Sistema de monitoreo de redes para Gigaredes Comunicaciones utilizando PRTG

Yivier Libardo Duran Alvear

Asesor

Ingeniero: Pedro Torres Silva

Programa académico

Ingeniería en Telecomunicaciones

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Ingenieria en Telecomunicaciones

2025

Resumen

El proyecto titulado “Sistema de Monitoreo de Redes para Gigaredes Comunicaciones utilizando PRTG” tiene como finalidad diseñar una solución técnica que permita la supervisión estructurada de la infraestructura de red híbrida, compuesta por tecnologías GPON y WiMAX, en la empresa Gigaredes Comunicaciones SAS. La propuesta surge ante la necesidad de detectar oportunamente fallas, especialmente aquellas relacionadas con la energía en nodos ubicados en zonas de difícil acceso, lo cual ha generado interrupciones frecuentes y aumento en el tiempo de respuesta. La metodología empleada se basa en el ciclo de vida del desarrollo de sistemas (SDLC), adaptado a una perspectiva exclusivamente de diseño, e incluye tres fases: diagnóstico de la infraestructura actual, diseño de la arquitectura lógica del sistema de monitoreo basado en PRTG, y elaboración de lineamientos técnicos para la supervisión remota de eventos críticos. Como producto final se entregará un diseño técnico documentado, que incluirá diagramas, propuesta de sensores, mapas jerárquicos, estrategias de visualización y pautas para una futura implementación. Este diseño busca servir como insumo para fortalecer la capacidad de monitoreo de la empresa, optimizar la planificación operativa y contribuir al desarrollo del sector de telecomunicaciones en entornos rurales y de difícil acceso.

Palabras clave: monitoreo de redes, GPON, WiMAX, PRTG, telecomunicaciones.

Contenido

Lista de Tablas

Lista de Figuras

Introducción

En el entorno actual de las telecomunicaciones, la supervisión eficiente de las redes constituye un factor estratégico para garantizar la continuidad del servicio, la estabilidad operativa y la satisfacción del cliente. Gigaredes Comunicaciones SAS, proveedor regional de servicios de conectividad, enfrenta dificultades crecientes en la gestión de su infraestructura híbrida basada en tecnologías GPON y WiMAX, especialmente en zonas rurales de difícil acceso. Las condiciones climáticas adversas, sumadas a la limitada capacidad de monitoreo en tiempo real, han incrementado la frecuencia de interrupciones no planificadas y los tiempos de respuesta ante fallas, afectando negativamente la calidad del servicio y la percepción del usuario final.

Frente a este panorama, el presente proyecto de grado propone el diseño técnico de un sistema de monitoreo de redes basado en la herramienta PRTG Network Monitor, ajustado a las particularidades topológicas y operativas de la red de Gigaredes. Aunque el proyecto no contempla la implementación práctica del sistema, busca generar un diseño robusto, replicable y fundamentado que pueda servir como insumo para su futura puesta en marcha por parte del equipo técnico de la empresa.

Para ello, se adopta un enfoque metodológico sustentado en una versión adaptada del Ciclo de Vida de Desarrollo de Sistemas (SDLC), que abarca únicamente las fases de análisis de requerimientos, diseño del sistema, validación documental y formulación de lineamientos técnicos. A lo largo del documento se abordará el planteamiento del problema, la justificación del proyecto desde una perspectiva académica, social y técnica, el marco conceptual que lo sustenta, y la propuesta detallada de la arquitectura lógica del sistema, incluyendo sensores sugeridos, alertas, tableros conceptuales y protocolos de supervisión remota.

Con este trabajo se pretende aportar una solución técnica estructurada a los retos de monitoreo que enfrentan las redes híbridas en contextos rurales, al tiempo que se fortalece el desarrollo profesional y académico del estudiante, mediante la aplicación de conocimientos teóricos a un caso real del sector de las telecomunicaciones.

Planteamiento del Problema

La empresa Gigaredes Comunicaciones SAS, dedicada a la provisión de servicios de Internet en zonas urbanas y rurales del Huila, opera con una infraestructura de red híbrida conformada por tecnologías GPON y WiMAX. A pesar de su cobertura regional y de contar con equipos de conectividad modernos, enfrenta importantes dificultades en la detección oportuna de fallas dentro de su red, particularmente en nodos ubicados en cerros o zonas de difícil acceso. Estas áreas presentan condiciones climáticas adversas —como vientos fuertes y lluvias intensas— que provocan cortes recurrentes en el suministro eléctrico, lo que a su vez genera interrupciones del servicio y períodos prolongados de inactividad.

La empresa no dispone actualmente de un sistema de monitoreo integral que le permita vigilar en tiempo real el estado operativo de sus dispositivos GPON y WiMAX. Esta carencia limita su capacidad para anticiparse a los eventos críticos, retrasa la atención técnica y dificulta la toma de decisiones informadas. Según datos internos, se ha registrado un incremento del 15 % en las quejas de conectividad y del 20 % en el tiempo promedio de resolución de incidencias en los últimos seis meses, lo cual evidencia una brecha importante en la gestión de fallas y la eficiencia operativa.

Esta situación no solo compromete la calidad del servicio, sino que también afecta la satisfacción del cliente y la reputación de la empresa en un mercado altamente competitivo. En particular, la imposibilidad de identificar rápidamente fallas energéticas o degradaciones de señal en enlaces inalámbricos complica la planeación de respuestas técnicas efectivas, como el traslado de plantas eléctricas o el reajuste de antenas emisoras. La ausencia de una arquitectura de monitoreo estructurada con alertas, sensores específicos y visualización jerárquica impide detectar los eventos de manera temprana y responder con agilidad.

En este contexto, se plantea la necesidad de diseñar un sistema técnico de monitoreo de redes adaptado a la infraestructura híbrida de Gigaredes Comunicaciones, que permita mejorar la visibilidad operativa, optimizar la gestión de eventos críticos y proporcionar una base sólida para decisiones técnicas basadas en datos. Esto conduce a la formulación de la siguiente pregunta orientadora:

¿Cómo diseñar un sistema de monitoreo, basado en la herramienta PRTG, que permita supervisar eficientemente la red híbrida GPON–WiMAX de Gigaredes Comunicaciones SAS, y que contribuya a la detección temprana de fallas y a la mejora de la gestión técnica en condiciones operativas adversas?

Justificación

El diseño de un sistema de monitoreo de redes para Gigaredes Comunicaciones SAS se justifica por su impacto en tres dimensiones fundamentales: académica, técnica-social y formativa. En primer lugar, desde una perspectiva académica y disciplinar, el proyecto representa una oportunidad concreta para aplicar competencias clave del programa de Ingeniería en Telecomunicaciones, como el diseño de soluciones de supervisión de redes, la integración de tecnologías convergentes (GPON–WiMAX) y la evaluación de herramientas especializadas como PRTG Network Monitor. La experiencia permite consolidar aprendizajes en gestión de redes, arquitectura lógica, indicadores de rendimiento y supervisión proactiva de infraestructura, en coherencia con los resultados de aprendizaje del plan de estudios.

Desde el ámbito técnico y social, el proyecto responde a una necesidad real y documentada de la empresa: la imposibilidad de detectar con anticipación fallas energéticas o degradaciones del servicio en nodos ubicados en zonas de difícil acceso. En regiones donde el acceso a servicios digitales es crítico para la educación, el trabajo y la comunicación —especialmente en sectores rurales— la falta de conectividad puede tener efectos adversos amplificados. Si bien el presente proyecto se limita al diseño, su desarrollo aporta una solución viable y estructurada que puede servir como hoja de ruta para una futura implementación, mejorando la resiliencia de la red, reduciendo los tiempos de respuesta ante incidentes, y aportando a la inclusión digital en contextos vulnerables.

En tercer lugar, desde un enfoque personal y formativo, el proyecto constituye una experiencia de síntesis profesional, al integrar conocimientos adquiridos durante la carrera con un problema real del entorno. Permite desarrollar habilidades en análisis crítico, documentación técnica, pensamiento sistémico y comunicación de soluciones complejas, además de establecer un vínculo colaborativo con una empresa del sector. Esta vivencia fortalece no solo las

capacidades técnicas del estudiante, sino también su perfil como futuro ingeniero con competencias para la innovación, la mejora continua y la toma de decisiones fundamentadas.

Finalmente, el diseño propuesto tiene un valor replicable y escalable. Puede ser adaptado por otras empresas de telecomunicaciones que enfrenten desafíos similares de supervisión en entornos geográficos complejos. De esta manera, el proyecto trasciende su aplicación puntual y se convierte en un insumo útil para el fortalecimiento de prácticas de monitoreo en redes híbridas del país.

Objetivos

Objetivo General

Diseñar un sistema de monitoreo de redes basado en PRTG Network Monitor para la infraestructura híbrida GPON y WiMAX de Gigaredes Comunicaciones SAS, que permita mejorar la supervisión técnica y anticipar fallas en nodos críticos.

Objetivos Específicos

Analizar la infraestructura de red actual de Gigaredes Comunicaciones SAS, enfocándose en los segmentos GPON y WiMAX, para identificar nodos críticos, condiciones operativas y necesidades de monitoreo.

Diseñar la arquitectura lógica del sistema de monitoreo con PRTG, definiendo sensores clave, niveles de alerta y esquemas de visualización para la supervisión de dispositivos y enlaces estratégicos.

Proponer una estrategia de supervisión remota de eventos críticos, especialmente fallas energéticas en zonas de difícil acceso, considerando criterios de prioridad operativa y escalabilidad futura.

Marco Teórico

Supervisión y Monitoreo de Redes: Fundamentos

El monitoreo de redes es un componente esencial en la gestión moderna de infraestructuras de telecomunicaciones. Consiste en la observación continua del estado de los dispositivos, enlaces y servicios de una red con el propósito de garantizar su disponibilidad, rendimiento y seguridad. Un sistema de monitoreo efectivo permite detectar fallas en tiempo real, generar alertas automáticas, visualizar el tráfico y analizar indicadores clave como el uso de ancho de banda, latencia, pérdidas de paquetes y disponibilidad de nodos (Kurose & Ross, 2021).

El valor estratégico del monitoreo radica en su capacidad para transformar datos operativos en decisiones técnicas informadas, optimizando la asignación de recursos, la planificación de mantenimiento y la atención de emergencias. En contextos con topologías complejas o condiciones ambientales adversas, el monitoreo es fundamental para garantizar la continuidad del servicio y anticiparse a eventos críticos.

Tecnología GPON: Arquitectura y Desafíos de Monitoreo

GPON (Gigabit Passive Optical Network) es una tecnología de red de acceso basada en fibra óptica que utiliza una arquitectura punto a multipunto. Permite brindar conectividad de alta velocidad a múltiples usuarios a través de una única fibra, dividiendo la señal mediante divisores ópticos pasivos. Entre sus características destacan su alta capacidad de transmisión (hasta 2.488 Gbps en bajada y 1.244 Gbps en subida), eficiencia energética y soporte para servicios con calidad de servicio diferenciada (QoS).

Desde el punto de vista del monitoreo, GPON requiere supervisión en componentes críticos como:

- OLT (Optical Line Terminal): corazón del sistema, donde se configuran servicios y se agregan las señales.
- ONT (Optical Network Terminal): equipos del usuario final, donde se deben monitorear niveles ópticos, errores y sincronización.
- Nivel óptico de enlace: es fundamental medir atenuación, pérdidas y latencia para garantizar la calidad del servicio.

En sistemas GPON, una degradación no detectada en el nivel óptico puede traducirse en una pérdida parcial del servicio, difícil de diagnosticar sin herramientas adecuadas de monitoreo.

Tecnología WiMAX: Operación y Retos Técnicos

WiMAX (Worldwide Interoperability for Microwave Access) es una tecnología de acceso inalámbrico de banda ancha, orientada a cubrir zonas de difícil acceso donde la instalación de fibra es limitada o costosa. Se implementa en configuraciones punto a multipunto, y puede operar en bandas licenciadas o no licenciadas, como la de 5 GHz, ampliamente utilizada por Gigaredes Comunicaciones SAS con equipos de la marca Ubiquiti.

Los principales parámetros de supervisión en una red WiMAX incluyen:

- RSSI (Received Signal Strength Indicator) y SNR (Signal to Noise Ratio): indicadores de calidad de la señal.
- Estado de los radios emisores/receptores.
- Disponibilidad de energía y respuesta ante interferencias.

Las condiciones climáticas, la interferencia electromagnética y la alineación de las antenas afectan significativamente el rendimiento de estos enlaces, lo que justifica un sistema de monitoreo que permita visualizar en tiempo real estos valores y generar alertas ante caídas o deterioros.

PRTG Network Monitor: Características, Ventajas y Casos de Uso

PRTG Network Monitor (Paessler Router Traffic Grapher) es una solución de software desarrollada por Paessler AG para la supervisión continua de redes de datos. Su diseño modular y su compatibilidad con múltiples protocolos —como SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation), NetFlow (sistema de monitoreo de flujo de red desarrollado por Cisco), Packet Sniffing, entre otros— lo convierten en una herramienta altamente adaptable a distintos entornos tecnológicos, incluidas redes híbridas como las de Gigaredes Comunicaciones SAS.

Entre sus características más destacadas se encuentran:

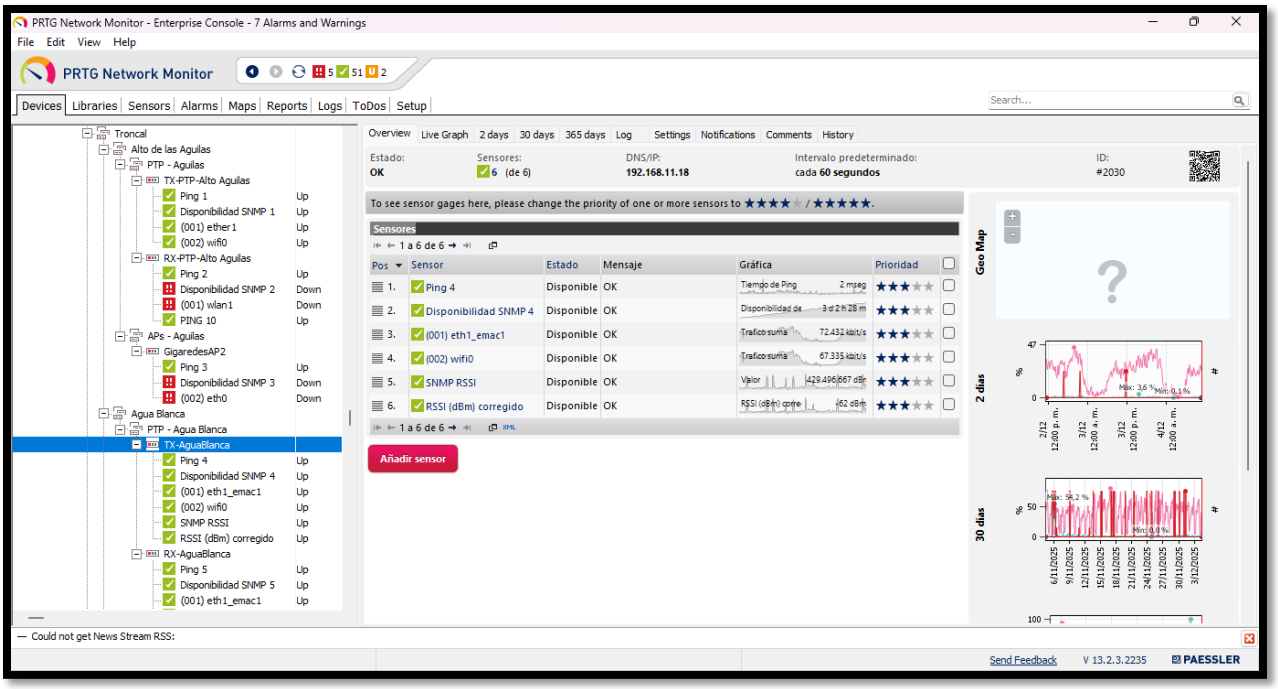
- Sensores personalizables, que permiten adaptar la supervisión a cada dispositivo específico (ONT, OLT, radios WiMAX, fuentes de energía).
- Alertas configurables, que notifican en tiempo real ante desviaciones de parámetros críticos.
- Tableros de control visuales, que permiten jerarquizar dispositivos y zonas, facilitando la interpretación operativa.
- Informes históricos automáticos, útiles para análisis de tendencias, auditorías y planificación de mantenimiento.

PRTG se distingue también por su interfaz intuitiva, su escalabilidad, y su soporte para entornos multivendor, lo cual es clave en infraestructuras como la de Gigaredes que combinan equipos de diferentes marcas y tecnologías (Ubiquiti, Mikrotik, Huawei, etc.). Casos documentados muestran que su uso reduce los tiempos de respuesta ante fallas en más de un 30 % y mejora la toma de decisiones técnicas al contar con visibilidad completa del estado de la red (Paessler AG, 2022).

En la Figura 1 se observa la interfaz principal de PRTG Network Monitor, en la que se organiza el árbol de dispositivos y se visualiza el estado de los sensores, alertas y gráficas de desempeño.

Figura 1

Interfaz principal de PRTG Network Monitor, donde se visualizan los dispositivos monitoreados.



Nota. Nota. Captura de pantalla de la interfaz principal de PRTG Network Monitor utilizada como referencia para el diseño del sistema de monitoreo de Gigaredes Comunicaciones SAS. En la vista se aprecia el árbol de dispositivos, el estado de los sensores y la navegación por pestañas para gráficos e historial, elementos base para la supervisión operativa por zonas.

Diseño de Sistemas de Monitoreo: Principios, Sensores y Alertas

El diseño de un sistema de monitoreo de redes requiere combinar principios de ingeniería de software, telecomunicaciones y gestión operativa. El objetivo no es solo recolectar datos, sino estructurar una arquitectura lógica que permita transformar eventos técnicos en información accionable. Para ello, se deben considerar los siguientes componentes clave:

- **Arquitectura jerárquica:** El sistema debe organizar los dispositivos en grupos lógicos (por ubicación, tipo, criticidad), facilitando la navegación y el análisis por parte del personal técnico.
- **Selección de sensores adecuados:** Cada tipo de dispositivo —sea una ONT (Optical Network Terminal), una antena Ubiquiti o un UPS (Uninterruptible Power Supply) — requiere sensores específicos (por ejemplo, latencia, tráfico, energía, temperatura, nivel óptico, etc.).
- **Definición de umbrales y categorías de alerta:** Se deben configurar valores de referencia para generar alertas en distintos niveles (informativas, advertencias, críticas), de forma que la atención pueda priorizarse según el impacto.
- **Visualización operativa:** El diseño debe contemplar dashboards y mapas de red que permitan ver el estado general y hacer zoom en los puntos críticos.
- **Escalabilidad y replicabilidad:** El sistema debe ser capaz de crecer junto con la red y permitir su adopción en otros entornos similares sin rediseño completo.

Además, se deben incluir mecanismos de registro histórico y exportación de datos, necesarios para realizar análisis longitudinales o justificar decisiones de inversión técnica.

Experiencias y Casos Similares: Aportes a la Solución Propuesta

Diversos estudios y aplicaciones en empresas del sector han demostrado los beneficios concretos de implementar sistemas de monitoreo como PRTG en redes mixtas o rurales. Por ejemplo, en un caso documentado por Smith et al. (2020), una red regional en el sur de México logró reducir en un 35 % los tiempos de detección de fallas tras la instalación de sensores jerarquizados en nodos remotos, usando una solución basada en SNMP con visualización en PRTG.

Otro ejemplo es el de Telecom Bolivia (Johnson, 2019), donde la incorporación de alertas automatizadas para caídas de energía en repetidores de zonas montañosas permitió mejorar la disponibilidad del servicio en más de 40 horas al mes. En ambos casos, los factores comunes fueron:

- La existencia de una infraestructura distribuida y heterogénea.
- Las dificultades de acceso físico a los nodos.
- La necesidad de visualización en tiempo real y priorización de alertas.

Estos antecedentes refuerzan la viabilidad del diseño propuesto en este proyecto y muestran que el uso de plataformas como PRTG es una estrategia válida y eficiente para redes híbridas en contextos operativos complejos como el de Gigaredes Comunicaciones SAS.

Metodología

El presente proyecto se enmarca en la modalidad de desarrollo tecnológico con alcance limitado al diseño técnico de un sistema de monitoreo de redes. No contempla la implementación operativa del sistema propuesto, sino la elaboración de un diseño funcional, fundamentado y adaptable a la infraestructura de la empresa Gigaredes Comunicaciones SAS.

La metodología adoptada corresponde a una versión adaptada del Ciclo de Vida de Desarrollo de Sistemas (SDLC), que incluye únicamente las fases de análisis, diseño y validación documental. Este enfoque permite estructurar de forma lógica y técnica el proceso de construcción del sistema sin incurrir en tareas de desarrollo o pruebas en campo.

Las fases del proyecto son las siguientes:

Análisis de la Infraestructura Actual

En esta fase se realiza una caracterización técnica de la red híbrida de Gigaredes Comunicaciones SAS, con énfasis en los nodos GPON y WiMAX. Se identifican puntos críticos, condiciones de operación adversas (como accesos difíciles y fallas energéticas), y requerimientos mínimos de monitoreo. Este análisis se apoya en entrevistas técnicas con el personal de soporte, revisión documental de la topología y análisis de registros históricos de fallas.

Diseño de la arquitectura lógica del sistema

A partir de los hallazgos del análisis, se desarrolla la propuesta de monitoreo utilizando la herramienta PRTG Network Monitor. El diseño incluye:

- Selección y descripción de sensores aplicables a dispositivos GPON y WiMAX.
- Definición de umbrales de alerta y categorías de criticidad.
- Agrupación jerárquica de dispositivos por zonas y funciones.

- Esquemas de visualización técnica, como dashboards, mapas de red y diagramas conceptuales.

Esta fase se desarrolla con apoyo de herramientas como Microsoft Visio, Lucidchart o The Dude para la diagramación, y recursos institucionales para la consulta técnica de manuales de equipos y configuración de PRTG.

Validación Documental del Diseño

La última fase consiste en una revisión crítica del diseño técnico propuesto, verificando su coherencia con la infraestructura real de la empresa, su viabilidad práctica y su alineación con los objetivos del proyecto. Esta validación se realiza a través de retroalimentación del tutor académico y del personal técnico de Gigaredes Comunicaciones. Además, se incluyen recomendaciones para una futura implementación, considerando los criterios de escalabilidad, sostenibilidad técnica y facilidad de adopción por parte del equipo operativo.

Técnicas e instrumentos de análisis

Se emplean técnicas mixtas de análisis, tanto cualitativas como cuantitativas:

- Revisión documental: análisis de diagramas de red, reportes de fallas, manuales técnicos de equipos GPON y Ubiquiti.
- Entrevistas semiestructuradas: con técnicos de Gigaredes para comprender las limitaciones actuales del monitoreo.
- Observación técnica indirecta: mediante análisis de registros operativos e informes de atención de incidentes.
- Estadística descriptiva básica: para interpretar indicadores operativos históricos (tiempos de respuesta, quejas, etc.).

Esta metodología permite alcanzar los objetivos propuestos sin requerir despliegue físico ni modificaciones en la red, cumpliendo con los criterios de un proyecto aplicable, técnico y viable dentro del marco del trabajo de grado en Ingeniería en Telecomunicaciones.

Criterios de Validación

Para el desarrollo de esta validación se consideraron los siguientes criterios:

Coherencia Técnica

Correspondencia entre los equipos reales de la red (Core, GPON y zona inalámbrica) y los sensores propuestos, garantizando compatibilidad con los protocolos utilizados (SNMP, WMI y Ping).

Viabilidad Operativa

Capacidad del diseño para facilitar la supervisión remota, la detección temprana de fallas y la priorización de eventos críticos, especialmente en nodos de difícil acceso.

Escalabilidad

Posibilidad de ampliar el sistema de monitoreo incorporando nuevos dispositivos, sensores o sedes sin alterar la arquitectura base.

Usabilidad

Claridad en la visualización de la información mediante mapas de red, dashboards y esquemas jerárquicos que permitan una interpretación rápida por parte del operador.

Mecanismos de Validación Documental

La validación del diseño se apoya en distintos elementos documentales desarrollados a lo largo del proyecto, entre los cuales se destacan:

- Diagramas conceptuales y mapas lógicos, elaborados con herramientas como Visio y The Dude, que representan la estructura general del sistema de monitoreo, la segmentación por zonas y la relación entre dispositivos, sensores y alertas.
- Tablas de sensores y parámetros monitoreados, donde se establecen los indicadores clave por tipo de equipo, junto con umbrales de advertencia y criticidad acordes a buenas prácticas de monitoreo de redes.
- Ejemplos de dashboards y mapas de estado, que permiten validar la forma en que la información puede organizarse visualmente para ofrecer una visión global de la red y facilitar la toma de decisiones.
- Guías ilustradas y procedimientos documentados, que demuestran la posibilidad de configurar el diseño propuesto directamente en la plataforma PRTG Network Monitor, confirmando su aplicabilidad técnica.

Resultado de la Validación

A partir del análisis de los elementos anteriores, se concluye que el diseño del sistema de monitoreo es técnicamente coherente, operativamente funcional y alineado con la infraestructura actual de Gigaredes Comunicaciones SAS. La validación documental evidencia que el sistema propuesto cumple con los objetivos específicos del proyecto, permite identificar nodos críticos, supervisar eventos relevantes y servir como base sólida para una futura implementación progresiva, ajustada a los recursos y necesidades de la organización.

Diseño Técnico del Sistema de Monitoreo

Como resultado principal de este proyecto se presenta el diseño técnico estructurado de un sistema de monitoreo de redes híbridas GPON–WiMAX, adaptado a las necesidades operativas y geográficas de Gigaredes Comunicaciones SAS. El diseño fue elaborado con base en los requerimientos identificados en la infraestructura actual de la empresa y se desarrolla dentro de la plataforma PRTG Network Monitor, elegida por su compatibilidad con protocolos estándar y su facilidad de integración con equipos multivendor.

Arquitectura Lógica del Sistema de Monitoreo

El sistema de monitoreo propuesto se estructura en tres zonas funcionales que reflejan la organización operativa de la red de Gigaredes Comunicaciones SAS: zona de core, zona de distribución GPON y zona inalámbrica. La arquitectura lógica está diseñada para facilitar la supervisión jerarquizada y geográficamente segmentada de los dispositivos clave, permitiendo la identificación rápida de fallas y el análisis de indicadores críticos en tiempo real.

Zona de Core

Esta zona corresponde al centro de operaciones de Gigaredes, donde se concentran los equipos principales encargados del enrutamiento, la provisión de servicios internos y la salida hacia Internet. Los dispositivos a monitorear en esta zona son:

- Servidor Mikrotik CCR1036-8G-2S+: equipo principal que recibe la conexión del proveedor y realiza el enrutamiento de todo el tráfico. Se propone monitorear CPU, uso de RAM, tráfico en interfaces, disponibilidad de puertos y latencia general.
- Servidor HP ProLiant DL360p con Proxmox: servidor de virtualización encargado de alojar múltiples servicios críticos como:
    - Sistema de gestión MikroTISP

    - Servidor VPN (Virtual Private Network) WireGuard
    - Servidor DNS (Domain Name System) local
- Cada máquina virtual será supervisada a través de sensores de uso de recursos (CPU, disco, red), así como disponibilidad del servicio.
- OLT Huawei MA5608T: equipo central del sistema GPON. Se propone monitorear el estado de los puertos PON, el tráfico agregado por puerto VLAN (Virtual Local Area Network), y los errores de transmisión o desconexión.
- UPS de respaldo: se integrará mediante sensores SNMP si es compatible, para vigilar parámetros como carga, voltaje de entrada/salida, tiempo de respaldo y estado de la batería.

Esta zona representa el "cerebro" de la red, por lo que su monitoreo debe tener el mayor nivel de prioridad y alertas con umbrales más estrictos.

Zona de distribución GPON

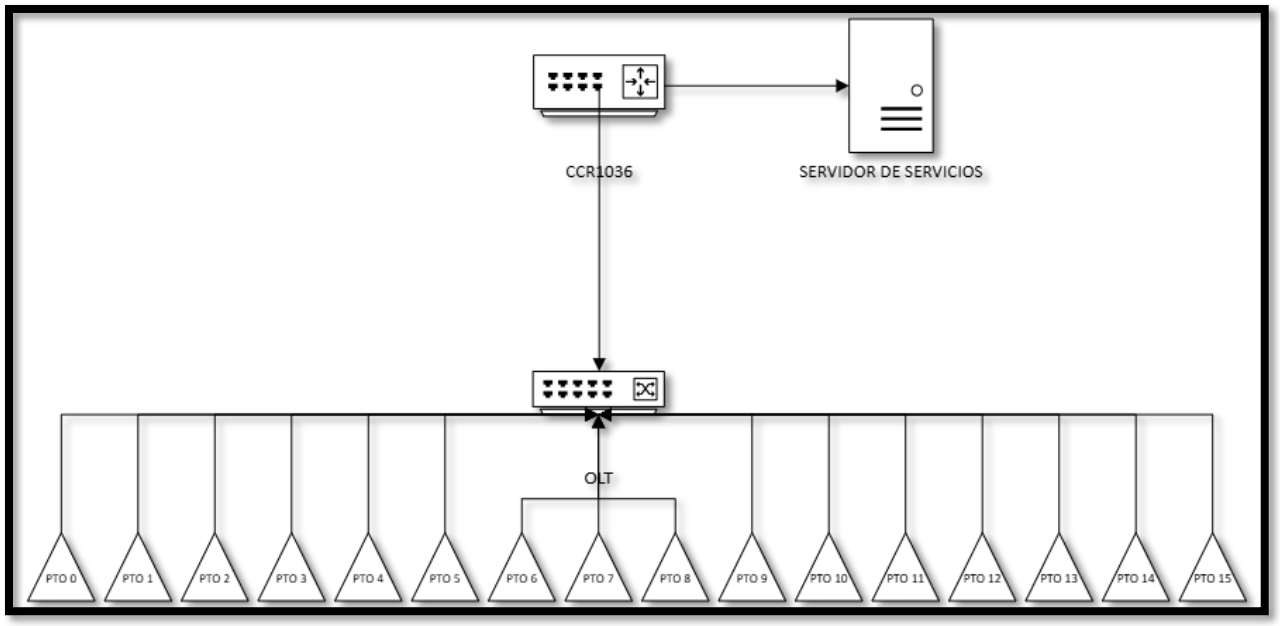
En esta zona se encuentra la segmentación del tráfico hacia los distintos sectores urbanos y rurales conectados mediante fibra óptica pasiva. Aunque no se realizará monitoreo directo a los clientes finales, se implementará supervisión a nivel de puertos VLAN en la OLT Huawei MA5608T, permitiendo:

- Observar el tráfico por sector o zona.
- Identificar congestiones o caídas masivas en segmentos específicos.
- Analizar tendencias de consumo para futuras decisiones de ampliación.
- Este nivel de supervisión permite mantener una visión global sin saturar el sistema con sensores individuales por cliente.

En la Figura 2 se presenta el diagrama unifilar de la interconexión entre la zona Core y la red de fibra óptica GPON de Gigaredes Comunicaciones SAS, donde se evidencia la OLT con una única tarjeta GPON y la distribución de sus 16 puertos PON.

Figura 2

Esquema de red GPON.



Nota. Diagrama unifilar que representa la interconexión entre la zona Core y la red de fibra óptica GPON de Gigaredes Comunicaciones SAS. En el esquema se identifica la OLT con una única tarjeta GPON y sus 16 puertos PON (PTO 0 a PTO 15), los cuales constituyen los puntos de salida hacia la red de acceso. Esta representación permite comprender la estructura básica de distribución GPON y facilita la identificación de los elementos críticos a supervisar dentro del sistema de monitoreo propuesto.

Zona Inalámbrica

La red inalámbrica de Gigaredes está compuesta por torres o nodos remotos que utilizan tecnología WiMAX en banda de 5 GHz. Esta zona incluye enlaces AP (Access Points) y enlaces

PTP (punto a punto) de interconexión. Se propone configurar sensores SNMP en cada uno de los radios para monitorear:

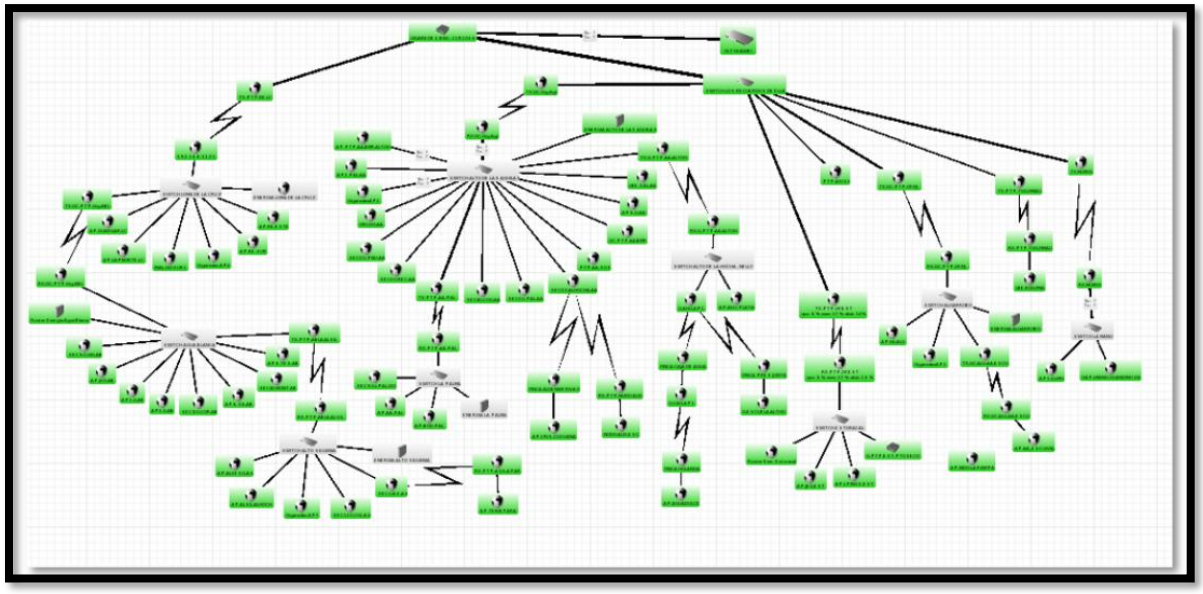
- RSSI y SNR en tiempo real.
- Estado de interfaz inalámbrica.
- Estado de conectividad (ping, latencia).
- Carga del dispositivo.

Este tipo de monitoreo permite detectar degradaciones por interferencia, orientación de antenas o condiciones climáticas adversas. Dado que estas torres están ubicadas en cerros o zonas de difícil acceso, se considera una de las zonas más críticas del sistema.

En la Figura 3 se presenta la topología general de la red de radioenlaces de Gigaredes Comunicaciones SAS, en la cual se identifican los diferentes nodos inalámbricos y su interconexión mediante enlaces en cascada, característica del diseño de la red de acceso inalámbrica.

Figura 3

Topología de red de radioenlace.



Nota. Diagrama que representa la topología de la red de radioenlaces de Gigaredes Comunicaciones SAS, donde se visualizan los distintos nodos inalámbricos interconectados mediante una estructura en cascada. El esquema permite identificar la jerarquía de los enlaces, los nodos principales y secundarios, así como los puntos críticos de interconexión, información fundamental para el diseño del sistema de monitoreo y la detección de posibles fallas que puedan afectar múltiples segmentos de la red.

Sensores Propuestos y Parámetros Monitoreados.

Con base en las especificaciones de los equipos utilizados por Gigaredes, se diseñó una propuesta de sensores compatibles con SNMP y API, que permiten la supervisión en tiempo real: Sensores para OLTs, APs y PTP(Huawei/Mikrotik/Ubiquiti):

- Estado de CPU (Central Processing Unit) y RAM (Random Access Memory).
- Tráfico en interfaces.
- Estado de servicio de puertos PON (Red Óptica Pasiva).
- Sensores ambientales:
    - Temperatura.
    - Voltaje.
    - Alerta de falla de red eléctrica.

La Tabla 1 presenta la relación de sensores propuestos por zona de la red, indicando los parámetros monitoreados y los umbrales de alerta sugeridos.

Tabla 1

Sensores propuestos y parámetros monitoreados por zona.

Zona	Dispositivo / Componente	Sensor propuesto	Parámetro monitoreado	Umbral de alerta sugerido
Core	Mikrotik CCR1036-8G-2S+	SNMP Traffic Sensor	Uso de ancho de banda por interfaz	> 85 % durante 10 minutos
		SNMP CPU Load Sensor	Uso de CPU	> 90 %
		SNMP Memory Sensor	Uso de RAM	> 85 %
Core	HP ProLiant DL360p (Proxmox VMs)	WMI or SNMP Service Sensor	Disponibilidad de MikroTISP, VPN y DNS	Servicio inactivo
		SNMP CPU / Disk Sensor	Uso de CPU y disco por VM	> 85 %
Core	OLT Huawei MA5608T	SNMP Custom Sensor (VLAN)	Tráfico por puerto/VLAN	Caída de tráfico o congestión persistente
		SNMP Interface Sensor	Estado de puerto	Puerto inactivo

Core	UPS de respaldo	SNMP UPS Sensor	Voltaje, carga, tiempo de respaldo	Voltaje bajo o batería crítica
Distribución GPON	Puerto PON en OLT	SNMP VLAN Traffic Sensor	Tráfico agregado por VLAN	Congestión > 85 %
		SNMP Optical Power Sensor (si aplica)	Atenuación óptica	< –28 dBm
Zona inalámbrica	Radios Ubiquiti (AP y PTP)	SNMP RSSI Sensor	Intensidad de señal (RSSI)	< –85 dBm
		SNMP SNR Sensor	Relación señal/ruido (SNR)	< 15 dB
		Ping Sensor / Packet Loss	Latencia / pérdida de paquetes	RTT > 80 ms o > 5 % pérdida
		SNMP Uptime Sensor	Tiempo en línea	Reinicios inesperados detectados

Nota. Los sensores y umbrales de alerta presentados en esta tabla corresponden a una propuesta de diseño del sistema de monitoreo y se establecen con base en buenas prácticas de supervisión de redes, las características técnicas de los equipos utilizados por Gigaredes Comunicaciones SAS y las condiciones operativas de su infraestructura híbrida GPON–WiMAX. Los valores definidos permiten identificar de manera temprana situaciones de congestión, degradación del

servicio, fallas energéticas y eventos críticos, sin que representen necesariamente una implementación activa del sistema.

Sensores Propuestos para la Zona Inalámbrica (AP y Radioenlaces)

La Tabla 2 presenta el conjunto de sensores propuestos para los puntos de acceso y radioenlaces inalámbricos que conforman la red de distribución de Gigaredes Comunicaciones SAS. Debido a la alta dispersión geográfica y a la criticidad operativa de estos nodos, se definieron sensores orientados principalmente a la supervisión de la disponibilidad, la calidad del enlace y el uso de las interfaces principales. Los parámetros y umbrales establecidos permiten detectar de forma temprana condiciones de degradación del servicio, como incrementos de latencia, pérdida de paquetes o comportamientos anómalos en el tráfico.

Tabla 2

Sensores propuestos y parámetros monitoreados por AP.

Equipo	**Sensor PRTG**	**Parámetro Monitoreado**	**Unidad**	**Umbral Warning**	**Umbral Crítico**
SEC90-GIG-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC90-GIG-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-JVO-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
AP-JVO-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP1-G-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP1-G-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP3-G-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP3-G-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC50-COR-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC50-COR-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

AP5-SIL-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP5-SIL-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC40-MONT-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC40-MONT-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP6-TES-AB	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP6-TES-AB	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
GigaredesAP1	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

GigaredesAP1	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-FA-ALG	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-FA-ALG	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-CRIS-CUCUANA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-CRIS-CUCUANA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
NODO-ALIX-ESC	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
NODO-ALIX-ESC	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
G-CAG-AP1	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
G-CAG-AP1	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-AGUADULCE	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-AGUADULCE	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
G-AHO-AP1	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
G-AHO-AP1	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-AH-CPLATA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-AH-CPLATA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

G-ESCUELA-ALTHO	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
G-ESCUELA-ALTHO	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-PTP-AA-BMR-ALTOH	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-PTP-AA-BMR-ALTOH	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP2-PAL-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP2-PAL-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
GigaredesAP2	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

GigaredesAP2	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
GRI-GVI-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
GRI-GVI-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP5-G-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP5-G-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC30-REC-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC30-REC-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC30-PNU-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
SEC30-PNU-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC40-COG-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC40-COG-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC30-PAL-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC30-PAL-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC30-ALHOCHA-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC30-ALHOCHA-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

PTP-AA-SOS	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
PTP-AA-SOS	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
GC-PTP-AA-BMR	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
GC-PTP-AA-BMR	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
LBE-SAL-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
LBE-SAL-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-AA_ESC-GVIA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

AP-AA_ESC-GVIA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-TEM-BPARA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-TEM-BPARA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-AL3ESQ-AS	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-AL3ESQ-AS	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-ALSIL-ALHOCH	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-ALSIL-ALHOCH	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
Gigaredes AP7	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
Gigaredes AP7	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC-CAS-AS	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC-CAS-AS	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC120-COL-AS	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC120-COL-AS	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
LBE-ROD-FMA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
LBE-ROD-FMA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

G-PTP-EST-PTOSECO	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
G-PTP-EST-PTOSECO	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-LPINOS-EST	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-LPINOS-EST	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-JEG-EST	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-JEG-EST	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP1-G-LMG	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

AP1-G-LMG	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
GAP-LMANO-GUANDINOZA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
GAP-LMANO-GUANDINOZA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
SEC90-LPAL-GVI	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
SEC90-LPAL-GVI	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-AA-PAL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-AA-PAL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-BOD-PAL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
AP-BOD-PAL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-GUARGAR-LC	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-GUARGAR-LC	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-LAPNORTE-LC	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-LAPNORTE-LC	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
INAL-GIGSUR1	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
INAL-GIGSUR1	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

Gigaredes AP4	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
Gigaredes AP4	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-RE-SUR	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-RE-SUR	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-RE-ESTE	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-RE-ESTE	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
PTP-AXIS2	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

PTP-AXIS2	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-NIDO-LAPAMPA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-NIDO-LAPAMPA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
AP-SECSUR-LC	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
AP-SECSUR-LC	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-GC-PTP-OF-FJL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-GC-PTP-OF-FJL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-GC-PTP-OF-FJL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
RX-GC-PTP-OF-FJL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-GC-PTP-FJL-NID	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-GC-PTP-FJL-NID	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-GC-PTP-FJL-NID	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-GC-PTP-FJL-NID	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-PTP-TOG-FIMAU	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-PTP-TOG-FIMAU	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

RX-PTP-TOG-FIMAU	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-PTP-TOG-FIMAU	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-PTP-MLMDG	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-PTP-MLMDG	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-PTP-MLMDG	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-PTP-MLMDG	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-GC-PTP-GIG-EST	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

TX-GC-PTP-GIG-EST	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-GC-PTP-GIG-EST	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-GC-PTP-GIG-EST	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-GC-PTP-GIG-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-GC-PTP-GIG-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-GC-PTP-GIG-AA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-GC-PTP-GIG-AA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-GC-PTP-Gig-ABL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
TX-GC-PTP-Gig-ABL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-GC-PTP-Gig-ABL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-GC-PTP-Gig-ABL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-PTP-RE-LC	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-PTP-RE-LC	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-PTP-RE-LC	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-PTP-RE-LC	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

TX-G-PTP-EST-PTOSECO	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-G-PTP-EST-PTOSECO	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-G-PTP-EST-PTOSECO	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-G-PTP-EST-PTOSECO	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-PTP-AA-PAL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-PTP-AA-PAL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-PTP-AA-PAL	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%

RX-PTP-AA-PAL	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-PTP-ABLA-ALSIL-2	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-PTP-ABLA-ALSIL-2	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-PTP-ABLA-ALSIL-2	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-PTP-ABLA-ALSIL-2	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-G-PTP-AA-ALTOH	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-G-PTP-AA-ALTOH	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-G-PTP-AA-ALTOH	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o	RTT > 100 ms o

				pérdida > 1%	pérdida > 3%
RX-G-PTP-AA-ALTOH	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
TX-GC-ALG-AA-ESCU	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
TX-GC-ALG-AA-ESCU	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-GC-ALG-AA-ESCU	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-GC-ALG-AA-ESCU	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-FINCA ARLAN FIN. LUCERO	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-FINCA ARLAN FIN. LUCERO	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

RX-FINCA CAJA DE AGUA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-FINCA CAJA DE AGUA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-FINCA HOLANDA	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-FINCA HOLANDA	SNMP tráfico	Uso de interfaz principal	Mbps	-	-
RX-FINCA ALDEMAR RIVAS	Ping	Latencia/Disponibilidad	ms/%	RTT > 50 ms o pérdida > 1%	RTT > 100 ms o pérdida > 3%
RX-FINCA ALDEMAR RIVAS	SNMP tráfico	Uso de interfaz principal	Mbps	-	-

Nota: La tabla presenta los sensores propuestos para la supervisión de puntos de acceso (AP) y enlaces inalámbricos de la red de Gigaredes Comunicaciones SAS, utilizando principalmente sensores de latencia, disponibilidad y tráfico mediante PRTG Network Monitor. Los umbrales de advertencia (Warning) y críticos se establecen con base en parámetros operativos aceptables para

enlaces inalámbricos, permitiendo identificar de forma temprana degradaciones en el desempeño, congestión de interfaces o pérdidas de conectividad. Los sensores de tráfico no incluyen umbrales definidos, ya que su función principal es el análisis de comportamiento y tendencias históricas, más que la generación de alertas inmediatas.

Umbrales y Alertas Sugeridos

La definición de umbrales de alerta constituye un elemento crítico dentro del diseño del sistema de monitoreo, ya que permite clasificar los eventos según su nivel de impacto operativo y facilitar la toma de decisiones por parte del personal técnico. En este proyecto, los umbrales se establecen con el objetivo de anticipar fallas, detectar degradaciones progresivas del servicio y priorizar la atención de eventos críticos en la infraestructura de Gigaredes Comunicaciones SAS.

Clasificación de Severidad

El sistema de monitoreo propuesto adopta un esquema de severidad basado en dos niveles principales, alineados con las convenciones de la plataforma PRTG Network Monitor:

Advertencia (Warning). Indica una condición anómala o un comportamiento fuera de los rangos normales de operación que, si bien no representa una interrupción inmediata del servicio, puede escalar a una falla crítica si no se atiende oportunamente.

Crítico (Critical). Representa una condición que afecta directamente la disponibilidad, el desempeño o la estabilidad del servicio, requiriendo intervención inmediata del área técnica.

Esta clasificación permite al operador priorizar eventos, reducir tiempos de diagnóstico y enfocar los recursos en los nodos con mayor impacto sobre los usuarios finales.

Criterios de Definición de Umbrales

Los umbrales de alerta definidos en el diseño se establecieron considerando los siguientes criterios:

- Buenas prácticas de monitoreo de redes IP e inalámbricas, ampliamente documentadas en entornos ISP.
- Condiciones reales de operación observadas en la infraestructura de Gigaredes, especialmente en zonas rurales y de difícil acceso.
- Capacidad de los equipos monitoreados, evitando umbrales excesivamente estrictos que generen alertas falsas o saturación de notificaciones.
- Impacto operativo del evento, priorizando métricas que afecten directamente la experiencia del usuario, como latencia, pérdida de paquetes y calidad del enlace.

Umbrales Aplicados por Tipo de Parámetro

De manera general, los umbrales definidos se aplican según el tipo de métrica monitoreada:

Disponibilidad y Latencia (Ping). Se establecen valores de advertencia ante incrementos sostenidos en el tiempo de respuesta o pérdidas leves de paquetes, y niveles críticos cuando la latencia supera valores aceptables o se presenta una pérdida significativa que compromete el servicio.

Uso de Recursos (CPU, Memoria y Disco). Los umbrales permiten identificar condiciones de sobrecarga progresiva que puedan derivar en degradación del desempeño o reinicios inesperados de los equipos.

Tráfico de Red (SNMP Traffic). Se consideran eventos de advertencia cuando el uso del ancho de banda se aproxima a la capacidad máxima de la interfaz, y eventos críticos cuando se mantiene un nivel de congestión que puede afectar la calidad del servicio.

Parámetros Inalámbricos (RSSI y SNR). Los umbrales definidos permiten detectar degradaciones en la calidad del enlace, facilitando la identificación temprana de interferencias, desalineaciones o cambios en el entorno radioeléctrico.

Relación con la Visualización y la Estrategia Operativa

Los niveles de severidad definidos se reflejan directamente en los dashboards y mapas operativos mediante una codificación visual estandarizada, donde el color verde indica operación normal, amarillo condiciones de advertencia y rojo eventos críticos. Esta representación facilita la supervisión continua y la rápida identificación de incidentes prioritarios.

Asimismo, los umbrales establecidos se integran con la estrategia de supervisión remota para eventos críticos, permitiendo activar notificaciones y procedimientos de atención diferenciados según la severidad del evento, optimizando la gestión operativa de la red.

Visualización y Dashboards Operativos

La visualización de la información constituye un componente esencial del sistema de monitoreo propuesto, ya que permite al personal técnico interpretar de forma rápida y precisa el estado de la red, identificar eventos anómalos y priorizar acciones correctivas. En este diseño, la plataforma PRTG Network Monitor se utiliza para centralizar la información proveniente de los distintos sensores y presentarla mediante dashboards y vistas gráficas organizadas por zonas operativas.

Organización de Dashboards por Zonas

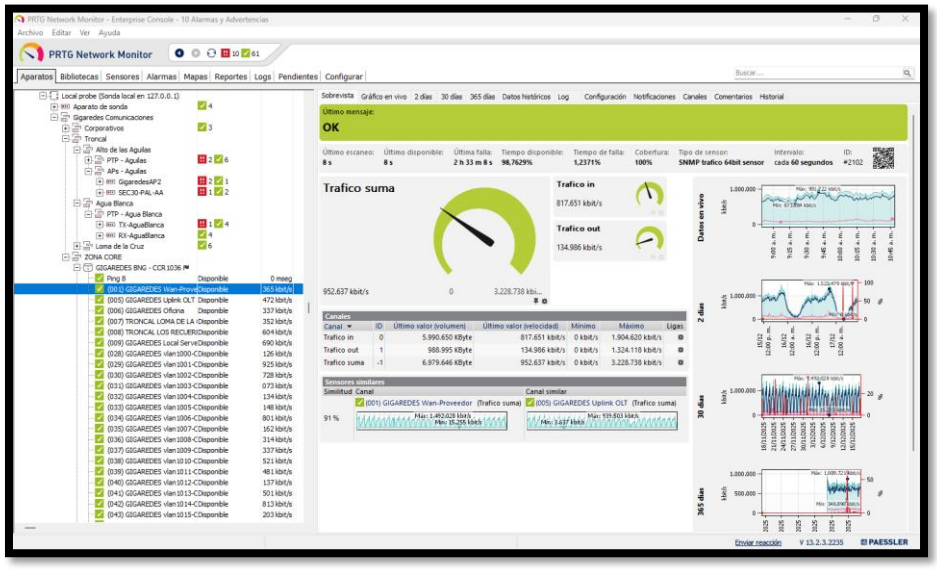
Los dashboards se estructuran de acuerdo con la segmentación lógica de la red, agrupando los dispositivos y sensores en Zona Core, Distribución GPON y Zona Inalámbrica. Esta organización permite al operador obtener una visión global del estado de cada segmento y localizar rápidamente el origen de una falla o degradación del servicio. En los paneles principales se visualiza el estado general de los sensores, empleando una codificación de colores estándar (verde, amarillo y rojo) que facilita la lectura inmediata del estado operativo.

En la Figura 4 se presenta el dashboard general de monitoreo por zonas implementado en PRTG Network Monitor, el cual consolida en una sola vista el estado operativo de los

dispositivos y sensores del Core, la red de distribución GPON y la zona inalámbrica. Esta visualización permite al operador supervisar el tráfico agregado, el estado de las interfaces críticas y la disponibilidad general de la red, facilitando la detección temprana de eventos que puedan afectar la continuidad del servicio.

Figura 4

Dashboard general de monitoreo por zonas en PRTG Network Monitor



Nota: El dashboard presenta una vista consolidada del estado de los sensores organizados por zonas operativas de la red (Core, distribución GPON y zona inalámbrica), permitiendo visualizar de forma centralizada el tráfico agregado, el comportamiento de las interfaces y el estado general de los dispositivos monitoreados. La codificación visual y las gráficas históricas facilitan la identificación temprana de eventos anómalos y apoyan la toma de decisiones operativas.

Visualización de Métricas Críticas

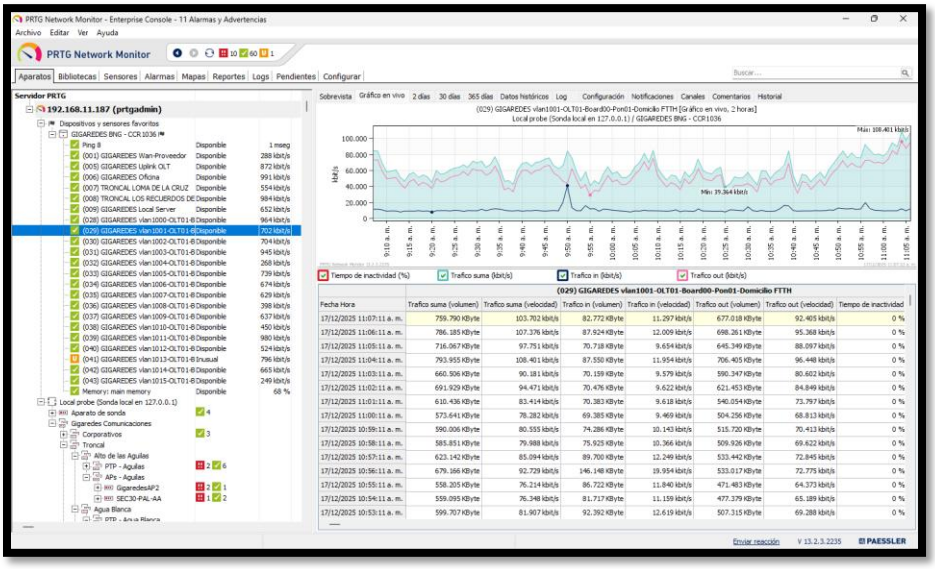
El sistema de monitoreo presenta de forma gráfica las métricas más relevantes para la operación de la red, tales como el tráfico de red, la latencia, la pérdida de paquetes y la calidad de los enlaces inalámbricos. Las gráficas históricas permiten identificar patrones de

comportamiento, picos de uso y tendencias anómalas que podrían derivar en eventos críticos si no se atienden oportunamente.

Como se observa en la Figura 5, el sistema de monitoreo permite visualizar de forma histórica el comportamiento del tráfico de red, facilitando la identificación de picos de consumo, variaciones anómalas y tendencias que pueden afectar la estabilidad y el desempeño del servicio.

Figura 5

Gráfica de Tráfico SNMP para una VLAN/Interfaz Monitoreada



*Nota***.** La figura muestra la visualización histórica del tráfico de red correspondiente a la VLAN/interfaz 1001 monitoreada mediante sensores SNMP en la plataforma PRTG Network Monitor. En la gráfica se representan de forma diferenciada los valores de tráfico entrante (*Traffic in*), tráfico saliente (*Traffic out*) y tráfico total (*Traffic sum*), permitiendo analizar el comportamiento del ancho de banda a lo largo del tiempo como una métrica crítica para la operación de la red. Este tipo de visualización facilita la identificación de patrones de uso, picos de consumo y variaciones anómalas que pueden estar asociadas a eventos de congestión, cambios en la demanda de los usuarios o condiciones operativas particulares del sector

monitoreado. Asimismo, la disponibilidad de datos históricos y métricas agregadas permite al operador realizar análisis comparativos, evaluar tendencias y anticipar posibles saturaciones de capacidad, contribuyendo a una gestión más eficiente y proactiva de la red. Esta visualización se integra al diseño del sistema de monitoreo propuesto, permitiendo a Gigaredes Comunicaciones SAS supervisar de forma continua el desempeño de las VLAN críticas de la red GPON y apoyar la toma de decisiones operativas orientadas a la calidad del servicio

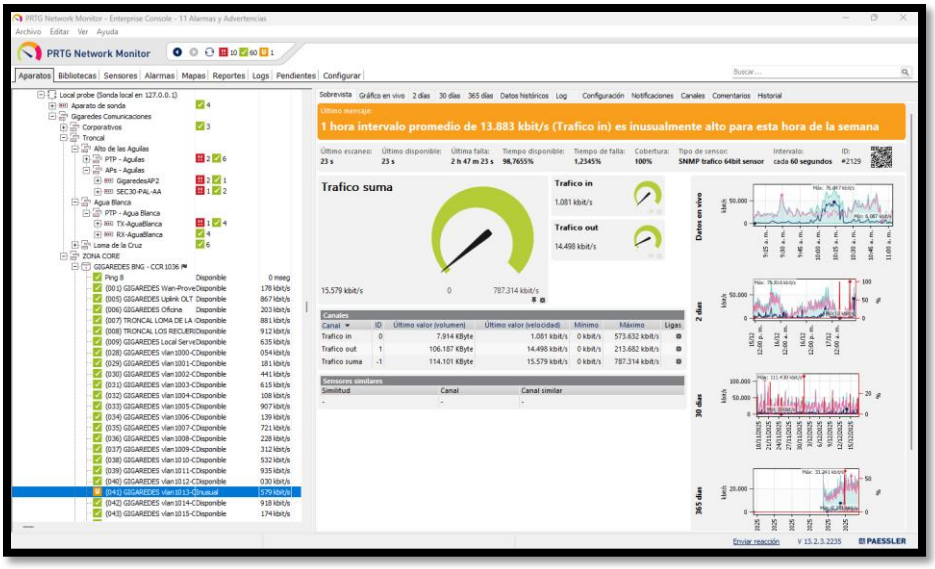
Representación Visual de Alertas

Cuando un sensor supera los umbrales definidos, PRTG genera alertas que se reflejan tanto en los dashboards como en las vistas individuales de cada sensor. Estas alertas permiten identificar condiciones de advertencia o criticidad, como congestión de tráfico, degradación de enlaces o comportamientos inusuales en el consumo de ancho de banda. La visualización inmediata de estos eventos facilita la toma de decisiones y reduce los tiempos de respuesta ante incidentes.

Como se evidencia en la Figura 6, el sistema de monitoreo genera alertas visuales automáticas cuando se presentan desviaciones significativas respecto a los patrones normales de operación, permitiendo una respuesta rápida ante condiciones de advertencia o criticidad.

Figura 6

Ejemplo de alerta generada por comportamiento anómalo del tráfico



Nota. La figura muestra una alerta generada por la plataforma PRTG Network Monitor cuando un sensor supera los umbrales operativos previamente definidos, debido a un comportamiento inusual del tráfico detectado mediante la comparación del valor promedio del intervalo con patrones históricos para la misma franja horaria. Este mecanismo de alertamiento permite identificar de manera oportuna anomalías operativas, como picos atípicos de consumo o variaciones inesperadas en la demanda, facilitando la intervención temprana del personal técnico y contribuyendo a la continuidad y estabilidad del servicio.

Soporte a la Operación y Toma de Decisiones

La combinación de dashboards, gráficas históricas y alertas visuales proporciona una herramienta efectiva para la supervisión continua de la red. Este enfoque permite al operador priorizar la atención de nodos críticos, realizar análisis preliminares antes de una intervención en campo y respaldar la estrategia de supervisión remota definida en el proyecto.

Diagramas Conceptuales del Sistema de Monitoreo

Como parte del diseño técnico del sistema de monitoreo propuesto para Gigaredes Comunicaciones SAS, se presenta un diagrama unifilar de la red, el cual permite visualizar de

manera general la topología de la infraestructura actual y los principales puntos donde se plantea la supervisión de servicios y enlaces críticos.

El diagrama no representa de forma explícita la arquitectura interna del sistema de monitoreo ni la configuración detallada de sensores y alertas; sin embargo, cumple un papel fundamental como base conceptual, ya que permite identificar los nodos estratégicos sobre los cuales se estructura el diseño del monitoreo propuesto.

Diagrama Unifilar de la Red y Puntos Críticos de Supervisión

La Figura 7 muestra la interconexión entre los principales componentes de la red de Gigaredes, incluyendo el Core, la infraestructura GPON y la zona inalámbrica, evidenciando la relación jerárquica y funcional entre estos segmentos. A partir de esta representación se identifican los siguientes elementos clave:

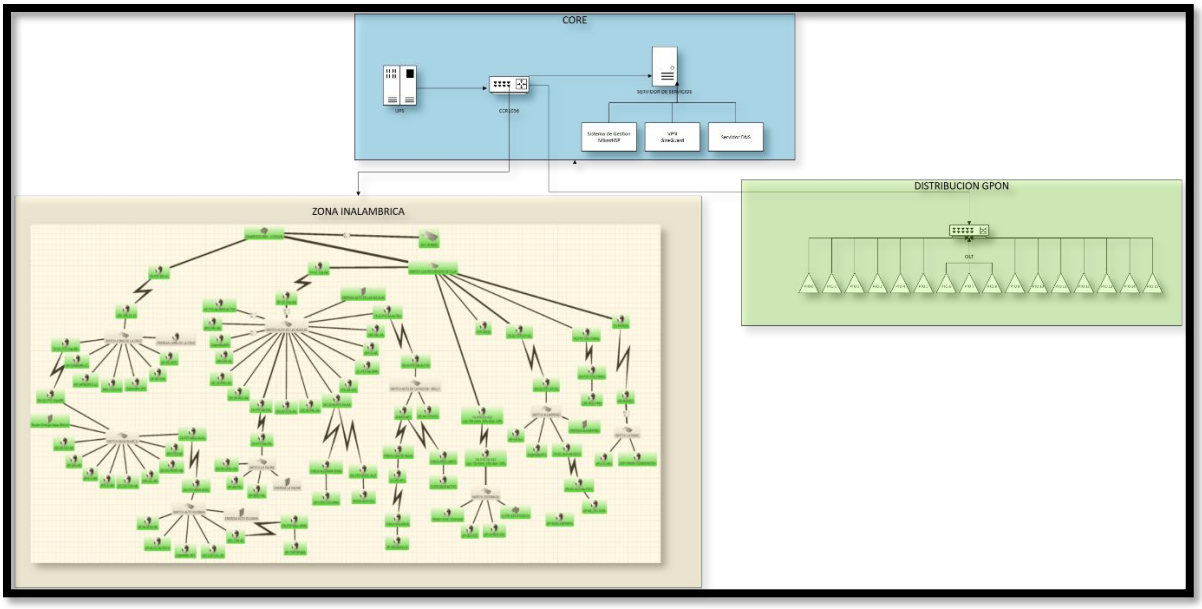
Zona Core. Conformada por el router principal, servidores y equipos de borde, desde donde se concentra el tráfico y se gestionan los servicios críticos. Estos nodos se consideran de alta prioridad para el monitoreo debido a su impacto global en la operación de la red.

Distribución GPON. Representada por la OLT y los enlaces de acceso hacia los distintos sectores, permitiendo identificar los puntos donde se concentra el tráfico por VLAN y donde pueden presentarse eventos de congestión o fallas masivas.

Zona Inalámbrica. Compuesta por enlaces punto a punto y puntos de acceso, generalmente ubicados en cerros o zonas de difícil acceso, los cuales requieren especial atención debido a su exposición a fallas energéticas, interferencias y condiciones ambientales adversas.

Figura 7

Representación unifilar de la arquitectura de red y puntos estratégicos de monitoreo.



Nota. Diagrama unifilar que representa la relación entre el Core, la red GPON y la zona inalámbrica de Gigaredes Comunicaciones SAS. La representación permite identificar los puntos estratégicos definidos para supervisión dentro del sistema de monitoreo propuesto. Elaboración propia con base en documentación técnica de la empresa.

Relación del Diagrama con el Diseño del Sistema de Monitoreo

Si bien el diagrama unifilar describe principalmente la topología de red, este se utiliza como insumo técnico para definir la arquitectura lógica del monitoreo, la agrupación de dispositivos en la plataforma PRTG y la asignación de sensores según la criticidad de cada nodo. A partir de esta base se establece:

- La segmentación del sistema de monitoreo por zonas (Core, GPON e inalámbrica).
- La selección de sensores específicos para cada tipo de equipo, de acuerdo con su función y nivel de impacto operativo.
- La priorización de alertas, enfocada en nodos críticos identificados en el diagrama, especialmente aquellos ubicados en zonas de difícil acceso.

Alcance del Uso del Diagrama

El diagrama unifilar presentado no pretende sustituir los esquemas detallados de configuración del sistema de monitoreo, sino que complementa el diseño técnico al proporcionar una visión global de la red sobre la cual se fundamentan las decisiones de supervisión. Su función principal es servir como referencia visual para comprender la distribución de la infraestructura y justificar la ubicación de sensores, dashboards y estrategias de monitoreo definidas en secciones posteriores del documento.

Guía Ilustrada y Paso a Paso para la Creación y Visualización de Sensores en PRTG Network Monitor

La presente guía tiene un carácter ilustrativo y demostrativo, y se incluye con el propósito de evidenciar la viabilidad técnica del diseño del sistema de monitoreo propuesto. Los procedimientos descritos no constituyen un manual exhaustivo de implementación, sino un conjunto de ejemplos representativos que permiten validar que los sensores, dispositivos y esquemas de visualización definidos pueden configurarse de manera efectiva en la plataforma PRTG Network Monitor, de acuerdo con la infraestructura real de Gigaredes Comunicaciones SAS.

Registro de un Nuevo Dispositivo en PRTG

Para iniciar el monitoreo, es necesario registrar cada equipo dentro del árbol de dispositivos de PRTG. Este procedimiento permite integrar los elementos de red al sistema de supervisión y habilitar la posterior creación de sensores.

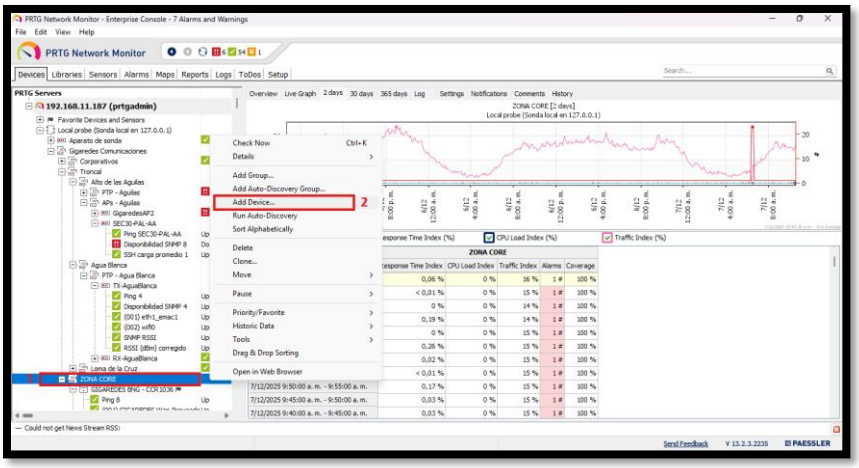
Inicialmente, se accede a la opción de agregar dispositivo dentro del grupo correspondiente (Core, GPON o Wireless), como se muestra en la Figura 8.

Posteriormente, se configuran los datos básicos del equipo, tales como nombre e dirección IP o DNS del dispositivo, según se observa en la Figura 9.

Finalmente, se definen las credenciales y parámetros SNMP necesarios para la comunicación con el equipo, tal como se presenta en la Figura 10. Una vez guardada la configuración, el dispositivo queda disponible para la creación de sensores y su monitoreo continuo.

Figura 8

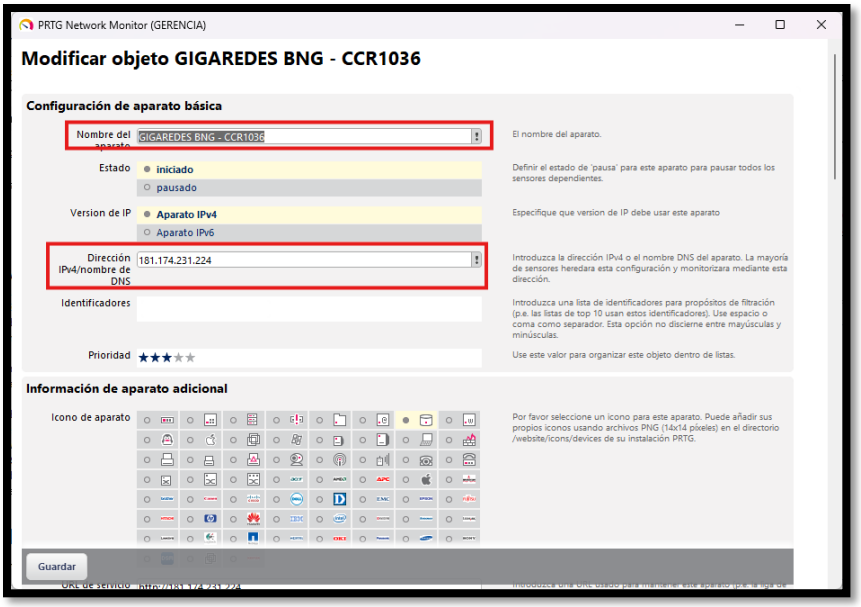
Registro de un nuevo dispositivo en PRTG Network Monitor



Nota. Interfaz de PRTG Network Monitor que muestra la opción para agregar un nuevo dispositivo dentro del árbol de monitoreo, paso inicial para la creación de sensores y supervisión.

Figura 9

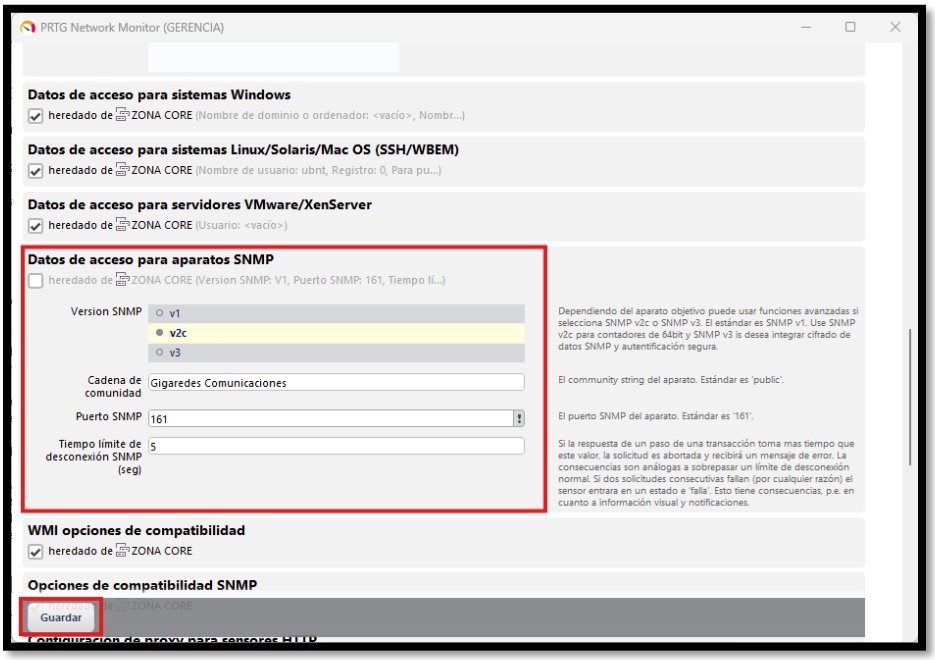
Configuración del nombre y dirección IP del dispositivo en PRTG.



Nota. Ventana de configuración básica donde se define la identificación del equipo y su dirección IP o nombre DNS, información necesaria para su reconocimiento dentro del sistema de monitoreo.

Figura 10

Configuración de parámetros SNMP del dispositivo.



Nota. Sección de configuración en la que se establecen la versión SNMP, comunidad y puerto de comunicación, parámetros esenciales para la recolección de información del equipo monitoreado.

Creación de sensores básicos

Una vez registrado el dispositivo en PRTG, es posible añadir sensores SNMP estándar que permiten supervisar el estado operativo de los equipos de red. Estos sensores recopilan métricas como uso de CPU, memoria, tráfico de interfaces y tiempo de actividad.

El proceso inicia seleccionando el dispositivo y accediendo a la opción de agregar sensor, como se observa en la Figura 11.

Posteriormente, se eligen los tipos de sensores requeridos, entre ellos memoria y tráfico de red, según se presenta en la Figura 12.

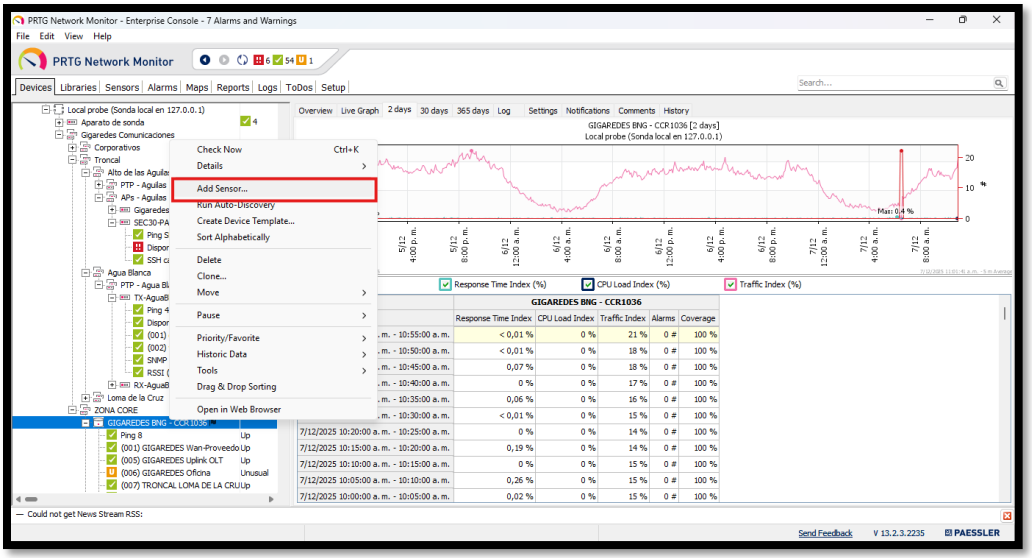
La configuración específica de cada sensor, incluyendo la selección de parámetros de memoria monitoreada, se muestra en la Figura 13.

Una vez creados los sensores, PRTG genera paneles de visualización que permiten analizar el comportamiento histórico de las métricas. Un ejemplo de visualización del sensor de memoria se presenta en la Figura 14, mientras que la supervisión del tráfico de una interfaz WAN se evidencia en la Figura 15.

Estos sensores constituyen la base del monitoreo operativo continuo, permitiendo detectar variaciones de desempeño y anticipar posibles eventos de saturación o degradación del servicio.

Figura 11

Selección de la opción para añadir sensores a un dispositivo en PRTG.



Nota. Interfaz de PRTG Network Monitor donde se muestra el acceso a la opción Add Sensor, paso inicial para incorporar sensores de monitoreo al dispositivo seleccionado.

Ejemplo Práctico: Monitoreo del Router Mikrotik CCR1036 (Core)

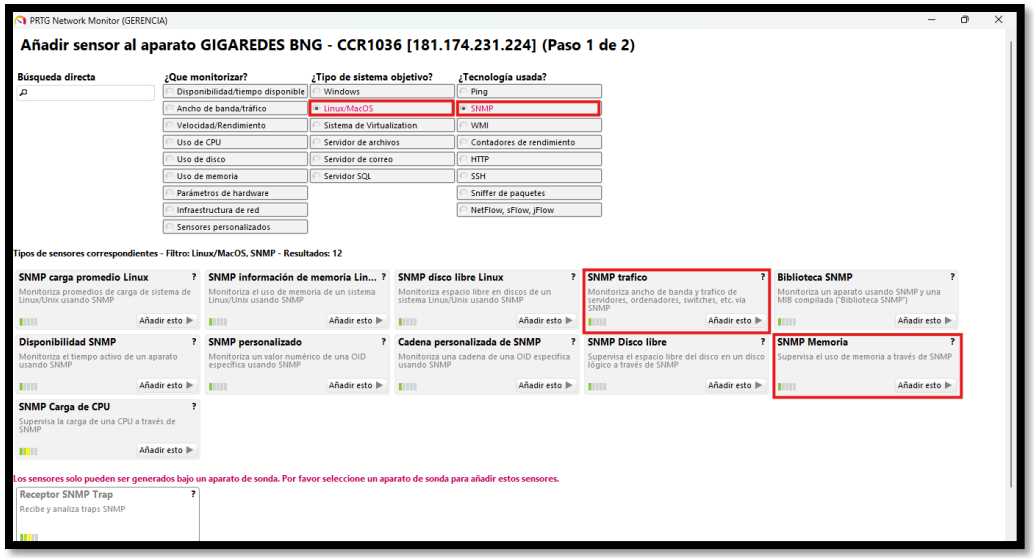
El router Mikrotik CCR1036 constituye un elemento crítico dentro de la infraestructura de Gigaredes Comunicaciones SAS, debido a su función en el enrutamiento y distribución del tráfico principal de la red. Por esta razón, su supervisión resulta prioritaria dentro del sistema de monitoreo propuesto.

Para su seguimiento se emplean sensores SNMP orientados a evaluar el uso de CPU, memoria, tráfico por interfaz y tiempo de actividad (uptime), métricas que permiten identificar sobrecargas, degradaciones de desempeño o eventos anómalos en la operación del equipo.

Este esquema de monitoreo posibilita contar con información continua sobre el estado del nodo central de la red y facilita la detección temprana de incidentes que puedan afectar la prestación del servicio.

Figura 12

Selección de sensores SNMP de memoria y tráfico.



Nota. Pantalla de búsqueda de sensores en la que se identifican sensores SNMP de memoria y tráfico disponibles para su incorporación al monitoreo del equipo.

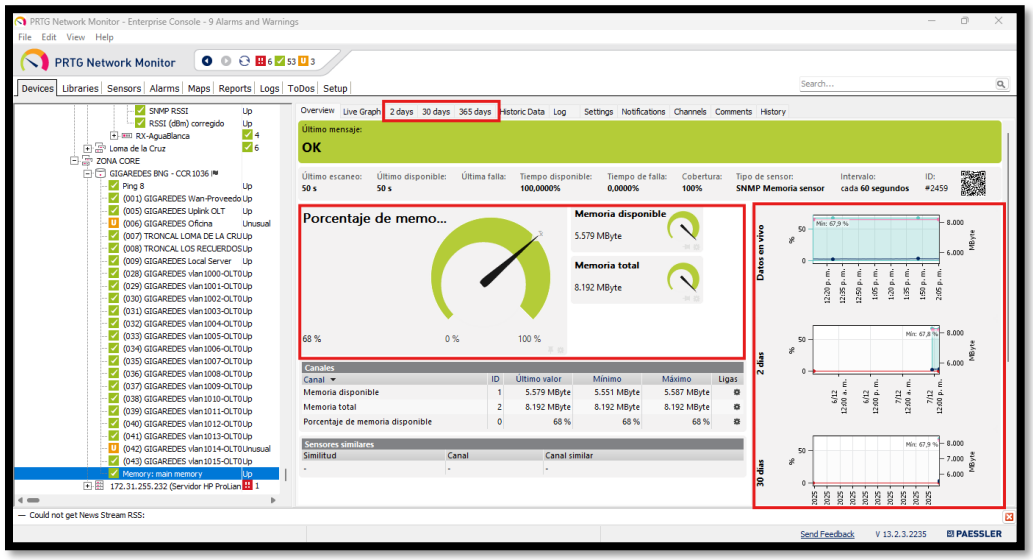
Figura 13

Configuración del sensor de memoria del dispositivo.

Nota. Ventana de configuración donde se define el tipo de memoria a supervisar y los parámetros básicos del sensor, necesarios para la recolección de métricas del equipo.

Figura 14

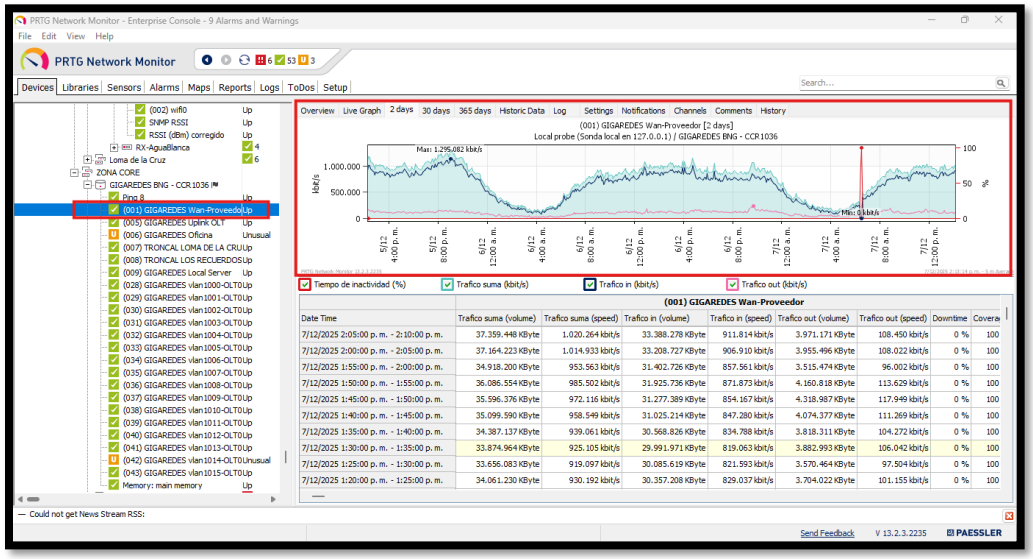
Visualización del sensor de memoria en PRTG.



Nota. Panel de monitoreo que presenta el porcentaje de memoria utilizada y su comportamiento histórico, permitiendo evaluar la carga del equipo en el tiempo.

Figura 15

Visualización del sensor de tráfico de una interfaz WAN.



Nota. Gráfica de tráfico entrante y saliente obtenida mediante sensor SNMP, utilizada para analizar el uso de ancho de banda y detectar variaciones de consumo.

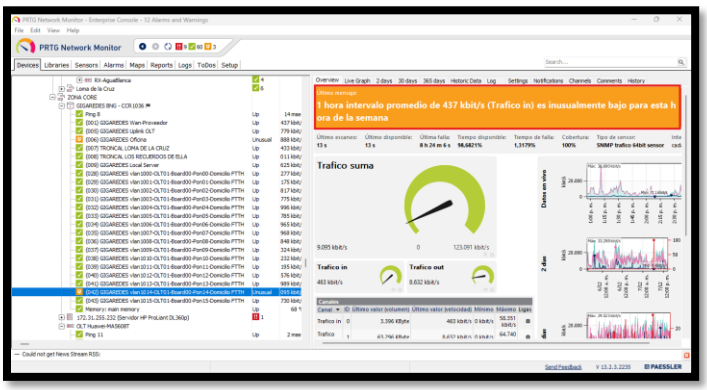
Monitoreo de Tráfico de VLAN desde el Servidor Mikrotik

El servidor Mikrotik actúa como punto central para la supervisión del tráfico asociado a las VLAN utilizadas en la red GPON. En este esquema, PRTG obtiene la información desde las interfaces y subinterfaces configuradas en el Mikrotik, sin consultar directamente la OLT. Este enfoque permite analizar el comportamiento del tráfico por sector FTTH y detectar variaciones relevantes en la demanda.

El procedimiento consiste en seleccionar el dispositivo Mikrotik dentro del árbol de equipos, añadir sensores de tráfico SNMP y asociarlos a las interfaces o VLAN correspondientes. La asignación de nombres estandarizados facilita la identificación de cada sector monitoreado y su seguimiento operativo.

Figura 16

Visualización del sensor de tráfico asociado a una VLAN en el router CCR1036.



Nota. Panel de monitoreo de PRTG Network Monitor que muestra el comportamiento del tráfico entrante y saliente de una VLAN supervisada mediante sensores SNMP, permitiendo evaluar su variación en el tiempo.

Análisis de la Alerta Observada. Como se observa en la Figura 16, el sistema genera una alerta de tipo Unusual cuando detecta que el tráfico actual se encuentra significativamente por debajo del patrón histórico registrado para la misma franja horaria. Este mecanismo se basa en el análisis comparativo de datos históricos almacenados por la plataforma.

- Un comportamiento de tráfico inferior al esperado puede asociarse a diversos factores, entre ellos:
- Variaciones normales en la actividad de usuarios
- Desconexión parcial de clientes
- Fallas en el sector FTTH
- Problemas de energía en nodos intermedios
- Interrupciones de fibra óptica
- Limitaciones en enlaces troncales

Aunque la alerta no implica una caída total del servicio, sí representa una desviación relevante que requiere verificación operativa.

Implicaciones Operativas. Ante este tipo de eventos, el análisis cruzado con otras VLAN, el estado energético de nodos y los reportes de usuarios permite determinar si se trata de una variación normal o de un incidente técnico.

El uso de sensores SNMP en el Mikrotik, combinado con el análisis histórico de PRTG, fortalece la detección temprana de anomalías y contribuye a una gestión preventiva de la red. Esto mejora la capacidad de respuesta del proveedor y favorece la continuidad del servicio.

Monitoreo de Radioenlaces Ubiquiti / Mimosa / MikroTik

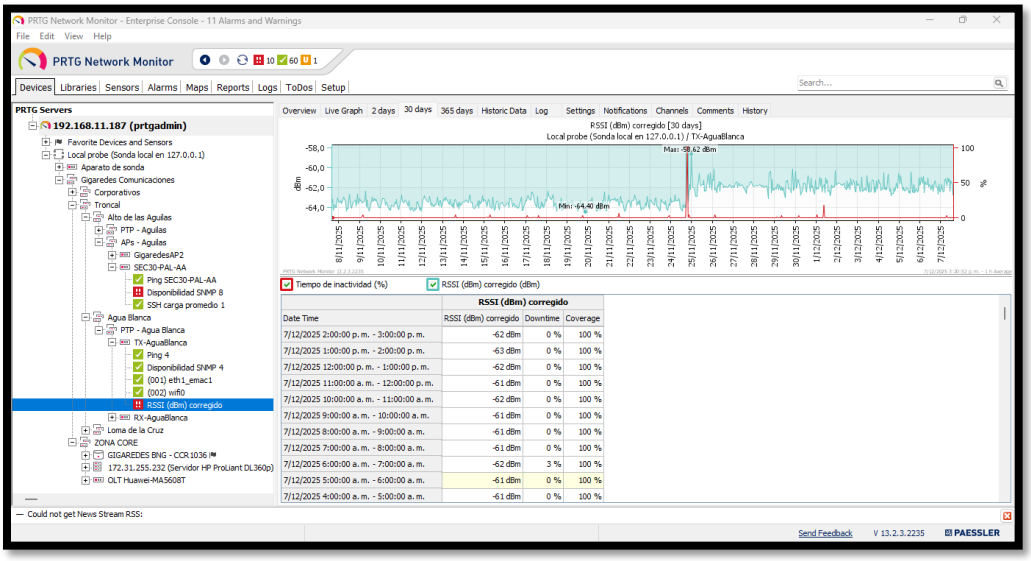
Los radioenlaces requieren supervisión continua de parámetros como intensidad de señal, relación señal-ruido y estabilidad del enlace. Para ello se emplean sensores SNMP que permiten

evaluar el desempeño inalámbrico y detectar variaciones que puedan afectar la calidad del servicio.

Entre los sensores más utilizados se encuentran RSSI, SNR, latencia, pérdida de paquetes y tráfico, los cuales proporcionan una visión integral del estado del enlace..

Figura 17

Visualización del sensor RSSI de un enlace punto a punto.



Nota. Interfaz de PRTG Network Monitor que muestra la variación histórica del RSSI (dBm) de un radioenlace supervisado mediante sensores SNMP.

Como se observa en la Figura 17, el sensor de RSSI corregido del enlace presenta inicialmente valores entre –63 dBm y –64 dBm, lo que indica un margen de señal reducido y mayor sensibilidad a interferencias.

Posteriormente se evidencia un cambio abrupto en la curva, asociado a un ajuste de frecuencia realizado por el área técnica. Tras esta modificación, el nivel de señal se estabiliza en rangos aproximados de –58 dBm a –60 dBm.

Una mejora de 4 a 6 dB representa un incremento significativo en la calidad del enlace, ya que implica mayor potencia recibida, menor impacto de interferencias y mejor estabilidad en la transmisión.

Este resultado confirma la efectividad del ajuste aplicado y demuestra la utilidad del monitoreo continuo para evaluar decisiones técnicas y optimizar el desempeño de los enlaces inalámbricos.

Supervisión Energética Remota (UPS)

Las unidades de alimentación ininterrumpida (UPS) constituyen un elemento clave para garantizar la continuidad del servicio en nodos críticos de la red. Su monitoreo mediante SNMP permite supervisar parámetros como nivel de carga de batería, voltaje, tiempo de autonomía y estado operativo.

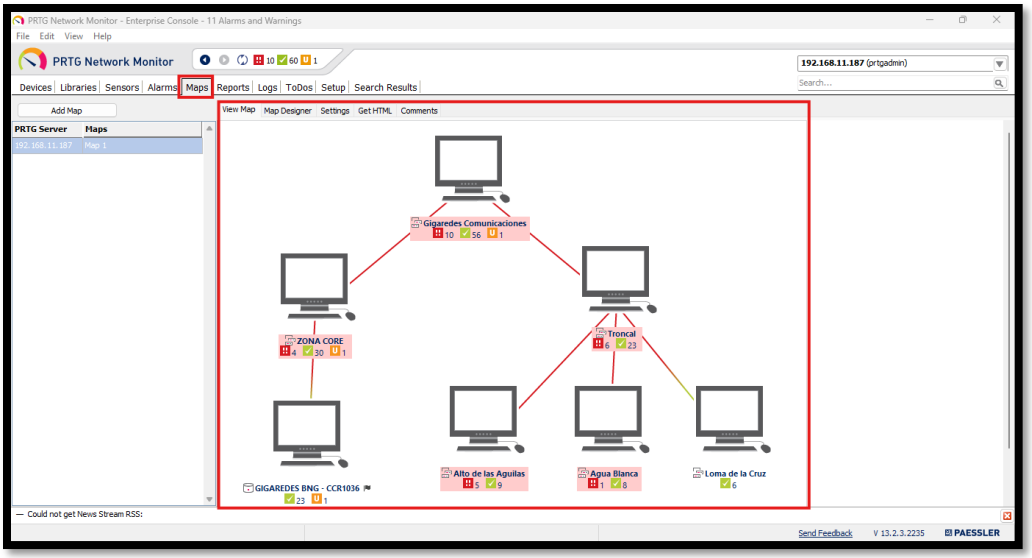
La integración de estos sensores dentro de PRTG facilita la detección temprana de fallas eléctricas y contribuye a la toma de decisiones preventivas en sitios de difícil acceso.

Creación de Dashboards Operativos (Maps)

Los dashboards operativos permiten consolidar en una sola vista el estado general de la red, integrando métricas críticas de tráfico, disponibilidad y energía. A través de la herramienta Maps de PRTG es posible organizar visualmente los dispositivos y sensores más relevantes para la operación.

Figura 18

Ejemplo de mapa de dispositivos en PRTG Network Monitor.



Nota. Mapa de supervisión que representa de forma gráfica el estado de dispositivos y sensores organizados por zonas de la red, facilitando la visualización centralizada de eventos y condiciones operativas.

Como se observa en la Figura 18, la representación gráfica de dispositivos permite identificar rápidamente el estado de cada segmento de la red y priorizar la atención sobre nodos críticos.

En conjunto, los ejemplos desarrollados en esta sección evidencian que el diseño del sistema de monitoreo propuesto es técnicamente viable y compatible con la infraestructura de Gigaredes Comunicaciones SAS. La incorporación de sensores, la visualización de métricas y el análisis de alertas demuestran que el sistema puede implementarse de forma progresiva, apoyando el cumplimiento de los objetivos del proyecto y fortaleciendo la gestión operativa de la red.

Estrategia de Supervisión Remota para Eventos Críticos

La supervisión remota de la infraestructura híbrida de Gigaredes Comunicaciones SAS constituye un componente esencial para garantizar la continuidad operativa de sus servicios,

especialmente en nodos ubicados en cerros o zonas de difícil acceso donde las fallas energéticas y las condiciones climáticas adversas afectan con mayor frecuencia la disponibilidad del sistema. Con base en el diseño técnico propuesto y en las necesidades operativas identificadas durante el análisis de la infraestructura actual, se establece la siguiente estrategia de supervisión remota, orientada a priorizar eventos críticos, facilitar la toma de decisiones y asegurar la escalabilidad futura del sistema.

Priorización Operativa de los Nodos Supervisados

El monitoreo debe estructurarse bajo un esquema jerárquico de criticidad, permitiendo asignar distintos niveles de prioridad a los dispositivos según su impacto en la continuidad del servicio:

Prioridad 1 – Zona de Core. Incluye el router Mikrotik CCR1036, el servidor Proxmox y la OLT Huawei MA5608T. Cualquier alerta crítica en esta zona compromete la totalidad del servicio, por lo que debe atenderse de manera inmediata.

Prioridad 2 – Zona Inalámbrica (AP y PTP). Nodos ubicados en torres remotas donde las fallas energéticas y la degradación del enlace afectan barrios o veredas completas. Requieren vigilancia constante y respuesta rápida.

Prioridad 3 – Zona de Distribución GPON. Supervisión de puertos PON y VLAN para detectar caídas masivas o congestión, permitiendo intervenciones planificadas sin necesidad de desplazamiento físico.

Procedimiento de Detección y Atención Remota de Eventos Críticos

La estrategia de supervisión remota se basa en la interacción entre sensores SNMP, reglas de alerta y tableros visuales configurados en PRTG. El procedimiento sugerido es el siguiente:

Detección Automática. Los sensores de energía, latencia, tráfico y calidad de enlace identifican variaciones fuera de los umbrales establecidos.

Clasificación. PRTG asigna la alerta a categoría informativa, advertencia o crítica según el impacto estimado.

Notificación Inmediata. Alertas críticas → notificación directa vía Telegram o correo al personal técnico.

- Advertencias → revisión en dashboard central.
- Informativas → registro histórico.

Diagnóstico Remoto. El técnico verifica:

- Estado del enlace principal y secundario.
- Carga y voltaje reportado por UPS.
- Calidad de señal RSSI/SNR.
- Tráfico en interfaces críticas.

Decisión Operativa.

- Si la falla puede resolverse mediante acciones remotas, se ejecuta desde la central.
- Si la falla requiere intervención física, se prioriza el desplazamiento según el impacto detectado.

Estrategia de Notificación y Comunicación Remota

Para garantizar la atención eficaz, se sugiere configurar un sistema de notificaciones escalonado:

- Canal 1: Telegram técnico para alertas críticas.
- Canal 2: Correo electrónico administrativo para advertencias prolongadas.
- Canal 3: Dashboard en PRTG para supervisión continua.

Escalabilidad Futura de la Estrategia

El diseño contempla la posibilidad de expansión sin rediseño profundo:

- Integración de monitoreo ambiental.
- Supervisión energética avanzada.
- Automatización de tareas.
- Incremento gradual de sensores.
- Centralización multi-sede mediante sondas remotas.

Esta estrategia fortalece el cumplimiento del tercer objetivo específico del proyecto y articula los elementos técnicos del diseño para permitir una gestión remota, eficiente y proactiva de la infraestructura de Gigaredes Comunicaciones SAS.

Conclusiones

A partir del análisis de la infraestructura de red de Gigaredes Comunicaciones SAS, se identificaron los principales componentes del Core, la distribución GPON y la zona inalámbrica, así como los nodos críticos que requieren supervisión continua. Este análisis permitió reconocer las condiciones operativas actuales y las necesidades de monitoreo, cumpliendo con el primer objetivo específico del proyecto.

El diseño de la arquitectura lógica del sistema de monitoreo basado en PRTG Network Monitor permitió definir de manera estructurada los sensores, métricas y umbrales necesarios para la supervisión de dispositivos y enlaces estratégicos. La segmentación por zonas y la selección de sensores adecuados evidencian que el sistema propuesto es coherente con la infraestructura existente y responde al segundo objetivo específico planteado.

La propuesta de una estrategia de supervisión remota para eventos críticos, con énfasis en fallas energéticas y nodos ubicados en zonas de difícil acceso, establece un esquema de priorización operativa y notificación que fortalece la capacidad de respuesta ante incidentes. Esta estrategia cumple con el tercer objetivo específico, al considerar criterios de criticidad y escalabilidad futura.

Desde el punto de vista de la infraestructura, el diseño del sistema de monitoreo mediante PRTG Network Monitor se adapta a la topología y a las tecnologías utilizadas por Gigaredes Comunicaciones SAS, integrando de forma centralizada la supervisión del Core, la red GPON y los radioenlaces. Esto demuestra que la herramienta seleccionada es adecuada para soportar un sistema de gestión de red orientado a la detección temprana de fallas y al control operativo del servicio.

En conjunto, el proyecto cumple con el objetivo general al diseñar un sistema de monitoreo técnicamente viable, documentado y alineado con las necesidades reales de la red,

garantizando una base sólida para la gestión y supervisión de la infraestructura, sin requerir implementación inmediata.

Recomendaciones

Se recomienda implementar de manera progresiva el sistema de monitoreo diseñado, iniciando por los nodos críticos del Core y los enlaces principales de distribución, con el fin de validar en operación real los sensores y umbrales definidos durante el análisis de la infraestructura.

Se sugiere complementar el diseño propuesto con pruebas piloto en zonas representativas de la red GPON y de la infraestructura inalámbrica, lo que permitiría ajustar los umbrales de alerta y optimizar la configuración de sensores según el comportamiento real del tráfico y la calidad de los enlaces.

Es recomendable integrar el sistema de monitoreo con mecanismos formales de notificación y gestión de incidentes, como alertas automáticas y procedimientos documentados de atención, fortaleciendo la estrategia de supervisión remota planteada en el proyecto.

Para futuras fases, se aconseja ampliar el sistema de monitoreo incorporando métricas adicionales relacionadas con la experiencia del usuario y el desempeño de servicios, lo que contribuiría a una gestión más integral de la red.

Finalmente, se recomienda mantener actualizada la documentación del sistema de monitoreo y los diagramas asociados, de manera que el diseño propuesto pueda adaptarse a cambios en la infraestructura y servir como referencia para la toma de decisiones técnicas y operativas.

Referencias

Paessler AG. (n.d.). *PRTG Network Monitor Manual*. Recuperado de https://www.paessler.com/manuals/prtg

Ubiquiti Networks. (n.d.). *Guía de instalación y configuración de equipos Ubiquiti*. Recuperado de https://www.ui.com/download

MikroTik. (n.d.). *The Dude Manual*. Recuperado de https://mikrotik.com/thedude

Johnson, M. (2019). *Implementación de sistemas de monitoreo en telecomunicaciones rurales*. Journal of Network Operations, 12(3), 55–68.

Smith, J., López, A., & Rodríguez, D. (2020). *Casos de éxito en el monitoreo proactivo de redes híbridas*. Revista Latinoamericana de Telecomunicaciones, 8(2), 23–35.

Redes Antioqueñas de Comunicaciones. (2021). *Informe técnico: Monitoreo en entornos rurales con PRTG*. Semana TIC Antioquia. Medellín, Colombia.

Rae

El presente proyecto tuvo como propósito diseñar un sistema de monitoreo de red basado en la plataforma PRTG Network Monitor para la empresa Gigaredes Comunicaciones SAS, con el fin de mejorar la supervisión de su infraestructura de telecomunicaciones y fortalecer los procesos de gestión operativa del servicio. La red analizada integra tecnologías GPON y enlaces inalámbricos, desplegadas en zonas urbanas y rurales, lo que genera retos asociados a la disponibilidad, el control del tráfico y la detección oportuna de fallas.

Como metodología, se realizó inicialmente un análisis de la infraestructura actual, identificando los principales componentes del Core, la red de distribución GPON y la zona inalámbrica, así como los nodos críticos que requieren monitoreo permanente. Posteriormente, se diseñó la arquitectura lógica del sistema de monitoreo, definiendo sensores, métricas y umbrales de alerta adecuados para cada tipo de dispositivo y tecnología. Asimismo, se propuso una estrategia de supervisión remota orientada a la atención de eventos críticos, especialmente fallas energéticas y degradaciones en enlaces ubicados en zonas de difícil acceso.

El proyecto no contempló la implementación del sistema, por lo que la validación se realizó de manera documental, mediante diagramas conceptuales, tablas de sensores, ejemplos de dashboards y guías ilustrativas que evidencian la viabilidad técnica del diseño propuesto. Los resultados permiten concluir que la plataforma PRTG Network Monitor se ajusta a las necesidades de la infraestructura de Gigaredes Comunicaciones SAS y constituye una herramienta adecuada para soportar un sistema de gestión de red orientado a la detección temprana de fallas, la priorización operativa y la toma de decisiones.

Finalmente, el diseño desarrollado proporciona una base sólida para una futura implementación progresiva del sistema de monitoreo, contribuyendo a mejorar la continuidad del servicio y la gestión integral de la red.