



INSTITUTO DE EDUCACIÓN SUPERIOR PRIVADO

“IDAT”

**PROGRAMA DE ESTUDIOS EN ADMINISTRACIÓN DE
REDES Y COMUNICACIONES DE DATOS**

**DISEÑO DE UNA RED DE DATOS PARA UNA EMPRESA DE VENTAS
PARA INTERCONECTAR SU SEDE PRINCIPAL CON SUS
SUCURSALES, 2026**

**Trabajo de aplicación profesional para obtener el título Profesional Técnico en
Administración de Redes y Comunicaciones de Datos**

VILCA ARIZANCA SERGIO EFRAIN

(0009-0004-0069-8274)

Lima – Perú

2026

Dedicatoria

Dedico este trabajo a mi familia y mis amigos por su constante apoyo y por ser mi mayor fuente de inspiración. Gracias por su comprensión y confianza a aquellos que me impulsan a seguir avanzando y creer siempre en uno mismo.

Índice General

Resumen Ejecutivo	11
Introducción	12
Capítulo I	14
Aspectos Generales	14
Nombre del Proyecto	14
Tipo de Proyecto	14
Equipo del Proyecto	14
Planteamiento del Problema	15
Objetivos	15
<i>Objetivo General</i>	15
<i>Objetivos Específicos</i>	15
Antecedentes	16
Descripción del Proyecto	17
Justificación del Proyecto	17
Interesados del Proyecto	18
Alcance del Proyecto	18
Capítulo II	20
Estudio de Mercado	20
Selección de Dispositivos de Red	20
Selección de Software de Monitoreo de Red	22
Cuadros Comparativos de Fabricantes de Dispositivos de Red	23
Selección de Switch de Acceso	24
Selección de Switch de Capa3	25
Comparación de Fabricantes Firewall	26
Selección de Firewall	26
Capítulo III	28
Estudio Técnico	28
Marco Teórico	28
Tipos de Redes	29
<i>Red de Área Amplia (WAN)</i>	29
<i>Red de Área Metropolitana (MAN)</i>	29
<i>Red de Área Local (LAN)</i>	30

<i>Red de Área Local Inalámbrica (WLAN)</i>	30
Tipos de Topologías de Red	31
<i>Topología Bus</i>	31
<i>Topología Estrella</i>	32
<i>Topología Anillo</i>	32
<i>Topología Malla</i>	33
<i>Topología Árbol</i>	33
Tipos de Equipo de Red	34
<i>Router</i>	34
<i>Switch</i>	34
<i>Access Point (AP)</i>	35
<i>Firewall</i>	35
Cable de Red	35
<i>Par Trenzado</i>	36
<i>Fibra Óptica</i>	37
Tecnología.....	37
<i>Energía Sobre Ethernet (POE)</i>	37
<i>Red de Área Local Virtual (VLAN)</i>	39
<i>Seguridad de Puertos (Port Security)</i>	40
<i>Red Privada WAN - Hub-and-Spoke</i>	40
<i>Red Privada Virtual (VPN)</i>	41
Protocolos de Red	42
<i>Protocolo de Enlace Troncal de VLAN (VTP)</i>	42
<i>Protocolo Seguro de Caparazón (SSH)</i>	42
<i>Protocolo de Direccionamiento de Tipo de Enlace-Estado (OSPF)</i>	43
<i>Protocolo de Enrutador de Reserva Activa (HSRP)</i>	43
<i>Protocolo de Traducción de Direcciones de Red (NAT)</i>	44
<i>Protocolo Simple de Administración de Red (SNMP)</i>	45
Seguridad y Acceso.....	45
<i>Cifrado de Datos (VPN IP Sec)</i>	45
<i>Firewall Perimetral</i>	46
Software de Monitoreo	46
<i>PRTG</i>	46
<i>Zabbix</i>	47

Metodología	48
<i>Preparar</i>	48
<i>Planificar</i>	48
<i>Diseñar</i>	49
<i>Implementar</i>	49
<i>Operar</i>	49
<i>Optimizar</i>	49
Desarrollo del trabajo.....	50
<i>Descripción de la Infraestructura Actual</i>	50
<i>Análisis de la Infraestructura Actual</i>	54
<i>Criterios de Diseño de la Topología de la Red Propuesta</i>	54
<i>Descripción de la Infraestructura Propuesta</i>	55
<i>Segmentación de la Red Propuesta</i>	57
Configuración del Equipamiento de la Red Propuesta	65
Configuraciones de Equipos Realizadas en la Topología de Red.....	66
<i>Configuración del Protocolo VTP</i>	68
<i>Configuración VLANs</i>	70
<i>Configuración de Port Security</i>	74
<i>Configuración de Spanning-tree + Portfast + BPDUGuard</i>	78
<i>Configuración Interfaz Virtual Switch (SVI)</i>	79
<i>Configuración Puerto Troncal (Trunk)</i>	83
<i>Configuración de HSRP</i>	86
<i>Configuración del Protocolo DHCP</i>	87
<i>Configuración Enrutamiento Dinámico OSPF</i>	88
<i>Configuración Enrutamiento Estático</i>	90
<i>Seguridad de Inicio de Sesión</i>	90
<i>Configuración de Acceso Remoto Seguro mediante SSH</i>	93
<i>Configuración SNMP</i>	94
<i>Configuración PRTG</i>	94
Pruebas Operativas y Resultados	96
<i>Pruebas Operativas de la Solución de DHCP</i>	96
<i>Pruebas Operativas de la Solución de Port Security</i>	98
<i>Pruebas Operativas de la Solución de Enrutamiento</i>	100
<i>Pruebas Operativas de la Solución de SSH</i>	103

Pruebas Operativas de la Solución del Sistema de Monitoreo	108
Capitulo IV.....	109
Estudio de Costos.....	109
Costos de equipamiento	109
Costos de Implementación.....	110
Costos de contratación de Servicio de Internet.....	111
Resumen del Costo Total de Equipamiento e Implementación	112
Conclusiones	113
Recomendaciones	115
Referencia Bibliográficas.....	117
Anexos	120

Índice de Tablas

Tabla 1	Integrante del Proyecto	14
Tabla 2	Tabla de Comparación – Software Monitoreo	22
Tabla 3	Cuadro Comparativo de Switches – Capa de Acceso	23
Tabla 4	Cuadro Comparativo de Switches L3	25
Tabla 5	Comparación de fabricantes Firewall	26
Tabla 6	Plan de Direccionamiento IP, Áreas y Equipamiento Actual.....	51
Tabla 7	Resumen de análisis de la Red Actual	54
Tabla 8	Resumen de la Infraestructura de Red Propuesta – Sede Principal	56
Tabla 9	Resumen de la Infraestructura de Red Propuesta – Sucursales	57
Tabla 10	Equipos propuestos – Sede Principal y sucursales	57
Tabla 11	Distribución de la Red – VLANs para las Áreas de Servicio	58
Tabla 12	Distribución de Red - Direccionamiento IP de VLAN de Gestión.....	59
Tabla 13	Direccionamiento IP de Switch Core - Sede Principal	59
Tabla 14	Direccionamiento IP de Switch Core - Sucursal G4S.....	60
Tabla 15	Direccionamiento IP de Switch Core - Sucursal Orquídeas	60
Tabla 16	Direccionamiento de Red – Sede Principal (Central Tower).....	61
Tabla 17	Direccionamiento de Red – Sucursal 1(G4S)	61
Tabla 18	Direccionamiento de Red – Sucursal 2 (Orquídeas).....	62
Tabla 19	Planificación de la Segmentación y Escalabilidad de la Red	63
Tabla 20	Costos de Equipamiento	109
Tabla 21	Costos de Implementación.....	110
Tabla 22	Costos de servicio de Internet y conexión Privada	111
Tabla 23	Resumen de Costo Total de la Implementación.....	112

Índice de Figuras

Figura 1	Estudio de marcas líderes de equipos de Red	21
Figura 2	PRTG Network Monitor	23
Figura 3	Switch - HPE Aruba CX 6000– R8N85A.....	24
Figura 4	Cisco C9300-48T-A	25
Figura 5	HPE Aruba CX 6200M 24G 4SFP+	26
Figura 6	Fortinet - FortiGate 60F	27
Figura 7	Mapa conceptual del trabajo de aplicación.....	28
Figura 8	Red de Área WAN	29
Figura 9	Red de Área Metropolitana.....	30
Figura 10	Red de Área Local	30
Figura 11	Red de Área local Inalámbrica.....	31
Figura 12	Topología de red - Bus	31
Figura 13	Topología de red – Estrella	32
Figura 14	Topología de red – Anillo	32
Figura 15	Topología de red - Malla.....	33
Figura 16	Topología de red - Árbol.....	33
Figura 17	Equipo de red - Router	34
Figura 18	Equipo de red - Switch.....	34
Figura 19	Equipo de red – Access Point.....	35
Figura 20	Equipo de red – Firewall.....	35
Figura 21	Comparativo de categoría de cable de red	36
Figura 22	Cable de red – Par Trenzado	37
Figura 23	Cable de red - Fibra.....	37
Figura 24	Tecnología POE – Switch Pasivo y Activo.....	38
Figura 25	Tecnología POE – Tipos de Equipos Soportados	39
Figura 26	Segmentos de VLANs.....	39
Figura 27	Seguridad de Puertos (Port Security).....	40
Figura 28	Tecnología – WAN Privada (Hub and Spoke)	41
Figura 29	Tecnología - VPN.....	41
Figura 30	Protocolo de Enlace Troncal - VTP	42
Figura 31	Protocolo Seguro de Caparazón -SSH	42
Figura 32	Protocolo de Direccionamiento de Tipo Enlace-Estado (OSPF)	43
Figura 33	Protocolo de Enrutador de Reserva Activa (HSRP)	44
Figura 34	Protocolo de Traducción de Direcciones de Red (NAT).....	44
Figura 35	Protocolo Simple de Administración de Red (SNMP)	45
Figura 36	Seguridad y acceso – Cifrado de datos (VPN IPSec)	46
Figura 37	Seguridad y Acceso – Firewall Perimetral.....	46
Figura 38	Software de Monitoreo – PRTG Network Monitor	47
Figura 39	Software de Monitoreo – Zabbix	47
Figura 40	Metodología PPDIOO Cisco.....	48
Figura 41	Infraestructura Actual de la Red	53

Figura 42	Topología de Red Propuesta	64
Figura 43	Packet Tracer - Simulación ISP / Sedes	67
Figura 44	Configuración del Protocolo VTP - SW-LMCentral-CORE1	68
Figura 45	Configuración del Protocolo VTP - SW-LMCentral-CORE2	68
Figura 46	Configuración del Protocolo VTP - SW-LM-Access01.....	68
Figura 47	Configuración del Protocolo VTP - SW-LM-Access02.....	69
Figura 48	Configuración del Protocolo VTP - SW-LM-Access03.....	69
Figura 49	Configuración del Protocolo VTP - SW-LM-Access04.....	70
Figura 50	Configuración del Protocolo VTP - SW-LM-Access05.....	70
Figura 51	Configuración de las VLANs - SW-LMCentral-CORE1	71
Figura 52	Configuración de las VLANs - SW-LMCentral-CORE2	71
Figura 53	Configuración de las VLANs - SW-LM-Access01	72
Figura 54	Configuración de las VLANs - SW-LM-Access02	72
Figura 55	Configuración de las VLANs - SW-LM-Access03	73
Figura 56	Configuración de las VLANs - SW-LM-Access04	73
Figura 57	Configuración de las VLANs - SW-LM-Access05	74
Figura 58	Configuración de Port Security - SW-LM-Access01.....	75
Figura 59	Configuración de Port Security - SW-LM-Access02.....	76
Figura 60	Configuración de Port Security - SW-LM-Access03.....	76
Figura 61	Configuración de Port Security - SW-LM-Access04.....	77
Figura 62	Configuración de Port Security - SW-LM-Access05.....	77
Figura 63	Configuración de STP SW-LMCentral-CORE1	78
Figura 64	Configuración de STP SW-LMCentral-CORE2	78
Figura 65	Configuración de STP del SW-LM-Access01 al 05	79
Figura 66	Configuración de Interfaz SVI - Switch SW-LMCentral-CORE1	79
Figura 67	Configuración de Interfaz SVI - Switch SW-LMCentral-CORE2	80
Figura 68	Configuración de Interfaz SVI - Switch SW-LM-Access01.....	80
Figura 69	Configuración de Interfaz SVI - Switch SW-LM-Access02.....	80
Figura 70	Configuración de Interfaz SVI - Switch SW-LM-Access03.....	81
Figura 71	Configuración de Interfaz SVI - Switch SW-LM-Access04.....	81
Figura 72	Configuración de Interfaz SVI - Switch SW-LM-Access05.....	81
Figura 73	Configuración de Interfaz SVI - Switch Sw-Paso1	82
Figura 74	Configuración de Interfaz SVI - Switch Sw-Paso2	82
Figura 75	Configuración de Interfaz SVI - Switch Sw-Paso3	82
Figura 76	Configuración Puerto Troncal - Switch SW-LMCentral-CORE1	83
Figura 77	Configuración Puerto Troncal - Switch SW-LMCentral-CORE2	84
Figura 78	Configuración Puerto Troncal - Switch SW-LM-Access01.....	84
Figura 79	Configuración Puerto Troncal - Switch SW-LM-Access02.....	84
Figura 80	Configuración Puerto Troncal - Switch SW-LM-Access03.....	84
Figura 81	Configuración Puerto Troncal - Switch SW-LM-Access04.....	85
Figura 82	Configuración Puerto Troncal - Switch SW-LM-Access05.....	85
Figura 83	Configuración Puerto Troncal - Switch SW-LM-Sw-Paso1	85
Figura 84	Configuración Puerto Troncal - Switch SW-LM-Sw-Paso2.....	85

Figura 85	Configuración Puerto Troncal - Switch SW-LM-Sw-Paso3	85
Figura 86	Configuración HSRP - Switch SW-LMCentral-CORE1	86
Figura 87	Configuración HSRP - Switch SW-LMCentral-CORE2	87
Figura 88	Configuración DHCP - Switch SW-LMCentral-CORE1 y 2.....	88
Figura 89	Configuración Enrutamiento OSPF - SW-LMCentral-CORE1 y 2.....	89
Figura 90	Configuración Enrutamiento Estático - Switch SW-LMCentral-CORE1 y 2 ..	90
Figura 91	Configuración Seguridad de Inicio de Sesión.....	91
Figura 92	Configuración Seguridad de Inicio de Sesión - Autenticación AAA.....	92
Figura 93	Configuración Security Shell (SSH).....	93
Figura 94	Configuración SNMP.....	94
Figura 95	Configuración PRTG	95
Figura 96	Configuración PRTG – Logs	95
Figura 97	Pruebas Operativas y Resultados DHCP - VLAN 10 en SW-LMCentral- CORE1 y 2	97
Figura 98	Pruebas Operativas y Resultados Port Security – Antes del Bloqueo de Puerto 98	98
Figura 99	Pruebas Operativas y Resultados Port Security – Bloqueo de Puerto	99
Figura 100	Pruebas Operativas y Resultados Port Security - Bloqueo DHCP	99
Figura 101	Pruebas Operativas y Resultados Port Security - Bloqueo Ping.....	100
Figura 102	Pruebas Operativas de la Solución de Enrutamiento	100
Figura 103	Prueba de Enrutamiento – Ping PC Sede Principal a Sucursal G4S.....	101
Figura 104	Prueba de Enrutamiento – Ping PC Sucursal G4S a Sede Principal.....	102
Figura 105	Pruebas Operativas de la Solución SSH – SW-LMCentral-CORE1	103
Figura 106	Pruebas Operativas de la Solución SSH – SW-LMCentral-CORE2	103
Figura 107	Pruebas Operativas de la Solución SSH – SWLM-Access01.....	104
Figura 108	Pruebas Operativas de la Solución SSH – SWLM-Access02.....	104
Figura 109	Pruebas Operativas de la Solución SSH – SWLM-Access03.....	105
Figura 110	Pruebas Operativas de la Solución SSH – SWLM-Access04.....	105
Figura 111	Pruebas Operativas de la Solución SSH – SWLM-Access05.....	106
Figura 112	Pruebas Operativas de la Solución del HSRP - SW-LMCentral-CORE1	107
Figura 113	Pruebas Operativas de la Solución del HSRP - SW-LMCentral-CORE2.....	107
Figura 114	Pruebas del Sistema de Monitoreo – Logs.....	108
Figura 115	Pruebas del Sistema de Monitoreo – Disponibilidad.....	108
Figura 116	Cronograma de Implementación.....	110

Resumen Ejecutivo

El presente trabajo tuvo como finalidad desarrollar una propuesta de diseño de red de datos para una empresa de ventas. Actualmente, la empresa cuenta con tres sedes, la sede principal se encuentra en la ciudad de Lima distrito La Molina (Central Tower) y las sucursales se encuentran en el distrito de San Isidro (G4S y Orquídeas). Este proyecto se centra en su sede principal, sede Central Tower – La Molina en Lima, dado que al ser la sede principal necesita una mejora en la infraestructura de red y la conectividad de las otras dos sucursales nos apoyaremos con una solución de red WAN por el ISP a contratar. La necesidad de este proyecto surgió a raíz de los problemas de conectividad y lentitud en la transmisión de datos y voz que afectaban las operaciones diarias generando pérdidas económicas y dificultades en la gestión interna. Con el propósito de resolver estas deficiencias, se aplicó la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar), utilizada por Cisco para el desarrollo de infraestructuras de red empresariales. Esta metodología permitió estructurar el proyecto de forma ordenada, asegurando un diseño escalable, confiable y alineado con los requerimientos de la organización. Durante el desarrollo del trabajo, se realizó un análisis detallado de los requerimientos técnicos y de conectividad, así como una evaluación de los equipos y software necesarios para la gestión y monitoreo de la red. Finalmente, se elaboró una topología de red optimizada que permite la interconexión eficiente entre la sede principal y sus sucursales y se validó su funcionamiento mediante simulaciones en el software Cisco Packet Tracer, comprobando el cumplimiento de los objetivos planteados.

Palabras claves: Firewall; Red de datos; conectividad; escalabilidad; confidencialidad; integridad y disponibilidad.

Introducción

En la actualidad, las empresas del sector de ventas dependen en gran medida de la tecnología para garantizar la eficiencia operativa, la comunicación interna y la satisfacción del cliente. La empresa objeto de estudio se dedica a la comercialización de servicios de venta, brindando asesoría personalizada a cada cliente para la administración estratégica de su capital, con el objetivo de obtener resultados rentables y sostenibles. Este modelo de negocio requiere una infraestructura tecnológica sólida, segura y de alta disponibilidad, que asegure la continuidad operativa y la protección de la información confidencial.

Debido al crecimiento de la organización y a la necesidad de mantener una comunicación entre sus sedes, se evidenció la falta de una red estructurada en la sede principal y la falta de comunicación con sus dos sucursales. La falta de tener una red modular de datos en la sede principal generaba problemas de conectividad, lentitud en el acceso a los sistemas y limitaciones en la transferencia de información, afectando la productividad y la atención al cliente.

Por tal motivo, el presente proyecto tiene como finalidad diseñar una red de datos confiable y segura, donde también se emplee la interconexión de la sede principal con sus sucursales, garantizando un flujo de información ágil, seguro y estable. El diseño propuesto se basa en la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar), la cual permite desarrollar infraestructuras de red empresariales bajo un enfoque estructurado y eficiente.

La implementación de una red con alta disponibilidad contribuirá a minimizar los tiempos de inactividad, optimizar el desempeño de las operaciones críticas y fortalecer la comunicación entre las diferentes áreas de la empresa. De esta manera, el proyecto busca mejorar la productividad organizacional, garantizar la continuidad de los servicios y brindar una base tecnológica sólida para el crecimiento futuro de la compañía.

En el primer capítulo, se definió el proyecto en general. A partir del nombre del proyecto, tipo y equipo de proyecto. De igual modo, se planteó la justificación de este mismo y el alcance.

En el segundo capítulo, se aborda el estudio del mercado, con la finalidad de analizar y comparar los equipos de diferentes fabricantes para elegir los dispositivos de red que se acoplen y cubran con las necesidades de la empresa de ventas.

En el tercer capítulo se presenta el estudio técnico, que incluye el marco teórico, los conceptos de seguridad perimetral, el diseño de la arquitectura de red, los diagramas correspondientes, las configuraciones realizadas, así como las pruebas operativas y los resultados obtenidos mediante el simulador de red.

En el cuarto capítulo, se incluyeron el estudio de costo del proyecto, el cual comprende, el costo de equipos adquiridos, de igual modo, el costo del software del sistema de monitoreo para llevar a cabo este proyecto.

Finalmente, se presentan las conclusiones y recomendaciones del presente trabajo de aplicación profesional.

Capítulo I

Aspectos Generales

Nombre del Proyecto

El presente trabajo de aplicación profesional lleva por nombre “Diseño de una Red de Datos para una Empresa de Ventas para Interconectar su Sede Principal con sus Sucursales”.

De acuerdo con la finalidad expresada en el título, este proyecto tiene como objetivo diseñar una red de datos moderna, redundante, escalable, óptima y segura, que permita interconectar la sede principal con sus dos sucursales, garantizando la continuidad operativa, la protección de los activos digitales, el cumplimiento de las normativas vigentes y la confianza de los clientes.

Tipo de Proyecto

El presente proyecto corresponde a un trabajo de aplicación profesional enfocado en el análisis y diseño de una red de datos empresarial para una empresa de ventas, con el propósito de interconectar su sede principal con sus dos sucursales de manera eficiente.

Este proyecto no se limita únicamente a la configuración básica de dispositivos de red, sino que integra tecnologías orientadas a la disponibilidad, escalabilidad y seguridad.

Asimismo, se promueve el uso de una arquitectura unificada y centralizada, que permita la gestión coordinada de las soluciones de conectividad asegurando la integridad, confidencialidad y disponibilidad de la información dentro del entorno empresarial.

Equipo del Proyecto

A continuación, se presenta al representante y su rol en el trabajo de aplicación profesional.

Tabla 1

Integrante del Proyecto

Nombre	Código	Rol
Vilca Arizanca Sergio	A1507431	Especialista de Redes

Planteamiento del Problema

La empresa de ventas objeto de estudio presenta diversas deficiencias en su infraestructura de red, evidenciadas en problemas de conectividad, interrupciones frecuentes en el servicio y bajo rendimiento. Estas fallas afectan directamente la productividad del personal, la atención al cliente y la gestión de las operaciones comerciales, generando pérdidas económicas y retrasos en los procesos internos. Además, la falta de un diseño estructurado y seguro expone a la organización a riesgos tecnológicos, como accesos no autorizados, pérdida de datos o vulnerabilidades en la comunicación entre los departamentos.

Ante este escenario, surge la necesidad de diseñar una red de datos moderna, escalable y de alta disponibilidad, que permita interconectar eficientemente la sede principal con sus dos sucursales, garantizando una comunicación segura, estable y confiable. Con ello, se busca optimizar el flujo de información, mejorar la continuidad operativa y fortalecer la infraestructura tecnológica que soporte el crecimiento y las futuras demandas de la empresa.

Objetivos

Objetivo General

Diseñar una red de datos de alta disponibilidad para una empresa de ventas, que permita interconectar la sede principal con sus dos sucursales, garantizando una comunicación eficiente, segura y estable, así como la continuidad operativa y la integridad de la información entre todas las sedes.

Objetivos Específicos

- Analizar la situación actual de la infraestructura de red y los requerimientos tecnológicos de la empresa para identificar las necesidades de conectividad, seguridad y redundancia que aseguren la disponibilidad de los servicios entre las sedes.

- Diseñar la topología de red propuesta, aplicando principios de segmentación, escalabilidad y alta disponibilidad.
- Seleccionar los equipos y dispositivos de red adecuados, mediante un análisis comparativo de sus características técnicas y su compatibilidad con la solución propuesta.
- Elaborar las configuraciones de los dispositivos que conformas la solución propuesta.
- Realizar pruebas de verificación y simulación para validar el desempeño y la funcionalidad del diseño propuesto en un entorno controlado.
- Evaluar los costos referenciales asociados a la implementación de la red, considerando equipamiento, software y servicios complementarios.

Antecedentes

Zambrana y López (2015), en la investigación titulada “Diseño de una red LAN para la empresa Comercial Edgar Detrinidad S.A.” (Universidad Nacional Autónoma de Nicaragua – UNAN, Nicaragua), desarrollaron una propuesta de diseño de red LAN empresarial con el objetivo de mejorar la conectividad y el desempeño de la red interna. El estudio analizó la infraestructura existente y propuso una arquitectura LAN organizada, lo que permitió optimizar la comunicación entre las áreas de la empresa y mejorar la eficiencia en la transmisión de datos.

Castillo (2022), en la investigación titulada “Diseño de una red de alta disponibilidad y redundancia con la finalidad de garantizar la conectividad de la UNMSM” (Universidad Nacional Mayor de San Marcos, Perú), propuso un diseño de red con alta disponibilidad, basado en el análisis de la infraestructura existente y en la incorporación de mecanismos de redundancia, con el fin de garantizar la continuidad de los servicios de conectividad institucional.

Descripción del Proyecto

El presente proyecto tiene como finalidad diseñar una red de datos moderna y de alta disponibilidad para una empresa de ventas, con el propósito de mejorar la infraestructura de red en la sede principal y solicitar una solución de conectividad para interconectar su sede principal con sus dos sucursales garantizando una comunicación continua, segura y eficiente entre todas las sedes. La propuesta considera el desarrollo de una infraestructura de red escalable, confiable y redundante, que asegure la integridad de los datos, el óptimo desempeño de los servicios y la continuidad de las operaciones.

Para ello, se llevará a cabo un análisis de la situación actual, la identificación de los requerimientos técnicos y de conectividad, así como el diseño lógico y físico de la red, orientado a mejorar la eficiencia, la seguridad y la disponibilidad del entorno tecnológico de la empresa. Este diseño busca proporcionar una base sólida para futuras expansiones y soportar el crecimiento operativo y comercial de la organización.

Justificación del Proyecto

El presente proyecto se justifica por la necesidad de mejorar la infraestructura de red de una empresa de ventas, la cual requiere mantener una comunicación estable, segura y continua entre su sede principal y sus dos sucursales para garantizar el correcto desarrollo de sus operaciones comerciales. La red actual presenta limitaciones de conectividad, lentitud en la transmisión de datos y falta de redundancia, lo que afecta la productividad de los empleados, la eficiencia en los procesos internos y la calidad del servicio al cliente.

Con el diseño de una red de datos de alta disponibilidad, se busca asegurar la continuidad operativa, optimizar el rendimiento de los sistemas corporativos y fortalecer la seguridad de la información, permitiendo una comunicación confiable entre las sedes. Además, esta propuesta contribuirá al crecimiento tecnológico y competitivo de la empresa,

brindando una base sólida para la expansión futura y mejorando la eficiencia general de sus operaciones.

También se justifica tecnológicamente debido a que se basa en la necesidad de modernizar la infraestructura de red de la empresa mediante la implementación de tecnologías de alta disponibilidad, redundancia y seguridad, que garanticen la conectividad permanente y la integridad de los datos entre la sede principal y sus dos sucursales.

La propuesta contempla el uso de equipos de red de nivel empresarial, capaces de ofrecer mayor capacidad de procesamiento, estabilidad y gestión centralizada, además de la segmentación de la red mediante VLANs y la implementación de enlaces redundantes para asegurar la continuidad de los servicios ante posibles fallos. Estas mejoras tecnológicas permitirán optimizar el desempeño de la red, reducir los tiempos de inactividad y garantizar una comunicación eficiente y segura, acorde con las exigencias tecnológicas y operativas del sector comercial.

Interesados del Proyecto

A continuación, se detallan los interesados del presente proyecto:

- Gerente General
- Jefe de Sistemas
- Jefe de Administración
- Jefe de RR. HH
- Jefe de soporte TI

Alcance del Proyecto

El alcance del presente trabajo de aplicación profesional considera lo siguiente:

- Análisis de la situación actual de la red de la Empresa.
- Identificación del problema de la red.
- Selección de productos.

- Planteamiento de una solución, configuraciones, pruebas operativas.
- Estudio de costos

No se considera dentro del alcance del proyecto la implementación de la conectividad hacia las sucursales, ya que se solicitará una solución WAN privada al Proveedor de Internet; tampoco se incluye el cableado estructurado, la implementación de puntos eléctricos en los gabinetes, la configuración de servidores ni la evaluación técnica y económica de sistemas UPS.

Los productos esperados del proyecto incluyen la documentación técnica del diseño de red, el listado de equipos recomendados con su respectivo análisis de costo-beneficio, la propuesta de configuración de los dispositivos de red y los resultados de las pruebas operativas que validan la disponibilidad y rendimiento de la solución.

Capítulo II

Estudio de Mercado

Selección de Dispositivos de Red

El presente proyecto se centra en el diseño de una red LAN de alta disponibilidad, escalable y segura para una empresa de ventas con tres sedes ubicadas en la ciudad de Lima. La sede principal se encuentra en el distrito de La Molina (Central Tower), mientras que las sedes sucursales están ubicadas en el distrito de San Isidro (G4S y Orquídeas). El objetivo principal es garantizar una comunicación eficiente, estable y segura entre la sede principal y las sucursales, optimizando la conectividad interna y contribuyendo a la continuidad de las operaciones comerciales.

Para la selección de los equipos de red, se consideraron criterios técnicos, de rendimiento, soporte y costo-beneficio, buscando una solución equilibrada entre fiabilidad, escalabilidad y compatibilidad con la infraestructura existente. De acuerdo con la recomendación del área de sistemas y la solicitud del gerente de la empresa, se determinó la implementación de equipos Cisco Systems para el entorno LAN, debido a su alto desempeño, durabilidad y soporte técnico especializado. La experiencia previa de la organización demostró que los dispositivos Cisco presentan una mayor vida útil y estabilidad operativa en comparación con otras marcas utilizadas anteriormente.

Cisco Systems, Inc., empresa con sede en San José, California (EE. UU.), es líder mundial en el desarrollo de soluciones de conectividad y telecomunicaciones, destacando por su innovación y soporte integral. Además, mantiene alianzas estratégicas con fabricantes y desarrolladores de software reconocidos, como Intel, VMware, Red Hat, NetApp, SAP, Oracle y Microsoft, lo que permite una integración eficiente con diversas plataformas empresariales.

Para la interconexión entre las tres sedes, se ha considerado una solución de conectividad WAN privada provista por el proveedor de Internet, implementada bajo una arquitectura Hub and Spoke. En este esquema, la sede principal ubicada en Lima, distrito de La Molina (Central Tower) actúa como nodo central, mientras que las sedes sucursales ubicadas en San Isidro (G4S y Orquídeas) funcionan como nodos remotos, permitiendo una comunicación eficiente y administrada entre las distintas ubicaciones.

Asimismo, se ha definido la implementación de firewalls de la marca Fortinet, específicamente dispositivos FortiGate, los cuales estarán ubicados únicamente en la sede principal y cumplirán funciones de seguridad perimetral, tales como el control y restricción de accesos, el filtrado de tráfico hacia páginas web y redes no autorizadas, y la aplicación de políticas de seguridad para la protección de la red interna y la información corporativa

Figura 1

Estudio de marcas líderes de equipos de Red



Nota. Fuente www.gartner.com

La elección de Fortinet se basa en su reconocimiento internacional en seguridad de redes, respaldado por estudios de Gartner Inc., lo que, en conjunto con la tecnología Cisco en la capa LAN, permite un diseño de red alineado con los objetivos del proyecto y la metodología PPDIOO.

Selección de Software de Monitoreo de Red

Se realizó un estudio del mercado, con la finalidad de elegir el mejor software de monitoreo de red que se adapte a las necesidades de la empresa de ventas. Debido a ello, nos enfocamos en que este software sea flexible, fácil de administrar y eficiente. Asimismo, nos debe permitir garantizar la estabilidad de los servicios de red.

En la tabla 2, se muestra un cuadro comparativo entre el software de monitoreo de red PRTG Network Monitor y Zabbix

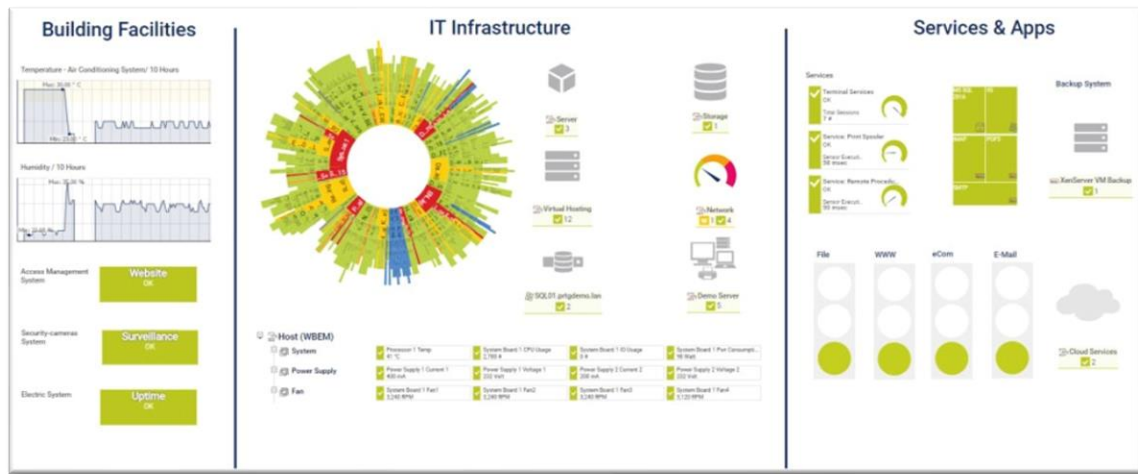
Tabla 2

Tabla de Comparación – Software Monitoreo

Características	PRTG Network Monitor	Zabbix
Ancho de banda	Monitorizado	Monitorizado
Base de datos	Monitorizado	Monitorizado
Aplicaciones	Monitorizado	Monitorizado
Servidores	Monitorizado	Monitorizado
LAN	Monitorizado	Monitorizado
GUI	Si	Si
Instalación	Sencilla	Compleja
Administración	Sencilla	Compleja

El software para el Monitoreo de Red a elegir fue PRTG Network Monitor, dado que, nos permite supervisar toda la infraestructura de red de la empresa de ventas. Además, nos permite tener una visión global del rendimiento y estado de la red. Asimismo, nos permite asegurar la disponibilidad de todos los componentes críticos que puedan afectar el negocio y mitigarlos para una mejor productividad.

A continuación, se mostrará una imagen del software de monitoreo PRTG.

Figura 2*PRTG Network Monitor*

Cuadros Comparativos de Fabricantes de Dispositivos de Red

Los switches son equipos de red que se utilizan para interconectar diversos equipos dentro de una misma red.

En la tabla 3, se muestra un cuadro comparativo entre 2 switches de diferentes fabricantes investigados en nuestro análisis de mercado para el switch que se va a implementar en la capa de acceso.

Tabla 3*Cuadro Comparativo de Switches – Capa de Acceso*

Características	C1300-48T-4G	HPE Aruba CX 6000
Puertos:	48x10/100/1k GB	48 x Gigabit RJ-45 con PoE/PoE+
Port SFP:	4 x Gb SFP	4 x Gb SFP
Numero de VLANs:	4096	4096
Rendimiento:	77.38 Mpps	130.94 Mpps
Tablas de direcciones MAC:	16k	16k
Capa del interruptor:	L2	L2/L3 ligera (capas de enrutamiento básicas)
Memoria DRAM:	1 GB DDR4	512 MB
Memoria Flash:	512 MB	4 GB
Admite PoE:	NO PoE+	Si PoE+
Costo	Medio	Alto

Selección de Switch de Acceso

De acuerdo con la tabla comparativa realizada entre los modelos Cisco C1300-48T-4G y HPE Aruba CX 6000 48G PoE 4SFP (R8N85A), se selecciona el switch HPE Aruba CX 6000 48G PoE como dispositivo de acceso para el proyecto. Esta elección se fundamenta en que el modelo Aruba ofrece las capacidades necesarias para el entorno de la empresa, incluyendo 48 puertos Gigabit con soporte PoE/PoE+, 4 uplinks SFP, soporte de múltiples VLANs y funcionalidades de capa 3 administrable, cumpliendo los requerimientos de segmentación, rendimiento y gestión de la red.

Si bien el Cisco C1300-48T-4G es un equipo confiable para entornos de oficina, su falta de soporte PoE limita la alimentación directa de teléfonos IP, puntos de acceso y otros dispositivos PoE, lo que implicaría soluciones adicionales. En cambio, el HPE Aruba CX 6000 48G PoE integra esta funcionalidad, ofreciendo una relación costo-beneficio más adecuada y permitiendo garantizar el desempeño, seguridad y escalabilidad requeridos sin incrementar innecesariamente el presupuesto del proyecto.

En la Figura 2, se presenta el switch HPE Aruba CX 6000 48G PoE 4SFP (R8N85A), seleccionado de acuerdo con la evaluación comparativa realizada y los requerimientos técnicos definidos para la capa de acceso.

Figura 3

Switch - HPE Aruba CX 6000– R8N85A



Tabla 4*Cuadro Comparativo de Switches L3*

Características	C9300-48T-A	WS-C3750X-24P-S	CX 6200M 24G
Puertos	48	24	24
Port SFP:	No	4	4
Número de VLANs:	4094	1005	4094
Rendimiento de Renvío:	190.48 Mpps	65.5 Mpps	95.2 Mpps
Capacidad de conmutación:	256 Gbps	160 Gbps	128 Gbps
Soporte SVI:	Si	Si	Si
Tabla de Direcciones MAC:	32000	12000	32000
Capa de interruptor:	L2 / L3	L3	L3
Admite PoE:	No	Si	No

Selección de Switch de Capa3

De acuerdo con la tabla comparativa, se seleccionan los switches Cisco Catalyst C9300-48T-A y Aruba CX 6200M 24G 4SFP+ como equipos de Capa 3, debido a su alta capacidad de conmutación, soporte para hasta 4094 VLANs y funcionalidades avanzadas de enrutamiento. El Cisco Catalyst C9300-48T-A, con sistema operativo IOS XE, destaca por su diseño robusto, escalable y su capacidad para operar en el núcleo de la red, mientras que el Aruba CX 6200M, basado en AOS-CX, resulta adecuado para la capa de distribución, ofreciendo un balance entre rendimiento y eficiencia. Estas características permiten garantizar una infraestructura confiable y escalable para la implementación del proyecto en la sede principal.

A continuación, se mostrará imágenes de los switches:

Figura 4*Cisco C9300-48T-A*

Figura 5*HPE Aruba CX 6200M 24G 4SFP+*

En el presente proyecto, para la interconexión de las sucursales se utilizará el HPE Aruba CX 6200M 24G 4SFP+. Este switch ya se encontraba implementado en la sede principal y será reutilizado en una de las sucursales, mientras que se adquirirá un equipo adicional para la segunda sucursal.

Comparación de Fabricantes Firewall

Para la selección del firewall, se realiza una comparación entre 3 modelos de los siguientes: Sophos (XGS 133), Fortinet (FortiGate 100F) y Fortinet (FortiGate 60F). Los detalles comparativos se presentan a continuación.

Tabla 5*Comparación de fabricantes Firewall*

Modelo	Sophos, XGS 136	FORTIGATE 60F	FORTIGATE 100F
Conectividad	10 × GE cobre + 2 × 2.5 GE cobre + 2 × SFP (según SKU exacto).	10 × GE RJ-45 (incluye 2 WAN, 1 DMZ, 7 internas)	22 × GE RJ-45 (incluye 2 × WAN, 1 × DMZ, 1 × Mgmt, 2 × HA) + 4 × SFP + 2 × 10 GE SFP+ (FortiLink)
Rendimiento	Firewall throughput ≈ ~11.5 Gbps (publicado por fabricante/distribuidores)	Firewall: ~10 Gbps (1518 byte) / ~10 Gbps (512 byte) / ~6 Gbps (64 byte) VPN IPsec: ~6.5 Gbps	Firewall: ~20 Gbps (1518 byte) / ~18 Gbps (512 byte) / ~10 Gbps (64 byte) VPN IPsec: ~11.5 Gbps
Costo	Alto	S/1989	S/7199

Selección de Firewall

Para la selección del firewall, Fortinet FortiGate se considera una solución de nueva generación (NGFW) ampliamente reconocida por su rendimiento, escalabilidad y enfoque

integral en la seguridad. Este dispositivo integra múltiples funciones de protección, como inspección profunda de paquetes (DPI), prevención de intrusiones (IPS), filtrado web, control de aplicaciones y VPN (IPsec/SSL) en una sola plataforma, permitiendo una gestión centralizada y eficiente de la seguridad perimetral.

De acuerdo con la comparativa técnica entre diversos fabricantes, se selecciona el modelo FortiGate 60F por su rendimiento. Este ofrece un rendimiento de hasta 10 Gbps, ideal para sucursales medianas.

Figura 6

Fortinet - FortiGate 60F



Capítulo III

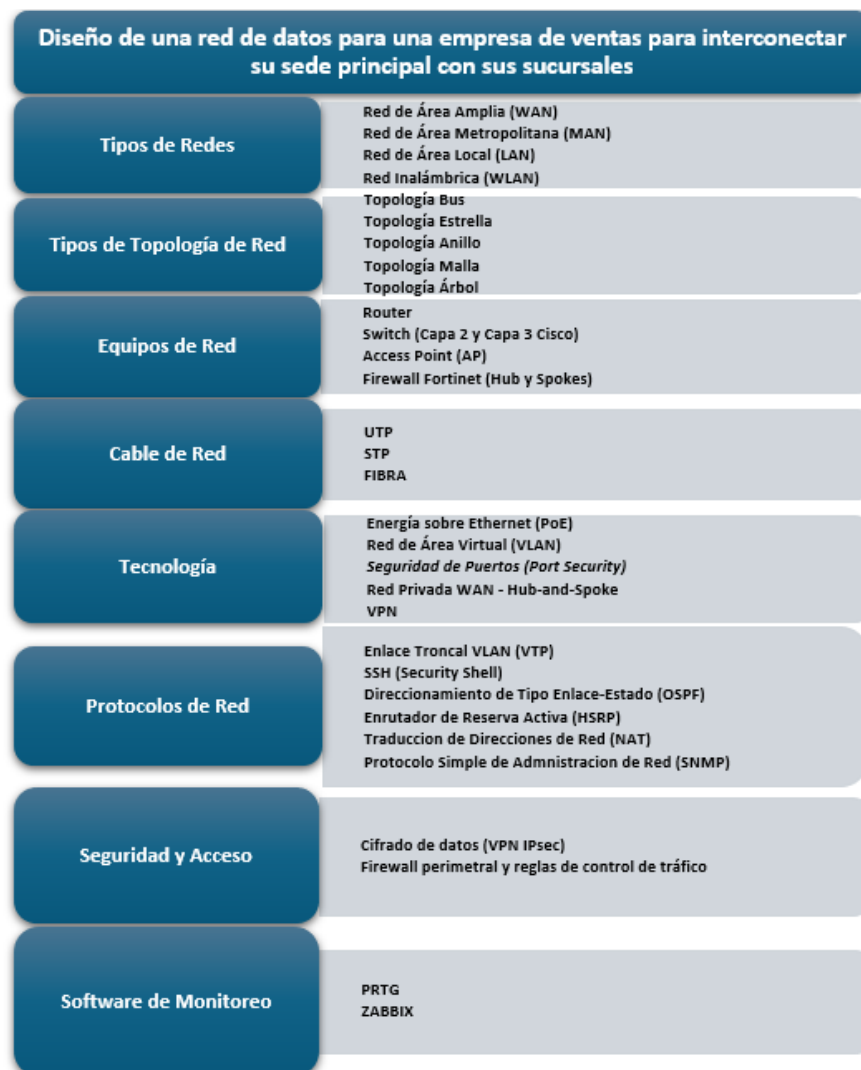
Estudio Técnico

Marco Teórico

En este capítulo se presentan los conceptos y fundamentos teóricos que sustentan el diseño e implementación de redes de comunicación empresariales.

Figura 7

Mapa conceptual del trabajo de aplicación



La información se recopiló a partir de bibliografía especializada y documentación técnica, y constituye la base conceptual para el desarrollo de una red LAN de alta

disponibilidad y la interconexión segura entre las sedes de la empresa. Finalmente, se incluye un mapa conceptual que sintetiza los elementos principales de la arquitectura propuesta.

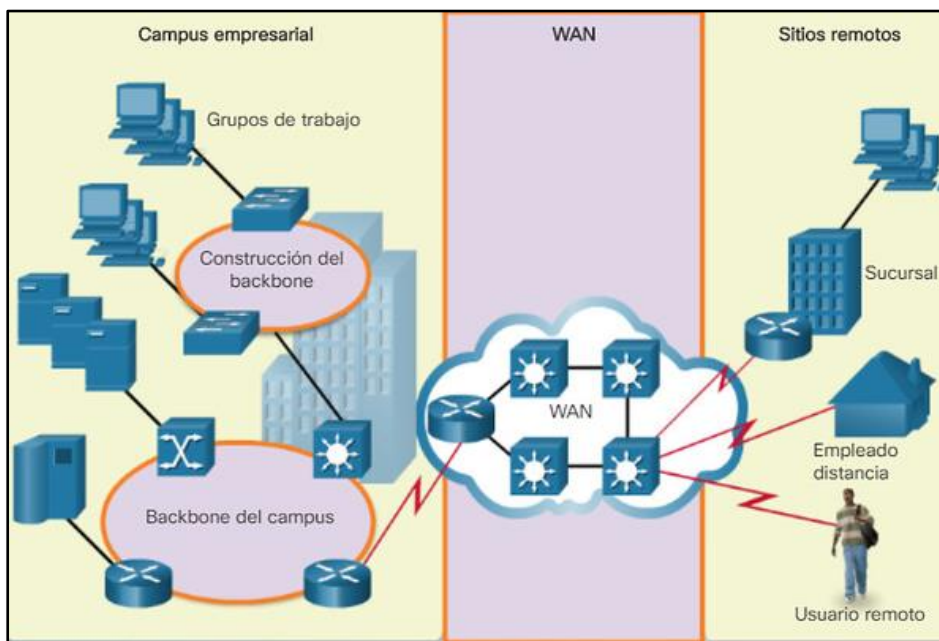
Tipos de Redes

Red de Área Amplia (WAN)

Una red de área amplia (WAN), es una red que interconecta diversas redes LAN que se encuentran en distintos lugares geográficos como regiones, ciudades y países. Estas redes son creadas por diversas organizaciones o empresas, tales como los proveedores de servicio de internet (ISP), que hacen posible la instalación de redes WAN en todo el mundo.

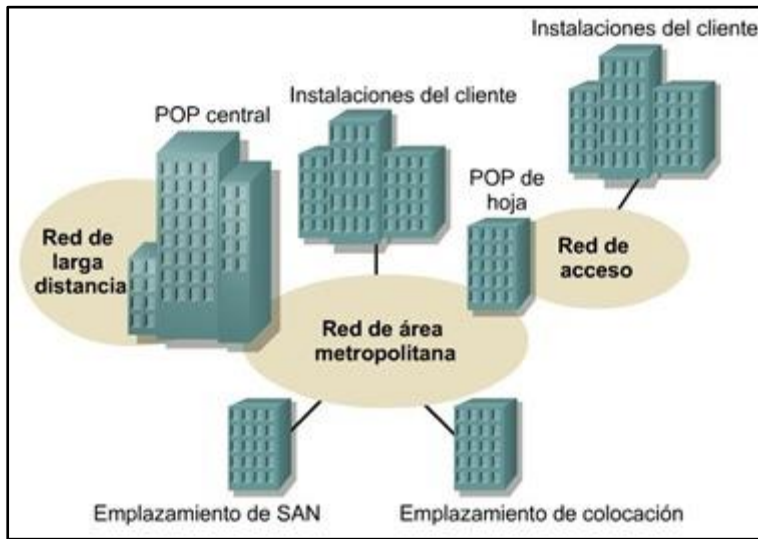
Figura 8

Red de Área WAN

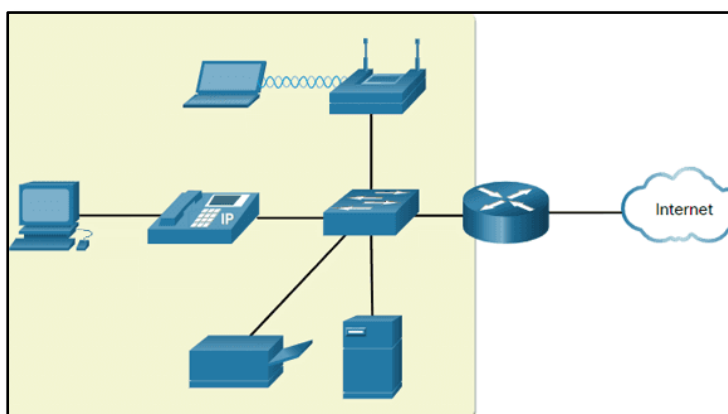


Red de Área Metropolitana (MAN)

Una red de área metropolitana (MAN) conecta varias redes locales (LAN) dentro de una ciudad o región cercana. Su objetivo es facilitar la comunicación y el intercambio de datos entre oficinas o sucursales cercanas. Proporciona velocidades de transmisión más altas que una WAN y mayor cobertura que una LAN. Es ideal para organizaciones que necesitan interconectar múltiples sedes dentro de un área urbana.

Figura 9***Red de Área Metropolitana******Red de Área Local (LAN)***

Una red de área local (LAN) facilita la interconexión y comunicación entre distintos dispositivos dentro de un espacio limitado, como hogares, oficinas o empresas. Su alcance es menor en comparación con redes de mayor cobertura, como las WAN. Estas redes suelen conectarse mediante medios físicos, siendo el cable Ethernet el más comúnmente utilizado.

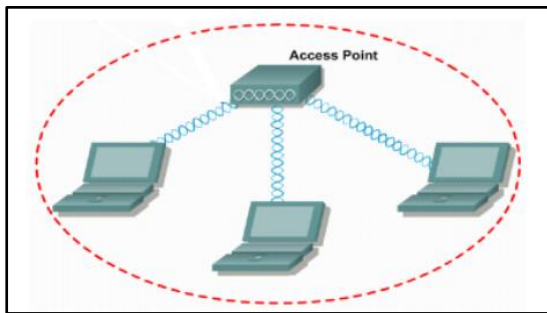
Figura 10***Red de Área Local******Red de Área Local Inalámbrica (WLAN)***

Una red de área local inalámbrica permite la interconexión de múltiples dispositivos mediante la tecnología Wi-Fi, transmitiendo datos a través de señales de radiofrecuencia. Este

tipo de red se utiliza principalmente en entornos domésticos, oficinas y organizaciones empresariales.

Figura 11

Red de Área local Inalámbrica



Tipos de Topologías de Red

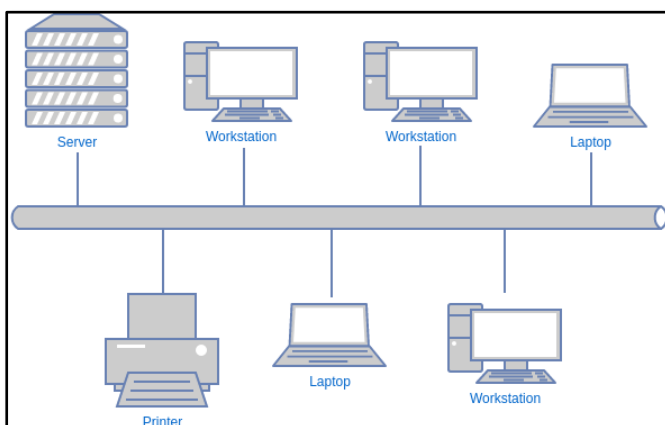
Las topologías de red nos permiten comprender el estado actual en el que se encuentra diseñada una red, este diseño puede estar planteado de forma física o lógica.

Topología Bus

La topología Bus organiza todos los equipos sobre un mismo canal físico que funciona como vía principal de transmisión. Cada dispositivo comparte ese medio y envía o recibe información según corresponda. Aunque su diseño es simple, depende totalmente del cable central y su rendimiento disminuye cuando hay muchos equipos, por lo que hoy solo se estudia con fines conceptuales.

Figura 12

Topología de red - Bus

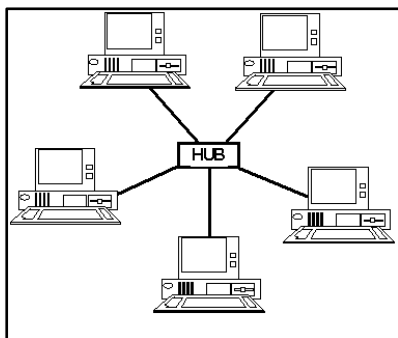


Topología Estrella

En este tipo de topología, todos los dispositivos se enlazan directamente a un equipo central, normalmente un switch. Este componente actúa como punto de coordinación del tráfico y permite administrar la red de forma más ordenada. Es la estructura más utilizada en redes actuales porque facilita la detección de fallas y evita que un problema en un dispositivo afecte a los demás. Solo la interrupción del equipo central podría comprometer toda la red.

Figura 13

Topología de red – Estrella

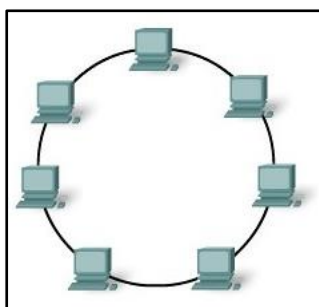


Topología Anillo

La topología Anillo une cada equipo con el siguiente hasta formar un circuito cerrado por donde circulan los datos. La información avanza pasando por cada nodo hasta llegar al destinatario. Su funcionamiento reduce el desorden del tráfico, pero tiene un inconveniente: si un punto del anillo presenta fallas, toda la comunicación puede interrumpirse, a menos que se utilicen mecanismos de doble anillo o protección.

Figura 14

Topología de red – Anillo

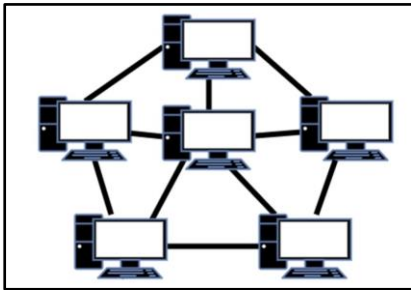


Topología Malla

En la topología Malla los equipos cuentan con múltiples rutas de conexión entre sí, lo que genera varios caminos posibles para llegar a un destino. Esta característica les otorga una gran tolerancia a fallos, ya que la red puede seguir operando, aunque uno de los enlaces se caiga. No obstante, implementar una malla completa requiere muchos cables y configuraciones adicionales, por lo que comúnmente se aplica en forma parcial en entornos empresariales.

Figura 15

Topología de red - Malla

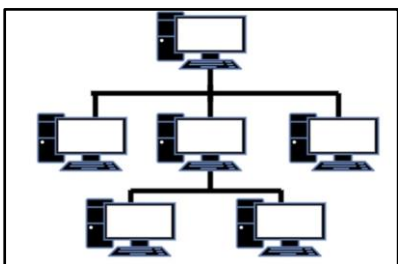


Topología Árbol

La topología Árbol plantea una estructura por niveles: en la parte superior se encuentran los dispositivos de mayor jerarquía y, a partir de ellos, se ramifican segmentos que conectan a más equipos. Esta organización facilita la expansión de la red y es típica en redes LAN modernas, ya que permite dividir la infraestructura en capas (núcleo, distribución y acceso) para administrar mejor el tráfico y el crecimiento.

Figura 16

Topología de red - Árbol



Tipos de Equipo de Red

Router

Los routers son dispositivos avanzados que permiten interconectar redes ubicadas en diferentes áreas geográficas y requieren administración especializada para garantizar un enrutamiento eficiente del tráfico.

Figura 17

Equipo de red - Router



Switch

Un switch es un dispositivo de red que conecta múltiples equipos dentro de una misma LAN, permitiendo la comunicación eficiente entre ellos. Su función principal es facilitar la creación de redes locales y ofrecer escalabilidad al incorporar nuevos dispositivos sin afectar el rendimiento.

Figura 18

Equipo de red - Switch



Access Point (AP)

Es un dispositivo de red que permite la conexión de equipos inalámbricos a la red LAN, utilizando tecnología Wi-Fi para proporcionar acceso y extender la cobertura inalámbrica.

Figura 19

Equipo de red – Access Point



Firewall

Es un dispositivo o sistema de seguridad que controla el tráfico de red, permitiendo o bloqueando comunicaciones según políticas definidas, con el fin de proteger la infraestructura informática frente a accesos no autorizados y amenazas externas.

Figura 20

Equipo de red – Firewall



Cable de Red

Los cables de red se utilizan como medio físico para la comunicación segura entre distintos equipos, como routers, switches y computadoras. A diferencia de la fibra óptica,

están compuestos por cuatro pares de hilos de cobre trenzado, lo que les proporciona mayor flexibilidad y permite la transmisión de datos mediante pulsos eléctricos. En la categoría 6 se incorporó un separador interno para reducir la diafonía y las interferencias electromagnéticas (EMI). Aunque externamente los cables pueden parecer similares, existen diversas categorías que difieren en capacidad y rendimiento.

A continuación, se presentará un cuadro comparativo con las diferencias que existen entre las categorías presentadas.

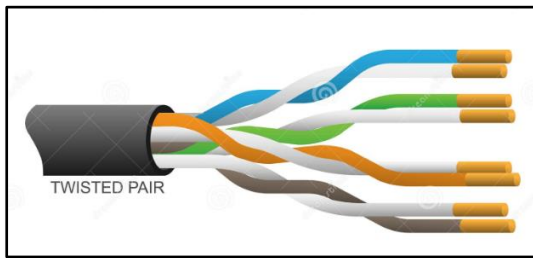
Figura 21

Comparativo de categoría de cable de red

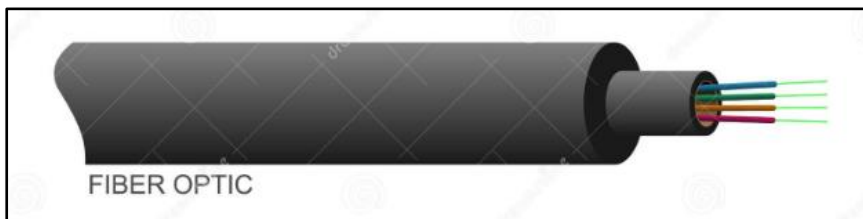
 ETHERNET CAT 5 Velocidad: 100 Mbps Frecuencia: 100 Mhz Descarga: 15.5 MB/s	 ETHERNET CAT 5e Velocidad: 1 000 Mbps Frecuencia: 100 Mhz Descarga: 150.5 MB/s
 ETHERNET CAT 6 Velocidad: 1 000 Mbps Frecuencia: 250 Mhz Descarga: 150.5 MB/s	 ETHERNET CAT 6A Velocidad: 10 000 Mbps Frecuencia: 500 Mhz Descarga: 1.250 MB/s ó 1,25 GB/s
 ETHERNET CAT 7 Velocidad: 10 000 Mbps Frecuencia: 600 Mhz Descarga: 1.25 GB/s	 ETHERNET CAT 7A Velocidad: 10 000 Mbps Frecuencia: 1 000 Mhz Descarga: 1.25 GB/s

Par Trenzado

Es un medio de transmisión compuesto por hilos de cobre entrelazados por pares, utilizado principalmente en redes LAN. Su diseño reduce las interferencias electromagnéticas y permite la transmisión de datos mediante señales eléctricas a diferentes velocidades según su categoría.

Figura 22*Cable de red – Par Trenzado***Fibra Óptica**

Es un medio de transmisión basado en hilos de vidrio o plástico que transportan datos mediante pulsos de luz. Ofrece altas velocidades, baja atenuación y es ideal para conexiones de larga distancia y entornos que requieren gran ancho de banda.

Figura 23*Cable de red - Fibra***Tecnología**

A pesar de contar con recursos económicos limitados, las microempresas deben considerar la mejora de las tecnologías utilizadas en su infraestructura de red LAN. Esto permitirá optimizar el rendimiento y garantizar una mayor disponibilidad de los servicios de red. Además, a largo plazo, reducirán los costos asociados a nuevas implementaciones y disminuirán las pérdidas económicas ocasionadas por fallas o interrupciones en los servicios de conectividad.

Energía Sobre Ethernet (POE)

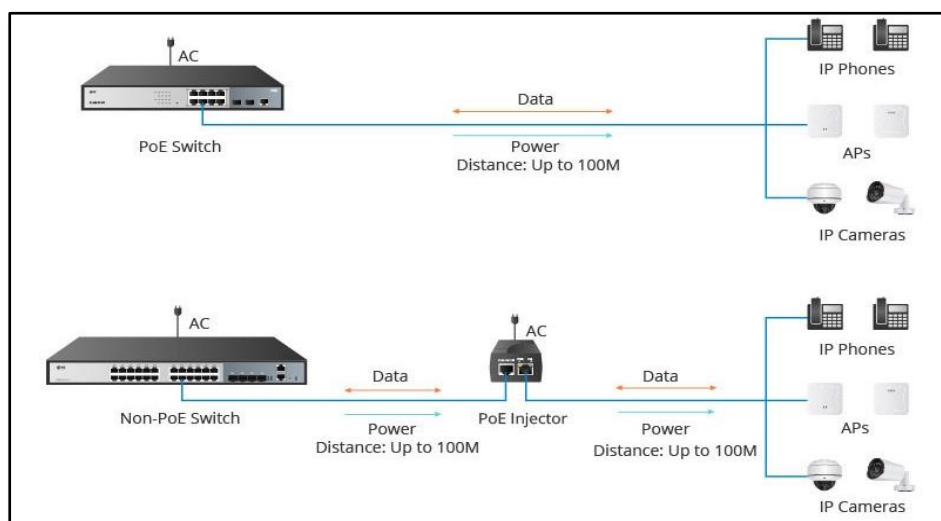
Es La tecnología Power over Ethernet (PoE), estandarizada por el IEEE en el año 2003, permite transmitir simultáneamente energía eléctrica y datos a través de un mismo

cable Ethernet. Gracias a ello, dispositivos como teléfonos IP, cámaras de seguridad y puntos de acceso pueden alimentarse sin necesidad de adaptadores de corriente adicionales, lo que reduce costos de instalación y simplifica el despliegue de la infraestructura. El suministro de energía PoE puede provenir de un switch PoE activo, capaz de negociar automáticamente la potencia adecuada para cada dispositivo, o de un inyector PoE. Sin embargo, el uso de inyectores pasivos puede resultar riesgoso debido a que no regulan ni negocian el voltaje suministrado. Por ello, se recomienda emplear switches PoE activos, ya que garantizan un suministro de energía seguro y compatible con los equipos conectados.

En la figura 23, se presenta una imagen en la cual se puede visualizar cómo funciona la tecnología POE utilizando un switch o un inyector POE.

Figura 24

Tecnología POE – Switch Pasivo y Activo

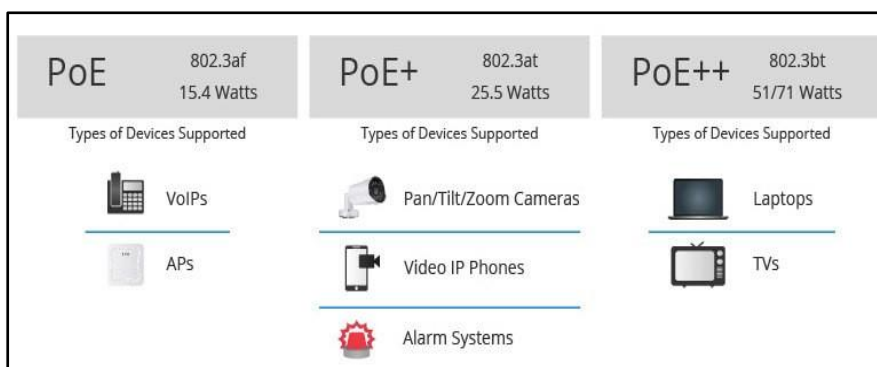


La tecnología PoE cuenta con varios estándares definidos por el IEEE. El primero de ellos es 802.3af, introducido en 2003, el cual permite suministrar energía a dispositivos de bajo consumo, como teléfonos IP y puntos de acceso inalámbrico. Posteriormente, en 2009 se publicó el estándar 802.3at, conocido como PoE+, diseñado para equipos que requieren mayor potencia, tales como cámaras IP de mayor capacidad, teléfonos de videoconferencia y ciertos sistemas de seguridad. El estándar más reciente es 802.3bt, también denominado

PoE++, establecido en 2018. Este ofrece niveles de potencia significativamente superiores, orientados a dispositivos que demandan un consumo energético elevado. Sin embargo, debido a su reciente incorporación al mercado, aún no es ampliamente adoptado por los fabricantes de equipos de red. Cabe mencionar que, al estar basado en la infraestructura Ethernet, PoE mantiene la limitación típica de esta tecnología: la distancia máxima entre el switch PoE y el dispositivo conectado no debe exceder los 100 metros.

Figura 25

Tecnología POE – Tipos de Equipos Soportados

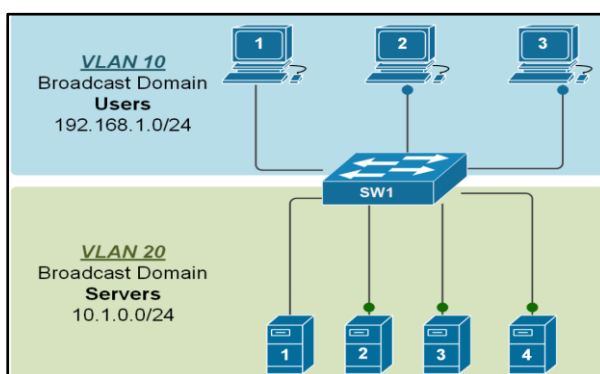


Red de Área Local Virtual (VLAN)

Es una red lógica que se crea dentro de la misma infraestructura física con el fin de separar el tráfico en grupos independientes. Esta segmentación permite organizar la red por áreas o funciones, mejorar la seguridad, reducir el dominio de broadcast y optimizar el desempeño general de la red sin necesidad de instalar más equipos físicos.

Figura 26

Segmentos de VLANs

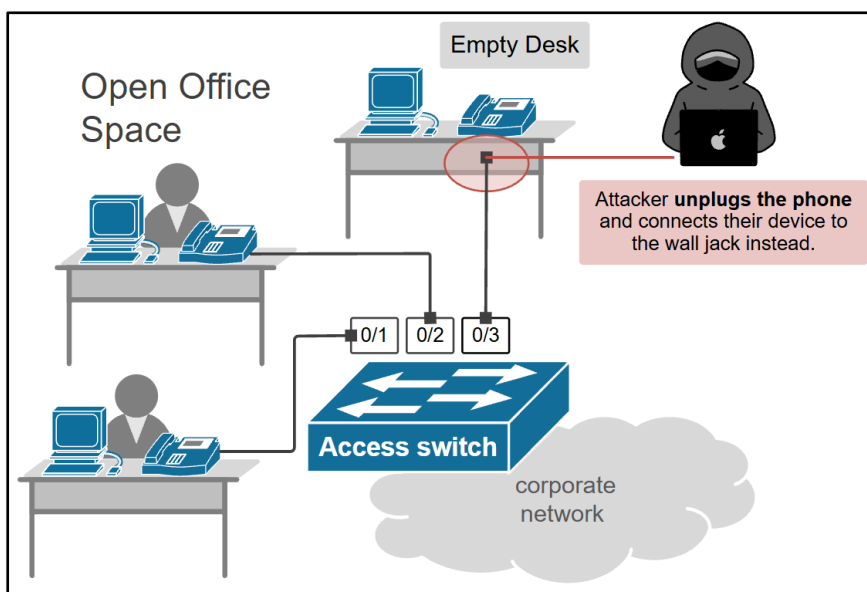


Seguridad de Puertos (Port Security)

Es un mecanismo de seguridad utilizado en switches que permite controlar qué dispositivos pueden conectarse a un puerto específico mediante la restricción de direcciones MAC. Esta tecnología ayuda a prevenir accesos no autorizados, limitar ataques de suplantación y fortalecer la protección de la red, permitiendo definir cuántas y cuáles direcciones MAC pueden asociarse a cada puerto.

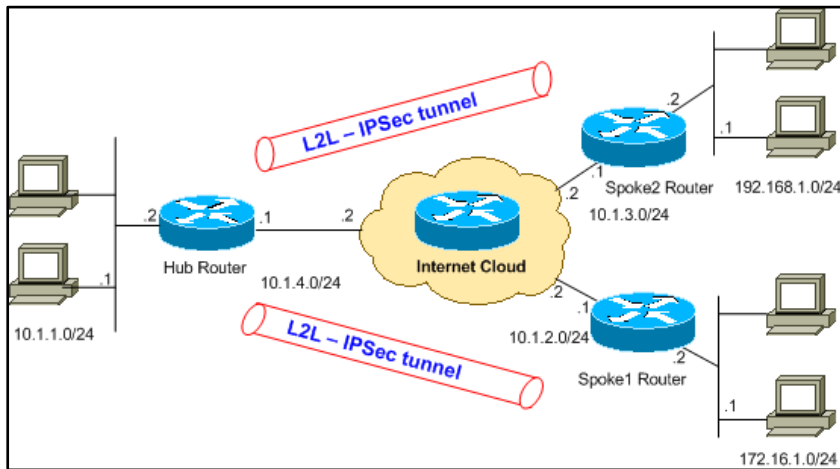
Figura 27

Seguridad de Puertos (Port Security)

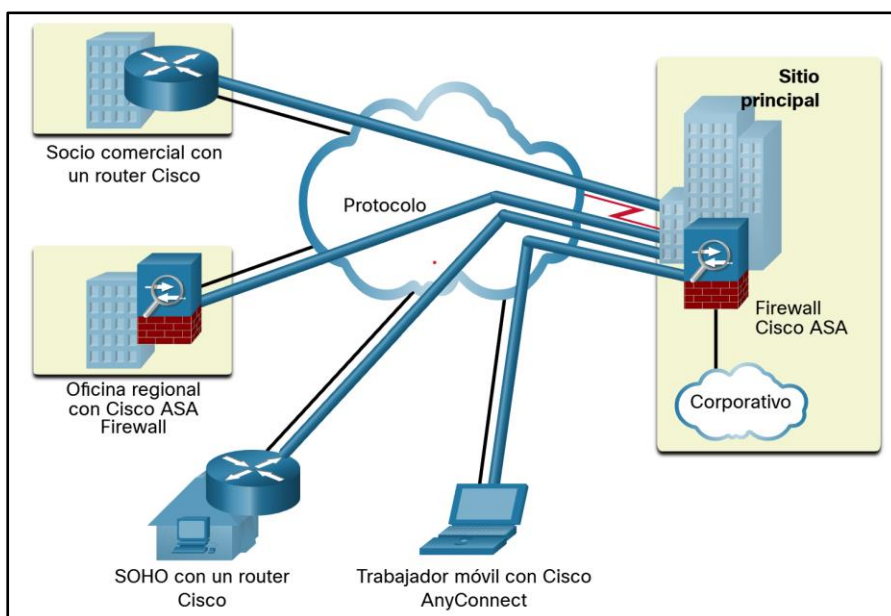


Red Privada WAN - Hub-and-Spoke

Es una arquitectura de red que permite interconectar de manera privada y segura una sede principal con múltiples sucursales mediante enlaces dedicados o virtuales. Su función principal es centralizar el tráfico de las oficinas remotas hacia un nodo central (“hub”), desde donde se gestionan la comunicación, el acceso a aplicaciones y la seguridad de los datos. Esta topología facilita la administración y el control de la red, permitiendo que las sucursales se conecten a los recursos corporativos de manera confiable, aunque la comunicación entre sucursales siempre pasa por el hub, garantizando una gestión uniforme de la información.

Figura 28*Tecnología – WAN Privada (Hub and Spoke)***Red Privada Virtual (VPN)**

Es una tecnología que permite crear una conexión segura y cifrada a través de redes públicas, como Internet. Su función principal es establecer un túnel privado que garantice la confidencialidad, integridad y autenticidad de los datos, permitiendo que sedes, sucursales o usuarios remotos accedan a los recursos internos de una organización como si estuvieran físicamente dentro de la red corporativa.

Figura 29*Tecnología - VPN*

Protocolos de Red

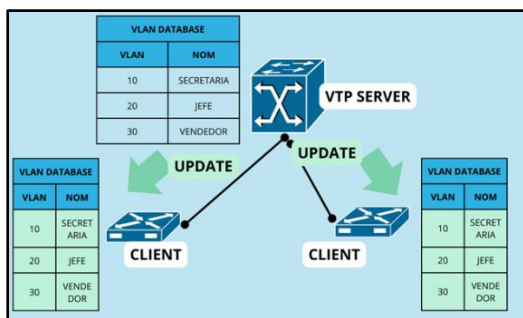
A continuación, se presentarán los protocolos que se implementarán en el presente proyecto.

Protocolo de Enlace Troncal de VLAN (VTP)

Este protocolo utilizado en redes con switches Cisco nos permite administrar de forma centralizada la creación, modificación y eliminación de VLANs. Su función es distribuir automáticamente la información de VLAN entre los switches pertenecientes al mismo dominio, evitando configuraciones manuales repetitivas y reduciendo errores de administración.

Figura 30

Protocolo de Enlace Troncal - VTP

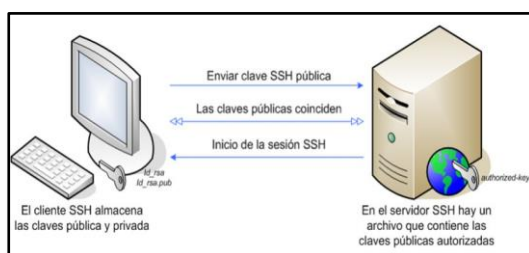


Protocolo Seguro de Caparazón (SSH)

Es un protocolo que permite acceder y administrar dispositivos de red o servidores de forma remota de manera segura. Utiliza técnicas de cifrado para proteger la comunicación, evitando que la información sea interceptada o modificada durante la conexión.

Figura 31

Protocolo Seguro de Caparazón -SSH

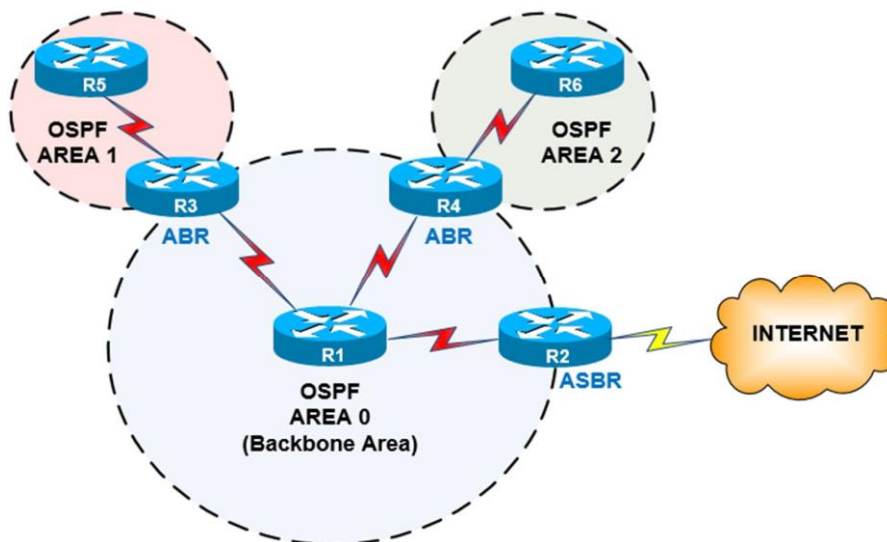


Protocolo de Direccionamiento de Tipo de Enlace-Estado (OSPF)

El protocolo OSPF (Open Shortest Path First) es un protocolo de enrutamiento de tipo estado de enlace que permite administrar el tráfico dentro de una red de manera eficiente, escalable y segura. Su diseño ofrece compatibilidad entre diferentes fabricantes, lo que facilita su implementación en entornos con equipos heterogéneos. OSPF es capaz de identificar rápidamente cualquier cambio en la topología dentro de un mismo Sistema Autónomo y recalcular rutas óptimas sin generar bucles, proporcionando así una visión precisa y actualizada del estado completo de la red.

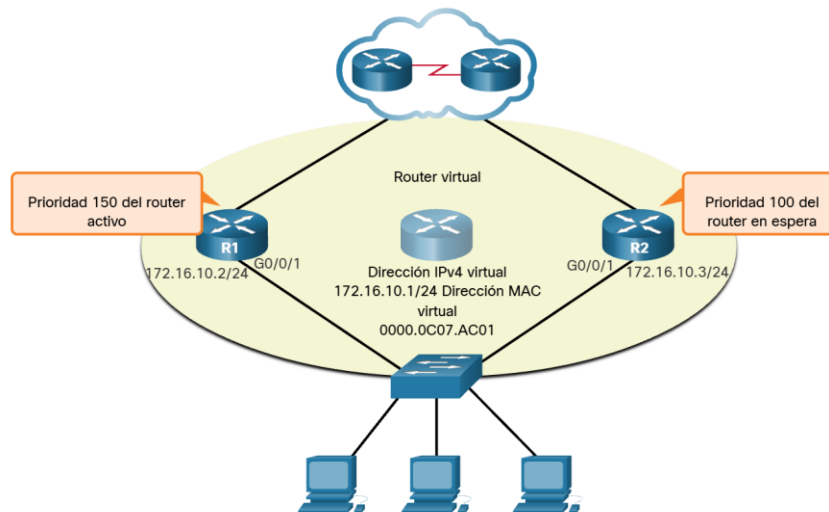
Figura 32

Protocolo de Direccionamiento de Tipo Enlace-Estado (OSPF)

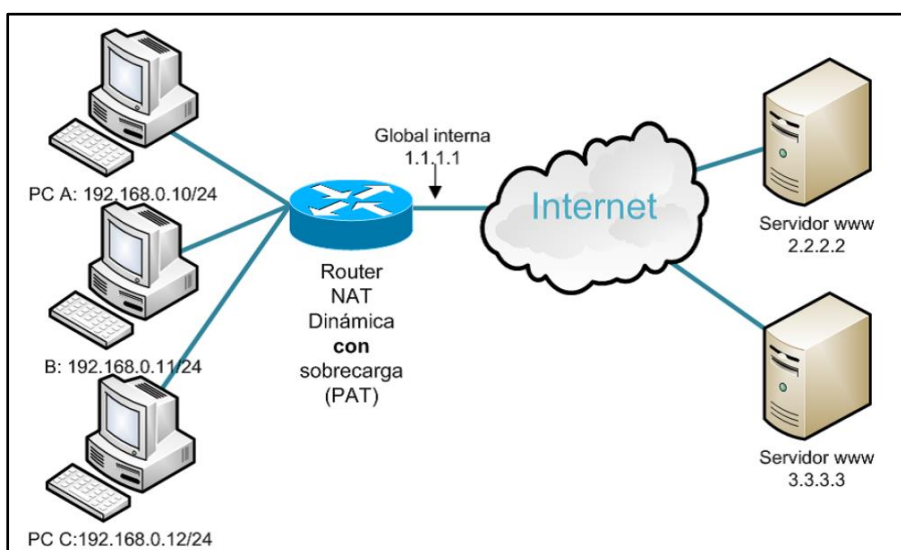


Protocolo de Enrutador de Reserva Activa (HSRP)

El protocolo HSRP es un mecanismo de redundancia desarrollado por Cisco que permite asegurar la disponibilidad del enrutamiento en una red. Para ello, varios routers trabajan de manera conjunta formando un grupo, en el cual uno actúa como router activo y otro como respaldo. Si el router activo falla, el router en espera asume automáticamente la función de reenvío de paquetes, garantizando la continuidad del servicio sin interrupciones para los usuarios.

Figura 33*Protocolo de Enrutador de Reserva Activa (HSRP)**Protocolo de Traducción de Direcciones de Red (NAT)*

Es un mecanismo que permite modificar las direcciones IP en los paquetes que viajan entre una red interna y la red externa. Su función principal es permitir que varios dispositivos dentro de una red privada accedan a Internet utilizando una única dirección IP pública. Además, contribuye a la seguridad al ocultar las direcciones internas y optimiza el uso del espacio disponible de direcciones IPv4.

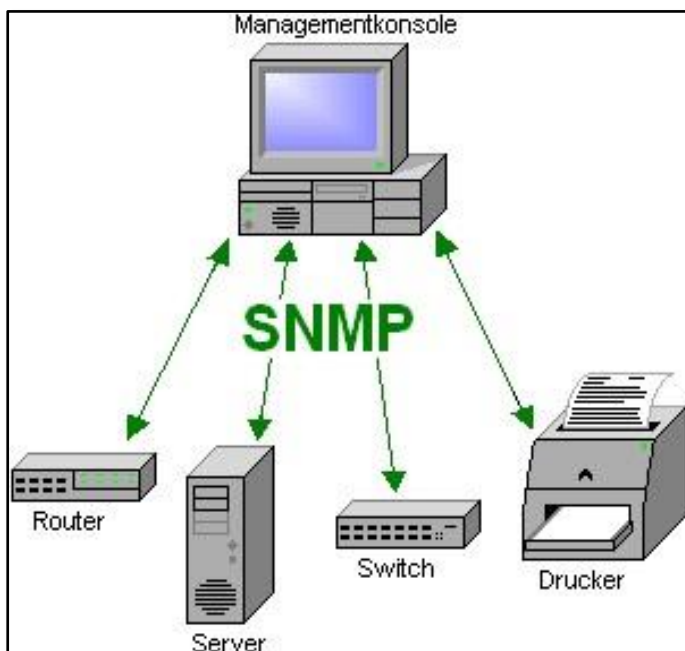
Figura 34*Protocolo de Traducción de Direcciones de Red (NAT)*

Protocolo Simple de Administración de Red (SNMP)

SNMP es un protocolo que facilita el intercambio de información de administración entre los dispositivos de red. En la actualidad cuenta con distintas versiones, entre ellas podemos encontrar la versión SNMPv1, SNMPV2 y SNMPv3. La versión de SNMP3 es la más recomendada por su seguridad, pero a su vez es un poco más tediosa de configurar. Este protocolo es muy usado por los softwares de monitoreo de red, tales como PRTG, Nagios, Zabbix, etc.

Figura 35

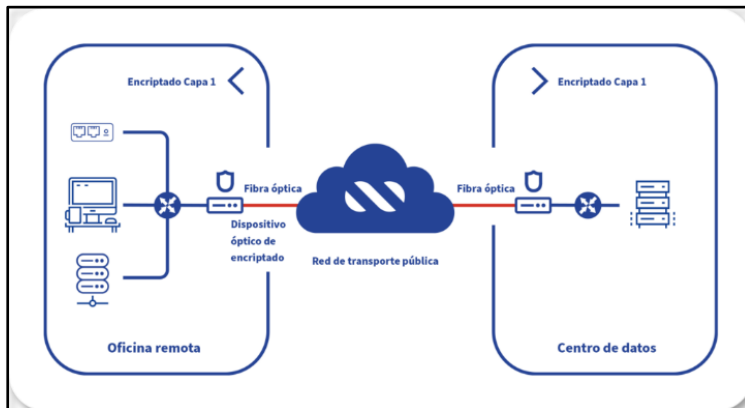
Protocolo Simple de Administración de Red (SNMP)



Seguridad y Acceso

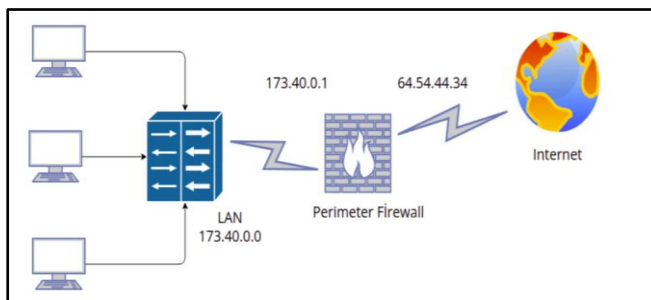
Cifrado de Datos (VPN IP Sec)

La VPN IPsec es una tecnología que permite crear comunicaciones seguras a través de Internet mediante el cifrado de los datos. Su función es proteger la información mientras viaja entre dos puntos, evitando que sea interceptada o modificada. Es ampliamente utilizada para conectar de forma segura sedes remotas, usuarios móviles o dispositivos corporativos.

Figura 36*Seguridad y acceso – Cifrado de datos (VPN IPSec)*

Firewall Perimetral

Un firewall perimetral es un dispositivo que se ubica en el borde de la red para protegerla del tráfico no autorizado proveniente de Internet u otras redes externas. Su funcionamiento se basa en reglas que permiten, bloquean o inspeccionan el tráfico según políticas de seguridad definidas, garantizando un acceso controlado y reduciendo amenazas.

Figura 37*Seguridad y Acceso – Firewall Perimetral*

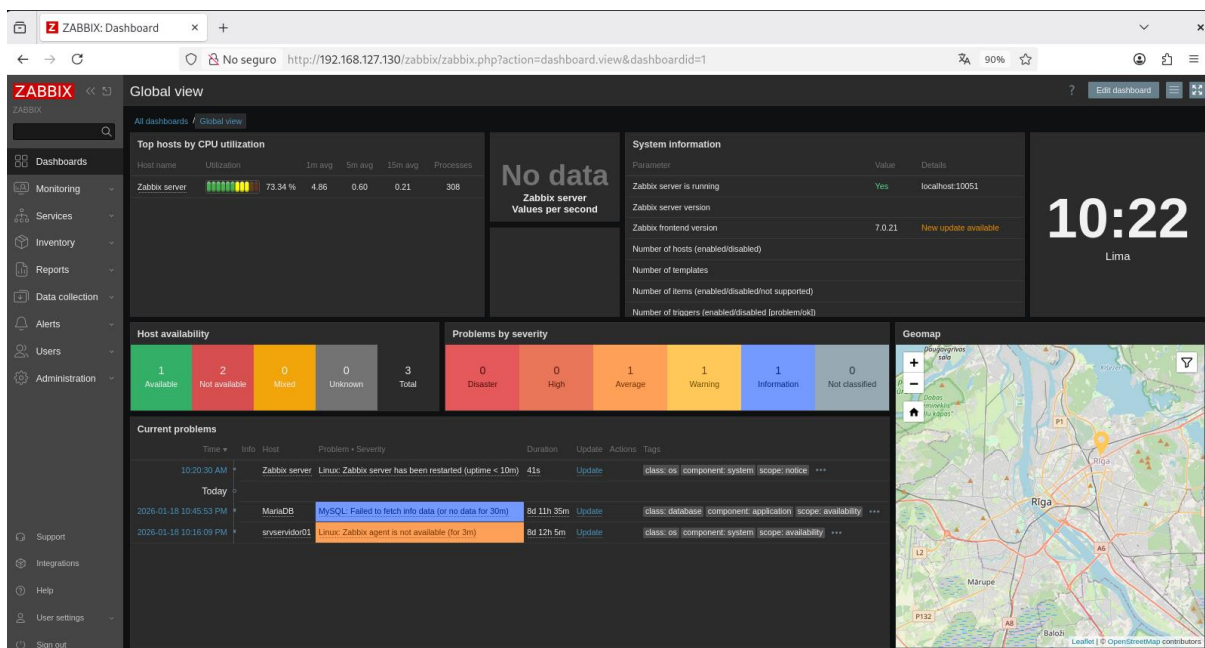
Software de Monitoreo

PRTG

PRTG Network Monitor es una herramienta de monitoreo que supervisa el estado, disponibilidad y rendimiento de dispositivos y servicios de red mediante sensores. Permite detectar fallas rápidamente y generar alertas en tiempo real.

Figura 38*Software de Monitoreo – PRTG Network Monitor***Zabbix**

Zabbix es una plataforma de monitoreo de código abierto que permite vigilar servidores, redes y aplicaciones. Ofrece gráficos, alertas y paneles de control, facilitando la detección de problemas de capacidad, rendimiento o funcionamiento.

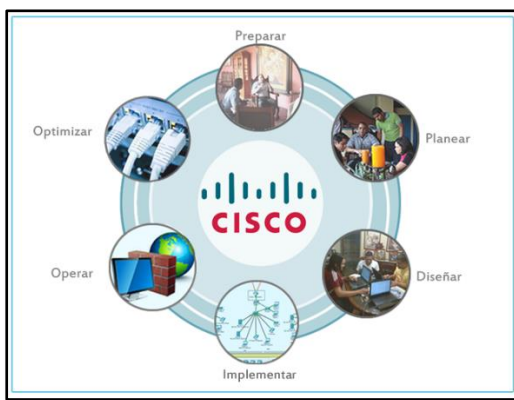
Figura 39*Software de Monitoreo – Zabbix*

Metodología

El presente trabajo aplicativo se elaboró siguiendo la metodología PPDIOO, que fue desarrollada por Cisco. Este modelo ofrece un enfoque ordenado y sistemático para planificar, diseñar, implementar y administrar infraestructuras de red durante todo su ciclo de vida. A continuación, se detalla cómo se aplicó cada una de sus fases dentro del desarrollo de este proyecto.

Figura 40

Metodología PPDIOO Cisco



Preparar

Es la etapa donde se identifican las necesidades del negocio y se define el problema que la red debe resolver. Aquí se establecen los objetivos, el alcance y la viabilidad inicial del proyecto.

Planificar

Para esta etapa se definieron los objetivos sobre la infraestructura actual y los requerimientos técnicos. Se evalúan recursos, riesgos, necesidades de conectividad, segmentación de red y seguridad.

Diseñar

En esta fase se desarrolla la arquitectura lógica y física de la red. Se definen VLAN, direccionamiento IP, protocolos, seguridad, topología y selección de equipos. Esta fase produce el diseño técnico según las necesidades detectadas.

Implementar

Esta etapa corresponde a la ejecución del diseño donde se utiliza un simulador para los equipos de red según la topología propuesta. Se integran switches, routers y firewalls, y se aplican las políticas de segmentación, configuraciones y pruebas funcionales.

Operar

Durante esta etapa la red entra en funcionamiento real. Se realiza monitoreo, soporte, resolución de incidentes y verificación del rendimiento, la disponibilidad y el cumplimiento de las políticas de seguridad. Esto permitió validar la funcionalidad del diseño en un entorno simulado.

Optimizar

En esta última fase se realizaron evaluaciones en distintos escenarios simulados de falla con el fin de verificar el correcto funcionamiento de los mecanismos de alta disponibilidad y failover. A partir de estas pruebas se detectaron oportunidades de mejora en la coordinación entre los dispositivos, por lo que se ajustaron las políticas de acceso, los parámetros del protocolo de redundancia y ciertas configuraciones del enrutamiento dinámico. Estos ajustes permitieron disminuir los tiempos de recuperación y aumentar el nivel de disponibilidad del servicio. Como resultado, la infraestructura diseñada demuestra cumplir con los requerimientos planteados y presenta la flexibilidad necesaria para adaptarse a futuras necesidades operativas y de seguridad.

Desarrollo del trabajo

A continuación, se detalla la topología de red que actualmente emplea la empresa de ventas, la cual presenta limitaciones en disponibilidad, seguridad y capacidad de interconexión entre la sede principal y sus sucursales. Con base en este análisis, se introduce también la topología propuesta, diseñada para implementar una arquitectura de red de alta disponibilidad que asegure la continuidad operativa, fortalezca la seguridad y permita una comunicación eficiente entre todas las sedes de la organización, en concordancia con los objetivos planteados en este trabajo de aplicación profesional.

Descripción de la Infraestructura Actual

La empresa cuenta con una sede principal en La Molina y dos sucursales, G4S y Orquídea, que operan de manera independiente sin interconexión, lo que limita la comunicación directa y el acceso compartido a recursos tecnológicos. Cada sede dispone de su propio servicio de Internet con un router de borde proporcionado por su ISP; la sede principal refuerza la seguridad perimetral con un firewall Fortigate 60F, mientras que en las sucursales las funciones de router y firewall son asumidas por los equipos del proveedor de Internet.

En la sede principal, la conmutación está a cargo de un switch core HPE CX 6200M 24G 4SFP+ (Aruba), que permite una gestión avanzada del tráfico y segmentación de la red, complementado por switches de acceso HPE 2530 y TP-Link TL-SG108 para ampliar la conectividad. Además, cuenta con un servidor Lenovo para servicios corporativos y un access point TP-Link AX1500 para Wi-Fi. En las sucursales G4S y Orquídea, la conmutación central la realiza un switch D-Link DGS-1052, con distribución a usuarios finales mediante switches DGS-3120-24 y TP-Link TL-SG108, y acceso inalámbrico proporcionado por access points TP-Link AX1500.

Debido a que las sedes operan como entornos aislados, actualmente no existe una administración centralizada de la red, ni acceso compartido a sistemas o servicios corporativos, lo cual limita la escalabilidad, la gestión eficiente y la disponibilidad de los recursos tecnológicos. Esta situación motiva el diseño de una arquitectura de red basada en un modelo jerárquico, utilizando la solución Hub and Spoke provista por el proveedor de servicios de Internet, la cual permitirá interconectar las sedes y mejorar la infraestructura tecnológica de la organización. A continuación, se presenta la tabla correspondiente del direccionamiento IP, las áreas operativas y el equipamiento de red de las sedes actuales.

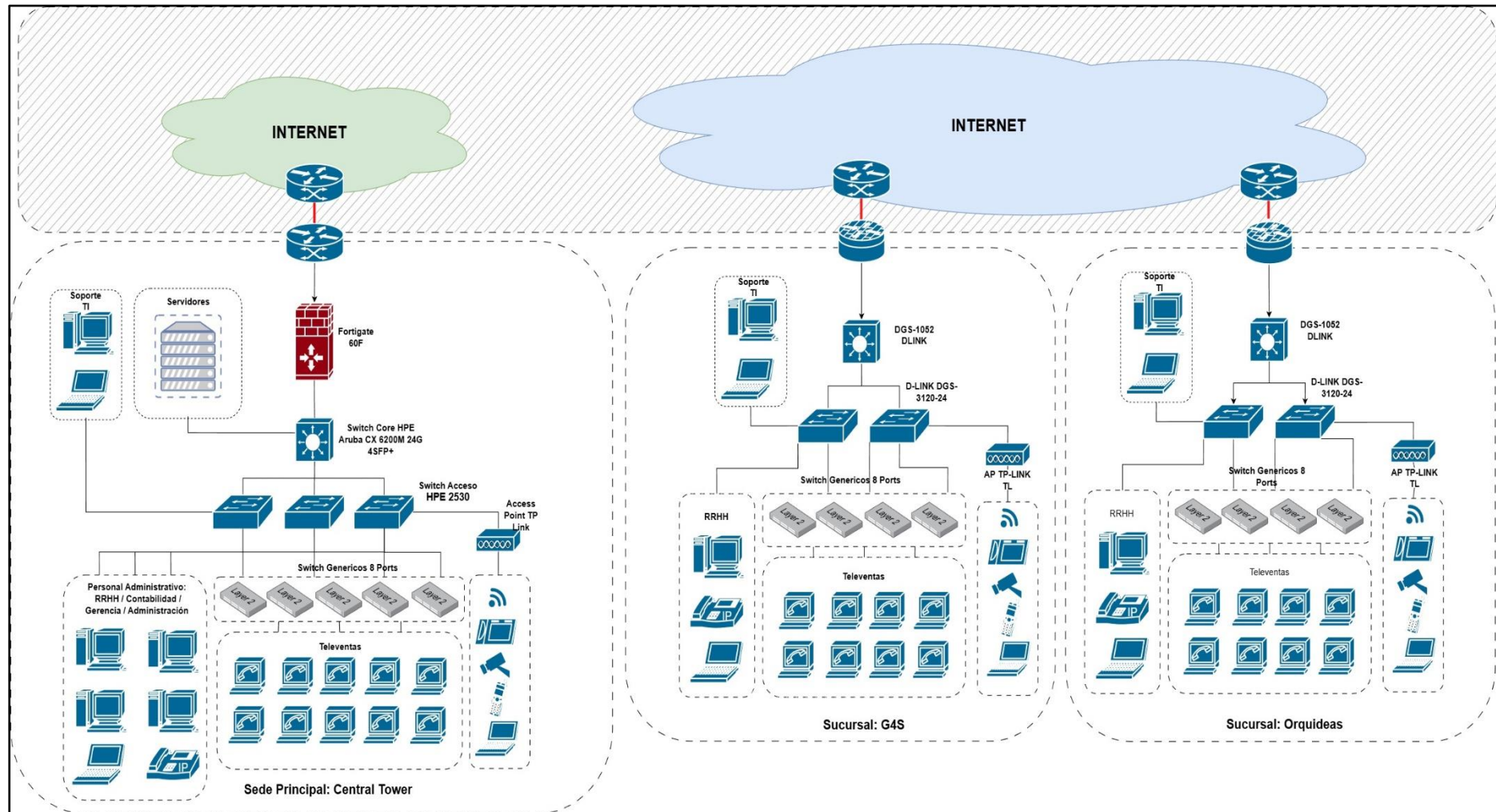
Tabla 6

Plan de Direccionamiento IP, Áreas y Equipamiento Actual

Categoría	Sedes	Elemento / Equipo	Descripción /Detalles
Red LAN	Todas las sedes	192.168.100.0/24 (red privada)	Rango IP privado para la red interna del modem
Áreas de la Organización	Sede Principal (La Molina)	Soporte TI, Logística, Contabilidad, RRHH, Administración, Marketing, Ventas 1, Ventas 2, Gerencia	Áreas operativas que hacen uso de la red LAN y de los servicios corporativos centralizados.
	Sucursales (G4S y Orquídea)	Soporte TI, Logística, RRHH, Ventas 1, Ventas 2, Ventas 3	
Servicios y Recursos de Red	Sede Principal (La Molina)	DNS, Active Directory, Web, Base de Datos	Servidores que ofrecen servicios esenciales a toda la red
Equipos de Red	Sede Principal (La Molina)	Router del ISP	Equipo proporcionado por el proveedor de Internet.
		Firewall Fortigate 60F	Dispositivo de seguridad perimetral encargado del filtrado, control de tráfico y protección de la red.

		Switch Core L3 HPE CX 6200M 24G 4SFP+ (Aruba)	Actúa como distribuidor principal de la red
		Switch de Acceso L2 HPE 2530	Distribuyen la conectividad a las áreas organizativas
		Switch TP-Link TL-SG108	Amplían la conectividad en zonas específicas de la sede.
	Sucursales (G4S y Orquídea)	Router + Firewall del ISP	Equipo proporcionado por el proveedor de Internet que gestiona la conexión y la seguridad básica.
		Switch Core D-Link DGS-1052	Actúa como distribuidor principal de la red
		Switch de Acceso D-Link DGS-3120-24	Distribuyen la conectividad hacia las áreas de trabajo.
		Switch TP-Link TL-SG108	Utilizados para ampliar la conectividad en áreas específicas.
Proveedor de Internet	Todas las sedes	MOVISTAR Y CLARO	Proveedor responsable que brinda una Conexión de 2500 Mbps para la Principal y la Sucursales con 1500 Mbp

En la Figura 40 se presenta la topología actual de la red, la cual muestra la infraestructura de comunicaciones implementada en la organización, incluyendo la interconexión entre la sede principal y las sedes remotas. La arquitectura contempla un firewall perimetral, un switch de Capa 3 en el núcleo de la red y switches de acceso que distribuyen la conectividad a los distintos usuarios y dispositivos finales. Asimismo, se evidencia la segmentación de la red mediante VLANs y la integración de servicios cableados e inalámbricos. Esta topología permite identificar el estado actual de la red y constituye la base para el análisis y la propuesta de mejora del presente proyecto.

Figura 41*Infraestructura Actual de la Red*

Notas: Estos diseños evidencian una red no escalable y que la conectividad no es tan eficiente entre las diferentes áreas.

Análisis de la Infraestructura Actual

En el análisis del diseño de la arquitectura de la red existente se detectaron varios aspectos vulnerables que pueden comprometer la operación continua, la protección de los datos y el rendimiento general del sistema tecnológico. A continuación, se presenta el análisis de la red actual que sintetiza los hallazgos más relevantes.

Tabla 7

Resumen de análisis de la Red Actual

Características	Descripción Técnica	Impacto
Infraestructura sin tolerancia a fallos	La red no cuenta con rutas alternativas ni equipos en alta disponibilidad	Un desperfecto en el router o switch central puede interrumpir parcial o totalmente las operaciones
Único enlace WAN disponible	Existe una sola ruta de salida a Internet proporcionada por un único operador	Si ocurre una caída en la línea o falla el proveedor, el acceso a servicios externos se ve completamente afectado
Segmentación inexistente	Todos los dispositivos conviven en un mismo segmento IP	Aumenta la exposición ante malware y limita el control del tráfico entre áreas
Falta de herramientas de supervisión	No se implementan sistemas para monitorear rendimiento, estado de enlaces o eventos críticos	Los problemas pueden pasar desapercibidos, generando tiempos de caída prolongados
Control de acceso débil	No se aplican políticas de identificación ni validación por usuario o equipo	Eleva la probabilidad de que personas o dispositivos no autorizados accedan a información sensible

Criterios de Diseño de la Topología de la Red Propuesta

- La propuesta de la nueva topología de red se diseña en función de tres criterios principales: disponibilidad, seguridad y escalabilidad, los cuales se detallan a continuación:
- Disponibilidad: La red debe mantenerse operativa aun ante fallas de hardware o interrupciones de conexión, ya que los servicios requieren una continuidad permanente de gestión. Para ello, se plantea el uso de enlaces de distintos

proveedores de internet con mecanismos de balanceo y conmutación automática, además de incorporar redundancia mediante FHRP y firewalls configurados en alta disponibilidad.

- Seguridad: Es fundamental garantizar la protección frente a accesos no autorizados, amenazas internas y externas, y cumplir con las regulaciones del sector corporativo relacionadas con la gestión de riesgos y la protección de datos. Por este motivo, se propone integrar dispositivos de seguridad para aplicar segmentación por VLAN y gestionar estrictamente los accesos a la red inalámbrica.
- Escalabilidad: La infraestructura debe permitir el crecimiento de la entidad sin requerir un rediseño completo de la red. En ese sentido, se plantea un enfoque modular basado en switches de núcleo de alto rendimiento y en la utilización de múltiples VLAN que puedan ampliarse conforme se incorporen nuevas áreas o servicios.

Descripción de la Infraestructura Propuesta

En la topología propuesta se centra en la sede principal ya que opera como punto central de conectividad, seguridad y salida a Internet. Las dos sucursales se enlazan mediante conexiones WAN LAN-to-LAN provistas por el operador, permitiendo que todo el tráfico corporativo y la navegación hacia Internet se gestionen desde la sede principal la cual contara con la conexión de dos proveedores de internet.

En la sede principal se implementará dos firewalls de nueva generación en alta disponibilidad (HA), encargado de la protección perimetral, el control de acceso, la inspección de tráfico y la aplicación de políticas unificadas para todas las sedes. De este modo, la seguridad y la administración se centralizan, garantizando un control robusto y homogéneo.

La red interna se organiza con switches de núcleo la cual tendrá redundancia y alta disponibilidad ya que es donde se distribuye la conexión hacia las sucursales y switches de acceso, lo que permite una estructura escalable y ordenada para gestionar las VLAN corporativas, los servidores internos y las áreas de trabajo. La segmentación por VLAN separa las distintas áreas operativas, mejorando la seguridad, el rendimiento y la gestión del tráfico. El diseño considera además gestión de monitoreo asegurando la rápida detección de fallos y una operación eficiente de toda la red corporativa. A continuación, en la siguiente tabla se muestra el resumen de la infraestructura de la red propuesta.

Tabla 8

Resumen de la Infraestructura de Red Propuesta – Sede Principal

Categoría	Dispositivo	Descripción	Función
Proveedor de Internet	Router ISP 1	Solución ON Empresas (Internet Publica) y (WAN privada - L2L)	Conexión Internet primaria
	Router ISP 2		Conexión Internet respaldo
Proveedor de Wan Privada	Router L2L-Wan privada		Conexión WAN privada L2L
	Router L2L-Wan de respaldo		Conexión WAN privada L2L respaldo
Seguridad	FWLM1 - FWLM2	2 FortiGate 60F (HA) - Firewall Perimetral	Seguridad perimetral, inspección de tráfico, alta disponibilidad
Protocolos de Redundancia	SW-LMCentral-CORE1 / SW-LMCentral-CORE2	2 switches L3 en redundancia (FHRP)	Protocolo de redundancia para puerta de enlace predeterminada
Switches de Acceso	SW-LM-Access01-5	5 switches L2 en redundancia con los Switches core vlan/vtp/stp/portsecurity	Distribuyen conectividad cableada

Tabla 9*Resumen de la Infraestructura de Red Propuesta – Sucursales*

Categoría	Dispositivo	Descripción	Función
Routers L2L - sucursales	RTO-WANG4S-L2L RTO-WANOrquideas-L2L	Solución ON Empresas (WAN privada - L2L)	L2L sucursales San Isidro
Switches Core - sucursales	SW-G4S-CORE SW-ORQUIDEAS-CORE	1 Switch L3 - Core 1 Switch L3 - Core	Puerta de enlace predeterminadas de redes internas
Switches de Acceso - sucursales	SW-G4S-Access01-4 SW-ORQUIDEAS-Access01-4	4 Switch conectados a SwCore vlan/vtp/stp/portsecurity	Distribuyen conectividad cableada

Tabla 10*Equipos propuestos – Sede Principal y sucursales*

Sede	Modelo	Descripción	Cantidad
Principal (Central Tower)	FortiGate 60F	Control de tráfico, protección contra amenazas	2
	C9300-48T-A	Switch L3 48 Ports Gb, no POE, Distribución	2
	HPE Aruba CX 6000 48G PoE 4SFP	Switch L2 48 Ports Gb, PoE/PoE+, 4 puertos SFP Uplink	5
Sucursal (G4S)	Switch L3 – HPE CX 6200M 24G 4SFP+	Switch L3 48 Ports Gb + 4SFP, sin POE, Distribución	1
	HPE Aruba CX 6000 48G PoE 4SFP	Switch L2 48 Ports Gb, 4 PoE/PoE+, 4 puertos SFP Uplink	4
Sucursal (Orquídeas)	Switch L3 - HPE CX 6200M 24G 4SFP+	Switch L3 48 Ports Gb + 4SFP, sin POE, Distribución	1
	HPE Aruba CX 6000 48G PoE 4SFP	Switch L2 48 Ports Gb, 4 PoE/PoE+, 4 puertos SFP Uplink	4

Segmentación de la Red Propuesta

Para la segmentación de la red propuesta, se definieron bloques de direcciones IP privadas para cada sede, asegurando una distribución lógica y escalable acorde a los servicios y áreas de la organización.

- Sede Principal: Bloque 172.16.0.0/18, subdividido en VLANs con máscaras /24 para cada área o servicio, permitiendo hasta 254 hosts por VLAN.
- Sucursal 1: Bloque 172.16.64.0/18, subdividido en VLANs /24 para cada área o servicio, manteniendo hasta 254 hosts por VLAN.
- Sucursal 2: Bloque 172.16.128.0/18, subdividido en VLANs /24 para cada área o servicio, con capacidad para 254 hosts por VLAN.

Cada VLAN fue planificada con el objetivo de garantizar la escalabilidad del direccionamiento IP, la aislación de tráfico según áreas funcionales y la optimización de la administración de la red. Asimismo, se incorporaron prácticas de seguridad mediante la VLAN nativa (VLAN 99) para el transporte de tramas sin etiquetar en enlaces troncales y la VLAN Isolated (VLAN 1000) para puertos no utilizados o dispositivos aislados, operando únicamente en capa 2 y sin asignación de dirección IP.

A continuación, se detallan los segmentos de red propuestos para su asignación correspondiente a cada VLAN y área de la empresa.

Tabla 11

Distribución de la Red – VLANs para las Áreas de Servicio

VLAN	Nombre	Descripción
10	Gerencia	Hosts – Gerencia
20	Logística	Hosts – Logística
30	Contabilidad	Hosts – Contabilidad
40	RRHH	Hosts – RRHH
50	Adm/Marke	Hosts – Adm. y Marketing
60	Ventas 1	Hosts – Ventas 1
70	Ventas 2	Hosts – Ventas 2
80	Ventas 3	Hosts – Ventas 3
85	ATC	Hosts – ATC
90	Seguridad	Hosts – Seguridad
100	WiFi Guest	WiFi – Invitados
110	WiFi Operaciones	WiFi – Operaciones
120	Voz	Voz – IP Phones
130	Servidores	Hosts – Sala de Servidores
140	Soporte TI	Hosts – Soporte TI
150	Gestión	Gestión – Infraestructura
160	DMZ	Servidores – DMZ
170	L2L (Tránsito)	Tránsito – Enlaces L2L

99	Nativa	VLAN Nativa – Troncales
1000	Isolated	Puertos Aislados – Cuarentena

En la siguiente tabla, se presenta el direccionamiento IP para la gestión remota de los equipos de red mediante los segmentos VLAN de gestión propuestos para cada sede principal y sucursales.

Tabla 12

Distribución de Red - Direccionamiento IP de VLAN de Gestión

Sede	Subred de Gestión	Máscara	Rango de Hosts Válidos	Propósito
Central Tower	172.16.14.0/24	255.255.255.0	172.16.14.1 – 172.16.14.254	Gestión remota de equipos de la sede principal
G4S	172.16.75.0/24	255.255.255.0	172.16.75.1 – 172.16.75.254	Gestión remota de equipos para la sucursal 1 y 2
Orquídeas	172.16.139.0/24	255.255.255.0	172.16.139.1 – 172.16.139.254	

En la siguiente tabla, Configuración del direccionamiento IP para Switchs Core.

Tabla 13

Direccionamiento IP de Switch Core - Sede Principal

VLAN / Área	Active	Standby	IP GW Virtual	Subred / Prefijo
10 – Gerencia	172.16.0.252	172.16.0.253	172.16.0.254	172.16.0.0/24
20 – Logística	172.16.1.252	172.16.1.253	172.16.1.254	172.16.1.0/24
30 – Contabilidad	172.16.2.252	172.16.2.253	172.16.2.254	172.16.2.0/24
40 – RRHH	172.16.3.252	172.16.3.253	172.16.3.254	172.16.3.0/24
50 – Adm/Marke	172.16.4.252	172.16.4.253	172.16.4.254	172.16.4.0/24
60 – Ventas 1	172.16.5.252	172.16.5.253	172.16.5.254	172.16.5.0/24
70 – Ventas 2	172.16.6.252	172.16.6.253	172.16.6.254	172.16.6.0/24
85 – ATC	172.16.7.252	172.16.7.253	172.16.7.254	172.16.7.0/24
90 – Seguridad	172.16.8.252	172.16.8.253	172.16.8.254	172.16.8.0/24
100 – WiFi Guest	172.16.9.252	172.16.9.253	172.16.9.254	172.16.9.0/24
110 – WiFi Operaciones	172.16.10.252	172.16.10.253	172.16.10.254	172.16.10.0/24
120 – Voz	172.16.11.252	172.16.11.253	172.16.11.254	172.16.11.0/24
130 – Servidores	172.16.12.252	172.16.12.253	172.16.12.254	172.16.12.0/24
140 – Soporte TI	172.16.13.252	172.16.13.253	172.16.13.254	172.16.13.0/24
150 – Gestión	172.16.14.252	172.16.14.253	172.16.14.254	172.16.14.0/24
160 – DMZ	172.16.15.252	172.16.15.253	172.16.15.254	172.16.15.0/24
170 - L2L (Tránsito)	172.16.16.252	172.16.16.253	172.16.16.251	172.16.16.248/29

Tabla 14*Direccionamiento IP de Switch Core - Sucursal G4S*

VLAN	Área / Servicio	Subred / Prefijo
20	Logística	172.16.64.1/24
40	RRHH	172.16.65.1/24
60	Ventas 1	172.16.66.1/24
70	Ventas 2	172.16.67.1/24
80	Ventas 3	172.16.68.1/24
90	Seguridad	172.16.69.1/24
100	WiFi Guest	172.16.70.1/24
110	WiFi Operaciones	172.16.71.1/24
120	Voz	172.16.72.1/24
130	Servidores	172.16.73.1/24
140	Soporte TI	172.16.74.1/24
150	Gestión	172.16.75.1/24

Tabla 15*Direccionamiento IP de Switch Core - Sucursal Orquídeas*

VLAN	Área / Servicio	Subred / Prefijo
20	Logística	172.16.128.1/24
40	RRHH	172.16.129.1/24
60	Ventas 1	172.16.130.1/24
70	Ventas 2	172.16.131.1/24
80	Ventas 3	172.16.132.1/24
90	Seguridad	172.16.133.1/24
100	WiFi Guest	172.16.134.1/24
110	WiFi Operaciones	172.16.135.1/24
120	Voz	172.16.136.1/24
130	Servidores	172.16.137.1/24
140	Soporte TI	172.16.138.1/24
150	Gestión	172.16.139.1/24

En la siguiente Tabla, se presenta el plan de direccionamiento IP de la Sede Principal:

Bloque 172.16.0.0/18, subdividido en VLANs con máscaras /24 para cada área o servicio, permitiendo hasta 254 hosts por VLAN.

Tabla 16*Direccionamiento de Red – Sede Principal (Central Tower)*

VLAN	Área / Servicio	Red IP	Prefijo
10	Gerencia	172.16.0.0	/24
20	Logística	172.16.1.0	/24
30	Contabilidad	172.16.2.0	/24
40	RRHH	172.16.3.0	/24
50	Adm/Marke	172.16.4.0	/24
60	Ventas 1	172.16.5.0	/24
70	Ventas 2	172.16.6.0	/24
85	ATC	172.16.7.0	/24
90	Seguridad	172.16.8.0	/24
100	WiFi Guest	172.16.9.0	/24
110	WiFi Operaciones	172.16.10.0	/24
120	Voz	172.16.11.0	/24
130	Servidores	172.16.12.0	/24
140	Soporte TI	172.16.13.0	/24
150	Gestión	172.16.14.0	/24
160	DMZ	172.16.15.0	/24
170	L2L (Tránsito)	172.16.16.248	/29
99	Nativa	—	—
1000	Isolated	—	—

En la siguiente Tabla, se presenta el plan de direccionamiento IP de la Sucursal 1 (G4S): Bloque 172.16.64.0/18, subdividido en VLANs /24 para cada área o servicio, manteniendo hasta 254 hosts por VLAN.

Tabla 17*Direccionamiento de Red – Sucursal 1(G4S)*

VLAN	Área / Servicio	Red IP	Prefijo
20	Logística	172.16.64.0	/24
40	RRHH	172.16.65.0	/24
60	Ventas 1	172.16.66.0	/24
70	Ventas 2	172.16.67.0	/24
80	Ventas 3	172.16.68.0	/24
90	Seguridad	172.16.69.0	/24
100	WiFi Guest	172.16.70.0	/24
110	WiFi Operaciones	172.16.71.0	/24
120	Voz	172.16.72.0	/24
130	Servidores	172.16.73.0	/24
140	Soporte TI	172.16.74.0	/24
150	Gestión	172.16.75.0	/24
170	L2L (Tránsito)	172.16.76.248	/29
99	Nativa	—	—
1000	Isolated	—	—

En la siguiente Tabla, se presenta el plan de direccionamiento IP de la Sucursal 2:

Bloque 172.16.128.0/18, subdividido en VLANs /24 para cada área o servicio, con capacidad para 254 hosts por VLAN.

Tabla 18

Direccionamiento de Red – Sucursal 2 (Orquídeas)

VLAN	Área / Servicio	Red IP	Máscara
20	Logística	172.16.128.0	/24
40	RRHH	172.16.129.0	/24
60	Ventas 1	172.16.130.0	/24
70	Ventas 2	172.16.131.0	/24
80	Ventas 3	172.16.132.0	/24
90	Seguridad	172.16.133.0	/24
100	WiFi Guest	172.16.134.0	/24
110	WiFi Operaciones	172.16.135.0	/24
120	Voz	172.16.136.0	/24
130	Servidores	172.16.137.0	/24
140	Soporte TI	172.16.138.0	/24
150	Gestión	172.16.139.0	/24
170	L2L (Tránsito)	172.16.140.248	/29
99	Nativa	—	—
1000	Isolated	—	—

En la siguiente Tabla, se presenta la planificación jerárquica de la segmentación de la red, partiendo del bloque privado 172.16.0.0/12, el cual permite la creación de hasta 64 subredes con prefijo /18 destinadas a sedes independientes. Cada sede dispone de un bloque /18 que es subdividido en VLANs con prefijo /24, garantizando capacidad suficiente para las distintas áreas de la empresa y permitiendo una expansión ordenada sin solapamiento de direccionamiento IP.

Tabla 19*Planificación de la Segmentación y Escalabilidad de la Red*

Nivel de Segmentación	Bloque IP Asignado	Prefijo	Capacidad de Subredes	Hosts por Subred	Propósito / Justificación
Red Privada Corporativa	172.16.0.0	/12	64 bloques /18	—	Base de direccionamiento escalable
Sede (nivel geográfico)	172.16.0.0 – 172.31.255.255	/18	64 sedes posibles	—	Bloque, sin solapamientos y con escalabilidad
Área / Servicio (VLAN)	Subred por sede	/24	64 VLANs por sede	254	Segmentación lógica por área

En la Figura 41 se presenta la topología de red propuesta, en la cual se incorpora un diseño orientado a la alta disponibilidad y resiliencia de la infraestructura. La arquitectura contempla redundancia en los switches de núcleo, firewalls en alta disponibilidad (HA) y enlaces WAN, con el fin de garantizar la continuidad del servicio ante fallas de equipos o enlaces. Asimismo, se implementa un esquema jerárquico que optimiza la comunicación entre la sede principal y las sedes remotas, mejorando la seguridad, el rendimiento y la escalabilidad de la red. Esta topología propuesta permite fortalecer la operación de los servicios críticos y responde a los requerimientos de crecimiento y disponibilidad del proyecto.

Como se aprecia en la Figura 41, la infraestructura de red cuenta con dos enlaces a Internet provistos por ON Empresas, los cuales son balanceados mediante routers y equipos de conmutación intermedios. Los firewalls FortiGate 60F operan en alta disponibilidad (HA) y se encuentran conectados al switch de núcleo Cisco C9300-48T-A, el cual centraliza el tráfico de la red.

La capa de acceso está conformada por múltiples switches organizados en VLANs segmentadas (VLAN 10, 20, 30, 40, entre otras). Asimismo, se emplean controladores inalámbricos a los que se conectan los puntos de acceso, asignados a las VLAN 100 y 110. Para garantizar la redundancia y evitar bucles en la topología, se implementa el Protocolo de Árbol de Expansión (STP), asegurando la estabilidad de la red en el diseño de núcleo contraído.

Configuración del Equipamiento de la Red Propuesta

En esta sección se describen las configuraciones realizadas en los dispositivos que conforman la infraestructura de red propuesta, considerando un diseño de núcleo contraído. Se incluye la asignación del direccionamiento IP, la segmentación de la red mediante VLANs, la implementación de protocolos de enrutamiento dinámico y estático, así como la configuración de enlaces redundantes y mecanismos de alta disponibilidad, tales como FHRP en los switches de Capa 3 del núcleo, con el objetivo de garantizar un adecuado rendimiento, alta disponibilidad y continuidad operativa entre la sede principal y las sucursales.

Asimismo, se detallan las configuraciones de seguridad implementadas en el diseño, incluyendo políticas de control de acceso, reglas de traducción de direcciones de red (NAT) y esquemas de alta disponibilidad (HA) en los firewalls FortiGate, además de los mecanismos de tolerancia a fallos (failover) y las soluciones de monitoreo que permiten supervisar el estado y desempeño de la red. Todo ello contribuye a fortalecer la resiliencia, confiabilidad y seguridad de la infraestructura propuesta.

Configuraciones de Equipos Realizadas en la Topología de Red

Las configuraciones de los equipos de red fueron simuladas en el software Packet Tracer, debido a las limitaciones de este software, no se está considerando todas las configuraciones de las Sucursales centrándose más en la Sede Principal. Asimismo, no se está contemplando las configuraciones que se realizaran en los equipos del proveedor de internet.

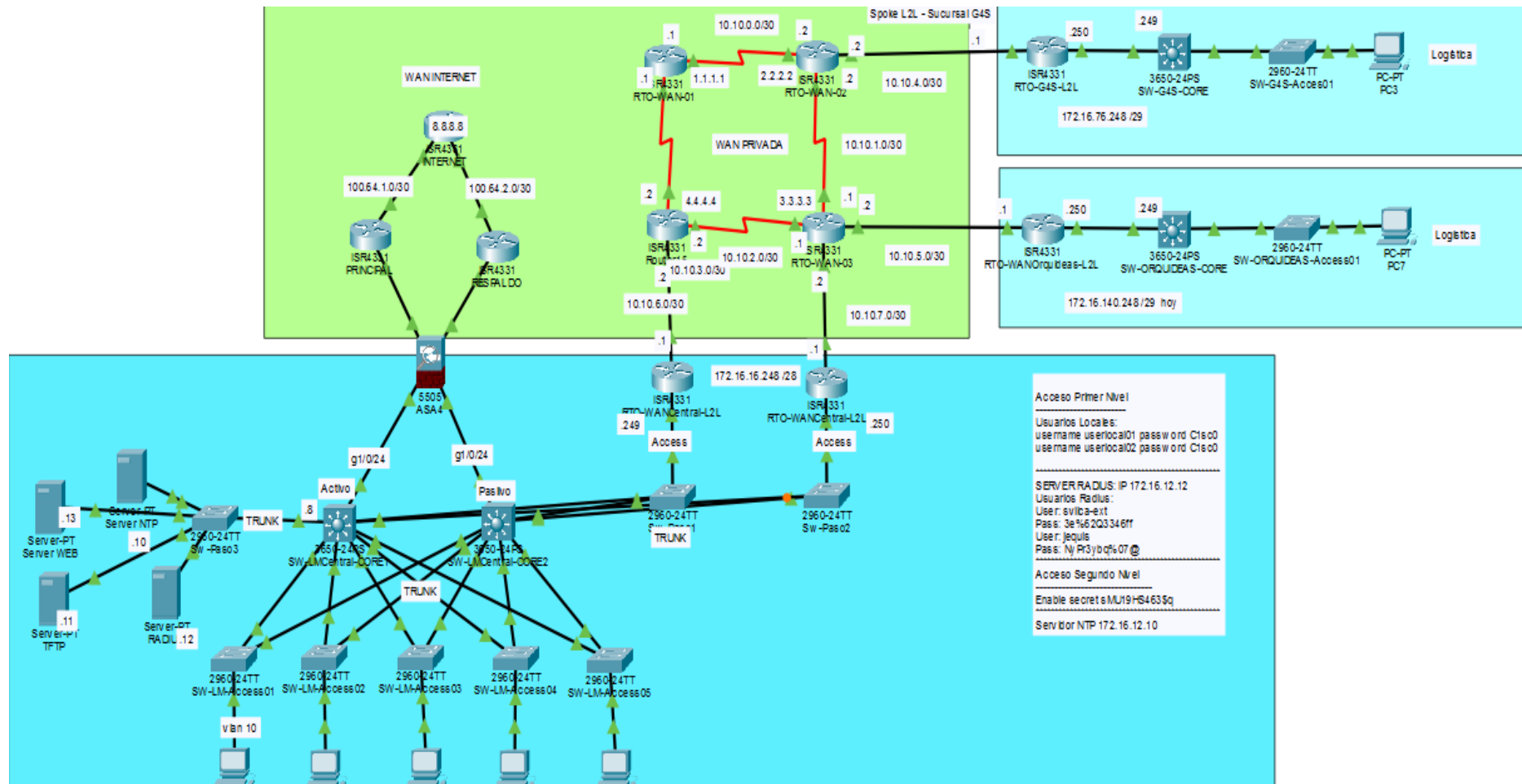
A continuación, se detallará las configuraciones realizadas en los equipos de red:

- VTP
- VLANs
- Port Security
- Spanning Tree Protocol (STP)
- Interfaz Virtual Switch (SVI)
- Configuración Puerto Troncal (Trunk)
- Configuración HSRP
- DHCP
- Enrutamiento OSPF
- Enrutamiento Estático
- Seguridad de Inicio de Sesión
- SSH
- Protocolo SNMP
- Configuración PRTG

A continuación, se presentará la topología diseñada en el software Packet Tracer.

Figura 43

Packet Tracer - Simulación ISP / Sedes



Nota: La topología presentada representa el diseño lógico de la red propuesta simulada en el Packet Tracer.

Configuración del Protocolo VTP

En el switch SW_CORE se configuro el servidor VTP con la finalidad de replicar las VLANs en todos los switches que se encuentran en la capa de acceso. A continuación, se presentará la configuración del servidor VTP en el Switch capa 3.

Figura 44

Configuración del Protocolo VTP - SW-LMCentral-CORE1

```
SW-LMCentral-CORE1#show vtp status
VTP Version capable       : 1 to 2
VTP version running       : 2
VTP Domain Name           : g4s.com
VTP Pruning Mode          : Disabled
VTP Traps Generation      : Disabled
Device ID                 : 0002.1757.D800
Configuration last modified by 172.16.0.252 at 3-2-93 05:43:10
Local updater ID is 172.16.0.252 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode        : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 24
Configuration Revision     : 0
MDS digest                : 0x30 0xF0 0x58 0x49 0x42 0xC2 0x32 0x4C
                           0xB6 0x68 0xD4 0x87 0x14 0xBF 0x5C 0xED
SW-LMCentral-CORE1#
```

A continuación, se presentarán las imágenes que hacen referencia a la configuración de los clientes VTP en los switches capa 2.

Figura 45

Configuración del Protocolo VTP - SW-LMCentral-CORE2

```
SW-LMCentral-CORE2#show vtp status
VTP Version capable       : 1 to 2
VTP version running       : 2
VTP Domain Name           : g4s.com
VTP Pruning Mode          : Disabled
VTP Traps Generation      : Disabled
Device ID                 : 0006.2A40.9700
Configuration last modified by 0.0.0.0 at 3-2-93 05:27:59
Local updater ID is 172.16.0.253 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode        : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 24
Configuration Revision     : 95
MDS digest                : 0x75 0xBA 0x43 0xA5 0xC7 0x82 0x56 0x71
                           0xB2 0x7E 0x45 0xBB 0x63 0xD0 0xF9 0xBC
SW-LMCentral-CORE2#
```

Figura 46

Configuración del Protocolo VTP - SW-LM-Access01

```

SW-LM-Access01#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : g4s.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 00D0.58C2.1400
Configuration last modified by 0.0.0.0 at 3-2-93 05:27:59

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 24
Configuration Revision   : 95
MD5 digest               : 0x75 0xBA 0x43 0xA5 0xC7 0x82 0x56 0x71
                          0xB2 0x7E 0x45 0xBB 0x63 0xD0 0xF9 0xBC

SW-LM-Access01#

```

Figura 47*Configuración del Protocolo VTP - SW-LM-Access02*

```

SW-LM-Access02#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : g4s.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0060.3E69.6900
Configuration last modified by 0.0.0.0 at 3-2-93 05:27:59

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 24
Configuration Revision   : 95
MD5 digest               : 0x75 0xBA 0x43 0xA5 0xC7 0x82 0x56 0x71
                          0xB2 0x7E 0x45 0xBB 0x63 0xD0 0xF9 0xBC

SW-LM-Access02#

```

Figura 48*Configuración del Protocolo VTP - SW-LM-Access03*

```

SW-LM-Access03#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : g4s.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0050.0FBA.0900
Configuration last modified by 0.0.0.0 at 3-2-93 05:27:59

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 24
Configuration Revision   : 95
MD5 digest               : 0x75 0xBA 0x43 0xA5 0xC7 0x82 0x56 0x71
                          0xB2 0x7E 0x45 0xBB 0x63 0xD0 0xF9 0xBC

SW-LM-Access03#

```

Figura 49*Configuración del Protocolo VTP - SW-LM-Access04*

```

SW-LM-Access04#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : g4s.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.644C.EC00
Configuration last modified by 0.0.0.0 at 3-2-93 05:27:59

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 24
Configuration Revision   : 95
MD5 digest               : 0x75 0xBA 0x43 0xA5 0xC7 0x82 0x56 0x71
                          : 0xB2 0x7E 0x45 0xBB 0x63 0xD0 0xF9 0xBC

SW-LM-Access04#

```

Figura 50*Configuración del Protocolo VTP - SW-LM-Access05*

```

SW-LM-Access05#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : g4s.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.6411.B000
Configuration last modified by 0.0.0.0 at 3-2-93 05:27:59

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 24
Configuration Revision   : 95
MD5 digest               : 0x75 0xBA 0x43 0xA5 0xC7 0x82 0x56 0x71
                          : 0xB2 0x7E 0x45 0xBB 0x63 0xD0 0xF9 0xBC

SW-LM-Access05#

```

Configuración VLANs

A continuación, se mostrará la configuración de las VLANs en todos los switches de la red. Asimismo, se mostrará la asignación de las VLANs a los puertos de red de cada Switch. Se implementó la VLAN 1000 denominada *ISOLATE* como VLAN de aislamiento, destinada a la asignación de puertos no utilizados. Dichos puertos fueron configurados en modo acceso y mantenidos en estado administrativo *shutdown*, con el objetivo de prevenir accesos no autorizados y fortalecer la seguridad de la red.

Figura 51*Configuración de las VLANs - SW-LMCentral-CORE1*

```
SW-LMCentral-CORE1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	
20	Logistica	active	
30	Contabilidad	active	
40	RRHH	active	
50	Adm_Marketing	active	
60	Ventas-01	active	
70	Ventas-02	active	
80	Ventas-03	active	
85	ATC	active	
90	Seguridad	active	
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	
130	Servidores	active	
140	Soporte_TI	active	Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
150	Gestion	active	
170	Lan_to_Lan	active	
1000	Isolated	active	Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11 Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15 Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19 Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23 Gig1/0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SW-LMCentral-CORE1#
```

Figura 52*Configuración de las VLANs - SW-LMCentral-CORE2*

```
SW-LMCentral-CORE2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	
20	Logistica	active	
30	Contabilidad	active	
40	RRHH	active	
50	Adm_Marketing	active	
60	Ventas-01	active	
70	Ventas-02	active	
80	Ventas-03	active	
85	ATC	active	
90	Seguridad	active	
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	
130	Servidores	active	
140	Soporte_TI	active	Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
150	Gestion	active	
170	Lan_to_Lan	active	
1000	Isolated	active	Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11 Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15 Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19 Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23 Gig1/0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SW-LMCentral-CORE2#
```

Figura 53*Configuración de las VLANs - SW-LM-Access01*

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	Fa0/1
20	Logistica	active	Fa0/2, Fa0/3, Fa0/4
30	Contabilidad	active	Fa0/5, Fa0/6
40	RRHH	active	Fa0/7, Fa0/8
50	Adm_Marketing	active	Fa0/9, Fa0/10
60	Ventas-01	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
70	Ventas-02	active	
80	Ventas-03	active	
85	ATC	active	
90	Seguridad	active	
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	
130	Servidores	active	
140	Soporte_TI	active	
150	Gestion	active	
170	Lan_to_Lan	active	
1000	Isolated	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

SW-LM-Access01#

Figura 54*Configuración de las VLANs - SW-LM-Access02*

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	
20	Logistica	active	
30	Contabilidad	active	
40	RRHH	active	
50	Adm_Marketing	active	
60	Ventas-01	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15
70	Ventas-02	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
80	Ventas-03	active	
85	ATC	active	
90	Seguridad	active	
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	
130	Servidores	active	
140	Soporte_TI	active	
150	Gestion	active	
170	Lan_to_Lan	active	
1000	Isolated	active	
1002	fddi-default	active	

Figura 55*Configuración de las VLANs - SW-LM-Access03*

```
SW-LM-Access03#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	
20	Logistica	active	
30	Contabilidad	active	
40	RRHH	active	
50	Adm_Marketing	active	
60	Ventas-01	active	
70	Ventas-02	active	
80	Ventas-03	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15
85	ATC	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20
90	Seguridad	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	

Figura 56*Configuración de las VLANs - SW-LM-Access04*

```
SW-LM-Access04#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	
20	Logistica	active	
30	Contabilidad	active	
40	RRHH	active	
50	Adm_Marketing	active	
60	Ventas-01	active	
70	Ventas-02	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20
80	Ventas-03	active	
85	ATC	active	
90	Seguridad	active	
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	
130	Servidores	active	
140	Soporte_TI	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
150	Gestion	active	
170	Lan_to_Lan	active	
1000	Isolated	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SW-LM-Access04#
```

Figura 57*Configuración de las VLANs - SW-LM-Access05*

```
SW-LM-Access05#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	Gerencia	active	
20	Logistica	active	
30	Contabilidad	active	
40	RRHH	active	
50	Adm_Marketing	active	
60	Ventas-01	active	
70	Ventas-02	active	
80	Ventas-03	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15
85	ATC	active	
90	Seguridad	active	
99	Nativa	active	
100	Wifi_guest	active	
110	Wifi_operaciones	active	
120	Voz	active	
130	Servidores	active	
140	Soporte_TI	active	
150	Gestion	active	
170	Lan_to_Lan	active	
1000	Isolated	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SW-LM-Access05#
```

Configuración de Port Security

En la presente propuesta se ha implementado Port Security como un mecanismo de seguridad en la capa de acceso de la red, con la finalidad de restringir el acceso no autorizado a la infraestructura de red. Esta funcionalidad permite controlar los dispositivos que pueden conectarse a los puertos físicos de los switches, fortaleciendo la seguridad a nivel de acceso.

Por motivos de seguridad, se ha configurado que cada puerto de acceso reconozca únicamente un dispositivo, permitiendo el registro de una sola dirección MAC por puerto. Esta medida contribuye a prevenir la conexión de equipos no autorizados y a mitigar posibles ataques, como el MAC flooding.

A continuación, se presenta la configuración aplicada de Port Security en los switches de la capa de acceso, la cual refleja las políticas de seguridad definidas para el control y protección del acceso a la red.

Figura 58

Configuración de Port Security - SW-LM-Access01

```
SW-LM-Access01#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	2	1	0	Restrict
Fa0/2	2	0	0	Restrict
Fa0/3	2	0	0	Restrict
Fa0/4	2	0	0	Restrict
Fa0/5	2	0	0	Restrict
Fa0/6	2	0	0	Restrict
Fa0/7	2	0	0	Restrict
Fa0/8	2	0	0	Restrict
Fa0/9	2	0	0	Restrict
Fa0/10	2	0	0	Restrict
Fa0/11	2	0	0	Restrict
Fa0/12	2	0	0	Restrict
Fa0/13	2	0	0	Restrict
Fa0/14	2	0	0	Restrict
Fa0/15	2	0	0	Restrict
Fa0/16	2	0	0	Restrict
Fa0/17	2	0	0	Restrict
Fa0/18	2	0	0	Restrict
Fa0/19	2	0	0	Restrict
Fa0/20	2	0	0	Restrict
Fa0/21	2	0	0	Restrict
Fa0/22	2	0	0	Restrict
Fa0/23	2	0	0	Restrict
Fa0/24	2	0	0	Restrict

```
SW-LM-Access01#
```

```
SW-LM-Access01#show port-security interface fastEthernet 0/1
```

```
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 2
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0001.4376.7769:10
Security Violation Count : 0
```

```
SW-LM-Access01#
```

Figura 59*Configuración de Port Security - SW-LM-Access02*

```
SW-LM-Access02#show port-security
```

Secure	Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
	Fa0/1	2	0	0	Restrict
	Fa0/2	2	0	0	Restrict
	Fa0/3	2	0	0	Restrict
	Fa0/4	2	0	0	Restrict
	Fa0/5	2	0	0	Restrict
	Fa0/6	2	0	0	Restrict
	Fa0/7	2	0	0	Restrict
	Fa0/8	2	0	0	Restrict
	Fa0/9	2	0	0	Restrict
	Fa0/10	2	0	0	Restrict
	Fa0/11	2	0	0	Restrict
	Fa0/12	2	0	0	Restrict
	Fa0/13	2	0	0	Restrict
	Fa0/14	2	0	0	Restrict
	Fa0/15	2	0	0	Restrict
	Fa0/16	2	0	0	Restrict
	Fa0/17	2	0	0	Restrict
	Fa0/18	2	0	0	Restrict
	Fa0/19	2	0	0	Restrict
	Fa0/20	2	0	0	Restrict
	Fa0/21	2	0	0	Restrict
	Fa0/22	2	0	0	Restrict
	Fa0/23	2	0	0	Restrict
	Fa0/24	2	0	0	Restrict

```
SW-LM-Access02#
```

Figura 60*Configuración de Port Security - SW-LM-Access03*

```
SW-LM-Access03#show port-security
```

Secure	Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
	Fa0/1	2	0	0	Restrict
	Fa0/2	2	0	0	Restrict
	Fa0/3	2	0	0	Restrict
	Fa0/4	2	0	0	Restrict
	Fa0/5	2	0	0	Restrict
	Fa0/6	2	0	0	Restrict
	Fa0/7	2	0	0	Restrict
	Fa0/8	2	0	0	Restrict
	Fa0/9	2	0	0	Restrict
	Fa0/10	2	0	0	Restrict
	Fa0/11	2	0	0	Restrict
	Fa0/12	2	0	0	Restrict
	Fa0/13	2	0	0	Restrict
	Fa0/14	2	0	0	Restrict
	Fa0/15	2	0	0	Restrict
	Fa0/16	2	0	0	Restrict
	Fa0/17	2	0	0	Restrict
	Fa0/18	2	0	0	Restrict
	Fa0/19	2	0	0	Restrict
	Fa0/20	2	0	0	Restrict
	Fa0/21	2	0	0	Restrict
	Fa0/22	2	0	0	Restrict
	Fa0/23	2	0	0	Restrict
	Fa0/24	2	0	0	Restrict

```
SW-LM-Access03#
```

Figura 61*Configuración de Port Security - SW-LM-Access04*

```
SW-LM-Access04#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	2	0	0	Restrict
Fa0/2	2	0	0	Restrict
Fa0/3	2	0	0	Restrict
Fa0/4	2	0	0	Restrict
Fa0/5	2	0	0	Restrict
Fa0/6	2	0	0	Restrict
Fa0/7	2	0	0	Restrict
Fa0/8	2	0	0	Restrict
Fa0/9	2	0	0	Restrict
Fa0/10	2	0	0	Restrict
Fa0/11	2	0	0	Restrict
Fa0/12	2	0	0	Restrict
Fa0/13	2	0	0	Restrict
Fa0/14	2	0	0	Restrict
Fa0/15	2	0	0	Restrict
Fa0/16	2	0	0	Restrict
Fa0/17	2	0	0	Restrict
Fa0/18	2	0	0	Restrict
Fa0/19	2	0	0	Restrict
Fa0/20	2	0	0	Restrict
Fa0/21	2	0	0	Restrict
Fa0/22	2	0	0	Restrict
Fa0/23	2	0	0	Restrict
Fa0/24	2	0	0	Restrict

```
SW-LM-Access04#
```

Figura 62*Configuración de Port Security - SW-LM-Access05*

```
SW-LM-Access05#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	2	0	0	Restrict
Fa0/2	2	0	0	Restrict
Fa0/3	2	0	0	Restrict
Fa0/4	2	0	0	Restrict
Fa0/5	2	0	0	Restrict
Fa0/6	2	0	0	Restrict
Fa0/7	2	0	0	Restrict
Fa0/8	2	0	0	Restrict
Fa0/9	2	0	0	Restrict
Fa0/10	2	0	0	Restrict
Fa0/11	2	0	0	Restrict
Fa0/12	2	0	0	Restrict
Fa0/13	2	0	0	Restrict
Fa0/14	2	0	0	Restrict
Fa0/15	2	0	0	Restrict
Fa0/16	2	0	0	Restrict
Fa0/17	2	0	0	Restrict
Fa0/18	2	0	0	Restrict
Fa0/19	2	0	0	Restrict
Fa0/20	2	0	0	Restrict
Fa0/21	2	0	0	Restrict
Fa0/22	2	0	0	Restrict
Fa0/23	2	0	0	Restrict
Fa0/24	2	0	0	Restrict

```
SW-LM-Access05#
```

Configuración de Spanning-tree + Portfast + BPDUGuard

La configuración controlada de Spanning-tree evita reconvergencias innecesarias en la capa de acceso y mejora la estabilidad general de la red. Este enfoque sigue buenas prácticas de diseño en redes empresariales y contribuye a la escalabilidad y disponibilidad del sistema.

Figura 63

Configuración de STP SW-LMCentral-CORE1

```
SW-LMCentral-CORE1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: default Gerencia Logistica Contabilidad RRHH Adm_Marketin
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is disabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	4	0	0	4	8
VLAN0010	1	0	0	7	8
VLAN0020	1	0	0	7	8
VLAN0030	1	0	0	7	8
VLAN0040	1	0	0	7	8
VLAN0050	1	0	0	7	8
VLAN0060	1	0	0	7	8
VLAN0070	1	0	0	7	8
VLAN0080	0	0	0	8	8
VLAN0085	1	0	0	7	8
VLAN0090	1	0	0	7	8
VLAN0099	0	0	0	8	8
VLAN0100	0	0	0	8	8
VLAN0110	1	0	0	7	8
VLAN0120	1	0	0	7	8
VLAN0130	1	0	0	7	8
VLAN0140	1	0	0	7	8
VLAN0150	1	0	0	7	8
VLAN0160	3	0	0	5	8
VLAN0170	0	0	0	8	8
VLAN01000	0	0	0	8	8

21 vlans	21	0	0	147	168

```
SW-LMCentral-CORE1#
```

Figura 64

Configuración de STP SW-LMCentral-CORE2

```
SW-LMCentral-CORE2#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is disabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	4	0	0	3	7
VLAN0010	4	0	0	3	7
VLAN0020	5	0	0	2	7
VLAN0030	5	0	0	2	7
VLAN0040	4	0	0	3	7
VLAN0050	4	0	0	3	7
VLAN0060	4	0	0	3	7
VLAN0070	4	0	0	3	7
VLAN0080	0	0	0	7	7
VLAN0085	4	0	0	3	7
VLAN0090	5	0	0	2	7
VLAN0099	0	0	0	7	7
VLAN0100	5	0	0	2	7
VLAN0110	4	0	0	3	7
VLAN0120	4	0	0	3	7
VLAN0130	4	0	0	3	7
VLAN0140	4	0	0	3	7
VLAN0150	4	0	0	3	7
VLAN0160	4	0	0	3	7
VLAN0170	4	0	0	3	7
VLAN01000	0	0	0	7	7

21 vlans	76	0	0	71	147

```
SW-LMCentral-CORE2#
```

Figura 65*Configuración de STP del SW-LM-Access01 al 05*

```
SW-LM-Access01#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast            is disabled
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN00001	1	0	0	2	3
VLAN00010	0	0	0	3	3
VLAN00020	1	0	0	2	3
VLAN00030	1	0	0	2	3
VLAN00040	1	0	0	2	3
VLAN00050	1	0	0	2	3
VLAN00060	1	0	0	2	3
VLAN00070	1	0	0	2	3
VLAN00080	3	0	0	0	3
VLAN00085	1	0	0	2	3
VLAN00090	1	0	0	2	3
VLAN00099	3	0	0	0	3
VLAN0100	2	0	0	1	3
VLAN0110	1	0	0	2	3
VLAN0120	1	0	0	2	3
VLAN0130	1	0	0	2	3
VLAN0140	1	0	0	2	3
VLAN0150	1	0	0	2	3
VLAN0160	1	0	0	2	3
VLAN0170	1	0	0	2	3
VLAN01000	3	0	0	0	3
21 vlans	27	0	0	36	63

Configuración Interfaz Virtual Switch (SVI)

La interfaz SVI fue configurada dentro de la VLAN administrativa (VLAN 150 – Gestión) en cada switch de la red. A continuación, se presenta la configuración correspondiente de la interfaz SVI implementada en los switches de la empresa, la cual permite la administración y supervisión centralizada de los dispositivos de red.

Figura 66*Configuración de Interfaz SVI - Switch SW-LMCentral-CORE1*

```
SW-LMCentral-CORE1#show vlan id 150
```

VLAN Name	Status	Ports
150 Gestion	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	0	0

```
SW-LMCentral-CORE1#show interfaces vlan 150
Vlan150 is up, line protocol is up
Hardware is CPU Interface, address is 000d.bd01.b302 (bia 000d.bd01.b302)
Internet address is 172.16.14.252/24
```

Figura 67*Configuración de Interfaz SVI - Switch SW-LMCentral-CORE2*

```
SW-LMCentral-CORE2#show vlan id 150
```

VLAN	Name	Status	Ports
150	Gestion	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	-	0	0


```
SW-LMCentral-CORE2#show interfaces vlan 150
Vlan150 is up, line protocol is up
Hardware is CPU Interface, address is 00e0.f953.6003 (bia 00e0.f953.6003)
Internet address is 172.16.14.253/24
```

Figura 68*Configuración de Interfaz SVI - Switch SW-LM-Access01*

```
SW-LM-Access01#show vlan id 150
```

VLAN	Name	Status	Ports
150	Gestion	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	-	0	0


```
SW-LM-Access01#show interfaces vlan 150
Vlan150 is up, line protocol is up
Hardware is CPU Interface, address is 00d0.bc6e.db01 (bia 00d0.bc6e.db01)
Internet address is 172.16.14.1/24
```

Figura 69*Configuración de Interfaz SVI - Switch SW-LM-Access02*

```
SW-LM-Access02#show vlan id 150
```

VLAN	Name	Status	Ports
150	Gestion	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	-	0	0


```
SW-LM-Access02#show interfaces vlan 150
Vlan150 is up, line protocol is up
Hardware is CPU Interface, address is 0000.0c0c.7e01 (bia 0000.0c0c.7e01)
Internet address is 172.16.14.2/24
```

Figura 70*Configuración de Interfaz SVI - Switch SW-LM-Access03*

```
SW-LM-Access03#show vlan id 150
```

VLAN Name	Status	Ports
150 Gestion	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150 enet	100150	1500	-	-	-	-	-	0	0

```
SW-LM-Access03#show interfaces vlan 150
Vlan150 is up, line protocol is up
  Hardware is CPU Interface, address is 0000.0c2c.6c01 (bia 0000.0c2c.6c01)
  Internet address is 172.16.14.3/24
```

Figura 71*Configuración de Interfaz SVI - Switch SW-LM-Access04*

```
SW-LM-Access04#show vlan id 150
```

VLAN Name	Status	Ports
150 Gestion	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150 enet	100150	1500	-	-	-	-	-	0	0

```
SW-LM-Access04#show interfaces vlan 150
Vlan150 is up, line protocol is up
  Hardware is CPU Interface, address is 0007.ec9b.9601 (bia 0007.ec9b.9601)
  Internet address is 172.16.14.4/24
```

Figura 72*Configuración de Interfaz SVI - Switch SW-LM-Access05*

```
SW-LM-Access05#show vlan id 150
```

VLAN Name	Status	Ports
150 Gestion	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150 enet	100150	1500	-	-	-	-	-	0	0

```
SW-LM-Access05#show interfaces vlan 150
Vlan150 is up, line protocol is up
  Hardware is CPU Interface, address is 0009.7c2d.0001 (bia 0009.7c2d.0001)
  Internet address is 172.16.14.5/24
```

Figura 73*Configuración de Interfaz SVI - Switch Sw-Paso1*

```
Sw-Paso1#show vlan id 150
```

VLAN	Name	Status	Ports
150	Gestion	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	-	0	0


```
Sw-Paso1#show interfaces vlan 150
Vlan150 is up, line protocol is up
  Hardware is CPU Interface, address is 0000.0c32.a201 (bia 0000.0c32.a201)
  Internet address is 172.16.14.6/24
```

Figura 74*Configuración de Interfaz SVI - Switch Sw-Paso2*

```
Sw-Paso2#show vlan id 150
```

VLAN	Name	Status	Ports
150	Gestion	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	-	0	0


```
Sw-Paso2#show interfaces vlan 150
Vlan150 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.5c08.2001 (bia 0060.5c08.2001)
  Internet address is 172.16.14.7/24
```

Figura 75*Configuración de Interfaz SVI - Switch Sw-Paso3*

```
Sw-Paso3#show vlan id 150
```

VLAN	Name	Status	Ports
150	Gestion	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
150	enet	100150	1500	-	-	-	-	-	0	0


```
Sw-Paso3#show interfaces vlan 150
Vlan150 is up, line protocol is up
  Hardware is CPU Interface, address is 0030.a328.e601 (bia 0030.a328.e601)
  Internet address is 172.16.14.8/24
```

Configuración Puerto Troncal (Trunk)

En el diseño de la red se emplean interfaces troncales entre los switches con el objetivo de transportar múltiples VLAN a través de un único enlace físico. Esta configuración permite la segmentación lógica del tráfico de red, optimizando el uso de la infraestructura y facilitando la interconexión entre los switches de acceso, distribución y núcleo. Asimismo, se garantiza la correcta propagación de las VLAN definidas en la red, manteniendo la separación del tráfico y asegurando la escalabilidad y flexibilidad del diseño.

A continuación, se mostrará la configuración de los puertos troncales en los switches de capa de acceso y Core.

Figura 76

Configuración Puerto Troncal - Switch SW-LMCentral-CORE1

```
SW-LMCentral-CORE1(config)#interface range gigabitEthernet1/0/1-8
SW-LMCentral-CORE1(config-if-range)# switchport mode trunk
SW-LMCentral-CORE1(config-if-range)# switchport trunk native vlan 99
SW-LMCentral-CORE1(config-if-range)# switchport trunk allowed vlan 10,20,30,40,50,60,70,80,85,90,100,110,120,130,140,150,160,170,99
SW-LMCentral-CORE1(config-if-range)# no shutdown
SW-LMCentral-CORE1(config-if-range)#end
```

```
SW-LMCentral-CORE1#show interfaces trunk
Port          Mode          Encapsulation  Status        Native vlan
Gig1/0/1      on            802.1q         trunking      99
Gig1/0/2      on            802.1q         trunking      99
Gig1/0/3      on            802.1q         trunking      99
Gig1/0/4      on            802.1q         trunking      99
Gig1/0/5      on            802.1q         trunking      99
Gig1/0/6      on            802.1q         trunking      99
Gig1/0/7      on            802.1q         trunking      99
Gig1/0/8      on            802.1q         trunking      99

Port          Vlans allowed on trunk
Gig1/0/1      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/2      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/3      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/4      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/5      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/6      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/7      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/8      10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
```

Figura 77*Configuración Puerto Troncal - Switch SW-LMCentral-CORE2*

```
SW-LMCentral-CORE2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig1/0/1	on	802.1q	trunking	99
Gig1/0/2	on	802.1q	trunking	99
Gig1/0/3	on	802.1q	trunking	99
Gig1/0/4	on	802.1q	trunking	99
Gig1/0/5	on	802.1q	trunking	99
Gig1/0/6	on	802.1q	trunking	99
Gig1/0/7	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig1/0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/3	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/4	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/5	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/6	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig1/0/7	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 78*Configuración Puerto Troncal - Switch SW-LM-Access01*

```
SW-LM-Access01#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 79*Configuración Puerto Troncal - Switch SW-LM-Access02*

```
SW-LM-Access02#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 80*Configuración Puerto Troncal - Switch SW-LM-Access03*

```
SW-LM-Access03#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 81*Configuración Puerto Troncal - Switch SW-LM-Access04*

```
SW-LM-Access04#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 82*Configuración Puerto Troncal - Switch SW-LM-Access05*

```
SW-LM-Access05#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 83*Configuración Puerto Troncal - Switch SW-LM-Sw-Paso1*

```
Sw-Paso1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 84*Configuración Puerto Troncal - Switch SW-LM-Sw-Paso2*

```
Sw-Paso2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Gig0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170
Gig0/2	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Figura 85*Configuración Puerto Troncal - Switch SW-LM-Sw-Paso3*

```
Sw-Paso3#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Gig0/1	10,20,30,40,50,60,70,80,85,90,99-100,110,120,130,140,150,160,170

Las interfaces configuradas como enlaces troncales fueron establecidas en modo trunk utilizando el estándar IEEE 802.1Q, definiendo la VLAN 99 como VLAN nativa y restringiendo las VLANs permitidas a aquellas necesarias para la operación de la red, con el fin de mejorar la seguridad y la organización del tráfico.

Configuración de HSRP

En este trabajo de aplicación profesional se implementa el protocolo HSRP con el fin de asegurar la alta disponibilidad de la red y evitar puntos únicos de falla en la puerta de enlace. Mediante la creación de un Gateway virtual, HSRP permite que, ante la caída del equipo activo, el dispositivo de respaldo asuma automáticamente el enrutamiento, garantizando la continuidad del servicio para las VLAN y los usuarios finales.

A continuación, se mostrará la configuración HSRP de los switches Core.

Figura 86

Configuración HSRP - Switch SW-LMCentral-CORE1

```
SW-LMCentral-CORE1#show standby brief
```

P indicates configured to preempt.							
Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl110	10	110	P	Active	local	172.16.0.253	172.16.0.254
Vl150	10	110	P	Active	local	172.16.14.253	172.16.14.254
Vl170	170	110	P	Active	local	172.16.16.253	172.16.16.251
Vl120	10	110	P	Active	local	172.16.1.253	172.16.1.254
Vl130	10	110	P	Active	local	172.16.2.253	172.16.2.254
Vl140	10	110	P	Active	local	172.16.3.253	172.16.3.254
Vl150	10	110	P	Active	local	172.16.4.253	172.16.4.254
Vl160	10	110	P	Active	local	172.16.5.253	172.16.5.254
Vl170	10	110	P	Active	local	172.16.6.253	172.16.6.254
Vl185	10	110	P	Active	local	172.16.7.253	172.16.7.254
Vl190	10	110	P	Active	local	172.16.8.253	172.16.8.254
Vl100	10	110	P	Active	local	172.16.9.253	172.16.9.254
Vl110	10	110	P	Active	local	172.16.10.253	172.16.10.254
Vl120	10	110	P	Active	local	172.16.11.253	172.16.11.254
Vl130	10	110	P	Active	local	172.16.12.253	172.16.12.254
Vl140	10	110	P	Active	local	172.16.13.253	172.16.13.254
Vl160	10	110	P	Active	local	172.16.15.253	172.16.15.254

```
SW-LMCentral-CORE1#
```

Figura 87*Configuración HSRP - Switch SW-LMCentral-CORE2*

```
SW-LMCentral-CORE2#show standby brief
```

P indicates configured to preempt.

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl110	10	100	P	Standby	172.16.0.252	local	172.16.0.254
Vl1170	170	100	P	Standby	172.16.16.252	local	172.16.16.251
Vl1150	10	100	P	Standby	172.16.14.252	local	172.16.14.254
Vl120	10	100	P	Standby	172.16.1.252	local	172.16.1.254
Vl130	10	100	P	Standby	172.16.2.252	local	172.16.2.254
Vl140	10	100	P	Standby	172.16.3.252	local	172.16.3.254
Vl150	10	100	P	Standby	172.16.4.252	local	172.16.4.254
Vl160	10	100	P	Standby	172.16.5.252	local	172.16.5.254
Vl170	10	100	P	Standby	172.16.6.252	local	172.16.6.254
Vl185	10	100	P	Standby	172.16.7.252	local	172.16.7.254
Vl190	10	100	P	Standby	172.16.8.252	local	172.16.8.254
Vl1100	10	100	P	Standby	172.16.9.252	local	172.16.9.254
Vl1110	10	100	P	Standby	172.16.10.252	local	172.16.10.254
Vl1120	10	100	P	Standby	172.16.11.252	local	172.16.11.254
Vl1130	10	100	P	Standby	172.16.12.252	local	172.16.12.254
Vl1140	10	100	P	Standby	172.16.13.252	local	172.16.13.254
Vl1160	10	100	P	Standby	172.16.15.252	local	172.16.15.254

```
SW-LMCentral-CORE2#
```

Configuración del Protocolo DHCP

El servicio DHCP ha sido implementado directamente en los switches de núcleo (Core1 y Core2) de la red empresarial, con el objetivo de garantizar alta disponibilidad y redundancia en la asignación automática de direcciones IP. Al contar con dos switches Core en esquema de respaldo, se evita la dependencia de un único servidor y se asegura la continuidad del servicio ante posibles fallas.

Asimismo, los switches Core gestionan de forma centralizada el servicio DHCP tanto para la sede principal como para las dos sucursales, permitiendo una administración unificada del direccionamiento IP en toda la red corporativa. Para las redes remotas, se emplea el comando `ip helper-address` a fin de reenviar las solicitudes DHCP hacia el núcleo, mientras que las VLANs locales no requieren dicha configuración.

Por otro lado, las VLANs destinadas a funciones de control y seguridad, como la VLAN Nativa y la VLAN Black Hole, no cuentan con configuración DHCP, ya que no están orientadas al uso de usuarios finales.

A continuación, se mostrará la configuración DHCP de los switches Core.

Figura 88

Configuración DHCP - Switch SW-LMCentral-CORE1 y 2

```

ip dhcp pool VLAN10-Gerencia
network 172.16.0.0 255.255.255.0
default-router 172.16.0.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN10Gerencia
network 172.16.0.0 255.255.255.0
default-router 172.16.0.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN20Logstica
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN30Contabilidad
network 172.16.2.0 255.255.255.0
default-router 172.16.2.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN40RRHH
network 172.16.3.0 255.255.255.0
default-router 172.16.3.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN50Adm/Marke
network 172.16.4.0 255.255.255.0
default-router 172.16.4.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN60Ventas-1
network 172.16.5.0 255.255.255.0
default-router 172.16.5.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN100WiFi-Guest
network 172.16.9.0 255.255.255.0
default-router 172.16.9.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN110WiFi-Operaciones
network 172.16.10.0 255.255.255.0
default-router 172.16.10.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN140SoporteTI
network 172.16.13.0 255.255.255.0
default-router 172.16.13.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN70Ventas-2
network 172.16.6.0 255.255.255.0
default-router 172.16.6.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN85ATC
network 172.16.7.0 255.255.255.0
default-router 172.16.7.254
dns-server 8.8.8.8
domain-name g4s.com
ip dhcp pool VLAN90Seguridad
network 172.16.8.0 255.255.255.0
default-router 172.16.8.254
dns-server 8.8.8.8
domain-name g4s.com

ip dhcp excluded-address 172.16.0.1 172.16.0.10
ip dhcp excluded-address 172.16.1.1 172.16.1.10
ip dhcp excluded-address 172.16.2.1 172.16.2.10
ip dhcp excluded-address 172.16.3.1 172.16.3.10
ip dhcp excluded-address 172.16.4.1 172.16.4.10
ip dhcp excluded-address 172.16.5.1 172.16.5.10
ip dhcp excluded-address 172.16.6.1 172.16.6.10
ip dhcp excluded-address 172.16.7.1 172.16.7.10
ip dhcp excluded-address 172.16.8.1 172.16.8.10
ip dhcp excluded-address 172.16.9.1 172.16.9.10
ip dhcp excluded-address 172.16.10.1 172.16.10.10
ip dhcp excluded-address 172.16.13.1 172.16.13.10

```

Configuración Enrutamiento Dinámico OSPF

En el presente proyecto se implementó, mediante simulación, el protocolo de enrutamiento dinámico OSPF (Open Shortest Path First) con el objetivo de evaluar la interconexión entre la sede principal, las sedes remotas y los enlaces WAN. Para este diseño se definió el área 0 como el backbone del dominio OSPF, asignándolo a los enlaces WAN,

mientras que la sede principal, la Sucursal 1 y la Sucursal 2 fueron configuradas en las áreas 1, 2 y 3, respectivamente.

El direccionamiento IP interno considerado en la simulación corresponde a los bloques 172.16.0.0/18 para la sede principal, 172.16.64.0/18 para la Sucursal 1 y 172.16.128.0/18 para la Sucursal 2, los cuales son anunciados dinámicamente mediante OSPF. Las direcciones IP de los enlaces WAN, configuradas con máscaras /30, representan direccionamiento del proveedor y se utilizan únicamente para la interconexión entre sedes bajo una topología Hub and Spoke.

Esta implementación simulada de OSPF permite validar el diseño de enrutamiento propuesto y analizar su comportamiento en un entorno empresarial de ventas.

Figura 89

Configuración Enrutamiento OSPF - SW-LMCentral-CORE1 y 2

```
SW-LMCentral-CORE1#show ip route ospf
 10.0.0.0/30 is subnetted, 8 subnets
O IA   10.10.0.0 [110/130] via 172.16.16.249, 00:06:30, Vlan170
        [110/130] via 172.16.16.250, 00:06:30, Vlan170
O IA   10.10.1.0 [110/66] via 172.16.16.250, 00:06:30, Vlan170
O IA   10.10.2.0 [110/66] via 172.16.16.249, 00:06:30, Vlan170
        [110/66] via 172.16.16.250, 00:06:30, Vlan170
O IA   10.10.3.0 [110/66] via 172.16.16.249, 00:06:30, Vlan170
O IA   10.10.4.0 [110/67] via 172.16.16.250, 00:06:30, Vlan170
O IA   10.10.5.0 [110/3] via 172.16.16.250, 00:06:30, Vlan170
O IA   10.10.6.0 [110/2] via 172.16.16.249, 00:06:30, Vlan170
O IA   10.10.7.0 [110/2] via 172.16.16.250, 00:06:30, Vlan170
 172.16.0.0/16 is variably subnetted, 60 subnets, 3 masks
O IA   172.16.64.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.65.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.66.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.67.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.68.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.69.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.70.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.71.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.72.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.73.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.74.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.75.0 [110/69] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.76.248 [110/68] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.128.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.129.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.130.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.131.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.132.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.133.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.134.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.135.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.136.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.137.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.138.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.139.0 [110/5] via 172.16.16.250, 00:06:30, Vlan170
O IA   172.16.140.248 [110/4] via 172.16.16.250, 00:06:30, Vlan170
```

```

SW-LMCentral-CORE1#show ip route connected
C    172.16.0.0/24    is directly connected, Vlan10
C    172.16.1.0/24    is directly connected, Vlan20
C    172.16.2.0/24    is directly connected, Vlan30
C    172.16.3.0/24    is directly connected, Vlan40
C    172.16.4.0/24    is directly connected, Vlan50
C    172.16.5.0/24    is directly connected, Vlan60
C    172.16.6.0/24    is directly connected, Vlan70
C    172.16.7.0/24    is directly connected, Vlan85
C    172.16.8.0/24    is directly connected, Vlan90
C    172.16.9.0/24    is directly connected, Vlan100
C    172.16.10.0/24   is directly connected, Vlan110
C    172.16.11.0/24   is directly connected, Vlan120
C    172.16.12.0/24   is directly connected, Vlan130
C    172.16.13.0/24   is directly connected, Vlan140
C    172.16.14.0/24   is directly connected, Vlan150
C    172.16.15.0/24   is directly connected, Vlan160
C    172.16.16.248/29 is directly connected, Vlan170

```

Configuración Enrutamiento Estático

La configuración de rutas estáticas por defecto con redundancia fue implementada en ambos switches de núcleo, con el fin de garantizar la continuidad del servicio de enrutamiento ante fallas de uno de los dispositivos Core. Esta arquitectura permite que cualquiera de los switches asuma el rol activo, manteniendo la conectividad hacia redes externas mediante un Gateway principal y uno secundario, definidos a través de la distancia administrativa. A continuación, se mostrará la configuración del enrutamiento estático en el switch Core.

Figura 90

Configuración Enrutamiento Estático - Switch SW-LMCentral-CORE1 y 2

```

ip route 0.0.0.0 0.0.0.0 172.16.16.249
ip route 0.0.0.0 0.0.0.0 172.16.16.250 100

```

Seguridad de Inicio de Sesión

En la configuración de seguridad de inicio de sesión se consideró la implementación de contraseñas robustas tanto para el modo usuario como para el modo privilegiado en los switches de la empresa. Estas credenciales fueron configuradas con mecanismos de encriptación, con la finalidad de fortalecer la seguridad y prevenir accesos no autorizados a la infraestructura de red.

Adicionalmente, se implementó un servidor RADIUS centralizado, en el cual se registraron todos los dispositivos de red seleccionados para el desarrollo del proyecto. Cada equipo de red fue asociado en el servidor RADIUS mediante su nombre de dispositivo (hostname) y su dirección IP de gestión, permitiendo así una administración centralizada y un control más estricto de los accesos.

De esta manera, la infraestructura cuenta tanto con usuarios locales configurados en cada dispositivo de red, utilizados como mecanismo de respaldo, como con autenticación centralizada a través del servidor RADIUS, lo que mejora la escalabilidad, la trazabilidad de accesos y la seguridad general del sistema.

A continuación, se presenta la configuración correspondiente a la seguridad de inicio de sesión, la cual fue aplicada de manera uniforme en todos los switches que conforman la red empresarial.

Figura 91

Configuración Seguridad de Inicio de Sesión

```
SW-LM-Access05#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-LM-Access05(config)#no ip domain-lookup
SW-LM-Access05(config)#banner motd #
Enter TEXT message.  End with the character '#'.
*****
*                                     *
*              CONEXA - RED CORPORATIVA              *
*                                     *
*  AVISO LEGAL:                                     *
*  Este sistema es de uso exclusivo de CONEXA.         *
*  El acceso est permitido nicamente a personal      *
*  autorizado.                                         *
*                                     *
*  Cualquier acceso no autorizado ser monitoreado    *
*  y sancionado conforme a las polticas internas     *
*  y la normativa vigente.                           *
*                                     *
*****
#

SW-LM-Access05(config)#username userlocal01 password C1sc0
SW-LM-Access05(config)#username userlocal02 password C1sc0
SW-LM-Access05(config)#line console 0
SW-LM-Access05(config-line)#login local
SW-LM-Access05(config-line)#exec-timeout 1 30
SW-LM-Access05(config-line)#exit
SW-LM-Access05(config)#enable secret sMU19HS463$q
SW-LM-Access05(config)#service password-encryption
SW-LM-Access05(config)#aaa new-model
SW-LM-Access05(config)#radius-server host 172.16.12.12 key abc123
SW-LM-Access05(config)#aaa authentication login default group radius local
```

A continuación, se presenta la configuración correspondiente a la autenticación AAA con RADIUS de inicio de sesión para la gestión de equipos de red, la cual fue aplicada de manera uniforme en todos los switches que conforman la red empresarial.

Figura 92

Configuración Seguridad de Inicio de Sesión - Autenticación AAA

```
SW-LM-Access05(config)#aaa new-model
SW-LM-Access05(config)#radius-server host 172.16.12.12 key abc123
SW-LM-Access05(config)#aaa authentication login default group radius local
```

```
SW-LM-Access04#show running-config | section aaa
aaa new-model
aaa authentication login default group radius local
SW-LM-Access04#show running-config | include radius
aaa authentication login default group radius local
radius-server host 172.16.12.12 auth-port 1645 key abc123
SW-LM-Access04#show running-config | section vty
line vty 0 4
  login authentication default
  transport input ssh
line vty 5 15
SW-LM-Access04#
```

The screenshot shows the RADIUS configuration window with the 'Services' tab selected. The 'AAA' section is active, showing 'Service' as 'On' and 'Radius Port' as '1645'. Below this, the 'Network Configuration' section contains fields for 'Client Name', 'Client IP', 'Secret', and 'ServerType' (set to 'Radius'). A table lists six configured clients, all using 'Radius' as the server type and 'abc123' as the key. The 'User Setup' section at the bottom shows a table with two users: 'jequis' and 'svilca-ext', each with a unique password.

	Client Name	Client IP	Server Type	Key
1	SW-ORQUIDEAS-CORE	172.16.139.1	Radius	abc123
2	SW-ORQUIDEAS-Access01	172.16.139.2	Radius	abc123
3	SW-ORQUIDEAS-Access02	172.16.139.3	Radius	abc123
4	SW-ORQUIDEAS-Access03	172.16.139.4	Radius	abc123
5	SW-ORQUIDEAS-Access04	172.16.139.5	Radius	abc123
6	SWLM-Access01	172.16.14.1	Radius	abc123

	Username	Password
1	jequis	NyPr3ybq%07@
2	svilca-ext	3e%62Q3346ff

Configuración de Acceso Remoto Seguro mediante SSH

Se ha implementado el protocolo SSH (Secure Shell) en todos los switches de la empresa con el objetivo de garantizar la seguridad en el acceso remoto a los equipos de red, protegiendo la información intercambiada durante las sesiones de administración.

Esta configuración fue aplicada de manera uniforme en todos los switches de la organización, permitiendo una administración segura y centralizada mediante el uso de un servidor RADIUS para la autenticación de usuarios. Adicionalmente, se configuraron usuarios locales como mecanismo de contingencia, asegurando el acceso administrativo en caso de indisponibilidad del servidor de autenticación centralizado.

Asimismo, se estableció una segunda capa de seguridad a través de la contraseña del modo privilegiado, la cual es requerida para realizar cambios en la configuración de los equipos, fortaleciendo así el control de acceso y la protección de la infraestructura de red.

Figura 93

Configuración Security Shell (SSH)

```
SW-G4S-Acces01(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
SW-G4S-Acces01(config)#ip domain-name www.conexa.com
SW-G4S-Acces01(config)#ip ssh authentication-retries 3
SW-G4S-Acces01(config)#ip ssh time-out 90
SW-G4S-Acces01(config)#crypto key generate rsa
The name for the keys will be: SW-G4S-Acces01.www.conexa.com
Choose the size of the key modulus in the range of 360 to 4096 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]

SW-G4S-Acces01(config)#line vty 0 4
*Feb 1 2:25:0.44: %SSH-5-ENABLED: SSH 2 has been enabled
SW-G4S-Acces01(config-line)#login authentication default
SW-G4S-Acces01(config-line)#transport input ssh
SW-G4S-Acces01(config-line)#end
SW-G4S-Acces01#wr
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
SW-G4S-Acces01#
```

Configuración SNMP

Se ha configurado SNMP con la finalidad de monitorear la red con el software PRTG. A continuación, se mostrará la configuración de SNMP. Dicha configuración se replicó en todos los switches de la empresa de ventas.

Figura 94

Configuración SNMP

```
SW-IMCentral-CORE1(config)#snmp-server community RedesCisco rw
%SNMP-5-WARMSTART: SNMP agent on host SW-IMCentral-CORE1 is undergoing a warm start
SW-IMCentral-CORE1(config)#
```

Configuración PRTG

Se ha implementado el sistema de monitoreo PRTG Network Monitor con la finalidad de garantizar el adecuado rendimiento de la red, asegurar la disponibilidad de los equipos y optimizar el uso del ancho de banda. Asimismo, esta herramienta permite la configuración de notificaciones, alarmas e informes, lo que facilita la supervisión continua de los servicios.

Cabe precisar que, debido a que el software Packet Tracer no permite la implementación directa de herramientas de monitoreo como PRTG, dicha configuración se ha realizado en un entorno real correspondiente a la empresa. En el PRTG se procedió a registrar los equipos de red de la empresa, configurando el sensor PING con el objetivo de monitorear la disponibilidad y el estado operativo de los dispositivos de red.

A continuación, se presentará la configuración de los equipos de red y del sensor PING en PRTG. De igual manera, se detallará la configuración de las notificaciones e informes generados por el sistema de monitoreo.

Figura 95

Configuración PRTG

Página principal

Dispositivos

Bibliotecas

Sensores

Alarmas

Mapas

Informes

Registro

Tiquetes

Configuración

Dispositivos

Grupo Raíz

Resumen

2 días

30 días

365 días

Alarmas

Log

Gestión

1

W 1

✓ 24

(de 26)

S

M

L

XL

SEDE PRINCIPAL – CENTRAL TOWER

SW-LMCentral-CORE2

✓ Ping

SWLM-Access01

✓ Ping

SWLM-Access02

✓ Ping

SWLM-Access03

✓ Ping

SWLM-Access04

✓ Ping

SWLM-Access05

✓ Ping

Sw-Paso1

✓ Ping

Sw-Paso2

✓ Ping

Sw-Paso3

✓ Ping

SW-LMCentral-CORE1

✓ Ping

SEDE SUCURSAL – SAN ISIDRO G4S

SW-G4S-CORE

✓ Ping

SW-G4S-Access01

✓ Ping

SW-G4S-Access02

✓ Ping

SW-G4S-Access03

✓ Ping

SW-G4S-Access04

✓ Ping

Figura 96

Configuración PRTG – Logs

Página principal Dispositivos Bibliotecas Sensores Alarmas Mapas Informes Registro Tiquetes Configuración									
Nuevas entradas de log 23									
1/2/2026 15:49:15	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-Access03	+	Ping	OK	0 ms			
1/2/2026 15:49:13	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access04	+	Ping	OK	0 ms			
1/2/2026 15:49:11	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access03	+	Ping	OK	0 ms			
1/2/2026 15:49:09	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access02	+	Ping	OK	0 ms			
1/2/2026 15:49:07	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access01	+	Ping	OK	0 ms			
1/2/2026 15:49:05	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-CORE	+	Ping	OK	0 ms			
1/2/2026 15:49:01	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-Access02	+	Ping	OK	0 ms			
1/2/2026 15:48:59	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-Access01	+	Ping	OK	0 ms			
1/2/2026 15:48:57	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-CORE	+	Ping	OK	0 ms			
1/2/2026 15:48:55	SEDE PRINCIPAL – CENTRAL TOW...	SW-LMCentral-CORE1	+	Ping	OK	0 ms			
1/2/2026 15:48:53	SEDE PRINCIPAL – CENTRAL TOW...	Sw-Paso3	+	Ping	OK	0 ms			
1/2/2026 15:48:51	SEDE PRINCIPAL – CENTRAL TOW...	Sw-Paso2	+	Ping	OK	0 ms			
1/2/2026 15:48:19	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-Access03			Objeto secundario creado	Sensor 'Ping'			
1/2/2026 15:48:19	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-Access03	+	Ping	Desconocido	Aun no hay datos			
1/2/2026 15:48:19	SEDE SUCURSAL – SAN ISIDRO G4S	SW-G4S-Access03	+	Ping	Generado	Consulte el historial del objeto para obtener detalles.			
1/2/2026 15:48:11	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access04			Objeto secundario creado	Sensor 'Ping'			
1/2/2026 15:48:11	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access04	+	Ping	Desconocido	Aun no hay datos			
1/2/2026 15:48:11	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access04	+	Ping	Generado	Consulte el historial del objeto para obtener detalles.			
1/2/2026 15:48:02	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access03			Objeto secundario creado	Sensor 'Ping'			
1/2/2026 15:48:02	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access03	+	Ping	Desconocido	Aun no hay datos			
1/2/2026 15:48:02	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access03	+	Ping	Generado	Consulte el historial del objeto para obtener detalles.			
1/2/2026 15:48:00	SEDE PRINCIPAL – CENTRAL TOW...	Sw-Paso2	+	Ping	Desconocido	Este sensor no ha recibido datos por 163 segundos.			
1/2/2026 15:48:00	SEDE PRINCIPAL – CENTRAL TOW...	Sw-Paso3	+	Ping	Desconocido	Este sensor no ha recibido datos por 160 segundos.			
1/2/2026 15:48:00	SEDE PRINCIPAL – CENTRAL TOW...	SW-LMCentral-CORE1	+	Ping	Desconocido	Este sensor no ha recibido datos por 157 segundos.			
1/2/2026 15:47:32	SEDE SUCURSAL – SAN ISIDRO OR...	SW-ORQUIDEAS-Access02			Objeto secundario creado	Sensor 'Ping'			

Pruebas Operativas y Resultados

Se realizaron diversas pruebas en esta implementación, a continuación, se presentarán los resultados exitosos que se realizaron en los equipos de red propuestos utilizando el software Packet Tracer.

Pruebas Operativas de la Solución de DHCP

En la red actual de la empresa, el servicio DHCP se encuentra implementado en un servidor basado en Windows Server 2012, operando como único punto de asignación dinámica de direcciones IP. Debido a esta arquitectura, el servicio DHCP no se encuentra configurado directamente en los switches de núcleo (SW_CORE), siendo necesario el uso del agente retransmisor DHCP (DHCP Helper) para permitir la asignación de direcciones IP a las distintas VLANs de la red.

En la propuesta de mejora, se plantea la implementación del servicio DHCP directamente en los switches CORE, los cuales operan bajo un esquema de alta disponibilidad mediante el protocolo HSRP. Esta configuración permite que ambos switches CORE mantengan la misma configuración del servicio DHCP, garantizando redundancia y continuidad del servicio, de tal manera que, ante la caída de uno de los equipos, el switch CORE de respaldo asume automáticamente la operación sin afectar la asignación de direcciones IP.

Asimismo, esta arquitectura posiciona a los switches CORE como el punto central de provisión del servicio DHCP, no solo para la sede principal, sino también para las sedes remotas, asegurando una gestión centralizada, mayor disponibilidad y una mejora significativa en la confiabilidad del servicio.

A continuación, se presentarán algunas pruebas que validan el correcto funcionamiento del servicio DHCP en las diferentes VLANs de la empresa, así como la conmutación por error del servicio en el entorno de alta disponibilidad propuesto.

Figura 97

Pruebas Operativas y Resultados DHCP - VLAN 10 en SW-LMCentral-CORE1 y 2

```

ip dhcp pool VLAN10Gerencia
network 172.16.0.0 255.255.255.0
default-router 172.16.0.254
dns-server 8.8.8.8
ip dhcp excluded-address 172.16.0.1 172.16.0.10

```

IP address	Client-ID/ Hardware address	Lease expiration	Type
172.16.0.11	0001.4376.7769	--	Automatic

SW-LMCentral-CORE1#

```

SW-LMCentral-CORE2#show ip dhcp binding

```

IP address	Client-ID/ Hardware address	Lease expiration	Type
172.16.0.11	0001.4376.7769	--	Automatic

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 172.16.0.11

Subnet Mask 255.255.255.0

Default Gateway 172.16.0.254

DNS Server 8.8.8.8

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:43FF:FE76:7769

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Pruebas Operativas de la Solución de Port Security

Se está implementando Port Security con la finalidad de reforzar la seguridad de acceso a los puertos de los switches que serán desplegados en la empresa. Para ello, se ha configurado esta funcionalidad de manera que cada puerto de acceso registre una única dirección MAC, permitiendo únicamente la conexión de un solo dispositivo autorizado.

En caso de que un equipo distinto intente conectarse utilizando el mismo puerto de red, el puerto será bloqueado automáticamente, evitando accesos no autorizados y posibles riesgos de seguridad en la red.

A continuación, se realizarán las pruebas correspondientes de Port Security. Para ello, se procederá a desconectar el equipo actualmente conectado al puerto FastEthernet 0/1 y, posteriormente, se conectará un equipo diferente al mismo puerto, con el objetivo de verificar el correcto funcionamiento del mecanismo de seguridad implementado.

Figura 98

Pruebas Operativas y Resultados Port Security – Antes del Bloqueo de Puerto

```
SW-LM-Access01#show port-security interface fastEthernet 0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 2
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0001.4376.7769:10
Security Violation Count : 0

SW-LM-Access01#
```

Al conectar un tercer equipo, el puerto se bloquea porque Port Security solo permite el aprendizaje de dos direcciones MAC.

Figura 99*Pruebas Operativas y Resultados Port Security – Bloqueo de Puerto*

```

interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.4376.7769
 switchport port-security mac-address sticky 0030.A39B.1037
 spanning-tree portfast
 spanning-tree bpduguard enable

```

```

SW-LM-Access01#show port-security interface fastEthernet 0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 2
Total MAC Addresses     : 2
Configured MAC Addresses : 0
Sticky MAC Addresses    : 2
Last Source Address:Vlan : 0002.16A0.004D:10
Security Violation Count : 1

SW-LM-Access01#%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0002.16A0.004D on port FastEthernet0/1.

```

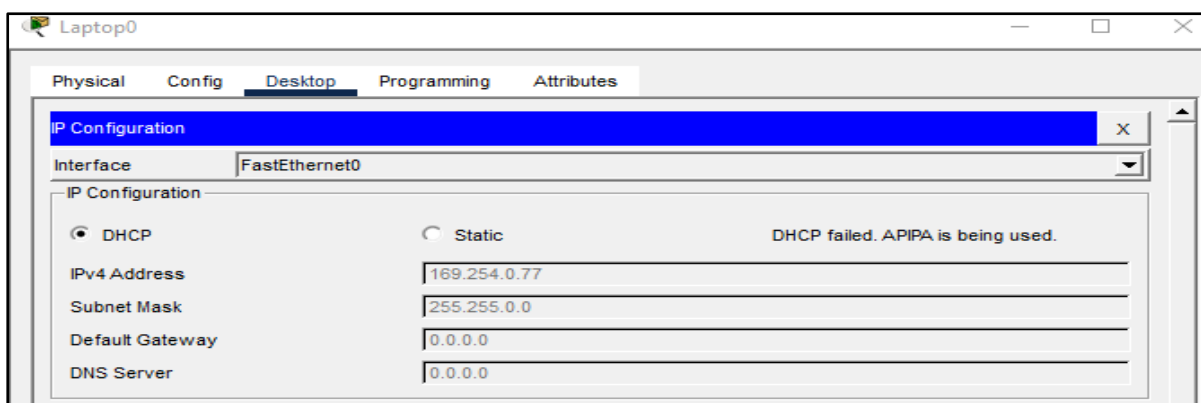
```

SW-LM-Access01#show port-security interface fastEthernet 0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 2
Total MAC Addresses     : 2
Configured MAC Addresses : 0
Sticky MAC Addresses    : 2
Last Source Address:Vlan : 0002.16A0.004D:10
Security Violation Count : 4

SW-LM-Access01#

```

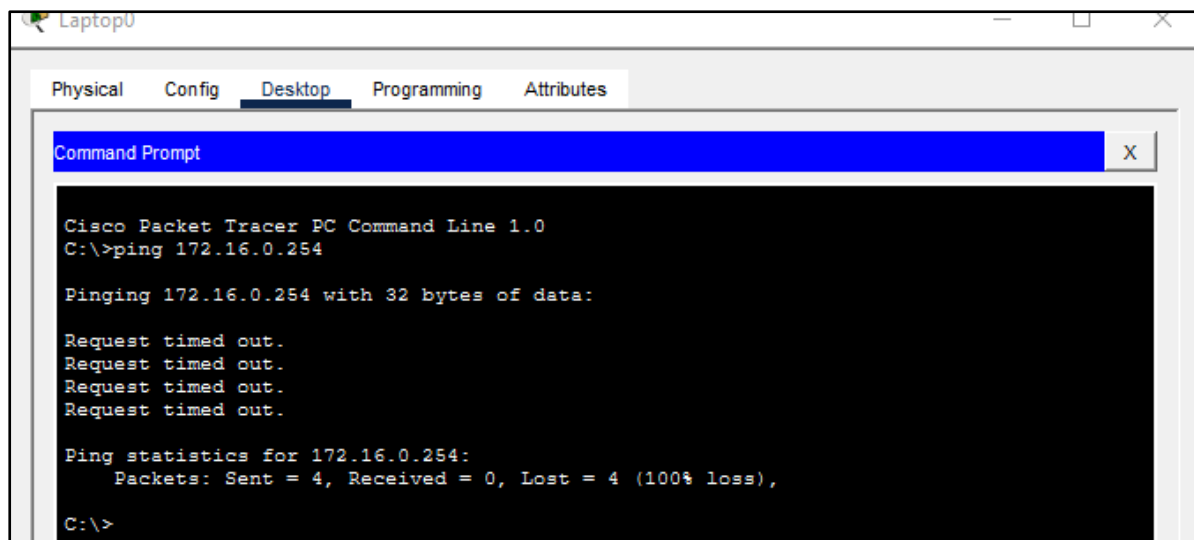
A continuación, se logra visualizar que el nuevo equipo conectado al puerto FastEthernet 0/1 no tiene acceso a la red. Debido a ello, el servidor DHCP no le puede brindar una dirección IP.

Figura 100*Pruebas Operativas y Resultados Port Security - Bloqueo DHCP*

A continuación, se puede visualizar que el nuevo equipo no tiene acceso a la red.

Figura 101

Pruebas Operativas y Resultados Port Security - Bloqueo Ping

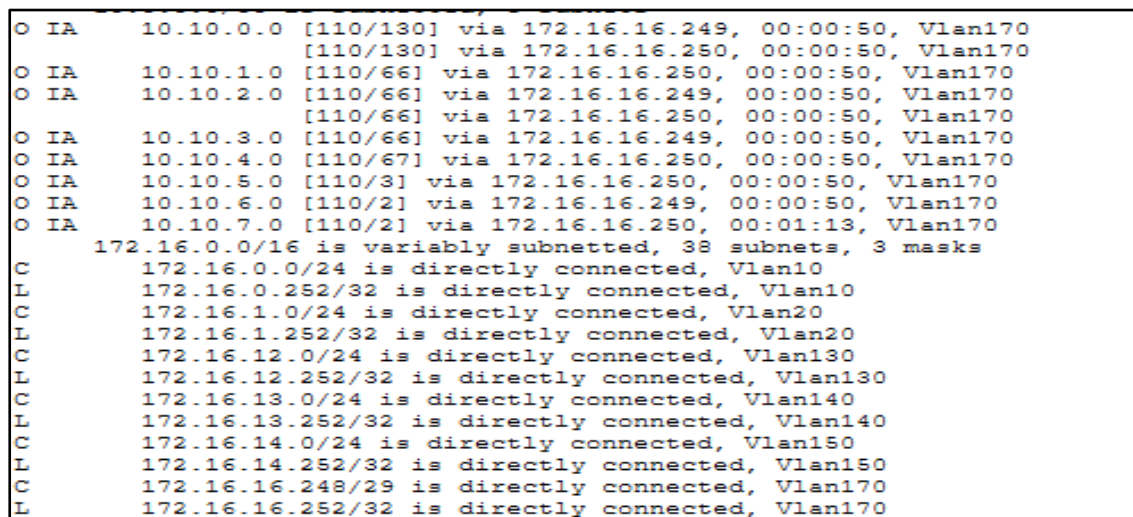


Pruebas Operativas de la Solución de Enrutamiento

A continuación, se visualizará la solución de enrutamiento empleado en la empresa de ventas. Dicha solución fue implementada en los switches CORE y contempla el uso del protocolo de enrutamiento OSPF, con la finalidad de facilitar la administración de la red. Asimismo, se está contemplando el uso de enrutamiento estático con la finalidad de redirigir todo el tráfico de datos a internet y la interconexión WAN.

Figura 102

Pruebas Operativas de la Solución de Enrutamiento



```

O IA 172.16.64.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.65.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.66.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.67.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.68.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.69.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.70.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.71.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.72.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.73.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.74.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.75.0/24 [110/69] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.76.248/29 [110/68] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.128.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.129.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.130.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.131.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.132.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.133.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.134.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.135.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.136.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.137.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.138.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.139.0/24 [110/5] via 172.16.16.250, 00:00:50, Vlan170
O IA 172.16.140.248/29 [110/4] via 172.16.16.250, 00:00:50, Vlan170

```

Ahora bien, la integración de las redes de las sedes remotas las debe realizar el proveedor de internet, en este laboratorio se ha tomado en consideración el área 2 y 3 para la configuración de OSPF en las sedes remotas de la empresa de ventas. A continuación, se visualizarán los resultados exitosos de las pruebas de enrutamiento entre la sede central y las sedes remotas empleando el protocolo OSPF tomando en cuentas los bloques de la sede principal: 172.16.0.0/18 y el bloque IP para sucursal: 172.16.64.0/18.

Figura 103

Prueba de Enrutamiento – Ping PC Sede Principal a Sucursal G4S

```

PC0
Command Prompt
C:\>
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: g4s.com
    Link-local IPv6 Address . . . . .: FE80::201:43FF:FE76:7769
    IPv6 Address . . . . . : ::
    IPv4 Address. . . . . : 172.16.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::
                                   172.16.0.254

Bluetooth Connection:

    Connection-specific DNS Suffix...: g4s.com
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . . : ::
    IPv4 Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : ::
                                   0.0.0.0

```

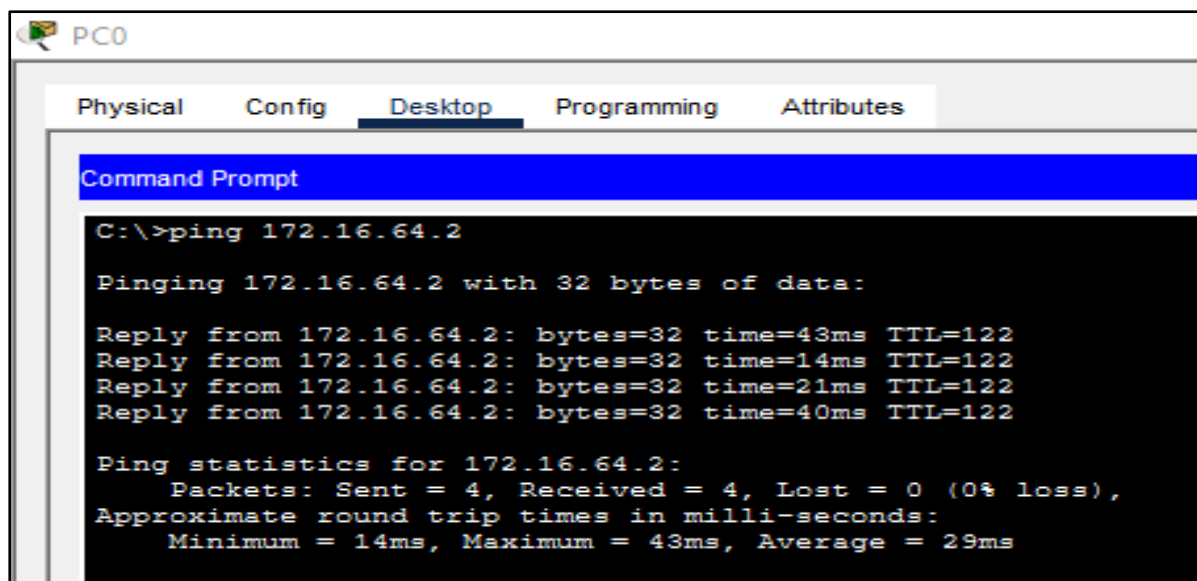
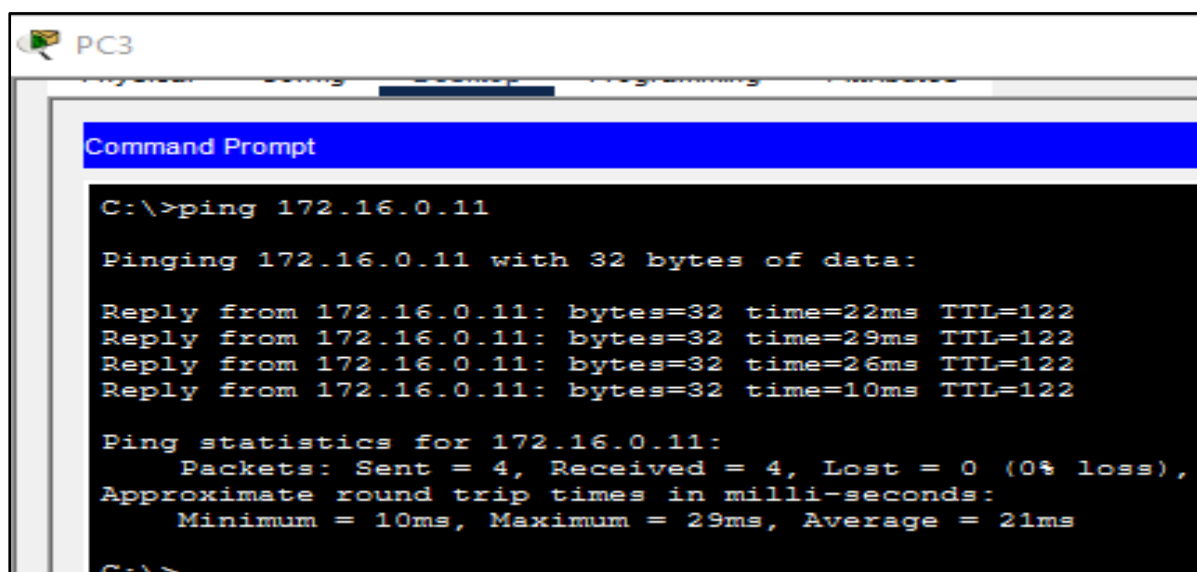
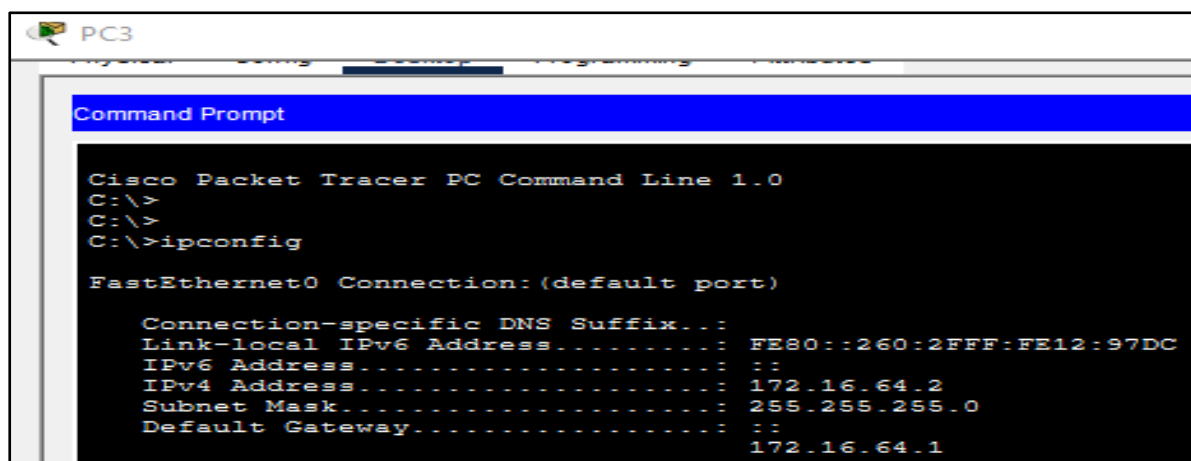


Figura 104

Prueba de Enrutamiento – Ping PC Sucursal G4S a Sede Principal



Pruebas Operativas de la Solución de SSH

Se ha configurado SSH en los switches de la empresa de ventas, con la finalidad de administrar de forma segura estos equipos remotamente.

A continuación, se mostrarán las pruebas realizadas de la solución SSH en los switches de la empresa de ventas donde nos conectaremos de una PC de la Sucursal G4S a los equipos de la sede Principal Central Tower la PC tiene como IP **172.16.64.2/24** perteneciente al bloque **172.16.64.0/18** de esa misma sucursal.

Figura 105

Pruebas Operativas de la Solución SSH – SW-LMCentral-CORE1

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::260:2FFF:FE12:97DC
    IPv6 Address...:
    IPv4 Address...: 172.16.64.2
    Subnet Mask...: 255.255.255.0
    Default Gateway...: 172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...:
    IPv6 Address...:
    IPv4 Address...: 0.0.0.0
    Subnet Mask...: 0.0.0.0
    Default Gateway...: 0.0.0.0

C:\>ssh -l userlocal01 172.16.14.252

Password:
SW-LMCentral-CORE1>en
Password:
SW-LMCentral-CORE1#show ssh
SW-LMCentral-CORE1#show ssh
Connection      Version Mode Encryption      Hmac      State      Username
0               1.99  IN   aes128-cbc      hmac-sha1  Session Started  userlocal01
0               1.99  OUT  aes128-cbc      hmac-sha1  Session Started  userlocal01
*No SSHv1 server connections running.
SW-LMCentral-CORE1#
```

Figura 106

Pruebas Operativas de la Solución SSH – SW-LMCentral-CORE2

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::260:2FFF:FE12:97DC
    IPv6 Address...:
    IPv4 Address...: 172.16.64.2
    Subnet Mask...: 255.255.255.0
    Default Gateway...: 172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...:
    IPv6 Address...:
    IPv4 Address...: 0.0.0.0
    Subnet Mask...: 0.0.0.0
    Default Gateway...: 0.0.0.0

C:\>ssh -l userlocal01 172.16.14.253

Password:
SW-LMCentral-CORE2>en
Password:
SW-LMCentral-CORE2#show ssh
SW-LMCentral-CORE2#show ssh
Connection      Version Mode Encryption      Hmac      State      Username
0               1.99  IN   aes128-cbc      hmac-sha1  Session Started  userlocal01
0               1.99  OUT  aes128-cbc      hmac-sha1  Session Started  userlocal01
*No SSHv1 server connections running.
SW-LMCentral-CORE2#
```

Figura 107

Pruebas Operativas de la Solución SSH – SWLM-Access01

```

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:2FFF:FE12:97DC
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 172.16.64.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: 172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: 0.0.0.0

C:\>ssh -l svilca-ext 172.16.14.1

% Connection refused by remote host
C:\>
C:\>ssh -l svilca-ext 172.16.14.1

Password:
SW-LM-Access01>en
Password:
SW-LM-Access01#show ssh

```

Connection	Version	Mode	Encryption	Hmac	State	Username
0	1.99	IN	aes128-cbc	hmac-sha1	Session Started	svilca-ext
0	1.99	OUT	aes128-cbc	hmac-sha1	Session Started	svilca-ext

```

%No SSHv1 server connections running.
SW-LM-Access01#

```

Figura 108

Pruebas Operativas de la Solución SSH – SWLM-Access02

```

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:2FFF:FE12:97DC
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 172.16.64.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: 172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: 0.0.0.0

C:\>ssh -l svilca-ext 172.16.14.2

% Connection refused by remote host
C:\>
C:\>ssh -l svilca-ext 172.16.14.2

Password:
SW-LM-Access02>en
Password:
SW-LM-Access02#show ssh

```

Connection	Version	Mode	Encryption	Hmac	State	Username
0	1.99	IN	aes128-cbc	hmac-sha1	Session Started	svilca-ext
0	1.99	OUT	aes128-cbc	hmac-sha1	Session Started	svilca-ext

```

%No SSHv1 server connections running.
SW-LM-Access02#

```

Figura 109

Pruebas Operativas de la Solución SSH – SWLM-Access03

```

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:2FFF:FE12:97DC
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 172.16.64.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .:
                                172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:
                                0.0.0.0

C:\>ssh -l svilca-ext 172.16.14.3
! Connection refused by remote host
C:\>ssh -l svilca-ext 172.16.14.3

Password:
SW-LM-Access03>en
Password:
SW-LM-Access03#show ssh

```

Connection	Version	Mode	Encryption	Hmac	State	Username
0	1.99	IN	aes128-cbc	hmac-sha1	Session Started	svilca-ext
0	1.99	OUT	aes128-cbc	hmac-sha1	Session Started	svilca-ext

```

!No SSHd server connections running
SW-LM-Access03#

```

Figura 110

Pruebas Operativas de la Solución SSH – SWLM-Access04

```

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:2FFF:FE12:97DC
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 172.16.64.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .:
                                172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:
                                0.0.0.0

C:\>ssh -l svilca-ext 172.16.14.4

Password:
SW-LM-Access04>en
Password:
SW-LM-Access04#show ssh

```

Connection	Version	Mode	Encryption	Hmac	State	Username
0	1.99	IN	aes128-cbc	hmac-sha1	Session Started	svilca-ext
0	1.99	OUT	aes128-cbc	hmac-sha1	Session Started	svilca-ext

```

!No SSHd server connections running
SW-LM-Access04#

```

Figura 111*Pruebas Operativas de la Solución SSH – SWLM-Access05*

```

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:2FFF:FE12:97DC
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 172.16.64.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .:
    :
    :
    172.16.64.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:
    :
    :
    0.0.0.0

C:\>ssh -l svilca-ext 172.16.14.5
% Connection refused by remote host
C:\>ssh -l svilca-ext 172.16.14.5
Password:
SW-IM-Access05>en
Password:
SW-IM-Access05#show ssh

```

Connection	Version	Mode	Encryption	Hmac	State	Username
0	1.99	IN	aes128-cbc	hmac-sha1	Session Started	svilca-ext
0	1.99	OUT	aes128-cbc	hmac-sha1	Session Started	svilca-ext

```

No SSHv1 server connections running.
SW-IM-Access05#

```

Pruebas Operativas de la Solución del HSRP

Se implementó HSRP (Hot Standby Router Protocol) entre los switches CORE1 y CORE2 para garantizar alta disponibilidad en la red de la sede central. Durante las pruebas operativas, se verificó que el switch activo manejaba el tráfico principal y que, en caso de falla, el switch en espera asumía automáticamente el rol de activo, asegurando la continuidad del servicio.

A continuación, se mostrarán las pruebas realizadas de la solución HSRP, en las cuales se desconectó uno de los switches Core para comprobar la conmutación automática y el correcto funcionamiento del protocolo.

Figura 112*Pruebas Operativas de la Solución del HSRP - SW-LMCentral-CORE1*

```

C:\>ping 172.16.64.2

Pinging 172.16.64.2 with 32 bytes of data:

Reply from 172.16.64.2: bytes=32 time=85ms TTL=122
Reply from 172.16.64.2: bytes=32 time=76ms TTL=122
Reply from 172.16.64.2: bytes=32 time=15ms TTL=122
Reply from 172.16.64.2: bytes=32 time=26ms TTL=122

Ping statistics for 172.16.64.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 85ms, Average = 50ms

C:\>tracert 172.16.64.2

Tracing route to 172.16.64.2 over a maximum of 30 hops:

  1  0 ms      3 ms      0 ms      172.16.0.252
  2  0 ms      10 ms     10 ms     172.16.16.250
  3  11 ms     0 ms      10 ms     10.10.7.2
  4  58 ms     20 ms     11 ms     10.10.1.2
  5  12 ms     21 ms     13 ms     10.10.4.1
  6  267 ms    156 ms    44 ms     172.16.76.249
  7  37 ms     21 ms     41 ms     172.16.64.2

Trace complete.

```

Notas: Ping y Tracert 172.16.0.11 (Central Tower) a 172.16.64.2 (G4S)

Figura 113*Pruebas Operativas de la Solución del HSRP - SW-LMCentral-CORE2*

```

C:\>ping 172.16.64.2

Pinging 172.16.64.2 with 32 bytes of data:

Reply from 172.16.64.2: bytes=32 time=13ms TTL=122
Reply from 172.16.64.2: bytes=32 time=62ms TTL=122
Reply from 172.16.64.2: bytes=32 time=21ms TTL=122
Reply from 172.16.64.2: bytes=32 time=21ms TTL=122

Ping statistics for 172.16.64.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 62ms, Average = 29ms

C:\>tracert 172.16.64.2

Tracing route to 172.16.64.2 over a maximum of 30 hops:
  1  0 ms      0 ms      18 ms     172.16.0.253
  2  15 ms     0 ms      0 ms      172.16.16.250
  3  10 ms     12 ms     11 ms     10.10.7.2
  4  10 ms     12 ms     11 ms     10.10.1.2
  5  29 ms     18 ms     10 ms     10.10.4.1
  6  11 ms     59 ms     11 ms     172.16.76.249
  7  20 ms     10 ms     24 ms     172.16.64.2

Trace complete.

C:\>

```

Notas: Ping y Tracert 172.16.0.11 (Central Tower) a 172.16.64.2 (G4S) – Desconexión de Switch Core 1 y se Activa del Switch Core 2 que estaba en Standby.

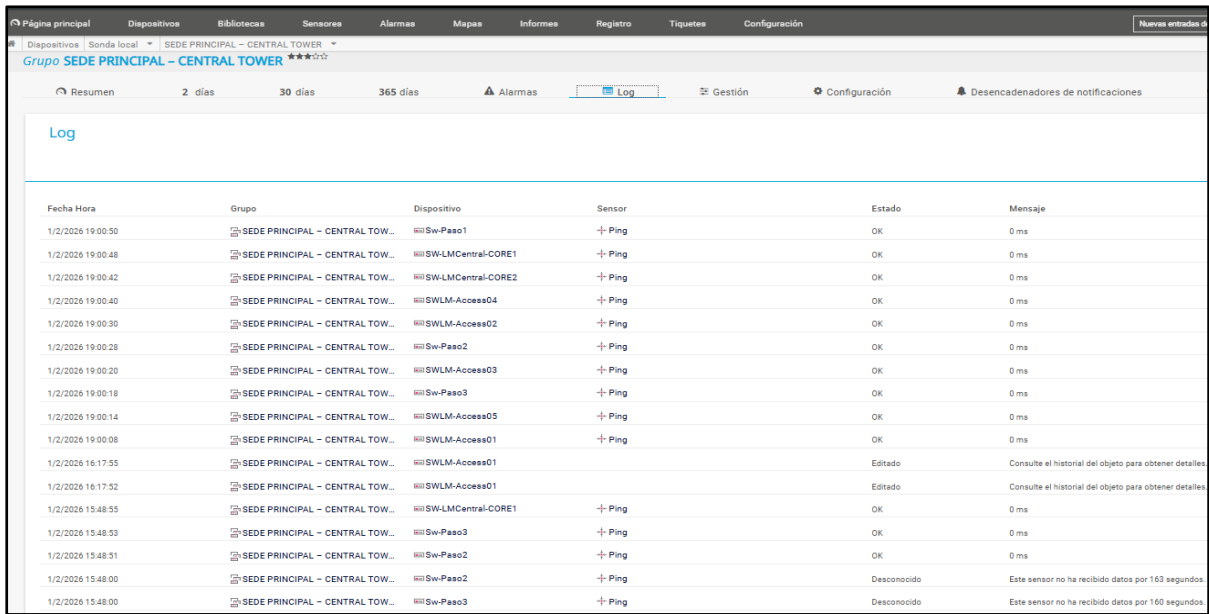
Pruebas Operativas de la Solución del Sistema de Monitoreo

El software de monitoreo PRTG nos permite supervisar el monitoreo de diversos equipos de la empresa de ventas.

A continuación, se presentará los registros Logs que se registran en el sistema de monitoreo PRTG a los equipos de la empresa de ventas. Dichas pruebas se replican en todos los equipos de la empresa de ventas.

Figura 114

Pruebas del Sistema de Monitoreo – Logs



Fecha Hora	Grupo	Dispositivo	Sensor	Estado	Mensaje
1/2/2026 19:00:30	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso1	+ Ping	OK	0 ms
1/2/2026 19:00:48	SEDE PRINCIPAL - CENTRAL TOW...	SW-LM-Central-CORE1	+ Ping	OK	0 ms
1/2/2026 19:00:42	SEDE PRINCIPAL - CENTRAL TOW...	SW-LM-Central-CORE2	+ Ping	OK	0 ms
1/2/2026 19:00:40	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso04	+ Ping	OK	0 ms
1/2/2026 19:00:30	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso02	+ Ping	OK	0 ms
1/2/2026 19:00:28	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso2	+ Ping	OK	0 ms
1/2/2026 19:00:20	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso03	+ Ping	OK	0 ms
1/2/2026 19:00:18	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso3	+ Ping	OK	0 ms
1/2/2026 19:00:14	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso05	+ Ping	OK	0 ms
1/2/2026 19:00:08	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso01	+ Ping	OK	0 ms
1/2/2026 16:17:55	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso01		Editado	Consulte el historial del objeto para obtener detalles
1/2/2026 16:17:52	SEDE PRINCIPAL - CENTRAL TOW...	SWLM-Acceso01		Editado	Consulte el historial del objeto para obtener detalles
1/2/2026 15:48:55	SEDE PRINCIPAL - CENTRAL TOW...	SW-LM-Central-CORE1	+ Ping	OK	0 ms
1/2/2026 15:48:53	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso3	+ Ping	OK	0 ms
1/2/2026 15:48:51	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso2	+ Ping	OK	0 ms
1/2/2026 15:48:00	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso2	+ Ping	Desconocido	Este sensor no ha recibido datos por 163 segundos
1/2/2026 15:48:00	SEDE PRINCIPAL - CENTRAL TOW...	Sw-Paso3	+ Ping	Desconocido	Este sensor no ha recibido datos por 160 segundos

Figura 115

Pruebas del Sistema de Monitoreo – Disponibilidad



Capítulo IV

Estudio de Costos

Costos de equipamiento

En esta sección se detallan los costos estimados del equipamiento necesario para la implementación de la infraestructura de red propuesta. Se consideran dispositivos de seguridad perimetral, switches de núcleo y de acceso, así como licencias de software y herramientas de monitoreo, los cuales son fundamentales para garantizar alta disponibilidad, seguridad, rendimiento y escalabilidad en la red diseñada.

En la tabla 20 se presenta los costos del equipamiento propuesto para la solución.

Tabla 20

Costos de Equipamiento

Ítem	Nombre del Producto	Cantidad	Precio Unitario	Precio Total
1	Firewall FortiGate 60F	1	2200,00	2200,00
2	Licencia UTM + FortiCare 5 año	2	6606,00	13212,00
3	Switch L3 Cisco C9300-48T-A	2	31000,00	62000,00
4	SmartNet 8×5×NBD - C9300-48T-A - 5 años de soporte	2	7700,00	15400,00
5	Aruba CX 6200M 24G 4SFP+ (L3)	1	6000,00	6000,00
6	HPE Aruba Networking Foundational Care 24x7 5 Year Technical Support Service	2	8011,00	16022,00
7	Switch L2 HPE Aruba CX 6000 48G PoE 4SFP	13	6072,00	78936,00
8	HPE Aruba Networking Foundational Care 8×5×NBD CX 6000 48G - 5 años	13	1113,00	14469,00
9	PRTG Network Monitor	1	0,00	0,00
			Total, en Soles (S/.)	208239,00

De acuerdo con la información detallada en la Tabla 20, el costo total del equipamiento requerido para la implementación de la infraestructura de red propuesta en el presente trabajo de aplicación profesional asciende a S/. 208239,00, monto que contempla la adquisición de dispositivos de seguridad, switches de núcleo y de acceso, así como las

Costos de contratación de Servicio de Internet

En esta sección se detallan los costos asociados a la contratación de los servicios de conectividad a Internet y de la red WAN privada, necesarios para garantizar el acceso a servicios externos y la interconexión segura entre la sede principal y las sucursales.

A continuación, se presenta el resumen de los costos correspondientes a los servicios de Internet y conectividad WAN, cuyos montos se encuentran expresados en soles (S/.), permitiendo una evaluación clara y transparente de la inversión requerida.

Tabla 22

Costos de servicio de Internet y conexión Privada

ISP	Descripción	Cantidad	Ancho de banda	Costo Mensual Unitario	Total Mensual	Total Anual
ON	Servicio de Internet dedicado – Router principal (Activo)	1 plan	500 Mb	S/ 6,500	S/ 6,500	S/ 78,000
ON	Servicio de Internet dedicado – Router Respaldo (Pasivo)					
ON	Servicio WAN Privada L2L – Router principal (Activo)	1 plan	100 Mb	S/ 1,500	S/ 1,500	S/ 18,000
ON	Servicio WAN Privada L2L – Router de respaldo (Pasivo)					
ON	Servicio WAN Privada L2L – Router L2L (sucursales)	2	50 Mb	S/ 900	S/ 1,800	S/ 10,800
ON	Servicio Sip Trunk Integración con PBX IP, SLA empresarial, IP fija (15 - 30 canales)	3		S/ 500	S/ 1,500	S/ 18,000
Total en Soles					S/ 11,300	S/ 124,800

Según se observa en la Tabla 22, el costo anual de los servicios de conectividad a Internet y de la red WAN privada proporcionados por ON Empresas asciende a S/. 124,800, monto que incluye los enlaces principales y de respaldo en la sede principal, así como la conectividad WAN L2L destinada a las sucursales.

Resumen del Costo Total de Equipamiento e Implementación

En esta sección se presentan los costos totales asociados al equipamiento y a la implementación de la infraestructura de red propuesta, con el propósito de brindar una estimación clara, precisa y transparente de la inversión requerida para la ejecución del proyecto de tesis. Este resumen consolida los costos correspondientes a la adquisición de los equipos de red, licencias de software y servicios de implementación necesarios para su correcta puesta en funcionamiento.

A continuación, se muestra el detalle consolidado de estos costos en la tabla correspondiente, cuyos montos se encuentran expresados en soles (S/.), facilitando su análisis y evaluación económica.

Tabla 23

Resumen de Costo Total de la Implementación

Ítem	Concepto	Costo (S/.)
1	Costos de Equipamiento	S/ 208,239
2	Costos de Implementación	S/ 12,190
3	Costos Anuales de Servicios de Internet y WAN	S/ 124,800
	Costo Total del Proyecto	S/ 345,229

De acuerdo con la Tabla 23, el costo total del proyecto para la implementación de la infraestructura de red propuesta asciende a S/. 345,229, monto que contempla los costos de equipamiento, los servicios de implementación y los costos anuales asociados a los servicios de conectividad a Internet y WAN privada.

Conclusiones

Conclusión 1

Se diseñó la red de datos de alta disponibilidad para la empresa de ventas permitiendo la interconexión de la sede principal con sus dos sucursales garantizando de esta manera una comunicación eficiente, segura y estable, así como la continuidad operativa y la integridad de la información entre todas las sedes.

Conclusión 2

Se analizó la situación actual de la infraestructura de red, la cual permitió identificar las deficiencias significativas como la conectividad, rendimiento, seguridad y ausencia de redundancia, lo cual justificó la necesidad de una solución integral basada en un diseño estructurado, escalable y orientado a la alta disponibilidad.

Conclusión 3

Se diseñó la topología de red propuesta, basada en un diseño de núcleo contraído, considerando los principios de segmentación, escalabilidad y redundancia. Para ello, en lo que respecta a la alta disponibilidad, se utilizaron dos switches L3 en alta disponibilidad (HA). Asimismo, se segmentó la red teniendo en cuenta su escalabilidad. Adicionalmente, se buscó una solución WAN L2L, permitiendo una administración centralizada desde la sede central, optimizando el flujo de tráfico, mejorando el rendimiento de la red y fortaleciendo los niveles de seguridad y control.

Conclusión 4

Se seleccionaron equipos de redes de los fabricantes de Cisco (Cisco Switch L3 - C9300-48T-A) y HPE (HPE Aruba CX 6000 48G PoE 4SFP / HPE Switch L3 - Aruba 2930F 48G + 4SFP(sin PoE)) así como soluciones de seguridad perimetral de Fortinet (FortiGate 60F) en alta disponibilidad, tras realizar un estudio de mercado que permitió evitar la adquisición de equipos sobrevalorados. Dado que se consideró adquirir equipos con las

mejores características técnicas, estos se adaptan a las necesidades de la empresa, logrando un alto rendimiento de la red.

Conclusión 5

Se elaboraron las configuraciones de los dispositivos que conforman la solución propuesta, las cuales incluyen direccionamiento IP estructurado, segmentación por VLAN, implementación de protocolos de redundancia como VRRP y mecanismos de seguridad perimetral, que contribuyen a mejorar significativamente la disponibilidad de los servicios y la tolerancia a fallos en la red corporativa.

Conclusión 6

Se realizaron pruebas de verificación y simulación para validar el desempeño y la funcionalidad del diseño propuesto. Los resultados en la red LAN mostraron latencias inferiores a 1 ms, sin pérdida de paquetes. Asimismo, las pruebas en la red WAN privada entre la Sucursal 1, la Sucursal 2 y la Sede Principal registraron latencias promedio entre 20 y 30 ms, con una tasa de pérdida de paquetes del 0 % y un jitter inferior a 5 ms. Adicionalmente, las pruebas realizadas con teléfonos IP Cisco conectados a switches Aruba evidenciaron un correcto funcionamiento del servicio de voz, manteniendo valores de latencia adecuados para VoIP. En conjunto, estos resultados confirman la estabilidad, confiabilidad y correcto desempeño del diseño propuesto.

Conclusión 7

Se evaluaron los costos referenciales asociados a la implementación de la red. El análisis de costos demuestra que la inversión total del proyecto, ascendente a S/ 345,229, es coherente y proporcional a los beneficios obtenidos, permitiendo implementar una infraestructura de red segura, escalable y de alta disponibilidad, alineada con las necesidades operativas y estratégicas de la empresa.

Recomendaciones

Recomendación 1

Se recomienda a la empresa implementar el diseño de red propuesto de manera progresiva, priorizando la sede principal, con el fin de asegurar una transición controlada y minimizar el impacto en las operaciones comerciales durante el proceso de despliegue.

Recomendación 2

Se recomienda supervisar y coordinar adecuadamente con el proveedor de servicios la operación de la solución de conectividad contratada, la cual incluye enlaces redundantes para la salida a Internet y la red WAN privada LAN-to-LAN, a fin de garantizar la disponibilidad y continuidad operativa de la red.

Recomendación 3

Realizar capacitaciones periódicas al personal encargado, el mantenimiento preventivo físico anualmente de los equipos de red, asimismo, el mantenimiento lógico cada 6 meses, con la finalidad de no perder el rendimiento de los equipos.

Recomendación 4

Es conveniente validar y mantener siempre el monitoreo y la gestión de la red, así como los sistemas de seguimiento de eventos y respaldo de logs, los cuales permiten detectar de manera temprana incidentes, degradaciones de rendimiento o fallas en los enlaces de comunicación.

Recomendación 5

Se sugiere evaluar, en trabajos futuros, la implementación de servicios adicionales de seguridad, tales como sistemas de detección y prevención de intrusos (IDS/IPS), segmentación avanzada mediante microsegmentación y políticas de acceso basadas en identidad.

Recomendación 6

Se recomienda considerar la inclusión de planes de contingencia y recuperación ante desastres, así como la evaluación de soluciones de respaldo energético (UPS) y alta disponibilidad a nivel de servidores, con el fin de fortalecer aún más la resiliencia de la infraestructura tecnológica.

Recomendación 7

Se recomienda documentar y mantener actualizada la arquitectura de red y las configuraciones de los dispositivos implementados, con el fin de facilitar la administración, el mantenimiento y la rápida resolución de incidencias en la infraestructura de red.

Referencia Bibliográficas

- Business Empresarial. (2022, 20 de octubre). ¿Cuánto puede perder una empresa si sufre una caída en su infraestructura digital? [Artículo web]. Business Empresarial.
<https://www.businessempresarial.com.pe/cuanto-puede-perder-una-empresa-si-sufre-una-caida-en-su-infraestructura-digital/>
- Castillo Altamirano, J. A. (2022). Diseño de una red de alta disponibilidad y redundancia con la finalidad de garantizar la conectividad de la UNMSM.
<https://cybertesis.unmsm.edu.pe/item/356b374f-f80b-4fe8-ba95-e556c6fc85d0>
- CCNA desde Cero. (s. f.). SNMP: funcionamiento y configuración [Artículo web]. CCNA desde Cero. <https://ccnadesdecero.es/snmp-funcionamiento-configuracion/>
- CCNA desde Cero. (2020). Cómo configurar OSPF [Artículo web]. CCNA desde Cero.
<https://ccnadesdecero.com/curso/como-configurar-ospf/>
- Charlene. (2022). Explicación sobre los estándares PoE y el vataje PoE.
<https://community.fs.com/es/blog/understanding-poe-standards-and-poe-wattage.html>
- Charlene. (2022). ¿Qué es un Switch PoE y cómo funciona?
<https://www.fs.com/es/blog/what-is-a-poe-switch-and-how-does-it-work-4980.html>
- Charlene. (2022). ¿Qué es un Switch PoE y cómo funciona?
<https://community.fs.com/es/blog/what-is-a-poe-switch-and-how-does-it-work.html>
- Cisco. (s. f.). Conceptos básicos de redes: fundamentos y componentes de una red empresarial [Artículo web]. Cisco Systems.
https://www.cisco.com/c/es_mx/solutions/small-business/networking/switches.html
- Cisco Systems. (2008). Cómo funcionan las redes privadas virtuales [Nota técnica]. Cisco Systems. https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html
- Cisco Systems. (2018). Configuración de la dirección IPv4 de la interfaz de VLAN en un switch a través de la CLI [Nota técnica]. Cisco Systems.
https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb5722-configure-vlan-interface-ipv4-address-on-an-sx350-or-sg350x.html
- Cisco Systems. (2020). Enfoque del ciclo de vida PPDIOO de Cisco [En línea].
<https://www.cisco.com>
- Cisco Systems. (2025, 15 de mayo). Uso de HSRP para proporcionar redundancia en una red BGP de varias conexiones [Nota técnica]. Cisco Systems.
https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/13768-hsrp-bgp.html

- Cisco Systems. (2025, 17 de octubre). Configuración de un túnel IPsec de LAN a LAN entre dos routers [Nota técnica]. Cisco Systems.
https://www.cisco.com/c/es_mx/support/docs/routers/1700-series-modular-access-routers/71462-rtr-l2l-ipsec-split.html
- Cisco Systems. (2025, 24 de noviembre). Configuración de SSH en routers y switches IOS [Nota técnica]. Cisco Systems. https://www.cisco.com/c/es_mx/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
- De Luz, S. (2025, 16 de agosto). VLANs: qué son, tipos y para qué sirven [Artículo web]. RedesZone. <https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>
- Fortinet. (s. f.). Firewall perimetral: definición y funcionamiento [Artículo web]. Fortinet. <https://www.fortinet.com/lat/resources/cyberglossary/perimeter-firewall>
- Fortinet. (s. f.). Protocolo simple de administración de red (SNMP): qué es y para qué sirve [Artículo web]. Fortinet. <https://www.fortinet.com/lat/resources/cyberglossary/simple-network-management-protocol>
- FS.com. (s. f.). Active vs. passive PoE switch: diferencias y aplicaciones [Artículo web]. FS.com. <https://www.fs.com/es/blog/active-vs-passive-poe-switch-4225.html>
- Fundación Proydesa. (2025). ¿Qué es el cableado estructurado y por qué es importante? [Artículo web]. Fundación Proydesa. <https://www.proydesa.org/portal/noticias/1898-que-es-el-cableado-estructurado-y-por-que-es-importante>
- Henderson, R. (2025, 19 de noviembre). Internet es más frágil de lo que parece: cómo un solo fallo puede tumbar servicios globales [Artículo web]. Bloomberg Línea. <https://www.bloomberglinea.com/tecnologia/internet-es-mas-fragil-de-lo-que-parece-como-un-solo-fallo-puede-tumbar-servicios-globales/>
- MercadoIT. (2017, 5 de septiembre). Las 10 empresas más potentes en redes empresariales. Recuperado de <https://mercadoit.com/blog/analisis-opinion-it/las-10-empresas-mas-potentes-en-redes-empresariales/>
- NetworkGeeks. (s. f.). 1.0 Bienvenida al curso y presentación [Curso en línea sobre fundamentos de redes, modelos de red, LAN, MAN, WAN, WLAN, topologías de red, direccionamiento IP, protocolos de comunicación y conceptos básicos de CCNA]. NetwGeeks. <https://netwgeeks.com/lessons/1-0-bienvenida-al-curso-y-presentacion/>
- Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL). (s. f.). Ficha de tarifa – SIRT. https://serviciosweb.osiptel.gob.pe/ConsultaSIRT/Buscar/FrmVerTarifa.aspx?pTarifa=161952&utm_source=chatgpt.com
- Osío, G. (2023). 5 razones por las que las empresas deben modernizar sus sistemas de redes de TI. PrensarioHub. Recuperado de <https://www.prensariohub.com/5-razones-por-las-que-las-empresas-deben-modernizar-sus-sistemas-de-redes-de-ti/>

Perú Data. (2025, 5 de mayo). Qué es un switch HPE Aruba y para qué sirve en tu empresa [Artículo web]. Perú Data Consult.

<https://www.perudataconsult.net/blogs/articulos/que-es-un-switch-hpe-aruba-y-para-que-sirve-en-tu-empresa/>

Zambrana Flores, I., & López Potoy, L. (2016). Diseño de una red LAN, para la empresa Comercial Edgar Detrinidad S.A. (CEDE TSA) en el año 2015. Otra tesis, Universidad Nacional Autónoma de Nicaragua.

<https://repositorio.unan.edu.ni/id/eprint/3173/1/1424.pdf>

Anexos

Anexo 1: Especificaciones Técnicas del Firewall Fortinet FortiGate 60F

Categoría	Especificación
Modelo	FortiGate 60F (FG-60F)
Puertos / Interfaces	10 × GE RJ45 (2 WAN, 1 DMZ, 5 LAN, 2 FortiLink) (Router-Switch.com)
USB / Consola	1 × USB, 1 × Consola RJ45 (Router-Switch.com)
Wi-Fi integrado	No (solo cableado) (Router-Switch.com)
Firewall Throughput	10 Gbps (UDP 1518/512/64) (Router-Switch.com)
Firewall Latencia	~3.3–4 μs (Router-Switch.com)
Firewall PPS (paquetes/s)	9 Mpps (Router-Switch.com)
Concurrent Sessions (TCP)	700 000 (Router-Switch.com)
Nuevas sesiones/s (TCP)	35 000 (Router-Switch.com)
Políticas de Firewall	5 000 (Router-Switch.com)
IPsec VPN Throughput	6.5 Gbps (Router-Switch.com)
Túneles IPsec (GW-to-GW / Cliente-to-GW)	200 / 500 (Router-Switch.com)
SSL-VPN Throughput	~900 Mbps (Router-Switch.com)
IPS Throughput (Enterprise)	1.4 Gbps (Router-Switch.com)
NGFW Throughput	1 Gbps (Router-Switch.com)
Threat Protection Throughput	700 Mbps (Router-Switch.com)
Application Control Throughput	~1.8 Gbps (Router-Switch.com)
Capacidad de VPN SSL concurrente	Recomendado hasta ~200 usuarios (Router-Switch.com)
Soporte VDOMs	10 (IT-Planet Onlineshop)
Soporte FortiAP	Sí (cantidad depende de FortiOS) (Accelerator)
Procesador	FortiASIC SOC4 (IT-Planet Onlineshop)
Memoria / Almacenamiento	Memoria interna / SSD depende del SKU; 60F básico suele no incluir SSD (Router-Switch.com)
Consumo de energía	~17 W promedio / ~18.5 W máximo (Manuals+)
Temperatura de operación	0 °C – 40 °C (Manuals+)
Altitud operativa	Hasta ~2250 m (Manuals+)
Certificaciones / Cumplimiento	FCC, CE, UL/cUL, CB, VCCI, etc. (Manuals+)
Factor de forma	Desktop (sin ventilador) (quanti.com.mx)
Dimensiones aprox.	~216 × 160 × 38 mm (Hardware Online)
Peso aproximado	~0.9 – 1.0 kg (Hardware Online)

Anexo 2: Especificaciones Técnicas del Switch Cisco Catalyst C9300-48T-A (L3)

Componente	Especificación
Total de puertos de cobre 10/100/1000 o Multigigabit	48
Fuente de alimentación AC predeterminada	350 W AC
Cisco StackWise-480	Sí
Cisco StackPower	Sí
Capacidad de conmutación	256 Gbps en el modelo Gigabit Ethernet de 48 puertos
Característica	Valor
Total de puertos de cobre 10/100/1000 o Multigigabit	48
Fuente de alimentación AC predeterminada	350 W AC
Cisco StackWise-480	Sí
Cisco StackPower	Sí
Capacidad de conmutación	256 Gbps en el modelo Gigabit Ethernet de 48 puertos
Ancho de banda de apilamiento (Stacking bandwidth)	480 Gbps
Número total de direcciones MAC	32,000
Número total de rutas IPv4	32,000
Entradas de enrutamiento IPv6	16,000
Escalabilidad de enrutamiento multicast	8,000
Entradas de escalabilidad QoS	5,120
Entradas de escalabilidad ACL	5,120
Buffer de paquetes por SKU	16 MB
Entradas FNF (Flexible NetFlow)	64,000 flujos
Memoria DRAM	8 GB
Memoria Flash	16 GB
IDs de VLAN	4,000
Total de interfaces virtuales conmutadas (SVI)	2,000
Soporte de Jumbo Frames	9,198 bytes
Total de puertos enrutados por stack Serie 9300	208
Ancho de banda inalámbrico por switch	Hasta 96 Gbps
Tasa de reenvío (Forwarding rate)	154.76 Mpps
Dimensiones (Alto × Ancho × Profundidad)	1.73 × 17.5 × 17.5 pulgadas
Peso	16.33 libras
Tiempo medio entre fallas (MTBF)	299,000 horas
Certificaciones de seguridad	UL 60950-1, CAN/CSA-C222.2 No. 60950-1, EN 60950-1, IEC 60950-1, AS/NZS 60950.1, IEEE 802.3
Certificaciones de emisiones electromagnéticas	47 CFR Parte 15, CISPR 22 Clase A, EN 300 386 V1.6.1, EN 55022 Clase A, EN 55032 Clase A, CISPR 32 Clase A, EN 61000-3-2, EN 61000-3-3, ICES-003 Clase A, TCVN 7189 Clase A, V-3 Clase A, CISPR 24, EN 300 386, EN 55024, TCVN 7317
Cumplimiento ambiental (RoHS)	Nivel 5

Anexo 3: Especificaciones Técnicas del Switch Aruba CX 6200M 24G 4SFP+ (L3)

Característica	Especificación
Modelo	HPE Aruba Networking CX 6200 24G 4SFP+
Product Number	R8Q67A
Diferenciador	Non-PoE
Consumo de energía	75 W a 230 VAC
Voltaje de entrada	100V–120V / 200V–240V
Puertos	24 × 10/100/1000BASE-T
	4 × 1/10G SFP+ (2 LRM, 2 LRM con MACsec 256)
	1 × puerto de consola USB-C
	1 × puerto USB Type-A (host)
	1 × puerto OOBM
	1 × puerto de consola RJ-45
Latencia	1 Gbps: 2.28 µs
	10 Gbps: 1.46 µs
Capacidad de conmutación	128 Gbps
Capacidad de stacking	Hasta 8 miembros
Rendimiento (Throughput)	Hasta 95.2 Mpps
Procesador	CPU Quad-core Arm® Cortex-A72 a 1.8 GHz
Memoria	8 GB DDR4
Almacenamiento	16 GB eMMC
Fuente de poder	2 ranuras para fuentes hot-swappable

Anexo 4: Especificaciones Técnicas del Switch HPE Aruba CX 6000 Series 48G PoE 4SFP (L2)

Característica	Especificación
Modelo / Producto	HPE Aruba Networking CX 6000 48G Class4 PoE 4SFP 370W
Número de producto	R8N85A
Tipo de PoE	Clase 4 PoE / PoE+
Consumo de energía	Máximo sin PoE: 45 W
	Máximo con PoE: 480 W
Voltaje de entrada	100–127 VAC / 200–240 VAC
Puertos	48 × puertos 10/100/1000BASE-T
	4 × puertos SFP de 1 Gb
	Soporta estándares PoE IEEE 802.3af y 802.3at
	1 × puerto de consola USB-C
	1 × puerto USB Tipo-A (host)
Latencia	1 Gbps: 1.9 µs
Capacidad de conmutación	104 Gbps
Rendimiento (Throughput)	77.3 Mpps
Procesador y memoria	CPU: Doble núcleo Arm® Cortex-A9 @ 1016 MHz
	Memoria: 4 GB DDR3
	Almacenamiento flash: 16 GB eMMC
Capacidad PoE	370 W PoE Clase 4 / PoE+

Funciones de gestión	Gestión flexible compatible con HPE Aruba Networking Central, interfaz web GUI, CLI y software HPE Aruba Networking Switch Multi-Edit
Temperatura de operación	Máximo de 0 °C a 45 °C (32 °F a 113 °F) hasta 5000 ft (1.5 km)
	Reducción de 1 °C por cada 1000 ft (305 m) desde 5000 ft hasta 10,000 ft (3.0 km)
Peso	5.0 kg
Dimensiones	4.4 × 44.2 × 30.5 cm
Garantía	Garantía limitada de por vida (según condiciones del fabricante)