet 1/1/2

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,60

Switch(config-if)# exit
```

Paso 2: configuración de la interfaz de conexión al switch Main-Switch2 como troncal

```
Switch(config)# interface gigabitEthernet 1/1/4

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,60

Switch(config-if)# exit
```

Paso 3: configuración de puertos de acceso a las VLANs

// Asignar puertos a VLAN 10

```
Switch(config)# interface range gigabitEthernet 1/0/17 – 1/0/24

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 10

Switch(config-if-range)# exit
```

// Asignar puertos a VLAN 20

```
Switch(config)# interface range gigabitEthernet 1/0/3 – 1/0/10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
```

// Asignar puertos a VLAN 60

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 60
Switch(config-if-range)# exit
```

D.4.8 Configuración del switch del primer piso

Paso 1: configuración de la interfaz de conexión al switch Main-Switch1 como troncal

```
Switch(config)# interface gigabitEthernet 1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 40,50
Switch(config-if)# exit
```

Paso 2: configuración de la interfaz de conexión al switch Main-Switch2 como troncal

```
Switch(config)# interface gigabitEthernet 1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 40,50
```

```
Switch(config-if)# exit
```

Paso 3: configurar los puertos de acceso en las VLANs

// Asignar puertos a VLAN 40

```
Switch(config)# interface range gigabitEthernet 1/0/3 – 1/0/14
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 40
Switch(config-if-range)# exit
```

// Asignar puertos a VLAN 50

```
Switch(config)# interface range gigabitEthernet 1/0/21 – 1/0/24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 50
Switch(config-if-range)# exit
```

D.4.9 Configuración del switch del segundo piso

Paso 1: configuración de la interfaz de conexión al switch Main-Switch1 como troncal

```
Switch(config)# interface gigabitEthernet 1/1/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 30,20,40
Switch(config-if)# exit
```

Paso 2: configuración de la interfaz de conexión al switch Main-Switch2 como troncal

```
Switch(config)# interface gigabitEthernet 1/1/5
```

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

Switch(config-if)# switchport trunk allowed vlan 30,20,40

Switch(config-if)# exit
```

Paso 3: configuración de los puertos de acceso en las VLANs

// Asignar puertos a VLAN 30

```
Switch(config)# interface range gigabitEthernet 1/0/3 – 1/0/10

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 30

Switch(config-if-range)# exit
```

// Asignar puertos a VLAN 20

```
Switch(config)# interface range gigabitEthernet 1/0/18 – 1/0/24

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 20

Switch(config-if-range)# exit
```

// Asignar puertos a VLAN 40

```
Switch(config)# interface gigabitEthernet 1/0/1

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 40

Switch(config-if-range)# exit
```

D.5 Pruebas y verificacion

D.5.1 Pruebas de conectividad entre dispositivos

Para verificar la conectividad, se utilizó un dispositivo final (PC) conectado a las VLAN 10, 20, 30, 40 y 50. Desde esta PC, se ejecutaron pruebas de ping dirigidas a otros equipos pertenecientes a cada una de las VLAN mencionadas.

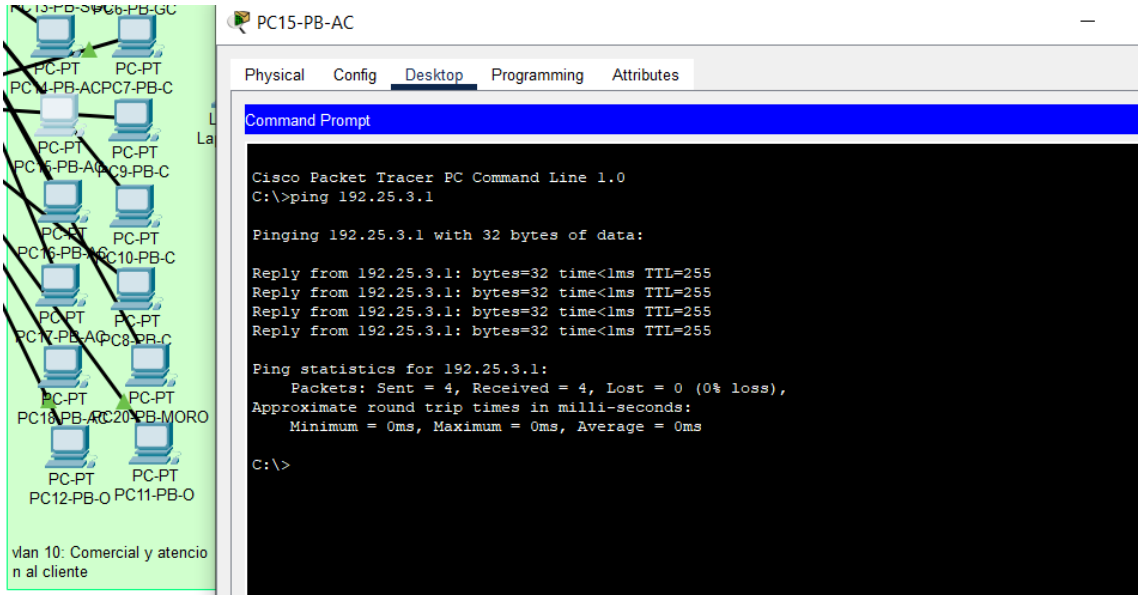


Figura D.5.1: Prueba de conectividad de la VLAN 10 a la 40
Fuente: Elaboración propia

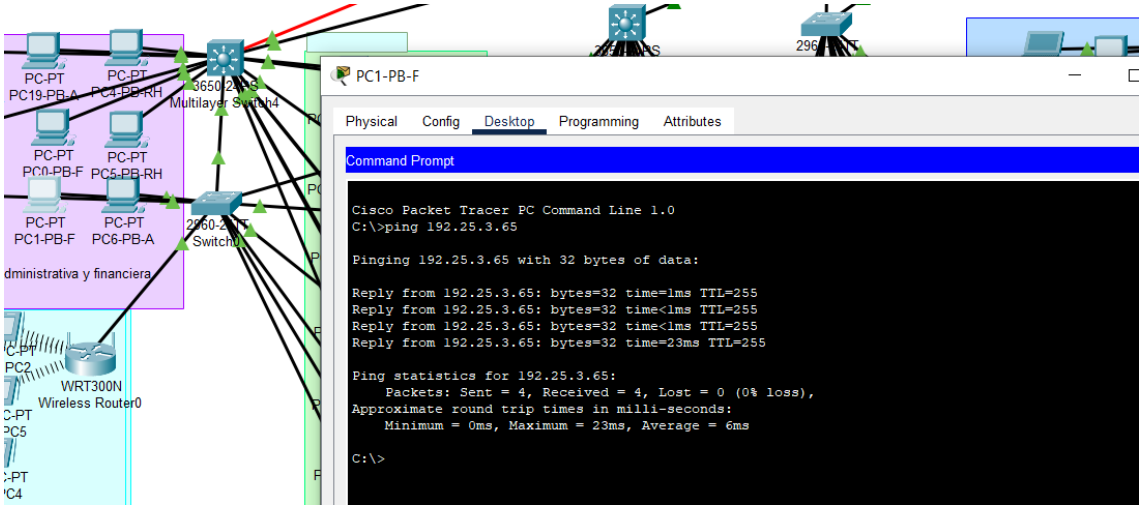


Figura D.5.2: Prueba de conectividad de la VLAN 40 a la 10
Fuente: Elaboración propia

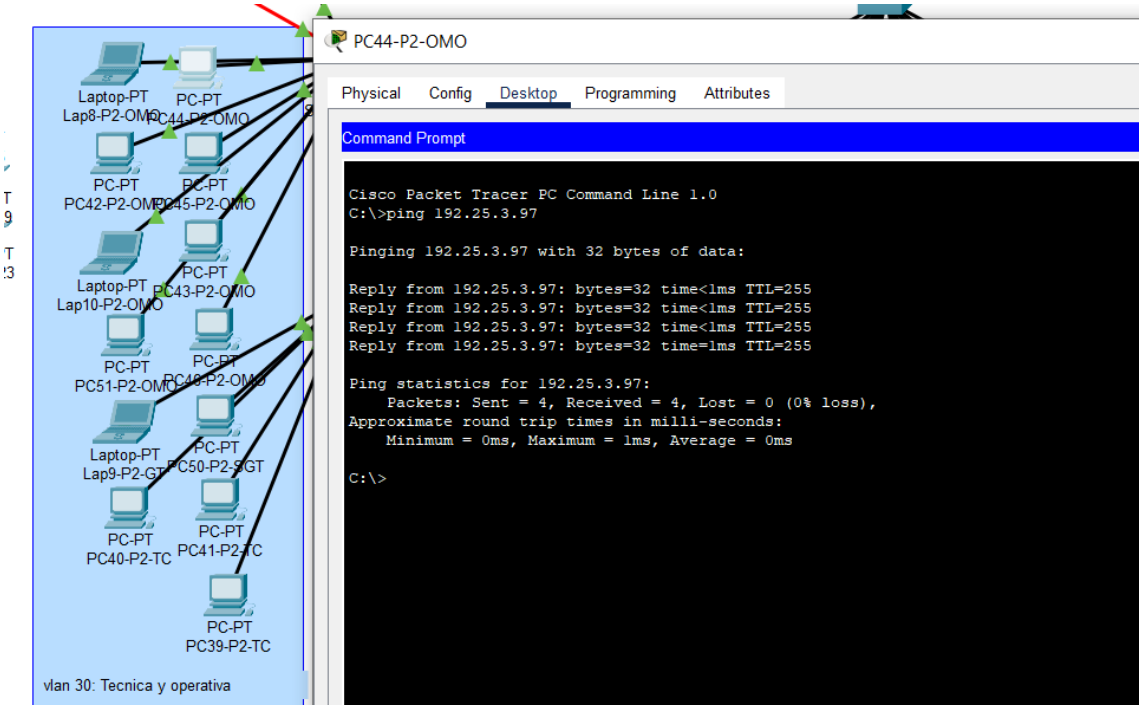


Figura D.5.3: Prueba de conectividad de la VLAN 30 a la 40
Fuente: Elaboración propia

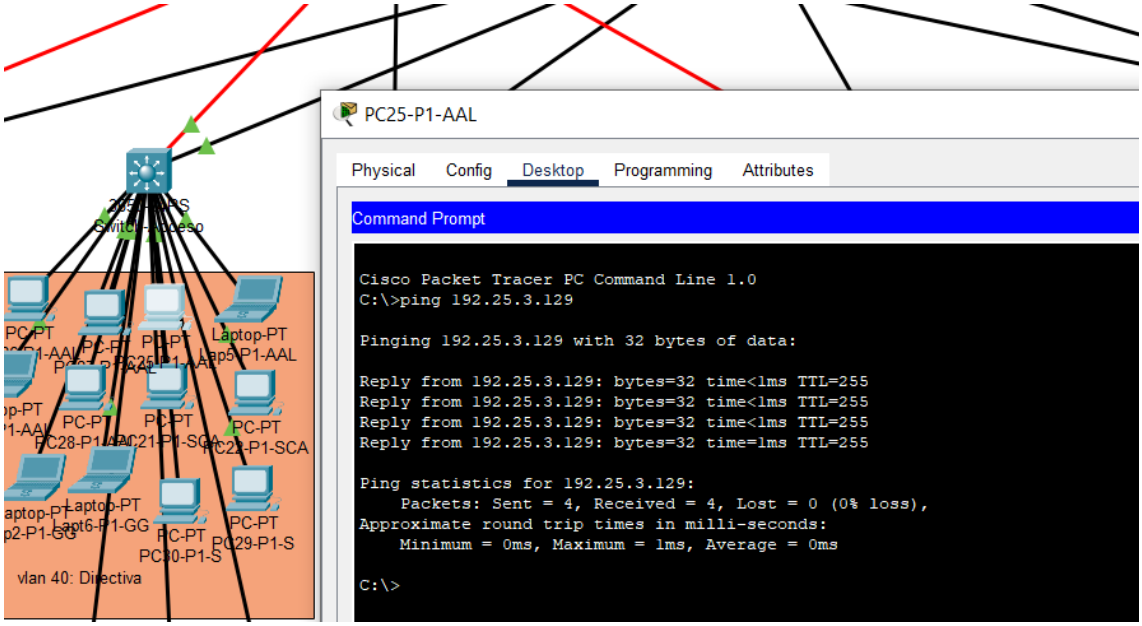


Figura D.5.4: Prueba de conectividad de la VLAN 40 a la 50
Fuente: Elaboración propia

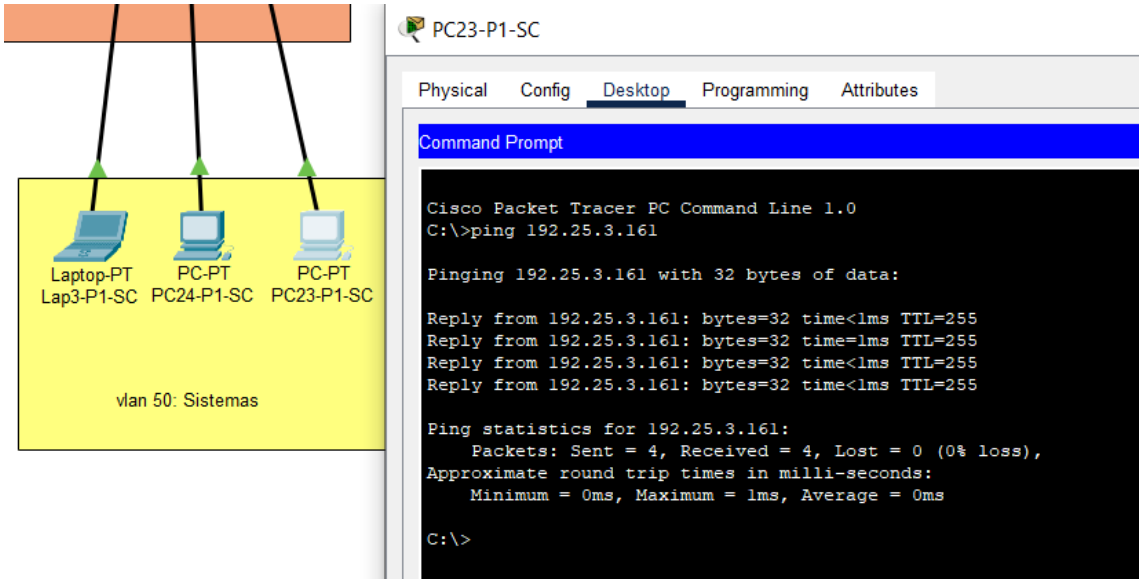


Figura D.5.5: Prueba de conectividad de la VLAN 50 a la 40
Fuente: Elaboración propia

Para verificar la conectividad entre los routers, se envió un mensaje desde R1 hacia R2, confirmando así el correcto funcionamiento del enlace.

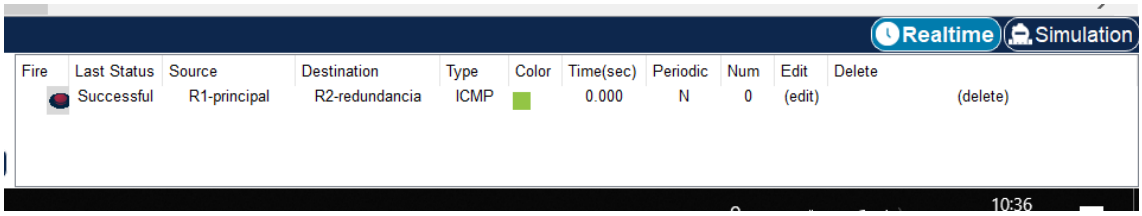


Figura D.5.6: Prueba de conectividad del Router1 al Router2
Fuente: Elaboración propia

Para verificar la operatividad del enlace entre el MAIN-SWITCH1 y el router R1, se llevó a cabo una prueba de conectividad mediante el envío de mensajes ICMP entre ambos dispositivos.

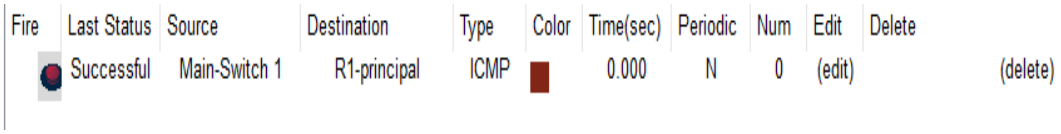


Figura D.5.7: Prueba de conectividad del Switch principal al Router1
Fuente: Elaboración propia

Con el fin de verificar la conexión entre el MAIN-SWITCH2 y el router R2, se realizó una prueba de comunicación mediante el envío de un mensaje entre ambos equipos.

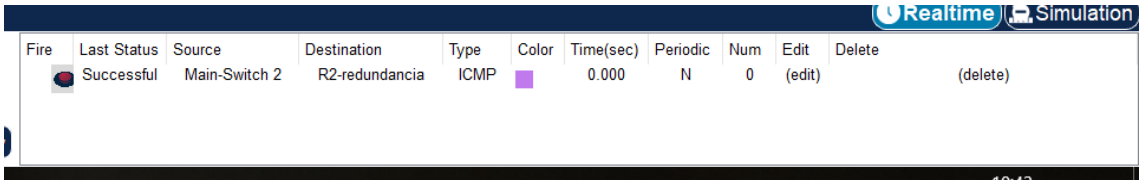


Figura D.5.8: Prueba de conectividad del Switch de respaldo al Router2
Fuente: Elaboración propia

D.5.2 Pruebas de Redundancia (HSRP)

Se debe verificar que HSRP esté funcionando correctamente, con uno de los routers en el rol de Active y el otro como Standby. Para ello, se accede a la consola de comandos del router R1, donde está configurado HSRP, y se ejecuta el comando “show standby brief.” Si en la columna "Standby" aparecen las direcciones IP asociadas a las distintas VLANs, se confirma que la configuración es correcta.

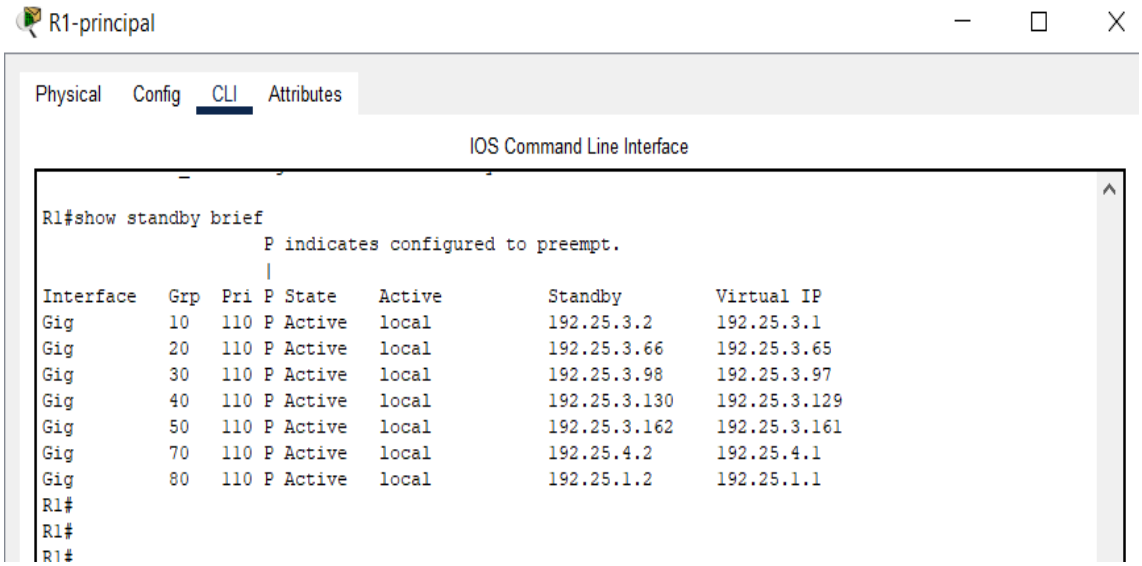


Figura D.5.9: Prueba de redundancia del Router1
Fuente: Elaboración propia

De igual forma, para verificar la correcta configuración del protocolo HSRP en el router redundante (R2), se debe acceder a su consola y ejecutar el mismo comando: show standby brief. Esto permitirá comprobar que el router R2 ha asumido correctamente el rol de Standby dentro del grupo HSRP.

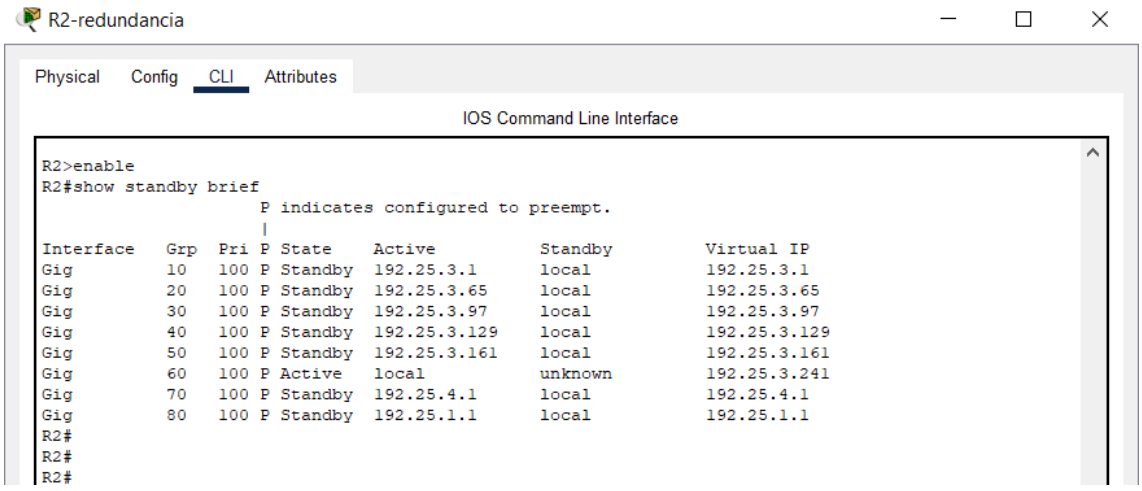


Figura D.5.10: Prueba de redundancia del Router2
Fuente: Elaboración propia

D.5.3 Pruebas de configuración de VLANs y Troncales

Validar la correcta segmentación y propagación de VLANs en los switches.

Se realizó la verificación de todas las VLANs en los switches principales y secundarios ubicados en los IDFs. Esta comprobación se llevó a cabo mediante capturas de pantalla que muestran las VLANs activas, utilizando el comando show vlan brief.

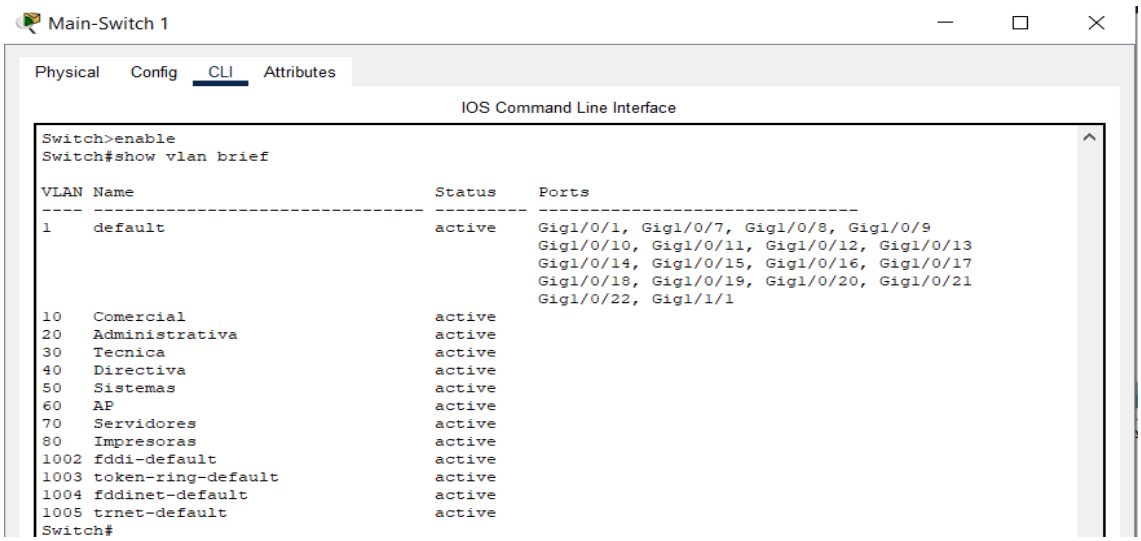


Figura D.5.11: Prueba de configuración de las VLANs en el Switch principal
Fuente: Elaboración propia

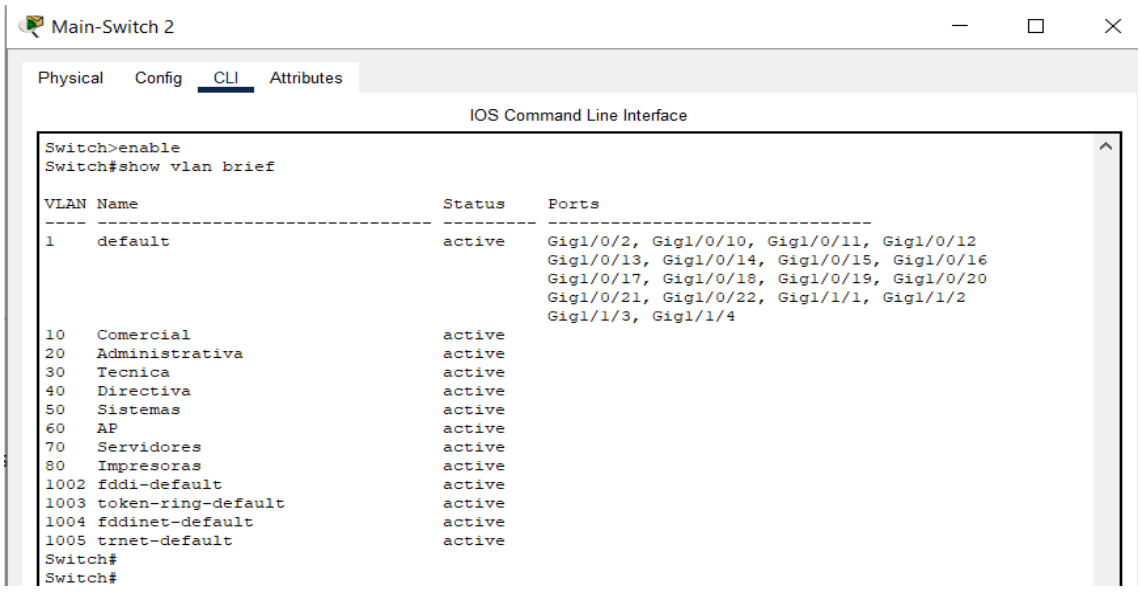


Figura D.5.12: Prueba de configuración de las VLANs en el Switch secundario

Fuente: Elaboración propia

A diferencia de los switches principales, en los switches secundarios no solo se muestran las VLANs configuradas, sino también los puertos que han sido asignados a cada una de ellas. Esta información es útil para verificar la correcta distribución de las VLANs en los dispositivos de acceso, asegurando que cada equipo esté conectado al puerto correspondiente según su área o departamento.

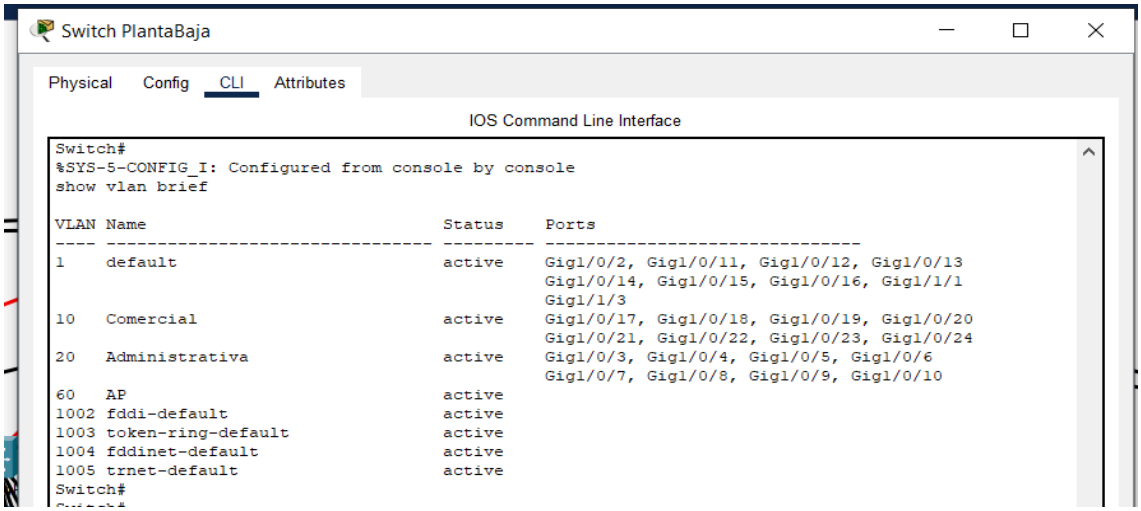


Figura D.5.13: Prueba de configuración de las VLANs en el SwitchPB
Fuente: Elaboración propia

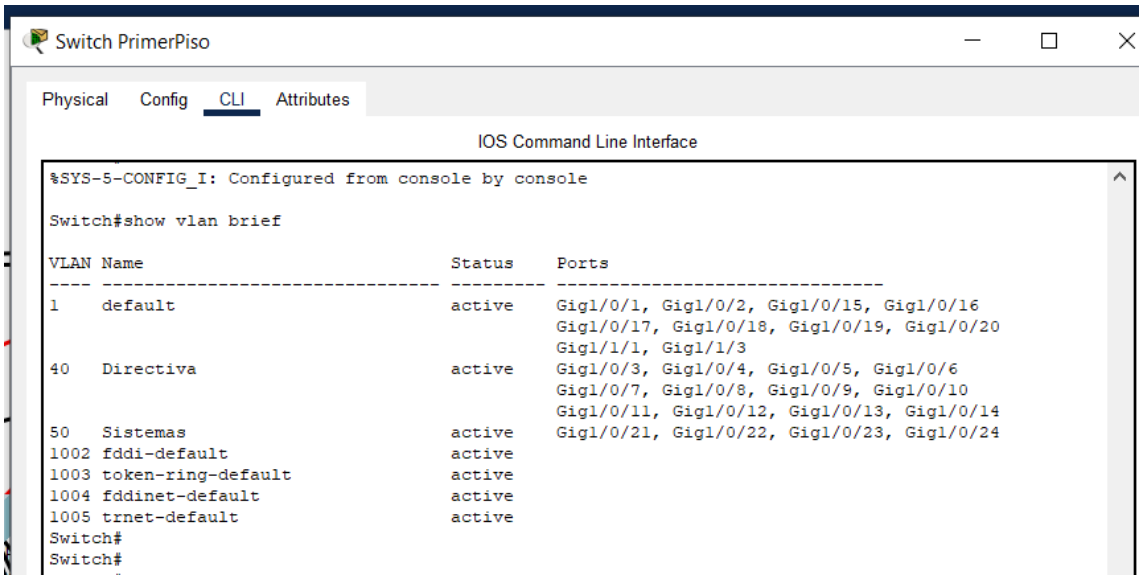


Figura D.5.14: Prueba de configuración de las VLANs en el SwitchPP
Fuente: Elaboración propia

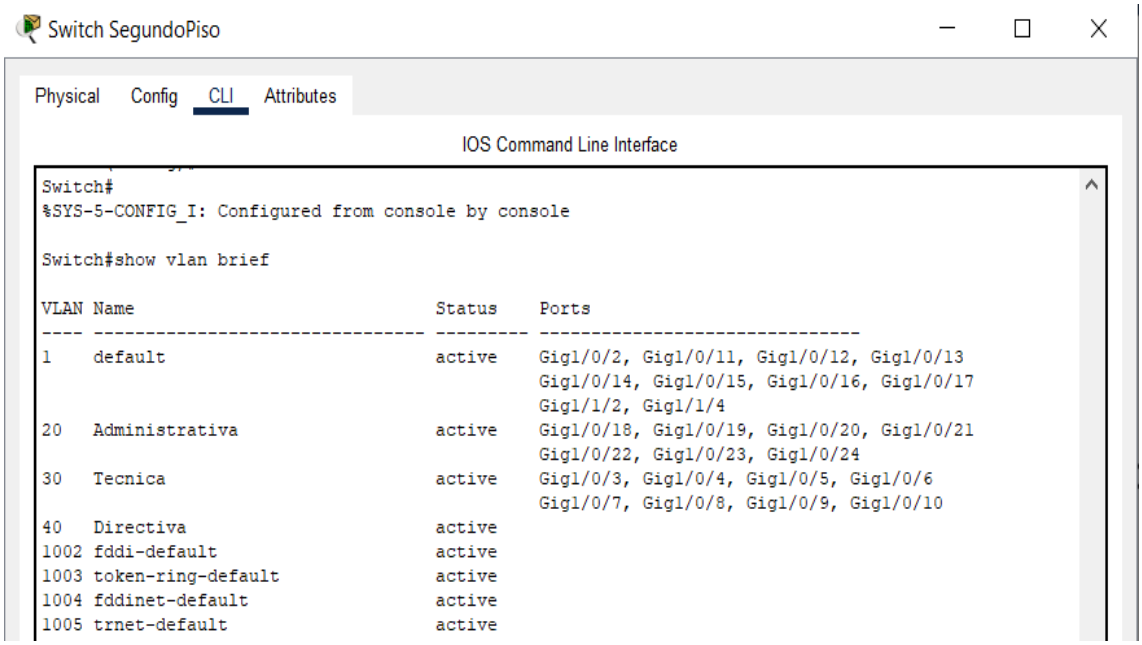


Figura D.5.15: Prueba de configuración de las VLANs en el SwitchSP
Fuente: Elaboración propia

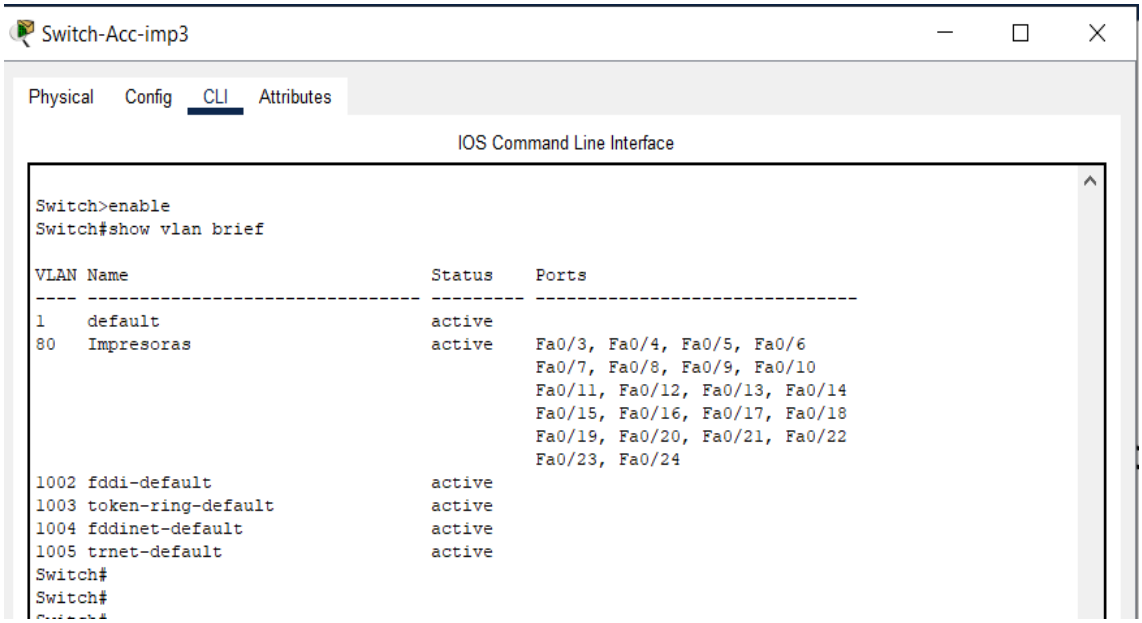


Figura D.5.16: Prueba de configuración de las VLANs en el SwitchIMP3
Fuente: Elaboración propia

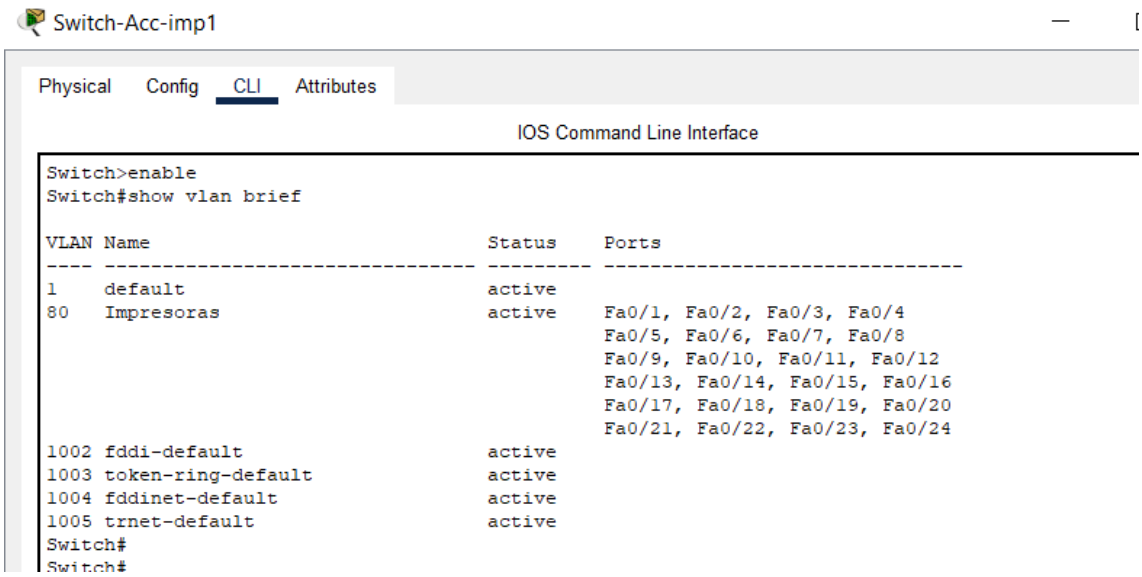


Figura D.5.17: Prueba de configuración de las VLANs en el SwitchIMP1
Fuente: Elaboración propia

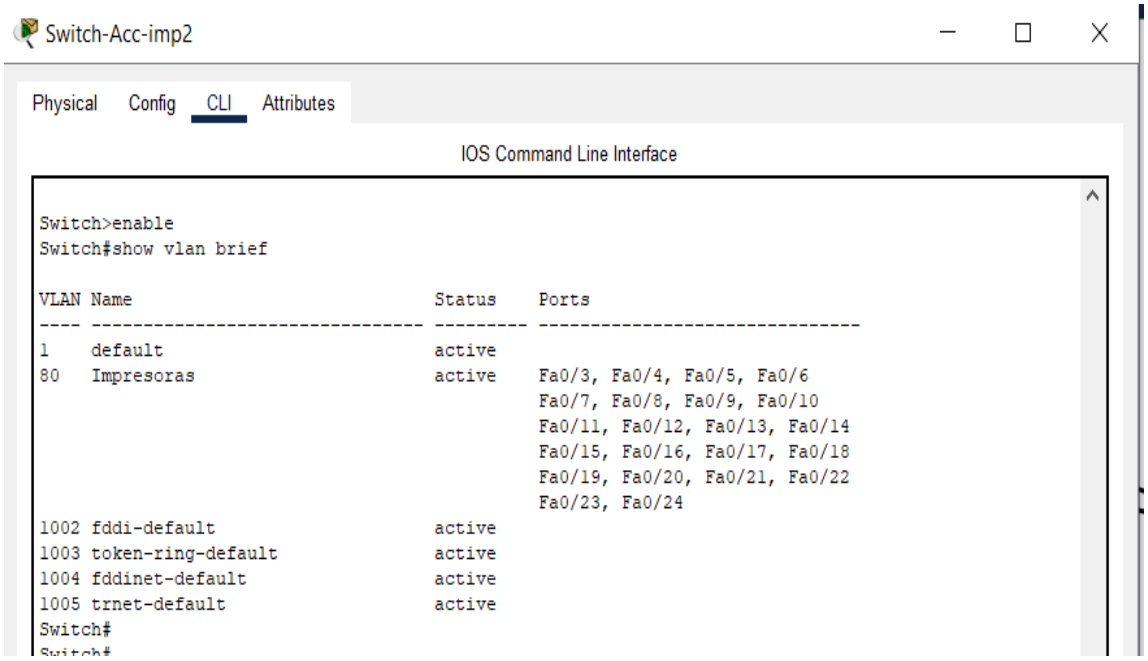


Figura D.5.18: Prueba de configuración de las VLANs en el SwitchIMP2
Fuente: Elaboración propia

Validación de enlaces troncales en los switches del MDF

Para comprobar que los enlaces troncales de los switches principales están funcionando correctamente, se utiliza el comando “show interfaces trunk”. Este comando permite visualizar los puertos configurados en modo troncal, así como las VLANs permitidas que están siendo transportadas a través de dichos enlaces. Esta verificación es fundamental para asegurar la conectividad entre los switches y la correcta propagación del tráfico de VLANs en toda la red.0

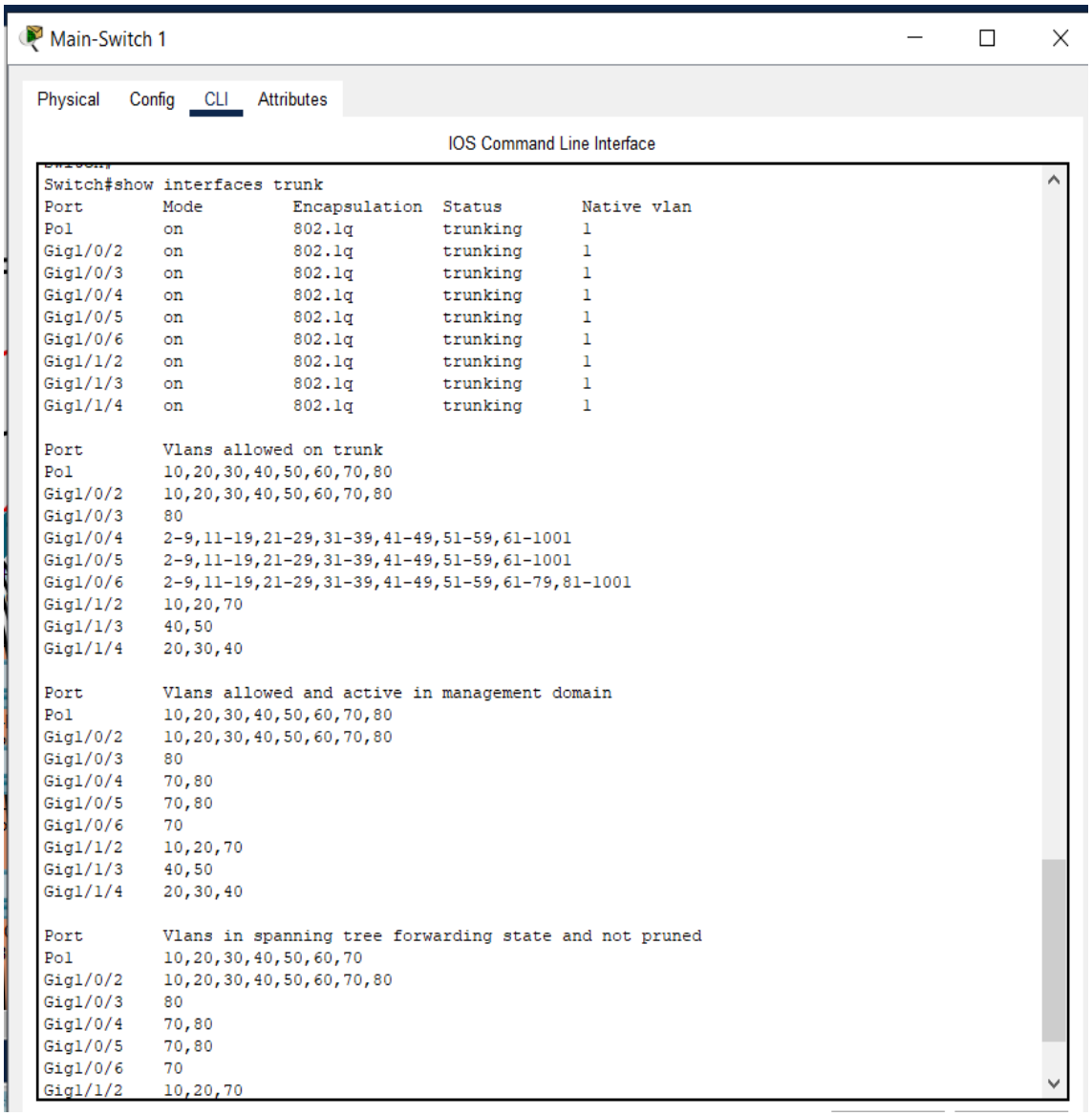


Figura D.5.19: Validación del enlace troncal en el Switch principal
Fuente: Elaboración propia

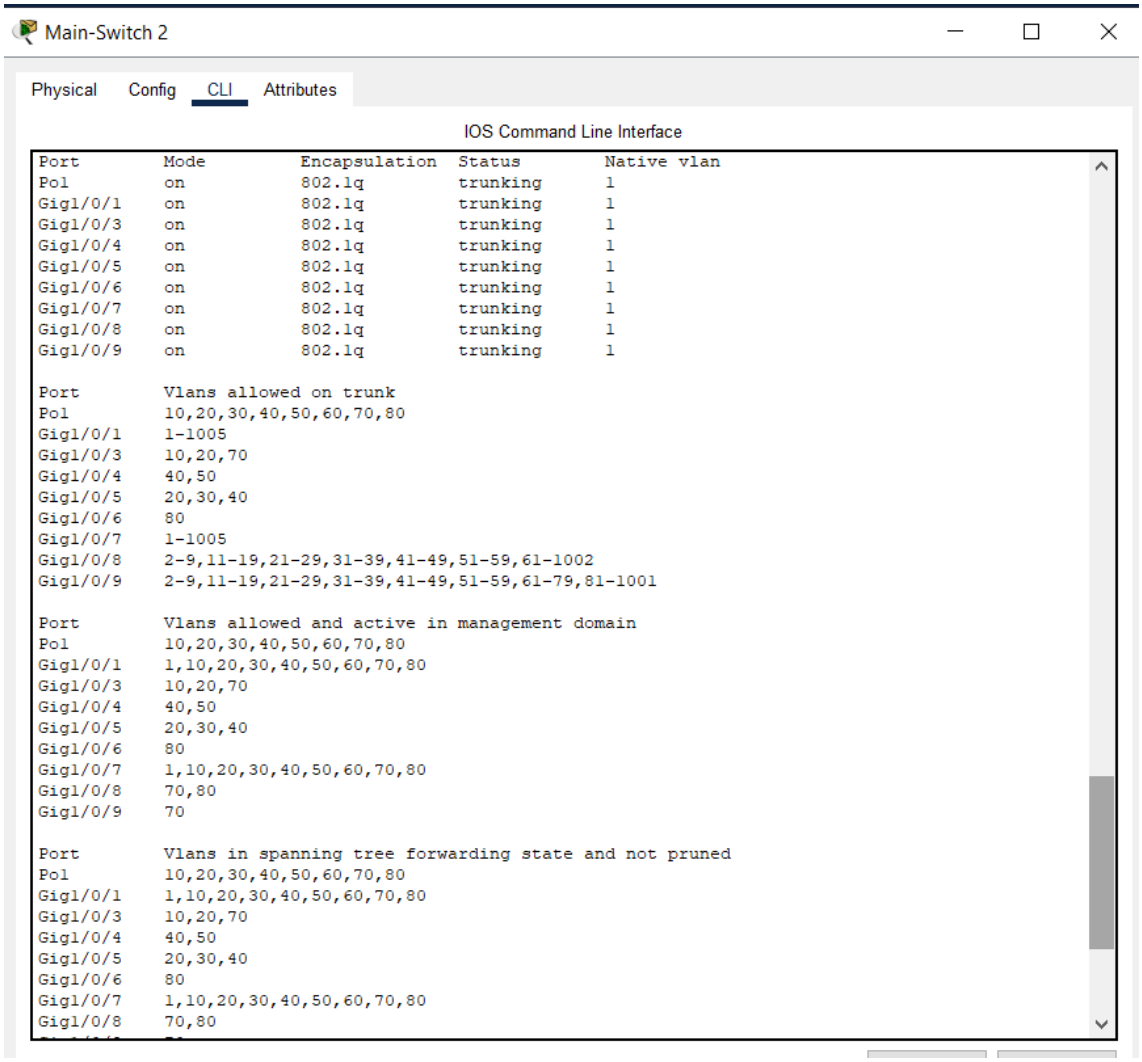


Figura D.5.20: Validación del enlace troncal en el Switch secundario
Fuente: Elaboración propia

Verificación de conexión en la VLAN 20 en el Switch PlantaBaja al Switch SegundoPiso

Se realiza una prueba de conectividad desde una PC perteneciente a la VLAN 20, ejecutando el comando “ping” seguido de la dirección IP asignada al switch correspondiente. Esta verificación permite comprobar que existe comunicación adecuada entre el dispositivo final y el equipo de red que administra esa VLAN.

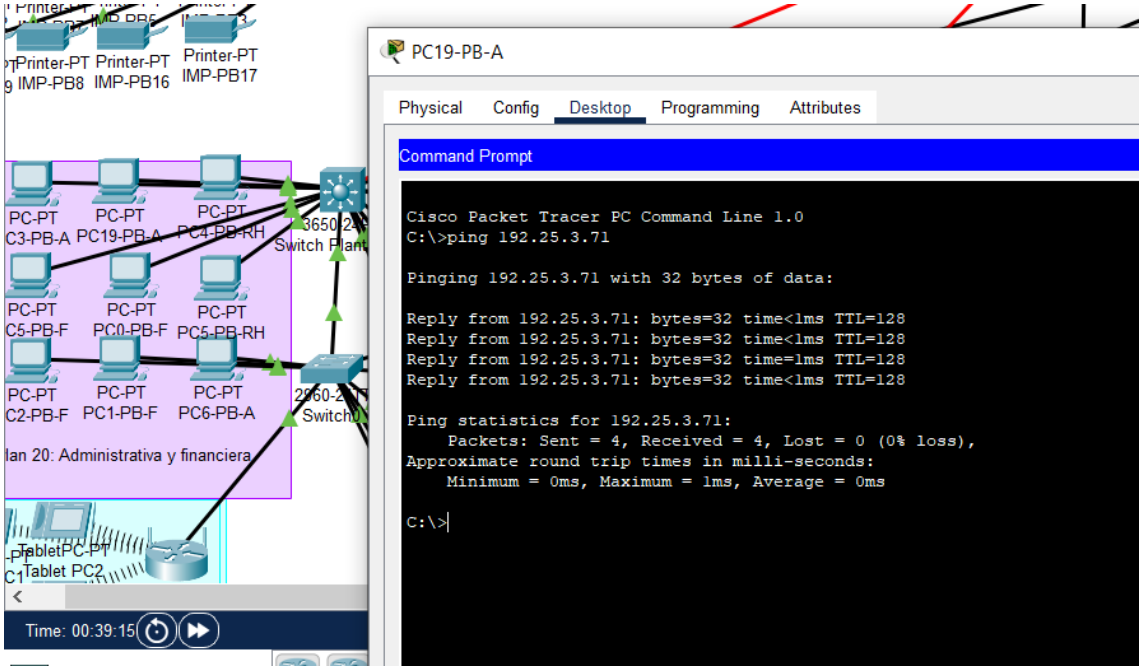


Figura D.5.21: Verificación de conexión mediante ping de la VLAN 20 al SwitchSP
Fuente: Elaboración propia

También es posible comprobar la conectividad entre dispositivos enviando mensajes entre ellos, lo que permite simular el funcionamiento real de una empresa, donde equipos pertenecientes a distintas VLANs necesitan comunicarse eficientemente.

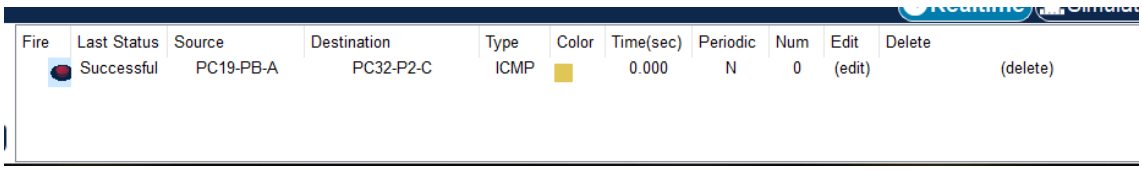


Figura D.5.22: Verificación de conexión mediante simulación de mensajes de la VLAN 20 al SwitchSP
Fuente: Elaboración propia

D.5.4 Pruebas de DHCP

Asegurar que las direcciones IP se asignen automáticamente a los dispositivos finales.

Se valida la dirección IP obtenida por una PC perteneciente a la VLAN 40 utilizando el comando “ipconfig,” el cual permite visualizar la configuración IP del equipo. A continuación, se

realiza una prueba de conectividad mediante el comando “ping” hacia otra PC para comprobar la comunicación entre dispositivos dentro de la misma VLAN.

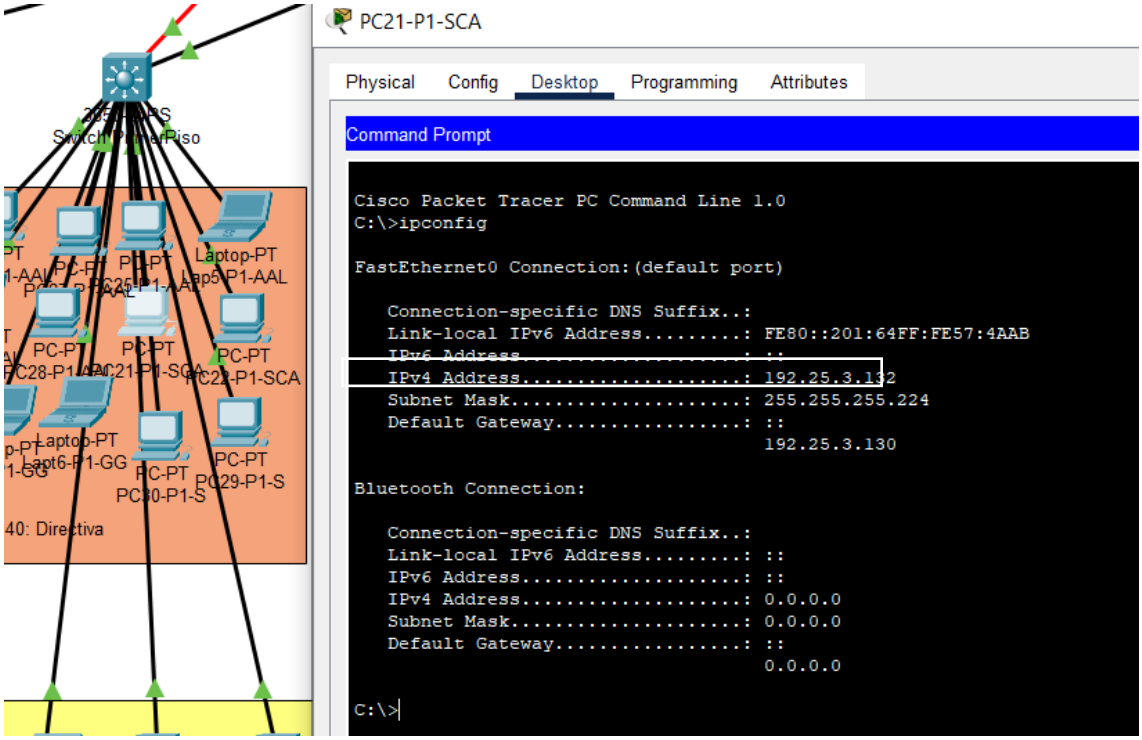


Figura D.5.23: Verificación de conexión de DHCP en la PC21
Fuente: Elaboración propia

Como se puede observar en la prueba de conectividad mediante ping, la dirección IP asignada automáticamente por el servidor DHCP fue obtenida de forma exitosa.

Otra forma de verificar que las direcciones IP están siendo asignadas correctamente a través de DHCP es mediante la visualización de las direcciones MAC de los dispositivos junto con sus respectivas IPs asignadas. Esto se realiza en el router principal utilizando el comando “show ip dhcp binding”, como se muestra en la siguiente imagen.

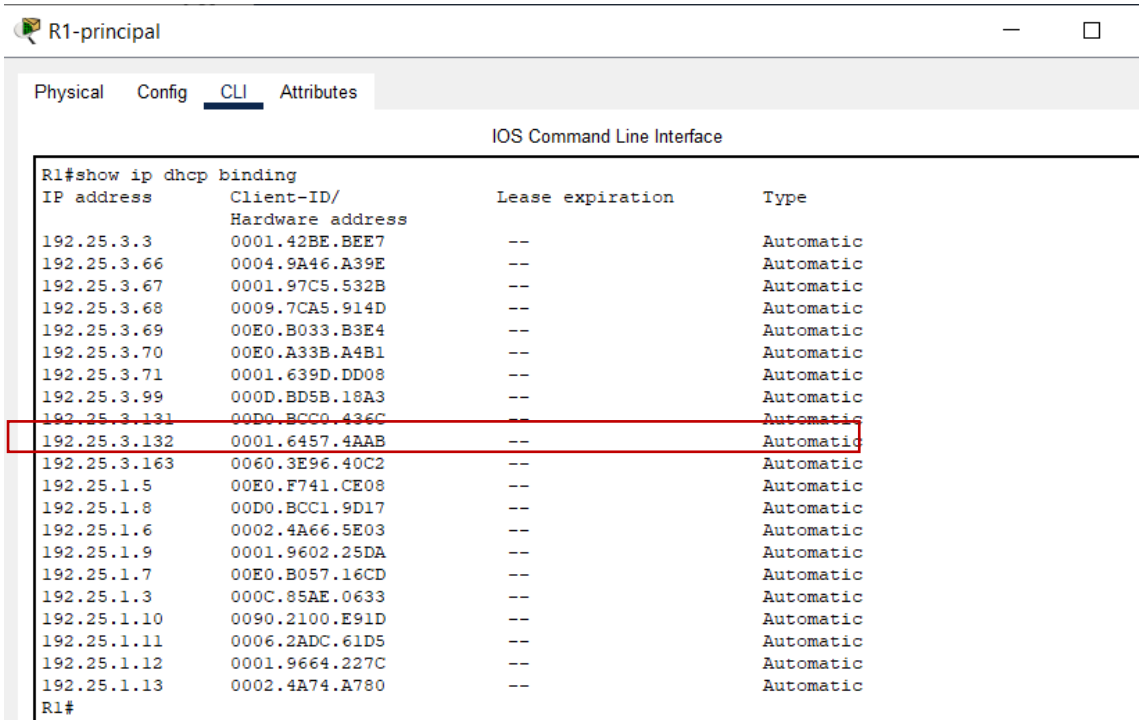


Figura D.5.24: Verificación de conexión de DHCP en el Router principal
Fuente: Elaboración propia

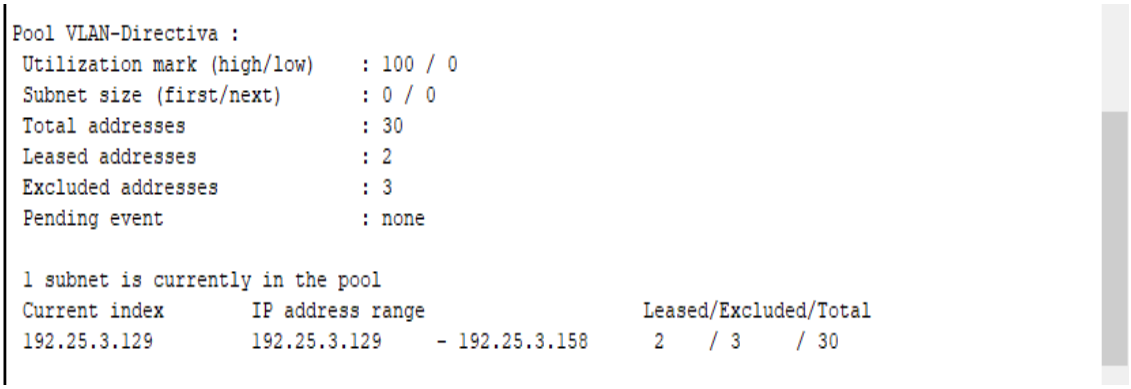


Figura D.5.25: Verificación de conexión de DHCP de la VLAN Directiva
Fuente: Elaboración propia

D.5.5 Pruebas de EtherChannel

Se procede a comprobar el correcto funcionamiento de los enlaces EtherChannel configurados entre los switches MDF.

Para verificar el estado del EtherChannel, se accede a la consola de configuración del switch principal y se ejecuta el comando “show etherchannel summary”. Este comando proporciona un resumen del estado de los grupos EtherChannel, mostrando una letra P (de Port-channel) al lado de los puertos activos.

La letra P indica que el puerto forma parte activa del canal y que la conexión se encuentra establecida correctamente. Si ambos puertos involucrados muestran la letra P, significa que la comunicación por EtherChannel está funcionando correctamente.

En la imagen siguiente se puede observar cómo los puertos Gig1/0/23 y Gig1/0/24 aparecen con la letra (P) al final, confirmando que están agrupados en un Port-Channel activo.

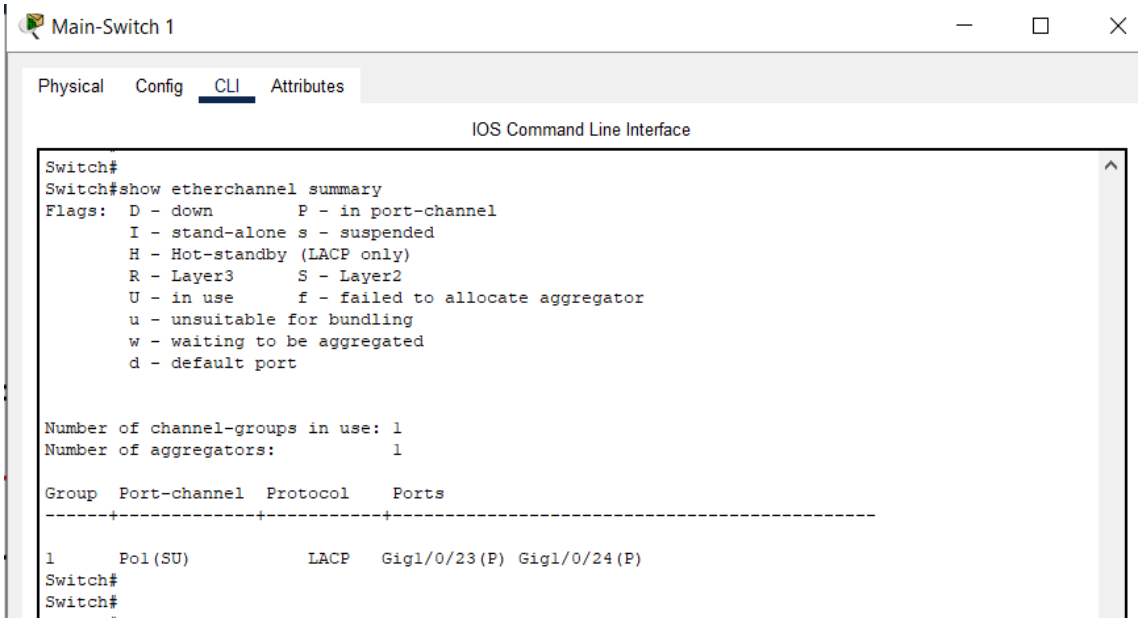


Figura D.5.26: Verificación de conexión de EtherChannel en el Switch principal
Fuente: Elaboración propia

D.5.6 Registro de resultados

Durante cada una de las pruebas realizadas, se registraron los resultados obtenidos en una tabla con el fin de documentar posibles errores, inconsistencias o ajustes necesarios en la configuración de la red.

Prueba Realizada	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Observaciones / Ajustes Realizados
Conectividad entre PCs en VLAN 10	Se hace ping entre dos PCs ubicadas en la VLAN 10.	Respuesta exitosa del ping.	Comunicación establecida correctamente.	Sin observaciones.
Conectividad entre VLANs mediante router-on-a-stick	Ping desde PC en VLAN 20 a una PC en VLAN 30.	Comunicación inter-VLAN exitosa.	Ping exitoso.	Se verificó la configuración de subinterfaces en el router.
Verificación de DHCP en VLAN 40	Se revisa la asignación automática de IP mediante "ipconfig".	IP asignada dentro del rango definido.	Dirección IP asignada correctamente por el router.	DHCP funcionando correctamente.
Estado de los enlaces troncales	Se ejecuta el comando "show interfaces trunk" en el switch principal.	Se listan las interfaces en modo trunk y VLANs permitidas.	Troncales activos y transportando las VLANs asignadas.	Se ajustaron VLANs permitidas en un puerto.

Verificación de HSRP	Se ejecuta "show standby brief" en ambos routers.	Un router en estado *Active* y el otro en *Standby*.	R1: Active – R2: Standby (esperado).	Configuración de HSRP verificada.
Verificación de EtherChannel	Se ejecuta "show etherchannel summary" en el switch principal.	Puertos con estado (P) indicando inclusión en EtherChannel.	Puertos Gig1/0/23 y Gig1/0/24 en estado (P).	EtherChannel activo y funcional.
Visualización de direcciones DHCP asignadas	Se ejecuta "show ip dhcp binding" en el router principal.	Lista de direcciones IP asignadas con su correspondiente MAC.	Todas las IPs se encuentran correctamente asignadas.	DHCP comprobado exitosamente.
Comunicación R1 – R2	Ping entre R1 y R2 para verificar la redundancia.	Comunicación exitosa.	Ping correcto entre ambos routers.	Redundancia validada.

Tabla 8: Registro de resultados
Fuente: Elaboración propia

D.6 Mantenimiento y escalabilidad

D.6.1 Monitoreo y Mantenimiento de la Red

1.Documentación de la Red

- Se debe mantener un registro actualizado de la configuración de todos los dispositivos, incluyendo routers, switches y servidores. En la simulación, esto incluye la

configuración del router R1 principal, el router de respaldo y el router adicional utilizado como firewall y NAT.

- Los diagramas lógicos y físicos presentados en capítulos anteriores servirán como base para cualquier actualización o diagnóstico futuro.

D.6.2 Escalabilidad de la Red

1.Planificación de Direccionamiento

La red fue diseñada considerando el crecimiento futuro mediante una planificación eficiente del direccionamiento IP. Se utilizaron subredes optimizadas para cada VLAN, con un número adecuado de direcciones disponibles para expansión. Además, se reservaron bloques IP sin asignar que pueden ser utilizados para futuras VLANs o servicios.

2.Incremento de Capacidad Física

- Los switches principales (MDF) y de distribución (IDF) incluidos en la simulación cuentan con puertos libres, lo que permite la conexión de nuevos dispositivos sin necesidad de reemplazar equipos existentes.
- En caso de un crecimiento considerable, se contempla la incorporación de switches apilables (stackable) o la implementación de enlaces adicionales para balancear la carga.
- El uso de EtherChannel entre switches del MDF proporciona mayor capacidad de transferencia y facilita la escalabilidad sin sacrificar disponibilidad o desempeño.

3.Implementación de Redundancia

Se configuró el protocolo HSRP (Hot Standby Router Protocol) para garantizar la alta disponibilidad de la red. Esta configuración permite que un router asuma el control automáticamente si el otro falla.

En una red real, este mecanismo puede complementarse o sustituirse con otros protocolos de redundancia como VRRP (Virtual Router Redundancy Protocol) o GLBP (Gateway Load Balancing Protocol) para mejorar el balanceo de carga y la tolerancia a fallos.

4.Segmentación Adicional

Si la red lo requiere, es posible implementar nuevas VLANs dedicadas a proyectos temporales, departamentos específicos, invitados o dispositivos IoT. Esto facilita la administración del tráfico, mejora la seguridad y permite una mayor personalización de la red.

D.6.3 Respuesta ante Fallas

1.Diagnóstico

Durante la simulación, se utilizaron herramientas de diagnóstico como ping, tracert, y show ip interface brief para verificar la conectividad y el estado de las interfaces.

En un entorno real, estas pruebas deben realizarse de forma periódica para garantizar la integridad operativa de la red.

Adicionalmente, las Listas de Control de Acceso (ACLs) configuradas en el router con funciones de firewall permiten monitorear y restringir el tráfico, lo que también facilita la identificación de posibles fallos o accesos no autorizados.

2.Plan de Recuperación

Aunque en una simulación no se puede implementar un plan de recuperación completo, se propuso una estrategia básica que incluye:

- Revisión de configuraciones clave como NAT, HSRP y rutas estáticas ante eventos de desconexión externa.
- Reemplazo inmediato de enlaces físicos en caso de fallas en el cableado.

- Supervisión de puertos críticos para detectar degradación en el rendimiento.

En un entorno real, este plan debe documentarse formalmente e incluir políticas de respaldo de configuraciones, inventario de hardware de reemplazo, tiempos de recuperación (RTO), y puntos de recuperación de datos (RPO).

D.7 Lista de comandos claves

D.7.1 Listado de commandos criticos

- **Router**

```
ip nat inside source list 1 interface GigabitEthernet0/1 overload
```

ip nat inside source: Esta parte indica que se van a traducir las direcciones IP de origen de la red interna (es decir, del lado “inside” de NAT).

list 1: Hace referencia a una Access Control List (ACL) con número 1.

interface GigabitEthernet0/1: Especifica que el router usará la IP pública de esta interfaz como la IP de origen traducida para el tráfico saliente.

overload: Permite que muchos dispositivos internos compartan una sola dirección IP pública mediante asignación de diferentes puertos.

- **Switch**

```
switchport mode trunk
```

Le dice al puerto que no se comportará como un acceso (una sola VLAN), sino como un trunk, transportando múltiples VLANs.

- **Verificaciones**

```
show ip nat translations
```

Sirve para mostrar las traducciones activas de NAT (Network Address Translation) que se están llevando a cabo en un router.

D.7.2 Listado de comandos de verificación

Router;

show ip interface brief: Muestra un resumen del estado de todas las interfaces del router, incluyendo su IP y si están "up" o "administratively down".

show running-config: Permite revisar la configuración actual aplicada al router. Es útil para verificar IPs, rutas, ACLs, NAT, DHCP, HSRP, etc.

show startup-config: Muestra la configuración guardada en la NVRAM que se carga al iniciar el router.

show cdp neighbors: Confirma qué dispositivos Cisco están directamente conectados, sus interfaces y plataformas.

show standby [brief]: Verifica el estado del protocolo HSRP: muestra cuál es el router activo y en espera, junto con la prioridad y el estado por VLAN.

show ip route: Muestra la tabla de enrutamiento del router, indicando las rutas estáticas y dinámicas aprendidas (por RIP, OSPF, EIGRP, etc.).

show ip ospf neighbor: Muestra las relaciones de vecindad OSPF con otros routers, útil para diagnosticar problemas de adyacencia.

show ip eigrp neighbors: Similar al anterior, pero para verificar vecinos EIGRP y asegurar conectividad dinámica.

show ip protocols: Muestra los protocolos de enrutamiento dinámico configurados y las redes que están siendo anunciadas.

show ip nat translations: Muestra la tabla de traducciones NAT activas (inside → outside), útil para verificar la correcta traducción de direcciones IP privadas.

show ip nat statistics: Presenta estadísticas de paquetes NAT traducidos, drops y otras métricas de rendimiento.

show access-lists: Muestra todas las listas de control de acceso (ACLs) configuradas, su contenido y números o nombres asociados.

show running-config | include access-group: Filtra la configuración para ver en qué interfaces se han aplicado las ACLs mediante access-group.

show ip dhcp binding: Muestra la lista de direcciones IP asignadas a través de DHCP junto con las MACs asociadas.

show ip dhcp pool: Verifica los pools DHCP configurados, número de direcciones disponibles y estadísticas de uso.

show arp: Muestra la tabla ARP con las IPs y MACs conocidas por el router, útil para verificar resolución de direcciones.

ping [IP]: Verifica la conectividad a otro host o dispositivo mediante ICMP.

traceroute [IP]: Diagnostica la ruta que siguen los paquetes hacia un destino, útil para identificar cuellos de botella o fallas.

Switch

show interfaces status: Verifica el estado administrativo y operativo de cada puerto del switch, incluyendo velocidad y tipo de conexión.

show vlan brief: Muestra todas las VLANs creadas en el switch y los puertos asignados a cada una.

show vlan id <vlan-id>: Detalla los puertos específicos que pertenecen a una VLAN determinada.

show interfaces trunk: Verifica los puertos que están configurados en modo trunk, sus VLANs permitidas y el estado de encapsulamiento (dot1q).

show interfaces switchport: Proporciona información detallada del modo de cada interfaz (access, trunk, dynamic), VLAN nativa, etc.

show cdp neighbors: Similar al comando en routers, muestra dispositivos directamente conectados al switch.

show spanning-tree: Muestra el estado del protocolo STP por VLAN, roles de puertos (root, designated, blocking) y la topología.

show spanning-tree vlan <vlan-id>: Detalla la información STP solo para una VLAN específica.

show etherchannel summary: Muestra los grupos de EtherChannel configurados, los puertos que los integran y su estado (activo, standby, etc.).

show interfaces port-channel <número>: Da información detallada sobre el canal de agregación (EtherChannel).

show mac address-table: Muestra la tabla de direcciones MAC del switch y en qué puerto fueron aprendidas, útil para rastrear dispositivos conectados.

ping [IP]: Al igual que en routers, permite verificar conectividad desde switches con capacidad de L3.

D.7.3 Listado de ACLS utilizadas

ACL para NAT

access-list 1 permit 192.25.3.0 0.0.0.255

access-list 1 permit 192.25.1.0 0.0.0.63

access-list 1 permit 192.25.4.0 0.0.0.7

ACL para filtrado de tráfico en el Router Firewall (Permitir tráfico interno hacia internet**)**

access-list 100 permit ip 192.25.3.0 0.0.0.255 any

access-list 100 permit ip 192.25.1.0 0.0.0.63 any

access-list 100 permit ip 192.25.4.0 0.0.0.7 any

ACL para filtrado de tráfico en el Router Firewall (Bloquear tráfico no deseado hacia redes internas**)**

access-list 101 deny ip any 192.25.3.0 0.0.0.255

access-list 101 deny ip any 192.25.1.0 0.0.0.63

access-list 101 deny ip any 192.25.4.0 0.0.0.7

access-list 101 permit ip any any

- La ACL 100 permite que las redes internas envíen tráfico hacia internet.
- La ACL 101 bloquea tráfico no autorizado proveniente de internet hacia las redes internas.

D.8 Glosario de términos

VLAN: es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física.

NAT: es una tecnología fundamental en el ámbito de las redes que permite la traducción de direcciones IP dentro de una red privada a una dirección IP pública.

HSRP: Protocolo que ofrece redundancia para puertas de enlace predeterminadas.

IDF: significa Cuadro de distribución individual, es una sala o gabinete que se conecta a una distribución principal o MDF

MDF: es el eje central o el corazón de la red. es una estructura de distribución de señales para conectar equipo de redes y telecomunicaciones a los cables y equipos que corresponden al proveedor de servicios de telefonía, Internet, entre otros.

ISP: es una organización que ofrece diversos servicios para que los usuarios puedan acceder y utilizar Internet.

RIP: Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

OSPF: es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

DHCP: es un protocolo cliente-servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace de predeterminada.

D.8.1 Referencias

Byte, B. (18 de julio de 2017). *Bitacora Byte*. Obtenido de Bitacora Byte: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

CISCO. (2 de agosto de 2022). *cisco*. Obtenido de cisco: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html

Fernandez, R. P. (s.f.). *raulprietofernandez.net.* Obtenido de raulprietofernandez.net: https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ripv2-con-packet-tracer

Marcelo. (26 de noviembre de 2020). *ccnadesdecero.com*. Obtenido de ccnadesdecero.com: https://ccnadesdecero.com/curso/como-configurar-ospf/

MichelyLopez. (7 de 20 de 2019). *CISCO Community*. Obtenido de CISCO Community: https://community.cisco.com/t5/blogs-routing-y-switching/configuraci%C3%B3n-de-redundancia-de-gateway-con-el-protocolo-hsrp/ba-p/3894288

Ruiz, M. (16 de febrero de 2022). *GitHub.* Obtenido de GitHub: https://marcosruiz.github.io/posts/tutorial-vlan-packet-tracer/

Ruiz, M. (16 de mayo de 2023). *GitHub*. Obtenido de GitHub: https://marcosruiz.github.io/posts/tutorial-nat-estatico-packet-tracer/

Sepulveda, M. (s.f.). *eclassvirtual*. Obtenido de eclassvirtual: https://eclassvirtual.com/configuracion-de-dhcp-en-cisco-router/

Tucker, L. P. (21 de diciembre de 2023). *abcXperts*. Obtenido de abcXperts: https://abcxperts.com/hsrp-vrrp-glbp-entendiendo-los-protocolos-clave-para-la-redundancia-en-redes/