IMPLEMENTACIÓN DE UN SISTEMA ACS USANDO CWMP EN UNA RED FTTH/GPON PARA LA EMPRESA TELCOFIBER S.A.S.

Trabajo de Grado
Modalidad: Práctica Profesional

ANDRÉS FELIPE BUITRÓN MUÑOZ
Código: 100614021018

Asesor: Ing. Andrés Osiris López Martínez
Director: Ing. Alejandro Toledo Tovar. MSc

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo I+D Nuevas Tecnologías en Telecomunicaciones (GNTT)
Popayán - Cauca
2023

IMPLEMENTACIÓN DE UN SISTEMA ACS USANDO CWMP EN UNA RED FTTH/GPON PARA LA EMPRESA TELCOFIBER S.A.S.

Trabajo de Grado
Modalidad: Práctica Profesional

ANDRÉS FELIPE BUITRÓN MUÑOZ
Código: 100614021018

Asesor: Ing. Andrés Osiris López Martínez
Director: Ing. Alejandro Toledo Tovar. MSc

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo I+D Nuevas Tecnologías en Telecomunicaciones (GNTT)
Popayán - Cauca

2023

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ACRÓNIMOS

AAA	*Authentication, Authorization and Accounting,* Autenticación, Autorización y Contabilidad
ACS	*Auto Configuration Server,* Servidor de Configuración Automática
BRAS	*Broandband Remote Access Server*, Acceso Remoto de Banda Ancha
CRC	Comisión de Regulación de Comunicaciones
CPE	*Customer Premises Equipment*, Equipo Local del Cliente
CPU	*Central Processing Unit*, Unidad Central de Proceso
CWMP	*CPE WAN Management Protocol*, Protocolo de Gestión de WAN de CPE
DHCP	*Dynamic Host Configuration Protocol,* Protocolo Dinámico de Configuración de Host
DNS	*Domain Name System*, Sistema de Nombres de Dominio
EAP	*Protected Extensible Authentication Protocol*, Protocolo de Autenticación Extensible Protegido
EDR	*Equal Dispersion Ranging,* Sistema de Medición de Dispersión Igual
EPON	*Ethernet Passive Optical Network*, Red Óptica Pasiva de Ethernet
FAT	*Fiber Access Terminal*, Terminal de Acceso a la Fibra
FC-F	*Ferrule Connector***,** Conector de Ferrule
FDT	*Fiber Distribution Terminal*, Terminales de Distribución de Fibra
FP-LD	*Fabry-Perot Laser Diode,* Diodo Láser Fabry-Perot
FTTB	*Fiber To The Business*, Fibra Óptica Hasta el Negocio
FTTC	*Fiber To The Curb*, Fibra Óptica Hasta la Acera
FTTH	*Fiber To The Home,* Fibra Hasta el Hogar
FTTN	*Fiber To The Node*, Fibra Óptica Hasta el Nodo
GEM	*GPON Encapsulation Method*, Método de Encapsulación GPON
GPON	*Gigabit-Capable Passive Optical Network*, Red Óptica Pasiva con Capacidad de Gigabit

HTTP	*Hipertext Transfer Protocol,* Protocolo de Transferencia de Hipertexto
IP	*Internet Protocol*, Protocolo de Internet
ISP	*Internet Service Provider*, Proveedor de Servicios de Internet
LC	*Connector Lucent,* Conector Lucent
ODF	*Optical Distribution Frame*, Distribuidor de Fibra Óptica
OLT	*Optical Line Terminal,* Terminal de Línea Óptica
ONT	*Optical Network Terminal,* Terminal de Red Óptica
OSP	*Outside Plant*, Planta Externa
OTDR	*Optical Time Domain Reflectometer*, Reflectómetro Óptico en el Dominio del Tiempo
P2P	*Point to Point*, De Igual a Igual
PLOAM	*Physical Layer Operations, Administration,* Protocolo de Operación y Mantenimiento de la Capa Física
PON	*Passive Optical Network,* Red Óptica Pasiva
PPPoE	*Point To Point Protocol Over Ethernet*, Protocolo Punto a Punto Sobre Ethernet
PSTN	Public Switched Telephone Network, Red Telefónica Pública Conmutada
QoS	*Quality of Service,* Calidad del Servicio
RADIUS	*Remote Access Dial In User Service,* Servicio de Usuario de Acceso Telefónico de Autenticación Remota
SOAP	*Simple Object Access Protocol,* Protocolo Simple de Acceso a Objetos
SSL	*Secure Sockets Layer*, Seguridad de la Capa de Transporte
TDM	*Time Division Multiplexing*, Multiplexación por División de Tiempo
TDMA	*Time Division Multiple Access*, Acceso Múltiple por División de Tiempo
TIC	Tecnologías de la Información y las Comunicaciones
TR-069	*Technical Report 069,* Reporte Técnico 069
TR-098	*Technical Report 098,* Reporte Técnico 098

VLAN *Virtual Local Area Network,* Red de Área Local Virtual

VPN *Virtual Private Network*, Red Privada Virtual

WAN *Wide Area Network,* Red de Área Amplia

WDM *Wavelength Division Multiplexing,* Multiplexación por División de Longitud de Onda

WPAD *WEB Proxy Autodiscovery Protocol),* Protocolo de Autodescubrimiento de Proxy WEB

1 CAPÍTULO: INTRODUCCIÓN.

Es fundamental comprender el funcionamiento general de TELCOFIBER S.A.S. y sus actividades comerciales, con el fin de conocer su convicción, objetivos y proyecciones, los cuales se encuentran representados en su misión y visión. TELCOFIBER S.A.S. es una empresa dedicada al sector de las telecomunicaciones y la tecnología, la cual busca ofrecer servicios de alta calidad a sus clientes a través de la implementación de soluciones innovadoras y una constante actualización tecnológica.

1.1 TELCOFIBER S.A.S

Figura 1.1 Logotipo de TELCOFIBER S.A.S. [1]

Esta Empresa dedicada a brindar soluciones integrales en ingeniería de TICS, legalmente constituida como una sociedad por acciones simplificada con registro mercantil No 46270 del 27 de agosto del 2019 y número de identificación tributaria NIT 901316179-5 y por medio del cual el Ministerio de Tecnologías de la información y las Comunicaciones MINTIC le otorgó el registro único de TIC No 96004915 del 18 de septiembre de 2019 [1].

TELCOFIBER S.A.S. se dedica principalmente a proveer servicios de Internet (ISP-Internet Service Provider) en los municipios de Santander de Quilichao, Santa Rosa y Almaguer en el Departamento del Cauca. La empresa ofrece sus servicios a través de canales de Internet dedicados o corporativos y canales de banda ancha, utilizando su red de arquitectura Fibra Hasta el Hogar (FTTH-*Fiber To The Home*) con tecnología de Red Óptica Pasiva con Capacidad de Gigabit (GPON- Gigabit-*Capable Passive Optical Network*).

La excelencia en el servicio y la rápida respuesta ante las adversidades son características distintivas de TELCOFIBER S.A.S., lo que ha impulsado la necesidad constante de ampliar su red. Para ello, la empresa cuenta con una planta técnica especializada en tecnología GPON, encargada de la ampliación, mantenimiento preventivo y correctivo de la red. Además, el personal técnico está capacitado para brindar soporte técnico a los usuarios y realizar instalaciones adecuadas en todos los parámetros estéticos y métricos de potencia, con el fin de ofrecer el mejor servicio a los nuevos usuarios.

Gracias a su enfoque en la calidad del servicio, la ampliación constante de su red y la atención oportuna a sus clientes, TELCOFIBER S.A.S. se ha consolidado como un fuerte competidor en el mercado de las telecomunicaciones y la tecnología en la región.

1.1.1 MISIÓN.

"Suministrar soluciones tecnológicas a todos a todos los sectores como una empresa líder en el Departamento de Cauca, impulsando el desarrollo de nuestros colaboradores orientada a generar valor a la sociedad, clientes, comprometidos con el desarrollo continuo de la región" [1].

1.1.2 VISIÓN.

"En el año 2023 ser la mejor empresa que proporcione servicios de telecomunicaciones a través de redes tecnológicamente actualizadas y modernas a través de fibra óptica hasta el hogar, cumpliendo la normatividad vigente e impulsando el crecimiento económico productivo de la región, logrando que todos los habitantes de la ciudad de Santander de Quilichao, accedan a Internet por fibra óptica bajo premisas de calidad y tarifas equitativas" [1].

1.2 PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la demanda por el servicio de Internet está en constante aumento, lo que se traduce en una mayor cobertura de redes por parte de los ISP y una amplia oferta de servicios de conexión para hogares. Por esta razón, resulta fundamental que los ISP brinden un servicio de calidad para posicionarse en el mercado y abarcar el mayor porcentaje posible de nuevos hogares conectados.

No obstante, es aún más importante que la Calidad del Servicio (QoS-*Quality of Service*) no se vea comprometida por el incremento en el número de usuarios. Mantener la excelencia en el servicio es fundamental para la permanencia del cliente, por lo que los ISP deben asegurarse de ofrecer una experiencia de conexión satisfactoria que no se vea afectada por la cantidad de usuarios conectados simultáneamente.

Es por ello que los ISP deben implementar políticas y herramientas que permitan gestionar de manera efectiva el ancho de banda, la latencia y otros aspectos técnicos que influyen en la calidad del servicio. Solo así podrán mantenerse como líderes en el mercado y garantizar la satisfacción de sus clientes.

En este contexto, es fundamental destacar la importancia de los protocolos de gestión para los Equipos Locales del Cliente (CPE-*Customer Premises Equipment*) en las Redes de Área Amplia (WAN-*Wide Area Network*). Estos protocolos, que se utilizan a través de servidores de autoconfiguración, permiten realizar configuraciones, aprovisionamiento, monitoreo y actualización de firmware de manera remota.

El uso de estos protocolos resulta especialmente relevante porque permite adelantarse a posibles daños al conocer el estado en el que se encuentra un CPE. Además, también contribuye a reducir la interferencia con la configuración de optimización de red de los dispositivos de los usuarios, como la configuración del mejor canal Wi-Fi [2].

La empresa TELCOFIBER S.A.S., con sede principal en Santander de Quilichao, actualmente carece de un Servidor de Configuración Automática (ACS-*Auto Configuration Server*), lo que implica que no hay implementación de protocolos o estándares para la configuración, actualización o aprovisionamiento de los CPE en su red FTTH/GPON. En consecuencia, todas las fallas relacionadas con los CPE se atienden de manera personalizada por los técnicos a medida que el cliente las reporta, y debido a que no se dispone de información previa acerca de las posibles fallas, los técnicos deben seguir un protocolo de soporte técnico que comienza verificando si el CPE enciende y si existe un enlace físico por fibra óptica a la red de acceso FTTH.

Una vez finalizado este proceso, se verifica la Red de Área Local Virtual (VLAN-*Virtual Local Area Network*) en la interfaz de configuraciones del CPE, a la que se accede a través de un equipo conectado a la red e ingresando a la dirección de Protocolo de Internet (IP-*Internet Protocol*) de la puerta de enlace. Aquí se corroboran los detalles del username y password, así como la dirección IP y la potencia del enlace óptico. En el peor de los casos, si no se logra solucionar la falla, se restablece el equipo a su configuración de fábrica y se solicita a través de llamada telefónica al ingeniero encargado que proporcione los datos necesarios para realizar el aprovisionamiento nuevamente. Si no se puede solucionar la falla, se debe instalar un nuevo equipo y aprovisionarlo nuevamente. Todo este proceso puede llevar un tiempo considerable, lo que resulta en retrasos para algunos clientes y genera un costo elevado por despliegue de recursos logísticos, así como una mala experiencia por parte de los usuarios.

Ante los inconvenientes descritos, resulta imprescindible contar con una herramienta que permita la gestión, administración y diagnóstico de los CPE. Dichas herramientas deben ser altamente seguras, flexibles y escalables, tal como se señala en [3]. La implementación del protocolo CWMP a través de un ACS puede reducir significativamente el tiempo de respuesta a problemas relacionados con los CPE, lo que se traduce en un ahorro sustancial al evitar desplegar recursos logísticos por la disminución de solicitudes de visitas técnicas.

Dado el crecimiento constante de la empresa, es prácticamente obligatorio contar con una herramienta que permita la administración y gestión remota de los CPE de forma segura. Esta necesidad debe ser solventada lo antes posible para cumplir con requisitos constantes como el diagnóstico, optimización, actualizaciones y, sobre todo, Auto-Aprovisionamiento y Auto-Configuración. De esta manera, se logra que la ejecución de estas tareas pase prácticamente desapercibida para los usuarios, liberando así al servicio técnico de la empresa de tareas de gestión y reduciendo la cantidad de visitas por soporte técnico.

Este trabajo de grado en modalidad práctica profesional pretende solventar esta necesidad implementando un sistema ACS usando CWMP en una red FTTH/GPON para la empresa TELCOFIBER S.A.S. Este protocolo se implementa en la capa de abstracción y se basa en comunicación bidireccional usando Protocolo Simple de Acceso a Objetos (SOAP-*Simple Object Access Protocol*)/HTTP entre los CPE y el ACS, esto permite la configuración automática y remota, así como la gestión y actualización de firmware. Además, aparte del mantenimiento remoto brinda diagnósticos de los CPE gracias al monitoreo constante del estado y rendimiento de estos equipos.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Implementar un sistema ACS que permita el monitoreo, actualización y configuración de los equipos de usuario usando CWMP de una red FTTH/GPON para la empresa TELCOFIBER S.A.S.

1.3.2 OBJETIVOS ESPECÍFICOS

- Describir las características de la arquitectura física y lógica de la redFTTH/GPON, ubicada en Santander de Quilichao perteneciente a la empresaTELCOFIBER S.A.S.

- Diseñar un esquema para el funcionamiento conjunto de un ACS con CWMP que permita el acceso remoto para monitorizar, configurar y actualizar un grupo de CPE, de la red FTTH/GPON perteneciente a la empresa TELCOFIBER S.A.S.

- Desplegar el sistema ACS en la red FTTH/GPON ubicada en Santander de Quilichao perteneciente a la empresa TELCOFIBER S.A.S.

- Evaluar el sistema ACS desplegado, en las condiciones reales de funcionamiento.

1.4 APORTE

Este trabajo de grado hace su contribución en temas de especial interés a la facultad y al departamento de telecomunicaciones en los siguientes aspectos:

- Descripción detallada de las características de la arquitectura física y lógica de la red FTTH/GPON.

- Implementar un sistema ACS usando CWMP en la red FTTH/GPON.

Automatizar el proceso de aprovisionamiento de los CPE de los nuevos usuarios, así como reducir significativamente el tiempo de respuesta ante fallos haciendo uso de copias de seguridad de las configuraciones de los CPE para reestablecer los servicios inmediatamente se presenten las fallas.

1.5 METODOLOGÍA

El modelo en cascada es un modelo de proceso de desarrollo de software que se divide en etapas consecutivas, cada una se basa en los resultados de la etapa anterior. Este modelo es conocido como "en cascada" debido a que los resultados de cada etapa fluyen hacia la siguiente [4].

Las etapas típicas del modelo en cascada incluyen análisis de requisitos, diseño, implementación y pruebas. Cada etapa produce un producto que es utilizado como entrada

para la siguiente. Este enfoque es adecuado para proyectos de software con requisitos claros y bien definidos y un alcance limitado. Sin embargo, puede ser menos efectivo en proyectos con requisitos cambiantes o en entornos altamente inciertos.

En la Figura 1.2 se observa el diagrama con las cinco etapas definidas para el proyecto siguiendo el modelo en cascada, con la flecha se indica la secuencia de las etapas.

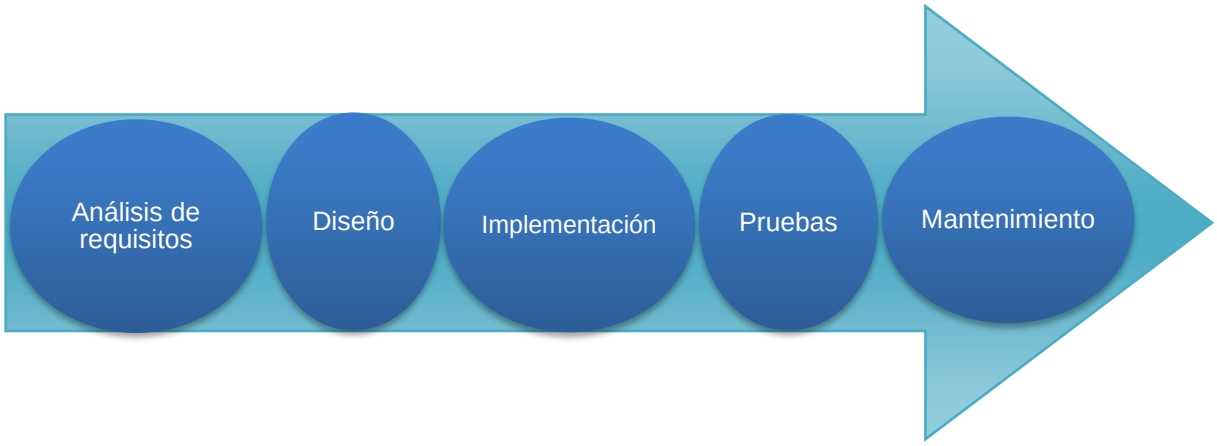

Figura 1.2 Diagrama Secuencial Metodología en Cascada

Cada etapa genera un producto que es utilizado como entrada para la siguiente. La etapa de pruebas es un punto crítico, ya que puede requerir la retroalimentación y la resolución de problemas en las etapas anteriores. El mantenimiento es una etapa continua que se lleva a cabo después de la entrega del software.

- Análisis de requisitos: en esta etapa se recopila información sobre las necesidades y expectativas del usuario para el software. Se identifican los requisitos funcionales y no funcionales y se establece un alcance claro para el proyecto.

- Diseño: en este punto se establece un plan para el desarrollo del software. Se definen la arquitectura del sistema, la estructura de datos y la interfaz de usuario.

- Implementación: en esta etapa se codifica el software y se crean las pruebas unitarias.

- Pruebas: en esta etapa se realizan pruebas para asegurarse de que el software cumpla con los requisitos y funcione correctamente. Se pueden realizar pruebas unitarias, de integración y de sistema.

- Mantenimiento: una vez que el software ha sido entregado y puesto en funcionamiento, se lleva a cabo el mantenimiento para corregir errores y mejorar el rendimiento.

Es importante destacar que el modelo en cascada puede variar en función de la organización y del proyecto que se esté trabajando, y que algunas etapas pueden ser combinadas o modificadas.

2 CAPÍTULO: MARCO TEÓRICO

En términos generales, una red de telecomunicaciones se puede definir como un conjunto de nodos y enlaces de un sistema cableado, radio, óptico u otro sistema electromagnético, incluyendo todos sus componentes físicos y lógicos necesarios para asegurar la conexión entre dos o más puntos (fijos o móviles, terrestres o espaciales) para fines de telecomunicaciones [5]. La creciente demanda por conexiones de alta velocidad y calidad ha llevado a que la mayoría de los ISP implementen redes de fibra óptica, ya que la capacidad de estos sistemas aumenta exponencialmente para soportar el incremento en la demanda por anchos de banda grandes, que se debe al aumento en el tráfico de datos generado por los servicios de Internet, como el Triple Play que se encuentra presente en la mayoría de los hogares, y los servicios en la nube que cada vez son más adoptados por las empresas.

Los proveedores de servicios de Internet ofrecen a los usuarios acceso a Internet y todos los servicios relacionados mediante diversas tecnologías de redes de acceso. Sin embargo, entre todas las tecnologías adoptadas para satisfacer las crecientes demandas de ancho de banda a corto, medio y largo plazo, destaca la red óptica pasiva con capacidad de gigabit, que utiliza la tecnología FTTH. En Colombia, el aumento del uso de fibra óptica por parte de los ISP en los últimos tres años ha sido significativo, tal como lo demuestran las estadísticas presentadas en el Data flash de Internet fijo de la Comisión de Regulación de Comunicaciones (CRC), como se puede ver en la Figura 2.1 [6].

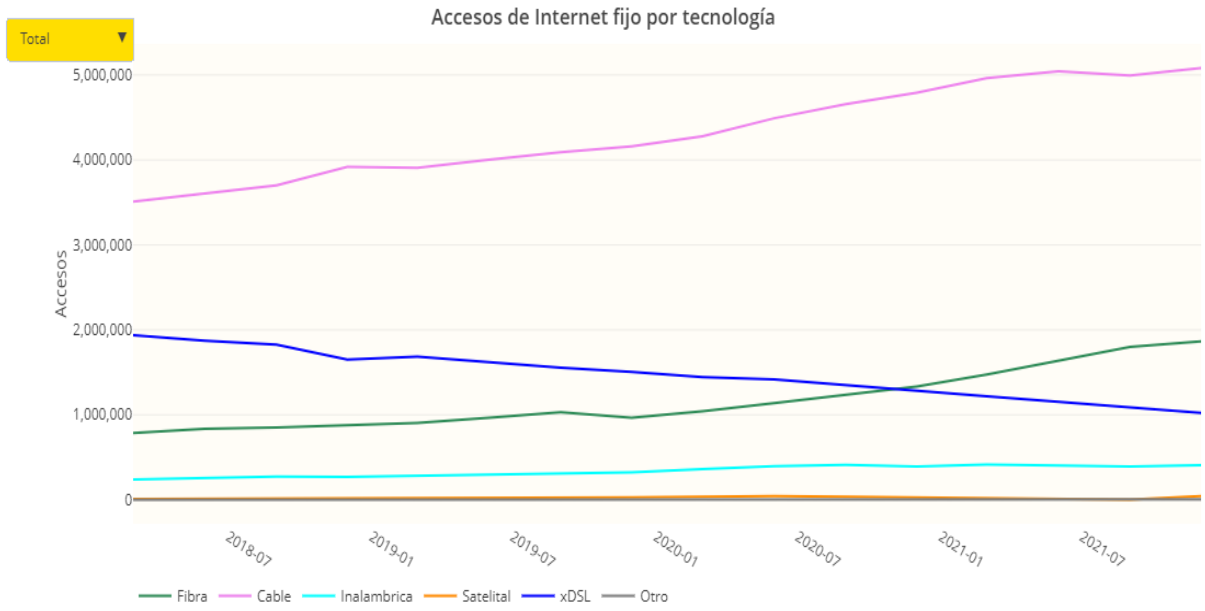

Figura 2.1 Acceso de Internet Fijo por Tecnología [6]

En la Figura 2.2 se puede observar que la velocidad del Internet que se alcanza con fibra óptica no tiene comparación con las demás tecnologías, esto se debe en gran medida a la implementación de GPON, ya que esta estructura permite tasas de bit asimétricas como una estructura de tramas que va desde los 662 Mbps hasta 2.5 Gbps [6].

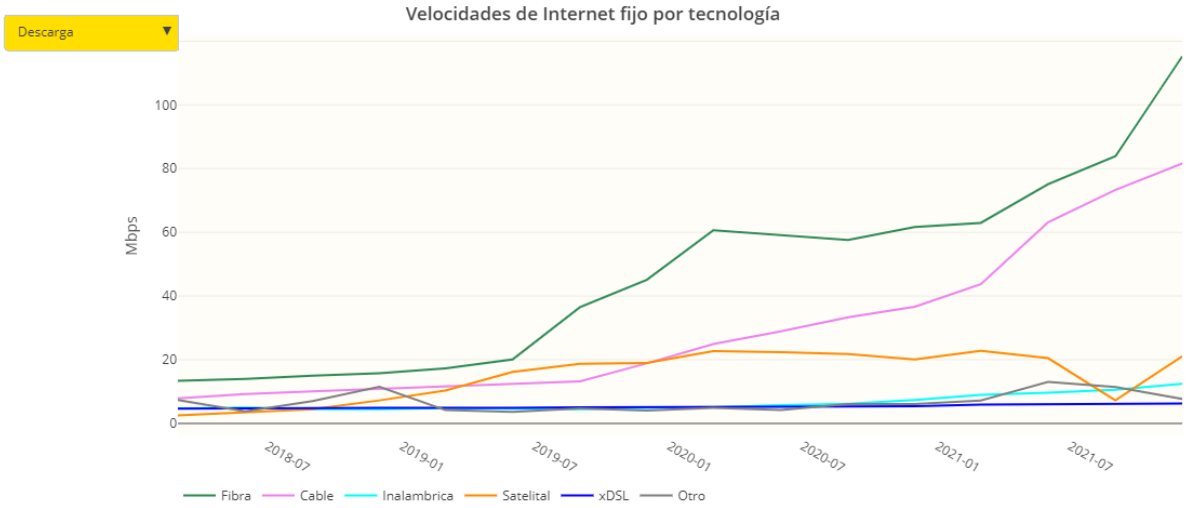

Figura 2.2 Velocidades de Internet Fijo por Tecnología [6]

2.1 REDES FTTH-GPON.

2.1.1 FTTH

La tecnología FTTH forma parte del conjunto de tecnologías FTTx, donde la "x" se refiere a la distancia que cubre la red óptica pasiva (PON-*Passive Optical Network*) utilizada para proporcionar conectividad de banda ancha hasta el extremo de la fibra que llega al usuario final. La figura 2.3 muestra un ejemplo de implementación de la tecnología FTTx [7].

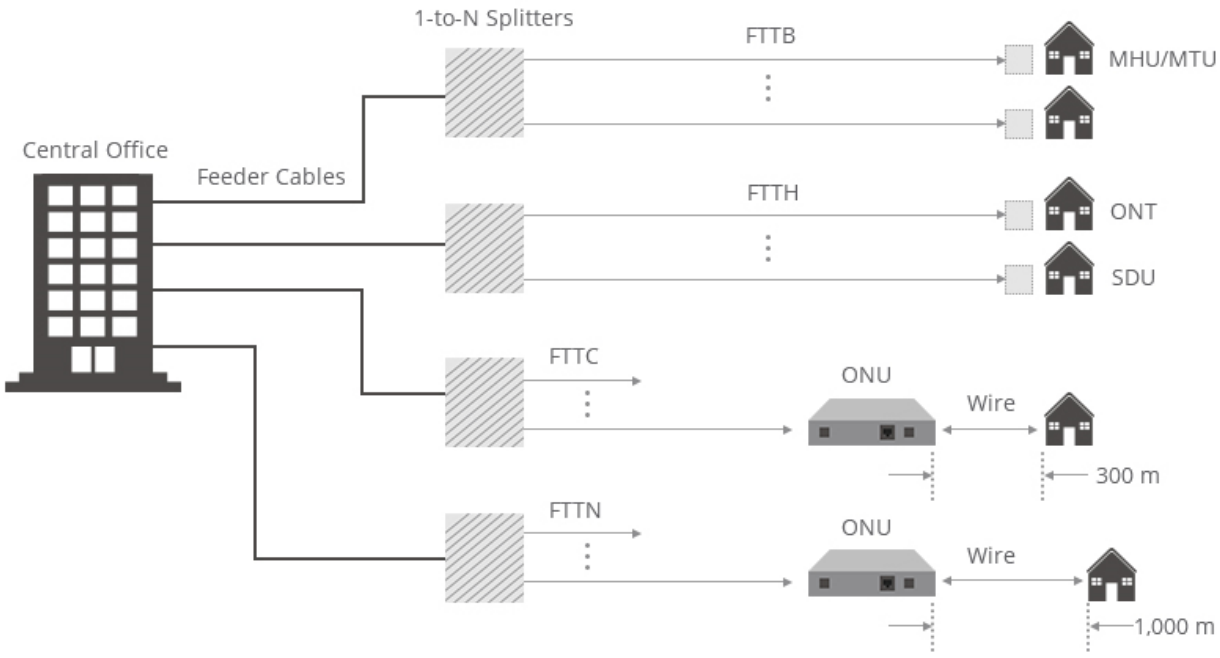

Figura 2.3 Implementación FTTX [7]

- **Fibra Hasta el Nodo (FTTN-*Fiber To The Node*):** hace referencia al tendido de fibra óptica desde un conmutador ubicado en una oficina central hasta un nodo intermedio, y a partir de ahí se usa cable ya sea par trenzado o coaxial para llegar hasta el usuario final en un rango de cobertura de 1000 metros.

- **Fibra Hasta la Acera (FTTC-*Fiber To The Curb*):** El despliegue de fibra se realiza desde la oficina central hasta un conmutador que se ubica aproximadamente a unos 300 metros de los usuarios finales.

- **Fibra Hasta el Hogar (FTTH-*Fiber To The Home*):** En este caso el despliegue de fibra que inicia desde el conmutador en la oficina central llega directamente hasta el hogar del usuario, en Fibra Hasta el Negocio (FTTB-*Fiber To The Business*) el despliegue de fibra es el mismo, la diferencia está en que la ubicación del usuario final es un establecimiento comercial que por lo general requiere un ancho de banda más grande.

2.1.2 Red de acceso FTTH.

La tecnología FTTH se implementa junto con la Red Óptica Pasiva (PON) para crear una arquitectura punto a multipunto, lo que permite que una sola fibra pueda conectar hasta 256 instalaciones mediante divisores ópticos que no necesitan alimentación adicional. La gran ventaja de FTTH es que proporciona un ancho de banda mucho mayor en comparación con otras tecnologías disponibles en el mercado, gracias a la baja atenuación de la fibra óptica. Por lo tanto, la fibra es un componente esencial de la red.

- **Elementos de la red de acceso FTTH.**

Existen 5 elementos fundamentales en la red de acceso FTTH y son la Terminal de Línea Óptica (OLT-*Optical Line Terminal*), splitter o divisores ópticos, fibra óptica, Terminal de Red Óptica (ONT-*Optical Network Terminal*) y por último los conectores que hacen parte del conjunto de planta externa.

- **OLT:** Este dispositivo es esencial dentro de la red de acceso FTTH, ya que permite conectar una troncal de fibra óptica y se ubica en la oficina central. Su función principal es controlar el tráfico de la red, administrar el buffer y asignar el ancho de banda a los usuarios. Además, cuenta con otras funciones importantes en la gestión de la red [8].

- **Splitter o divisor óptico:** Es un componente pasivo con una amplia gama de longitudes de onda, una pérdida de señal extremadamente baja y una alta fiabilidad. Su función principal es dividir la potencia de una señal óptica, lo que significa que la potencia de entrada se divide en un número determinado de fibras a la salida. Debido a sus características, el divisor óptico es un elemento esencial en la arquitectura de la PON utilizada en FTTH.

  Existen dos tipos de splitters: los balanceados y los desbalanceados. Los splitters balanceados tienen una relación de división dada por potencias de dos, lo que significa

que la potencia de salida es igual para todos los hilos, independientemente del número. La Tabla 2.1 muestra los valores de relación de división para los splitters balanceados. Por otro lado, los splitters desbalanceados sólo dividen la potencia de la señal en dos, pero de manera asimétrica. La Tabla 2.2 muestra que en los dos enlaces de salida de este tipo de splitter, la relación porcentual de potencia puede ser 60/40, 70/30 o 80/20 [9].

Es importante destacar que ambos tipos de splitter son elementos pasivos con un amplio rango de operación de longitud de onda, una pérdida de señal baja y alta fiabilidad.

Tabla 2.1 Splitter Balanceados

Relación de división	Pérdidas por inserción (dB)
1:2	3.5
1:4	7
1:8	10.25
1:16	13.48
1:32	17.5

Tabla 2.2 Splitter Desbalanceados

División porcentual	Pérdidas por inserción (dB)
1/99	0.30-21.6
2/98	0.4/18.7
5/95	0.5-14.6
10/90	0.7-11
15/85	1-7.9
20/80	1.4-7.9
25/75	1.7-6.95
30/70	1.9-6
35/65	2.3-5.35
40/60	2.7-4.7
45/65	3.15-4.15

Es importante tener en cuenta que los valores mostrados en las tablas anteriores son una referencia general y pueden variar ligeramente dependiendo del fabricante. La elección del tipo de splitter a utilizar dependerá de la topología de la red adoptada, ya que este dispositivo se encarga de la ramificación de la red PON de acuerdo con la aplicación que el ISP tenga prevista para su red. Por lo tanto, es esencial que se realice una evaluación cuidadosa de la topología de la red antes de elegir un splitter específico para asegurar el rendimiento óptimo de la red FTTH.

- **Fibra Óptica:** es el medio de transmisión de datos más importante en la actualidad. Consiste en un hilo flexible, ligero y transparente que permite que la luz se propague a través de él. Estas características son esenciales por dos razones: en primer lugar, cuando la luz viaja por el aire a largas distancias, sufre grandes pérdidas. En segundo

lugar, la fibra óptica permite guiar las ondas de luz a través de largas distancias con pérdidas despreciables. Todos los componentes que componen un cable de fibra óptica se muestran en la Figura 2.4.

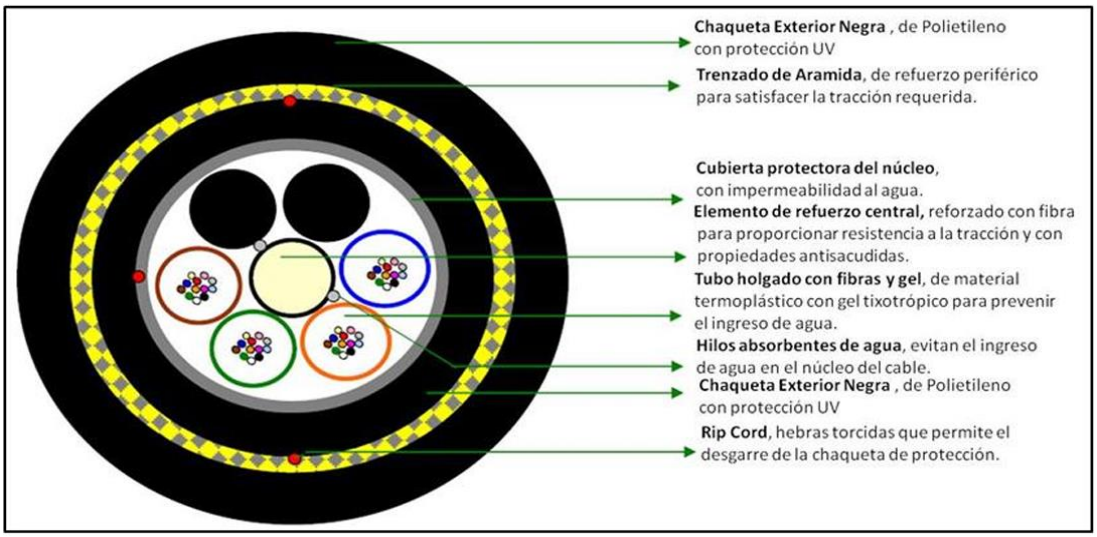

Figura 2.4 Características del cable de fibra óptica [10].

En el mercado se encuentran disponibles dos clases de fibra:

- **Fibra Óptica Monomodo:** es diseñada con un diámetro de núcleo entre 8 y 10 µm, además, cuenta con un revestimiento de 125 µm. Su costo de transmisión de datos es alto pero su capacidad de transmisión a distancias superiores a 100km es muy alta. Su atenuación depende de la longitud de onda utilizada, siendo de 0.40 dB/km para 1310nm, de 0.2-0.3 dB/km para 1490nm y de 0.2 db/km o menos para la longitud de onda de 1550. La introducción de tecnología como Multiplexación por División de Longitud de Onda en Paralelo (PWDM-*Parallel Wavelength Division Multiplexing*) han aumentado su capacidad de transmisión [11].

- **Fibra Óptica Multimodo:** Esta fibra óptica tiene un diámetro de núcleo entre 50 y 62.5 µm, su atenuación y ancho de banda dependen de la longitud de onda en la que esté trabajando, 3.5 db/km y 200MHz*km en la longitud de onda de 850 nm y 1.5 dB/km 600 MHz*km para la longitud de onda de 1300 nm. Una de las diferencias más marcadas con respecto a la fibra monomodo es que admite varios modos de propagación debido al diámetro del núcleo [11].

- **ONT:** situada en el extremo de la red de acceso, cumple una función esencial en el lado de los usuarios. Este dispositivo combina un módem y un router: en su función de módem, convierte la señal óptica que viaja a través de la fibra en señal eléctrica, o viceversa. Por otro lado, la función de router le permite actuar como un intérprete de estas señales para que puedan ser retransmitidas, ya sea mediante conexión Wi-Fi o por cable. En resumen, la ONT es un componente clave para permitir la conexión de los usuarios finales a la red de fibra óptica [12].

Una ONT cuenta con una serie de parámetros configurables para establecer la red Wi-Fi, siendo las bandas de frecuencia de 2.4GHz o 5GHz las más relevantes. La principal diferencia entre estas bandas radica en la cobertura y la velocidad, siendo la banda de 5GHz la mejor opción para redes Wi-Fi en hogares debido a su mayor velocidad, aunque no todos los dispositivos son compatibles con esta banda. Por lo tanto, es necesario consultar al usuario para elegir la banda más adecuada. Es importante destacar que la elección de la banda no garantiza la mejor experiencia de usuario, ya que el desempeño de la red también depende del canal que se seleccione. Para la banda de 2.4GHz, existen 14 canales superpuestos con un ancho de banda de 22MHz y una separación de 5MHz, como se muestra en la Figura 2.5.

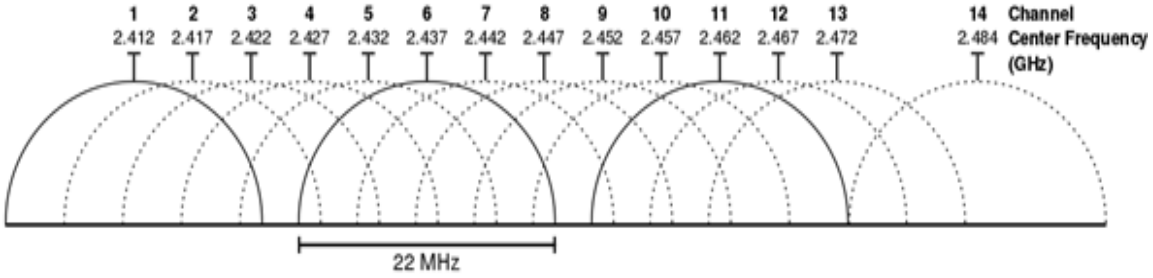

Figura 2.5 Canales Wi-Fi Banda 2.4GHz [13]

La banda de 5GHz ofrece un mayor número de opciones de canal, con un total de 25 canales no superpuestos y un ancho de banda de 20MHz. Sin embargo, es importante tener en cuenta que la mayoría de ONT soportan hasta 16 canales y estos pueden ser agrupados en súper canales de 2, 4 o incluso 8 canales, como se muestra en la Figura 2.6. Es importante considerar estas opciones al configurar la red Wi-Fi para garantizar la mejor experiencia para los usuarios.

Figura 2.6 Canales Wi-Fi Banda 5GHz [14]

- **Elementos de Planta externa (OSP-*Outside Plant*):** estos elementos son los conectores de fibra óptica, se utilizan cables mucho más flexibles en los extremos de la red para la conexión de los equipos activos, existen dos tipos de estos cables:

- **Pigtail:** poseen un conector óptico en solo un extremo del cable para ser conectado directamente a cualquier equipo, en el otro extremo del cable el hilo de fibra se une a la red por fusión o conector mecánico.

- **Latiguillo:** es un conjunto de cables de fibra óptica rodeados de kevlar para protegerlos y mejorar significativamente su resistencia a la tracción. Está cubierto por una capa aislante de un material llamado LSZH y su revestimiento está hecho de sílice para confinar la luz en el núcleo.

Existen varias clases de los dos tipos de cables y estas dependen del tipo de conector que se fabrique, en la Figura 2.7 se ven los tipos de conectores.

Figura 2.7 Conectores ópticos [15]

- **Conector de Ferrule (FC-*Ferrule Connector*):** Este conector es conocido por su método de fijación mediante rosca, lo que lo hace altamente resistente a vibraciones y lo convierte en una opción popular en dispositivos de alta precisión como el Reflectómetro Óptico en el dominio del tiempo (OTDR-*Optical Time Domain Reflectometer*). Este tipo de conector tiene una pérdida de inserción promedio de 0.2 dB y una pérdida de retorno comúnmente inferior a 35 dB.

- **Conector Cuadrado (SC-*Square Connector*)**: Este conector utiliza una férula de cerámica para su sistema de acoplamiento push-pull, siendo uno de los más populares a nivel mundial debido a su bajo costo y su uso en redes Gigabit Ethernet, especialmente en topologías punto a punto. La pérdida de inserción típica es de 0.2dB y la pérdida de retorno es generalmente inferior a 35dB.

- **Conector Lucent (LC-*Lucent Connector*):** Se puede considerar como la nueva generación de los conectores SC ya que es la mitad del tamaño, de ahí que su uso en la oficina central sea recurrente, aunque se puede encontrar push-pull LC en enganchado. Su pérdida de inserción es alrededor de 0.1 dB y de retorno 35dB.

- **MU**: es una versión miniaturizada del conector SC que utiliza una férula de 1.25 mm en lugar de la férula de 2.5 mm utilizada por el conector SC estándar. La pérdida de inserción del conector MU oscila entre 0.2 dB y 0.4 dB y de retorno 35dB.

- **Punta Recta (ST- Straight Tip):** es similar en estructura al conector FC, pero su cierre es en bayoneta, lo que lo hace más robusto y adecuado para aplicaciones industriales. La pérdida de inserción del conector ST es de 0.2 dB y la pérdida de retorno es de hasta 35 dB.

2.1.3 GPON.

GPON es una tecnología que permite respaldar tanto servicios conocidos como aquellos en desarrollo, dirigidos a clientes residenciales y corporativos. Esto se debe a que GPON ofrece la capacidad de acceso a grandes anchos de banda con costos accesibles para los usuarios.

PON es un avance tecnológico que ha permitido cumplir el objetivo de proporcionar una red eficaz y rápida para usuarios de todo tipo. Esta tecnología utiliza la topología punto a multipunto, mediante el uso de divisores ópticos pasivos que dirigen el tráfico de la red para abarcar grandes áreas. Esto reduce significativamente la cantidad de fibra necesaria para la instalación, lo que a su vez reduce los costos de mantenimiento y consumo de energía al no requerir elementos activos entre la OLT y la ONT.

Existen cinco estándares creados para aprovechar la tecnología PON: Red Óptica Pasiva Asimétrica (APON-*Asymmetric Passive Optical Network*) estandarizado por la ITU-T (G.983), Ethernet Sobre Redes Ópticas Pasivas (EPON-*Ethernet Passive Optical Network*) estandarizado por IEEE 802.3ah, BPON recomendado por ITU-T G983, Red Óptica Pasiva con Capacidad de Gigabit (GPON-*Gigabit Passive Optical Network*) también recomendado por ITU-T (G.984), que es el estándar más adoptado a nivel mundial y por ultimo Red óptica pasiva Gigabit Ethernet (GEPON-*Gigabit Ethernet Passive Optical Network*) estandarizado por IEEE 802.3ah.

GPON es una tecnología versátil que utiliza un formato de trama eficiente para transmitir paquetes con longitud variable a velocidades de gigabit/s. Toda la descripción de GPON se encuentra en las recomendaciones ITU-T G984.1 a G984.4, distribuidas de la siguiente

manera: G984.1 describe las características generales de GPON, G984.2 Especificaciones de la Capa Dependiente de los Medios Físicos (PMD-*Physical Medium Dependent*), G.984.3 Especificación de la capa de transmisión y por último G.984.4 Especificación de Gestión Control de la ONT.

En GPON, todo el flujo de tráfico se transmite a través de una sola fibra, utilizando dos canales para distinguir el tipo de tráfico: un canal ascendente y un canal descendente. Para diferenciar estos canales, se utiliza un sistema llamado Multiplexación por División de Longitud de Onda (WDM-Wavelength Division Multiplexing), donde se establece la longitud de onda de 1310 nm para el canal ascendente y de 1490 nm para el descendente.

Gracias a GPON, es posible ofrecer velocidades de transmisión mayores o iguales a 1.2 Gbit/s para FTTH (Fiber to the Home). Existen dos combinaciones de velocidades de transmisión disponibles en este marco: simétrica y asimétrica [16].

> "Asimétrica- 1.24Gbit/s sentido ascendente 2.488Gbit/s sentido descendente".

> "Simétrica- 2.488Gbit/s sentido ascendente 2.488Gbit/s sentido descendente".

- **Transferencia de datos en GPON**

En GPON, no se utilizan dispositivos activos y los divisores ópticos no permiten la selección del tráfico para una ONT específica en el canal descendente que va desde la OLT hacia las ONT. Por lo tanto, todas las ONT son receptoras del tráfico que sale de la OLT (ver Figura 2.8), lo que significa que cada ONT acepta los paquetes que le corresponden y descarta inmediatamente el resto del tráfico.

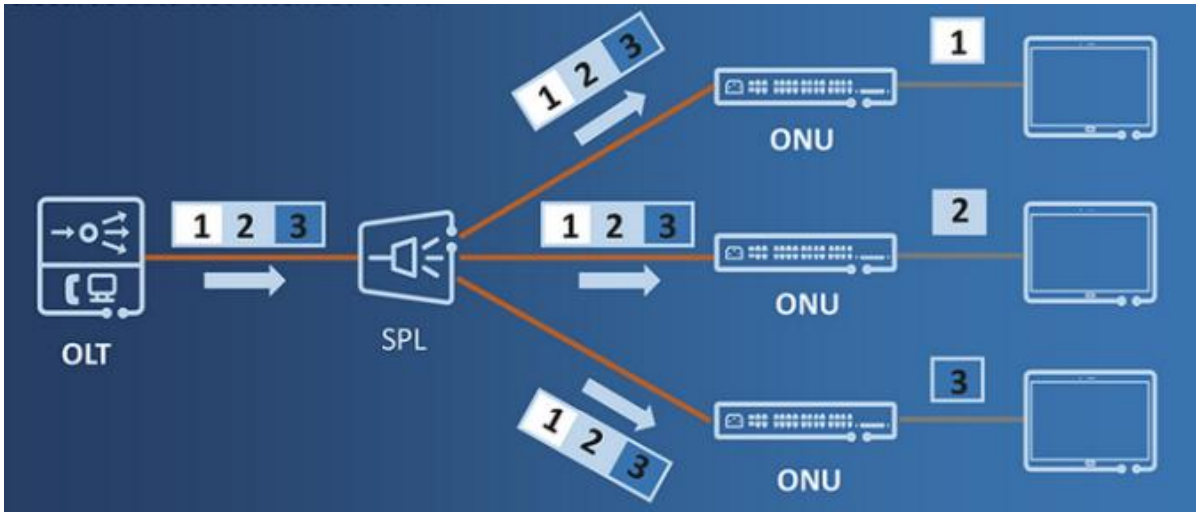

Figura 2.8 Enlace descendente [17]

La forma en que funciona este proceso es simple: la OLT envía paquetes a todas las ONT utilizando una longitud de onda de 1490 nm a través de la red. Los paquetes no se ven afectados, ya que solo pasan por los divisores ópticos que son dispositivos pasivos y solo

propagan la luz con su respectiva división de potencia a sus múltiples salidas. Es así como los paquetes llegan a cada ONT, pero solo se realiza la recepción de aquellos identificados por el ONU ID. En cada ONT o Unidad de Red Óptica (ONU-*Optical Network Unit*), se realiza un filtrado de todos estos datos basado en el ID de puerto del Método de Encapsulación GPON (GEM-*GPON Encapsulation Method*).

En el caso del tráfico ascendente que fluye desde las ONT hacia la OLT, se utiliza la Multiplexación por División de Tiempo (TDM-*Time Division Multiplexing*) en la longitud de onda de 1310 nm. En este método, la OLT identifica con precisión qué ONT está generando el tráfico mediante una relación de ranura temporal, tal como se muestra en la Figura 2.9. Cada ONT tiene asignada una ventana temporal de 125 µs para transmitir ráfagas de información, lo que significa que solo la información de una ONT puede salir del divisor óptico en el sentido inverso a la OLT en cualquier momento.

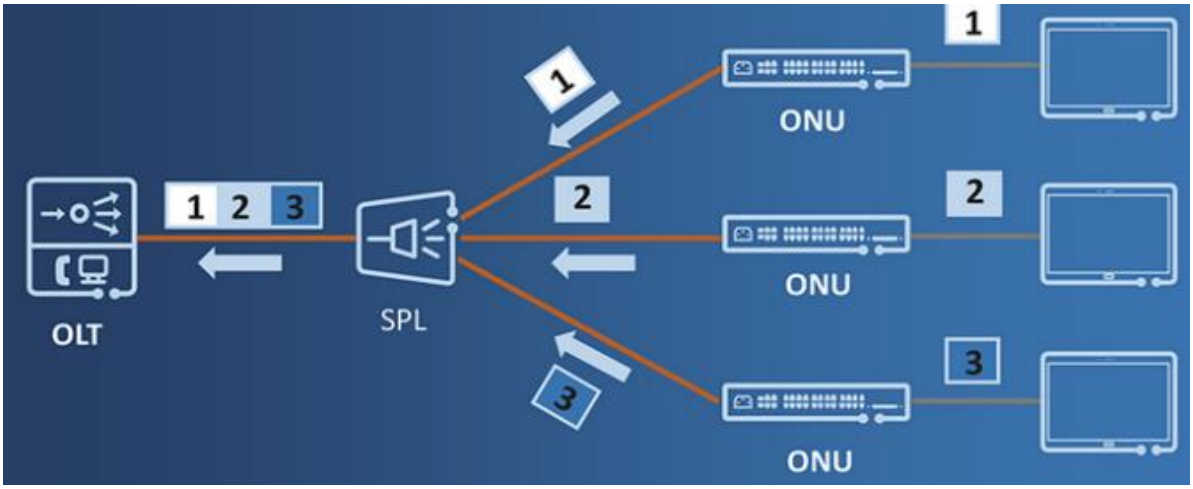

Figura 2.9 Enlace ascendente [17]

La autenticación y sincronización de todas las ONT que están conectadas a la red son obligatorias para que los dos sistemas descritos anteriormente puedan funcionar de manera adecuada. En este proceso, GEM juega un papel fundamental, ya que dentro de una trama GEM se encuentra la información que proporciona el Protocolo de Operación y Mantenimiento de la Capa Física (PLOAM-*Physical Layer Operations, Administration*), siendo GEM el protocolo de enlace de datos entre la ONT y la OLT. De esta manera se marca la gran diferencia respecto a la tecnología EPON, y es que en GPON las tramas GEM de longitud 125 µs encapsulan las tramas Ethernet. Por lo tanto, la trama GEM es esencial para el funcionamiento de la topología punto a multipunto, ya que contribuye significativamente a superar las dificultades de la capa física y proporciona elementos de administración para el ancho de banda, así como una ayuda esencial en la detección de errores.

En [16], se define el alcance lógico como la distancia máxima entre una ONT y la OLT, la cual es de 60 km. Sin embargo, el alcance físico máximo es de 20 km, aunque para garantizar la transmisión a velocidades iguales o superiores a 1.2 Gbit/s mediante el diodo láser Fabry-Perot (FP-LD), se recomienda un máximo de 10 km. Uno de los factores limitantes de la capa física es el ancho espectral, que según la normativa ITU-T G.984.2 debe ser de 20 dB y se

fija en 1 nm para despliegues de 0 a 40 km y de 20 a 60 km [18]. Para obtener el mejor rendimiento de los componentes ópticos y mantener los niveles de potencia óptica, GPON utiliza el sistema de medición de dispersión igual (EDR, por sus siglas en inglés) que tiene tres rangos de atenuación típicos: Clase B+, Clase C y Clase C+ [18].

Tabla 2.3 Clases de Atenuación

Clase de atenuación	Rango de atenuación (dB)	Alcance físico máximo (Km)	Distancia de fibra diferencial (Km)
B+	13 – 28	40	40
C	12 – 30	40	40
C+	17 – 32	60	40

GPON es ampliamente utilizado por los operadores para implementaciones de FTTH y se ha establecido como una parte integral en la prestación de servicios de banda ancha. Cabe destacar que el cable de fibra óptica tiene un ancho de banda prácticamente ilimitado y su capacidad está limitada solo por el hardware operativo utilizado [19]. Por lo tanto, las limitaciones en la distancia que se puede alcanzar entre una ONT y la OLT dependen en gran medida de la potencia óptica que presenta el equipo para la transmisión y la sensibilidad de recepción. En la Tabla 2.4 se muestra una comparación entre las dos clases de transceptores más comúnmente utilizados en GPON [20].

Tabla 2.4 Clases de Transceptores

	Equipo	Potencia [dBm]	Sensibilidad [dBm]
B+	OLT	1,5 a 5	-28 a -8
	ONT	0,5 a 5	-27 a -8
C+	OLT	3 a 7	-32 a -12
	ONT	0,5 a 5	-30 a -8

Para determinar la potencia óptica necesaria para la transmisión en una red GPON, es necesario realizar un cálculo de pérdidas que tenga en cuenta varios factores. A la potencia de transmisión se le deben restar las pérdidas por inserción de los divisores ópticos (consulte la Tabla 2.1 y la Tabla 2.2), las pérdidas de inserción y retorno de los conectores que se utilicen, y la pérdida de inserción del cable de fibra. Esta última varía según la longitud de onda y el tipo de fibra: 0.40 dB/Km para una longitud de onda de 1310 nm y 0.2 dB/Km para 1490 nm, ambas mediciones son para fibra monomodo. Por último, se debe sumar la pérdida por empalme, que puede ser de alrededor de 0.3 dB si es mecánico, un valor significativo en comparación con el empalme por fusión que es de 0.01 dB en promedio.

2.1.4 Topologías FTTH/GPON.

FTTH/GPON hace uso de dos topologías conocidas en su red de acceso: Punto a Punto (P2P-*Point to Point*) y Punto a Multipunto (P2MP-*Point to Multipoint*), generalmente las dos coexisten dentro de esta arquitectura.

- **P2P:** En este caso la relación es 1:n, lo que significa que se requiere desplegar n hilos de fibra por cada n clientes para que el usuario final pueda obtener toda la capacidad del ancho de banda que ofrece el proveedor de servicios de Internet. Aunque los costos de operación y mantenimiento son bajos, el costo para su despliegue es muy elevado, ya que se necesita un conmutador ethernet en la oficina central y otro en las instalaciones del usuario conectados a través del estándar ethernet. Por lo tanto, este tipo de topologías se implementa comúnmente para usuarios corporativos.

- **P2MP:** esta topología es la más utilizada en FTTH/GPON, debido a que los hilos de fibra se conectan a divisores ópticos pasivos antes de llegar a la ONT, permitiendo que varios usuarios compartan un solo hilo de fibra, dependiendo de la relación del divisor óptico ver Figura 2.10. Esto resulta en una disminución significativa de los costos de despliegue.

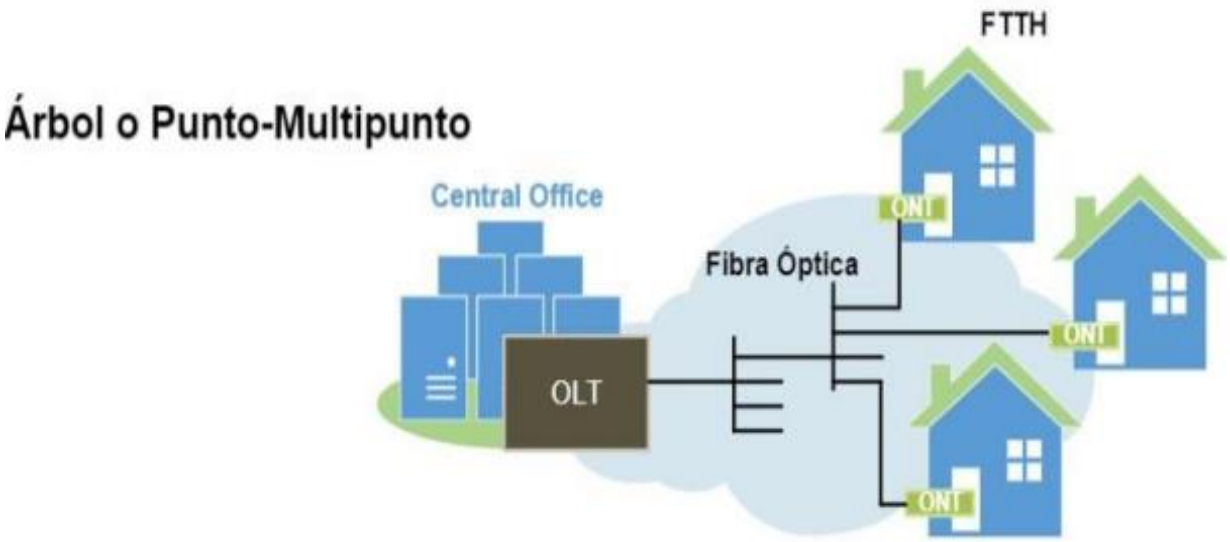

Figura 2.11 Topología punto a multipunto [21]

En este apartado, es crucial destacar la capacidad de usuarios que pueden conectarse a través de un solo hilo de fibra conectado a un puerto de la OLT. La OLT tiene una tarjeta que puede tener hasta 16 puertos, y cada uno tiene la capacidad de conectar hasta 128 abonados. Esto se traduce en una capacidad máxima de conexión simultánea de hasta 2048 abonados por tarjeta. Generalmente, una OLT tiene la capacidad de hasta 16 tarjetas, aunque esto puede variar dependiendo de la marca utilizada.

2.1.5 Arquitectura FTTH/GPON

En la arquitectura de red se definen claramente cinco áreas empezando por el núcleo de red, oficina central, línea o red de alimentación, red de distribución y por último el área del cliente como se ven en la Figura 2.11.

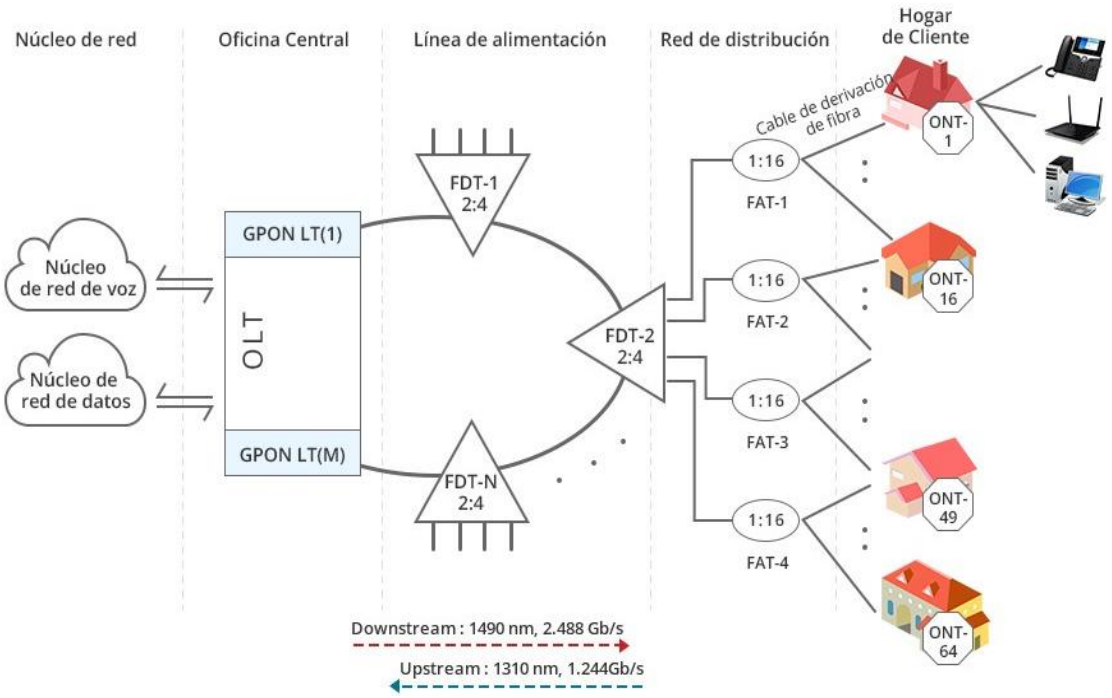

Figura 2.12 Arquitectura FTTH/GPON [22]

Generalmente, el núcleo de la red y la oficina central se ubican en el mismo lugar, mientras que la red de alimentación, distribución y área del usuario conforman la planta externa, pero se separan en función de su rol y los equipos que intervienen.

- **Núcleo de Red**

En esta área se encuentran ubicados los equipos y servidores del ISP, que incluyen el servidor de Autenticación, Autorización y Contabilidad (AAA-*Authentication, Authorization, Accounting*), el servidor de Acceso Remoto de Banda Ancha (BRAS-*Broadband Remote Access Server*), la Red Telefónica Conmutada (PSTN-*Public Switching Telephone Network*) y los dispositivos del proveedor de televisión.

- **Oficina Central**

Esta área se compone por la OLT y el Distribuidor de Fibra Óptica (ODF-*Optical Distribution Frame*).

- **Línea o Red de Alimentación**

La primera área de la planta externa se refiere al tendido de fibra que se conecta en un extremo al ODF ubicado en la oficina central y en el otro extremo se empalma con los Terminales de Distribución de Fibra (FDT-*Fiber Distribution Terminal*) que cuentan con divisores ópticos de nivel 1. Por lo general, los FDT se ubican en instalaciones aéreas, como mangas, y el tendido de cable se conoce como fibra de nivel 1. En esta área, también se incluyen las conexiones a los equipos de alimentación, como transformadores y generadores de energía, para garantizar el suministro eléctrico a lo largo de la red.

- **Red de Distribución**

En esta área, se inicia en el empalme del tendido de fibra con el splitter de nivel 1 dentro del FDT y se extiende hasta un Terminal de Acceso a la Fibra (FAT-*Fiber Access Terminal*) donde se encuentra un splitter de nivel 2. Por lo tanto, esta sección del tendido de cable se conoce como fibra de nivel 2. Usualmente, los FAT se ubican en el sector de los usuarios, sujetos en la parte alta de los postes en puntos estratégicos.

- **Área de usuarios**

Es el área final de la planta externa, porque es donde se realiza el empalme de la fibra entre el splitter de nivel 2 ubicado dentro de la FAT y en el otro extremo se empalma con un pigtail que se conecta a la ONT que se encuentra dentro de las instalaciones del usuario, el tendido de está fibra se conoce como fibra de nivel 3, como su uso es para la instalación directa al usuario esta fibra es de un diámetro pequeño lo que significa que es más ligera y sobre todo flexible [23].

2.1.6 Aprovisionamiento dentro de la red FTTH/GPON.

En este apartado se encuentra las funciones de los equipos ubicados en la oficina central del ISP.

- **Autenticación, Autorización y Contabilidad (AAA-Authentication, Authorization and Accounting).**

La seguridad es fundamental en cualquier red, por lo que autenticar, autorizar y registrar se convierte en un modelo efectivo para cumplir esta función, ya que permite identificar y controlar el acceso de los usuarios a los servicios que se ofrecen y llevar un registro del uso que hacen de los mismos.

La importancia del uso de AAA en el control de acceso a los recursos radica en que permite la flexibilidad en la configuración de los parámetros de seguridad, evitando que el control de acceso se base en direcciones IP estáticas y permitiendo una gestión más sencilla de los cambios en la red.

- **Autenticación.**

El proceso de autenticación es fundamental para garantizar la seguridad de la red, ya que permite determinar la legitimidad de cada usuario a través de la verificación de su identidad mediante el nombre de usuario y la credencial de acceso, generalmente una contraseña. Todos los usuarios de la red deben pasar por este proceso para poder acceder a los servicios y recursos de la red.

- **Authorization.**

La fase de autorización es crucial en el proceso de control de acceso a la red, ya que es aquí donde se establecen los permisos y limitaciones que tiene el usuario autenticado. En esta etapa se determinan los servicios y recursos a los que el usuario tiene acceso, así como la asignación de ancho de banda y otras configuraciones específicas para su cuenta.

En resumen, la autorización se encarga de establecer los límites y alcances de las acciones que el usuario puede realizar en la red.

- **Accounting.**

El proceso de contabilidad se encarga del registro y monitoreo del uso de la red por parte de los usuarios. Durante este proceso se almacena información detallada acerca de las credenciales de los usuarios, los servicios a los que tienen acceso, el tráfico que generan y el tiempo que permanecen haciendo uso de la red. Toda esta información se utiliza con fines administrativos, de facturación y para la planificación de estrategias futuras en la red. La contabilidad es esencial para garantizar un uso adecuado de la red y para mantener un control preciso de su funcionamiento.

- **Servicio de Usuario de Acceso Telefónico de Autenticación Remota (RADIUS-*Remote Access Dial In User Service*).**

RADIUS es un protocolo que implementa el modelo AAA para gestionar los usuarios, el acceso y uso de los servicios que ofrece un ISP. La información que se recopila con el modelo AAA comienza cuando el host de un usuario se conecta a la red y envía el nombre de usuario y la contraseña. Para que esta información se envíe, un router actúa como intermediario entre dos nodos y la comunicación directa se lleva a cabo a través del protocolo PPP, que redirige la petición del host a un servidor RADIUS.

Antes de que el router pueda asignar una dirección IP al host, el servidor RADIUS verifica las credenciales mediante el Protocolo de Autenticación Extensible Protegido (PEAP-Protected Extensible Authentication Protocol) o el Protocolo de Autenticación Extensible (EAP-Extensible Authentication Protocol). Si la verificación es correcta, se permite el acceso y se realiza la provisión de una dirección IP. En la Figura 2.12 se puede observar el esquema de su funcionamiento.

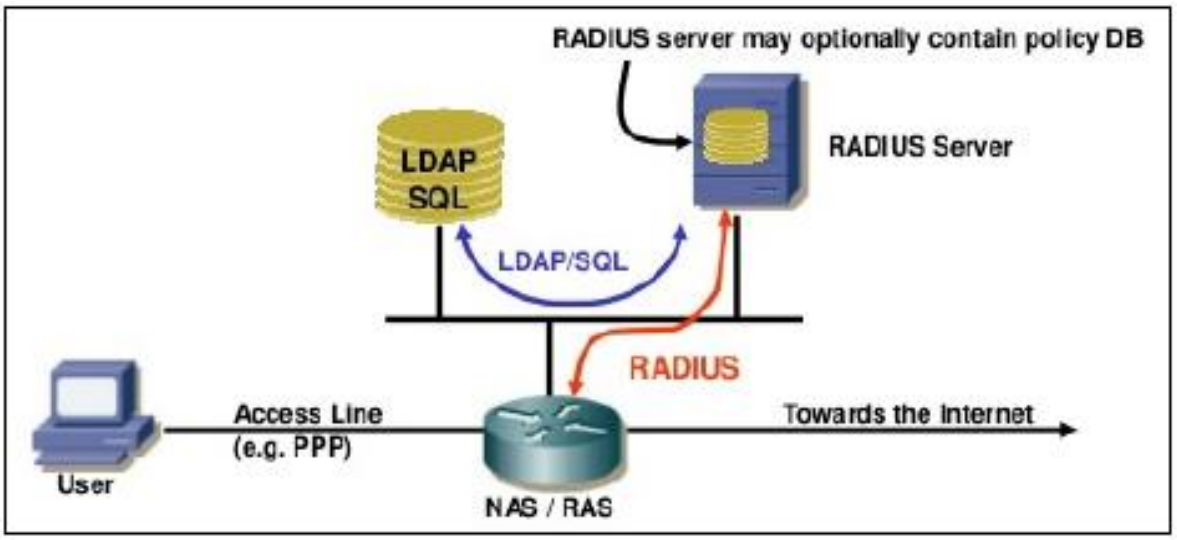

Figura 2.13 Esquema de Funcionamiento RADIUS [24]

- **Aprovisionamiento de los recursos de red (direcciones IP).**

La idea principal del aprovisionamiento de los recursos de red es asignar una dirección IP a un dispositivo cliente, ya sea de manera estática o dinámica, a través de un servidor. Este proceso es importante para garantizar que todos los dispositivos de la red tengan una dirección IP única y puedan comunicarse correctamente. En la asignación estática, la dirección IP se configura manualmente y permanece fija, mientras que en la asignación dinámica se asigna una dirección IP disponible temporalmente al dispositivo cliente. El aprovisionamiento de recursos de red también puede incluir la asignación de otros recursos como nombres de dominio y servidores DNS.

- **Protocolo de Configuración Dinámica de Host (DHCP-*Dynamic Host Configuration Protocol*).**

Este protocolo existe en una red con arquitectura cliente/servidor y su función es proveer de forma dinámica el direccionamiento IP, aunque no es el único parámetro de red que se puede configurar, pero si el más relevante. Este protocolo de configuración es indispensable para garantizar la interoperabilidad de diferentes redes y la configuración de distintos dispositivos.

El protocolo DHCP asigna direcciones IP estáticas, dinámicas y automáticas, en cualquiera de los tres casos se establecen:

- Dirección IP única.
- Máscara de Subred
- Dirección Gateway predeterminada
- Sistema de Nombre de Dominio (DNS-*Domain Name System*)
- Protocolo de Autodescubrimiento de Proxy WEB (WPAD-*WEB Proxy Autodiscovery Protocol*)

DHCP es estable ya que brinda garantías de renovación periódica y de restablecimiento del enlace, porque en el momento que el servidor no esté disponible, el cliente seguirá presentando una solicitud hasta que el servidor esté de nuevo en línea y le asigne una dirección IP.

A pesar de las ventajas significativas que brinda DHCP, es importante considerar una desventaja en cuanto a seguridad se refiere, ya que este protocolo no cuenta con mecanismos de autenticación, autorización y contabilidad (AAA) ni otros métodos de seguridad, lo que lo expone a posibles ataques.

- **Opción 43.**

El protocolo DHCP utiliza varias opciones para comunicarle a un CPE la dirección IP donde se encuentra un servidor ACS, en este caso se trata de Vendor Specific Information u Opción 43.

Gracias a esta Opción el CPE puede solicitar la dirección IP del ACS al servidor DHCP con un mensaje DHCP REQUEST, en el cual el CPE le informa al servidor DHCP que se encuentra en la capacidad de soportar el protocolo CWMP, una vez el servidor tiene esta

información envía como respuesta un DHCP OFFER en el cual contiene la dirección IP del ACS como se puede ver en la Figura 2.13.

Figura 2.14 Esquema Funcional Opción 43 [24]

- **Protocolo Punto a Punto (PPP-*Point to Point Protocol*).**

Este protocolo trabaja en la capa de enlace de datos y tiene como función aprovisionar un direccionamiento IP para establecer una conexión directa entre dos nodos. Por ejemplo, puede establecer un enlace entre dos routers sin ningún otro dispositivo que intervenga. Una gran ventaja de PPP es su seguridad, ya que hace uso de AAA.

- **Protocolo Punto a Punto Sobre Ethernet (PPPoE-*Point to Point Protocolo Over Ethernet*)**

Es un protocolo de red que encapsula PPP en una capa Ethernet. Esto permite establecer una conexión IP sobre un enlace Ethernet y aprovechar las funciones de autenticación, autorización y compresión que se ofrecen en PPP.

PPPoE puede realizar la identificación virtual de un dispositivo dentro de una red Ethernet, lo que permite establecer un enlace serial con dicho dispositivo. Se utiliza para la transmisión de paquetes IP siguiendo las reglas establecidas por el protocolo PPP. Además, todas las direcciones IP se asignan sólo cuando el enlace PPPoE está abierto, lo que permite el direccionamiento dinámico.

- **Aprovisionamiento Automático.**

El aprovisionamiento automático o autoaprovisionamiento es una aplicación de software que permite reconocer un CPE (Customer Premises Equipment) en el momento en que se conecta a la red de acceso, y así el ISP (Internet Service Provider) le proporciona servicios de forma inmediata, evitando que el personal técnico del ISP tenga que realizar todas las configuraciones necesarias para establecer el enlace y proporcionar los servicios manualmente.

Dado que la demanda por servicios de Internet en el contexto actual de la sociedad aumenta considerablemente, el sistema de aprovisionamiento de los ISP debe converger a la automatización. Cuanto mayor sea el número de usuarios y servicios que se ofrezcan, mayor será el número y nivel de configuración que se debe realizar en los CPE, y si este proceso

se realiza de forma manual, elevará los costos y el tiempo del proceso, comprometiendo la calidad del servicio prestado por el ISP.

En el proceso de autoaprovisionamiento intervienen el protocolo CWMP como canal que permite la comunicación entre el ACS y un CPE. Una vez establecido este canal, entra en funcionamiento SOAP, el cual realiza el envío de peticiones entre el ACS y el CPE, y por último, el estándar TR-098, que proporciona la especificación del modelo de datos que utiliza el CPE.

A continuación, se observa el diagrama de flujos de la comunicación entre un CPE y un ACS ver Figura 2.14.

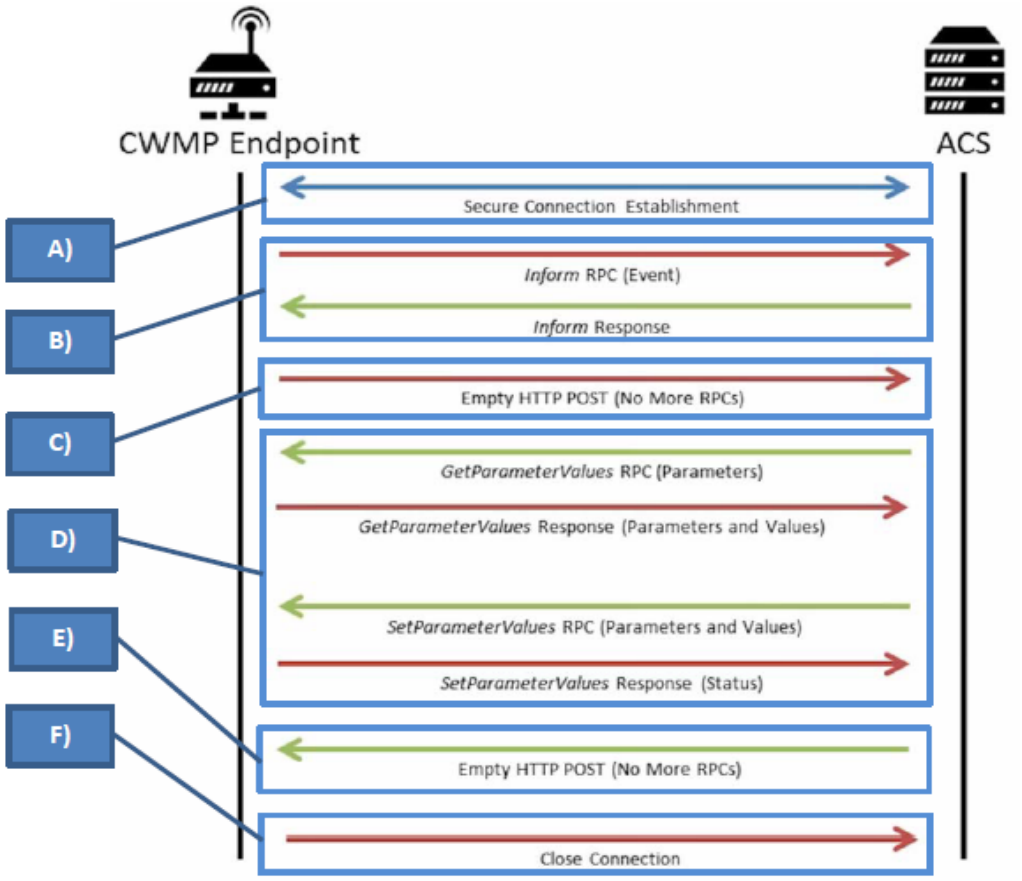

Figura 2.15 Diagrama de Flujo de la Comunicación entre un CPE y ACS [24]

En este ejemplo se da por hecho que es la primera vez que el CPE se conecta a la red de acceso, y en esta circunstancia es el CPE quien inicia la comunicación enviando la primera petición solicitando una conexión.

i. Una vez establecida la conexión, la seguridad de la comunicación se proporciona mediante la Seguridad de la capa de transporte (SSL- *Secure Socket Layer*).

ii. En este paso, el CPE envía un mensaje de Llamada a Procedimiento Remoto (RPC-Remote Procedure Call) al ACS, que contiene información sobre el estado del CPE.

A continuación, el ACS responde con un mensaje de confirmación de la petición (inform response), indicando al CPE que su solicitud ha sido aceptada.

iii. Después de esto, el CPE envía una solicitud vacía (Empty HTTP POST - No More RPC) para informar al ACS que la sesión establecida sigue abierta y que está listo para recibir indicaciones del ACS.

iv. Una vez que el ACS recibe esta solicitud vacía, comienza a enviar indicaciones RPC al CPE. Estas pueden incluir configuraciones o solicitudes de parámetros específicos del CPE. Por ejemplo, si se desea asignar un valor a un parámetro determinado, el ACS enviará un RPC de SetParameterValue al CPE, quien responderá con un RPC de SetParameterValue Response, que indica el nuevo estado de ese parámetro.

v. Una vez que el ACS ha completado todas las operaciones necesarias, envía una solicitud vacía (Empty HTTP POST - No More RPC) para indicar al CPE que no hay más indicaciones RPC por enviar.

vi. Por último, al recibir esta solicitud vacía, el CPE envía una solicitud de cierre de conexión (Close Connection) al ACS para cerrar la conexión.

- **CWMP o Reporte Técnico 069 (TR-069-*Technical Report 069*)**

Es un estándar definido por la Broadband Forum que establece un protocolo que actúa en la capa de aplicación con el fin de lograr la administración remota de los CPE [25], donde su principal función es proveer la comunicación entre un CPE y un ACS.

CWMP funciona en la capa de aplicación para permitir la gestión remota de los CPE. A diferencia de la opción 66 de DHCP, que solo permite la descarga de archivos, CWMP permite la gestión y configuración de un CPE conectado a la red mediante un ACS.

En el ejemplo de la Figura 2.14, se puede observar que el intercambio de mensajes entre el ACS y el CPE se realiza mediante los protocolos SOAP/HTTP. A continuación, se describe brevemente el funcionamiento de estos protocolos en la gestión remota.

- **SOAP**

Es un protocolo para el intercambio de información estructurada entre sistemas distribuidos. Utiliza el lenguaje de marcado extensible (XML-*Extensible Markup Language*) como formato para la mensajería. SOAP se basa en HTTP o, con más frecuencia, en HTTPS, y también utiliza SMTP para establecer el canal y la comunicación entre el ACS y los CPE.

La elección del formato XML para SOAP es importante, ya que permite realizar solicitudes de servicios web y obtener respuestas independientemente del idioma, el sistema operativo y la plataforma en la que se ejecuta el proceso. Esto hace que SOAP sea un protocolo de intercambio de información muy flexible y compatible con diferentes tipos de sistemas.

- **Reporte Técnico 098 (TR098-*Technical Report 098*)**

Este estándar define el modelo de datos utilizado por CWMP para la gestión remota de los dispositivos. Proporciona una descripción detallada de la puerta de enlace del dispositivo y especifica los diferentes modelos de datos relacionados con los métodos de TR069 para la gestión de dispositivos. El modelo de datos se estructura mediante objetos y parámetros, lo que permite una organización clara y jerárquica de la información. TR098 es esencial para el correcto funcionamiento de CWMP, ya que proporciona el marco para la comunicación y la gestión de dispositivos en la red [26].

- Objeto: puede ser el contenedor de un parámetro e incluso de otros objetos.

- Parámetro: Es el nombre o valor que puede tener un parámetro dentro de la configuración de un CPE al cual es accesible por parte del ACS para lectura o escritura.

En la tabla se puede ver parámetros y objetos de uso recurrente de InternetGatewayDevice.

Tabla 2.6 **InternetGateWayDevice.ManagementServer [26]:** Parámetros de asociación entre ACS y CPE.

ConnectionRequestUsernamme	Nombre de usuario para autenticación
ConnectionRequestPassword	Contraseña para autenticar
PeriodicInformEnable	Para determinar si el CPE debe enviar información periódica al ACS
PeriodicalInformInterval	Define el periodo entre cada mensaje que debe enviar el CPE al ACS.

Tabla 2.7 **IntenerGateWayDevice.DeviceInfo [26]:** Para información general de un CPE.

Manufacturer	Nombre del Fabricante del CPE
ManufacturerOUI	Es un valor único de identificación de organización del CPE
SerialNumber:	Es un valor fijo que representa el serial de un CPE.

- **Llamada a Procedimiento Remoto (RPC-*Remote Procedure Call*)**

A diferencia de otros protocolos, RPC no es un protocolo en sí mismo, sino más bien un programa basado en SOAP que permite la comunicación bidireccional entre ACS y CPE. Todas las funciones necesarias para el autoaprovisionamiento son implementadas mediante RPC. Por ejemplo, la operación descrita en el paso i del diagrama de flujos en la Figura 2.14 es una llamada RPC. En total, existen cuatro operaciones RPC fundamentales para la gestión remota de dispositivos mediante CWMP. Estas operaciones permiten la gestión y configuración de los dispositivos CPE conectados a la red mediante un ACS.

- **Objetos:** como se ve en la sección anterior esta función agrupa parámetros para realizar aportes a un CPE.

  - **Add Objet:** El ACS puede crear instancias de objetos dentro del CPE como conexiones WAN por ejemplo.

  - **Delete Object:** El ACS puede eliminar las instancias que se encuentren en el CPE.

- **Parámetros:** Estos parámetros están basados en el modelado de datos descrito en TR-098.

  - **GetParameterValue:** Por medio de esta función RPC el ACS solicita información al ACS de uno o varios parámetros.

  - **SetParameterValue:** Esta función permite al ACS asignar un valor a uno o varios parámetros.

- **Ficheros:** RPC de archivos de configuración que se pueden generar o introducir.

  - **Download:** Con esta función el ACS le indica al CPE que debe descargar un fichero ya sea para actualización o configuración.

- **Mantenimiento:** RPC para gestión y monitorización de CPE.

  - **Inform:** Esta función es utilizada por el CPE para iniciar sesión dentro del ACS como se observó en el diagrama de flujos en la Figura 2.14, sin embargo, ése no es su único uso ya que también permite enviar el estado de uno o varios parámetros si así lo solicita el ACS.

- **Reboot:** Con este RPC el ACS reinicia un CPE de ser necesario por ejemplo después de una actualización.

Las funcionalidades principales de CWMP para administrar los diferentes tipos de CPE son las siguientes:

- **Autoconfiguración y aprovisionamiento dinámico de servicios**

La autoconfiguración y el aprovisionamiento dinámico de servicios son mecanismos que permiten la configuración y provisión de servicios de forma automática en el momento en que un CPE se conecta por primera vez a la red de acceso de banda ancha. Además, estos mecanismos también permiten la reconfiguración del CPE en cualquier momento mediante una iniciativa asincrónica del ACS. Esto resulta en una gestión más eficiente y automatizada de los CPE, lo que se traduce en una mejor experiencia del usuario y un menor tiempo de inactividad en la red.

- **Gestión de imágenes de software/firmware**

Por medio de CWMP se puede identificar la versión de firmware de un CPE, así como administrar la descarga de la misma iniciada por el ACS o el CPE en caso de ser necesario, y notificar al ACS si la descarga fue exitosa.

- **Supervisión de estado, rendimiento y diagnóstico**

CWMP permite monitorear el estado de uno o varios CPE, proporcionando información relevante al ACS sobre el rendimiento del equipo. Además, el CPE mantiene información disponible para que el ACS pueda usarla en la identificación y resolución de problemas de conectividad o servicios que estén fallando. Finalmente, se pueden realizar pruebas de diagnóstico predefinidas para descartar problemas y acelerar el proceso de identificación de fallas, o simplemente notificar cambios en el estado de un CPE. En resumen, CWMP facilita la supervisión de estado, rendimiento y diagnóstico de los CPE.

2.1.7 ACS (Auto Configuration Server)

ACS es un servidor de administración que se encarga de controlar, monitorear y configurar cualquier tipo de dispositivo CPE compatible con CWMP. Es un enlace crucial entre el departamento de soporte técnico y los CPE conectados a la red. A través del ACS, se automatiza el aprovisionamiento remoto, así como las actualizaciones de software y firmware.

El ACS puede iniciar sesiones asíncronas para informar al CPE de cualquier cambio de configuración. Esto es posible gracias a la configuración automática de los servicios que requieren la reconfiguración del dispositivo CPE en tiempo real. Esto se puede utilizar, por ejemplo, para garantizar que los usuarios finales tengan acceso inmediato a los servicios a los que se suscriben, sin tener que esperar al siguiente contacto casual [24].

Existen diferentes herramientas de software que realizan el funcionamiento de un ACS, las cuales se pueden agrupar en dos categorías: herramientas privadas y herramientas de código abierto (Open Source). Sin embargo, varias de las herramientas de código abierto han dejado de recibir actualizaciones desde hace varios años, por lo que se presentarán solo las que se encuentren vigentes.

- **AXESS**

Desarrollado por Axiros para gestionar principalmente CPE que soporten CWMP, aunque cada vez amplía la gama de protocolos de gestión abiertos que son compatibles con los estándares realizados por la Broadband Forum. Esto hace de AXESS una aplicación muy flexible y, sobre todo, escalable al momento de interactuar con múltiples CPE.

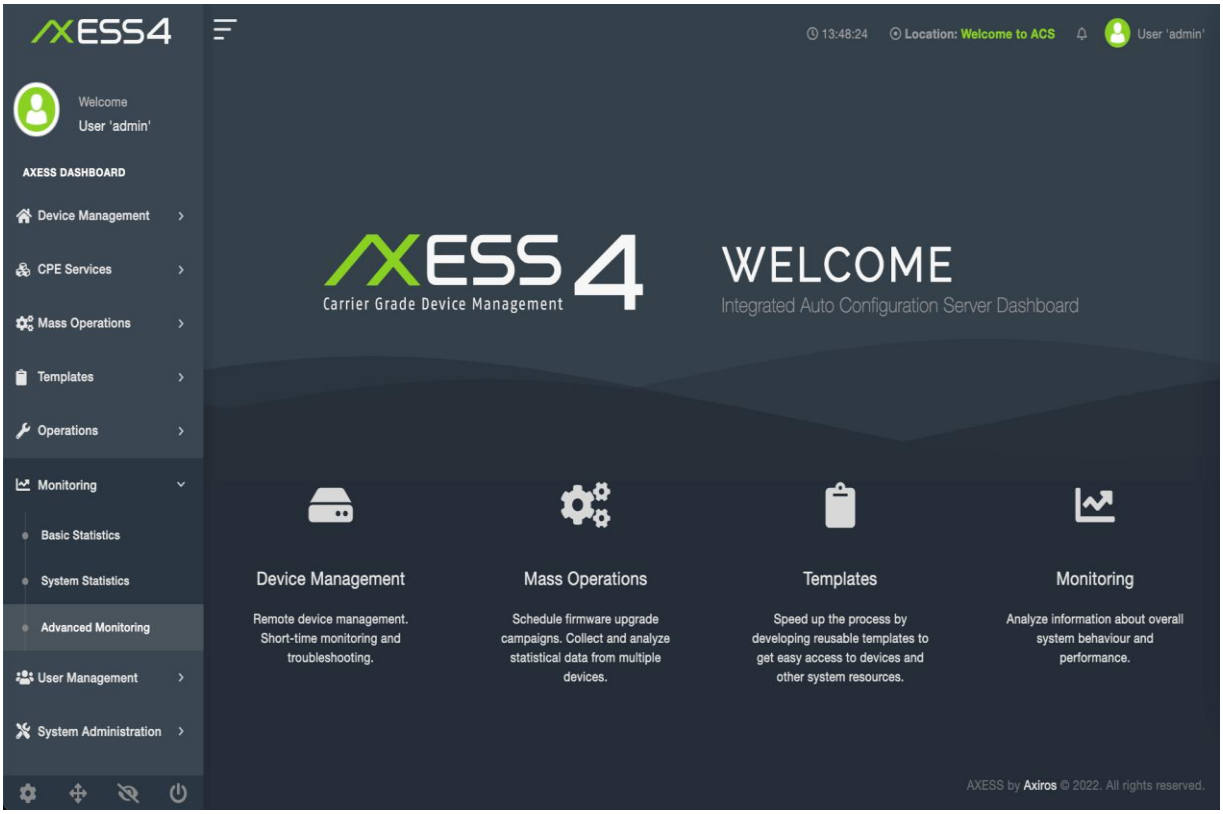

Figura 2.16 Interfaz de Usuario AXESS [27]

AXESS cuenta con una interfaz de administración completamente personalizable y soporte de más de 100 idiomas.

- Características
  - Gestión de dispositivos de manera remota.
  - Aprovisionamiento automático
  - Monitoreo
  - Soporte
  - Motor de flujo de trabajo
  - Gestión inteligente de firmware
  - Gestión de seguridad
  - Múltiples protocolos NBI, que pueden extenderse por solicitud
  - Interoperabilidad
  - Permisos para agregar, visualizar, editar y borrar.
  - Presenta servicios de correo, syslog, XML-RPC, SOAP, cliente JMS
  - Matriz de seguridad
  - Permite personalizar los sistemas de autorización.
  - Programación de operaciones en masa
  - Motor de flujo multi step
  - Soporta Solaris
  - Incluye Bases de datos en SQL
  - Agrupación de CPE

- **AVsystem**

Esta empresa cuenta con dos herramientas para servicios ACS, la primera es la Plataforma de Gestión Unificada (UPM-Unified Management Plataform) y la segunda es Cloud ACS.

- **PMU**

  Es una solución de software integral para la gestión de dispositivos de red y servicios de múltiples proveedores

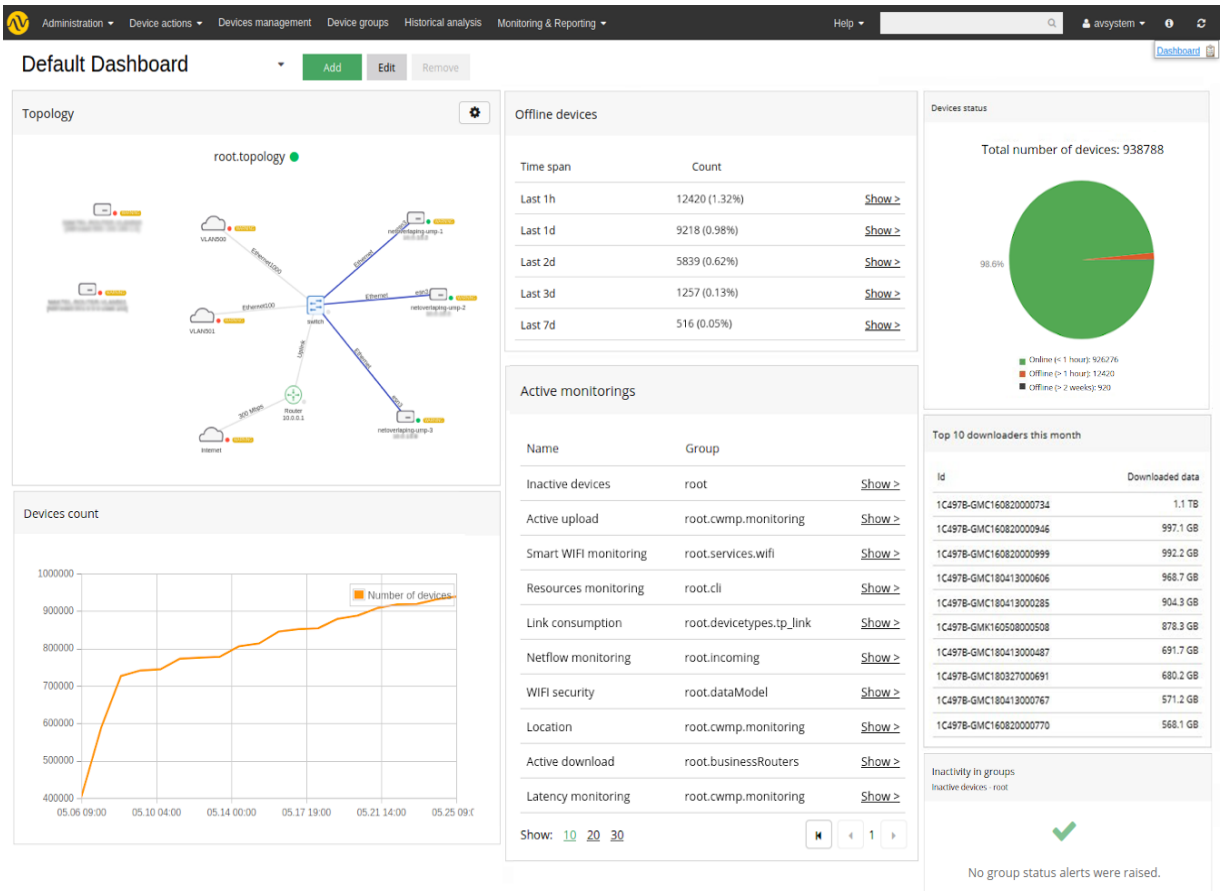

Figura 2.17 Interfaz de Usuario UPM [28]

➢ Características:

- Configuración y activación automática de servicios
- Administración y actualización de firmware
- Monitoreo proactivo
- Soporta a clientes
- Agrupación de dispositivos
- Interfaz unificada
- Auditorias de seguridad
- SOAP y API REST integración automatizada
- Servicio de localización geográfica

- **CLOUD ACS**

Los ISP pueden administrar los dispositivos remotamente usando el modelo de Software Como un Servicio (SaaS-Software as a Service).

Cloud ACS de AVSystem es una solución de administración y aprovisionamiento de dispositivos de IoT (Internet de las cosas) basada en la nube que permite a los usuarios configurar, actualizar y monitorizar dispositivos de manera eficiente y centralizada.

Figura 2.18 Interfaz de Usuario CLOUD ACS [28]

➢ Características:

- Aprovisionamiento de dispositivos
- Actualización de firmware
- Gestión remota
- Monitoreo
- Agrupación
- Gestión masiva simplificada
- Integración con otros sistemas vía API
- Redundancia geográfica para prevenir pérdida de datos

- ***Friedlytech***

Plataforma amigable de administración de dispositivos unificados (UDMP-The *Friendly Technologies Unified Device Management Platform*) con una interfaz Web muy funcional; ver Figura 2.18.

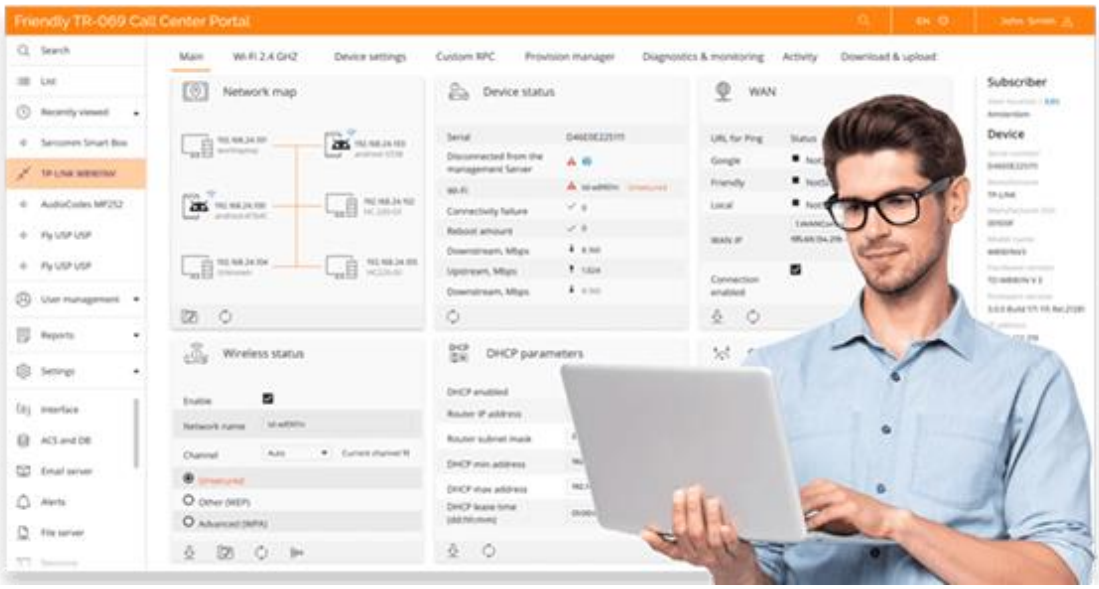

Figura 2.19 Interfaz de Usuario Friedlytech [29]

Este motor es multipropósito realiza la gestión del ciclo de vida de un CPE.

➢ Características:
- Gestión de dispositivos unificada, escalable y robusta
- Plataforma de servicios al usuario TR-369
- Pruebas de velocidad y latencia
- Optimización de Wi-Fi
- Monitoreo QoE
- Centro de soporte técnico
- Portal de autoayuda
- Generador de informes de Inteligencia Comercial (BI *Intelligence Business*).
- Automatización del aprovisionamiento de servicios.

- ***EasyCWMP***

Desarrollado por PIVA Software, esta solución es Open Source GOLv2 del estándar CWMP, aunque su última versión la 1.8.6 fue lanzada en 2019 es ampliamente utilizada y está diseñado en dos secciones como se ve en la Figura 2.19.

➢ EasyCWMP core: La comunicación entre el ACS y un CPE se da a través del otor TR069 que está desarrollado en C.

- EasyCWMP DataModel: Aquí se encuentra el modelo de datos para CWMP como TR098, TR181, TR104 entre otros, estos métodos son los que ejecuta el ACS como por ejemplo GET,SET,Add como se ve en la Figura 2.19.

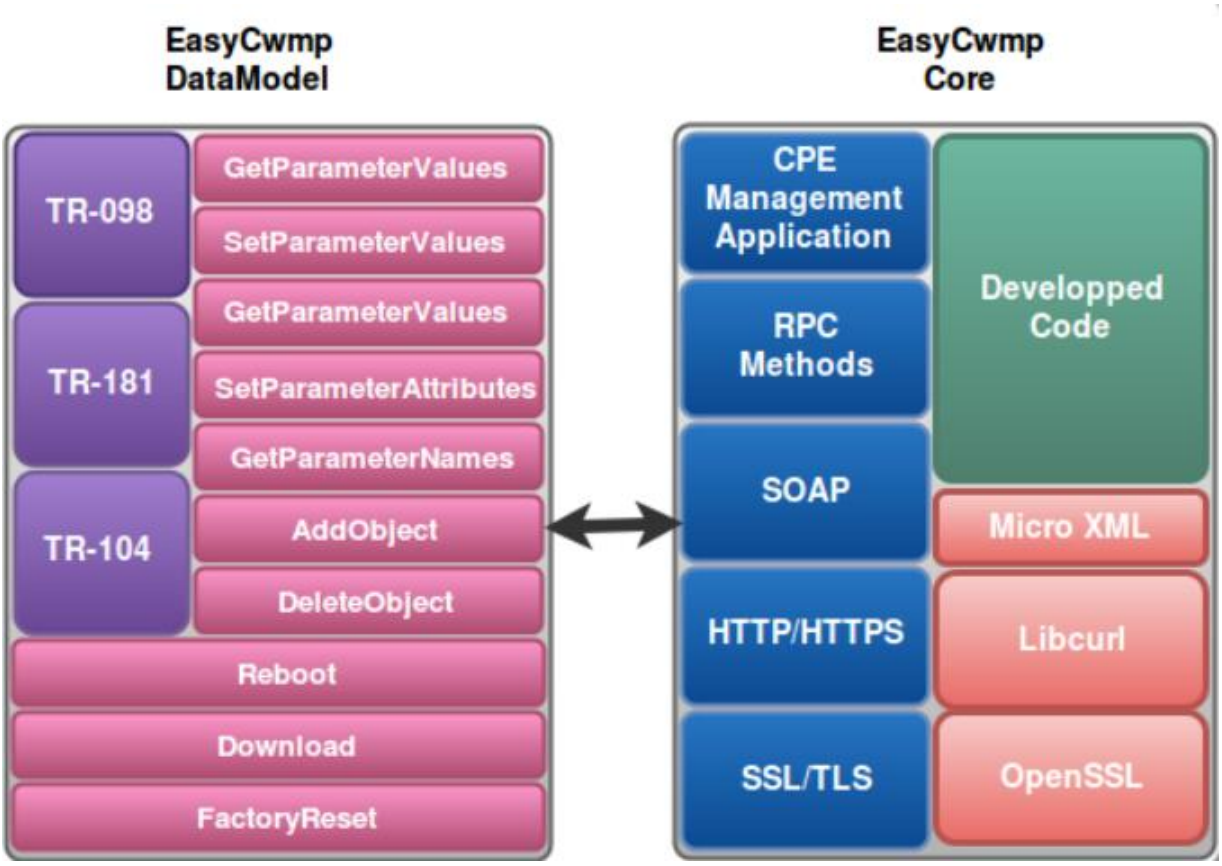

Figura 2.20 Sección dual EasyCwmp [30]

El diseño en dos secciones tiene como objetivo realizar de forma independiente la ejecución del método CWMP del motor CWMP para que el proceso de probar funciones e incluir nuevas funciones sea sencillo.

EasyCWMP cuenta con una solución Premiun en la cual el modelo de datos está implementado en C y la versión gratuita se implementa en Shell, la principal diferencia es tiempo de ejecución, ya que en C un GetParameterValue puede tardar milisegundos y en Shell alrededor de 20 segundos.

- Características:
  - Sencillez en el proceso de actualización del DataModel
  - Fácil adaptación con sistemas operativos LINUX y POSIX
  - Documentación amplia
  - Acepta todos los métodos CWMP
  - Integra HTTP, HTTPS, FTP para transferir archivos
  - Implementa SSL
  - Soporta IPV6

- ***GenieACS***

Es la solución Open Source para gestión CWMP más actualizada, su última versión GenieACS 1.2.9 fue lanzada el 22 de agosto de 2022. Cuenta con una interfaz gráfica que es opcional ver Figura 2.20, y una API para con la cual se pueden establecer parámetros, preset, eliminar dispositivos de la base de datos, borrar tareas, buscar dispositivos por su ID o su dirección MAC entre muchas otras funciones.

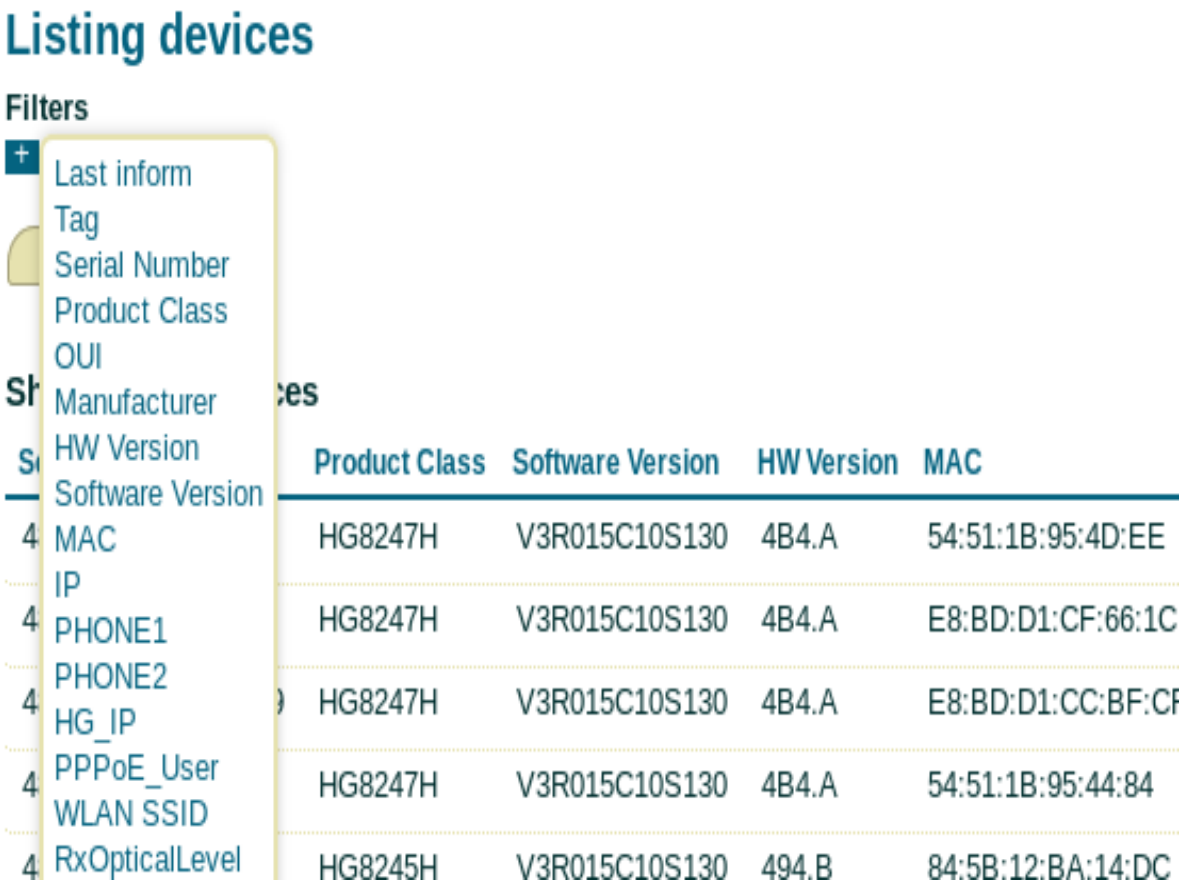

Figura 2.21 Interfaz de Usuario GenieACS [31]

➢ Funcionalidades y características.

- Cuenta con una comunidad de desarrollo muy amplia y documentación completa
- Soporte Comercial
- GenieACS permite el aprovisionamiento remoto de dispositivos
- Integración fácil de GenieACS por HTTP.
- Construido sobre Node.js y su base de datos es MongoDB.

Con el fin de tener una visión amplia y comparativa de cada una de las opciones planteadas se presenta en la Tabla 2.8 un cuadro puntualizando las diferencias en sus características.

Tabla 2.8 Características de los ACS

Característica	AXIROS	AVsystem	EASYCWMP	Friendly Technologies	GenieACS
Gratuidad	✗	✗	✓	✗	✓
Código abierto	✗	✗	✓	✗	✓
Personalizable	✓	✓	✗	✓	✓
Soporte SNMP	✓	✓	✗	✓	✓
Soporte TR-069	✓	✓	✓	✓	✓
Soporte para múltiples protocolos	✓	✓	✗	✓	✓
Interfaz de usuario amigable	✓	✓	✗	✓	✓
Escalabilidad	✓	✓	✗	✓	✓
Soporte HTTP	✓	✓	✓	✓	✓
Soporte SSH	✓	✓	✗	✓	✓
Soporte SSL	✓	✓	✓	✓	✓
Soporte SNMPv3	✓	✓	✓	✓	✓
Encriptación	✓	✓	✓	✓	✓
Soporte para múltiples dispositivos	✓	✓	✗	✓	✓
Integración por API RESTful	✓	✓	✓	✓	✓
Integración por API SOAP	✓	✓	✗	✗	✗
Soporte multilingüe	✓	✓	✗	✓	✓
Base de datos Propia	✓	✓	✗	✓	✗
Base de datos Externa	✓	✓	✓	✓	✓

De acuerdo a la comparación de características, se puede considerar que las herramientas de AXIROS y AVSystem son las más completas en términos de seguridad y compatibilidad con distintos protocolos de gestión. Estas herramientas ofrecen numerosas soluciones para los diferentes requisitos en el desarrollo de un proyecto. Sin embargo, al no ser de código abierto, pueden presentar dificultades de adaptabilidad para satisfacer necesidades específicas. En estos casos, es necesario recurrir a pagos por suscripción de soporte para solventar dichas necesidades. Esta dependencia de pagos puede constituir una limitación al momento de implementar cualquiera de estas dos herramientas en un proyecto de gestión de dispositivos.

Si lo que se requiere es una herramienta adaptable y personalizable desde la fuente para adecuarla a las necesidades particulares, se destaca la herramienta GenieACS. Aunque GenieACS soporta menos protocolos de gestión que AXIROS y AVSystem, se caracteriza por su alto rendimiento en el manejo de grandes volúmenes de dispositivos. Esto le permite destacarse frente a su competidor directo en la categoría open-source, EASYCWMP.

3 CAPÍTULO: DESCRIPCIÓN DE LA ARQUITECTURA FÍSICA Y LÓGICA DE LA RED FTTH/GPON DE LA EMPRESA TELCOFIBER S.A.S.

TELCOFIBER S.A.S. ofrece servicios de Internet banda ancha y televisión a través de su red de acceso FTTH, cada suscriptor necesita un enlace físico y lógico para acceder a los servicios, por lo que es muy importante conocer los equipos y entender sus funciones en todo el tendido de la red de acceso FTTH.

Toda la información presentada en este capítulo se basa en el conocimiento y experiencia obtenidos a través de múltiples sesiones de consulta con el Ingeniero encargado del diseño y ampliación de la red de acceso FTTH. Además, se han realizado recorridos detallados por todo el tendido de la red para comprender la función de cada equipo y se han mantenido sesiones regulares con el Ingeniero responsable de la gestión y administración de la red para profundizar en el proceso de prestación de servicios y el aprovisionamiento de los mismos. De esta manera, se ha logrado obtener un conocimiento completo de los equipos y su función dentro de la red de la Empresa TELCOFIBER S.A.S.

Para una mejor comprensión, se describirá primero la parte física de la red FTTH/GPON, comenzando desde los equipos presentes en la oficina central, la fibra, splitters, CPE, entre otros. Con todo este conocimiento adquirido, se procederá a describir la arquitectura lógica, presentando así cómo se realiza la transmisión de datos a través de la red FTTH/GPON de la empresa TELCOFIBER S.A.S.

3.1 Arquitectura Física

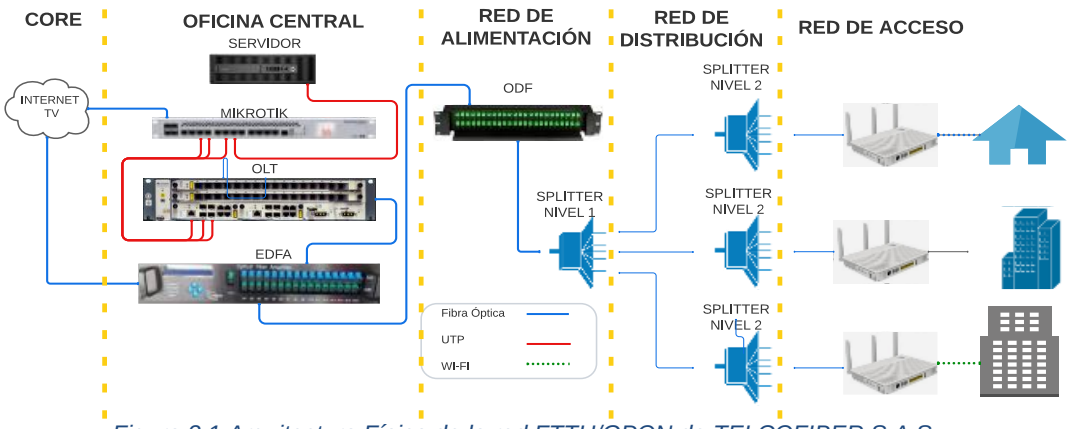

Figura 3.1 Arquitectura Física de la red FTTH/GPON de TELCOFIBER S.A.S.

La descripción de la arquitectura física de la red FTTH/GPON de la Empresa TELCOFIBER S.A.S. se enfoca en los elementos necesarios para brindar servicios de Internet y TV a los usuarios. Para entender mejor esta arquitectura, se divide en cinco áreas, las cuales se mantendrán vigentes en el futuro a pesar del crecimiento constante de la empresa. Como se muestra en la Figura 3.1, el despliegue de ampliaciones sigue el mismo patrón que se ha utilizado en todo el tendido de la red de acceso FTTH.

Los equipos se agrupan por áreas de la red y se describen en orden desde la recepción de la fibra del proveedor de primer nivel de Internet y TV en la oficina central, hasta la ONT en el área del usuario, pasando por todos los splitters necesarios y los elementos generales que se instalan en las calles. Esta descripción detallada permitirá una mejor comprensión de la arquitectura física de la red FTTH/GPON de TELCOFIBER S.A.S. y su funcionamiento en la prestación de servicios de Internet y TV a los usuarios finales.

3.1.1 Oficina Central (Nodo)

Se toma desde el CORE hasta el ODF porque éstos se encuentran ubicados dentro de la oficina central como se ve en la Figura 3.2.

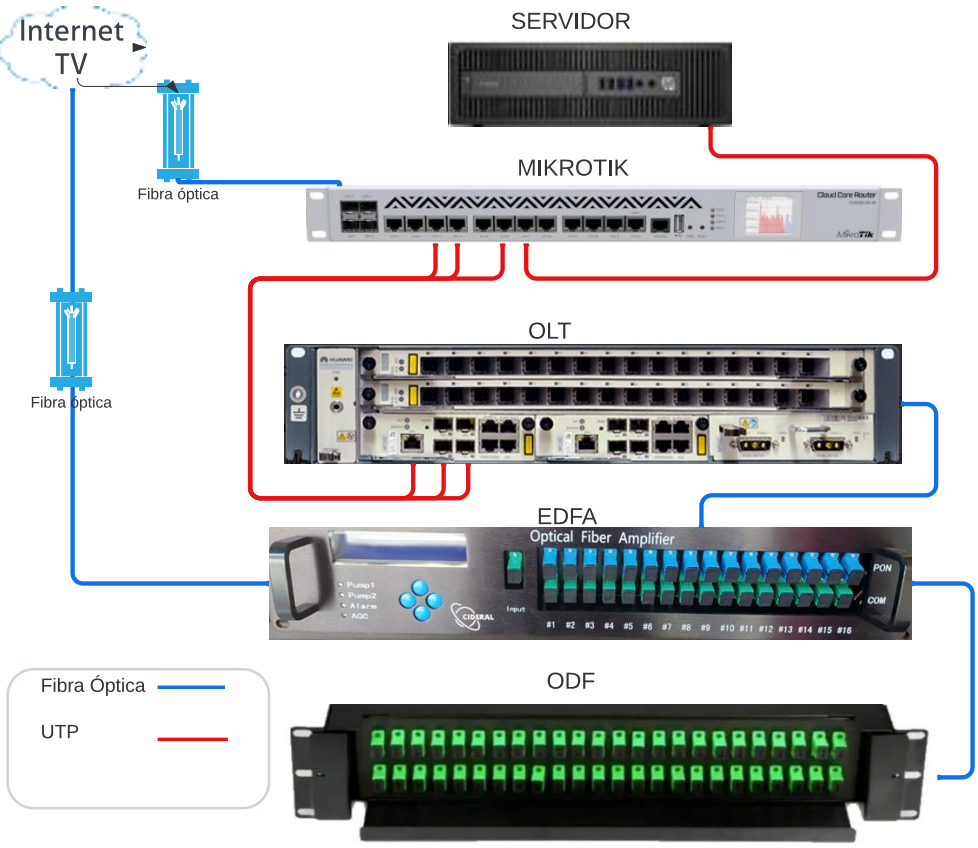

Figura 3.2 Equipos presentes en la oficina central

En la Figura 3.2 se observa que del proveedor de primer nivel llegan dos hilos de fibra: uno destinado al servicio de Internet que se conecta directamente al Mikrotik y otro para el servicio de televisión que se conecta al EDFA.

- **Mikrotik CCR1036-12G-4S:** Es un enrutador de alta gama que cumple una función crucial en la red de acceso FTTH/GPON de TELCOFIBER S.A.S. Con 36 núcleos a 1.2GHz y una memoria RAM de 4 GB, este dispositivo es capaz de procesar grandes cantidades de datos en tiempo real. Además, cuenta con una pantalla para lectura de temperatura, un puerto USB y un puerto RJ45 de consola, lo que facilita su configuración y mantenimiento.

Este enrutador posee 12 puertos Gigabit Ethernet y 4 puertos SFP, los cuales se utilizan para recibir el latiguillo de fibra proveniente del proveedor de primer nivel de Internet y televisión. En la Figura 3.3, se puede observar el recuadro rojo que indica la ubicación de estos puertos. Los puertos ETH 3, 4 y 6 se utilizan para conectar UTP hacia la OLT, mientras que el puerto ETH 7 se usa para conectar UTP hacia el servidor. De esta manera, el Mikrotik CCR1036-12G-4S cumple un rol fundamental en la recepción y distribución de los servicios de Internet y televisión en la red de acceso FTTH/GPON de TELCOFIBER S.A.S.

Figura 3.3 Mikrotic CCR

- **Hewlett Packard ProDesk:** Es un servidor que cuenta con un procesador i7 de séptima generación, 16GB de memoria RAM y un disco duro de 1Tera en estado sólido. Este servidor se conecta al Mikrotik mediante un puerto Ethernet.

- **OLT Huawei SmartAX 5608T:** Es un terminal utilizado por operadores de redes de telecomunicaciones GPON/EPON, como se muestra en la Figura 3.4. Esta OLT está equipada con un panel principal de control MA5608T GE/10G Uplink (MCUD1) que se encarga de la conmutación y agregación de servicios, así como de la gestión, configuración y control del dispositivo.

  El panel MDCU1 incluye dos puertos GE (GE0 y GE1), donde se conectan los UTP provenientes de los puertos ETH3 y ETH4 del Mikrotik, respectivamente, como se observa en el recuadro azul de la Figura 3.4. Además, cuenta con dos puertos GE/10GE y un puerto ETH, donde se conecta el UTP que proviene del puerto ETH6 del Mikrotik, como se indica en el recuadro verde de la Figura 3.4.

  El OLT también cuenta con el módulo de alimentación MPWD, señalado en el recuadro naranja, y dos tarjetas de servicio. La primera tarjeta, señalada con la flecha azul, es una placa de interfaz GPON GPFD de 16 puertos con módulo de encapsulación SFP B+/C+/C++, mientras que la segunda tarjeta, señalada con la flecha amarilla, es una tarjeta GPBD de 8 puertos con módulo de encapsulación SFP C+/C++.

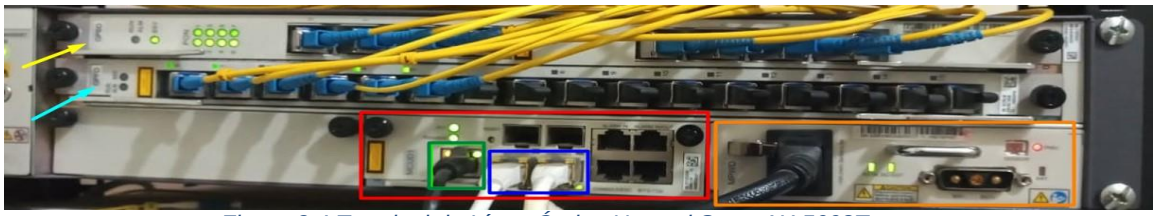

Figura 3.4 Terminal de Línea Óptico Huawei SmartAX 5608T

- **Tranceiver SFP**: Los transceptores SFP, como se muestran en la Figura 3.5, son módulos utilizados para modular y demodular señales ópticas. Su función en la recepción

de la señal es convertir la señal óptica en eléctrica, mientras que en la transmisión se encargan de convertir la señal eléctrica en óptica. Estos módulos son interfaces utilizadas en equipos de red, como se muestra en las tarjetas de la Figura 3.5, para conectar enlaces PON.

Figura 3.5 SFP Huawei

Existen tres tipos de módulos de encapsulación SFP que son bidireccionales, transmiten en la longitud de onda 1490 nm y reciben en la longitud de onda 1310 nm. Estos módulos utilizan un conector SC/UPC y tienen un alcance máximo de 20 km. En la tabla 3.1 se presentan las características principales de cada uno de estos módulos.

Tabla 3.1 Especificación SPF

Especificación	Mínima potencia óptica salida	Máxima potencia óptica salida	Sensibilidad máxima receptor	Potencia óptica de sobrecarga	Ratio de extinción
SFP tipo B+	1.5 dBm	5 dBm	-28 dBm	-8 dBm	8.2 dB
SFP tipo C+	3 dBm	7 dBm	-32 dBm	-12 dBm	8.2 dB
SFP tipo C++	6 dBm	10 dBm	-35 dBm	-15 dBm	8.2 dB

- **Amplificador de Fibra Dopada con Erbio (EDFA-*Erbium Doped Fiber Amplifier)* CIDERAL:** Es un Amplificador diseñado para operar en la banda de 1550 nm con un factor de ruido típico de 5 dB y proporcionar una ganancia de 22 dB. Este dispositivo se conecta a los hilos de fibra con conectores (SC/UPC) que están conectados a los puertos GPON de las tarjetas GPBD y GPFD presentes en la OLT, como se puede apreciar en la Figura 3.6.

Figura 3.6 EDFA

- **ODF**: Es el distribuidor de fibra óptica que se muestra en la Figura 3.7. Cuenta con 48 puertos para conectores SC/APC, donde se reciben los cables de fibra óptica conectados

a los puertos COM de conector SC/APC del EDFA. Además, cuenta con una bandeja de organización de hilos de fibra y empalmes.

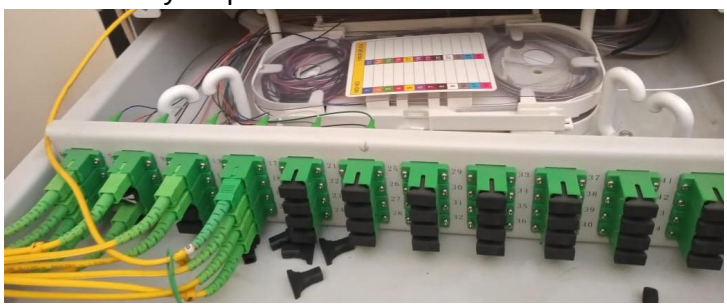

Figura 3.7 ODF

- **Patch Cord**: Este cable de fibra óptica tiene una longitud de 2 metros y su objetivo es la conexión óptica entre equipos de telecomunicaciones. En la Figura 3.8 se observan las tres combinaciones de patch cord que se utilizan y se diferencian por los conectores en los extremos, ya sean APC, UPC, LC o SC. Pueden ser dúplex o simplex, pero siempre bajo los estándares G652, G655 y G657 de la ITU. Esta última es la más usada en los últimos años en aplicaciones FTTH.

Figura 3.8 Patch Cord

3.1.2 RED de Alimentación

En esta área se encuentra el tramo del tendido de fibra de nivel uno que parte desde la bandeja de organización de fibra del ODF ver Figura 3.9 donde se empalma un pigtail con la fibra de nivel 1.

Figura 3.9 Bandeja de organización del ODF

TELCOFIBER ha desplegado un cable Todo Dieléctrico Auto Soportado (ADSS-*All Dielectric Self Supported*) de 24 hilos, modelo GYFXTY/ASU 24 FO, que cumple con el estándar

G.625.D de la ITU. Este cable está recubierto con aramida, gel y hilo de sangrado, y cuenta con tres buffers, cada uno de ellos con ocho hilos de fibra. La Figura 3.10 muestra cómo se ve este cable.

Figura 3.10 Cable de Fibra Óptica de 24 Hilos

Este tendido de primer nivel llega hasta un FDT conocido como mufla en el ámbito laboral. Este elemento de empalme horizontal, ubicación en una posición aérea, cuenta con un sistema de organización interior para adecuar y manipular los hilos de fibra óptica en sus cuatro cassetes de empalme, una válvula de presurización, cuatro puertos de entrada/salida de 2 cm y un oval para realizar sangría. Además, su cubierta exterior está fabricada con plástico rígido, lo que proporciona protección contra golpes, humedad y los rayos UV, como se observa en la Figura 3.11. Todo esto con el fin de garantizar la duración del empalme de fibra óptica en este caso con el splitter de primer nivel.

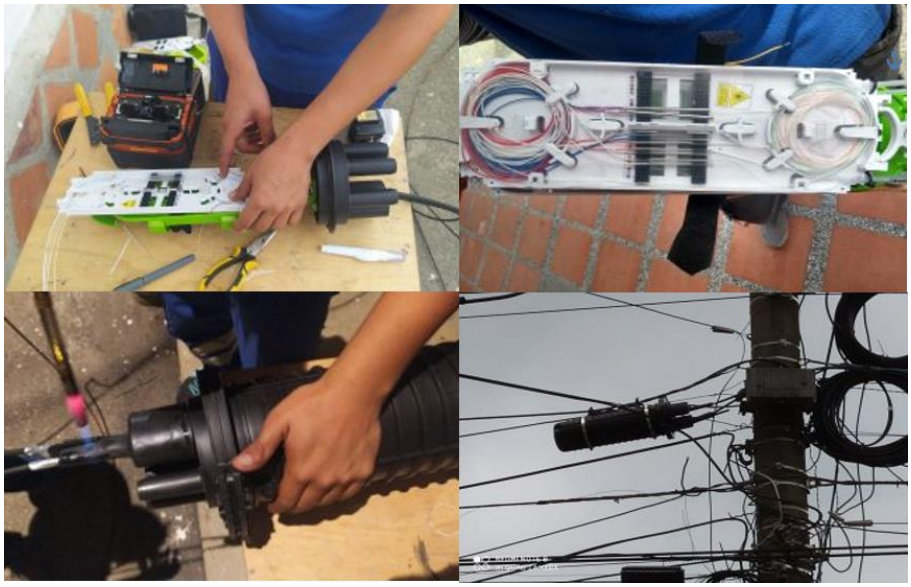

Figura 3.11 FDT o mufla

3.1.3 Red de distribución

Como se mencionó en el capítulo anterior, en este tramo de la red, los elementos pasivos llamados splitters toman el protagonismo, ya que por medio de ellos se realizan las ramificaciones para lograr que el tendido de la red pueda cubrir la mayor parte del territorio. Para esta parte del tendido de la red, se utilizan fibras ópticas de 6, 8 y 12 hilos que parten desde el FDT donde se encuentra el splitter principal, hasta los puntos en el municipio donde se ubican las FAT y se empalma al splitter de segundo nivel.

Los splitter de primer nivel utilizados en este tramo de la red pueden ser simétricos o asimétricos, y su uso depende estrictamente de los requerimientos en el diseño de la ramificación de la red FTTH.

En la Figura 3.12 se observa un splitter simétrico, en el cual ingresa una fibra y pueden salir varias fibras, todas con el mismo nivel de potencia. Su relación de división es de 1:N, donde N puede tomar valores de 2, 4, 8, 16.

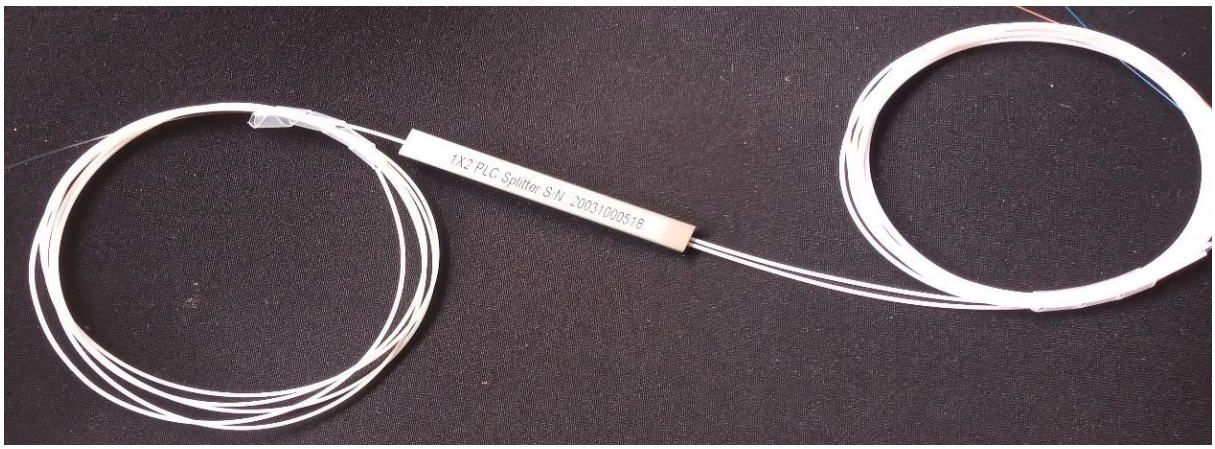

Figura 3.12 Splitter Simétrico

Los splitter asimétricos que se usan tienen una relación de división 1:2 pero la potencia de la señal óptica en sus dos salidas tiene un porcentaje diferente, generalmente esta potencia es distribuida en porcentajes de 90/10, 80/20, 70/30, y 60/40. Estos splitter se utilizan en cascada dentro de los FDT para las ramificaciones como se muestra en la Figura 3.13.

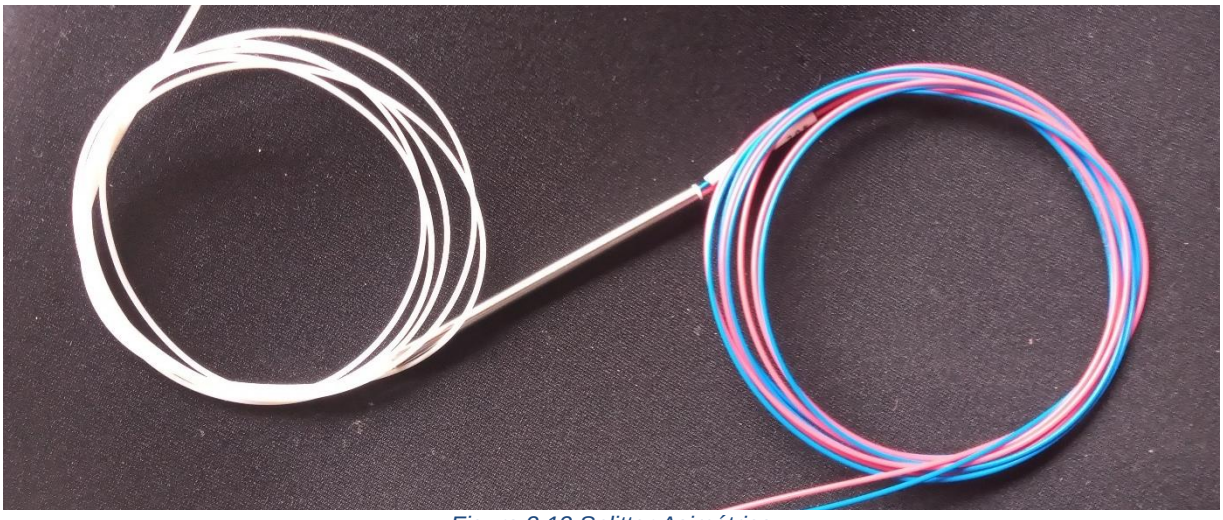

Figura 3.13 Splitter Asimétrico

La fibra FiberHome de 6, 8, y 12 hilos es monomodo y son todos cables ADSS. TELCOFIBER S.A.S. utiliza estos cables para su red FTTH debido a su alta capacidad para resistir tensión, ya que cuentan con Polímeros Reforzados con Fibras (FRP-*Fiber Reinforced Polymers*). Esta estructura interna determina la fuerza de tracción y, por ende, la distancia máxima que puede soportar el cable, conocida como span. En esta estructura están presentes los buffer,

que son contenedores para encapsular varios hilos de fibra óptica con el fin de proteger e identificarlos. También se incluye un hilo de sangrado, cuya función es permitir abrir el cable sin romper las fibras y así manipular solo el hilo que se necesita, reduciendo así el número de empalmes en la red como se puede ver en la Figura 3.14.

Figura 3.14 Fibra FiberHome

En la Tabla 3.2, se presentan las características de las fibras utilizadas en todo el tendido de la red de distribución incluyendo la de primer nivel de la red troncal de la empresa TELCOFIBER S.A.S.

Tabla 3.2 Características de la Fibra

Fibra	ITU-T	Span	Buffer	FRP	Hilo de sangrado
GYFXTY / ASU 6 FO	G.652.D	60m	1	2 de 1mm	Si
GYFXTY / ASU 8 FO	G.652.D	60m	2	2 de 1 mm	Si
GYFXTY / ASU 12 FO	G.652.D	100m	1	2 de 1.8mm	Si
GYFXTY / ASU 24 FO	G.652.D	200m	2	2 de 3 mm	Si

3.1.4 RED DE ACCESO

Este tendido de la red FTTH es en el que se llega hasta al interior de la residencia del usuario donde se conecta al CPE en este caso una ONT a través de una fibra de tercer nivel llamada drop, el despliegue comienza desde el splitter de segundo nivel que está empalmado a la red de distribución dentro de una FAT y se ubica en los postes del municipio.

La FAT está equipada con una bandeja de organización de hilos de fibra y tiene la capacidad de soportar splitter de 8 y 16 hilos como se observa en la Figura 3.16, su material de construcción es de plástico rígido para protección contra los rayos UV y cuenta con el grado de protección IP66, este grado significa que es totalmente hermético al polvo y protege contra el contacto y el agua.

Figura 3.15 Interior y cubierta Exterior de una FAT

En el interior de la Fat se encuentra un splitter de segundo nivel simétrico cuya relación de división es de 1:N, donde N puede tomar valores de 4, 8, y 16. La principal diferencia con el splitter simétrico de primer nivel es que estos cuentan en sus salidas con un conector SC/APC como se ve en la Figura 3. 16.

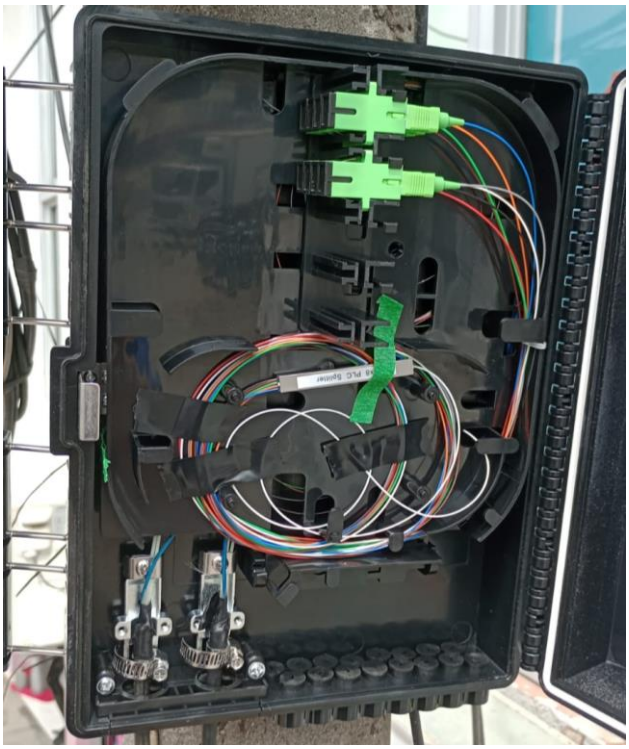

Figura 3.16 Splitter de segundo nivel ubicado dentro de la FAT

El splitter de segundo nivel simétrico se conecta a un pigtail de conector SC/APC, que a su vez se empalma con la fibra óptica Drop de tercer nivel. Esta conexión se organiza en la bandeja de la FAT, como se muestra en la Figura 3.15. Es importante tener en cuenta que en este punto se conectan directamente todas las fibras de cada usuario, por lo que la densidad de hilos de fibra puede ser bastante grande. Esto puede causar estrés en la fibra, lo que aumenta la pérdida de potencia y puede impedir que se establezca el servicio correctamente. Por lo tanto, la organización adecuada en la bandeja es crucial para garantizar un servicio óptimo.

La fibra Drop de tercer nivel es un cable monomodo que transporta un solo hilo de fibra óptica. Este cable es utilizado en instalaciones residenciales debido a su flexibilidad y su capacidad de soportar curvaturas agudas sin afectar el rendimiento óptico. Además, cuenta con un alambre galvanizado llamado mensajero de 1.2mm, el cual tiene como objetivo soportar la tensión a la que pueda ser sometido y evitar la fractura del hilo de fibra óptica. Al igual que las fibras utilizadas en las áreas anteriores, cuenta con las mismas características de los cables ADSS, tales como resistencia a la tracción y protección contra los agentes ambientales. La Figura 3.16 muestra un ejemplo de la estructura de un cable Drop de tercer nivel.

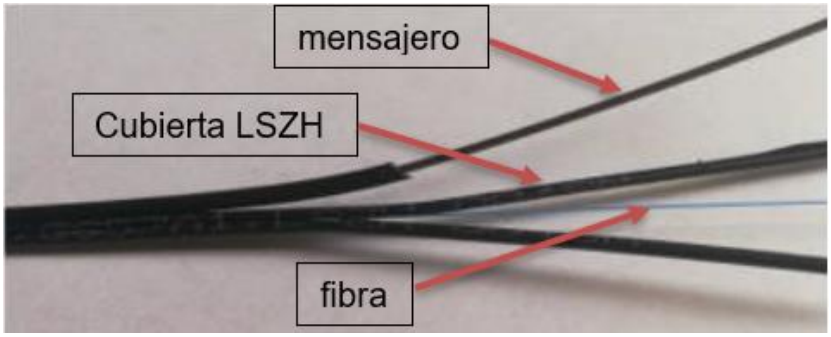

Figura 3.17 Fibra DROP de un solo hilo

Para concluir, en el extremo de la fibra Drop de tercer nivel se realiza un empalme con un pigtail SC/APC, el cual se conecta a la ONT. Normalmente, se manejan dos modelos de ONT de la marca Huawei, aunque en un porcentaje menor también se utiliza el modelo de la marca ZTE. En la tabla siguiente se presentan los diferentes modelos de ONT y sus características.

Tabla 3.3 Modelos y Características de ONT

Modelo	Sensibilidad RX	Potencia TX
Huawei HG8546M	-34 dB	5 dB
Huawei EG8141A5	-34 dB	7 dB
ZTE ZXHN F663NV3A	-34 dB	7dB

La configuración de todos los parámetros en las ONT que se manejan es la misma y se realiza mediante la interfaz web de la ONT, a la que se accede a través de la dirección IP de la puerta de enlace. En el caso de Huawei, la dirección IP es 192.168.100.1, y el nombre de usuario y la contraseña pueden variar según el fabricante. En las Figuras (3.18-3.21) se muestra un ejemplo de configuración de una ONT Huawei HS8545M5. El proceso comienza

con la verificación de los parámetros ópticos, seguido de la configuración de WAN, la activación de los puertos LAN y, por último, la configuración del nombre de usuario y la contraseña para la red Wi-Fi.

Figura 3.18 Parámetros ópticos

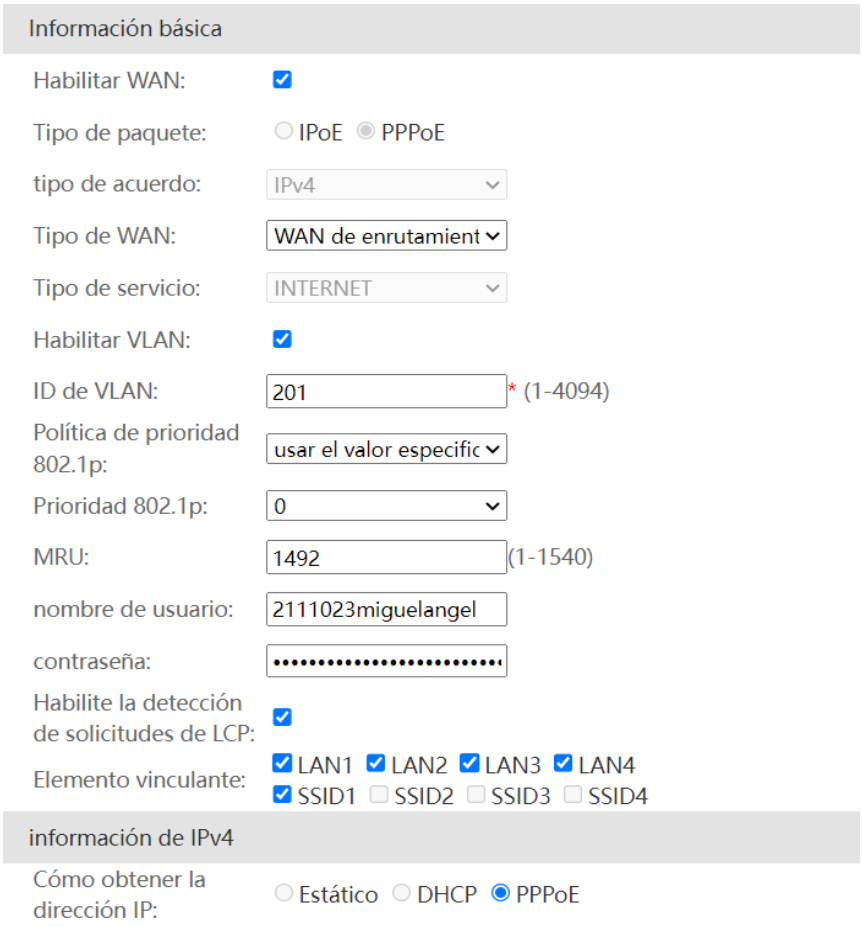

Figura 3.21 Configuración de WAN

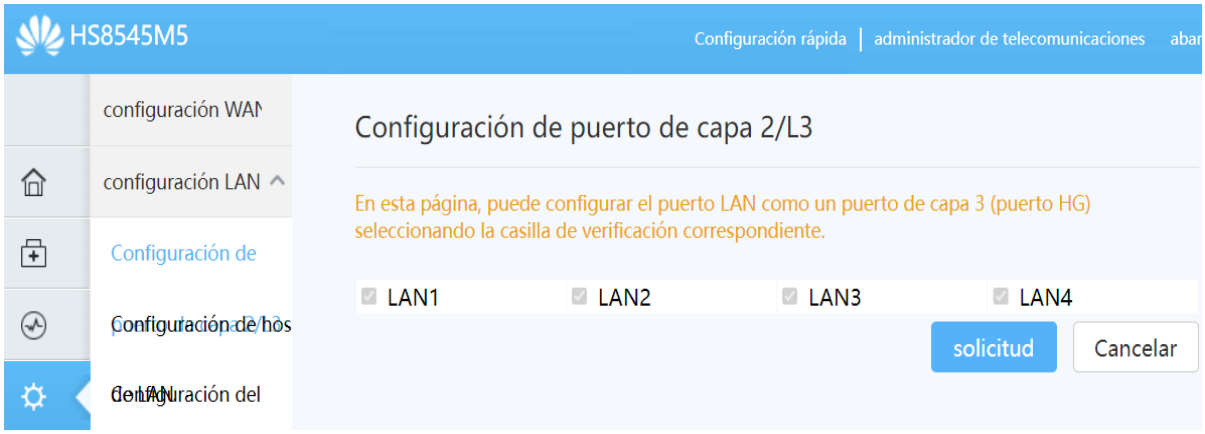

Figura 3.22 Activación de Puertos LAN

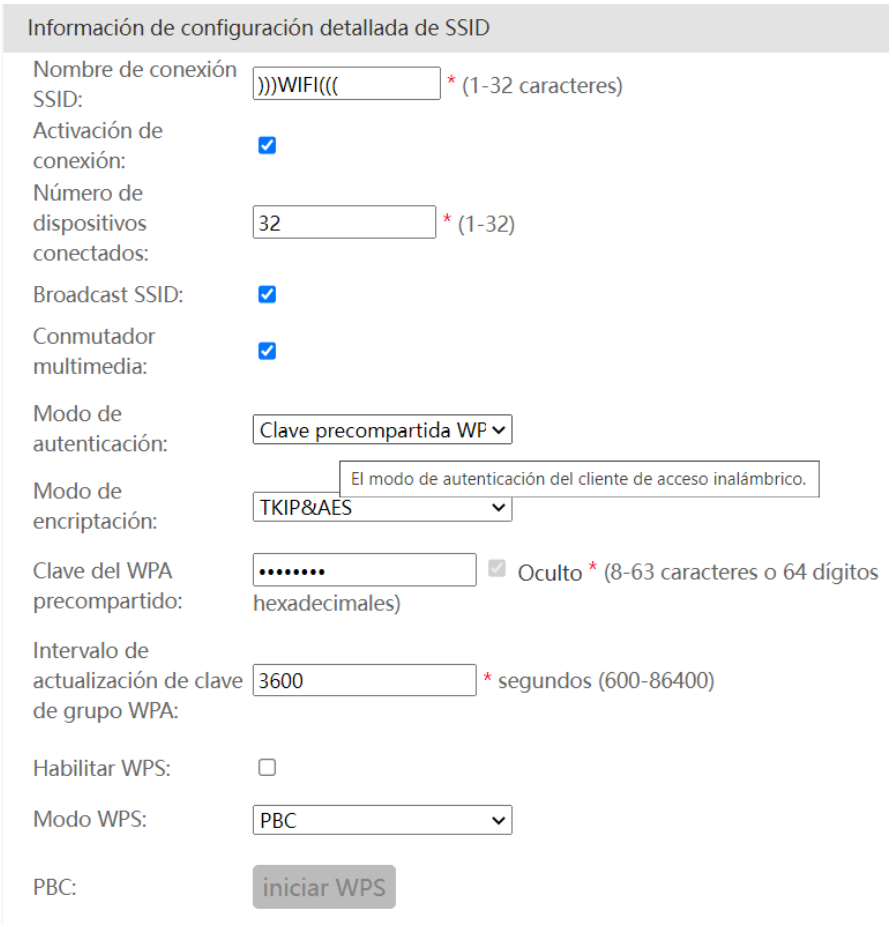

Figura 3.23 Habilitación y configuración de la red Wi-Fi

Ninguna de las ONT actualmente en uso cuenta con puerto CATV. Para proporcionar el servicio de televisión en instalaciones que lo requieren, se utiliza un dispositivo llamado mini nodo, que separa el canal de 1550nm, como se muestra en la Figura 3.2. Este dispositivo recibe el enlace en el puerto SC/APC y lo emite en el puerto SC/UPC, al cual se conecta un patch cord que va directamente a la ONT. Por último, el cable coaxial se conecta directamente al televisor.

Figura 3.24 Mini Nodo

3.1.5 Funcionamiento de la red FTTH desde el proveedor hasta la ONT.

En esta sección se describe el funcionamiento de los equipos en la oficina central, comenzando por el Mikrotik. El Mikrotik es donde se realiza la recepción de la fibra óptica de un canal dedicado del ISP principal por uno de los puertos SFP. Es un router de clase 6 que trabaja en la capa 3, al cual se accede a través de una aplicación llamada winbox, como se muestra en la Figura 3.23. A través de esta interfaz, se realizan múltiples configuraciones, incluyendo firewall, routing, MPLS, VPN, HotSpot, QoS, DHCP, NAT, balanceo de tráfico, balanceo de cargas, proxy, queue y backup.

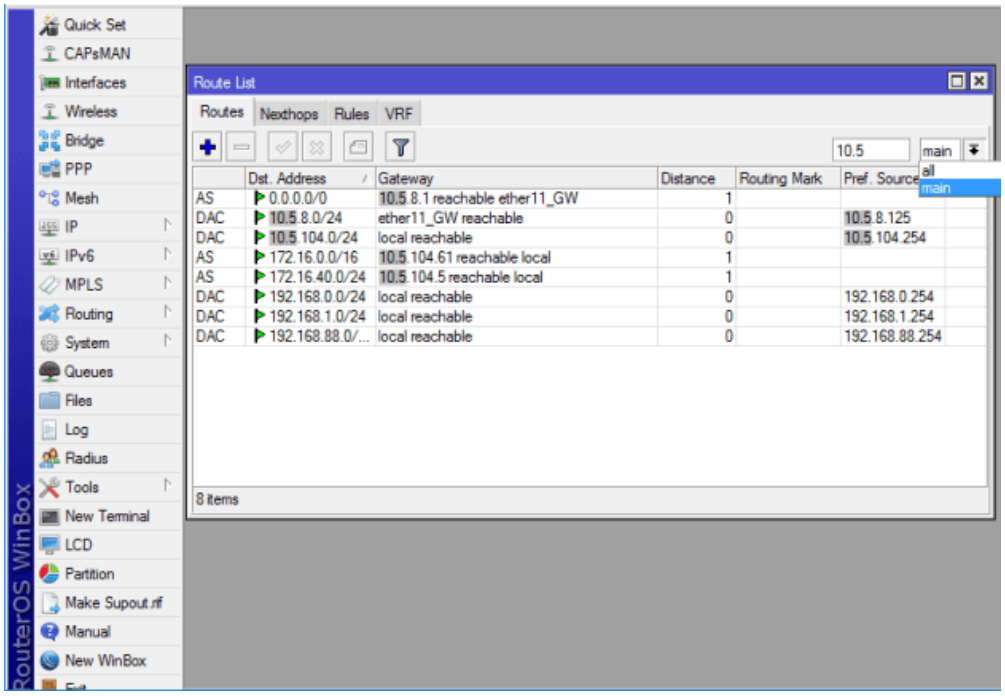

Figura 3.25 Interfaz de Winbox

Luego, se conecta el Mikrotik a la OLT mediante un cable UTP desde los puertos 1G/ETH en configuración de agregados. A continuación, se describen las configuraciones que se realizan en este dispositivo:

- Se configura los servicios y parámetros de red necesarios para establecer un enlace directo con el Mikrotik.

- Se crean y configuran las VLAN 101, 201, 301, 302, 303, 304, 305, 518 y 3967. La VLAN 101 se utiliza para la gestión de ONT, la 201 para dar salida a Internet al servicio Banda Ancha, las VLAN 301 a 305 son para los usuarios con canales de servicio dedicado, y las VLAN 518 y 3967 son para los proveedores de primer nivel contratados por la empresa.

- Se realiza el direccionamiento para establecer las IP privadas que se asignan a los usuarios para la autenticación por PPPoE en el Router Mikrotik.

- Se crean los perfiles con el ancho de banda que se le entrega al usuario.

- Se realiza el aprovisionamiento de ONT.

- Se puede verificar parámetros de las ONT.

Estas configuraciones permiten el establecimiento y la gestión de la red de fibra óptica desde la oficina central.

```
TELCOFIBER(config)#display ont info by-sn 4857544322B86F9E
  ------------------------------------------------------------
  F/S/P                   : 0/1/0
  ONT-ID                  : 13
  Control flag            : active
  Run state               : online
  Config state            : normal
  Match state             : match
  DBA type                : SR
  ONT distance(m)         : 1723
  ONT battery state       : not support
  Memory occupation       : 41%
  CPU occupation          : 1%
  Temperature             : 57(C)
  Authentic type          : SN-auth
  SN                      : 4857544322B86F9E (HWTC-22B86F9E)
  Management mode         : OMCI
  Software work mode      : normal
  Isolation state         : normal
  ONT IP 0 address/mask   : 172.16.50.3/24
  Description             : 2111023miguelangel
  Last down cause         : dying-gasp
  Last up time            : 2023-03-20 08:40:29+08:00
  Last down time          : 2023-03-20 08:37:09+08:00
---- More ( Press 'Q' to break ) ----
```

Figura 3.27 Parámetros de Potencia Óptica Proporcionados por la OLT

El servidor cuenta con un software de virtualización de servidores llamado Citrix Hypervisor, en el cual se alojan dos máquinas virtuales que utilizan el sistema operativo open source CentOS8. En la primera máquina virtual se ha instalado un servidor Radius, mientras que en la segunda se encuentra el sistema de monitoreo Cactic.

A continuación, se describirá el trayecto que sigue la señal óptica desde la OLT hasta la ONT en los hogares de los usuarios. Es importante tener en cuenta que en la OLT se dispone de dos tarjetas de interfaz GPON: una de 8 puertos y otra de 16, para un total de 24 puertos GPON, de los cuales actualmente se utilizan 12. Cada puerto dispone de su módulo SFP, del cual la señal sale con una potencia de +6 dB. Se ha diseñado la red de forma que siempre se respete el límite de potencia de los receptores en las ONT.

En primer lugar, se detallará el camino que sigue la señal óptica a través de los splitters en la red hasta llegar al hogar del usuario. Posteriormente, se realizará el cálculo del splitting y las pérdidas por inserción para verificar el diseño de la red FTTH.

En la Figura 3.25 se puede observar el mapa de distribución de la red en el territorio urbano de Santander de Quilichao, incluyendo la ubicación de los splitters de primer y segundo nivel, y la conexión entre la OLT y el EDFA. La línea punteada indica que la mayoría de los puertos van directamente hasta el ODF, ya que el servicio de TV es nuevo y se está migrando paulatinamente.

Figura 3.28 Distribución de la Red Física en el Territorio de Santander de Quilichao

En primer lugar, el enlace entre la OLT y el ODF es directo, sin requerir ningún tipo de splitting. El recorrido de primer nivel abarca aproximadamente 40 metros de fibra óptica en tendido aéreo desde el puerto del ODF hasta el splitter principal de 1:8 simétrico.

La red FTTH se diseñó de manera desbalanceada, lo que implica que uno de los ocho hilos que salen del splitter principal se utiliza para realizar una red en cascada de splitter desbalanceados, cuya relación de splitting es progresiva. En consecuencia, se efectúa un empalme entre el hilo número 1 (azul) del splitter principal y un splitter 1:2 desbalanceado con una relación de splitting de 20/80. A su vez, la salida número 1 de este splitter, que lleva el 20% de la potencia de la señal, se empalma con el splitter de segundo nivel de 1:8 simétrico con conector SC/APC, que se ubica en la FAT, para finalmente conectarse a los usuarios en cada uno de estos puertos.

En el Hilo número 2 del splitter 20/80, donde se encuentra el 80% de la potencia de la señal, se conecta un splitter 30/70. Al igual que en el caso anterior, en el hilo número 1 que lleva el 30% de la potencia, se empalma un splitter de segundo nivel 1:8. Finalmente, en el hilo número 2 que tiene el 70% de la potencia, se conecta un splitter simétrico 1:2 con relación de splitting 50/50. A cada uno de estos hilos se les empalma un splitter simétrico 1:8 de segundo nivel. Cabe aclarar que, en algunos casos donde las pérdidas por inserción de distancia no son altas, se puede ampliar la cascada con un splitter 40/60 justo después de usar el 30/70.

Se destaca que el procedimiento descrito anteriormente se realiza para cada puerto activo en la OLT. Además, se menciona que se puede llegar a un máximo de 128 usuarios por puerto GPON de la OLT.

Es de suma importancia tener en cuenta las pérdidas por inserción en el tendido de la red de fibra desde la OLT hasta el usuario final, para evitar superar los límites de sensibilidad de RX de las ONT y lograr que una ONT se enganche al enlace físico. "Enganche" es un término técnico que se utiliza para determinar el éxito del enlace físico, el cual ocurre cuando la potencia se mantiene por debajo del límite. En cada SFP que se encuentra en los puertos GPON, la potencia de la señal es de +6 dB, y a este valor se le deben restar todas las pérdidas por inserción mencionadas en la Tabla 3.4.

Tabla 3.4 Pérdidas por inserción en el diseño de la red FTTH/GPON

COMPONENTES DE RED	CANTIDAD	PÉRDIDA [dB]
Patch cord SC/APC – SC/UPC	1	0.3
Pigtail SC/APC	2	0.3
Splitter 1:8 Primer Nivel Simétrico	1	10.29
Splitter 1:2 20/80 desbalanceado	1	7.11/1.04
Splitter 1:2 30/70 desbalanceado	1	5.63/1.87
Splitter 1:2 50/50 Simétrico	1	3.6/3.6
Empalmes	6	0.02
Fibra monomodo	KM	0.3
Splitter 1:8 Segundo nivel Simétrico	1	10.29
Pigtail SC/UPC	1	0.3

Si se tiene el primer caso donde se utiliza sólo el primer splitter 20/80 de la cascada para conectar el splitter de segundo nivel y luego los usuarios, se tendría una potencia en la ONT.

$$P_{RX} = 6 - (0.3 \times 4) - (10.29 \times 2) - 7.11 - 0.12 = \ -23.01dB \ \pm pérdidas\ por\ distancia$$

Y en el caso donde se usa la cascada completa quedaría de la siguiente manera:

$$P_{RX} = 6 - (0.3 \times 4) - (10.29 \times 2) - 1.04 - 1.87 - 3.6 - 0.20 = \ -22.53dB \ \pm pérdidas\ por\ km$$

En un entorno real, el valor de las pérdidas por inserción puede oscilar entre 22 dB y 28 dB, y estas variaciones son generadas por diferentes factores. Entre ellos, se encuentran el fenómeno de reflexión, la distancia del enlace, la cantidad de empalmes y su calidad, la calidad de la fibra óptica, la calidad de los splitters y las impurezas en los conectores.

Es importante tener en cuenta estos factores para evitar que las pérdidas por inserción superen los límites permitidos y así garantizar un enlace óptimo. Además, es recomendable realizar mediciones periódicas para detectar posibles problemas y corregirlos a tiempo.

Si la ONT recibe la potencia óptima, se realizará el enganche de inmediato, y la ONT estará lista para ser aprovisionada y brindar acceso a Internet. Durante este proceso, se debe asignar al usuario una dirección IP privada mediante el protocolo DHCP. Además, se realiza una Traducción de Direcciones de Red (NAT-*Network Address Translation*) para permitir que los usuarios de banda ancha accedan a Internet a través de una dirección IP pública proporcionada por el proveedor internacional de servicios de Internet.

Es importante tener en cuenta que, además de las direcciones IP públicas utilizadas para brindar acceso a Internet a los usuarios de banda ancha, también se tienen direcciones IP públicas configuradas para dar salida a Internet a los usuarios que tienen contratado un canal dedicado. En este caso, la asignación de direcciones IP públicas se realiza de manera diferente, pero el objetivo es el mismo: permitir que los usuarios accedan a Internet a través de una conexión de alta velocidad y confiable.

3.2 Arquitectura Lógica

El objetivo de describir esta arquitectura es brindar una comprensión detallada de la función que cumplen los dispositivos pasivos y activos en el proceso de envío y recepción de datos de los usuarios de la red FTTH/GPON de TELCOFIBER S.A.S. Para lograr esto, se presenta en la Figura 3.26 el diagrama de la arquitectura lógica de la red FTTH/GPON.

La figura proporcionará una vista general de la red, lo que permitirá a los usuarios entender cómo se conectan los diferentes elementos y cómo se lleva a cabo el proceso de envío y recepción de datos. Al comprender la arquitectura de la red, los usuarios podrán identificar y solucionar problemas de manera más efectiva y optimizar el rendimiento de su conexión. En resumen, la descripción de esta arquitectura es esencial para garantizar una experiencia de usuario satisfactoria en la red FTTH/GPON de TELCOFIBER S.A.S.

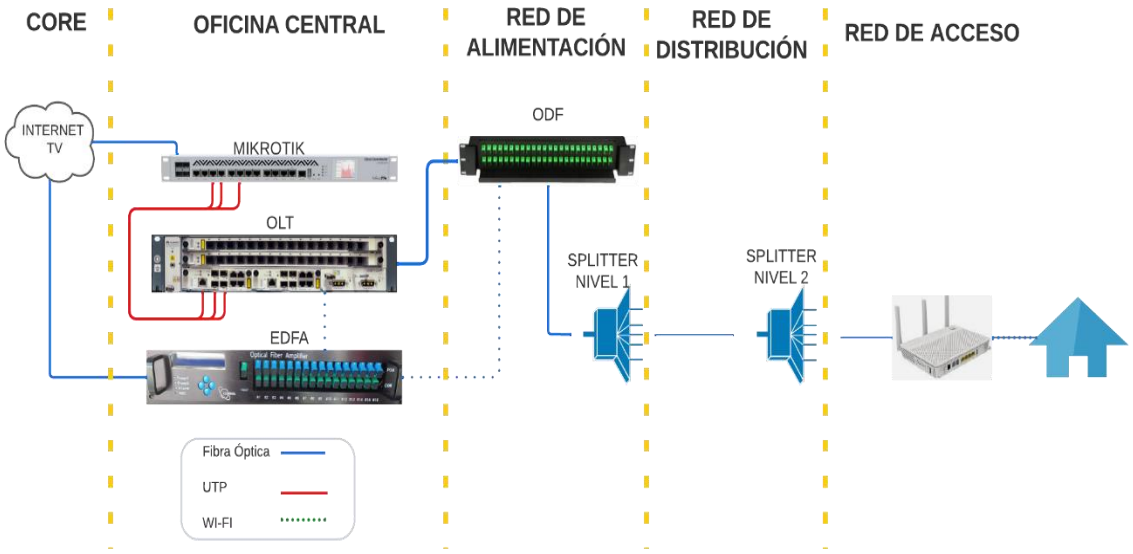

Figura 3.29 Arquitectura Lógica de la Red FTTH/GPON de la Empresa TELCOFIBER S.A.S

Como se puede observar en la Figura 3.26, la conexión entre la OLT, el EDFA y el ODF se indica con una línea punteada. Esto se debe a que el EDFA solo amplifica y combina la longitud de onda de 1550 nm utilizada por la señal de TV, con las longitudes de onda de 1490 nm del enlace descendente y 1310 nm del enlace ascendente. De esta manera, el EDFA asegura una transmisión eficiente de la señal a través de la red FTTH/GPON de TELCOFIBER S.A.S. Es importante destacar que la amplificación del EDFA es necesaria para garantizar una señal de calidad en el enlace descendente, ya que la señal se debilita a medida que se extiende por la red. En resumen, el uso del EDFA es esencial para asegurar un rendimiento óptimo en la red FTTH/GPON de TELCOFIBER S.A.S.

Lógica del enlace descendente: n una red FTTH/GPON implica la comunicación que se da desde la OLT hasta las ONT ubicadas en los hogares o empresas de los usuarios finales. Este proceso comienza con la asignación de un identificador único, que será la dirección MAC, y una dirección de grupo (GEM) por parte de la OLT.

La dirección MAC es un identificador único asignado a cada dispositivo de red, incluidas las ONT, para que puedan comunicarse en la red. La dirección GEM, por otro lado, se utiliza para identificar el servicio que se está transmitiendo a través de la red. Por ejemplo, puede ser una transmisión de video o una conexión de Internet.

Una vez asignadas las direcciones MAC y GEM, la OLT envía la señal óptica a través de la fibra óptica hasta la ONT correspondiente. La señal se divide en diferentes longitudes de onda utilizando la técnica de multiplexación por división de longitud de onda (WDM), lo que permite que varios servicios se transmitan a través de la misma fibra óptica.

En la ONT, la señal se desmultiplexa y se envía a los dispositivos del usuario final, como el router o el decodificador de TV, a través de los puertos Ethernet o de video correspondientes. Cada usuario final recibe su propia señal de longitud de onda dedicada para garantizar la privacidad y seguridad de los datos transmitidos.

Lógica del enlace ascendente: El enlace ascendente en la red FTTH/GPON es para la transmisión de datos desde los terminales de los usuarios en este caso ONT hasta la OLT ubicada en la oficina central.

El enlace ascendente es crucial para el acceso a Internet y otros posibles servicios de comunicaciones desde las ONT. Aquí se presenta paso a paso el camino que siguen los datos desde la ONT hasta la OLT.

I. Generación de datos: La información es generada por un dispositivo de usuario

II. Procesamiento a nivel de capa 2: Este procesamiento de nivel 2 se refiere a la jerarquía OSI donde la capa 2 se encarga de la transmisión de datos entre dispositivos dentro de una misma red local. En el caso de la red FTTH//GPON este procesamiento implica los protocolos siguientes:

- 802.1p: define una priorización de la transmisión de paquetes basada en la asignación de 8 bits de información de prioridad para cada paquete. Esta prioridad se utiliza para determinar el orden en el que los paquetes deben ser transmitidos en una red congestionada.
- 802.1Q: especifica un mecanismo de virtualización LAN, que permite segmentar una red LAN física en varias redes lógicas (VLANs) diferentes, cada una con su propia dirección MAC.
- 802.1ad: define un mecanismo para crear una VLAN doble (Q-in-Q), que permite que varios proveedores de servicios de red ofrezcan servicios separados en una sola red compartida.

Estos protocolos se utilizan para mejorar la eficiencia y gestionar tráfico Ethernet antes de su transmisión hacia la OLT.

III. Encriptación del tráfico: Este proceso se realiza para garantizar la seguridad y privacidad de los datos.

IV. Encapsulación de datos: Los paquetes de datos generados son encapsulados en una trama GEM para su transmisión en el enlace ascendente.

V. Configuración en T-CONT: En este paso se agrupan tramas GEM en T-CONT (colas) que es una estructura de datos que define la forma de agrupar paquetes de datos y les asigna un ancho de banda determinado para su transmisión a través de la red. La configuración de T-CONT en una red GPON incluye la asignación de un identificador único a cada T-CONT y la definición del ancho de banda requerido para cada uno de ellos. La OLT utiliza esta información para priorizar y controlar el tráfico de datos que fluye a través de la red hacia los terminales de usuario con el fin de mejorar la eficiencia de la transmisión.

VI. Mapa de Ancho de Banda (BWmap-Bandwidth Map): Esta herramienta utilizada en redes FTTH/GPON permite a la OLT gestionar y asignar los recursos de ancho de banda disponibles para cada terminal de usuario. Este mapa permite la asignación dinámica de

ancho de banda en función de las necesidades y usos de cada usuario, lo que permite asegurar una gestión eficiente de los recursos y un mejor rendimiento de la red. El Mapa de Ancho de Banda se actualiza regularmente a través de mensajes de Informe de Ancho de Banda Dinámico Ascendente (DRBu) que son enviados por las ONT a la OLT y con esto la OLT establece turnos a cada ONT para que pueda enviar los datos T-CONT.

VII. Transmisión a través del enlace: Las tramas GEM se envían en forma de ráfagas desde la ONT hasta la OLT haciendo su recorrido por los splitter de segundo y primer nivel pasando por el ODF.

VIII. Recepción de los datos: La OLT recibe las tramas GEM cuya carga útil contiene los las tramas Ethernet. Estas tramas son enviadas al mikrotik el cual hace el control de firewall y finaliza el proceso enrutando las tramas en la red del proveedor de primer nivel y puedan tener salida a Internet.

En la transmisión de datos en el enlace ascendente es esencial evitar la colisión de tramas para evitar la pérdida de datos y para esto se utiliza el protocolo de Control de Acceso al Medio (MAC-Media Access Control) y así poder controlar y coordinar la transmisión de paquetes de datos en el enlace ascendente. Este protocolo permite a la OLT evitar la colisión de paquetes de datos y garantizar la transmisión eficiente.

Se usa TDMA como protocolo MAC y funciona de la siguiente manera:

- División en tiempo: El ancho de banda disponible se divide en unidades de tiempo, por ejemplo, en slots o frames.
- Asignación de slots: Cada dispositivo de usuario se asigna uno o varios slots para transmitir sus paquetes de datos.
- Transmisión secuencial: Los dispositivos de usuario transmiten sus paquetes de datos secuencialmente, de acuerdo a su asignación de slots.
- Control de acceso: Cada dispositivo de usuario espera su turno para transmitir, basándose en la información sobre la asignación de slots, y sólo transmite sus paquetes de datos cuando le toca.
- Monitoreo: Se monitorea continuamente el uso de los slots y se realiza ajustes en la asignación de tiempo si es necesario para evitar la colisión de paquetes de datos.

La sincronización a la hora de asignar los slots es la clave para el éxito de TDMA y en este caso dicha sincronización se realiza con el método de ranging.

Este proceso sincroniza todas las ONT con la OLT; durante el proceso de ranging la OLT mide el tiempo de retorno de una señal enviada a los dispositivos de usuario y usa esta información para sincronizar la transmisión de datos.

En un sistema TDMA que utiliza el método de ranging, la OLT asigna un tiempo específico para que cada dispositivo de usuario realice su ranging. Durante este tiempo, cada dispositivo de usuario envía una señal a la OLT, y la OLT mide el tiempo de retorno de la señal. Con esta información, la OLT puede calcular la distancia aproximada del dispositivo de usuario y, en consecuencia, determinar cuándo deben iniciar y finalizar las transmisiones de datos.

El ranging permite una mejor sincronización entre los dispositivos de usuario y la OLT y, por lo tanto, permite una transmisión de datos más eficiente y confiable en un sistema TDMA.

4 CAPÍTULO: ESQUEMA DE ACS UTILIZANDO CWMP

Tener un esquema funcional del ACS que usa CWMP es importante porque permite comprender la arquitectura del sistema y cómo funcionan sus diferentes componentes, identificar y resolver problemas, planificar y escalar el sistema permitirá expandir los servicios y mejorar el rendimiento del sistema a medida que el ISP crece. Un esquema funcional detallado del sistema ACS puede ser utilizado como una herramienta de documentación para el personal del ISP, y también puede ser utilizado para capacitar a los nuevos empleados sobre el sistema. Esto ayudará al personal a comprender el sistema y a trabajar con él de manera más efectiva.

En este capítulo se analiza la infraestructura con la que cuenta la empresa para realizar el proyecto, se identifican las necesidades que se desean solventar y el alcance del proyecto, y con base a este análisis se elige la herramienta software que cumpla con los requisitos. Además, se describe cómo es el funcionamiento de esta herramienta con los equipos de la red.

De esta manera se obtiene un diseño de esquema funcional, que puede ser desplegado, es decir implementado para los CPE en la red y probado todas sus características para verificar que solventa las necesidades que presenta la empresa TELCOFIBER S.A.S

4.1 Diseño del Esquema ACS.

Para comenzar a diseñar el esquema ACS que utiliza CWMP, se inicia con el análisis de requisitos para tomar la decisión sobre la herramienta software ACS adecuada. En diferentes reuniones con los ingenieros de la empresa, se realizó un análisis exhaustivo de los requisitos para el diseño del sistema, teniendo en cuenta factores económicos y los recursos disponibles, tanto de hardware como de software. También se evaluaron las necesidades específicas del proceso de soporte y se identificaron las posibles soluciones para cubrirlas. Se establecieron los recursos necesarios, características y funcionalidades que debe tener el sistema, incluyendo su funcionamiento y escalabilidad, para satisfacer las necesidades de la empresa.

4.1.1 Análisis de requisitos.

Este análisis es producto de observación directa y entrevistas recurrentes con los ingenieros encargados de la planta externa e interna de la red y también con el equipo técnico de soporte para comprender el proceso de cómo se detecta y se da solución a las fallas, y qué se hace para evitar que estas fallas interrumpan la prestación de servicios nuevamente.

Las necesidades que se tienen en el proceso de soporte recaen principalmente en poder contar con un sistema de información eficiente para eliminar los supuestos a la hora de determinar la causa de una falla, poder realizar configuraciones necesarias en los momentos oportunos de manera remota a los dispositivos CPE y poder enviar actualizaciones de firmware

de ser requerido y así evitar pérdida deliberada de tiempo a la hora de dar solución en los procesos de soporte.

Teniendo en cuenta las necesidades identificadas en el proceso de soporte técnico en la empresa TELCOFIBER S.A.S., el sistema debe ser capaz de suplir todas estas necesidades. Para lograr esto, se definieron las siguientes funciones:

- El sistema debe realizar ping constante a los dispositivos.
- Debe consultar información relevante periódicamente al CPE.
- Debe ser capaz de modificar parámetros puntuales del CPE.
- Debe ser capaz de enviar archivos firmware para actualización de ser requerido.

Es importante que el sistema sea escalable, dado que TELCOFIBER S.A.S. tiene un gran potencial de crecimiento y se espera un aumento en el número de CPE conectados a la red. Por lo tanto, el sistema debe ser capaz de manejar grandes cantidades de dispositivos conectados sin presentar inconvenientes. Además, a medida que la empresa crece y se implementan nuevos servicios, se requerirá la gestión de una gama más amplia de dispositivos. Por último, el sistema debe ser compatible con software externo para mejorar la gestión general de la empresa.

Tabla 4.1 Requisitos funcionales y no funcionales

REQUISITOS FUNCIONALES	**DESCRIPCIÓN**
Registro de CPE	El ACS debe ser capaz de detectar los dispositivos en la red y registrarlos en su base datos a través del intercambio de mensajes “inform”.
Gestión y monitoreo de CPE	El ACS debe permitir la gestión y monitoreo de los dispositivos en la red FTTH que sean compatibles con el protocolo CWMP.
Detección y reporte de fallas en el servicio	El sistema tiene que detectar anomalías en diferentes parámetros ya sea de potencia óptica o consumo de recursos del CPE.
Configuración y actualización	El ACS debe permitir configurar o actualizar uno o varios parámetros de los CPE.
Políticas de seguridad	En el sistema ACS se debe poder implementar políticas de acceso para autenticar y autorizar solo al personal de la empresa que se encuentre capacitado.
Generación de reportes de estado y rendimiento	El sistema debe ser capaz de brindar reportes de estado con información valiosa del estado y rendimiento de todos los dispositivos que están registrados en el sistema.
Integración con software externo	El ACS debe ser capaz de realizar integraciones futuras con software externos que estén trabajando en la gestión y operación de la empresa.

REQUISITOS NO FUNCIONALES	
Disponibilidad	El sistema debe monitorear en tiempo real 24/7 todos los dispositivos registrados en él.
Escalabilidad	Debido a que la empresa crece constantemente el ACS debe soportar el incremento de los CPE sin sufrir fallas en su funcionamiento.
Seguridad	El tráfico de gestión contiene datos sensibles tanto de los usuarios como de la empresa por lo que es obligatorio separarlo de cualquier otro servicio.
Fiabilidad	El sistema debe funcionar de manera correcta para evitar interrupciones del servicio y evitar pérdidas de tiempo en la gestión de CPE.
Usabilidad	El funcionamiento del sistema debe ser fácil de aprender y comprender por parte del personal de la empresa.
Eficiencia	El ACS tiene que ser rápido en la ejecución de tareas para optimizar la gestión de los CPE.
Compatibilidad	El sistema como los CPE deben ser compatibles con el mismo protocolo de gestión y así poder ser registrados y administrados por la empresa.
Open-Source	El sistema debe permitir acceso al código fuente para ser adaptado a los intereses de la empresa.
Costo	El sistema debe ser libre de pagos por licencia, solo de soporte en caso de ser requerido.

4.1.2 Selección de la herramienta ACS.

Cada una de las herramientas vistas cuentan con una gran variedad de funcionalidades para realizar la gestión de dispositivos en la red, sin embargo AXESS desarrollado por AXIROS es la más completa, pues no solo soporta más protocolos de gestión, y su interfaz web es mucho más sofisticada si no que sus servicios en la nube para gestión más allá de tr-069 es mucho más amplia, sin embargo esta no se adapta a los requisitos solicitados ya que dos de ellos es sin costo de licencia y debe ser open-source, esto descarta las opciones AXEES, AVsystem y Friendly Technologies, dejando las únicas solo las opciones de EasyCwmp y GenieACS.

En este contexto, se destaca la herramienta GenieACS sobre EasyCwmp porque soporta más protocolos de gestión, a pesar de ser open source su personalización no es muy sencilla por lo que resultaría muy difícil su adaptación a las necesidades de la empresa, además, no está diseñada para soportar un gran volumen de dispositivos por lo que no sería una opción escalable y dejó de recibir actualizaciones desde el 2017, que a comparación de GenieACS su última versión la 1.2.9, fue lanzada el 22 de agosto de 2022.

Además, GenieACS cuenta con una API muy completa que permite su integración con software externo, lo que lo hace altamente escalable. Asimismo, su interfaz web es muy intuitiva, lo que facilita su uso y configuración.

4.1.3 Infraestructura de red con la que se cuenta para el proyecto.

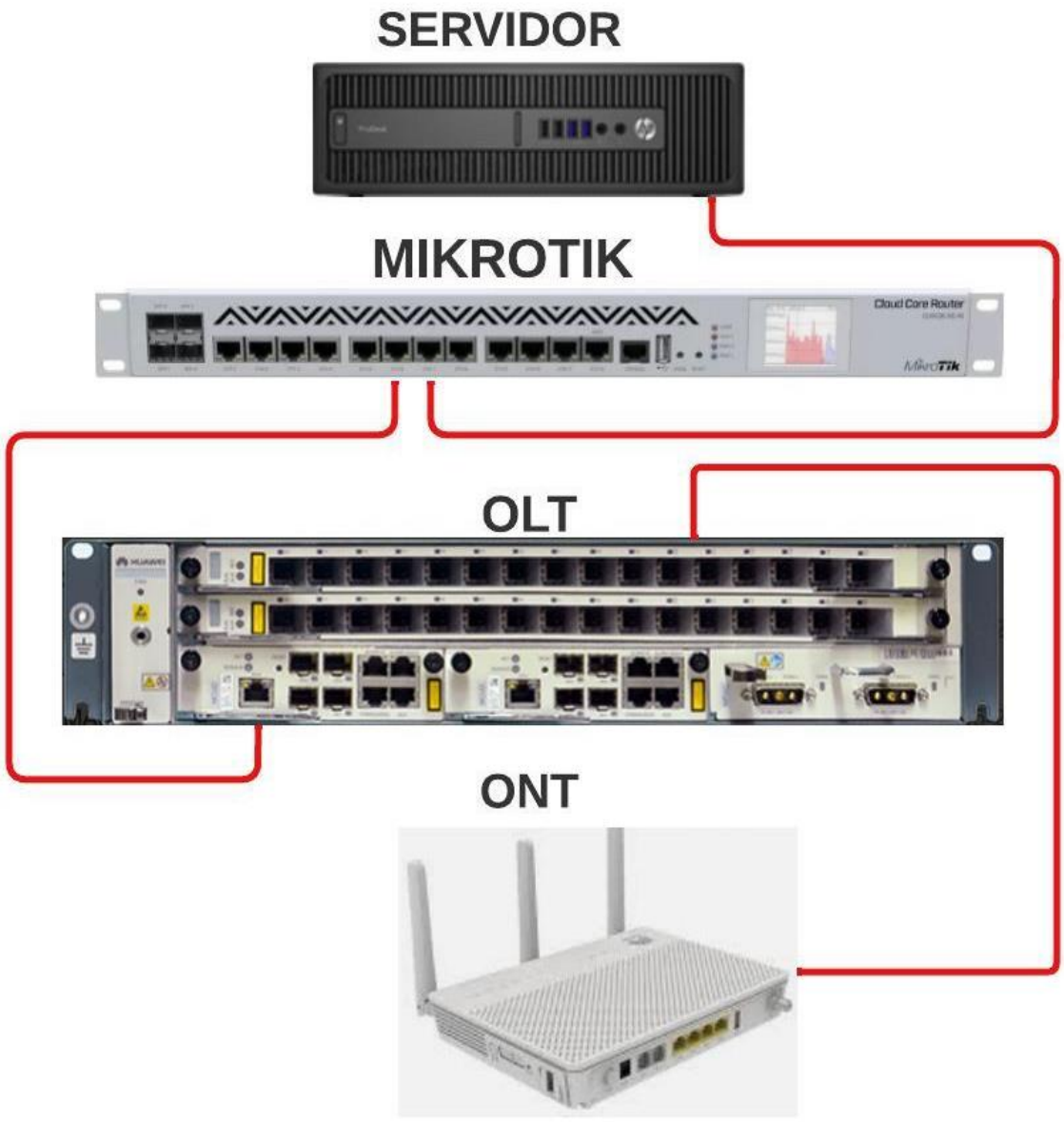

Figura 4.1 Infraestructura para el proyecto

En el servidor se encuentra instalado un Hipervisor Citrix, el cual permite alojar máquinas virtuales y asignar los recursos necesarios para su funcionamiento. En la Figura 4.2 se muestra una imagen de la máquina virtual en actividad dentro de Citrix, donde se pueden observar los recursos asignados resaltados en los recuadros rojos.

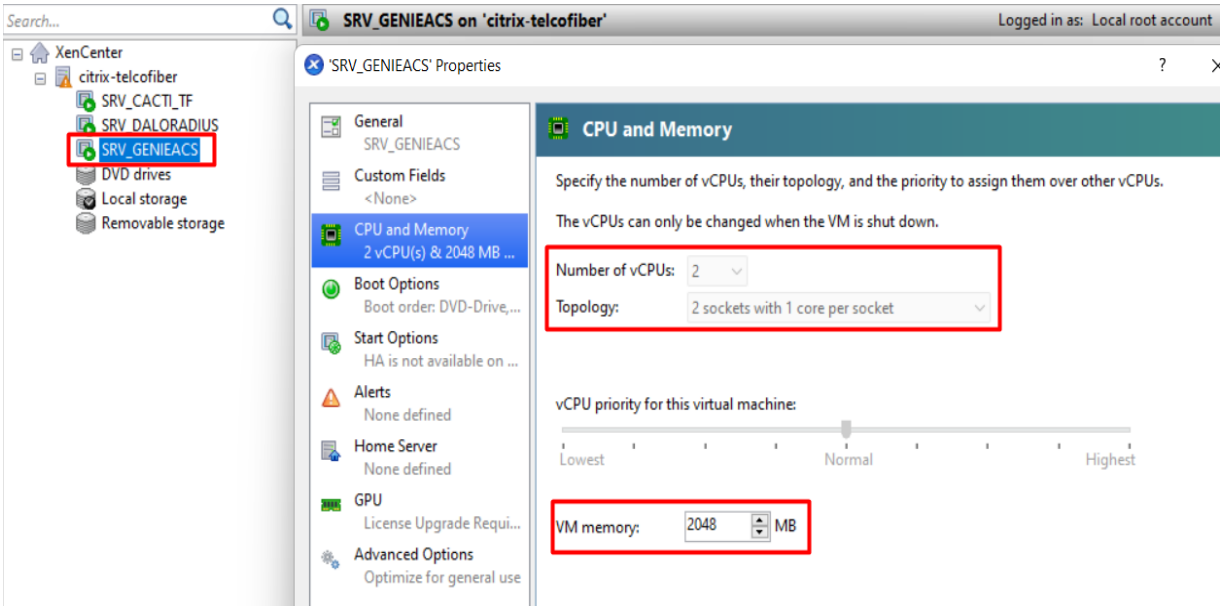

Figura 4.2 Citrix Hipervisor

La Figura 4.3 muestra la interfaz gráfica de usuario del Router Mikrotik con la versión de RouterOS 6.49.7, donde se realizan las configuraciones de direccionamiento IP y creación de VLAN para la gestión remota.

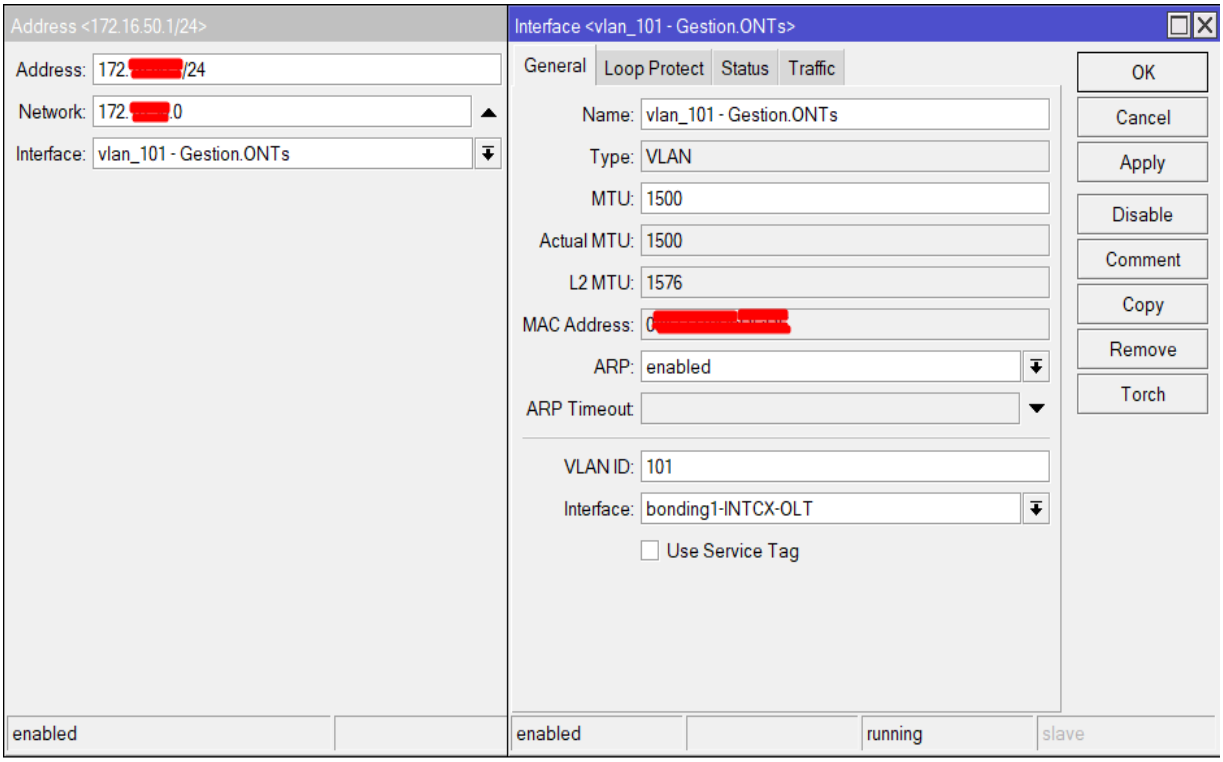

Figura 4.3 RouterOS

Para la OLT se configura el servicio VLAN que será la 101, DBA profile, ONT line profile. En la Figura 4.4 está la configuración de VLAN, en la Figura 4.5 la adición del servidor tr069, y finalmente la configuración de Lineprofile en la Figura 4.6. En este dispositivo también se configura el GEM port y T-CONT.

```
TELCOFIBER(config)#display vlan 101
{ <cr>|inner-vlan<K>|to<K> }:

  Command:
          display vlan 101
  VLAN ID: 101
  VLAN name: VLAN_0101
  VLAN type: smart
  VLAN attribute: common
  VLAN description: GESTION_ONTs
  VLAN forwarding mode in control board: VLAN-MAC
  VLAN forwarding mode: VLAN-MAC
  VLAN broadcast packet forwarding policy: forward
  VLAN unknown multicast packet forwarding policy: forward
  VLAN unknown unicast packet forwarding policy: forward
  VLAN bind service profile ID: -
  VLAN bind RAIO profile index: -
  VLAN priority: -
  -------------------------------
   F /S /P     Native VLAN  State
  -------------------------------
   0 /3 /0                1  up
   0 /3 /1                1  up
  -------------------------------
  Standard port number: 2
  ---------------------------------------------------------------
   INDEX  TYPE  STATE F /S /P   VPI  VCI   FLOWTYPE FLOWPARA
  ---------------------------------------------------------------
       0  gpon  up    0 /0 /0   32   0     vlan     101
   13007  gpon  up    0 /1 /3   8    2     vlan     101
  ---------------------------------------------------------------
  Service virtual port number: 2
  Note: F--Frame, S--Slot, P--Port,
        VPI indicates CM index for DOCSIS,
        v/e--vlan/encap, pritag--priority-tagged
```

Figura 4.4 ONT-VLAN 101

```
TELCOFIBER(config)#display ont tr069-server-profile all
 ------------------------------------------------------------
 Profile ID     Profile Name                    Binding Times
 ------------------------------------------------------------
 30             GENIEACS                        1
 ------------------------------------------------------------
 Total: 1
```

Figura 4.5 tr069-server-profile

```
TELCOFIBER(config)#display ont-lineprofile gpon profile-id 69
  ------------------------------------------------------------
  Profile-ID           :69
  Profile-name         :TR069_PROFIL
  Access-type          :GPON
  ------------------------------------------------------------
```

Figura 4.6 Lineprofile

Se usa ONT Huawei EG8145V5, en la Figura 4.7 se observa su información principal del dispositivo para este caso particular.

Figura 4.7 Información del dispositivo

4.1.4 Descripción de GenieACS

Teniendo claro la infraestructura disponible con la que se cuenta para el proyecto, el alcance y su escalabilidad se describe de manera más amplia la opción seleccionada GenieACS.

GenieACS es un software de gestión de dispositivos de red de código abierto y gratuito que permite a los ISP gestionar y monitorizar sus dispositivos CPE de forma remota.

Este es un sistema de gestión de dispositivos de red que funciona a través de un servidor central y agentes de software instalados en los dispositivos de red que se desean gestionar. El proceso de funcionamiento se puede describir en los siguientes pasos:

I. Descubrimiento: Para comenzar el proceso de gestión de CPE lo primero que ocurre es el descubrimiento de los dispositivos que están conectados a la red. Este proceso se realiza mediante el uso de Protocolo Simple de Administración de Red (SNMP-*Simple Network Management Protocol*).

El proceso de descubrimiento en GenieACS se puede describir de la siguiente manera:

a. El servidor GenieACS envía solicitudes de descubrimiento a los CPE conectados a la red utilizando SNMP.

b. Los CPE responden con un mensaje que contiene su identidad, hardware, versión de software y algunas otras características.

c. El servidor GenieACS registra esta información en su base de datos mongoDB para su posterior uso en la gestión del CPE.

d. Una vez que se descubren todos los CPE, GenieACS inicia el proceso de gestión de dispositivos.

Todos los pasos a continuación usan el modelo de datos del estándar TR098 cuya función principal en GenieACS es proporcionar una estructura unificada para la gestión de CPE. TR098 establece un conjunto de parámetros cuyo propósito es configurar, monitorear y detectar CPE en la red de acceso.

II. Provisionamiento: implica establecer valores a los parámetros necesarios en el CPE, como la dirección IP, la configuración del servicio de red, VLAN, credenciales de acceso entre otros.

III. Monitoreo: Se trata de recopilar información relevante sobre el rendimiento y estado operativo de los CPE.

IV. Diagnóstico: Cuando se detecta un problema en un CPE, se utiliza su capacidad de diagnóstico para identificar el problema y ofrecer soluciones para que esto no vuelva a ocurrir.

V. Actualización: Enviar archivos de imagen ISO para la actualización de firmware, o archivos de configuración para corrección de problemas.

VI. Informes: El servidos ACS proporciona información detallada sobre el rendimiento de los CPE y la calidad del servicio ofrecido.

VII. Gestión de configuración: El servicod ACS realiza esta gestiona de configuraciones de los CPE para asegurarse de que su funcionamiento sea eficiente y con los estándares requeridos.

Es pertinente mencionar las ventajas y desventajas que se encontraron durante el análisis exhaustivo que se le realizó a la versión 1.2.9 de GenieACS.

- ***Ventajas de GenieACS 1.2.9:***

  - Interfaz de usuario intuitiva y fácil de usar para administrar dispositivos de red y servicios.
  - Compatibilidad con una amplia gama de dispositivos CPE, incluidos enrutadores, módems y decodificadores.
  - Permite a los proveedores de servicios de Internet configurar y actualizar dispositivos de forma remota, lo que reduce los costos operativos y mejora la eficiencia.
  - GenieACS permite a los proveedores de servicios de Internet monitorear el rendimiento de los dispositivos en tiempo real y detectar problemas antes de que afecten la calidad del servicio.
  - Ofrece la capacidad de realizar diagnósticos y solucionar problemas de forma remota, lo que reduce el tiempo de inactividad y mejora la satisfacción del cliente.

- ***Desventajas de GenieACS 1.2.9:***

  - Aunque GenieACS es una herramienta poderosa, la configuración puede ser compleja para los usuarios que no se destacan con el software.
  - GenieACS puede requerir hardware adicional y personal especializado para la implementación y el mantenimiento.
  - Aunque GenieACS es un software de código abierto gratuito, puede haber costos adicionales asociados con la implementación y personalización de la herramienta.
  - La versión 1.2.9 no cuenta con información amplia acerca de cómo configurar algunas funciones novedosas de esta versión.

La documentación disponible en la página web oficial para la instalación de GenieACS es muy concisa y eficiente. Además, cuenta con un foro muy activo que resulta útil para resolver dudas acerca de posibles fallos durante la instalación.

Esta poderosa herramienta de gestión tiene como prerrequisitos para su instalación.

- Está desarrollado en Node.js, un entorno de tiempo de ejecución de JavaScript del lado del servidor y se utiliza como la plataforma de desarrollo para construir la aplicación de gestión de dispositivos de red y necesita la versión Node.js 12.13 como minimo.

- Utiliza MongoDB como su base de datos principal porque es escalable, flexible, rápida, fácil de usar e integrable con Node.js y necesita la versión MongoDB 3.6 o mayores.

GenieACS es una plataforma de gestión de dispositivos de red que consta de varios componentes que trabajan juntos para proporcionar una solución completa de gestión de dispositivos de red. A continuación, se describen los diferentes componentes de GenieACS:

- GenieACS CWMP: Este es el componente que se comunica directamente con los CPE mediante el protocolo CWMP. De esta manera se recopila datos y estadísticas de los CPE, como la versión del firmware, la configuración y los informes de estado. También puede enviar comandos de configuración a los dispositivos de red.

- GenieACS NBI: Este componente proporciona una interfaz de programación de aplicaciones (API) para que otros sistemas puedan trabajar de manera integrada con GenieACS. Los usuarios pueden enviar solicitudes a través de la API para obtener datos y realizar cambios en los CPE gestionados.

- GenieACS FS: Es el sistema de archivos que se utiliza para almacenar archivos de configuración u otros recursos. Brinda un sistema de versionado y control que alimenta un historial de los cambios que se realizan en los archivos.

- GenieACS UI: Es la interfaz de usuario Web que permite visualizar y administrar los CPE gestionados por el servidor GenieACS. También presenta una vista general de los dispositivos de red, tiene la capacidad filtrar etiquetas para realizar búsquedas de un CPE en específico o agruparlos. Además, posee la capacidad para ver y editar la configuración de los CPE.

La correcta configuración de cada uno de los componentes de GenieACS es esencial para su correcto funcionamiento, ya que cada uno trabaja de manera individual pero en conjunto conforman la plataforma completa. GenieACS CWMP se encarga de la comunicación directa con los dispositivos de red, escuchando en el puerto 7547, mientras que GenieACS NBI proporciona una API para que otros sistemas puedan integrarse con GenieACS y utiliza el puerto 7557. Por su parte, GenieACS FS utiliza el puerto 7567 para el sistema de archivos utilizado por GenieACS para almacenar recursos y GenieACS UI proporciona una interfaz de usuario web para la gestión de dispositivos de red, utilizando el puerto 3000. En la Figura 4.8 se puede observar el estado actual de cada uno de los componentes de GenieACS.

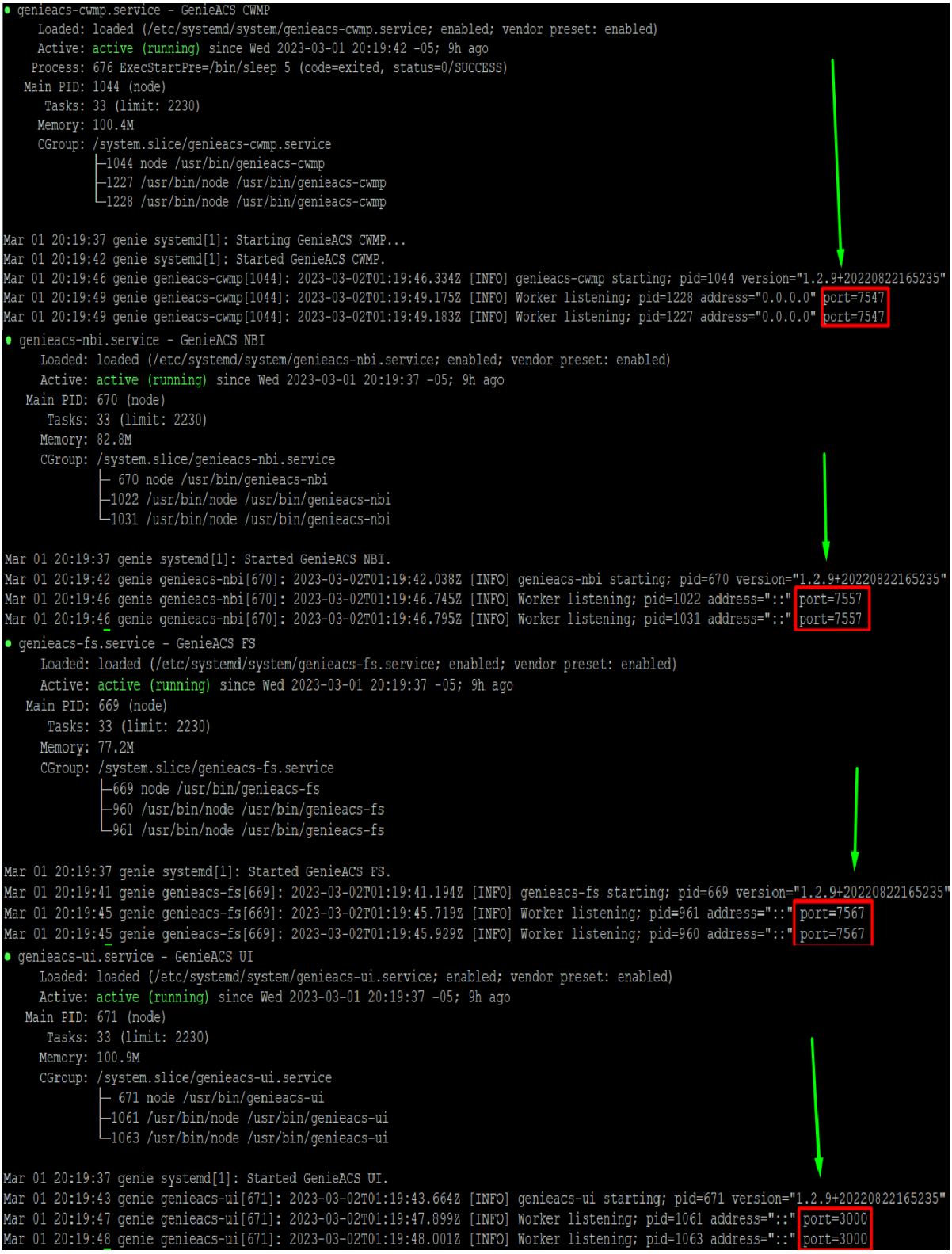

Figura 4.8 Estado de todos los componentes de GenieACS

Una vez instalado y con todos sus componentes activos se accede a la interfaz web por medio de la dirección IP privada clase A 10.XXX.XXX.XXX en el puerto 3000 como se ve en la Figura 4.9.

Figura 4.9 Interfaz general de GenieACS

Por defecto, las credenciales para acceder a la interfaz web son "admin" y "admin" como nombre de usuario y contraseña. Se recomienda cambiarlas inmediatamente por seguridad. Una vez que se ha iniciado sesión en la interfaz como un usuario administrador, se pueden observar todas las funcionalidades que ofrece el sistema, que se describen a continuación.

En la pestaña de dispositivos se puede ver una lista de todos los CPE que han sido registrados en GenieACS, aunque algunos de ellos ya no estén activos. También se puede usar una opción de filtro para buscar un CPE específico por su número de serie o dirección IP (que en este caso no se muestran por motivos de seguridad de la empresa). Además, es posible agrupar varios CPE según su clase de producto o versión de software, por ejemplo.

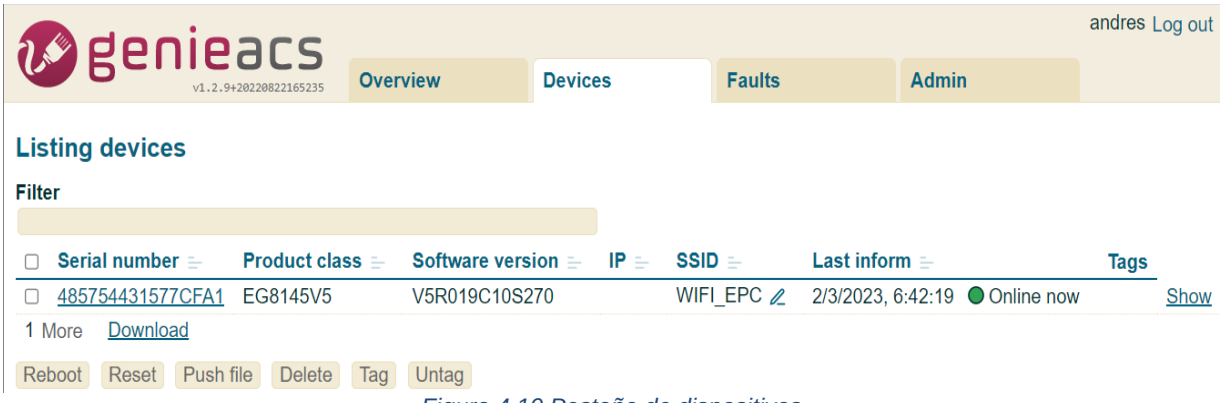

Figura 4.10 Pestaña de dispositivos

En esta pestaña se pueden configurar diferentes columnas de datos para visualizar información adicional de los CPE, dependiendo de lo que se considere pertinente. En la Figura 4.10 se muestra un ejemplo de una modificación realizada, en la cual se asignó una dirección IP incorrecta a la interfaz WAN con el fin de ilustrar los cambios y verificar su correcto funcionamiento.

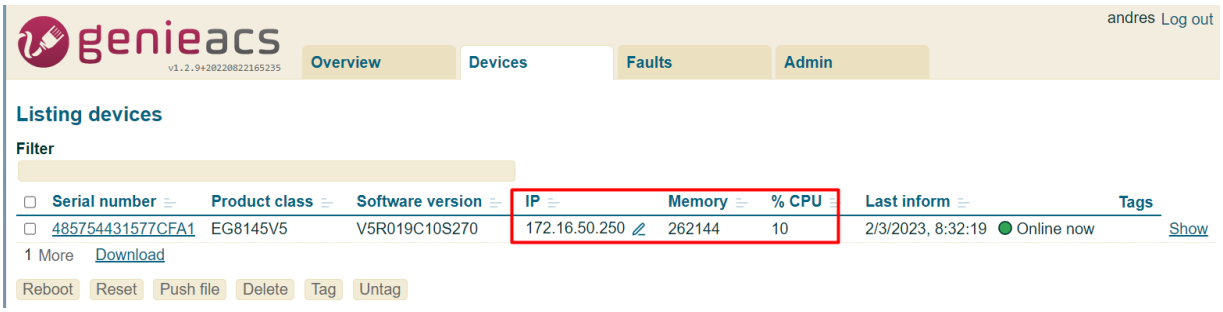

Figura 4.11 Interfaz Web editada

Se selecciona el dispositivo para que aparezca un menú con más detalles acerca del dispositivo, tal como se observa en la Figura 4.11.

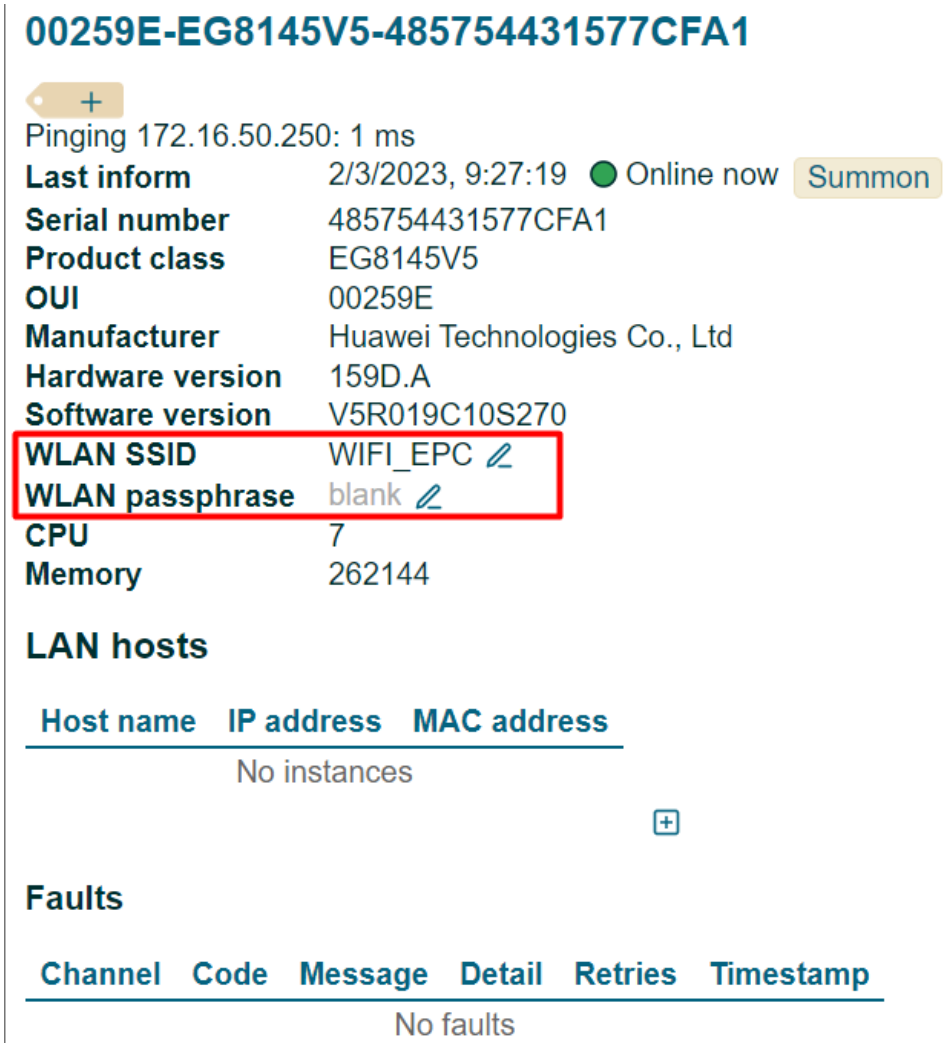

Figura 4.12 Detalles del dispositivo

En la Figura 4.12 se muestra información adicional acerca del dispositivo que no se encuentra en la vista previa, como por ejemplo el ping al CPE, OUI, fabricante y otros datos que se pueden añadir según la necesidad. También se puede observar en el recuadro rojo que se pueden editar los valores de WLAN SSID y WLAN passphrase, y que cualquier cambio se verá reflejado inmediatamente. A pesar de que WLAN aparece en blanco, se puede editar, pero el CPE informa este dato en blanco debido a cuestiones legales.

La Figura 4.13 muestra una lista de los parámetros virtuales que se pueden utilizar en GenieACS, y es notable que la lista contiene un total de 630 parámetros para el CPE. La importancia del modelo de datos TR098 radica en que permite a GenieACS recopilar información específica de los dispositivos de red y gestionarlos de manera eficiente a través de los protocolos de comunicación CWMP.

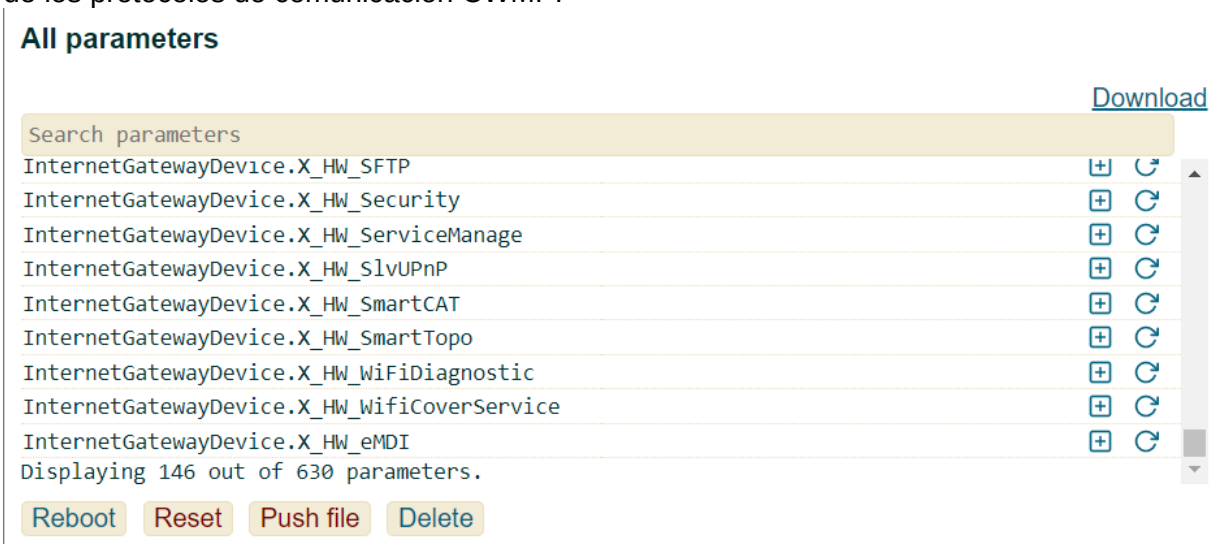

Figura 4.13 Filtro de parámetros virtuales

En la parte inferior se observan 4 botones que describen a continuación:

Reboot: para hacer un reinicio rápido del dispositivo seleccionado para finalizar algún proceso que esté generando inconvenientes en el rendimiento del dispositivo y causando interrupciones en el servicio.

Reset: lleva al CPE a sus configuraciones de fábrica, esto proceso libera todo el espacio en la memoria o si tiene problemas de rendimiento que se solucionan con un Reboot o errores en su configuración que pueden ser difíciles de identificar, sin embargo, es importante tener en cuenta que al regresar a su estado de fábrica un CPE, se borrarán todas las configuraciones personalizadas y datos almacenados en él, lo que incluye los datos de conexión a Internet y las configuraciones de red inalámbrica. Por lo tanto, es importante realizar un back up de los datos importantes antes de realizar este proceso y configurar el CPE nuevamente después del restablecimiento.

Push file: aquí se puede seleccionar un archivo de un equipo local o directamente en el servidor ACS y cargarlo al dispositivo seleccionado. Este archivo puede ser una imagen ISO de actualización de firmware, un script para la configuración de parámetros específicos, o un archivo de configuración para un servicio en particular, entre otros.

Delete: en la interfaz web de GenieACS 1.2.9 permite eliminar un objeto o parámetro específico en un dispositivo. Al hacer clic en el botón "Delete", se eliminará el objeto o parámetro seleccionado en el dispositivo. Esta función puede ser útil cuando se necesita eliminar un objeto o parámetro que está causando problemas en el dispositivo o cuando se necesita realizar una limpieza en la configuración del dispositivo. Sin embargo, es importante tener precaución al utilizar esta función, ya que la eliminación de objetos o parámetros importantes puede causar problemas en el funcionamiento del dispositivo.

La pestaña de Overview permite observar la cantidad de dispositivos que se encuentran en línea, los que estuvieron activos las últimas 24 horas o que ya llevan mucho tiempo inactivos, esto puede ser útil para identificar los dispositivos que ya no sé encuentran conectados en la red y así eliminarlos del sistema para que esos registros no consuman recursos.

Faults es una pestaña muy útil que enseña las tareas que salieron mal, las iteraciones que lleva dicha tarea y el detalle del por qué no se pudo realizar, sin embargo, es más eficiente revisar los logs de GenieACS en un terminal de línea para esta tarea.

La pestaña "Admin" en la interfaz de GenieACS 1.2.9 se utiliza para administrar el sistema y la configuración de GenieACS. Aquí es donde los usuarios con permiso de administradores pueden realizar tareas como crear y administrar cuentas de usuario, configurar la autenticación y autorización, configurar el servidor de correo electrónico, configurar la copia de seguridad y restaurar la base de datos, y ajustar la configuración de seguridad. También se pueden gestionar las notificaciones del sistema y de los eventos de GenieACS desde esta pestaña. En resumen, la pestaña "Admin" es donde se pueden realizar tareas administrativas de GenieACS y configurar el sistema para adaptarse a las necesidades de la organización.

En la Figura 4.14 se pueden ver en la parte izquierda todas las opciones que como usuario administrador se tiene acceso y el listado de presets.

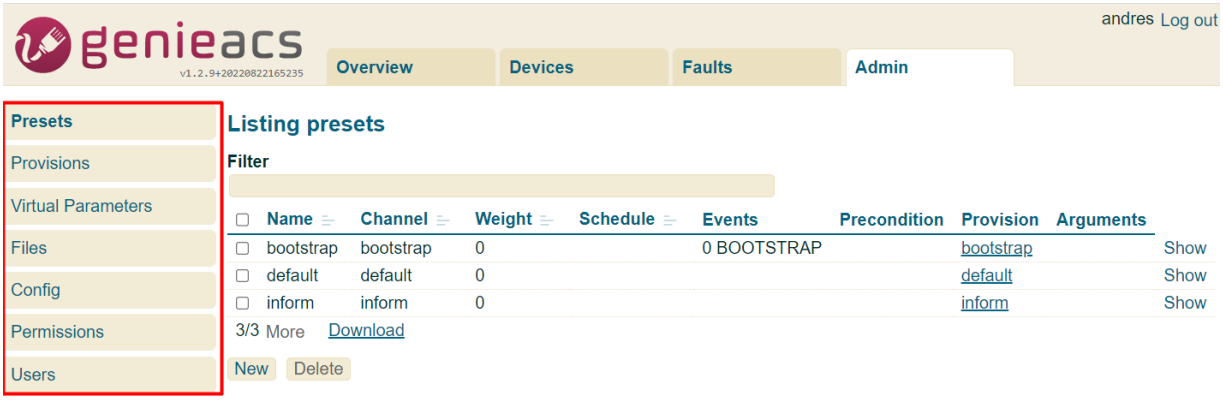

Figura 4.14 Pestaña administrador

La primera opción que se ve es Presets, que es un conjunto de valores predefinidos para ciertos parámetros de configuración de dispositivos. Estos se pueden aplicar a uno o varios dispositivos simultáneamente, lo que permite realizar cambios de configuración masivos en toda la red de manera eficiente y coherente.

Un preset puede incluir valores para varios parámetros, como la configuración de la red, la seguridad, los servicios, etc. Al aplicar un preset a un dispositivo, se sobrescriben los valores existentes en los parámetros incluidos en el preset con los valores predefinidos.

Los presets pueden ser creados y personalizados según las necesidades de la red y los dispositivos, y se pueden aplicar en cualquier momento a uno o varios dispositivos. Los presets son una característica útil para ahorrar tiempo y asegurar la coherencia en la configuración de dispositivos.

GenieACS trae configurado tres presets en su instalación inicial, Bootstrap, defaultd e inform, y a cada uno se le asigna un Channel, Weight, Schedule, Events, Precondition, Provision, y Arguments de ser necesario, en la Figura 4.15 se observa la opción de editar el preset bootstrap y se procede a explicar cada una de las características que se le pueden asignar a este preset.

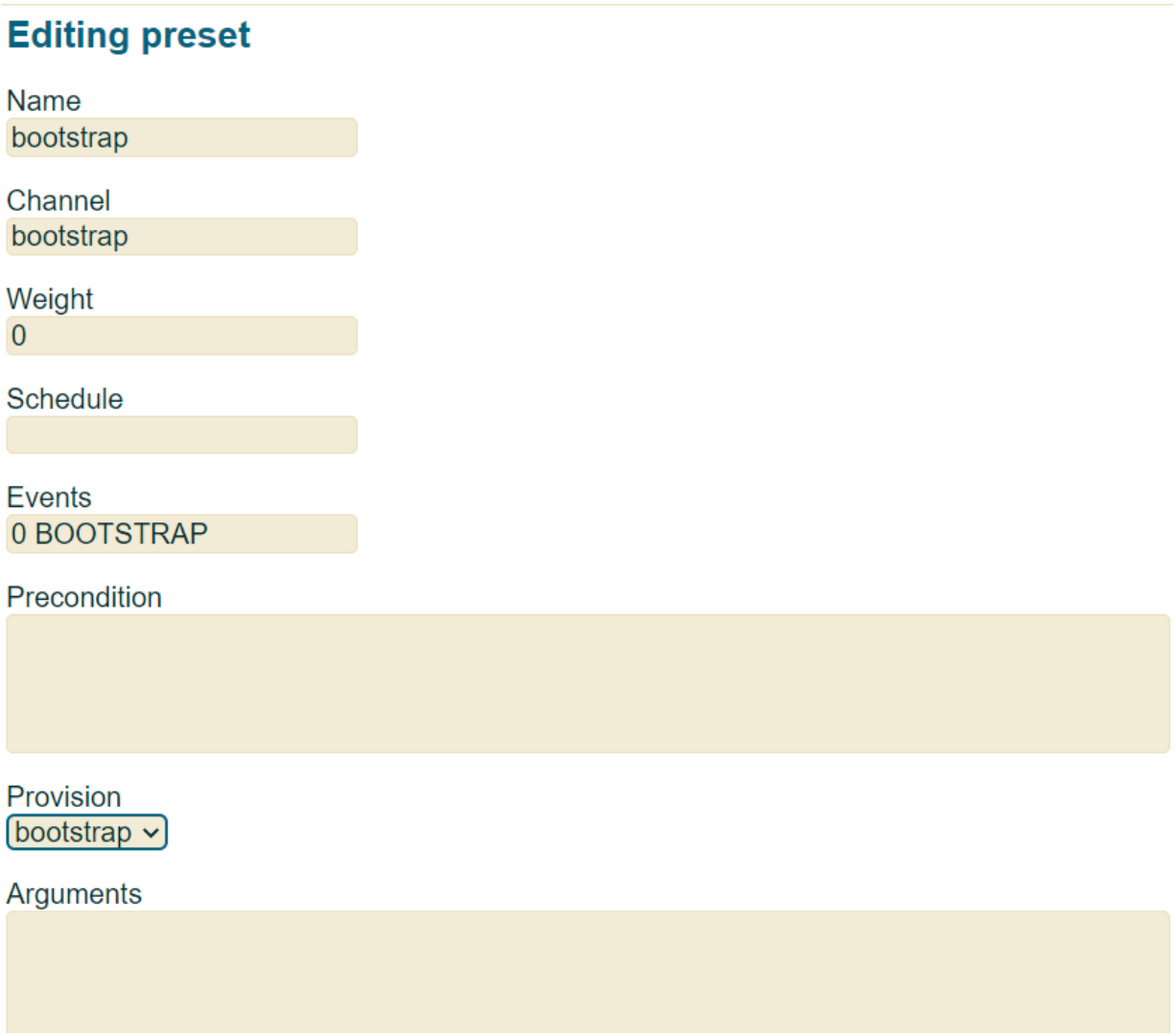

Figura 4.15 Información de Preset bootstrap

Channel: en un preset se refiere al canal de comunicación por la cual se envía un conjunto de parámetros o configuraciones a un dispositivo. Cada canal puede tener diferentes configuraciones que se envían a los dispositivos de manera individual o en grupos, según la necesidad.

Por ejemplo, si se quiere enviar un conjunto de configuraciones para habilitar una funcionalidad específica a un grupo de dispositivos, se puede crear un canal en el preset con las configuraciones necesarias para esa funcionalidad y aplicarlo a ese grupo de dispositivos. Así mismo, si se necesita enviar un conjunto diferente de configuraciones para habilitar una funcionalidad diferente a otro grupo de dispositivos, se puede crear otro canal en el preset con las configuraciones necesarias para esa funcionalidad y aplicarlo al grupo de dispositivos correspondiente.

En resumen, los canales en un preset permiten la aplicación de diferentes configuraciones a grupos o dispositivos específicos de acuerdo a las necesidades del operador.

Weight: es el "peso" de un preset y se refiere a la prioridad relativa de un preset en relación con otros presets que se han asignado al mismo dispositivo. Es un número entero que se puede asignar al preset.

Cuando varios presets se han asignado a un dispositivo, GenieACS los evalúa en orden de peso, desde el preset con el peso más bajo hasta el preset con el peso más alto. Si dos o más presets tienen el mismo peso, se evalúan en orden alfabético por nombre. Esto significa que el preset con el peso más alto tendrá la última palabra en la configuración de un dispositivo. Si dos o más presets contienen la misma configuración, el valor del preset con el peso más alto será el valor que se utiliza.

Schedule: se refiere a la programación de cuándo se debe aplicar ese preset a un dispositivo. Es decir, se puede programar un preset para que se aplique en un horario específico o en una fecha determinada. Esto es útil para programar cambios en la configuración de un dispositivo en momentos específicos, por ejemplo, para aplicar actualizaciones o realizar tareas de mantenimiento programado.
Event: se refiere a la configuración de eventos que activarán el preset. Un evento puede ser una solicitud de informe periódico, una solicitud de informe de error, una solicitud de configuración o una solicitud de conexión.

En la sección "Eventos" de un preset, se puede configurar qué eventos activarán el preset y cómo se procesarán. Por ejemplo, se puede especificar que el preset se aplique solo a las solicitudes de configuración que contengan ciertos parámetros, o que el preset se aplique solo a las ONT que garanticen ciertos criterios, como tener cierto firmware o cierta versión de hardware.

En resumen, la sección "Events" de un preset permite configurar cuándo y cómo se utiliza el preset a los dispositivos gestionados por GenieACS.

Precondition: es una condición previa que se debe cumplir antes de que se ejecute el preset. Esto puede incluir la verificación de la existencia de un valor específico en el dispositivo o la confirmación de que se han cumplido ciertas condiciones antes de que se aplique el preset.

La Precondition es una forma de garantizar que se cumplan ciertos requisitos antes de ejecutar una acción en el dispositivo, lo que puede ayudar a evitar problemas y errores en el proceso de configuración. Por ejemplo, si se desea aplicar un preset que configure una nueva red Wi-Fi en el dispositivo, se puede establecer una condición previa para confirmar que el dispositivo tenga un módulo Wi-Fi activo antes de aplicar la configuración. Si el dispositivo no tiene un módulo Wi-Fi activo, el preset no se ejecutará y se mostrará un mensaje de error en la consola de GenieACS.

Provision: se refiere a las acciones específicas que se realizarán en un dispositivo cuando se le aplica un preset. Estas acciones pueden incluir la configuración de parámetros, la actualización del firmware, la creación de nuevos usuarios, la instalación de certificados, entre otros. Por ejemplo, se puede configurar un preset que determine ciertos valores de configuración en los dispositivos que cumplan con los criterios especificados. La acción de provisionar puede incluir la configuración de parámetros, la reinicialización de la ONT a la configuración de fábrica, entre otras acciones. La provisión de un preset se ejecuta en función de su programación, ya sea manualmente o en un horario establecido.

El propósito de la provisión es automatizar el proceso de configuración de los dispositivos y garantizar que todos los dispositivos tengan la misma configuración y firmware, lo que facilite la administración de la red y reduzca los errores humanos.

La provision de un preset se configura mediante la pestaña "Provisioning" en la interfaz de usuario de GenieACS. En esta sección, se pueden configurar los parámetros específicos que se aplicarán a los dispositivos cuando se ejecute el preset.

Arguments: En GenieACS 1.2.9, el campo "Argumentos" en un preset se refiere a los valores que se le pasan al script o comando que se ejecuta como parte de ese preset. Estos argumentos son específicos del script o comando que se está acabando y pueden variar en función de lo que se esté haciendo en el preset.

Por ejemplo, si se está terminando un script que reinicia la ONT, se puede pasar el argumento "-r" al script para indicarle que debe realizar un reinicio completo. De esta manera, el script sabe qué acción tomar al ser ejecutado como parte del preset.

En resumen, los argumentos en un preset se utilizan para personalizar la acción que se está produciendo como parte de ese preset y deben ser definidos cuidadosamente para asegurarse de que se están pasando los valores correctos al script o comando que se está produciendo.

Opción de Provisions que es donde se realiza el scrpit que se le asigna al preset como se explicó antes, en la Figura 4.16 se ve el script de la provision default y que está asignada al preset default.

Figura 4.16 Editing Provision

En este scrpit se ve una función de aprovisionamiento que actualiza ciertos parámetros básicos cada hora. Utilice la función “declare()” para definir los parámetros que se actualizarán periódicamente y establecerá su valor en el tiempo actual en milisegundos, más el valor de una hora en milisegundos (3600000).

Los parámetros que se actualizan incluyen información sobre el hardware y el software del dispositivo, las direcciones MAC e IP de la conexión WAN, el SSID de la red inalámbrica, el nombre y la dirección IP y MAC de los hosts conectados a la red local.

Es importante destacar que el campo de contraseña no se actualiza periódicamente porque los CPE siempre informan contraseñas en blanco por motivos de seguridad y legalidad.

Opción de Virtual Parameters en la interfaz de administración de GenieACS permite la creación de parámetros virtuales que no existen en el dispositivo, pero que pueden ser creados para ser utilizados en el sistema de GenieACS.

Estos parámetros pueden ser útiles para crear condiciones, scripts y presets, por ejemplo, para comparar los valores de dos parámetros o para realizar operaciones matemáticas.

Un ejemplo de un parámetro virtual podría ser crear un parámetro que represente el número total de clientes en un servidor de DHCP. Para hacer esto, se podría crear un script que se ejecute periódicamente y que consulte el número de clientes DHCP en el servidor. Este valor se puede almacenar en un parámetro virtual creado en GenieACS y luego se puede utilizar en condiciones, scripts y presets para realizar acciones específicas basadas en el número total de clientes DHCP.

En resumen, los parámetros virtuales en la pestaña de Virtual Parameters de la interfaz de administración de GenieACS son una forma de crear parámetros personalizados y útiles para automatizar y personalizar el sistema de gestión de dispositivos de GenieACS.

La opción de Files en la administración de GenieACS 1.2.9 permite cargar y administrar diferentes tipos de archivos que se utilizan en la gestión de dispositivos. Al hacer clic en "Nuevo", se puede crear un nuevo archivo y especificar su tipo de archivo y su información asociada como se puede apreciar en la Figura 4.17.

Figura 4.17 Creación de archivos

Las cinco opciones disponibles para el tipo de archivo son las siguientes:

I. Imagen de actualización de firmware: se utiliza para cargar imágenes de firmware de dispositivos que se pueden utilizar para actualizar el firmware de los mismos.

II. Contenido web: se utiliza para cargar contenido web que puede ser entregado a los dispositivos, como archivos HTML, CSS, JavaScript, imágenes, etc.

III. Vendor Configure File: se utiliza para cargar archivos de configuración específicos del proveedor que se pueden entregar a los dispositivos.

IV. Tone File: se utiliza para cargar archivos de tono de llamada que pueden funcionar en dispositivos de telefonía.

V. Ringer File: se utiliza para cargar archivos de tono de timbre a los dispositivos de telefonía.

En cuanto a las casillas de OUI, Product Class y Version, estas se utilizan para identificar el dispositivo para el cual se está cargando el archivo. La OUI (Organizational Unique Identifier) es un identificador único asignado a cada fabricante de dispositivos. La Product Class es un identificador único para un tipo específico de dispositivo, y la Version se refiere a la versión del firmware del dispositivo para el cual se está cargando el archivo.

Al especificar esta información junto con el tipo de archivo, GenieACS puede asegurarse de que los archivos se cargan y entreguen a los dispositivos correctos de manera efectiva.

En la pestaña "config" se encuentran las configuraciones de la aplicación GenieACS en sí. A continuación, se presentan algunas de las configuraciones que se pueden encontrar en la lista:

- "MongoDB Connection String": esta configuración especifica la cadena de conexión a la base de datos MongoDB que GenieACS utiliza para almacenar y recuperar datos del dispositivo.

- "Web UI Username" y "Web UI Password": estas configuraciones habilitan las credenciales necesarias para iniciar sesión en la interfaz web de GenieACS.

- "ACS URL": esta configuración define la URL que los dispositivos utilizarán para comunicarse con GenieACS, y debe coincidir con la dirección IP o el nombre de dominio utilizado para acceder a la interfaz web de GenieACS.

- "Inform Interval": esta configuración establece la frecuencia con la que los dispositivos deben informar a GenieACS sobre su estado y los datos del dispositivo.

- "Max Concurrent Tasks": esta configuración define el número máximo de tareas que GenieACS puede realizar simultáneamente.

- "NBI Listening Port": esta configuración especifica el puerto que GenieACS escucha para las solicitudes de la API de red de banda ancha (NBI).

- "UI Listening Port": esta configuración define el puerto en el que GenieACS escucha para las solicitudes de la interfaz web.

- "Log Level": esta configuración establece el nivel de registro para la aplicación, lo que determina cuántos detalles se registran en los archivos de registro de GenieACS.

Estas son solo algunas de las configuraciones que se pueden encontrar en la pestaña "config" de la interfaz de administración de GenieACS. Cada una de ellas se puede ajustar según las necesidades específicas de la implementación de GenieACS o crear una nueva configuración

de ser requerida, estas opciones se visualizan en la parte inferior como se aprecia en la Figura 4.18.

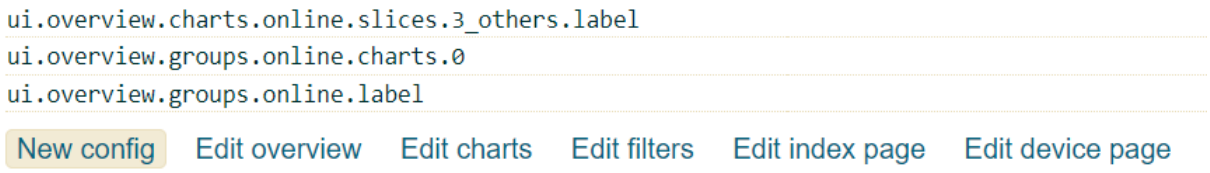

Figura 4.18 Panel de configuraciones

En la Figura 4.19 se observan algunas configuraciones con respecto a la autenticación y configuración de la interfaz Web.

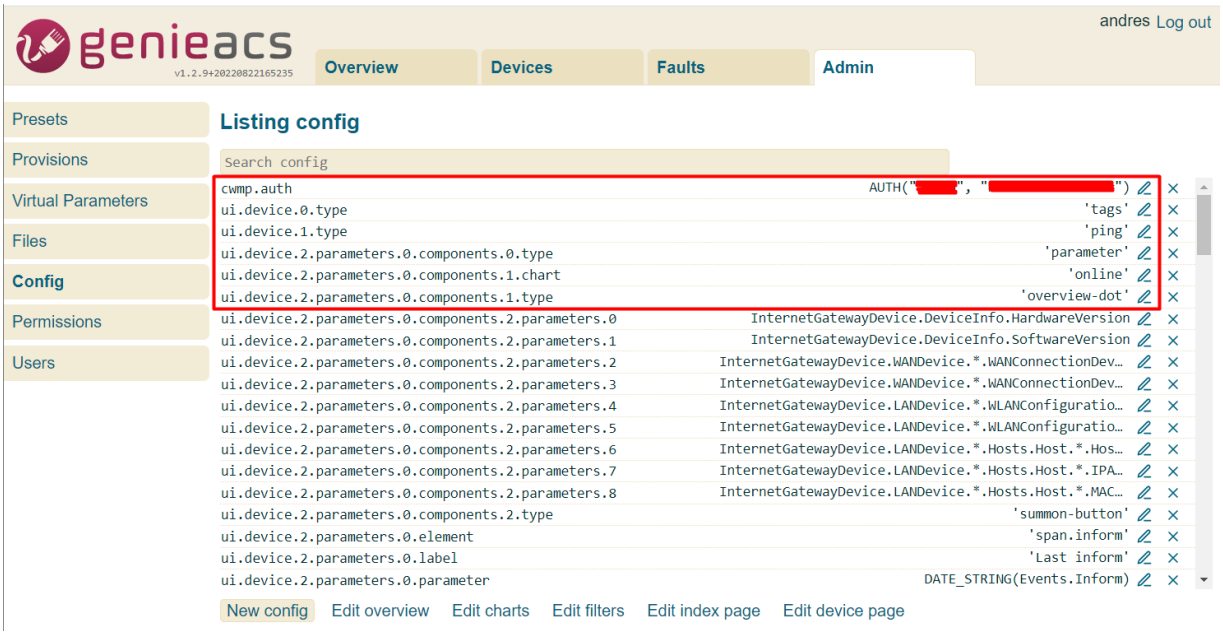

Figura 4.19 Lista de configuraciones

- **cwmp.auth**: Esta configuración proporciona las credenciales de autenticación para el protocolo CWMP (CPE WAN Management Protocol) utilizado por GenieACS para comunicarse con los dispositivos administrados. Inicialmente esta configuración cómo algunas otras no aparecen en esta lista porque el Genieacs las establece por defecto, por ejemplo el nombre de usuario es "admin" y la contraseña es "admin" por lo que se es recomendable realizar estas configuraciones para establecer credenciales más seguras.

- **ui.device.0.type**: Esta configuración establece el tipo de dispositivo en la interfaz de usuario. En este caso, se establece como "etiquetas".

- **ui.device.1.type**: Esta configuración establece el tipo de dispositivo en la interfaz de usuario. En este caso, se establece como "ping".

- **ui.device.2.parameters.0.components.0.type**: Esta configuración establece el tipo de componente para el primer parámetro del dispositivo 2 en la interfaz de usuario. En este caso, se establece como "parámetro".

- **ui.device.2.parameters.0.components.1.chart**: Esta configuración establece el tipo de gráfico para el segundo componente del primer parámetro del dispositivo 2 en la interfaz de usuario. En este caso, se establece como "online".

- **ui.device.2.parameters.0.components.1.type**: Esta configuración establece el tipo de componente para el segundo parámetro del dispositivo 2 en la interfaz de usuario. En este caso, se establece como "overview-dot".

Como se puede ver en la Figura 4.19, se ofrecen opciones para editar las diferentes pestañas de la interfaz web, lo que permite visualizar la información relevante para los intereses de la empresa. Los cambios que se realizaron en las secciones anteriores se hicieron en respuesta a las solicitudes de la empresa durante el análisis de requisitos.

Por último, se encuentran las opciones de "Permisos" y "Usuarios", ambas pestañas trabajan conjuntamente. En la sección de "Permisos" se asignan los recursos a los roles y se otorgan los permisos correspondientes para cada recurso, mientras que en la sección de "Usuarios" se pueden crear nuevos usuarios y asignarles roles. Estas opciones son muy útiles para establecer la jerarquía administrativa del sistema.

Una vez se han definido los recursos con los que cuenta la empresa para el proyecto, las funcionalidades que debe tener el sistema y se ha seleccionado la herramienta adecuada, se procede a diseñar el esquema de funcionamiento del sistema.

El diseño de un esquema para el funcionamiento conjunto de un ACS con CWMP que permita el acceso remoto para monitorizar, configurar y actualizar un grupo de CPE de una red FTTH/GPON puede ser complejo y requerir la consideración de varios componentes.

Componentes:

- ACS (Automated Configuration Server): Es el servidor que se encarga de gestionar los dispositivos CPE.

- CWMP (CPE WAN Management Protocol): Es el protocolo que se utiliza para la comunicación entre los dispositivos CPE y el ACS.

- CPE (Customer Premises Equipment): Son los dispositivos que se instalan en los hogares o empresas de los clientes, como los enrutadores o módems.

- Red FTTH/GPON: Es la red de fibra óptica que conecta los CPE con el servidor ACS.

Consideraciones:

- Seguridad: Es fundamental garantizar que la comunicación entre el ACS y los CPE se realice de manera segura y que se implementen medidas de autenticación y encriptación.
- Compatibilidad: Los CPE deben ser compatibles con el protocolo CWMP para poder ser gestionado por el ACS.

- Escalabilidad: El sistema debe ser capaz de manejar un gran número de dispositivos CPE de manera eficiente.

- Disponibilidad: El sistema debe estar disponible en todo momento para garantizar que los CPE estén siempre conectados y funcionando correctamente.

- Actualizaciones: El sistema debe ser capaz de actualizar los CPE de manera remota y sin interrupciones en el servicio.

- Monitoreo: El sistema debe permitir la monitorización en tiempo real de los CPE para detectar y solucionar problemas de manera proactiva.

En la Figura 4.20 se aprecia las interacciones entre los componentes de la red, las VLAN que son utilizadas para el acceso a Internet y la VLAN de gestión.

Esquema Gráfico funcional del servidor ACS en la red FTTH/GPON

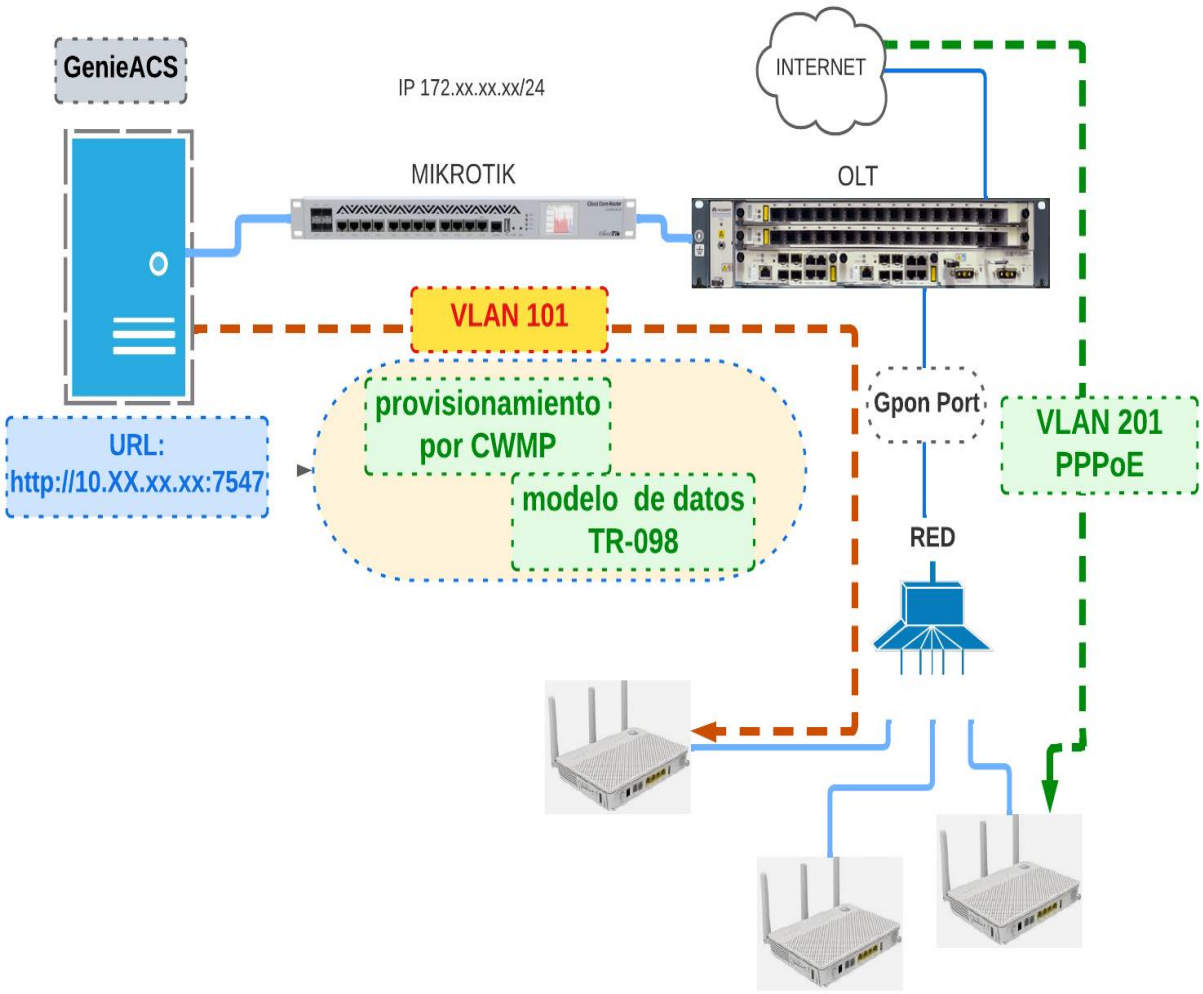

Figura 4.20 Esquema Funcional

El proceso de funcionamiento sintetizado se describe en los siguientes pasos.

I. Se configuran los datos del ACS URL, username y password en el ACS.

II. El CPE utiliza el protocolo CWMP para establecer una conexión con el ACS utilizando los datos de configuración del ACS, enviando un mensaje informando al ACS de que está disponible para su gestión, este mensaje es un “inform” que contiene el número de serie, modelo y firmware entre otros datos y el ACS responde a la ONT con un mensaje de confirmación en el cual le proporciona su propia información de identificación.

III. La ONT y el ACS intercambian mensajes en formato XML utilizando CWMP para realizar diversas operaciones, como la obtención de parámetros de configuración, la realización de diagnósticos y la actualización de firmware.

4.2 Despliegue del sistema ACS

En esta sección se proporcionará una descripción más detallada del proceso de registro de una ONT en GenieACS y las funciones que se pueden realizar una vez que la ONT está registrada en el sistema. Es importante destacar que, a diferencia de la instalación básica del servidor GenieACS en una máquina virtual local, en este caso se llevará a cabo todo en un entorno real, ya que los equipos necesarios para la implementación básica no están disponibles para simulaciones previas de prueba.

Se explicará cómo se realiza el proceso de registro de una ONT en el sistema y las opciones disponibles una vez que la ONT termina este proceso. Esto ayudará a entender el funcionamiento del sistema desplegado en la red FTTH/GPON.

Primero, es necesario enviar los datos de configuración del ACS, para lo cual se debe agregar en la OLT un perfil de servidor TR-069 con el identificador de perfil 30 y el nombre de perfil TR_069. Luego, se especifica la URL del servidor ACS remoto, que en este caso es "http:10.XX.XX.XX:7547", así como el nombre de usuario y contraseña. Esto se puede observar en la Figura 4.21. Al hacer esto, la OLT podrá conectarse al servidor ACS remoto para realizar la gestión y configuración remota de los ONT que se conecten a ella.

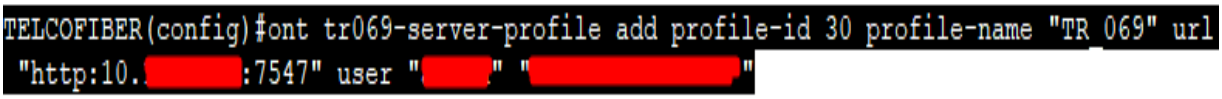

Figura 4.21 Perfil de servidor TR-069

Una vez que se ha creado el Perfil de servicio, se debe asignar un Puerto de servicio que está conectado a la ONT. El Service Port es el punto de conexión lógico entre la OLT y cada ONT, y se utiliza para establecer la conexión entre ambos dispositivos.

La configuración del Service Profile en el Service Port se logra mediante la creación de un Service VLAN que se asocia al Service Port. Esta VLAN se utiliza para separar el tráfico de datos del tráfico de gestión y configuración TR-069. Se configura la VLAN en el Service Port y se asigna el Service Profile correspondiente. En el esquema funcional se utiliza la VLAN 101, aunque esta configuración no se muestra debido a políticas de seguridad de la empresa.

Una vez completado este proceso, la OLT envía los datos de configuración del ACS a la ONT. La recepción de estos datos se refleja en la interfaz web de la ONT, a la cual se accede a través de la Gateway para verificar el éxito en la recepción de los datos de configuración, como se puede observar en el recuadro azul de la Figura 4.22.

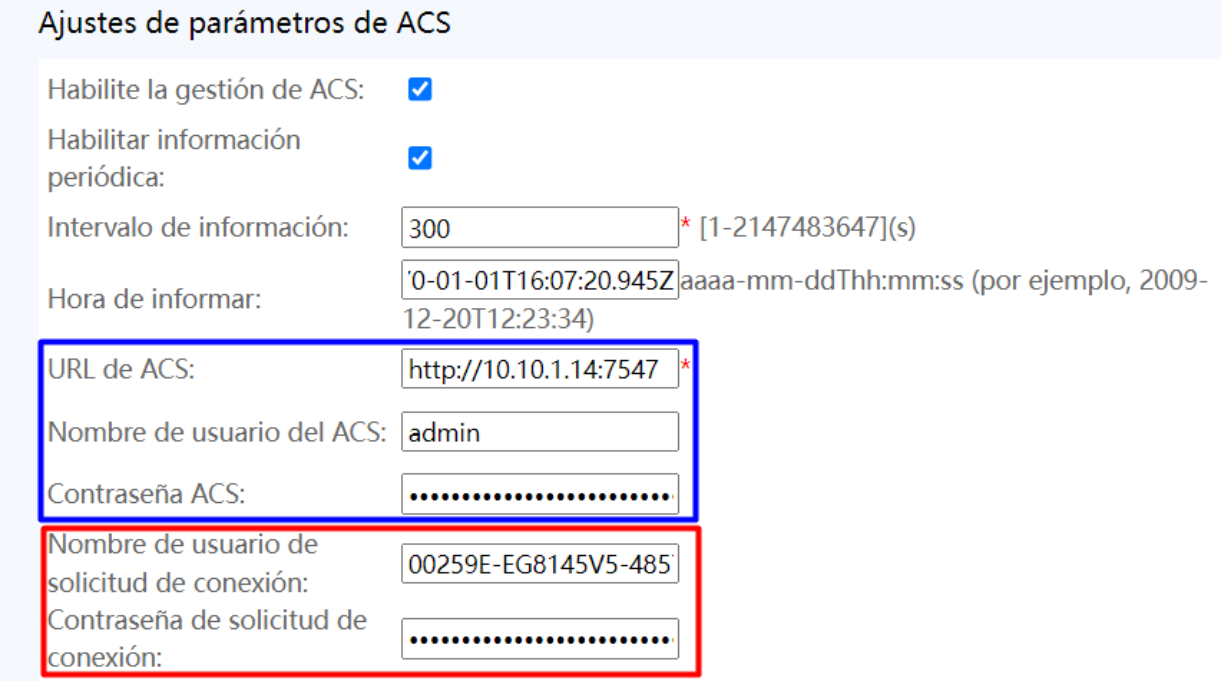

Figura 4.22 Verificación de configuración del ACS en la interfaz Web

Se establece una conexión segura entre la ONT y el ACS a través de un proceso de autenticación y cifrado mutuo. En primer lugar, la ONT envía un mensaje HTTPS POST al ACS con sus credenciales de acceso. A continuación, el ACS auténtica a la ONT y le envía un certificado de seguridad. Este certificado se utiliza para establecer una conexión segura y encriptada entre el ACS y la ONT, lo que garantiza la autenticidad y confidencialidad de los datos que se intercambian durante la comunicación. La ONT utiliza este certificado para cifrar todas las comunicaciones futuras con el ACS y así mantener la seguridad de la información que se transmite.

Registro de la ONT: después de establecer la conexión segura se da la siguiente comunicación entre la ONT y el ACS.

I. La ONT verifica el certificado de seguridad y si es válido, procede a enviar un mensaje "inform" al ACS con su información de identificación (por ejemplo, número de serie, modelo, etc.).

II. El ACS recibe el mensaje "inform" y lo procesa. A continuación, envíe un mensaje "inform-request" a la ONT, en el que se incluyen los siguientes datos:

- URL de solicitud de conexión: La dirección URL del ACS.
- Connection Request User Name: El nombre de usuario que la ONT confirmó para conectarse de forma segura con el ACS.
- Connection Request Password: La contraseña que la ONT confirma para conectarse de forma segura con el ACS.
- ACS URL: La dirección URL del ACS.
- Intervalo de informe: El intervalo de tiempo en el que la ONT emitió mensajes "inform" al ACS.
- Puerto de solicitud de conexión: El número de puerto que la ONT usó para conectar de forma segura con el ACS.

Estos datos se pueden visualizar en el recuadro rojo de la Figura 4.22.

III. La ONT recibe el mensaje "inform-request" del ACS y almacena los datos que contiene.

IV. La ONT establece una conexión segura con el ACS utilizando el Connection Request URL, Connection Request User Name y Connection Request Password enviados en el mensaje "inform-request".

V. La ONT envía un mensaje "transfer-complete" al ACS para confirmar que se ha registrado correctamente.

Una vez finaliza este proceso, la ONT se puede ver en la interfaz Web de GenieACS y se puede verificar los datos de la misma en la base de datos como se observa en la Figura 4.23.


```
> db.devices.find()
{ "_id" : "00259E-EG8145V5-485754431577CFA1", "InternetGatewayDevice" : { "BulkD
ata" : { "_object" : true, "_writable" : true }, "Capabilities" : { "_object" :
true, "_writable" : false }, "DHCPv4" : { "_object" : true, "_writable" : true }
, "DHCPv6" : { "_object" : true, "_writable" : true }, "DNS" : { "_object" : tru
e, "_writable" : true }, "DeviceConfig" : { "_object" : true, "_writable" : fals
e }, "DeviceInfo" : { "HardwareVersion" : { "_object" : false, "_timestamp" : IS
ODate("2023-03-04T00:22:18.099Z"), "_type" : "xsd:string", "_value" : "159D.A",
"_writable" : false }, "ProvisioningCode" : { "_object" : false, "_timestamp" :
ISODate("2023-03-04T00:22:18.099Z"), "_type" : "xsd:string", "_value" : "", "_wr
itable" : true }, "SoftwareVersion" : { "_object" : false, "_timestamp" : ISODat
e("2023-03-04T00:22:18.099Z"), "_type" : "xsd:string", "_value" : "V5R019C10S270
", "_writable" : false }, "SpecVersion" : { "_object" : false, "_timestamp" : IS
ODate("2023-03-04T00:22:18.099Z"), "_type" : "xsd:string", "_value" : "1.0", "_w
ritable" : false }, "_object" : true, "_writable" : true, "AccessType" : { "_obj
ect" : false, " writable" : false }, "AdditionalHardwareVersion" : { " object" :
```


Figura 4.23 Colección dispositivos de la base de datos de GenieACS

La respuesta de esta solicitud en MongoDB es un documento en formato JSON. Cada documento representa un registro en la colección y tiene un formato clave-valor, donde las claves son los nombres de los campos y los valores son los valores correspondientes para cada registro.

Ahora que la ONT está registrada en GenieACS, es posible monitorear y gestionar los parámetros que se configuraron tanto en el Frontend como en el Backend. Para llevar a cabo esta tarea, se utilizó una ONT que ya estaba prestando servicios de Internet, lo que permitió observar la eficacia operativa del sistema.
Escenario ONT prestando servicio de Internet dedicado.

En este escenario, después del registro, solo se realizan solicitudes de informe de estado a las ONT para no afectar su funcionamiento actual y comenzar a monitorear estos dispositivos. En la Figura 4.24 se pueden observar algunos de estos mensajes. Además, la empresa tiene la opción de configurar y actualizar estos dispositivos a través del sistema.

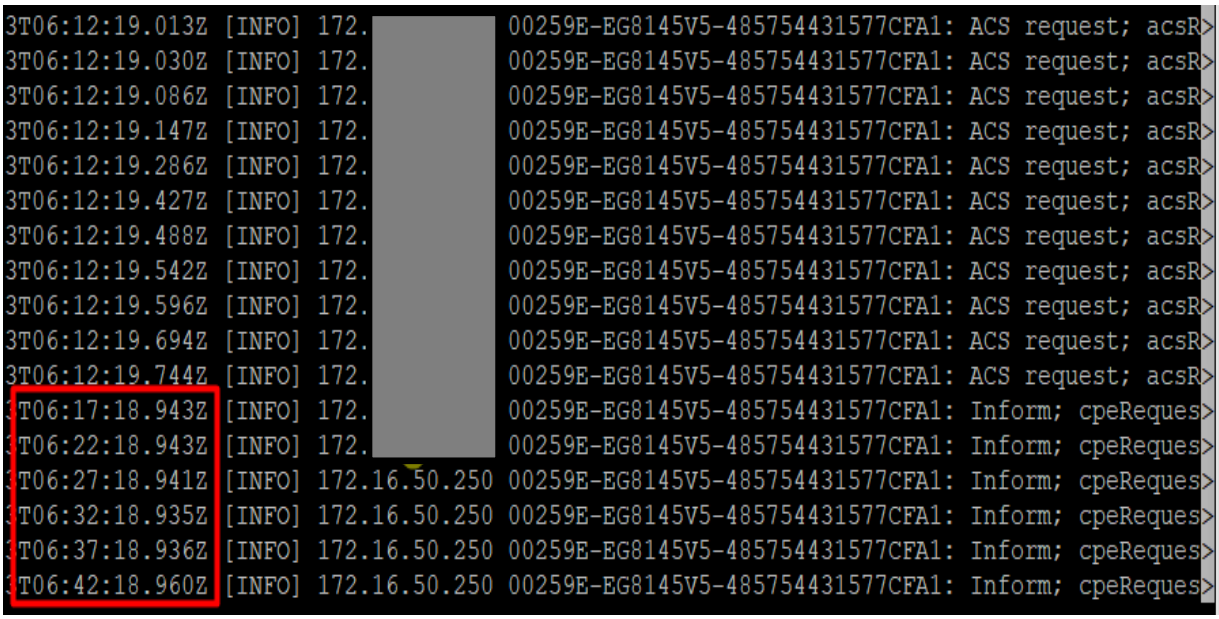

Figura 4.24 Registros Log de las solicitudes de información

En el recuadro rojo se puede observar que la respuesta con el informe de estado por parte de la ONT se realiza cada 5 minutos. Esto se debe a que se estableció en la configuración del ACS en la ONT un valor "inform periodic" de 300 segundos, como se puede ver en la Figura 4.22.

Para realizar configuraciones sencillas no necesariamente se deben crear presets, asiganar eventos que lo disparen ni precondiciones que se deban cumplir, en este caso se realiza un cambio para que los informes de estado de una ONT sean más seguidos y para esto se accede a la interfaz Web, se selecciona el dispositivo y en la parte de “All parameters” se elige *InternetGatewayDevice.ManagementServer.PeriodicInformInterval* que en el recuadro azul se ve que está en 300 segundos, inmediatamente se selecciona el parámetro, se introduce el nuevo valor que ahora será de 200 y se coloca en cola (queue) como se ve en la Figura 4.25.

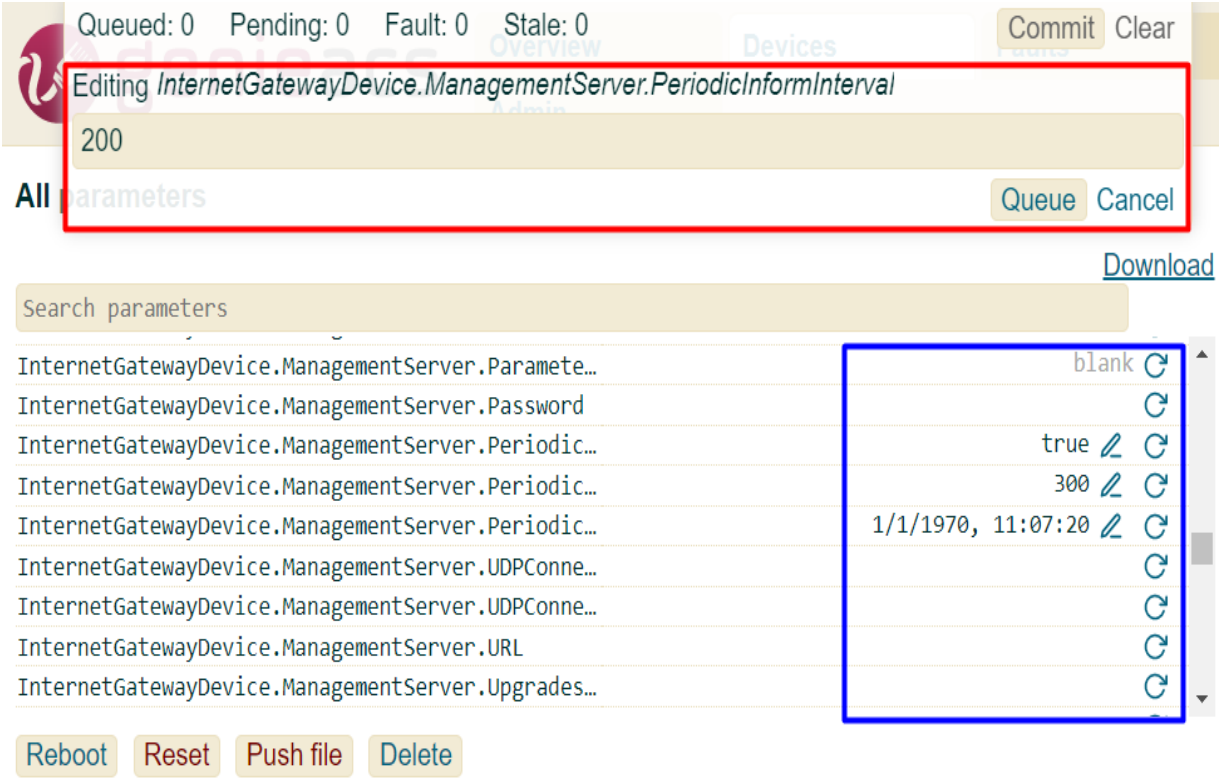

Figura 4.25 Edición de parámetro

Una vez se pone en cola se confirma él envió con el siguiente mensaje ver Figura 4.26.

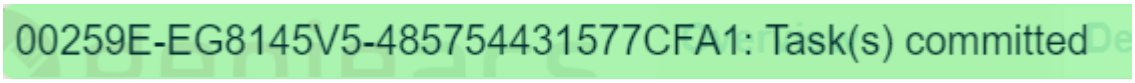

Figura 4.26 Confirmación de Task

Y se verifica el cambio en la interfaz Web de la ONT ver Figura 4.27.

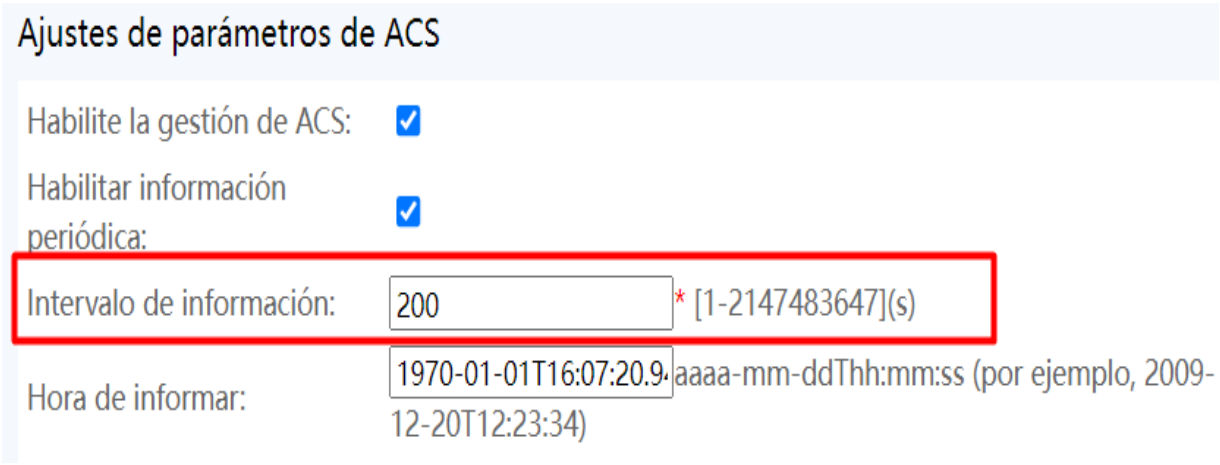

Figura 4.27 Verificación del parámetro editado

Por supuesto no todos los parámetros se pueden editar, algunos solo se pueden leer y los que tienen el signo + es porque no se encuentra establecido este parámetro en la ONT y se puede agregar uno de ser necesario.

4.3 Evaluación del sistema ACS

Para verificar la eficiencia y disponibilidad del sistema se diseña un plan de pruebas donde se interactúa con cada una de las funcionalidades de manera individual y conjunta que se ofrecen y así garantizar el cumplimiento del proyecto.

4.3.1 Plan de pruebas

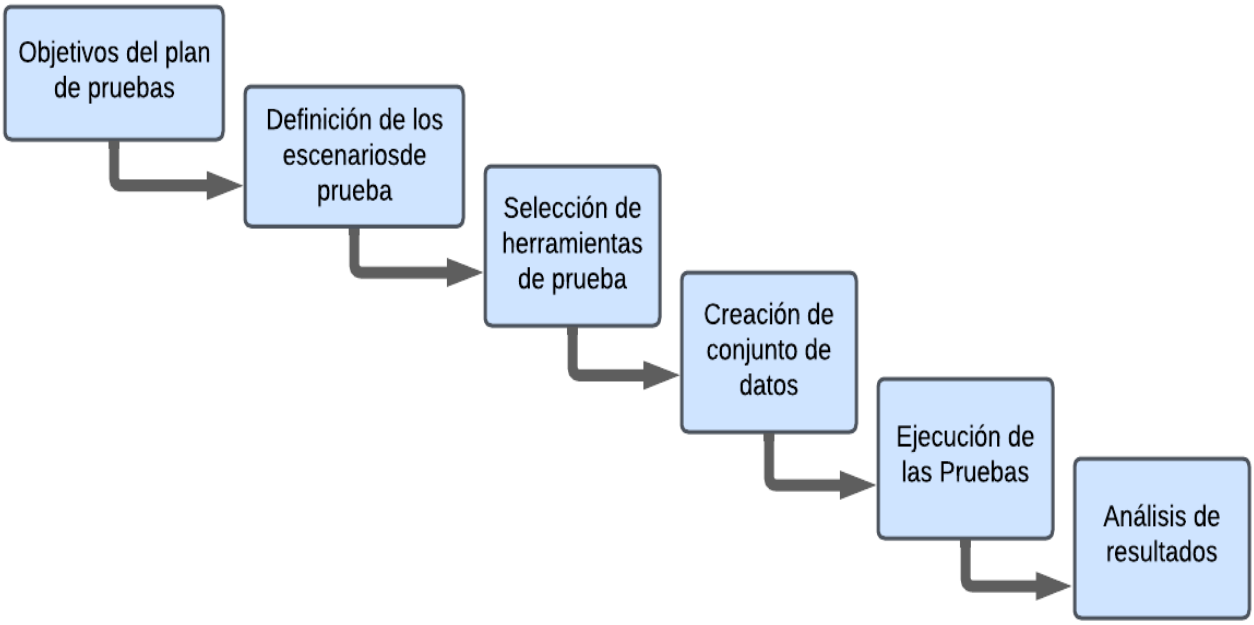

Figura 4.28 Plan de pruebas

4.3.2 Objetivos del plan de pruebas

Probar la estabilidad del sistema, probar la escalabilidad del sistema realizando peticiones al sistema a través de RESTful API y determinar condiciones para uso futuro, detectar errores funcionales en funcionalidades específicas y la complejidad de las mismas, medir el rendimiento del sistema.

4.3.3 Escenarios de prueba:

Lo que se pretende en este paso es identificar los flujos de trabajo críticos del sistema y los casos de uso más comunes, y en ese orden de ideas el caso más crítico es cuando se aplica un RESET al CPE por parte de los usuarios, este error humano es muy común ya que los clientes creen que al realizar esto todas las fallas van a cesar, cuando lo que realmente sucede es que se elimina cualquier configuración e imposibilita brindar servicios por parte del ISP ya que el CPE no se puede autenticar ni autorizar para acceder a los servicios; con este escenario se pone a prueba la capacidad del sistema para restablecer el servicio ante estas fallas. El segundo es cuando un CPE se conecta por primera vez a la red FTTH/GPON y por último están las peticiones a través de RESTful API para integración con software externo.

Los casos de uso más comunes que permite la herramienta GenieACS en cuanto a monitoreo son:

- Disponibilidad de dispositivos en la red.
- Estado de los dispositivos.
- Actividad de dispositivos GenieACS puede monitorear la actividad del dispositivo, como la carga de trabajo del procesador, la memoria que está en ejecución, el estado de ocupación de la memoria, porcentaje de Unidad Central de Proceso (CPU- *Central Processing Unit*) y la cantidad de equipos conectados a la red, lo que permite identificar posibles problemas de rendimiento.
- Firmware y actualizaciones: GenieACS puede monitorear el firmware y las actualizaciones de software para garantizar que los dispositivos estén actualizados y protegidos contra posibles vulnerabilidades.
- Presentación de información oportuna para descubrir fallas en la red.
- Orden jerárquico de acceso al sistema.

La finalidad de definir y poner a prueba estos escenarios es probar la estabilidad del sistema y su impacto en el rendimiento los CPE.

4.3.4 Herramientas de Prueba:

Para verificar el intercambio de mensajes se cuenta con la herramienta tshark que permite filtrar paquetes por un puerto específico o entre dos direcciones IP y los registros log de GenieACS y las ONT para observar el tiempo que tardan los procesos de envío de datos.

4.3.5 Conjunto de datos:

En este paso se recoge la información que es útil para la realización de las pruebas, es por esto que se presenta la siguiente variedad de información con el fin de probar diferentes funcionalidades:

La versión de GenieACS es 1.2.9, los CPE son Huawei de los cuales se tiene EG8145V5 con versión de software V5R019C10S270 y HS8545M5 con versión de software V5R019C00S030 para ONT y Router Cisco CCR1036-12G-4S, servicios de Internet dedicado y banda ancha, se configuraron 3 tipos de usuarios en la interfaz Web de genieACS, Gerencia, Administración y Monitoreo.

4.3.6 Ejecución de pruebas.

Se establecieron tres tipos de pruebas para evaluar el sistema en las condiciones reales de funcionamiento, funcionales, de rendimiento y por último interoperabilidad, en las cuales en las pruebas funcionales se toman de manera individual la disponibilidad, estado, actividad y actualización de los dispositivos en la red. En segundo lugar, se realizaron pruebas de rendimiento del sistema para identificar el consumo de recursos computacionales al agregar nuevos CPE, más configuraciones y aumentando el tiempo de solicitud de información, aumentando así el tráfico de datos que el ACS debe procesar. En tercer lugar, se prueba la capacidad del sistema para trabajar conjuntamente con software externo a través de la API. Y en cuarto lugar se realizaron pruebas de seguridad de acceso a la plataforma y de políticas de seguridad del ACS para la API.

I. Monitoreo de la disponibilidad de los dispositivos en la red.

En esta prueba se tiene un grupo de CPE los cuales van a ser desconectados y reconectados a la red de acceso FTTH paulatinamente sin eliminar su registro en el sistema, esto para poder visual en el panel principal de los dispositivos su cambio de estado con la configuración de colores dependiendo la hora de su último mensaje “inform”.

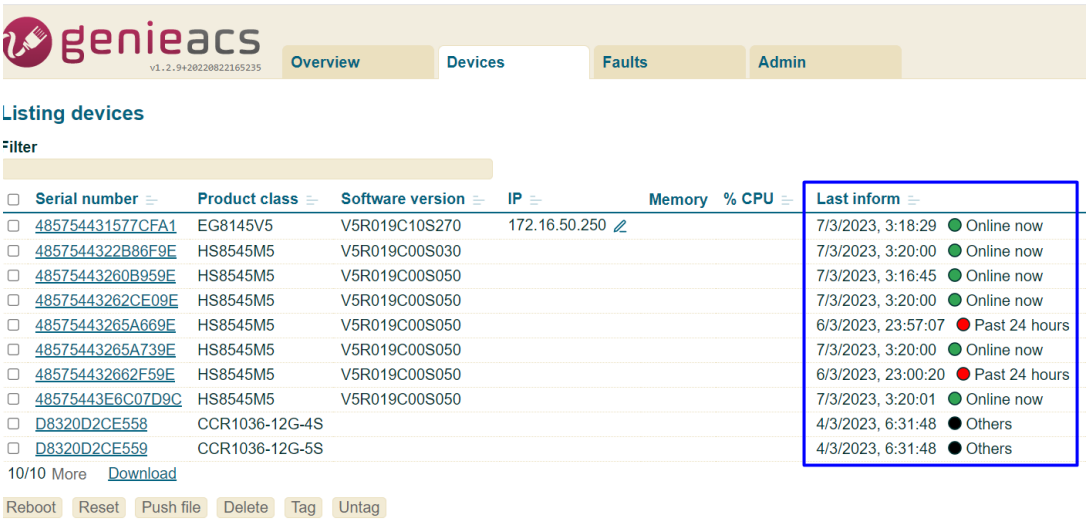

Figura 4.29 Disponibilidad de los dispositivos conectados a la Red FTTH/GPON

En el recuadro azul se puede apreciar la última vez que los dispositivos enviaron un informe de su estado al ACS y además se configuró 3 colores, negro para dispositivos que llevan más de 24 horas desde su último informe, rojo para los que llevan menos de 24 horas desde el último informe y en verde los qué están online.

II. Monitoreo del estado de los Dispositivos.

En esta prueba se toma la información Óptica detallada de los CPE en la red FTTH y se compara con la que se encuentra en la interfaz Web de cada CPE correspondiente y así verificar la exactitud de cada dato presentado por el sistema.

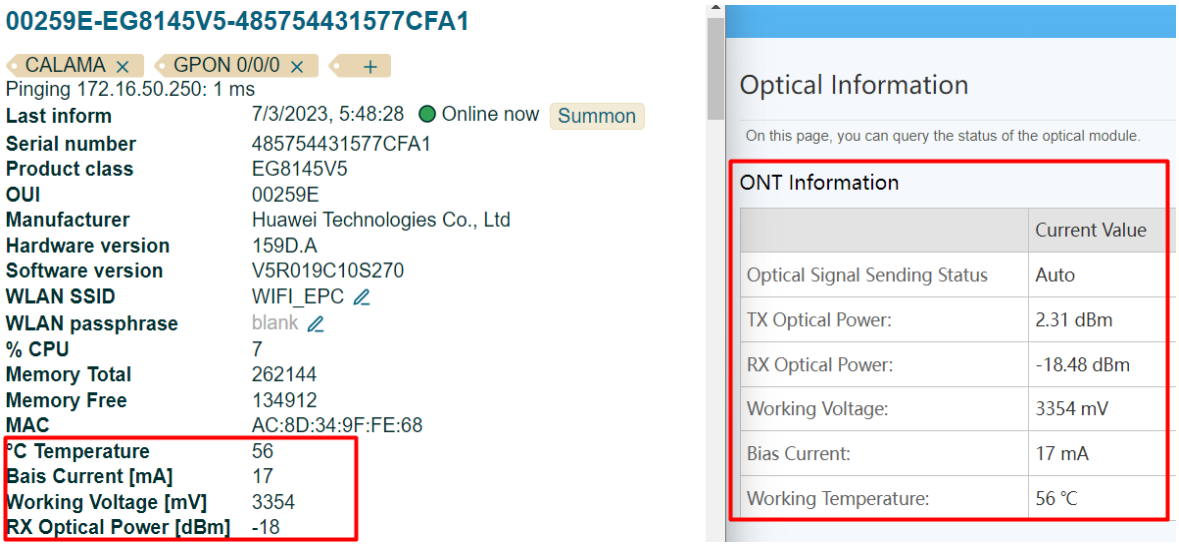

Figura 4.30 Estado de Dispositivos

En la Figura 4.30 se puede observar la exactitud de los datos obtenidos por medio del modelo de datos de tr098, estos datos son relevantes para que la empresa pueda tener certeza de la calidad de servicio qué brinda a sus usuarios.

III. Monitoreo de la actividad del dispositivo.

En esta prueba se toma un grupo de CPE y se verifican los datos que proporciona el sistema con los propios del CPE en su interfaz Web en diferentes horarios para ver más allá de la exactitud de los datos el rendimiento de los mismos en momentos de bastante tráfico de datos.

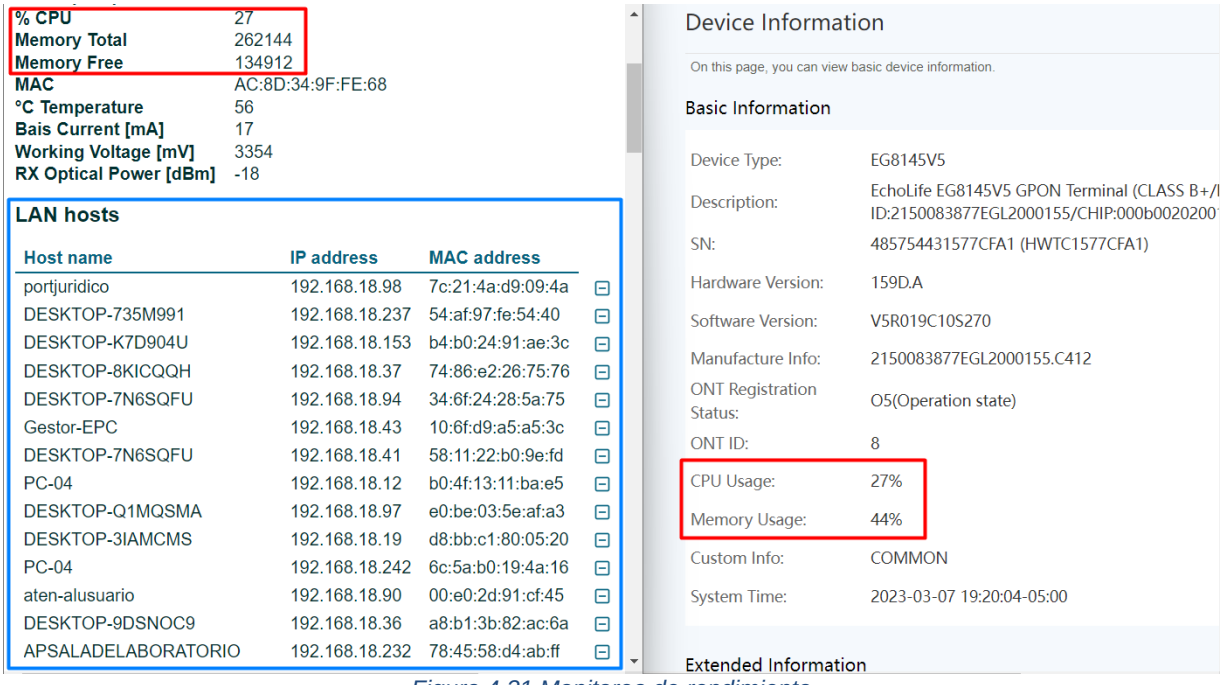

Figura 4.31 Monitoreo de rendimiento

En la Figura 4.31 se puede corroborar la exactitud de los datos que se quieren traer a colación para el monitoreo del rendimiento de los CPE en los entornos a los que son sometido, un factor interesante que se puede apreciar en el recuadro azul es que se puede obtener los datos de todos los dispositivos que estén conectados a la red del usuario sin importar cómo este diseñada su red interna y aunque se pueden realizar varias configuraciones para algunos de estos host, se decidió deshabilitar esas funciones ya que esto se realiza única y exclusivamente para monitorear el rendimiento del CPE.

IV. Monitoreo del firmware y actualizaciones.

En esta prueba se elige un dispositivo en la red con 3 diferentes distintivos “OUI”, “Product Class” y “Version” para asegurarse de seleccionar el dispositivo correcto y se selecciona el tipo de archivo que se quiere enviar, por último se verifica la recepción del archivo en la interfaz de gestión del dispositivo en este caso WINBOX.

Esta prueba se realizó en equipos Mikrotik debido a que en pruebas de actualización de firmware que se realizaron con anterioridad a iniciar el proyecto algunas ONT presentaron fallas al permitir acceso Web a través de la Gateway es por esto que esta función se declaró para los routers Mikrotik.

En este caso se envía un paquete con npk para activar el módulo TR-069 en el mikrotik que después de recibir el archivo solo se debe reiniciar para que instale el nuevo módulo.

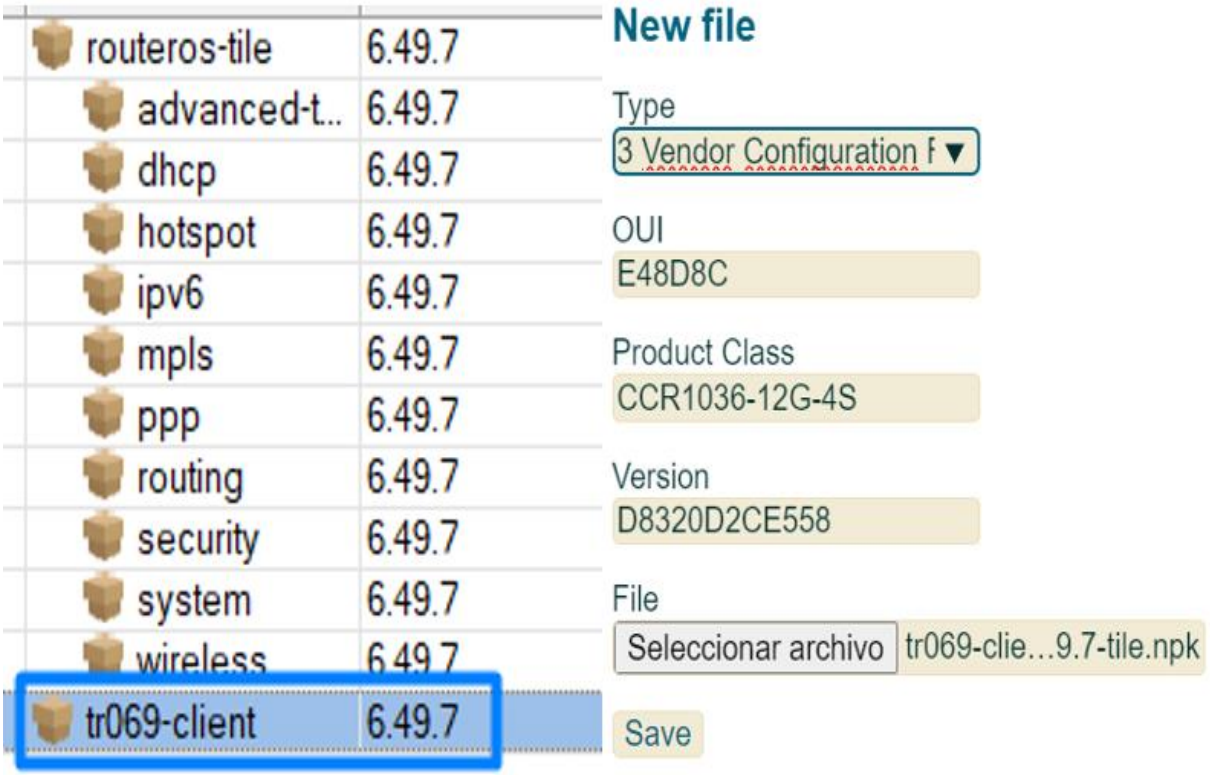

Figura 4.32 Envío de pakage npk

V. Información oportuna.

En este caso se desea que al momento de presentarse fallas en la red, el sistema pueda presentar información que sea útil para encontrar la falla y repararla lo antes posible, una de las mejores formas para ayudar a ubicar un posible daño de fibra donde pueda ocurrir una masiva afectación es agrupar por sectores y por la interfaz GPON de la que están conectados.

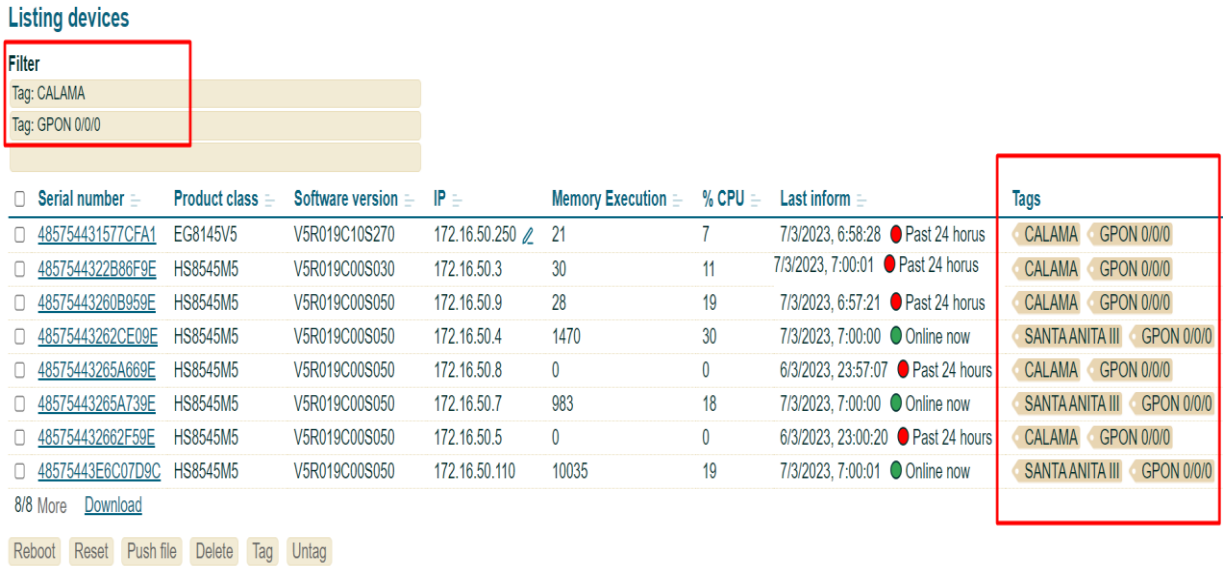

Figura 4.33 Tags

Los Tags son una herramienta para agrupar CPE y en este caso esos Tags ayudaron a determinar que el daño no se encontraba en el splitter principal dado que tres CPE seguían en línea, aunque en un barrio aledaño pertenecen a la misma interfaz GPON así que el daño de fibra bajo ninguna circunstancia se solucionará en el splitter principal, y así dirigir los esfuerzos en la FAT donde desprende el ramal que conecta estas tres CPE.

VI. Orden jerárquico de acceso al sistema.

Es muy importante mantener el control de acceso a esta herramienta, dado que desde ella se puede por equivocación no solo afectar el servicio de un solo usuario sino de todos los dispositivos en la red de manera inmediata y es por esto que se debe establecer un orden.

Primero, es necesario crear los tres perfiles: gerencia, admin y monitor. Gerencia tendrá todos los permisos, mientras que admin no podrá editar usuarios existentes y monitor solo podrá acceder a los dispositivos y parámetros virtuales. Después, se debe ingresar a la interfaz web y verificar que las opciones restringidas para cada perfil no estén disponibles.

El primer perfil que se prueba es el de la gerencia y como se ve en la Figura 4.34 tiene todas las opciones disponibles que ofrece el Frontend de GenieACS.

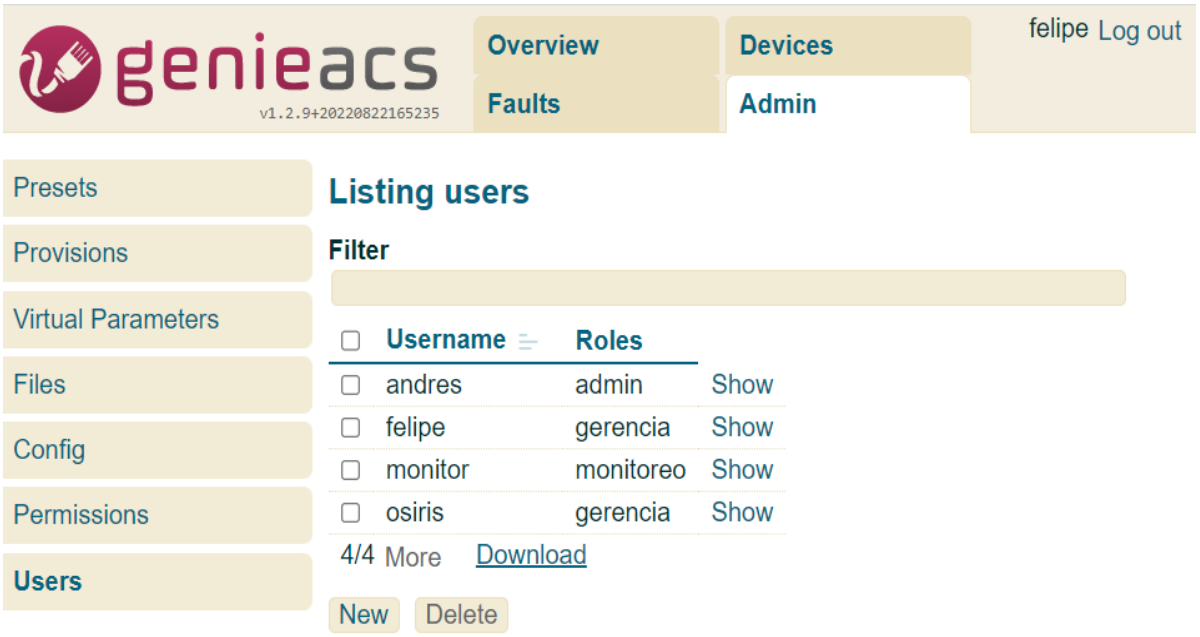

Figura 4.34 Perfil gerencia

En la Figura 4.35 se observa que en el panel de la izquierda ya no se encuentra la pestaña de usuarios. Por tanto, la gestión del acceso a la plataforma queda exclusivamente en manos de la gerencia.

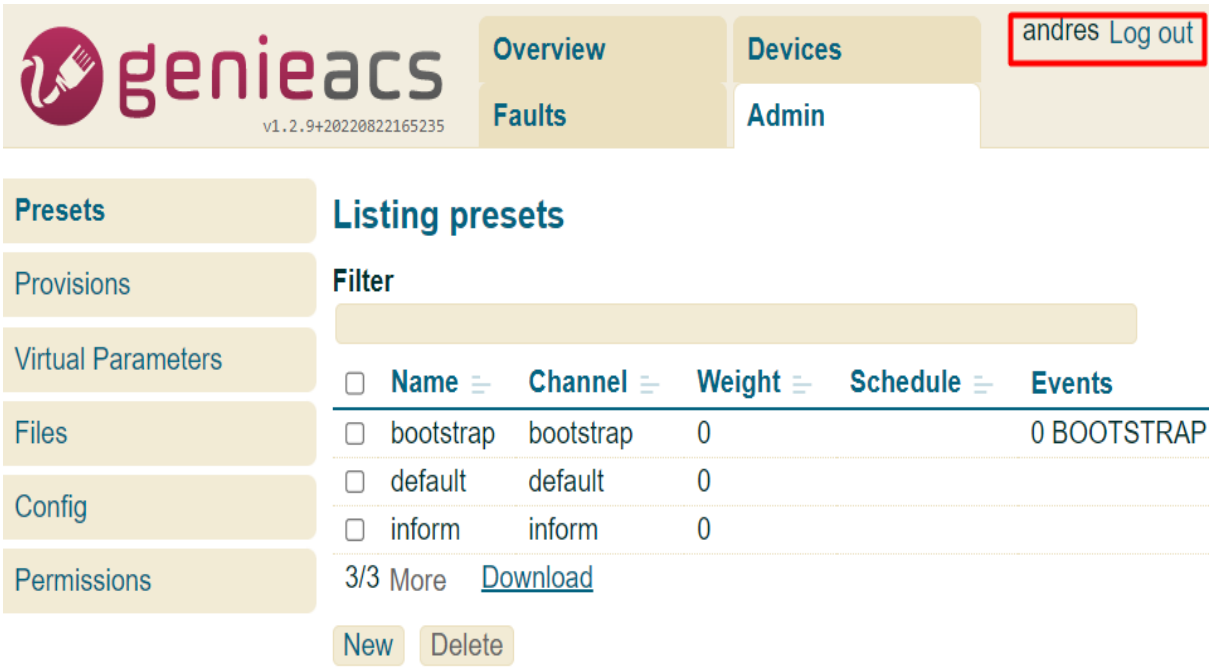

Figura 4.35 Perfil admin

En la Figura 4.36 se aprecia que al perfil de monitor se habilita los parámetros virtuales para realizar configuraciones sencillas que no afecten la conexión a la red del dispositivo en cuestión y de ningún otro a través de los presets.

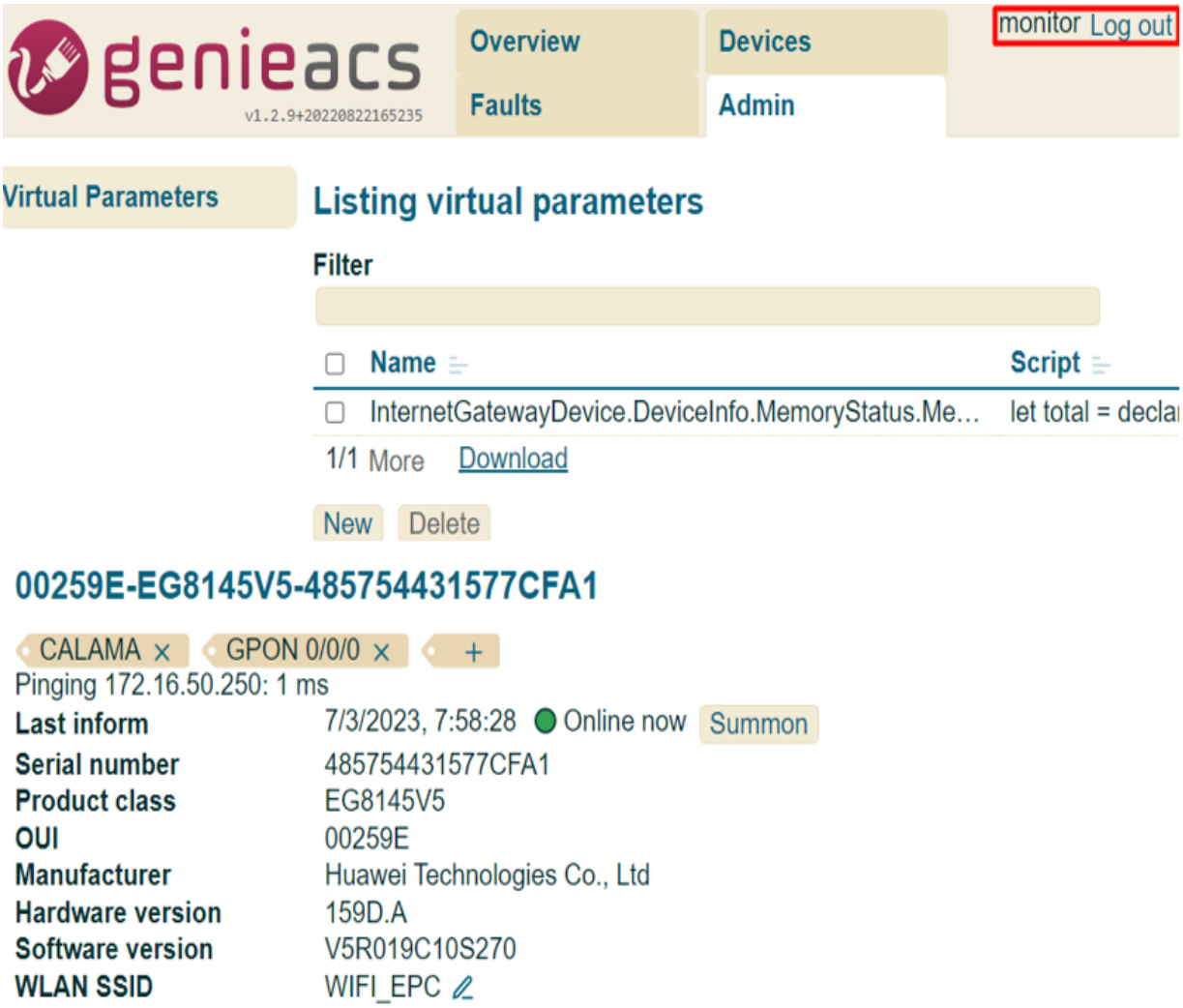

Figura 4.36 Perfil monitor

4.3.7 Escenarios complejos.

Para los casos donde una ONT se le aplica un “reset” y regresa a su configuración de fábrica o cuando una ONT se conecta por primera vez a la red el proceso es el mismo, y es que para esto se puede diseñar una cadena de presets que se ejecuten cuando una ONT tuvo un “reset” o cuando recibe una solicitud de conexión por primera vez. En este caso se diseñaron dos preset “Detectar” y “reconfigurar”.

Al preset “Detectar” se le asigna un weight de 0 y una “provision” con el mismo nombre “Detectar”, esta “provision” es un script que se suscribe a los parámetros de Connection Request y espera a que llegue el Connection Request Username para verificar si la WAN ya está configurada o no. Si no está configurada, activa el preset “reconfigurar”.

El preset “reconfigurar” se le asigna un peso de 1, la precondición de que se haya ejecutado el preset “Detectar” y una “provision” con el mismo nombre “reconfigurar”, este script establece los parámetros de la conexión WAN PPPoE y las vinculaciones LAN y WLAN correspondientes en un dispositivo de red.

Cada línea comienza con “declare”, que es una función utilizada en la plataforma TR-069 para declarar y configurar parámetros. A continuación, se proporciona el nombre del parámetro y el valor que se le asignará.

Para la conexión WAN PPPoE, se establecen los siguientes parámetros:

ServiceName: se establece en "Internet"
Enable: se habilita la conexión PPPoE
LinkType: se establece en "IPV4"
Name: se establece en "WAN PPPoE"
X_HW_VLAN: se establece en "201"
X_HW_8021p: se establece en "0"
X_HW_LCPEnable: se habilita la detección de enlaces LCP
X_HW_LCPDetectionEnable: se habilita la detección de LCP
X_HW_MRU: se establece en "1492"
Username: se establece en "******"
Password: se establece en "*******"

Luego se vinculan las interfaces LAN y WLAN al dispositivo de conexión WAN PPPoE establecido anteriormente:

InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.1.WANConnectionDevice: se establece en "InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1"
InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.2.WANConnectionDevice: se establece en "InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1"
InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.3.WANConnectionDevice: se establece en "InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1"
InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.4.WANConnectionDevice: se establece en "InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1"
InternetGatewayDevice.LANDevice.1.WLANConfiguration.1.WANConnectionDevice: se establece en "InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1"

Es de recordar que al sufrir un reset la ONT pierde los datos de configuración del ACS y es por eso que se deben reenviar desde la OLT por medio del siguiente comando

```
TELCOFIBER>enable

TELCOFIBER#config

TELCOFIBER(config)#interface gpon 0/0

TELCOFIBER(config-if-gpon-0/0)#ont tr069-server-config 0 0 profile-id 30

TELCOFIBER(config-if-gpon-0/0)#
```

Figura 4.37 Envío de datos del ACS desde la OLT

Entonces para entender un poco mejor lo que ocurre aquí, se explica lo que sucede con el comando “ont tr069-server-config 0 0 profile-id 30” y es que en la primera parte “ont tr0g9-server-config” se utiliza en una interfaz GPON de la OLT para configurar la conexión TR069 para una ONT específica conectada a esa interfaz. Los dos ceros seguidos indican ONT-SLOT que es el número de ranura de la ONT y ONT-PORT que es número de puerto de la ONT y el PROFILE-ID es el ID del perfil TR069. Una vez se ejecuta este comando la ONT recibe los datos de configuración del ACS casi de inmediato.

Una vez se establece la conexión entre el ACS y el CPE empieza la comunicación RPC en la cual el ACS recibe el estado actual del CPE y lo almacena en su base de datos, pero esto no significa que el CPE ya quedará registrado en el ACS queda en un estado como se observa en la Figura 4.38 en el que aparece en la base de datos, y en la interfaz de Web de GenieACS online e incluso llamar algunos datos, sin embargo no se le pueden enviar tareas, realizar ping, sus parametros virtuales se limitan demasiado y por supuesto no permite enviarle ningún preset.

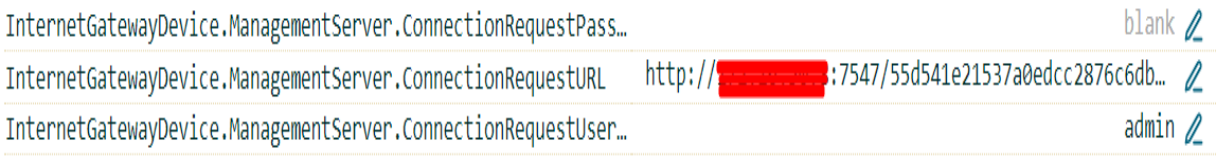

Figura 4.38 Registro inconcluso

Es aquí donde el preset Detectar toma importancia porque crea de manera aleatoria el Username y Password y los envía al CPE y se verifican en la interfaz WEB tanto de la ONT cómo de GenieACS.

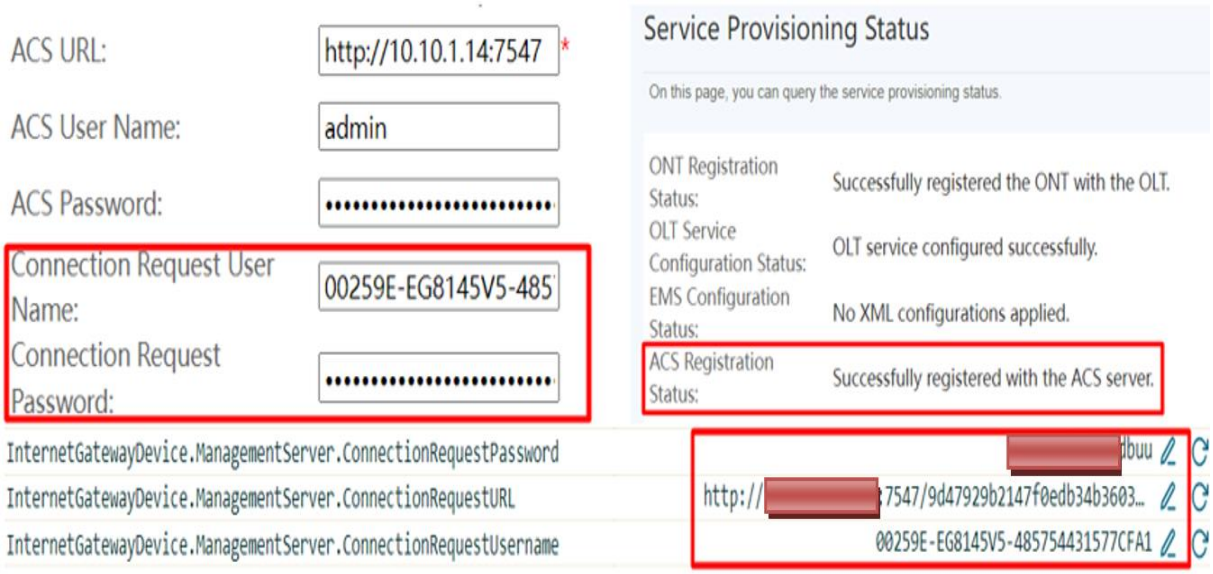

Figura 4.39 Verificación de Registro exitoso

Cuando el registro es exitoso el ACS espera que el CPE le envíe los datos de Connection Request y así activar automáticamente el preset “reconfigurar” para crear la WAN. La “provision” de este preset se encarga de activar el preset “reconfigurar” una única vez porque de lo contrario se crearía la WAN cada vez que se reciba un informe periódico por parte del CPE.

Y así queda configurada y aprovisionada la WAN en la ONT ver Figura 4.40.

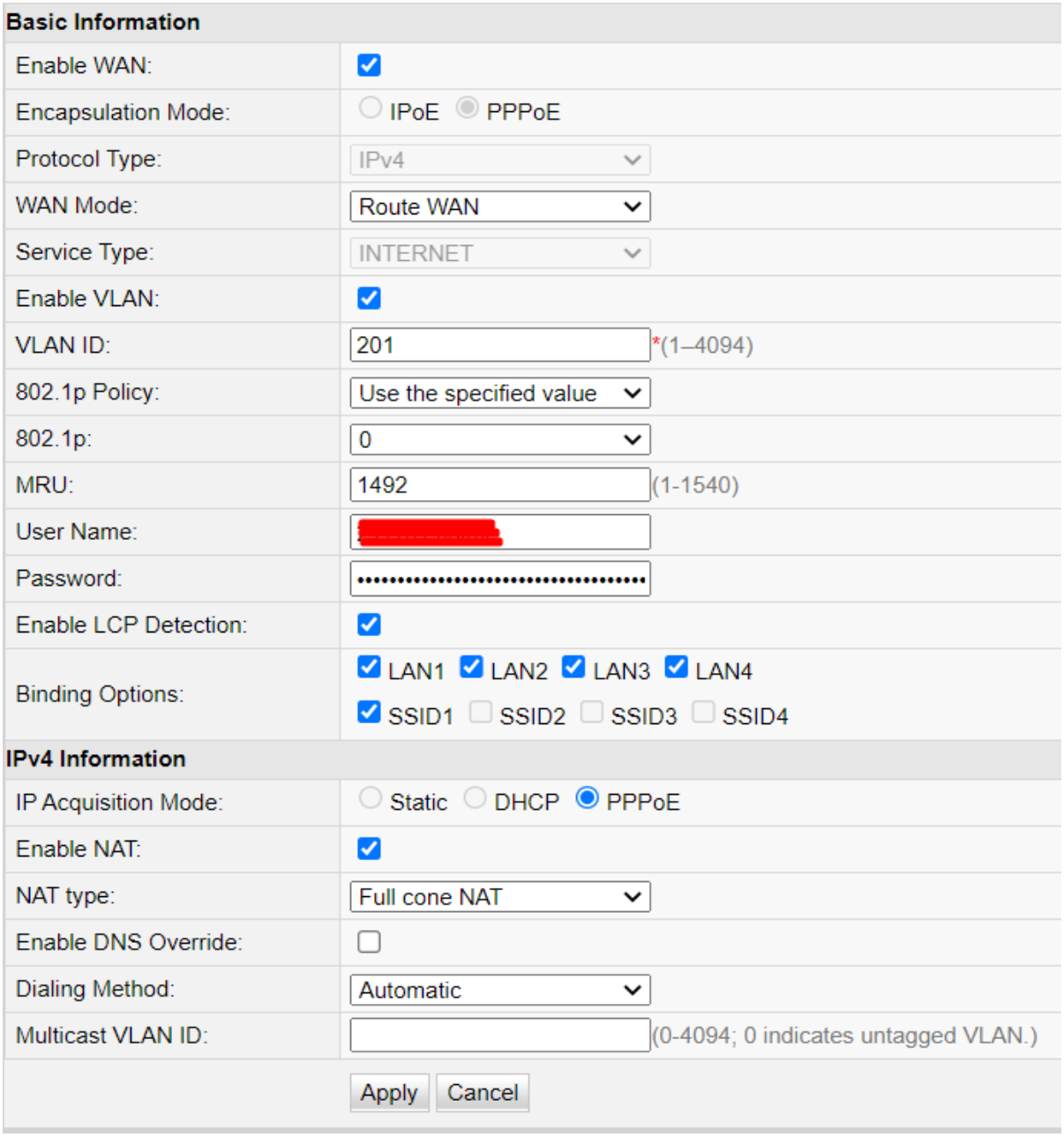

Figura 4.40 Aprovisionamiento WAN PPPoE

Nota: si se requiere crear más conexiones WAN se pueden añadir al mismo script o crear un script y agregarlo a un nuevo preset y con la precondición de que se cumpla el preset “reconfigurar”.

Se debe probar el funcionamiento de la API para futuras implementaciones y para esto se realizaron dos casos, el primero que es una petición POST desde una conexión VPN a la API para solicitar la información completa de todos los dispositivos almacenados en la base de datos.

Para esto se crearon dos archivos genie.js y genie.html en la Figura 4.41 se observa el código para genie.js.

```
// Habilitar CORS en la respuesta
const corsHeaders = {
    'Access-Control-Allow-Origin': '*',
    'Access-Control-Allow-Methods': 'GET,PUT,POST,DELETE,PATCH,OPTIONS',
    'Access-Control-Allow-Headers': 'Content-Type, Authorization, Content-Length, X-Requested-With'
  };

// configuración de la API de GenieACS
const genieacsApiCon[redacted]
  baseURL: 'http://10.10.1.14:7557',
  auth: {
    username: 'admin',
    password: 'RAd10m0l0t0v7.*'
  }
};

// función para obtener los datos de los dispositivos
async function getDevices() {
  try {
    const response = await axios.get('/devices', genieacsApiConfig);
    return response.data;
  } catch (error) {
    if (error.response && error.response.data) {
        console.error(error.response.data);
      } else {
    console.error(error);
  }
 }
}
// obtener los datos de los dispositivos
async function main() {
    const devices = await getDevices();
    console.log(devices);
}
main();
```

Figura 4.41 Archivo genie.js

Este archivo .js es un script en JavaScript que habilita CORS (Cross-Origin Resource Sharing) en la respuesta y configura una API de GenieACS. El script también contiene una función asincrónica "getDevices()" que utiliza la biblioteca Axios para realizar una solicitud HTTP GET a la ruta '/devices' de la API de GenieACS y retorna los datos de respuesta en formato JSON.

La función "main()" utiliza la función "getDevices()" para obtener los datos de los dispositivos, y luego los registra en la consola utilizando la función "console.log()".

El archivo HTML tiene la estructura que se ve en la Figura 4.42.

```html
<!DOCTYPE html>
<html>
<head>
  <title>Ejemplo GenieACS API</title>
  <meta charset="utf-8">
  <script src="https://unpkg.com/axios/dist/axios.min.js"></script>
  <script src="genie.js"></script>
</head>
<body>
  <h1>Dispositivos en GenieACS</h1>
  <ul id="devices-list"></ul>
  <script>
    // función para obtener los datos de los dispositivos
    async function getDevices() {
      try {
        const response = await axios.get('/devices', genieacsApiConfig);
        return response.data;
      } catch (error) {
        console.error(error);
      }
    }
    // función para agregar los dispositivos a la lista
    function renderDevices(devices) {
      const devicesList = document.getElementById('devices-list');
      devices.forEach(device => {
        const li = document.createElement('li');
        li.textContent = device._id;
        devicesList.appendChild(li);
      });
    }
    // obtener los datos de los dispositivos y renderizarlos en la lista
    getDevices().then(devices => {
      if (devices) {
        renderDevices(devices);
      } else {
        console.error('No se pudieron obtener los dispositivos');
      }
    });
  </script>
</body>
</html>
```

Figura 4.42 Archivo genie.html

Al ejecutar este archivo html, en la consola del navegador se encuentra el siguiente error.

```
Access to XMLHttpRequest at 'http://1[redacted]:7557/devices' from origin 'null' has been blocked  genie.html:1
by CORS policy: Response to preflight request doesn't pass access control check: No 'Access-Control-Allow-
Origin' header is present on the requested resource.
```

Figura 4.43 Error Políticas CORS

Este error indica que el servidor en http://10.**.**.**:7557 no está permitiendo que la solicitud se realice desde el origen (dominio, protocolo y puerto) que estás utilizando. En otras palabras, el servidor está configurado con una política de seguridad de intercambio de recursos de origen cruzado (CORS) que bloquea las solicitudes desde orígenes que no están explícitamente permitidos.

En este caso, la solicitud está siendo realizada desde un origen "null" que es común cuando se ejecuta una página localmente en el navegador. El servidor debe incluir en su respuesta un encabezado "Access-Control-Allow-Origin" que permita la solicitud desde el origen especificado. Como se puede ver en el archivo .js proporcionado, se incluye un encabezado "Access-Control-Allow-Origin: *" en la respuesta para permitir todas las solicitudes desde cualquier origen. Sin embargo, en este caso, la respuesta del servidor no está incluyendo ese encabezado, lo que provoca el error. Aunque no se puede visualizar los datos como se pretende con el archivo genie.html si se pueden ver en formato json, ver Figura 4.44.

Gmail YouTube Maps TR-069 Training | q... TR069 Managemen... Página 2 de ¿Cómo...


```
[
{"_id":"E48D8C-CCR1036%2D12G%2D4S-D8320D2CE558","Device":{"DeviceInfo":{"HardwareVersion":
{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:string","_value":"v1.0"},"ProvisioningCode":
{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:string","_value":""},"SoftwareVersion":
{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:string","_value":"6.49.7"},"_object":true},"ManagementServer":
{"AliasBasedAddressing":{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:boolean","_value":false,"_writable":false},"ConnectionRequestPassword":
{"_object":false,"_timestamp":"2023-03-
04T11:31:48.132Z","_type":"xsd:string","_value":"1zenyvzzndw","_writable":true},"ConnectionRequestURL":
{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:string","_value":"http://10.10.1.1:7547/24fc883a81dfd3d1623e25a56dba1a599
984","_writable":false},"ConnectionRequestUsername":{"_object":false,"_timestamp":"2023-03-
04T11:31:48.132Z","_type":"xsd:string","_value":"E48D8C-CCR1036%2D12G%2D4S-
D8320D2CE558","_writable":true},"InformParameter":
{"_object":true,"_writable":true},"InformParameterNumberOfEntries":
{"_object":false,"_writable":false},"ParameterKey":{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:string","_value":"","_writable":false},"Password":
{"_object":false,"_writable":true},"PeriodicInformEnable":{"_object":false,"_timestamp":"2023-03-
04T11:31:48.131Z","_type":"xsd:boolean","_value":true,"_writable":true},"PeriodicInformInterval":
{"_object":false,"_timestamp":"2023-03-
04T11:31:48.131Z","_type":"xsd:unsignedInt","_value":300,"_writable":true},"URL":
{"_object":false,"_writable":true},"Username":
{"_object":false,"_writable":true},"_object":true,"_timestamp":"2023-03-
04T08:18:24.905Z"},"RootDataModelVersion":{"_object":false,"_timestamp":"2023-03-
04T11:31:48.128Z","_type":"xsd:string","_value":"2.11"},"_object":true,"_writable":false},"_deviceId":
{"_Manufacturer":"MikroTik","_OUI":"E48D8C","_ProductClass":"CCR1036-12G-
4S","_SerialNumber":"D8320D2CE558"},"_lastBoot":"2023-03-04T08:18:24.905Z","_lastInform":"2023-03-
04T11:31:48.127Z","_registered":"2023-03-04T08:18:24.905Z","_timestamp":"2023-03-
04T11:31:48.127Z","_tags":["Mikrotik"]},
{"_id":"E49D8C-CCR1036%2D12G%2D5S-D8320D2CE559","Device":{"DeviceInfo":{"HardwareVersion":
```


Figura 4.44 Respuesta en formato json

Lo que verifica que la API funciona correctamente solo que para ser implementada de una manera adecuada se deben considerar varios factores de seguridad.

Aunque la API RESTful de GenieACS es una forma conveniente de interactuar con los datos de GenieACS, no es recomendable que un software externo interactúe directamente con ella. Esto se debe a que la API puede exponer información sensible y permitir acciones peligrosas como eliminar dispositivos o cambiar parámetros críticos.

Por lo tanto, se recomienda utilizar un servidor intermedio que actúe como un "proxy" o intermediario entre el software externo y la API de GenieACS. El servidor intermedio puede autenticar y autorizar al software externo, así como limitar y controlar las acciones que se pueden realizar en la API de GenieACS. Además, el servidor intermedio también puede realizar tareas adicionales como el caching, la optimización de solicitudes, el manejo de errores, etc.

De esta manera, se mejora la seguridad de la integración y se reduce el riesgo de que la información sensible sea expuesta o manipulada por software no autorizado.

ES importante aclar que en los escenarios complejos se toma solo una cadena de preset, sin embargo, se crearon otros para diferentes objetivos, pero el modo de operación es el mismo.

4.3.8 Análisis.

I. Prueba del ACS para monitoreo de la disponibilidad de dispositivos.

a. Visualización de los resultados: La prueba muestra una visualización clara de los resultados a través de un cuadro de estado que utiliza diferentes colores para representar la disponibilidad de los dispositivos. Esto es útil para tener una rápida identificación visual de los dispositivos que están en línea y aquellos que no lo están.

b. Configuración de los colores: La configuración de los colores utilizados para representar el estado de los dispositivos es importante, ya que permite identificar fácilmente aquellos que han enviado un informe de estado recientemente y aquellos que no lo han hecho en más de 24 horas. Esto permite que el administrador pueda tomar acciones en consecuencia.

c. Actualización de los datos: Es importante verificar si los datos se actualizan regularmente y si se están recopilando los datos correctos. En este caso, la prueba ha sido exitosa y los datos se están actualizando correctamente.

d. Acciones a tomar: Finalmente, es importante evaluar si se están tomando las acciones necesarias en consecuencia a la información proporcionada por la prueba. Por ejemplo, en este caso, los dispositivos que no han enviado un informe de estado en más de 24 horas son mikrotik y es porque es mucho más sencillo gestinarlos por RouterOS y los archivos se pueden subir y programar su envió desde GenieACS cuando se requiera

por ende era mejor desconectarlos del servidor para que el mikrotik no eleve su nivel de procesamiento ni llene de información irrelevante la memoria del ACS.

II. Prueba del ACS para monitoreo del estado de los dispositivos.

En esta prueba se determinó la exactitud con la que el ACS hace lectura de los parámetros de funcionamiento de una ONT comparando los datos presentados por el sistema en el panel principal de los dispositivos con la información que brinda la interfaz Web de cada CPE, pero este resultado va más allá, porque si se aumenta considerablemente el tiempo del "inform periodic" pueden ocurrir desfases entre los resultados que brinda el ACS y los que se ven en la interfaz de la ONT.

III. Prueba de Monitoreo de la actividad de dispositivos.

Esta prueba es de suma relevancia para el aprovechamiento del sistema por parte de la empresa, puesto que brinda la información constante para realizar un balance entre el trabajo al que está siendo sometido el CPE y los recursos propios del dispositivo y esto ayuda a corroborar lo dicho en la prueba anterior, y es que al momento de realizar esta prueba el CPE tenía 159 dispositivos conectados como se ve en la Figura 4.45, y apenas tenía en uso un 27% de CPU y la capacidad de su memoria menor al 50%.

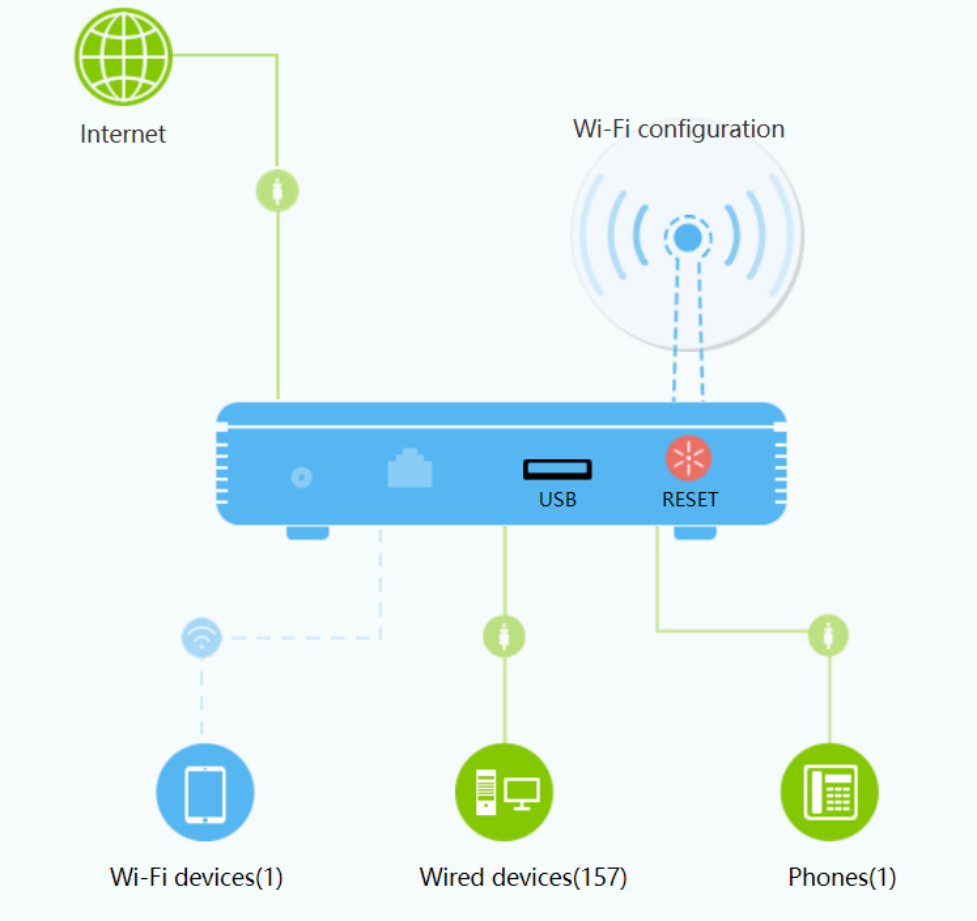

Figura 4.45 Dispositivos conectados a un CPE

IV. Prueba de Monitoreo de firmware y actualizaciones.

A pesar de que no se pudo probar en las ONT, su desarrollo fue todo un éxito para dispositivos Mikrotik en cuanto a la velocidad de carga del archivo en relación al tamaño del mismo pues el archivo npk que contiene el módulo de instalación de tr069 pesa 272KB y el pakage que contiene todos los módulos tiene un tamaño de 22MB que no es más de lo que pesa cualquier firmware de ONT.

V. Prueba de presentación de información oportuna para descubrir fallas en la red.

En esta prueba se estableció que la información presentada por el ACS tiene relevancia para la toma de decisiones oportunas para optimizar el proceso de servicio técnico, agrupar los dispositivos por etiquetas y la opción que se configuró para que se pueda tener varias opciones de filtrado es muy útil para descartar sectores donde un posible fallo en la fibra pueda estar generando molestias en la prestación de servicios y no solo eso, agrupar por etiquetas de un nuevo modelo de CPE o uno muy antiguo que se esté usando permite monitorearlos de forma más personalizada y retirarlos del servicio de ser necesario.

VI. Prueba de orden jerárquico.

Esta prueba tiene una intención muy clara y es poder asignar responsabilidades garantizando que no habrá intromisiones en la labor de un operario del sistema, así una vez definidas las responsabilidades que se le asignan a una persona también se puede supervisar el cumplimiento de las mismas pues solo ese operario tiene acceso a las funcionalidades que le corresponden, además todas sus acciones dentro del sistema quedan en los registros log etiquetados por su perfil.

VII. Prueba de aprovisionamiento después de un reset.

Esta prueba requirió de bastantes iteraciones para obtener un resultado exitoso ya que el modelo de datos puede variar dependiendo del firmware de la ONT y de la versión de GenieACS, cómo se trabajó con la versión más reciente no se encuentra la suficiente información sobre el modelo de datos y a pesar de que la comunidad de desarrollo es activa en el foro oficial de GenieACS, fue una tarea tediosa y que requirió bastante tiempo, sin embargo sin importar lo engorroso que pudo ser el proceso de creación de los preset, su funcionamiento es todo un éxito ya que los presets se ejecutan bastante rápido, una ONT que acaba de sufrir un reset tarda entre 30 a 40 segundo en tener aprovisionada la conexión WAN.

VIII. Prueba API para escalabilidad del sistema.

Debido a la potencial cantidad de dispositivos que se puedan llegar a gestionar a través de GenieACS se hace necesario pensar en una posible integración con un software externo que permita utilizar los datos que extrae el ACS de los CPE y los use con otros sistemas que también ayudan a la gestión de la red, también se puede pensar en enviar datos,

configuraciones enteras desde un software externo y todo se haría a través de la API, así que la prueba no solo era para verificar su configuración en las variables de entorno del ACS, si no probar su nivel de seguridad y es precisamente este punto el más importante de la API, por lo pronto CORS cumple su objetivo pero si se piensa en integración con software externo.

IX. Prueba de rendimiento del sistema y afectación a los CPE.

Las pruebas de monitoreo y configuración de parámetros realizadas anteriormente tuvieron 29 iteraciones variando el “Inform periodic”, las primeras 10 aumentando cada iteración 30 segundos hasta llegar 300 segundos, a partir de ahí el aumento era de 300 segundos hasta llegar a 6000 segundos, en un inicio se toma un periodo muy corto para determinar si está periodicidad tenía alguna consecuencia en el nivel de CPU o memoria pero esto no fue así, El uso de CPU sube mientras se está usando la interfaz Web del CPE y aun así ese aumento no supera el 3%. Sin embargo, en GenieACS al tener 30 segundos de periodicidad en los informes y tareas en bucle por error de codificación a más de 150 CPE se hizo necesario aumentar un núcleo más a la máquina virtual en el Hipervisor Citrix para que el servidor pueda procesar todas las solicitudes.

5 CAPÍTULO: CONCLUSIONES Y TRABAJOS FUTUROS.

I. El sistema ACS que utiliza el protocolo CWMP permite al ISP reducir significativamente el tiempo de respuesta ante las fallas reportadas por los usuarios en los CPE. Este es el mayor beneficio que ofrece el sistema al ISP, ya que la ejecución de un preset se refleja en pocos segundos en las ONT, ya sea para reconfigurar o editar un parámetro. Esto evita la necesidad de enviar un equipo técnico hasta la ubicación del usuario, lo que representa un ahorro en tiempo y costos para el proveedor de servicios de Internet.

II. GenieACS es una herramienta sumamente útil para los ISP, ya que proporciona información detallada para identificar las causas de las fallas y así prevenir problemas futuros. Además, permite analizar el rendimiento del CPE en su función diaria, considerando el número de usuarios conectados, el porcentaje de uso de CPU y de memoria, lo que permite diagnosticar y prevenir situaciones de colapso en los CPE. En resumen, GenieACS es una herramienta esencial para la optimización del servicio técnico de los ISP.

III. La aplicación del modelo de datos TR-098 puede resultar un poco tediosa, ya que no se encuentra mucha información más allá de la proporcionada por el Broadband Forum. Sin embargo, es necesario destacar que la comunidad de desarrollo de GenieACS es muy activa y colaborativa, incluso en su versión gratuita. Además, el foro de Huawei ofrece ayuda para la implementación de TR-069 en sus equipos. Aunque el acceso premium de GenieACS tiene un costo, la comunidad de desarrollo y el foro de Huawei son herramientas valiosas y gratuitas para quienes deseen implementar este modelo de datos.

IV. Aunque la API RESTful de GenieACS es una forma conveniente de interactuar con los datos de GenieACS, no es recomendable que un software externo interactúe directamente con ella. Esto se debe a que la API puede exponer información sensible y permitir acciones peligrosas como eliminar dispositivos o cambiar parámetros críticos.

    Por lo tanto, se recomienda utilizar un servidor intermedio que actúe como un "proxy" o intermediario entre el software externo y la API de GenieACS. El servidor intermedio puede autenticar y autorizar al software externo, así como limitar y controlar las acciones que se pueden realizar en la API de GenieACS. Además, el servidor intermedio también puede realizar tareas adicionales como el caching, la optimización de solicitudes, el manejo de errores, etc.

V. A pesar de que CWMP es poco conocido en el ámbito de acceso a Internet, es indispensable si se pretende administrar volúmenes grandes de dispositivos, ya que permite una gestión y configuración remota de dispositivos de red de manera estandarizada y segura, lo que facilita enormemente el trabajo de los proveedores de servicios y los administradores de red. Al utilizar un protocolo estándar, se evitan las incompatibilidades entre diferentes dispositivos y sistemas de gestión, lo que reduce los errores y acelera los procesos de gestión de la red.

Además, CWMP es un protocolo seguro que utiliza el cifrado de extremo a extremo para proteger los datos de configuración y gestión durante la transmisión. Esto garantiza que los datos sensibles no sean interceptados ni manipulados por terceros no autorizados.

VI. GenieACS es una plataforma de gestión de dispositivos de código abierto que proporciona una solución escalable y flexible para la gestión de dispositivos, es altamente personalizable y no afecta su funcionamiento con cantidades grandes de dispositivos, además de que su interfaz Web es muy intuitiva y fácil de usar.

VII. Una de las grandes falencias de los ISP en la prestación de sus servicios es el soporte técnico, ya que es proporcional al crecimiento la empresa, esta área consume más dinero cada día y por eso es necesario reducir los índices de costos operativos para tener una rentabilidad adecuada, y es por esto que este sistema ACS usando CWMP en la red FTTH/GPON se implementó para hacer en segundos lo que antes se tardaba horas.

5.1 Trabajos futuros.

Se puede usar la API RESTful para integrar el servidor radius, cacti con GenieACS para automatizar todo el proceso de aprovisionamiento de los CPE y aumentar la capacidad de gestión y monitoreo.

Realizar una investigación detallada del modelo de datos TR098 para CWMP con las distintas versiones de las herramientas OpenSource de gestión remota que incluya la configuración de los dispositivos de acceso a Internet existentes hoy en el mercado.

6 CAPÍTULO: REFERENCIAS

[1] TELCOFIBER, "quienes-somos." Accedido: Diciembre. 12, 2021 [En línea] Disponible: https://www.telcofiber.com/index.php/quienes-somos

[2] AVSystem, “AVSystem - Shaping the world of connected devices.” Accedido: Diciembre. 12, 2021 [En línea]. Disponible en: https://www.avsystem.com/crashcourse/tr069/

[3] J. F. López, “Análisis del impacto económico de la implementación del protocolo TR-069 en los CPE´S de la empresa de telecomunicaciones PUNTONET”, Escuela Politécnica Nacional, Ecuador, 2019 [En línea]. Disponible: http://bibdigital.epn.edu.ec/handle/15000/20271

[4] R. S. Pressman, Ingeniería del software: un enfoque práctico, 7ma ed. México: Mac Graw Hill, 2013.

[5] MINTIC, “Redes de Telecomunicaciones”. Accedido: Diciembre. 12, 2021 [En línea]. Disponible: https://mintic.gov.co/portal/inicio/5235:

[6] Comisión de Regulación de Comunicaciones, "Data Flash 2022-011: Internet Fijo", Mayo 6, 2022 [En línea]. Disponible: https://postdata.gov.co/dataflash/data-flash-2022-011-Internet-fijo

[7] Margarita, "A Comprehensive Understanding of FTTx Network", FS Community, blog, Julio 27, 2020 [En línea]. Disponible: https://community.fs.com/blog/a-comprehensive-understanding-of-fttx-network.html

[8] Luis Jimenez, "Aprendiendo los conceptos de OLT, ONU y ONT," Huawei Enterprise Community, Junio 21, 2019 [En línea]. Disponible: https://forum.huawei.com/enterprise/es/aprendiendo-los-conceptos-de-olt-onu-y-ont/thread/540747-100275

[9] Peterson Fontes, "Splitter: quando utilizar os modelos balanceado e desbalanceado?," Cianet, blog, Agosto 14, 2021 [En línea]. Disponible: https://www.cianet.com.br/blog/infraestrutura-e-tecnologia/splitter-quando-utilizar-os-modelos-balanceado-e-desbalanceado/

[10] OSIPTEL, "Anexo: Técnicas de cableado." Accedido: Marzo 7, 2022 [En línea] Disponible: https://www.osiptel.gob.pe/media/3zkdviy1/anexo-tecnicas-cable.pdf

[11] Worton, “¿Cuál es la diferencia entre fibra monomodo y multimodo?”, FS community, blog, Julio 6, 2021 [En línea]. Disponible: https://community.fs.com/es/blog/single-mode-vs-multimode-fiber-whats-the-difference.html

[12] USI, "¿Qué es una ONT o Terminal de Red Óptica?," Junio 22, 2020. [En línea]. Disponible: https://www.usi.org.uy/noticias-y-eventos/2020/6/22/que-es-una-ont-o-terminal-de-red-optica-1043

[13] Acrylic Wi-Fi. "Por qué se utilizan canales Wi-Fi 1, 6 y 11 en 2.4GHz," Acrylic Wi-Fi Blog, blog, Septiembre 9, 2016 [En línea]. Disponible: https://www.acrylicwifi.com/blog/por-que-se-utilizan-canales-wifi-1-6-y-11-en-2-4ghz/

[14] J. M. Salcedo, "¿Qué canales WiFi son los mejores en la banda de 5 GHz en España?," BandaAncha, Enero 3, 2023 [En línea]. Disponible: https://bandaancha.eu/articulos/canales-wifi-banda-5-ghz-espana-mejor-9826

[15] Gy ty C3 Comunicaciones, "Jumpers - Cableados especiales para torres y estaciones." Accedido: Octubre 21, 2022 [En línea]. Disponible: https://www.c3comunicaciones.es/Fichas/Jumpers.pdf

[16] ITU-T, “G.984.1: Redes ópticas pasivas con capacidad de Gigabits: Características generales,” Marzo, 2008 [En línea]. Disponible: https://www.itu.int/rec/T-REC-G.984.1/es.

[17] J. Orozco, "Configuración de servicios en entornos GPON,” tesis de maestría, Universidad Politécnica de Valencia, Valencia, España, 2019.

[18] Z. Abdellaoui, Y. Dieudonne y A. Aleya, “Design, implementation and evaluation of a Fiber To The Home (FTTH) access network based on a Giga Passive Optical Network GPON,” ELSEVIER, vol. 10, p. 100058, 2021 [en línea]. Disponible: https://doi.org/10.1016/j.array.2021.100058

[19] Ufinet, “¿Qué es fibra hasta el hogar, o FTTH?”. Accedido: Diciembre 12, 2022 [En línea] Disponible: https://www.ufinet.com/es/servicios/ftth/

[20] J. M. Salcedo, "¿Qué es la potencia óptica y cómo afecta a nuestras conexiones?," BandaAncha, Febrero 3, 2023 [En línea]. Disponible: https://bandaancha.eu/articulos/que-potencia-optica-como-afecta-10192

[21] E. López Pastor, “FTTH Course - Module 1,” ResearchGate, pp. 20-25, 2015 [En línea]. Disponible: https://www.researchgate.net/publication/280068933

[22] D. Juan, "Una visión general de la red de acceso FTTH con GPON", Medium, blog, Noviembre 13, 2018 [En línea]. Disponible: https://xxxamin1314.medium.com/una-visión-general-de-la-red-de-acceso-ftth-con-gpon-104bc8973d65

[23] A. M. El-Sherbini, "Design and implementation of a Fiber to the Home (FTTH) access network based on GPON," Journal of Computer Science, vol. 10, no. 5, pp. 824-833, 2014 [En línea]. Disponible: DOI:10.5120/16015-5050

[24] J. H. Mervyn Hopkins, "CPE WAN Management Protocol (CWMP)", Tesis de maestría, Universidad Politécnica de Valencia, España, 2018.

[25] Boardband Forum, “TR-069 CPE WAN Management Protocol,” Junio, 2020. [En línea]. Disponible: https://www.broadband-forum.org/technical/download/TR-069_Amendment-6_Corrigendum-1.pdf

[26] Broadband Forum, "TR-098 CPE WAN Management Protocol Data Model for TR-069," Noviembre, 2014 [En línea]. Disponible: https://cwmp-data-models.broadband-forum.org/tr-098-1-8-0.html

[27] Axiros, "AX69 - Out of the Box ACS". Accedido: Octubre. 10, 2022 [En línea] Disponible: https://es.axiros.com/products/ax69-out-of-the-box-acs

[28] AVSystem, "Unified Device Management Platform". Accedido: Diciembre. 23, 2022 [En línea] Disponible: https://www.avsystem.com/products/unified-device-management-platform/

[29] Friendly Technologies, "TR-069 Device Management". Accedido: Octubre. 23, 2022 [En línea] Disponible: https://friendly-tech.com/products/tr-069-device-management/

[30] EasyCwmp, "Tutorial". Accedido: Octubre. 25, 2022 [En línea] Disponible: https://easycwmp.org/tutorial/

[31] GenieACS. “GenieACS - An Open Source TR-069 ACS”. Accedido: Agosto. 10, 2022 [En línea] Disponible: https://genieacs.com/