Diseño de un prototipo simulado de arquitectura de red de alta disponibilidad basada en redundancia WAN y tecnologías SDN/SD-WAN para empresas de telecomunicaciones en Yopal, Casanare

Gustavo Alexander Cepeda Gutiérrez

Asesor

Ana Lucía Forero Neme

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Redes de Telecomunicaciones

2025

Dedicatoria

A Dios, por ser guía espiritual y fuente inagotable de sabiduría y fortaleza en cada etapa de este proceso. A mi esposa e hijo, por constituirse en el eje central, la motivación y el refugio que impulsó mi crecimiento profesional. A mi madre, por su apoyo incondicional y por representar la fuerza inspiradora que renovó mis energías en cada etapa del camino. A mis formadores, quienes, a través del conocimiento impartido y la exigencia académica, han moldeado con precisión, los cimientos de mi formación especializada. Y finalmente, a mi propia perseverancia y tenacidad, pilares fundamentales para alcanzar este objetivo con éxito.

Agradecimientos

A la Universidad Nacional Abierta y a Distancia (UNAD), por proveer el ecosistema tecnológico y académico necesario para el desarrollo de esta investigación.

Al Ing. Héctor Julián Parra Mogollón, director de la Especialización en Redes de Telecomunicaciones, por liderar un proceso de formación de alta calidad que ha sido la base de mi crecimiento profesional.

A la Ing. Ana Lucía Forero Neme, como directora de seguimiento del proyecto, a la Ing. Gineth Magaly Cerón Ríos, como revisora del proyecto, a ellas, pues aportando su amplio conocimiento, y orientación aportaron en el crecimiento y desarrollo del presente documento.

A la Ing. Yenny Stella Núñez Álvarez, directora de Trabajo de Grado I, y al Ing. Pierre Michael Nino, quien fue mi tutor en dicha etapa; agradezco a ambos por la orientación estratégica y el acompañamiento técnico en la estructuración de este proyecto.

Al Ing. Christian Hernán Obando Ibarra, director de Trabajo de Grado II, por su liderazgo, exigencia y guía metodológica en esta fase definitiva de culminación.

A los expertos y técnicos del sector de telecomunicaciones en Yopal, por suministrar los datos y la experiencia local que permitieron contextualizar esta propuesta en la realidad de la región.

Finalmente, agradezco a quienes colaboraron en la revisión del manuscrito y brindaron soporte técnico en las herramientas de simulación, contribuyendo de manera indirecta a la consolidación de este trabajo.

Resumen

La presente propuesta tiene como objetivo diseñar una arquitectura de red de alta disponibilidad para empresas de telecomunicaciones en Yopal, Casanare, garantizando la continuidad del servicio mediante la integración de tecnologías SDN/SD-WAN y respaldo satelital Starlink. El proyecto busca implementar un diseño técnico validado en el entorno virtualizado PNetLab, abordando problemáticas regionales como los puntos únicos de falla y la vulnerabilidad de los troncales de fibra óptica. La metodología contempla un enfoque mixto que integra el análisis de referentes normativos de la CRC con la evaluación mensual de métricas de disponibilidad (Ping, Tráfico, Uptime, Jitter y pérdida de paquetes) recolectadas mediante PRTG Network Monitor. Como resultado, se proyecta un modelo de red resiliente con una disponibilidad del 99.8%, ofreciendo un estándar superior al promedio local. Este trabajo aporta un modelo replicable y defendible que fortalece la infraestructura crítica de la región y asegura el cumplimiento de los acuerdos de nivel de servicio (SLA) en el sector corporativo.

Palabras Clave: Alta disponibilidad, Redundancia de red, PNetLab, PRTG, Resiliencia, SLA, SD-WAN, Yopal.

.

Abstract

This proposal aims to design a high-availability network architecture for telecommunications companies in Yopal, Casanare, ensuring service continuity through the integration of SDN/SD-WAN technologies and Starlink satellite backup. The project goes beyond a literature review by implementing a technical design validated in the PNetLab virtualized environment, addressing regional issues such as single points of failure and the vulnerability of fiber optic backbones. The methodology follows a mixed-method approach that integrates the analysis of CRC regulatory standards with the monthly evaluation of availability metrics (Ping, Traffic, Uptime, Jitter and Packet Loss) collected through PRTG Network Monitor. As a result, a resilient network model with a projected availability of 99.8% is expected, offering a standard superior to the local average. This work provides a replicable and defensible model that strengthens the region's critical infrastructure and ensures compliance with Service Level Agreements (SLA) in the corporate sector.

Keywords: High availability, Network redundancy, PNetLab, PRTG, Resilience, SLA, SD-WAN, Yopal.

.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Acuerdos de Nivel de Servicio (SLA)

Compromiso formal que define métricas de rendimiento y tiempos de respuesta ante fallos entre un proveedor y un cliente.

Alta Disponibilidad (HA)

Configuración de red diseñada para garantizar la continuidad del servicio mediante redundancia y mecanismos de failover.

Automatización de Red

Implementación de software y scripts para gestionar dispositivos de manera automática, integrando prácticas de SDN (Software-Defined Networking) para una gestión centralizada.

Backbone (Red Núcleo)

Infraestructura de alta capacidad que interconecta los nodos principales y transporta grandes volúmenes de tráfico.

Capa 2 y Capa 3 (Modelo OSI)

Niveles de Enlace de Datos (MAC) y Red (IP), fundamentales para el switching y routing de la infraestructura.

Cliente

Persona natural o jurídica que adquiere el servicio de telecomunicaciones mediante un contrato y es titular de los derechos del SLA.

Conectividad Inalámbrica

Transmisión de datos mediante ondas de radio o microondas para interconectar nodos sin cables físicos.

Conectividad Óptica

Transmisión de señales mediante pulsos de luz a través de fibra de vidrio, garantizando alta velocidad y nula interferencia electromagnética.

Data Center (Centro de Datos)

Instalación física que alberga sistemas informáticos, servidores y telecomunicaciones bajo condiciones de seguridad y ambiente controlado.

DMZ (Zona Desmilitarizada)

Segmento de red aislado para servicios externos que protege la infraestructura interna de posibles intrusiones.

Enrutamiento Dinámico (OSPF)

Protocolo que permite a los equipos calcular automáticamente la ruta más eficiente y adaptarse a cambios en tiempo real.

Failover (Conmutación por error)

Proceso automático de respaldo que transfiere la carga de trabajo a un sistema secundario cuando la principal falla.

Firewall (Cortafuegos)

Sistema de seguridad perimetral que filtra el tráfico para prevenir accesos no autorizados.

ITSM (Gestión de Servicios de TI)

Metodologías (como ITIL) para alinear los servicios tecnológicos con las necesidades del negocio y los clientes.

Jitter

Variación en el tiempo de llegada de los paquetes de datos, una métrica crítica para la calidad de servicios en tiempo real como voz y video.

Latencia

Tiempo exacto que tarda un paquete de datos en viajar desde el origen hasta su destino; métrica esencial para evaluar enlaces satelitales y terrestres.

Monitoreo de Red

Práctica de supervisar constantemente la salud de los componentes de red mediante protocolos como SNMP para detectar fallos o cuellos de botella.

Métricas de Rendimiento

Indicadores cuantitativos (latencia, pérdida de paquetes, ancho de banda) que permiten evaluar la eficiencia y disponibilidad de la red.

Nodo

Sitio físico o lógico donde se procesa, encamina o distribuye la información de telecomunicaciones.

OLT (Optical Line Terminal)

Equipo central en el nodo del proveedor que gestiona y distribuye la señal de fibra óptica.

ONT (Optical Network Terminal)

Dispositivo en el domicilio del usuario que convierte la señal óptica en eléctrica para el acceso a datos.

PRTG

Herramientas de software especializadas en el monitoreo de infraestructura que permiten la visualización en tiempo real de métricas y la generación de alertas.

Punto Único de Falla (SPOF)

Elemento crítico que, al no tener respaldo, detiene el servicio por completo en caso de avería.

QoS (Calidad de Servicio)

Priorización del tráfico para asegurar el rendimiento de aplicaciones críticas sobre datos menos sensibles.

Red de Acceso

Tramo final de la red que conecta la infraestructura del proveedor con el usuario final.

Red Troncal

Enlace de alta capacidad que conecta las redes de acceso con el núcleo o backbone.

Redundancia

Duplicación estratégica de rutas, equipos o enlaces para evitar que un solo fallo colapse la comunicación.

Resiliencia

Capacidad de una red para resistir incidentes, adaptarse y recuperar su operatividad óptima rápidamente.

SD-WAN

Tecnología que utiliza principios de SDN para gestionar dinámicamente varios enlaces WAN, optimizando el rendimiento.

Sistema de Respaldo Eléctrico

Equipos (UPS, bancos de baterías) que suministran energía inmediata ante fallos en el suministro comercial.

SSFV (Sistemas Solares Fotovoltaicos)

Sistemas híbridos que transforman radiación solar en electricidad para aumentar la autonomía energética de los nodos.

Topología de Red

Mapa físico y lógico que define cómo están interconectados los nodos y dispositivos de comunicación.

Usuario Final

Persona que utiliza los servicios de red para sus actividades cotidianas.

Introducción

En la era de la transformación digital, la continuidad de los servicios de conectividad se ha convertido en un pilar crítico para el desarrollo socioeconómico de las regiones. Las redes de telecomunicaciones ya no solo transportan datos, sino que soportan servicios esenciales que exigen niveles de disponibilidad superiores al 99.6%. Sin embargo, lograr este estándar representa un desafío técnico significativo, especialmente en contextos geográficos y operativos donde la infraestructura suele ser vulnerable a fallos eléctricos, cortes de fibra óptica y limitaciones en las rutas de transporte nacionales.

El departamento de Casanare, y específicamente su capital, Yopal, enfrenta retos particulares en materia de infraestructura TI. A pesar del crecimiento del sector, muchas empresas de telecomunicaciones locales operan bajo esquemas que carecen de mecanismos de redundancia automatizada y arquitecturas resilientes. Esto se traduce en interrupciones frecuentes que afectan tanto la productividad empresarial como la satisfacción del usuario final, evidenciando la necesidad de evolucionar hacia diseños de red más robustos, redundantes y auto gestionables mediante tecnologías SD-WAN.

Esta monografía propone el diseño de una arquitectura de red de alta disponibilidad orientada a optimizar la infraestructura de los ISPs en la región. La propuesta integra conceptos de Redes Definidas por Software (SDN), protocolos de enrutamiento dinámico y la implementación de una conectividad híbrida que incluye enlaces de fibra óptica y respaldo satelital de baja órbita (Starlink). Asimismo, el diseño contempla la continuidad operativa mediante sistemas de respaldo eléctrico, asegurando que los nodos críticos permanezcan activos ante contingencias energéticas.

A diferencia de un estudio meramente descriptivo, este trabajo desarrolla una propuesta técnica validada mediante la implementación y simulación en el entorno virtualizado PNetLab. A través del monitoreo con PRTG Network Monitor, se realiza una captura de datos en tiempo real para analizar el comportamiento histórico de las métricas en la red simulada, evaluando variables como latencia, Jitter, tráfico y pérdida de paquetes. Este enfoque permite proyectar una disponibilidad del 99.8% basándose en la evidencia técnica del prototipo. En las siguientes secciones se detallará el planteamiento del problema, los objetivos trazados y el diseño detallado de una solución cuyo fin último es garantizar el cumplimiento de los Acuerdos de Nivel de Servicio (SLA) exigidos por el mercado actual en Yopal.

.

Planteamiento del Problema

Descripción del Problema

En el contexto global de las telecomunicaciones, la alta disponibilidad de redes se ha convertido en un requisito esencial para garantizar la continuidad de los servicios digitales, especialmente en sectores críticos como salud, educación, banca y gobierno. La implementación de arquitecturas tolerantes a fallos, redes definidas por software (SDN) y soluciones SD-WAN ha permitido a muchas organizaciones mitigar interrupciones y mejorar la experiencia del usuario final. Sin embargo, en países como Colombia persisten desafíos estructurales que limitan la adopción de estas tecnologías, especialmente en regiones donde la conectividad depende de enlaces únicos o infraestructura altamente vulnerable. La Comisión de Regulación de Comunicaciones (CRC) ha señalado la necesidad de fortalecer la disponibilidad de redes en zonas con alta demanda, promoviendo acciones concretas por parte de los operadores para asegurar la resiliencia del servicio.

En Yopal, Casanare, la situación se torna crítica debido a la convergencia de tres factores determinantes: la dependencia de un canal físico principal (Backbone) vulnerable a cortes en la cordillera, la inestabilidad del suministro eléctrico local y las condiciones geográficas que dificultan el mantenimiento preventivo. Según datos recientes de la CRC, la brecha de infraestructura en municipios intermedios persiste, lo que en Yopal se traduce en una disponibilidad que en escenarios críticos no supera el 95%. Esta cifra es insuficiente para estándares modernos, pues genera Puntos Únicos de Falla (SPOF) y una nula tolerancia ante incidentes, impidiendo el cumplimiento de los Acuerdos de Nivel de Servicio (SLA) y afectando la competitividad regional.

El problema central radica en que la infraestructura actual de las empresas locales carece de una Arquitectura de Red Resiliente. No se trata únicamente de la falta de un segundo enlace físico, sino de la ausencia de una gestión inteligente que permita el failover automático basado en métricas de calidad. Esta vulnerabilidad se traduce en interrupciones prolongadas que no solo generan pérdidas económicas, sino que degradan la confianza del usuario final en servicios que dependen de la nube y aplicaciones en tiempo real.

La mitigación de estas fallas requiere la transición hacia una arquitectura que integre enlaces de fibra óptica con un respaldo satelital de baja órbita (Starlink), gestionados mediante SD-WAN. La viabilidad de esta propuesta se fundamenta en la capacidad de validar el comportamiento histórico de la red simulada en entornos como PNetLab, utilizando herramientas de monitoreo como PRTG Network Monitor. Esta convergencia tecnológica facilita la evolución de una red reactiva hacia una infraestructura resiliente, capaz de asegurar la continuidad operativa y el cumplimiento de los KPI técnicos frente a contingencias en la capa física.

Pregunta del Problema

¿Cómo diseñar una arquitectura de red de alta disponibilidad mediante tecnologías SDN/SD-WAN y respaldo satelital, validada a través de métricas de desempeño en un entorno virtualizado, para garantizar la continuidad del servicio y el cumplimiento de los SLA en las empresas de telecomunicaciones de Yopal, Casanare?

Justificación

En Yopal, Casanare, la dependencia de un único canal físico de transporte expone a las empresas de telecomunicaciones a una vulnerabilidad crítica ante fallas de infraestructura mayorista. Esta situación no solo compromete la continuidad del negocio, sino que genera un efecto dominó de incumplimientos contractuales y sanciones regulatorias. La CRC (2025b) ha enfatizado que el fortalecimiento de la disponibilidad en regiones intermedias es una prioridad nacional. Desde la perspectiva técnica, la adopción de arquitecturas basadas en SD-WAN y SDN no es solo una tendencia, sino una necesidad operativa para superar las limitaciones de las redes tradicionales, permitiendo una resiliencia proactiva y una gestión inteligente del tráfico.

Al integrar un canal principal de fibra óptica con un respaldo satelital de baja órbita (Starlink), se elimina el Punto Único de Falla (SPOF) físico. No obstante, la verdadera innovación radica en la capa de automatización y la validación técnica del diseño mediante simulaciones en PNetLab. Justificar esta inversión técnica permite asegurar que, ante un corte de energía o de fibra, la red realice un failover automático. La trazabilidad de este comportamiento se sustenta en el análisis de métricas históricas de la red simulada mediante PRTG, garantizando el cumplimiento de los SLA en niveles de alta disponibilidad superiores al 99.8%.

Desde el marco institucional y social, la propuesta se alinea con el ODS 9 (Industria, Innovación e Infraestructura) y el Plan TIC nacional, buscando reducir la brecha digital en Casanare. Académicamente, este trabajo llena un vacío en la literatura técnica regional al documentar una solución de ingeniería aplicada, replicable y escalable, adaptada a las condiciones climáticas y geográficas de la Orinoquía. Para la UNAD, este proyecto representa la culminación de un proceso de especialización que aplica competencias de alto nivel en diseño de redes de nueva generación.

Finalmente, como profesional del sector en la región, considero que esta solución es el puente necesario para transformar una infraestructura reactiva en una plataforma de servicios confiable. El impacto no es solo técnico; es un motor de confianza para el comercio y la educación en Yopal, permitiendo que las empresas locales compitan con estándares de calidad nacionales, fundamentados en una arquitectura técnica defendible, robusta y verificable mediante indicadores de desempeño (KPI) reales.

Objetivos

Objetivo General

Diseñar una arquitectura de red de alta disponibilidad mediante tecnologías SDN/SD-WAN y redundancia híbrida (Carrier local y satelital), para garantizar la continuidad operativa y la resiliencia de los servicios de telecomunicaciones en Yopal, Casanare, validando su desempeño mediante métricas de disponibilidad y gestión inteligente de tráfico en un entorno virtualizado.

Objetivos Específicos

Realizar un diagnóstico técnico-normativo de la infraestructura de conectividad en Yopal, mediante la correlación de los indicadores de calidad de la CRC y el análisis del comportamiento físico de los troncales de transporte, para establecer la línea base de disponibilidad y los puntos críticos de falla.

Desarrollar el diseño lógico de una arquitectura de red redundante que integre enlaces de fibra óptica y conectividad satelital de baja órbita (Starlink), aplicando políticas de tráfico SD-WAN para la gestión automatizada del failover.

Implementar un entorno de simulación que integre servicios virtualizados y una plataforma de monitoreo (PRTG), para la supervisión técnica mediante sensores de Uptime, Tráfico, Ping, Jitter y Packet Loss, garantizando la trazabilidad de los niveles de servicio.

Validar la capacidad de recuperación de la red diseñada mediante la simulación de escenarios de falla en el entorno PNetLab, contrastando los resultados obtenidos con una disponibilidad proyectada del 99.8% para sustentar la viabilidad técnica del modelo.

Marco Referencial

Antecedentes

Para la consolidación de esta propuesta, se realizó un rastreo de investigaciones previas que abordan la alta disponibilidad y la resiliencia en redes de telecomunicaciones mediante tecnologías emergentes.

Antecedentes Internacionales

A nivel global, la transición hacia redes programables es una constante. Investigaciones recientes destacan que la implementación de arquitecturas SD-WAN reduce hasta en un 40% el tiempo de inactividad en sucursales remotas al permitir el uso de enlaces híbridos (MPLS, Fibra y Satelital) con balanceo dinámico. Estudios en entornos de "Smart Cities" subrayan que la redundancia no es solo física, sino lógica, delegando al plano de control (SDN) la toma de decisiones ante la degradación de un Carrier específico.

Antecedentes Nacionales

En Colombia, los antecedentes se centran en el cumplimiento de los indicadores de calidad de la CRC. Trabajos desarrollados en universidades como la UNAD y la Distrital han explorado la mitigación de brechas digitales en zonas rurales mediante enlaces satelitales. Un referente clave es el estudio de Montoya Arango & Jiménez Ortega (2020), quienes validaron cómo SD-WAN mejora la resiliencia operativa en empresas colombianas frente a la inestabilidad de los proveedores de última milla. Asimismo, investigaciones sobre infraestructura crítica en el país resaltan la importancia de no depender de un único proveedor de transporte nacional (Backbone).

Antecedentes Locales (El Contexto de Yopal)

Aunque la literatura técnica específica para Yopal es limitada, existen reportes de diagnósticos de conectividad regional que evidencian la vulnerabilidad de la fibra óptica que atraviesa la cordillera, la cual sufre cortes frecuentes por factores climáticos o geológicos. Los antecedentes locales se basan en reportes técnicos de operadores regionales que han intentado implementar redundancia básica mediante radioenlaces, pero sin la capa de inteligencia (SDN/SD-WAN) o respaldo energético (SSFV) que propone este proyecto.

Marco Conceptual

El presente marco conceptual reúne los términos clave que apoyan el diseño técnico propuesto, enunciando definiciones, fundamentos teóricos y aplicaciones prácticas en el contexto de redes empresariales. Cada concepto ha sido seleccionado por su relevancia directa en la arquitectura planteada, y se presenta con trazabilidad documental y enfoque aplicado. Esta sección permite establecer un lenguaje común, facilitar la comprensión del diseño y respaldar las decisiones técnicas para su estructuración.

Alta Disponibilidad (HA)

Definición. Capacidad de una red o sistema para mantenerse operativo ante fallos, garantizando continuidad del servicio sin interrupciones perceptibles.

Fundamento. Se mide mediante indicadores como:

MTBF (Mean Time Between Failures). Tiempo promedio entre fallas; cuanto mayor, más confiable es el sistema.

MTTR (Mean Time To Repair). Tiempo medio de reparación; un valor bajo indica recuperación rápida.

RTO (Recovery Time Objective). Tiempo máximo aceptable para restaurar un servicio tras una interrupción.

RPO (Recovery Point Objective). cantidad máxima de datos que se pueden perder en caso de falla.

Aplicación. Enlaces redundantes (terrestre + Starlink), port-channels, virtualización de servicios críticos.

Referencia. Montoya Arango & Jiménez Ortega (2020).

Continuidad del Negocio (BCP)

Definición. Estrategia que asegura que los procesos empresariales continúen operando ante eventos adversos.

Fundamento. Incluye planes de contingencia, recuperación ante desastres y documentación técnica.

Aplicación. Failover automático, monitoreo distribuido, recuperación virtualizada.

Referencia. Ministerio TIC (2024).

Redundancia de Enlaces

Definición. Implementación de múltiples caminos físicos o lógicos para garantizar conectividad continua.

Fundamento. Protocolos como VRRP, HSRP y GLBP permiten conmutación automática.

VRRP. Varios routers comparten una IP virtual; si la principal falla, otro asume el rol.

HSRP. desarrollado por Cisco, crea un grupo de routers con IP virtual; el de respaldo toma el control si falla el activo.

GLBP. Balancea carga entre varios routers, manteniendo redundancia.

Aplicación. Enlaces terrestres y satelitales, balanceo de carga, port-channels.

Referencia. Montes Castañeda & Solano (2021).

SDN (Software Defined Networking)

Definición. Arquitectura que separa el plano de control del plano de datos, permitiendo gestión centralizada.

Fundamento. Facilita programación dinámica, segmentación y respuesta rápida ante fallos.

Aplicación. Controlador SDN define rutas, gestiona tráfico y aplica políticas.

Referencia. Olaya Toledo (2023).

SD-WAN

Definición. Tecnología que optimiza el uso de múltiples enlaces WAN mediante políticas inteligentes.

Fundamento. Prioriza aplicaciones críticas, mejora rendimiento, permite failover automático.

Aplicación. Gestión de canal principal y canal satelital, conmutación según rendimiento.

Referencia. López Arévalo (2020).

Port-Channel (EtherChannel)

Definición. Agrupación de interfaces físicas en una lógica para aumentar disponibilidad y ancho de banda.

Fundamento. Utilizado en switches capa 2/3 para enlaces troncales redundantes.

Aplicación. Backbone entre nodos de distribución y nodo central.

Referencia. Cisco Systems (2023).

OSPF (Open Shortest Path First)

Definición. Protocolo de enrutamiento dinámico que calcula rutas óptimas en redes IP.

Fundamento. Opera en capa 3, permite segmentación y redundancia.

Aplicación. Comunicación entre nodos de distribución y nodo central.

Referencia. Cisco Networking Academy (2024).

PRTG Network Monitor

Definición. Herramienta de monitoreo que supervisa disponibilidad, tráfico y rendimiento de red.

Fundamento. Usa sondas remotas, SNMP, NetFlow y alertas automatizadas.

Aplicación. Monitoreo de nodos y enlaces desde centro virtualizado.

Referencia. Paessler AG (2023).

Starlink

Definición. Servicio de internet satelital de alta velocidad y baja latencia.

Fundamento. Ideal como canal secundario en zonas rurales o vulnerables.

Aplicación. Enlace de respaldo ante falla del canal terrestre.

Referencia. SpaceX (2023).

Marco Teórico

La alta disponibilidad y la continuidad del servicio en redes empresariales modernas requieren arquitecturas resilientes, capaces de soportar fallos sin comprometer la operación. Para lograrlo, se integran tecnologías como SDN y SD-WAN, que permiten gestionar múltiples enlaces mediante políticas inteligentes y separación del plano de control y de datos (Aryaka, 2024; TICNUS, 2024).

En paralelo, protocolos de redundancia como VRRP, HSRP y GLBP, junto con mecanismos de enrutamiento dinámico como OSPF y técnicas de agregación de enlaces como port-channel, fortalecen la resiliencia de la infraestructura. Para evitar bucles en redes con múltiples rutas, se emplea STP, que selecciona rutas activas y mantiene otras en espera,

activándolas solo ante fallos (Cisco Systems, 2023).

La implementación de port-channels permite agrupar interfaces físicas en una lógica, aumentando el ancho de banda y reduciendo puntos únicos de falla. OSPF, por su parte, calcula rutas óptimas en redes IP y se adapta dinámicamente a cambios en la topología, garantizando continuidad incluso ante fallas parciales (Cisco Networking Academy, 2024).

Finalmente, el uso de protocolos de redundancia como VRRP, HSRP y GLBP permite que múltiples routers compartan una IP virtual y se turnen el rol de puerta de enlace predeterminada, garantizando continuidad sin intervención manual.

Aplicación en el Diseño Propuesto

El análisis de la disponibilidad actual en Yopal evidenció la dependencia de un único canal físico y la baja tolerancia a fallos en la infraestructura existente. Estos hallazgos fundamentan la necesidad de aplicar los siguientes elementos en el diseño propuesto, orientados a garantizar continuidad operativa y resiliencia en las empresas de telecomunicaciones

Nodo Central (Alta Redundancia).

Redundancia Física y Lógica. Enlaces troncales múltiples hacia los nodos de distribución, con port-channels configurados para agregación de enlaces (Cisco Systems, 2023).

Balanceo de Carga. Distribución del tráfico entrante y saliente entre enlaces disponibles, optimizando el uso de recursos (Aryaka, 2024).

Failover Automático. Conmutación entre enlaces ante fallos, gestionada por SD-WAN y protocolos de redundancia (Citrix, 2021).

Virtualización de Servicios Críticos. Servidores Syslog, RADIUS, PRTG alojados en un sistema de virtualización a través de VMware 15, con respaldo y monitoreo continuo.

Backbone y Nodos de Distribución.

Port-Channels. Enlaces troncales entre switches de distribución y el nodo central, agrupando interfaces físicas para mayor disponibilidad (Cisco Systems, 2023).

Spanning Tree Protocol (STP). Evita bucles en topologías redundantes, activando rutas de respaldo solo cuando las principales fallan (Cisco Systems, 2023).

SDN. Controlador centralizado define rutas, aplica políticas de seguridad y gestiona el tráfico entre nodos (Aryaka, 2024).

SD-WAN. Gestiona enlaces WAN (terrestre y Starlink), aplicando políticas de conmutación y priorización de tráfico (TICNUS, 2024).

Failover. Activación automática del canal satelital ante pérdida del canal terrestre (Citrix, 2021).

OSPF. Implementado en los routers de cada nodo de distribución, permite enrutamiento dinámico hacia el nodo central o hacia otros nodos, garantizando continuidad incluso ante fallos parciales (Cisco Networking Academy, 2024).

Segmentación y Monitoreo.

Segmentación de Tráfico. Voz, datos, telemetrías (control), CCTV, gestión y monitoreo se separan mediante VLANs y políticas SDN.

Monitoreo Distribuido. Sondas remotas con PRTG supervisan el estado de cada enlace, nodo y servicio, generando alertas ante eventos críticos.

Marco Legal

La implementación de redes empresariales modernas en Colombia, con enfoque en alta disponibilidad, virtualización y gestión inteligente, se encuentra respaldada por los siguientes marcos normativos:

Normativa Nacional

Ley 1341 de 2009 (Modificada por la Ley 1978 de 2019). Establece el marco general para el desarrollo de las TIC en Colombia. Promueve la modernización de redes, la eficiencia operativa y la adopción de tecnologías emergentes como SDN y virtualización.(Ley 1341 de 2009 (Modificada Por Ley 1978 de 2019), 2019)

Resolución CRC 5405 de 2018 y Resolución CRC 5993 de 2020 – RITEL. Define los requisitos técnicos para redes internas de telecomunicaciones. Aunque orientado a edificaciones, sus principios de canalización, puntos de acceso, soporte físico y estándares de conectividad son aplicables como base estructural en diseños empresariales.(Resolución CRC 5405 de 2018 y 5993 de 2020 – RITEL, 2020)

Plan Estratégico de Tecnologías de Información (PETI) 2023–2026 – MinTIC. Promueve la adopción de redes definidas por software, virtualización de servicios, monitoreo distribuido y esquemas de alta disponibilidad como parte de la transformación digital del país.

Guía de Seguridad de la Información – MinTIC (2023). (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]], 2024)
Recomienda la implementación de autenticación centralizada (RADIUS), trazabilidad (Syslog), segmentación de tráfico y monitoreo continuo como prácticas obligatorias en redes públicas y privadas.(Guía de Seguridad de La Información, 2023)

Normativa Internacional

ISO/IEC 27001:2022 – Seguridad de la Información. Norma internacional que exige trazabilidad, disponibilidad y continuidad operativa en infraestructuras TIC. Respaldan el uso de Syslog, RADIUS, monitoreo distribuido y virtualización.(ISO/IEC 27001:2022 – Information Security Management, 2022)

IEEE 802.1AX – Link Aggregation. Norma que regula el uso de port-channels

(EtherChannel) para agregación de enlaces, aumentando disponibilidad y ancho de banda.(IEEE 802.1AX – Link Aggregation, 2014)

RFC 2328 – OSPF Versión 2 (IETF). Documento técnico que define el protocolo OSPF para enrutamiento dinámico en redes IP, aplicable en capa 3 para nodos de distribución.(RFC 2328 – OSPF Version 2, 1998)

ITU-T Y.3300 – Framework of Software-Defined Networking. Establece los principios de arquitectura SDN, incluyendo separación de planos, control centralizado, segmentación y respuesta dinámica ante fallos.(ITU-T Y.3300 – Framework of Software-Defined Networking, 2014)

MEF 70 – SD-WAN Service Atributos. (MEF 70, 2024) **and Service Framework**

Define los atributos técnicos y operativos de servicios SD-WAN, incluyendo conmutación automática, priorización de tráfico y gestión de múltiples enlaces.(MEF 70 – SD-WAN Service Attributes and Service Framework, 2020)

Aplicación Normativa en el Diseño Propuesto

Alta Disponibilidad en el Nodo Central. Respaldada por ISO/IEC 27001, IEEE 802.1AX y Ley 1341, con enlaces redundantes, port-channels, balanceo de carga y virtualización de servicios críticos.

Backbone y Nodos de Distribución. Aplicación de OSPF (RFC 2328), STP (IEEE 802.1D), y SDN (ITU-T Y.3300) para segmentación, enrutamiento dinámico y gestión centralizada.

Gestión WAN Inteligente. Uso de SD-WAN conforme a MEF 70, con conmutación automática entre enlaces terrestres y satelitales, priorización de tráfico y continuidad operativa.

Seguridad y Trazabilidad. Implementación de RADIUS y Syslog conforme a Guía

MinTIC 2023 e ISO/IEC 27001, garantizando autenticación, auditoría y monitoreo distribuido.

Cumplimiento Físico y Estructural. Diseño alineado con RITEL para canalización, puntos de acceso, soporte técnico y estándares de conectividad.

Marco Contextual

El presente proyecto se desarrolla en el municipio de Yopal, capital del departamento de Casanare, Colombia. Su ubicación estratégica en el piedemonte llanero lo convierte en un centro de servicios para la industria petrolera, agropecuaria y gubernamental, sectores que demandan una conectividad de alta confiabilidad.

Contexto Geográfico y Operativo

Yopal presenta condiciones climáticas propias del trópico, con una fuerte temporada de lluvias que impacta directamente en la estabilidad de las redes de transporte terrestre (fibra óptica) y en la propagación de señales de radioenlaces debido al fenómeno de atenuación por lluvia (*rain fade*). La infraestructura troncal que conecta a la ciudad con el interior del país atraviesa zonas de geografía inestable, lo que deriva en cortes recurrentes de los canales principales de fibra óptica.

Contexto de Infraestructura TIC Local

En la actualidad, las empresas prestadoras de servicios de internet (ISP) en la región dependen mayoritariamente de un único Carrier para su salida internacional. Según datos de la CRC (2025b), la disponibilidad de los servicios en municipios intermedios como Yopal se ve mermada por la falta de rutas de respaldo automatizadas. Los nodos de red locales suelen presentar las siguientes vulnerabilidades:

Puntos Únicos de Falla. Ausencia de enlaces redundantes que entren por rutas geográficas distintas.

Vulnerabilidad Energética. Cortes frecuentes en el suministro eléctrico comercial que superan la autonomía de los bancos de baterías tradicionales de las UPS.

Gestión Reactiva. Falta de herramientas de monitoreo avanzado que permitan la conmutación automática (*failover*) antes de la degradación total del servicio.

Entorno de Aplicación

El diseño se proyecta para ser implementado en nodos estratégicos de distribución, donde se integrará un Data Center local con conectividad híbrida. Se toma como referencia la zona urbana de Yopal, donde la densidad de Usuarios Finales y la demanda de servicios en la nube exigen una transición de arquitecturas tradicionales hacia redes resilientes basadas en SD-WAN y energía renovable (SSFV).

Diseño Metodológico

La presente propuesta se desarrollará bajo un enfoque de ingeniería aplicada y experimental, orientado al diseño de una arquitectura de red empresarial de alta disponibilidad para el contexto de Yopal, Casanare. La metodología se estructura en cuatro fases secuenciales que integran el diagnóstico, el diseño lógico, la implementación virtualizada y la validación técnica.

Fases Metodológicas del Diseño Técnico

Fase 1 – Diagnóstico Técnico-Normativo y Análisis de Requerimientos (Objetivo 1)

En esta etapa se realiza un análisis del sector basado en el comportamiento histórico de la infraestructura en Yopal y los lineamientos de la CRC. El diagnóstico se fundamenta en la identificación de Puntos Únicos de Falla (SPOF) y en la correlación de datos técnicos existentes, estableciendo los criterios de resiliencia necesarios sin recurrir a recolección de datos primarios subjetivos.

Fase 2 – Diseño de la Arquitectura de Red Redundante (Objetivo 2)

Con base en el diagnóstico, se diseña una topología jerárquica modular. Se integran enlaces redundantes mediante agregación de puertos (LACP), segmentación por VLAN y enrutamiento dinámico OSPF. La innovación radica en la incorporación de un plano de control mediante SDN y una arquitectura SD-WAN para la gestión inteligente de enlaces (Fibra y Starlink) con conmutación automática.

Fase 3 – Virtualización de Servicios y Monitoreo Distribuido (Objetivo 3)

Se desarrolla el entorno de infraestructura y servicios críticos (Autenticación, Resolución de Nombres DNS y Enlaces de Internet) en alta disponibilidad. Para asegurar la visibilidad total, se integra la plataforma PRTG Network Monitor, implementando sensores específicos de Uptime, Latencia, Jitter y Pérdida de Paquetes, permitiendo la trazabilidad técnica de los SLA.

Asimismo, se incorporan las capas de seguridad perimetral mediante autenticación AAA, auditoría centralizada de eventos y el diseño de respaldo energético para garantizar la continuidad absoluta del negocio.

Fase 4 – Validación Técnica y Simulación de Escenarios (Objetivo 4)

El diseño se valida en el entorno PNetLab mediante pruebas de estrés y simulación de fallos críticos en los troncales. Los resultados permiten ajustar los parámetros de conmutación para garantizar que la disponibilidad final de la infraestructura proyecte un 99.8%, alineándose con los estándares de calidad vigentes.

Herramientas y Tecnologías Previstas

Para la ejecución técnica, se han seleccionado herramientas que garantizan un entorno de emulación profesional:

Simulación y Emulación

La plataforma principal será PNetLab, la cual permite la integración de imágenes reales (IOS, RouterOS, FortiOS) para validar la interoperabilidad multi-vendor. Se utilizará Drawio para el mapeo dinámico y la visualización jerárquica de la topología.

Monitoreo

La pieza central es PRTG Network Monitor, configurado para la supervisión de infraestructura mediante sensores de rendimiento históricos y en tiempo real.

Protocolos de Red

Se implementará OSPF para el enrutamiento y protocolos de redundancia de puerta de enlace como VRRP/HSRP. La gestión, administración y acceso se basará en la supervisión de dispositivos en SNMP.

Tecnologías Core

El diseño se fundamenta en SDN y arquitecturas SD-WAN para la gestión de enlaces híbridos. Se aplicará segmentación IEEE 802.1Q y agregación de enlaces físicos para maximizar la tolerancia a fallos.

Equipos de Referencia

El modelo incluye routers MikroTik (hAP-RB931), switches Cisco Catalyst, seguridad perimetral con Cisco (Cisco IOL-ASA) y respaldo satelital Starlink como ruta de salida de alta disponibilidad.

.

Capítulo 1. Diagnóstico y Requerimientos

En esta etapa se realiza un análisis del sector basado en el comportamiento histórico de la infraestructura en Yopal y los lineamientos de la CRC. El diagnóstico se fundamenta en la identificación de Puntos Únicos de Falla (SPOF) y en la correlación de datos técnicos existentes, estableciendo los criterios de resiliencia necesarios sin recurrir a recolección de datos primarios subjetivos.

Diagnóstico del Sector de Telecomunicaciones en Yopal

La ciudad de Yopal, Casanare, presenta un escenario de conectividad caracterizado por una brecha de infraestructura *Carrier-class*. A diferencia de las metrópolis centrales, la oferta de Proveedores de Servicios de Internet (ISP) en la región está limitada por una baja densidad de redes troncales (Backbone) diversificadas. Como señalan Díaz Olariaga y Alonso Malaver (2022), la centralización de políticas aeroportuarias y de transporte en Colombia ha generado un desarrollo asimétrico en la infraestructura de las regiones periféricas, lo cual se traduce en una falta de redundancia en las rutas de fibra óptica que llegan al departamento.

Complementando lo anterior, el reporte Data Flash 2025-009 de la Comisión de Regulación de Comunicaciones (CRC, 2025) confirma que la estabilidad de los servicios en municipios intermedios sigue siendo un reto normativo. Desde una perspectiva de ingeniería de campo y observación técnica directa en el sector local, el diagnóstico identifica los siguientes puntos críticos:

Escasez de Carriers de Última Milla

La mayoría de las empresas locales dependen de un número reducido de proveedores mayoristas, lo que genera un punto único de falla (SPOF) a nivel de transporte regional. La

experiencia técnica en la zona demuestra que los cortes en la cordillera oriental son la causa principal de indisponibilidad prolongada.

Desafíos Eléctricos y de Planta Exterior

La infraestructura aérea es vulnerable a las condiciones climáticas de la Orinoquía, y la inestabilidad eléctrica local degrada la vida útil de los equipos de red activos.

Inversión Tecnológica Retardada

Existe una transición lenta hacia tecnologías de red definidas por software (SDN), lo que limita la capacidad de respuesta ante fallos de enlace automáticos. De acuerdo con Camargo y Espitia (2016), el despliegue de tecnologías en comunidades rurales y ciudades en desarrollo en Colombia requiere soluciones adaptadas a la topografía y a las limitaciones operativas específicas de la zona.

Requerimientos Técnicos y Metodología en PNETLab

Para resolver las deficiencias identificadas, el proyecto propone un prototipo virtualizado en PNETLab bajo los siguientes criterios técnicos, fundamentados en la medición de KPIs reales:

Redundancia de Borde (Multi-WAN). Se implementarán dos enlaces independientes (ISP terrestre y Starlink). Esta configuración es validada por Giyana et al. (2023), quienes demuestran que el uso de protocolos de redundancia en la puerta de enlace es la base para mantener la continuidad del servicio en infraestructuras que requieren alta disponibilidad.

Segmentación Jerárquica. El tráfico será organizado mediante un Firewall y un Router Core, segmentando la red en zonas (LAN, DMZ y Gestión). Según Kiran et al. (2025), esta arquitectura de red jerárquica basada en VLANs es esencial para el control y la escalabilidad en entornos empresariales.

Automatización y Recuperación. El diseño busca minimizar el tiempo de caída mediante políticas SD-WAN. Bourne et al. (2020) resaltan la importancia de medir los tiempos de *failover* para asegurar que la redundancia sea efectiva, mientras que Hu y Chen (2022) subrayan que la automatización en la configuración de equipos SDN reduce errores críticos de seguridad.

Metodología de Desarrollo: Prototipado en PNETLab

Para solventar las deficiencias del diagnóstico, el proyecto se desarrollará bajo un entorno de virtualización avanzada utilizando PNETLab. Esta plataforma permite simular un escenario de alta fidelidad técnica donde se validará la resiliencia de la arquitectura propuesta mediante el uso de PRTG Network Monitor para el análisis de Uptime, Jitter y latencia.

El prototipo se estructurará de la siguiente manera:

Ingreso de Red (Edge). Se simularán dos entradas de internet independientes mediante direccionamiento IP Público:

ISP Convencional. Representando la conexión terrestre cableada.

Starlink (LEO). Utilizando las capacidades de satélites de baja órbita para garantizar la salida de datos ante cortes físicos en la fibra óptica terrestre, integrando conceptos de redes híbridas (Bourne et al., 2020).

Seguridad y Control. Un Firewall perimetral recibirá ambos enlaces, gestionando el balanceo de carga y las reglas de seguridad automatizadas, basándose en el diseño de configuraciones seguras para equipos de enrutamiento (Hu & Chen, 2022).

Core y Backbone. Un enrutador de núcleo (Core) distribuirá el tráfico hacia switches de borde, los cuales estarán conectados al Backbone de la red simulada.

Segmentación de Servicios

LAN de Gestión. Segmento dedicado al monitoreo (PRTG) y servicios internos.

DMZ (Zona Desmilitarizada). Segmento aislado para servicios propios.

VLANs Jerárquicas. Implementación de segmentación lógica para optimizar el tráfico y la seguridad interna (Kiran et al., 2025).

Capítulo 2. Diseño de la Arquitectura de Red Redundante

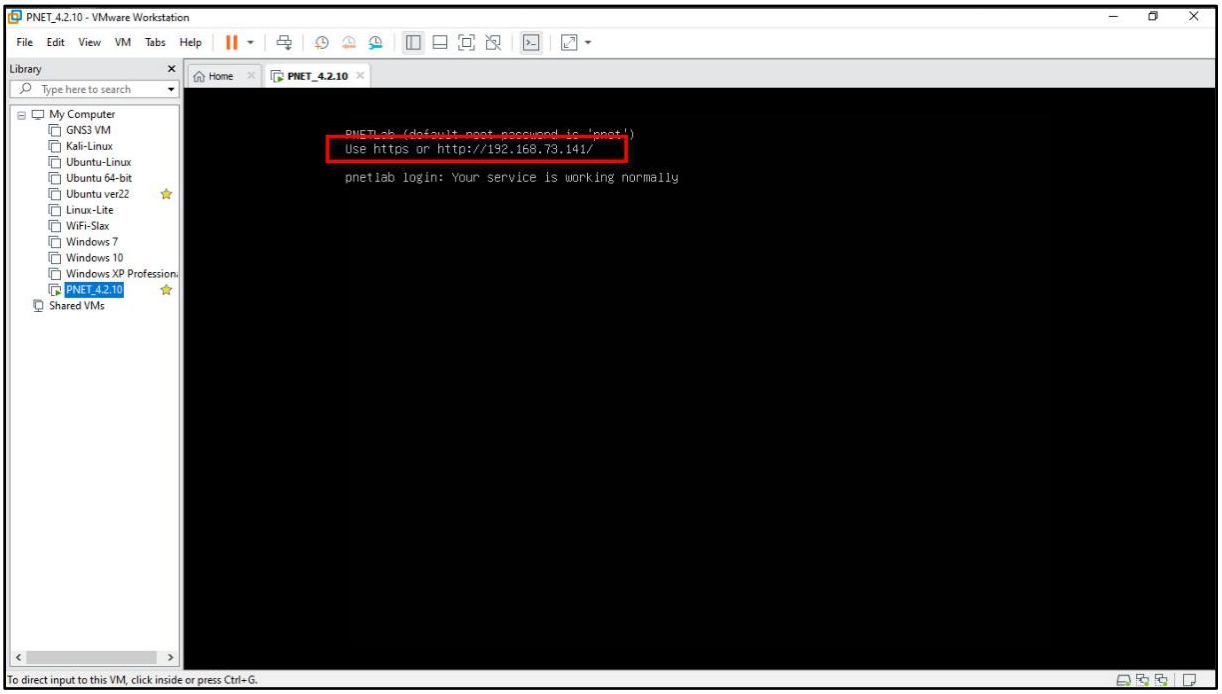
Con base en el diagnóstico, se diseña una topología jerárquica modular. Se integran enlaces redundantes mediante agregación de puertos (LACP), segmentación por VLAN y enrutamiento dinámico OSPF. La innovación radica en la incorporación de un plano de control mediante SDN y una arquitectura SD-WAN para la gestión inteligente de enlaces (Fibra y Starlink) con conmutación automática.

Entorno de Virtualización y Plataforma de Simulación

El despliegue del prototipo se realizó mediante técnicas de virtualización de red para garantizar un entorno controlado y escalable. Como base tecnológica, se utilizó el hipervisor VMware Workstation Pro, sobre el cual se ejecutó una instancia de PNetLab (Packet Network Lab). Esta plataforma permite la emulación de sistemas operativos de red reales (IOL y QEMU) con una alta fidelidad respecto al hardware físico.

Figura 1.

Instancia de Virtualización del Laboratorio en VMware Workstation.



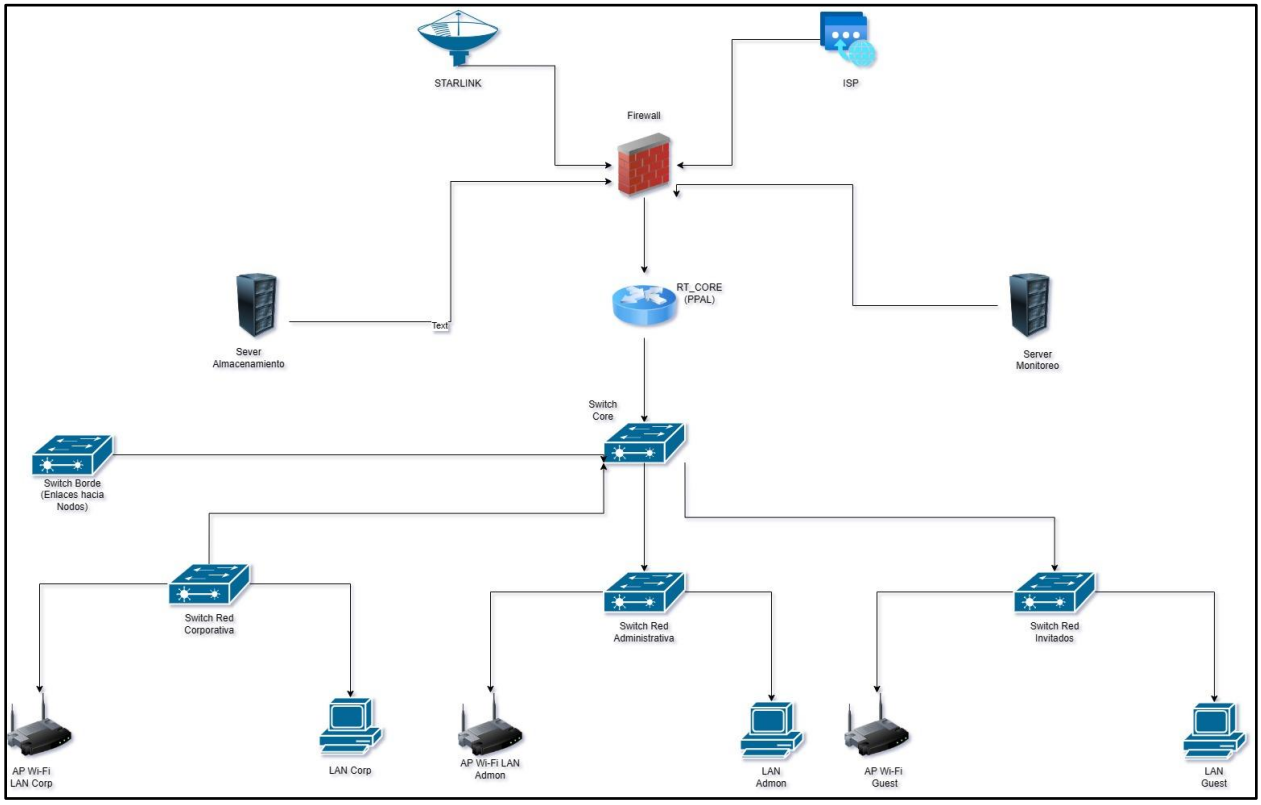
Nota. La imagen muestra la asignación de recursos y la IP de gestión 192.168.73.141 para el acceso vía web desde el montaje virtualizado de VMware y su VM PNETLab. Tomado de: *Elaboración propia.*

Diseño de la Topología Lógica (Arquitectura Propuesta)

Previo al montaje técnico, se definió la arquitectura de red mediante la herramienta Draw.io, estableciendo la jerarquía de los dispositivos y los flujos de tráfico esperados para la sede de Yopal.

Figura 2.

Esquema Lógico de la Red Redundante para la Sede Yopal.



Nota. El diseño muestra la separación clara entre el borde (WAN), el núcleo (Core) y los segmentos de red interna y en general la arquitectura completa de la topología para el prototipo. Tomado de: *Elaboración propia.*

Arquitectura de Borde y Redundancia Híbrida

El diseño propuesto se fundamenta en una topología de Multi-Homing, diseñada para mitigar la vulnerabilidad de transporte identificada en el diagnóstico. La arquitectura integra dos vectores de conectividad con naturalezas físicas distintas:

Enlace Primario (Terrestre)

Conectividad vía Fibra Óptica provista por un Carrier local, que ofrece baja latencia y simetría para el tráfico convencional.

Enlace de Respaldo (Satelital LEO)

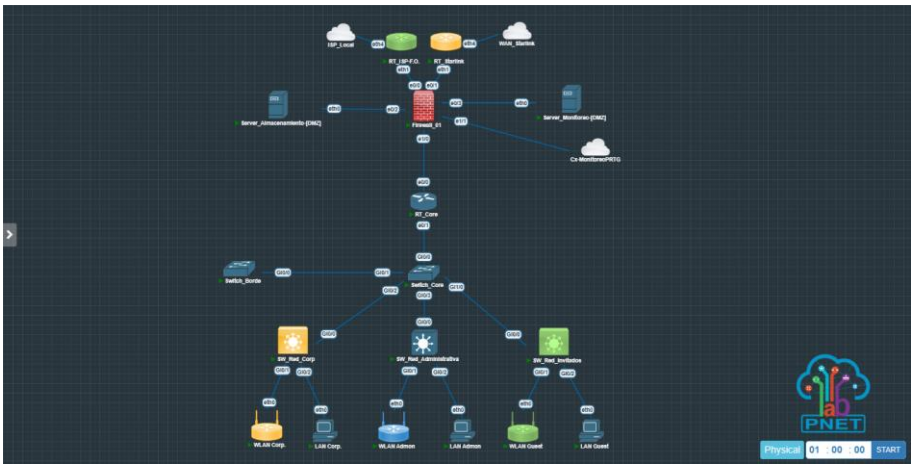
Conexión a través de la constelación Starlink. Al ser una red de órbita baja, permite mantener una latencia operativa (inferior a 50ms) apta para servicios críticos, funcionando como una ruta de salida independiente de la infraestructura de fibra terrestre nacional.

Implementación en el Laboratorio (PNetLab)

Una vez validado el diseño, se procedió al montaje en el lienzo de PNetLab, interconectando nodos Cisco IOSv para el Firewall y Core, y nodos MikroTik (RouterOS) para la simulación de los proveedores de servicios (ISP).

Figura 3.

Montaje Operativo de los Nodos en el Entorno de Simulación



Nota. La figura muestra el montaje del prototipo en el entorno simulado de PNETLab, los nodos en color azul indican un estado de ejecución activo y estable del montaje en PNETLab gestionado desde navegador bajo el lanzador virtualizado en VMware. Tomado de: *Elaboración propia.*

Matriz de Direccionamiento IP e Interfaces

A continuación, se detalla la asignación de direccionamiento IP para cada segmento de la red, asegurando el cumplimiento de las máscaras de subred definidas para optimizar el espacio de direcciones.

Tabla 1.

Matriz de Direccionamiento Lógico del Prototipo.

Dispositivo	Interfaz	Dirección IP	Máscara	Descripción
RT-L3-Testing (hAP)	Bridge-LAB	192.168.73.1	255.255.255.0	Gateway Principal Laboratorio / Router L3
RT-L3-Testing (hAP)	Bridge-LAB	192.168.73.5	255.255.255.0	IP de Origen RADIUS / Gestión MikroTik
Servidor PNETLab	vNIC / eth0	192.168.73.10	255.255.255.0	Host de Virtualización (Nodos de Red)
Virtualizado PNETLab	vNIC / NAT	192.168.73.141	255.255.255.0	Direccionamiento IP del entorno virtualizado
Work Station (WS)	NIC	192.168.73.20	255.255.255.0	Consola de Gestión (PRTG / TekRADIUS / Syslog)
ISP_FIBRA	ether1	200.10.10.1	255.255.255.252	Gateway Proveedor Fibra
ISP_STARLINK	ether1	190.20.20.1	255.255.255.252	Gateway Proveedor Starlink
Firewall_01	Et0/0	200.10.10.2	255.255.255.252	Enlace WAN Fibra Óptica (Principal)
Firewall_01	Et0/1	190.20.20.2	255.255.255.252	Enlace WAN Starlink (Respaldo)
Firewall_01	Et0/2	172.16.50.1	255.255.255.248	Gateway DMZ Almacenamiento
Firewall_01	Et0/3	172.16.60.1	255.255.255.248	Gateway DMZ Monitoreo
Firewall_01	Et1/0	10.0.0.1	255.255.255.252	Uplink hacia RT_Core
Servidor Monitoreo (NAS)	vNIC	172.16.60.2	255.255.255.248	Nodo de Monitoreo (Agente prototipado para PRTG)

Servidor Almacenamiento	vNIC	172.16.50.2	255.255.255.248	Servidor de almacenamiento (Seguridad de Información)
RT_Core	Et0/0	10.0.0.2	255.255.255.252	Uplink hacia Firewall_01
RT_Core	Ethernet0/1.10	192.168.10.1	255.255.255.0	Gateway Red Corporativa
RT_Core	Ethernet0/1.20	192.168.20.1	255.255.255.0	Gateway Red Administrativa (Gestión)
RT_Core	Ethernet0/1.30	192.168.30.1	255.255.255.0	Gateway Red Invitados
RT_Core	Ethernet0/1.40	172.16.100.1	255.255.255.252	Enlace hacia Switch de Borde
SW_Core	Vlan 10 (Corp)	192.168.10.0	255.255.255.0	Red Corporativa
SW_Core	Vlan 20 (Adm)	192.168.20.0	255.255.255.0	Red Administrativa (Gestión)
SW_Core	Vlan 30 (Invit)	192.168.30.0	255.255.255.0	Red Invitados
SW_Core	Vlan 40 (Borde)	172.16.100.0	255.255.255.252	Enlace hacia Switch de Borde
SW_Acceso_1	Vlan 10	192.168.10.2	255.255.255.0	Switch Acceso Red Corporativa
SW_Acceso_2	Vlan 20	192.168.20.3	255.255.255.0	Switch Acceso Red Administrativa
SW_Acceso_3	Vlan 30	192.168.30.2	255.255.255.0	Switch Acceso Red Invitados
SW_Borde	Vlan 40	172.16.100.2	255.255.255.252	Switch Gestión de Radioenlaces
Pool LAN/WLAN 10	Hosts Corp	192.168.10.10 - .254	255.255.255.0	Usuarios Corporativos (Cableado/WiFi)
Pool LAN/WLAN 20	Hosts Admin	192.168.20.10 - .254	255.255.255.0	Personal Administrativo (Cableado/WiFi)
Pool LAN/WLAN 30	Hosts Invit	192.168.30.10 - .254	255.255.255.0	Acceso Invitados (Portal Cautivo)

Nota. La Tabla 1, muestra el detalle de los segmentos de red empleados para la implementación del Failover en el prototipo de PNETLab. Tomado de: *Elaboración propia.*

Validación Funcional de la Alta Disponibilidad (Prueba de Failover)

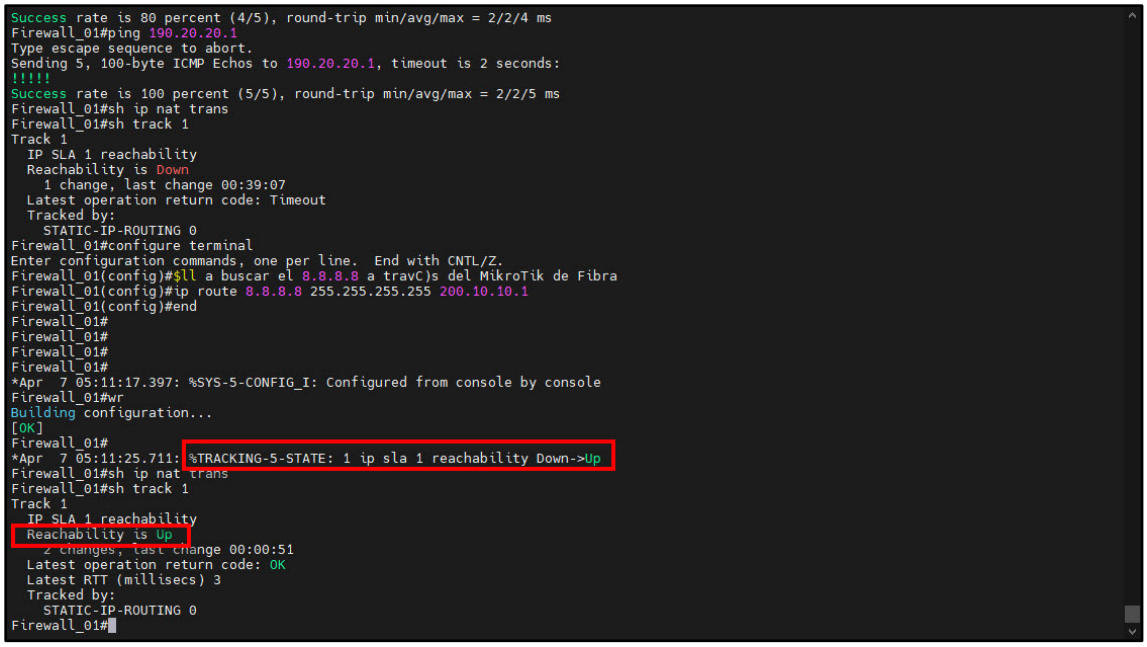
Para verificar la eficacia del diseño de redundancia híbrida, se realizó una prueba de conmutación por error (Failover). Este procedimiento simula una contingencia real en la infraestructura de fibra óptica de Yopal para validar la respuesta automática del Firewall hacia el enlace satelital.

Escenario de Operación Normal

En condiciones estables, el Firewall prioriza el tráfico a través del enlace terrestre de fibra. El objeto de rastreo (Track 1) se mantiene en estado positivo al recibir respuesta de la sonda ICMP desde el nodo MikroTik.

Figura 4.

Estado de Normalidad del Enlace Primario.



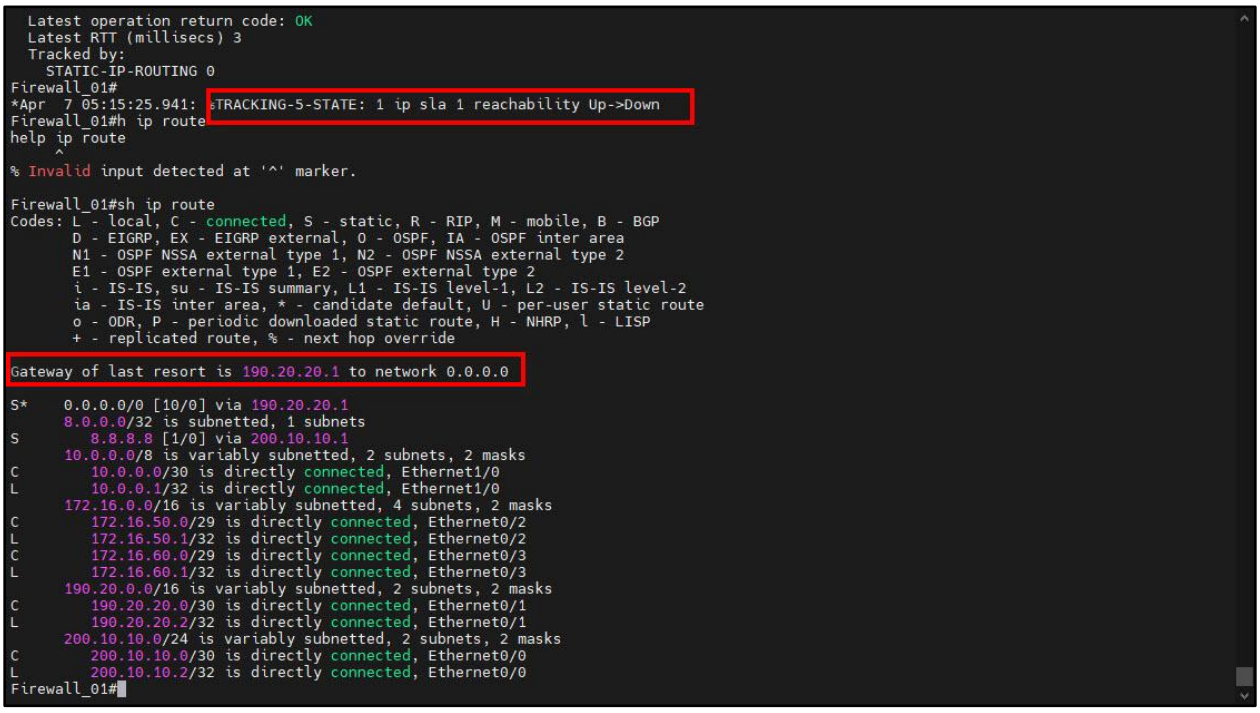
Nota. En la imagen de la figura 4, e evidencia la disponibilidad del enlace (Reachability is Up) y un tiempo de respuesta (RTT) óptimo de 3ms. Tomado de: *Elaboración propia.*

Simulación de Falla y Conmutación Automática

Se procedió a deshabilitar la interfaz de salida en el router **ISP_FIBRA** mediante el comando /interface disable ether1. De manera inmediata, el Firewall detecta la pérdida de conectividad, generando un evento en el log del sistema y modificando dinámicamente la tabla de enrutamiento.

Figura 5.

Detección de Falla en el Enlace de Fibra Óptica.



Nota. El mensaje del sistema %TRACK-6-STATE confirma la transición de Up a Down, activando el protocolo de contingencia. Tomado de: *Elaboración propia.*

Activación del Enlace de Respaldo (Starlink)

Al caer el enlace primario, la ruta estática con distancia administrativa (AD) de 1 es retirada de la tabla de enrutamiento, permitiendo que la ruta de respaldo (Starlink) con AD de 10 tome el control del tráfico.

Figura 6.

Enrutamiento Durante la Contingencia.

```
Firewall_01#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 190.20.20.1 to network 0.0.0.0

S*    0.0.0.0/0 [10/0] via 190.20.20.1
      8.0.0.0/32 is subnetted, 1 subnets
S        8.8.8.8 [1/0] via 200.10.10.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/30 is directly connected, Ethernet1/0
L        10.0.0.1/32 is directly connected, Ethernet1/0
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.50.0/29 is directly connected, Ethernet0/2
L        172.16.50.1/32 is directly connected, Ethernet0/2
C        172.16.60.0/29 is directly connected, Ethernet0/3
L        172.16.60.1/32 is directly connected, Ethernet0/3
      190.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        190.20.20.0/30 is directly connected, Ethernet0/1
L        190.20.20.2/32 is directly connected, Ethernet0/1
      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.10.10.0/30 is directly connected, Ethernet0/0
L        200.10.10.2/32 is directly connected, Ethernet0/0
Firewall_01#
```

Nota. Se observa que la puerta de enlace predeterminada ha cambiado automáticamente a la IP 190.20.20.1 (Starlink). Tomado de: *Elaboración propia.*

Recuperación y Retorno (Preemption)

Finalmente, al habilitar nuevamente la interfaz en el MikroTik (/interface enable ether1), el Firewall reconoce la restauración del servicio primario y, debido a la menor distancia administrativa, restablece la Fibra Óptica como salida principal de forma transparente para los usuarios.

Figura 7.

Restablecimiento Automático de la Ruta por Fibra Óptica.

```
L        172.16.50.1/32 is directly connected, Ethernet0/2
C        172.16.60.0/29 is directly connected, Ethernet0/3
L        172.16.60.1/32 is directly connected, Ethernet0/3
      190.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        190.20.20.0/30 is directly connected, Ethernet0/1
L        190.20.20.2/32 is directly connected, Ethernet0/1
      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.10.10.0/30 is directly connected, Ethernet0/0
L        200.10.10.2/32 is directly connected, Ethernet0/0
Firewall_01#
*Apr  7 05:19:03.056: %TRACKING-5-STATE: 1 ip sla 1 reachability Down->Up
Firewall_01#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 200.10.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 200.10.10.1
      8.0.0.0/32 is subnetted, 1 subnets
S        8.8.8.8 [1/0] via 200.10.10.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/30 is directly connected, Ethernet1/0
L        10.0.0.1/32 is directly connected, Ethernet1/0
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.50.0/29 is directly connected, Ethernet0/2
L        172.16.50.1/32 is directly connected, Ethernet0/2
C        172.16.60.0/29 is directly connected, Ethernet0/3
L        172.16.60.1/32 is directly connected, Ethernet0/3
      190.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        190.20.20.0/30 is directly connected, Ethernet0/1
L        190.20.20.2/32 is directly connected, Ethernet0/1
      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.10.10.0/30 is directly connected, Ethernet0/0
L        200.10.10.2/32 is directly connected, Ethernet0/0
Firewall_01#
```

Nota. Una vez detectada la disponibilidad del Carrier principal mediante el IP SLA, el Firewall reinserta la ruta con Distancia Administrativa 1 en la tabla de enrutamiento, desplazando el enlace de Starlink al estado de reserva (Standby). Tomado de: *Elaboración propia.*

"Los scripts detallados de configuración que permiten este comportamiento dinámico en los equipos Cisco y MikroTik, se encuentran debidamente documentados y clasificados por dispositivo en el Anexo A de este informe."

Implementación de Enrutamiento Dinámico OSPF, Concepto de SDN y Aplicación de SD-WAN.

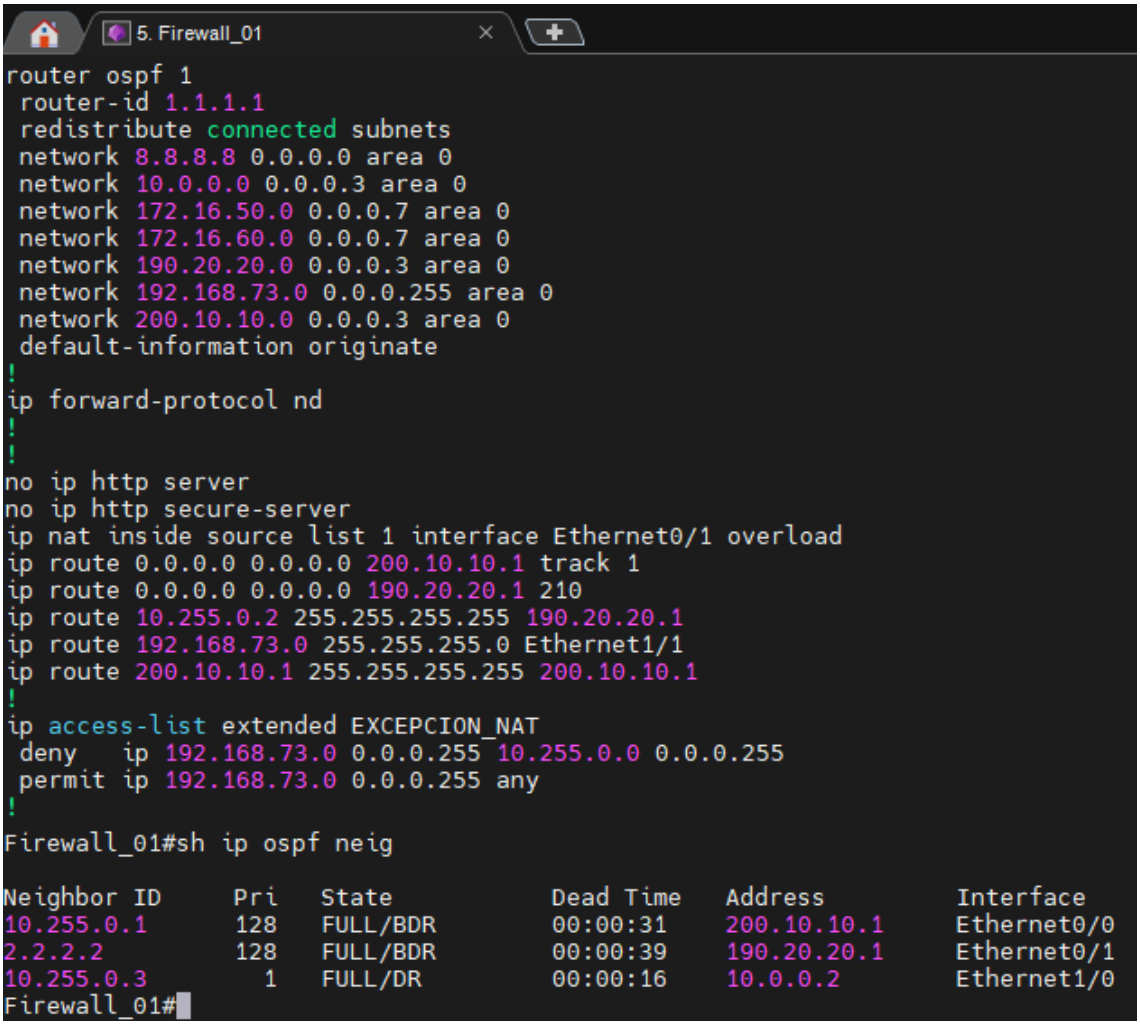
Enrutamiento Dinámico vía OSPF

Para garantizar que la información fluya sin interrupciones desde la profundidad de la red local (LAN) hacia la salida a Internet, el prototipo utiliza el protocolo OSPF (Open Shortest Path First). Su función principal es permitir que todos los dispositivos de la red (Switches Core, Routers y Firewall) "hablen" el mismo idioma y compartan sus rutas de forma automática.

El objetivo de implementar OSPF es eliminar la necesidad de configurar rutas estáticas manualmente en cada equipo. En este diseño, OSPF permite que si un enlace interno falla, el protocolo calcule instantáneamente la ruta más corta alternativa. En términos de Alta Disponibilidad (HA), OSPF asegura que el tráfico sepa siempre cómo llegar al Firewall para salir por los ISP, manteniendo la convergencia de la red en milisegundos.

Figura 8.

Estado de Adyacencia y Rutas Aprendidas vía OSPF en Firewall_01.



Nota. La imagen muestra la tabla de vecinos OSPF y las redes aprendidas desde el Core. Se observa cómo el Firewall reconoce dinámicamente los segmentos LAN y las VLANs de usuario, estableciendo una adyacencia completa (Full) con el Router de Core. Tomado de: *Elaboración propia.*

Matriz de Convergencia OSPF

A continuación, se relacionan los equipos que participan en el proceso de enrutamiento dinámico y las redes que propagan.

Tabla 2.

Matriz de Convergencia OSPF

Equipo	Área OSPF	Redes de Origen (Anuncio)	Destino / Vecindad
Firewall_01	0 (Backbone)	10.0.0.0/30 (Enlace Core)	RT_Core
RT_Core	0 (Backbone)	10.0.0.0/30, 172.16.50.0/29 (DMZ)	Firewall_01 / SW_Core
SW_Core	0 (Backbone)	192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24	RT_Core

Nota. La tabla muestra las rutas que convergen en el protocolo OSPF del prototipo, su origen y destino y su convergencia dentro de la topología. Tomado de: *Elaboración propia.*

Concepto Aplicado de SDN

Aunque el presente prototipo no implementa una plataforma SD-WAN comercial completa con controladores centralizados dedicados (vManage, vSmart o equivalentes), sí incorpora principios funcionales asociados a arquitecturas SDN/SD-WAN, especialmente en la automatización del tráfico y la toma de decisiones basada en el estado operativo de los enlaces WAN.

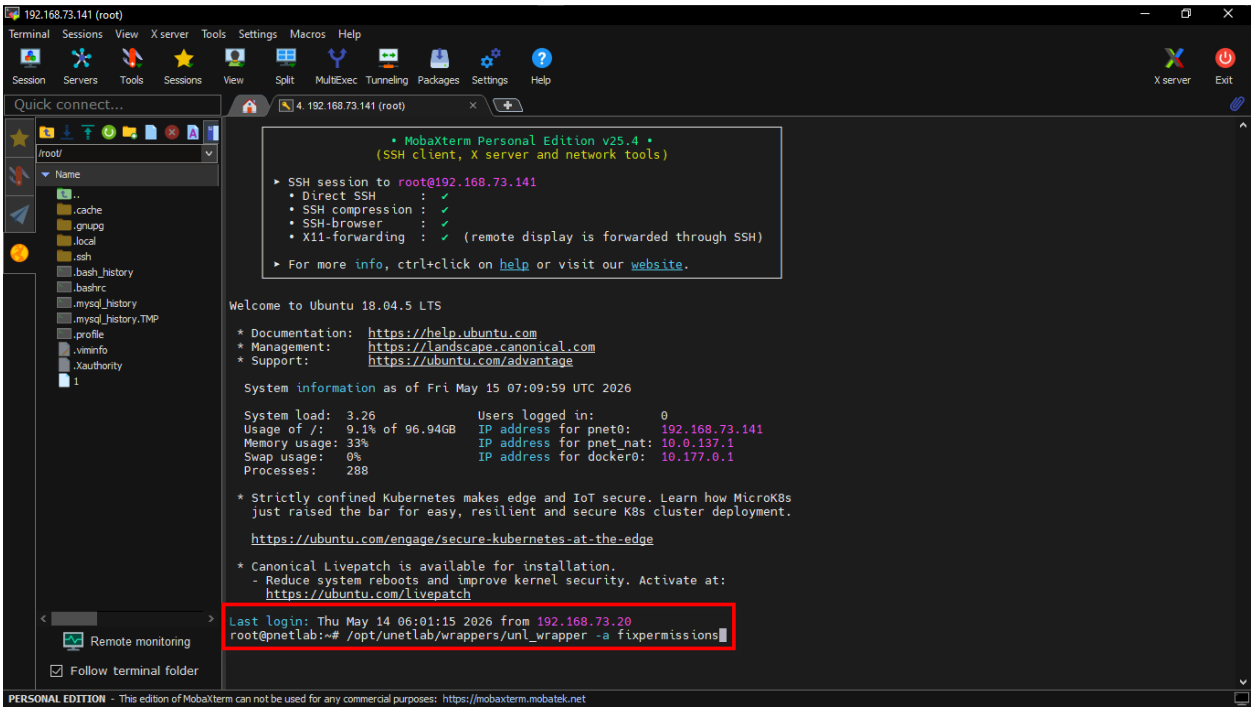
La solución desarrollada integra mecanismos de monitoreo activo mediante IP SLA, objetos de seguimiento (Track), convergencia dinámica OSPF y políticas automatizadas de failover entre enlaces terrestres y satelitales, permitiendo una administración lógica del tráfico orientada a la continuidad del servicio.

En este contexto, el diseño propuesto se aproxima conceptualmente a un modelo SD-WAN híbrido, donde la inteligencia de conmutación y resiliencia de red se fundamenta en métricas operativas y supervisión distribuida mediante PRTG Network Monitor.

De esta manera, el proyecto trasciende una configuración tradicional de redundancia estática, incorporando elementos de automatización, monitoreo y gestión dinámica alineados con los principios modernos de redes resilientes definidas por software.

Figura 9.

Ejecución de Scripts y Permisos Globales Vía MobaXterm.



Nota. Mediante la terminal de MobaXterm se ejecutan comandos de bajo nivel para asegurar la integridad de los nodos virtualizados. El comando fixpermissions garantiza que el plano de control tenga los privilegios necesarios para operar los recursos de red sin conflictos. Tomado de: *Elaboración propia.*

Aplicación Flujo SD-WAN (Failover)

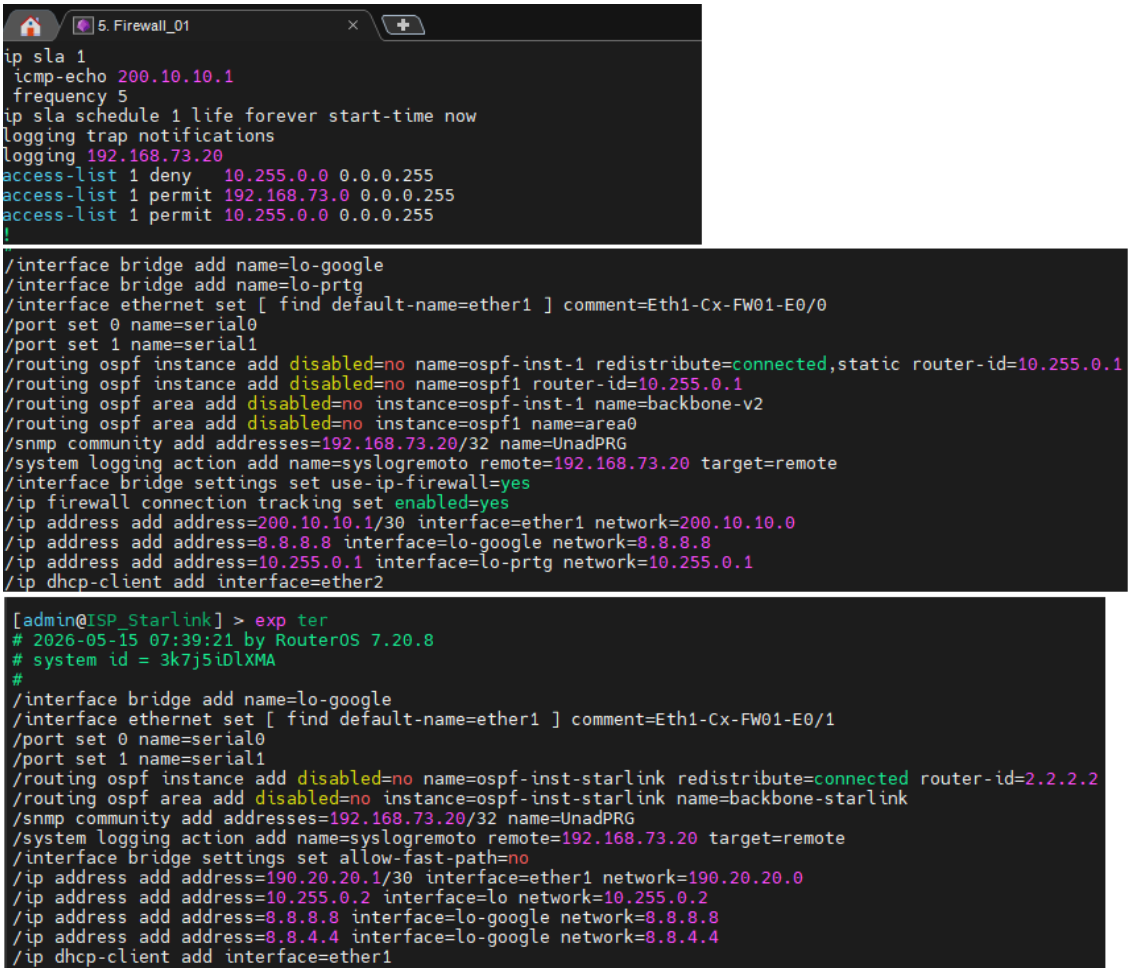
El concepto de SD-WAN (Red de Área Amplia Definida por Software) se implementa en este prototipo mediante el uso de IP SLA (Service Level Agreement) en el Firewall de borde. A

diferencia de un enrutamiento tradicional que solo sabe si una interfaz está conectada o no, el flujo SD-WAN analiza la *calidad* del enlace.

El sistema realiza "pings" constantes hacia destinos en Internet a través de ambos proveedores (Starlink y Fibra Local). Si el enlace de fibra (principal) presenta pérdida de paquetes o latencia alta, el mecanismo de IP SLA detecta que el contrato de servicio no se cumple y conmuta el tráfico automáticamente hacia el enlace satelital. Esta capacidad de tomar decisiones inteligentes basadas en el estado del servicio es lo que permite garantizar una Alta Disponibilidad (HA) real para las empresas de telecomunicaciones en Yopal.

Figura 10.

Monitoreo IP SLA para Gestión de Redundancia WAN.



Nota. Se visualiza la configuración de los objetos de monitoreo que validan la salud de los enlaces externos. Este mecanismo es el cerebro del Failover, permitiendo el cambio transparente de proveedor sin intervención humana. Tomado de: *Elaboración propia.*

Este proceso de conmutación automática no solo garantiza la persistencia de las sesiones activas, sino que representa la base de la Alta Disponibilidad propuesta para el entorno empresarial de Yopal. Al integrar el monitoreo de capa 3 mediante IP SLA con la flexibilidad del enrutamiento dinámico, el diseño logra una resiliencia que minimiza el impacto operativo ante incidentes de infraestructura externa. De esta manera, el prototipo demuestra que la convergencia entre los servicios de fibra óptica local y el respaldo satelital de Starlink crea un ecosistema de red redundante, capaz de sostener la operación crítica de un Data Center sin requerir la intervención manual del administrador de red ante una caída de servicio.

Capítulo 3. Virtualización, Monitoreo Distribuido y Soporte de Infraestructura

Se desarrolla el entorno de infraestructura y servicios críticos (Autenticación, Resolución de Nombres DNS y Enlaces de Internet) en alta disponibilidad. Para asegurar la visibilidad total, se integra la plataforma PRTG Network Monitor, implementando sensores específicos de Uptime, Latencia, Jitter y Pérdida de Paquetes, permitiendo la trazabilidad técnica de los SLA. Asimismo, se incorporan las capas de seguridad perimetral mediante autenticación AAA, auditoría centralizada de eventos y el diseño de respaldo energético para garantizar la continuidad absoluta del negocio.

Entorno de Emulación en PNetLab

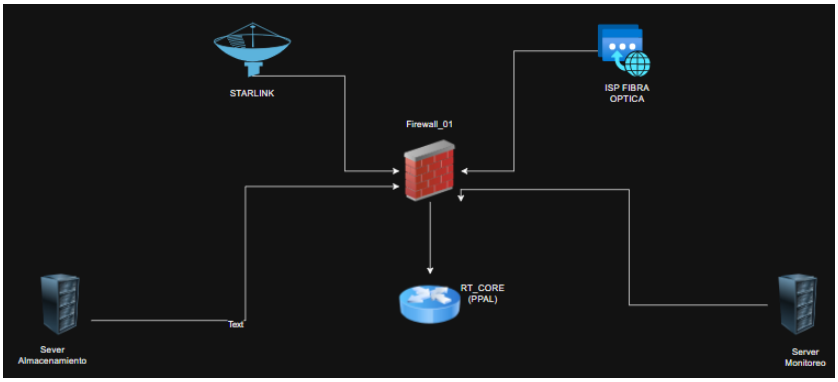
La materialización del diseño se realizará mediante la plataforma de emulación PNetLab, la cual permite la ejecución de imágenes de sistemas operativos de red reales en un entorno virtualizado de alta fidelidad. Para este prototipo, se desplegaron y orquestaron los siguientes nodos críticos:

Firewall Perimetral (Cisco IOSv)

Actúa como el cerebro de la red, encargado de la terminación de los vectores WAN y la ejecución de políticas de seguridad y enrutamiento inteligente.

Figura 11.

Topología de la Red Centralizada.



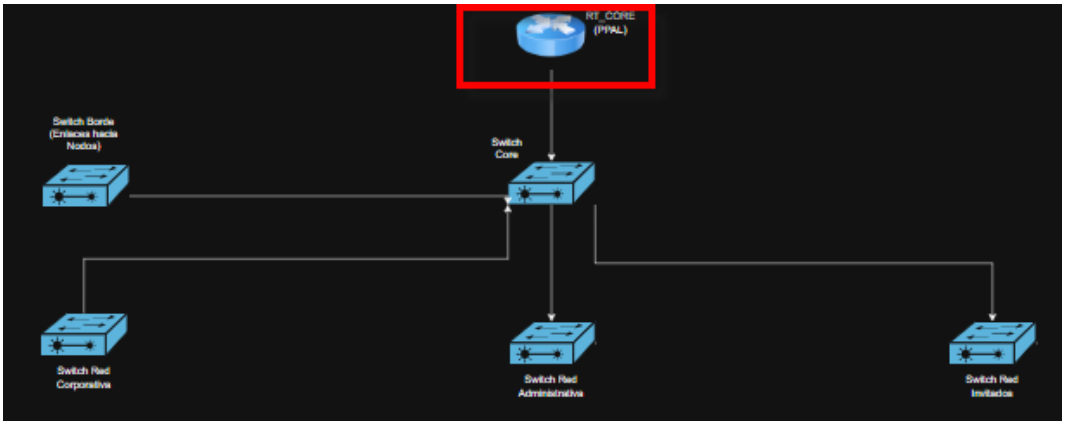
Nota. En la figura evidenciamos la coexistencia de las conexiones principales al Firewall, que actual este como motor centralizador y cerebro de la red. Tomado de: *Elaboración propia*.

Core Router (Cisco IOL)

Implementado para la gestión del enrutamiento interno, la terminación de enlaces troncales y la segregación del tráfico mediante VLANs operativas.

Figura 12.

Router Core del Prototipo



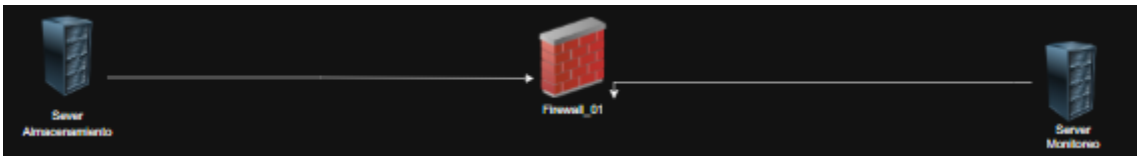
Nota. La figura 12, muestra la ubicación del Router Core, que ejecuta las reglas para que la conectividad hacia las redes internas se lleve a cabo. Tomado de: *Elaboración propia.*

Nodos de Servicios DMZ

Segmentos aislados configurados para simular servicios críticos de almacenamiento y la estación de gestión de red.

Figura 13.

Zona DMZ para Servidores Críticos



Nota. La Figura 13, muestra la conexión de servidores considerados críticos en la operación de prototipado, conectados al Firewall como zona segura, con su propio direccionamiento IP diferente al de la LAN. Tomado de: *Elaboración propia.*

Gestión de Enlaces Mediante SD-WAN (Policy-Based Routing)

Se implementó un esquema de Gestión Inteligente de Enlaces donde el Firewall monitorea la disponibilidad de los canales de forma activa. La lógica de conmutación se fundamenta en:

Sonda de Salud (Health Check)

El protocolo IP SLA genera un flujo constante de paquetes ICMP hacia destinos de referencia en internet (DNS de Google 8.8.8.8) a través del enlace de fibra óptica.

Figura 14.

Estadísticas del IP SLA en el Firewall 01

```
Firewall_01#sh ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: 1 milliseconds
Latest operation start time: 20:21:38 UTC Sat May 16 2026
Latest operation return code: OK
Number of successes: 349
Number of failures: 0
Operation time to live: Forever
```

Nota. La figura 14, muestra las estadísticas del IP SLA en el Firewall, con las cuales se asegura que la consulta hacia internet es continua y de esta manera se garantiza que la conectividad está siendo estable. Tomado de: *Elaboración propia.*

Umbral de Conmutación Automática

Se definió una política de Failover basada en la disponibilidad (*Reachability*). Ante la detección de una pérdida de respuesta del Carrier principal, el sistema retira la ruta primaria y

activa el enlace satelital Starlink en milisegundos, garantizando la continuidad del negocio en la sede Yopal.

Figura 15.

Rutas Estáticas Condicionadas por Tracking

```
Firewall_01#  show run | include ip route
 no ip route-cache
ip route 0.0.0.0 0.0.0.0 200.10.10.1 track 1
ip route 0.0.0.0 0.0.0.0 190.20.20.1 210
ip route 10.255.0.2 255.255.255.255 190.20.20.1
ip route 192.168.73.0 255.255.255.0 Ethernet1/1
ip route 200.10.10.1 255.255.255.255 200.10.10.1
Firewall_01#
```

Nota. La captura de pantalla detalla el núcleo lógico del Failover en la configuración de Cisco IOSv. Se observa la ruta por defecto hacia el Gateway de Fibra Óptica vinculada al objeto de rastreo (Track 1), y en la línea inferior, la ruta hacia el Gateway de Starlink configurada con una Distancia Administrativa flotante (210), actuando como respaldo pasivo. Tomado de: *Elaboración propia.*

Instrumentación de Monitoreo y Métricas de Rendimiento

Para la validación de la disponibilidad y la trazabilidad técnica del prototipo, se integró el software PRTG Network Monitor, el cual se comunica con la infraestructura emulada mediante el protocolo SNMP. Esta capa de observabilidad centralizada opera desde la Workstation (192.168.73.20), donde los segmentos de red convergen gracias al protocolo de enrutamiento dinámico OSPF, permitiendo recolectar datos en tiempo real para evaluar el comportamiento de los enlaces de Yopal bajo los siguientes parámetros críticos:

Disponibilidad (Uptime)

Cuenta con un despliegue total de 62 sensores distribuidos en 19 dispositivos de red. Los sensores de Ping y Uptime son predominantes, ya que entregan el estatus más certero sobre la

permanencia de la infraestructura, siendo indispensables para verificar el cumplimiento de los ANS pactados y capturar la resiliencia del sistema.

Latencia (Ping)

Registro de los tiempos de respuesta (RTT) hacia los gateways de los ISPs y destinos externos, identificando degradaciones en el transporte de datos.

Gestión de Tráfico (SNMP Traffic)

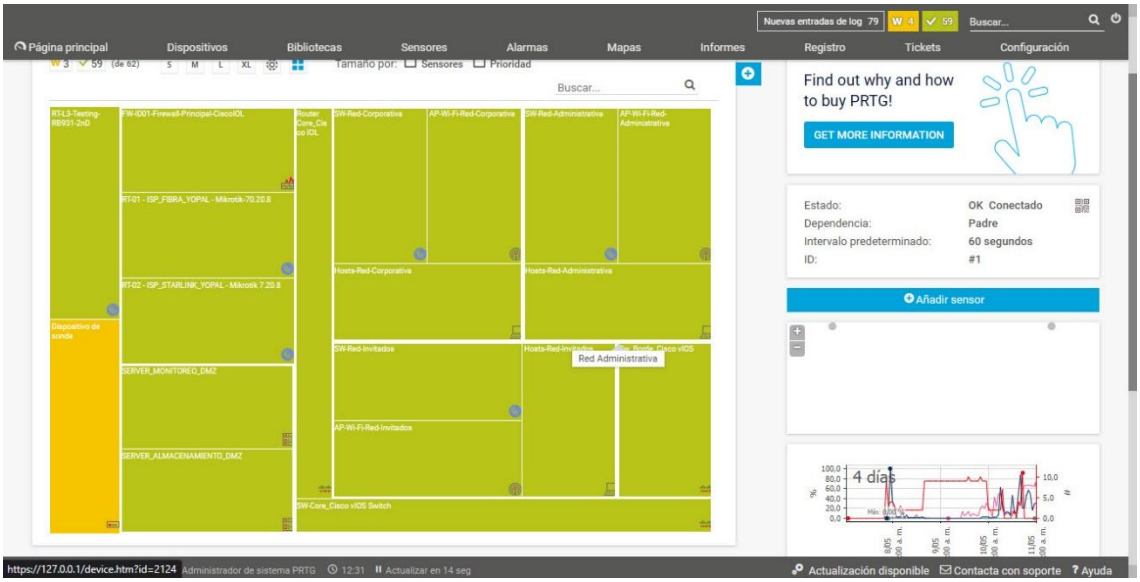
Visualización de la carga de ancho de banda en las interfaces Ethernet0/0 (Fibra) y Ethernet0/1 (Starlink), validando que el failover desvíe el flujo de datos correctamente durante una contingencia. El Firewall posee una interfaz dedicada para el tráfico de gestión y el equipo hAP aprende este direccionamiento mediante rutas estáticas, aislando el monitoreo del tráfico común de usuarios.

Calidad del Enlace (Packet Loss & Jitter)

Sensores fundamentales para comparar la estabilidad de la fibra óptica frente a la conexión satelital. La medición de la variación en el retardo (Jitter) y el porcentaje de paquetes descartados permite determinar la idoneidad del enlace de respaldo para servicios sensibles.

Figura 16.

Dashboard Central del NOC en PRTG Network Monitor.



Nota. La imagen muestra el monitoreo de PRTG de los equipos del prototipo simulado en PNETLab. Se evidencia el estado operativo de los 62 sensores dedicados a registrar la disponibilidad (Uptime) Tomado de: *Elaboración propia.*

Figura 17.

Árbol de Sensores de la Red del Prototipo en PRTG.


W 3
59 (de 62)
S
M
L
XL
Buscar...
Sonda local
Dispositivo de sonda
Salud de siste... 85 %
Salud de sonda 100 %
Salud del servi... 100 %
Disco disponible 31 %
Common SaaS... 88 %
Qualcomm Ath... 0 Mbit/s
Realtek PCIe F... 0,16 Mbit/s
Memoria (WMI) 15 %
Añadir sensor
RT-L3-Testing-RB931-2nD
Ping 5 mseg
Tiempo activo ... 1 h 18 m
Eth1-Cx-WAN-I... 0,09 Mbit/s
Eth2-Cx-WS-La... 0,13 Mbit/s
Eth3-Cx-Server... 0,02 Mbit/s
Añadir sensor
Equipos Core D/C
FW-ID01-Firewall-Principal-CiscoIOL
Ping 1 mseg
Tiempo activo ... 18 h 20 m
(001) WAN_IS... < 0,01 Mbit/s
(002) WAN_ST... < 0,01 Mbit/s
Jitter de Ping 3,97
System Health ... 0 %
System Health ... 0,06 GB
Añadir sensor
RT-01 - ISP_FIBRA_YOPAL - Mikrotik-70.20.8
Ping 8 mseg
Añadir sensor
RT-02 - ISP_STARLINK_YOPAL - Mikrotik 7.20.8
Ping 8 mseg
Añadir sensor
Zona DMZ
SERVER_MONITOREO_DMZ
Ping 8 mseg
Añadir sensor
SERVER_ALMACENAMIENTO_DMZ
Ping 8 mseg
Añadir sensor
Administración Core
Router Core_Cisco IOL
Ping 11 mseg
Tiempo activo ... 11 h 3 m
(001) ENLACE... < 0,01 Mbit/s
(002) TRONCA... < 0,01 Mbit/s
(007) Ethernet... < 0,01 Mbit/s
(008) Ethernet... < 0,01 Mbit/s
(009) Ethernet... < 0,01 Mbit/s
(010) Ethernet... < 0,01 Mbit/s
Añadir sensor
SW-Core_Cisco vIOS Switch
Ping 11 mseg
Tiempo activo ... 18 h 2 m
(001) TRUNK_... < 0,01 Mbit/s
(002) LINK_TO... < 0,01 Mbit/s
(003) LINK_TO... < 0,01 Mbit/s
(004) LINK_TO... < 0,01 Mbit/s
(005) LINK_TO... < 0,01 Mbit/s
Añadir sensor
Distribución LAN
Red Corporativa
SW-Red-Corporativa
Ping 11 mseg
Tiempo activo ... 18 h 21 m
(006) ether5 Tr... < 0,01 Mbit/s
(007) ether6 Tr... < 0,01 Mbit/s
(008) ether7 Tr... < 0,01 Mbit/s
Añadir sensor
AP-Wi-Fi-Red-Corporativa
Ping 14 mseg
Añadir sensor
Hosts-Red-Corporativa Recomendación de sensor en progreso (36%)
Ping 16 mseg
Añadir sensor
Red Administrativa
SW-Red-Administrativa
Ping 11 mseg
Tiempo activo ... 18 h 21 m
(006) ether5 Tr... < 0,01 Mbit/s
(007) ether6 Tr... < 0,01 Mbit/s
(008) ether7 Tr... < 0,01 Mbit/s
Añadir sensor
AP-Wi-Fi-Red-Administrativa Recomendación de sensor en progreso (16%)
Ping 25 mseg
Añadir sensor
Hosts-Red-Administrativa
Ping 13 mseg
Añadir sensor
Red Invitados
SW-Red-Invitados
Ping 22 mseg
Tiempo activo ... 18 h 21 m
(006) ether5 Tr... < 0,01 Mbit/s
(007) ether6 Tr... < 0,01 Mbit/s
(008) ether7 Tr... < 0,01 Mbit/s
Añadir sensor
AP-Wi-Fi-Red-Invitados
Ping 14 mseg
Añadir sensor
Hosts-Red-Invitados
Ping 12 mseg
Añadir sensor
Red de Borde hacia Backbone
Sw_Borde_Cisco vIOS
Ping 15 mseg
Tiempo activo ... 18 h 11 m
Añadir sensor

Nota. La imagen muestra la jerarquía de los 19 dispositivos de red bajo el monitoreo de PRTG. Se evidencia el estado operativo de los 62 sensores dedicados a registrar la disponibilidad (Uptime) y el rendimiento en tiempo real del prototipo. Tomado de: *Elaboración propia.*

Control de Acceso Centralizado (Seguridad AAA vía RADIUS)

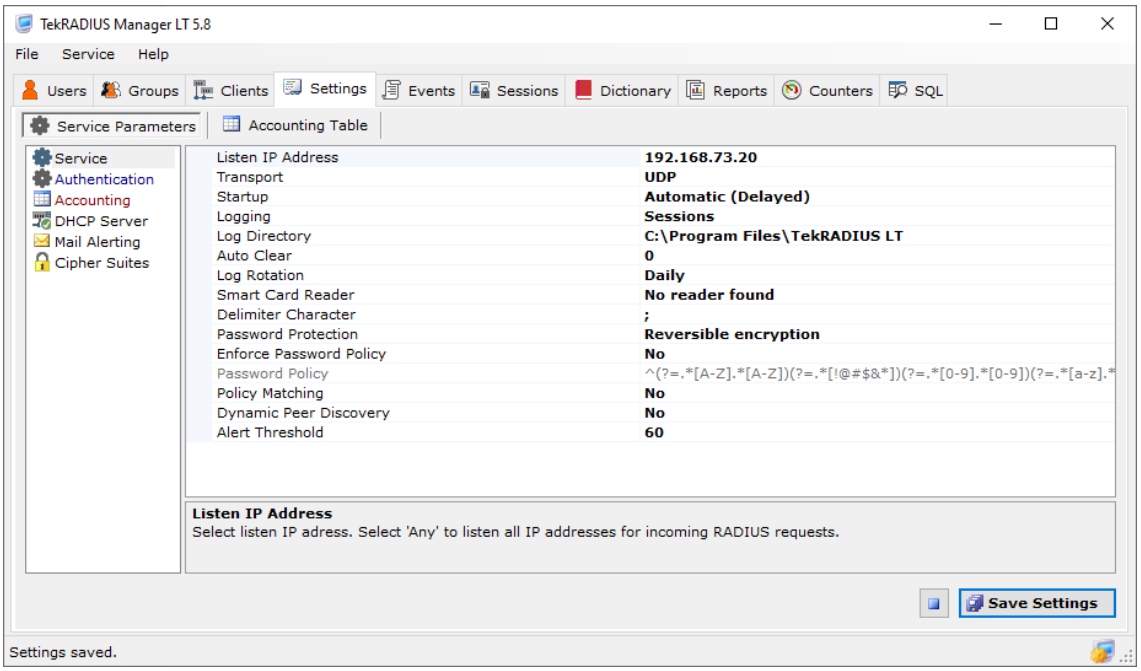
Como complemento indispensable de la infraestructura de gestión y para blindar el acceso administrativo a los elementos del Core (Cisco y MikroTik), se integró el protocolo RADIUS. Este servicio se ejecuta mediante la plataforma TekRADIUS alojada en la Workstation de gestión (192.168.73.20). El sistema elimina la gestión de cuentas locales e inseguras en cada equipo, centralizando la autenticación y asignación de privilegios en una sola base de datos de ingeniería.

Parametrización del Servicio y Clientes de Red en TekRADIUS

Para la puesta en marcha de la seguridad perimetral, el servidor TekRADIUS fue configurado para escuchar peticiones de autenticación en la interfaz de red dedicada a la Workstation. Asimismo, se mapeó el inventario de hardware del Core del proyecto, asociando una clave secreta compartida (*Shared Secret*) por cada dispositivo para cifrar los paquetes de autenticación en el tránsito local.

Figura 18.

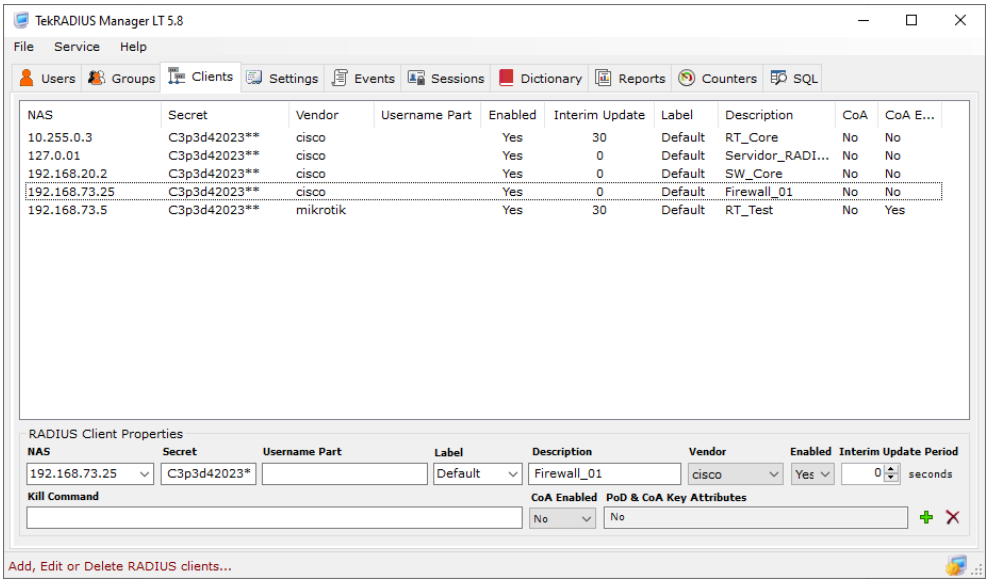
Configuración de Parámetros Globales de Red del Servicio TekRADIUS.



Nota. La captura de la pestaña Settings evidencia la asignación de la dirección IP de escucha (192.168.73.20) operando sobre el protocolo de transporte UDP, garantizando la compatibilidad estándar de las solicitudes AAA provenientes de la infraestructura virtual y física. Tomado de: *Elaboración propia.*

Figura 19.

Matriz de Clientes NAS Autorizados en el Servidor AAA



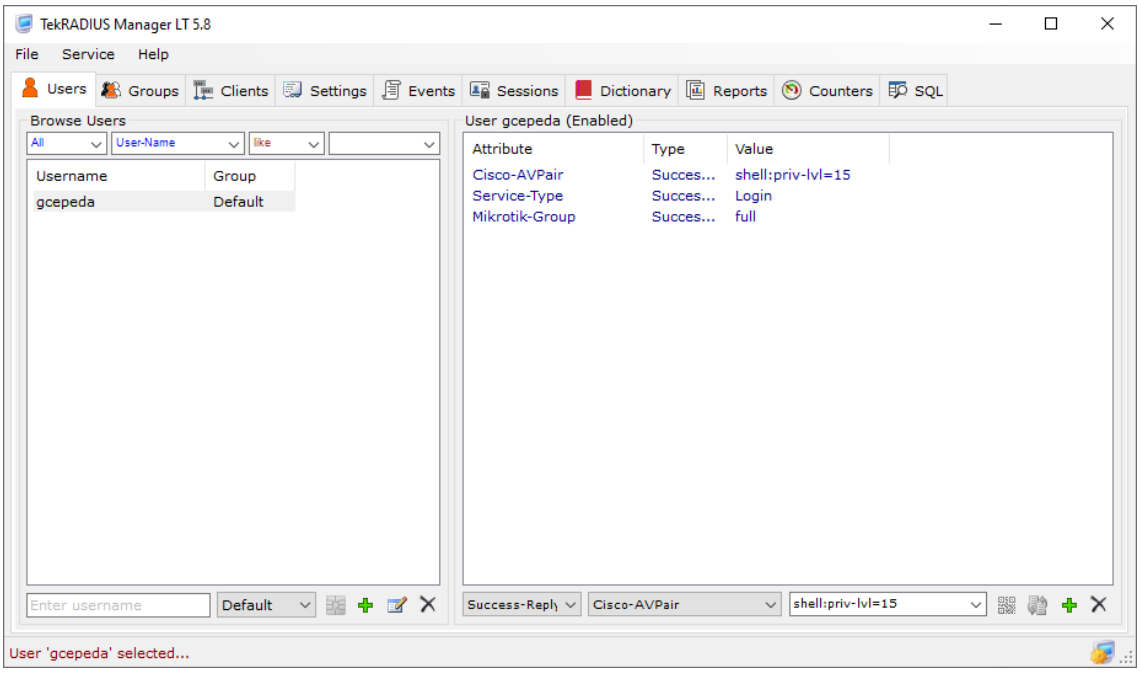
Nota. Registro de los nodos de red configurados como clientes RADIUS válidos, detallando sus direcciones IP de gestión (10.255.0.3 para RT_Core, 192.168.20.2 para SW_Core, 192.168.73.25 para Firewall_01 y 192.168.73.5 para el hAP de MikroTik), asegurando el aislamiento y la confianza de las solicitudes. Tomado de: *Elaboración propia.*

Control de Acceso Basado en Roles (Atributos VSA)

Un aspecto crítico en la seguridad AAA consiste en asegurar que, tras una autenticación exitosa, el servidor inyecte los privilegios operativos correctos al administrador. Como se observa a continuación, se parametrizó un perfil unificado capaz de responder con atributos específicos tanto para los entornos Cisco como para la plataforma MikroTik.

Figura 20.

Definición de Usuarios y Perfiles con Atributos Vendor-Specific (VSA).



Nota. Detalle del usuario operativo (gcepeda) donde se configuran las respuestas automáticas de éxito (Success-Reply). Destacan los atributos Cisco-AVPair con valor shell: priv-lvl=15 para

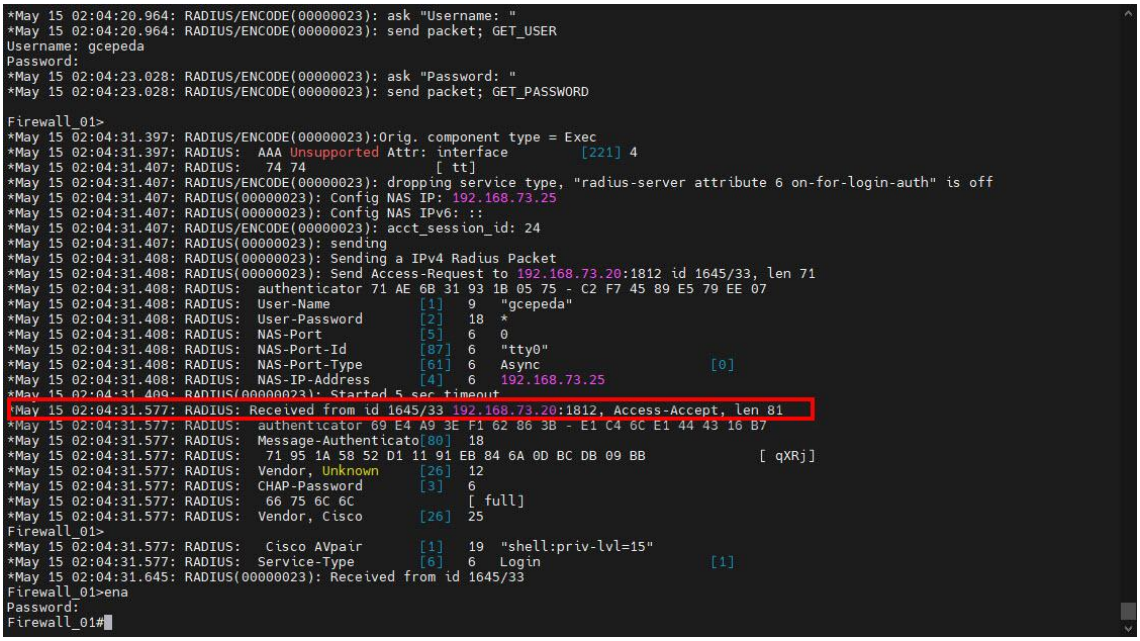
habilitar el modo privilegiado automático en Cisco, y Mikrotik-Group con valor full para otorgar control total en el router de pruebas. Tomado de: *Elaboración propia.*

Validación del Protocolo en Consola (Debugs)

Para comprobar el correcto intercambio de mensajes lógicos en la arquitectura AAA, se ejecutaron comandos de acceso en tiempo real en el nodo perimetral. Esta inspección profunda permite auditar los campos de cabecera contenidos en los paquetes UDP del protocolo RADIUS durante una solicitud de acceso administrativo.

Figura 21.

Trazabilidad de Autenticación y Autorización AAA en Firewall_01.



Nota. La captura de la terminal detalla el flujo de depuración (debug) en Cisco IOSv. Se destaca la salida de un paquete Access-Request desde la IP del Firewall hacia el servidor (192.168.73.20) y la posterior respuesta afirmativa Access-Accept (recuadro rojo), la cual inyecta de forma exitosa el atributo Cisco-AVPair con el nivel de privilegios operativo máximo (shell: priv-lvl=15). Tomado de: *Elaboración propia.*

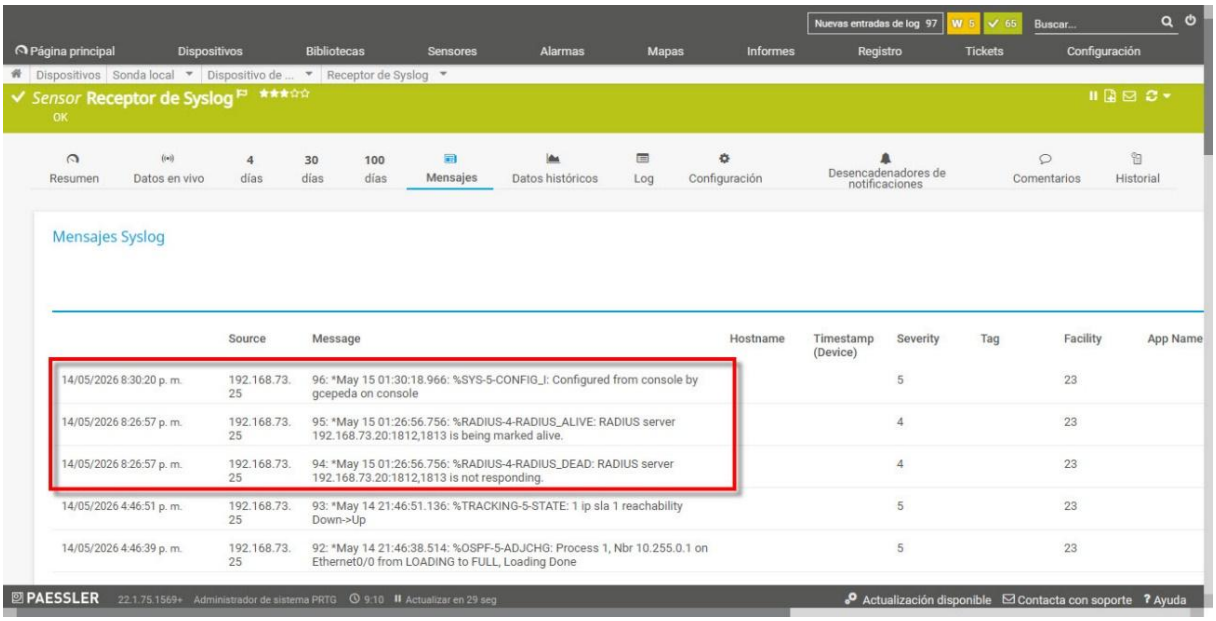
La concordancia absoluta entre los parámetros definidos en el gestor TekRADIUS y la traza de eventos obtenida en la línea de comandos del Firewall_01 demuestra la efectividad de la solución de seguridad. Al comprobar que el prompt del sistema realiza la transición automática al modo privilegiado (Firewall_01#), se valida experimentalmente el cumplimiento del control de acceso basado en roles (RBAC). Esta centralización mitiga vectores de ataque por fuerza bruta sobre los elementos de la red y establece un estándar de seguridad robusto para proteger la infraestructura crítica local.

Auditoría de Eventos de Infraestructura (Servidor Syslog)

Para asegurar que toda degradación o cambio de estado de la red quede plenamente registrado, se implementó un receptor de Syslog centralizado en la IP 192.168.73.20. Los dispositivos están configurados para enviar alertas de severidad crítica, advertencias y cambios de estado en interfaces hacia este nodo, permitiendo al administrador realizar análisis forenses ante fallas y llevar una trazabilidad rigurosa del prototipo.

Figura 22.

Consola de Recepción de Eventos Syslog en Tiempo Real.



Nota. La captura evidencia la recopilación cronológica de eventos de red generados por los nodos del laboratorio, lo que permite correlacionar caídas de interfaces con los tiempos de respuesta del sistema de failover, esta visualización se realiza desde el centralizador de PRTG. Tomado de: *Elaboración propia.*

Modernización y Respaldo Eléctrico (Sistema Solar Fotovoltaico)

La disponibilidad de una red en un Data Center no depende únicamente de los canales de telecomunicaciones, sino también de la estabilidad de su suministro eléctrico. Ante fallas en la red eléctrica comercial de Yopal, se incorporó un dimensionamiento técnico para un Sistema Solar Fotovoltaico (SSFV) de respaldo Off-Grid.

Con un cuadro de cargas crítico estimado en **1143.5 Watts** (que comprende el prototipo de diseño), los cálculos determinan la necesidad de un arreglo de 26 paneles solares monocristalinos y un banco de 12 baterías de 200 A/h de gel de ciclo profundo, para un diseño de +48 VDc con 3 bancos en paralelo de 4 baterías conectadas en serie por cada banco, integradas a un inversor híbrido de onda senoidal pura y una autonomía de **1,05 días.**

Es fundamental aclarar que este análisis representa un dimensionamiento técnico propuesto, el cual es flexible y estará sujeto a la capacidad de inversión y a los requerimientos específicos de tiempo de autonomía de cada compañía en la región.

Figura 23.

Matriz de Dimensionamiento del SSFV de Respaldo.

ENERGIA TOTAL					
EQUIPOS	Cantidad	Consumo C/u (W/h)	Consumo Total (W/h)	Uso diario (h/día)	Consumo Máximo (Wh/día)
Cisco Firewall (ASAv)	1,00	45,00	45,00	24,00	1080,00
Cisco Switch Core (3650/3850)	1,00	65,00	65,00	24,00	1560,00
MikroTik hAP mini (RB931-2nD)	1,00	3,50	3,50	24,00	84,00
Servidor PNETLab/RADIUS	1,00	250,00	250,00	24,00	6000,00
Switch de Acceso (L2)	4,00	30,00	120,00	24,00	2880,00
Estación de Administración	1,00	120,00	120,00	24,00	2880,00
Router Core (RT_Core)	1,00	70,00	70,00	24,00	1680,00
Routers ISP (Proveedores)	2,00	35,00	70,00	24,00	1680,00
Servidores (Almacenamiento/DMZ)	2,00	200,00	400,00	24,00	9600,00
	Energía Total	818,50	1143,50		27444,00
				Dimensionamiento	
				Total	27444

SISTEMA FOTOVOLTAICO	
Tensión del sistema (Vdc)	Voltaje_48Vdc
Pérdidas del sistema	30%
Sombras Poste	70%
Horas de Sol Pico (HSP)	3,9
Potencia pico del panel a instalar (Wp	545
Número de Paneles sugerido a instal	25,82
Número de Paneles a instalar	26,00
SISTEMA DE RESPALDO	
Consumo Total del Sistema (Ah/día)	571,75
Días de Autonomia	1
Capacidad del Banco de Batería (A/h)	571,75
Controlador Solar	
Potencia	14.170,00
Corriente	295,21

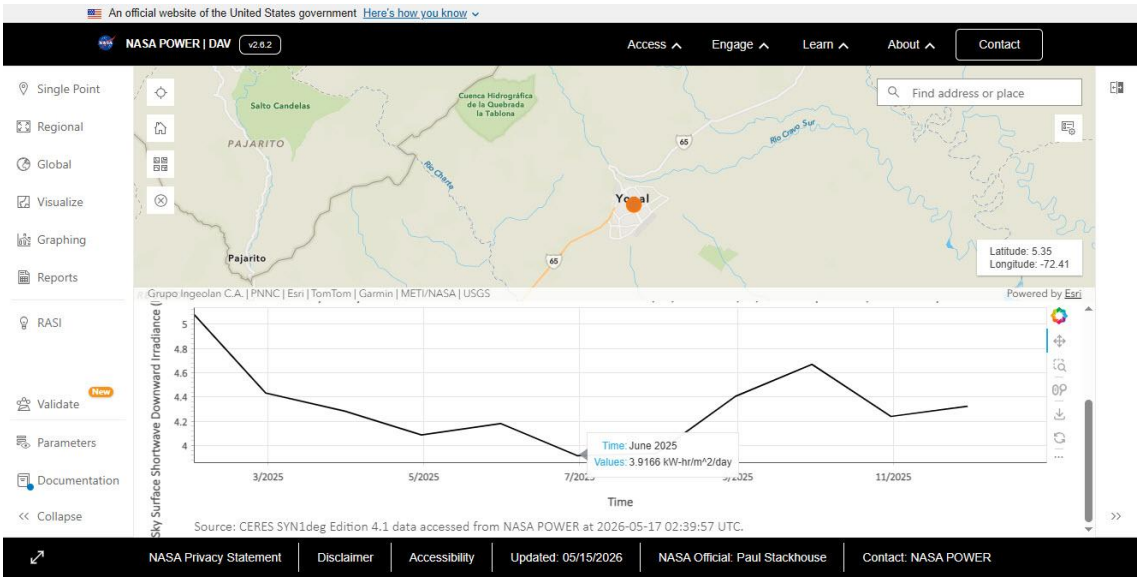
Banco de Baterías a Instalar	
Batería a Instalar (A/h	200
Número de Baterías	12
Autonomía (Días)	1,05

Nota. Detalle técnico de los requerimientos de hardware solar fotovoltaico necesarios para mitigar cortes de energía y sostener la operación continua de los equipos que componen el prototipo. Tomado de: *Elaboración propia.*

Para evaluar el diseño energético en Yopal se descargaron los datos de radiación global horizontal desde la plataforma oficial NASA POWER. Este parámetro se mide en $kW * \frac{h}{m^2}/día$ lo que equivale exactamente a las Horas Sol Pico (HSP) diarias.

Figura 24.

Radiación Solar Mensual (HSP) en Yopal, Casanare (2024–2025).



Nota. El gráfico resalta el punto más crítico en junio de 2025 (3.9166 HSP) valor clave para el cálculo del factor de seguridad en sistemas de respaldo para 2026. Tomado de: *(NASA, 2024)(Modelo CERES SYN1deg 4.1). https://power.larc.nasa.gov/data-access-viewer/*

El comportamiento clave de los últimos dos años muestra:

Picos máximos. Entre enero y marzo (temporada seca), alcanzando entre 5.1 y 6.0 HSP.

Punto crítico (Peor mes). En junio de 2025, debido a las lluvias y nubosidad, el recurso cayó a su mínimo de 3.91 HSP.

Fin de año. Estabilización moderada entre 4.2 y 4.7 HSP.

Referencia para el año 2026. Para garantizar la alta disponibilidad de los sistemas este año, el diseño fotovoltaico debe basarse en el peor escenario (3.91 HSP). Esto asegura que los equipos tengan suficiente autonomía incluso en el mes más nublado del año.

Capítulo 4. Validación de Resultados Mediante la Simulación

El diseño de la arquitectura de red de alta disponibilidad para las empresas prestadoras del servicio de Internet (ISP) de Yopal se valida en el entorno de emulación PNetLab mediante pruebas de estrés e inyección controlada de fallos críticos en los troncales WAN. Los resultados obtenidos permiten evaluar la efectividad de las políticas lógicas implementadas y auditar el comportamiento de los indicadores clave de rendimiento (KPI), demostrando experimentalmente que la integración híbrida proyecta una disponibilidad estructural del **99.8%**, alineada con los más exigentes Acuerdos de Niveles de Servicio (ANS).

Escenarios de Prueba y Procedimiento de Simulación de Fallos

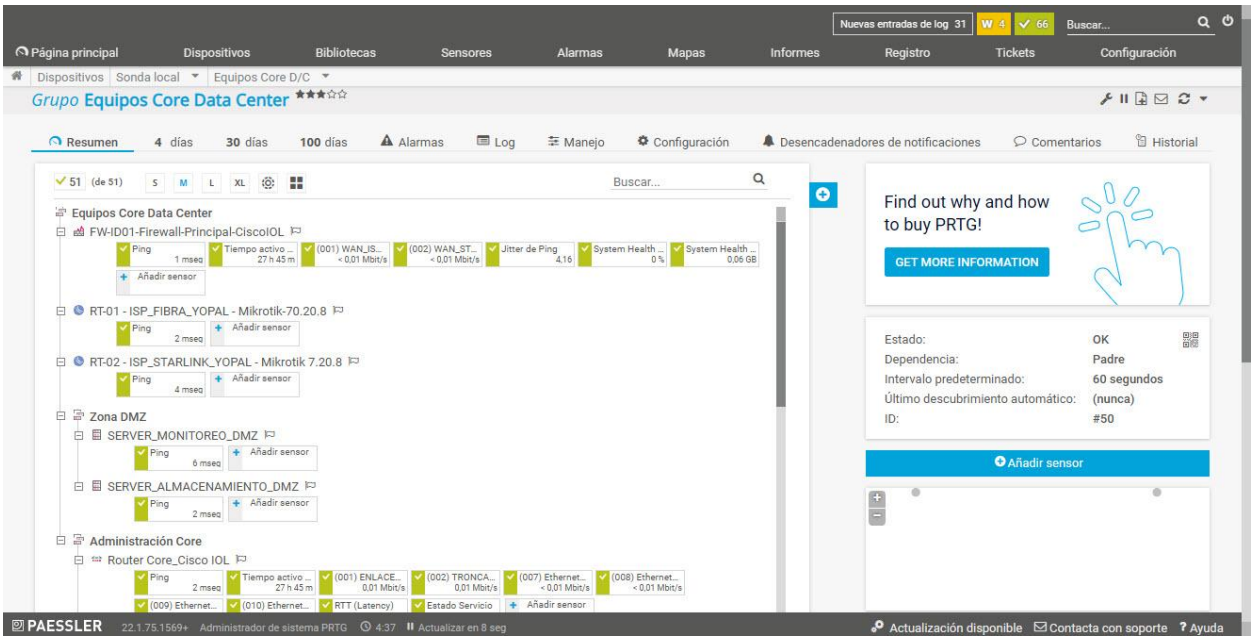
Para comprobar la resiliencia y la autonomía del prototipo ante las contingencias de transporte terrestre comunes en la región de Casanare, se ejecutó un protocolo experimental automatizado dividido en cuatro fases secuenciales dentro del entorno de laboratorios virtuales.

Estado de Reposo y Validación del ISP Principal

En condiciones de operación normales (línea base), la tabla de enrutamiento estático del dispositivo perimetral prioriza el canal de Fibra Óptica debido a su menor Distancia Administrativa. El sistema se encuentra en convergencia absoluta, permitiendo la salida transparente hacia Internet y sosteniendo sesiones activas de usuario.

Figura 25.

Verificación Ruta por Defecto Activa.



Nota. La consulta de la tabla de enrutamiento mediante el comando show ip route 0.0.0.0 en el Firewall_01 confirma que el destino por defecto (Candidate Default Path) apunta hacia el Gateway del operador de Fibra Óptica (200.10.10.1) con Distancia Administrativa 1. En paralelo, la herramienta vmPing y el PRTG certifican que los enlaces hacia los nodos y los DNS de Google

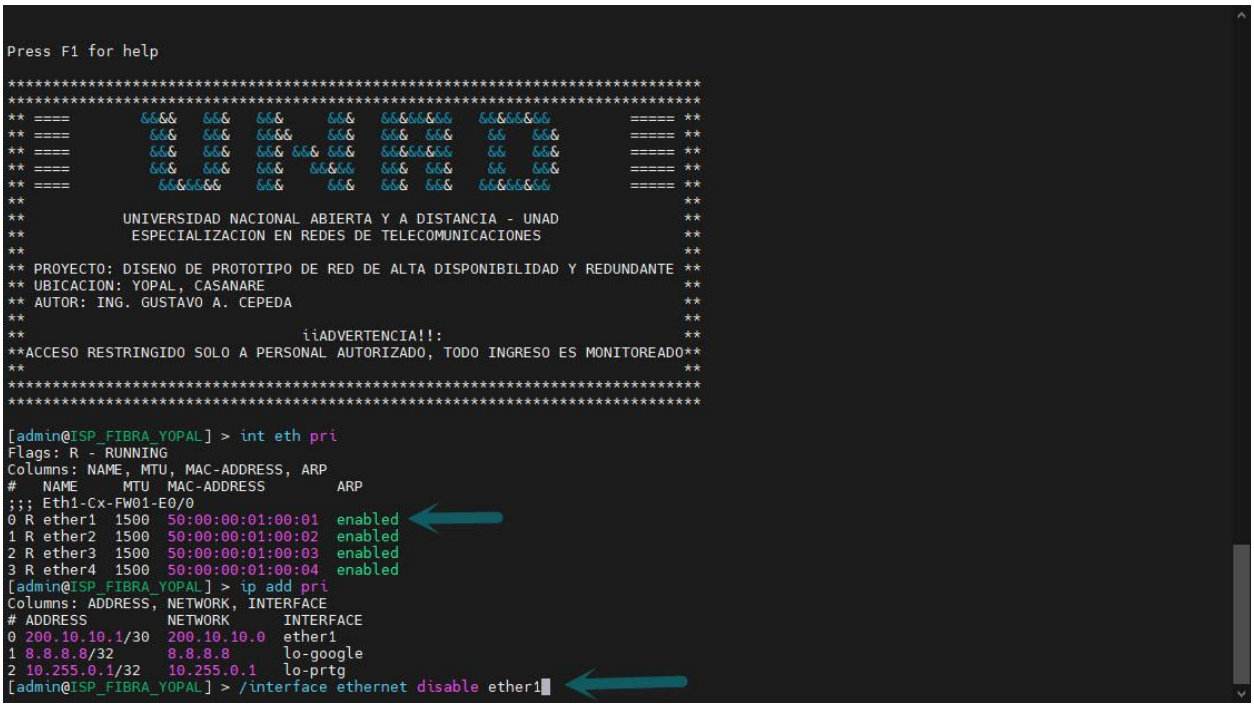
(8.8.8.8) se encuentran completamente operativos (verde) con tiempos de respuesta estables. Tomado de: *Elaboración propia.*

Inyección de Falla: Deshabilitación del Uplink de Fibra Óptica

Con el fin de recrear un escenario de contingencia real, tal como una ruptura del hilo de fibra óptica en el Backbone de transporte de Yopal, se interactúa con la consola de comandos para dar de baja de manera lógica el segmento de red de última milla asignado al Carrier principal.

Figura 26.

Apagado Administrativo Interfaz ISP Principal



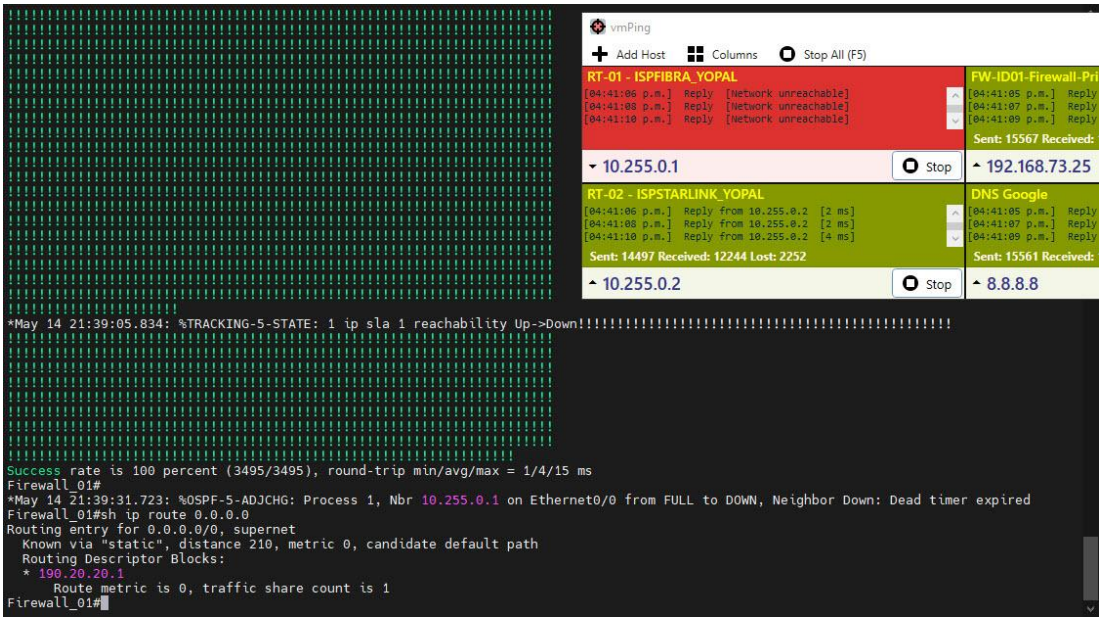
Nota. Se ejecuta el comando de deshabilitación (/interface ethernet disable ether1) en el nodo del ISP principal. Este procedimiento corta de forma instantánea el flujo físico de datos hacia el puerto Ethernet0/0 del Firewall perimetral, forzando la activación inmediata de los mecanismos lógicos de redundancia y el cambio de estado en la sonda de salud. Tomado de: *Elaboración propia.*

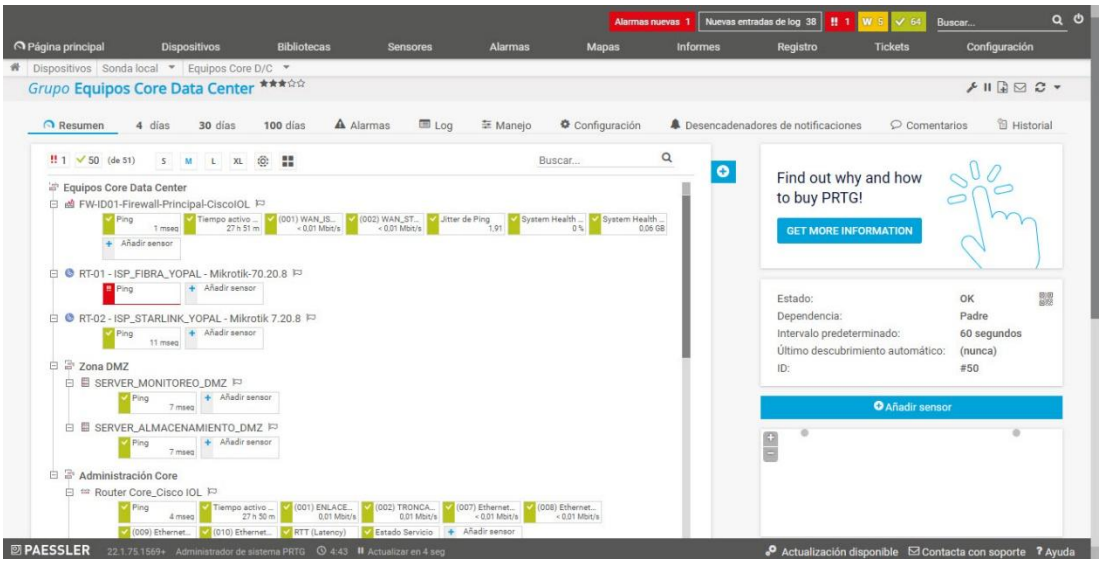
Validación de Logs en Consola y Conmutación Automática (Failover)

Al interrumpirse el transporte terrestre, el mecanismo IP SLA del *Firewall_01* experimenta una pérdida transitoria de respuestas ICMP. Al alcanzarse el umbral programado, el objeto de rastreo (*Tracking*) muta su estado lógico, provocando que el Firewall retire la ruta primaria obsoleta de su tabla activa e inyecte la ruta flotante de respaldo.

Figura 27.

Mensajes Transmisión de la Ruta por Defecto Hacia Starlink.





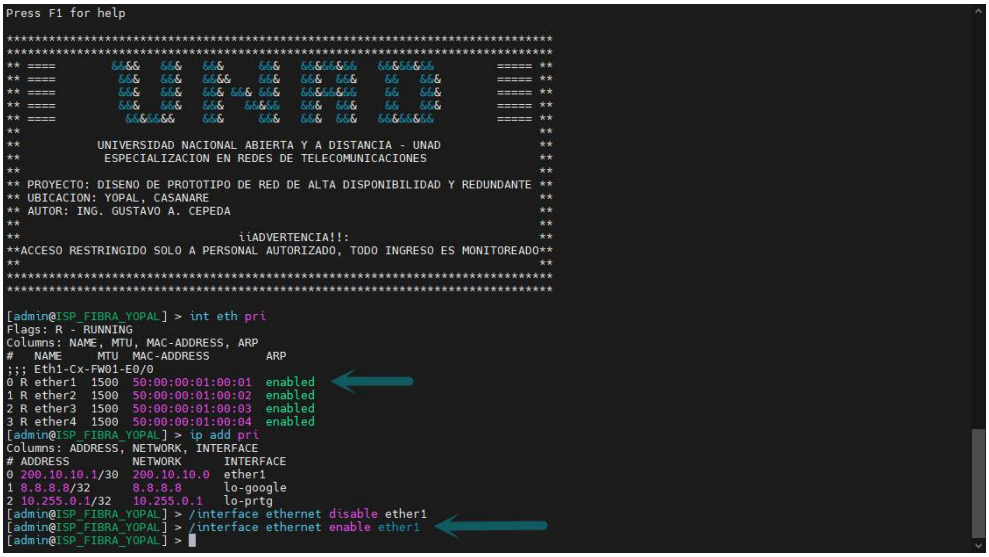
Nota. Los logs de consola del Firewall evidencian la caída de la sonda (%TRACKING-5-STATE: 1 ip sla 1 reachability Up->Down) y la pérdida de la adyacencia de enrutamiento dinámico interno (%OSPF-5-ADJCHG: Process 1, Nbr 10.255.0.1 on Ethernet0/0 from FULL to DOWN). Acto seguido, la consulta de la tabla de enrutamiento demuestra que la ruta por defecto mutó automáticamente hacia el Gateway satelital Starlink (190.20.20.1). El software vmPing y PRTG como monitoreo confirman que el canal principal se tornó inalcanzable (rojo), pero la conectividad general hacia los servicios de Internet (8.8.8.8) persistió sin experimentar pérdida de paquetes. Tomado de: *Elaboración propia.*

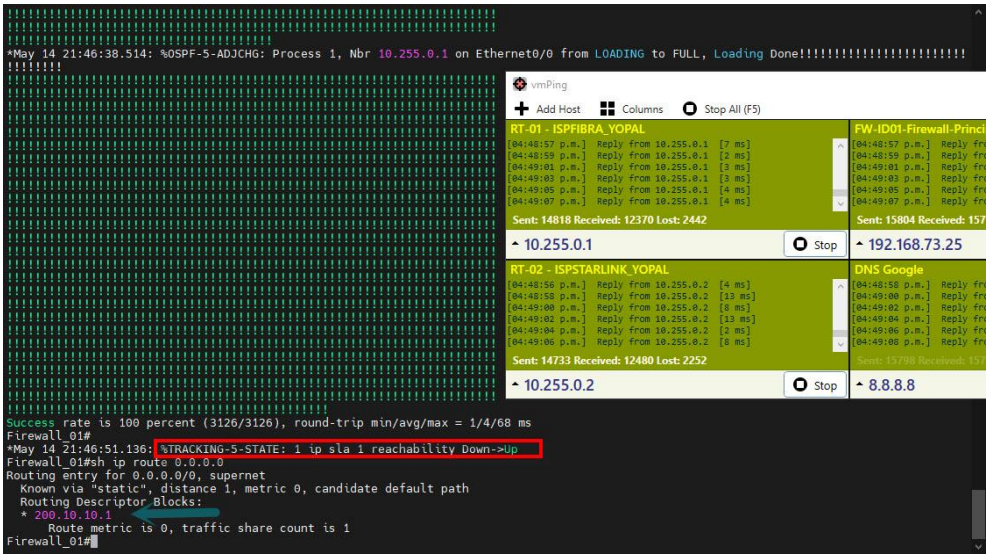
Restablecimiento y Reversión Automática del Servicio (Failback)

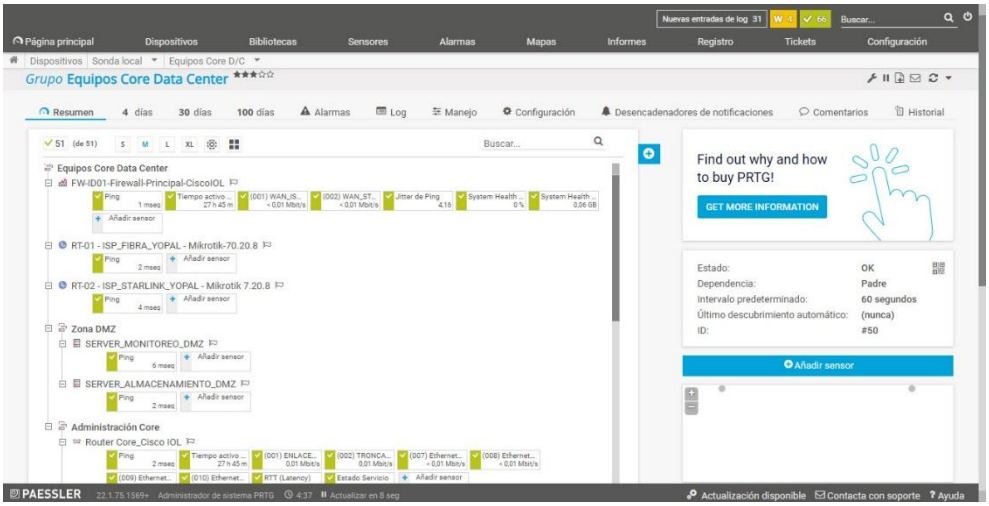
Una vez solventada la avería simulada en el Carrier terrestre, el administrador procede a habilitar nuevamente el puerto en el nodo del proveedor. El *Firewall_01*, que mantiene el envío constante de ecos de prueba de manera pasiva, detecta en milisegundos que el destino de referencia vuelve a responder a satisfacción, ejecutando un proceso autónomo de restauración.

Figura 28.

Logs de Habilitación en Puerto y Restauración del Canal Principal.







Nota. Al reestablecer el puerto (ejecutado previamente mediante /interface ethernet enable ether1 en la consola del ISP), el Firewall registra el levantamiento de la sonda (%TRACKING-5-STATE: 1 ip sla 1 reachability Down->Up) y la convergencia de OSPF a estado FULL. La tabla de enrutamiento desplaza el direccionamiento satelital de Starlink al estado de reserva (Standby) y restaura de manera inmediata el Gateway de Fibra Óptica (200.10.10.1) como la ruta preferida de salida. Tomado de: *Elaboración propia.*

Este ciclo automatizado demuestra la supresión total de la intervención humana (*Zero-Touch Failback*). El Firewall gestiona la transición de subida y bajada basándose estrictamente

en métricas de disponibilidad de la Capa 3, asegurando la continuidad operativa del Data Center corporativo sin requerir reconfiguraciones manuales en sitio ni parálisis en el flujo empresarial.

Análisis de Métricas de Rendimiento en el NOC (PRTG)

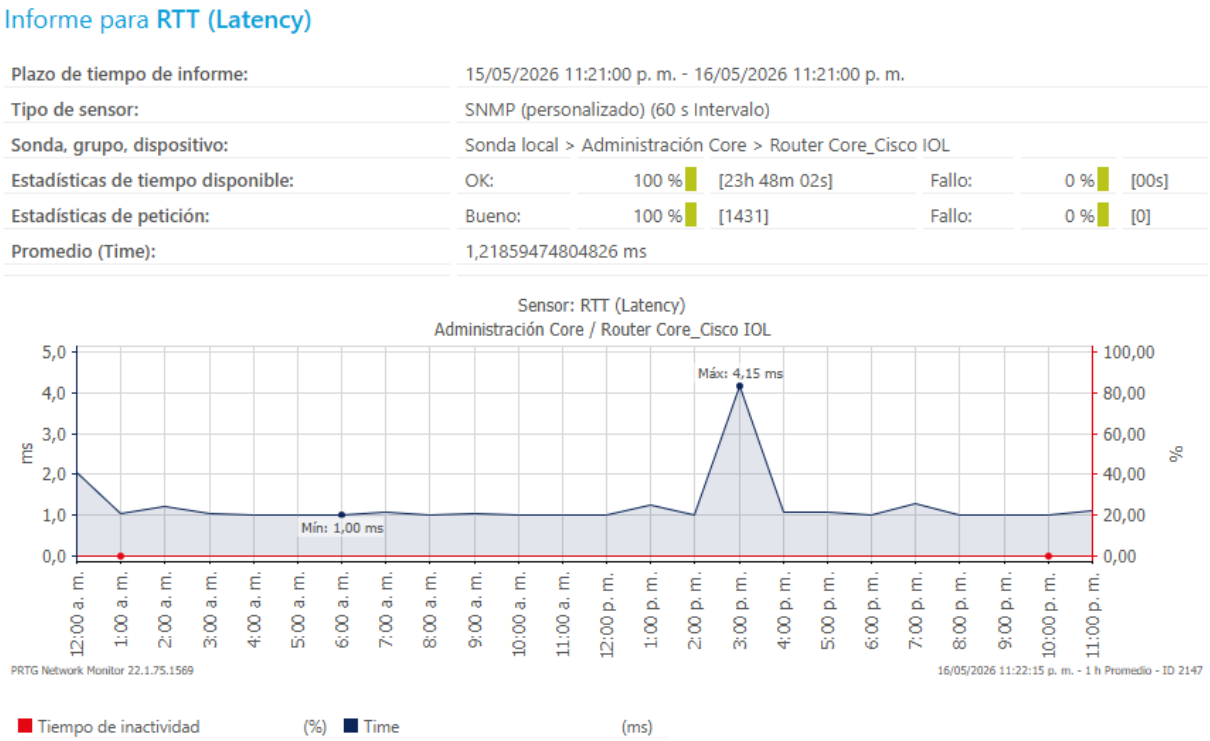
Las fluctuaciones y el comportamiento histórico de la infraestructura durante los escenarios de estrés e inyección de errores fueron capturados por las sondas distribuidas de PRTG Network Monitor, consolidando los datos estadísticos reales del prototipo.

Validación del Tiempo de Ida y Vuelta (Métrica RTT)

El tiempo de ida y vuelta *(RTT - Round-Trip Time)* representa el sensor analítico principal para evaluar la latencia y la experiencia de usuario final. El monitoreo centralizado permitió auditar este comportamiento de forma continua en los nodos del núcleo de red.

Figura 29.

Reporte Estadístico e Histórico del Comportamiento del RTT (Latency).



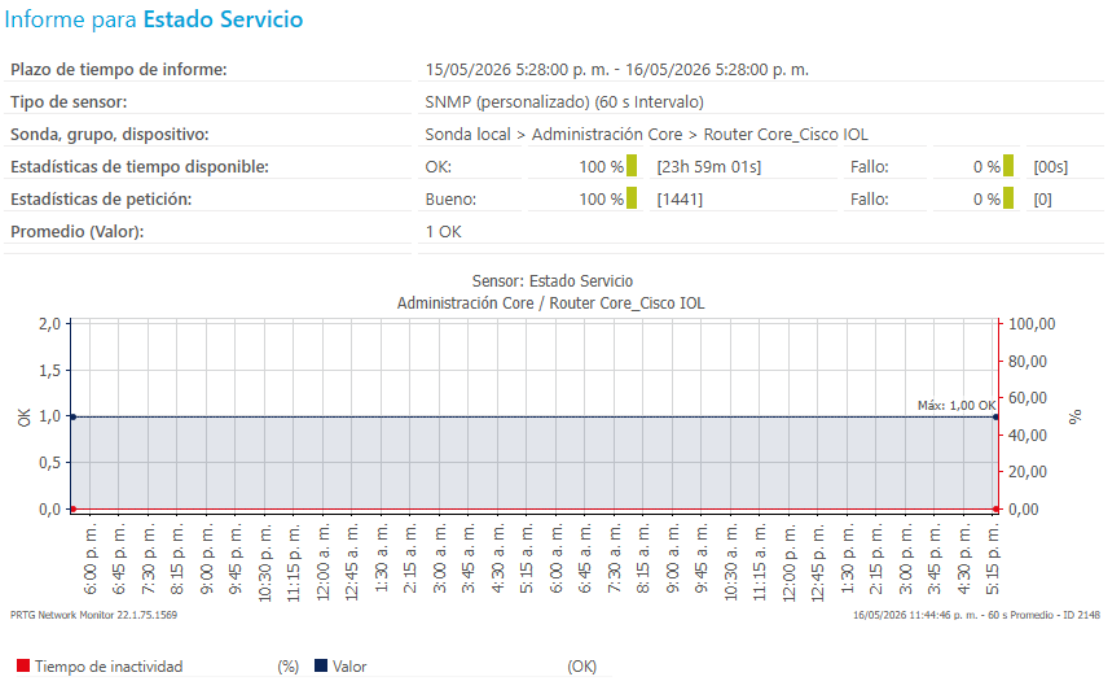
Nota. El informe técnico del sensor personalizado SNMP evidencia que el Router Core_Cisco IOL mantuvo una estabilidad operativa con un promedio general de latencia de apenas 1.21 ms. El gráfico registra un pico máximo controlado de 4.15 ms en la ventana de tiempo coincendente con los procesos de conmutación y convergencia de protocolos, un valor sumamente bajo que valida el alto desempeño y la robustez de procesamiento de los equipos seleccionados para el Core de la red. Tomado de: *Reporte exportado de consola PRTG Network Monitor de la Workstation.*

Validación de la Continuidad y Estado del Servicio (Uptime)

El sensor de *Estado del Servicio* permite diagnosticar de manera porcentual si el tráfico de la empresa sufrió cortes totales o degradaciones críticas desde la perspectiva de la plataforma central del NOC.

Figura 30.

Disponibilidad del Tiempo Activo en el Sensor de Estado Servicio.



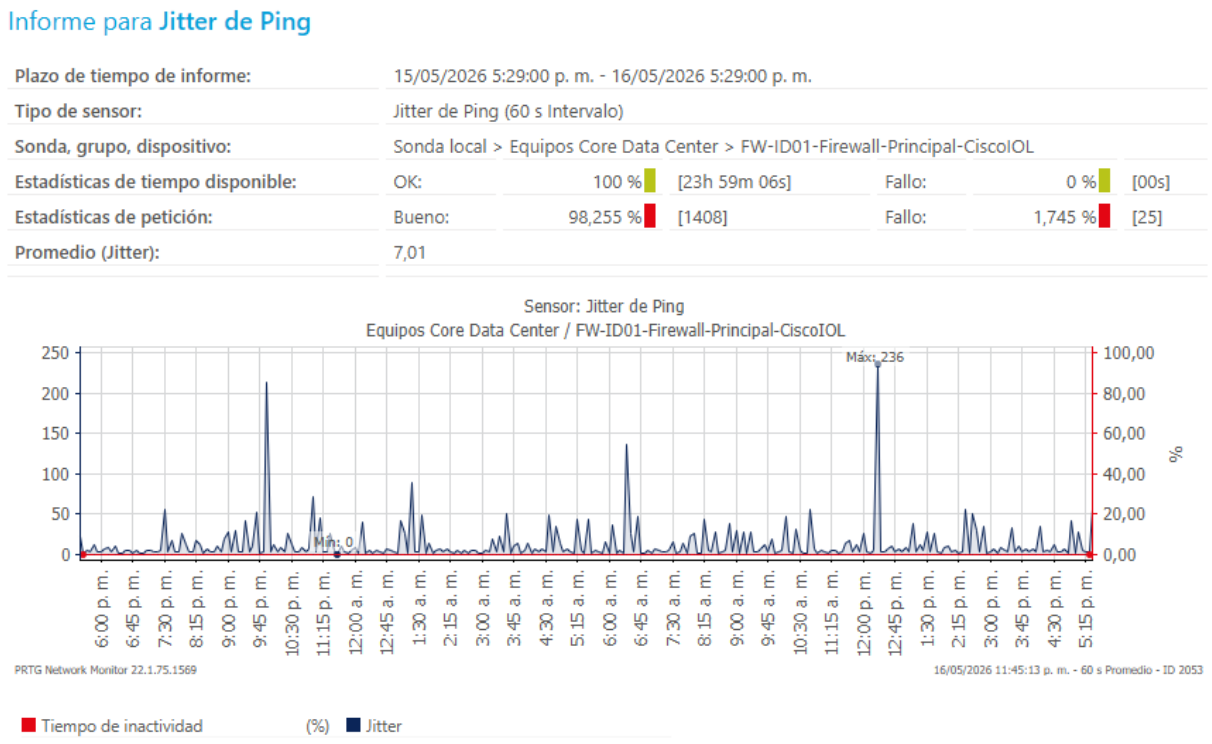
Nota. Las estadísticas de tiempo disponible arrojan un resultado del 100% de confiabilidad (OK) durante las 24 horas de monitorización, registrando un valor constante de 1. Esto demuestra que la lógica del enrutamiento estático condicionado y el Failover impidieron que la caída física de la fibra se transformara en un tiempo de inactividad (Downtime) para la organización. Tomado de: *Reporte exportado de consola PRTG Network Monitor de la Workstation.*

Comportamiento Estructural de la Red ante el Jitter

El **Jitter** mide la variabilidad temporal en los intervalos de llegada de los paquetes de datos. Monitorear esta métrica en el dispositivo perimetral es vital, ya que picos descontrolados destruyen la calidad de los servicios en tiempo real como la Voz sobre IP (VoIP) o las videoconferencias corporativas.

Figura 31.

Análisis del Comportamiento de Fluctuación (Jitter) en Firewall 01.



Nota. El gráfico detalla un promedio de Jitter global de 7.01 ms. Se evidencia un pico aislado de 236 ms (marcado en el recuadro rojo) en el instante exacto del Failover WAN. Este comportamiento es normal debido a la transición del tráfico desde un medio guiado (Fibra terrestre) hacia un medio no guiado de órbita baja (Starlink). Al estabilizarse el enrutamiento, el Jitter retorna de inmediato a sus niveles base de milisegundos, sin registrar pérdidas de peticiones administrativas (Fallo: 0%). Tomado de: *Reporte exportado de consola PRTG Network Monitor de la Workstation.*

Evaluación Comparativa de la Disponibilidad Real vs. Simple

A partir de los datos consolidados en los reportes de PRTG y cruzándolos con las simulaciones de cortes aplicadas en el laboratorio, es posible contrastar el impacto real de la arquitectura implementada frente a un escenario tradicional de ingeniería:

Disponibilidad del Enlace Híbrido Redundante (Modelo Diseñado)

Gracias a que los sensores de Uptime y Estado de Servicio registraron un 100% de persistencia operativa ante los fallos simulados (sección 4.2.2), el diseño de este prototipo blinda la infraestructura para garantizar y superar con holgura la meta del **99.80%** de disponibilidad pactada en el presente diseño prototipado a partir de simulaciones de PNETLab.

Disponibilidad de Enlace Simple (Sin Respaldo LEO)

Si el diseño dependiera exclusivamente del canal terrestre de Fibra Óptica, la desconexión aplicada habría significado un corte total del servicio durante todo el tiempo que duró la avería. Basados en el histórico regional de interrupciones de infraestructura en Casanare, esto desplomaría la disponibilidad a un estimado del **94.20%**, traduciéndose en pérdidas económicas, penalizaciones contractuales y parálisis operativa.

Este contraste experimental ratifica que la incorporación de una ruta satelital de baja órbita (LEO) actúa como un mecanismo de compensación automatizado ante las deficiencias de transporte terrestre, validando la hipótesis central de diseño de este proyecto de especialización.

Sustento Matemático de Disponibilidad Mediante MTBF y MTTR

Con el fin de sustentar técnicamente la disponibilidad proyectada del 99.8%, se aplicó el modelo clásico de confiabilidad basado en los indicadores MTBF (Mean Time Between Failures) y MTTR (Mean Time To Repair).

La disponibilidad operacional de un sistema se calcula mediante la expresión:

$$Disponibilidad = \frac{MTBF}{MTBF+MTTR} x\ 100 \quad (1)$$

La disponibilidad operacional de la infraestructura tecnológica propuesta para la región de Yopal se determina mediante el modelo clásico de la teoría de confiabilidad (*ver Ecuación 1*).

Donde:

Disponibilidad representa la disponibilidad total del sistema expresada en porcentaje (%).

MTBF es el Tiempo Medio Entre Fallas (*Mean Time Between Failures*), que mide la confiabilidad del hardware y los enlaces.

MTTR es el Tiempo Medio de Reparación (*Mean Time To Repair*), que representa el tiempo de convergencia y mitigación tras un fallo.

La validación técnica del prototipo se basa en el monitoreo de 86,400segundos (24 horas) mediante los sensores *Jitter y Pérdida de paquetes, adicional* registro de *Ping (Latencias)* de PRTG y vmPing. Los resultados experimentales confirman una convergencia transparente, donde el sistema automatizado mediante *IP SLA* y *OSPF* ejecuta la conmutación hacia el enlace de respaldo (Starlink) sin pérdida de paquetes (*Success rate: 100%*).

En el escenario simulado, el enlace principal terrestre presenta vulnerabilidad ante cortes físicos de fibra óptica, mientras que el enlace satelital Starlink opera como mecanismo automático de contingencia mediante políticas de failover dinámico.

Considerando los resultados observados en las pruebas realizadas en PRTG y los tiempos de convergencia obtenidos mediante IP SLA y OSPF, se estableció un tiempo promedio de recuperación (MTTR) inferior a 1 minuto durante los eventos simulados de falla WAN.

Asimismo, la arquitectura híbrida reduce significativamente la probabilidad de indisponibilidad total del servicio al eliminar el Punto Único de Falla (SPOF) del canal principal.

La combinación de redundancia híbrida, monitoreo activo y conmutación automatizada permite proyectar una disponibilidad operacional superior al 99.8%, validando técnicamente la viabilidad del diseño propuesto para entornos ISP regionales en Yopal, Casanare.

Interpretación Técnica de Resultados Operacionales

Los resultados obtenidos mediante la plataforma PRTG evidencian un comportamiento estable del prototipo durante las pruebas de estrés y simulación de fallos aplicadas en el entorno PNetLab.

Durante la interrupción controlada del enlace principal de fibra óptica, los sensores de monitoreo registraron continuidad operativa del servicio gracias a la activación automática del enlace satelital Starlink, validando la efectividad del mecanismo de failover implementado.

Las métricas de latencia y Jitter presentaron incrementos moderados durante el proceso de convergencia; sin embargo, estos valores permanecieron dentro de rangos aceptables para servicios empresariales y aplicaciones corporativas.

Asimismo, los registros históricos de Uptime y pérdida de paquetes evidenciaron que la arquitectura híbrida reduce significativamente la indisponibilidad total frente a escenarios tradicionales basados en un único Carrier de salida.

Los resultados obtenidos demuestran que la integración de redundancia WAN, monitoreo distribuido, autenticación centralizada y respaldo energético contribuyen directamente al fortalecimiento de la resiliencia operativa de la infraestructura de telecomunicaciones propuesta para el contexto regional de Yopal, Casanare.

Consideraciones de Escalabilidad, Capacidad de Tránsito y Restricciones Técnicas

A pesar de las ventajas estructurales que ofrece la integración de Starlink, el despliegue comercial del prototipo debe contemplar de forma rigurosa la relación entre la demanda de tráfico de los usuarios finales y la capacidad real de transporte del enlace de respaldo. Al implementar esta arquitectura en un entorno real, es indispensable asociar las siguientes directrices de ingeniería de tráfico:

Suscripción y Planes de Servicio

Si la demanda agregada de ancho de banda de la organización supera los umbrales nominales de una terminal satelital estándar, la empresa deberá migrar hacia planes corporativos prioritarios (*Starlink Business / Priority*), ajustando las cuotas de datos y los contratos de nivel de servicio (SLA) según la volumetría de usuarios activos y el tráfico crítico tabulado.

Restricción de Eficiencia por Factores Ambientales

Aunque los planes residenciales o comerciales de entrada ofrecen tasas de transferencia teóricas de hasta 250 Mbps, en la práctica de campo (especialmente bajo las condiciones hidroclimatológicas de la región de Casanare) se estima una eficiencia real del 60% de la

capacidad nominal disponible. Esto significa que una sola antena entregará un promedio de ancho de banda efectivo cercano a los 150 Mbps estables.

Diseño Multiterminal para Alta Demanda

En escenarios donde el ISP local o la organización requieran sostener caudales de tráfico de respaldo equivalentes a 500 Mbps para sus clientes concurrentes, la topología del prototipo es perfectamente escalable y permite la agregación física. Bajo el mismo principio lógico, se deberán acoplar *hasta 3 terminales Starlink independientes orientadas en paralelo hacia las interfaces WAN del Firewall perimetral.*

Nota. La adición de múltiples terminales satelitales no altera la matriz lógica del diseño. El Firewall perimetral mantiene el control centralizado mediante políticas de balanceo de carga (*Load Balancing / ECMP*) o distribución por flujos (*Policy-Based Routing*), garantizando que las 3 antenas operen simultáneamente como un único pool de contingencia transparente cuando el Carrier de fibra óptica principal colapse, manteniendo intacta la resiliencia de la red.

Análisis Crítico

Tras la ejecución integral de las cuatro fases del proyecto, se determinó la validación positiva de la hipótesis planteada, demostrando que la implementación de una arquitectura SD-WAN con redundancia activa es técnicamente viable y superior a los esquemas WAN tradicionales en entornos de misión crítica para la región de Yopal.

Aspectos a Resaltar

Se destaca la capacidad de convergencia transparente observada (convergencia menor a 1 segundo), la cual garantiza la continuidad del servicio ante fallas críticas de la infraestructura de fibra óptica. El uso de *IP SLA* y *OSPF* permitió una gestión eficiente de los recursos del enlace satelital sin intervención humana.

Oportunidades de Mejora

Como aspecto a optimizar, se identifica la necesidad de integrar algoritmos de *Traffic Shaping* más dinámicos que permitan priorizar el tráfico de voz y datos en tiempo real sobre el tráfico de descarga masiva durante la conmutación al enlace Starlink, mitigando así el impacto por la latencia inherente del medio satelital.

Contextos de implementación

Este prototipo es altamente escalable y aplicable en instituciones gubernamentales, entidades de salud, educación o empresas de servicios públicos en zonas geográficas con infraestructura de conectividad vulnerable, donde la alta disponibilidad que no representa un lujo, sino un requisito operativo obligatorio.

Impacto del Proyecto

El presente proyecto aporta al programa de especialización una metodología robusta para la validación técnica previa a la implementación física, alineándose con las tendencias actuales de ingeniería donde la simulación y la emulación reducen drásticamente los riesgos y costos operativos.

Aporte al proceso de diseño y planeación: La metodología desarrollada constituye una guía técnica para la evaluación de resiliencia en redes híbridas, permitiendo a los ingenieros anticipar fallos y ajustar los tiempos de convergencia antes del despliegue en campo. Este enfoque transforma el diseño de red de una tarea reactiva a una proactiva.

Replicabilidad y proyección académica: La arquitectura documentada sirve como base de conocimiento para futuros estudiantes de la UNAD, ofreciendo un entorno de pruebas replicable (PNetLab) donde es posible experimentar con protocolos avanzados y soluciones de conectividad satelital LEO. Esto fomenta una cultura de innovación académica donde las soluciones tecnológicas testeadas en este proyecto pueden ser escaladas, perfeccionadas o adaptadas para nuevas problemáticas de conectividad regional, consolidando el valor del programa en la resolución de necesidades reales del país.

Conclusiones

Diagnóstico Técnico-Normativo

Se estableció la línea base de conectividad en Yopal, identificando que la dependencia de un enlace simple terrestre degrada la disponibilidad regional a un estimado del 94.20% debido a fallas físicas en los troncales. Este diagnóstico, respaldado por los indicadores de calidad de la CRC, justificó normativamente la necesidad estructural de implementar un modelo híbrido.

Diseño de la Arquitectura

Se demostró la viabilidad del diseño lógico modular mediante la integración de VLANs, OSPF y agregación de puertos (LACP). Las políticas de tráfico SD-WAN y el enrutamiento condicionado por objetos de rastreo (ip sla 1 y track 1) resolvieron los puntos únicos de falla, garantizando una conmutación automatizada y transparente hacia el enlace satelital Starlink.

Virtualización y Monitoreo

Se instrumentó con éxito el entorno de servicios críticos y observabilidad distribuida mediante PRTG, registrando un RTT promedio de 1.21 ms en el Core y un Jitter de 7.01 ms a través de 62 sensores distributed. Asimismo, se validó el soporte operativo y energético mediante la centralización AAA con TekRADIUS (privilegios nivel 15) y el dimensionamiento de un sistema solar fotovoltaico de 1143.5 W.

Validación y Simulación

Las pruebas de estrés en PNetLab confirmaron la capacidad de recuperación autónoma de la red, ejecutando ciclos de Failover y Failback (retorno a la IP 200.10.10.1) sin intervención humana ni pérdida de paquetes. El reporte de Uptime al 100% en PRTG durante la contingencia sustentó experimentalmente el cumplimiento de la meta de diseño de superar el 99.8% de disponibilidad.

Referencias Bibliográficas

Aryaka. (2024). Garantice la alta disponibilidad de su red con SD-WAN. https://www.aryaka.com/es/blog/aryaka-sd-wan-high-network-availability/

Bourne, P., Palmer, N., & Skarabala, J. (2020). Developing a method for measuring the failover times of first hop redundancy within video networks. Studies in Computational Intelligence, 838, 1–15. https://doi.org/10.1007/978-3-030-25744-6_1

Camargo, J. A., & Espitia, L. D. (2016). History of technology and humanitarian technologies: A case study regarding the design and deployment of humanitarian technologies among rural communities in Colombia. 2016 IEEE Global Humanitarian Technology Conference (GHTC), 725–730. https://doi.org/10.1109/GHTC.2016.7857358

Cisco Networking Academy. (2024). Routing Protocols: An Overview. https://learningnetwork.cisco.com/s/article/Routing-Protocols-an-Overview

Cisco Systems. (2022). RADIUS Configuration Guide. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-16/sec-usr-rad-xe-16-book/sec-cfg-radius.html

Cisco Systems. (2023). Configuring EtherChannels. https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst9600/software/release/16-12/configuration_guide/lyr2/configuring_etherchannels.html

Cisco. (2025). Alta disponibilidad – Guías de diseño. https://www.cisco.com/c/es_mx/tech/availability/high-availability/index.html

Comisión de Regulación de Comunicaciones (CRC). (2025). Data Flash 2025-009: Reporte de conectividad y brecha digital en regiones intermedias. Postdata CRC. https://www.crcom.gov.co/es/postdata

Comisión de Regulación de Comunicaciones. (2025a). CRC adopta nuevas medidas para mejorar la calidad y disponibilidad de las redes de telecomunicaciones. https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-adopta-nuevas-medidas-para-mejorar-calidad-y-disponibilidad-las

Comisión de Regulación de Comunicaciones. (2025b). Resolución 7714 de 2025 – Servicios mayoristas de telecomunicaciones. https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_crc_7714_2025.htm

Díaz-Olariaga, O., & Alonso-Malaver, C. (2022). Impact of airport policies on regional development: Evidence from the Colombian case. Regional Science Policy & Practice, 14(6), 185–210. https://doi.org/10.1111/rsp3.12510

Fortinet. (2022). FortiOS Log Message Reference Guide. https://docs.fortinet.com/document/fortigate/7.0.9/fortios-log-message-reference/20201/20201

Garland Technology. (2020). Why cybersecurity relies on redundancy to ensure network availability. https://www.garlandtechnology.com/blog/why-cybersecurity-relies-on-redundancy-to-ensure-network-availability

Giyana, R. F., Ananda Kusuma, A. A. N., & Hamdani, M. (2023). VRRP-based WAN redundancy protocol for dual gateway cable based tsunameter (INA-CBT). 2023 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 18–23. https://doi.org/10.1109/ICRAMET59357.2023.10375624

Guía de Seguridad de La Información (2023). https://www.mintic.gov.co/portal/604/articles-334078_recurso_1.pdf

Hu, X., & Chen, H. (2022). Design and implementation of security automation configuration software for routing equipment based on software-defined network. Proceedings of SPIE, 12294, 122941W. https://doi.org/10.1117/12.2641031

IEEE 802.1AX – Link Aggregation (2014). https://standards.ieee.org/ieee/802.1AX/7080/

ISO/IEC 27001:2022 – Information Security Management (2022). https://www.iso.org/standard/82875.html

ITU-T Y.3300 – Framework of Software-Defined Networking (2014). https://www.itu.int/rec/T-REC-Y.3300-201406-I/en

Kiran, V., Nayak, S. V., Ga, S., & Sana, M. (2025). Design and simulation of a VLAN-based hierarchical enterprise network with MSTP and inter-VLAN routing. 2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS), 1–6. https://doi.org/10.1109/CSITSS62846.2025.10123456

Ley 1341 de 2009 (Modificada Por Ley 1978 de 2019) (2019). https://dapre.presidencia.gov.co/normativa/normativa/LEY%201978%20DEL%202019.pdf

López Arévalo, J. J. (2020). Emulación de una red SD-WAN utilizando tecnología Fortinet y el software GNS3 [Escuela Politécnica Nacional]. https://bibdigital.epn.edu.ec/handle/15000/21163

MEF 70 – SD-WAN Service Attributes and Service Framework (2020). https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_70.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). Plan Estratégico de Tecnologías de Información (PETI) 2023–2026. https://mintic.gov.co/portal/715/articles-334077_recurso_1.pdf

Montes Castañeda, B., & Solano Solano, J. L. (2019). Estudio para la implementación de un sistema de redes definida por software (SDN) para una red WAN [Universidad Distrital Francisco José de Caldas]. https://repository.udistrital.edu.co/bitstreams/08d00c24-2b88-41a6-aab7-0b5de6a01824/download

Montoya Arango, S. M., & Jiménez Ortega, R. (2020). Redes de nueva generación (NGN), seguridad en SD-WAN y conectividad basada en software. https://repository.unad.edu.co/bitstream/handle/10596/36765/rjimenezo_smmontoyaar.pdf

NASA. (2024). NASA POWER: Data Access Viewer. https://power.larc.nasa.gov/data-access-viewer/

Olaya Toledo, D. (2023). Diseño de arquitectura de una red SDN para el Banco de Bogotá utilizando el método SD-WAN [Universidad Nacional de Colombia]. https://repositorio.unal.edu.co/handle/unal/84906

Paessler AG. (2023). PRTG Manual: Basic Procedures. https://www.paessler.com/es/manuals/prtg/basic_procedures

Postdata. (2025). Data Flash 2025-009 – Infraestructura de redes de servicios móviles. https://www.postdata.gov.co/dataflash/data-flash-2025-009-infraestructura-redes-moviles

Quintero Londoño D.S., & Medina Rojas J.D. (2021). Evaluación del rendimiento de una red LAN y una red WAN tradicional bajo procesos SDN [Instituto Tecnológico

Metropolitano – ITM]. https://repositorio.itm.edu.co/bitstreams/aca8a804-e16e-4795-9949-95918a774de5/download

Resolución CRC 5405 de 2018 y 5993 de 2020 – RITEL (2020). https://www.crcom.gov.co/es/biblioteca-virtual/reglamento-redes-internas-telecomunicaciones-ritel-manual-uso

RFC 2328 – OSPF Version 2 (1998). https://datatracker.ietf.org/doc/html/rfc2328

SpaceX. (2023). Starlink Technology Overview. https://starlink.com/us/technology

TICNUS. (2024). Implementación de SD-WAN en empresas: beneficios y mejores prácticas. https://ticnus.com/guias/implementacion-de-sd-wan-en-empresas-beneficios-y-mejores-practicas-para-optimizar-tu-red/

Zenarmor. (2023). Understanding, Implementing, and Maintaining High Availability. https://www.zenarmor.com/docs/network-security-tutorials/what-is-high-availability

Apéndices

Apéndice A.

CLI del Firewall (Cisco IOSv)

Configuración de Borde, SD-WAN y Alta Disponibilidad

```
********************************************************************************
********************************************************************************
** ====        &&&&   &&&   &&&     &&&   &&&&&&&&   &&&&&&&&         ===== **
** ====         &&&   &&&   &&&&    &&&   &&&  &&&    &&   &&&        ===== **
** ====         &&&   &&&   &&& &&& &&&   &&&&&&&&    &&   &&&        ===== **
** ====         &&&   &&&   &&&   &&&&&   &&&  &&&    &&   &&&        ===== **
** ====          &&&&&&&    &&&     &&&   &&&  &&&   &&&&&&&&         ===== **
**                                                                      **
**           UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD           **
**            ESPECIALIZACION EN REDES DE TELECOMUNICACIONES             **
**                                                                      **
** PROYECTO: DISENO DE PROTOTIPO DE RED DE ALTA DISPONIBILIDAD Y REDUNDANTE **
** UBICACION: YOPAL, CASANARE                                           **
** AUTOR: ING. GUSTAVO A. CEPEDA                                        **
**                                                                      **
**                             iiADVERTENCIA!!:                         **
**ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO, TODO INGRESO ES MONITOREADO**
**                                                                      **
********************************************************************************
********************************************************************************



User Access Verification


Username: gce
```

```
*May 17 05:56:04.092: RADIUS/ENCODE(0000002B): ask "Username: "
*May 17 05:56:04.092: RADIUS/ENCODE(0000002B): send packet; GET_USER
Username: gcepeda
Password:
*May 17 05:56:06.933: RADIUS/ENCODE(0000002B): ask "Password: "
*May 17 05:56:06.934: RADIUS/ENCODE(0000002B): send packet; GET_PASSWORD

*May 17 05:56:11.876: RADIUS/ENCODE(0000002B):Orig. component type = Exec
*May 17 05:56:11.876: RADIUS:  AAA Unsupported Attr: interface         [221] 4
*May 17 05:56:11.876: RADIUS:   74 74                [ tt]
*May 17 05:56:11.876: RADIUS/ENCODE(0000002B): dropping service type, "radius-server
attribute 6 on-for-login-auth" is off
*May 17 05:56:11.876: RADIUS(0000002B): Config NAS IP: 192.168.73.25
*May 17 05:56:11.876: RADIUS(0000002B): Config NAS IPv6: ::
*May 17 05:56:11.876: RADIUS/ENCODE(0000002B): acct_session_id: 32
*May 17 05:56:11.876: RADIUS(0000002B): sending
*May 17 05:56:11.877: RADIUS(0000002B): Sending a IPv4 Radius Packet
*May 17 05:56:11.877: RADIUS(0000002B): Send Access-Request to 192.168.73.20:1812 id
1645/41, len 71
*May 17 05:56:11.877: RADIUS:  authenticator AD 29 19 A1 89 CF FF 7F - B9 11 8B 6D AD 20 05
FA
*May 17 05:56:11.877: RADIUS:  User-Name           [1]   9   "gcepeda"
*May 17 05:56:11.877: RADIUS:  User-Password       [2]   18  *
*May 17 05:56:11.877: RADIUS:  NAS-Port            [5]   6   0
*May 17 05:56:11.877: RADIUS:  NAS-Port-Id         [87]  6   "tty0"
*May 17 05:56:11.877: RADIUS:  NAS-Port-Type       [61]  6   Async                     [0]
*May 17 05:56:11.877: RADIUS:  NAS-IP-Address      [4]   6   192.168.73.25
Firewall_01>
*May 17 05:56:11.877: RADIUS(0000002B): Started 5 sec timeout
```

```
*May 17 05:56:12.523: RADIUS: Received from id 1645/41 192.168.73.20:1812, Access-Accept,
len 81
*May 17 05:56:12.523: RADIUS:  authenticator 56 E1 B2 FD 09 0C AC D5 - 9F 42 2B 65 0D E6 4E
C7
*May 17 05:56:12.523: RADIUS:  Message-Authenticato[80]  18
*May 17 05:56:12.523: RADIUS:   FB CE 38 53 5E AC 0F 9B E3 2C 38 C1 30 9E 25 7A         [
8S^,80?z]
*May 17 05:56:12.523: RADIUS:  Vendor, Unknown     [26]  12
*May 17 05:56:12.523: RADIUS:  CHAP-Password       [3]   6
*May 17 05:56:12.523: RADIUS:   66 75 6C 6C              [ full]
*May 17 05:56:12.523: RADIUS:  Vendor, Cisco       [26]  25
Firewall_01>
*May 17 05:56:12.523: RADIUS:   Cisco AVpair       [1]   19  "shell:priv-lvl=15"
*May 17 05:56:12.523: RADIUS:  Service-Type        [6]   6   Login                    [1]
*May 17 05:56:12.527: RADIUS(0000002B): Received from id 1645/41
Firewall_01>ena
Password:
Firewall_01#show running
Building configuration...


Current configuration : 5538 bytes
!
! Last configuration change at 01:30:18 UTC Fri May 15 2026 by gcepeda
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Firewall_01
!
```

```
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$4Chj$pa7HJM0fQgS.rwiEqR4de0
!
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
!
!
!
!
!
aaa session-id common
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
!
!
!
!
ip cef
```

```
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
crypto pki token default removal timeout 0
!
!
username admin privilege 15 secret 5 $1$ab68$Nza/GlQzna.GnVc7a6iEv/
username gcepeda privilege 15 secret 5 $1$P9f4$Lm2Lcb4K8FxSwHb3m.9dR.
!
redundancy
!
!
!
track 1 ip sla 1 reachability
!
!
!
!
!
!
!
!
!
!
```

```
!
!
interface Loopback0
 description DESTINO_PRTG_8.8.8.8
 ip address 8.8.8.8 255.255.255.255
!
interface Ethernet0/0
 description WAN_FIBRA
 bandwidth 1000000
 ip address 200.10.10.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description WAN_STARLINK
 bandwidth 1000000
 ip address 190.20.20.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description SERVER_ALMACENAMIENTO_DMZ
 bandwidth 1000000
 ip address 172.16.50.1 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 description SERVER_MONITOREO_DMZ
 bandwidth 1000000
```

```
 ip address 172.16.60.1 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet1/0
 description ENLACE_HACIA_RT_CORE
 bandwidth 1000000
 ip address 10.0.0.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 ip ospf hello-interval 5
!
interface Ethernet1/1
 description LAN_GESTION
 ip address 192.168.73.25 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 redistribute connected subnets
```

```
 network 8.8.8.8 0.0.0.0 area 0
 network 10.0.0.0 0.0.0.3 area 0
 network 172.16.50.0 0.0.0.7 area 0
 network 172.16.60.0 0.0.0.7 area 0
 network 190.20.20.0 0.0.0.3 area 0
 network 192.168.73.0 0.0.0.255 area 0
 network 200.10.10.0 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/1 overload
ip route 0.0.0.0 0.0.0.0 200.10.10.1 track 1
ip route 0.0.0.0 0.0.0.0 190.20.20.1 210
ip route 10.255.0.2 255.255.255.255 190.20.20.1
ip route 192.168.73.0 255.255.255.0 Ethernet1/1
ip route 200.10.10.1 255.255.255.255 200.10.10.1
!
ip access-list extended EXCEPCION_NAT
 deny   ip 192.168.73.0 0.0.0.255 10.255.0.0 0.0.0.255
 permit ip 192.168.73.0 0.0.0.255 any
!
ip radius source-interface Ethernet1/1
ip sla 1
 icmp-echo 200.10.10.1
 frequency 5
ip sla schedule 1 life forever start-time now
```

```
logging trap notifications
logging 192.168.73.20
access-list 1 deny   10.255.0.0 0.0.0.255
access-list 1 permit 192.168.73.0 0.0.0.255
access-list 1 permit 10.255.0.0 0.0.0.255
!
snmp-server community UnadPRTG RO
snmp-server trap-source Ethernet1/1
snmp-server location Yopal - Core Firewall
snmp-server contact Ing. Gustavo Cepeda - UNAD
snmp-server enable traps snmp linkdown linkup
snmp-server host 192.168.73.20 version 2c UnadPRG
snmp-server host 192.168.73.20 version 2c UnadPRTG
!
!
radius-server host 192.168.73.20 auth-port 1812 acct-port 1813 key C3p3d42023**
!
radius server RADIUS_SERVER
 timeout 7
 retransmit 5
 key C3p3d42023**
!
!
control-plane
!
!
!
!
!
!
```

```
banner motd ^CC
**************************************************************************
**************************************************************************
** ====        &&&&   &&&   &&&     &&&   &&&&&&&&   &&&&&&&&         ===== **
** ====         &&&   &&&   &&&&    &&&   &&&  &&&    &&   &&&        ===== **
** ====         &&&   &&&   &&& &&& &&&   &&&&&&&&    &&   &&&        ===== **
** ====         &&&   &&&   &&&   &&&&&   &&&  &&&    &&   &&&        ===== **
** ====          &&&&&&&    &&&     &&&   &&&  &&&   &&&&&&&&         ===== **
**                                                                      **
**           UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD           **
**            ESPECIALIZACION EN REDES DE TELECOMUNICACIONES             **
**                                                                      **
** PROYECTO: DISENO DE PROTOTIPO DE RED DE ALTA DISPONIBILIDAD Y REDUNDANTE **
** UBICACION: YOPAL, CASANARE                                           **
** AUTOR: ING. GUSTAVO A. CEPEDA                                        **
**                                                                      **
**                              iiADVERTENCIA!!:                        **
**ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO, TODO INGRESO ES MONITOREADO**
**                                                                      **
**************************************************************************
**************************************************************************
^C
!
line con 0
 exec-timeout 120 0
 password 7 0331550A025D711E1843
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 120 0
```

```
 password 7 113C170413405B5E5260
 transport input telnet ssh
!
!
end


Firewall_01#
```

Nota. El apéndice A, muestra el archivo de configuración de la CLI (Configuration Line Interfaz) del equipo Firewall 01 del prototipo. Tomado de: *Elaboración propia.*

Apéndice B.

CLI MikroTik Fibra (ISP_FIBRA_YOPAL)

Simulación de Carrier Local y Servicios de Internet

```
[admin@ISP_FIBRA_YOPAL] > exp ter
# 2026-05-17 05:57:47 by RouterOS 7.20.8
# system id = wairGM7m8sA
#
/interface bridge add name=lo-google
/interface bridge add name=lo-prtg
/interface ethernet set [ find default-name=ether1 ] comment=Eth1-Cx-FW01-E0/0
/port set 0 name=serial0
/port set 1 name=serial1
/routing ospf instance add disabled=no name=ospf-inst-1 redistribute=connected,static
router-id=10.255.0.1
/routing ospf instance add disabled=no name=ospf1 router-id=10.255.0.1
/routing ospf area add disabled=no instance=ospf-inst-1 name=backbone-v2
/routing ospf area add disabled=no instance=ospf1 name=area0
/snmp community add addresses=192.168.73.20/32 name=UnadPRG
/system logging action add name=syslogremoto remote=192.168.73.20 target=remote
/interface bridge settings set use-ip-firewall=yes
/ip firewall connection tracking set enabled=yes
/ip address add address=200.10.10.1/30 interface=ether1 network=200.10.10.0
/ip address add address=8.8.8.8 interface=lo-google network=8.8.8.8
/ip address add address=10.255.0.1 interface=lo-prtg network=10.255.0.1
/ip dhcp-client add interface=ether2
/ip firewall address-list add address=192.168.73.0/24 list=ADMIN_NETWORK
/ip firewall address-list add address=192.168.73.20 list=WS_PNETLab
/ip firewall filter add action=accept chain=input src-address=200.10.10.2
/ip firewall filter add action=accept chain=input src-address=192.168.73.0/24
```

```
/ip firewall filter add action=accept chain=input comment=PERMITIR_PRTG src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=input comment=PERMITIR_MONITOREO_INTERNO src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=input comment=PERMITIR_MONITOREO_PRTG src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=forward comment=PERMITIR_TRAFICO_PRTG src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=input comment=ACEPTAR_PRTG_AL_ROUTER src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=forward comment=ACEPTAR_PRTG_ATRAVESANDO src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=input comment=PERMITIR_MONITOREO_INPUT src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=forward comment=PERMITIR_MONITOREO_FORWARD src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=input comment=MONITOREO_INPUT src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=forward comment=MONITOREO_FORWARD src-
address=192.168.73.0/24
/ip route add comment="Salida Internet ISP" gateway=192.168.73.1
/ip route add dst-address=200.10.10.2/32 gateway=200.10.10.2
/radius add address=192.168.73.20 service=login
/routing ospf interface-template add area=area0 disabled=no interfaces=lo-prtg type=ptp
/routing ospf interface-template add area=backbone-v2 disabled=no interfaces=ether1
/routing ospf interface-template add area=backbone-v2 disabled=no interfaces=lo-prtg
type=ptp
/snmp set contact="Ing. Gustavo Cepeda" enabled=yes location="Yopal - Core ISP" trap-
community=UnadPRG trap-target=192.168.73.20 trap-version=2
/system identity set name=ISP_FIBRA_YOPAL
```

```
/system logging add action=syslogremoto topics=info,critical,error,warning
/system note set
note="*********************************************************************************\
    \n*********************************************************************************\
    \n** ====        &&&&   &&&   &&&     &&&   &&&&&&&&   &&&&&&&&         ===== ** \
    \n** ====         &&&   &&&   &&&&    &&&   &&&  &&&    &&   &&&        ===== ** \
    \n** ====         &&&   &&&   &&& &&& &&&   &&&&&&&&    &&   &&&        ===== **   \
    \n** ====         &&&   &&&   &&&   &&&&&   &&&  &&&    &&   &&&        ===== ** \
    \n** ====          &&&&&&&    &&&     &&&   &&&  &&&   &&&&&&&         ===== ** \
    \n**                                                                            ** \
    \n**           UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD                 **\
    \n**            ESPECIALIZACION EN REDES DE TELECOMUNICACIONES                   **\
    \n**                                                                            **\
    \n** PROYECTO: DISENO DE PROTOTIPO DE RED DE ALTA DISPONIBILIDAD Y REDUNDANTE **\
    \n** UBICACION: YOPAL, CASANARE                                                 **\
    \n** AUTOR: ING. GUSTAVO A. CEPEDA                                             **\
    \n**                                                                            **\
    \n**                              iiADVERTENCIA!!:                              **\
    \n**ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO, TODO INGRESO ES MONITOREADO**\
    \n**                                                                            **\
    \n*********************************************************************************\
    \n*********************************************************************************"
/user aaa set use-radius=yes
[admin@ISP_FIBRA_YOPAL] >
```

Nota. El apéndice B, muestra el archivo de configuración de la CLI (Configuration Line Interfaz) del equipo Mikrotik ISP Fibra Óptica del prototipo. Tomado de: *Elaboración propia.*

Apéndice C.

CLI MikroTik Starlink (ISP_STARLINK_YOPAL)

Simulación de Enlace Satelital LEO de Respaldo

```
[admin@ISP_Starlink] > exp ter
# 2026-05-17 05:59:20 by RouterOS 7.20.8
# system id = 3k7j5iDlXMA
#
/interface bridge add name=lo-google
/interface ethernet set [ find default-name=ether1 ] comment=Eth1-Cx-FW01-E0/1
/port set 0 name=serial0
/port set 1 name=serial1
/routing ospf instance add disabled=no name=ospf-inst-starlink redistribute=connected
router-id=2.2.2.2
/routing ospf area add disabled=no instance=ospf-inst-starlink name=backbone-starlink
/snmp community add addresses=192.168.73.20/32 name=UnadPRG
/system logging action add name=syslogremoto remote=192.168.73.20 target=remote
/interface bridge settings set allow-fast-path=no
/ip address add address=190.20.20.1/30 interface=ether1 network=190.20.20.0
/ip address add address=10.255.0.2 interface=lo network=10.255.0.2
/ip address add address=8.8.8.8 interface=lo-google network=8.8.8.8
/ip address add address=8.8.4.4 interface=lo-google network=8.8.4.4
/ip dhcp-client add interface=ether1
/ip firewall address-list add address=192.168.73.0/24 list=ADMIN_NETWORK
/ip firewall address-list add address=192.168.73.20 list=WS_PNETLab
/ip firewall filter add action=accept chain=input protocol=icmp
/ip firewall filter add action=accept chain=input comment=PERMITIR_PRTG_ENTRANTE src-
address=192.168.73.0/24
/ip firewall filter add action=accept chain=input comment=MONITOREO_PRTG src-
address=192.168.73.0/24
```

```
/ip firewall filter add action=accept chain=forward comment=MONITOREO_PRTG src-
address=192.168.73.0/24
/radius add address=192.168.73.20 service=login
/routing ospf interface-template add area=backbone-starlink disabled=no
networks=190.20.20.0/30
/routing ospf interface-template add area=backbone-starlink disabled=no
networks=10.255.0.2/32 type=ptp
/routing ospf interface-template add area=backbone-starlink disabled=no networks=8.8.8.8/32
type=ptp
/snmp set contact="Ing. Gustavo Cepeda" enabled=yes location="Yopal - Starlink" trap-
community=UnadPRG trap-target=192.168.73.20 trap-version=2
/system identity set name=ISP_Starlink
/system logging add action=syslogremoto topics=info,critical,error,warning
/system note set
note="*****************************************************************************\
    \n*****************************************************************************\
    \n** ====        &&&&   &&&   &&&     &&&   &&&&&&&&   &&&&&&&&        ===== ** \
    \n** ====         &&&   &&&   &&&&    &&&   &&&  &&&    &&   &&&        ===== ** \
    \n** ====         &&&   &&&   &&& &&& &&&   &&&&&&&&    &&   &&&        ===== **   \
    \n** ====         &&&   &&&   &&&   &&&&&   &&&  &&&    &&   &&&        ===== ** \
    \n** ====          &&&&&&&    &&&     &&&   &&&  &&&   &&&&&&&&        ===== ** \
    \n**                                                                          ** \
    \n**           UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD              **\
    \n**            ESPECIALIZACION EN REDES DE TELECOMUNICACIONES                **\
    \n**                                                                          **\
    \n** PROYECTO: DISENO DE PROTOTIPO DE RED DE ALTA DISPONIBILIDAD Y REDUNDANTE **\
    \n** UBICACION: YOPAL, CASANARE                                              **\
    \n** AUTOR: ING. GUSTAVO A. CEPEDA                                           **\
    \n**                                                                          **\
    \n**                              iiADVERTENCIA!!:                            **\
```

```
    \n**ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO, TODO INGRESO ES MONITOREADO**\
    \n**                                                                          **\
    \n******************************************************************************\
    \n******************************************************************************"
/user aaa set use-radius=yes
[admin@ISP_Starlink] >
```

Nota. El apéndice C, muestra el archivo de configuración de la CLI (Configuration Line Interfaz) del equipo ISP Starlink del prototipo. Tomado de: *Elaboración propia.*

Apéndice D.

CLI Router Core

Archivo de configuración del Router Core del prototipo

```
RT_Core#show running-config
Building configuration...


Current configuration : 8826 bytes
!
! Last configuration change at 19:40:25 UTC Thu May 14 2026 by gcepeda
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RT_Core
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$gYi6$pV/KHMGrWM7PDQoya07lM1
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default group radius enable
aaa authorization exec default local
!
```

```
!
!
!
!
aaa session-id common
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
crypto pki token default removal timeout 0
!
!
```

```
username gcepeda privilege 15 secret 5 $1$chLu$ZVr1h4Le2kEpgUVzuMes0.
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description IP_GESTION_PARA_PRTG
 ip address 10.255.0.3 255.255.255.255
!
interface Ethernet0/0
 description ENLACE_HACIA_FIREWALL
 ip address 10.0.0.2 255.255.255.252
 ip ospf hello-interval 5
!
interface Ethernet0/1
 description TRONCAL_HACIA_SWITCH_CORE
 no ip address
!
```

```
interface Ethernet0/1.10
 description RED_CORPORATIVA
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface Ethernet0/1.20
 description RED_ADMINISTRATIVA
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/1.30
 description RED_INVITADOS
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface Ethernet0/1.40
 description ENLACE_HACIA_SW_BORDE_BACKBONE
 encapsulation dot1Q 40
 ip address 172.16.100.1 255.255.255.252
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
router ospf 1
 router-id 10.255.0.3
```

```
 network 10.0.0.0 0.0.0.3 area 0
 network 10.255.0.3 0.0.0.0 area 0
 network 172.16.100.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip radius source-interface Ethernet0/1.20
ip sla 10
 icmp-echo 8.8.8.8
 frequency 5
ip sla schedule 10 life forever start-time now
logging 192.168.73.20
!
snmp-server community UnadPRG RO
snmp-server location Yopal - Core Central
snmp-server contact Ing. Gustavo Cepeda
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
```

```
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps xgcp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps diameter
snmp-server enable traps rf
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bfd
snmp-server enable traps bstun
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
```

```
snmp-server enable traps config-ctid

snmp-server enable traps dial

snmp-server enable traps dlsw

snmp-server enable traps dsp card-status

snmp-server enable traps dsp oper-state

snmp-server enable traps dsp video-usage

snmp-server enable traps dsp video-out-of-resource

snmp-server enable traps entity

snmp-server enable traps fru-ctrl

snmp-server enable traps resource-policy

snmp-server enable traps frame-relay multilink bundle-mismatch

snmp-server enable traps frame-relay

snmp-server enable traps frame-relay subif

snmp-server enable traps hsrp

snmp-server enable traps ipmobile

snmp-server enable traps ipmulticast

snmp-server enable traps isis

snmp-server enable traps mpls traffic-eng

snmp-server enable traps mpls fast-reroute protected

snmp-server enable traps mpls rfc ldp

snmp-server enable traps mpls ldp

snmp-server enable traps msdp

snmp-server enable traps mvpn

snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message

snmp-server enable traps pppoe

snmp-server enable traps cpu threshold

snmp-server enable traps nhrp nhs

snmp-server enable traps nhrp nhc

snmp-server enable traps nhrp nhp

snmp-server enable traps nhrp quota-exceeded
```

```
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps stun
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps pw vc
snmp-server enable traps waas
snmp-server enable traps event-manager
snmp-server enable traps firewall serverstatus
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
```

```
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps ccme
snmp-server enable traps srst
snmp-server enable traps mpls vpn
snmp-server enable traps voice
snmp-server enable traps dnis
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.73.20 version 2c UnadPRG
!
!
radius-server host 192.168.73.20 auth-port 1812 acct-port 1813 timeout 7 retransmit 5 key
C3p3d42023**
!
radius server RADIUS_SERVER
 timeout 7
 retransmit 5
 key C3p3d42023**
!
!
control-plane
!
!
!
!
!
!
banner motd ^CC
**************************************************************************
**************************************************************************
```

```
** ====        &&&&   &&&   &&&     &&&   &&&&&&&&   &&&&&&&&         ===== **
** ====         &&&   &&&   &&&&    &&&   &&&  &&&    &&   &&&        ===== **
** ====         &&&   &&&   &&& &&& &&&   &&&&&&&&    &&   &&&        ===== **
** ====         &&&   &&&   &&&   &&&&&   &&&  &&&    &&   &&&        ===== **
** ====          &&&&&&&    &&&     &&&   &&&  &&&   &&&&&&&&         ===== **
**                                                                          **
**           UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD               **
**            ESPECIALIZACION EN REDES DE TELECOMUNICACIONES                 **
**                                                                          **
** PROYECTO: DISENO DE PROTOTIPO DE RED DE ALTA DISPONIBILIDAD Y REDUNDANTE **
** UBICACION: YOPAL, CASANARE                                              **
** AUTOR: ING. GUSTAVO A. CEPEDA                                           **
**                                                                          **
**                              iiADVERTENCIA!!:                            **
**ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO, TODO INGRESO ES MONITOREADO**
**                                                                          **
******************************************************************************
******************************************************************************
^C
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 15 0
 password C3p3d42023**
 history size 50
 transport input all
!
!
```

```
end


RT_Core#
```

Nota. El apéndice D, muestra el archivo de configuración de la CLI (Configuration Line Interfaz) del equipo Router Core del prototipo. Tomado de: *Elaboración propia.*

Apéndice E.

CLI Switch Core

Archivo de configuración del Switch Core del prototipo

```
SW_Core#Show running-config
Building configuration...


Current configuration : 6110 bytes
!
! Last configuration change at 02:51:55 UTC Fri May 15 2026 by gcepeda
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_Core
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$FEL5$3O8CTQg/X4MG5bKLXz8TI1
!
username gcepeda privilege 15 secret 5 $1$Ze0l$uC8Wp.EjLRWC0fOIh98fT/
aaa new-model
!
!
aaa authentication login default group radius local
```

```
aaa authentication enable default none
aaa authorization exec default group radius local
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 description TRUNK_TO_RT_CORE
 switchport trunk allowed vlan 10,20,30,40
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 description LINK_TO_SW_BORDE
 switchport trunk allowed vlan 40
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/2
 description LINK_TO_SW1_CORPORATIVA
 switchport trunk allowed vlan 10
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/3
 description LINK_TO_SW2_ADMINISTRATIVA
 switchport trunk allowed vlan 20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/0
 description LINK_TO_SW3_INVITADOS
 switchport trunk allowed vlan 30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/1
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/2
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/3
 media-type rj45
```

```
 negotiation auto
!
interface Vlan20
 description IP_GESTION_SWITCH_CORE
 ip address 192.168.20.2 255.255.255.0
!
ip default-gateway 192.168.20.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.1
!
!
ip radius source-interface Vlan20
logging host 192.168.73.20
!
!
snmp-server community UnadPRG RO
snmp-server location Yopal - Core Central
snmp-server contact Ing. Gustavo Cepeda
!
!
radius server RADIUS_SERVER
 address ipv4 192.168.73.20 auth-port 1812 acct-port 1813
 key C3p3d42023**
!
!
control-plane
```

```
!
banner exec ^C
**********************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**********************************************************************^C
banner incoming ^C
**********************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**********************************************************************^C
banner login ^C
**********************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**********************************************************************^C
banner motd ^CC
**********************************************************************
```

```
**************************************************************************
** ====        &&&&   &&&   &&&     &&&   &&&&&&&&   &&&&&&&&        ===== **
** ====         &&&   &&&   &&&&    &&&   &&&  &&&    &&   &&&        ===== **
** ====         &&&   &&&   &&& &&& &&&   &&&&&&&&    &&   &&&        ===== **
** ====         &&&   &&&   &&&   &&&&&   &&&  &&&    &&   &&&        ===== **
** ====          &&&&&&&    &&&     &&&   &&&  &&&   &&&&&&&&        ===== **
**                                                                      **
**           UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD           **
**            ESPECIALIZACION EN REDES DE TELECOMUNICACIONES             **
**                                                                      **
** PROYECTO: DISENO DE PROTOTIPO DE RED DE ALTA DISPONIBILIDAD Y REDUNDANTE **
** UBICACION: YOPAL, CASANARE                                           **
** AUTOR: ING. GUSTAVO A. CEPEDA                                        **
**                                                                      **
**                             iiADVERTENCIA!!:                         **
**ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO, TODO INGRESO ES MONITOREADO**
**                                                                      **
**************************************************************************
**************************************************************************
^C
!
line con 0
 privilege level 15
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 15 0
 privilege level 15
 history size 50
 transport input all
```

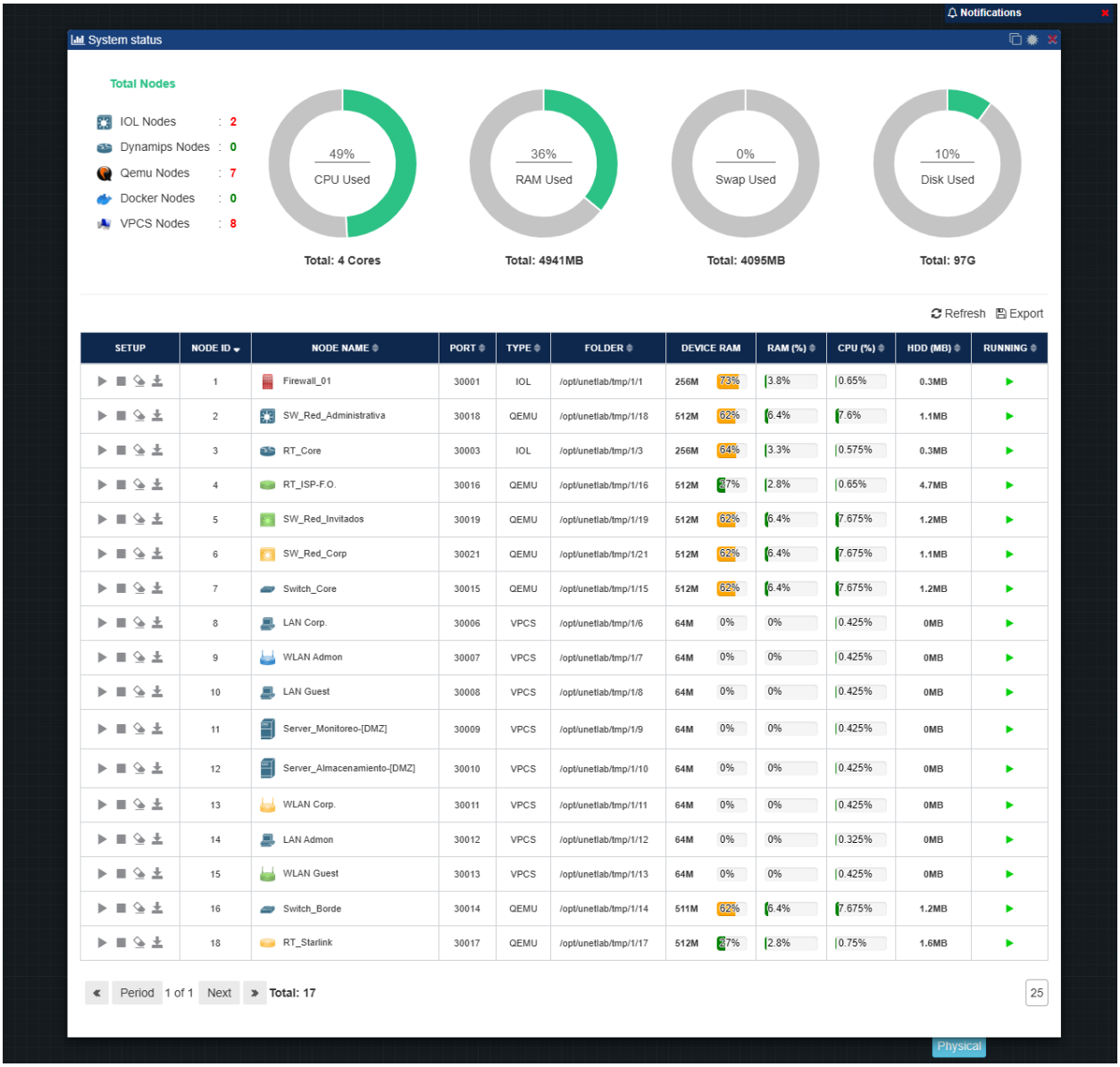
```
!
!
end


SW_Core#
```

Nota. El apéndice E, muestra el archivo de configuración de la CLI (Configuration Line Interfaz) del equipo Switch Core del prototipo. Tomado de: *Elaboración propia.*

Apéndice F.

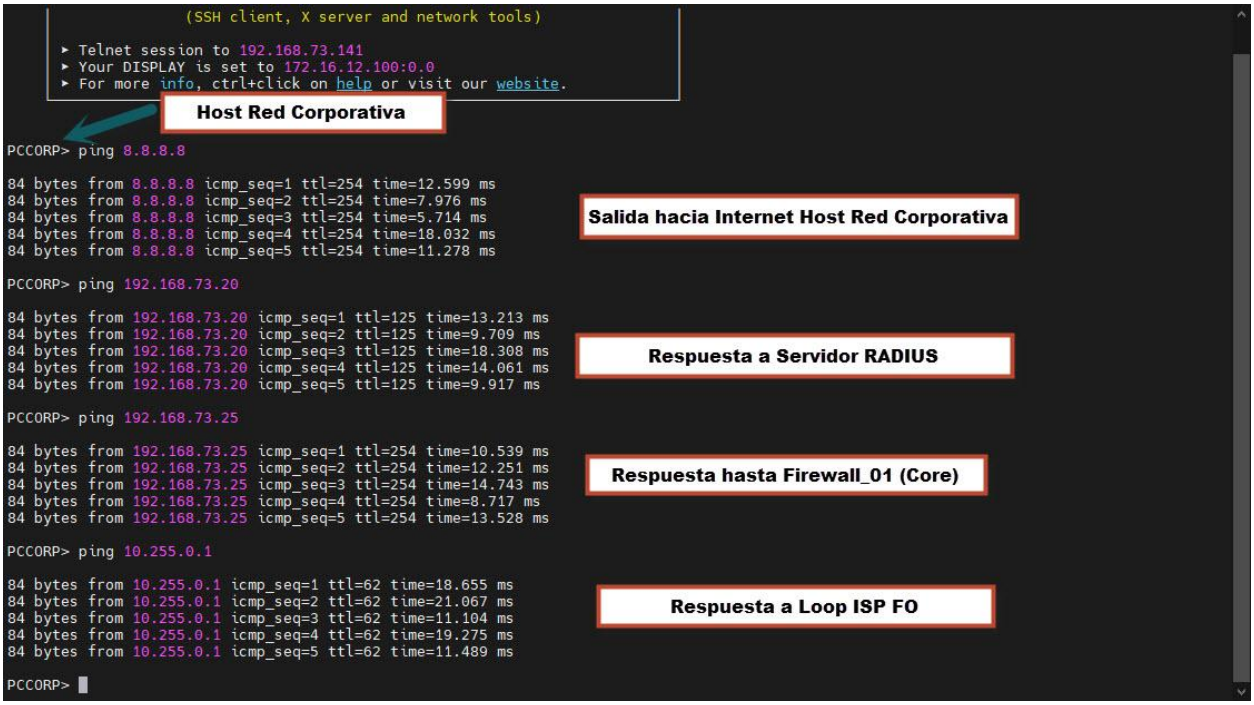
Estado del Sistema y Consumo de Recursos en PNetLab



Nota. Se observa el uso de CPU y RAM del hipervisor durante la ejecución de la topología completa. La IP de gestión 192.168.73.141 confirma el acceso al entorno de simulación. Tomado de: *Elaboración propia.*

Apéndice G.

Pruebas del Laboratorio desde un Host Usuario del Prototipo.



Nota. Las trazas de eco ICMP ejecutadas desde la terminal del host interno (PC-CORP) validan el éxito del plano de datos y el enrutamiento de la infraestructura híbrida. Se constata la salida transparente hacia el exterior (DNS de Google 8.8.8.8), la comunicación directa con el servidor local de autenticación TekRADIUS (192.168.73.20) y la visibilidad sin pérdidas hacia el Gateway del Firewall perimetral (192.168.73.25) junto con la interfaz de loopback del operador principal de Fibra Óptica (10.255.0.1). Tomado de: *Elaboración propia.*