

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

**FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y
TELECOMUNICACIONES**



**“DISEÑO DE UNA RED LAN DE ALTA DISPONIBILIDAD PARA
MEJORAR LA CALIDAD DE SERVICIO EN LA EMPRESA
CORPORACION SEHOVER”**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

PASTRANA SANDOVAL, HANS YEISON

**Villa El Salvador
2020**

DEDICATORIA

A mis padres, por su apoyo en todo momento tanto en el ámbito personal como profesional, siempre serán mi motivo para seguir adelante.

AGRADECIMIENTO

Al ingeniero Freddy Campos. Por su apoyo en cada una de las asesorías y sus recomendaciones en la elaboración de este trabajo.

ÍNDICE

LISTADO DE FIGURAS	vii
LISTADO DE TABLAS	ix
RESUMEN	10
INTRODUCCIÓN	11
OBJETIVOS	13
CAPÍTULO I: MARCO TEÓRICO	13
1.1 Bases Teóricas.....	13
1.1.1 Marco Teórico General	13
1.1.1.1 Red de área local.....	13
1.1.1.2 Tipos de topologías de red LAN.....	13
1.1.1.3 Estándares para redes LAN: IEEE 802.....	14
1.1.1.3.1 Estándar LAN IEEE 802.1:	14
1.1.1.3.2 Estándar LAN IEEE 802.2	14
1.1.1.3.3 Estándar LAN IEEE 802.3:	14
1.1.1.4 Modelos de redes	15
1.1.1.4.1 Modelo OSI.....	15
1.1.1.4.2 Modelo TCP/IP	15
1.1.1.4.3 Comparación entre OSI y TCP/IP.....	16
1.1.1.5 Jerarquía en la red.....	16
1.1.1.5.1 Niveles de red jerárquico	16
• Capa de acceso:.....	16
• Capa de distribución:.....	17
• Capa de núcleo:.....	17
1.1.1.6 Red de área virtual.....	17
1.1.1.6.1 Tipos de VLAN	17
1.1.1.7 Protocolos de alta disponibilidad.....	18
1.1.1.7.1 HSRP.....	18
1.1.1.7.2 STP.....	18
1.1.1.7.3 Etherchannel	19
• LACP	19
• PagP.....	19
1.1.1.7.4 EIGRP	19

1.1.1.8 Balanceo de carga	20
1.1.1.8.1 Balanceo de carga desigual	20
1.1.1.8.2 Algoritmo Dual	20
1.1.1.9 Protocolos de seguridad	21
1.1.1.9.1 Autenticación, Autorización y Contabilización (AAA).....	21
1.1.1.9.2 Secure Shell	22
1.1.1.10 Norma ISO/IEC 27002	23
1.1.2 Marco Teórico Especifico	24
1.2 Definición de términos básicos.....	29
CAPÍTULO II: METODOLOGÍA DE DESARROLLO DEL TRABAJO	
PROFESIONAL	31
Metodología.....	32
Figura N°1. Diagrama de flujo de la metodología del proyecto.	33
2.1 Delimitación temporal y espacial del trabajo	34
2.2 Determinación y análisis del problema.....	34
2.2.1 Determinación del problema	34
2.2.1.1 Situación actual de la red en la empresa	35
2.2.1.2 Detalle del histórico de la caída de la red	36
2.2.1.3 Proyectos actuales en la empresa	37
2.2.1.4 Impacto económico en un escenario actual.....	39
2.2.2 Análisis del problema	40
2.2.2.1 Análisis del estado de la infraestructura	40
2.2.2.2 Análisis cuantitativo de la infraestructura.....	41
2.2.2.3 Análisis económico para la empresa	42
2.2.2.4 Análisis cuantitativo de las áreas en la empresa	42
2.3 Modelo de solución propuesto:.....	43
2.3.1 Desarrollo del diseño de la red LAN asociado al CAPEX y OPEX.....	43
2.3.2 Validación del escenario a probar.	43
2.3.2.1 Proceso de validación de software	44
2.3.2.2 Parámetros del software	45
2.3.2.3 Validación de resultado.....	46
2.3.3 Modelo propuesto del diseño de la red LAN	46
2.3.4 Descripción de la topología a diseñar.	48
2.3.4.1 Proceso de configuración	48

2.3.4.1.1 Creación de VLAN.....	48
2.3.4.1.2 Centralizar la administración de VLAN	49
2.3.4.1.3 Configuración modo troncal y modo acceso.....	50
2.3.4.1.4 Configuración de protocolo Spanning Tree	51
2.3.4.1.5 VLAN de gestión.....	52
2.3.4.1.6 Configuración del protocolo Spanning Tree para dispositivos finales	52
2.3.4.1.7 Configuración Etherchannel	53
2.3.4.1.8 Configuración del protocolo HSRP	53
2.3.4.1.9 Asignación de dirección IP en CSW1 para enrutamiento	57
2.3.4.1.10 Asignación de dirección IP en R1 para enrutamiento.....	57
2.3.4.1.11 Configuración del protocolo EIGRP	58
2.4.4.2 Puerto seguro en los dispositivos	60
2.3.4.3 Configuración del protocolo SSH y AAA.....	60
2.4 Resultados	62
CONCLUSIONES.....	72
RECOMENDACIONES	73
BIBLIOGRAFÍA	74
ANEXOS	77

LISTADO DE FIGURAS

Figura N°1. Diagrama de flujo de la metodología del proyecto.	33
Figura N°2. Situación actual de la red empresarial.	35
Figura N°3. Situación en caso de una falla de interfaz entre SW1 y SW4.	36
Figura N°4. Estado del cableado.....	40
Figura N°5. Estado de los equipos.....	40
Figura N°6. Ecuación del costo total esperado	43
Figura N°7. Localización de la red en el mapa mundial	44
Figura N°8. Diseño de una red LAN en Riverbed Modeler.....	44
Figura N°9. Switch de distribución conectado a las subredes.....	45
Figura N°10. Parámetros de la red.....	45
Figura N°11. Simulación completa en Riverbed Modeler.....	46
Figura N°12. Modelo de diseño de la red LAN de alta disponibilidad.....	47
Figura N°13. Creación de VLAN en CSW1	49
Figura N°14. Creación de VTP en CSW1.....	49
Figura N°15. Configuración modo troncal en CSW1	50
Figura N°16. Configuración switch de acceso (ASW1)	51
Figura N°17. Configuración de protocolo Spanning tree en CSW1	51
Figura N°18. Configuración de protocolo Spanning tree en CSW2.....	51
Figura N°19. Creación de VLAN de gestión en ASW1	52
Figura N°20. Protocolo Spanning Tree para dispositivos finales.....	52
Figura N°21. Configuración LACP en CSW1	53
Figura N°22. Asignación de dirección IP para cada VLAN en CSW1.....	54
Figura N°23. Asignación de dirección IP para cada VLAN en CSW2.....	55
Figura N°24. Protocolo HSRP en CSW1.....	56
Figura N°25. Protocolo HSRP en CSW2.....	56
Figura N°26. Configuración de CSW1 hacia R1 y R2	57
Figura N°27. Asignación de dirección IP en R1.....	58
Figura N°28. Configuración del protocolo EIGRP en CSW1	59
Figura N°29. Configuración del protocolo EIGRP en R1.....	59
Figura N°30. Configuración de puerto seguro en ASW1	60
Figura N°31. Configuración del protocolo SSH y AAA	61

Figura N°32. Simulacion de la red LAN de alta disponibilidad	62
Figura N°33. Ping desde ordenador Logística hacia VLAN 10 y VLAN 20.....	63
Figura N°34. Ping desde ordenador Logística hacia VLAN 30 y VLAN 40.....	63
Figura N°35. Ping desde File Server hacia ordenadores Logística y AdmGer	64
Figura N°36. Ping desde File Server hacia ordenadores ComProy y TI.....	65
Figura N°37. Ping desde ordenador Logística a servidor ISP (Internet).....	66
Figura N°38. Ping desde ordenador AdmGer a servidor ISP (Internet).....	66
Figura N°39. Ping desde ordenador ComProy a servidor ISP (Internet)	67
Figura N°40. Ping desde ordenador TI a servidor ISP (Internet).....	67
Figura N°41. Ping desde ordenador Logística hacia internet simulando una falla física en la interfaz conectada entre ASW1 y CSW1.....	68
Figura N°42. Ruta de respaldo desde ordenador Logística a CSW2	69
Figura N°43. Ping desde ordenador AdmGer hacia internet simulando una falla física en CSW1.....	70
Figura N°44. Rutas de respaldo dirigidas a CSW2.....	70
Figura N°45. Acceso remoto a CSW1	71
Figura N°46. Acceso al servidor web	77
Figura N°47. Balanceo de carga desde ordenador Logística	78
Figura N°48. Raíz primaria en CSW1.....	78
Figura N°49. Servicio activo al simular falla en R1 y CSW1.....	79
Figura N°50. Servicio activo al simular falla en R2 y CSW2.....	79
Figura N°51. Servicio activo al simular falla en R1 y CSW2.....	80
Figura N°52. Servicio activo al simular falla en R2 y CSW1.....	80
Figura N°53. Credenciales del servidor AAA.....	81

LISTADO DE TABLAS

Tabla N°1. Topologías de red.....	14
Tabla N°2. Características LAN IEEE 802	15
Tabla N°3. Capas equivalentes del modelo OSI y TCP/IP	16
Tabla N°4. Delimitación de los tipos de VLAN.....	17
Tabla N°5. Tipos de protocolo Spaning Tree (STP)	18
Tabla N°6. Comparación de modos de trabajos.....	19
Tabla N°7. Terminología del algoritmo dual	21
Tabla N°8. Diferencias entre TACACS+ y RADIUS	22
Tabla N°9. Dominios de la norma ISO/IEC 27002.....	23
Tabla N°10. Diagrama de Gantt de actividades del presente año (2020)	34
Tabla N°11. Características del histórico de caídas en la red	37
Tabla N°12. Proyectos actuales de la empresa	38
Tabla N°13. Impacto económico en un escenario actual	39
Tabla N°14. Dispositivos de red en la compañía.....	41
Tabla N°15. Comparación de los gastos de la empresa	42
Tabla N°16. Cantidad de empleados de oficina en la empresa.....	42
Tabla N°17. Costo total esperado (OEC)	43
Tabla N°18. Características de los equipos asociado a cada subred.....	47
Tabla N°19. Asignación de VLAN para cada área de la empresa	48
Tabla N°20. Dirección IP para cada subred en CSW1 y CSW2.....	54
Tabla N°21. Asignación de subred en modo activo y respaldo para CSW1 y CSW2.....	54
Tabla N°22. Asignación de dirección IP en CSW1 y CSW2 para enrutamiento...	57
Tabla N°23. Asignación de dirección IP en R1 y R2 para enrutamiento	58

RESUMEN

En la actualidad la alta disponibilidad para los sistemas de redes y comunicaciones, son determinados como requerimientos cada vez más importante para las empresas, puesto que no deben permitir tiempos de inactividad en sus servicios. El presente trabajo se enfoca en la empresa Corporación Sehover, a fin de resolver el problema a posibles caídas de dispositivos físicos o lógicos de la red que ocasionan una pérdida de productividad y recuperación de tiempo para la reactivación del servicio, en efecto, perjudica la transferencia de información de los proyectos de la empresa, asimismo, genera un gran impacto económico negativo, dado que se tiene que impartir las obras a los clientes en los tiempos establecidos por contrato. En medio de este escenario se desarrolla la norma internacional ISO 27002, que se centra en las buenas prácticas para la gestión de la seguridad de la información. En adición a lo anterior, se propone el diseño de una red LAN con una característica de alta disponibilidad que soluciona el problema de las caídas de la red, basándose en un adecuado costo-beneficio como es la reducción del CAPEX y OPEX. De igual manera, se emplea una metodología adecuada que realiza pruebas de conceptos para el análisis respectivo del trabajo, terminando con la validación de los resultados obtenidos para aminorar ese impacto negativo y pérdidas de producción al mínimo en la empresa.

INTRODUCCIÓN

Dentro de toda organización es fundamental salvaguardar la información corporativa, ya que es el activo más valioso en cualquier institución. A fin de mitigar el menor impacto posible de daños informáticos, es fundamental tener una red que permita la continuidad de actividades obteniendo acceso a los archivos de la empresa en caso de desastres naturales y daños en los dispositivos físicos o lógicos. En adición, para lograr un uso adecuado de la información, es necesario la coordinación entre los usuarios y personal de TI para que el funcionamiento sea confiable.

La empresa Corporación Sehover, actualmente cuenta con una topología de red LAN simple sin redundancia, lo que ante una falla física en uno de los dispositivos de redes o en el cableado, originará que los empleados no accedan a la información corporativa, lo que en consecuencia afectará las labores de oficina y supervisiones de los diferentes proyectos que realiza la empresa en las distintas regiones del Perú. De acuerdo con la premisa previa, se hace de requerimiento tener una red LAN con alta disponibilidad que permita realizar trabajos de oficina sin temor a que se pueda perder información valiosa para la empresa. Debido a esto, una red que permita la continuidad de actividades corporativas, a pesar de fallos en los sistemas, es una opción práctica y fehaciente para las instituciones públicas y privadas, quienes podrán intercomunicar sus bases de datos con los diferentes dispositivos tecnológicos. De esta manera podrían proporcionar siempre el acceso a la información y a recursos internos de la red corporativa para los empleados. Es por ello que en este trabajo se presenta un modelo moderno de cómo usar la tecnología, y que tiene como objetivo general implementar una red LAN-WAN con alta disponibilidad, que permita minimizar el impacto que podría tener un fallo en un enlace o dispositivo, ya que se podría interrumpir las actividades laborales por horas o días, en efecto, esto generaría incomodidad y credibilidad con los clientes, asimismo, ocasionaría pérdidas económicas por las sanciones de no completar el proyecto en el plazo establecido según el contrato que se tenga.

En el capítulo 1 se describe el marco teórico, donde se detalla la definición de los protocolos de red a utilizar y los estados de arte relacionados al trabajo realizado. Adicional a ello, se define los términos básicos relacionados. En el capítulo 2 se describe una metodología adecuada para la resolución del problema, realizando pruebas de conceptos de la red. Luego se aclara la determinación y análisis del problema, donde se indica las características del lugar donde se realiza el trabajo. Posteriormente se describe el modelo de solución propuesto que contribuirá a la adquisición de información relevante considerando artículos de otros autores con los métodos y procedimientos que se deben realizar para validar el diseño de la red de alta disponibilidad. Al final se detalla los resultados obtenidos. Terminando con las conclusiones, recomendaciones, bibliografía y anexos correspondientes.

Durante el año pasado se reportó algunos problemas en la red, en los cuales, una de ellas fue la caída del servicio de internet por falta de confiabilidad y gestión en la red, no obstante, la gerencia opto por brindar las facilidades para la implementación de un servicio dedicado de internet a inicios del presente año y así evitar más multas por parte de sus clientes por causa de la falta del servicio, sin embargo, es necesario el diseño de una red que brinde la disponibilidad en todo momento. Entonces de este hecho descrito, se realiza la formulación del problema.

¿De qué forma un diseño de red LAN de alta disponibilidad permitirá a la empresa Corporación Sehover S.A.C. mejorar el nivel de servicios para los clientes de instituciones públicas y privadas?

OBJETIVOS

- a. General
Diseñar una red LAN-WAN de alta disponibilidad para minimizar el impacto ante fallas.
- b. Específicos
 - Reducir los tiempos de recuperación en la red, en caso de que se produzca un fallo en el servicio.
 - Determinar los equipos a usar como respaldo el cual se deben activar al instante de que el equipo principal sea afectado.
 - Caracterizar los protocolos asignados que habiliten las vías alternas de la manera más rápida que sea posible.

CAPÍTULO I: MARCO TEÓRICO

1.1 Bases Teóricas

1.1.1 Marco Teórico General

1.1.1.1 Red de área local

Es una red de datos que se aplica en un área reducida o pequeña, en el cual se conectan las estaciones de trabajo, terminales y dispositivos de un edificio u oficina. Esta tecnología conecta todos los equipos que comparten recursos o acceso a la información almacenada de manera local. Brinda conectividad permanentemente y utiliza las normas del modelo OSI. Algunas de las tecnologías LAN más comunes son Ethernet, FDDI y Token Ring, sin embargo, el estándar más utilizado es el Ethernet (Zheng, 2017)

1.1.1.2 Tipos de topologías de red LAN

En la Tabla N°1 se detalla los diferentes tipos de topologías de red LAN.

Estrella	En esta topología, cada nodo de los diferentes equipos se conecta directamente a un servidor central. Todos los datos dependen del servidor antes de alcanzar su destino. Esta es una topología común tanto en redes Ethernet como inalámbricas.
Malla	En esta topología, cada nodo se enlaza con los demás nodos. Como los nodos no está físicamente conectado a todos los demás, esto crea una conexión redundante. Una red en malla emplea dos distribuciones de conexión: topología de malla completa o de malla parcial. En la topología de malla completa, cada uno de los nodos se conecta directamente con todos los demás. En la topología de malla parcial, los nodos se conectan sólo a algunos de los otros nodos, no a todos.

Bus	Esta topología permite adicionar o retirar nodos sin interferir con el resto de los enlaces, sin embargo, ante un fallo en el medio de transmisión causaría la anulación de la red. Una de sus ventajas es que poseen un costo reducido y son fáciles de instalar, son empleadas en redes pequeñas y con poco tráfico
Anillo	Los nodos se conectan en serie alrededor del anillo, sería equivalente a unir extremos de una red en bus donde los datos se transmiten en una dirección, cruzando por todos los dispositivos que sean necesarios hasta llegar a su destino
Jerárquico	Esta topología de red, los elementos se enlazan de forma doble o masiva, constituyendo un nodo de enlace principal desde el que se ramifican los demás nodos. Ante posibles caídas de un enlace, no afectaría la comunicación en la red

Tabla N°1. Topologías de red
Fuente: Universidad de Valencia (2009).

1.1.1.3 Estándares para redes LAN: IEEE 802

El Instituto de Ingenieros Electricistas y Electrónicos (IEEE) establece un comité, denominado 802, donde detalla la elaboración de unos estándares para las redes de área local. El Comité IEEE 802 definió tres estándares: la Red Ethernet de Xerox con la denominación LAN IEEE 802.3, la Red Token Bus MAP de la compañía General Motors con la denominación LAN IEEE 802.4 y la Red Token Ring de la compañía IBM con la denominación LAN IEEE 802.5, como se detalla en la Tabla N°2. (Briceño, 2005)

1.1.1.3.1 Estándar LAN IEEE 802.1: Este estándar define direcciones para estaciones LAN de 48 bits en todos los estándares 802, asimismo, cada adaptador puede tener una dirección única. Los proveedores de tarjetas de interfaz de red están registrados ya que los tres primeros bytes de la dirección son asignados por el IEEE y ellos pueden crear una dirección única para cada uno de sus productos. (Cuazitl, 2013)

1.1.1.3.2 Estándar LAN IEEE 802.2: Detalla el protocolo de control de enlaces lógicos (LLC) del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación, usando el protocolo LLC el cual es derivado del protocolo de Alto nivel para Control de Enlaces de Datos (HDLC), y ambos son parecido en su operación. (Cuazitl, 2013)

1.1.1.3.3 Estándar LAN IEEE 802.3: Este estándar adquiere como base la red Ethernet, que define el método de Acceso Múltiple con Detección de Colisiones (CSMA/CD) sobre varios medios. Asimismo, se puede encontrar una cantidad de opciones que le dan al usuario flexibilidad y variedades en la mayor parte de las aplicaciones. (Cuazitl, 2013)

CARACTERISTICAS	LAN IEEE802.3	LAN IEEE 802.4	LAN 802.5
Topología	Barra / Árbol	Barra Física Anillo Lógico	Anillo Físico
Método de acceso	CSMA/CD	Barra de Contraseña (Token Bus)	Anillo de Contraseña (Token Ring)
Forma de Transmisión	Banda de Base/ Portadora Modulada	Banda de Base/ Portadora Modulada	Banda de Base
Velocidad de Transmisión	10 Mbps	1a 20 Mbps	1, 4 y 16 Mbps
Código de Línea	Manchester/DPSK	Manchester/ FSK, PSK	Differential Manchester
Medio de Transmisión	Cable Coaxial, Par Trenzado, Fibras Ópticas	Cable Coaxial Fibras Ópticas	Par Trenzado Fibras Ópticas
Distancia Máxima entre Estaciones	1500 (Con Repetidores)	800 m	100 m
Número Máximo de Estaciones	100 (Segmento de 500 m)	45	260

Tabla N°2. Características LAN IEEE 802
Fuente: Briceño (2005, p.366)

1.1.1.4 Modelos de redes

1.1.1.4.1 Modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos) detalla un sistema de reglas que proporciona a todos una serie de estándares que aseguren la compatibilidad de los diferentes equipos. De acuerdo con este modelo de red, explica la forma de como la información se transmite a través de la red y en adición a ello explica como los paquetes viajan a través de las capas de una red a otra. “Este modelo cuenta con 7 capas, cada uno con diferente función” (Zheng, 2017). Las capas del modelo OSI son: Capa física, capa de enlace de datos, capa de red, capa de transporte, capa de sesión, capa de presentación y capa de aplicación. (Aguirre et al., 2017)

1.1.1.4.2 Modelo TCP/IP

El modelo TCP/IP (Protocolo para el Control de Transmisión/ Protocolo de Internet), se encuentra determinado por cuatro capas, por lo que cada una se encarga de determinados aspectos en la comunicación y a su vez cada una brinda un servicio específico a la capa superior. Este modelo es usado para los sistemas de comunicación donde se describe un conjunto de reglas generales de operación para permitir que un equipo pueda conectarse con una red, adicional a esto, proporciona una conectividad de extremo a extremo, detallando la manera en que los datos deberían ser transmitidos y recibidos por el destinatario. (Aguirre et al., 2017)

1.1.1.4.3 Comparación entre OSI y TCP/IP

Existen algunas características entre estos modelos que lo hacen parecer similares, ya que el propósito para el que fueron creados sea el mismo de como viaja la información a través de una red. En la Tabla N°3 se compara ambos modelos.

Modelo OSI	Transmisión	Modelo TCP/IP
Aplicación (Servicios y Aplicaciones)	Datos	Aplicación
Presentación (Presentación de los datos)		
Sesión (Comunicación entre dispositivos de la red)		
Transporte (Comunicación extremo-extremo)	Segmentos	Transporte
Red (Dirección lógica IP)	Paquetes	Internet
Enlace de datos (dirección física MAC y LLC)	Tramas	Acceso a la Red
Física (Señal binaria)	Bits	

Tabla N°3. Capas equivalentes del modelo OSI y TCP/IP

Fuente: Aguirre et al. (2017)

1.1.1.5 Jerarquía en la red

Un diseño jerárquico implica dividir la red en capas que deben satisfacer las necesidades actuales de las organizaciones y adoptar nuevas tecnologías, cada capa proporciona funciones específicas que definen su función dentro de la red general. Se categoriza las redes según la cantidad de dispositivos que se atienden: red pequeña, red mediana y red grande. Donde existen 100, 1000 y más de 1000 dispositivos conectados respectivamente (Zheng, 2017).

1.1.1.5.1 Niveles de red jerárquico

- **Capa de acceso:** Se detalla el acceso el punto a través del cual los usuarios pueden ingresar en la red. Brinda acceso a la red para las terminales. La capa de acceso para la red empresarial incorpora switches de capa 2 y puntos de acceso que proporcionan conectividad entre las estaciones de trabajo y los servidores. Esta capa se encarga de: Ancho de banda compartido, ancho de banda conmutado, filtrado de la capa MAC y microsegmentación. (Zheng, 2017).

- **Capa de distribución:** Se detalla la concentración de los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo. Utilizando routers o switches multicapa, se puede proporcionar agregación de enlaces, redundancia y balanceo de carga. Usando listas de acceso y otros filtros para limitar lo que entra en el núcleo, es decir define las normas de red para manipular cierto tipo de tráfico y la incorporación de direcciones con el objetivo de preservar los recursos de tráfico innecesarios. (Zheng, 2017).
- **Capa de núcleo:** Ofrece una estructura de transporte fiable y optimizado para reenviar el tráfico de todos los dispositivos de la capa de distribución, por lo tanto, debe enviar grandes cantidades de datos a altas velocidades. El núcleo debe tener una alta disponibilidad y debe ser redundante. (Zheng, 2017).

1.1.1.6 Red de área virtual

Grupo de dispositivos que están configurados de un modo que puedan comunicarse como si estuvieran conectados por el mismo cable. Las VLAN segmentan lógicamente las redes conmutadas basándose en las funciones. Se utilizan las VLAN para tener escalabilidad, mayor seguridad y administrar el flujo de tráfico. (Gonzales, 2017)

1.1.1.6.1 Tipos de VLAN

De acuerdo con lo investigado, existen diferentes tipos de redes VLAN. Algunos de estos se determinan según la clase de tráfico o según la función que cumplan. En la Tabla N°4 se puntualiza los tipos de VLAN.

TIPOS DE VLAN			
VLAN Nativa	VLAN de Datos	VLAN Predeterminada	VLAN Administración
Es asigna a un puerto troncal 802.1Q. Los puertos de enlace troncal donde están conectados entre switches, donde la transmisión de tráfico asociado a más de una VLAN es posible.	Está configurada para gestionar el tráfico por usuarios, no obstante, sin tráfico de voz ni administración. A esta VLAN se conoce como VLAN de usuario.	Cuando se inicia un switch, por defecto todos los puertos forman parte de esta VLAN, que hace que cualquier dispositivo que se conecte al mismo, pueda comunicarse con los demás dispositivos.	Es una VLAN que se configura para acceder de manera remota a la administración del switch, mediante HTTP, Telnet, SSH o SNMP.

Tabla N°4. Delimitación de los tipos de VLAN
Fuente: Hospina (2017)

1.1.1.7 Protocolos de alta disponibilidad

1.1.1.7.1 HSRP

Hot Standby Router Protocol (HSRP) es el protocolo más utilizado para el despliegue de enrutadores tolerantes a fallos en una red, cuyo objetivo es proporcionar redundancia nivel de puerta de enlace en capa 3 del modelo OSI. HSRP fue desarrollado por Cisco y está documentado en RFC 2281 (documentos que contiene notas técnicas y organizacionales de internet) como “un protocolo que proporciona un mecanismo para admitir la conmutación por error no disruptiva del tráfico IP en determinadas circunstancias” (Li, Cole y Morton, 1998). HSRP proporciona un mecanismo para la detección y recuperación de fallas del enrutador y puerta de enlace. Donde las interfaces de dos o más enrutadores multicapa son asignadas a un grupo HSRP. Dentro de ello existe dos tipos de dispositivos, un enrutador denominado como “activo” quien se encarga de procesar los paquetes IP que son enviados a la dirección IP virtual, y otro enrutador del grupo es elegido como “respaldo”, el cual está listo para asumir el papel del enrutador “activo” en caso de que este último falle. Este cambio de rol se denomina conmutación por error. Si el enrutador de respaldo falla o se convierte en el enrutador activo, entonces se elige otro enrutador como enrutador en espera. Adicional a lo descrito, HSRP tiene la capacidad de activar una conmutación por error si la interfaz habilitada para HSRP en el enrutador deja de funcionar. (Cisco Systems, 2006)

1.1.1.7.2 STP

El Protocolo de árbol de expansión (STP) proporciona una topología sin bucles en una red con enlaces redundantes. Este protocolo se detalla en el estándar IEEE 802.1D, donde indica un intercambiando de mensajes BPDU con otros conmutadores para detectar bucles y a su vez se anula las demás rutas. Este protocolo garantiza una sola ruta activa entre dos dispositivos de red. (Cisco Systems, 2007). En la Tabla N°5 se describe los tipos del protocolo STP.

PVST	Utiliza el protocolo de enlace troncal ISL propiedad de Cisco, donde cada VLAN cuenta con una instancia de spanning tree y posee capacidad de balancear la carga de tráfico de la capa 2. Asimismo, incluye las extensiones BackboneFast, UplinkFast y Portfast
PVST+	Admite el protocolo ISL y enlace troncal 802.1Q. Asimismo, admite las extensiones de STP, el cual agrega mejoras en la protección de BPDU y en la protección de raíz.
PVST+ rápido:	Protocolo basado en el estándar IEEE 802.1w. Asimismo, posee convergencia más veloz que 802.1D y protección tanto de raíz como bucle. Donde se asigna prioridad en las rutas para cada subred.
RSTP:	Brinda convergencia más veloz que 802.1D. Implementa versiones genéricas de las extensiones STP propiedad de Cisco
MSTP:	Asigna varias VLAN a una misma instancia de spanning-tree, el cual fue inspirado en el protocolo STP de múltiples instancias (MISTP) de Cisco.

Tabla N°5. Tipos de protocolo Spaning Tree (STP)

Fuente: Huawei (2018)

1.1.1.7.3 Etherchannel

Es una tecnología normada de acuerdo con los estándares IEEE 802.3 full duplex Fast Ethernet. Donde se detalla la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace lo que permite sumar la velocidad de cada puerto físico Ethernet usado y de esta manera obtener un enlace troncal de alta velocidad. EtherChannel proporciona velocidades de enlace incrementales entre Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet. EtherChannel combina múltiples Fast Ethernet hasta 800 Mbps, Gigabit Ethernet hasta 8 Gbps y 10 Gigabit Ethernet hasta 80 Gbps. (Web Cisco, 2007)

- LACP: Link Aggregation Control Protocol, de acuerdo a la aplicación de este protocolo, es usado para controlar los enlaces y formar una troncal-ethernet que aumenta el ancho de banda del enlace. Este protocolo se basa en el estándar IEEE 802.3ad, donde se establece enlaces troncal-ethernet entre dispositivos de los diferentes proveedores. (Forum Huawei, 2019)
- PagP: Port Aggregation Protocol, de acuerdo con este protocolo, fue desarrollado por Cisco. Al igual que LACP, este protocolo también verifica los parámetros necesarios para formar el enlace troncal-ethernet. Sin embargo, ya que PAgP es un protocolo privado no se puede usar para establecer el enlace troncal-ethernet entre dispositivos de diferentes proveedores. (Forum Huawei, 2019)

En la Tabla N°6, se realiza una comparación entre estos dos protocolos.

	LACP	PagP
Port Mode	Passive	Auto
	Active	Desiable

Tabla N°6. Comparación de modos de trabajos.

Fuente: Forum Huawei (2019).

De la Tabla N°6 se visualiza que el modo de trabajo automático de la interfaz PagP es el mismo que el modo pasivo en LACP, mientras que el modo deseable es el mismo que el modo activo en LACP (Forum Huawei, 2019)

1.1.1.7.4 EIGRP

Protocolo de enrutamiento de puerta de enlace interior mejorado, propiedad de la compañía Cisco, el cual ofrece algoritmos de vector de distancias, que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Funciona como protocolo de enrutamiento para IP, el cual usa una tabla de ruteo donde guarda todas las redes disponibles, asimismo, encontrar los mejores caminos para llegar a su destino. Este protocolo tiene funciones de escalabilidad de redes, es decir, EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que otros protocolos de enrutamiento. Esto permite que una red tenga una arquitectura mejorada. (Cisco Systems, 2005)

- Tabla de vecinos: Cada router configurado con el protocolo EIGRP, mantiene una tabla de rutas vecinas que enumera a los routers adyacentes. Asimismo, existe una tabla de rutas vecinas por cada protocolo que admite EIGRP.
- Origen de la ruta: Identifica el router que publicó la primera ruta. Este campo se llena solo para las rutas que se aprenden de una fuente externa a la red EIGRP. El rotulado de rutas puede resultar particularmente útil con el encaminamiento basado en políticas.
- El protocolo EIGRP evita la aparición de bucles, asimismo, impide que se envíe actualizaciones por la misma interfaz por la que han sido recibidas.

1.1.1.8 Balanceo de carga

Se refiere al proceso en el que un equipo detecta varios caminos a una red específica a través de diferentes procesos de ruteo, en donde instala una ruta con la mínima distancia administrativa en la tabla de ruteo. Asimismo, selecciona una ruta entre varias existentes, a través del mismo proceso de ruteo con la misma distancia administrativa. Es decir, el router elige la trayectoria de la métrica más baja hacia el destino. Cada proceso de ruteo calcula su costo de forma diferente y es posible que se deban manipular los costos para alcanzar el balanceo de carga. Si el router recibe e instala varias trayectorias con el mismo costo y la misma distancia administrativa a un destino, puede ocurrir el balanceo de carga. La cantidad de trayectorias que se utilizan está limitada por la cantidad de entradas que el protocolo de ruteo coloque en la tabla de ruteo. Los procesos de ruteo EIGRP soporta el balanceo de carga de costos desiguales. Se usa el comando “variance” en la configuración del protocolo EIGRP para lograr el balanceo de carga de costos desiguales. (Cisco Systems, 2015)

1.1.1.8.1 Balanceo de carga desigual

Se define como balanceo de carga con rutas de costo distinto, es decir, capaz de realizar balanceo de carga desigual y equitativo a través de rutas con diferente métrica. El protocolo EIGRP brinda el balanceo de carga desigual, el cual divide el tráfico enviado por cada enlace en relación con su ancho de banda. Las métricas son utilizadas para decidir el porcentaje de tráfico de cada ruta. El proceso multiplica el valor varianza por la lista de sucesores factibles, asimismo, el resultado del cálculo indica el valor máximo de coste que se permite para que otras rutas puedan participar en el balanceo de carga, en donde valor de varianza es uno por defecto. (Cisco Systems, 2015)

1.1.1.8.2 Algoritmo Dual

Se utiliza para asegurar que no haya bucles en cada instancia a través del registro de una ruta en un dispositivo de red. En la Tabla N°7 se describe los términos del algoritmo dual.

Distancia advertida (AD)	Distancia notificada por un router vecino hacia un destino específico.
Distancia factible (FD)	Consiste en la mejor métrica desde un router vecino hasta el destino.
Condición factible (FC)	Condición que debe cumplirse para incorporar un posible camino a la tabla de topología.
Sucesor factible (FS)	Determina un router de respaldo para ser usado en caso de que la ruta al vecino se pierda.

Tabla N°7. Terminología del algoritmo dual

Fuente: Instituto Tecnológico Superior del Oriente del Estado de Hidalgo (2015)

- Query: Son mensajes de consulta emitidos por un router cuando pierde una ruta y no existe un sucesor factible en la tabla de topologías. Estas solicitudes se envían a los routers vecinos para determinar cuál de ellos puede alcanzar al destino.

1.1.1.9 Protocolos de seguridad

1.1.1.9.1 Autenticación, Autorización y Contabilización (AAA)

El acrónimo AAA corresponde a protocolos que realizan tres funciones: autenticación, autorización y contabilización (traducido del acrónimo en inglés). Este protocolo no se refiere a uno solo en particular, es decir, son una familia de protocolos que ofrecen las tres funciones descritas. Los servicios de seguridad de AAA proporcionan un marco principal para configurar el control de acceso en dispositivos de red, de esta manera se controla quien tiene permitido acceder a una red, controlar lo que puedan hacer y observar las acciones mientras accedan a la red de una compañía. (Cisco Systems, 2005)

- **Autenticación:** Se refiere que se debe usar un nombre de usuario y contraseña para acceder a los servicios de la red. (Cisco Systems, 2005)
- **Autorización:** Se refiere a los privilegios que tiene un usuario, basándose en su identidad y el estado verídico del origen. (Cisco Systems, 2005)
- **Contabilización:** Se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información se usa para la administración, planificación, facturación, entre otros propósitos. (Cisco Systems, 2005)
- **Sistema de control de acceso.**

Existen dos sistemas control de acceso que se ejecutan en los servidores AAA, uno es RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) y el otro es TACACS+ (Sistema de control de acceso del controlador de acceso a terminales), en la Tabla N°8 se realiza una comparación entre ambos protocolos.

TACACS +	RADIUS
Utiliza TCP puerto 49.	Utiliza UDP puerto 1812.
Cifra el cuerpo entero del paquete.	Cifra solo la contraseña del paquete.
Ofrece soporte multiprotocolo.	No admite multiprotocolo.
Dos métodos para controlar la autorización de los comandos en un enrutador, por usuario o por grupo.	No permite a los usuarios controlar qué comandos se pueden ejecutar en un enrutador.
Uso principal: Conexión de administración de red	Uso principal: Acceso a la red
Permite separar soluciones de autenticación.	Los paquetes enviados de servidor al cliente contienen información de autorización.

Tabla N°8. Diferencias entre TACACS+ y RADIUS
Fuente: Cisco Systems (2008)

En la Tabla N°8, se observa dos protocolos de seguridad que se utilizan para controlar el acceso a las redes. TACACS+ (sistema de control de acceso del controlador de acceso a terminales) el cual es desarrollado por Cisco y RADIUS (servicio de usuario de acceso telefónico de autenticación remota) que se describe en RFC 2865 ,asimismo, Cisco admite ambos protocolos. RADIUS brinda acceso remoto seguro a redes y servidores que no cuenten con autorización de acceso. TACACS+ es un protocolo de autenticación remota, que se utiliza para conectarse con un servidor de autenticación, asimismo, tiene escalabilidad a medida que las redes crecen y se adaptan a la nueva tecnología de seguridad que se presenta en cada periodo de tiempo. La arquitectura del protocolo TACACS + complementa la arquitectura de autenticación, autorización y contabilidad (AAA). (Cisco Systems, 2008)

1.1.1.9.2 Secure Shell

Secure Shell (SSH) es un protocolo de administración remota que utiliza el puerto 22 TCP, el cual permite a los usuarios controlar y modificar los dispositivos remotos a través de internet, mediante un mecanismo de autenticación como un usuario y contraseña, asimismo, para los datos transmitidos entre los dispositivos que se comunican desde el cliente al host y retransmitir la salida al cliente. El servicio se crea como un reemplazo para Telnet (protocolo sin cifrado) y utiliza técnicas criptográficas para garantizar que toda la información hacia el dispositivo remoto se encuentre cifrada. Existen 2 versiones de SSH, la versión 1 hace uso de algoritmos de cifrado patentados, sin embargo, algunas de estas patentes han expirado y se convierte en una versión vulnerable de seguridad, puesto que permite a un intruso insertar datos a la red. La versión 2 tiene un algoritmo de intercambio de claves mejorado que no es vulnerable al agujero de seguridad en la versión 1. (MIT, 2006)

1.1.1.10 Norma ISO/IEC 27002

La norma ISO (The International Organization for Standardization) brinda un grupo de normas que consolida la seguridad de la información, siendo representada por la serie 27000 en este caso particular, asimismo, la norma ISO/IEC 27002 establece el código de buenas prácticas para la mejora del sistema de gestión de seguridad de la información (SGSI) en las organizaciones, donde esta norma adquiere cada vez mayor importancia. A causa de incidentes en los sistemas de comunicación, el cual ha generado daños a la imagen del negocio o pérdida de información muy importante y generando como consecuencia pérdidas financieras sustanciales, es por ello por lo que las empresas buscan la estructuración de procesos para garantizar que sus servicios estén protegidos contra los diferentes tipos de amenazas virtuales y físicas. En medio de este escenario se establece la norma internacional ISO/IEC 27002 ya que es fundamental para la consolidación de la seguridad de la información, garantizando la continuidad y el mantenimiento de los procesos, alineados a los objetivos estratégicos de la organización. El principal objetivo de esta norma es establecer principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. El cual incluye la selección y administración de controles de la red, tomando en cuenta los riesgos que se encuentren en sus sistemas. En la Tabla N°9 se detalla los dominios que tiene esta norma. (Ostec,2018)

NORMA ISO/IEC 27002	
1	Política de seguridad de la información.
2	Organización de la seguridad de la información
3	Gestión de activos
4	Seguridad en recursos humanos
5	Seguridad física y del medio ambiente
6	Cifrado
7	Seguridad de las operaciones
8	Seguridad de las comunicaciones
9	Control de acceso
10	Adquisición, desarrollo y mantenimiento de sistemas
11	Gestión con los proveedores
11	Gestión de incidencias de seguridad de la información
13	Gestión de continuidad de negocio
14	Cumplimiento

Tabla N°9. Dominios de la norma ISO/IEC 27002

Fuente: Ostec (2018)

1.1.2 Marco Teórico Específico

En esta etapa se va a realizar una revisión del estado de arte tomado en cuenta para el presente trabajo.

En Estepa et al. (2011), refieren que las organizaciones dependen cada vez de servicios de aplicaciones para la gestión de almacenamiento corporativo, por eso no pueden permitir que se queden inoperativos a nivel de sistemas y aplicaciones de la red en sus centros de datos. En adición a ello, señalan que, ante una posible caída de la red, la productividad organizacional de cualquier empresa se quedara paralizada, lo que se convierte en una incertidumbre ya que muchas organizaciones no incluyen estos problemas en su diseño de red. A manera de solución, los autores proponen un nuevo enfoque basado en una función matemática del OEC (costo total esperado) para el diseño topológico de una red LAN el cual incluye el impacto de estas pérdidas de productividad en el diseño de la red, asimismo se logra minimizar el costo de producción y el costo de inproductividad que se tendría ante la inactividad de la red durante un período de operación. En tal sentido, se necesita diseñar redes que aseguren que sean confiables en redundancia y a la vez optimicen los gastos de inversión (CAPEX) y gastos de operación (OPEX). La fórmula fundamental que utilizan es la minimización del costo total esperado (Minimize OEC (A)) que se representa en la ecuación N°1.

$$\text{Minimizar OEC}(A) = A*U + C \dots\dots\dots (1)$$

Donde A representa el período esperado de operación de la red, U es el costo esperado de inproductividad debido a los tiempos de inactividad de la red en relación con las unidades de tiempo de A (A*U representa el OPEX esperado) y C representa el CAPEX.

Los autores realizan el proceso de una prueba de validación para llegar a un resultado, el cual tiene un costo-beneficio para la implementación y diseño de una red. La investigación se realizó en una planta industrial donde los accidentes que involucran enlaces o nodos son recurrentes, lo que es suficiente para ser aplicado en otros escenarios. Los resultados se muestran en una tabla con datos obtenidos para una topología de 7 nodos generada aleatoriamente sobre un 1 km² de superficie, el cual es comparado con otros métodos que son los siguientes: MST (minimum spanning tree), RCDN (Reliability Constrained Network Design).

En Sheghdara y Hassine (2019), afirman que es un requisito para las organizaciones contar con la alta disponibilidad en su sistema de red y comunicación, ya que no pueden permitir tiempos de inactividad en sus servicios. Los sistemas están en constante intercambio de datos en grandes cantidades por lo que se tiene que analizar cómo va a funcionar un sistema mientras se está ejecutando. Aplicando un análisis factible para recuperar momentos de alta disponibilidad mientras se ejecuta el sistema. Los autores realizan una prueba de concepto del protocolo HSRP para explicar y demostrar la aplicación de su herramienta, donde se evalúa eficacia de su herramienta otros estudios de casos reales de redes IP que ejecutan HSRP. El desarrollo de los autores brinda una ayuda para entender como un sistema de alta disponibilidad puede detectar fallas y minimizar el impacto que este tendría. Por lo que a lo largo del artículo los autores describen con eficacia el protocolo HSRP mientras comparan sus resultados con otros casos reales de redes. Este estudio profundiza el comportamiento en el tiempo de ejecución de un sistema, dando como resultado la aplicabilidad de un análisis dinámico de alta disponibilidad donde se aporta una herramienta denominada HA Analyzer, el cual demuestra de manera concisa los errores de comportamiento de alta disponibilidad que se da en la ejecución de una red.

La metodología que se utilizó en este artículo fue la siguiente: Identificación del problema, revisar la literatura, comparar las tecnologías con el trabajo relacionado, caracterizar parámetros de alta disponibilidad, proporcionar un enfoque para recuperar escenarios de alta disponibilidad, analizar escenarios de alta disponibilidad, prueba de concepto del HSRP, descripción y evaluación de la herramienta HA Analyzer, simulación y validación de resultados, proyecto concluido y trabajos a futuro.

El proceso de desarrollo del enfoque de los autores consta de seis pasos principales: (1) recopilar y filtrar las trazas de ejecución, (2) fusionar las trazas filtradas y ordenar la traza agregada, (3) segmentar la traza resultante fases de ejecución, (4) correlacionar la traza fases de ejecución identificadas, (5) detectar y diagnosticar de errores, (6) visualizar los resultados. Los cuales cada proceso se explica a continuación:

- Recopilación y filtrado de trazas de ejecución: Consta de un seguimiento de ejecución se compone de un conjunto de eventos en tiempo de ejecución que están ordenados cronológicamente.
- Fusión y ordenación de la traza en ejecución: Es un conjunto de archivos de texto filtrados, donde cada archivo corresponde a la traza de un solo sistema.
- Segmentación de la traza resultante en ejecución: Se refiere al proceso de identificación de eventos y acciones dentro del comportamiento de un sistema en ejecución.

- Correlación de las fases de ejecución: Se conecta las causas con los efectos. Aplicado como un enfoque de análisis de causa raíz (RCA) para encontrar las razones de las fallas en caso de una deficiencia en la seguridad del sistema.
- Detección y diagnóstico de errores: Se refiere al resultado de la fase de correlación que servirá como base para verificar el comportamiento de la característica de alta disponibilidad, asimismo, diagnosticar anomalías potenciales en las trazas recopiladas.
- Visualización de resultados: Los autores detallan una representación tabular para visualizar los resultados del análisis de trazas, donde se utilizan diferentes colores para distinguir los tipos de eventos y correlaciones, de esta manera, ver ejemplos de resultados relacionados con HSRP.

Como prueba de concepto, los autores han construido un prototipo, denominado HA Analyzer. Una herramienta que tiene como objetivo recuperar y analizar escenarios de alta disponibilidad de HSRP. Esta herramienta es una aplicación basada en Windows, desarrollada utilizando el lenguaje Microsoft.Net C# y Microsoft.Net Framework 4.5. Los autores detallan que para la detección y diagnóstico de errores en el contexto de HSRP, la fase de correlación tiene tres resultados posibles:

1. Traza muestra un comportamiento incorrecto de HSRP: La siguiente situación se realiza basado en la herramienta HA Analyzer, que se detalla a continuación:

- HSRP no detecta la falla y no se recupera: Una interfaz habilitada para HSRP llega a fallar, pero no produce ninguna degradación de la interfaz fallada o actualización de otra interfaz dentro del mismo grupo. Esta es una indicación de que la función HSRP no funciona en absoluto. Dado un seguimiento correcto de conmutación por error de HSRP y para imitar tal situación, mantenemos la falla de la interfaz y eliminamos tanto la degradación como la actualización de HSRP. Es decir, no se deben activar reglas de correlación después de la falla.
- HSRP no detecta el fallo, pero se produce una recuperación: Una interfaz habilitada para HSRP llega a fallar, pero este no la detecta, es decir, no produce una degradación de HSRP de la interfaz fallada. Sin embargo, se lleva a cabo una recuperación de HSRP. Esta es una indicación de que el protocolo no está funcionando correctamente, lo que puede llevar a que dos interfaces estén activas al mismo tiempo, dando un seguimiento correcto de la conmutación por error de HSRP y de esta forma se mantiene la falla de la interfaz, eliminando la degradación de HSRP y conservamos la actualización y recuperación de este.

2. Traza presenta un problema temporal: Durante una conmutación por error de HSRP el tiempo que tarda la interfaz de espera en activarse es mayor que el tiempo normal que se ha configurado. Los problemas se identifican como correlación “baja” entre sus fallas y sus fases de ejecución de recuperación.

3. Traza muestra un comportamiento correcto: Un escenario correcto del funcionamiento del protocolo HSRP, donde el sistema se recupera de una falla dentro de un período de tiempo, es decir, la fase que corresponde a la recuperación está a gran medida correlacionada con la fase que tiene la falla.

Los autores dan como resultado tablas de experimentos, donde la traza es segmentada y correlacionada en un formato tabular y diferenciado por colores donde se visualiza las fallas de enlace, las degradaciones HSRP y las entradas relacionadas con la recuperación. Similarmente tiene diversas tablas donde se adicionan una traza correcta, otra con errores sembrados y finalmente una columna descrita como "Problema diagnosticado" que proporciona los detalles del problema encontrado.

De lo anterior tenemos las siguientes discusiones referente a los artículos revisados:

- Por lo tanto, de Estepa et al. (2011), se deduce que el CAPEX y OPEX son importante para el diseño de una red LAN en cualquier organización, asimismo, este artículo es de interés como base para realizar el presente proyecto, con las restricciones de que no contamos con el software, sin embargo, si se cuenta con el análisis para realizar el cálculo matemático y con las ideas de los métodos a utilizar como es el método de empleado por los autores. Nótese que este artículo falta el modelo de los otros estudios que fueron comparados, no obstante, lo que aporta es de utilidad y beneficio para hacer la prueba que consiste en modelar el CAPEX Y OPEX en la aplicabilidad del proyecto.
- De Sheghdara y Hassine (2019), se deduce que el enfoque propuesto por los autores, denominado HA Analyzer, se adapta a la función de alta disponibilidad del protocolo HSRP, el cual fue totalmente automatizado para recuperar y analizar estas características durante la ejecución de un sistema, dado que los autores han evaluado de forma efectiva su herramienta propuesta mediante la realización de dos experimentos. Asimismo, esto ayuda a comprender cómo los sistemas de alta disponibilidad manejan las fallas y se recuperan en poco tiempo en caso de problemas en la red. Esto es de interés para realizar nuestro proyecto, ya que se toma como referencia el análisis del protocolo HSRP. Nótese que este articulo falta información sobre el software para capturar la simulación, sin embargo, lo que aportan es de consideración para realizar la prueba de concepto que consiste en modelar el diseño de nuestra red de alta disponibilidad.

1.2 Definición de términos básicos

LAN: Es una red de área local de dispositivos que conecta un área reducida a una casa, un departamento o un edificio

VLAN: Acrónimo de LAN virtual, es un método para crear redes lógicas independientes dentro de una misma red física.

Alta disponibilidad: Es la capacidad de un sistema de asegurar la continuidad operacional de servicios a pesar de alguna falla en el sistema o dispositivos.

Protocolo: Conjuntos de reglas o normas que hacen posible una comunicación entre dispositivos de red.

CAPEX: Las inversiones en bienes de capital, gastos en capital, son inversiones de capital que crean beneficios.

WAN: Red de computadoras que une varias redes locales, aunque no estén todos en una misma ubicación física.

STP: Protocolo de red de capa 2 del modelo OSI, el cual gestiona la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes

HSRP: Protocolo de red de capa 3 del modelo OSI, propiedad de Cisco, el cual permite el despliegue de enrutadores redundantes tolerantes a fallos en una red.

Ancho de banda: Espacio que ocupa una canal de comunicación.

Query: Mensajes de consulta emitidos por un router cuando pierde una ruta y no existe un sucesor factible en la tabla de topologías.

RFC: Request For Comments son publicaciones del Grupo de Trabajo de Ingeniería de Internet (IETF)

Jerarquía: Estructura que se establece según la importancia y función que cumple los dispositivos en una topología de red.

Balanceo de Carga: Distribución del tráfico entre dispositivos para compartir el trabajo a realizar entre varios procesos de información.

Topología: Representación gráfica del diseño de Red LAN, donde se muestra las interconexiones y dispositivos de red.

OPEX: Es un costo permanente para el funcionamiento de un producto, negocio o sistema.

ISO/IEC 27002: Norma internacional de gestión de buenas prácticas en servicios de tecnologías de la información.

Norma ANSI/TIA/EIA 568A/568B: Especifica los requerimientos mínimos para el cableado estructurado en oficinas o centros comerciales.

OSI: Modelo internacional de interconexión de sistemas abiertos y de referencia para los protocolos de la red.

Enlace: Vía de comunicación que une dos o más dispositivos.

BPDU: Unidades de datos que contienen información del protocolo Spanning tree (STP).

Latencia: Implica el retardo producido por la demora en la transmisión de paquetes dentro de la red.

Confiabilidad: Detallado como la capacidad de una red para seguir operativo bajo circunstancias, como una posible falla en la red.

Métrica: Valor que se asigna a una dirección IP de una interfaz de red determinada, el cual identifica el costo asociado con el uso de esa ruta.

SSH: Protocolo de red de capa 7 del modelo OSI, cuya función es el acceso remoto a un dispositivo por medio de un canal seguro en el que toda la información está cifrada.

Ping: Comando de diagnóstico que comprueba el estado de la comunicación con uno o varios equipos de una red que ejecutan una dirección IP.

TTL: Comando que se ejecuta en un ordenador para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.

Par trenzado: Comprende por cables de cobre entrelazados entre sí para reducir las interferencias.

Redundancia: Se define como la capacidad de una red que posee dos o más enlaces entre dispositivos.

Patch cord: Tipo de cable que se usa en las conexiones para los puntos de consolidación a los equipos de red, bajo los estándares TIA/EIA 568-A / 568-B.

AAA: Familia de protocolos que realizan tres funciones: autenticación, autorización y contabilización.

IP: Protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI

Wildcard: Máscara de bits que indica qué partes de una dirección IP son relevantes para la ejecución de una acción. Relacionado a la inversa de una máscara de subred.

CAPÍTULO II: METODOLOGÍA DE DESARROLLO DEL TRABAJO PROFESIONAL

En este contexto los trabajos se realizan en la empresa Corporación Sehover S.A.C., el cual se encuentra en el rubro de la construcción, a su vez forma parte del grupo CINTAC S.A. y Compañía del Acero del Pacífico el cual es una de las compañías más importantes en Chile. La empresa Corporación Sehover brinda servicios de construcción en su mayoría al estado peruano, mediante licitaciones que se dan en diferentes partes del país. Entre sus principales clientes están: Rutas de Lima, IIRSA Norte, IIRSA Sur y el Ministerio de Transportes y Comunicaciones. La empresa se dedica al mantenimiento, pavimentación y señalización de carreteras alrededor de distintas provincias del Perú. También se dedica al mantenimiento de puentes como es el caso del “Puente 24 de Julio”, el cual conecta los departamentos de Cajamarca y Amazonas. En adición a esto, la empresa se encuentra realizando pavimentación y señalización para el proyecto Línea 2 del Metro de Lima y Callao. De acuerdo con este contexto, se da por hecho que la empresa se encuentra trabajando ininterrumpidamente con el fin de cumplir como el mejor proveedor de servicios en señalización y seguridad vial, asimismo, a medida que realiza cada obra siempre tienen en cuenta el cuidado del medio ambiente porque no solo se dedica a la seguridad vial, sino también al cuidado del ecosistema. Su compromiso con sus clientes es realizar las obras bajo parámetros que no dañen ni contaminen el medio ambiente en los tiempos establecidos de cada contrato. En conclusión, la empresa se encuentra participando en los proyectos más importantes del país brindando un cuidado al medio ambiente.

Metodología

Este estudio se basa en un trabajo cuantitativo con un alcance experimental que beneficia a la empresa Corporación Sehover, el cual da solución al problema recurrente que tienen con las constantes caídas de la red. De acuerdo con lo descrito, se plantea una serie de pasos para solucionar el problema de la organización y de esta manera obtener los resultados previstos que será de gran utilidad para mejorar la calidad de servicio. Asimismo, se dará por concluido el trabajo. Los pasos de la metodología se explican a continuación:

- **Identificación del problema:** Se identificará el problema de la organización que afecta las labores de oficina y perjudican económicamente, aumentando cada vez más a largo plazo.
- **Levantamiento de la información:** Identificado el problema, se procede a buscar toda la información que sea relevante para encontrar una solución al problema de la organización.
- **Validación con la gerencia:** Se procede a solicitar a la gerencia, la ejecución del proyecto, el cual soluciona el problema de la red y evita que afecte las obras a futuro.
- **Determinación y Análisis del escenario a probar:** Se determina y analiza el problema, asimismo, se busca escenarios que muestren un alcance real de simulación para visualizar y aclarar puntos de la red que no sean precisos.
- **Prueba de concepto y desarrollo:** Se realiza la prueba de concepto de la red en una simulación lo más real posible en la organización, para validar los resultados. En adición, se desarrolla el modelo de solución.
- **Planteamiento del diseño:** Se realiza el diseño de la red con los protocolos necesarios que brinden una alta disponibilidad.
- **Validación de resultados mediante simulación:** Se obtiene el resultado final de la simulación y se verifica que todo esté en los parámetros necesarios para el proyecto, no obstante, si los resultados no se validan, se regresará a la determinación del escenario a probar para buscar otros softwares de simulación real.
- **Resultados previstos y proyecto concluido:** De acuerdo con lo descrito previamente, se realizaron todos los pasos necesarios de la metodología para lograr los resultados esperados y concluir con el proyecto que beneficiará a la organización donde se realiza el trabajo.

Este apartado de la metodología del proyecto se desarrolla de una forma intrínseca, el cual se visualiza en la Figura N°1.

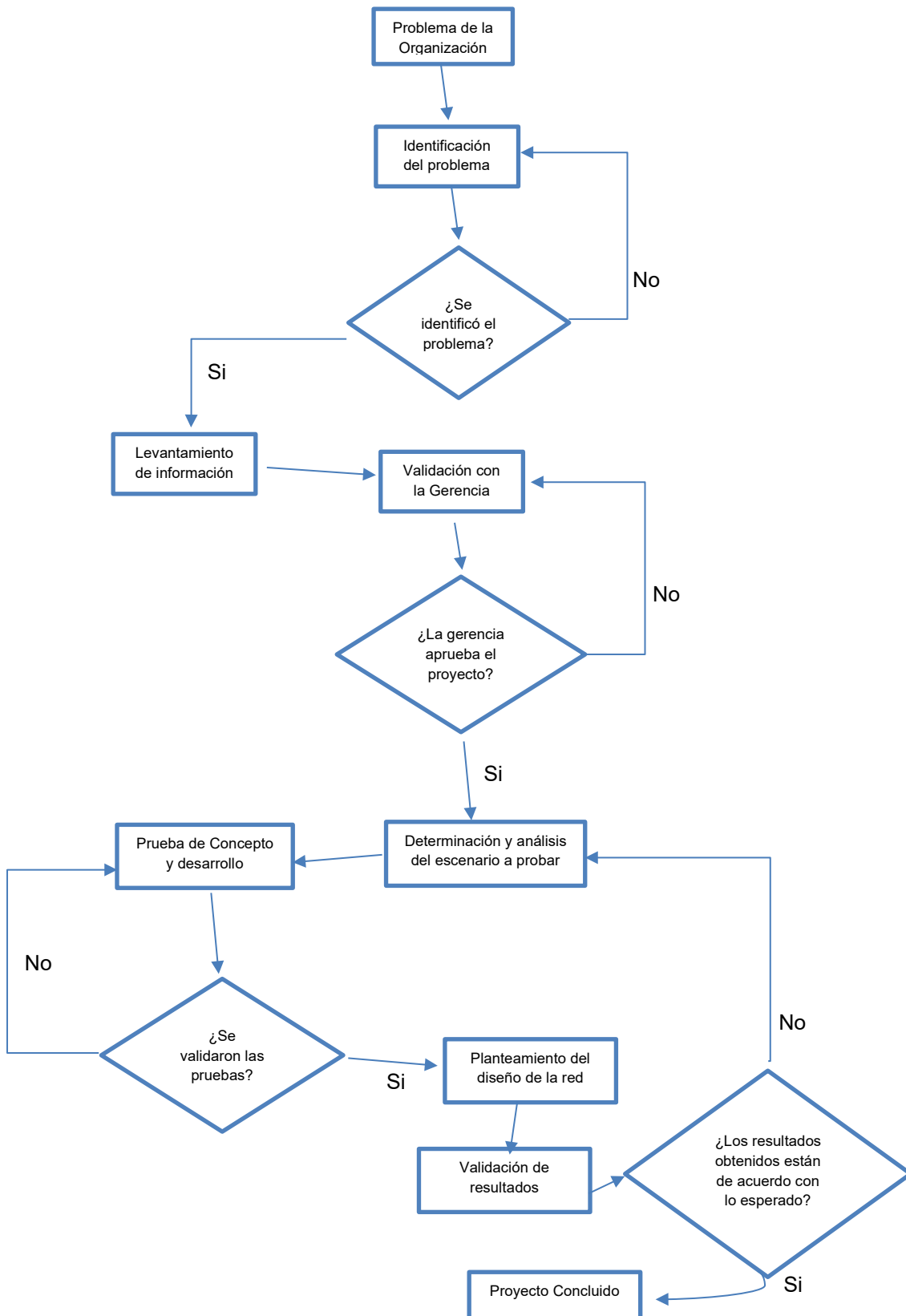


Figura N°1. Diagrama de flujo de la metodología del proyecto.

2.1 Delimitación temporal y espacial del trabajo

Temporal: El presente trabajo cubrirá 5 actividades. El cual comprende los siguientes pasos: Recopilación de información, aprobación del proyecto por parte de la gerencia, análisis del problema, desarrollo del proyecto, diseño y simulación. Asimismo, se visualiza las actividades en la Tabla N° 10.

Actividades	Inicio	Final	Duración	17-Set	22-Set	23-Set	30-Set	1-Oct	9-Oct	10-Oct	22-Oct	23-Oct	6-Nov
1. Recopilación	17/09/2020	22/09/2020	5 días										
2. Aprobación	23/09/2020	30/09/2020	7 días										
3. Análisis	1/10/2020	9/10/2020	7 días										
4. Desarrollo	10/10/2020	22/10/2020	12 días										
5. Diseño y Simulación	23/10/2020	6/11/2020	14 días										

Tabla N° 10. Diagrama de Gantt de actividades del presente año (2020)

Espacial: El diseño de la red es para la empresa Corporación Sehover SAC ubicada en el distrito de Chorrillos, Lima - Perú.

2.2 Determinación y análisis del problema:

2.2.1 Determinación del problema

Hoy en día, las organizaciones requieren cada vez más de la tecnología para que los empleados puedan acceder a servicios como ERP, bases de datos, correo electrónico, aplicaciones, entre otros. Asimismo, se necesita un correcto funcionamiento de la red LAN que establezca protocolos de redundancia y contingencia en las redes de comunicación que tiene la empresa, es decir, estimar una solución para minimizar el impacto que se tendrá si la empresa se queda sin servicio a nivel de sistema, el cual sea ocasionado por alguna falla física o lógica. Esto justifica la importancia de diseñar redes confiables que optimicen los recursos de la empresa, ya que ninguna organización puede permitir que se queden inoperativos a nivel de sistemas y aplicaciones de la red en sus centros de datos, porque la productividad organizacional de la empresa se quedará paralizada, esto se convierte en una incertidumbre ya que muchas compañías no incluyen estos problemas en su diseño de red. En esta realidad la empresa Corporación Sehover, cuenta con una red que se basa en una topología simple sin contingencia, es decir, ante posibles fallas en los dispositivos o en la red LAN, todas las áreas quedan afectadas para continuar en sus labores, asimismo, la empresa recibirá múltiples sanciones por parte de sus clientes, ya que no cumplirán con sus contratos en los tiempos establecidos si se llega a tomar muchas horas o incluso hasta días para la reactivación del servicio de la red.

2.2.1.1 Situación actual de la red en la empresa

La empresa donde se realiza el presente trabajo cuenta con una topología de red sin contingencia, como se muestra en la Figura N°4, producto de ello, ante un posible fallo en los enlaces o dispositivos, se perdería la conexión entre los recursos corporativos y los empleados de la empresa.

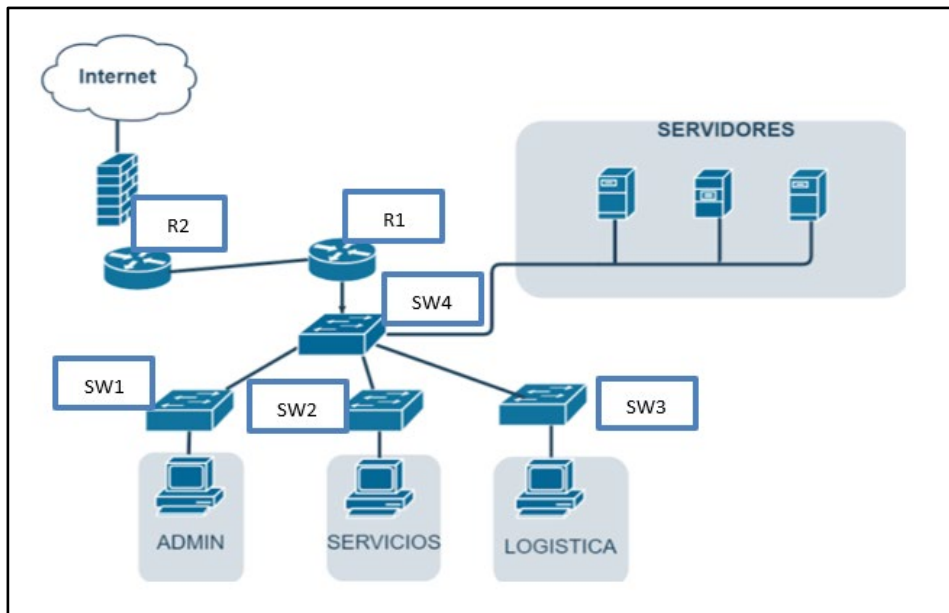


Figura N°2. Situación actual de la red empresarial.

De acuerdo con lo visualizado en la Figura N°2 se detalla la situación actual de la red LAN, donde todos los switches de acceso están conectados por un solo enlace, ocasionando constantes sobrecargas de información, asimismo, ante la caída de un switch de acceso, se perdería la comunicación para una determinada área, y ante la caída de servicio en el switch de distribución (SW4) se pierde la comunicación entre todas las áreas en la empresa. De acuerdo con lo descrito, en caso de que la interfaz entre el switch 4 y el switch 1 deja de funcionar, se perderá total comunicación con el área de administración, el cual incluye el área de gerencia y recursos humanos, asimismo, este posible problema se visualiza en la Figura N°3.

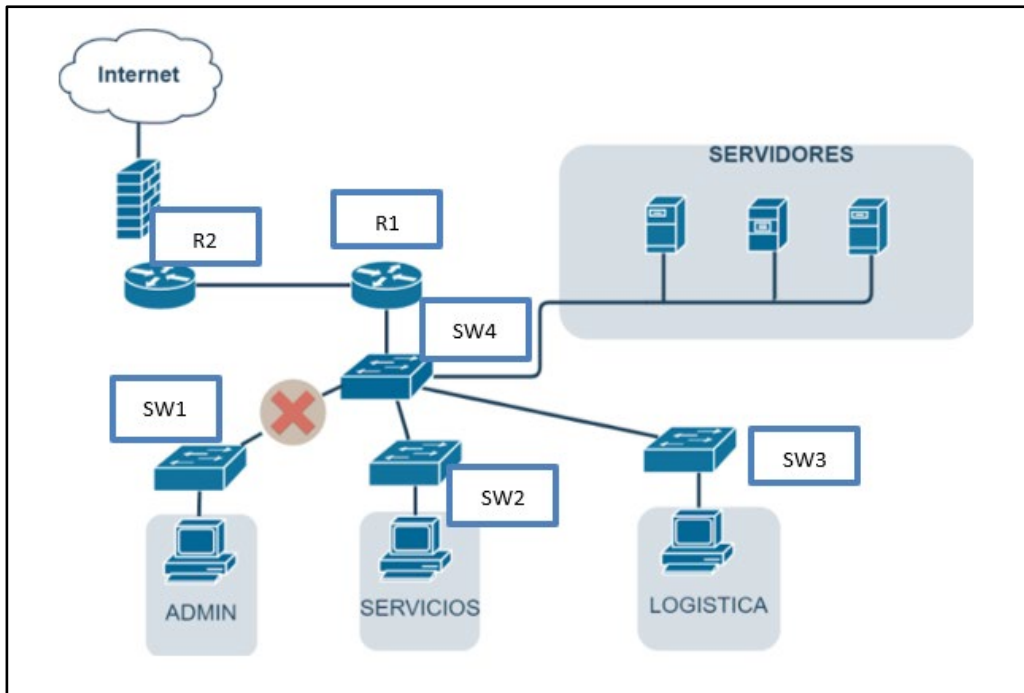


Figura N°3. Situación en caso de una falla de interfaz entre SW1 y SW4.

Como se muestra previamente en la Figura N°3, en caso de que la interfaz tenga un problema físico, el área de administración pierde comunicación total con los servicios de la red LAN. El cual puede tomar hasta un día en poder encontrar y solucionar este inconveniente, ya que ningún switch de acceso cuenta con gestión por ser de modelo obsoleto.

2.2.1.2 Detalle del histórico de la caída de la red

En setiembre del 2019 ocurrió una caída del servicio por problemas con las constantes caídas de internet, lo que llevo a tomar en levantar el servicio una 1 hora, en ese momento no hubo un gran impacto negativo, ya que la empresa contaba con 8 proyectos, además, se compartía la información mediante documentos de microsoft office y disco externo. Sin embargo, durante un corto periodo de tiempo, la cantidad de proyectos se incrementó, y en efecto volvió a ocurrir otras caídas en la red como se muestra en la Tabla N°11.

Caída de la red LAN en la empresa			
Fechas	Tiempos de Recuperación	Empleados Afectados	Impacto Económico
10/10/2019	1h	10	\$ 100
27/11/2019	2h	10	\$ 500
12/02/2020	4h	25	\$ 1200
27/05/2020	5h	30	\$ 2500
11/08/2020	5h	30	\$ 3000
Total	17h	105	\$ 7300

Tabla N°11. Características del histórico de caídas en la red

De acuerdo con el histórico explicado en la Tabla N°11, con el transcurrir del tiempo, vuelve a ocurrir otras caídas de la red y el impacto económico para la empresa es cada vez mayor afectando de forma recurrente a los mismos empleados, es decir, las pérdidas económicas son directamente proporcional a lo largo del tiempo que va aumentando los proyectos para la empresa. En este último reporte del 11 de agosto del presente año, la empresa contaba con 19 proyectos a nivel a nacional.

2.2.1.3 Proyectos actuales en la empresa

Actualmente la empresa cuenta con 36 proyectos a nivel nacional, donde a cada cliente le garantizan un tiempo de entrega para cada proyecto, dado que los proyectos obtenidos por la compañía son en un 90% de licitaciones con el estado peruano, como el ministerio de transportes y comunicaciones. Por lo tanto, es fundamental que las operaciones en la red tengan disponibilidad y confiabilidad en todo momento, en la Tabla N°12 se detalla los proyectos que tiene la empresa.

Proyectos de la empresa		
N° de Proyecto	Código de Proyecto	Descripción del Proyecto
1	01MP19	Servicio de Reciclado y Recapeo de la Carretera Sicuani -Santa Rosa y Pucara
2	01RL19	Señalización horizontal - Panamericana Norte - Rutas de Lima
3	01OB19	Señalización vial - Sausacocha
4	01CM19	Señalización horizontal y vertical - Tramo Pizana - San Juan - Carretera Tocache
5	02OB19	Señalización horizontal y tachas- Carretera Marcona y Chaparra
6	01VI19	Instalación de baldosas pododactiles – Videna - Signovial
7	03RL19	Suministro e instalación de muros New Jersey - Panamericana Sur - Rutas de Lima
8	28IN5A	Señalización horizontal y vertical - Tramo Carretera Ayacucho - Vicalshuaman
9	02MA19	Señalización horizontal y vertical - Tramo Campanilla Arbutus
10	01GV19	Señalización horizontal - Gesvias
11	05CX20	Conservación vial y suministros - Consorcio Oxapampa
12	01NO20	Señalización vial - Nueva Ciudad de Olmos
13	01RL20	Señalización horizontal y tachas - Panamericana Norte
14	01OD20	Señalización horizontal y barreras H3W5 - IIRSA SUR
15	11NCA	Señalización horizontal - Carretera Tramo 2 y 3 - Desviandes
16	01OP20	Operación de carreteras - Señalización horizontal - Red Vial 4
17	02OP20	Operación de carreteras - Instalación de barreras - Red Vial 4
18	01MA20	Construcción Málaga - Señalización horizontal Puente Reither - Von Humbolt
19	02OD20	Suministro e instalación de guardavías - IIRSA NORTE
20	03OD20	Señalización horizontal Tramo 1 y 3 - IIRSA NORTE
21	01OE20	Señalización horizontal Tramo 3 Inambari - Iñapari
22	01JM20	Señalización horizontal y vertical - Corredor Vial - Cocchabamba - Vado Grande
23	02CX20	Servicios integrales de gerenciamiento y logísticos - Consorcio Oxapampa
24	04CX20	Prestación de servicio administrativos y logísticos - Consorcio Oxapampa
25	018R20	Servicios Preoperativos - Consorcio Vial 8R
26	06CX20	Emergencias y riesgo potencial - Consorcio Oxapampa
27	01PU20	Servicios Preoperativos - Consorcio Pucara
28	02PU20	Servicios Administrativos - Consorcio Pucara
29	028R20	Servicios administrativos y logísticos - Consorcio Vial 8R
30	03CX20	Arrendamientos de Equipos - Consorcio Oxapampa
31	97IN1A	Gastos de ventas comerciales - Corporación Sehover
32	01OD20	Mantenimiento periódico de Puente 24 de Julio - Cajamarca - Amazonas
33	01SR20	Construcción y fabricación - Chutana
34	02OE20	Mantenimiento periódico - Bacheo y sello de Fisuras - Madre De Dios
35	03ML20	Servicio de Asfaltado Estación 26 y 27 - Consorcio M2 Lima
36	04ML20	Servicio de Asfaltado Estación 4 - Consorcio M2 Lima

Tabla N°12. Proyectos actuales de la empresa

De la Tabla N°12 se visualiza que, desde la última revisión de caída de la red a la actualidad, aumentó la cantidad de proyectos a nivel nacional, entonces en un escenario actual donde es posible la caída de la red de comunicación en la empresa, afectará enormemente en pérdidas económicas para la empresa y se perderá el estado de confianza con los clientes.

2.2.1.4 Impacto económico en un escenario actual

En la actualidad, la organización no puede permitir que exista una probabilidad de caída en la red y que se paralice todas las labores. Por ello se detalla en la Tabla N°13 el impacto que ocasiona una posible caída en la red. Los datos se calcularon basándose en información de la organización, utilizando métodos aritméticos.

Caída de la red por proyectos			
Cantidad de Proyectos	Tiempo de reactivación	Clientes Afectados	Impacto Económico
1	15min	1	\$ 400
4	1h	2	\$ 1600
12	3h	9	\$ 4800
20	4h	14	\$ 8000
36	7h	25	\$ 14 400

Tabla N°13. Impacto económico en un escenario actual

De lo anterior en la Tabla N°13, se observa que el tiempo de inactividad del servicio es proporcional a la cantidad de los proyectos, en efecto, al final se suman todos los proyectos, lo que da como resultado una pérdida de 14 400 dólares para la empresa por sanciones que recibiría al no cumplir con los contratos de los proyectos en el tiempo establecido. Es decir, la empresa está en constante riesgo económico porque tiene muchos proyectos en ejecución y no tiene un sistema de red con alta disponibilidad.

2.2.2 Análisis del problema

2.2.2.1 Análisis del estado de la infraestructura

- Cableado estructurado: La empresa no cuenta con una topología de red adecuada, donde existen switches en diversos pisos, distintas marcas y modelos generando cascadas. El cableado que se tiene es de categoría 5e. En la Figura N°4 se observa el estado del cableado.



Figura N°4. Estado del cableado

- Equipos obsoletos: Equipos sin administración y con procesadores obsoletos, el cual cuentan con más de 5 años en promedio de compra. En la Figura N°5 se visualiza el estado de un switch marca Satra.



Figura N°5. Estado de los equipos

- **Caída del servicio de internet:** La empresa cuenta con un internet hogar del proveedor Movistar, el cual no es un Internet dedicado, por ello se cae el servicio constantemente. Al no ser corporativo el tiempo de respuesta de soporte por parte del operador excede a las 4 horas de atención.
- **Seguridad de la información:** La Información de los usuarios se almacena en sus equipos locales y en equipos portátiles, asimismo, todos cuentan con el privilegio de control total. Los dispositivos USB no tienen restricción, cualquier usuario puede llevarse información a sus casas sin ningún inconveniente.
- **Procedimiento de respaldo:** La empresa no cuenta con un plan de backup, es decir, no cuentan con un procedimiento de respaldo de la información. Ante un problema grave de hardware o software, se pierde toda la información almacenada en los discos duros.
- **Navegación web sin restricciones:** Todos los empleados tienen salida libre a la navegación de internet, es decir, pueden acceder a las redes sociales, YouTube, Facebook entre otras aplicaciones y descargarlas, generando saturación del ancho de banda.

2.2.2.2 Análisis cuantitativo de la infraestructura.

La empresa cuenta con diferentes dispositivos de redes, entre los cuales se encuentran: routers, switches, servidores, impresoras, access point, cámaras, teléfonos, ordenadores de escritorio y ordenadores portátiles. En la Tabla N°14 se detalla la cantidad de equipos que existe en la compañía.

Equipos	Cantidad
Router	2
Switch	4
Access Point	5
Impresoras	5
Servidor	1
Cámaras	6
Desktop	8
Laptop	40

Tabla N°14. Dispositivos de red en la compañía

De acuerdo con lo previamente descrito, se observa que los equipos de red como el servidor, el switch de acceso que cuenta con 24 puertos, el router que realiza la conexión entre switches y también la conexión de salida a internet, se encuentran en mal estado de acondicionamiento dentro de un gabinete ubicado en el tercer piso en la oficina de la empresa, asimismo, los demás equipos se encuentran en diferentes pisos para su distribución.

2.2.2.3 Análisis económico para la empresa

De acuerdo con la cotización de los equipos que se usan para el proyecto, se compara con el promedio de las pérdidas económicas que ocasiona la inactividad del servicio anualmente, el cual se observa en la Tabla N°15.

OPEX y OPEX vs Pérdidas económicas			
Año	Costo de Implementación	Costo de operación	Pérdidas económicas
1	\$ 13 900	\$1000	\$14 400
2	-	\$1000	\$15 300
3	-	\$2000	\$17 000
Total	\$ 13 900	\$4000	\$46 700

Tabla N°15. Comparación de los gastos de la empresa

De acuerdo con la Tabla N°15, se visualiza que son mayores las pérdidas para la empresa en un periodo de 3 años porque no cuenta con los recursos de una buena red con disponibilidad en todo momento. Asimismo, en un catastrófico escenario donde tome días reparar la red, la compañía pasará por una gran crisis económica que lo puede llevar a la quiebra. Con esta premisa, se deduce que disponer de una red de alta disponibilidad se toma como una inversión, mas no como un gasto.

2.2.2.4 Análisis cuantitativo de las áreas en la empresa

La empresa está compuesta por 47 empleados de oficina en las diferentes áreas que existe, donde cada uno es productivo y están alineados con los objetivos de la compañía, asimismo, cada área está compuesta por gerentes, jefes, coordinadores, analistas, asistentes y practicantes. En la Tabla N°16 se detalla la cantidad de empleados por áreas.

Áreas	Usuarios
Administración	5
Gerencia	3
Comercial	9
Proyectos	7
Contabilidad	4
RRHH	3
Logística	14
TI	3
Total	48

Tabla N°16. Cantidad de empleados de oficina en la empresa

2.3 Modelo de solución propuesto:

2.3.1 Desarrollo del diseño de la red LAN asociado al CAPEX y OPEX: Se toma como referencia el modelo matemático de Estepa et al. (2011), descrito en el estado de arte, donde desarrolla una ecuación basado en minimizar los gastos de operación y de implementación. Se observa en la Figura N°6 las variables de cada costo para el diseño de la red.

$$\text{Minimizar } OEC(A) = A*U + C$$

Figura N°6. Ecuación del costo total esperado

Fuente: Estepa et al. (2011)

Donde A representa el período esperado de operación de la red, U es el costo esperado de improductividad debido a los tiempos de inactividad de la red en relación con las unidades de tiempo de A (A*U representa el OPEX esperado) y C representa el CAPEX. De acuerdo con los datos obtenidos de la Tabla N°15, la información sobre el costo total esperado (OEC) se observan en la Tabla N°17

Años	CAPEX	OPEX	OEC
1	\$ 13900	\$ 1000	\$ 14900
2	-	\$ 1000	\$ 1000
3	-	\$ 2000	\$ 2000

Tabla N°17. Costo total esperado (OEC)

El costo total esperado detallado en la Tabla N°17, muestra la inversión que realiza la empresa. En el primer año resulta en promedio 14 900 dólares, en el segundo y tercer año solo tomará unos gastos por operación y mantenimiento. Asimismo, ello garantiza la existencia de confiabilidad en los equipos que son parte del diseño de la red LAN de alta disponibilidad.

2.3.2 Validación del escenario a probar.

Se realiza la validación del escenario con un software de simulación, el cual sea lo más real posible con el entorno de la organización. Entonces, para realizar una prueba de concepto de la cantidad de paquetes que utiliza cada usuario, se realiza una simulación en la plataforma Riverbed Modeler Academic Edition 17.5, este programa es utilizado en las diferentes organizaciones a nivel mundial para modelar y simular sistemas de comunicaciones. El cual permite diseñar y estudiar el comportamiento de las redes, dispositivos, protocolos y aplicaciones, brindando escalabilidad en su plataforma. Asimismo, permite a los usuarios mejores procesos de investigación y de desarrollo de una red.

2.3.2.1 Proceso de validación de software

El proceso de la simulación empieza con el diseño una red LAN donde se encuentra un switch de distribución, el cual está conectado con los servidores y con las demás subredes, que representan las diferentes áreas que conforman la empresa. En la Figura N°7, FiguraN°8 y Figura N°9 se visualizan la locación, el diseño de la red y de qué manera está distribuido la red respectivamente.

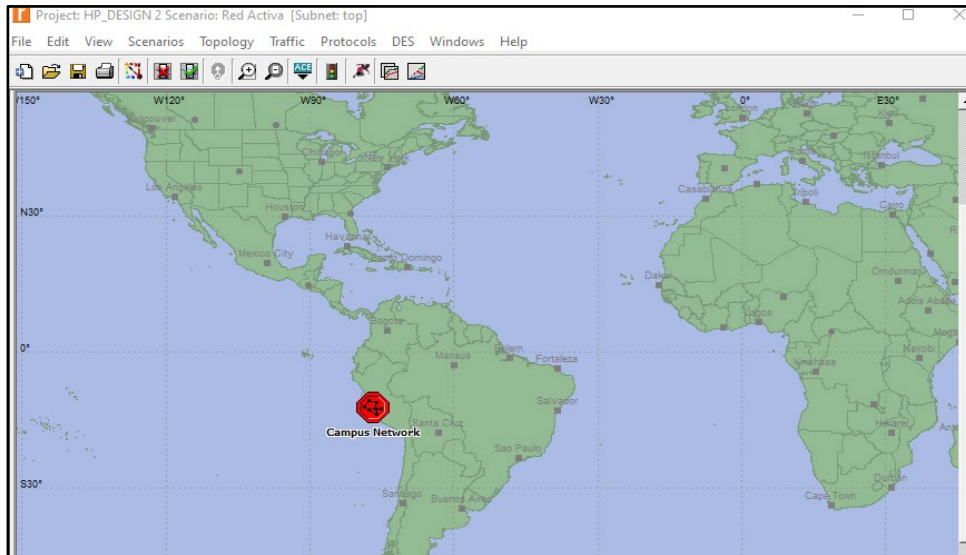


Figura N°7. Localización de la red en el mapa mundial

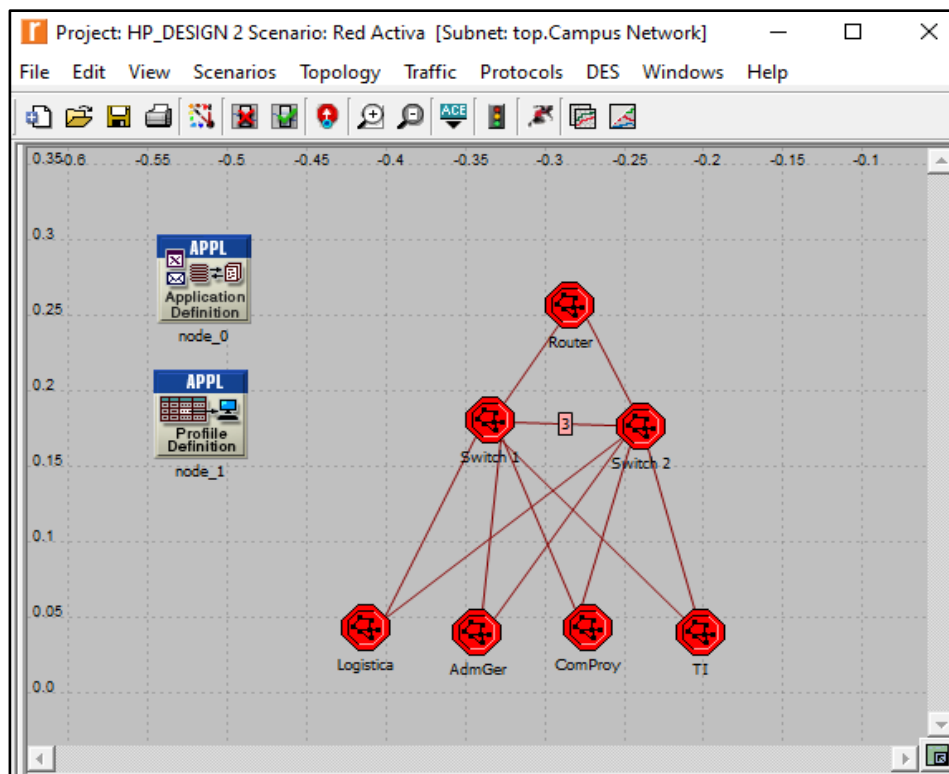


Figura N°8. Diseño de una red LAN en Riverbed Modeler

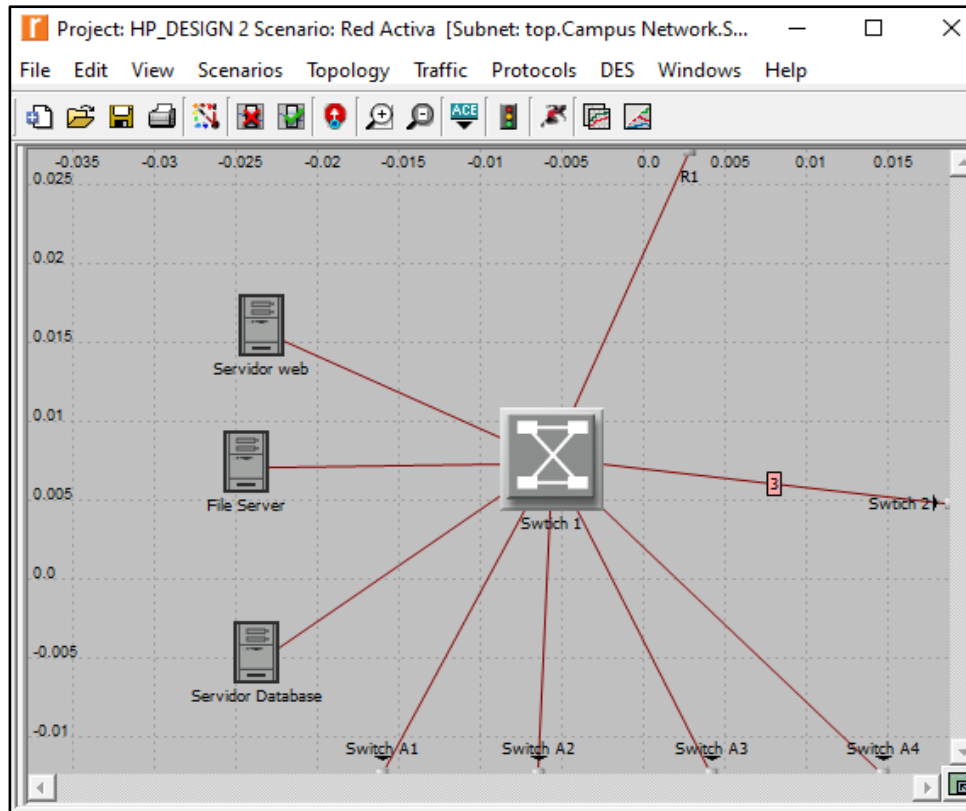


Figura N°9. Switch de distribución conectado a las subredes

2.3.2.2 Parámetros del software

Se asigna los parámetros del software en un tiempo de 30 minutos, asimismo para el proceso de ejecución de la simulación se incluye diferentes tipos de tráfico de red. Estos parámetros se visualizan en la Figura N°10.

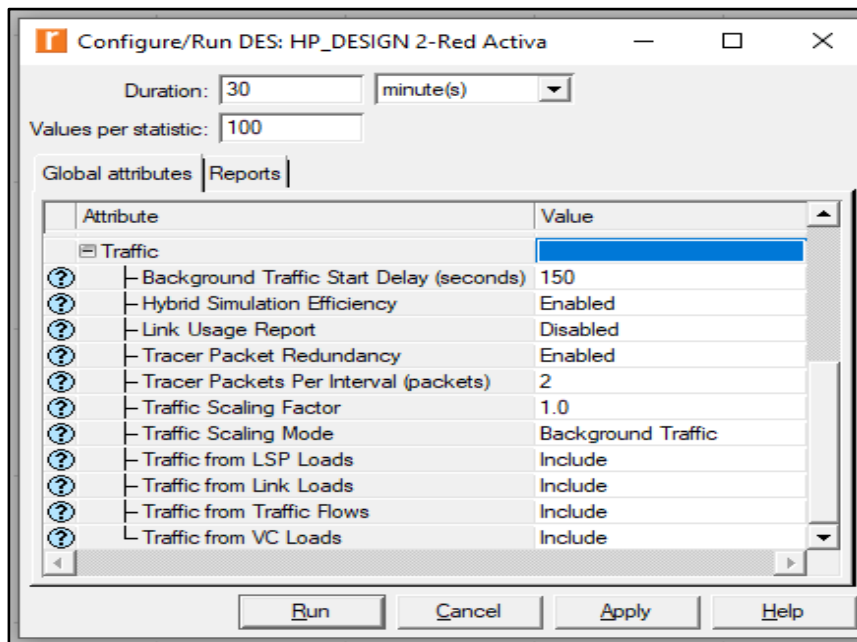


Figura N°10. Parámetros de la red

2.3.2.3 Validación de resultado

El software mide los eventos en un rango de 1 a 2 segundos con un uso de memoria de 40MB para la transferencia de paquetes por usuario, asimismo, se obtiene un balance óptimo de cargas en los enlaces de una red con diferentes tipos de tráfico en la red. La simulación se completa después de un periodo de 30 minutos, mostrando más de 10 000 000 eventos, los cuales son representando como envío de paquete de información, con una velocidad promedio de 2 425 866 eventos enviados por segundos de simulación, equivalente a 6 minutos en un caso real. Esto se visualiza en la Figura N°11.

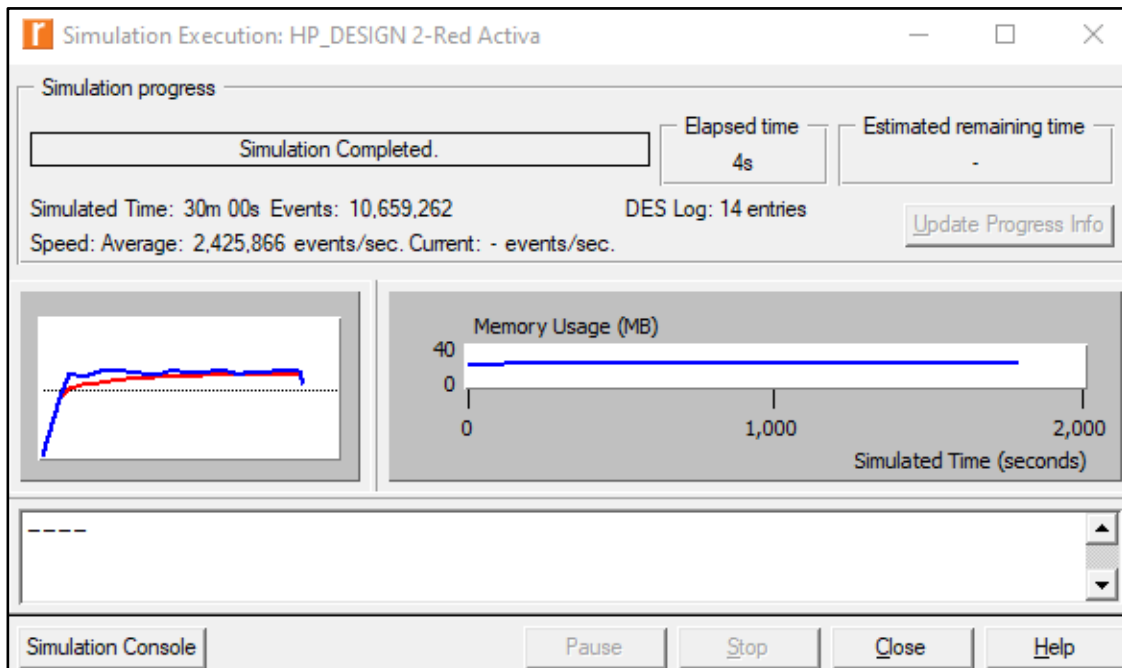


Figura N°11. Simulación completa en Riverbed Modeler

2.3.3 Modelo propuesto del diseño de la red LAN

Luego de validar el proceso óptimo de tráfico en la red, se diseña el modelo de la red LAN de alta disponibilidad, el cual muestra diferentes caminos que puede tomar una VLAN en caso de que ocurra una falla física o lógica en la red. En la Figura N°12 se visualiza el modelo propuesto para el diseño de la red LAN de alta disponibilidad.

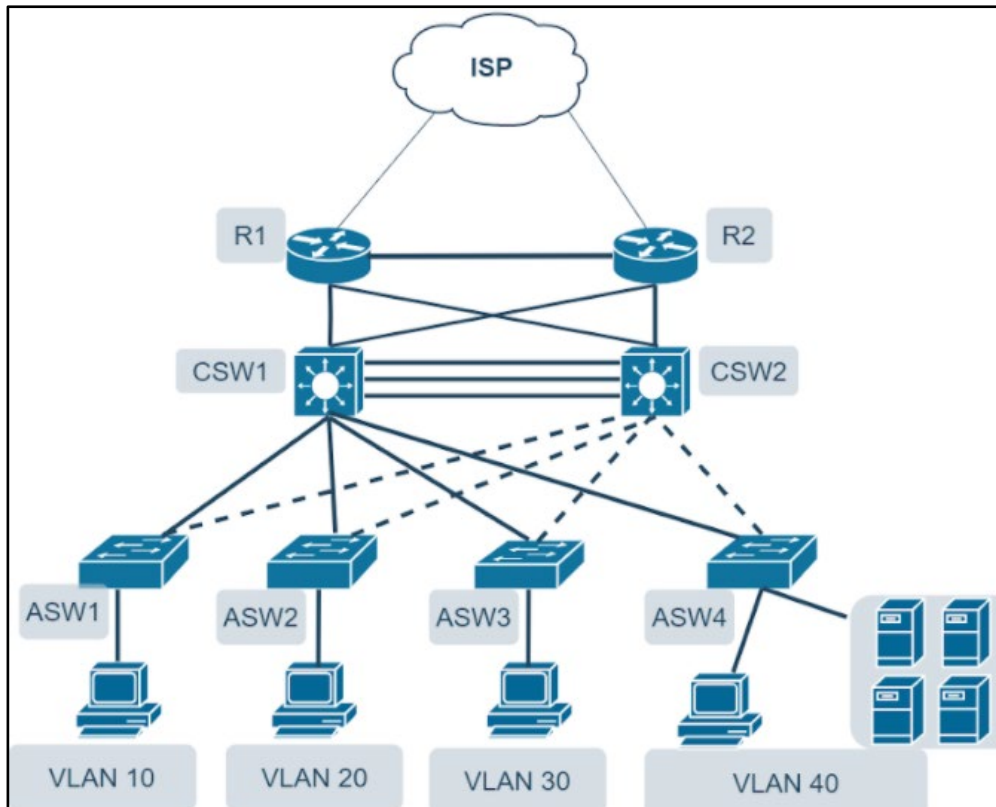


Figura N°12. Modelo de diseño de la red LAN de alta disponibilidad

De acuerdo con lo visualizado en la Figura N°12. Se desarrolla las características de los equipos en la Tabla N°18, relacionado a cada subred.

Equipos Cisco	Nombre	VLAN
Switch 1 Serie 2960 24P	ASW1	10
Switch 2 Serie 2960 24P	ASW2	20
Switch 3 Serie 2960 24P	ASW3	30
Switch 4 Serie 2960 24P	ASW4	40
Switch 1 Catalyst 3650 24P	CSW1	Todos
Switch 2 Catalyst 3650 24P	CSW2	Todos
Router 2 ISR 4331	R1	Todos
Router 1 ISR 4331	R2	Todos

Tabla N°18. Características de los equipos asociado a cada subred

2.3.4 Descripción de la topología a diseñar.

El diseño de la red LAN de alta disponibilidad se desarrolla en el software Packet Tracer versión 7.3.1, este programa es de propiedad de la empresa Cisco. Para el diseño se utiliza todos los protocolos de red necesarios que brinden una alta disponibilidad, asimismo, se ejecutan protocolos de seguridad a nivel de puertos y seguridad de gestión en dispositivos de manera remota, utilizando la autenticación, autorización y contabilidad de la red. Este apartado se basa en las buenas prácticas de la norma ISO/IEC 27002, en el dominio 13 que se visualizó previamente en la Tabla N°6, donde detalla la gestión de la continuidad del negocio, en los objetivos de control que refieren la continuidad de la seguridad de la información y redundancias (Alta disponibilidad de instalaciones de procesamiento). Es importante recalcar que la norma ISO/IEC 27002 tiene como principios la disponibilidad, la confiabilidad y la integridad de la información en cualquier organización que sea aplicado.

2.3.4.1 Proceso de configuración

Para el inicio de la configuración, en primer lugar, es necesario la cantidad de usuarios para crear las redes virtuales, el cual se detalla anteriormente en la Tabla N°13. Luego se asigna el enrutamiento entre subredes con los diferentes protocolos de alta disponibilidad para tener dispositivos de respaldo y diferentes enlaces redundantes, es decir, obtener otros caminos para la transmisión de paquetes de información para todas las subredes.

2.3.4.1.1 Creación de VLAN

La creación de subredes comienza con el nombramiento de cada una de ellas, el cual refieren cada área y las especificaciones que se tiene en la empresa, el cual se visualiza en la Tabla N°19.

VLAN	Nombre	Áreas y especificaciones
10	Logística	Área de Logística
20	ComProy	Área Comercial, Proyectos y RRHH
30	AdmGer	Área de Administración, Contabilidad y Gerencia
40	TI	Área de TI, servidores y otros dispositivos
90	Gestión	Gestión remota de los dispositivos

Tabla N°19. Asignación de VLAN para cada área de la empresa

El proceso de creación de VLAN se realiza en el primer switch de distribución de capa 3, nombrado como CSW1. Como se muestra en la Figura N°13.


```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname CSW1
CSW1(config)#exit
CSW1#vlan database
%SYS-5-CONFIG_I: Configured from console by console
CSW1(vlan)#vlan 10 name Logistica
VLAN 10 added:
Name: Logistica
CSW1(vlan)#vlan 20 name ComProy
VLAN 20 added:
Name: ComProy
CSW1(vlan)#vlan 30 name AdmGer
VLAN 30 added:
Name: AdmGer
CSW1(vlan)#vlan 40 name Tecnologia
VLAN 40 added:
Name: Tecnologia
CSW1(vlan)#vlan 90 name Gestion
VLAN 90 added:
Name: Gestion
CSW1(vlan)#exit

```

Figura N°13. Creación de VLAN en CSW1

2.3.4.1.2 Centralizar la administración de VLAN

Mediante la ejecución del protocolo VTP (Virtual Trunking Protocol), el cual ayuda a centralizar en un solo switch la administración de la red, asimismo, se comparte la VLAN a través de todos los switches del dominio. Es decir, se configura en CSW1 para mantener la conectividad entre todas las subredes, por ello ya no es necesario configurar la VLAN en el segundo switch de capa 3 denominado CSW2, sin embargo, se realiza el enrutamiento entre subredes ejecutando el comando "ip routing" más adelante cuando se asigne las direcciones IP. En la Figura N°14 se visualiza la configuración.

```

CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#vtp mode server
Device mode already VTP SERVER.
CSW1(config)#vtp domain sehover.com
Changing VTP domain name from NULL to sehover.com
CSW1(config)#vtp password LinuxSEH20*
Setting device VLAN database password to LinuxSEH20*
CSW1(config)#vtp version 2
CSW1(config)#exit

```

Figura N°14. Creación de VTP en CSW1

2.3.4.1.3 Configuración modo troncal y modo acceso

- Modo troncal en switches de capa 3: Se realiza la configuración de modo troncal en los dos switches de distribución, nombrados como CSW1 y CSW2 respectivamente. Se realiza la configuración modo troncal en las interfaces CSW1 conectados a los switches de acceso en las interfaces GigabitEthernet 1/0/1-4. Con el comando “switchport trunk encapsulation dot1q” se habilita la encapsulación en las interfaces de CSW1. En la Figura N°15 se visualiza la configuración.

```
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#interface GigabitEthernet 1/0/1
CSW1(config-if-range)#switchport trunk encapsulation dot1q
CSW1(config-if-range)#switchport mode trunk
CSW1(config-if-range)#switchport trunk allowed vlan 10,90
CSW1(config-if-range)#exit
CSW1(config)#interface GigabitEthernet 1/0/2
CSW1(config-if-range)#switchport trunk encapsulation dot1q
CSW1(config-if-range)#switchport mode trunk
CSW1(config-if-range)#switchport trunk allowed vlan 20,90
CSW1(config-if-range)#exit
CSW1(config)#interface GigabitEthernet 1/0/3
CSW1(config-if-range)#switchport trunk encapsulation dot1q
CSW1(config-if-range)#switchport mode trunk
CSW1(config-if-range)#switchport trunk allowed vlan 30,90
CSW1(config-if-range)#exit
CSW1(config)#interface GigabitEthernet 1/0/4
CSW1(config-if-range)#switchport trunk encapsulation dot1q
CSW1(config-if-range)#switchport mode trunk
CSW1(config-if-range)#switchport trunk allowed vlan 40,90
CSW1(config-if-range)#exit
```

Figura N°15. Configuración modo troncal en CSW1

- Modo troncal y acceso en switch de acceso: Se realiza la configuración en los switches de acceso, el primer switch de acceso es nombrado ASW1, donde las interfaces GigabitEthernet en el rango 0/1-2 están configurados en modo troncal, permitiendo el acceso de las VLAN 10 y 90. En el caso de las interfaces FastEthernet 0/1-24, están configurados en modo de acceso a la VLAN 10. En la Figura N°16 se visualiza la configuración.

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname ASW1
ASW1(config)#interface range GigabitEthernet 0/1-2
ASW1(config-if-range)#switchport mode trunk
ASW1(config-if-range)#switchport trunk allowed vlan 10,90
ASW1(config-if-range)#exit
ASW1(config)#interface range FastEthernet 0/1-24
ASW1(config-if-range)#switchport mode access
ASW1(config-if-range)#switchport access vlan 10
ASW1(config-if-range)#exit

```

Figura N°16. Configuración switch de acceso (ASW1)

2.3.4.1.4 Configuración de protocolo Spanning Tree

Se realiza la configuración del protocolo spanning tree en su versión “rapid per vlan spanning tree (rapid pvst)”, el cual rutea las subredes para que se capturen en un camino principal o secundario, de esta manera poder evitar bucles. En la Figura N°17 y Figura N°18 se visualiza la configuración para CSW1 y CSW2 respectivamente.

```

CSW1>enable
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#spanning-tree mode rapid-pvst
CSW1(config)#spanning-tree vlan 10,20,90 root primary
CSW1(config)#spanning-tree vlan 30,40 root secondary
CSW1(config)#exit

```

Figura N°17. Configuración de protocolo Spanning tree en CSW1

```

CSW2>enable
CSW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW2(config)#spanning-tree mode rapid-pvst
CSW2(config)#spanning-tree vlan 30,40 root primary
CSW2(config)#spanning-tree vlan 10,20,90 root secondary
CSW2(config)#exit

```

Figura N°18. Configuración de protocolo Spanning tree en CSW2

2.3.4.1.5 VLAN de gestión

Se realiza la configuración de una VLAN para la administración remota de los dispositivos de la red LAN, con la dirección IP 10.168.90.11/24 para el primer switch de acceso (ASW1) y con dirección de puerta de enlace 10.168.90.1. También se utiliza el rango de direcciones IP 10.168.90.12-16 para los demás dispositivos administrados como switch y router. Asimismo, se prosigue con las buenas prácticas de control de acceso según la norma ISO/IEC 27002. En la Figura N°19 se visualiza la configuración.

```
ASW1>enable
ASW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ASW1(config)#interface vlan 90
ASW1(config-if)#
%LINK-5-CHANGED: Interface Vlan90, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan90, changed state to up
ASW1(config-if)#ip address 10.168.90.11 255.255.255.0
ASW1(config-if)#ip default-gateway 10.168.90.1
ASW1(config)#exit
```

Figura N°19. Creación de VLAN de gestión en ASW1

2.3.4.1.6 Configuración del protocolo Spanning Tree para dispositivos finales

Se realiza la configuración del protocolo spanning tree ejecutando el comando “portfast” en el rango de interfaces FastEthernet 0/1-24, asimismo, se ejecuta el comando “bpdguard” para que no exista cambios en la red debido a los paquetes que son enviados por este protocolo, cabe recalcar que este comando solo se utiliza en dispositivos finales como: ordenadores, impresoras, servidores, entre otros. En la Figura N°20 se visualiza la configuración.

```
ASW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ASW1(config)#interface range FastEthernet 0/1-24
ASW1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
ASW1(config-if-range)#spanning-tree bpdguard enable
ASW1(config-if-range)#exit
```

Figura N°20. Protocolo Spanning Tree para dispositivos finales

2.3.4.1.7 Configuración Etherchannel

La configuración entre los switches de capa 3, nombrados como CSW1 y CSW2 respectivamente, están conectados entre las interfaces GigabitEthernet en el rango 1/0/22-24 y el modo de encapsulación esta con el parámetro “dot1q”, el cual se referencia en la norma IEEE802.1q. La configuración de la tecnología Etherchannel se realiza en su versión del protocolo LACP, este protocolo cuenta con modo activo y pasivo. Donde se configura un grupo de canales entre CSW1 y CSW2 en los cuales existen tres enlaces físicos y funcionan como un solo enlace lógico, es decir, este protocolo ayuda a incrementar el ancho de banda del enlace. Asimismo, se basa en el estándar IEEE 802.3ad, el cual permite establecer enlaces troncales entre dispositivos de los diferentes proveedores. En la Figura N°21 se visualiza la configuración.

```
CSW1>enable
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#interface range GigabitEthernet 1/0/22-24
CSW1(config-if-range)#channel-protocol lacp
CSW1(config-if-range)#channel-group 1 mode active
CSW1(config-if-range)#
Creating a port-channel interface Port-channel 1
CSW1(config)#interface port-channel 1
CSW1(config-if)#switchport trunk encapsulation dot1q
CSW1(config-if)#switchport mode trunk
CSW1(config-if)#switchport nonegotiate
CSW1(config-if)#switchport trunk allowed vlan 10,20,30,40,90
CSW1(config-if)#exit
```

Figura N°21. Configuración LACP en CSW1

2.3.4.1.8 Configuración del protocolo HSRP

Los Switches de capa 3 serán configurados como dispositivos de redundancia, es decir, un dispositivo funcionará como principal y el otro de contingencia para cada subred. De esta manera, aprovechar los recursos de ambos equipos donde se realiza el balanceo de cargas, configurando un dispositivo primario para cierta cantidad de subredes y otro dispositivo como secundario para el resto de las subredes. Para realizar la configuración del protocolo HSRP es necesario crear una dirección IP activa y de respaldo, para poder asignar a cada switch de distribución, los cuales el primer switch de capa 3, nombrado como CSW1, funciona como principal para algunas subredes y el segundo switch de capa 3, nombrado como CSW2, funciona como un dispositivo de respaldo para algunas subredes. En la Tabla N°20 se detalla cada dirección IP activa y de respaldo. Asimismo, en la Tabla N°21 se visualiza las subredes que serán asignadas como activa y respaldo para CSW1 y CSW2 respectivamente.

VLAN	IP VIRTUAL	IP ACTIVO	IP RESPALDO
10	10.168.10.1	10.168.10.2	10.168.10.3
20	10.168.20.1	10.168.20.2	10.168.20.3
30	10.168.30.1	10.168.30.3	10.168.30.2
40	10.168.40.1	10.168.40.3	10.168.40.2

Tabla N°20. Dirección IP para cada subred en CSW1 y CSW2

VLAN	CSW1	CSW2
10	Activo	Respaldo
20	Activo	Respaldo
30	Respaldo	Activo
40	Respaldo	Activo

Tabla N°21. Asignación de subred en modo activo y respaldo para CSW1 y CSW2

- Asignación IP para cada subred en CSW1: Se realiza la configuración para la asignación de direcciones IP en las diferentes interfaces para la comunicación entre cada subred, asimismo, con el comando “no shutdown”, se activan los puertos para su uso. En la Figura N°22 se visualiza la configuración.

```

CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#interface vlan 10
CSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
CSW1(config-if)#ip address 10.168.10.2 255.255.255.0
CSW1(config-if)#no shutdown
CSW1(config-if)#exit
CSW1(config)#interface vlan 20
CSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
CSW1(config-if)#ip address 10.168.20.2 255.255.255.0
CSW1(config-if)#no shutdown
CSW1(config-if)#exit
CSW1(config)#interface vlan 30
CSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
CSW1(config-if)#ip address 10.168.30.2 255.255.255.0
CSW1(config-if)#no shutdown
CSW1(config-if)#exit
CSW1(config)#interface vlan 40
CSW1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up
CSW1(config-if)#ip address 10.168.40.2 255.255.255.0
CSW1(config-if)#no shutdown
CSW1(config-if)#exit
CSW1(config)#ip routing
CSW1(config)#

```

Figura N°22. Asignación de dirección IP para cada VLAN en CSW1

- Asignación IP para cada subred en CSW2:

```

CSW2>enable
CSW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW2(config)#ip routing
CSW2(config)#interface vlan 10
CSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
CSW2(config-if)#ip address 10.168.10.3 255.255.255.0
CSW2(config-if)#no shutdown
CSW2(config-if)#exit
CSW2(config)#interface vlan 20
CSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
CSW2(config-if)#ip address 10.168.20.3 255.255.255.0
CSW2(config-if)#no shutdown
CSW2(config-if)#exit
CSW2(config)#interface vlan 30
CSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
CSW2(config-if)#ip address 10.168.30.3 255.255.255.0
CSW2(config-if)#no shutdown
CSW2(config-if)#exit
CSW2(config)#interface vlan 40
CSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up
CSW2(config-if)#ip address 10.168.40.3 255.255.255.0
CSW2(config-if)#no shutdown
CSW2(config-if)#exit
CSW2(config)#

```

Figura N°23. Asignación de dirección IP para cada VLAN en CSW2

- HSRP en CSW1: Se realiza la configuración del protocolo HSRP en CSW1, el cual permite el despliegue de enrutadores tolerantes de fallos en una red. Este protocolo tiene dos modos de operación el cual es el modo “activo” y el modo “standby”. Donde uno cumple la función de dispositivo principal de acuerdo con la prioridad que sea asignada. En este despliegue se asigna direcciones IP virtuales para la interfaz de las subredes, dando una prioridad de 200 para colocar en modo activo al CSW1, debido a que la prioridad por defecto es de 100. Luego el comando “standby track” es utilizado de seguimiento en espera para permitir especificar otra interfaz en el enrutador, el cual el protocolo HSRP tenga un monitoreo con el fin de alterar la prioridad para un grupo dado. En la Figura N°24 se visualiza la configuración.

```

CSW1>enable
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#interface vlan 10
CSW1(config-if)#standby 10 ip 10.168.10.1
CSW1(config-if)#standby 10 priority 200
CSW1(config-if)#standby 10 preempt
CSW1(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
CSW1(config-if)#standby 10 track GigabitEthernet 1/0/1
CSW1(config-if)#standby 10 track GigabitEthernet 1/0/22
CSW1(config-if)#standby 10 track GigabitEthernet 1/0/23
CSW1(config-if)#standby 10 track GigabitEthernet 1/0/24
CSW1(config-if)#exit

```

Figura N°24. Protocolo HSRP en CSW1

- HSRP en CSW2:

```

CSW2>enable
CSW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW2(config)#interface vlan 10
CSW2(config-if)#standby 10 ip 10.168.10.1
CSW2(config-if)#standby 10 priority 100
CSW2(config-if)#standby 10 preempt
CSW2(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
CSW2(config-if)#standby 10 track GigabitEthernet 1/0/1
CSW2(config-if)#standby 10 track GigabitEthernet 1/0/22
CSW2(config-if)#standby 10 track GigabitEthernet 1/0/23
CSW2(config-if)#standby 10 track GigabitEthernet 1/0/24
CSW2(config-if)#exit

```

Figura N°25. Protocolo HSRP en CSW2

2.3.4.1.9 Asignación de dirección IP en CSW1 para enrutamiento

Se realiza la asignación de dirección IP a cada interfaz Gigabit Ethernet de CSW1 y CSW2 para realizar el proceso de enrutamiento. Habilitando los puertos con el comando “shutdown”, asimismo se realiza la configuración en las interfaces que conectan CSW1 con los routers R1 y R2, asignando dirección IP de 10.0.0.1/30 y 12.0.0.1/30 respectivamente. En CSW1 se ejecuta el comando “no switchport” para que funcione como switch de capa 3. En la Tabla N°22 se visualiza las direcciones asignadas y en la Figura N°26 se visualiza la configuración para CSW1.

Enrutamiento	Subred	Interfaz	Dirección IP
CSW1-R1	10.0.0.0/30	Gigabit Ethernet 1/0/10	10.0.0.1
CSW1-R2	12.0.0.0/30	Gigabit Ethernet 1/0/11	12.0.0.1
CSW2-R1	12.0.0.4/30	Gigabit Ethernet 1/0/11	12.0.0.5
CSW2-R2	10.0.0.4/30	Gigabit Ethernet 1/0/10	10.0.0.5

Tabla N°22. Asignación de dirección IP en CSW1 y CSW2 para enrutamiento

```
CSW1>enable
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#interface GigabitEthernet 1/0/10
CSW1(config-if)#no switchport
CSW1(config-if)#ip address 10.0.0.1 255.255.255.252
CSW1(config-if)#no shutdown
CSW1(config-if)#exit
CSW1(config)#interface GigabitEthernet 1/0/11
CSW1(config-if)#no switchport
CSW1(config-if)#ip address 12.0.0.1 255.255.255.252
CSW1(config-if)#no shutdown
CSW1(config-if)#exit
```

Figura N°26. Configuración de CSW1 hacia R1 y R2

2.3.4.1.10 Asignación de dirección IP en R1 para enrutamiento

Se realiza la asignación de dirección IP a cada interfaz Gigabit Ethernet e interfaz serial respectivamente para realizar el proceso de enrutamiento. Habilitando los puertos con el comando “shutdown”, asimismo para la Interfaz serial se ejecuta el comando “clock rate” para realizar el proceso de sincronización de la conexión en serie con una velocidad de envío de datos de 100 000 bits por segundo. En la Tabla N°23 se visualiza las direcciones asignadas, asimismo en la Figura N°27 se visualiza la configuración para R1.

Enrutamiento	Subred	Interfaz	Dirección IP
R1 - CSW1	10.0.0.0/30	Gigabit Ethernet 0/0/0	10.0.0.2
R1 - CSW2	12.0.0.4/30	Gigabit Ethernet 0/0/1	12.0.0.6
R2 - CSW1	12.0.0.0/30	Gigabit Ethernet 0/0/1	12.0.0.2
R2 - CSW2	10.0.0.4/30	Gigabit Ethernet 0/0/0	10.0.0.6
R1 - ISP	11.0.0.0/30	Serial 0/1/0	11.0.0.1
R2 - ISP	11.0.0.4/30	Serial 0/1/0	11.0.0.5
R1 - R2	11.0.0.8/30	Serial 0/1/1	11.0.0.9
R2 - R1	11.0.0.8/30	Serial 0/1/1	11.0.0.10

Tabla N°23. Asignación de dirección IP en R1 y R2 para enrutamiento

```

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface GigabitEthernet 0/0/0
R1(config-if)#ip address 10.0.0.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface GigabitEthernet 0/0/1
R1(config-if)#ip address 12.0.0.6 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Serial 0/1/0
R1(config-if)#ip address 11.0.0.1 255.255.255.252
R1(config-if)#clock rate 1000000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Serial 0/1/1
R1(config-if)#ip address 11.0.0.9 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit

```

Figura N°27. Asignación de dirección IP en R1

2.3.4.1.11 Configuración del protocolo EIGRP

- Protocolo EIGRP en CSW1: Se realiza la configuración del protocolo EIGRP en el primer switch de distribución, denominado CSW1, se ejecuta el comando "router eigrp 1" y el comando "network" con la wildcard de cada subred, esto para poder encontrar "vecinos" en otras rutas de acceso, de esta manera se logra el enrutamiento dinámico entre dispositivos. Luego se ejecuta el comando "passive-interface (Nombre de interfaz)" para ahorrar ancho de banda, porque permite indicarle al router que por la interfaz (Nombre de interfaz) no envíe actualizaciones de su tabla de enrutamiento

EIGRP, tampoco emitir los mensajes. La ejecución de este comando es recomendada para interfaces conectados a dispositivos no enrutadores. En la Figura N°28 se visualiza la configuración

```
CSW1>enable
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#router eigrp 1
CSW1(config-router)#no auto-summary
CSW1(config-router)#network 10.0.0.0 0.0.0.3
CSW1(config-router)#network 12.0.0.0 0.0.0.3
CSW1(config-router)#network 10.168.90.0 0.0.0.255
CSW1(config-router)#passive-interface GigabitEthernet 1/0/1
CSW1(config-router)#passive-interface GigabitEthernet 1/0/2
CSW1(config-router)#passive-interface GigabitEthernet 1/0/3
CSW1(config-router)#passive-interface GigabitEthernet 1/0/4
CSW1(config-router)#passive-interface GigabitEthernet 1/0/22
CSW1(config-router)#passive-interface GigabitEthernet 1/0/23
CSW1(config-router)#passive-interface GigabitEthernet 1/0/24
CSW1(config-router)#exit
```

Figura N°28. Configuración del protocolo EIGRP en CSW1

- Protocolo EIGRP en R1: El protocolo EIGRP proporciona un sistema para equilibrar la carga sobre rutas de costos desiguales a través del comando “variance”, el cual va en un rango de número de 1 a 128, donde incluye las rutas con diferentes métricas. El valor de variación predeterminado es 1, el cual es utilizado para el equilibrio de carga de igual costo. Asimismo, se ejecuta el comando “network” con la wildcard de cada subred, esto para poder encontrar “vecinos” en otras rutas de acceso. De esta manera poder realizar un enrutamiento entre routers y switch de capa 3. En la Figura N°29 se visualiza la configuración.

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-if)#no auto-summary
R1(config-if)#variance 10
R1(config-if)#network 10.0.0.0 0.0.0.3
R1(config-if)#network 11.0.0.0 0.0.0.3
R1(config-if)#network 11.0.0.8 0.0.0.3
R1(config-if)#network 12.0.0.4 0.0.0.3
R1(config-if)#exit
```

Figura N°29. Configuración del protocolo EIGRP en R1

- El comando “no auto-summary” indica al router que no realice un resumen de las subredes que tiene asignada, porque creara una confusión en la red. El comando “variance” es un multiplicador que permite utilizar dos o más rutas para balancear carga hacia un mismo destino. La única condición será que estas rutas sean sucesores factibles, en caso contrario, EIGRP no las utilizará para el balanceo de cargas.

2.4.4.2 Puerto seguro en los dispositivos

Se realiza la configuración de puerto seguro en las interfaces que utiliza los dispositivos de la red, tanto switch como router. En las interfaces de modo acceso y modo troncal se ejecuta el comando “maximun” y se elige el valor 1 para que solo un dispositivo en esa interfaz se conecte y se ejecuta el comando “mac-address sticky”, el cual guarda la dirección MAC del dispositivo que se ha conectado, en este escenario para el switch de acceso 1 denominado como ASW1. Asimismo, en caso de que otro dispositivo se conecte a la interfaz del switch, no podrá acceder ya que inmediatamente se apagará la interfaz porque está ejecutando el comando “violation shutdown”. Esta configuración se visualiza en la Figura N°30.

```
ASW1#configure terminal
ASW1(config)#interface range FastEthernet 0/1-24
ASW1(config-if-range)#switchport mode access
ASW1(config-if-range)#switchport port-security
ASW1(config-if-range)#switchport port-security maximun 1
ASW1(config-if-range)#switchport port-security violation shutdown
ASW1(config-if-range)#switchport port-security mac-address sticky
ASW1(config-if-range)#exit
ASW1(config)#interface range GigabitEthernet 0/1-2
ASW1(config-if-range)#switchport mode trunk
ASW1(config-if-range)#switchport port-security
ASW1(config-if-range)#switchport port-security maximun 1
ASW1(config-if-range)#switchport port-security violation shutdown
ASW1(config-if-range)#switchport port-security mac-address sticky
ASW1(config-if-range)#exit
```

Figura N°30. Configuración de puerto seguro en ASW1

2.3.4.3 Configuración del protocolo SSH y AAA

Para realizar la configuración del protocolo SSH es necesario asignar un nombre de dominio y un nombre de host, ingresando a la configuración global, se ejecuta el comando “hostname” seguido del nombre que se asigna al dispositivo. Asimismo, se crean claves cifradas rsa (sistema criptográfico de clave pública), el cual se elige el valor 1024 para tener un alto grado de seguridad y poder generar la llave de forma rápida. En la Figura N°31 se visualiza el primer switch de capa 3, denominado como CSW1, el cual se toma como ejemplo para realizar el proceso de configuración del protocolo SSH en la versión 2 al ingresar con un usuario y contraseña.

```

CSW1>enable
CSW1#configure terminal
CSW1(config)#ip domain name sehover.com
CSW1(config)#crypto key generate rsa
The name for the keys will be: CSW1.sehover.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
CSW1(config)#ip ssh version 2
CSW1(config)#ip ssh time-out 30
CSW1(config)#ip ssh authentication-retries 2
CSW1(config)#aaa new-model
CSW1(config)#aaa authentication login adminremota group tacacs+ local enable
CSW1(config)#tacacs-server host 10.168.40.100 key adm$3H20*
CSW1(config)#line vty 0 15
CSW1(config-line)#transport input ssh
CSW1(config-line)#login authentication adminremota
CSW1(config-line)#exit
CSW1(config)#username userseho privilege 15 secret +LinuxS3H20*
CSW1(config)#enable secret *+S3h0v3R*+
CSW1(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO SOLO PERSONAL AUTORIZADO #
CSW1(config)#exit

```

Figura N°31. Configuración del protocolo SSH y AAA

Como se observa en la Figura N°30, se ha configurado el protocolo AAA, asignando un grupo con el nombre “adminremota” usando la configuración TACACS+, asimismo en el grupo se encuentra la configuración local de usuario para ser utilizado en caso de que hubiera una falla en el servidor AAA. El usuario que desea acceder a un determinado dispositivo de administración de la red tendrá 30 segundos y 2 intentos para ingresar las credenciales, de lo contrario perderá conexión con el dispositivo al que acceda.

2.4 Resultados

Los resultados se obtienen mediante simulación en el software Packet Tracer versión 7.3.1, donde se muestra rutas alternas en caso de que ocurra una falla física o lógica en la red LAN de alta disponibilidad. A cada equipo e interfaz se asigna una dirección IP para la comunicación entre usuarios con salida al servidor web y DNS. El router ISP simula el servicio de internet mediante la dirección IP 181.177.240.114/24. Este proveedor de internet en la actualidad cuenta con un servicio de firewall virtual, no obstante, es administrado por el personal de TI para las creaciones de diferentes políticas de seguridad de la información. En la Figura N°32 se visualiza la red LAN de alta disponibilidad.

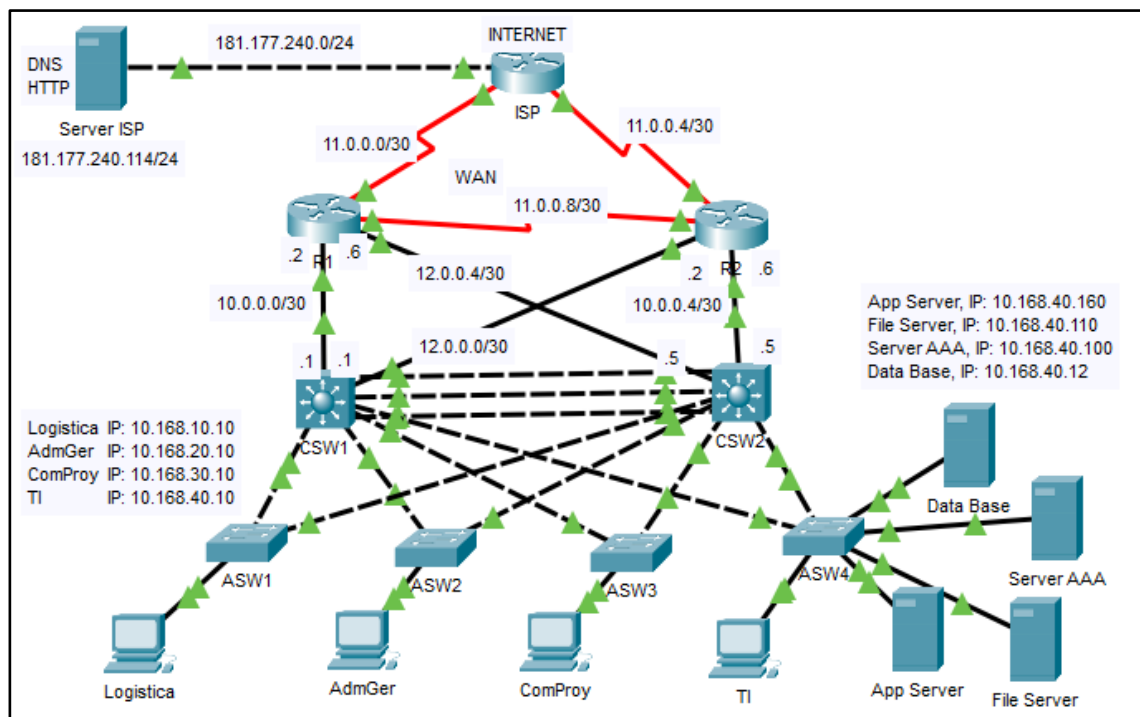


Figura N°32. Simulación de la red LAN de alta disponibilidad

- **Conexión entre subredes:** Para validar los resultados obtenidos, se realiza la comunicación entre VLAN, donde se ejecuta el comando “ping” desde el ordenador Logística hacia todas las subredes que existe. En la Figura N°33 se visualiza la comunicación hacia la VLAN 10 y VLAN 20. Asimismo, en la Figura N°34 se visualiza la comunicación hacia VLAN 30 y VLAN 40. El resultado confirma que los cuatro paquetes enviados de tamaño 32 bytes llegaron a las subredes y regresaron correctamente al ordenador con un tiempo máximo de 1ms. El periodo de validez indicado como TTL=255 corresponde al tiempo de expiración de un paquete de datos, siendo este su valor máximo.

```
Logistica
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.168.10.1

Pinging 10.168.10.1 with 32 bytes of data:

Reply from 10.168.10.1: bytes=32 time<1ms TTL=255
Reply from 10.168.10.1: bytes=32 time<1ms TTL=255
Reply from 10.168.10.1: bytes=32 time<1ms TTL=255
Reply from 10.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.168.20.1

Pinging 10.168.20.1 with 32 bytes of data:

Reply from 10.168.20.1: bytes=32 time<1ms TTL=255
Reply from 10.168.20.1: bytes=32 time<1ms TTL=255
Reply from 10.168.20.1: bytes=32 time<1ms TTL=255
Reply from 10.168.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura N°33. Ping desde ordenador Logística hacia VLAN 10 y VLAN 20

```
Logistica
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.168.30.1

Pinging 10.168.30.1 with 32 bytes of data:

Reply from 10.168.30.1: bytes=32 time<1ms TTL=255
Reply from 10.168.30.1: bytes=32 time<1ms TTL=255
Reply from 10.168.30.1: bytes=32 time<1ms TTL=255
Reply from 10.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.168.40.1

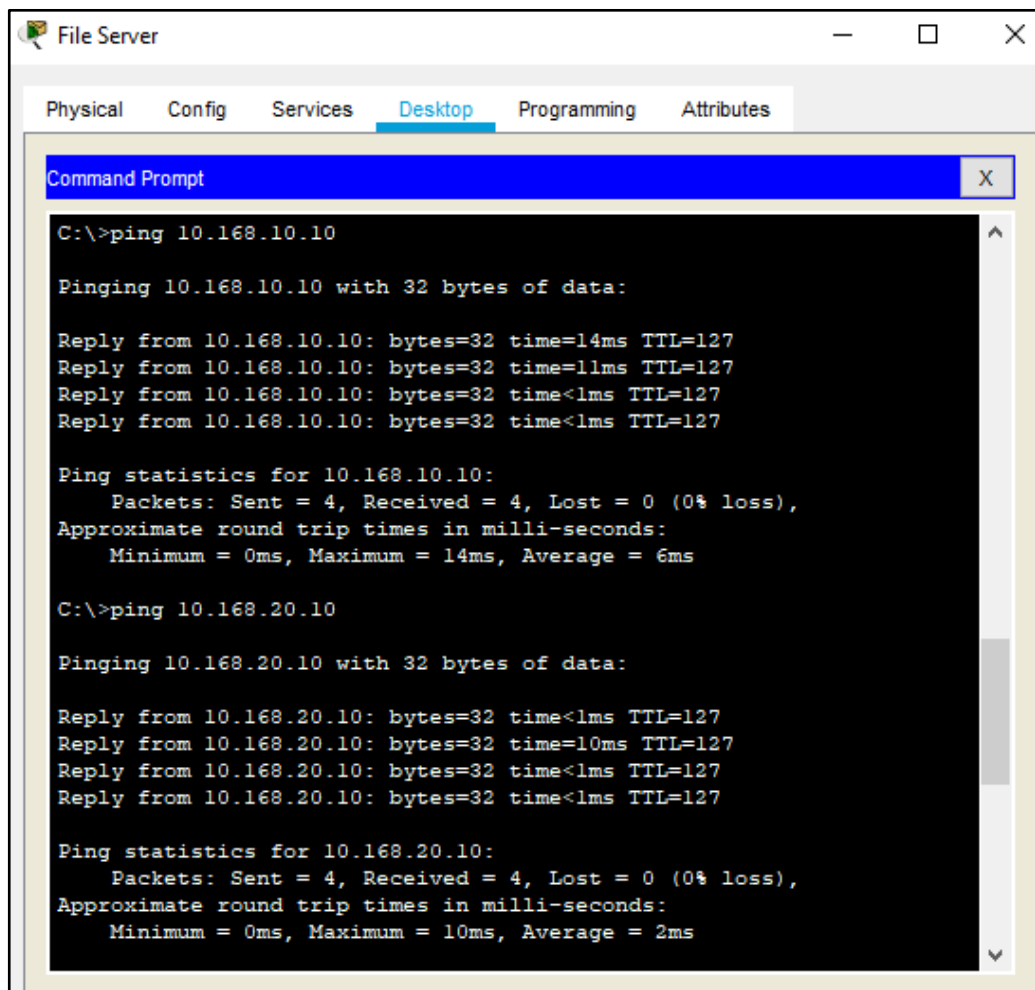
Pinging 10.168.40.1 with 32 bytes of data:

Reply from 10.168.40.1: bytes=32 time<1ms TTL=255
Reply from 10.168.40.1: bytes=32 time<1ms TTL=255
Reply from 10.168.40.1: bytes=32 time<1ms TTL=255
Reply from 10.168.40.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura N°34. Ping desde ordenador Logística hacia VLAN 30 y VLAN 40

- **Conexión con los servidores de la red:** Desde la VLAN 40 que representa el área de TI y los servidores, se ejecuta un “ping” desde el servidor de archivos hacia todos los ordenadores mostrados anteriormente en la Figura N°31. El resultado confirma que los cuatro paquetes enviados de tamaño 32 bytes llegaron a todos los ordenadores y regresaron correctamente al servidor con un tiempo máximo de 14ms. El periodo de validez indicado como TTL=127 corresponde a que el paquete a realizado el salto por un solo host, a diferencia de TTL=128 que corresponde a la misma subred donde se envía los paquetes y no hay ninguna perdida de paquete. El resultado se visualiza en la Figura N°35 y Figura N°36 respectivamente.



```
File Server
Physical Config Services Desktop Programming Attributes
Command Prompt
C:\>ping 10.168.10.10
Pinging 10.168.10.10 with 32 bytes of data:
Reply from 10.168.10.10: bytes=32 time=14ms TTL=127
Reply from 10.168.10.10: bytes=32 time=11ms TTL=127
Reply from 10.168.10.10: bytes=32 time<1ms TTL=127
Reply from 10.168.10.10: bytes=32 time<1ms TTL=127
Ping statistics for 10.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 6ms
C:\>ping 10.168.20.10
Pinging 10.168.20.10 with 32 bytes of data:
Reply from 10.168.20.10: bytes=32 time<1ms TTL=127
Reply from 10.168.20.10: bytes=32 time=10ms TTL=127
Reply from 10.168.20.10: bytes=32 time<1ms TTL=127
Reply from 10.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 10.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Figura N°35. Ping desde File Server hacia ordenadores Logística y AdmGer

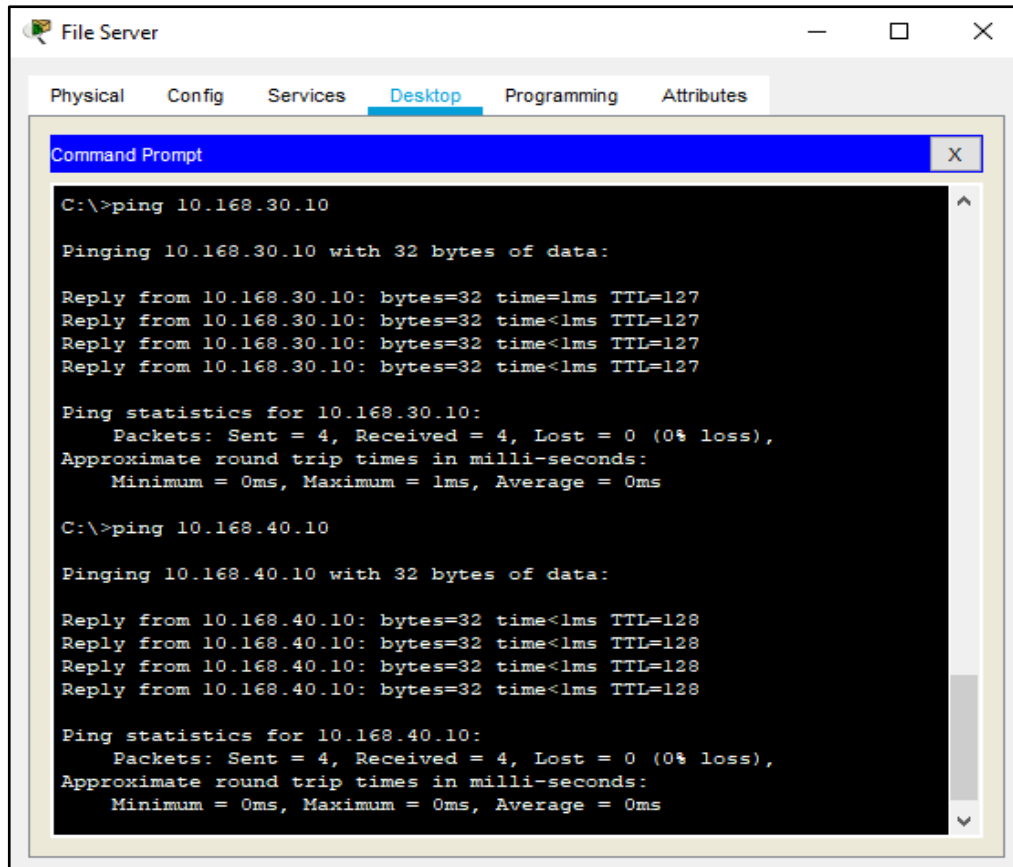


Figura N°36. Ping desde File Server hacia ordenadores ComProy y TI

- **Conexión a servidor ISP (Internet):** Desde los ordenadores Logística, AdmGer, ComProy y TI que se encuentran en las VLAN 10, 20, 30, y 40 respectivamente, se ejecuta un “ping” hacia el servidor ISP, el cual representa la salida a internet. El resultado confirma que los cuatros paquetes enviados de tamaño 32 bytes llegaron a todos los ordenadores y regresaron correctamente al servidor con un tiempo máximo de 10ms. El periodo de validez indicado como TTL=125 corresponde a que el paquete a realizado el salto por tres host y no hay ninguna perdida de paquete adicional. Estos resultados se visualizan en la Figura N°37, Figura N°38, Figura N°39 y Figura N°40 respectivamente para cada subred.

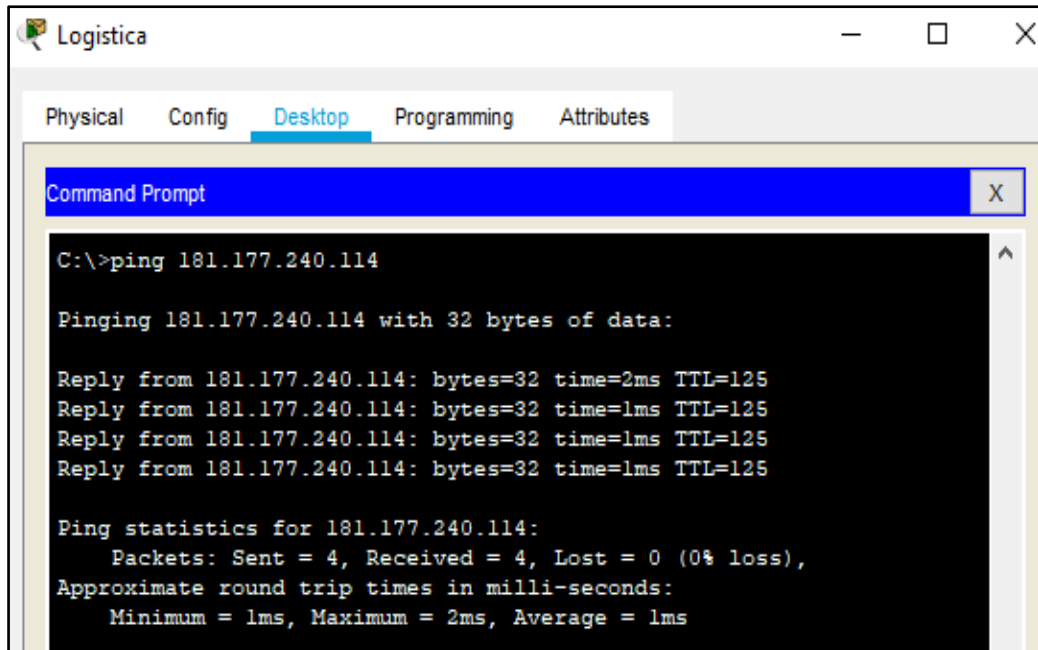


Figura N°37. Ping desde ordenador Logística a servidor ISP (Internet)

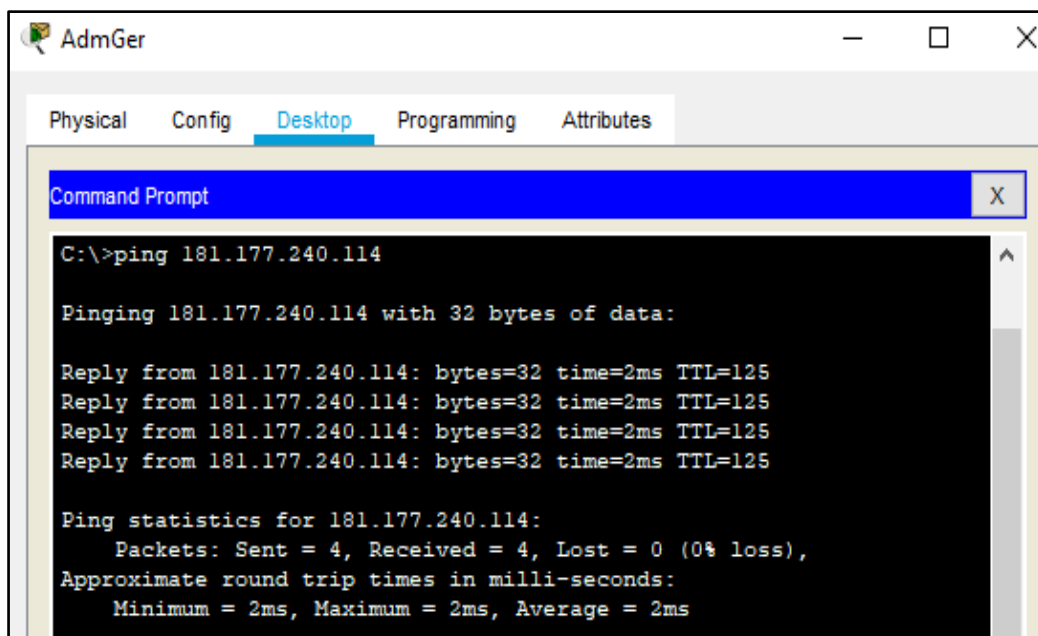


Figura N°38. Ping desde ordenador AdmGer a servidor ISP (Internet)

```
ComProy
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 181.177.240.114

Pinging 181.177.240.114 with 32 bytes of data:

Reply from 181.177.240.114: bytes=32 time=1ms TTL=125
Reply from 181.177.240.114: bytes=32 time=1ms TTL=125
Reply from 181.177.240.114: bytes=32 time=1ms TTL=125
Reply from 181.177.240.114: bytes=32 time=2ms TTL=125

Ping statistics for 181.177.240.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Figura N°39. Ping desde ordenador ComProy a servidor ISP (Internet)

```
TI
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 181.177.240.114

Pinging 181.177.240.114 with 32 bytes of data:

Reply from 181.177.240.114: bytes=32 time=1ms TTL=125
Reply from 181.177.240.114: bytes=32 time=10ms TTL=125
Reply from 181.177.240.114: bytes=32 time=1ms TTL=125
Reply from 181.177.240.114: bytes=32 time=1ms TTL=125

Ping statistics for 181.177.240.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms
```

Figura N°40. Ping desde ordenador TI a servidor ISP (Internet)

- **Resultado de la red LAN de alta disponibilidad ante falla en interfaz:** Se realiza un envío de paquetes mediante el comando “ping” hacia internet el cual tiene la dirección IP 181.177.240.114/24, asimismo, se desconecta la interfaz entre ASW1 y CSW1, simulando que ha ocurrido una falla en dicho enlace para validar el resultado exitoso del protocolo HSRP, es decir, se realiza él envío de ocho paquetes de prueba hacia internet y luego se desconecta la interfaz entre ASW1 y CSW1 verificando que pierde la conexión de cinco paquetes, sin embargo, la red detecta esta falla y elige otra ruta dirigida a CSW2 para tener salida a internet, dando como resultado la reactivación rápida del servicio . Este proceso se visualiza en la Figura N°41, de igual manera en la Figura N°42 se visualiza la ruta de respaldo dirigida a CSW2.

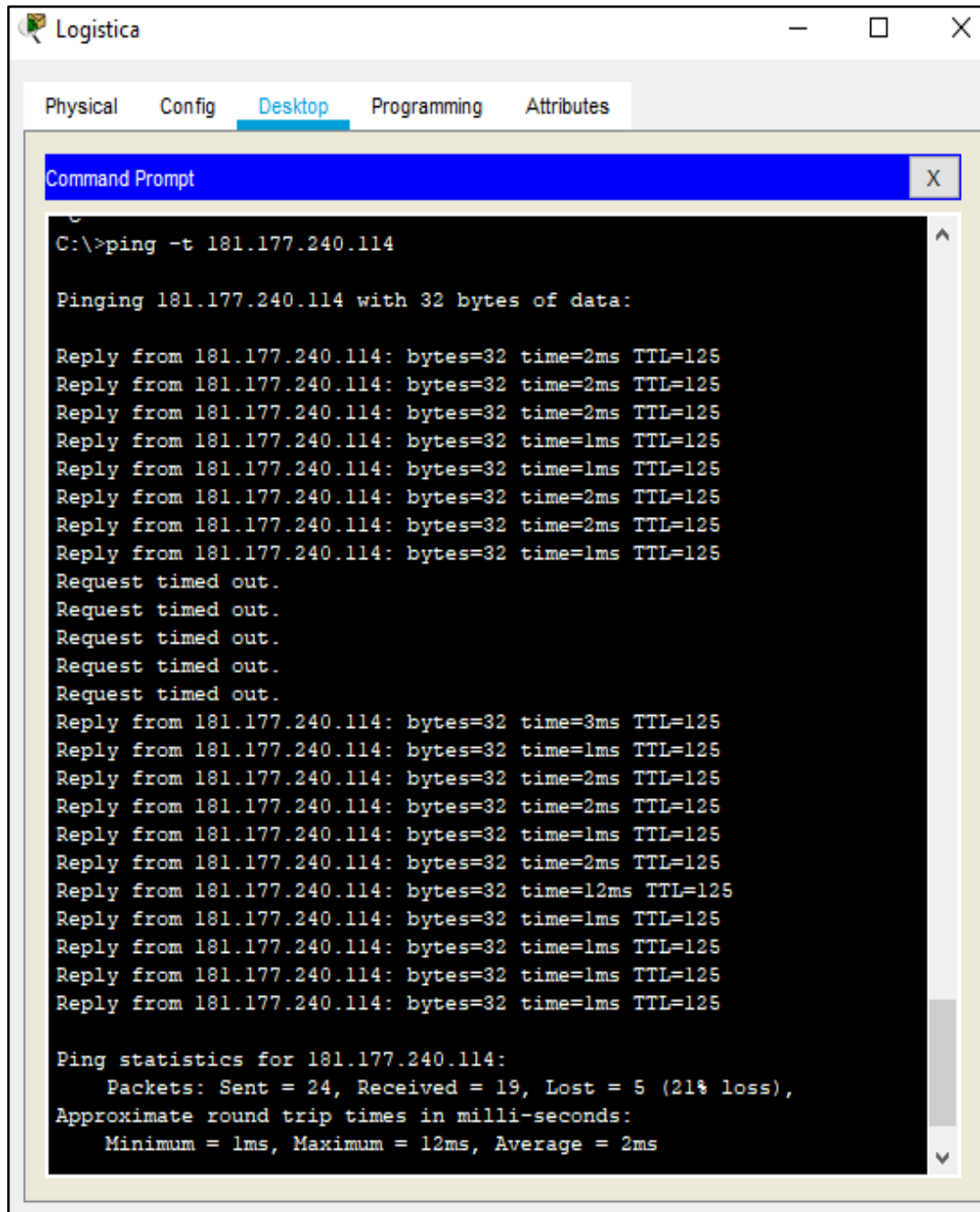


Figura N°41. Ping desde ordenador Logística hacia internet simulando una falla física en la interfaz conectada entre ASW1 y CSW1

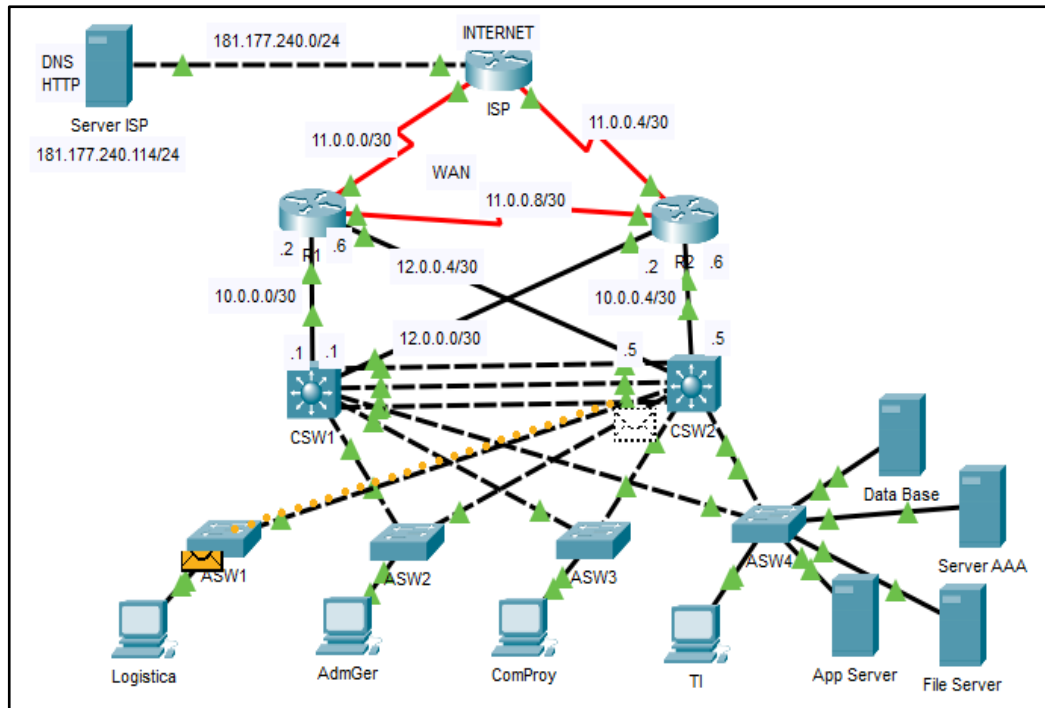


Figura N°42. Ruta de respaldo desde ordenador Logística a CSW2

- Resultado de red de alta disponibilidad ante falla de un dispositivo:** Se realiza un envío de paquetes mediante el comando “ping” hacia internet el cual tiene la dirección IP 181.177.240.114/24, asimismo, se desconecta CSW1, simulando que ha ocurrido una falla en dicho dispositivo para validar la red LAN de alta disponibilidad, es decir, se realiza el envío de ocho paquetes de prueba hacia internet y luego se desconecta CSW1, verificando que pierde la conexión de cinco paquetes, sin embargo, la red detecta esta falla y elige otras rutas dirigidas a CSW2 para tener salida a internet, dando como resultado la reactivación rápida del servicio . Este proceso se visualiza en la Figura N°43 y de igual manera en la Figura N°44 se visualiza las rutas de respaldo dirigidas a CSW2.

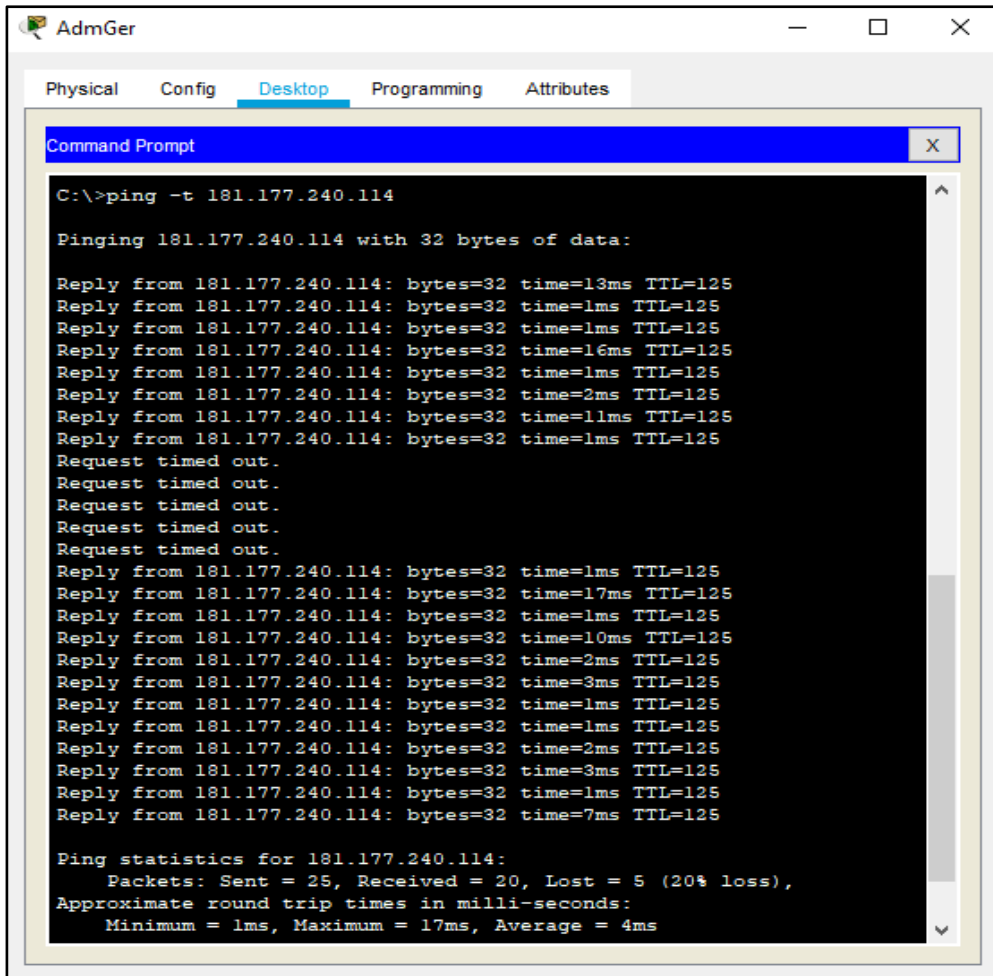


Figura N°43. Ping desde ordenador AdmGer hacia internet simulando una falla física en CSW1

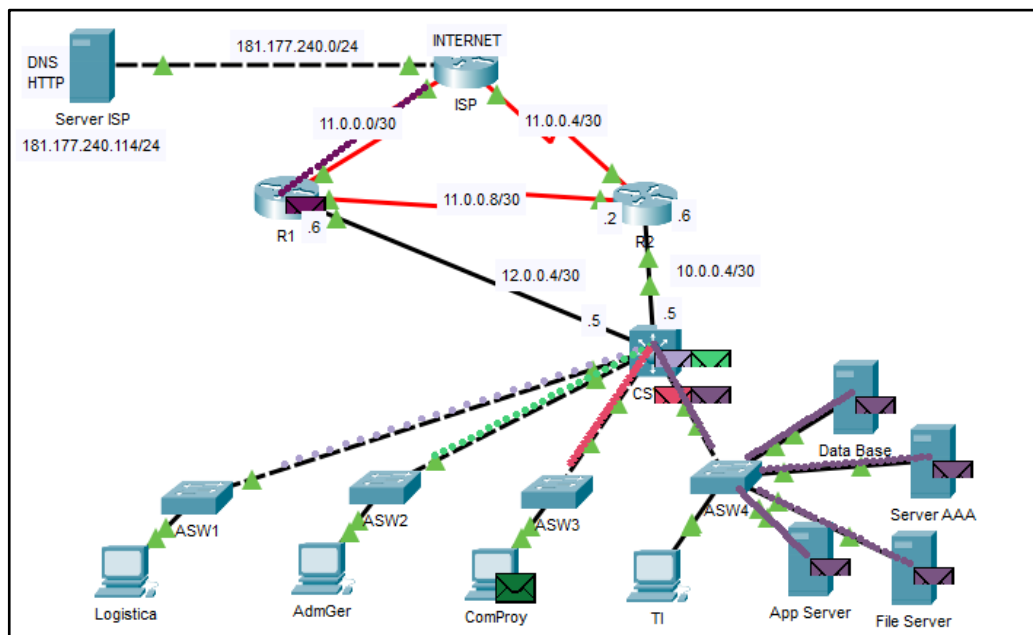
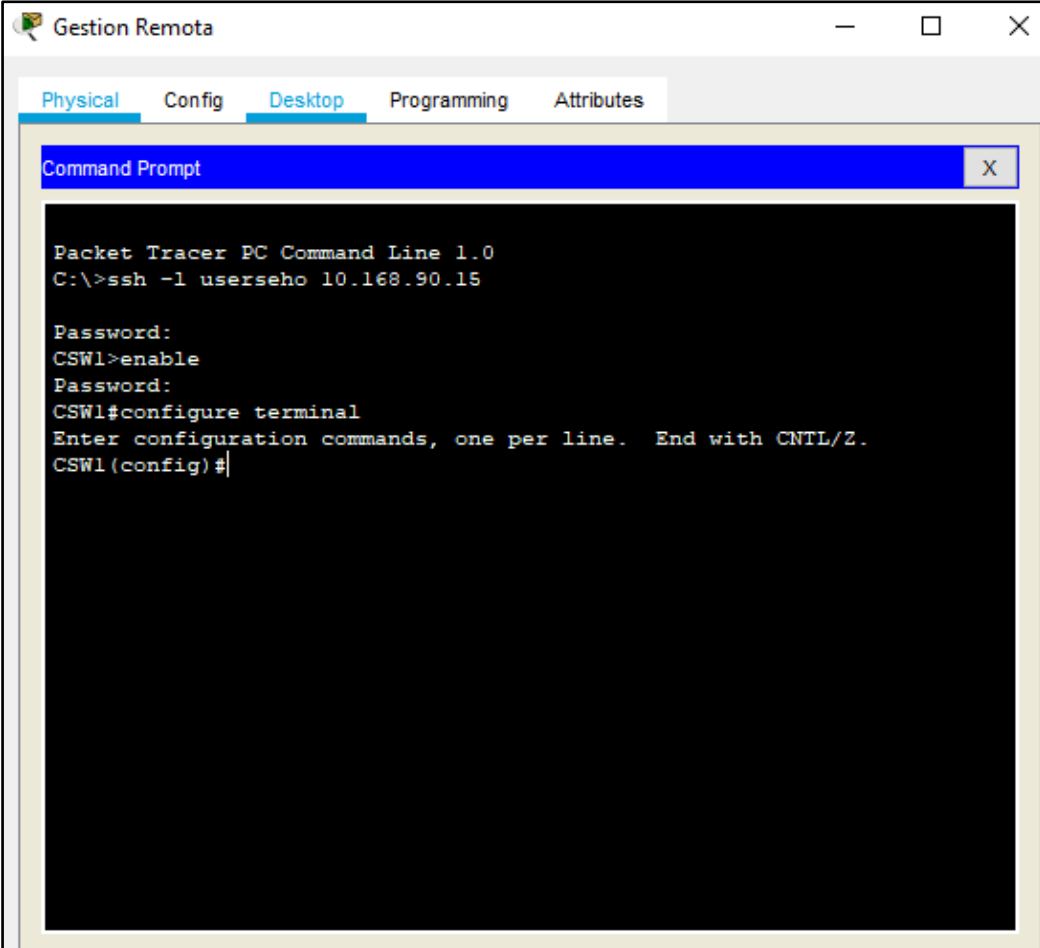


Figura N°44. Rutas de respaldo dirigidas a CSW2

- **Gestión remota:** Mediante el protocolo de administración remota SSH, se realiza la conexión a los dispositivos para realizar cualquier tipo de cambio en la administración de la red, en este caso, se toma como ejemplo el primer switch de distribución (CSW1) el cual tiene la dirección IP 10.168.90.15/24 para el acceso a la gestión remota, donde se ejecuta el comando “ssh -l (usuario) (IP)” para tener conexión. Asimismo, es necesario ingresar con el usuario creado, el cual es “userseho”, luego se ingresa la contraseña +LinuxS3H20*, no obstante, por motivos de seguridad la clave no se muestra en la pantalla. Finalmente, para habilitar el dispositivo y poder ingresar a la configuración global, se dispone de la contraseña *+S3h0v3R*+. El proceso se visualiza en la Figura N°45



The image shows a screenshot of a Packet Tracer PC Command Line window titled "Gestion Remota". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. Inside the window is a "Command Prompt" window with a black background and white text. The text in the Command Prompt is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ssh -l userseho 10.168.90.15

Password:
CSW1>enable
Password:
CSW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CSW1(config)#
```

Figura N°45. Acceso remoto a CSW1

CONCLUSIONES

- Se diseña una red LAN-WAN de alta disponibilidad para la empresa Corporación Sehover, el cual cuenta con protocolos, normas y estándares necesarios para que reduzcan los tiempos de activación de servicio en la red, el cual anteriormente tomaba horas y después del diseño solo se requiere de 5 a 10 segundos para la reactivación del servicio. Asimismo, se valida las buenas prácticas para la gestión de seguridad de la información.
- Se identifica los equipos necesarios para el diseño de la red los cuales fueron determinados en base a un análisis de la situación problemática, los equipos utilizados son los switches Cisco de la serie 2960 y 3650, asimismo, se utiliza los routers Cisco de la serie 4331. Estos equipos cuentan con niveles de redundancia y disponibilidad, es decir, existe un equipo activo y otro equipo de respaldo, de esta manera el equipo de respaldo asume el rol de activo en caso de que el equipo principal falle.
- Se define y valida los protocolos de alta disponibilidad y seguridad en la red, los cuales son los siguientes protocolos: STP en su versión RSTP, LACP, HSRP, EIGRP, SSH y AAA. De esta manera, se detecta caminos alternos para la transferencia de información entre todas las áreas de la empresa. Adicional a ello, se obtiene un balanceo de carga óptimo en la red

RECOMENDACIONES

Para elaborar el diseño de la red, se requiere personal con conocimiento de protocolos redundantes y seguridad en los diferentes modelos de comunicación. Asimismo, se administre de manera confiable la red LAN de alta disponibilidad, basándose en las normas de seguridad de la información y buenas prácticas como ISO/IEC 27002.

Tomar en cuenta artículos científicos relacionados al presente trabajo, que cuenten con documentos indexados en cuartil 1 y 2, el cual sirve para evaluar la importancia relativa de una revista dentro del total de revistas de su área a nivel internacional, asimismo, obteniendo los resultados esperados y adicionándole un valor agregado a cualquier trabajo.

Tener en cuenta que las normas ANSI/EIA/TIA 568A y 568B, describen como se arman los conectores RJ45, sin embargo, estas dos normas se diferencian por el orden de los colores de los pares a seguir. Si bien el uso de la norma 568B para cableado es la más utilizada, también en algunos casos se usa la norma 568A, por ello es necesario conocer el código de colores que rigen ambas normas.

Establecer políticas de seguridad de la información en conjunto con la política de seguridad de la empresa para obtener un diálogo continuo entre el área de TI y la compañía, asimismo, considerar los requisitos necesarios dentro de un enfoque de seguridad con dispositivos de aplicaciones de red.

BIBLIOGRAFÍA

- Estepa, R., Estepa, A., Cupertino, T., Vozmediano, J.M. y Madinabeitia, G. (2011). A Productivity-Based Approach to LAN Topology Design. *IEEE Communications Letters*, vol. 15, No. 3, pp. 349 – 351. Recuperado de: <https://ieeexplore.ieee.org/document/5704845>
- Sheghdara, M. y Hassine, J. (2019). Automatic retrieval and analysis of high availability scenarios from system execution traces: A case study on hot standby router protocol. *Journal of Systems and Software*, vol. 161, artículo 110490. Recuperado de: <https://www.sciencedirect.com/science/article/abs/pii/S016412121930264X>
- Zheng, L. (2017). *Diseño e implementación de una red lan para la empresa Palinda*. [Trabajo de titulación, Universidad San Francisco de Quito]. Recuperado de: <http://repositorio.usfq.edu.ec/bitstream/23000/6383/1/130874.pdf>
- Universidad de Valencia (2009). Redes de comunicación: Topologías y enlaces. *Sistemas industriales distribuidos*. Pp. 18-33. Recuperado de: https://www.uv.es/rosado/courses/sid/Capitulo2_rev0.pdf
- Buettrich S. y Escudero A. (2007). Topología e Infraestructura Básica de Redes Inalámbricas. *En Topología e Infraestructura* (1-22) UNAC. https://www.unac.edu.pe/images/inventario/documentos/manuales/topologia-e-infraestructura_guia_v02.pdf
- Cisco Systems (2006). *Hot Standby Router Protocol Features and Functionality*. <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.pdf>
- Briceño J. (2005). *Transmisión de datos*. Recuperado de <http://www.serbi.ula.ve/serbiula/libroselectronicos/Libros/trasmisiondedatos/pdf/librocompleto.pdf>
- Cuazitl M., (2013). *Normas IEEE*. (Estándar de Ethernet). Recuperado de <https://mariocuazitl.files.wordpress.com/2013/05/redesieee802.pdf>
- Corporación Oracle (2010). Modelo de arquitectura del protocolo TCP/IP. *Guía de administración del sistema: servicios IP*. Recuperado de: <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-10/>
- Cisco (2018). Protocolo spanning-tree (STP). *Switchs inteligentes Cisco*. Recuperado: https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-250-

- series-smart-switches/smb5303-configure-spanning-tree-protocol-stp-on-a-switch.html
- Cisco Systems (2007). Spanning Tree Protocol. *LAN Switching*. Recuperado de: <https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html>
 - Hospina Gonzales, M. (2017) *Diseño e implementación de VLAN para mejorar la eficiencia en la transmisión de datos en la municipalidad provincial de Huancayo* [Tesis de titulación, Universidad Nacional del centro del Perú] Recuperado de: http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/5038/T010_47190108_T.pdf?sequence=1&isAllowed=y
 - Li T., Li D., Cole B. y Morton P. (1998). Cisco Hot Standby Router Protocol (HSRP) *RFC 2281*. Recuperado de: <https://tools.ietf.org/html/rfc2281>
 - Forum Huawei, (5 de julio, 2019) What is the difference between lacp and pagp. *Switches*. <https://forum.huawei.com/enterprise/en/what-is-the-difference-between-lacp-and-pagp/thread/545699-861>
 - Cisco Systems (2016). Alta disponibilidad y funcionamiento redundante. Recuperado de: <http://www.cisco.com/c/en/us/td/docs/routers/asr9000/hardware/overview/guide/asr9kOVRGbk/asr9kOVRGHAredundancy.pdf>
 - Cisco Systems (2006) Hot Standby Router Protocol Features and Functionality. Recuperado de <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.pdf>
 - Aguirre E., Calva J., Guerrero A., Hernández A., Hernández S., Hernández G., (2017) Comparación de los modelos OSI y TCP/IP. *Universidad Autónoma del Estado de Hidalgo*. <https://www.uaeh.edu.mx/scige/boletin/huejutla/n10/r1.html>
 - Ostec (2018). *ISO 27002: Buenas prácticas para gestión de la seguridad de la información*. Recuperado de: <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi>
 - Cisco Systems (2005) Notas Técnicas de Troubleshooting. *Introducción a EIGRP*. Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html#eigrp_concepts

- Cisco Systems (2015) Notas Técnicas de Troubleshooting. *¿Cómo funciona el balanceo de cargas?* Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/5212-46.html
- Cisco Systems (2017). Rapid psvt. Recuperado de: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-6500-series-switches/72836-rapidpvt-mig-config.pdf
- Cisco Systems (2019) Sistema de control de acceso tacacs. *Los niveles de privilegio de IOS no pueden ver la configuración completa en ejecución.* Recuperado de: https://www.cisco.com/c/es_mx/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/23383-showrun.pdf
- Cisco Systems (2005) Configuring Basic AAA on an Access Server <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>
- Cisco Systems (2007). Basic TACACS+ Configuration Example. Recuperado de: <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10368-basictacacs.html>
- Huawei (2018) Ejemplos típicos de configuración de la serie S12700. *Guía de interfuncionamiento y reemplazo de protocolos de árbol de expansión en switches de Huawei e switches de Cisco.* Recuperado de: <https://support.huawei.com/enterprise/es/doc/EDOC1100027117?section=j01o>
- MIT (2006) Red Hat Enterprise Linux 4: Manual de referencia. *Capítulo 20: Protocolo SSH.* Recuperado de: <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html>
- Cisco Systems (2008) TACACS+ and RADIUS Comparison. Recuperado de: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>
- Instituto Tecnológico Superior del Oriente del Estado de Hidalgo (2015) Algoritmo dual. *Terminología.* Recuperado de: <https://www.itesa.edu.mx/netacad/scaling/course/module7/7.3.3.1/7.3.3.1.html>

ANEXOS

1. Conexión con el servidor web: Desde el navegador de la VLAN 10 que representa el área de logística de la empresa, se ingresa al dominio sehover.com desde el ordenador, donde se verifica con éxito la página web. Este resultado se visualiza en la Figura N°46.



Figura N°46. Acceso al servidor web

2. Balanceo de carga

Se visualiza el balanceo de carga, cuando se realiza el envío de un paquete de información de la subred Logística, el cual primero llega a CSW1 y luego cada paquete se distribuye por diferentes interfaces, para minimizar el tráfico de información por una misma ruta. Este resultado se visualiza en la Figura N°47.

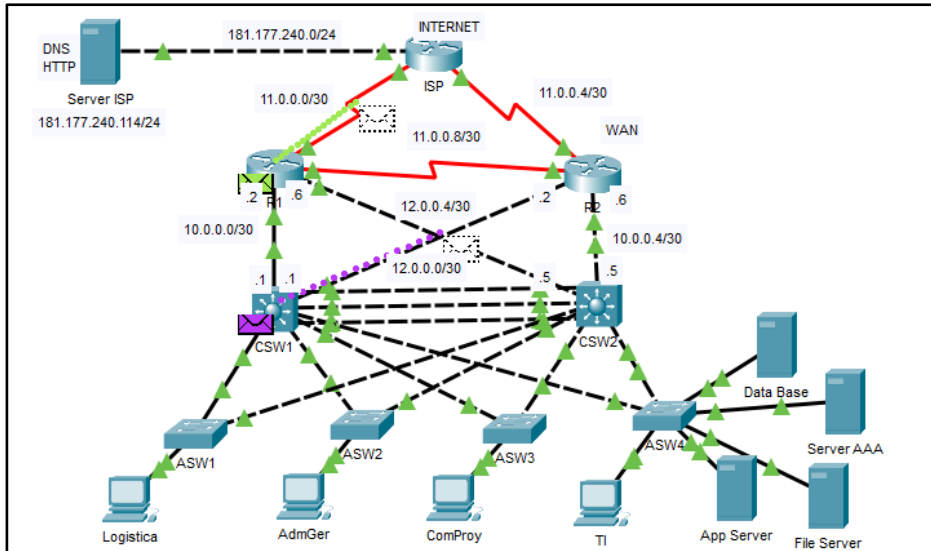


Figura N°47. Balanceo de carga desde ordenador Logística

3. VLAN 10 Y VLAN 20 como raíz primaria en CSW1

Este resultado se visualiza en la Figura N°48.

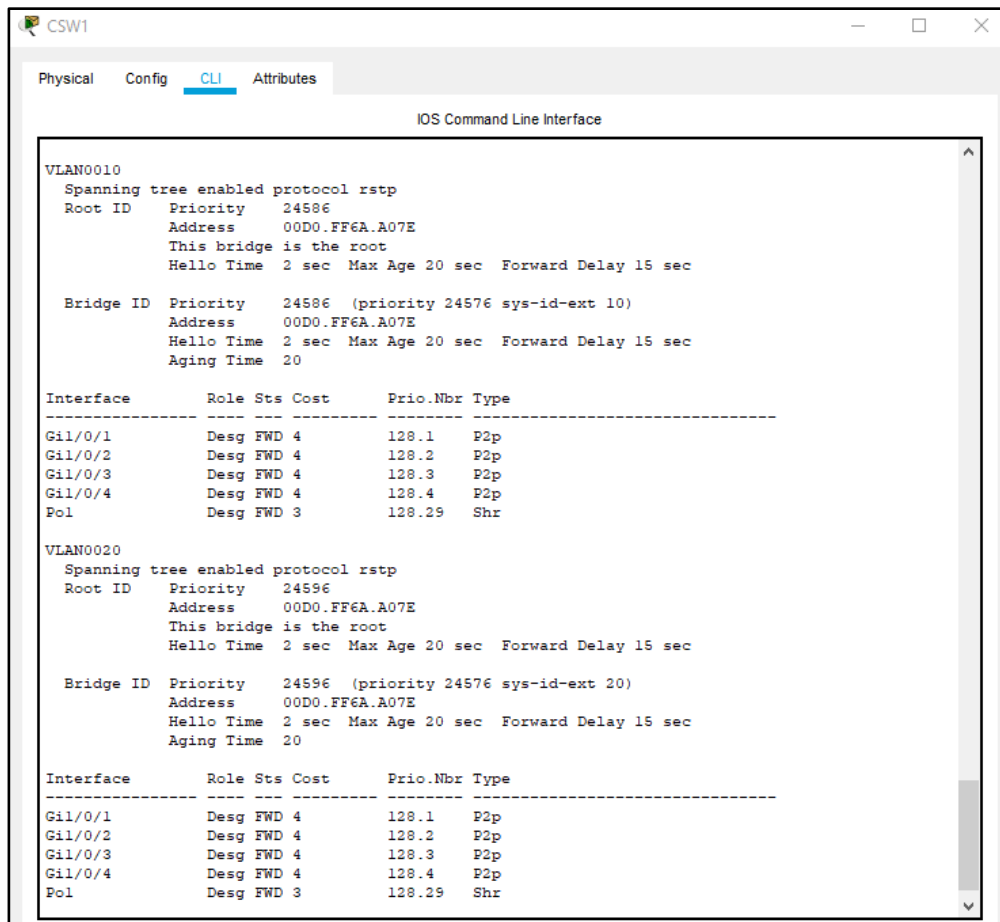


Figura N°48. Raíz primaria en CSW1

4. Servicio activo al simular falla en R1 y CSW1

Este resultado se visualiza en la Figura N°49.

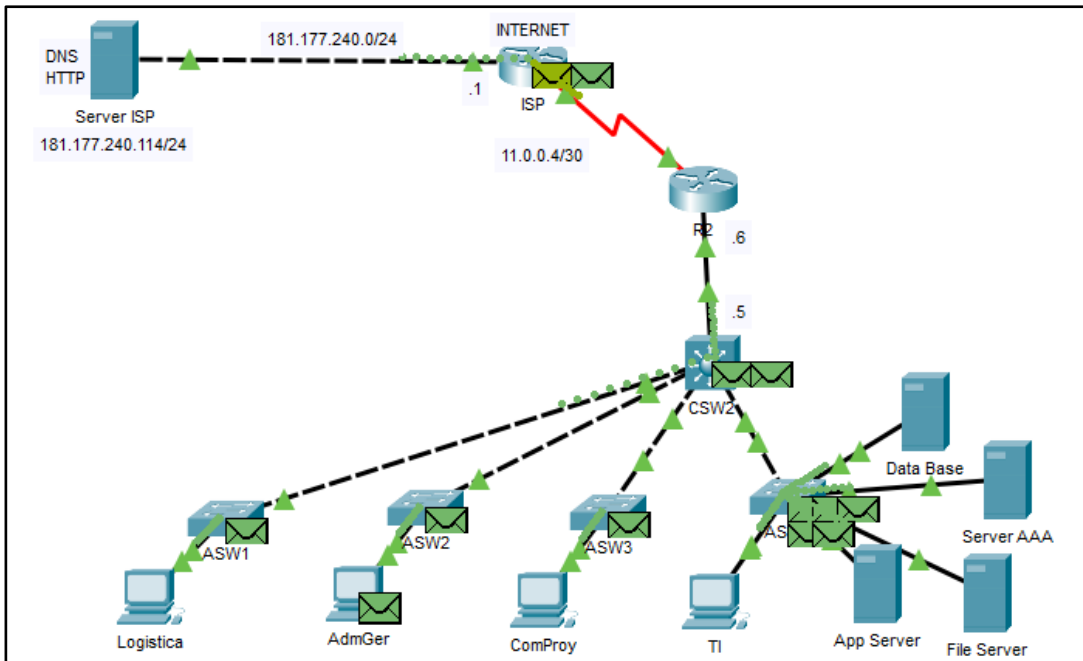


Figura N°49. Servicio activo al simular falla en R1 y CSW1

5. Servicio activo al simular falla en R2 y CSW2

Este resultado se visualiza en la Figura N°50.

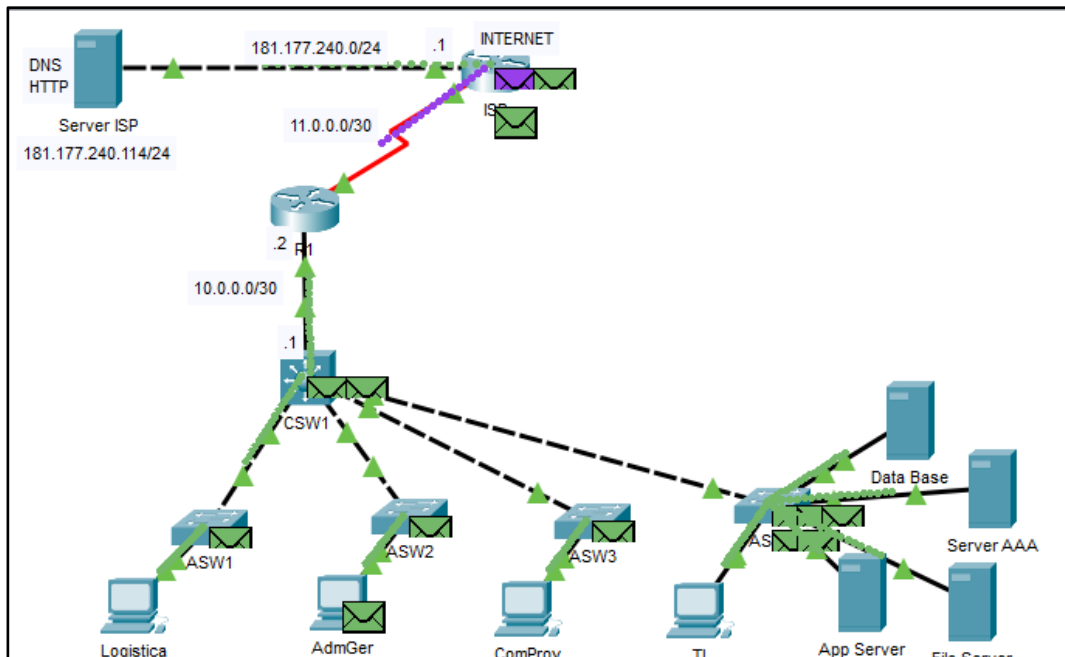


Figura N°50. Servicio activo al simular falla en R2 y CSW2

6. Servicio activo al simular falla en R1 y CSW2

Este resultado se visualiza en la Figura N°51.

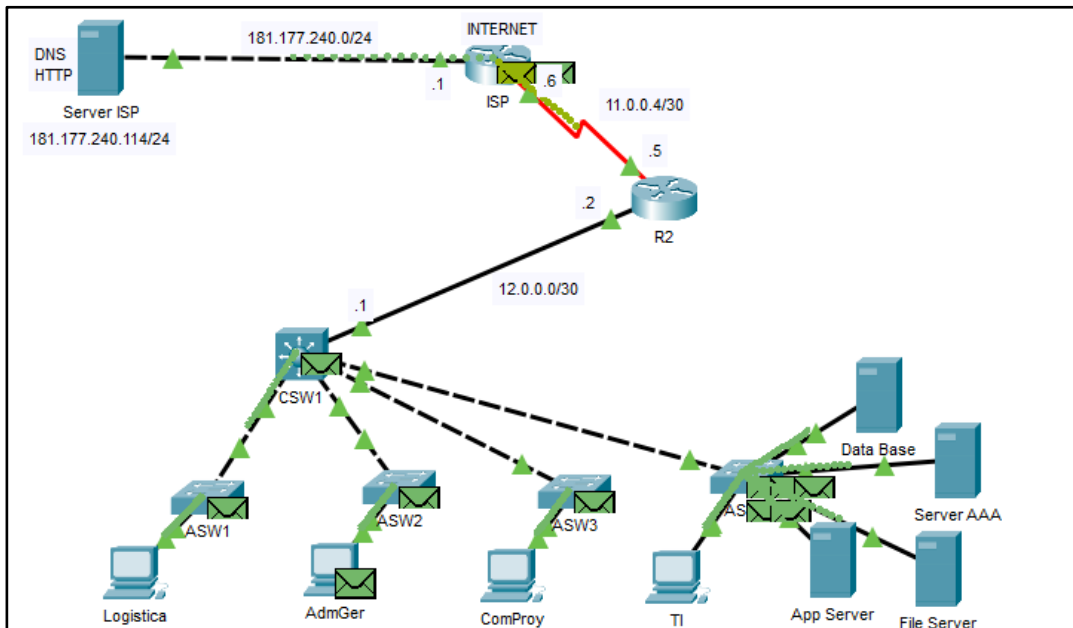


Figura N°51. Servicio activo al simular falla en R1 y CSW2

7. Servicio activo al simular falla en R2 y CSW1

Este resultado se visualiza en la Figura N°52.

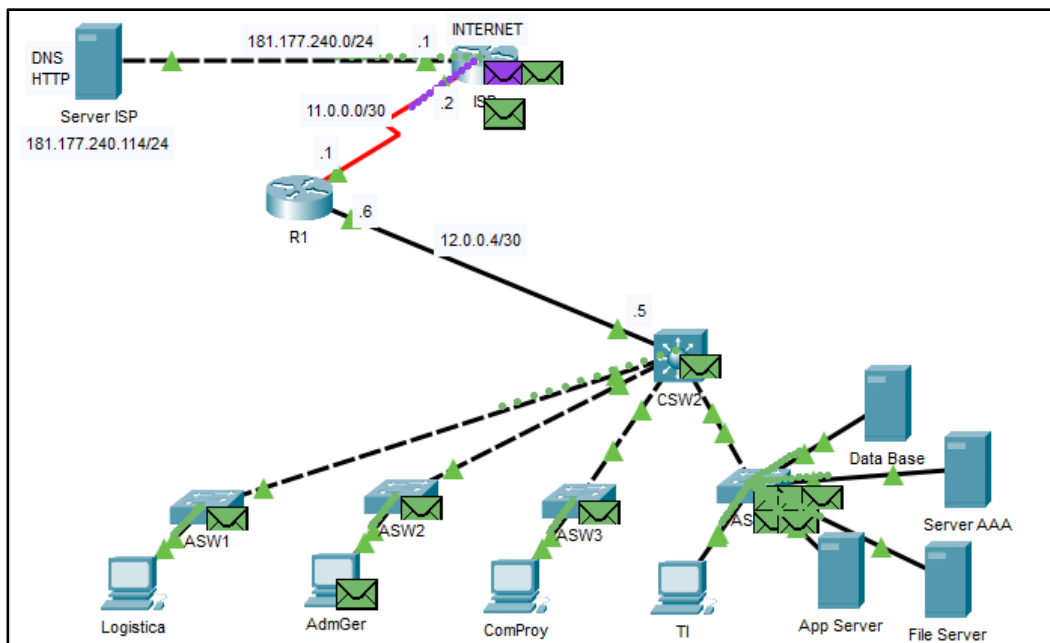


Figura N°52. Servicio activo al simular falla en R2 y CSW1

8. Registro del servidor AAA con la configuración TACACS+

Se realiza el registro de las credenciales en el servidor AAA. Este resultado se visualiza en la Figura N°53.

The screenshot shows the configuration interface for the AAA service. The 'Services' tab is active, and the 'AAA' service is selected in the left sidebar. The main configuration area is divided into 'Network Configuration' and 'User Setup'.

Network Configuration:

- Service: On Off
- Radius Port: 1645
- Client Name: CSW1, Client IP: 10.168.90.15
- Secret: adm\$3H20*
- ServerType: Tacacs

	Client Name	Client IP	Server Type	Key	
1	CSW1	10.168.90.15	Tacacs	adm\$3H20*	Add
2	CSW2	10.168.90.16	Tacacs	adm\$3H20*2	Save
3	R1	10.168.90.17	Tacacs	adm\$3H20*3	Remove
4	R2	10.168.90.18	Tacacs	adm\$3H20*4	

User Setup:

- Username: usertacacs, Password: +Linux\$3H20*a

	Username	Password	
1	usertacacs	+Linux\$3H20*a	Add

Figura N°53. Credenciales del servidor AAA