UNIVERSIDAD DE ANTIOQUIA

Buenas Prácticas en la Supervisión de Infraestructura de Red mediante Zabbix y Python

Carlos Andrés Mesa Roldán

Informe final para optar al título de Ingeniero de Telecomunicaciones

Semestre de Industria

Asesora Interna
Ana María Cárdenas Soto, PhD

Asesor Externo
Hernán Darío Yepes Montoya,
Msc. en Ingeniería de Telecomunicaciones

Universidad de Antioquia
Facultad de Ingeniería
Ingeniería de Telecomunicaciones
Medellín, Antioquia
2025

Cita		Carlos Andrés Mesa Roldán
Referencia Estilo IEEE (2020)	[1]	C. Mesa Roldán, "Buenas Prácticas en la Supervisión de Infraestructura de Red mediante Zabbix y Python", Semestre de Industria, Ingeniería de Telecomunicaciones, Universidad de Antioquia, Medellín, 2025.

Dedicatoria

Dedico este trabajo en primer lugar a Dios, quien de múltiples maneras se ha manifestado en mi vida, brindándome la oportunidad y las condiciones para avanzar en el camino hacia convertirme en un gran profesional. A mi familia, que nunca dejó de apoyarme, incluso en los momentos más difíciles de mi vida y de la universidad. A mis padres, quienes siempre priorizaron mis estudios por encima de cualquier bien material, guiándome con su ejemplo y amor incondicional. A mis abuelos, que ya no me acompañan físicamente, pero que siempre esperaron verme alcanzar esta meta; honraré su memoria siendo el reflejo de su legado. A mis hermanos menores, que siempre vieron en mí un ejemplo y me dieron la fuerza para continuar a pesar de las inseguridades. Y a mis profesores, quienes a lo largo de los años me retaron a dar lo mejor de mí, en especial a mis asesores, profesionales exitosos a quienes debo un profundo respeto y admiración.

Agradecimientos

Quiero expresar mi más profundo agradecimiento a mis padres, quienes con su esfuerzo y perseverancia me inculcaron valores éticos y morales que han sido pilares en mi formación académica y personal. Extiendo también mi gratitud a los profesores del Departamento de Ingeniería Electrónica y Telecomunicaciones de la Universidad de Antioquia, cuya dedicación y enseñanzas marcaron de manera significativa mi proceso de aprendizaje. A la empresa Padtec, por brindar las herramientas y el apoyo necesario en el desarrollo de este trabajo, y de manera especial a mis asesores, cuya experiencia y orientación fueron fundamentales para consolidar los conocimientos que hoy se reflejan en este documento.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

ASE	Amplified Spontaneous Emission
AWG	Arrayed Waveguide Grating
BER	Bit Error Rate
CPU	Central Processing Unit
DWDM	Dense Wavelength Division Multiplexing
ICMP	Internet Control Message Protocol
MySQL	My Structured Query Language
NMS	Network Management System
OSNR	Optical Signal Noise Ration
OSPF	Open Shortest Path First
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Networks

RESUMEN

La supervisión de redes ópticas, IP y MPLS demanda la adopción de buenas prácticas internacionales que garanticen la continuidad, confiabilidad y seguridad de la infraestructura de telecomunicaciones. En redes ópticas, estas prácticas permiten gestionar parámetros como la atenuación, la capacidad y la resiliencia física, mientras que en redes IP y MPLS aseguran un funcionamiento eficiente de los protocolos de enrutamiento, la calidad del servicio (QoS) y la priorización del tráfico en entornos multiservicio.

Con el fin de fortalecer la gestión proactiva, se desarrolló una plataforma integral basada en Zabbix y Python. Zabbix proporciona la capacidad de monitoreo avanzado de las redes, mientras que Python complementa con la automatización de procesos, el análisis de datos recolectados y la detección temprana de patrones anómalos. Esta sinergia permite prever posibles daños, anticipar fallos y generar alertas significativas que facilitan la toma de decisiones oportunas.

En conjunto, la aplicación de buenas prácticas técnicas recomendadas por la ITU-T, ISO/IEC, TM Forum y fabricantes líderes, junto con el soporte de la plataforma Zabbix–Python, asegura una operación estandarizada, resiliente y predictiva en infraestructuras de transporte óptico, IP y MPLS.

Palabras clave **—Python, MPLS, SNMP, IP, Equipos ópticos, fabricante.**

ABSTRACT

The supervision of optical, IP, and MPLS networks requires the adoption of international best practices to ensure the continuity, reliability, and security of telecommunication infrastructures. In optical networks, these practices allow efficient management of parameters such as attenuation, capacity, and physical resilience, while in IP and MPLS networks they guarantee optimal operation of routing protocols, quality of service (QoS), and traffic prioritization in multiservice environments.

To strengthen proactive management, an integrated platform was developed based on Zabbix and Python. Zabbix provides advanced network monitoring capabilities, while Python complements it with process automation, data analysis, and early detection of anomalous patterns. This synergy enables the prediction of potential damages, the anticipation of failures, and the generation of meaningful alerts that support timely decision-making.

Overall, the application of technical best practices recommended by ITU-T, ISO/IEC, TM Forum, and leading vendors, together with the support of the Zabbix–Python platform, ensures standardized, resilient, and predictive operation of optical, IP, and MPLS transport infrastructures.

Keywords —Python, MPLS, SNMP, IP, Optical equipment, Vendor.

I. INTRODUCCIÓN

En el panorama actual de las telecomunicaciones, la gestión y el monitoreo eficiente del desempeño en redes ópticas son fundamentales para garantizar tanto la calidad del servicio (QoS) como la continuidad operativa de las infraestructuras de comunicación. En este contexto, se vuelve cada vez más relevante no solo supervisar el funcionamiento de la red, sino también anticipar posibles fallos, prever daños potenciales y proponer soluciones proactivas que aseguren la resiliencia y eficiencia del sistema. Este trabajo se centra en la implementación de un sistema integral que no solo permita el monitoreo de variables críticas de desempeño en los niveles óptico e IP, sino que también habilite mecanismos de análisis proactivo- orientados a la detección temprana de fallos y la generación de acciones preventivas en las redes de los distintos clientes.

Este proyecto titulado "Buenas Prácticas en la Supervisión de Infraestructura de Red mediante Zabbix y Python" se enfoca en el diseño e implementación de un sistema integral de monitoreo que no solo aprovecha las capacidades de Zabbix, como software de monitoreo para la supervisión avanzada de redes IP, sino que también incorpora el uso de Python como herramienta como herramienta complementaria para la automatización de tareas a través de scripts y librerías especializadas. Python permitirá procesar y analizar los datos recolectados por los OID (objetos identificadores) de Zabbix, facilitando una comprensión más profunda del comportamiento de la red tanto en el nivel lógico (IP, protocolos de enrutamiento, latencia, errores) como en el nivel físico, especialmente en infraestructuras de transporte óptico (DWDM). Esta sinergia entre Zabbix y Python permite construir un modelo de analítica contextual, capaz de identificar patrones de desempeño, anticipar fallos y generar alertas significativas que contribuyan a una operación más eficiente y proactiva de la red.

Además, se desea realizar una comparativa sistemática entre los resultados obtenidos y las buenas prácticas de implementación recomendadas por organismos internacionales y referentes técnicos de la industria, como TM Forum, ITU-T, ISO/IEC, y fabricantes líderes. Este enfoque permite identificar brechas, proponer mejoras y fortalecer la toma de decisiones técnicas y estratégicas en los entornos de red evaluados. Adicionalmente, la estructura desarrollada sienta las bases para la proyección futura de modelos de aprendizaje automático, que aprovechen los datos históricos y la correlación de eventos para mejorar la capacidad predictiva del sistema y avanzar hacia una gestión más autónoma e inteligente de las redes.

II. OBJETIVOS

1. OBJETIVO GENERAL

Desarrollar un algoritmo de análisis de datos de monitoreo de redes de transporte ópticas, que permita identificar patrones operativos, anticipar fallos y comparar la Configuración de la red con buenas prácticas, mediante el uso del software de monitoreo Zabbix y herramientas de procesamiento de datos desarrolladas en Python

2. OBJETIVOS ESPECÍFICOS

- Identificar las variables más relevantes que impactan el desempeño de las redes de transporte ópticas, con el fin de priorizar su monitoreo y captura de datos con una frecuencia suficiente para detectar patrones de desempeño.
- Obtener un set de datos relacionados con las variables identificadas, mediante la Configuración de Zabbix para la supervisión de redes IP y ópticas, utilizando los OID (objetos identificadores) presentes en los equipos de red de la marca Datacom, así como en otros equipos de red comercializados y soportados por la empresa.
- Crear un algoritmo en Python, para el análisis de los datos recolectados por el servidor a través del protocolo SNMP (Simple Network Management Protocol) y SSH, que permita evaluar el comportamiento de los distintos parámetros y contrastarlos con buenas prácticas dados por el fabricante o estándares internacionales.
- Desarrollar un dashboard que permita la visualización amigable de los datos y su comparación con un desempeño esperado y realizar recomendaciones.

III. PRESENTACIÓN DE LA EMPRESA

Padtec S.A. es una multinacional brasileña fundada en 2001, con sede principal en Campinas, São Paulo. La compañía se especializa en el desarrollo de soluciones flexibles y de alta capacidad para transmisiones ópticas de larga distancia, basadas en tecnología de Multiplexación por División en Longitud de Onda Densa (DWDM).

Su portafolio incluye una amplia gama de productos diseñados para redes que atienden las necesidades de operadores de gran escala, integradores, carriers de carriers, proveedores de servicios y otros actores estratégicos del sector de telecomunicaciones. Además, a través de alianzas con empresas como Datacom, Padtec ha ampliado su portafolio hacia soluciones de capa 2 y capa 3, fortaleciendo su oferta integral en infraestructura de redes.

Impulsada por una fuerte orientación hacia la investigación y el desarrollo (I+D), Padtec se caracteriza por su capacidad innovadora para superar grandes distancias, romper barreras tecnológicas y ofrecer soluciones que contribuyen a conectar el mundo de manera eficiente, inteligente y resiliente.

IV. MARCO TEÓRICO

1. HISTORIA DE LA INTERNET

Internet nació en los años 70 a partir de un programa de DARPA que buscaba interconectar redes heterogéneas mediante una arquitectura abierta. En 1974, Vinton Cerf y un investigador de DARPA diseñaron el TCP/IP, protocolo que se convirtió en la base de Internet y fue adoptado oficialmente por el Departamento de Defensa en 1980.

Durante los años 80, la NSF expandió su alcance al sector académico mediante la NSFNET, creando una red troncal que interconectaba centros de supercomputación y conectaba redes regionales y locales. Paralelamente, aparecieron redes comerciales y, en los 90, la gestión pasó gradualmente del gobierno al sector privado.

En 1995, la NSF se retiró de la operación directa de la red, consolidando un ecosistema de proveedores comerciales interconectados. Actualmente, la evolución de Internet es gestionada por organismos como el IETF (desarrollo de estándares), la Internet Society (mantenimiento de estándares) y la ICANN (gestión de dominios y direcciones). [1]

2. PARÁMETROS DE LA RED DWDM

A continuación, se presentarán de manera breve algunos elementos clave de las redes DWDM, con el propósito de comprender con mayor claridad el papel que desempeñan los distintos equipos de red en este tipo de infraestructura. Asimismo, se busca dimensionar la importancia de estos elementos y resaltar cómo la aplicación de buenas prácticas contribuye al óptimo desempeño y a una mejor experiencia en la red.

Fundamentos de la Multiplexación DWDM y su Integración con IP

La tecnología DWDM (Dense Wavelength Division Multiplexing) constituye uno de los pilares fundamentales de las redes ópticas modernas, ya que posibilita la transmisión simultánea de múltiples señales ópticas a través de una sola fibra. Este principio se basa en la multiplexación de varias longitudes de onda, cada una transportando un canal independiente, lo que permite aprovechar de forma eficiente la enorme capacidad de la fibra óptica.

En una red DWDM, la señal óptica se genera a partir de transmisores láser, cada uno ajustado a una longitud de onda específica. Estas señales se combinan en un multiplexor DWDM, son transmitidas a través de la fibra, amplificadas mediante EDFA (Erbium-Doped Fiber Amplifiers) y finalmente separadas en un demultiplexor para ser entregadas a los receptores correspondientes. Adicionalmente, componentes como los OADM (Optical Add-Drop Multiplexers) permiten insertar o extraer canales en puntos intermedios de la red, incrementando la flexibilidad y escalabilidad de la infraestructura [2], como se puede apreciar en la ***Figura 1***.

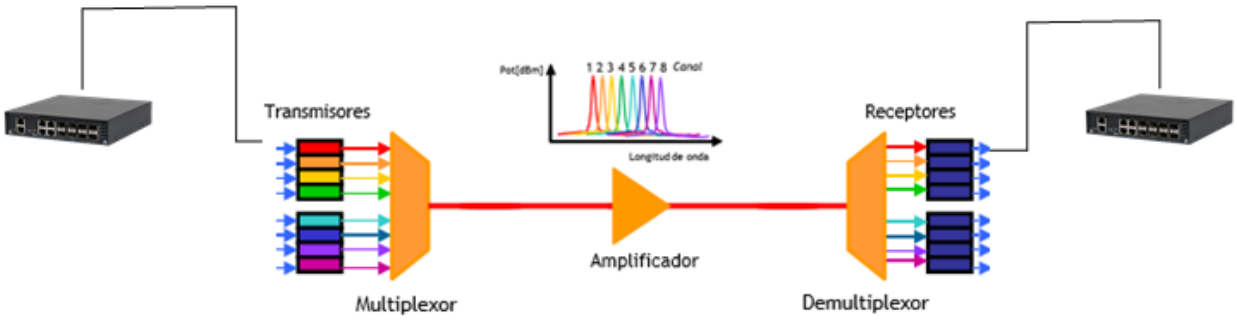


Figura 1: Redes IP a través de redes DWDM.

Un aspecto crucial de esta tecnología es su transparencia, lo que significa que las longitudes de onda pueden transportar diferentes tipos de tráfico y protocolos sin importar su formato. De esta manera, DWDM soporta simultáneamente IP, ATM, SONET/SDH y Ethernet, facilitando la coexistencia de múltiples servicios (voz, video y datos) sobre la misma infraestructura óptica [3].

En este contexto surge la arquitectura IP over DWDM (IPoDWDM), que elimina capas intermedias como SONET/SDH y permite que los paquetes IP se transmitan directamente sobre las longitudes de onda ópticas. Esta integración ofrece ventajas significativas:

- Reducción de latencia, al eliminar conversiones innecesarias entre capas.
- Mayor eficiencia en el uso del ancho de banda, aprovechando plenamente la capacidad de la fibra.
- Simplificación de la arquitectura de red, al reducir equipos intermedios y costos operativos.

No obstante, la implementación de DWDM y su uso para el transporte de IP plantea desafíos técnicos asociados a las características físicas del medio óptico. Fenómenos como la atenuación, la dispersión cromática y la relación señal-ruido óptico (OSNR) deben ser mitigados mediante técnicas de compensación, amplificación y monitoreo de calidad de señal para garantizar la correcta entrega de paquetes en largas distancias. [4]

En suma, la combinación de DWDM con IP constituye una solución estratégica para el crecimiento de internet y los servicios digitales, ofreciendo gran capacidad, escalabilidad y eficiencia, siendo un elemento clave en la evolución hacia redes troncales de alta velocidad y baja latencia.

En este contexto, resulta fundamental comprender los aspectos técnicos que hacen posible la implementación eficiente de estas redes. Entre ellos destacan parámetros como el espaciamiento entre canales, direcciones de propagación de la señal DWDM, potencias y ancho de banda en los sistemas DWDM de última generación. A continuación, se presentan las características más relevantes de este tipo de redes, con el fin de dar una visión clara de su funcionamiento y sus implicaciones en el despliegue de infraestructuras ópticas de alta capacidad.

2. ELEMENTOS DE LA RED DWDM

2.1. Fuentes de luz

Una propiedad clave de la propagación de ondas, es que si las ondas de luz tienen diferentes longitudes de onda, no se interfieran entre sí dentro de un medio.

Un láser puede generar pulsos de luz con una longitud de onda muy precisa. Cada una de estas longitudes de onda puede actuar como un canal de información independiente. Al combinar pulsos de diferentes longitudes de onda, es posible transmitir simultáneamente múltiples canales a través de una única fibra óptica, lo que maximiza la capacidad de transmisión y la eficiencia del sistema. Es clave en estos elementos su potencia, longitud de onda central y ancho espectral muy fino, para evitar que interfieran entre sí en sistemas DWDM. Igualmente se prefieren que sean tipo DFB por su estabilidad y ancho espectral.

2.2. Multiplexores

El multiplexor (MUX) es el equipo encargado de combinar las señales de entrada y, posteriormente, dividir esta señal dentro del sistema DWDM. El MUX integra diferentes señales de los clientes, que pueden variar en protocolo y velocidad. A cada una de estas señales se le asigna una longitud de onda específica, tanto para transmisión como para recepción, y se unifican en un solo haz de luz para ser transmitidas a través de la fibra óptica.

En el extremo receptor, el demultiplexor (DEMUX) separa nuevamente los componentes de la luz para entregar cada servicio de manera individual. Cabe resaltar que, en la práctica, lo más común es implementar sistemas bidireccionales, donde se utilizan dos fibras: una destinada a la transmisión y otra a la recepción, lo que permite mayor eficiencia y control en la gestión de la señal. No obstante, también existen soluciones unidireccionales en las que todo el tráfico se concentra en una sola dirección. Tanto los multiplexores como los demultiplexores pueden ser diseñados con tecnología pasiva o activa.

En la ***Figura 2*** se presenta un ejemplo de multiplexor y demultiplexor de 8 canales, donde se distinguen claramente las entradas y salidas correspondientes a cada canal. Adicionalmente, se incluyen los puertos COM, que permiten la gestión de la señal compuesta: COM OUT entrega la señal ya multiplexada, lista para ser enviada hacia el amplificador, mientras que COM IN recibe la señal proveniente de la planta externa, preparada para ser demultiplexada en los distintos canales.

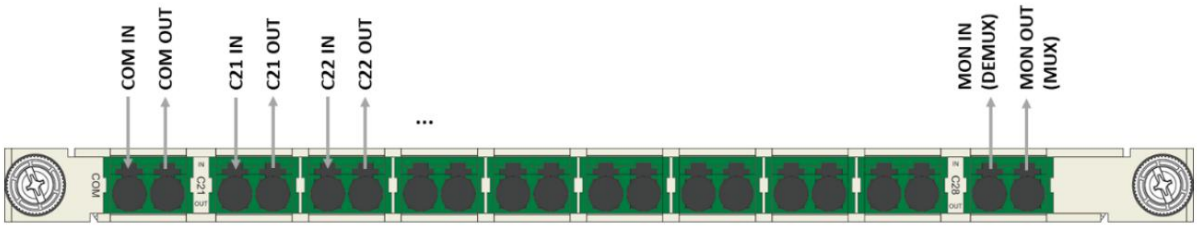


Figura 2: MUX/DEMUX Slim marca Padtec.

Fuente: LightPad i6400G Platform.

2.3. Amplificadores ópticos

Estos dispositivos son fundamentales en los sistemas DWDM, ya que su función principal es amplificar las señales que se propagan a través de la fibra, contrarrestando así los efectos de la atenuación. Los dos tipos de amplificadores ópticos más utilizados son el EDFA (Erbium-Doped Fiber Amplifier) y el amplificador Raman [4].

2.3.1. Amplificadores EDFA

Los amplificadores de fibras dopados con erbio (EDFA) son particularmente populares, operando en la región de 1550 nm, que es la ventana principal para sistemas DWDM. Estos dispositivos amplifican señales mediante un proceso llamado “emisión estimulada”, donde se utilizan diodo laser de bombeo para excitar electrones en la fibra. Los amplificadores EDFA pueden alcanzar ganancias de hasta 30 dB con potencias de bombeo relativamente bajas.

En la ***Figura 3*** se puede observar el comportamiento tanto de la señal como del ruido durante el proceso de amplificación en una topología típica DWDM. Es importante destacar que el EDFA amplifica de manera indiscriminada cualquier señal que reciba; sin embargo, también introduce un componente adicional de ruido debido a un fenómeno conocido como emisión espontánea amplificada (ASE, Amplified Spontaneous Emission).

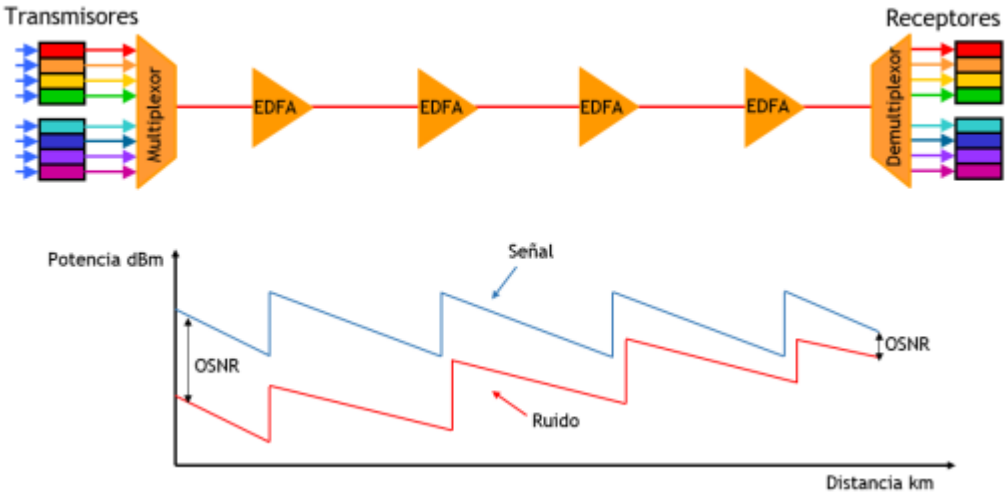


Figura 3: Desempeño del OSNR con amplificadores en cascada.

Este fenómeno ocurre porque los iones de Erbio, al regresar espontáneamente a su estado fundamental tras ser excitados, emiten fotones en la banda C (1500–1570 nm). Dichos fotones, al ser amplificados junto con la señal óptica de interés, incrementan el nivel de ruido acumulado en el sistema. Como consecuencia, la calidad de la señal se degrada cada vez que atraviesa un amplificador EDFA.

En un sistema que emplea N amplificadores, la degradación es acumulativa, por lo que el OSNR total al final del enlace puede calcularse mediante la Ecuación 3, donde OSNR representa la relación señal a ruido óptica asociada a cada amplificador en cascada.

$$\mathrm{OSNR}_{acumulado}(\mathrm{dB}) = \left(\frac{1}{\frac{1}{OSNR_{1(dB)}}+\frac{1}{OSNR_{2(dB)}}+\cdots+\frac{1}{OSNR_{N(dB)}}}\right) \quad (3)$$

Por otro lado, los amplificadores tipo Raman utilizan el efecto de dispersión estimulada Raman (SRS) para amplificar señales directamente en la fibra, aunque requieren potencias más altas, son más costosos de operar y no agregan ruido. Ambos tipos de amplificadores son importantes para mejorar la capacidad y el alcance de las comunicaciones ópticas.

3. PROTOCOLOS RELEVANTES EN LA CAPA DE RED

En la actualidad, el Protocolo de Internet (IP) constituye un pilar esencial en la arquitectura de las redes de comunicación, ya que permite la interconexión eficiente de dispositivos en un entorno cada vez más digitalizado. En esta sección se abordarán diversos elementos y protocolos que deben considerarse para el desarrollo del proyecto.

3.1. Red

Una red es un conjunto de dispositivos interconectados mediante medios de transmisión, que permiten el intercambio de datos, recursos e información bajo protocolos comunes. [5]

3.2. Dirección IP

Identificador único de un dispositivo en una red (pueden ser *IPV4* o *IPV6*).

3.3. Enrutamiento

El enrutamiento es el proceso mediante el cual un dispositivo de red selecciona la mejor trayectoria disponible para enviar paquetes de datos desde el origen hasta el destino, a través de una o varias redes interconectadas.

Existen dos grandes tipos:

- **Enrutamiento estático:** las rutas son configuradas manualmente por el administrador.
- **Enrutamiento dinámico:** los equipos de red utilizan protocolos (OSPF, RIP, BGP, EIGRP, etc.) para intercambiar información de rutas y adaptarse automáticamente a cambios en la red.[5]

3.3.1. OSPF (Open Shortest Path First)

Gracias a que es un protocolo de estado de enlace, detecta los cambios en la red y recalcula rutas de forma rápida, garantizando disponibilidad y resiliencia.

3.4. MPLS (Multiprotocol Label Switching)

Es una tecnología de conmutación y encaminamiento en redes de telecomunicaciones que dirige los paquetes de datos utilizando **etiquetas (labels)** en lugar de direcciones IP tradicionales.

En lugar de que cada router analice la cabecera IP para decidir hacia dónde enviar un paquete, MPLS asigna una etiqueta corta y fija. [6]

4. Gestión de redes

El primer componente principal en la gestión de redes consiste en el dispositivo que debe ser gestionado. Los distintos equipos gestionados reciben el nombre de (NEs). Para ser gestionado adecuadamente, deben participar en el proceso de gestión.

Para ser administrado, un elemento de red debe ofrecer una interfaz de gestión a través de la cual un sistema de gestión pueda comunicarse con dicho elemento con fines de administración. Por ejemplo, la interfaz de gestión permite que el sistema de gestión envíe una solicitud al elemento de red. Esta podría ser, por ejemplo, una solicitud para configurar una subinterfaz, recuperar datos estadísticos sobre la utilización de un puerto, u obtener información sobre el estado de una conexión.

4.1. Comunicación Manager-Agente

En la terminología de la gestión de redes, *manager* y *agent* son términos fundamentales: el primero hace referencia a los sistemas que gestionan, mientras que el segundo corresponde a los sistemas que son gestionados.

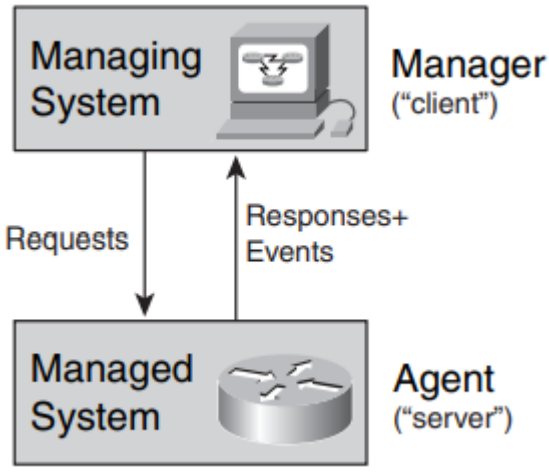


Figura 4: Relación cliente servidor.

Fuente 1:lexander-clemm-network-management-fundamentals-2007[1].pdf

Una relación de comunicación asimétrica muy conocida es la de cliente/servidor. Por lo tanto, vale la pena resaltar la relación entre manager/agent y cliente/servidor.

Como se muestra en la ***figura 4***, el agent corresponde con un servidor, mientras que el mánager se asemeja a un cliente.

4.2. Base de información de Gestión (MIB)

Es un almacén de datos conceptual que representa la visión de gestión de un dispositivo administrado. Los datos en la MIB constituyen la información de gestión y sirven como referencia para las operaciones de administración.

Por ejemplo, los puertos de red de un dispositivo pueden verse como una tabla conceptual, donde cada puerto corresponde a una fila y sus propiedades (como protocolo soportado o número de paquetes transmitidos) aparecen como columnas.

La MIB no es una base de datos real, sino una representación abstracta del dispositivo. Cuando una aplicación de gestión modifica una entrada en la MIB, en realidad se está cambiando la configuración del dispositivo físico y, con ello, su comportamiento en la red.

4.3. Protocolo SNMP (Simple Network Management Protocol)

El SNMP es el protocolo estándar más empleado para la gestión de redes IP, ya que permite la comunicación entre el *manager* y los *agents* con el fin de supervisar, configurar y recibir notificaciones de los dispositivos gestionados. La información intercambiada se basa en la MIB (Management Information Base), lo que garantiza un modelo uniforme de representación de datos.

SNMP opera sobre UDP y define tres operaciones fundamentales:

- **Get**: el *manager* consulta parámetros del agente.
- **Set**: el *manager* modifica valores de configuración en el agente.
- **Trap/Inform**: el agente notifica al *manager* eventos o cambios relevantes.

A lo largo del tiempo, el protocolo ha evolucionado en distintas versiones, que se diferencian principalmente por las mejoras en eficiencia y seguridad:

- **SNMPv1**: primera versión (1988), caracterizada por su simplicidad. Proporciona operaciones básicas de consulta y configuración, pero con mecanismos de seguridad muy limitados (solo autenticación basada en *community strings* en texto plano).

- **SNMPv2c**: introdujo mejoras en eficiencia y nuevas operaciones, como *GetBulk* para recuperar grandes volúmenes de información. Sin embargo, su seguridad seguía siendo débil, al mantener el mismo esquema de *community strings*.
- **SNMPv3**: versión más robusta y actualmente recomendada. Incorpora un marco de seguridad que permite autenticación, control de acceso y cifrado de la información, garantizando la integridad y confidencialidad de los datos intercambiados.

  En la actualidad, **SNMPv3** constituye el estándar en entornos críticos debido a sus capacidades de seguridad, mientras que SNMPv1 y v2c siguen presentes en redes heredadas por su simplicidad de implementación. [7]

5. Equipos de red

5.1. Router

Un Router es un dispositivo que enruta la información a través de distintos caminos, asegurando el cumplimiento de políticas, protocolos y medidas de seguridad. Su función principal es facilitar la comunicación eficiente entre el emisor y el receptor, contribuyendo a la creación de amplias redes de comunicación.

En el ámbito de las telecomunicaciones, los Routers a menudo se confunden con otros dispositivos como concentradores de red, módems o switches. Sin embargo, gracias a su capacidad avanzada de procesamiento de datos, los Routers pueden integrar las funciones de estos dispositivos y conectarse con ellos para optimizar el acceso a internet o para conFigurar redes empresariales más robustas.

El funcionamiento de un router se basa en la gestión de datos de la red mediante paquetes. Estos paquetes contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples, como interacciones web. Cada paquete de datos está compuesto por varias capas, una de las cuales transporta información importante, como el emisor, el tipo de datos, el tamaño y, lo más importante, la dirección IP, que es fundamental para el protocolo de internet. El router es capaz de leer esta capa, priorizar los datos y seleccionar la ruta óptima para la transmisión de cada paquete de datos

En este proyecto se emplearán switches Datacom con funcionalidades de capa 3, equivalentes a las de un router. Estos dispositivos recibirán una serie de Configuraciones que serán recolectadas mediante el protocolo SNMP y, posteriormente, analizadas a través de un algoritmo desarrollado en Python

5.2. Switch

Los switches son dispositivos esenciales en cualquier red, ya que su función principal es conectar múltiples dispositivos, como computadoras, puntos de acceso inalámbricos, impresoras y servidores, dentro de la misma red. Un switch facilita la comunicación y el intercambio de información entre los dispositivos conectados, permitiendo que operen de manera coordinada y eficiente.

Además de conectar dispositivos, los switches gestionan el flujo de datos en la red mediante la segmentación de tráfico, lo que reduce la congestión y mejora el rendimiento general. Utilizan direcciones MAC (Media Access Control) para dirigir los datos al dispositivo correcto, lo que garantiza una transmisión eficiente y segura. Los switches también pueden ser conFigurados para manejar tráfico de red más avanzado, como la priorización de ciertos tipos de datos o la creación de VLANs (Virtual Local Area Networks), que segmentan una red física en varias redes lógicas para mejorar la seguridad y la gestión del tráfico [8].

En la ***Figura 5*** se presenta el switch Datacom, un dispositivo que, además de cumplir con las funciones propias de conmutación, incorpora características avanzadas propias de un router. Entre ellas se destacan el soporte para enrutamiento de capa 3, la segmentación de redes mediante VLANs, y la gestión eficiente del tráfico. Adicionalmente, este equipo ofrece la posibilidad de implementar MPLS (Multiprotocol Label Switching), siempre que se adquiera la licencia correspondiente, lo que lo convierte en una solución versátil para entornos de red de alto rendimiento.

***Figura 5*:** Switch DM4370

Fuente: DATACOM. Productos switches.

5.3. SERVIDOR

Un servidor es un equipo de cómputo diseñado para manejar, procesar y almacenar grandes cantidades de datos, además de proporcionar servicios a otros dispositivos en una red. Los servidores son fundamentales en infraestructuras tecnológicas, ya que soportan aplicaciones críticas, gestionan bases de datos, alojan sitios web y permiten la comunicación y colaboración entre diferentes sistemas y usuarios.

Para este proyecto, se utilizará el servidor Dell PowerEdge R660xs (ver la Figura 4), diseñado para ofrecer un alto rendimiento con una combinación equilibrada de recursos de procesamiento, memoria y almacenamiento. Este servidor es ideal para aplicaciones exigentes como el monitoreo de redes, ya que cuenta con procesadores escalables que proporcionan una robusta capacidad de procesamiento, garantizando un desempeño óptimo. Su arquitectura está optimizada para maximizar la eficiencia energética y la capacidad de enfriamiento, aspectos importantes para la operación continua y fiable en entornos de centros de datos. La capacidad de expansión del servidor permite la incorporación de múltiples unidades de almacenamiento y tarjetas de red de alta velocidad, facilitando el manejo de grandes volúmenes de datos y monitoreo en tiempo real de múltiples variables de desempeño. Al utilizar Zabbix en este servidor, se garantiza una plataforma de monitoreo potente y escalable, capaz de gestionar de manera eficiente las necesidades de supervisión de redes complejas, proporcionando alertas precisas y análisis detallados que son esenciales para mantener la disponibilidad y calidad del servicio en infraestructuras de telecomunicaciones.

Figura 6: Servidor PowerEdge R660xs.

6. ZABBIX

Zabbix fue desarrollado por Alexei Vladishev y actualmente es mantenido por la empresa Zabbix SIA. Su propósito principal es ofrecer una solución integral para el monitoreo de infraestructuras tecnológicas, abarcando redes, servidores, máquinas virtuales, bases de datos, sitios web, servicios en la nube y aplicaciones empresariales.

Gracias a sus capacidades, Zabbix permite recopilar y visualizar en tiempo real parámetros críticos de desempeño —como RX, TX u OSNR en equipos de red— facilitando la supervisión proactiva, la detección temprana de fallos y la optimización del rendimiento del sistema. Esta herramienta es ampliamente utilizada en entornos corporativos por su flexibilidad, escalabilidad y compatibilidad con diversos protocolos de monitoreo.[7]

6.1. Funcionamiento de Zabbix

Para este proyecto, Zabbix se ha instalado en el servidor Dell PowerEdge R660xs, con un sistema operativo en la máquina virtual Ubuntu 24.04 (Noble), para recolectar y monitorear la información de las interfaces óptica utilizando el protocolo SNMP.

Zabbix es compatible con agentes para sistemas operativos como Linux, Mac y Windows, que se instalan en los servidores y estaciones de trabajos a ser monitoreados. También permite la supervisión en tiempo real de una variedad de dispositivos, incluidos impresoras, routers, switches, y sensores de temperatura y humedad. [9]

- **Alertas configurables:** Ofrece la capacidad de configurar notificaciones personalizadas para eventos específicos en la red.
- **Gráficos en tiempo real:** Proporciona visualizaciones actualizadas al instante de los datos monitorizados, facilitando la interpretación y análisis.
- **Capacidad de monitoreo:** Permite una supervisión detallada de múltiples dispositivos y servicios en la red.
- **Almacenamiento de datos históricos:** Conserva un registro de los datos monitorizados para análisis y referencias futuras.
- **Configuración dinámica:** Facilita ajustes en tiempo real para adaptarse a las necesidades cambiantes de la red.

6.2. Ventajas de Zabbix

Utilizar Zabbix para el monitoreo de red en este proyecto presenta varias ventajas significativas:

- **Código abierto y seguridad:** Zabbix es una solución de código abierto, lo que permite su uso sin restricciones y ofrece seguridad mediante la disponibilidad de su código fuente. Además de Zabbix, se incluyen todos los componentes necesarios, como Linux, Apache, MySQL/PostgreSQL y PHP.
- **Administración centralizada:** Zabbix cuenta con un sistema de administración centralizado, accesible a través de una interfaz web que permite gestionar todos los dispositivos de la red desde un único lugar, facilitando la supervisión y el control.
- **Gestión de usuarios:** El sistema incluye un manejo robusto de usuarios, con autenticación mediante contraseñas, asegurando que solo personal autorizado pueda acceder y gestionar la red.
- **Alertas automatizadas:** Zabbix permite conFigurar alertas automáticas, que se envían a dispositivos específicos a través de correo electrónico o SMS cuando se detecta un problema en la red, asegurando una respuesta rápida a cualquier incidente.
- **Detección de dispositivos:** Tiene la capacidad de identificar y monitorear una amplia variedad de dispositivos de red, como routers, switches, servidores, impresoras y otros periféricos, utilizando varios protocolos como SNMP (versiones 1, 2 y 3).

- **Visualización de datos:** Zabbix integra capacidades avanzadas de visualización que facilitan el trabajo con los datos de la red, permitiendo análisis más rápidos e inteligentes.
- **Mantenimiento de datos:** Incluye un sistema de limpieza que mantiene los datos actualizados y organizados, lo que es importante para una gestión eficiente y precisa de la red.

6.3. Características de Zabbix

- **Monitorización proactiva**
  - Zabbix permite la monitorización sin agente, lo que significa que puede supervisar dispositivos y servicios sin necesidad de instalar software adicional.
  - Puede monitorizar servicios remotos como FTP, SSH, HTTP, entre otros, asegurando la disponibilidad y rendimiento de aplicaciones críticas.
  - Ofrece soporte completo para el protocolo SNMP en sus versiones 1, 2 y 3, incluyendo la gestión de traps SNMP.

7. ELEMENTOS DE ZABBIX

7.1. Agente Zabbix

Un componente esencial de Zabbix es su capacidad para monitorear recursos de red en tiempo real, utilizando el protocolo SNMP. El agente nativo de Zabbix, desarrollado en lenguaje C, está diseñado para ejecutarse en múltiples plataformas compatibles, como Linux y Windows. Este agente es responsable de recopilar datos cruciales sobre el rendimiento de los dispositivos en la red, incluyendo el uso de CPU, memoria, capacidad de disco, interfaces de red, y la velocidad de transmisión de datos.[9]

La versatilidad del agente permite a Zabbix integrar y supervisar diversos sistemas operativos y dispositivos de manera eficiente, asegurando que todos los aspectos críticos de la red sean monitorizados continuamente. Esto garantiza que los administradores de red tengan acceso a

información detallada y precisa en tiempo real, facilitando la toma de decisiones informadas y la rápida resolución de problemas.

7.2. Ítems

Los elementos en Zabbix son módulos que recopilan datos de un host. Al configurar un nuevo host, es necesario agregar estos elementos para iniciar la recopilación de datos en tiempo real. Esto permite un monitoreo continuo y preciso del rendimiento y estado del host, asegurando una supervisión efectiva de la red. [9]

7.3. Host y grupos de hosts

Los hosts en Zabbix representan los dispositivos que se van a monitorear, como servidores, estaciones de trabajo, routers, y switches. Para una mejor organización, estos dispositivos pueden agruparse en "group hosts", lo que facilita la gestión y supervisión de múltiples equipos dentro de una misma categoría o función. Esta estructura organizada permite un monitoreo más eficiente y centralizado de los dispositivos en la red.

7.4. Plantillas o templates

En Zabbix, el uso de plantillas es una estrategia eficiente para optimizar la Configuración y reducir la carga de trabajo. Una plantilla es un conjunto predefinido de entidades que pueden aplicarse a varios hosts de manera conveniente. Estas entidades incluyen elementos (ítems), disparadores (triggers), gráficos, tableros (dashboards), reglas de descubrimiento de bajo nivel (low-level discovery rules), y escenarios web.

Dado que muchos dispositivos en el mercado son idénticos o muy similares, una plantilla creada para uno de ellos puede reutilizarse en otros con características similares. Al vincular una plantilla a un host o dispositivo, todas las entidades incluidas se añaden automáticamente al host, lo que facilita el monitoreo y asegura una Configuración consistente y eficiente en toda la infraestructura de red.

7.5. Discovery

Zabbix ofrece una funcionalidad de descubrimiento automático de redes que es tanto flexible como eficaz, diseñada para acelerar la implementación del sistema y simplificar su gestión. Este proceso de descubrimiento en Zabbix se basa en varios métodos:

Información del agente SNMP: Emplea datos obtenidos a través del protocolo SNMP para descubrir y agregar dispositivos a la red.

Información del agente de Zabbix: Utiliza los datos recopilados por los agentes de Zabbix instalados en los dispositivos para identificar nuevos hosts y servicios.

Rangos de IP: Permite identificar y agregar dispositivos en un rango específico de direcciones IP.

Disponibilidad de servicios externos: Detecta dispositivos y servicios externos que están disponibles en la red.

Este enfoque integral permite a Zabbix automatizar la detección de dispositivos y servicios, reduciendo el tiempo necesario para la configuración inicial y garantizando una administración más eficiente de la red. [10]

7.6. Interfaz web

Zabbix facilita el acceso a los datos de monitoreo y Configuraciones a través de una interfaz web accesible desde cualquier plataforma. Esta interfaz basada en la web permite a los administradores gestionar y visualizar la información de monitoreo de manera eficiente, sin importar el sistema operativo o dispositivo que estén utilizando.

8. PYTHON

Python es uno de los lenguajes de programación más utilizados en la actualidad gracias a su simplicidad, versatilidad y amplia comunidad de desarrolladores. En el campo del análisis de texto ofrece ventajas notables, ya que cuenta con librerías especializadas como NLTK, spaCy, TextBlob y scikit-learn [11], que facilitan tareas como:

- Procesamiento de Lenguaje Natural (NLP): segmentación de oraciones, tokenización de palabras, lematización y eliminación de stopwords.

- Extracción de información: identificación de entidades nombradas (personas, lugares, organizaciones) y palabras clave.
- Análisis de sentimientos y clasificación: evaluación de opiniones en texto y categorización de documentos.
- Análisis estadístico y visualización: gracias a librerías como pandas, NumPy y matplotlib, es posible procesar grandes volúmenes de texto y visualizar patrones.

Estas funcionalidades hacen de Python una herramienta ideal para proyectos de monitoreo, correlación de eventos y generación de reportes automáticos basados en datos no estructurados. Por ejemplo, a la hora de analizar texto como la Configuración de red dada por los equipos de red.

8.1. API de Python para Conectarse con Zabbix

Zabbix es una plataforma de monitoreo de clase empresarial que permite supervisar servidores, aplicaciones, dispositivos de red y servicios en tiempo real. Python dispone de una API oficial y de librerías como py-zabbix, que simplifican la interacción con Zabbix desde scripts o aplicaciones externas.

Las principales funcionalidades de la API de Zabbix con Python son:

- Autenticación y gestión de sesiones mediante tokens seguros.
- Consulta de métricas en tiempo real de equipos monitoreados (uso de CPU, memoria, tráfico de red, etc.).
- Automatización de tareas como creación de hosts, plantillas o ítems de monitoreo.
- Extracción de datos históricos para su análisis y correlación con otros eventos. [9]
- Integración con otras aplicaciones para generar reportes, dashboards personalizados o sistemas de alertas inteligentes.

Gracias a esta integración, es posible desarrollar soluciones avanzadas que combinen el poder de análisis de Python con la capacidad de monitoreo en tiempo real de Zabbix, facilitando así la detección temprana de fallas y la optimización del rendimiento de la red y los sistemas.

9. METODOLOGÍA

Tabla 1 :Metodologia a implementar.

1. Identificar las variables más relevantes que impactan el desempeño de las redes de transporte ópticas, con el fin de priorizar su monitoreo y captura de datos con una frecuencia suficie	1.1. Se consultó y documentó información de organismos como TM Forum, ITU-T, ISO/IEC 20000 e ISO/IEC 30141. 1.2. Se identificaron los parámetros clave en el desempeño de los clientes que requerían un seguimiento detallado mediante la plataforma de monitoreo seleccionada.
2. Obtener un set de datos relacionados con las variables identificadas, mediante la Configuración de Zabbix para la supervisión de redes IP y ópticas, utilizando los OID (objetos identificadores) presentes en los equipos de red de la marca Datacom, así como en otros equipos de red comercializados y soportados por la empresa	2.1. Se documentó el procedimiento de instalación de la plataforma Zabbix en una máquina virtual. 2.2. Se instaló Zabbix en el servidor disponible. 2.3. Se conFiguraron los distintos OID en los equipos Datacom. 2.4. Se recolectaron los parámetros y datos identificados de interés.
3. Crear un algoritmo en Python, para el análisis de los datos recolectados por el servidor a través del protocolo SNMP (Simple Network Management Protocol), que permita evaluar el comportamiento de los distintos parámetros y contrastarlos con buenas prácticas dados por el fabricante o estándares internacionales	3.1. Se realizaron pruebas de consultas básicas mediante la conexión a la API de Zabbix desde un entorno en Python. 3.2. Se instalaron las librerías necesarias para la extracción de información desde texto plano semi-estructurado, común en la salida de los comandos de los dispositivos de red. 3.3. Se extrajeron los parámetros y datos de interés definidos anteriormente.
4. Desarrollar un dashboard que permita la visualización amigable de los datos y su comparación con un desempeño esperado y realizar recomendaciones	4.1. Se seleccionó la herramienta más adecuada para la visualización de datos, generación de estadísticas y presentación de recomendaciones dirigidas a los clientes. 4.2. Se integraron los datos tratados en Python con la herramienta elegida para crear dashboards interactivos orientados al análisis de información relevante. 4.3. La evaluación se llevó a cabo en conjunto con el personal de Padtec, tomando como referencia la retroalimentación del cliente, quien definió y

priorizó las métricas de mayor relevancia para sus necesidades.

10. RESULTADOS

A continuación, se muestra un consolidado a través del siguiente diagrama de flujo, donde se pueden apreciar los momentos más relevantes en la elaboración del actual proyecto.

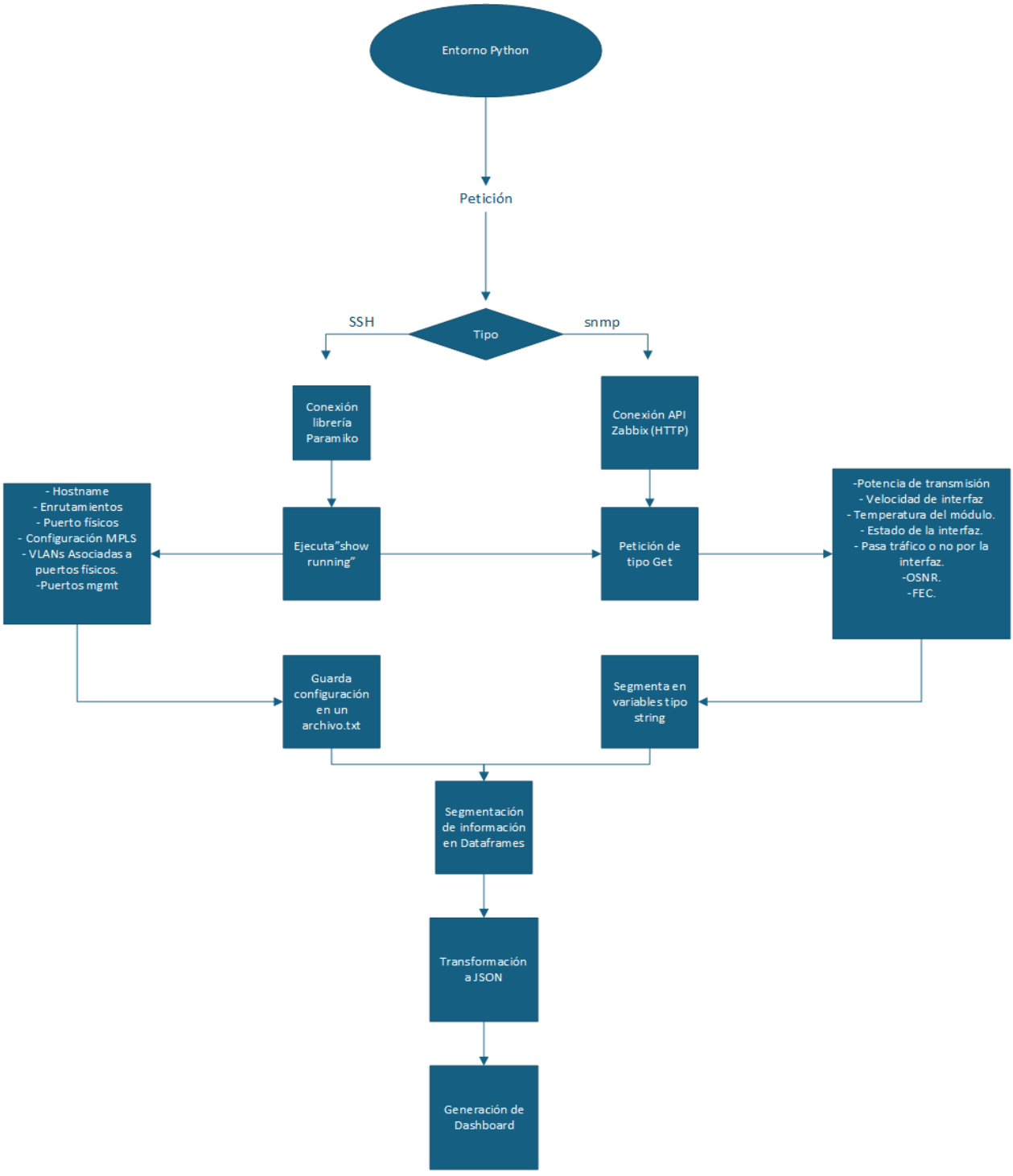


Figura 7: Algoritmo implementado.

CONFIGURACIÓN DEL PROTOCOLO SNMP

Para establecer una comunicación adecuada entre los quipos DATACOM y el entorno Python, es necesario configurar correctamente el protocolo SNMP, ya que este permite responder a las solicitudes de los mediante los OID y las distintas peticiones que se realicen desde el servidor donde se corra Python.

El primer paso consiste en asegurar un direccionamiento correcto de las interfaces, garantizando que el router disponga de una dirección IP dentro de la misma red que el servidor y del entorno Python, lo que facilita una conectividad exitosa.

Una vez establecida la conectividad entre los dispositivos, se procede a la Configuración del protocolo SNMP en el router. Para ello, se utilizan los siguientes comandos.

```
# configure terminal
# snmp agent version v2c
# snmp agent ip 192.168.128.34
# snmp agent enabled
# commit
```

1. IMPLEMENTACIÓN DEL HYPER-V EN EL SERVIDOR

Para la instalación del hipervisor encargado de gestionar las máquinas virtuales, se utilizó la aplicación Hyper-V de Windows. Para ello, fue necesario descargar la imagen ISO correspondiente y realizar la instalación en el servidor mediante una unidad USB de arranque que contuviera dicha imagen. Al finalizar el proceso, el sistema presenta las siguientes opciones. [10]

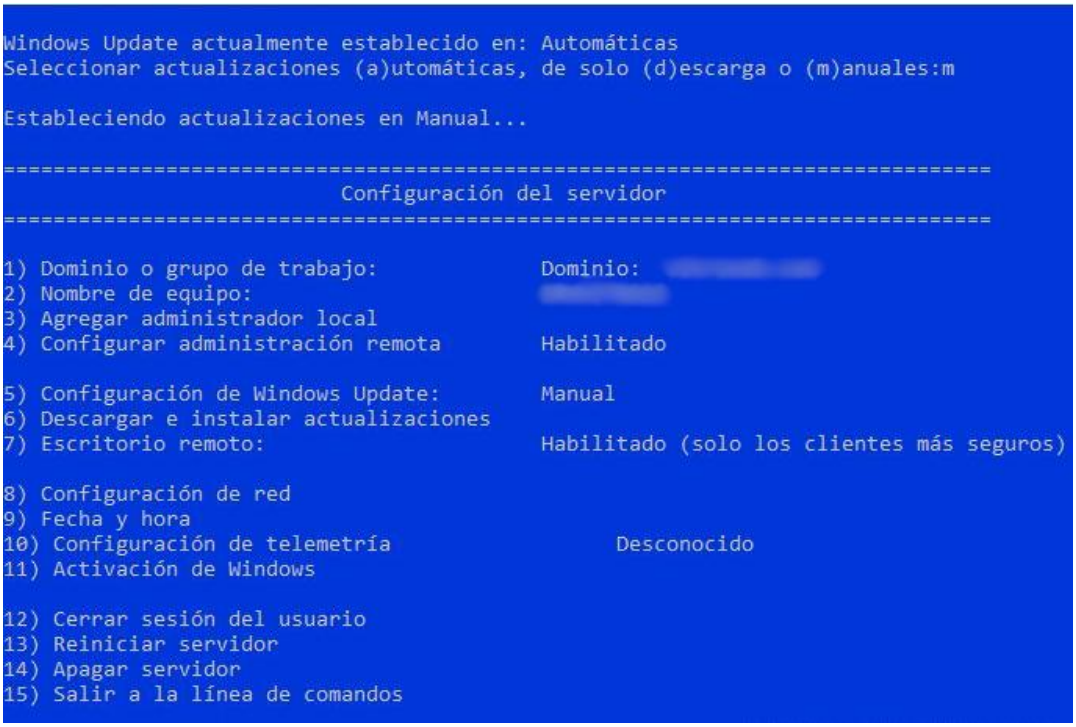


Figura 8: Configuración del servidor.

2. SISTEMA DE MONITOREO

En la primera fase, Zabbix se implementa como una herramienta fundamental para supervisar parámetros clave, tales como:

1. ***POT RX (Power Optical Receive / Potencia óptica recibida):*** Es la medida de la intensidad de la señal óptica que un receptor (como un módulo óptico, transceptor o puerto de una OLT/ONT) recibe a través de una fibra óptica.[12]

Recomendación:

- Mantener la potencia óptica dentro del rango de sensibilidad del receptor, que depende del tipo de módulo óptico.
- Valores típicos: entre –28 dBm y –8 dBm para SFP/GPON; en DWDM puede variar según el amplificador o la modulación.
- Riesgo: Si la potencia es muy alta, puede saturar el receptor; si es muy baja, habrá pérdida de paquetes o desconexión del enlace.

  Normas relacionadas: ITU-T G.984 (GPON), ITU-T G.694 (DWDM).

2. ***POT TX (Power Optical Transmit / Potencia óptica transmitida):*** Es la medida de la intensidad de la señal óptica emitida por un dispositivo transmisor (como una OLT, ONT o transceptor óptico) hacia la fibra óptica.[12]

Recomendación:

- Debe estar dentro del rango nominal especificado por el fabricante del transceptor.
- Valores típicos: entre 0 dBm y +5 dBm para enlaces largos (DWDM), o –3 dBm a +2 dBm para GPON.
- Ajustar la potencia si hay amplificadores o atenuadores intermedios.
- Riesgo: Exceso puede dañar el receptor remoto o distorsionar la señal.

3. ***OSNR (Optical Signal-to-Noise Ratio)*****:** Es un parámetro que mide la calidad de una señal óptica en un sistema de comunicaciones de fibra. Indica la proporción entre la potencia de la señal útil y la potencia del ruido óptico presente en el mismo ancho de banda.[13]

Recomendación:

- Mantener OSNR ≥ 20 dB para sistemas 10G y ≥ 25 dB para 100G o DWDM coherente.
- Un valor bajo de OSNR indica alta interferencia o degradación óptica.
- Normas: ITU-T G.692, G.959.1.
- Buena práctica: Monitorear OSNR por canal para evitar degradación progresiva.

4. ***FEC (Forward Error Correction):*** Es una técnica empleada en los sistemas de comunicación óptica para detectar y corregir errores en los datos sin necesidad de retransmisión.[14]

El principio básico consiste en añadir bits redundantes al flujo de datos transmitido, los cuales permiten al receptor identificar y reparar errores ocasionados por ruido, atenuación o distorsión durante la transmisión por la fibra óptica.

Recomendación:

- Mantener FEC activo en enlaces de larga distancia o cuando se usen tasas >10 Gbps.
- Verificar que el BER (Bit Error Rate) antes de FEC sea ≤ 1E–3 y después de FEC ≤ 1E–12.
- Norma: ITU-T G.975 (FEC en sistemas ópticos).
- Buena práctica: Activar FEC cuando la potencia o el OSNR estén cerca de los límites mínimos.

5. Estatus del puerto*:* Indica el estado operativo y administrativo de un puerto físico o lógico dentro de un dispositivo de red óptico, como una OLT, ONT, switch o router. Este parámetro permite determinar si el puerto está habilitado, activo, en error, o fuera de servicio, y es fundamental para el monitoreo y diagnóstico de la red.[15]

Recomendación:

- Supervisar constantemente el estado (UP/DOWN).
- Estado DOWN frecuente: revisar cableado, conectores, SFP, potencia RX.
- En equipos GPON/EPON, el puerto debe mostrar estado operativo "O5" para sesión activa.
- Buena práctica: Usar alarmas SNMP o Zabbix para detectar caídas automáticas.

6. ***Estatus operativo***

Recomendación:

- Indica si el puerto o módulo está funcional, administrativamente habilitado y sin fallos.

- Administratively down: deshabilitado por configuración.
- Operationally down: problema físico o de señal.
- Mantener sincronía entre el estado administrativo y operativo.

7. ***Negociación (Auto-Negotiation)*****:** Representa el estado funcional actual de un puerto, interfaz o dispositivo dentro de una red óptica. A diferencia del estatus administrativo (que depende de la configuración del usuario o del sistema), el estatus operativo refleja si el elemento realmente está funcionando y transmitiendo datos de manera efectiva. [15]

Recomendación:

- En enlaces Ethernet o ópticos eléctricos (SFP RJ45): mantener auto-negociación activa si ambos extremos la soportan.
- En enlaces ópticos fijos (10G, DWDM): suele deshabilitarse y fijarse la velocidad manualmente.
- Evitar desajustes (duplex mismatch) entre extremos.
- Norma: IEEE 802.3 (Ethernet).

8. Temperatura: La temperatura en un sistema óptico se refiere al valor térmico operativo de los componentes electrónicos y ópticos de un dispositivo, como módulos SFP/GPON, transceptores, OLTs, o ONTs. Se mide en grados Celsius (°C) y constituye un parámetro crítico para garantizar la estabilidad, rendimiento y vida útil del equipo.

Recomendación:

- Rango seguro típico para transceptores: 0°C a 70°C (comercial), –40°C a 85°C (industrial).
- Mantener ventilación adecuada y evitar puntos calientes en el rack.
- Riesgo: altas temperaturas afectan la potencia óptica y reducen la vida útil del SFP.
- Normas: Telcordia GR-468 (calificación de componentes ópticos).

9. Tiempo de actividad (Uptime): El tiempo de actividad (Uptime) es el período continuo durante el cual un dispositivo o sistema de red óptico permanece en funcionamiento sin interrupciones. Se mide normalmente en horas, días o porcentajes (%) y refleja la disponibilidad operativa del equipo.[16]

Recomendación:

- Uptime alto indica estabilidad del enlace.
- Reinicios frecuentes sugieren fallos eléctricos, térmicos o de configuración.
- En equipos de red críticos, se recomienda >99.9% de disponibilidad anual (equivale a menos de 9 h de caída/año).
- Referencia: ITU-T E.800 (métricas de calidad y disponibilidad).

Estos indicadores resultan esenciales para garantizar el éxito del proyecto. Una vez adquirido un conocimiento sólido del protocolo SNMP y tras realizar prácticas de Configuración en la máquina virtual, se procedió a la implementación de Zabbix en el servidor local de la empresa.

2.1. Instalación del servidor Zabbix 7.0 LTS

Se ha destinado un espacio en el servidor local para la instalación de una máquina virtual con el sistema operativo Ubuntu Server 24.04. Esta distribución de Linux, al ser gratuita y de código abierto, resulta adecuada para los objetivos del proyecto.
Para garantizar un funcionamiento óptimo, Zabbix requiere recursos mínimos de hardware, tanto en memoria física como en espacio en disco. La capacidad necesaria varía según la cantidad de equipos (*hosts*) y los parámetros a monitorear; sin embargo, se recomienda contar con al menos 8 GB de espacio en disco y 2 núcleos de CPU.
Cumplidos estos requisitos, el siguiente paso consiste en descargar la versión de Zabbix correspondiente al sistema operativo, seleccionando en la página oficial la opción compatible con Ubuntu 24.04.

2.1.1. Instalación del repositorio

Lo primero que se debe hacer es la instalación del repositorio oficial de Zabbix lo cual es necesario ejecutar los siguientes pasos y consigo los respectivos comandos en el servidor:

1. Instalar el repositorio de Zabbix.

```
# rpm -Uvh
https://repo.zabbix.com/zabbix/7.4/release/alma/10/noarch
/zabbix-release-latest-7.4.el10.noarch.rpm
```

`# dnf clean all` Instala el servidor, la interfaz y el agente de Zabbix.

```
# dnf install zabbix-server-mysql zabbix-web-mysql
zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-
policy zabbix-agent
```

2. Crear base de datos inicial.

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4
collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by
'password';
mysql> grant all privileges on zabbix.* to
zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

En el servidor Zabbix, importe el esquema y los datos iniciales. Se le pedirá que ingrese la contraseña recién creada.

```
# zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz |
mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

3. ConFigurar la base de datos para el servidor Zabbix

```
DBPassword=password
```

4. Inicia los procesos del agente y del servidor Zabbix

```
# systemctl restart zabbix-server zabbix-agent httpd php-
fpm
```

```
# systemctl enable zabbix-server zabbix-agent httpd php-fpm
```

2.1.2. Configuración de la interfaz web

Una vez verificado que todos los servicios se encuentran activos, es posible acceder a la interfaz de Zabbix mediante la URL correspondiente a la dirección IP 192.168.128.35 del servidor En este caso, el acceso se realiza ingresando:

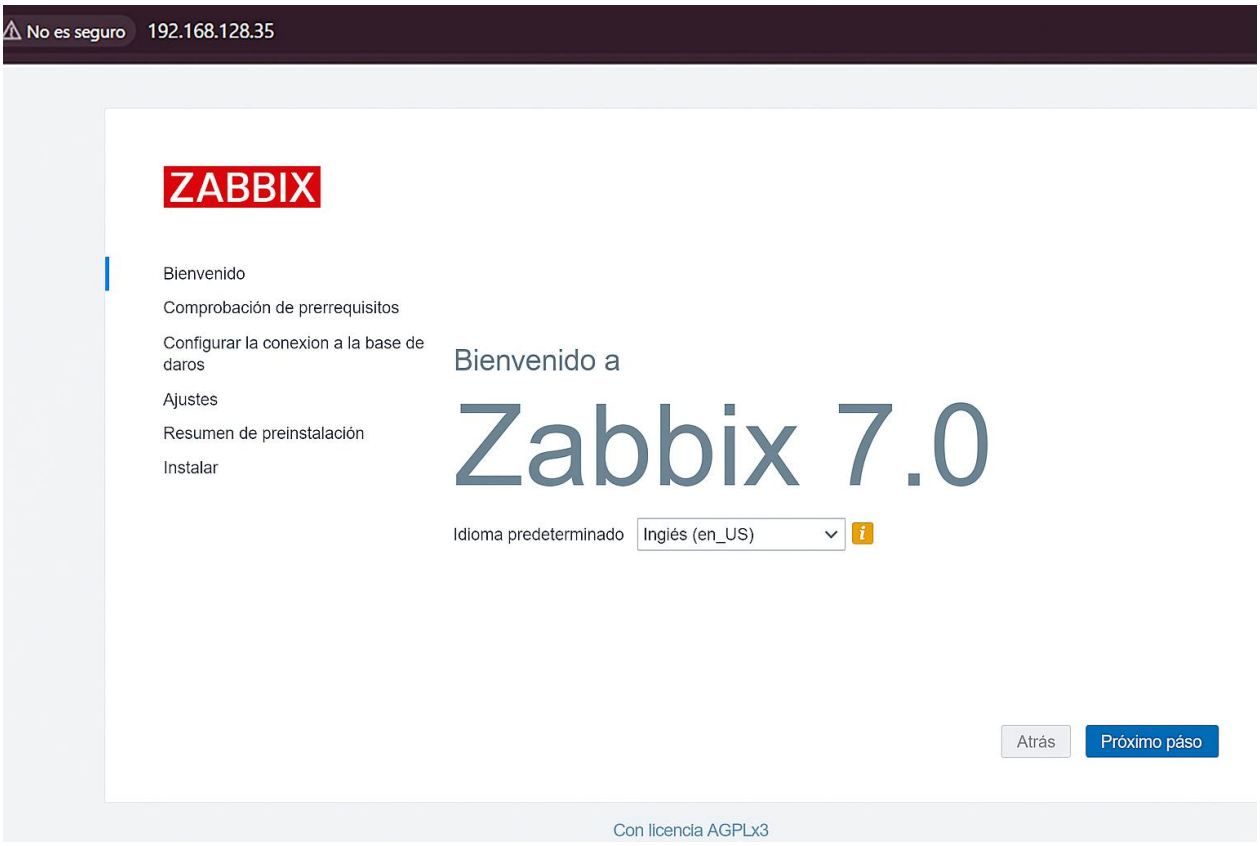


Figura 9: Interfaz de bienvenida.

2.1.3. Análisis de prerrequisitos

Al ingresar a la interfaz, el siguiente paso consiste en verificar los requisitos previos del servidor. Es indispensable que todos los componentes aparezcan en estado **“OK”**,

ya que solo de esta manera es posible continuar con el proceso de instalación.

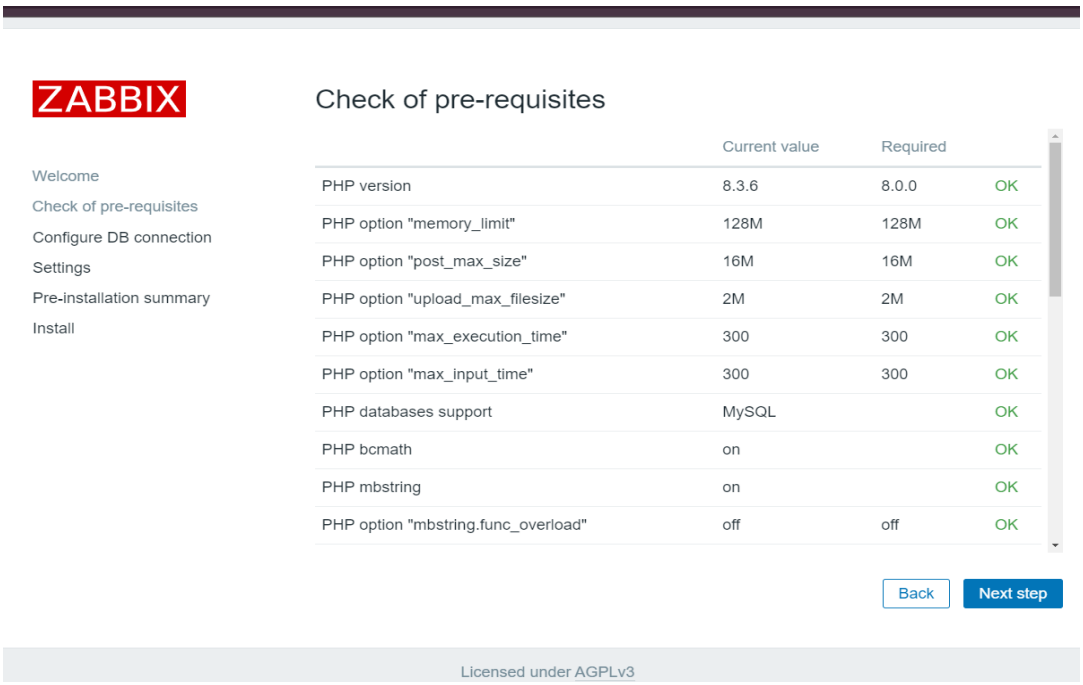


Figura 10: Prerrequisitos web.

2.1.4. Configuración de la conexión a la base de datos

Al avanzar en el asistente, es necesario conFigurar la conexión con la base de datos, tal como se muestra en la siguiente Figura. Para ello, se deben utilizar las Configuraciones establecidas previamente durante la instalación de la base de datos.

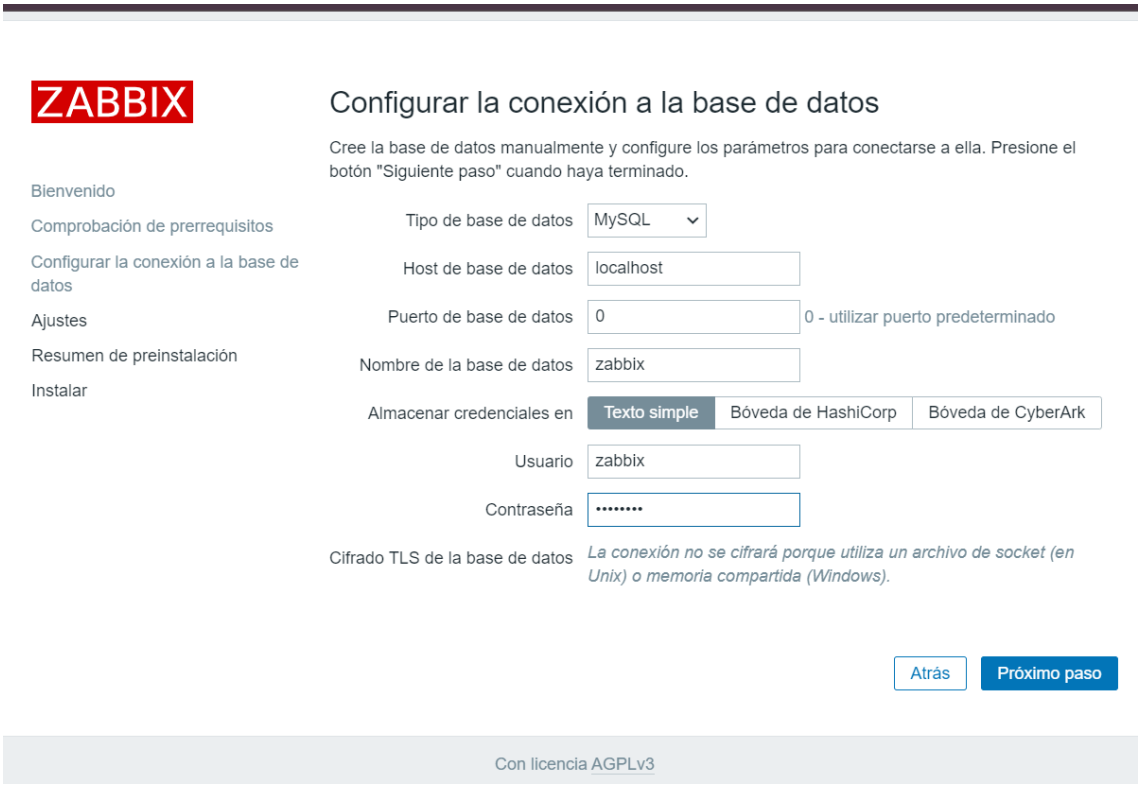


Figura 11: Configuración de la base de datos MySQL.

2.1.5. Ajustes adicionales.

Como parte de los ajustes adicionales, es necesario asignar un nombre al servidor o, en su defecto, mantener los valores predeterminados, tal como se muestra en la siguiente Figura. Esta Configuración permite diferenciar fácilmente entre varios servidores. En este caso, se utilizará el nombre "Padtec". Asimismo, se debe seleccionar la zona horaria y el tema de la interfaz gráfica.

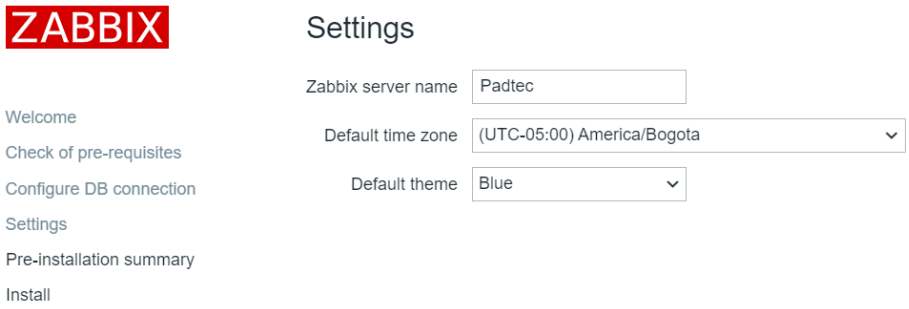


Figura 12: Configuraciones adicionales.

2.1.6. Resumen de preinstalación.

En esta sección se validan los parámetros configurados previamente, como el nombre de la base de datos, el usuario y la contraseña, antes de proceder con la instalación. Es importante tener presente que, en esta etapa, pueden surgir errores relacionados con el proceso de instalación que deben ser corregidos para continuar adecuadamente.[10]

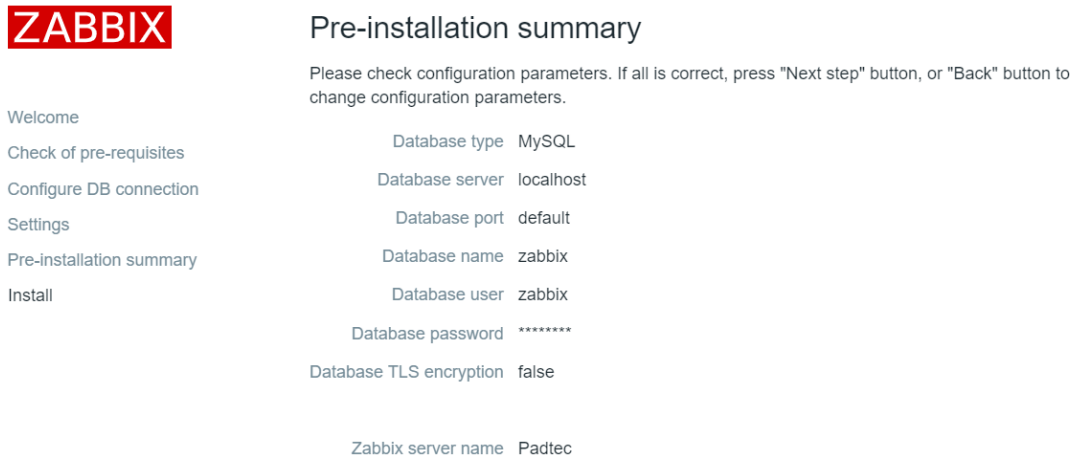


Figura 13: Resumen de instalación.

2.1.7. Instalación de Zabbix

Como paso final de la instalación, tras completar el asistente, se mostrará un mensaje indicando que el proceso ha sido exitoso En este punto, basta con hacer clic en “Finalizar” para concluir la instalación.

2.1.8. Inicio de sesión

Al concluir la instalación, la interfaz redirige automáticamente a la página de inicio de sesión. Para acceder al servidor, se debe ingresar con el usuario "Admin" y la contraseña predeterminada "zabbix", estos son las contraseñas por defecto.

2.1.9. Interfaz Zabbix

Al iniciar sesión, se mostrará la página principal de Zabbix. En esta vista se presentan diversos parámetros, como el estado del sistema, que confirma si el Zabbix Server está en funcionamiento (yes) junto con el puerto de conexión (10051). También se despliega información sobre los hosts activos, los problemas detectados y un panel de

control con los componentes necesarios para el monitoreo de la red (ver la siguiente Figura).[10]

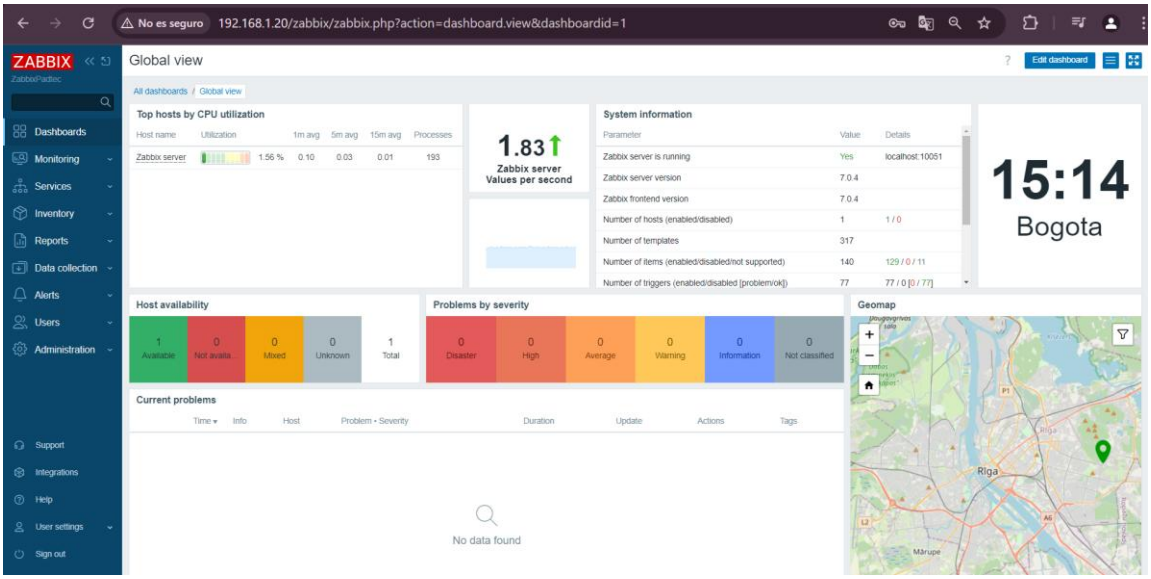


Figura 14: Panel de control.

2.1.10. Crecación de un host

La Configuración de grupos de Host permitirá la organización y el almacenamiento de múltiples host en Zabbix, sirviendo como un distintivo para todos los dispositivos que pertenezcan a este grupo. La creación de un host permitirá integrar un equipo en Zabbix para su posterior monitorización.

Para conFigurar un host en Zabbix, es necesario dirigirse nuevamente a la sección Recopilación de datos y seleccionar la opción Host. Allí se mostrará la lista de los hosts previamente creados. En la parte superior derecha de la pantalla, se debe hacer clic en Create host para añadir uno nuevo.

En la Configuración del nuevo host, se completan los parámetros solicitados de la siguiente manera (ver la siguiente Figura):

- Host name: Datacom1→ corresponde al nombre del primer router que será monitoreado.
- **Templates:** Network Generic Device by SNMP → se selecciona esta plantilla estándar para todos los routers.

- **Host groups:** Proyecto → grupo al cual pertenecerán los dispositivos de este proyecto.
- **Interfaces:** se debe ingresar la dirección IP con la que se configuro el protocolo snmp y que esta vinculada al equipo en general, sin importar el puerto físico.
    - Puerto predeterminado para SNMP: 161
    - Versión utilizada: SNMPv2

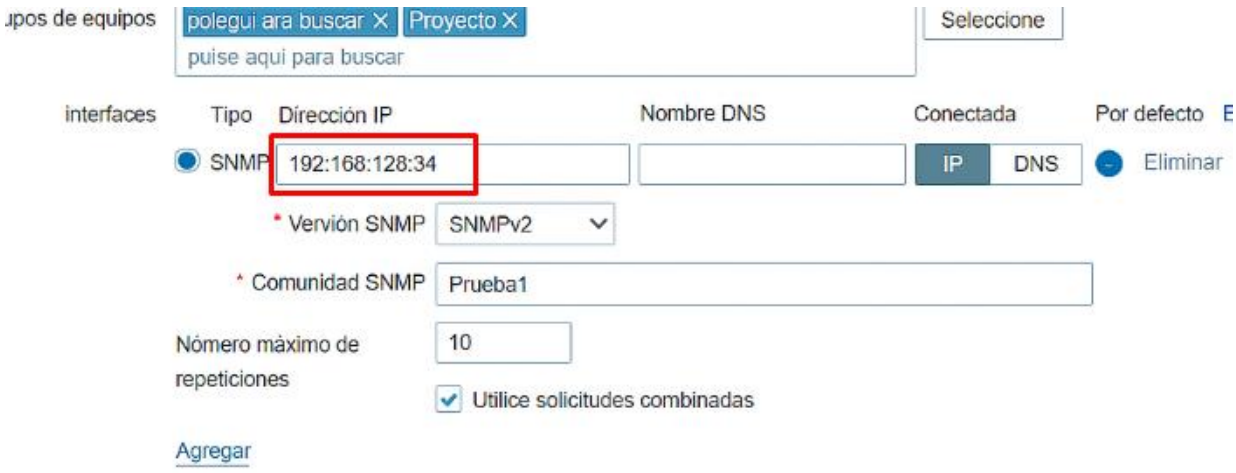


***Figura 15*:** Configuración de un host.

2.1.11. Parámetros que monitorear

Una vez configurados los hosts y comprobada la comunicación con el servidor de Zabbix a través de SNMP, el siguiente paso consiste en identificar las variables que se van a monitorear. Dichas variables pueden ser accedidas a través de los MIBS, los cuales son especificados gracias a la documentación del proveedor, DATACOM. [17]

En este caso, al no utilizar una plantilla específica, el cual es el caso de interes, se seleccionarán de manera manual los parámetros más relevantes, especialmente aquellos relacionados con el desempeño de las redes ópticas. Estos se presentan a continuación:

Tabla 2 :OID que identifica los parámetros.

Parametro	OID
Power Optical Receive / Potencia óptica recibida	**.1.3.6.1.4.1.3709.3.6.8.2.1.1.2.68190210.1**
Power Optical Transmit / Potencia óptica transmitida	**.1.3.6.1.4.1.3709.3.6.8.2.1.1.3. 68190210.1**
Optical Signal-to-Noise Ratio (OSNR)	**.1.3.6.1.4.1.3709.3.6.8.2.1.1.1. 68190210.1**
Forward Error Correction (FEC)	**.1.3.6.1.4.1.3709.3.6.8.2.1.1.1.68190210.1**
UP/DOWN	**.1.3.6.1.2.1.2.2.1.7.68190210**
Velocidad de la interfaz	**.1.3.6.1.2.1.2.2.1.5.68190210**
Uptime	**1.3.6.1.2.1.1.3.0**
Temperatura	**.1.3.6.1.4.1.3709.3.6.8.1.1.1.1.68190210**

2.1.12. Configuracion de monitores

Para crear un monitor en Zabbix, se debe ingresar nuevamente a la sección Recopilación de datos y seleccionar la opción Equipos. Allí se listan todos los equipos creados. A continuación, se selecciona el apartado Monitores del equipo al cual se le desea asociar el monitor y, en la parte superior derecha de la pantalla, se hace clic en *Crear monitor*. En la Configuración del nuevo monitor, los parámetros deben completarse de la siguiente manera (ver la siguiente Figura):

Nombre: corresponde a la variable que se va a monitorear.

Tipo: Tipo de protocolo utilizado por el dispositivo.

Monitor: net.if.pout

Tipo de información: Numérico (coma flotante) → define el tipo de valor a recopilar.

Interfaz del equipo: 192.168.128.35:161 → dirección IP y puerto asociados a la interfaz que se va a monitorear.

SNMP OID: .1.3.6.1.4.1.3709.3.6.8.1.1.1.1.68190210→ identificador que corresponde a la temperatura del módulo

Unidad: Grados → unidad en la que se expresará el valor.

Intervalo de actualización: 1m → frecuencia de actualización, donde "m" corresponde a minutos.

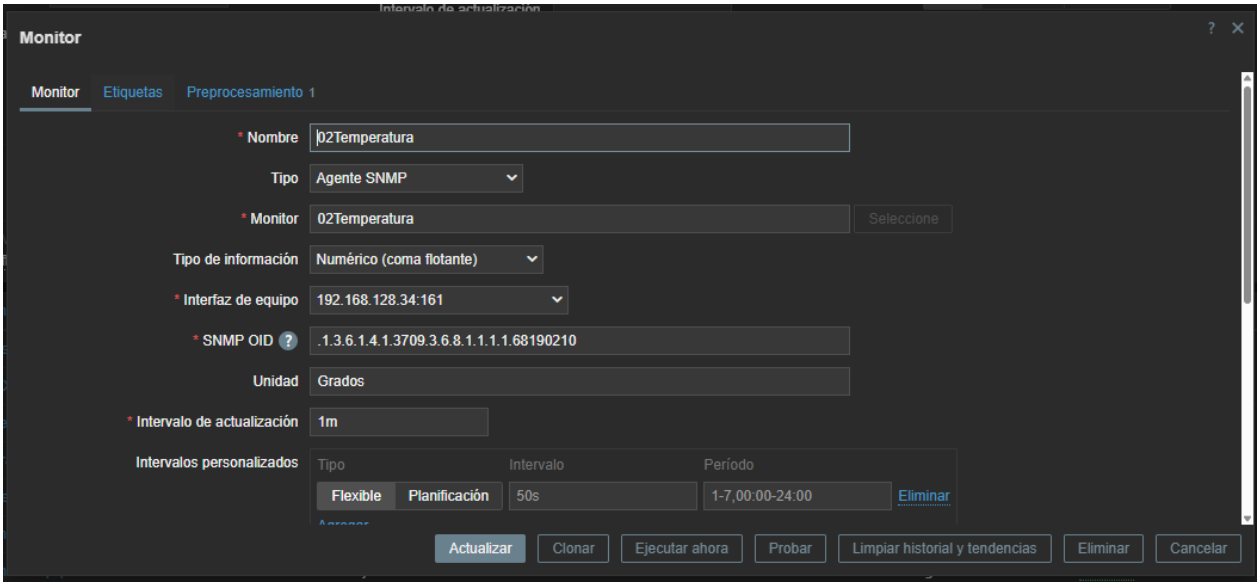


Figura 16: Configuración de un parámetro.

El proceso descrito se repite de manera continua para cada uno de los parámetros definidos previamente y que resultan de interés para el monitoreo.

1. ENTORNO PYTHON

Python desempeñará un papel fundamental en el desarrollo del proyecto, ya que a través de este lenguaje se realizarán tareas clave, tales como la conexión con el servidor de Zabbix para la importación de la información recolectada mediante los MIB, la ejecución de peticiones directas al equipo Datacom con el fin de obtener la Configuración de red, y, finalmente, la integración de los datos en un dashboard que permita presentar la información de manera clara y accesible al cliente.

1.1. Conexión entre el servidor zabbix y el enotrono Python

Con el objetivo de migrar la información recolectada por Zabbix hacia Python, se implementó un script que permite establecer una conexión entre ambos entornos utilizando la API de Zabbix.

El proceso se realiza de la siguiente manera:

1.1.1. Definición de parámetros de conexión

Se especifica la URL del servidor Zabbix, junto con las credenciales de acceso (usuario y contraseña).

```
# ZABBIX_URL = "http://192.168.128.35/zabbix"
# ZABBIX_USER = "Admin"
# ZABBIX_PASSWORD = "zabbix"
```

1.1.2. Conexión al servidor Zabbix

Se crea un objeto `ZabbixAPI` con la URL del servidor y se inicia sesión con las credenciales.

```
# zapi = ZabbixAPI(ZABBIX_URL)
# zapi.login(ZABBIX_USER, ZABBIX_PASSWORD)
```

1.1.3. **Verificación de usuario autenticado**

Se consulta la API para obtener información sobre el usuario que inició sesión, validando así que la conexión fue exitosa.

```
# user = zapi.user.get(output=["username", "name",
"surname"])[0]
# print(f"Conectado como {user['name']}
{user['surname']} ({user['username']})")
```

1.1.4. **Obtención de la lista de hosts monitoreados**

Se consulta a la API para obtener la lista de hosts registrados en Zabbix, mostrando su ID y nombre.

```
# hosts = zapi.host.get(output=["hostid", "name"])
# for host in hosts:
    print(f"Host ID: {host['hostid']} - Nombre:
{host['name']}")
```

Con lo anterior se confirma un buen funcionamiento en la conexión entre el servidor Zabbix y el entorno Python, validando que:

- El usuario Zabbix Administrator (Admin) logró autenticarse correctamente.
- Se obtuvo la lista de hosts registrados en Zabbix, como se puede observar en la siguiente Figura:

```
# Obtener lista de hosts
hosts = zapi.host.get(output=["hostid", "name"])
for host in hosts:
    print(f"Host ID: {host['hostid']} - Nombre: {host['name']}")
```

```
Conectado como Zabbix Administrator (Admin)
Host ID: 10084 - Nombre: Zabbix server
Host ID: 10671 - Nombre: Datacom
```

```
[14]: from pyzabbix import ZabbixAPI
      import datetime
```

Figura 17: Prueba de conexión.

Con la técnica aplicada anteriormente, se procede a la extracción de los parámetros definidos en la sección *Parámetros Elegidos*, garantizando así que la información recolectada corresponda con las variables críticas seleccionadas para el monitoreo.

1.2. Extracción de parámetros de red

Es fundamental extraer parámetros de la red, tales como los asociados a interfaces lógicas y físicas, VLANs configuradas, así como protocolos de enrutamiento como OSPF y MPLS, entre otros. Esto permite analizar el estado actual de la Configuración y, a partir de dicho análisis, proponer al usuario mejores prácticas para optimizar el desempeño y la gestión de su infraestructura de red.

- **Hostname (Nombre del dispositivo):**

  Representa el identificador único asignado a un equipo de red dentro de la infraestructura. Este nombre permite la fácil identificación del dispositivo en tareas de gestión, monitoreo, registro de eventos y resolución de incidencias. Un hostname correctamente configurado evita confusiones al administrar múltiples nodos o elementos de red.

  [RFC 1178 — Choosing a Name for Your Computer. Internet Engineering Task Force (IETF), 1990.]

Recomendación:

• Asignar nombres descriptivos y únicos por ubicación o función (ej. Core-Switch-Bogotá).

• Evitar nombres genéricos o duplicados.

• Mantener coherencia en la nomenclatura dentro de toda la red.

- **Interfaz de Gestión (Management Interface):**

  Es una interfaz dedicada al acceso administrativo y monitoreo del dispositivo fuera de la red de producción. Su propósito es permitir la configuración, diagnóstico y mantenimiento incluso si las interfaces operativas están inactivas.

  [ITU-T Recommendation M.3010 — Principles for a Telecommunications Management Network, ITU, 2015.]

  Recomendación:

  • Configurar una IP de gestión separada del tráfico de usuario.

  • Restringir el acceso a redes seguras o VLANs de administración.

  • Usar autenticación fuerte y cifrado (SSH, HTTPS, SNMPv3).

- **Interfaces Físicas (Physical Interfaces):**

  Corresponden a los puertos o enlaces físicos que conectan el dispositivo con otros equipos o medios de transmisión (fibra óptica, cobre, etc.). Su configuración incluye parámetros como velocidad, estado operativo, modo de puerto y negociación.

  [IEEE Std 802.3-2018 — Ethernet Standard, IEEE, 2018.]

  Recomendación:

  • Mantener coherencia de velocidad y dúplex entre extremos.

  • Supervisar el estado “shutdown” o errores físicos.

  • Documentar cada interfaz con su propósito y conexión.

- **VLANs (Virtual Local Area Networks):**

  Permiten segmentar una red física en dominios lógicos de broadcast independientes, mejorando la seguridad, escalabilidad y rendimiento. Cada VLAN agrupa dispositivos según criterios de función o departamento.

  [IEEE Std 802.1Q-2018 — Virtual Bridged Local Area Networks, IEEE, 2018.]

  Recomendación:

  • Asignar VLANs según políticas de tráfico y seguridad.

• Evitar VLAN 1 para administración o tráfico sensible.

• Usar nombres descriptivos y documentar las asignaciones.

- **OSPF (Open Shortest Path First):**

  Es un protocolo de enrutamiento interno (IGP) basado en el algoritmo de estado de enlace (Dijkstra). Calcula rutas óptimas dentro de un área o dominio de enrutamiento y soporta jerarquías mediante áreas para escalabilidad.

  [RFC 2328 — OSPF Version 2, IETF, 1998.]

  Recomendación:

  • Configurar correctamente el Router ID y las áreas.

  • Mantener un diseño jerárquico (backbone y áreas).

  • Ajustar los timers y autenticar vecinos OSPF.

- **MPLS (Multiprotocol Label Switching):**

  Tecnología que acelera el reenvío de paquetes mediante etiquetas (labels) en lugar de direcciones IP, permitiendo ingeniería de tráfico, VPNs y priorización de servicios.

  [RFC 3031 — Multiprotocol Label Switching Architecture, IETF, 2001.]

  Recomendación:

  • Habilitar la licencia MPLS solo cuando se requiera.

  • Configurar LSR_ID y vecinos LDP.

  • Aprovechar MPLS para VPNs, QoS y rutas resilientes.

- **SNMP (Simple Network Management Protocol):**

  Protocolo que permite la supervisión y control remoto de dispositivos de red mediante la consulta de objetos dentro de una base MIB (Management Information Base).

  [RFC 1157 — Simple Network Management Protocol (SNMP), IETF, 1990.]

  Recomendación:

  • Usar versiones seguras (SNMPv3).

  • Cambiar la comunidad por defecto (“public”).

  • Restringir el acceso SNMP solo a estaciones autorizadas.

1.2.1. Extracción de Configuraciones de red a través de SSH con Python.

Es importante resaltar que el equipo de red Datacom y el servidor de monitoreo Zabbix cuentan con una dirección IP propia, la cual permite realizar distintas peticiones de administración, ya sea mediante SNMP o SSH. De igual forma, el entorno de ejecución de Python se encuentra alojado en una máquina que también posee una dirección IP en la misma red o con conectividad hacia el equipo de interés.

A partir de esta máquina se inicia la petición SSH hacia el Datacom, tal como se muestra en el script: se establecen las credenciales de acceso, se ejecuta el comando remoto `show running-conFigura` y se obtiene la Configuración activa del dispositivo. Posteriormente, dicha Configuración puede visualizarse en pantalla o almacenarse en un archivo de texto para fines de respaldo o auditoría.

```
# host = "192.168.128.34"   # IP del equipo Datacom
# username = "admin"        # usuario SSH
# password = "admin"        # contraseña
```

Aquí se define la IP del equipo de red (Datacom, en este caso), así como el usuario y contraseña que usarás para conectarte vía SSH.

```
# ssh = paramiko.SSHClient()
# ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
# ssh.connect(host, username=username, password=password)
```

Se crea un cliente SSH con Paramiko, una Liberia que implementa los protocolos SSHv2 y SFTP, permitiendo así conexiones con dispositivos o servidores**.** Luego se conFigura la política para aceptar automáticamente claves de host desconocidas (`AutoAddPolicy`). Y finalmente, se establece la conexión al dispositivo de red usando la IP y credenciales.

```
# stdin, stdout, stderr = ssh.exec_command("show running-
conFigura")
```

Con el anterior commando se envia el comando `show running-conFigura` para finalmente capturar la salida a este comando con la siguiente línea de código:

```
# conFigura = stdout.read().decode()
```

La Configuración del equipo de red será almacenada en una variable denominada `running conFigura:`

1.2.2. Segmentación de parámetros relevantes en la Configuración de red con regex

Los equipos de red (routers, switches, etc.) guardan su Configuración como texto plano estructurado**.** Como se puede apreciar a continuación:

```
hostname Router1
!
interface TenGigabitEthernet 1/0/1
 ip address 192.168.1.1 255.255.255.0
 speed 10000
 duplex full
 no shutdown
!
router ospf 1
 router-id 1.1.1.1
 area 0
  interface TenGigabitEthernet 1/0/1
!
snmp community public
snmp agent version 2c
```

!

Para la identificación de los parámetros relevantes dentro de la Configuración del equipo de red se emplean expresiones regulares (regex). Este mecanismo permite reconocer patrones definidos a partir de palabras clave y estructuras específicas del archivo de Configuración. De esta manera, es posible automatizar la extracción de información crítica, como direcciones IP, interfaces, parámetros de enrutamiento o Configuraciones de protocolos, garantizando precisión y eficiencia en el análisis de la información.

Si bien se pueden extraer diferentes parámetros de la Configuración, la selección de estos debe responder a las necesidades específicas del cliente. A continuación, se presenta el proceso de extracción aplicado al caso de OSPF, resaltando aquellos parámetros que resultan indispensables para garantizar la adopción de buenas prácticas en enrutamiento.

4. RESULTADOS DE LA BUENAS PRACTICADAS DADO UN EQUIPO DE RED EN EL DASHBOARD

La capacidad de analizar los datos obtenidos a través de Python permite identificar áreas de mejora en la infraestructura de red, lo que contribuye a aumentar la calidad de transmisión en los dispositivos ofrecidos por la empresa. Para este propósito, se utilizaron librerías como pandas para la manipulación y limpieza de los datos, y ***plotly.graph_objects*** junto con ***plotly.express*** para la generación de gráficas dinámicas e interactivas que facilitaron el análisis comparativo de las métricas recolectadas, permitiendo obtener una visión clara y detallada del comportamiento de la red en diferentes escenarios.

4.1. Hostname.

En el primer dashboard se presenta la validación del parámetro **Hostname**, donde se evidencia que el dispositivo de red analizado cuenta con el identificador **AGG_A**. Esta Configuración se considera una buena práctica, ya que permite reconocer de manera clara el equipo dentro de la infraestructura, facilitando su administración, monitoreo y trazabilidad en las operaciones de red.

Hostname	Recommendation
AGG_A	Good practice: Hostname configured to identify the network device.

Figura 18: Hostname del equipo.

Hostname	Recomendación
DM4370	Recomendación: Asigne un nuevo nombre de host. Es una buena práctica para identificar el dispositivo de red de manera única y descriptiva.

Figura 19: Equipo sin Hostname y recomendación.

4.2. Interfaz de gestión

En este segundo dashboard se visualiza la Configuración de la interfaz de gestión del dispositivo de red. Se observa que el equipo dispone de una interfaz habilitada para administración (mgmt 1/1/1) con la dirección IP 192.168.0.25/24, lo cual confirma la presencia de un canal dedicado para la gestión remota y local del dispositivo. Esta práctica es considerada recomendable, ya que facilita la administración centralizada, mejora la seguridad al separar el tráfico de gestión del tráfico de producción y asegura un acceso confiable para las tareas de supervisión y mantenimiento.

Has_Management_Interface	Interface	IP_Address	Recomendación
true	mgmt 1/1/1	192.168.128.34/24	Buena práctica: Una interfaz de gestión es útil para la administración del dispositivo. Además, permite realizar tareas de monitoreo y configuración fuera de la red de producción, incrementando la seguridad y evitando interferir con el tráfico de usuario.

Figura 20: Interfaz para la gestión del equipo.

4.3. Interfaces físicas

En este dashboard se presenta un resumen del estado de las interfaces físicas del dispositivo de red. Se observa que el equipo cuenta con puertos de 10G (ten-gigabit-ethernet) y 100G (hundred-gigabit-ethernet), todos conFigurados en modo full-duplex, con un valor de MTU de 12262 y en estado operativo (No Shutdown). El hecho de que las interfaces no se encuentren apagadas refleja que están habilitadas y listas para su uso en la transmisión de datos. Asimismo, la disponibilidad de puertos de diferentes capacidades (10G y 100G) aporta flexibilidad para soportar tanto enlaces de agregación de alta capacidad como conexiones de menor escala, lo cual resulta esencial en entornos de telecomunicaciones que requieren escalabilidad y desempeño en la infraestructura de red.

Physical Interfaces

Interface	Speed	Duplex	MTU	Shutdown Status	Switchport Mode
ten-gigabit-ethernet 1/1/21	10G	full	12262	No Shutdown	N/A
ten-gigabit-ethernet 1/1/22	10G	full	12262	No Shutdown	N/A
ten-gigabit-ethernet 1/1/23	10G	full	12262	No Shutdown	N/A
ten-gigabit-ethernet 1/1/24	10G	full	12262	No Shutdown	N/A
hundred-gigabit-ethernet 1/1/1	100G	full	12262	No Shutdown	N/A
hundred-gigabit-ethernet 1/1/2	100G	full	12262	No Shutdown	N/A
hundred-gigabit-ethernet 1/1/3	100G	full	12262	No Shutdown	N/A

Figura 21: Estado de las interfaces.

4.4. VLANS

En este dashboard se muestran las VLANs configuradas en el dispositivo y las interfaces asociadas a cada una de ellas. Se observa la presencia de varias VLANs (30, 40, 90 y 100), distribuidas en diferentes puertos físicos como hundred-gigabit-ethernet 1/1/1, 1/1/2, 1/1/3 y ten-gigabit-ethernet 1/1/2. Esta Configuración evidencia la segmentación de la red en dominios de broadcast separados, lo que favorece la organización del tráfico, mejora la seguridad y permite optimizar el desempeño de la infraestructura. Además, la asignación de interfaces específicas a cada VLAN facilita la gestión y el control del tráfico, garantizando un mejor aprovechamiento de los recursos de red.

VLANs

VLAN	Interfaces
100	
30	
40	
90	
30	hundred-gigabit-ethernet-1/1/2
40	hundred-gigabit-ethernet-1/1/1
90	hundred-gigabit-ethernet-1/1/3
100	ten-gigabit-ethernet-1/1/2

Figura 22: VLANS creadas.

4.5. Configuración OSPF

En la tabla de OSPF Configuration and Recommendations se observa que la interfaz l3-VLAN100 participa en el protocolo OSPF dentro del área 0, que corresponde al área backbone del enrutamiento. El Router ID se encuentra asignado a la interfaz loopback-1, lo cual es una buena práctica para asegurar la estabilidad de la identificación del router en la red. Asimismo, se confirma que el área está correctamente configurada (Has_Area = true), y en la columna de Best Practices se valida que las áreas están definidas adecuadamente, lo que garantiza un diseño consistente y alineado con las recomendaciones de implementación de OSPF.

OSPF_Interface	Area	Router_ID	Recomendación
l3-VLAN100	0	loopback-1	Buena práctica: OSPF está correctamente configurado. Se han definido interfaces, áreas y un Router ID. Esto garantiza una operación estable del enrutamiento dinámico.

***Figura 23**:* Configuraciones para el enrutamiento OSPF.

OSPF_Interface	Area	Router_ID	Has_Area	Mejores Prácticas
null	null	null	false	Recomendación: Configure áreas OSPF para una mejor escalabilidad e ingeniería de tráfico.

Figura 24: Carencia de configuraciones OSPF.

4.6. Configuración MPLS

En la sección de MPLS Configuration se evidencia que el LSR_ID está asignado a la loopback-1, lo cual es recomendable ya que garantiza consistencia en la identificación del router dentro de la red MPLS. Aunque no se registran vecinos conFigurados (Neighbor: N/A), el estado de la licencia (License_Status: Enabled) confirma que la funcionalidad de MPLS se encuentra activa. La recomendación indica que la licencia de MPLS está correctamente habilitada, lo que permite que el dispositivo pueda participar en escenarios de conmutación de etiquetas y servicios avanzados de red una vez se establezcan vecinos y rutas MPLS.

Neighbor	LSR_ID	License_Status	Recomendación
null	loopback-1	Enabled	Recomendación: configurar vecinos LDP, verificar protocolo LDP activo.

Figura 25: Configuración MPLS.

Neighbor	LSR_ID	License_Status	Recomendación
null	null	Enabled	Recomendación: La licencia MPLS está habilitada, pero no se encontraron vecinos ni LSR_ID configurados. Aproveche la licencia MPLS configurando vecinos (LDP) y LSR_ID para habilitar funciones como ingeniería de tráfico, VPNs de capa 3 y priorización de tráfico (QoS).

Figura 26: Carencia de configuraciones MPLS.

4.7. Configuración SNMP

En la sección de SNMP Configuration se observa que la comunidad configurada es public, con soporte para las versiones v2c y v3. No se identifica explícitamente una dirección IP asociada al servicio (N/A), lo que indica que no está delimitado un host de gestión específico en la Configuración. Como recomendación, se sugiere cambiar la cadena de comunidad pública por motivos de seguridad, dado que el uso de public representa una vulnerabilidad al ser una cadena conocida y ampliamente explotada en accesos no autorizados.

Community	Versions	IP Address	Recommendation
public	v2c, v3	N/A (IP not explicitly found in config)	Recommendation: Change the public SNMP community string for security.

Figura 27: Configuración SNMP sin IP.

4.8. IP de las interfaces

En la sección de Interfaces con direcciones IP se detalla la asignación de direcciones a las distintas interfaces del dispositivo. La interfaz l3-VLAN30 cuenta con la dirección 10.100.100.1/24, mientras que las interfaces de capa 3 poseen Configuraciones punto a punto: 30.30.30.2/30, 40.40.40.1/30 y 90.90.90.1/30. Adicionalmente, la interfaz de gestión (mgmt) se encuentra en la red 192.168.0.25/24, separada de las redes de producción, lo que facilita la administración remota. Finalmente, la interfaz loopback está configurada con la dirección **3.3.3.3/32**, la cual generalmente se utiliza como identificador único del router y es clave para protocolos de enrutamiento y servicios como OSPF o MPLS.

Interface	IP Address
l3-VLAN30	10.100.100.1/24
l3	30.30.30.2/30
l3	40.40.40.1/30
l3	90.90.90.1/30
mgmt	192.168.0.25/24
loopback	3.3.3.3/32

Figura 28: Interfaces configuradas.

4.10. Recomendaciones para los parámetros traídos desde Zabbix

El valor FEC = 1 indica que la función de corrección de errores está habilitada, pero en este caso no aplica, porque el enlace no está trabajando en la longitud de onda de 1550 nm, donde normalmente se utiliza FEC para enlaces de larga distancia. El sistema opera en 1310 nm o 1490 nm, longitudes de onda típicas de enlaces GPON o EPON de corta o media distancia, en los que la corrección FEC no es necesaria.

Nombre	Key	Valor	Recomendación
02FEC02	02FEC02	1	• No aplica: el enlace trabaja en 1310 nm o 1490 nm, no en 1550 nm.

Figura 29: FEC.

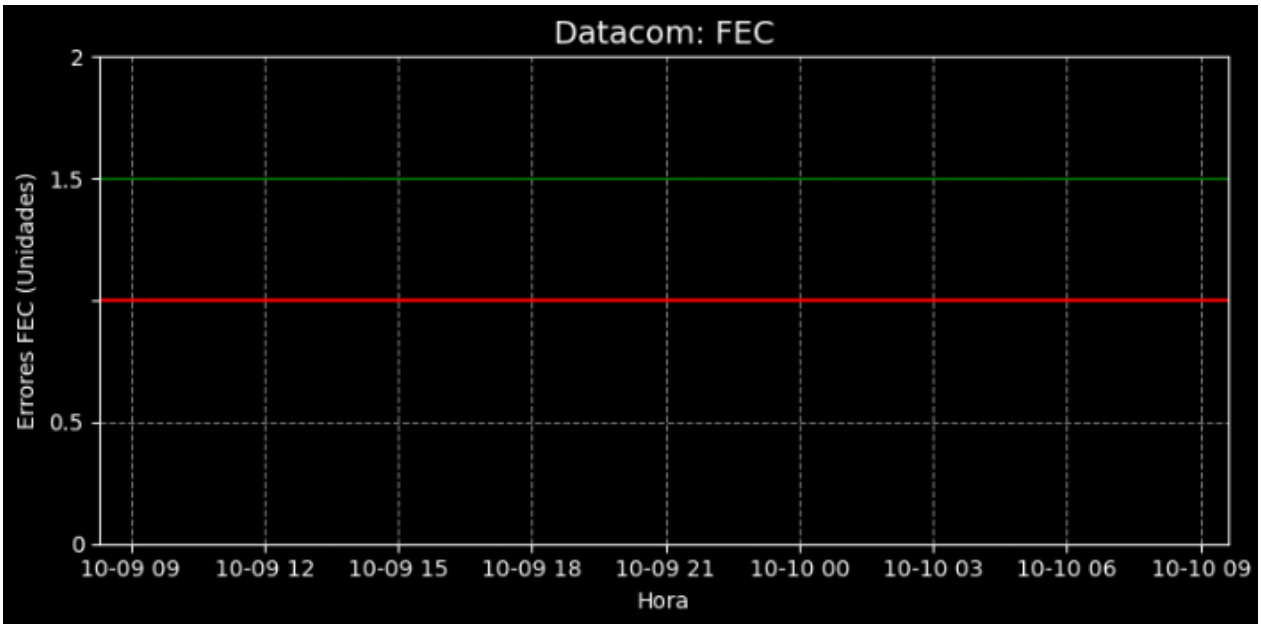


Figura 30: FEC (Gráfica).

El estatus del puerto indica el estado actual de funcionamiento de una interfaz de red. Este parámetro permite saber si el puerto se encuentra activo (UP) y transmitiendo datos correctamente, o inactivo (DOWN) debido a fallas o desconexiones. En este caso, el puerto 2 opera a 10 Gbps, lo que significa que pertenece a una interfaz de alta velocidad usada comúnmente para enlaces troncales o interconexiones entre equipos de red de gran capacidad.

Nombre	Key	Valor	Recomendación
02UP/DONW	02IfAdminStatus02	INTERFAZ OPERATIVA	El puerto se encuentra activo y en funcionamiento.

Figura 29: Estatus del puerto 2 10Gbps.

El OSNR es un parámetro que indica la relación entre la potencia de la señal óptica útil y el nivel de ruido presente en el canal. Este valor es fundamental para evaluar la calidad de transmisión en enlaces ópticos, especialmente en sistemas DWDM o de larga distancia.

En este caso, la tabla muestra que el valor medido es "1", pero la recomendación aclara que no aplica, ya que el enlace trabaja en longitudes de onda de 1310 nm o 1490 nm, y el OSNR se utiliza principalmente para enlaces que operan en 1550 nm, donde se emplean amplificadores ópticos.

Nombre	Key	Valor	Recomendación
02OSNR	02OSNR02	1	• No aplica: el enlace trabaja en 1310 nm o 1490 nm, no en 1550 nm.

Figura 30: OSNR del puerto 2 10Gbps.

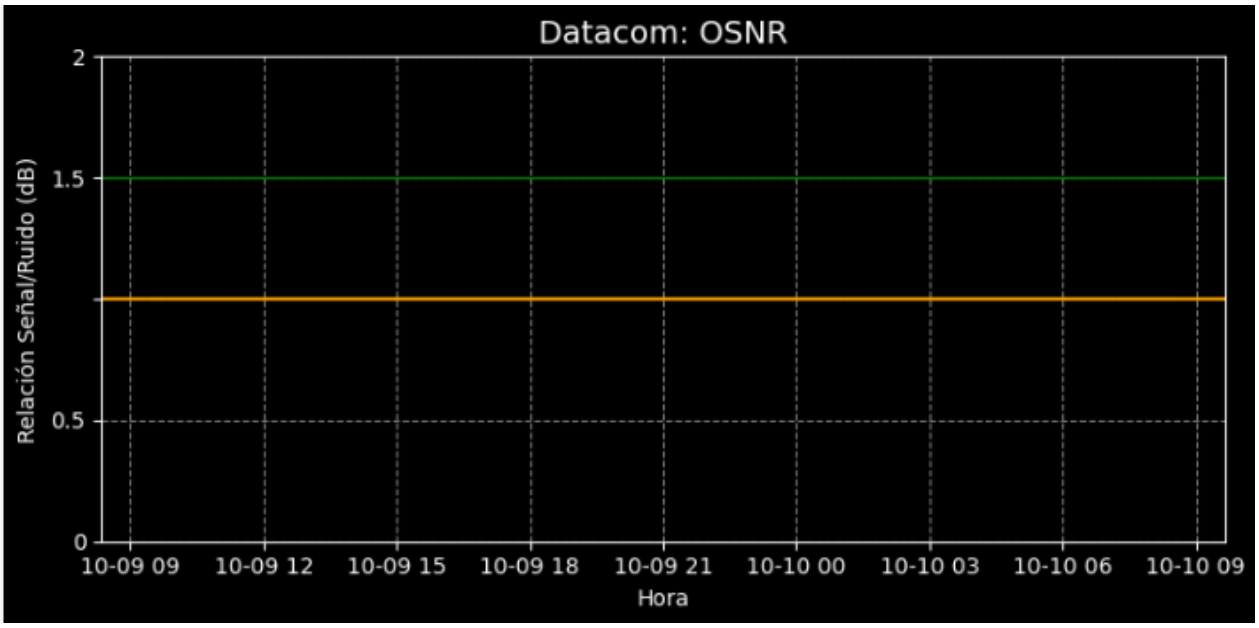


Figura 30: OSNR del puerto 2 10Gbps (Gráfica).

El valor mostrado, –12.76 dBm, representa el nivel de potencia que llega al receptor óptico del transceptor. Este parámetro es crucial para determinar si la señal óptica llega con suficiente intensidad para garantizar una recepción confiable sin errores.

De acuerdo con los rangos típicos mencionados (entre –28 dBm y –8 dBm para módulos SFP/GPON), el valor medido se encuentra dentro del rango aceptable, lo que indica que la potencia recibida es adecuada y el enlace está funcionando correctamente.

Nombre	Key	Valor	Recomendación
02RX02	02RX	-12.76 dB	• Valores típicos: entre –28 dBm y –8 dBm para SFP/GPON; en DWDM puede variar según el amplificador o la modulación.

Figura 31: RX puerto 2 10Gbps.

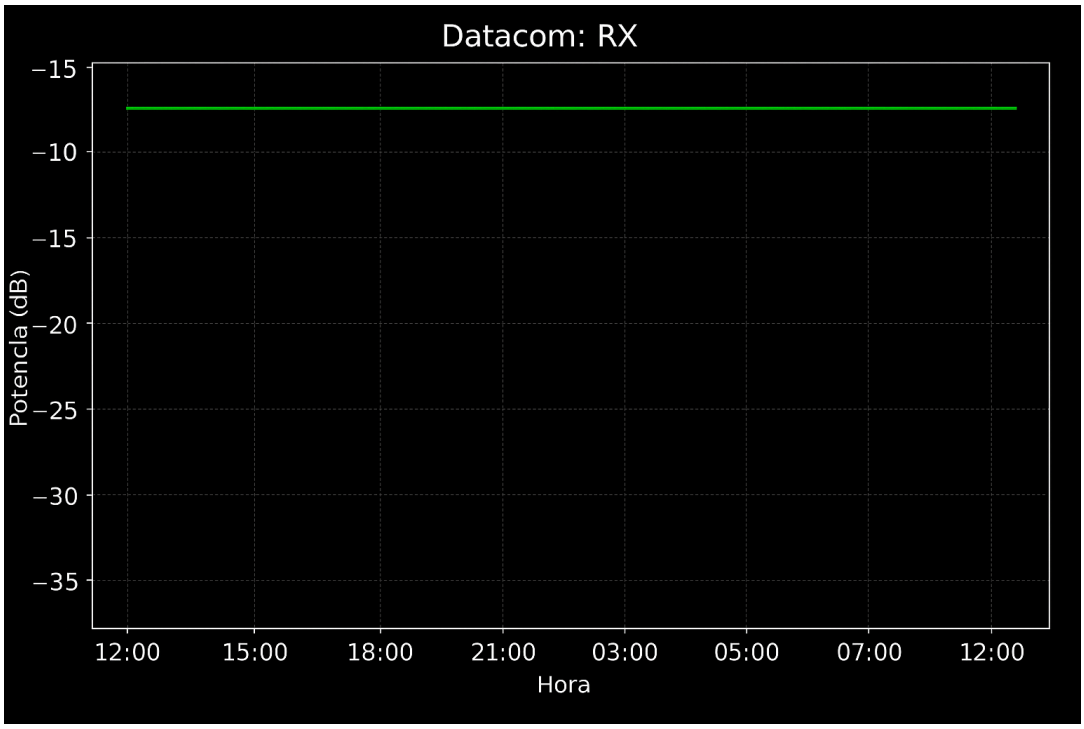


Figura 32: RX puerto 2 10Gbps (Gráfica).

Este valor indica la intensidad con la que el transmisor óptico está emitiendo la señal hacia la fibra. De acuerdo con los rangos de referencia proporcionados —entre 0 dBm y +5 dBm para enlaces de larga distancia (DWDM), o entre –3 dBm y +2 dBm para sistemas GPON—, la potencia medida se encuentra dentro del rango operativo recomendado.

Por tanto, el transmisor se encuentra funcionando correctamente y entregando una señal con potencia adecuada para garantizar una transmisión estable y sin degradación significativa a lo largo del enlace óptico.

Nombre	Key	Valor	Recomendación
02TX02	02TX	-2.34 dB	• Debe estar dentro del rango nominal especificado por el fabricante del transceptor. • Valores típicos: entre 0 dBm y +5 dBm para enlaces largos (DWDM), o −3 dBm a +2 dBm para GPON.

Figura 32: TX del puerto 2 10Gbps.

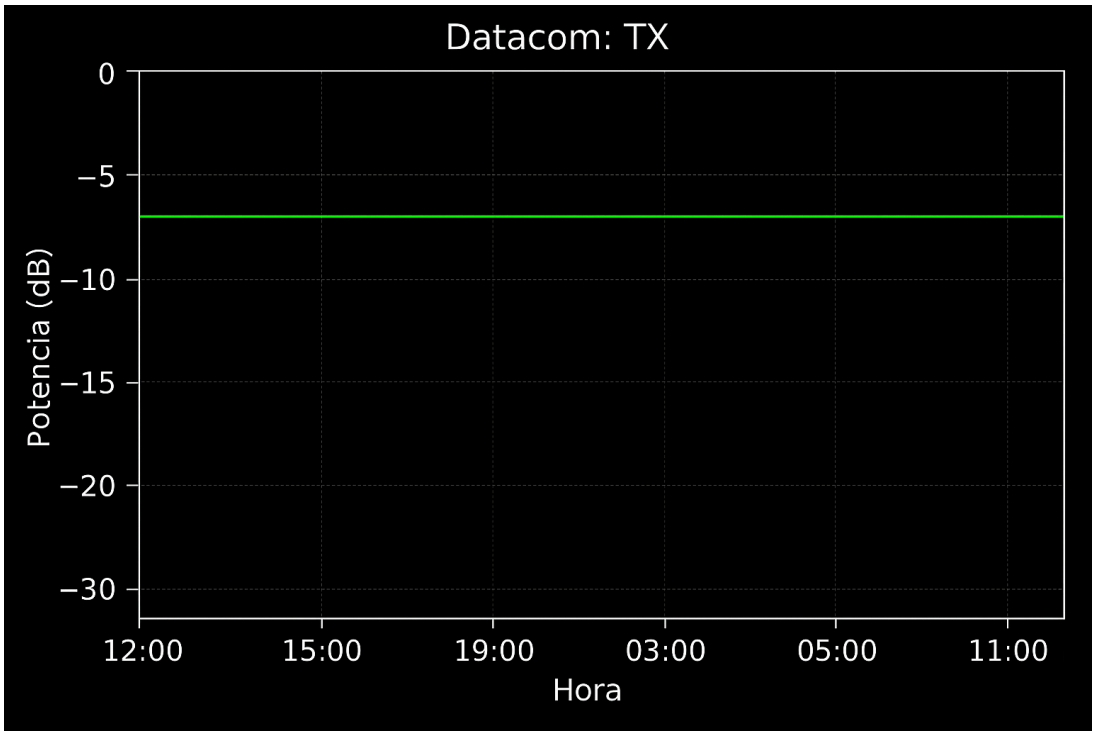


Figura 33: TX del puerto 2 10Gbps (Gráfica).

Este resultado indica que el módulo óptico opera dentro del rango térmico seguro establecido por la mayoría de los fabricantes, que suele estar entre 0 °C y 70 °C. Mantener la temperatura dentro de este margen es fundamental para evitar fallos en la transmisión y preservar la estabilidad del enlace.

Por lo tanto, se puede concluir que el transceptor presenta un funcionamiento normal, sin riesgo de sobrecalentamiento ni degradación del rendimiento óptico.

Nombre	Key	Valor	Recomendación
02Temperatura	02Temperatura	34.35	• Temperatura 34.35°C dentro del rango seguro (0°C a 70°C).

Figura 33: Temperatura puerto 2 10Gbps (Gráfica).

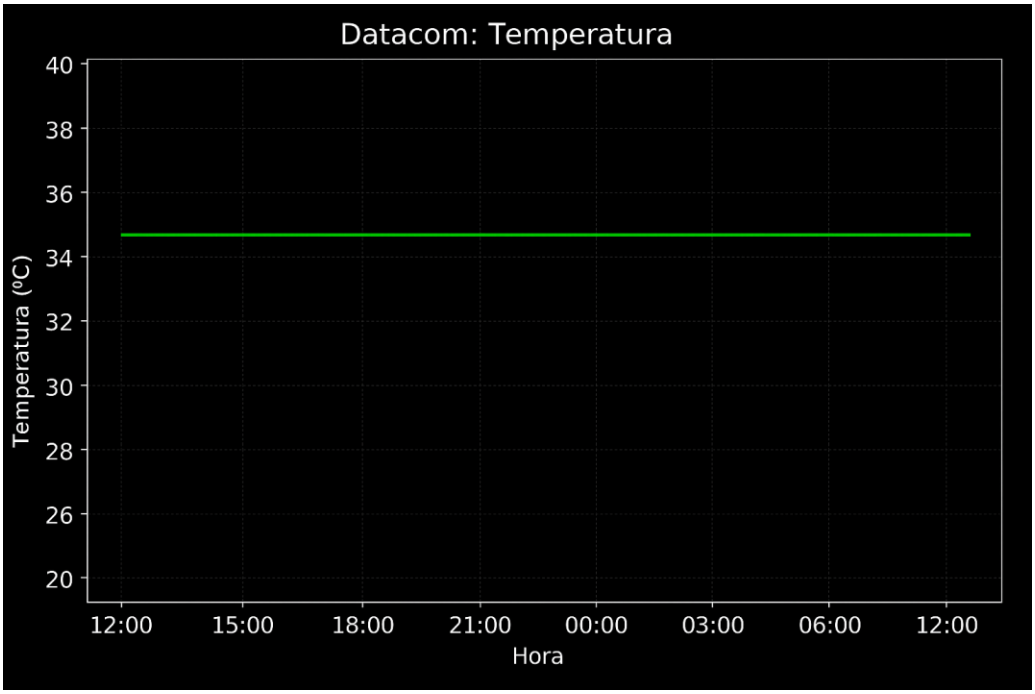


Figura 34: Temperatura puerto 2 10Gbps (Gráfica).

El parámetro de velocidad (02Velocidad) muestra un valor de 4294967295, el cual corresponde a una velocidad en bps.

Por otro lado, el uptime (472111) indica el tiempo transcurrido desde el último reinicio del equipo, expresado en segundos.

En ambos casos, no se dispone de una recomendación específica, ya que estos valores son informativos.

Nombre	Key	Valor	Recomendación
			del rango seguro (0°C a 70°C).
02Velocidad	02ifSpeed02	4294967295	• No se pudo determinar una recomendación para este parámetro.
Uptime	sysUpTime	472111	• No se pudo determinar una recomendación para este parámetro.

Figura 34: Información adicional.

Aunque no se cuenta con una recomendación respaldada por un estándar o buena práctica específica, se incluyen gráficas que ofrecen una perspectiva más clara sobre el desempeño y la condición real del equipo, como se podrá apreciar en la ***Figura 35.***

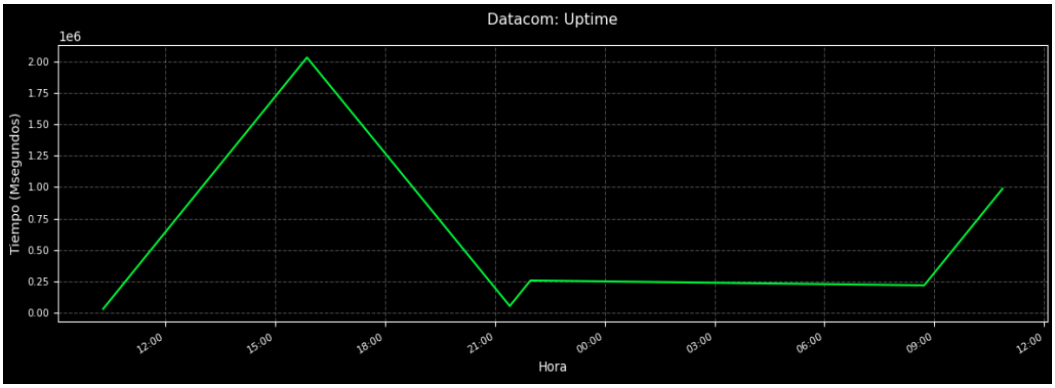


Figura 35: Uptime del dispositivo.

También se realiza el mismo análisis con la variable correspondiente a la velocidad de la interfaz, con el fin de observar su comportamiento a lo largo del tiempo y evaluar posibles variaciones en el desempeño del enlace.

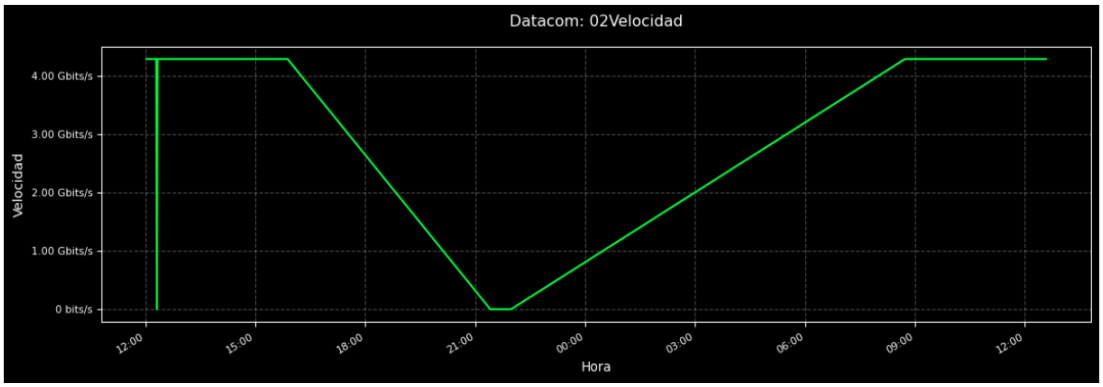


Figura 36: Velocidad de la interfaz.

CONCLUSIONES

- El identificar las variables más relevantes a nivel de la capa 1 y, en especial, de la capa 3 resulta determinante en el desempeño de la red, ya que estas capas concentran tanto la calidad física de la transmisión como la eficiencia en el encaminamiento de los paquetes. La correcta priorización de estas variables garantiza que el monitoreo no solo detecte anomalías relacionadas con degradaciones en la señal óptica, pérdidas o ruido, sino también con aspectos asociados al tráfico, la congestión y el uso de recursos en la capa de red. De esta manera, se asegura una captura de datos con la frecuencia suficiente para anticipar patrones de desempeño, lo cual es clave para la prevención de fallas y la optimización continua de la infraestructura.

- Mediante la Configuración de Zabbix se consiguió obtener un set de datos confiable relacionado con dichas variables, aprovechando los OID presentes en equipos Datacom y otros dispositivos de red soportados por la empresa, lo que aseguró una supervisión completa de la infraestructura IP y óptica.

- Python, en conjunto con protocolos como SSH y SNMP, es una herramienta clave en el monitoreo y análisis del comportamiento de la red, ya que permite procesar datos relevantes y compararlos con buenas prácticas y estándares internacionales, fortaleciendo la gestión y optimización de la infraestructura.

- Python y sus herramientas para la creación de dashboards interactivos, se logra resumir de manera clara el funcionamiento de la red, facilitando la visualización de los parámetros monitoreados y su comparación con valores de referencia. Esta solución no solo simplificó la detección de desviaciones en el desempeño, sino que también permitió anticiparse a posibles fallas en cuanto a la gestión, seguridad y funcionamiento de la red, contribuyendo a una mayor estabilidad y calidad del servicio.

11. REFERENCIAS

[1] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). *A Brief History of the Internet*. Internet Society (ISOC). Recuperado de https://www.internetsociety.org/internet/history/

[2] ITU-T Recommendation G.694.1. (2020). *Spectral grids for WDM applications: DWDM frequency grid*. International Telecommunication Union.

[3] Ramaswami, R., Sivarajan, K. N., & Sasaki, G. H. (2010). *Optical Networks: A Practical Perspective* (3rd ed.). Morgan Kaufmann.

[4] Agrawal, G. P. (2012). *Fiber-Optic Communication Systems* (4th ed.). Wiley-Interscience.

[5] IEEE Standards Association, *IEEE Standard 610.7-1995 – Terms Pertaining to Data Communications and Networking*, IEEE, 1995.

[6] J. Moy, *OSPF Version 2*, IETF RFC 2328, 1998.

[7] J. Case, R. Mundy, D. Partain, and B. Stewart, *Introduction to Version 3 of the Internet-Standard Network Management Framework*, IETF RFC 3410, Dec. 2002.

[8] Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer Networks* (5th ed.). Pearson.

[9] Zabbix SIA. *Zabbix Documentation 7.0 – The Enterprise-Class Monitoring Platform*. Disponible en: https://www.zabbix.com/documentation/current.

[10] M. Muñoz Arroyave, "Implementación de plataforma de monitoreo de variables de desempeño ópticas de interfaces OpenZR+ sobre plataformas desagregadas por medio de Zabbix y Grafana para aplicaciones IPoDWDM", Semestre de Industria, Ingeniería de Telecomunicaciones, Universidad de Antioquia, Medellín, 2024.

[11] S. Bird, E. Klein y E. Loper, *Natural Language Processing with Python*, O'Reilly Media, 2009.

[12] Cisco Systems, *Understanding Optical Power Budget and Loss in Fiber Networks*, Cisco Optical Networking Documentation, 2023. [En línea]. Disponible en: https://www.cisco.com/.

[13] ITU-T Recommendation G.697, *Optical monitoring for DWDM systems*, International Telecommunication Union, 2021.

[14] ITU-T Recommendation G.975.1, *Forward Error Correction for High Bit-Rate DWDM Submarine Systems*, International Telecommunication Union, 2019.

[15] ITU-T Recommendation G.984.3, *Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification*, International Telecommunication Union, 2020.

[16] Cisco Systems. (2023). *Monitoring system uptime and availability in optical networks*. Cisco Optical Networking Documentation.}

[17] DATACOM, "Support Center," Accessed: 10 07, 2025. [Online]. Available:

https://supportcenter.datacom.com.br/.

12. ANEXOS

ANEXO A: *Características Switche Datacom*

Velocidad de cable con reenvío, filtrado y calidad de servicio (QoS) L2, L3 y MPLS basados en hardware, VLAN IEEE802.1Q con capacidades Q-in-Q y VLAN Translate, Agregación de enlaces y LACP, Soporte para aplicaciones Ring a través de protocolos EAPS o ERPS, STP/RSTP para protección de bucle, Túnel de protocolo lento L2 (L2CP), Hasta 8 colas de QoS por puerto, Enrutamiento estático y enrutamiento dinámico mediante protocolos OSPF y BGP, Redundancia de IP virtual a través del protocolo VRRP, Funcionamiento como enrutador de borde de etiqueta o enrutador de conmutación de etiqueta mediante encapsulación MPLS, LDP para distribución de etiquetas en infraestructura de red MPLS, Límite de velocidad de entrada y salida, Programación de paquetes mediante los modos SP y WFQ, Coincidencias de ACL por puerto, dirección MAC, IP, DSCP, TCP/UDP, Interfaz de administración CLI con Telnet/SSH Soporte TACACS y RADIUS para administración de políticas de acceso y gestión.

ANEXO B: *Características Servidor PowerEdge.*

El Dell PowerEdge R660xs es un servidor en rack 1U diseñado para alto rendimiento en entornos de telecomunicaciones y centros de datos. Incorpora procesadores Intel® Xeon® Scalable de 4.ª generación de hasta 32 núcleos, soporta hasta 2 TB de memoria DDR5 con ECC y ofrece capacidad para 8 unidades SAS/SATA/NVMe de 2,5” con opciones RAID. Dispone de interfaces de red de alta velocidad (1/10/25/40/100 GbE) mediante tarjetas de expansión, junto con gestión remota a través de iDRAC9. Su arquitectura optimizada garantiza eficiencia energética, refrigeración con ventiladores redundantes hot-swap y alta confiabilidad. Presenta un formato compacto de rack 1U con dimensiones de 42,8 mm x 482 mm x 744 mm y un peso aproximado de 17,6 kg, lo que lo convierte en una opción robusta para la implementación de plataformas de

monitoreo como Zabbix, permitiendo un manejo eficiente de grandes volúmenes de datos y el análisis en tiempo real de múltiples variables de desempeño.


Departamento de Ingeniería Electrónica y de Telecomunicaciones

UNIVERSIDAD DE ANTIOQUIA
1803
Facultad de Ingeniería

Buenas Prácticas en la Supervisión de Infraestructura de Red mediante Zabbix y Python.

PRACTICANTE: Carlos Andrés Mesa Roldán
ASESORES: Ana María Cárdenas Soto – Hernán Darío Yepes

PROGRAMA: Ingeniería de Telecomunicaciones
Semestre de la práctica: 2025-2

Introducción

El proyecto, titulado "Buenas Prácticas en la Supervisión de Infraestructura de Red mediante Zabbix y Python", combina las capacidades de Zabbix como plataforma de monitoreo con Python como herramienta para automatizar tareas y analizar datos recolectados por los OID de Zabbix. Esta integración posibilita un análisis más profundo del comportamiento de la red, identificando patrones de desempeño y alertas proactivas.Asimismo, se plantea una comparación con estándares y buenas prácticas internacionales (TM Forum, ITU-T, ISO/IEC, entre otros) para detectar brechas y proponer mejoras. Finalmente, el trabajo sienta las bases para incorporar modelos de aprendizaje automático que aprovechen los datos históricos para fortalecer la capacidad predictiva y la gestión inteligente de las redes.

Objetivos

- Identificar las variables más relevantes que impactan el desempeño de las redes de transporte ópticas.
- Utilizar los OIDs con el fin de obtener un conjunto de datos sobre las variables más relevantes que permitan analizar el desempeño de la red.
- Crear un algoritmo en Python, para el análisis de los datos recolectados .
- Desarrollar un dashboard que permita la visualización amigable de los datos.

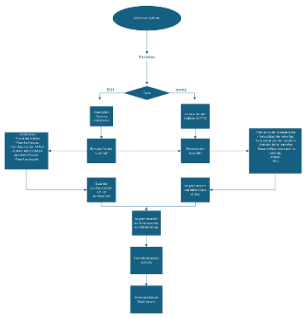
Metodología

- Identificar las variables más relevantes que impactan el desempeño de las red.
- Obtener un set de datos relacionados con las variables identificadas.

Parámetro	OID
Power Optical Receive / Potencia Óptica recibida	.1.3.6.1.4.1.3709.3.6.2.1.1.3.16.1001.0.1
Power Optical Transmit / Potencia Óptica transmitida	.1.3.6.1.4.1.3709.3.6.2.1.1.3.15.1001.0.1
Optical Signal-to-Noise Ratio (OSNR)	.1.3.6.1.4.1.3709.3.6.2.1.1.11.1001.0.1
Forward Error Correction (FEC)	.1.3.6.1.4.1.3709.3.6.2.1.1.11.1001.0.1
ER/EVMPN	.1.3.6.1.2.1.2.2.1.7.1001
Velocidad de la interfaz	.1.3.6.1.2.1.31.1.1.1.15.1001
Duplex	.1.3.6.1.2.1.10.163
Temperatura	.1.3.6.1.4.1.42551.6.8.1.1.1.1.1001

- Identificar qué mejoras se pueden realizar para aumentar la capacidad total permitida.

  (Ver sección de resultados)
- Crear un algoritmo en Python, para el análisis de los datos recolectados por el servidor a través del protocolo SNMP y SSH.



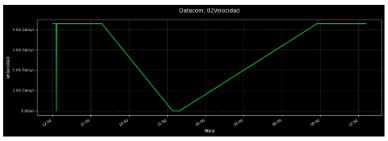
- Desarrollar un dashboard que permita la visualización amigable de los datos.

  (Ver sección de resultados)

Resultados

Los resultados obtenidos presentan una serie de recomendaciones orientadas a mejorar el desempeño de la red, proporcionando además una visión general sobre su estado actual. Dichas recomendaciones permiten identificar oportunidades de mejora ,preveer posibles fallos en la infraestructura y establecer acciones que contribuyan a un funcionamiento más eficiente y estable de la red.

OSPF_Interface	Area	Router_ID	Recomendación
13-VLAN100	0	loopback 1	Buena práctica: OSPF está correctamente configurado. Se han definido interfaces, áreas y un Router ID. Esto garantiza una operación estable del enrutamiento dinámico.



Conclusiones

- Identificar las variables más relevantes en las capas 1 y 3 es fundamental para el desempeño de la red, ya que estas determinan tanto la calidad física de la transmisión como la eficiencia del encaminamiento.
- A través de la configuración de Zabbix se logró obtener un conjunto de datos confiable sobre las variables identificadas, utilizando los OID de los equipos Datacom y otros dispositivos soportados por la empresa, garantizando así una supervisión integral de la infraestructura IP y óptica.
- Python, en conjunto con protocolos como SSH y SNMP, es una herramienta clave en el monitoreo y análisis del comportamiento de la red
- Python y sus herramientas para la creación de dashboards interactivos logra resumir de manera clara el funcionamiento de la red.

DATOS DE CONTACTO DEL AUTOR:

+57 3128370475 carlos.mesar@udea.edu.co https://www.linkedin.com/in/carlos-mesa-228b4622b/