Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Herramientas virtualizadas para evaluación y gestión de redes ópticas pasivas

INGE-2744

Proyecto Integrador

Previo la obtención del Título de:

Ingeniero en Telecomunicaciones

Presentado por:

Steveen Daniel Rios Monar

Stefany Dayanna López Quezada

Guayaquil - Ecuador

Año: 2024

Dedicatoria

Steveen Daniel Rios Monar

El presente proyecto está dedicado a la comunidad de telecomunicaciones en **ESPOL**, con la esperanza de que inspire el aprendizaje, la innovación y el crecimiento de futuros proyectos. A lo largo de mi formación, he desarrollado un profundo cariño por esta carrera, que me ha brindado tanto conocimientos como una visión del impacto que la tecnología puede tener en el mundo.

Mi deseo es que este proyecto siembre una semilla que motive a nuevas generaciones a explorar, asumir retos y contribuir con la innovación. Espero que el club **CERIT**, del cual tuve el honor de formar parte, sea uno de los principales beneficiarios de esta herramienta, aprovechándola para seguir fomentando la colaboración, el aprendizaje y el desarrollo de nuevas oportunidades que impulsen el progreso de nuestra carrera y más allá.

Dedicatoria

Stefany Dayanna López Quezada

Con profundo amor y gratitud dedico esta tesis a mis padres, **Julio** y **Graciela**, quienes me ensañaron el valor de la perseverancia, trabajo duro y resiliencia. Y cuyo esfuerzo, sacrificio y apoyo incondicional me han permitido llegar hasta aquí. A mis hermanos, **Ángel, Allyson y Mathías**, que con su apoyo y energía me animaron a dar lo mejor de mí.

Con respeto y cariño, la dedico también a quienes ya no están, pero siguen vivos en mis recuerdos y acciones: **mi papito Manuel y mi papi Lino**, personas ejemplares y fundamentales en mi vida, así como a mi querido primo **Anthony "Toño"** y a mi buen amigo **Erick**, cuyas vidas se apagaron demasiado pronto, pero su huella permanecerá en mis experiencias, metas y sueños.

Este logro no es solo mío, sino de cada uno de ustedes, por haberme acompañado a lo largo de este camino.

Agradecimientos

Steveen Daniel Rios Monar

Este proyecto representa el esfuerzo, la dedicación y el apoyo de muchas personas a lo largo de mi formación. Agradezco profundamente a mis padres, **Sixto** e **Isabel**, y a mi hermana, **Daysi**, por su amor incondicional, por todo el esfuerzo que han realizado a lo largo de mi vida, y por ser mi mayor motivación. A mi tutor, **German**, por su orientación e inspiración que recibí para el enfoque de este proceso. A mi compañera, **Stefany**, por su ardua colaboración durante mi recuperación. A mi pareja, **Melanny**, y a aquellas personas especiales que mantengo cerca de mí, por su apoyo y contribución en cada desafío. Este logro es el reflejo de un camino compartido, y a todos los que fueron parte de él, les expreso mi más sincera gratitud.

Agradecimientos

Stefany Dayanna López Quezada

Expreso mi más profunda gratitud a todas las personas que han formado parte de esta etapa en mi vida. A mis amigos y compañeros con los que he compartido aprendizajes y retos. Muchos de ellos ya han alcanzado sus metas profesionales, y a los que aún están en este camino, espero que este proyecto contribuya a su aprendizaje y les motive a explorar nuevos campos.

A mis docentes, la mayoría de los cuales han sido una fuente de inspiración en este viaje.

A mi compañero **Steveen**, por su ayuda y amistad a lo largo de los años. A mi tutor, **German**, por su orientación y motivación durante mi formación profesional. A mi pareja, **Gabriel**, por su paciencia y cariño.

Y especialmente a mi familia por su sacrificio y confianza en mí. A cada uno de ustedes les estaré siempre agradecida.

Declaración Expresa

Nosotros Steveen Daniel Rios Monar y Stefany Dayanna López Quezada acordamos y reconocemos que:

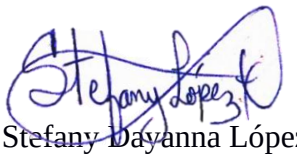
La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, viernes 11 de octubre del 2024.

Steveen Daniel Rios Monar



Stefany Dayanna López Quezada

Evaluadores

Firmado electrónicamente por:
MARIA ANTONIETA
ALVAREZ VILLANUEVA

Ph.D. María Antonieta Álvarez Villanueva

Profesor de Materia

Firmado electrónicamente por:
GERMAN RICARDO
VARGAS LOPEZ

Ph.D. Germán Ricardo Vargas López

Tutor de proyecto

(Nota: Nombres completos y firmado electrónicamente)

Resumen

En el presente proyecto se consiguió implementación de una infraestructura virtualizada basada en funciones de red, con la capacidad de supervisar y gestionar redes ópticas pasivas (PON) dentro de un entorno académico, específicamente, el laboratorio de Redes de Telecomunicaciones de Espol.

Para llevar a cabo este proceso, fue necesario complementar la infraestructura de red existente en el laboratorio de Redes de Telecomunicaciones en Espol, creando una red más fiable y capaz de soportar el despliegue de estos nuevos servicios.

La tecnología principal seleccionada fue la virtualización de funciones de red (NFV), para conseguir una administración centralizada del sistema mediante herramientas de software libre, tales como, Proxmox, que sirve como servidor principal donde se alojarán distintas máquinas virtuales y contenedores como OPNsense, utilizado para el enrutamiento y firewall, y LibreNMS para el monitoreo de tráfico en tiempo real.

Como resultado, se logró: una administración centralizada, optimización del tráfico de red y reducción de costos operativos. Planteando las bases para el desarrollo de sistemas más complejos dentro del marco de prácticas académicas.

Palabras Clave: NFV, monitorización, software libre, Proxmox, máquinas virtuales

Abstract

In this project, the implementation of a virtualized infrastructure based on network functions, with the ability to monitor and manage passive optical networks (PON) within an academic environment, specifically, the Telecommunications Networks laboratory at Espol, was achieved.

To conduct this process, it was necessary to complement the existing network infrastructure in the Telecommunications Networks laboratory at Espol, creating a more reliable network capable of supporting the deployment of these new services.

The main technology selected was the network functions virtualization (NFV), to achieve a centralized administration of the system through free software tools, such as Proxmox, which serves as the main server where different virtual machines and containers such as OPNsense, used for routing and firewall, and LibreNMS for real-time traffic monitoring will be hosted.

As a result, centralized administration, optimization of network traffic and reduction of operating costs were achieved. Laying the foundations for the development of more complex systems within the framework of academic practices.

Keywords: *NFV, monitoring, open-source software, Proxmox, virtual machines*

Índice general

Abreviaturas

ARP Address Resolution Protocol

BGP Border Gateway Protocol

CDP Cisco Discovery Protocol

CPU Central Processing Unit

FDP Foundry Discovery Protocol

GPON Gigabit Passive Optical Network

IAAS Infrastructure as a Service

ISP Internet Service Provider

LLDP Link Layer Discovery Protocol

NFV Network Functions Virtualization

NIST National Institute of Standards and Technology

NUMA Non-Uniform Memory Access

OLT Optical Line Terminal

ONT Optical Network Terminal

OS Operating System

OSPF Open Shortest Path First

OSS Operations Support System

OTT Over-The-Top

PON Passive Optical Network

SDN Software-Defined Networking

SNMP Simple Network Management Protocol

VM Virtual Machine

VNFM Virtual Network Function Manager

VNFs Virtual Network Functions

Simbología

% Porcentaje

°C Grados Celsius (unidad de temperatura)

dBm Decibel-mili watt (unidad de potencia en telecomunicaciones)

GB Gigabyte (unidad de almacenamiento de datos)

Gbps Gigabits por segundo (unidad de velocidad de transmisión de datos)

Índice de figuras

Índice de tablas

Capítulo 1

1.1 Introducción

La creciente demanda de servicios de telecomunicaciones más rápidos y con capacidad para manejar altos volúmenes de tráfico a menor costo, ha impulsado el desarrollo de tecnologías emergentes, como las Redes de Acceso Óptico Pasivo (Passive Optical Network, PON), una de las redes tecnológicamente más avanzadas y potentes [1]. Debido a sus grandes beneficios, es importante su correcto diseño, gestión y protección para garantizar tanto su funcionalidad y seguridad, contribuyendo al crecimiento económico, tecnológico y social [2]. Sin embargo, dicha gestión en entornos educativos, como el Laboratorio de Redes de Telecomunicaciones de la Escuela Superior Politécnica del Litoral (ESPOL), enfrenta problemas por la falta de integración entre la red física y una plataforma que permita su administración.

Este capítulo analiza los problemas de gestión en redes PON y presenta la virtualización como una herramienta capaz de proporcionar centralización, adaptabilidad y escalabilidad a la red. Brindando a los usuarios la oportunidad de inclusive virtualizar funciones de red (Network Function Virtualization, NFV), tales como enrutamiento y firewall, independientemente del hardware [3]. En el caso de los estudiantes del laboratorio, implementar estas tecnologías les permitirá contar con herramientas para gestionar eficientemente la red y mejorar sus capacidades en el análisis de redes.

1.2 Descripción del problema

La administración de la infraestructura de una red PON es fundamental para garantizar su eficiencia y proporcionar calidad en la prestación de servicios de telecomunicaciones, dada su capacidad para manejar grandes volúmenes de datos [1]. La falta de un sistema de gestión centralizado limita la optimización de la red, afectando su rendimiento y adaptabilidad a nuevas necesidades y tecnologías [4].

En las tareas de administración de red se presentan también otro tipo de barreras, como la dependencia de software propietario, que dificulta la gestión eficiente de los sistemas de red,

principalmente al restringir la autonomía del usuario para adaptar el sistema a sus necesidades. Por el contrario, el software libre ofrece ventajas significativas, como la reducción de costos de licencia, la independencia de proveedores, la interoperabilidad entre sistemas mediante protocolos abiertos, como el protocolo Simple de Administración de Red (Simple Network Management Protocol, SNMP), y su alta flexibilidad [5].

Actualmente, el Laboratorio de Redes de Telecomunicaciones de ESPOL no cuenta con una infraestructura de red física correctamente establecida para la gestión adecuada de redes PON. Aunque dispone de equipos dedicados, como la OLT [1]Huawei MA5608T, no se ha implementado una infraestructura lo suficientemente robusta que permita una administración integral (Figura 1 *Infraestructura inicial*), además, este equipo incluye software licenciado, lo que limita las opciones de administración. Por otro lado, los dispositivos como ONT y enrutadores, se gestionan de forma independiente, requiriendo acceder a cada equipo por separado para validar configuraciones básicas, dificultando la simulación y evaluación de tareas de administración de redes en un entorno educativo orientado a la práctica y experimentación.

Es así como, NFV emerge como una tecnología que permite realizar funciones específicas, como enrutamiento y cortafuegos, independientemente del hardware dedicado [3]. Esta tecnología facilita la administración y escalabilidad de recursos en redes PON, siendo favorable en entornos que demandan una gestión flexible y centralizada de múltiples dispositivos de red [6].

La relevancia de este problema radica en que una gestión eficiente de la red es fundamental para el desarrollo de infraestructuras TIC tanto en el ámbito académico y empresarial. Las variables de interés para abordar este problema incluyen:

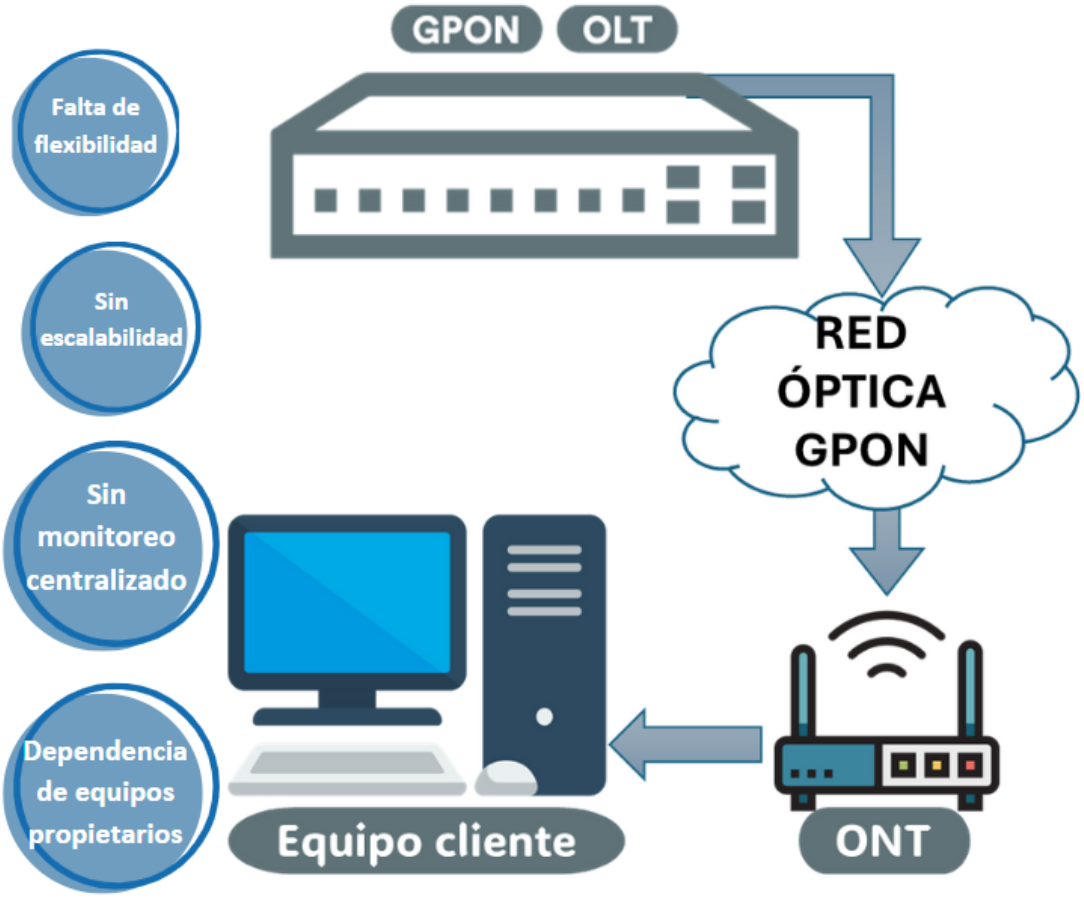
- Centralización de la gestión de red
- Flexibilidad y escalabilidad.

[1] La OLT Huawei MA5608T dispone de softwares como iMaster NCE o U2000, que son propietarios, para su administración.

- Interoperabilidad entre sistemas.
- Entorno educativo orientado a la práctica.

Figura 1

Infraestructura inicial del laboratorio



1.3 Justificación del problema

El Laboratorio de Redes de Telecomunicaciones de ESPOL es un espacio que contribuye significativamente a la formación de futuros profesionales. Por ello, es importante que cuente con una red operativa, con la capacidad de ser administrada de forma integral, brindando la oportunidad a los estudiantes de adquirir competencias en la gestión de redes PON.

En este espacio, al carecer de una infraestructura robusta debido, principalmente, a las limitaciones presupuestarias para la adquisición de nuevos equipos, surgen dificultades para implementar estas prácticas que implican el uso de tecnologías ampliamente adoptadas en el

mercado actual. Estas tecnologías permiten redes más ágiles y fácilmente expandibles, lo que coloca a los estudiantes en una situación desfavorable para desarrollar competencias relacionadas con las prácticas de tecnologías emergentes.

Utilizar software propietario para la administración del hardware dedicado, no resulta lo más conveniente. Algunos estudios [7] sugieren que el software privado o propietario, además de representar costes operativos adicionales, impone dependencia de proveedores y restringe la modificación del código fuente, resultando especialmente desfavorable para el laboratorio donde lo que se busca es flexibilidad. Por otro lado, la adopción de tecnologías de código abierto permite economizar recursos y adaptar la red a las necesidades del usuario, permitiendo la creación de entornos más versátiles y económicos, alineándose con las necesidades de instituciones académicas.

Como antecedente, existen proyectos comerciales como VOLTHA, que han implementado virtualización en redes PON, lo que les permitió gestionar su sistema de manera flexible y compatible con diversos proveedores de equipos, manejando varias redes de banda ancha de forma unificada [8].

En este sentido, se identifica que es necesario complementar la infraestructura física del laboratorio, y mediante software de código libre con capacidades de administración de red, centralizar el control y permitir su evaluación desde un punto de administración. Esta iniciativa puede servir como base para prácticas académicas y proyectos de investigación en el laboratorio, que promueva un enfoque de innovación y flexibilidad en la enseñanza tradicional.

Inclusive trascendiendo el ámbito académico, se tiene el caso de operadores de telecomunicaciones que, para mejorar su competitividad frente a servicios Over-The-Top (OTT), operan con infraestructuras costo-eficientes, dado que optaron por la implementación de tecnologías como la virtualización de funciones de red (NFV, Network Functions Virtualization), para centralizar su red y volverla más competitiva en el mercado [5]. También utilizan alternativas

como la infraestructura en la nube para ofrecer servicios tales como Infraestructura como Servicio (IaaS[2]), ampliando su oferta más allá de las comunicaciones tradicionales y compitiendo con empresas como Amazon, Facebook, Google y Microsoft [5].

En conclusión, la importancia de esta problemática radica en la necesidad de ofrecer a los estudiantes una formación práctica en un entorno alineado con las tecnologías de vanguardia en la industria, como la integración de la virtualización con software libre para centralizar y optimizar la gestión de recursos. Esta carencia en la administración, principal problema del Laboratorio de Redes de Telecomunicaciones puede ser abordada mediante soluciones flexibles y económicas, capaces de crecer tanto en el ámbito académico como en el comercial.

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar una infraestructura basada en funciones de red virtualizadas para la administración de redes GPON mediante software libre, orientada a entornos educativos y de telecomunicaciones.

1.4.2 Objetivos específicos

- Diseñar la infraestructura virtualizada basada en funciones de red para la administración de redes ópticas, especificando las herramientas de software libre y los componentes necesarios para la virtualización de funciones clave como enrutamiento, firewall y análisis de tráfico.
- Implementar las funciones de red en el entorno virtualizado, asegurando una integración flexible y funcional que permita la administración y supervisión centralizada de los componentes de red.

[2]IASS permite que el usuario acceda a recursos sean de computación, procesamiento, almacenamiento para ejecutar software especifico, pero no a la infraestructura subyacente de la nube [35].

- Evaluar la eficiencia de las funciones de red virtualizadas en la red GPON, analizando su rendimiento en condiciones operativas para asegurar que cumplan con los requisitos de administración y supervisión centralizada.

1.5 Marco teórico

1.5.1 Redes PON como base de la infraestructura de las telecomunicaciones

En los esfuerzos por mejorar la calidad de servicios de telecomunicaciones, se han desarrollado tecnologías que permitan a los usuarios mejores experiencias en la conexión, como lo es la tecnología PON [9]. De acuerdo con Casademont et al., las redes PON son un tipo de red de telecomunicaciones a través de fibra óptica que transportar grandes volúmenes de tráfico a altas velocidad mediante componentes pasivos[3] y ofrecen servicios de internet, voz y televisión desde una central hasta múltiples usuarios finales [10].

Redes GPON: Estructura

La Red Óptica Pasiva Gigabit (Gigabit Passive Optical Network, GPON[4]) es una tecnología PON que cuenta con altas capacidades de transferencia de datos. Desempeña un papel importante en las telecomunicaciones modernas, ya que cuenta con infraestructura confiable que satisface la creciente demanda de datos y velocidad, permitiendo aplicaciones avanzadas y conexiones simultáneas de múltiples dispositivos [11].

La infraestructura GPON cuenta con una Terminal de línea óptica (Optical Line Terminal, OLT), que convierte las señales eléctricas provenientes de la troncal del proveedor de servicios de internet (ISP) y las transforma en señales ópticas enviándolas a la Terminal de red óptica (Optical Networking Terminal, ONT) de cada usuario final [11].

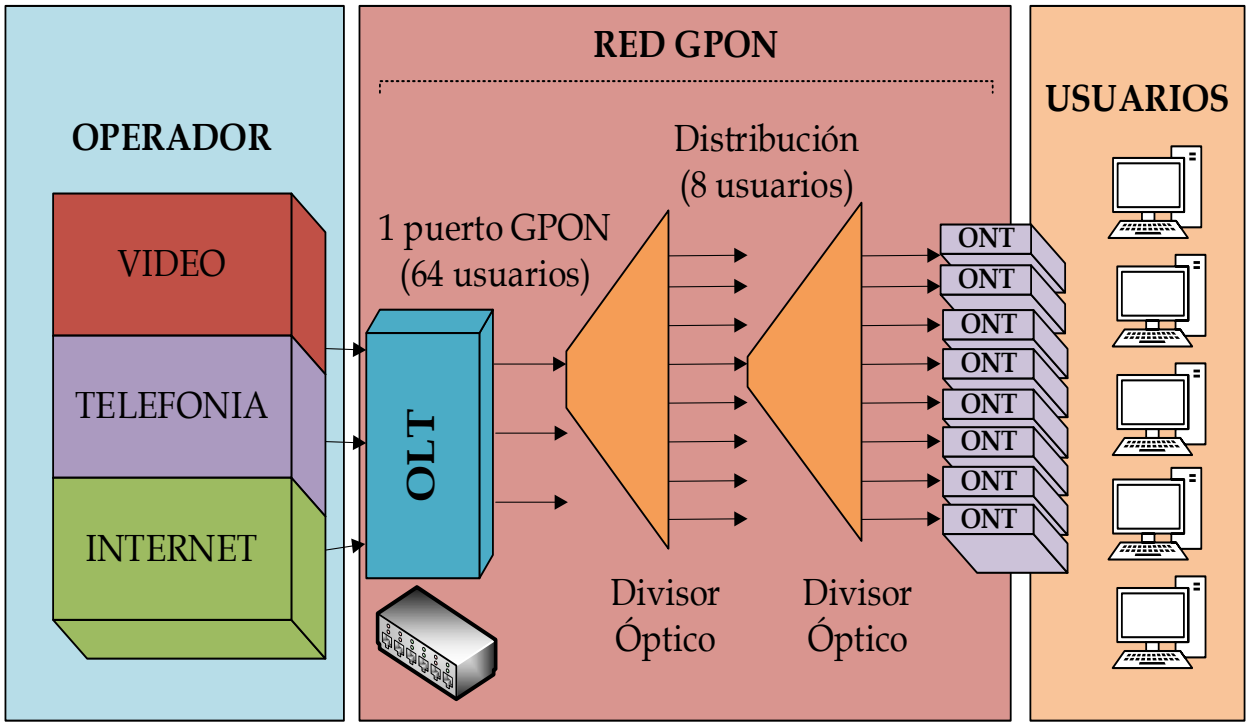
[3] Elementos pasivos no requiere energía para transmitir la señal óptica de un punto a otro como splitters, atenuadores ópticos, fibra óptica, empalmes y conectores.

[4] GPON alcanza velocidades de descarga de hasta 2.488 Gbps y en carga hasta 1.244 Gbps.

Las ONTs se encuentran interconectadas mediante splitters, que reciben y distribuyen el tráfico. La red puede incorporar varios splitters; por ejemplo, la Figura 2, muestra una configuración 1:8, donde la señal se multiplexa para llegar a varios usuarios.

Figura 2.

Estructura Red GPON (Reproducción tomada de [11])



1.5.2 Administración y supervisión de redes

De acuerdo con Millan, se plantea que la administración de redes consiste en un conjunto de técnicas orientadas a mantener una red operativa, eficiente, segura y bien documentada, con un monitoreo constante y una planificación adecuada. De tal manera que se obtengan métricas para optimizar recursos, como el ancho de banda [12].

Existen varias alternativas para monitorear una red, la principal diferencia está en cómo se capturan los datos supervisados, el más común es la monitorización activa SNMP. De acuerdo con Calvo, es un proceso que implica un monitoreo continuo de los equipos para obtener información precisa sobre el estado actual. Se logra este proceso mediante sondeos repetitivos, por lo general, cada 5 minutos, esperando una respuesta de los dispositivos supervisados. [13].

Según su sitio oficial [14], LibreNMS es una herramienta para monitorizar la red de código abierto que ofrece servicios para la gestión y supervisión de red de forma integral, el cual trabaja bajo SNMP[5], y puede instalarse en cualquier sistema operativo (Operating System, OS) Linux, como Debian, Ubuntu, Red Hat Enterprise Linux, etc. Cuenta también, con un sistema de alertas personalizables que envía notificaciones a través de múltiples canales, como correo electrónico, IRC y Slack [14].

1.5.3 Virtualización

Con base en lo planteado por Ulloa, la virtualización permite instalar múltiples OS como máquinas virtuales (Virtual Machine, VM) en un único equipo físico llamado host. De esta manera, se tienen múltiples sistemas funcionando de forma aislada, que aprovechan al máximo los recursos de hardware, como puertos habilitados, la conexión de red, particionamiento, capacidad de procesamiento CPU, memoria, etc. La evolución de la virtualización ha ampliado su uso en diversos entornos, facilitando el acceso remoto a través de internet o intranet [15].

Ventajas de la virtualización

La ventaja principal es que, al ejecutar varios OS en un solo equipo, se maximiza el uso del hardware y simulando VM independientes, se centraliza el almacenamiento, facilitando la gestión de servidores y aplicaciones sin equipos físicos adicionales. Esto implica directamente en la reducción de costos y riesgos, mejorando la flexibilidad y optimizando el rendimiento del sistema [15]. Otro beneficio adicional se encuentra en la consolidación de servidores para reducir equipos físicos, mayor disponibilidad y menos tiempo de inactividad, mejor respaldo, recuperación rápida ante fallos, y escalabilidad para ajustarse a las necesidades sin altos costos.

[5] LibreNMS se integra también con protocolos como CDP, FDP, LLDP, OSPF, BGP, y ARP, mediante los cuales es capaz de descubrir automáticamente dispositivos conectados a la red, facilitando su integración en infraestructuras existentes.

1.5.4 Virtualización de las funciones de red (NFV)

Como menciona Gray y Nadeau, NFV se refiere a una tecnología que permite virtualizar funciones de red, como un enrutador, convirtiéndolas en una instancia de hardware independiente del software. Estas instancias, llamadas Funciones de red virtualizadas (Virtualized Network Functions, VNFs), funcionan como VM que consumen recursos de cómputo como RAM, disco y procesamiento [16].

Existen dos términos que suelen relacionarse, pero se refieren a tecnologías distintas de virtualización. Por un lado, está NFV virtualiza funciones de red específicas, mientras que SDN (Software Defined Network) separa el control de la red de los dispositivos físicos, permitiendo una gestión centralizada del tráfico [16].

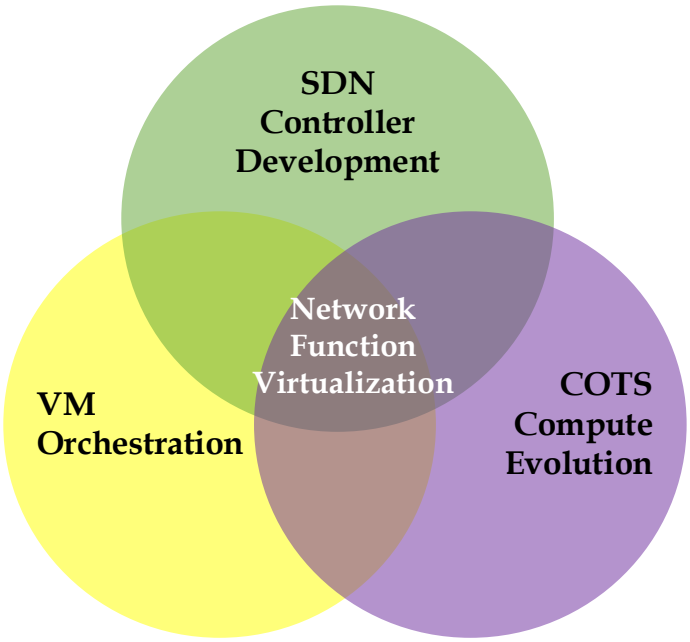
La Figura 3, muestra tres tecnologías fundamentales que hacen posible la implementación de NFV, de forma más eficaz y adaptable. Esta tecnología se encuentra en la intersección de estas tres áreas [16]:

- **SDN Controller Development:** Desarrollo de controladores para SDN.
- **VM Orchestration:** Coordinación de servidores o máquinas virtuales, para la administración de recursos de la red.
- **COTS [6]Compute Evolution:** Utilización de equipos comerciales estándar, COTS (Commercial Off-The-Shelf), disponibles en el mercado.

[6] COTS son capaces de soportar servicios de red virtualizados, en lugar de depender de equipos específicos o propietarios.

Figura 3.

Convergencia para habilitación de NFV (Reproducción tomada de **[16]***)*



Componentes de una Arquitectura NFV

De acuerdo con Huawei Enterprise s.f. e [17] n, se planteó la siguiente arquitectura en la Figura 4. *Infraestructura básica NFV (Reproducción tomada de [18])*, para NFV, detallando sus partes más importantes:

1. **Sistemas de soporte a las operaciones (Operational Support Systems, OSS)**

Orquestador: Controla en su totalidad la arquitectura NFV, encargado gestionar el ciclo de vida de las VNFs.

- **Gestor de VNFs (VNFM):** Cada VNF cuenta un VNF Manager (VNFM) para que gestione sus actividades, asegurando que cumpla con las funciones que se le designan.
- **Gestor de la Infraestructura Virtualizada (VIM):** Gestiona los recursos de procesamiento, almacenamiento y redes. Garantiza que los recursos asignados a la VNF sean necesarios para desplegarse en un entorno virtual.

2. **Sistema de Gestión de Elementos (EMS)**

Gestiona los las VNFs a nivel individual. El EMS se comunica con el VNFM para informar sobre el estado de cada función de red.

3. **VNFs**

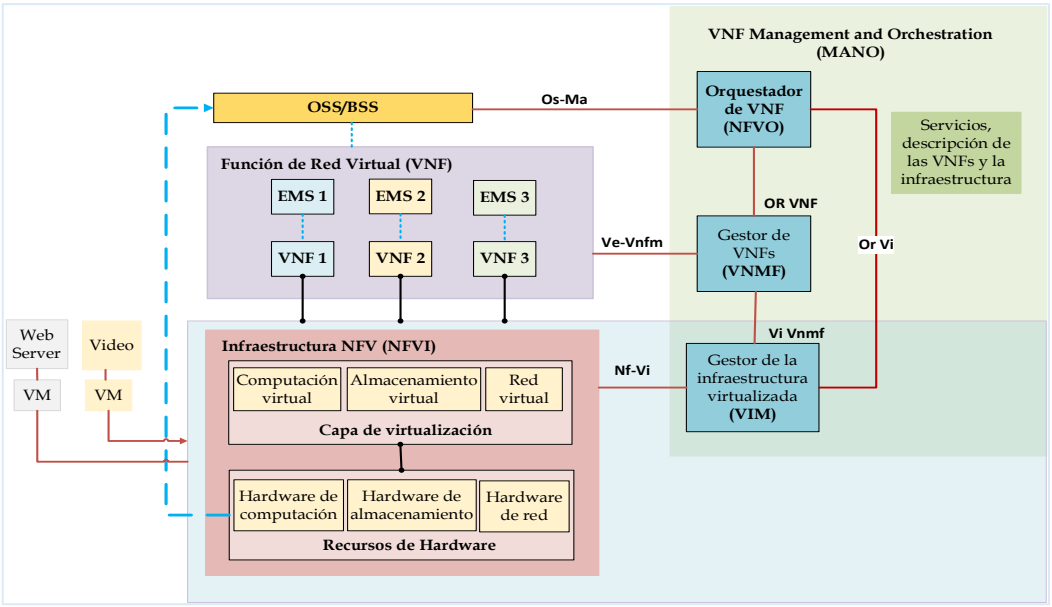
Las VNF son las funciones de red, que normalmente se ejecuten en hardware dedicado, como cortafuegos, equilibradores de carga y enrutadores, pero que ahora se despliegan en software dentro de una infraestructura virtual y requieren de un EMS para operar [18].

4. **Infraestructura NFV (NFVI)**

- **Computación virtual:** Procesa los datos que necesita la VNF para funcionar, similar al procesador de un ordenador.
- **Almacenamiento virtual:** Proporciona espacio de almacenamiento para los datos que necesita la VNF para funcionar, los recursos son asignados dependiendo el equipo físico.
- **Red virtual:** Gestiona la comunicación entre VNFs, permitiéndoles comunicarse y transferir datos.
- **Capa de Virtualización:** Funciona como intermediaria entre los equipos físicos y las funciones virtualizadas, los recursos físicos, como servidores, se presentan a las VNF como recursos virtuales.
- **Recursos de Hardware:** Incluye el equipamiento físico como servidores y equipos de red.

Figura 4.

Infraestructura básica NFV (Reproducción tomada de [18])



1.5.5 Evaluación de la eficiencia de funciones de red

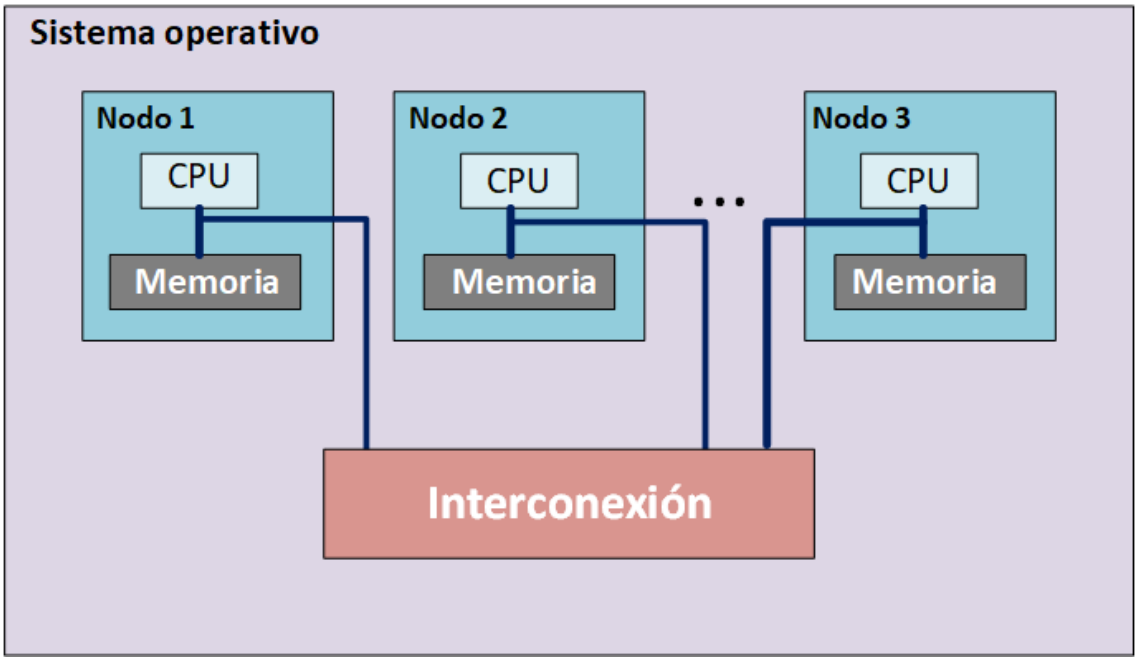
Para evaluar la infraestructura NFV se toman en cuenta diferentes técnicas como: el rendimiento de la red, la optimización de recursos, y la resiliencia del sistema en caso de fallos o anomalías. Intel señala en [19], que con estrategias como el anclaje de CPU y la afinidad NUMA (Non-Uniform Memory Access), que consiste en que cada VM comparte memoria[7], CPU y recursos PCI en el mismo nodo NUMA (Figura 5), la eficiencia de las VNFs mejora significativamente.

Una red eficiente es la cual optimiza la asignación de recursos físicos a funciones específicas, reduce variaciones entre núcleos y mitiga efecto de latencia en tareas críticas.

[7] El empleo de páginas grandes disminuye la carga de gestión de memoria, lo que permite a las VNFs manejar grandes volúmenes de datos más rápido y eficientemente, algo necesario en funciones que trabajen en capa 3, como enrutamiento, y tareas como el análisis de tráfico en entornos de telecomunicaciones [37].

Figura 5.

Infraestructura NUMA (Reproducción tomada de **[19]***)*



Capítulo 2

2.1 Metodología

En este capítulo se evalúan los requerimientos del laboratorio con el objetivo de diseñar e implementar una infraestructura que sea funcional para la gestión de redes PON, que cubra las necesidades identificadas. Con base en los requerimientos, se analizaron diferentes tecnologías para la elección de las soluciones más optimas basándose en criterios como: curva de aprendizaje moderada, código abierto, escalabilidad, adaptabilidad y bajo costo. Se seleccionó NFV como la tecnología de virtualización a emplear, el hipervisor Proxmox VE como servidor principal, las herramientas LibreNMS y OPNsense como herramientas de monitorización, gestión y seguridad de la red, y SNMP como el protocolo principal de comunicación.

Por último, se detallan los aspectos éticos y legales relacionados con la adquisición de software en el sector público, con mayor énfasis a las soluciones de código abierto, justificando de esta forma las elecciones realizadas.

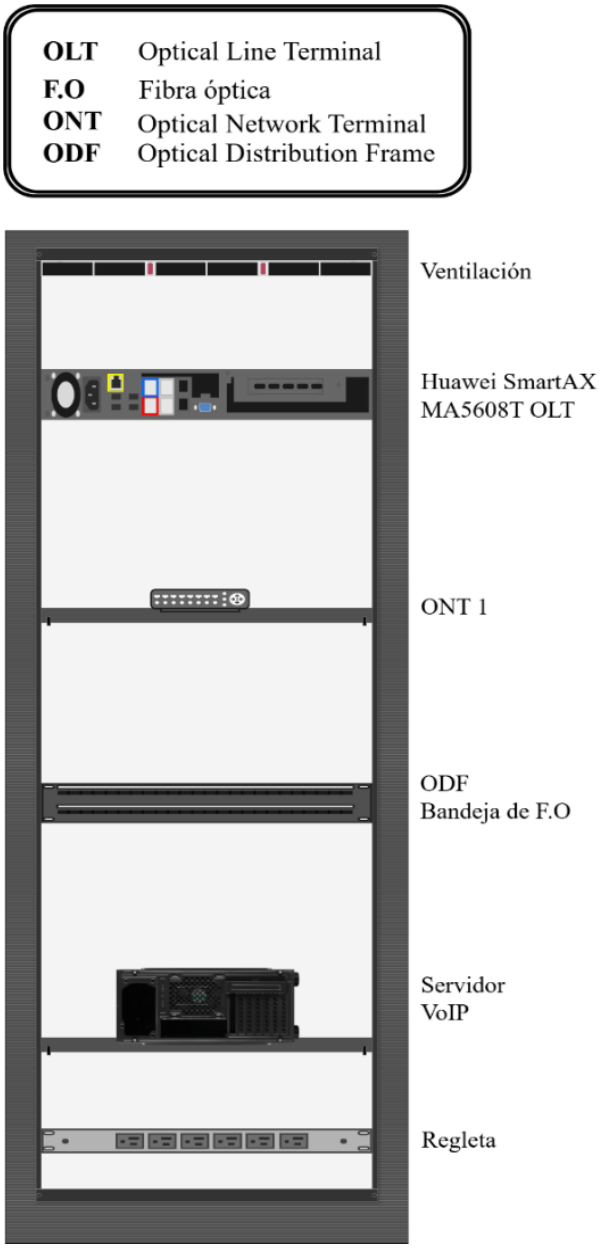
2.2 Análisis de requerimientos

El laboratorio contaba inicialmente con equipos como OLT, ONT y ODF, utilizados para realizar prácticas elementales sobre redes de fibra óptica (FO) (Figura 6). Sin embargo, esta infraestructura al no ser suficiente para cubrir las necesidades identificadas por el cliente se consideró necesario su complementación, para levantar una red capaz de cumplir con los requerimientos establecidos.

Como parte del análisis, se destacó la necesidad de que el sistema sea flexible y capaz de adaptarse a nuevas demandas. También se evaluó el aprovechamiento de recursos físicos para mitigar el impacto económico. Asimismo, se consideró la segmentación de redes para lograr una mayor eficiencia operativa y la supervisión inteligente del tráfico, con el objetivo de permitir una monitorización en tiempo real del desempeño del sistema. Como último requerimiento, se contempló una gestión remota de dispositivos y redes, que permitiese una administración centralizada mediante puertos dedicados de acceso remoto.

Figura 6.

Infraestructura Rack inicial



El análisis detallado de los requerimientos se presenta a continuación:

Flexibilidad en las características de gestión de red

Se centró en la necesidad de que el sistema sea flexible para adaptarse a nuevas demandas, como la incorporación de nuevos servicios o el aumento del tráfico. Para ello, se propone un entorno que permitiera realizar modificaciones, agregar o eliminar recursos de manera ágil, sin comprometer el funcionamiento general.

Aprovechamiento de recursos físicos

Este requerimiento se enfocó en usar eficientemente los recursos físicos o materiales a disposición del laboratorio. Es decir, asignar y compartir el hardware disponible entre diferentes funciones, servicios, o características, esto tuvo especial relevancia en el laboratorio, donde se evitó la compra de equipos dedicados y superó limitantes presupuestarias.

Segmentación de redes para eficiencia operativa

El objetivo de este requerimiento fue organizar y optimizar el tráfico en la red para mejorar su eficiencia y seguridad. Por ello, fue importante implementar una estrategia que agrupase dispositivos en segmentos físicos y lógicos diferentes mediante una gestión out-of-band. Esto optimizó el flujo de datos, redujo la congestión, facilitó la administración remota, y adicionó una capa de seguridad al generar independencia entre las redes [20].

Supervisión inteligente del tráfico de red

Este requerimiento abordó la necesidad de supervisar en tiempo real el tráfico para detectar posibles problemas, monitorear y hacer pruebas que evalúen el rendimiento de la red. Por ello, se priorizó la implementación de herramientas que facilitaran el análisis del flujo de datos, asegurando un rendimiento eficiente y continuo de la red.

Gestión remota de dispositivos y redes

Este requerimiento trató sobre la necesidad de gestionar de manera remota tanto los dispositivos de red como funciones clave de la infraestructura, con la finalidad de facilitar el control, reducir la intervención física y mejorar la eficiencia operativa. Para cumplir esto, se hace uso de herramientas como Wake on Lan para la administración centralizada y remota, y SNMP que recolecta información de recursos de cada dispositivo de red. Haciendo posible una gestión centralizada que al integrarse con la habilitación de puertos de acceso remoto dedicados facilita la administración de toda la red.

2.3 Diseño conceptual

El diseño conceptual del proyecto no solo se centró en la arquitectura y estructura general de la red, sino también en la selección de las tecnologías más convenientes para garantizar que abarquen las necesidades identificadas. En este apartado, se determinaron las tecnologías y criterios utilizados para su elección:

2.3.1 Selección y configuración de componentes

Posterior al análisis de los requerimientos, se evaluó la infraestructura integrada para estimar su alineación con las necesidades del cliente. Este análisis evidenció la necesidad un entorno administrable con servicios y capacidades de red para realizar pruebas y evaluaciones funcionales. Por ello, NFV surgió como una solución inherente por su adaptabilidad a cambios, expansiones futuras y optimización de recursos evitando grandes inversiones en hardware.

Como un concepto arraigado, está la tecnología SDN[8], debido a que el proyecto requiere virtualizar funciones como monitoreo, gestión remota, firewall, enrutamiento, conmutación, gestión de ancho de banda, entre otros, sin necesidad de controlar todo el tráfico de la red, SDN resulta en una solución no apropiada a estos requerimientos.

2.3.2 Selección del modelo de hipervisor

Con NFV, como herramienta de solución identificada, se trabajó en el despliegue de un modelo de hipervisor. Siguiendo el enfoque propuesto por Molina en [21], se planteó la evaluación y comparación de plataformas como Proxmox VE, VMware vSphere, Microsoft Hyper-V, para determinar su adecuación a la solución del proyecto:

[8] **SDN:** Gestiona el tráfico de red de forma centralizada mediante la separación del plano de control y datos [16].

Tabla 1

Comparativa: Proxmox VE, VMware vSphere y Hyper-V

Característica	Proxmox VE	VMware vSphere	Microsoft Hyper-V
Tipo de virtualización	KVM [9]y LXC[10]	VMware ESXi (VM)	Hyper-V (VM)
Licencia	Open Source - GPL	Comercial	Comercial (incluído en Windows Server)
Gestión Centralizada	A través de Proxmox Web GUI	Interfaz web por medio de vSphere Web Client	Mediante MMC [11]y herramientas como SCVMM
Escalabilidad	Alta, cuenta con clústeres de nodos	Alta, con clústeres y vSphere HA	Alta, incluye hasta 64 nodos virtuales en un único clúster
Compatibilidad de Sistema Operativo	Alta con Linux, Windows, BSD, Solaris, AIX	Alta con Windows y Linux	Alta con Windows Server y algunas distribuciones Linux
Contenedores	Soporte nativo para contenedores LXC	Sin nativo, pero soporta Docker a través de plugins	Sin soporte nativo, pero soporta contenedores mediante Windows Server
Integración con redes	Compatible con SDN y administración de recursos de red mediante bridges	Integración con SDN y vSwitch	Integración con redes virtuales y SDN a través de Windows Server

[9] **KVM:** VM basada en el kernel de código abierto que permite crear VM en máquinas de Linux físicas.

[10] **LXC:** Linux Containers, contenedores de código abierto. Crea y ejecuta contenedores en GNU/Linux.

[11] **MMC:** Microsoft Management Console (MMC) es una herramienta que permite a los usuarios avanzados y administradores de sistemas configurar y supervisar el sistema operativo de Microsoft Windows.

Característica	Proxmox VE	VMware vSphere	Microsoft Hyper-V
Monitorización de redes	Integración con herramientas como Zabbix, Nagios, y otros	Integración con vRealize Operations y otros	SCVMM [12]y herramientas de Microsoft
Requisitos de hardware	Bajo, compatible con hardware más accesible	Alto, requiere servidores especializados	Requiere servidores con soporte de hardware para Hyper-V

Se concluyó que Proxmox VE cuenta con el perfil adecuado para cumplir con las necesidades del proyecto. Al ser un software de codigo abierto que trabaja bajo licencia GPL libre de costos, ofreció una relación costo-beneficio favorable, ajustándose a las limitaciones presupuestarias anteriormente mencionadas. Además, características como su escalabilidad, tipo de virtualización y adaptabilidad, fueron destacadas. Por último, una característica importante es que sus bajos requisitos de hardware inicial lo hicieron accesible, incluso en infraestructuras con recursos limitados, como la planteada en este proyecto, en comparación con otras alternativas comerciales como VMware vSphere.

2.3.3 Selección de software para la gestión y seguridad de redes

Se evaluaron dos softwares que estuvieran alineados al análisis de requerimientos. En este contexto, se compararon dos soluciones de firewall de código abierto: pfSense y OPNsense. De acuerdo con el sitio WunderTech en [22], se destacó que OPNsense cuenta con cierta facilidad de configuración, interfaz más intuitiva y actualizaciones más eficientes. Además, considerando reducir costos y la preferencia por soluciones comunitarias, junto con su aplicabilidad en redes no extensas, OPNsense fue seleccionado por su facilidad de configuración en entornos pequeños.

[12] **SCVMM:** Integración con System Center Virtual Machine Manager, habilitado para Azure Arc.

Tabla 2

Comparativa entre pfSense y OPNsense

Característica	pfSense	OPNsense
Origen	Desarrollado por M0n0wall, basado en FreeBSD.	Fork de pfSense, basado también en FreeBSD.
Licencia	Licencia BSD (Open Source).	
Interfaz de usuario	Técnica, menos intuitiva y robusta.	Moderna, más amigable y fácil de usar.
Rendimiento	Ideal para redes grandes y complejas.	Ideal para redes pequeñas y medianas.
Funciones de seguridad	Firewall avanzado cuenta con soporte para IPsec y OpenVPN.	Firewall avanzado[13].
Plugins/Extensiones	Amplia variedad de plugins, los cuales requieren configuración adicional.	Soporte para plugins, cuenta con funcionalidades nativas como Proxy transparente y HAProxy. [14]
Monitoreo de red	Cuenta con gráficos básicos, se requiere plugins adicionales.	Gráficos interactivos, cuenta con monitoreo en tiempo real integrados.
Costo	Gratuito, con opciones de soporte comercial.	

[13] OPNsense cuenta con soporte para IPsec, OpenVPN y WireGuard integrado.

[14] **HAProxy:** Equilibrador de carga tcp o http de código abierto.

2.3.4 Selección de software de monitorización de redes

Se optó por utilizar LibreNMS como solución para software de monitoreo por diversas razones, entre las que se tiene su interfaz amigable, facilidad de configuración y adecuada integración con protocolos de comunicación activa como SNMP. Asimismo, este cuenta con un sistema de alertas flexible y alta capacidad de escalabilidad, lo cual lo posiciona como una alternativa óptima a integrar en el proyecto. De acuerdo con diversas comparativas [23] [24] y tomando como referencia la información de los sitios oficiales [25] [14], se resaltan las principales diferencias entre ambos softwares simplificando la visualización de sus fortalezas y limitaciones en el contexto del proyecto:

Tabla 3

Comparativa: LibreNMS y Zabbix[15]

Característica	LibreNMS	Zabbix
Tipo de Software	De monitorización basado en código abierto	De monitorización basado en código abierto con servicios pagados si se requiere soporte avanzado
Facilidad de uso	Interfaz intuitiva, facilidad de configuración. Ideal para implementaciones rápidas y no tan complejas.	Interfaz más técnica y avanzada, con mayor curva de aprendizaje
Capacidad de monitoreo	Diseñado para monitoreo de dispositivos e infraestructuras de red con integración de SNMP	Incluye monitoreo de servidores, dispositivos de red, aplicaciones, etc
Escalabilidad	Buena escalabilidad, adecuado para redes medianas a grandes	Escalable, adecuado para redes grandes

[15] Zabbix propone una estructura más comercial en torno al soporte, mientras que LibreNMS se mantiene como una solución completamente comunitaria.

Característica	LibreNMS	Zabbix
Integración con otros sistemas	Integración eficaz con herramientas como RANCID [16]y Collectd[17], mejorando sus capacidades de monitoreo.	Amplias opciones de integración, cuenta con una API segura que facilita la integración con diversas aplicaciones de terceros.
Documentación y soporte	Cuenta con una comunidad dedicada. Soporte por lo general en línea y documentación web.	Extensa documentación y gran comunidad. Con servicios de soporte comercial

2.3.5 Protocolo para gestión remota e interconexión

Fue indispensable garantizar la interoperabilidad entre los dispositivos, las herramientas seleccionadas trabajan con SNMP que permite la gestión centralizada de la red a través de tareas de supervisión y recolección de datos en tiempo real. A continuación, se presenta el detalle de dicho análisis [26]:

Tabla 4.

Características de Protocolo SNMP

Característica	SNMP
Función	Supervisión y monitoreo de dispositivos de red
Arquitectura	Gestor-agente
Uso Principal	Supervisión del estado y rendimiento de dispositivos
Seguridad	SNMPv3 incluye autenticación y cifrado

SNMP [18]resultó ideal para recolectar métricas sobre el rendimiento en tiempo real de la red, incluyendo estados de tráfico, uso de ancho de banda, etc.

[16] **RANCID:** Encargado de la gestión de configuraciones.
[17] **Collectd:** Encargado de recopilar métricas.
[18] SNMP integra un modelo GET/SET, ideal para tareas de supervisión y monitoreo.

2.4 Sistema propuesto

2.4.1 Definición de la topología lógica

En la Figura 7, se presenta el sistema propuesto el cual se estructuró en tres áreas funcionales para facilitar la visibilidad e identificación de las funciones y servicios virtualizados.

A continuación, se describe cada una de ellas:

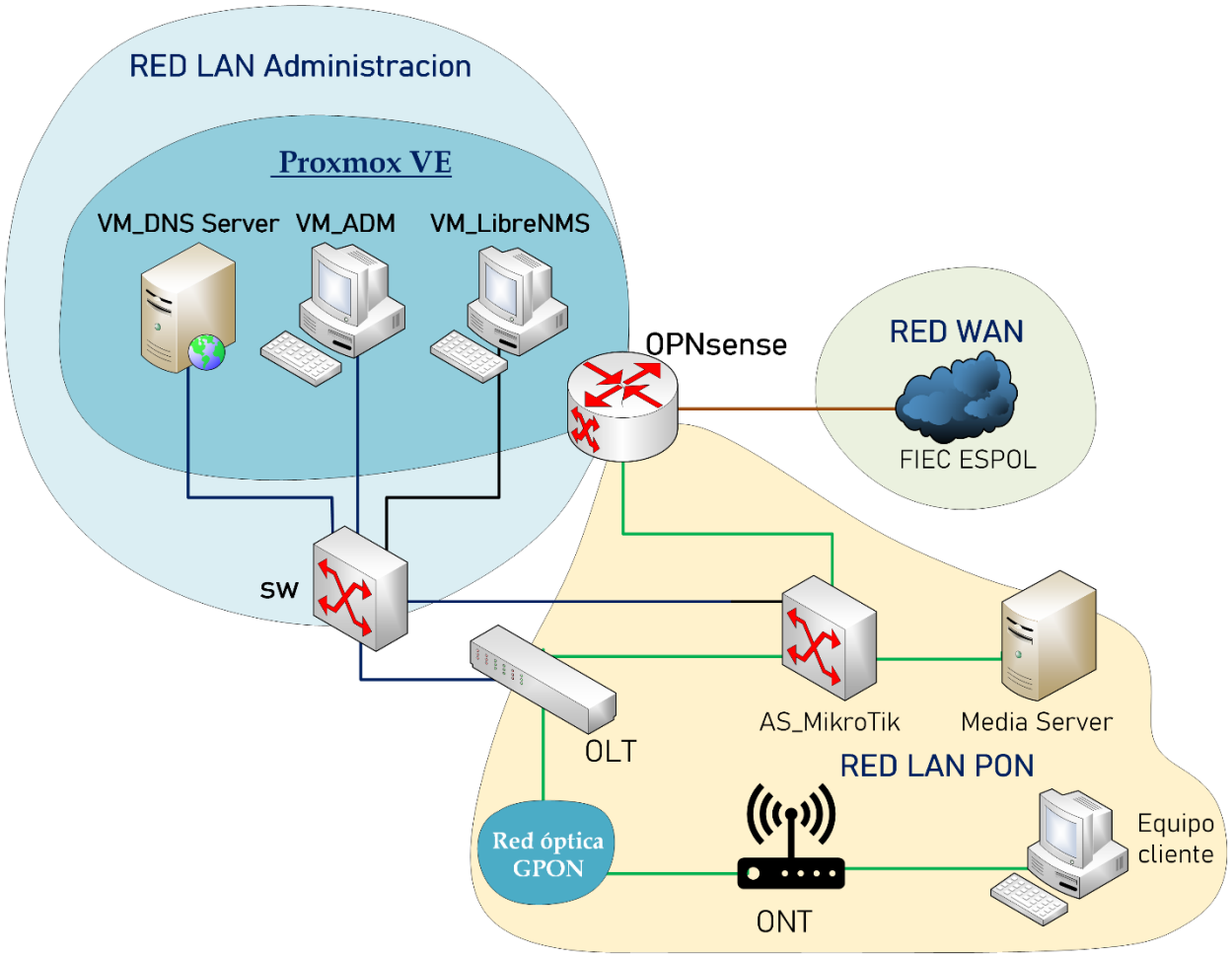
a) RED LAN Administración: En esta área de la red, se presentó la conmutación de datos con privilegios de administrador, que tiene como finalidad manejar la red. Se configuró también una VM denominada VM_LibreNMS, el cual asigna y monitorea las redes. Esta área conecta a un dispositivo central que tiene integrado el Proxmox server que cumple la función de entrono de virtualización, encargado de gestionar el tráfico de la red y conectar de manera centralizada las demás funciones y servicios de red.

b) RED WAN: Esta área conectó la red del laboratorio con la red externa de la FIEC, proporcionando acceso a servicios externos (internet) y acceso al entorno de red de la institución. Se instaló un Switch denominado AS_MikroTik el cual distribuiría el tráfico por la red GPON para redirigirlo al servidor multimedia, en función de las necesidades del cliente.

c) Red LAN PON: Esta es la red PON que se extiende desde el OLT y equipo ONT del cliente. Esta fue la red de mayor importancia, ya que es aquí donde se generó el mayor tráfico de datos, y se monitoreó la conmutación, donde se obtuvieron los datos necesarios para la evaluación del rendimiento y las pruebas de testbed.

Figura 7.

Diseño de infraestructura lógica/física



2.4.2 Definición de la Arquitectura NFV

La Arquitectura NFV en este proyecto se definió de tal forma que permita virtualizar funciones clave de red tradicionalmente implementadas en hardware físico, integrándolas en un entorno virtualizado gestionado por Proxmox. Estas funciones incluyeron el enrutamiento, análisis de tráfico y monitoreo, optimizando la administración y supervisión de la red GPON.

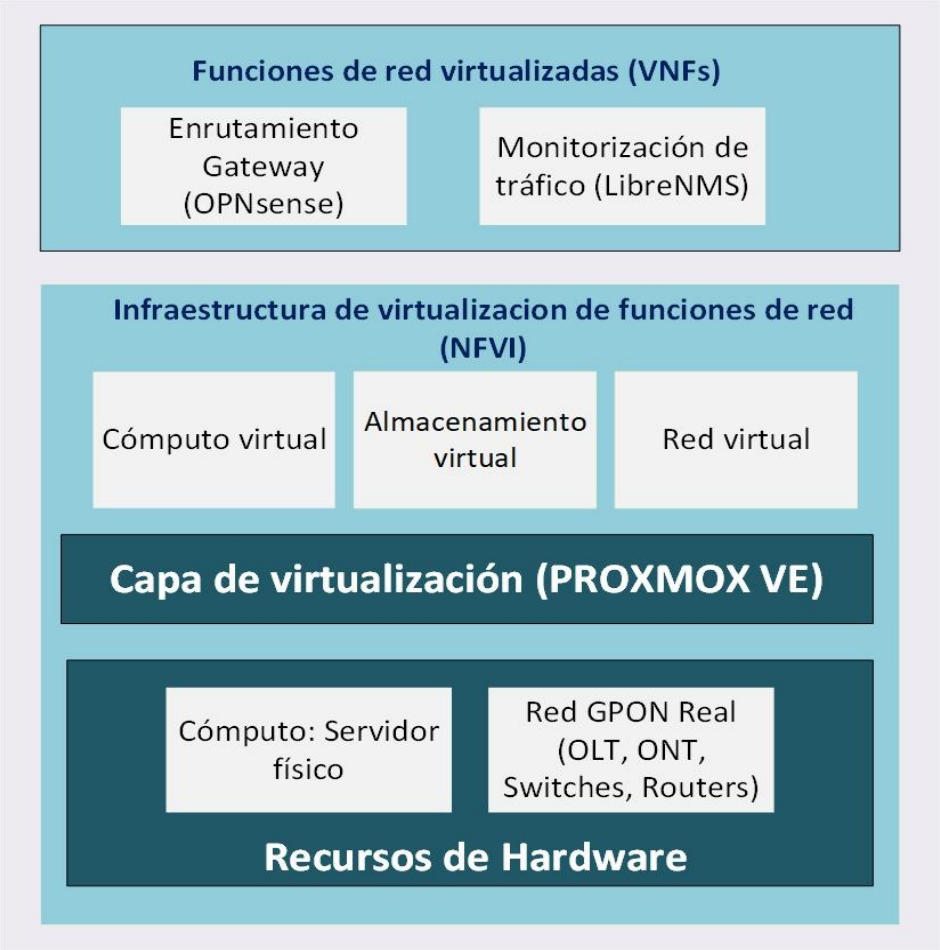
Proxmox como plataforma de virtualización:

El hipervisor Proxmox se utilizó para alojar las VNFs, configuradas como VMs independientes, asegurando una arquitectura modular y flexible, donde es posible realizar expansiones o cambios según la necesidad del laboratorio. Aquí se gestionó los recursos físicos del servidor, como CPU y memoria, asignándolos directamente a las VMs. En cuanto a

conectividad, en el hipervisor se configuraron puentes de red (bridges) para conectar los adaptadores de red físicos del equipo que funciona como servidor a las VMs, garantizando que el tráfico entrante desde la red GPON pudiera ser procesado por las VNFs de manera eficiente.

Figura 8

Arquitectura NFV aplicada a la gestión de redes PON



2.5 Consideraciones Éticas y Legales

Consideraciones sobre la adquisición de software en el sector público

Para el desarrollo de este proyecto, se estudiaron, además, las disposiciones establecidas en el Decreto Ejecutivo No. 1425, que regula la adquisición de software en el sector público ecuatoriano [27].

Se detalla a continuación, los artículos relacionados con las actividades que se han ido desarrollando en el entorno de virtualización:

Artículo 1: Orden de prelación en la adquisición de software

El artículo 1 establece que *"las entidades contratantes del sector público deberán preferir la adquisición de software de código abierto con importante componente de valor agregado ecuatoriano [...]."*

En otras palabras, establece que es aconsejable priorizar el uso de herramientas de código abierto, -para este caso específico, se utiliza Proxmox y OPNsense- que respondan al reto de la sostenibilidad tecnológica. Además, si se desarrollan localmente adaptaciones o configuraciones específicas, se podría añadir un componente de valor ecuatoriano.

Artículo 2: Justificación de la selección de software

El artículo 2 indica que "*toda adquisición de software deberá estar debidamente justificada, especialmente si no se ajusta al orden de prelación establecido en el artículo anterior*".

Esto significa, que en caso de requerir herramientas que no sean de código libre, es necesario incluir una justificación técnica convincente, detallando el por qué las opciones de mayor prioridad (software libre) no son adecuadas para la tarea en cuestión.

Artículo 3: Autorización del MINTEL para excepciones

Según el artículo 3, "*las adquisiciones de software que no cumplan con el orden de prelación deberán contar con la autorización previa del Ministerio de Telecomunicaciones y de la Sociedad de la Información. En el caso de no ser posible la adquisición o desarrollo de software de código abierto [...], se procederá con el segundo orden de clase de prelación, previo a la autorización de Ministerio de Telecomunicaciones y Sociedad de la Información*".

En este sentido, cualquier herramienta internacional tomada en cuenta para el proyecto debe ser evaluado y aprobado por el MINTEL para asegurar que las excepciones estén en línea con los intereses tecnológicos del país.

Capítulo 3

3.1 Resultados y análisis

En este capítulo se abordará la implementación de las herramientas utilizadas para el levantamiento de la infraestructura virtualizada basada en funciones de red, implementada en el laboratorio de Redes de Telecomunicaciones.

Se explicará el despliegue, instalación y breve configuración de las herramientas utilizadas, como son: Proxmox V, el entorno de virtualización; OPNsense y LibreNMS, las herramientas que trabajan como funciones de red. Junto con los servicios habilitados en cada una de estas funciones, que permitieron supervisar la red y garantizar su eficiencia en la administración, centralización y capacidad de monitoreo. Se describirán los cambios realizados tanto a la infraestructura física como virtual, para conseguir una red robusta, escalable y segura para la gestión de redes en un contexto educativo.

El capítulo también incluye un análisis de los resultados obtenidos, en donde se evalúan métricas como el rendimiento de los recursos asignados a las VMs, la confiabilidad del tráfico de red, los hosts asociados en el tráfico y el monitoreo proactivo mediante herramientas como LibreNMS y Ntopng.

Por último, se realizan pruebas reales en la red para validad que cumpla con la efectividad del proyecto, estableciendo, además, servicios que permitan el autodescubrimiento de los equipos, demostrando cómo el diseño de la infraestructura virtualizada satisface las necesidades del laboratorio, optimizando la administración y el desempeño de la red PON.

3.2 Levantamiento de la infraestructura física

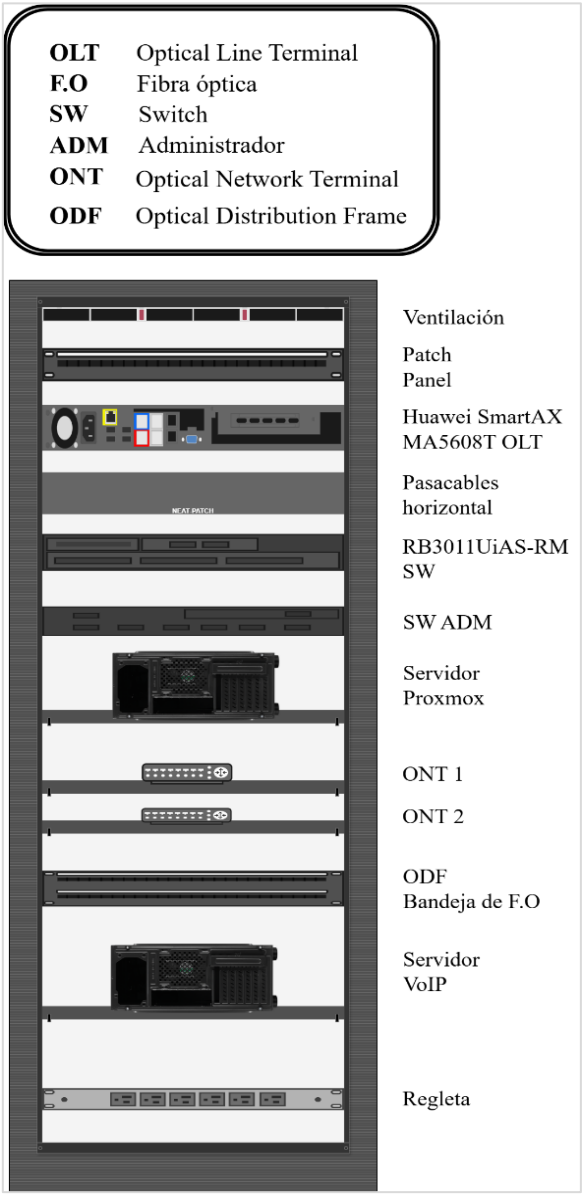
En la Figura 1, se representó la infraestructura física inicial con la que se contaba en el rack del laboratorio. Sin embargo, esta al no cumplir con las necesidades del cliente, se optó por complementarla, agregando nuevos equipos (

Apéndice A: lista de equipos iniciales y agregados), para lograr una red con mayor robustez capaz de implementar el sistema de virtualización. Estos cambios se orientaron a aprovechar los

recursos disponibles en el laboratorio y optimizar su desempeño para cumplir con las expectativas del cliente (Figura 9).

Figura 9

Infraestructura Rack final



3.3 Despliegue entorno de virtualización Proxmox VE

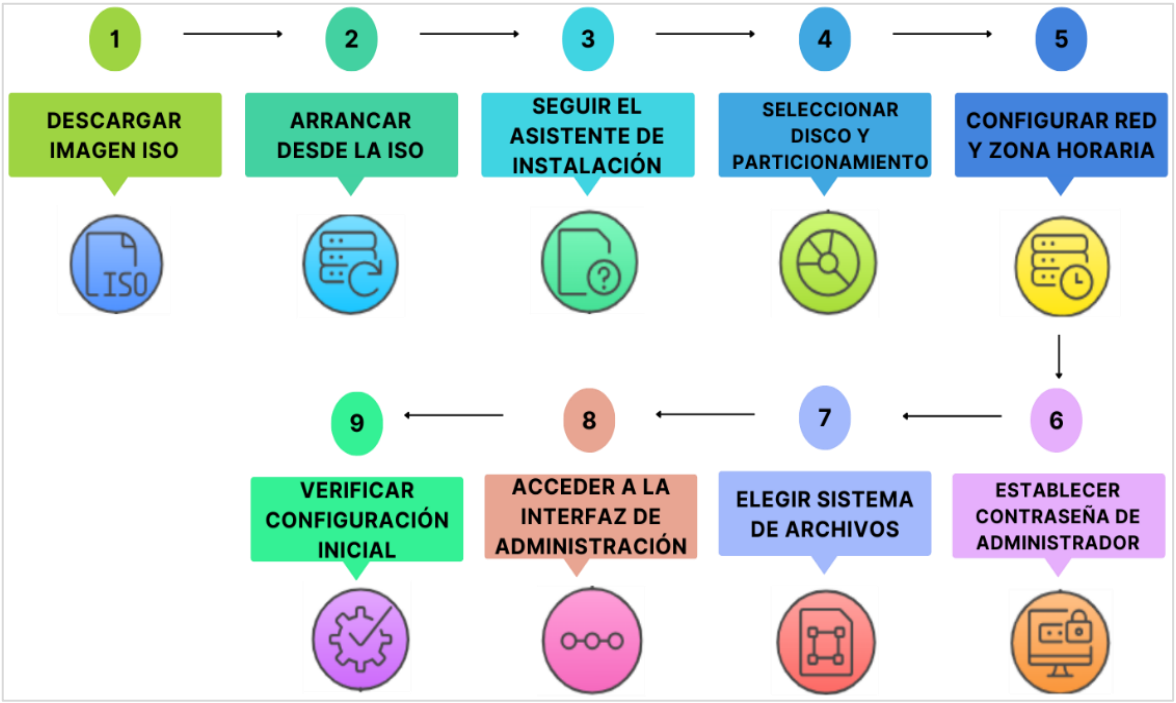
El despliegue del proyecto abarca la instalación del software, configuración de los recursos físicos y virtuales, así como la preparación del sistema para integrar servicios. De tal manera, que sea posible optimizar tanto el rendimiento como la administración de la red.

Como se detalla en la Figura 10, el despliegue de Proxmox VE comienza con la descarga de su imagen ISO oficial, que cuenta con un sistema Debian de 64 bits. Desde el BIOS del servidor físico donde se instalará Proxmox se inicia la imagen ISO descargada, y se siguen los pasos que indica el asistente de instalación, esta instalación corresponde a una estándar, la cual es recomendada para la mayoría de los usuarios.

Por consiguiente, se selecciona el disco, los particionamientos para el sistema, se ajustan parámetros de red y zona horaria, como un proceso de instalación normal. El instalador solicitara una clave de acceso para el usuario de administración por defecto “root”, que se configura en este paso.

Figura 10

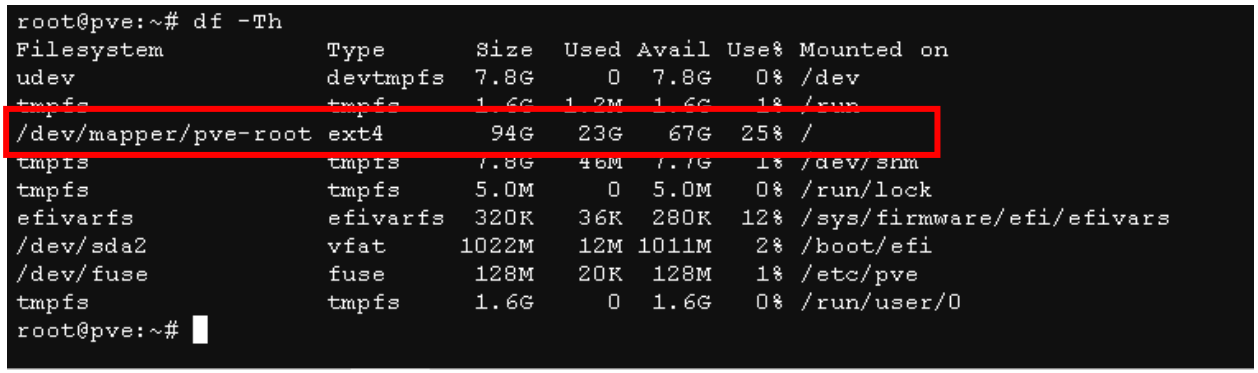
Proceso de instalación de Proxmox VE



Se selecciona el sistema de archivos, sea ext4 (equipos con recursos limitados sin necesidades avanzadas) o ZFS (para servidores con suficiente RAM de al menos 8 GB) dependiendo las necesidades del usuario, en este caso se seleccionó ext4.

Figura 11

Sistema de archivos ext34



Por último, es posible acceder a la interfaz de administración desde un navegador web apuntando al puerto 8006 (Figura 12). Existe también la instalación para usuarios avanzados, donde se ejecuta el instalador Proxmox sobre un sistema Debian existente, aunque esto requiere conocimientos técnicos adicionales [28].

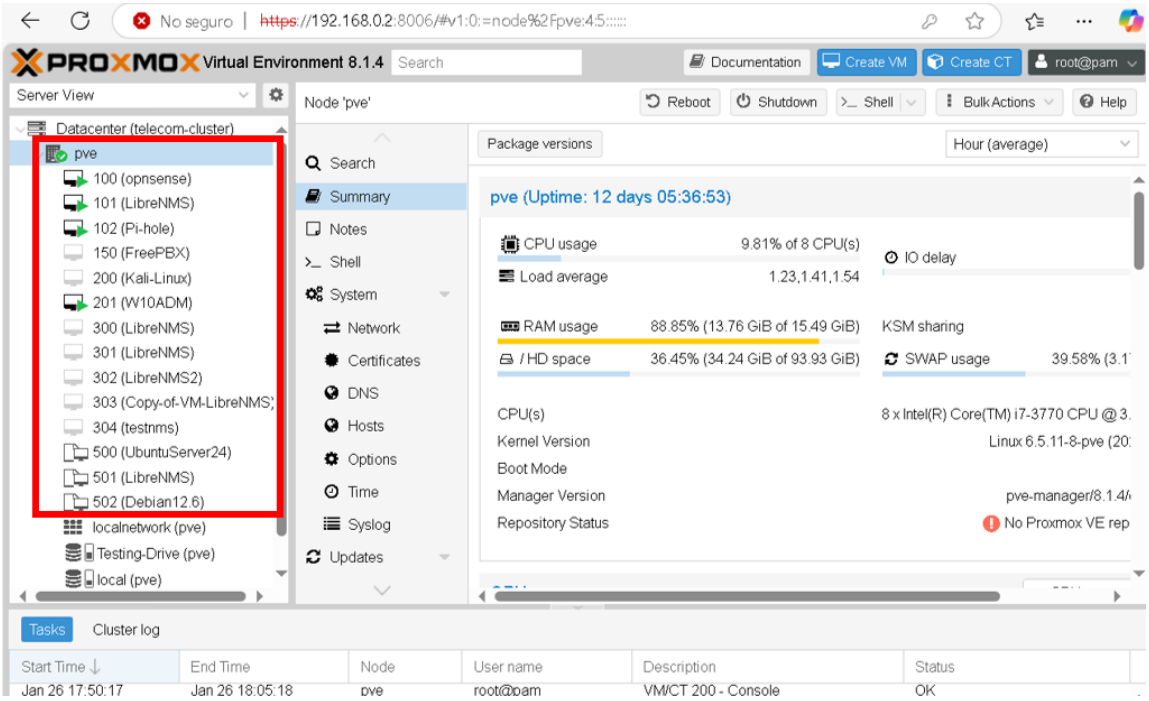
3.3.1 *Análisis de la interfaz y configuración de VMs*

Se presenta la interfaz de administración del hipervisor Proxmox VE, donde es posible la creación y gestión de las VMs -que se encuentran enmarcadas en el cuadro rojo-, que alojan los servicios y funciones necesarias para el proyecto. A continuación, se explican las funcionalidades virtualizadas que se han configurado dentro del nodo “pve”:

- **VM OPNsense:** Configurada como gateway y enrutador con servicios de monitoreo.
- **VM LibreNMS:** Cuenta con varias instancias, utilizadas para el monitoreo de redes. Sus direcciones IP asignadas son 101, 300, 301, 302.
- **VM W10ADM:** Máquina de administración y pruebas de software con asignación 201.

Figura 12

Interfaz GUI Proxmox VE



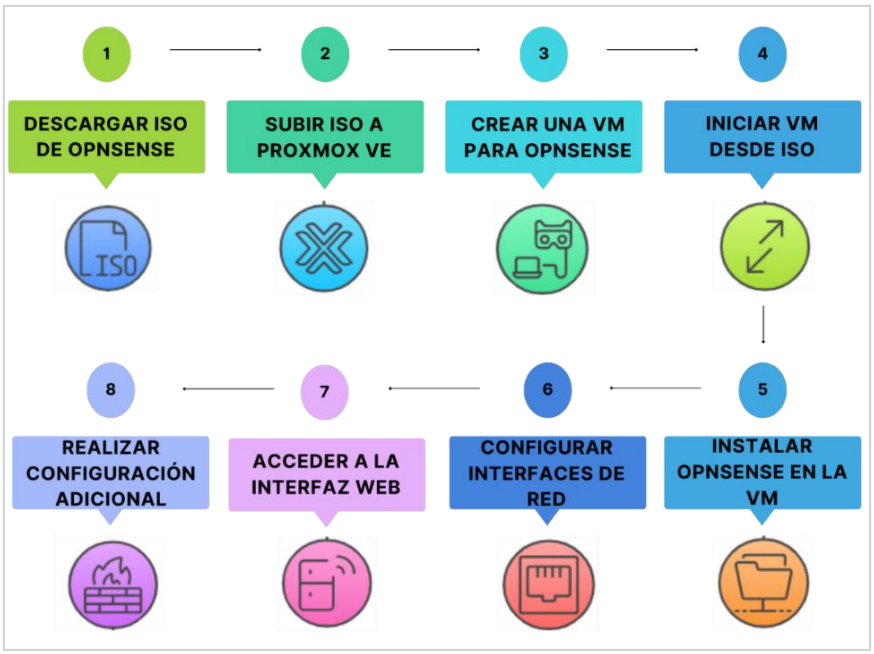
3.4 Despliegue y configuración de OPNsense

La integración de OPNsense en Proxmox VE, tal como se detalla en la Figura 13, inicia con la descarga de la ISO oficial en el repositorio de Proxmox. Se crea una VM con la configuración de los recursos de hardware, las interfaces de red para WAN y LAN y la selección de la ISO como método de arranque. Una vez arrancada la VM, se procede con la instalación de OPNsense siguiendo las instrucciones del instalador. Por último, se configuran las interfaces de red, tanto de la dirección de acceso a la WAN y la dirección asignada a la interfaz para acceso a OPNsense.

Se procede con las pruebas de conectividad, para validar acceso a la interfaz web desde la LAN para realizar las configuraciones pertinentes (Apéndice B: pruebas de conectividad), completando de esta manera, la integración del cortafuegos en el entorno virtualizado [29] [30].

Figura 13

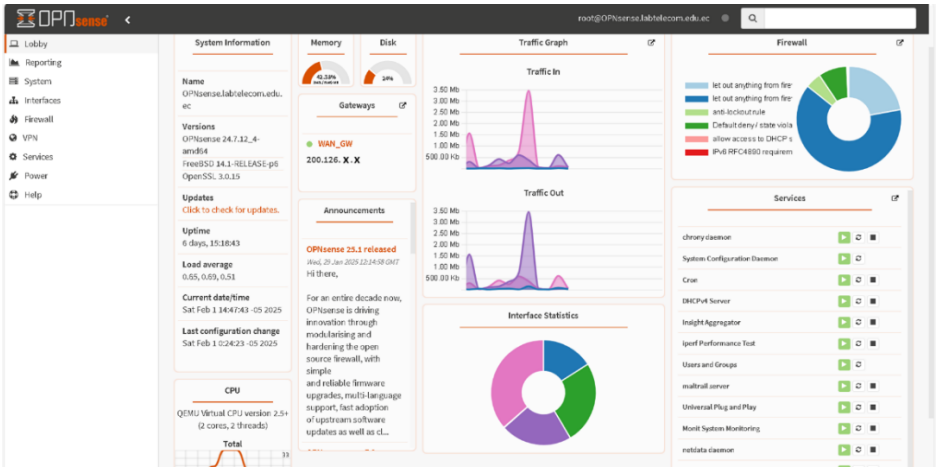
Fases del despliegue de OPNsense



En la Figura 14, se puede visualizar el dashboard principal de OPNsense, que proporciona información como: versión instalada, nombre de los dispositivos conectados, tiempo de actividad, actualizaciones disponibles, estadísticas de uso de memoria y disco, estado de los gateway configurados, gráficas del tráfico entre interfaces, reglas de firewall configuradas y lista de los servicios configurados en estado activo o inactivo, permitiendo su gestión directa desde el panel, de manera más rápida y eficiente.

Figura 14

Dashboard principal OPNsense

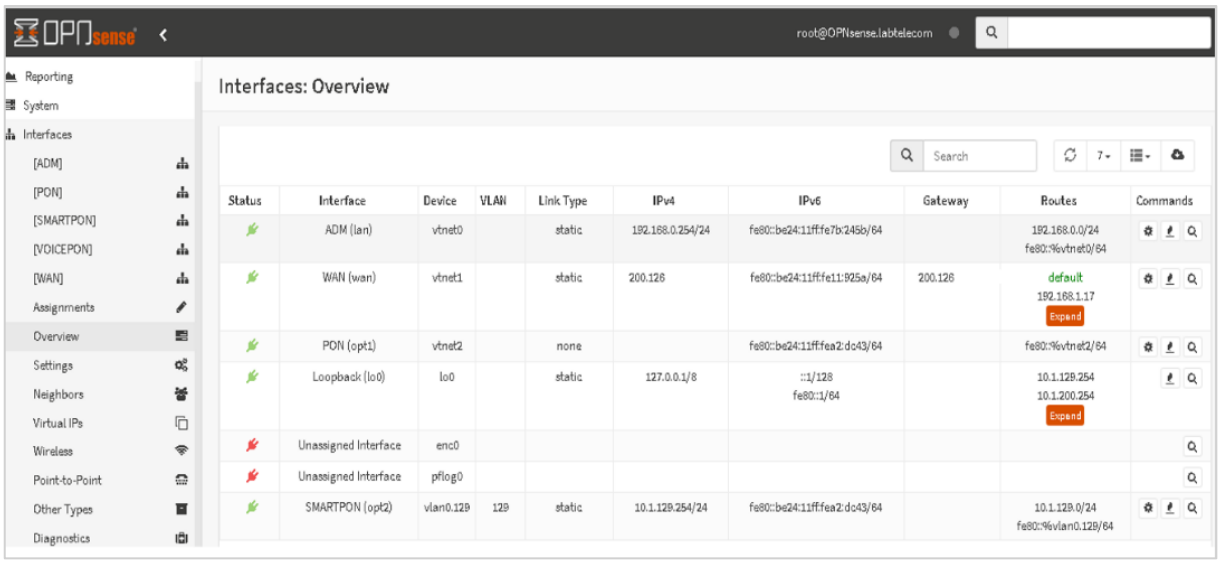


3.4.1 *Enrutamiento y gestión de tráfico*

La Figura 15, se muestra la sección Interfaces: Overview en la configuración de OPNsense, donde a cada interfaz configurada se le asignó un adaptador de red virtual asociado a un dispositivo específico, identificado por nombre y dirección MAC. Además, se han configurado las direcciones IP y la segmentación de red para crear las VLANs de la red PON [31].

Figura 15

Interfaces configuradas en OPNsense



Desde OPNsense también se pueden realizar diagnósticos de conectividad, como el envío de tramas, pings, captura de paquetes, y consulta de la tabla ARP para mapear direcciones IP a direcciones MAC [32]. Con el objetivo de facilitar la comunicación entre dispositivos y permitir actividades de troubleshooting [19] de manera eficiente (Figura 16) (Figura 17).

[19] **Troubleshooting:** Consiste en la capacidad de diagnosticar y resolver de manera efectiva un incidente.

Figura 16

Tabla ARP

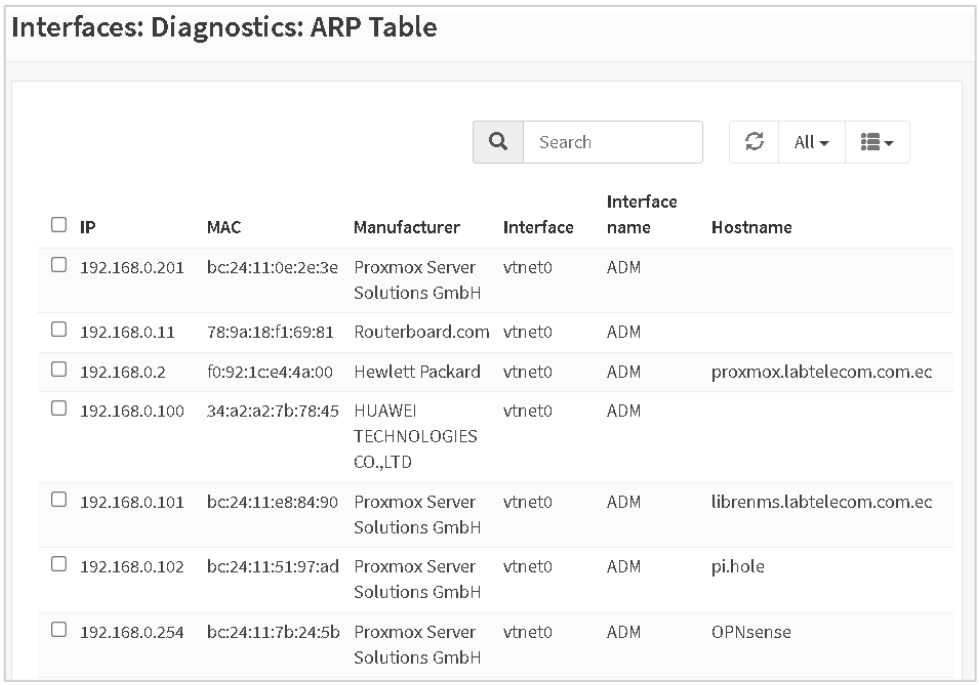
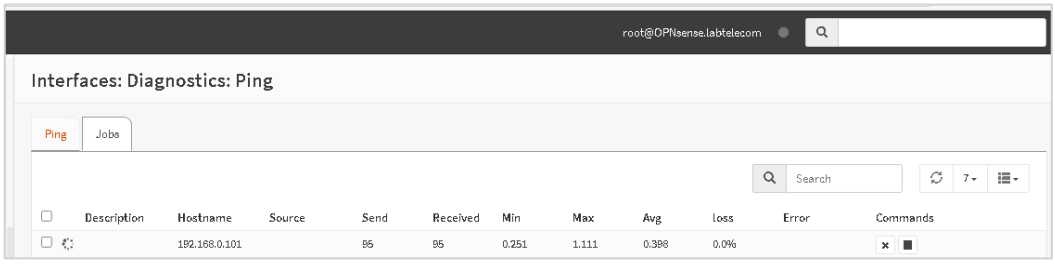


Figura 17

Pruebas de ping en OPNsense hacia LibreNMS



3.4.2 Servicios habilitados

Se describirán en detalle las funcionalidades, puertos utilizados y principales características de cada uno de los servicios configurados en OPNsense, destacando su importancia dentro de la infraestructura implementada:

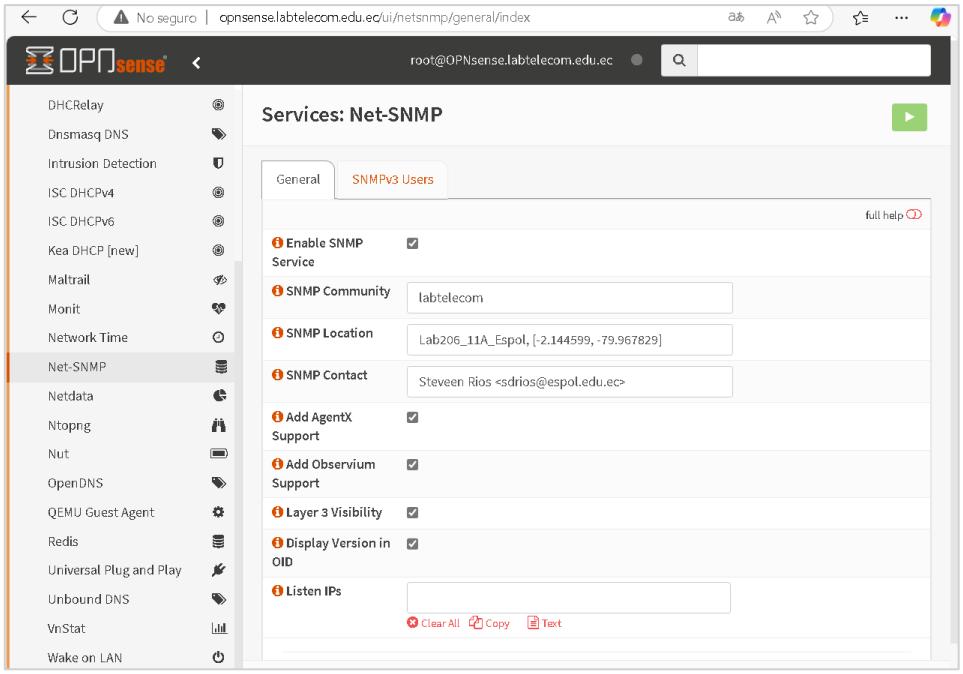
Habilitación SNMP

OPNsense es compatible con SNMP v3 y v2, incluyendo autenticación y cifrado, para garantizar la seguridad en la transmisión de datos. Hace posible monitorear y gestionar dispositivos en la red, además de, recopilar métricas de rendimiento y estado de los equipos. En este caso, se

ha configurado una comunidad SNMP denominada “labtelecom”, como se puede observar a continuación:

Figura 18

Servicio habilitado SNMP



Si se habilita esta herramienta complementaria (Net-SNMP), es posible enviar datos como el de la Figura 19, a sistemas externos de monitoreo, como LibreNMS, PRTG, o Zabbix, para una gestión centralizada de múltiples dispositivos. En este caso, OPNsense actúa como un agente SNMP, retransmitiendo estadísticas de tráfico, estado de la interfaz y otros datos de rendimiento a un sistema externo que interpreta esta información.

De tal forma, como se muestra a continuación, es posible verificar tráfico IP y paquetes enviados desde cada una de las interfaces configuradas, además de tomar métricas de los recursos consumidos como memoria del CPU y estado del sistema desde OPNsense.

Figura 19

Paquetes enviados en la interfaz WAN desde OPNsense

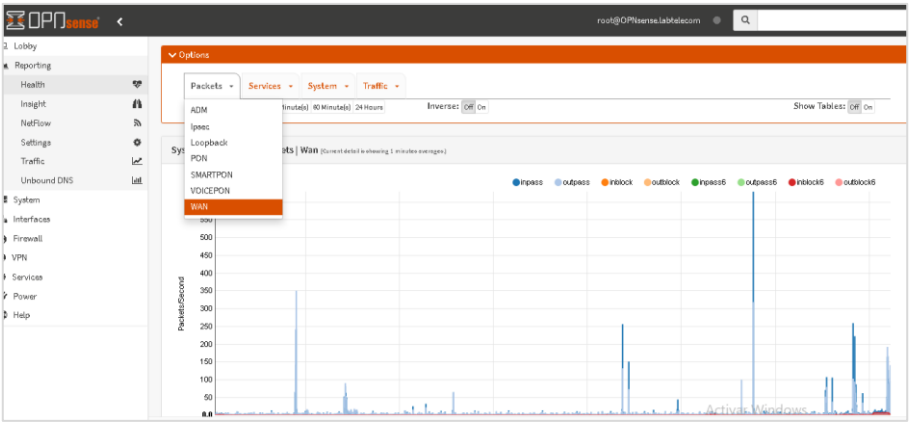


Figura 20

Tráfico IP en la interfaz WAN desde OPNsense

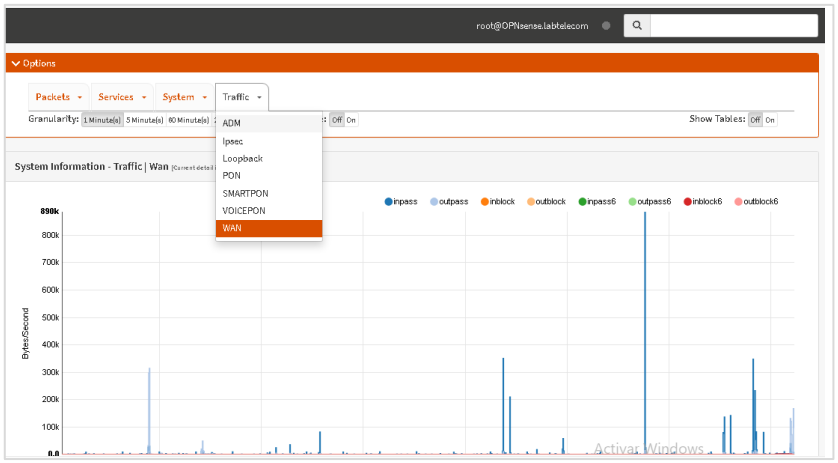


Figura 21

Estado del sistema

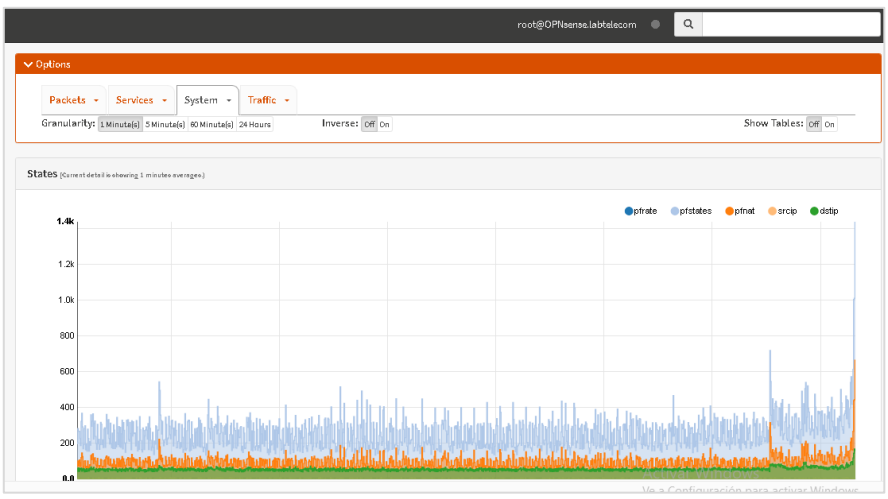
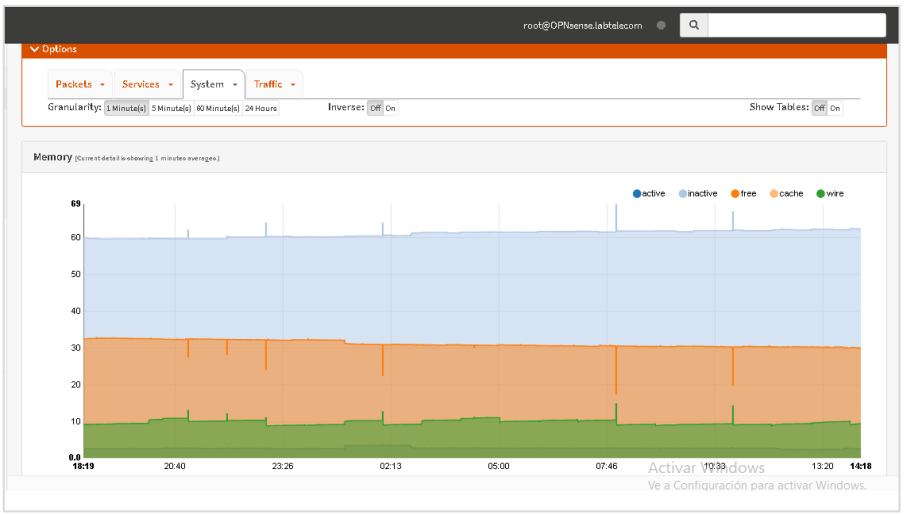


Figura 22

Memoria consumida por el sistema general

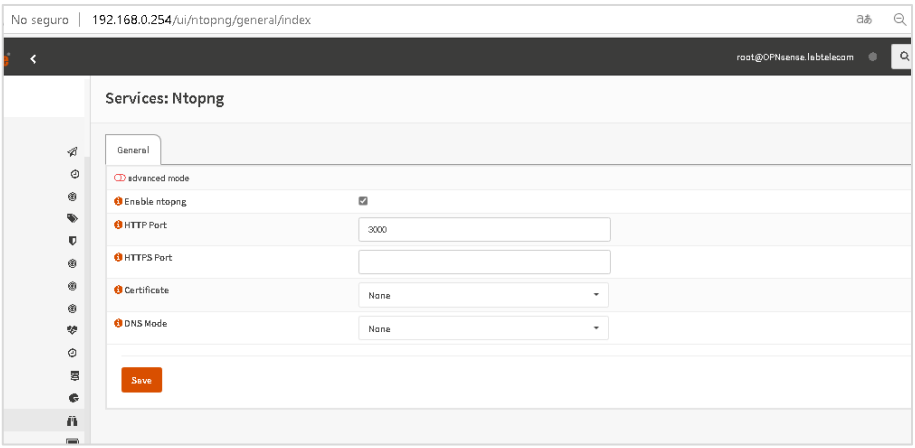


Habilitación de plugin Ntopng

Ntopng se encarga de proporcionar información en tiempo real del tráfico de red. Es capaz de identificar los hosts de mayor actividad, protocolos utilizados y detectar posibles anomalías. Este servicio se habilitó en OPNsense mediante el puerto 3000, accesible a través de la interfaz web, pero también analiza todo el tráfico a través de las interfaces monitorizadas.

Figura 23

Servicio habilitado Ntopng



Aunque en esta sección se describe la habilitación del servicio Ntopng, en la sección 3.4.2 se realizará una evaluación de las métricas analizadas mediante el monitoreo que este realiza, como

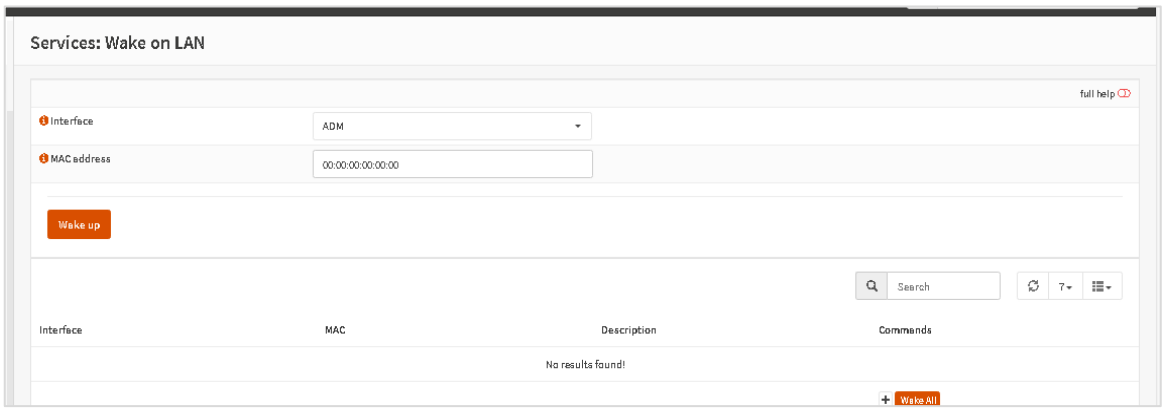
el tráfico, la localización de hosts, los estados de interfaces y equipos, entre otros, tal manera, que sea posible validar la efectividad del proyecto.

Wake on LAN (WoL): Encendido Remoto

Wake on Lan o por sus sigas WoL corresponde a un estándar de redes Ethernet y tiene como finalidad encender o activar una computadora de red configurada correctamente mediante un mensaje de red [33]. Consiste en enviar un "paquete mágico", que no es un más que un prefijo de sincronización FF en hexadecimal equivalente a 11111111 en binario, a los dispositivos conectados, por lo que el paquete se transmite a todos los dispositivos en la red local LAN, el dispositivo objetivo lo detecta y procede a encenderse.

Figura 24

Servicio Wake on Lan



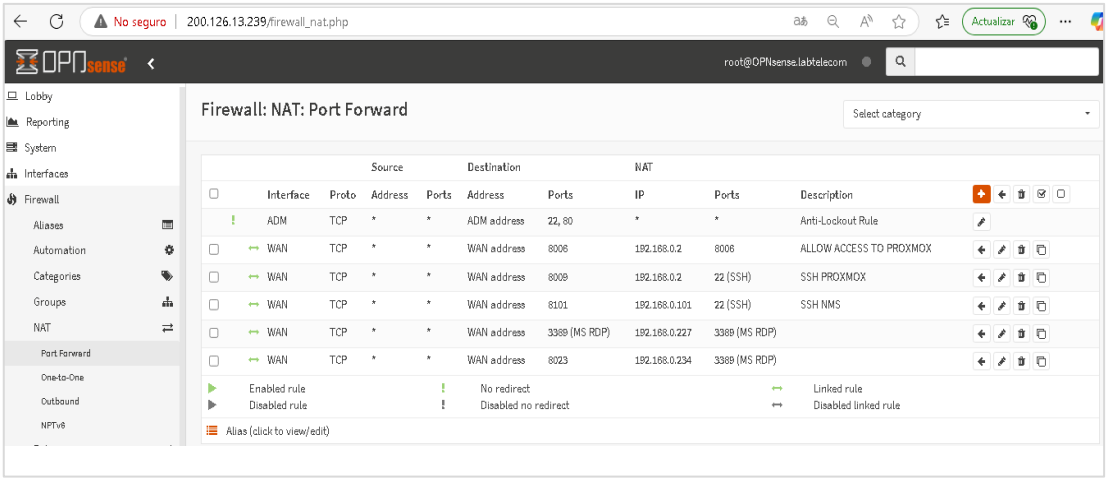
OPNsense tiene integrado el servicio WoL, para ello es necesario especificar la interfaz de red y la direccion MAC del dispositivo que debe encenderse remotamente. Además, que el dispositivo objetivo debe estar configurado para admitir WoL en su tarjeta de red y BIOS.

Configuración de Firewall

La primera línea de defensa en la red es el Firewall, en el caso de OPNsense debido a la necesidad de acceder a servicios específicos como Proxmox o el entorno de administración, se configuraron reglas NAT para reenvío de puertos, con la finalidad de facilitar el acceso a estos servicios, tal como se observa en la Figura 25.

Figura 25

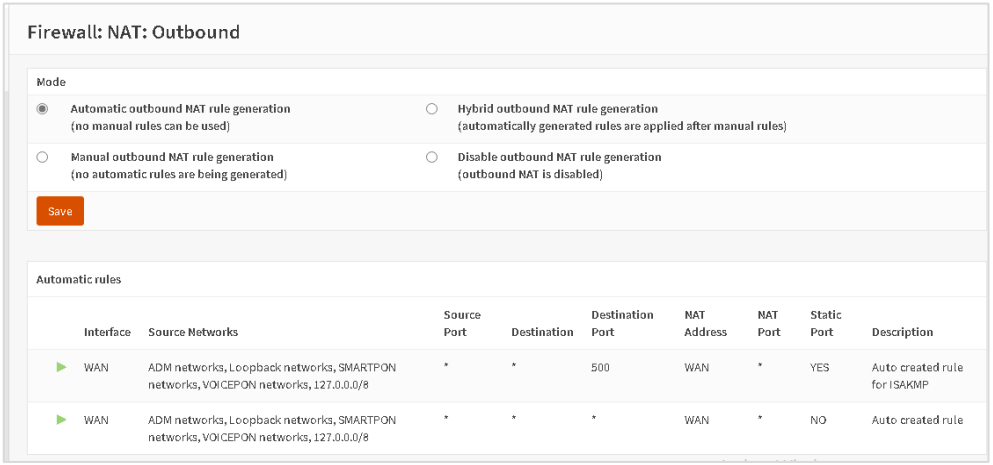
Reglas de Port Forward configuradas en el firewall OPNsense



La Figura 26, muestra la interfaz de configuración de las reglas NAT: Outbound en el firewall de OPNsense. En este caso, el modo seleccionado es “Automático”, por lo que el sistema, detecta las interfaces que se han configurado, WAN y LAN, y crea reglas básicas NAT de salida que permiten que las redes internas, como la LAN, se comuniquen con redes externas, como internet, utilizando la dirección IP pública asignada a la interfaz WAN. De esta forma no será necesario configurar manualmente el filtro.

Figura 26

Configuración de reglas NAT salientes en OPNsense



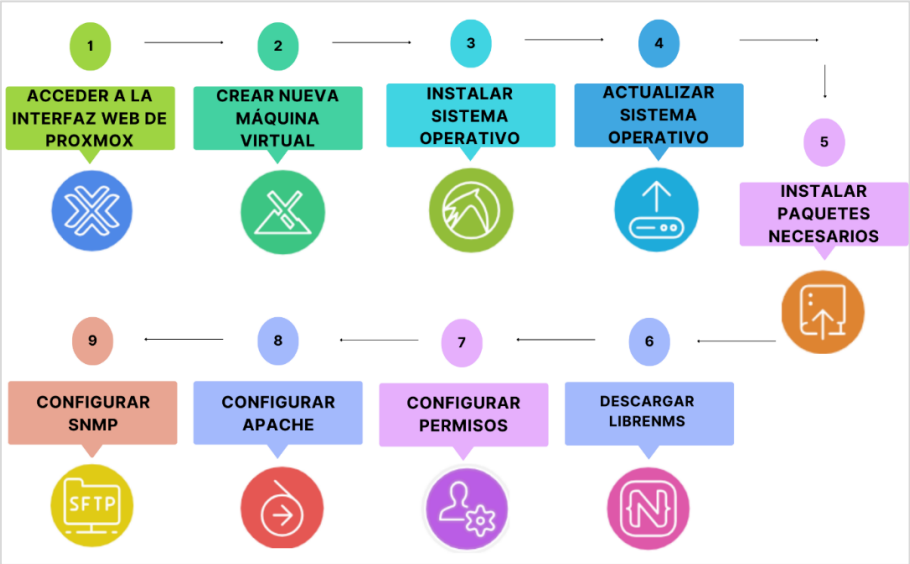
3.5 Despliegue y configuración de LibreNMS

El despliegue de LibreNMS consiste en la instalación y configuración de este. Como se observa en la Figura 27, se detalla el flujo de pasos para realizar este proceso. Primero, es necesario acceder a Proxmox y seleccionar el nodo que se está utilizando, “pve”, para crear una VM llamada LibreNMS en su interior. Luego, se selecciona el Sistema Operativo (SO) Linux, y como variante Debian/Ubuntu y se asignan los recursos a la nueva VM; otorgándole 2 CPUs, 2 GB de RAM y 40 GB de almacenamiento. Finalmente, se configura una interfaz de red bridge.

Posteriormente, se instala SO utilizando la ISO de Ubuntu Server previamente cargada. Una vez instalado, el sistema se actualiza con el comando `sudo apt update && sudo apt upgrade`. Para luego, instalar los paquetes necesarios, como MySQL, Apache, PHP y, principalmente, SNMP, mediante el siguiente comando: `sudo apt install -y apache2 mysql-server php php-cli php-mysql snmp`. Se descarga LibreNMS con el comando `sudo git clone https://github.com/librenms/librenms.git`, para configurar los permisos mediante `sudo chown -R www-data:www-data librenms`, y finalmente, ejecutar la instalación.

Figura 27

Fases de despliegue de LibreNMS



Entre pasos adicionales, está la configuración de la base de datos accediendo a MySQL y la configuración de Apache y SNMP, por último, se reinicia el sistema. Tras iniciar sesión en el navegador utilizando la dirección IP de la VM, se completa la instalación de LibreNMS, se debe habilitar también la monitorización en Proxmox configurando SNMP en el host y añadiéndolo como dispositivo en LibreNMS. También es posible acceder mediante la dirección librenms.labtelecom.com.ec esto dado que se configuro en PI-Hole, una herramienta de bloqueo de anuncios y rastreadores en toda la red que actúa como servidor DNS interno, la IP de LibreNMS para facilitar la identificación y monitoreo del servidor (Apéndice B: pruebas de conectividad y configuraciones realizadas).

3.5.1 Descubrimiento automático de dispositivos

Gracias a protocolos como SNMP, es posible habilitar funcionalidades como el auto discovery en LibreNMS, una función muy útil que permite detectar automáticamente dispositivos conectados a la red de tal manera que los agrega al monitoreo.

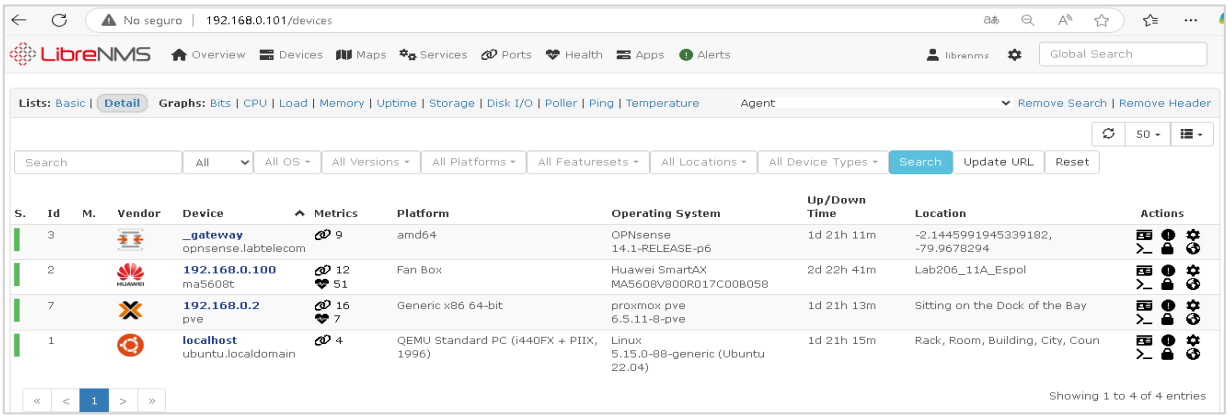
Características del Auto Discovery en LibreNMS:

- **Detección Automática:** Detecta dispositivos conectados a la red, no se necesita agregación manual de los mismos.
- **Compatibilidad con SNMP:** Descubre detalles como interfaces, métricas de rendimiento, tráfico entre otras y topologías, mediante información transmitida por SNMP.
- **Integración de Dispositivos:** A medida que se detectan dispositivos nuevos, se integran automáticamente al monitoreo.
- **Soporte de Topologías:** Es posible descubrir equipos conectados en cascada, como switches, routers e inclusive hosts conectados.
- **Flexibilidad:** Para el escaneo de la red, es posible configurar rangos de direcciones IP o subredes específicas.

- **Monitoreo Centralizado**: Con la integración de Proxmox, LibreNMS puede recopilar datos no solo del host Proxmox (el nodo físico) sino también de cada VM que ejecuta.

Figura 28

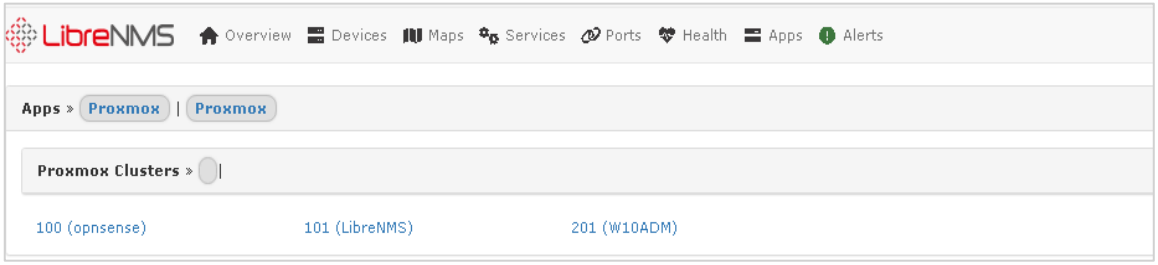
Dispositivos detectados automáticamente en LibreNMS



La Figura 29, muestra una lista de VM, organizadas como parte de un único clúster de Proxmox. Esto facilita la gestión y monitoreo a través de LibreNMS.

Figura 29

Integración de Proxmox en LibreNMS con VMs monitoreados automáticamente



3.6 Análisis de Resultados

3.6.1 Estabilidad de recursos: Eficiencia en la asignación a VMs con Proxmox VE

Los recursos fueron asignados a las VMs según las funciones que desempeñen. Por ejemplo, OPNsense, con un disco 40 GB de espacio utiliza el 3,93% de sus 2 CPU y el 83,49% de sus 8 GB de RAM asignados, reflejando un alto uso de memoria debido a las funciones que debe desempeñar, esto dado la cantidad de servicios que se habilitaron (Figura 30). Por otro lado, LibreNMS, con 40 GB de espacio en disco, mantiene un uso bajo de CPU, un 0,26% de 4

procesadores y a nivel de memoria consume un 66,52% de 2 GB (Figura 32). Por último, W10ADM, que es la VM de administración desde donde se gestiona la red, presenta un mayor consumo de CPU, con un 13,52% de 4 procesadores y de RAM un 82,64% de 4 GB, así como un disco dedicado de 96 GB (Figura 31).

De este modo, se puede crear una red escalable y adaptable. Por ejemplo, si hay que sustituir un servidor de supervisión por otro más robusto, basta con apagar la VM existente y encender la nueva, sin tener que interrumpir toda la infraestructura.

Figura 30

Uso de recursos VM OPNsense

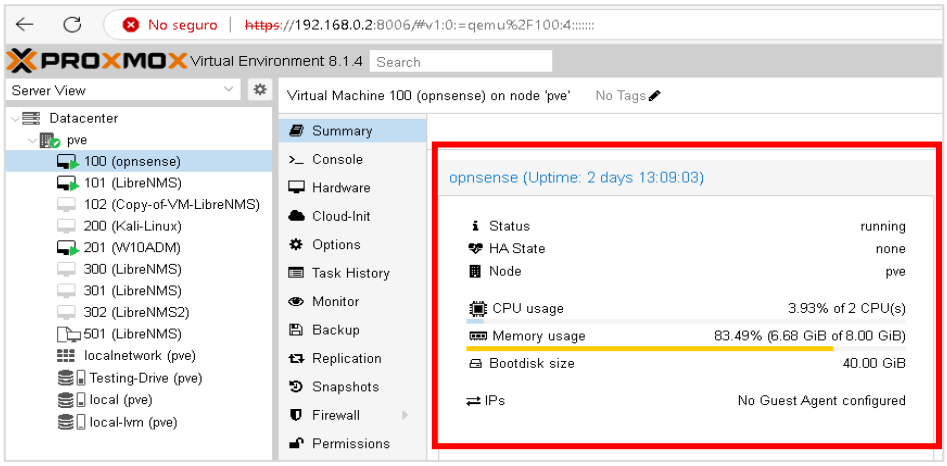


Figura 31

Uso de recursos VM administración

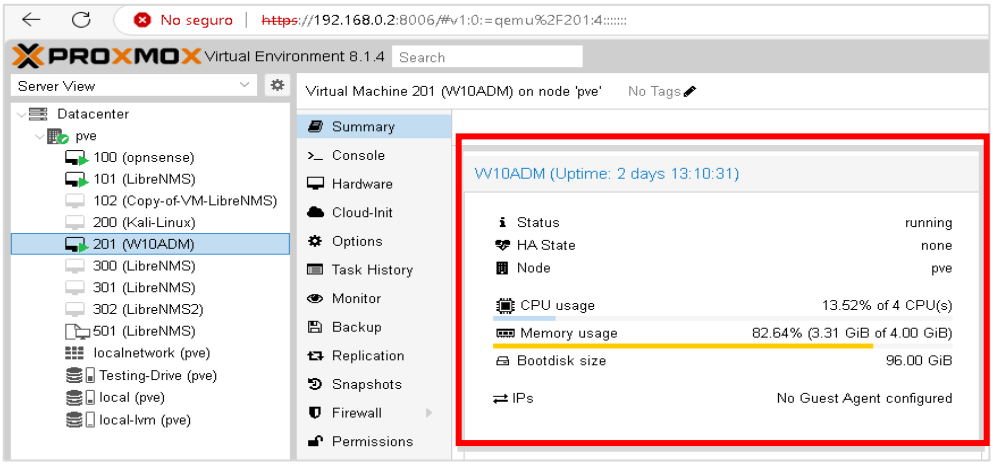
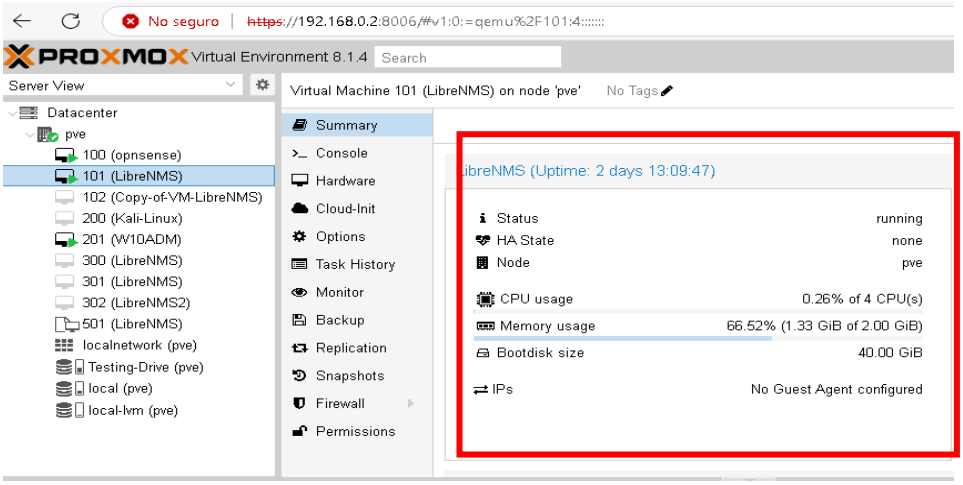


Figura 32

Uso de recursos VM LibreNMS

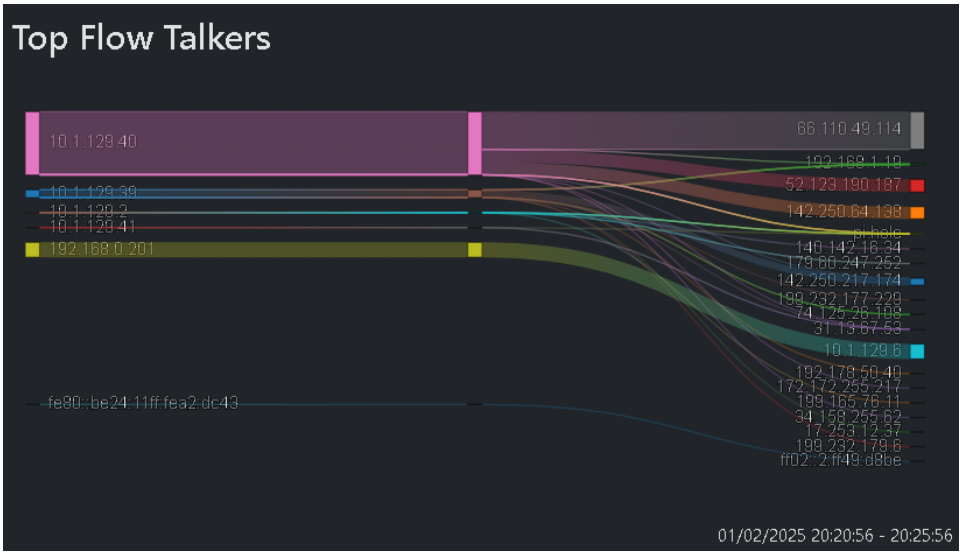


3.6.2 Confiabilidad del tráfico: Métricas monitorizadas con Ntopng

El servicio de Ntopng evalua distintas métricas para revisar, y analizar trafico a nivel IP a tarves de la red, dentro de la infraestructura que emula un pequeño ISP. Por ejemplo, la Figura 33, de Top Flow Talkers en ntopng, muestra las conexiones activas de mayor impacto en términos de volumen de tráfico, permitiendo identificar los orígenes y destinos de los datos en la red. Se identifican distintos origenes, como el correspondiente a la direccion IP 10.1.129.10 que ademas, cumple con la funcion de cliente.

Figura 33

Flujo de tráfico entre origen y destino

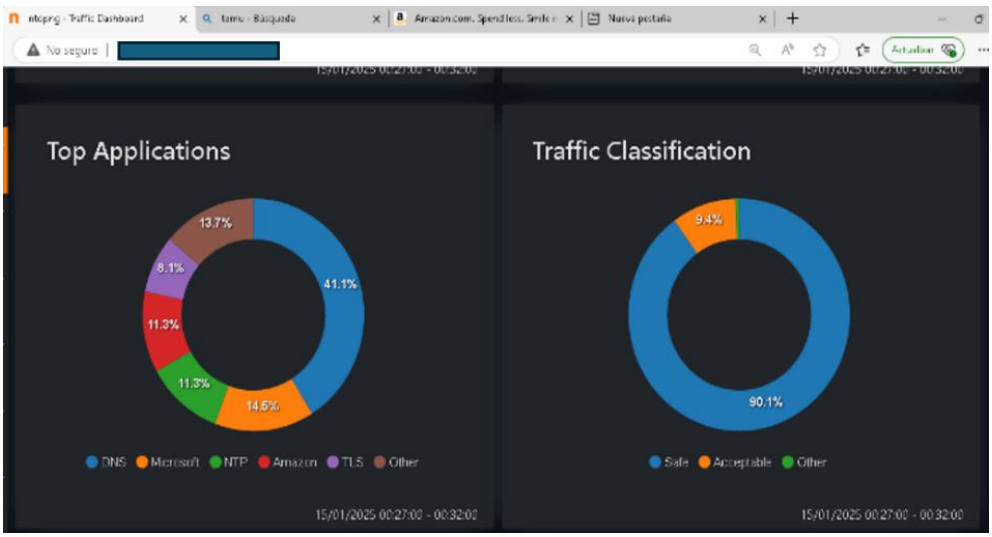


La Figura 34, muestra las aplicaciones o protocolos que mas se utilizan en la red, clasificados por porcentaje de tráfico (Top Applications). Los de mayor porcentaje son las consultas DNS (41.1%), lo cual es normal ya que se realizan consultas para resolver nombres de dominio a direcciones IP, tambien captura tráfico hacia servicios de Microsoft, como Office 365, OneDrive o actualizaciones de Windows. Además, como se observa es capaz de realizar consultas hacia Amazon Web services (AWS).

Entre los protocolos que captura ntopng, se tiene NTP, que sirve para sincronizar los relojes de los sistemas informáticos entre servidor cliente [34]. TLS (8.1%), que representa el tráfico encriptado por HTTPS para navegación web segura. Y en caso de no registrarse dentro de alguna de las categorias anteriores, lo registra como otros (8.1%). También se clasifica el tráfico por nivel de seguridad (Traffic Clasification): tráfico seguro que está permitido por las políticas de red, tráfico que se considera aceptable pero que puede requerir supervisión, y tráfico sin clasificar que puede incluir conexiones desconocidas o sospechosas.

Figura 34

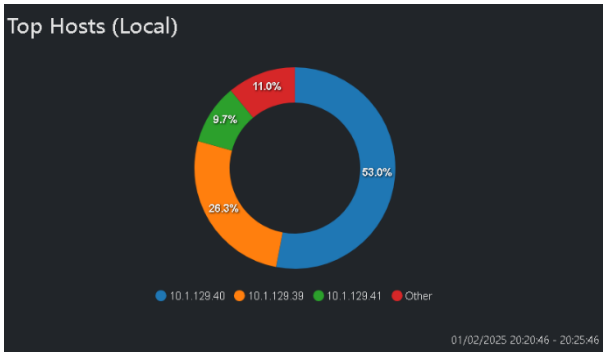
Principales aplicaciones y clasificación del tráfico según su nivel de seguridad en la red



La Figura 35, muestra los hosts que representen mayor tráfico en la red, como firewall y enrutador, OPNsense (IP 200.126.X.X) gestiona todo el tráfico entrante y saliente de los dispositivos conectados, lo que lo convierte en el host con mayor consumo de tráfico (98.6%).

Figura 35

Configuración de red y análisis de tráfico del host principal

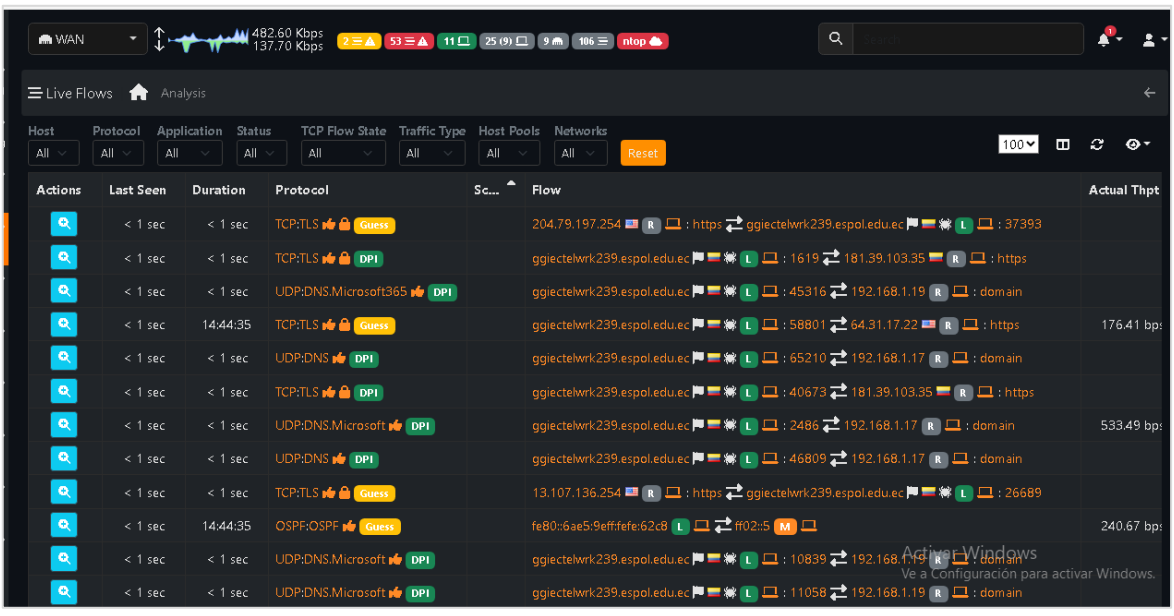


La Figura 36, en comparación a las gráficas anteriores, proporciona más detalle de la información de tráfico de datos en tiempo real, es posible validar que dispositivos están consumiendo ancho de banda, la trayectoria de los datos, incluyendo información sobre los protocolos, IPs, servicios, y volúmenes exactos de tráfico involucrados.

Es útil en casos de que se necesite diagnosticar problemas, detectar conexiones sospechosas, monitorear los flujos críticos, o para auditar el tráfico de un dispositivo en específico. Para este caso se monitoreó el tráfico en la Red WAN, pero también es posible supervisar cada una de las interfaces configuradas, incluyendo sus VLANs.

Figura 36

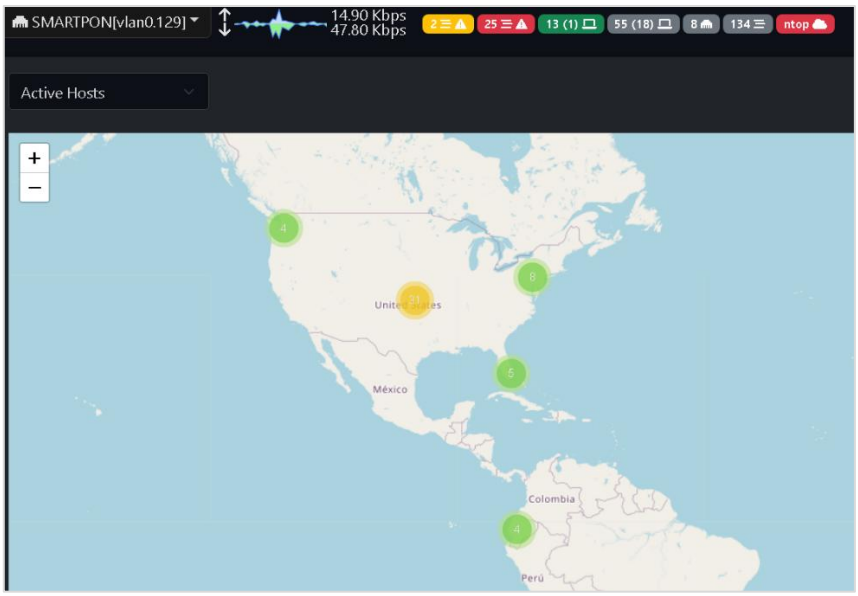
Conexiones activas en tiempo real: protocolos, servicios, IPs y tráfico generado



Otro resultado de Ntopng fue un mapa de geolocalización obtenido desde la función geomap, que localiza el flujo de datos hacia los servidores o host donde se están comunicando. En este caso, se observa un mapa de calor según la cantidad de host por región, Estados Unidos es una localidad que destaca en el mapa, ya que corresponde al alojamiento físico de la mayoría de los servidores a los que se está conectando (Figura 37).

Figura 37

Visualización geográfica de los hosts activos



3.6.3 Evaluación del ancho de banda: Tráfico de red con LibreNMS

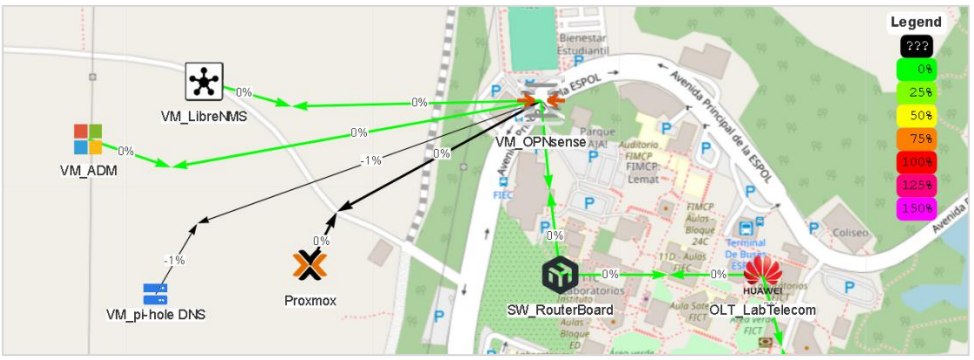
En la Figura 38, se presentan los dispositivos conectados a la red y sus respectivos enlaces, junto con los niveles de saturación entre cada uno.

Los porcentajes indican el uso de ancho de banda en cada enlace, mientras que, los colores de las líneas reflejan el nivel de uso del enlace:

- **Verde:** Tráfico bajo (menos del 25% del ancho de banda).
- **Amarillo a rojo:** Tráfico moderado a alto (más del 50%).
- **Magenta:** Enlace con sobrecarga critica (más del 150%).

Figura 38

Visualización de conectividad y estado de tráfico en la red usando LibreNMS

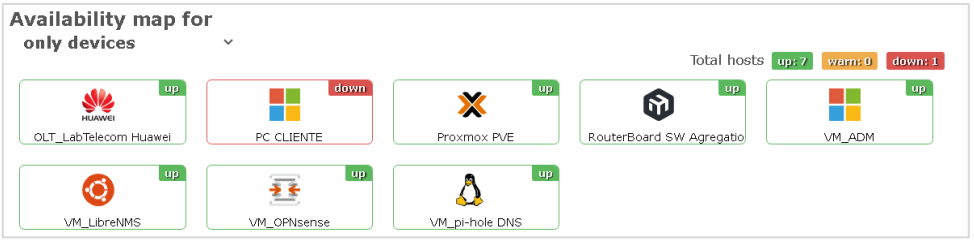


Con este mapa, es posible ver cuanto tráfico está pasando entre los dispositivos y si algún enlace está sobrecargado, saturado o presente problemas de tráfico.

Además, una forma rápida de monitorear el estado de los dispositivos de red es revisando el mapa de disponibilidad en la red, donde en caso de que una interfaz no este arriba, se anunciará una alarma con un icono down indicando que hay problemas en el equipo (Figura 39).

Figura 39

Mapa de disponibilidad de dispositivos en la red



3.6.4 Parámetros críticos: Monitorización para garantizar la estabilidad con LibreNMS

En el caso de la OLT Huawei 192.168.0.10 es posible monitorear, de forma proactiva, interfaces como los módulos SFP con su potencia (dBm) y temperatura (°C) registrada junto a sus umbrales específicos -solo módulo 0/0/0 se encuentra en funcionamiento-, para descartar problemas de atenuación o latencia (Figura 40) (Figura 41). En caso de que los valores registrados no estén dentro de los umbrales establecidos, se visualizara la alarma gráfica y se recibe una notificación mediante Slack.

Figura 40

Alarma de potencia elevada para módulo SFP detectada en LibreNMS

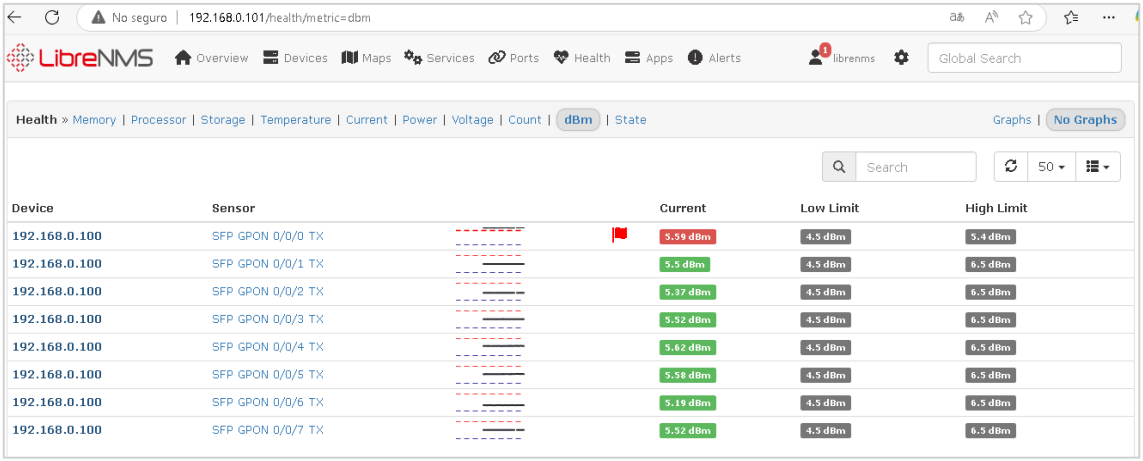
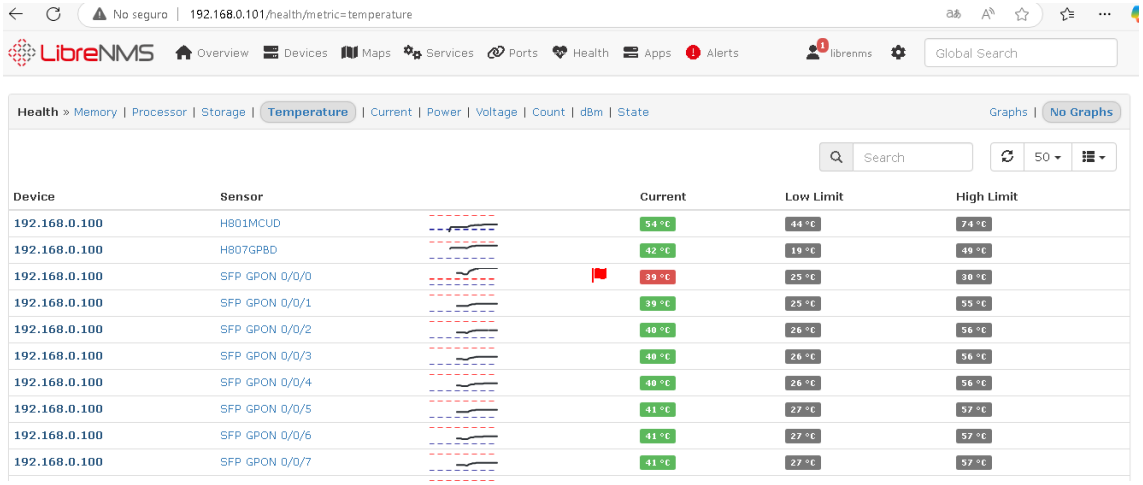


Figura 41

Alarma de temperatura elevada para modulo SFP detectada en LibreNMS



Para poder ensenarle al sistema que condiciones debe medir para enviar las notificaciones, se deben crear las regla, para ello, se establecen mediante condiciones las distintas evaluaciones que el sistema debe hacer antes de notificar una alarma.

3.6.5 Alertas y notificaciones: Supervisión proactiva para asegurar la confiabilidad de la red

Es posible configurar cuantas reglas y transportes sean necesarios (Apéndice C:) para notificar eventos en la red. Una vez configurados, cuando se presenten alarmas, como en este caso, de potencia o temperatura elevada para los módulos SFP, lo que podría causar una posible atenuación en el enlace, las notificaciones llegaran de la siguiente manera:

Figura 42

Notificación de potencia óptica elevada recibida en Slack

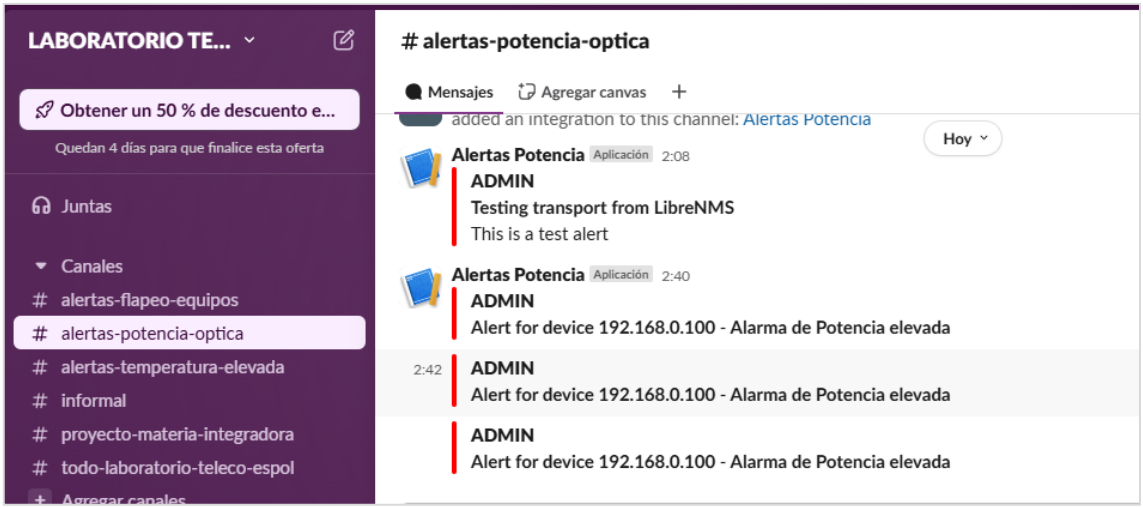
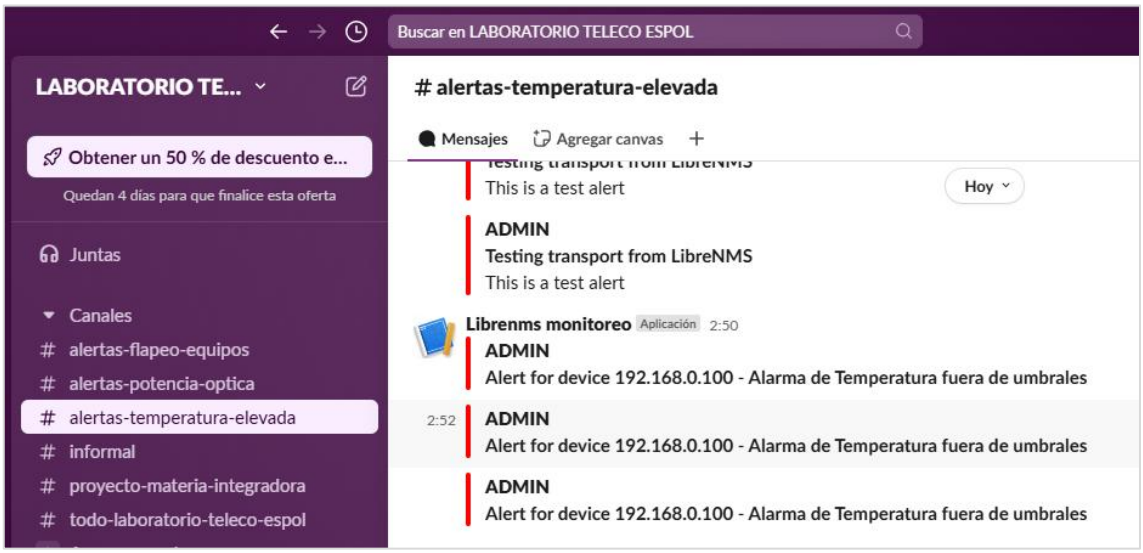


Figura 43

Notificación de temperatura elevada recibida en Slack



Capítulo 4

4.1 Conclusiones y recomendaciones

El desarrollo de este trabajo ha demostrado que es posible implementar una infraestructura virtualizada orientada a redes GPON capaz de optimizar la administración y supervisión de redes en un entorno educativo, centralizando la gestión de la red, mediante el uso de herramientas de software libre como Proxmox, OPNsense y LibreNMS, para virtualizar funciones claves como lo son enrutamiento, Firewall, monitoreo de tráfico.

Entre las fortalezas del proyecto se destacan la flexibilidad con la que cuenta el sistema actual, ya que los recursos y servicios son manejados ahora desde un punto central, lo que conlleva a que las tareas de operatividad sean mucho más sencillas. Asimismo, el utilizar software libre no solo se redujo los posibles costos operativos y de licencias, sino también proporcionó autonomía en la administración de la red y el aprendizaje practico.

A pesar de las metas alcanzadas, uno de los principales desafíos durante el desarrollo del proyecto fue la dependencia de hardware de gama media, lo que en ciertos escenarios limitó el rendimiento de la red. Se utilizó una computadora disponible en el laboratorio para ejecutar el servidor Proxmox en lugar de un equipo dedicado, este equipo asigna los recursos a las VMs según su capacidad disponible, lo que dificulta la integración de más dispositivos y servicios. Esto, en ciertos escenarios, también generó latencia en la conexión debido a la carga del sistema.

En comparación con estudios relacionados, este proyecto se distingue por integrar tecnologías de virtualización y redes ópticas dentro de un contexto académico, esta propuesta de valor lo diferencia de otros enfoques completamente comerciales o industriales. El propósito de simular escenarios realistas que posibiliten la gestión de redes mediante herramientas relativamente accesibles representa un aporte académico, brindando la oportunidad a los estudiantes de mejorar sus competencias en el manejo de tecnologías modernas.

4.1.1 Conclusiones

- Se diseñó una infraestructura virtualizada orientada a la administración eficiente de redes GPON, utilizando herramientas de software libre como Proxmox, OPNsense y LibreNMS. El diseño abarco desde la selección de las herramientas necesarias para levantar las funciones a virtualizar hasta el despliegue de cada una, siendo estas, enrutamiento, firewall y análisis de tráfico. De tal manera que no solo sea posible optimizar de recursos, sino también crear un entorno adaptable y adecuado para fines educativos, diseñado para facilitar el aprendizaje práctico y el desarrollo de competencias técnicas en la administración de redes ópticas.
- Se logró implementar las funciones de red fundamentales, dentro de Proxmox trabajando como plataforma central. Al integrar OPNsense, se logró configurar servicios de firewall y enrutamiento avanzados, por otro lado, LibreNMS proporcionó capacidades de monitoreo del tráfico de la red en tiempo real. Consiguiendo una gestión centralizada y flexible de los recursos, reduciendo la complejidad operativa y permitiendo que el entorno se adapte a las necesidades específicas del laboratorio.
- Se demostró que la infraestructura virtualizada satisface los requisitos de administración y supervisión centralizada de manera efectiva, gracias a las pruebas realizadas en la red GPON. La herramienta Ntopng, hizo posible la identificación de métricas como el ancho de banda, el tráfico entre los dispositivos, la estabilidad de los recursos asignados a cada VM y la identificación de los distintos hosts que acceden a la red. Destacando la eficiencia y confiabilidad del sistema, siendo este capaz de operar bajo condiciones reales, con gran potencial para mejorar las practicas académicas sobre gestión de redes ópticas.

4.1.2 Recomendaciones

- Se recomienda la configuración de una conexión WAN alternativa, que sirva como enlace Backup, para garantizar que la operatividad del sistema no se vea afectada. Esta WAN,

permita balancear el tráfico y proporcione salida para superar restricciones de la red de ESPOL. Se pueden utilizar las capacidades de OPNsense, como failover y políticas de tráfico, para desviar ciertos servicios o tráfico por esta WAN secundaria.

- De ser posible, se recomienda la implementación equipos dedicados para este tipo de entornos, como servidores rack o blade equipados, procesadores con mayores capacidades de memoria ECC y almacenamiento NVMe, para simular escenarios más complejos y garantizar la estabilidad y rendimiento del sistema.
- Se sugiere adicionar un nodo a Proxmox para formar un clúster, de tal manera que se pueda distribuir los recursos entre los distintos nodos y habilitar características como la migración en vivo de VMs. Esto facilitaría la creación de copias de seguridad automáticas en caso de algún fallo. Y mediante el monitoreo centralizado, sería posible supervisar el estado del clúster y realizar configuraciones para garantizar estabilidad operativa en la infraestructura.
- Se sugiere implementar mayores filtros de seguridad, para una protección más robusta contra amenazas, incorporando sistemas que protejan la red, como Suricata, un software open source IDS (intrusion detection systems) /IPS (intrusion prevention systems), complementando las funcionalidades de firewall implementadas en OPNsense.

Referencias

[1] M. C. E. Boquera, Servicios Avanzados de telecomunicación, Madrid: Díaz de Santos, S.A., 2003.

[2] P. CABANTOUS, Redes informáticas: Guía práctica para la gestión, seguridad y supervisión, Madrid: Editorial Eni, 2024.

[3] C. Bottini, «Virtualización de redes,» de Virtualización de redes, RedUSERS, 2022, p. 27.

[4] D. A. Brihuega, Administración de redes telemáticas, Madrid: Madrid, 2015.

[5] R. J. M. Tejedo, «Ramonmillan.com,» 2012. [En línea]. Available: https://www.ramonmillan.com/documentos/competenciaoperadoresvsott.pdf. [Último acceso: 3 Octubre 2024].

[6] Cisco, «Cisco,» Cisco, 11 Mayo 2023. [En línea]. Available: https://www.cisco.com/c/es_mx/support/cloud-systems-management/prime-infrastructure/series.html. [Último acceso: 2 Octubre 2024].

[7] S. Universidad de Sevilla, «Dialnet,» 25 Julio 2003. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=876562. [Último acceso: 13 Octubre 2024].

[8] V. S. Sosa, «Cinvestav,» Cinvestav, 2024. [En línea]. Available: https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/GestionRedes.pdf. [Último acceso: 21 Octubre 2024].

[9] Amazon Web Services, «Amazon,» 2024. [En línea]. Available: https://aws.amazon.com/es/what-is/iaas/. [Último acceso: 13 Octubre 2024].

[10] J. P. A. L. C. I. V. B. M. A. C. i. A. X. H. S. M. C. C. M. C. C. R. V. F. E. G. V. X. S. L. C. Jordi Casademont i Serra, Redes de comunicaciones: De la telefonía móvil a internet, Cataluña: Universitat Politècnica de Catalunya. Iniciativa Digital Politècnica, 2010.

[11] J. M. H. Moya, Telecomunicaciones. Tecnologías, Redes y Servicios. 2ª edición actualizada, Madrid: Grupo Editorial RA-MA, 2014.

[12] J. M. Millan Esteller, Técnicas y procesos en infraestructuras de telecomunicaciones 2.ª edición 2024, San Fernando de Henares: Ediciones Paraninfo, S.A, 2024.

[13] Á. L. C. García, Gestión de redes telemáticas. IFCT0410, 2016: IC Editorial, 2016.

[14] LibreNMS, «LibreNMS,» LibreNMS, 2023. [En línea]. Available: https://www.librenms.org/#features. [Último acceso: 13 Octubre 2024].

[15] L. F. U. Z., «LA VIRTUALIZACIÓN Y SU IMPACTO EN LAS CIENCIAS COMPUTACIONALES,» Revista Digital Lámpsakos, nº 2, pp. 118-121, 2009.

[16] K. Gray y T. D. Nadeau, Network Function Virtualization, Chennai: Morgan Kaufmann, 2016.

[17] Huawei, «Huawei,» 20 Mayo 2021. [En línea]. Available: https://forum.huawei.com/enterprise/es/arquitectura-de-referencia-de-nfv/thread/667224901850906624-667212887476809728. [Último acceso: 11 Noviembre 2024].

[18] J. G. Herrera, «Researchgate,» [En línea]. Available: https://www.researchgate.net/figure/Figura-8-Arquitectura-OPNFV-basada-en-la-arquitectura-NFV-de-NFV-ISG_fig6_299347478. [Último acceso: 8 Noviembre 2024].

[19] INTEL CORPORATION, «INTEL,» 2015. [En línea]. Available: https://www.intel.la/content/dam/www/public/lar/xl/es/documents/white-papers/end-to-end-optimized-nfv-paper-spa.pdf.. [Último acceso: Noviembre 6 2024].

[20] Huawei, «Huawei,» 23 Julio 2015. [En línea]. Available: https://support.huawei.com/enterprise/en/knowledge/EKB1000082843. [Último acceso: 10 Diciembre 2024].

[21] M. R. M. Álvarez, «Repositorio PUCE,» 22 Diciembre 2023. [En línea]. Available: https://repositorio.puce.edu.ec/items/b7389280-493a-4ef7-81c4-0ba2b5ff9240/full. [Último acceso: Diciembre 1 2024].

[22] Wundertech, «wundertech,» 5 Mayo 2024. [En línea]. Available: https://www.wundertech.net/pfsense-vs-opnsense/. [Último acceso: 2 Diciembre 2024].

[23] «G2,» [En línea]. Available: https://www.g2.com/compare/librenms-vs-zabbix. [Último acceso: Diciembre 4 2024].

[24] Librenms, «docs Librenms,» [En línea]. Available: https://docs.librenms.org/Extensions/Rancid/?utm_source=chatgpt.com. [Último acceso: 12 Diciembre 2024].

[25] «ZABIXX,» 2024. [En línea]. Available: https://www.zabbix.com/. [Último acceso: 12 Diciembre 2024].

[26] Á. Gómez, Auditoría de seguridad informática, Ediciones de la U, 2022.

[27] Ministerio de Telecomunicaciones y de la Sociedad de la Información, «REGLAMENTO PARA LA ADQUISICION DE SOFTWARE,» 11 Octubre 2017. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/03/Decreto-Ejecutivo-No.-1425-Adquisicion-de-Software.pdf. [Último acceso: 21 Diciembre 2024].

[28] PROXMOX, «PVE PROXMOX,» 28 Noviembre 2024. [En línea]. Available: https://pve-proxmox-com.translate.goog/wiki/Installation?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc. [Último acceso: 10 Enero 2025].

[29] OPNsense, «OPNsense,» [En línea]. Available: https://opnsense.org/users/get-started/. [Último acceso: 15 Enero 2024].

[30] Zenarmor, «Zenarmor,» 10 Agosto 2021. [En línea]. Available: https://www.zenarmor.com/docs/network-security-tutorials/opnsense-installation. [Último acceso: 15 Enero 2025].

[31] OPNsense, «OPNsense Overview,» 2025. [En línea]. Available: https://docs.opnsense.org/manual/interfaces_overview.html. [Último acceso: 15 Enero 2025].

[32] OPNsense, «OPNsense Diagnostics,» 2025. [En línea]. Available: https://docs.opnsense.org/manual/diagnostics_interfaces.html. [Último acceso: 15 Enero 2025].

[33] Dell, «Dell,» 2025. [En línea]. Available: https://www.dell.com/support/kbdoc/es-es/000129137/qu%C3%A9-es-wake-on-lan-gu%C3%ADa-de-soluci%C3%B3n-de-problemas-y-pr%C3%A1cticas-recomendadas#:~:text=WOL%20es%20un%20protocolo%20est%C3%A1ndar,de%20bajo%20consumo%20de%20energ%C3%ADa.. [Último acceso: 15 Enero 2024].

[34] «Redes Zone,» 15 Agosto 2024. [En línea]. Available: https://www.redeszone.net/tutoriales/internet/que-es-protocolo-ntp/. [Último acceso: 15 Enero 2025].

[35] L. Joyanes, Sistemas de Información en la empresa, Alpha Editorial, 2015.

[36] R. P. N. MINDA, «Repositorio UTN,» 2023. [En línea]. Available: https://repositorio.utn.edu.ec/bitstream/123456789/13427/2/04%20RED%20322%20TRABAJO%20GRADO.pdf. [Último acceso: 4 Noviembre 2024].

[37] Á. L. C. García, Gestión de redes telemáticas. IFCT0410, Málaga: IC Editorial, 2014.

[38] «Solar Winds,» [En línea]. Available: https://www.solarwinds.com/es. [Último acceso: 7 Noviembre 2024].

[39] «CISCO,» CISCO, [En línea]. Available: https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/series.html. [Último acceso: 7 Noviembre 2024].

[40] K. L. D. S. F. L. F. Michel S. Bonfim, «Arxiv,» 4 Junio 2018. [En línea]. Available: https://arxiv.org/pdf/1801.01516. [Último acceso: 1 Diciembre 2024].

[41] P. proxmox, «Pve proxmox,» 28 Noviembre 2024. [En línea]. Available: https://pve.proxmox.com/wiki/Certificate_Management. [Último acceso: 5 Diciembre 2024].

[42] «Forum proxmox,» 6 Abril 2021. [En línea]. Available: https://forum.proxmox.com/threads/encrypting-proxmox-ve-best-methods.88191/. [Último acceso: 5 Diciembre 2024].

[43] A. M. M. G. P. Coral Calero, «Calidad de producto y proceso de software,» de Calidad de producto y proceso de software, Madrir, RA-MA Editorial, 2010.

[44] Ministerio de Telecomunicaciones y de la Sociedad de la Información, «Reglamento general de la ley organica de la proteccion de datos personales,» [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf?utm. [Último acceso: Diciembre 11 2024].

[45] LibreNMS, «LibreNMS,» 2025. [En línea]. Available: https://docs-librenms-org.translate.goog/Installation/Install-LibreNMS/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc. [Último acceso: 15 Enero 2025].

Apéndice A: lista de equipos iniciales y agregados

Tabla 5

Equipos iniciales del laboratorio de Redes de Telecomunicaciones

Equipos iniciales	
OLT Huawei MA5608T	1
Ont Huawei	1
PC Cliente	1
Patch Cord Extensión Ethernet	1

Tabla 6

Equipos finales infraestructura Rack Laboratorio de Telecomunicaciones

Equipos agregados	
Patch panel	1
PC servidor:	1
-Tarjeta PCI 2 GE RJ45	
Switch no administrable	1
Router MikroTik RB3011	1
Ont Huawei	1
Patch Cord Extensión Ethernet	1
Adaptador USB-RJ45 GEth	1
Plug inteligente Tapo P115	1

Apéndice B: pruebas de conectividad y configuraciones realizadas

Verificación conectividad:

En este apartado se detallan la prueba de conectividad realizada para garantizar una correcta comunicación entre la red interna (LAN) y la red externa (Internet).

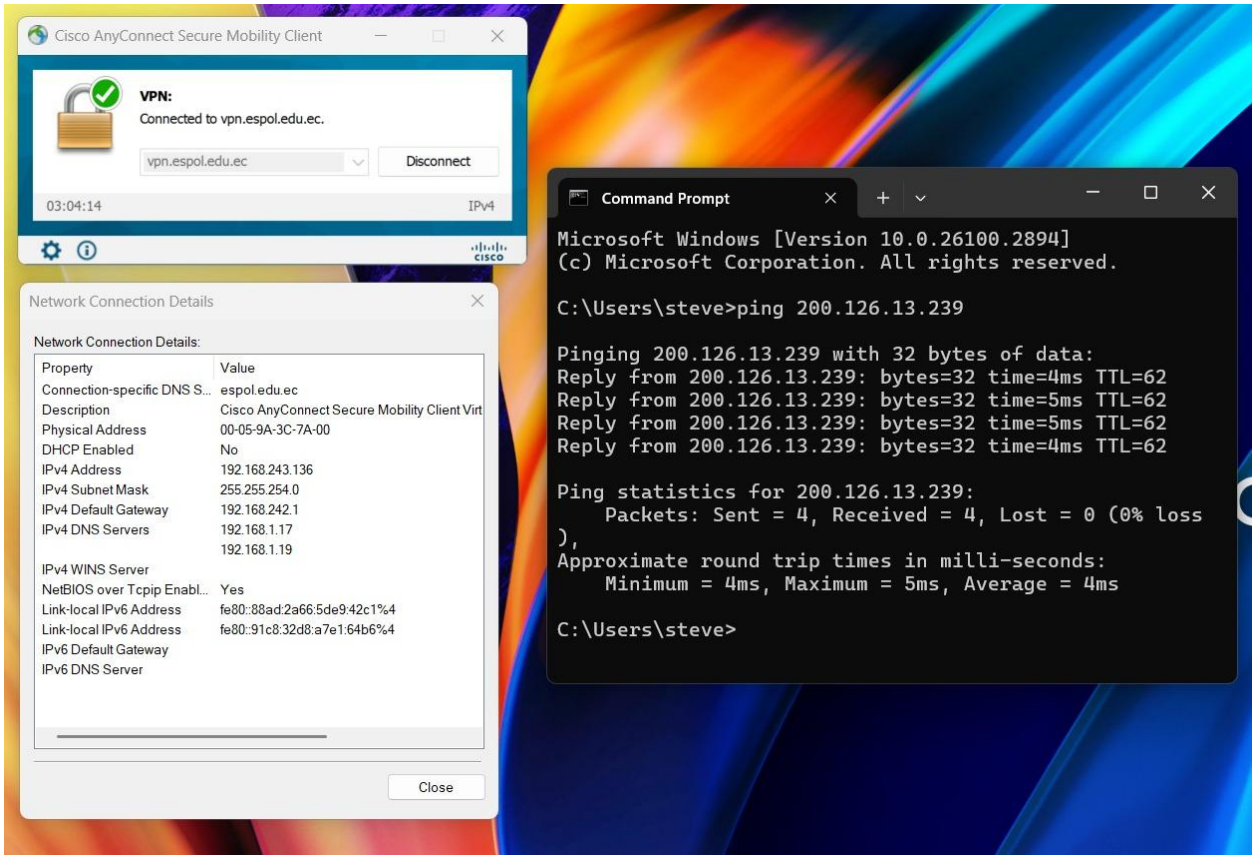
Mediante la VPN de ESPOL se cuenta con acceso seguro a los recursos internos de la red institucional desde ubicaciones remotas. Para ello, es necesario que el usuario se conecte a la VPN

utilizando el cliente Cisco AnyConnect. Se valida en "Network Connection Details" de la conexión de red para asegurarse de que las direcciones IPv4 y DNS específicas de la red ESPOL se han asignado correctamente.

Una vez establecida la conexión, se verifica conectividad con OPNsense mediante ping desde el equipo local a la direccion 200.129.xxx.xxx, comprobando que es satisfactoria. Esto confirma que la conexión VPN está operativa y que se tiene acceso exitoso al servidor OPNsense.

Figura 44

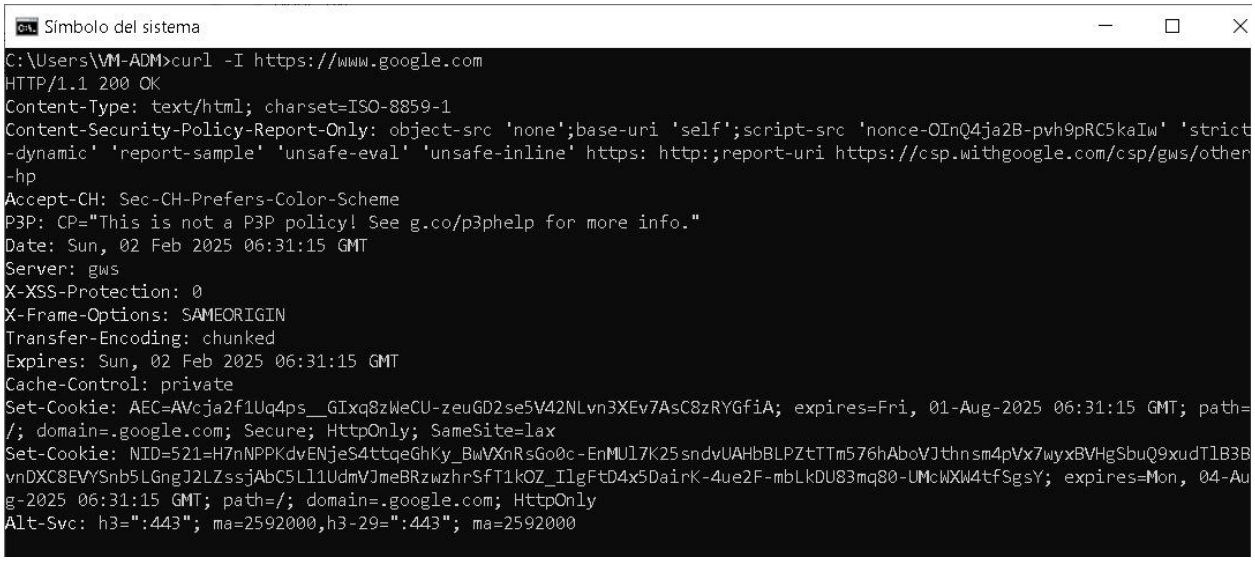
Prueba de acceso al servidor OPNsense



Se verifica la conectividad y la respuesta del servidor. Al ejecutar el comando `curl -I https://www.google.com`, se envió una solicitud HTTP de tipo HEAD al servidor de Google. Se confirma mediante el código de respuesta 200 OK, que el servidor es accesible desde el equipo de cliente, y responde a los encabezados HTTP esperados.

Figura 45.

Respuesta del servidor de Google mediante una solicitud HTTP

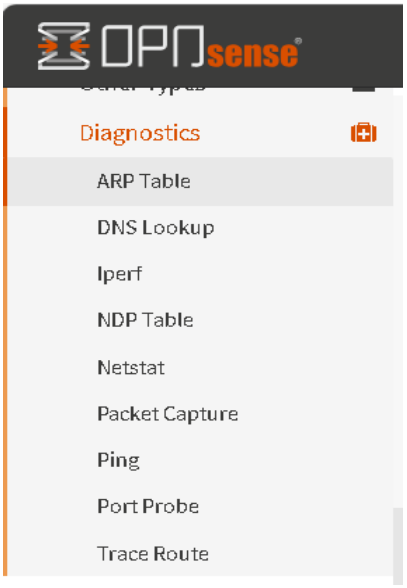


Herramientas de troubleshooting y regla de firewall:

Se cuenta, además, con algunas herramientas para tareas de troubleshooting disponibles:

Figura 46.

Herramientas de interfaces

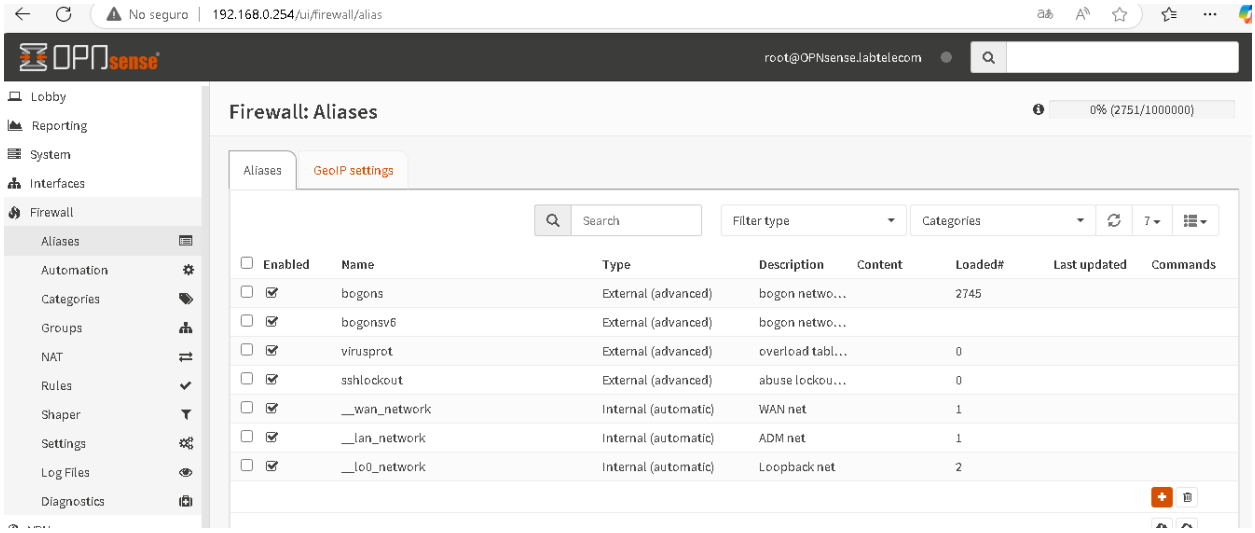


A continuación, se puede visualizar la configuración alias en el cortafuegos OPNsense, una herramienta que permite agrupar direcciones IP, redes o puertos para simplificar la creación

de reglas de seguridad. Por ejemplo, bogons y virusprot, ayudan a bloquear redes no válidas o sospechosas.

Figura 47

Configuración Aliases dentro las reglas de firewall de OPNsense



Servidor Pi-Hole:

Pi-hole se utilizó como servidor DNS interno para gestionar y resolver nombres de dominio en la red local.

La dirección IP 192.168.0.11 se configuró como librenms.labtelecom.com.ec para facilitar la identificación servidor LibreNMS. La resolución DNS se validó mediante pruebas de consulta directa e inversa y se documentó en los registros de Pi-hole.

Figura 48

Configuración de registros DNS locales en Pi-hole

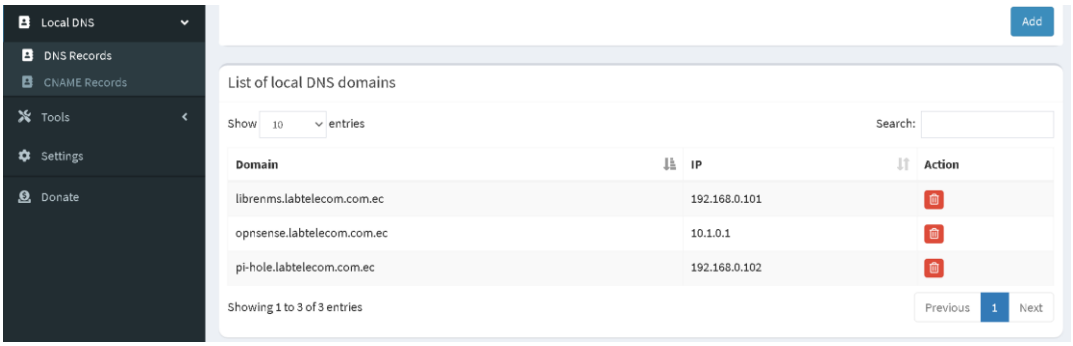
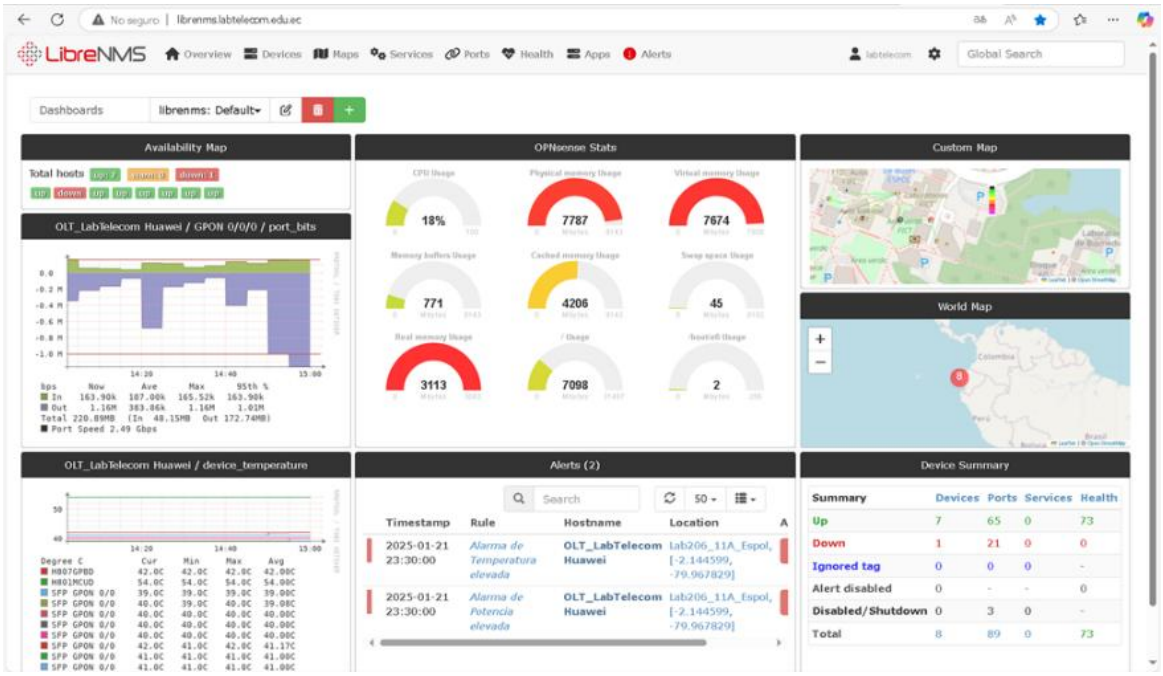


Figura 49

Acceso interfaz web LibreNMS mediante DNS

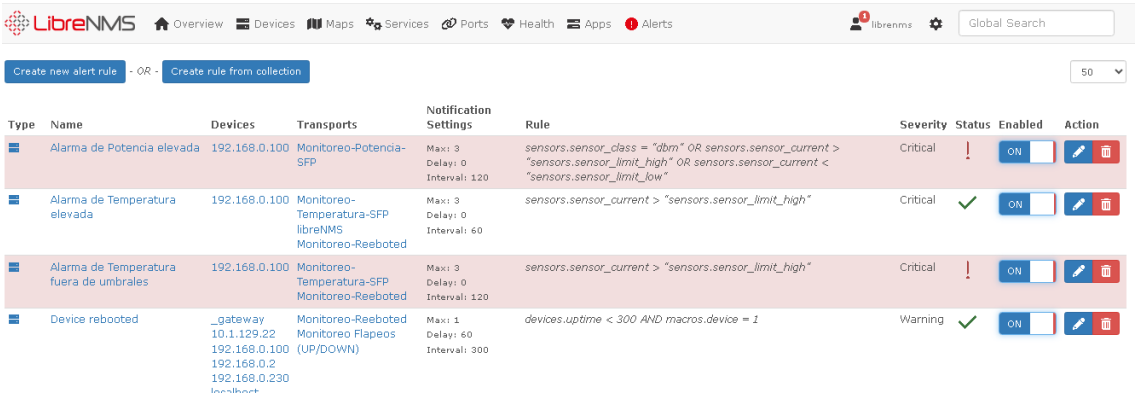


Apéndice C: reglas y notificaciones configuradas

Alertas y notificaciones: Supervisión proactiva para asegurar la confiabilidad de la red

Figura 50

Reglas configuradas



Transportes configurados para recibir alertas:

Se estableció un sistema de alarmas, que envíe notificaciones mediante la configuración de transportes en LibreNMS, indicando las condiciones más críticas del sistema, específicamente de los módulos SFP.

Las alarmas fueron configuradas en Slack, donde necesario la creación de una app y un nuevo webhook, se realiza la validación de test de notificaciones y ya está para funcionar

Figura 51

Transportes configurados