UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

ADMINISTRACIÓN DE LAS CONEXIONES A INTERNET DE LOS USUARIOS DE LA EMPRESA SITEC DE LA CIUDAD DE IBARRA EN BASE A LA ARQUITECTURA AAA Y EL PROTOCOLO PPPOE UTILIZANDO EQUIPOS MIKROTIK.

Trabajo de Grado previo a la obtención del título de Ingeniera en Telecomunicaciones.

AUTOR:

Eliana Carolina Quinatoa Aguirre

DIRECTOR:

Ing. Fabián Geovanny Cuzme Rodríguez, Msc

Ibarra, 2024

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003886163		
APELLIDOS Y NOMBRES:	Quinatoa Aguirre Eliana Carolina		
DIRECCIÓN:	Ibarra, Ejido de Caranqui		
EMAIL:	ecquinatoaa@utn.edu.ec		
TELÉFONO FIJO:	062652452	**TELÉFONO MÓVIL:**	0960639599
DATOS DE LA OBRA			
TÍTULO:	ADMINISTRACIÓN DE LAS CONEXIONES A INTERNET DE LOS USUARIOS DE LA EMPRESA SITEC DE LA CIUDAD DE IBARRA EN BASE A LA ARQUITECTURA AAA Y EL PROTOCOLO PPPOE UTILIZANDO EQUIPOS MIKROTIK.		
AUTOR (ES):	Quinatoa Aguirre Eliana Carolina		
FECHA: DD/MM/AAAA	24/01/2024		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**		
TITULO POR EL QUE OPTA:	Ingeniera en Telecomunicaciones		
ASESOR /DIRECTOR:	**Msc. Jaime Michilena/ Msc. Fabián Cuzme**		

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 28 días del mes de Febrero de 2024.

EL AUTOR:

Eliana Carolina Quinatoa Aguirre

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCAS APLICADAS

CERTIFICACIÓN:

MAGÍSTER FABIÁN CUZME, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que el presente trabajo de titulación "ADMINISTRACIÓN DE LAS CONEXIONES A INTERNET DE LOS USUARIOS DE LA EMPRESA SITEC DE LA CIUDAD DE IBARRA EN BASE A LA ARQUITECTURA AAA Y EL PROTOCOLO PPPOE UTILIZANDO EQUIPOS MIKROTIK" ha sido desarrollado por la señorita Eliana Carolina Quinatoa Aguirre bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

Ing. Fabián Geovanny Cuzme Rodríguez, Msc.
DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Este trabajo se lo dedico a mis ángeles en el cielo Genoveva, Marina y Raimundo por cuidarme y bendecirme siempre, a mi abuelito Julio, a mi compañero fiel Nacho por todas las noches que se desveló junto a mí, a mi hermano Francis el motor de mi vida, a mis padres por todo el sacrificio y los esfuerzos que realizaron para permitirme cumplir mis objetivos, a mi novio Pablo por su apoyo incondicional, a mis tías Mirian y Maritza, a mi pequeña Rafa la alegría de mi vida, a mi familia, amigos y docentes que han sido parte fundamental de esta etapa de mi vida.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Mi gratitud principalmente a Dios, por todas sus bendiciones. Agradezco a mis padres por su apoyo incondicional a lo largo de toda mi vida estudiantil y por su aliento en los momentos más difíciles. Agradezco a mis tías, tíos, primas y primos que siempre estuvieron pendientes y nunca me dejaron sola. Quiero agradecer a mi novio Pablo y su familia que han sido gran apoyo , soporte y refugio. Gracias a mis amigas y amigos, de CIERCOM y CITEL por todos los momentos compartidos, los éxitos y las tristezas, especialmente a Vivi, Merce y Eri, mis compañeras de lucha y confidentes. Agradezco de manera especial al ingeniero Fernando Obando por su apertura y apoyo durante la realización de este trabajo y la confianza brindada dentro de su empresa.

Mi agradecimiento al Msc. Fabián Cuzme y Msc. Jaime Michilena por su guía en el desarrollo de este trabajo.

Gracias a todas las personas que formaron parte de esta etapa de mi vida, a los docentes que me brindaron sus conocimientos, mis profesores y compañeros del Grupo de Danzas Tradicionales UTN, por todos los recuerdos imborrables que se quedan grabados para siempre en mi corazón, por hacer de esta etapa la más linda y divertida, y sobre todo que los días malos sean más llevaderos.

Infinitas gracias a todos!

RESUMEN

Este proyecto se centra en la gestión del acceso a Internet para los usuarios de SITEC en Ibarra utilizando arquitectura AAA e implementando PPPoE con dispositivos MikroTik. El estudio establecerá objetivos específicos, incluyendo la investigación teórica sobre AAA y PPPoE, el diseño del proceso y la arquitectura, la implementación de la gestión de usuarios utilizando Radius y PPPoE, y la realización de pruebas para verificar la efectividad de la solución propuesta.

El proceso metodológico consiste en el estudio de la arquitectura AAA y el protocolo PPPoE para el desarrollo del marco teórico del proyecto, como siguiente fase la implementación y el diseño de la arquitectura basada en los principios AAA, por último, la integración de Proxmox como hipervisor, el router MikroTik para el control de acceso de usuarios y los servidores Radius para la funcionalidad AAA.

Los resultados de la implementación mostraron mejoras significativas en el control de acceso de usuarios, la seguridad y la gestión administrativa. El sistema implementado ha permitido monitorizar, controlar y supervisar de mejor forma el inicio de sesión de los usuarios y responder eficazmente a los problemas identificados. La implementación exitosa de AAA y PPPoE en SITEC es un paso importante hacia la optimización de la gestión de usuarios de Internet. La transición del control IP tradicional a un sistema de seguridad más avanzado se ajusta a las mejores prácticas del sector y proporciona un entorno de red más eficaz y fiable.

Palabras clave: Arquitectura AAA, administración de usuarios, autenticación PPPoE, Gestión de usuarios PPPoE.

ABSTRACT

This project focuses on managing Internet access for SITEC users in Ibarra using AAA architecture and implementing PPPoE with MikroTik devices. The study will establish specific objectives, including theoretical research on AAA and PPPoE, the design of the process and architecture, the implementation of user management using Radius and PPPoE, and testing to verify the effectiveness of the proposed solution.

The methodological process involves studying AAA architecture and the PPPoE protocol to develop the theoretical framework of the project. The next phase consists of implementing and designing the architecture based on AAA principles. Finally, Proxmox is integrated as a hypervisor, the MikroTik router for user access control, and Radius servers for AAA functionality.

The implementation results showed significant improvements in user access control, security, and administrative management. The implemented system has allowed for better monitoring, control, and supervision of user logins and effective response to identified issues. The successful implementation of AAA and PPPoE in SITEC is an important step towards optimizing Internet user management. Transitioning from traditional IP control to a more advanced security system aligns with industry best practices and provides a more effective and reliable network environment.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

INDICE DE TABLAS

Capítulo I: Antecedentes

En este capítulo se detallada los requerimientos necesarios para el desarrollo del presente trabajo de titulación, siendo estos: el tema elegido, la problemática, los objetivos, el alcance, la justificación con la finalidad de concluir este proyecto de una manera exitosa.

1.1. Tema

ADMINISTRACIÓN DE LAS CONEXIONES A INTERNET DE LOS USUARIOS DE LA EMPRESA SITEC DE LA CIUDAD DE IBARRA EN BASE A LA ARQUITECTURA AAA Y EL PROTOCOLO PPPOE UTILIZANDO EQUIPOS MIKROTIK.

1.2. Problema

La empresa Servicio de Internet y Telecomunicaciones SITEC SA. ubicada en la ciudad de Ibarra, es una empresa ecuatoriana que opera como revendedores de Telecomunicaciones, la empresa fue fundada el 21 de agosto de 2019 (EMIS, 2019) . La principal actividad económica de la empresa es la reventa de servicios de telecomunicaciones (suministros de servicios telefónicos y de internet en instalaciones con disponibilidad hacia todas las personas y negocios). Dentro de la clasificación de la actividad económica se encuentra en la sección Información y Comunicación (Ecuador, 2019). La empresa en su gama de servicios ofrece varios planes de Internet de fibra óptica acorde con la necesidad del usuario. Brinda cuatro opciones de planes para el usuario, como son: Plan Básico (10 Megas), Plan Clásico (20 Megas), Plan Máster (30 Megas) y Plan Furious (50 Megas).

Actualmente, la empresa se maneja con el control de usuarios y acceso a la red por IP y contraseñas, se cuenta con un servidor con Hipervisor Proxmox para el levantamiento de

servicios como el Radius para la Arquitectura de Autorización, Autenticación, Auditoría (AAA) y con un equipo de control ccr1071 Mikrotik donde se establece el acceso hacia internet y firewall, el control de accesos a la red se realiza por medio de listas de control de acceso (ACL) y la implementación de colas para el control de ancho de banda. La activación del acceso de usuarios a internet se lleva de la siguiente manera, se ingresa un nuevo usuario dentro de la red del servidor de ISP, la autenticación se realizaba por reconocimiento de la dirección ip asignada al cliente, el servidor reconoce dicha dirección y le permite el acceso al servicio. De acuerdo con el contrato firmado en la instalación, la ausencia de pagos será una razón para suspender el servicio temporalmente hasta que se registre el pago del valor pendiente, la ejecución de suspensión del servicio de internet ha llevado a determinados usuarios a configurar los equipos a su conveniencia, ejecutando un cambio de la dirección ip asignada por otra dirección que les permita acceder al servicio sin inconvenientes.

Al descubrir el problema, la empresa requiere realizar la migración del acceso por ip a una autenticación a través de un servidor RADIUS que brinda los mecanismos necesarios con respecto a la seguridad informática. La arquitectura que se desea implementar es la AAA para la gestión administrativa a través de un servidor Radius, brinda mayor seguridad a la base de datos donde se encuentran almacenados y registras las conexiones y datos de clientes. La autenticación en la gestión de clientes que se desea implementar es a través de otro servidor Radius basado en el protocolo PPPoE que utiliza una encapsulación PPP y trabaja en la capa Ethernet, se desea cambiar y eliminar cualquier acceso de control por ip sin una previa asignación de usuario, el protocolo mencionado anteriormente, es utilizado para proveer conexión de banda ancha, ofrece los servicios de autenticación, cifrado, mantenimiento y compresión.

1.3. Objetivos

1.3.1. Objetivo General

Implementar la gestión de las conexiones a internet de los usuarios de la empresa SITEC de la ciudad de Ibarra basado en la Arquitectura de Autenticación, Autorización y Auditoría (AAA) y el protocolo Punto a Punto sobre Ethernet (PPPoE) utilizando equipos Mikrotik.

1.3.2. Objetivos Específicos

- Investigar acerca de la arquitectura AAA y el protocolo PPPoE para la documentación teórica del proyecto.
- Diseñar los procesos y la arquitectura que se implementará basado en la arquitectura AAA.
- Implementar la arquitectura definida que permita la conexión de los usuarios a internet con una autenticación PPPoE a través de servidores Radius.
- Establecer pruebas de funcionamiento para comprobar que se ejecute la implementación realizada.

1.4. Alcance

En la empresa el control de usuarios y los accesos se lo realiza por IP, la implementación de los métodos de autenticación y niveles de acceso de servicios le permitirá a la red tener un mejor control del uso de los recursos que ofrece la red, como el ancho de banda y un control de los usuarios que se encuentran dentro de la lista de suspensión de servicio por falta de pago.

El levantamiento del servidor RADIUS y la arquitectura AAA se realiza dentro del servidor con hipervisor proxmox, para la gestión administrativa, a través de un equipo Mikrotik ccr1071 se realiza el control de acceso y firewall a través de ACL y la implementación de colas para controlar el ancho de banda, el acceso por IP que se utiliza actualmente será reemplazado por el acceso a través de la asignación de un usuario y contraseña. El servidor Radius permite la implementación de una red que tenga el servicio de autenticación, autorización y auditoría, este servidor se implementó en el nodo principal de la ciudad. La arquitectura principal que se implementará en el rediseño de la red de la empresa es la arquitectura AAA, que brinda lo que se menciona anteriormente, los servicios de autenticación, autorización y auditoría:

Autenticación: Para realizar la autenticación se instaló el servidor RADIUS el cual permite 3 tipo de autenticación con certificados digitales (EAP-TLS) Roser (2002), EAP protegido (PEAP) y EAP TTLS. Para que el usuario tenga acceso a la red lo debe realizar por cualquiera de estos 3 métodos de autenticación, si el proveedor del servicio no ha definido por defecto el acceso que se va a implementar. La autenticación engloba la información con la que se va a identificar de forma única cada usuario dentro del sistema, esto se lo realiza con un nombre y una contraseña. El administrador es el encargado de monitorear y agregar o eliminar los usuarios en el sistema (Calvete, 2020).

Autorización: El punto de información de políticas que tiene la red al servidor de directorio es OpenLDAP en el cual se realiza el almacenamiento de la información de cada usuario que ingresa a la red. Este proceso es el que agregar o deniega el acceso de un usuario individual a una red informática y sus recursos. Cada usuario recibe diferentes niveles de autorización que son los que limitan el acceso a la red y los recursos asociados. Los servicios de

autorización permiten la asignación de rutas, filtrado de direcciones IP, administración de ancho de banda y encriptación (Calvete, 2020).

Auditoría: En esta fase de auditoría AAA, el usuario una vez que se ha autenticado y autorizado, puede enviar una petición de la auditoría para que se inicie la sesión que será respondida por el servidor Radius, se inicia un registro de conexión con datos que muestran el inicio/fin de sesión, los datos que se han transferido. Facilitando que el administrador revise de forma práctica los problemas de seguridad y de acceso operativo que se pudieron generar anteriormente (Calvete, 2020).

Un servidor RADIUS permite una gran cantidad de autenticaciones y autorizaciones en otros softwares, como en el operador usando Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet (PPPoE). PPPoE amplía la capacidad original de PPP al permitir una conexión virtual punto a punto sobre una arquitectura de red Ethernet multipunto, es un protocolo muy utilizado por los ISP para proporcionar servicios de Internet de alta velocidad por la línea de abonado digital (DSL), de los cuales el más popular es el ADSL, utiliza métodos estándar de encriptación, autenticación y compresión especificados por PPP. Cuando se inicia una sesión PPPoE, la dirección IP de destino sólo se utiliza cuando la sesión está activa. La dirección IP se libera después de cerrar la sesión, lo que permite una reutilización eficiente de las direcciones IP (Charlene, 2020).

Con respecto a los equipos, se conoce que dentro de un servidor Mikrotik se puede ejecutar más de un servicio PPPoE (con diferentes nombres y perfiles), cada uno de los servicios PPPoE puede autenticar a los usuarios de Internet utilizando uno o varios servidores Radius. El Mikrotik consulta al servidor Radius sobre la autenticación de un usuario PPPoE sólo si este usuario no está en su base de datos local. Los atributos de la conexión a Internet de un cliente

(IP, GW, DNS, ancho de banda, etc.) se pueden definir en el perfil del cliente en Mikrotik (Hoxha, 2017).

Cabe recalcar que la arquitectura AAA será implementada en los equipos de control administrativo y red de control como equipos Mikrotik, los servicios de sistema de nombres de dominio (DNS), zabix y las VPN (virtual private network- red privada virtual), la autenticación PPPoE será netamente parte de la gestión de usuarios, es decir, aplicada en los routers de cada usuario.

1.5. Justificación

El servicio de internet hoy en día es una necesidad básica para el hogar, el 91.81% de la población dispone de acceso a este servicio y se conecta a través de un dispositivo que le permite acceder a Internet, ya sea para ocio, estudios, trabajo (ARCOTEL, 2019). En base al crecimiento de la población, que utiliza internet se han creado distintas ISP que brindan sus paquetes de servicio, a conveniencia del usuario. Como todo negocio se basa en una primera inversión económica que permite la implementación y el diseño de la red que brindará el servicio a los usuarios contratantes, en este diseño e implementación de primer plano se realiza el levantamiento de la red, configuraciones básicas en los equipos, con el pasar del tiempo la empresa analiza los cambios que se deben realizar dentro de la misma de acuerdo con los problemas que se van presentando a lo largo de los años.

La empresa requiere implementar un servidor Radius basado en la arquitectura AAA que permite la autenticación, autorización y auditoría para las gestiones administrativas (Fernández, 2014), la empresa cuenta con colaboradores que tendrán acceso a los servidores e información de

los clientes a través de la autenticación de un usuario y contraseña a través de Radius, este servidor tendrá conexión con otro servidor Radius el cual será el que almacene a los clientes y en el cual se implementará el ingreso de nuevos clientes y las configuraciones de ancho de banda, colas y accesos a internet a través de un equipo Mikrotik que permite la gestión de los usuarios, una vez que se tiene la conexión entre estos servidores Radius, se logra autenticar a las Unidad de red óptica ONU que permiten a los usuarios finales conectarse a internet, el servidor Radius de la gestión de clientes utiliza la configuración del protocolo PPPoE, mientras que el servidor Radius de la gestión de administración se basa en el cumplimiento de la arquitectura AAA a través de la cual permite que se hagan análisis de las personas que acceden al servidor y realizan cambios con permisos de administrador (Hoxha, 2017).

Capitulo II: Fundamento Teórico

En el presente capítulo se redacta la sustentación teórica que permita facilitar e introducirse de mejor forma en el trabajo planteado, donde se podrá conocer acerca de la gestión y administración de redes, la seguridad que una red debe poseer, los protocolos AAA y PPPoE que son los que se implementan para el funcionamiento del servicio.

2.1 Gestión y Administración de una Red

La gestión de una red de datos se considera compleja porque comprende una mezcla de diferentes servicios como: voz, vídeo, además de datos; la interconexión de varios tipos de redes LAN, MAN y WAN; el uso de múltiples medios de comunicación como: par trenzado, cable coaxial, fibra óptica, satélite, microondas; varios protocolos de comunicación que incluyen TCP/IP, SPX/IPX, SNA; el uso de muchos sistemas operativos como DOS, NetWare, Windows, UNIX y varias arquitecturas de red como: Ethernet, Token Ring, FDDI. Se encuentran involucrados varios elementos de administración de red como (Caicedo, 2013):

- Objetos: constituye los elementos del nivel más bajo, es decir los aparatos que se administran.
- Agentes: programas que coleccionan información de administración del sistema en algún nodo de la red. Se transmite información sobre:
    - Notifica los problemas
    - Datos de diagnóstico
    - Identificación y características del nodo

- Administrador: programas en conjunto que se ubican en un punto central, a donde se dirigen los mensajes que requieren alguna acción o poseen información solicitada por el administrador al agente.

UIT y OSI realizan una descripción de las tareas y funciones que deben realizarse en el proceso de gestión de la red y lo definen así: La gestión de red es la suma total de todas las políticas, procedimientos implicados en la planificación, configuración, control y monitorización de los elementos que componen una red para asegurar el uso eficiente y eficaz de sus recursos. Esto se reflejará en la calidad de los servicios ofrecidos. Las tres dimensiones de la gestión de redes se definen de la siguiente manera (Caicedo, 2013):

- Dimensión funcional: explica la asignación de tareas de gestión a través de áreas funcionales.
- Dimensión temporal: explica la división del proceso de gestión en diferentes fases cíclicas, incluidas las fases de planificación, ejecución y funcionamiento.
- Dimensión Escenario: explica todos los demás escenarios además del escenario de gestión de la red.

2.1.1 Administración de una red y las Conexiones

- Mejorar la continuidad del funcionamiento de la red con mecanismos adecuados de control y supervisión, solución de problemas y dotación de recursos.
- Hacer un uso eficiente de la red y aprovechar mejores recursos como el ancho de banda.
- Reducir costes mediante el control de gastos y mejores mecanismos de facturación

- Aumentar la seguridad de la red protegiéndola de accesos no autorizados, imposibilitando que personas ajenas puedan entender la información que circula por ella.
- Controlar los cambios y actualizaciones de la red para que perturben lo menos posible el servicio a los usuarios.
- Prestar servicios de apoyo (Molero, Villaruel, Aguirre, & Martínez, 2010).

2.2 Seguridad de la Red

La seguridad de las redes es un término amplio que abarca multitud de tecnologías, dispositivos y procesos. En su acepción más simple, se trata de un conjunto de normas y configuraciones diseñadas para proteger la integridad, confidencialidad y accesibilidad de las redes informáticas y los datos mediante tecnologías tanto de software como de hardware. Todas las organizaciones, independientemente de su tamaño, industria o infraestructura, necesitan un cierto grado de soluciones de seguridad de red para protegerse del panorama cada vez más amplio de ciber amenazas (Huerta, 2002).

La arquitectura de red actual es compleja y hace frente a un entorno de amenazas que cambia constantemente y a determinados atacantes que intentan encontrar y explotar vulnerabilidades. Estas vulnerabilidades pueden desarrollarse en un amplio número de áreas, incluidos dispositivos, datos, aplicaciones, usuarios y ubicaciones. Por este motivo, hoy en día se utilizan muchas herramientas y aplicaciones de gestión de la seguridad de la red que se ocupan de las amenazas y los exploits individuales y también del incumplimiento de la normativa. Cuando sólo unos minutos de inactividad pueden causar una interrupción generalizada y un daño

masivo a la cuenta de resultados y la reputación de una organización, es esencial que estas medidas de protección estén en su lugar (Huerta, 2002).

La seguridad de la red es muy importante para la protección de los datos y la información de los clientes, mantener seguros los datos que se han compartido y garantizar un acceso y un rendimiento de la red fiables, así como protección frente a las ciber amenazas.

Una solución de seguridad de red bien diseñada reduce los gastos generales y protege a las organizaciones de las costosas pérdidas que se producen por una violación de datos u otro incidente de seguridad. Garantizar el acceso legítimo a sistemas, aplicaciones y datos permite las operaciones empresariales y la prestación de servicios y productos a los clientes (Huerta, 2002).

2.2.1 Principios de Seguridad

Una "red segura" es un blanco móvil. A medida que se descubren nuevas vulnerabilidades y nuevos métodos de ataque, un usuario relativamente poco sofisticado puede potencialmente lanzar un ataque devastador contra una red desprotegida. Los ataques a la red están evolucionando en su sofisticación y en su capacidad para evadir la detección. Además, los ataques son cada vez más selectivos y tienen mayores consecuencias financieras para sus víctimas (Watkins & Wallace, 2009).

Confidencialidad. Es la garantía de que la información no se revelará a personas, grupos, procesos o dispositivos no autorizados. Los datos altamente confidenciales deben cifrarse para que terceros no puedan descifrarlos fácilmente. Sólo se permite el acceso a quienes están autorizados a ver la información (Murray, 2023). El objetivo del principio de confidencialidad es

mantener la información personal en privado y garantizar que sólo sea visible y accesible para aquellas personas que la posean o la necesiten para desempeñar sus funciones organizativas (Ray, 2023)

Integridad. Debe salvaguardarse la exactitud e integridad de la información vital. Los datos no deben alterarse ni destruirse durante su transmisión y almacenamiento. Esto implica asegurarse de que un sistema de información no es manipulado por entidades no autorizadas. Deben establecerse políticas para que los usuarios sepan cómo utilizar correctamente el sistema (Murray, 2023). Incluye la protección contra cambios no autorizados (adiciones, supresiones, alteraciones, etc.) en los datos. El principio de integridad garantiza que los datos sean exactos y fiables y que no se modifiquen de forma incorrecta, ya sea accidental o malintencionadamente (Ray, 2023)

Disponibilidad. La disponibilidad es la protección de la capacidad de un sistema para hacer que los sistemas de software y los datos estén totalmente disponibles cuando un usuario los necesite (o en un momento determinado). El propósito de la disponibilidad es hacer que la infraestructura tecnológica, las aplicaciones y los datos estén disponibles cuando se necesiten para un proceso organizativo o para los clientes de una organización(Ray, 2023). Esto significa que los usuarios autorizados tengan acceso oportuno y fácil a los servicios de información. Los recursos y la infraestructura de TI deben seguir siendo sólidos y plenamente funcionales en todo momento, incluso en condiciones adversas, como problemas con las bases de datos o caídas. Implica protegerse contra códigos maliciosos, piratas informáticos y otras amenazas que podrían bloquear el acceso al sistema de información (Murray, 2023).

No Repudio. Esta medida de seguridad está diseñada para establecer la validez de una transmisión, mensaje u originador, o un medio de verificar la autorización de un individuo para recibir información específica. La autenticación impide la suplantación de identidad y exige que los usuarios confirmen sus identidades antes de que se les permita el acceso a los sistemas y recursos. Esto incluye nombres de usuario, contraseñas, correos electrónicos, datos biométricos y otros (Murray, 2023).

Autenticidad. Este atributo garantiza que el remitente de los datos disponga de una prueba de entrega y que el destinatario disponga de una prueba de la identidad del remitente, de modo que ninguna de las partes pueda negar el envío, la recepción o el acceso a los datos. Los principios de seguridad deben utilizarse para probar las identidades y validar el proceso de comunicación (Murray, 2023).

2.2.2 Amenazas y Vulnerabilidades en las Redes

Una vulnerabilidad de red es una debilidad en el software, hardware o procesos organizativos que, cuando es explotada por una amenaza, puede llevar a una brecha de seguridad. Estas vulnerabilidades no físicas a menudo involucran software o datos, como un sistema operativo que no está actualizado y podría ser infectado por un virus, lo que podría propagarse a través de la red (Firch, 2022).

Amenazas. Las amenazas a través de la red suelen ser de dos tipos básicos:

Amenazas pasivas a la red. Actividades como escuchas telefónicas y escaneos inactivos que están diseñadas para interceptar el tráfico que viaja a través de la red.

Amenazas activas a la red. Actividades como ataques de denegación de servicio (DoS) y ataques de inyección SQL en los que el atacante intenta ejecutar comandos para interrumpir el funcionamiento normal de la red (Firch, 2022).

Para ejecutar un ataque de red con éxito, los atacantes deben normalmente piratear activamente la infraestructura de una empresa para explotar vulnerabilidades de software que les permitan ejecutar comandos de forma remota en sistemas operativos internos. Los ataques DoS y el secuestro de redes compartidas (ejemplo: cuando un usuario corporativo está en una red WiFi pública) de comunicaciones son excepciones. Los atacantes suelen obtener acceso a los sistemas operativos internos a través de amenazas enviadas por correo electrónico que primero comprometen un conjunto de máquinas, luego instalan malware controlado por el atacante, y así proporcionan al atacante la capacidad de moverse lateralmente. Esto aumenta la probabilidad de no ser detectado al principio, al tiempo que proporciona un punto de entrada casi sin esfuerzo para el atacante. Según un reciente informe de inteligencia de seguridad de Microsoft, más del 45% del malware requiere algún tipo de interacción con el usuario, lo que sugiere que el correo electrónico dirigido al usuario, diseñado para engañarlo, es una táctica principal utilizada por los atacantes para establecer su acceso (Firch, 2022).

Algunas amenazas están diseñadas para interrumpir las operaciones de una organización en lugar de recopilar información de forma silenciosa para obtener beneficios económicos o espionaje. El enfoque más popular se denomina ataque de denegación de servicio (DoS). Estos ataques saturan los recursos de la red, como las pasarelas web y de correo electrónico, los routers, los conmutadores, etc., e impiden el acceso de los usuarios y las aplicaciones, lo que en última instancia desconecta un servicio o degrada gravemente su calidad. Estos ataques no requieren necesariamente un pirateo activo, sino que se basan en la capacidad de los atacantes de

escalar el tráfico hacia una organización para aprovecharse de una infraestructura mal configurada y protegida. Esto significa que a menudo hacen uso de una red de sistemas informáticos comprometidos que trabajan en tándem para abrumar al objetivo, lo que se conoce como ataque de denegación de servicio distribuido (DDoS). En muchos casos, los atacantes lanzan ataques DoS y DDoS mientras intentan un pirateo activo o envían amenazas maliciosas por correo electrónico para camuflar sus verdaderos motivos ante los equipos de seguridad de la información creando distracciones (Firch, 2022).

Vulnerabilidades. Una vulnerabilidad de la red es un punto débil o un defecto en el software, el hardware o los procesos organizativos que, cuando se ve comprometido por una amenaza, puede dar lugar a una violación de la seguridad. Las vulnerabilidades de red no físicas suelen afectar al software o a los datos. Por ejemplo, un sistema operativo (SO) puede ser vulnerable a ataques de red si no está actualizado con los últimos parches de seguridad. Si se deja sin parchear, un virus podría infectar el sistema operativo, el host en el que se encuentra y, potencialmente, toda la red (Firch, 2022).

Las vulnerabilidades físicas de la red implican la protección física de un activo, como encerrar un servidor en un armario o asegurar un punto de entrada con un torniquete.

Software obsoleto o sin parches que expone los sistemas que ejecutan la aplicación y potencialmente toda la red. Los desarrolladores de software lanzan constantemente nuevos parches para corregir fallos y errores con el fin de reducir las vulnerabilidades. Algunas aplicaciones tienen millones de líneas de código, lo que hace que las vulnerabilidades sean una parte inevitable del despliegue de software. Como resultado, los desarrolladores despliegan parches en el software para remediar estas vulnerabilidades, aunque los parches también pueden

ser actualizaciones de rendimiento o de características. Mantener la seguridad del código del software es una batalla constante, ya que grandes empresas como Facebook, Apple y Microsoft lanzan parches a diario para defenderse de las nuevas ciber amenazas. No es raro que los proveedores de software y hardware anuncien fechas de fin de vida (EOL). Estos productos heredados ya no suelen ser rentables y su mantenimiento cuesta recursos (desarrolladores de software).

Cortafuegos / sistemas operativos mal-configurados que permiten o tienen activadas políticas por defecto. Una de las amenazas más importantes para una organización es exponer su red interna o sus servidores a Internet. Cuando están expuestos, los actores de amenazas pueden espiar fácilmente su tráfico, robar datos o comprometer su red (Firch, 2022).

Técnicas de Ataque. Ataques de ingeniería social que engañan a los usuarios para que faciliten información personal, como un nombre de usuario o una contraseña. Los ataques de ingeniería social se han convertido en un método popular utilizado por los actores de amenazas para eludir fácilmente los protocolos de seguridad de autenticación y autorización y obtener acceso a una red. Estos ataques han aumentado significativamente en los últimos 5 años, convirtiéndose en un negocio lucrativo para los hackers. Los usuarios internos suponen el mayor riesgo de seguridad para una organización, normalmente porque no tienen formación o no son conscientes de la amenaza. Descargar accidentalmente un archivo adjunto o hacer clic en un enlace a un sitio web con código malicioso puede costar miles de dólares en daños. Los tipos más comunes de ataques de ingeniería social incluyen:

- Correos electrónicos de phishing: Una estafa por correo electrónico de phishing es una amenaza en línea que parece proceder de un usuario o empresa legítimos. Estas

estafas intentan engañar a los usuarios para que proporcionen información confidencial, como un nombre de usuario y una contraseña, descarguen o abran una aplicación o transfieran dinero.

- Spear phishing: El spear phishing es similar al phishing en el sentido de que intenta engañar al usuario. Sin embargo, los ataques de spear phishing están diseñados para utilizar información personal para que el usuario haga clic en un enlace. A veces también utilizan la urgencia o un riesgo de valor monetario para cebar a sus víctimas.
- Vishing: Whaling es un tipo de ataque de phishing que se dirige a un ejecutivo o directivo de alto perfil con más información crítica que perder. Los correos electrónicos de whaling se diferencian de otros ataques de phishing en que los correos electrónicos y las páginas web que sirven para la estafa parecen ser oficiales.
- Vishing: Vishing, la combinación de voz y phishing, es un ataque de phishing que tiene lugar a través del teléfono, normalmente una línea VoIP (Voz sobre IP). Los actores de la amenaza son capaces de utilizar herramientas específicas de los sistemas VoIP, pirateando así sus marcadores automáticos para enviar mensajes robotizados desde una dirección VoIP falsa.
- Smishing: El smishing es un ciberataque que utiliza mensajes de texto SMS para engañar a sus víctimas para que proporcionen información confidencial a un actor de la amenaza.
- Spam: El spam ha estado plagando nuestra bandeja de entrada desde el inicio de la comunicación por correo electrónico. El spam es un intento de enviar correos electrónicos masivos a un gran número de usuarios.

- Pharming: El pharming es un tipo de ataque de ingeniería social que desvía el tráfico del sitio web de un usuario a un sitio falso. Similar al phishing, el pharming se produce cuando se instala un código en el ordenador que modifica la URL de destino por la del atacante.
- Tailgating: No todos los ataques de ingeniería social se realizan a distancia o con el uso de un dispositivo electrónico. Tailgating es un tipo más simple de ataque de ingeniería social en el que el actor de la amenaza obtiene acceso físico a una instalación siguiendo a un usuario a través de un punto de control de seguridad.
- Shoulder surfing: El shoulder surfing es un tipo de ingeniería social que se refiere a la obtención de información personal o privada a través de la observación directa. Es muy fácil para un actor de amenaza mirar casualmente por encima del hombro de un empleado para ver su monitor.
- Buceo en contenedores: Se trata de un reconocimiento de ingeniería social. Los actores de la amenaza buscan cualquier dato o pista que puedan conseguir. Buscan números de cuenta, eventos especiales, nombres de contactos, números y mucho más.

2.3 Tunelización

El tunneling en la red es una técnica utilizada para transmitir datos de manera segura entre redes sin que otros puedan conocerlos. Puedes pensar en ello como un pasadizo secreto o un túnel al que solo tú tienes acceso, donde puedes enviar y recibir datos sin preocuparte por miradas indiscretas.

El funcionamiento del tunneling de red implica envolver los datos en paquetes encapsulados que parecen tráfico normal en la red pública. Al llegar a su destino, los paquetes se desencapsulan y descifran. Por lo general, un paquete consta de dos partes:

- Encabezado: Contiene información de protocolo y enrutamiento, como las direcciones IP de origen y destino.
- Carga útil: Los datos reales que se envían.

El tunneling asegura que tus datos permanezcan seguros y protegidos mientras viajan a través del túnel privado en una red pública. Además, no tienes que preocuparte por retrasos o interrupciones causados por otros usuarios en la red pública. Existen principalmente dos tipos de túneles de red:

- Túnel de Red Privada Virtual (VPN): Los túneles VPN son los más comunes y permiten a los usuarios conectarse de forma segura a redes remotas a través de Internet público. Esto les otorga acceso a recursos al otro lado del túnel sin preocuparse por riesgos de seguridad. Las VPN también ofrecen cifrado, lo que dificulta que personas ajenas al túnel intercepten o lean los datos.
- Túnel Secure Shell (SSH): Los túneles SSH proporcionan una conexión cifrada entre un servidor y un cliente a través de una red no segura, como Internet. Los túneles SSH se pueden utilizar para transferencias de archivos seguras, ejecución de comandos a distancia y reenvío de puertos, lo que resulta útil en centros de datos y grandes empresas con un departamento de TI centralizado que supervisa a trabajadores dispersos.

Existen varios protocolos utilizados en el tunneling de red, como el Protocolo de Tunneling Punto a Punto (PPTP), el Protocolo de Tunneling de Capa 2 (L2TP), la Seguridad de Protocolo de Internet (IPsec), la Capa de Conexión Segura (SSL) y la Seguridad de la Capa de Transporte (TLS), entre otros.

Las ventajas del tunneling de red incluyen:

- Mayor Seguridad: El tunneling garantiza la seguridad y la privacidad de los datos, impidiendo el acceso no autorizado y los intentos de interceptación.
- Creación de VPN: Los túneles VPN proporcionan un medio seguro para que los usuarios remotos se conecten a redes distantes, ofreciendo cifrado para proteger los datos transmitidos.
- Reducción de Latencia y Mejora de la Velocidad: Algunos protocolos de tunneling pueden reducir la latencia y mejorar la velocidad de la red al optimizar la transmisión de datos.
- Escalabilidad: Los túneles de red facilitan la escalabilidad de los recursos de la red sin interrupciones.
- Gestión más Sencilla: Para redes más grandes que necesitan mantenerse organizadas, el tunneling permite a los administradores gestionar diferentes segmentos de red por separado sin afectar el rendimiento ni las medidas de seguridad de los demás.
- Mayor Flexibilidad: Los túneles brindan flexibilidad para configurar redes y utilizar diferentes protocolos y aplicaciones en diferentes partes de la infraestructura, todo mientras se mantienen conexiones seguras entre ellos.
- Compatibilidad con Protocolos No Compatibles: El tunneling puede admitir el tráfico de diferentes tipos de protocolos que pueden no ser compatibles con algunos

dispositivos de hardware, lo que podría evitar que ciertas aplicaciones funcionen adecuadamente en esos dispositivos debido a problemas de compatibilidad.

Elusión de Firewalls de ISP: El tunneling se puede utilizar para sortear restricciones impuestas por reglas locales de firewall o limitaciones de ISP. Esto puede ser útil si estás tratando de acceder a servicios bloqueados en ciertas regiones o países debido a leyes de censura u otros problemas regulatorios.

Las desventajas del tunneling de red incluyen riesgos de seguridad si no se configura correctamente, la necesidad de hardware y software específicos en algunos casos, posibles problemas de compatibilidad y el riesgo.

2.4 PPPoE (Point-To-Point Protocol Over Ethernet)

PPPoE (Point-to-Point Protocol over Ethernet) es un tipo de tecnología de línea de abonado digital (DSL) que permite conectar un ordenador u otro dispositivo a una red mediante una conexión Ethernet. Es una variación del Protocolo Punto a Punto (PPP) estándar que se utiliza para las conexiones telefónicas, pero está diseñado para funcionar con el protocolo Ethernet (Shami & Maier, 2008).

El protocolo PPPoE permite a un usuario establecer una sesión PPP a través de una conexión Ethernet, lo que permite el uso de características PPP como la autenticación y el cifrado para la conexión. El protocolo PPPoE suele ser utilizado por los proveedores de servicios de Internet (ISP) para proporcionar a los clientes un servicio DSL.

Una conexión PPPoE suele constar de dos componentes principales: el cliente PPPoE y el servidor PPPoE. El cliente PPPoE es el ordenador o dispositivo que inicia la conexión, mientras que el servidor PPPoE suele ser proporcionado por el ISP y gestiona la conexión en el lado de la red.

El protocolo PPPoE utiliza dos tipos de mensajes: PPPoE Discovery y PPPoE Session. Los mensajes PPPoE Discovery se utilizan para encontrar servidores PPPoE en la red y establecer una sesión. Los mensajes de Sesión PPPoE se utilizan para establecer, configurar y terminar la sesión PPP.

En resumen, el protocolo PPPoE se utiliza para establecer y finalizar la conexión PPP a través de una red Ethernet, permitiendo el uso de funciones PPP como la autenticación y el cifrado. Es comúnmente utilizado por los ISP para proporcionar servicios DSL a sus clientes (Shami & Maier, 2008).

2.4.1 Arquitectura del Servicio PPPoE

La arquitectura del servicio PPPoE (Point-to-Point Protocol over Ethernet) es un marco que establece el proceso de configuración y gestión de conexiones de red a través de este protocolo. Esta arquitectura se compone de varios elementos clave (Hellberg, Greene, & Boyes, 2006):

Cliente PPPoE: Este es el dispositivo que inicia la conexión utilizando PPPoE, que puede ser un router, módem DSL o incluso una computadora personal. El cliente se autentica ante el servidor PPPoE y solicita acceso a la red.

Servidor PPPoE: El servidor PPPoE es un dispositivo dentro de la red que responde a las solicitudes de conexión del cliente. Su función principal es autenticar al cliente, verificar sus credenciales y, si son válidas, establecer una sesión PPP con el cliente. Además, puede asignar direcciones IP y otras configuraciones necesarias.

Acceso a la Red Ethernet: PPPoE se utiliza comúnmente en redes de acceso de banda ancha, como DSL y fibra óptica. La infraestructura física de Ethernet permite la transmisión de datos entre el cliente y el servidor PPPoE.

Protocolo PPP: PPPoE aprovecha el protocolo PPP para encapsular los datos del cliente y transmitirlos de manera segura a través de la red. PPP ofrece capacidades de autenticación y compresión de datos, lo que lo hace adecuado para conexiones de banda ancha.

Sesión PPPoE: Una vez que la conexión se establece entre el cliente y el servidor PPPoE, se crea una sesión PPPoE que permite la transferencia de datos, lo que habilita servicios como la navegación por Internet y otros en línea.

Autenticación y Seguridad: La autenticación del cliente es fundamental en esta arquitectura. El cliente debe proporcionar credenciales válidas, como un nombre de usuario y contraseña, al servidor PPPoE para acceder a la red, lo que garantiza un nivel de seguridad en la conexión.

Gestión de Sesiones: La arquitectura PPPoE incluye funciones para gestionar y supervisar las sesiones de conexión. Esto permite a los proveedores de servicios de Internet (ISP) controlar y facturar el uso de la red de manera efectiva (Hellberg, Greene, & Boyes, 2006).

2.4.2 Métodos de Autenticación más Utilizados en Conexiones PPPoE

Los métodos de autenticación más utilizados en conexiones PPPoE incluyen (Hellberg, Greene, & Boyes, 2006):

Autenticación de Contraseña: Este método utiliza un nombre de usuario y una contraseña para verificar la identidad del usuario. El cliente PPPoE proporciona las credenciales al servidor PPPoE durante la fase de autenticación.

Autenticación CHAP (Challenge Handshake Authentication Protocol): CHAP es un protocolo de autenticación más seguro que utiliza un desafío y una respuesta. El servidor envía un desafío al cliente, que responde utilizando una función de hash criptográfico. Este método protege las credenciales del usuario durante la transmisión.

Autenticación PAP (Password Authentication Protocol): A diferencia de CHAP, PAP transmite la contraseña en texto claro durante la autenticación, lo que lo hace menos seguro. Sin embargo, aún se utiliza en algunas implementaciones.

Certificados Digitales: En este método, se utilizan certificados digitales para autenticar al cliente y al servidor. Los certificados se emiten a cada parte y se utilizan para verificar su identidad mutua.

Token de Seguridad: Los tokens de seguridad, como tarjetas inteligentes o dispositivos generadores de contraseñas, pueden utilizarse para autenticar a los usuarios (Hellberg, Greene, & Boyes, 2006).

MS-CHAP v2: Dentro del ámbito de la seguridad en las redes, la autenticación desempeña un papel crítico en la protección de datos y la privacidad de los usuarios. Uno de los protocolos de autenticación más comunes y ampliamente utilizado es el Microsoft Challenge

Handshake Authentication Protocol version 2 (MS-CHAP v2). MS-CHAP v2 se ha establecido como un estándar de facto en la autenticación de usuarios en diversas aplicaciones, incluyendo conexiones VPN basadas en el Protocolo PPTP (Point to Point Tunneling Protocol).

La importancia de la seguridad en la autenticación radica en garantizar que únicamente usuarios legítimos tengan acceso a los recursos de la red, mientras se protege contra posibles amenazas y ataques cibernéticos. MS-CHAP v2, por ejemplo, es un protocolo basado en contraseñas que verifica la identidad de los usuarios mediante el intercambio de desafíos y respuestas.

Sin embargo, es esencial destacar que MS-CHAP v2 en su implementación original puede presentar desafíos de seguridad, especialmente en el contexto de conexiones VPN basadas en PPTP. Microsoft ha advertido sobre posibles vulnerabilidades en esta configuración, lo que puede poner en riesgo la confidencialidad de los datos transmitidos.

PEAP mejora la seguridad al encapsular el tráfico de autenticación MS-CHAP v2 en el protocolo TLS, lo que proporciona una capa adicional de protección.

La implementación de PEAP-MS-CHAP v2 en las conexiones VPN es un enfoque efectivo para mejorar la seguridad de la autenticación. Para lograrlo, se requiere la configuración adecuada en los servidores, como el Windows Routing and Remote Access Server (RRAS). Estos servidores deben permitir únicamente conexiones que utilicen la autenticación PEAP y rechazar las conexiones de clientes que empleen MS-CHAP v2 o EAP-MS-CHAP v2 (Raj, 2022).

2.5 Arquitectura AAA

La arquitectura AAA es un modelo para diseñar e implantar controles de seguridad en un sistema informático. El acrónimo "AAA" significa Autenticación, Autorización y Contabilidad.

Se utiliza comúnmente en la seguridad de redes, y normalmente se implementa mediante el uso de un servidor o servicio dedicado que proporciona la funcionalidad AAA, como un Servicio de Autenticación Remota de Acceso Telefónico de Usuarios (RADIUS) o un servidor del Sistema de Control de Acceso de Controladores de Acceso Terminal (TACACS). También puede implementarse en sistemas operativos, bases de datos y algunos otros servidores.

Proporciona un enfoque sólido para gestionar conexiones de red al garantizar que solo usuarios autorizados obtengan acceso, que tengan los permisos adecuados y que sus actividades se registren y supervisen para mantener la seguridad y la integridad de la red.

2.5.1 Autenticación

En la arquitectura AAA (Autenticación, Autorización y Contabilidad), la autenticación es el proceso de verificación de la identidad de un usuario o sistema. Consiste en asegurarse de que la entidad que dice ser quien es o lo que es, es realmente esa entidad. El objetivo principal de la autenticación es confirmar la validez de la identidad de un usuario y comprobar si tiene derecho a acceder al sistema o a la red. La autenticación puede realizarse a través de diversos métodos, como:

- algo que el usuario conoce, como una contraseña o una frase de contraseña
- algo que el usuario tiene, como una tarjeta inteligente o un token

- algo que el usuario es, como una huella dactilar o el reconocimiento facial.

Estos métodos se denominan a veces "factores" de autenticación, y el uso de múltiples factores se conoce como autenticación "multifactor" o "de dos factores".

El proceso de autenticación suele implicar que un usuario o sistema presente algún tipo de credencial, como un nombre de usuario y una contraseña, a un servidor de autenticación, que a continuación verifica las credenciales con una base de datos de identidades válidas. Si las credenciales son válidas, el usuario o sistema obtiene acceso al sistema o red. Si las credenciales no son válidas, se deniega el acceso. El éxito o fracaso de la autenticación se registra en el sistema de contabilidad, que forma parte de la arquitectura AAA, y puede utilizarse para auditoría y resolución de problemas.

El proceso mediante el cual se verifica la identidad del usuario que intenta conectarse a la red es la autenticación en PPPoE es. La arquitectura AAA permite que este proceso sea sólido y seguro. Algunos fundamentos teóricos relacionados incluyen:

- Criptografía: La autenticación a menudo implica el uso de técnicas criptográficas, como algoritmos de hash y cifrado, para proteger las credenciales del usuario durante la transmisión y garantizar que no sean interceptadas por atacantes.
- Protocolos de Autenticación: La arquitectura AAA puede admitir múltiples métodos de autenticación, como EAP (Extensible Authentication Protocol), que se basa en un marco teórico sólido para la autenticación segura y flexible (Nakhjiri & Nakhjiri, 2005).

2.5.2 Autorización

La autorización es el proceso de determinar qué acciones puede realizar un usuario o sistema una vez autenticado. Tiene en cuenta los roles y permisos del usuario dentro del sistema, y está diseñado para garantizar que los usuarios tengan el nivel mínimo de acceso necesario para realizar sus funciones laborales.

Suele implementarse mediante el uso de listas de control de acceso (ACL) o mecanismos de control de acceso basados en roles (RBAC). En un sistema basado en ACL, los permisos se asignan a usuarios individuales o grupos de usuarios en función de cada recurso. Por ejemplo, un usuario puede tener acceso de lectura a un archivo, pero no de escritura. En un sistema basado en RBAC, los permisos se asignan a roles, y los usuarios se asignan a uno o más roles. Los roles definen qué acciones puede realizar un usuario. Por ejemplo, a un rol de "administrador" se le puede conceder acceso total a un sistema, mientras que a un rol de "invitado" sólo se le puede conceder acceso de lectura.

Es importante tener en cuenta que la autorización y la autenticación están estrechamente relacionadas. La autenticación determina quién es un usuario, mientras que la autorización determina qué acciones puede realizar ese usuario. Un usuario debe ser autenticado antes de poder ser autorizado, y el proceso de autorización normalmente se basa en el proceso de autenticación para determinar la identidad del usuario.

Al igual que la autenticación, el éxito o el fracaso de la autorización se registra en el sistema de contabilidad, que forma parte de la arquitectura AAA, y puede utilizarse para la auditoría y la resolución de problemas.

Una vez que un usuario se ha autenticado correctamente, la autorización determina qué recursos y servicios específicos están disponibles para ese usuario en la red. Fundamentos teóricos relacionados incluyen:

- Políticas de Acceso: Las políticas de autorización se basan en principios de control de acceso, que se rigen por el principio de mínimo privilegio. Este principio establece que los usuarios solo deben tener acceso a los recursos esenciales para su trabajo, reduciendo así la superficie de ataque.
- Modelo RBAC: El Modelo de Control de Acceso Basado en Roles (RBAC) es una teoría fundamental que se utiliza para asignar derechos y permisos a usuarios en función de sus roles dentro de una organización, lo que contribuye a una autorización más eficiente y segura (Nakhjiri & Nakhjiri, 2005).

2.5.3 Auditoría

En la arquitectura AAA (Autenticación, Autorización y Contabilidad), la contabilidad es el proceso de registro y seguimiento de los eventos del sistema y las acciones de los usuarios. El objetivo principal de la contabilidad es recopilar información sobre el uso del sistema o la red, detectar anomalías y proporcionar pruebas en caso de incidente. La contabilidad suele implicar el registro de información como:

- intentos de inicio de sesión, tanto exitosos como fallidos
- horas de inicio y fin de las sesiones de usuario
- comandos ejecutados por los usuarios
- cambios de configuración realizados en el sistema

- archivos a los que han accedido los usuarios
- uso de recursos (por ejemplo, ancho de banda, espacio en disco).

Esta información se registra en un servidor o servicio dedicado, a menudo denominado servidor de contabilidad o servidor AAA, que puede utilizarse para supervisar, auditar y solucionar problemas. Los registros contables pueden utilizarse para:

- Rastrear la actividad de los usuarios para identificar comportamientos sospechosos o anómalos.
- Supervisar el uso de la red para identificar posibles problemas de seguridad.
- Proporcionar pruebas de la actividad del usuario, para ayudar con la respuesta a incidentes y el análisis forense.
- Facturación y devolución de cargos

Es importante tener en cuenta que se necesita una arquitectura de registro eficiente para poder procesar y analizar esta enorme cantidad de datos, y también para tener en cuenta la seguridad y la privacidad de los usuarios, así como el cumplimiento de la normativa.

La contabilidad en PPPoE implica la recopilación y el registro de información detallada sobre las sesiones de los usuarios, como el tiempo de conexión, el tráfico generado y otros datos relacionados con la actividad de la red. Algunos fundamentos teóricos relevantes son (Nakhjiri & Nakhjiri, 2005):

- Auditoría de Seguridad: La contabilidad juega un papel crucial en la auditoría de seguridad, que se basa en teorías de control y cumplimiento normativo para garantizar

que las actividades de la red cumplan con las políticas establecidas y las regulaciones gubernamentales.

- Gestión de Recursos: La contabilidad proporciona datos sobre el uso de recursos de red, lo que es esencial para la gestión de recursos y la planificación de capacidad, basadas en teorías de gestión de operaciones y teoría de colas.

2.6 Modelo OSI con el Protocolo PPPoE y AAA

El modelo OSI (Open Systems Interconnection) actúa como un marco conceptual que ayuda a comprender las interacciones de varios protocolos de redes en una red. Cuando se integra el protocolo PPPoE y AAA en el modelo OSI, obtenemos una visión de cómo contribuyen colectivamente a la comunicación de la red y refuerzan la seguridad, en la Tabla 1., se puede visualizar la explicación de esta relación.

Tabla 1

Relación del Modelo OSI con los Protocolos PPPoE y AAA

CAPA MODELO OSI	PROTOCOLO PPPoE	PROTOCOLO AAA
Capa Física		
Capa Enlace de Datos	PPPoE funciona fundamentalmente a nivel de enlace de datos. Encapsula tramas PPP en tramas Ethernet, lo que permite la transmisión de paquetes PPP a través de redes Ethernet. Un cliente PPPoE inicia una sesión que	

	encapsula tramas PPP en tramas Ethernet, lo que permite establecer una conexión punto a punto a través de la red Ethernet.	
Capa de Red	Mientras que PPPoE funciona principalmente en la capa de enlace de datos, el protocolo punto a punto (PPP) encapsulado en PPPoE funciona en la capa de red y más allá. PPP es el responsable del establecimiento, configuración y mantenimiento de las conexiones punto a punto y proporciona funciones como autenticación, cifrado de datos y compresión.	La capa de red se ocupa del encaminamiento y envío de paquetes de datos. Los protocolos AAA pueden interactuar aquí para determinar si un usuario o dispositivo está autorizado a acceder a un recurso de red concreto, especialmente en situaciones como el acceso remoto o las VPN.
Capa de Transporte		Proporciona comunicación de extremo a extremo mediante mecanismos como la segmentación, el control de flujo y la corrección de errores. Los protocolos AAA pueden utilizar la capa de transporte para garantizar que los mensajes de autenticación y autorización se entregan de forma fiable en las interacciones cliente-servidor.

Capa Sesión	
Capa Presentación	Esta capa se encarga de traducir, cifrar y comprimir los datos. Los protocolos AAA pueden utilizar técnicas de cifrado en esta capa para proteger los datos sensibles de autenticación y autorización mientras atraviesan la red.
Capa Aplicación	La capa de aplicación alberga la funcionalidad de los servicios AAA, que facilita la autenticación de usuarios, define los derechos de acceso a los recursos (autorización) y lleva un registro del uso (contabilidad). Protocolos como RADIUS y TACACS+ funcionan a este nivel, proporcionando servicios AAA completos a los administradores de red.

2.7 Radius

RADIUS (Remote Authentication Dial-In User Service) es un protocolo AAA (Autenticación, Autorización y Contabilidad), lo que significa que puede manejar las tres funciones: Autenticación, Autorización y Contabilidad. RADIUS se utiliza normalmente para

autenticar y autorizar a usuarios remotos que intentan conectarse a una red, y también proporciona una forma de rastrear y registrar información sobre la actividad de los usuarios en la red (Hassel, 2002).

Cuando un usuario intenta conectarse a una red, el cliente RADIUS (por ejemplo, un router, un conmutador o un concentrador VPN) envía las credenciales del usuario (por ejemplo, nombre de usuario y contraseña) al servidor RADIUS para su validación. A continuación, el servidor coteja las credenciales con su base de datos de usuarios y responde al cliente con un mensaje que indica si las credenciales del usuario son válidas. Una vez autenticado el usuario, el servidor RADIUS puede comprobar sus permisos y funciones para determinar qué acciones puede realizar en la red. El servidor también puede proporcionar al cliente la información necesaria para configurar los controles de acceso y las políticas QoS para el usuario.

A medida que el usuario se conecta, el cliente RADIUS envía mensajes de contabilidad de inicio y final al servidor RADIUS que registran cuándo el usuario se conecta y desconecta, así como otra información sobre su actividad en la red, como los recursos a los que ha accedido y la cantidad de ancho de banda utilizada. Esta información puede utilizarse con fines de facturación y reembolso, así como para solucionar problemas y realizar auditorías (Hassel, 2002).

La arquitectura RADIUS consta de dos componentes principales: el cliente RADIUS y el servidor RADIUS.

El cliente RADIUS suele ser un dispositivo como un enrutador, un conmutador o un concentrador VPN que proporciona acceso a la red a los usuarios. Cuando un usuario intenta conectarse a la red, el cliente RADIUS le pide sus credenciales y las envía al servidor RADIUS para su validación.

El servidor RADIUS es responsable de gestionar la base de datos de usuarios, que incluye información como nombres de usuario y contraseñas, así como roles y permisos para cada usuario. El servidor también gestiona el proceso de autenticación y autorización, y es responsable de registrar y rastrear la actividad de los usuarios en la red.

El cliente y el servidor RADIUS se comunican a través de una red mediante el protocolo RADIUS, que se basa en el Protocolo de Datagramas de Usuario (UDP). Cuando un usuario intenta conectarse a la red, el cliente RADIUS envía un mensaje de solicitud de acceso al servidor RADIUS, que incluye las credenciales del usuario. A continuación, el servidor RADIUS valida las credenciales en su base de datos de usuarios y responde con un mensaje Access-Accept o Access-Reject, indicando si las credenciales del usuario son válidas.

En general, la arquitectura RADIUS permite la gestión centralizada de la autenticación, autorización y contabilidad de usuarios, lo que puede mejorar la seguridad y el cumplimiento, simplificar la gestión de usuarios y dispositivos y proporcionar mejores capacidades de seguimiento, facturación y resolución de problemas (Hassel, 2002).

2.7.1 Métodos de autenticación de servidores RADIUS

El servidor RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación y autorización que se utiliza para controlar el acceso de los usuarios a una red. El servidor RADIUS actúa como un intermediario entre el usuario y el recurso al que se desea acceder, verificando la identidad del usuario y autorizando su acceso (Mira, 2023). Los métodos de autenticación de servidores RADIUS se pueden clasificar en dos categorías principales:

Métodos basados en contraseña: Estos métodos utilizan una contraseña compartida entre el usuario y el servidor RADIUS para verificar la identidad del usuario. Los métodos basados en contraseña más comunes son PAP (Protocolo de autenticación de contraseña) y CHAP (Protocolo de autenticación de desafío-respuesta) (Mira, 2023).

PAP: es un método de autenticación simple y eficiente que utiliza una contraseña compartida para verificar la identidad del usuario. El usuario introduce su nombre de usuario y contraseña, que luego se comparan con una base de datos almacenada en el servidor RADIUS. Si las contraseñas coinciden, se concede el acceso al usuario. Es un método de autenticación poco seguro, ya que transmite la contraseña del usuario en texto plano. Esto la hace vulnerable a la interceptación por parte de un atacante.

CHAP: es un método de autenticación más seguro que PAP. Utiliza un mecanismo de desafío-respuesta para verificar la identidad del usuario. El servidor RADIUS envía un desafío aleatorio al usuario, que luego lo encripta usando su contraseña y lo envía de vuelta al servidor. El servidor descifra la respuesta usando la misma contraseña almacenada en su base de datos. Si la respuesta descifrada coincide con el desafío original, se concede el acceso al usuario. Es un método de autenticación más seguro que PAP porque no transmite la contraseña del usuario en texto plano.

MS-CHAP: Es un método de autenticación que se basa en CHAP. Fue desarrollado por Microsoft y se utiliza en las implementaciones de VPN PPTP de Microsoft. Es un método de autenticación similar a CHAP, pero utiliza un algoritmo de cifrado más fuerte para proteger la contraseña del usuario.

EAP: Es un marco extensible que permite utilizar una amplia gama de métodos de autenticación. Es el método de autenticación más utilizado en redes inalámbricas. Permite al

servidor RADIUS seleccionar el método de autenticación más adecuado para cada usuario, en función de sus requisitos de seguridad.

Métodos basados en certificados: Estos métodos utilizan certificados digitales para verificar la identidad del usuario. Los certificados digitales son documentos electrónicos que contienen información sobre el propietario del certificado, como su nombre, dirección y firma digital (Mira, 2023).

Además de los métodos mencionados anteriormente, los servidores RADIUS también pueden admitir otros métodos de autenticación, como:

- EAP-TLS: Utiliza certificados digitales para una autenticación segura.
- Inicio de sesión UNIX: Aprovecha las cuentas de usuario y contraseñas existentes en un sistema UNIX.
- Autenticación basada en tokens: Emplea contraseñas de uso único u otros tokens para un acceso seguro.

La elección del método de autenticación adecuado depende de los requisitos de seguridad específicos de la red. Los factores que deben tenerse en cuenta a la hora de elegir un método de autenticación son (Mira, 2023):

- La seguridad: El método de autenticación debe ser lo suficientemente seguro para proteger la red de los ataques.
- El rendimiento: El método de autenticación debe ser lo suficientemente eficiente para no afectar al rendimiento de la red.
- La facilidad de uso: El método de autenticación debe ser fácil de usar para los usuarios.

Capítulo III: Diseño de la Arquitectura

Este capítulo proporciona una visión detallada de la situación actual de la empresa. Se aborda la problemática específica, se ofrece una descripción técnica tanto del hardware como del software utilizados. Además, se analiza la arquitectura general, se detalla el diseño de procesos internos y se presenta el desarrollo integral del proyecto. En particular, se enfoca en el proceso de administración de usuarios dentro de la empresa y se profundiza en las configuraciones específicas de equipos y servidores.

3.1 Situación Actual

La empresa SITEC SA, con sede en la ciudad de Ibarra, Ecuador, se constituyó el 21 de agosto de 2019 y se destaca como revendedora de servicios de telecomunicaciones, centrándose en suministrar servicios telefónicos e internet a instalaciones con disponibilidad para la comunidad y empresas locales. De acuerdo con la clasificación económica en Ecuador para el año 2019, la actividad principal de SITEC se encuentra en la sección de Información y Comunicación (Ecuador, 2019). En este contexto, es esencial comprender la misión y visión de SITEC S.A., que reflejan su compromiso con la innovación, el desarrollo comunitario y la excelencia en el servicio.

Misión

«La misión de SITEC S.A es impulsar la conectividad de alta velocidad y calidad en la zona norte del país, mediante tecnologías de vanguardia que fomenten el desarrollo y la

integración en el mundo digital. Nuestra empresa se compromete a promover el crecimiento y el bienestar de las comunidades a las que servimos, a través de la innovación constante y la excelencia en el servicio. Buscamos tener un impacto positivo en la sociedad, mejorando la calidad de vida y contribuyendo al progreso de Ecuador en la era digital (SITEC S.A., 2023).»

Visión

«La visión de SITEC S.A es convertirnos en uno de los principales líderes del mercado de servicios de Internet mediante una expansión estratégica que nos permita llegar a un mayor número de usuarios. Buscamos destacarnos por ofrecer conexiones de alta velocidad y servicios de telecomunicaciones altamente confiables que superen las expectativas de nuestros clientes. Nuestro objetivo es ser reconocidos no solo por nuestra tecnología de vanguardia, sino también por proporcionar un servicio al cliente excepcional en todo momento. Nos esforzamos por construir relaciones sólidas y duraderas con nuestros usuarios y ser un motor de crecimiento para nuestra comunidad (SITEC S.A., 2023).»

Actualmente dentro de su cartera de servicios, SITEC ofrece diversos planes de Internet basados en tecnología de fibra óptica, diseñados para satisfacer las diversas necesidades de los usuarios. Estos planes incluyen:

Plan Básico Eco Speed 60 Megas: Una opción que proporciona una velocidad de conexión de 60 megabits por segundo, ideal para usuarios con necesidades básicas de navegación y descarga de datos.

Plan Clásico 100 Megas: Ofrece una velocidad de conexión de 100 megabits por segundo, destinada a usuarios que requieren una mayor velocidad para actividades en línea como streaming de video, juegos en línea y descargas más rápidas.

Plan Premium UltraStream 150 Megas: Con una velocidad de conexión de 150 megabits por segundo, este plan está diseñado para usuarios que demandan un rendimiento más alto, especialmente en entornos donde múltiples dispositivos están conectados simultáneamente para brindar una experiencia en línea de alta gama.

Plan Furious 200 Megas: La opción más avanzada, con una velocidad de conexión de 200 megabits por segundo, adecuada para usuarios con necesidades intensivas de ancho de banda, como empresas o hogares con múltiples usuarios y dispositivos conectados.

Plan Ultimate SpeedMaster 300 Megas: La opción más efectiva para velocidad ultra rápida, adecuado para realizar descargas, Streaming y juegos en línea sin interrupciones y a gran velocidad.

La oferta diversificada de planes demuestra el compromiso de SITEC en adaptarse a las diferentes demandas y requerimientos de sus clientes. Al proporcionar servicios de Internet a través de fibra óptica, la empresa busca ofrecer conexiones más rápidas y confiables, mejorando así la experiencia de conectividad para la comunidad local. Este enfoque estratégico puede contribuir al desarrollo de una infraestructura de telecomunicaciones más robusta y avanzada en la región de Ibarra.

3.2 Descripción de la Problemática

En la actualidad, la compañía gestiona el control de usuarios y el acceso a la red a través de direcciones IP y contraseñas. Cuenta con un servidor que utiliza Hipervisor Proxmox para servicios como Radius, encargado de la Arquitectura de Autorización, Autenticación y Auditoría (AAA). Asimismo, dispone de un equipo ccr1071 Mikrotik para controlar el acceso a internet y

administrar el firewall, utilizando listas de control de acceso (ACL) y colas para regular el ancho de banda.

El proceso de activación del acceso a internet implica agregar nuevos usuarios a la red del servidor ISP. Anteriormente, la autenticación se basaba en el reconocimiento de la dirección IP asignada al cliente, pero algunos usuarios han modificado la configuración de sus equipos para mantener el acceso al servicio, generando problemas como la falta de pagos.

Frente a estos desafíos, la empresa ha decidido migrar de un acceso basado en IP a una autenticación mediante un servidor RADIUS. Esta implementación de la arquitectura AAA busca mejorar la seguridad de la base de datos que almacena y registra las conexiones y datos de los clientes. La autenticación para la gestión de clientes se realizará mediante otro servidor RADIUS basado en el protocolo PPPoE, que utiliza una encapsulación PPP en la capa Ethernet. Este cambio tiene como objetivo eliminar el control de acceso por IP sin asignación de usuario previa. El protocolo PPPoE, utilizado para ofrecer conexiones de banda ancha, proporciona servicios de autenticación, cifrado, mantenimiento y compresión.

3.3 Descripción Técnica de Hardware y Software

En este apartado se proporciona un análisis detallado de los componentes físicos y lógicos esenciales en la infraestructura de tecnología de la empresa, examina minuciosamente tanto el hardware, abarcando desde servidores hasta dispositivos de red, como el software, que comprende desde sistemas operativos hasta aplicaciones especializadas. La comprensión integral de estos aspectos técnicos es fundamental para evaluar la capacidad, eficiencia y seguridad del entorno tecnológico de la organización.

3.3.1 Mikrotik ccr1036

Es un enrutador de alto rendimiento diseñado para uso industrial, con un avanzado CPU de 36 núcleos que destaca en el procesamiento de paquetes extensivos, siendo la elección óptima para aplicaciones que requieren millones de paquetes por segundo. Alojado en un estuche compacto de montaje en rack de 1U, este enrutador está equipado con doce puertos Ethernet Gigabit, cuatro puertos SFP, un cable de consola serie y un puerto USB. La versión actualizada r2 incluye características mejoradas como 4GB de RAM integrados, una ranura M.2 integrada, un puerto USB de tamaño completo y fuentes de alimentación redundantes para una mayor redundancia. Esta sólida combinación de capacidades de hardware posiciona al CCR1036-12G-4S como una solución de primera categoría para entornos de redes exigentes (Mikrotik, 2023).

Características. La Tabla 2., detalla las especificaciones físicas y técnicas del Router Mikrotik ccr1036:

Tabla 2

Especificaciones del Router

Código de producto	**CCR1036-12G-4S**
Arquitectura	TILE
CPU	TLR4-03680
Cantidad de núcleos de CPU	36
Frecuencia nominal de la CPU	1.2 GHz
Dimensiones	443 x 193 x 44 mm
Licencia de RouterOS	6

Sistema operativo	RouterOS
Tamaño de RAM	4 GB
Tamaño de almacenamiento	1 GB
Tipo de almacenamiento	NAND
MTBF	Aproximadamente 200,000 horas a 25°C
Temperatura ambiente probada	-20°C a 60°C
Aceleración de hardware Ipsec	Sí
N° entradas de corriente alterna	2
Rango de entrada de corriente alterna	100-240
Consumo máximo de energía	60 W
Tipo de refrigeración	2 ventiladores
Puertos Ethernet 10/100/1000	12
DDMI de SFP	Sí
Puertos SFP	4
Puerto de consola serial	RJ45
Número de puertos USB	1
Reinicio de energía USB	Sí
Tipo de ranura USB	USB tipo A
Corriente USB máxima (A)	1
Número de ranuras M.2	1
Monitor de temperatura de la CPU	Sí
Monitor de temperatura de la PCB	Sí
Monitor de voltaje	Sí
Botón de modo	Sí
Zumbador	Sí

Fuente: (Mikrotik, 2023)

3.3.2 Hipervisor Proxmox

Proxmox Virtual Environment es una plataforma completa y de código abierto para la gestión de servidores en virtualización empresarial. Integra de manera estrecha el hipervisor KVM y los contenedores de Linux (LXC), así como funciones de almacenamiento y redes definidas por software, todo en una sola plataforma. Con la interfaz de usuario integrada basada en web, puedes gestionar máquinas virtuales (VMs) y contenedores, garantizar alta disponibilidad para clústeres o utilizar las herramientas integradas de recuperación ante desastres con facilidad (Proxmox, 2023).

La solución ofrece cómputo, red y almacenamiento en una única plataforma. Sus características de clase empresarial y su enfoque 100% basado en software hacen de Proxmox VE la elección perfecta para virtualizar tu infraestructura de TI, optimizar los recursos existentes y aumentar la eficiencia con gastos mínimos. Al combinar dos tecnologías de virtualización en una única plataforma, Proxmox VE proporciona máxima flexibilidad a tu entorno de producción. Utiliza la virtualización completa de KVM para imágenes de Windows y Linux, y contenedores ligeros para ejecutar aplicaciones Linux sin conflictos (Proxmox, 2023).

Características. Proxmox VE es ideal para virtualizar infraestructuras de TI, optimizar recursos existentes y aumentar la eficiencia con un enfoque totalmente basado en software. Combina las tecnologías de virtualización KVM y LXC, brindando flexibilidad para ejecutar cargas de trabajo de aplicaciones tanto en Windows como en Linux. Además, Proxmox VE

fomenta la contribución a su proyecto de código abierto y ofrece servicios de soporte y formación empresarial. Las características principales de Proxmox son (Proxmox, 2023):

- Virtualización de Servidores
- Gestión Centralizada
- Clustering (Agrupamiento)
- Autenticación
- Clúster de alta disponibilidad (HA) de Proxmox VE
- Redes conectadas
- Opciones de almacenamiento flexibles
- Almacenamiento definido por software con Ceph
- Cortafuegos Proxmox VE
- Copia de seguridad/restauración
- Integración del servidor de copia de seguridad de Proxmox

3.3.3 DaloRadius

Es una plataforma web RADIUS avanzada diseñada para gestionar Hotspots y despliegues de ISP de propósito general. Ofrece una gestión de usuario completa, informes gráficos, contabilidad e integración con GoogleMaps para la geo-localización (GIS). DaloRadius está escrito en PHP y JavaScript, y utiliza una capa de abstracción de base de datos, lo que significa que es compatible con muchos sistemas de bases de datos, entre ellos los populares MySQL, PostgreSQL, Sqlite, MsSQL, y muchos otros (DaloRadius, 2007).

Se basa en una implementación de Freeradius con un servidor de base de datos que sirve como backend. Entre otras funciones, implementa ACL, integración de GoogleMaps para la ubicación visual de hotspots/puntos de acceso y muchas más características. DaloRadius es esencialmente una aplicación web para gestionar un servidor RADIUS, por lo que teóricamente puede gestionar cualquier servidor RADIUS, pero específicamente gestiona Freeradius y su estructura de base de datos. Desde la versión 0.9-3, DaloRadius ha introducido una capa de abstracción de base de datos en toda la aplicación basada en el paquete PHP PEAR:DB, que admite una variedad de servidores de bases de datos (DaloRadius, 2007).

3.3.4 WinBox

MikroTik RouterOS representa un sistema operativo diseñado inicialmente para MikroTik RouterBOARD, un hardware específico. Sin embargo, su versatilidad permite su implementación en PCs o máquinas virtuales, transformándolos en enrutadores multifuncionales con capacidades integrales.

RouterOS se fundamenta en el kernel Linux v2.6, lo que confiere robustez y estabilidad al sistema operativo. Esta base tecnológica ofrece una amplia gama de funcionalidades y herramientas avanzadas para la gestión y administración de redes. Es esencial para los administradores principiantes adquirir un conocimiento básico en redes informáticas para aprovechar al máximo las capacidades de RouterOS (Hashemi, 2022).

Winbox emerge como una herramienta indispensable para la administración y monitoreo de MikroTik RouterOS. Esta aplicación, con una interfaz gráfica intuitiva y rápida, permite una configuración eficiente del enrutador, adaptándose tanto a sistemas nativos win32 como Linux y

macOS mediante la emulación de Wine. A pesar de su naturaleza gráfica, Winbox replica funcionalidades de la consola, siendo vital para tareas específicas como el monitoreo en tiempo real del tráfico y la gestión de archivos (Ashley, 2022).

Configuraciones Avanzadas en MikroTik. Mikrotik ofrece una gran variedad de utilidades que pueden implementarse en varios campos de las telecomunicaciones (Hashemi, 2022):

- Enrutamiento: Implementación de rutas y protocolos para la gestión óptima del tráfico.
- Firewall: Configuración de reglas de seguridad para proteger la red contra amenazas externas.
- Gestión BW: Administración del ancho de banda para garantizar un rendimiento óptimo de la red.
- Punto de Acceso Inalámbrico: Despliegue y configuración de redes inalámbricas para conectividad extendida.
- Pasarela Hotspot: Implementación de puntos de acceso para ofrecer servicios de Internet en áreas específicas.
- Servidor VPN: Configuración de redes privadas virtuales para garantizar conexiones seguras y confiables entre dispositivos.

La administración eficiente de MikroTik RouterOS requiere una comprensión profunda de sus herramientas y funcionalidades, especialmente de Winbox. La correcta implementación y configuración de las diferentes características, como enrutamiento, firewall y gestión de ancho de

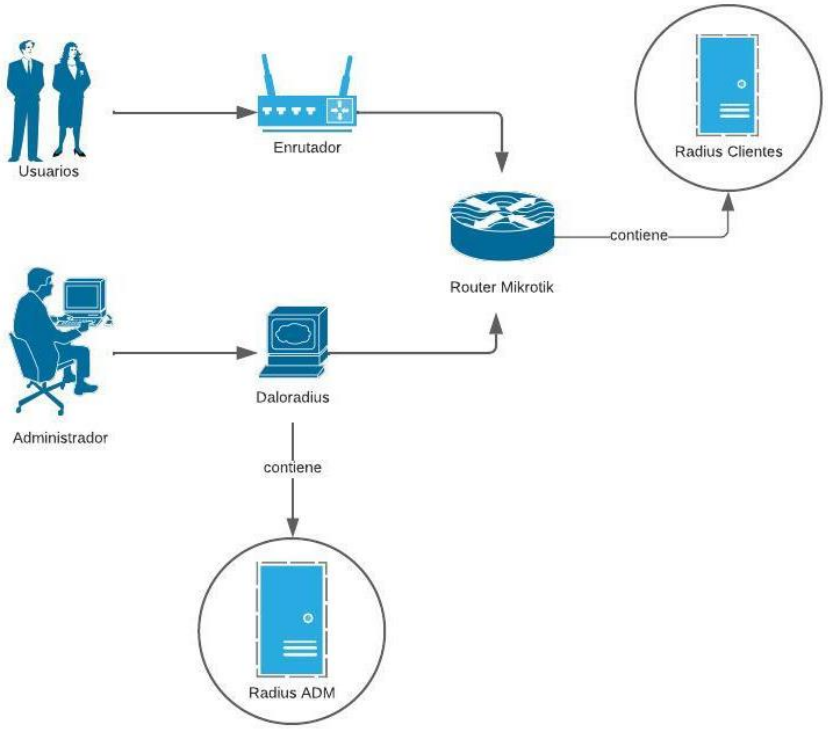
banda, son cruciales para optimizar el rendimiento y la seguridad de la red. En este contexto, el marco teórico proporciona una base conceptual y práctica para abordar de manera sistemática los desafíos asociados con la administración de MikroTik RouterOS y sus configuraciones avanzadas (Ashley, 2022).

3.4 Arquitectura

En la Figura 1., se muestra una posible estructura para llevar a cabo la administración de las conexiones a Internet de los usuarios de la empresa SITEC en la ciudad de Ibarra, empleando la arquitectura AAA y el protocolo PPPoE con dispositivos MikroTik, implica una serie de pasos bien definidos para asegurar la seguridad, escalabilidad y una gestión eficaz.

Figura 1

Arquitectura



Nota. En la imagen se muestra el diagrama de arquitectura que se implementa en el proyecto y sus componentes.

- Gestión de Usuarios y Credenciales: Crear un registro centralizado que contenga la información de los usuarios, incluyendo sus credenciales de autenticación, roles y permisos.
- Punto de Acceso con Equipos MikroTik: Colocar el dispositivo MikroTik en el borde de la red para operar como punto de acceso PPPoE. Configurar perfiles PPPoE que definan límites de ancho de banda y políticas de autorización de acuerdo con los roles de los usuarios.
- Servidor AAA: Desarrollar un servidor AAA encargado de gestionar la autenticación, autorización y registro de las conexiones. Optar por un servidor RADIUS, como FreeRADIUS, para colaborar con los dispositivos MikroTik.
- Proceso de Autenticación y Autorización: Al intentar la conexión a la red, verificar las credenciales del usuario y determinar los permisos correspondientes. Establecer comunicación entre el servidor AAA y los equipos MikroTik utilizando el protocolo RADIUS.
- Gestión de Sesiones PPPoE: Delegar a los dispositivos MikroTik la gestión de la autenticación PPPoE y establecer sesiones individuales para los usuarios. Aplicar las políticas de autorización definidas previamente en el servidor AAA a cada sesión PPPoE.
- ONU (Unidad de Red Óptica): Dispositivos ubicados en los hogares o empresas de los usuarios. Se conectan a través de fibra óptica y sirven como el punto de conexión principal.

- Registro y Control de Actividad: Configurar el servidor AAA para registrar la actividad de los usuarios, incluyendo detalles como el tiempo de conexión y el consumo de datos. Proveer información valiosa para la facturación y seguimiento de la actividad.
- Monitoreo y Resolución de Problemas: Utilizar herramientas de monitoreo para supervisar el rendimiento de la red y detectar problemas en tiempo real. Establecer procedimientos efectivos para solucionar problemas de conectividad y desempeño.

3.5 Diseño de Procesos

En esta sección, se detallan los procesos cruciales necesarios para llevar a cabo con éxito el proyecto. Se describen paso a paso los procedimientos para la configuración de PPPoE, el proceso de autenticación, la integración con el servidor Radius y el acceso posterior a los equipos de red.

La configuración de PPPoE implica la especificación de diversos parámetros, como encapsulación, configuraciones de VLAN, modo de obtención de IP, y definición de parámetros relacionados con IP, tales como dirección, máscara de subred, puerta de enlace y servidor DNS. El proceso de autenticación garantiza una validación segura de los usuarios antes de acceder a los recursos de la red. La integración de PPPoE con el servidor Radius mejora la seguridad y facilita la gestión centralizada de perfiles de usuario, posibilitando una autorización y contabilidad eficientes. Finalmente, la provisión de acceso a los equipos de red implica establecer conexiones seguras, implementar controles de acceso y asegurar que las configuraciones se alineen con los objetivos generales del proyecto.

Antes de iniciar el proceso de registro de clientes en los servidores y sistemas, se realiza una fase crucial de actualización de datos, como se detalla en la Figura 2. Durante este paso, se escanean físicamente los contratos firmados por los usuarios, y la información relevante se introduce en una base de datos organizada en una hoja de cálculo Excel. Esta base de datos sirve como un repositorio estructurado donde se registran los detalles de cada usuario.

Con el objetivo de facilitar la migración a PPPoE, se asignan los parámetros necesarios, como el número de cédula del usuario, el plan de servicio contratado y detalles específicos para la configuración PPPoE. Esto incluye la asignación de direcciones local y remota, número de puerto, así como nombre de usuario y contraseña para la autenticación en la red. Este enfoque ordenado y sistematizado asegura una migración eficiente y precisa hacia el nuevo sistema, garantizando que cada cliente cuente con la configuración adecuada para el servicio PPPoE.

El detallado proceso de configuración de PPPoE para los clientes abarca pasos esenciales para asegurar un acceso seguro y eficiente a los servicios de Internet. Inicia en el entorno de Winbox con la creación de una lista de direcciones IP disponibles, estableciendo así una base para asignaciones posteriores. Luego, se procede a la creación de una interfaz VLAN, actuando como un mecanismo de segmentación de red para una gestión más efectiva. Posteriormente, se asigna una dirección IP específica a la recién creada VLAN, verificando y visualizando esta dirección IP para garantizar la correcta asignación. A continuación, se crea una dirección LAN local y remota dentro de la VLAN, estableciendo las bases para la conectividad interna y externa del usuario.

El siguiente paso implica la implementación de un servicio PPPoE, crucial en la autenticación y asignación dinámica de direcciones IP a los usuarios. Se establecen parámetros

detallados para la autenticación y contabilidad del servicio PPPoE, contribuyendo a un control preciso y seguro de la conexión.

En cuanto al proceso de autenticación que sigue el cliente una vez registrado en la red, se configura la verificación de credenciales, como contraseñas, tokens, datos biométricos o certificados digitales, para validar la autenticidad de la entidad solicitante de acceso. La incorporación de clientes implica un registro sistemático asignando una identificación única, generalmente el número de cédula, junto con una contraseña. Una vez autenticados, los clientes reciben parámetros de red específicos, asignándose direcciones IP locales y remotas, asegurando una interacción de red racionalizada y segura.

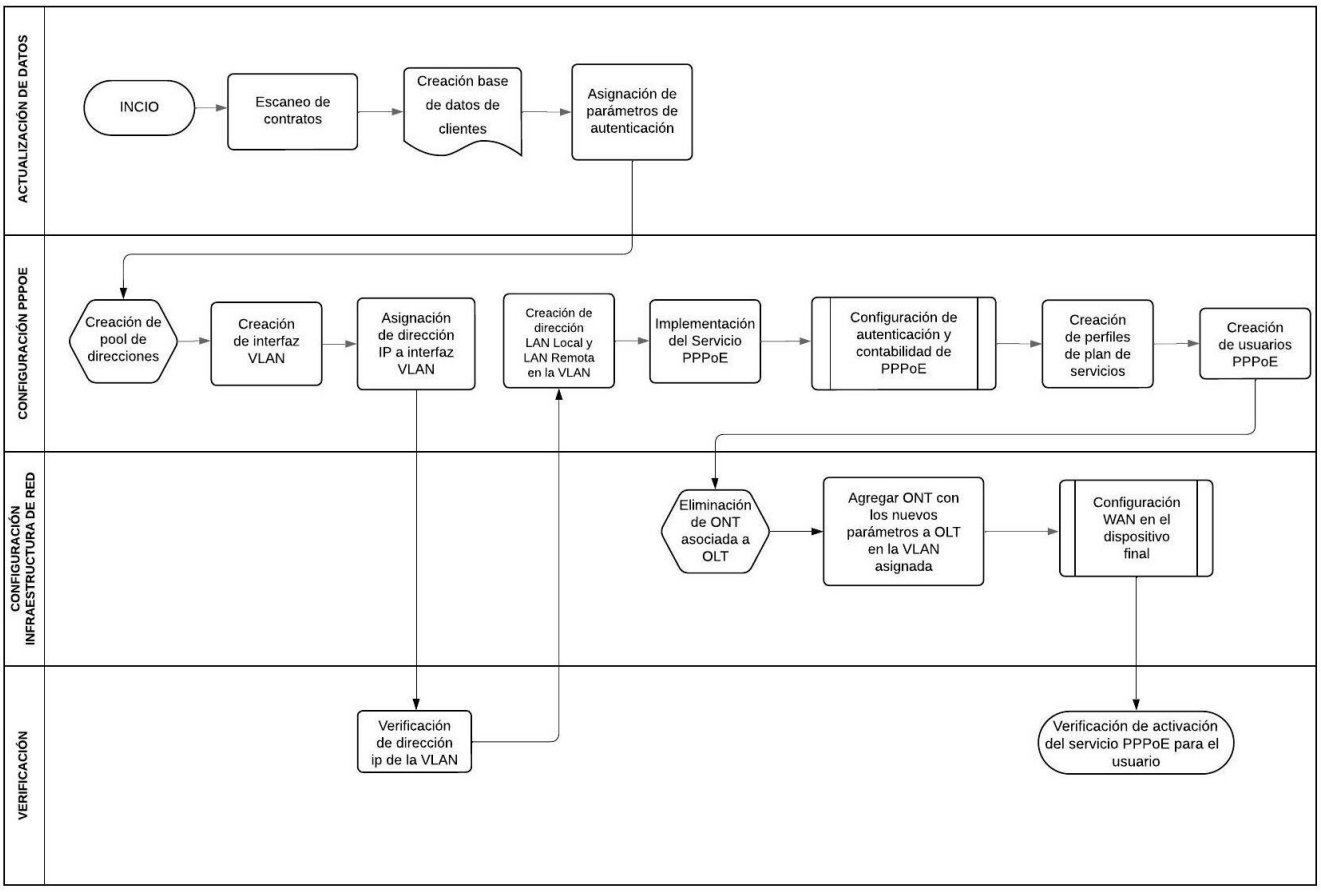
A través de la delimitación de funciones, la aplicación de sólidos mecanismos de autenticación y el mantenimiento de un enfoque estructurado de los componentes físicos y lógicos, el diseño de este proceso pretende fomentar un marco de autenticación seguro, eficiente y escalable para la empresa. Adaptándose a las necesidades específicas de los usuarios, se desarrollan perfiles de servicios personalizados. Posteriormente, se genera un usuario único permitiendo el acceso al servicio PPPoE de manera individualizada. En el ámbito de la infraestructura de red, se procede a la eliminación de la Optical Network Terminal (ONT) asociada al usuario en la Optical Line Terminal (OLT), seguido de la inclusión de la ONT en la VLAN designada para el usuario. Se configura una Wide Area Network (WAN) en el dispositivo final del usuario, estableciendo así la conexión a la red más amplia.

Finalmente, se verifica minuciosamente la correcta configuración y activación del servicio PPPoE en el enrutador MikroTik del usuario, garantizando que el acceso a Internet se realice de manera óptima y segura. Este proceso integral proporciona una estructura detallada

para la implementación exitosa del servicio PPPoE para los clientes, asegurando una experiencia de usuario eficiente y confiable.

Figura 2

Proceso de Configuración PPPoE para clientes



Nota. En la imagen se detalla el proceso de implementación del servicio PPPoE para en todas sus etapas.

El proceso detallado de configuración PPPoE para administradores desempeña un papel fundamental en el establecimiento y mantenimiento de una red segura y eficiente, como se muestra en la Figura 3. Inicia con la integración exitosa del servidor RADIUS con el protocolo PPPoE, requiriendo una secuencia de pasos meticulosamente diseñados. La primera fase

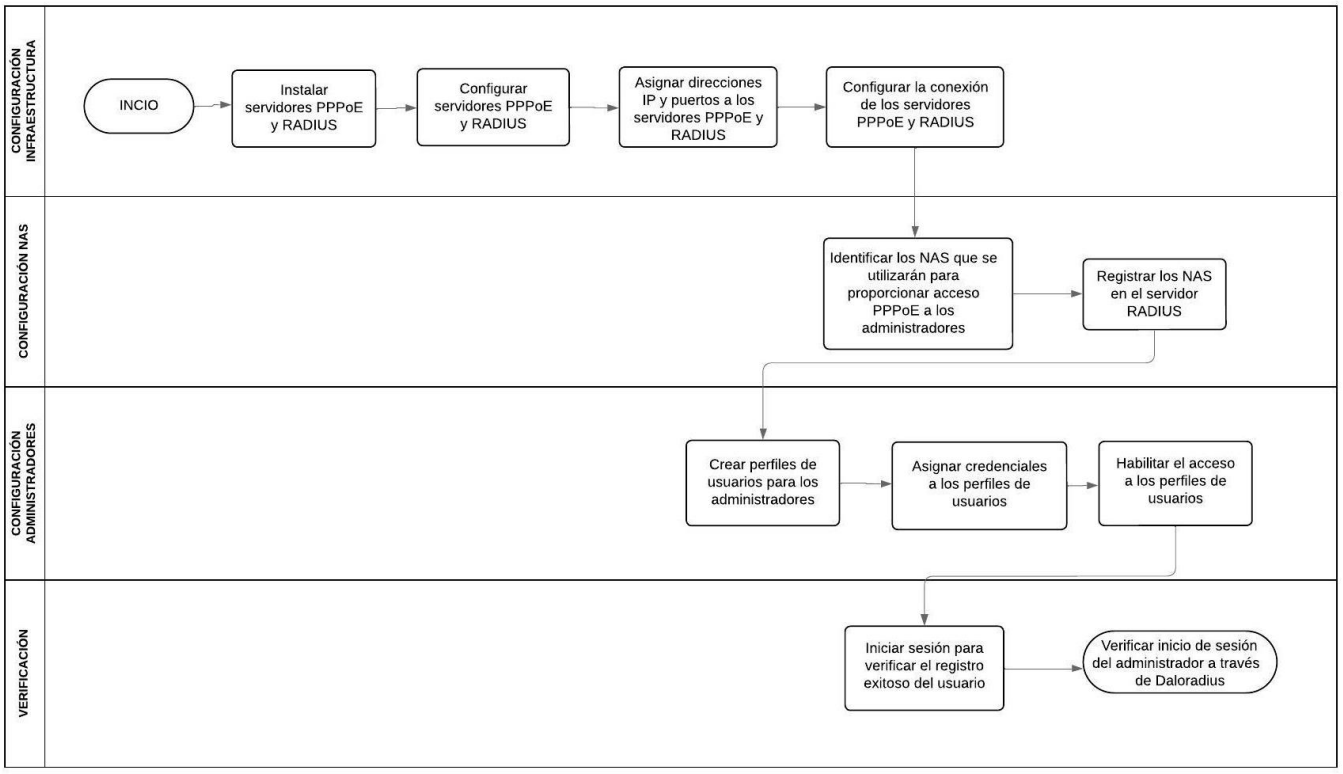
comprende la configuración de servidores dedicados para PPPoE y RADIUS, estableciendo así la infraestructura esencial. El registro de servidores de acceso a la red (NAS) en Daloradius marca el comienzo, asegurando la correcta integración entre servidores y dispositivos de acceso a la red.

En el ámbito de la autenticación, se añaden usuarios con credenciales y funciones específicas, permitiendo una gestión de acceso individual basada en roles. Este proceso aborda tanto aspectos físicos como lógicos. En el plano físico, se asignan credenciales de administrador, renovadas anualmente para garantizar seguridad y relevancia. La parte lógica implica la asignación de identificaciones únicas y la integración de perfiles en el sistema RADIUS, configurando nombres de usuario y contraseñas específicos.

El personal administrativo obtiene acceso meticuloso a componentes clave de la red, ajustado según la jerarquía organizativa y funciones. Los privilegios se adaptan cuidadosamente a las responsabilidades individuales para garantizar seguridad y eficacia operativa. La verificación del estado de usuario activo y la conexión segura entre la red central y el servidor Radius son pasos cruciales. Habilitar la Autenticación, Autorización y Contabilidad (AAA) para los administradores concluye este proceso, añadiendo una capa de seguridad al exigir autenticación antes del acceso a la red.

Figura 3

Proceso de Configuración PPPoE para administradores



Nota. En la imagen se muestra el proceso de configuración de PPPoE para los usuarios que ingresan en el área de administración, lo cual permite llevar un control de accesos y evitar intrusos.

3.5.1 Especificaciones de los Equipos y Herramientas

La herramienta principal para la implementación de servicios es Proxmox, sobre la cual se ha construido el sistema operativo Debian 11 para respaldar Daloradius. A continuación, se detallan los requisitos de cada una de estas plataformas para garantizar su funcionamiento adecuado. Proxmox, como la herramienta central, orquesta los servicios de virtualización y

requiere una configuración de hardware sólida para gestionar eficazmente las máquinas virtuales. Debian 11, como sistema operativo subyacente, proporciona un entorno estable para alojar y ejecutar la aplicación Daloradius. Comprender y cumplir con los requisitos específicos de Proxmox y Debian 11 son pasos fundamentales para establecer una infraestructura confiable y eficiente para la implementación de servicios en este sistema.

En la Tabla 3. se especifica los requerimientos para la instalación realizando el dimensionamiento del sistema, donde se requiere almacenar y procesar hasta 10 usuarios, en relación con el escenario de la empresa, tomando en cuenta que sería 10 usuarios el máximo de almacenamiento:

Tabla 3

Requerimientos Generales del sistema

Requerimientos	Daloradius	Freeradius	Debian 11	Proxmox
CPU	Procesador 1 Núcleo			Procesador 2 núcleos
Memoria RAM	1 GB de RAM	1 GB de RAM	4 GB de RAM	8 GB de RAM
Almacenamiento	1 GB	1 GB	10 GB de espacio en disco duro	32GB de espacio libre en disco

Para la memoria RAM: El requisito mínimo de funcionamiento es de 512MB de RAM para Daloradius se asigna 1GB, se han asignado recursos de memoria RAM según los requisitos mínimos y consideraciones de holgura, el requisito mínimo es 512 MB de RAM dedicada para FreeRADIUS y 256 MB para su funcionamiento por lo tanto se asigna 1GB (Cepeda & Proaño, 2007). Para Debian 11 los requisitos mínimos son 2 GB de RAM dedicada para Daloradius y FreeRADIUS y 512 MB para funcionamiento del sistema se ha asignado un total de 4GB de

RAM, lo que garantiza suficiente holgura y capacidad de respuesta del sistema (Debian.org, 2004). En el entorno de Proxmox, se ha reservado un mínimo de 4GB de RAM para la instancia de Debian 11, con un total de 8GB asignados para asegurar un funcionamiento fluido y eficiente de los servicios de FreeRADIUS y Daloradius alojados en la máquina virtual.

Para el almacenamiento: El requisito mínimo es 100MB de espacio en disco para Daloradius y su base de datos, se sugiere asignar 150MB de espacio en disco para FreeRADIUS, por lo tanto, se ha reservado 1GB de espacio en disco para Daloradius y su base de datos, así como también para FreeRADIUS y su base de datos, asegurando suficiente espacio para el funcionamiento actual y futuras actualizaciones, Además, se ha dedicado un total de 10GB de espacio en disco duro (300MB de espacio en disco para la implementación de Daloradius y FreeRADIUS, incluyendo sus bases de datos y archivos del sistema), se ha asignado un espacio significativo de 32GB en disco para la instalación del sistema operativo Proxmox VE y el almacenamiento de imágenes de máquinas virtuales, como Debian, asegurando suficiente espacio para el crecimiento y la expansión de la infraestructura virtualizada.

El acceso al equipo otorga al administrador un conjunto de capacidades para administrar y supervisar varias funcionalidades de la red. Estas capacidades abarcan:

Configuración de WAN y LAN: El administrador tiene la autoridad para configurar y ajustar la configuración de la red de área amplia (WAN) y la red de área local (LAN), lo que garantiza un rendimiento óptimo de la red y una conectividad adaptada a las necesidades de la organización.

Control de ancho de banda: La capacidad de regular y asignar recursos de ancho de banda permite al administrador priorizar las actividades críticas de la red, lo que garantiza un funcionamiento fluido y minimiza los posibles cuellos de botella.

Enrutamiento de paquetes: Al supervisar el enrutamiento de paquetes, el administrador puede dictar cómo viajan los datos a través de la red, optimizando la eficiencia y asegurando que la información llegue a su destino previsto de forma segura y rápida.

Gestión de clientes: La capacidad de agregar o eliminar usuarios finales garantiza que la red siga siendo escalable y sirva de manera eficiente a su usuario.

Capítulo IV: Implementación y Pruebas de Funcionamiento de la Arquitectura

En este capítulo, se aborda de manera exhaustiva el proceso integral de implementación del proyecto, detallando las instalaciones y configuraciones específicas llevadas a cabo en cada programa o equipo utilizado. Además, se examina minuciosamente la verificación de cambios de dirección realizados por los usuarios, lo que se busca contrarrestar con la ejecución del proyecto, buscando siempre garantizar la integridad y seguridad de la red.

4.1 Implementación de la Arquitectura

Cada fase de esta etapa crítica se describe minuciosamente, evidenciando la disposición estratégica de recursos esenciales y su alineación precisa con los objetivos predefinidos del proyecto. La documentación detallada de cada paso no solo asegura la transparencia y la trazabilidad de las acciones emprendidas, sino que también sienta las bases para validar y reproducir los resultados obtenidos. Este enfoque metódico y riguroso se establece como un pilar fundamental en el marco de este trabajo de titulación, garantizando coherencia, eficacia operativa y una base sólida para futuras investigaciones o implementaciones.

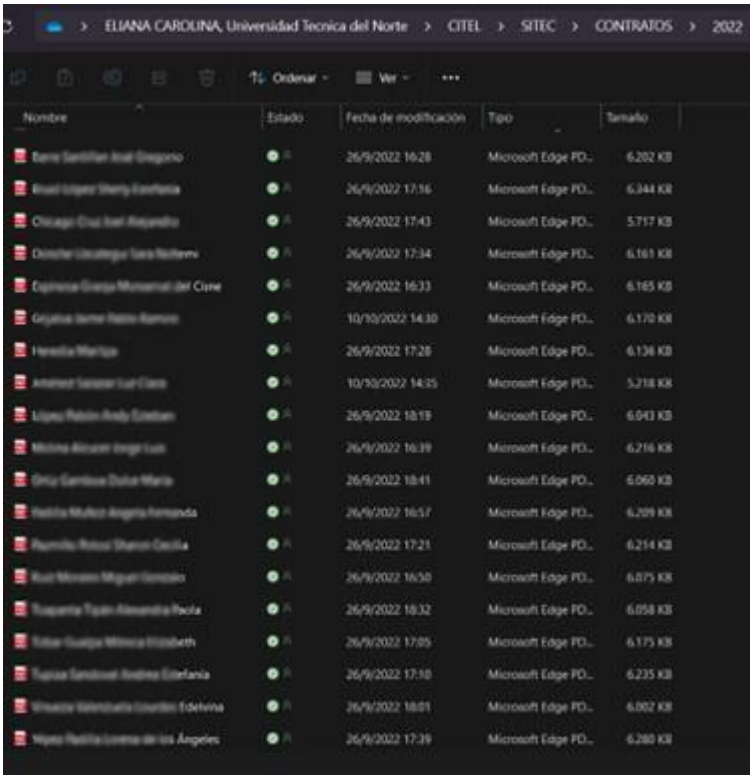
4.1.1 Gestión de Usuarios y Credenciales

Al llevar anteriormente un sistema de registro para contratos impresos, se identificó una gestión desorganizada de la documentación, con contratos que carecían de información o documentación completa. Para abordar este problema, se inició un proceso de digitalización integral de todos los contratos, que se visualizan en la Figura 4. Este enfoque busca mejorar el

control y realizar una exhaustiva actualización de datos, eliminando y añadiendo la información necesaria para establecer una base de datos completa y actualizada.

Figura 4

Contratos Digitalizados



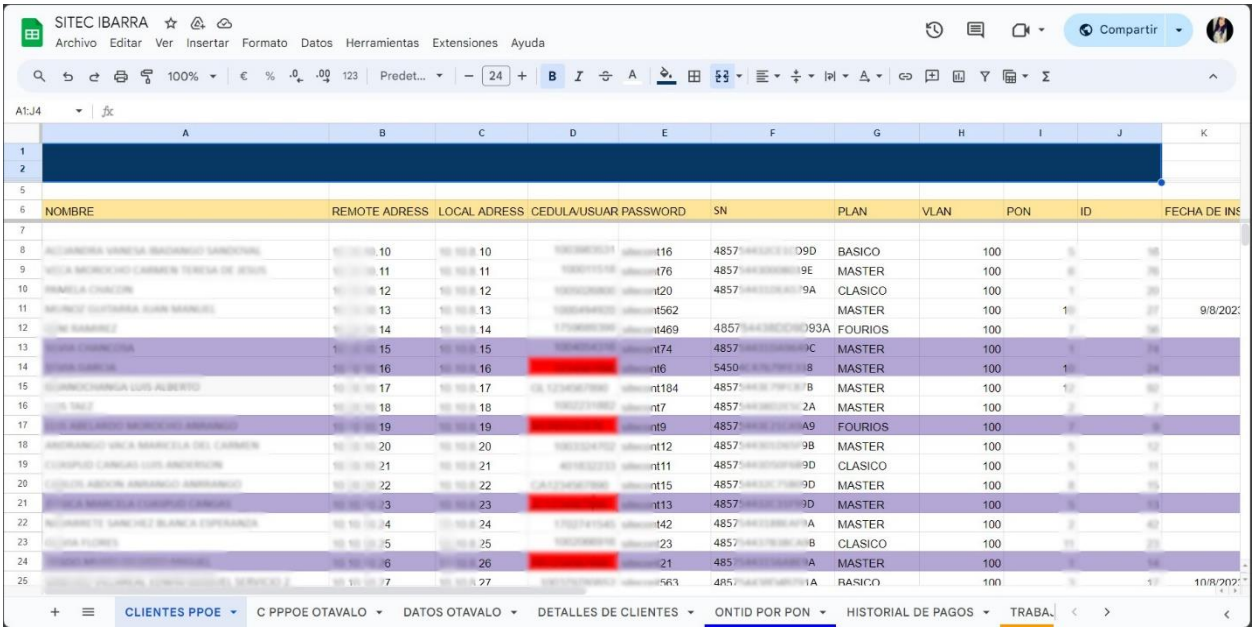
Nota. En la imagen se puede visualizar los contratos digitalizados para un mejor manejo de los datos de cada cliente, se registra con los nombres completos del titular del contrato.

Se ha implementado una base de datos en Excel con el propósito de mantener un registro organizado de los clientes. Como se muestra en la Figura 5. en la base de datos, se visualizan los contratos que presentan información incompleta, facilitando así la identificación de áreas de mejora. Además, se ha incorporado la asignación de direcciones IP y la generación de nombres de usuario y contraseñas para el proceso de autenticación. Esta herramienta proporciona una

solución eficiente para la gestión integral de clientes, mejorando la calidad y consistencia de la información registrada.

Figura 5

Base de Datos Clientes



Nota. En la imagen se puede visualizar los datos de los clientes en los cuales se registra nombres completos, números de cédula, teléfono, plan contratado, en la misma base se asignará información sobre las direcciones ip local y remota, el usuario y la contraseña de cada usuario para su autenticación PPPoE.

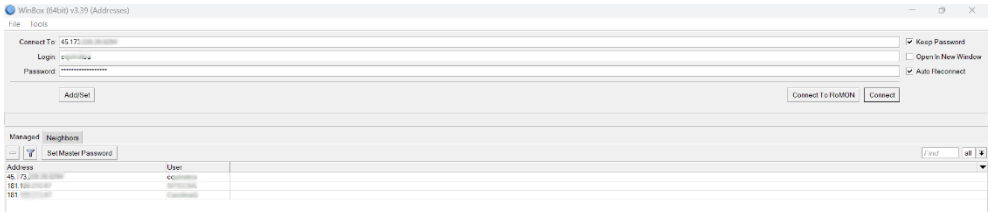
4.1.2 Configuración en Equipo Mikrotik

Las primeras configuraciones se llevan a cabo en Winbox, en la Figura 6., se visualiza la ventana del programa. Al iniciar, solicita ingresar las credenciales y datos necesarios para conectarse al nodo. Estos datos incluyen la dirección IP, el nombre de usuario y la contraseña de

acceso. Cada usuario cuenta con privilegios distintos que determinan su capacidad para efectuar cambios y configuraciones específicas. Una vez que el usuario se ha autenticado con éxito, se accede a la ventana principal de Winbox, desde donde se podrán realizar las configuraciones necesarias en el nodo correspondiente. Este proceso asegura un acceso seguro y controlado, garantizando que cada usuario tenga las autorizaciones apropiadas para llevar a cabo sus funciones específicas en el sistema.

Figura 6

Ventana Principal Winbox



Nota. Se presenta en la imagen la ventana principal de Winbox, mostrando un menú desplegable en la parte izquierda que ofrece diversas opciones. Esta interfaz proporciona una visión clara y accesible de las funcionalidades disponibles en el programa, facilitando la navegación y configuración de los elementos necesarios en el nodo.

En el proceso de creación de una nueva interfaz, se accede a la opción "Interfaces" y se procede a generar una interfaz VLAN. Se establece la Unidad Máxima de Transferencia (MTU) en 1500, definiendo así el tamaño máximo de los paquetes antes de la fragmentación. Se habilita la opción ARP, y se establece la conexión con la interfaz de la OLT deseada. Para la asignación del nombre de la VLAN se considera los parámetros de la primera letra de la ubicación del nodo y el número de LAN a la cual pertenece la VLAN, como se visualiza en la Tabla 4.

Tabla 4

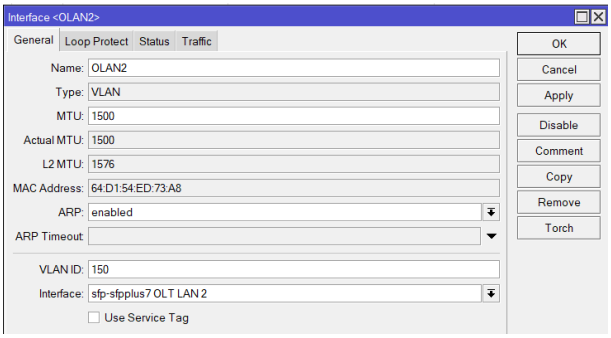
Parámetros de asignación nombre de VLAN

Nombre VLAN	ID	Sector
OLAN1	100	Norte de Ibarra
OLAN2	150	Centro de Ibarra

Este procedimiento garantiza una configuración precisa de la interfaz, permitiendo una transmisión eficiente de datos sin comprometer la integridad de la información debido a la fragmentación y se puede visualizar en la Figura 7.

Figura 7

Creación de Interfaz VLAN 150

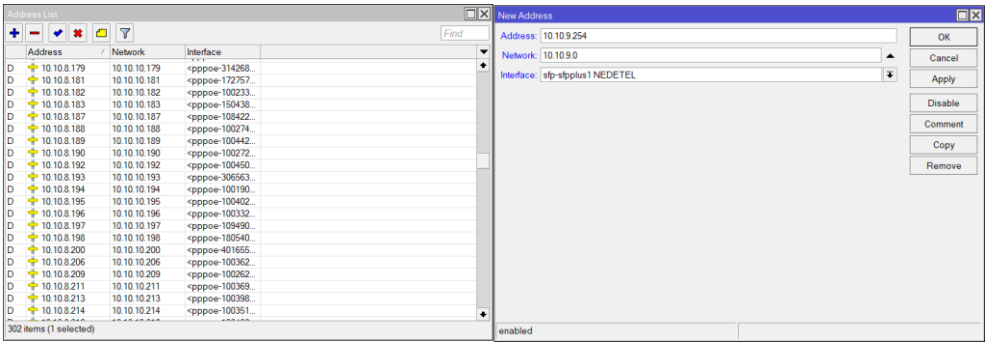


Nota. En la imagen se visualiza la creación de la interfaz que lleva por nombre OLAN1 para la VLAN 150.

Se crea un nuevo rango de direcciones que se utilizará en la red, como se muestra en la Figura 8. Este rango, que abarca desde 10.10.9.0 hasta 10.10.9.254, será asignado a los usuarios conforme se registren mediante la autenticación PPPoE. Esta medida proporciona una estructura ordenada y predefinida para la asignación de direcciones IP, facilitando la gestión y organización de la red.

Figura 8

Lista de Direcciones

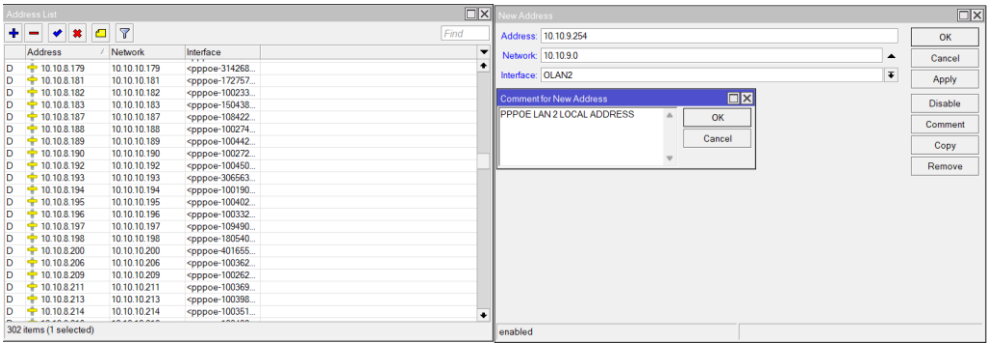


Nota. En la imagen se puede visualizar las direcciones que se encuentran registradas y la creación del rango de direcciones dentro del nodo.

En el proceso de creación de la interfaz VLAN, se procede a añadir una nueva dirección IP que será asignada a dicha interfaz. Se ingresan los detalles de la dirección, como la dirección IP, la máscara de red, la red a la que pertenece y la interfaz recién creada, como se visualiza en la Figura 9. Además, el programa proporciona la opción de incluir un comentario para la dirección, permitiendo al administrador agregar información relevante para una mejor comprensión y gestión de la configuración de la interfaz.

Figura 9

Creación de una nueva dirección para VLAN 150

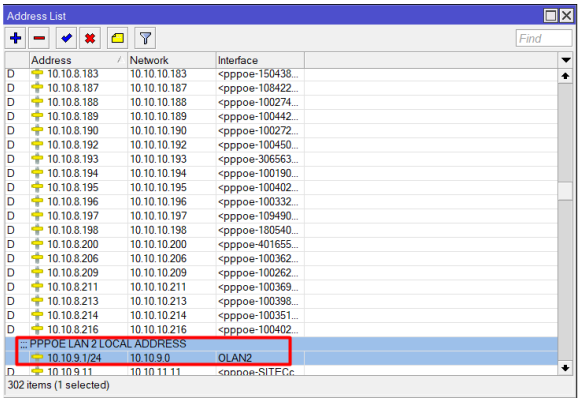


Nota. Para esta dirección se utiliza las configuraciones de la dirección, a esta vlan se le asigna la dirección 10.10.9.254 con la máscara /24, esta vlan pertenece a la red 10.10.9.0, en la sección comentario se especifica que la vlan pertenece a la LAN2.

Tras la creación exitosa de la interfaz, esta se muestra claramente en la lista de direcciones registradas en el programa en la Figura 10., indicando su disponibilidad para el registro de usuarios. Este paso fundamental establece las bases para la incorporación eficiente de usuarios dentro de dicha interfaz, marcando un hito en el proceso de configuración y preparando el terreno para la implementación efectiva de la autenticación PPPoE.

Figura 10

Visualización de la dirección creada



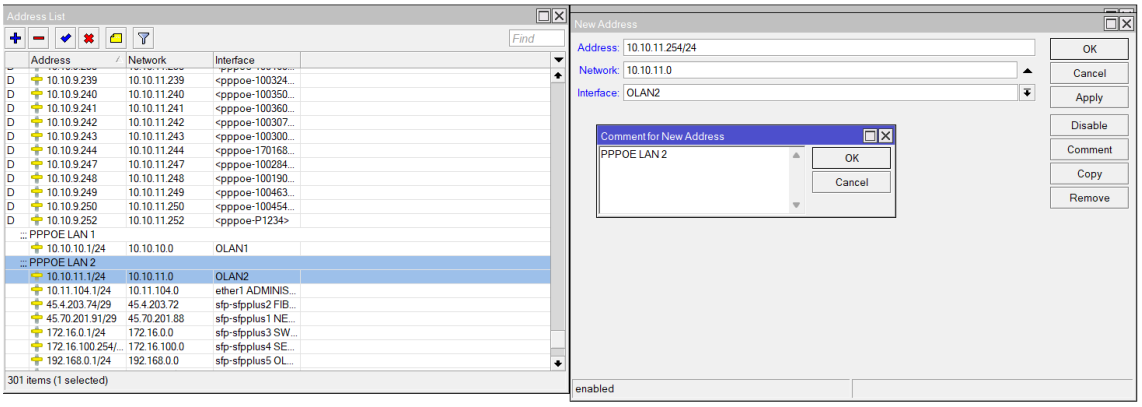
Nota. En la imagen se visualiza que la dirección de red ha sido creada con todos los parámetros y asignada a la VLAN 150, esta vlan almacenará todos los usuarios de este grupo.

El mismo procedimiento se replica para instaurar la dirección correspondiente a la LAN Remota dentro de la VLAN 150, como se muestra en la Figura 11. Esto garantiza coherencia en la configuración de las direcciones IP asociadas a diferentes interfaces, permitiendo una organización sistemática y una gestión eficaz de la red. La duplicación de este paso para la LAN

Remota consolida la cohesión en la estructura de direcciones y facilita la posterior administración y supervisión de la red en su totalidad.

Figura 11

Creación de dirección LAN Remota dentro VLAN 150



Nota. Para la creación de la LAN Remota se asigna la dirección 10.10.11.254 con la máscara /24, dentro de la red 10.10.11.0 en la interfaz VLAN 150.

4.1.3 *Levantamiento y Configuración de Servidor AAA*

En esta sección se detalla información sobre detalles específicos del sistema operativo seleccionado y el gestor de administración utilizado. Se destacará las razones fundamentales que motivaron su elección frente a otras alternativas disponibles, considerando las diversas funcionalidades que ofrecen herramientas similares en el ámbito.

Instalación Debian 11. Para establecer una máquina virtual en Proxmox, es necesario seguir ciertos pasos específicos, este proceso se detalla a profundidad en el Anexo A. Para verificar la funcionalidad del sistema operativo el usuario accede a través de Proxmox al nodo en el cual se encuentra disponible la máquina virtual con el sistema operativo en este caso la versión Debian 1, que se visualiza en la Figura 12. Cabe destacar que se realiza el uso de Debian 11,

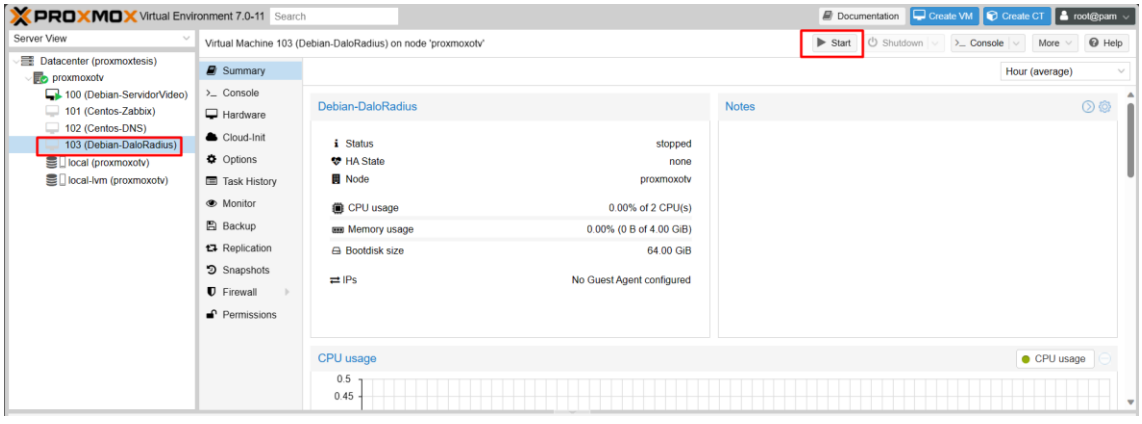
también denominado "Bullseye", porque presenta características que lo distinguen en el entorno de los sistemas operativos Linux.

Una de sus principales fortalezas radica en su estabilidad, respaldada por un proceso meticuloso de pruebas y una política de actualizaciones coherente. Esta fiabilidad se complementa con una comunidad activa y dedicada, lo que facilita la solución de problemas y el intercambio de conocimientos entre usuarios. Además, Debian 11 se beneficia de herramientas de gestión de paquetes, como APT, que simplifican la administración y actualización de software.

Desde el punto de vista de la seguridad, ofrece mecanismos y actualizaciones que refuerzan la protección del sistema. Su diseño modular proporciona a los usuarios la libertad de personalizar el sistema según las exigencias específicas, desde configuraciones básicas hasta ajustes más elaborados, se posiciona como una opción confiable y versátil para múltiples escenarios y usuarios.

Figura 12

Debian-Daloradius en Proxmox

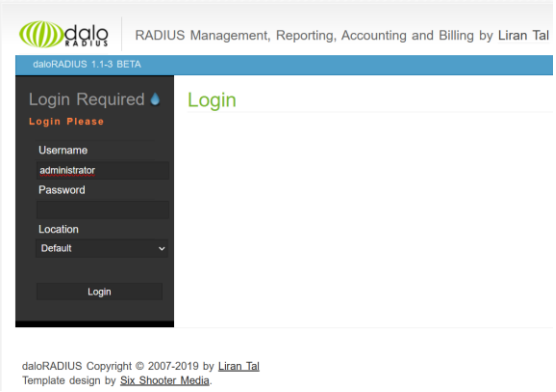


Nota. En la imagen se evidencia la existencia de la máquina virtual con el sistema operativo Debian 11 sobre el cual se realizará las configuraciones para la instalación de Daloradius, por esta razón se nombra a la máquina virtual como Debian-Daloradius.

Instalación DaloRadius. La administración de usuarios se lleva a cabo mediante la plataforma basada en RADIUS denominada DaloRadius. La instalación de esta herramienta implica seguir detenidamente los procedimientos detallados en el Anexo B. Posteriormente, se realiza una verificación exhaustiva del funcionamiento de DaloRadius a través de su interfaz web, que se visualiza en la Figura 13., dicha interfaz es fácil de usar, lo que proporciona una experiencia fluida a los administradores, facilitando una gestión de usuarios y una configuración de red eficientes. La integración de la herramienta con FreeRADIUS mejora sus capacidades, asegurando procesos robustos de autenticación, autorización y contabilidad. Ofrece funciones completas de generación de informes, lo que permite a los administradores obtener información valiosa sobre el uso de la red y las actividades de los usuarios. La flexibilidad y escalabilidad de la herramienta la convierten en la opción preferida para gestionar la autenticación de usuarios y el control de acceso en diversos entornos de red.

Figura 13

Interfaz Web Daloradius



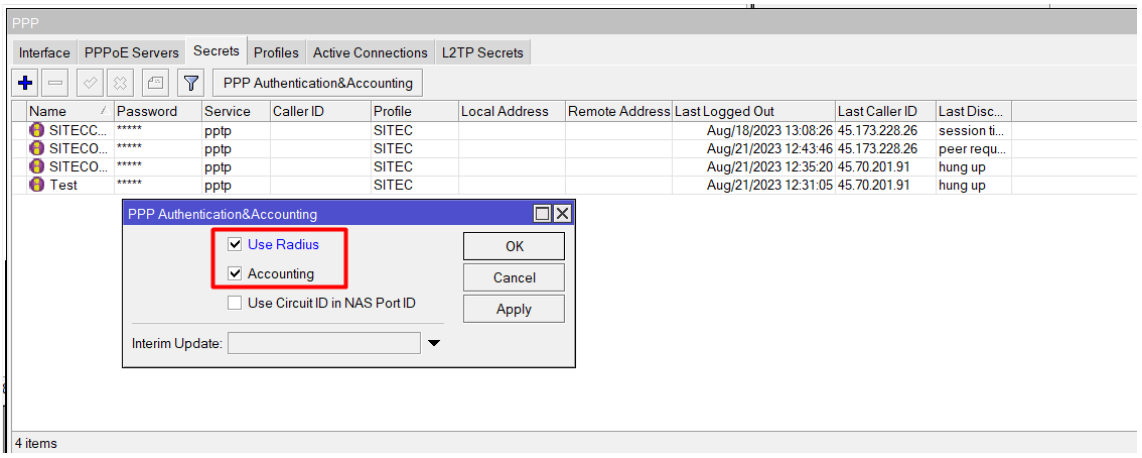
Nota. La interfaz web de Daloradius, accesible a través de la dirección IP del servidor, constituye un punto central para la configuración y administración de servicios de red. En este entorno, la autenticación con un usuario y contraseña previamente definidos permite a los administradores llevar a cabo ajustes y personalizaciones esenciales. Este acceso autorizado no solo facilita la configuración detallada de servicios, sino que también garantiza un entorno seguro y controlado para la administración eficiente de la infraestructura de red.

4.1.4 Proceso de Autenticación y Autorización

En la sección "Secret", se realiza la configuración de dos parámetros esenciales para la autenticación y contabilidad PPP: "Use Radius" y "Accounting", tal como se muestra en la Figura 14. Ambos parámetros deben estar habilitados mediante la marca de verificación correspondiente. Esta configuración es crucial para garantizar un adecuado funcionamiento del proceso de autenticación y la posterior contabilidad de las conexiones PPP, asegurando así una gestión eficiente y precisa de las interacciones de los usuarios.

Figura 14

Configuración de Autenticación y Contabilidad PPP

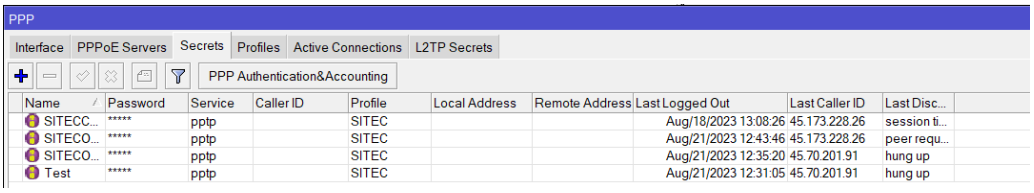


Nota. En la imagen se puede visualizar la selección de dos parámetros importantes dentro de esta configuración, estos parámetros son Use Radius y Accounting, una vez seleccionados únicamente se da el OK para guardar la configuración.

Actualmente, el procedimiento de autenticación se efectúa mediante PPTP para las conexiones de la Red Privada Virtual (VPN), tal como se muestra en la Figura 15. Este enfoque proporciona una capa adicional de seguridad y permite a los usuarios establecer conexiones remotas de forma segura. La implementación de la autenticación a través de PPTP se ajusta a los requisitos específicos de la empresa SITEC, garantizando la confidencialidad y la integridad de los datos en las comunicaciones virtuales.

Figura 15

Situación actual de autenticación de VPN



Nota. En la imagen se puede visualizar que la autenticación de los usuarios que se conectan a través de una VPN se realiza a través de PPPTP, todos estos usuarios se encuentran dentro del perfil SITEC.

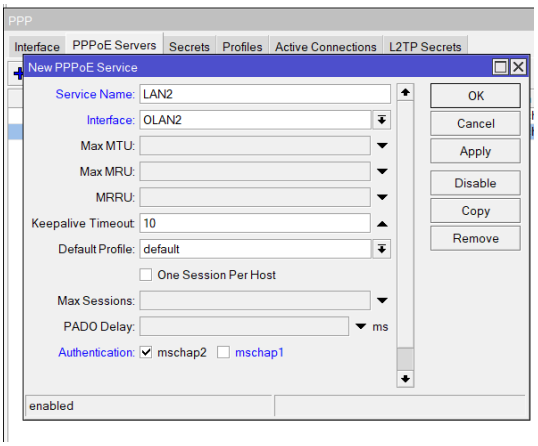
4.1.5 Gestión de Sesiones PPPoE

Dentro del menú principal de Winbox, la opción PPP brinda acceso a la configuración detallada del nuevo servicio PPPoE, que se implementará como parte integral del proyecto. Al

crear un nuevo servicio como se muestra en la Figura 16., se asigna un nombre identificativo, se especifica la interfaz correspondiente, y se realiza la selección del tipo de autenticación deseado. Este proceso es esencial para establecer las bases de un servicio PPPoE eficiente y seguro, adaptado a las necesidades específicas del proyecto en cuestión.

Figura 16

Creación de Servicio para PPPoE



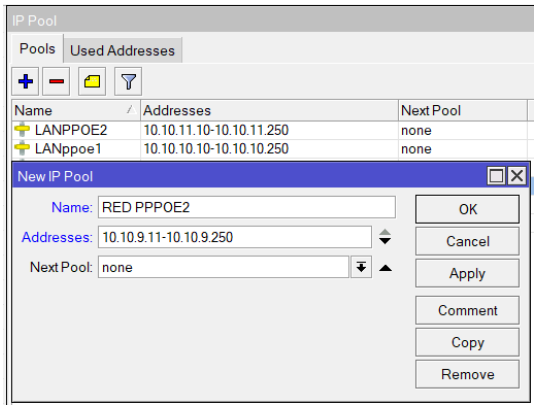
Nota. El servicio se denomina "LAN2", indicando su asociación con la LAN correspondiente. Es crucial resaltar que se ha seleccionado la autenticación MSCHAP2 debido a las numerosas ventajas que ofrece. Esta elección se fundamenta en la robustez y seguridad que proporciona MSCHAP2, contribuyendo así a la implementación de un servicio de autenticación PPPoE confiable y protegido para la OLT en cuestión.

En el proceso de configuración de la red local, se procede a la creación de un Pool de direcciones IP utilizando la opción IP Pool, tal como se muestra en la Figura 17. Este paso es esencial para establecer la conectividad de los dispositivos dentro de la LAN y designar una dirección de Gateway. Este Pool de direcciones no solo facilita la gestión eficiente de las

direcciones IP, sino que también asegura una conectividad coherente y segura para los dispositivos dentro de la red local. La asociación de este Pool con una interfaz específica garantiza una asignación ordenada y automatizada de direcciones IP a los dispositivos de la LAN.

Figura 17

Pool de Direcciones LAN Local



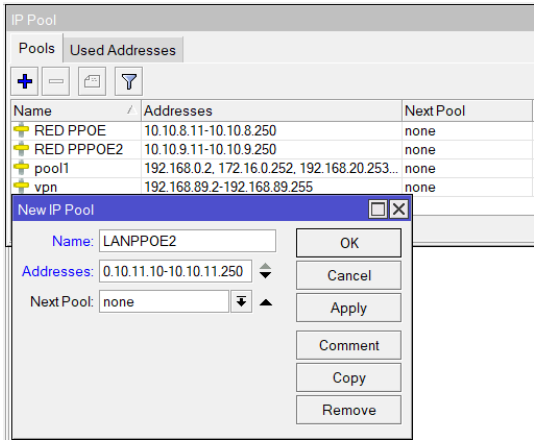
Nota. Al definir un nombre representativo para la red y especificar el rango de direcciones que se asignará, se establece un conjunto de direcciones disponibles para la asignación dinámica a los dispositivos conectados, en este caso la dirección que se asigna es desde la 10.10.9.11 hasta la 10.10.9.250.

En congruencia con el procedimiento anterior, se procede a la creación de un Pool de direcciones destinado a la LAN Remota, que también cumple la función de ser la dirección de red asociada, tal como se muestra en la Figura 18. Al igual que en el caso de la LAN Local, este Pool de direcciones se configura mediante la opción IP Pool. En esta etapa, se asigna un nombre descriptivo para la red y se especifica el rango de direcciones que estará disponible para su asignación dinámica a los dispositivos conectados en la LAN Remota. Este proceso garantiza una gestión eficaz de las direcciones IP y contribuye a mantener una conectividad estable y

segura para los dispositivos dentro de esta red específica. Asociar este Pool con la interfaz correspondiente asegura una distribución ordenada y automatizada de direcciones IP a los dispositivos de la LAN Remota.

Figura 18

Pool de direcciones LAN Remota



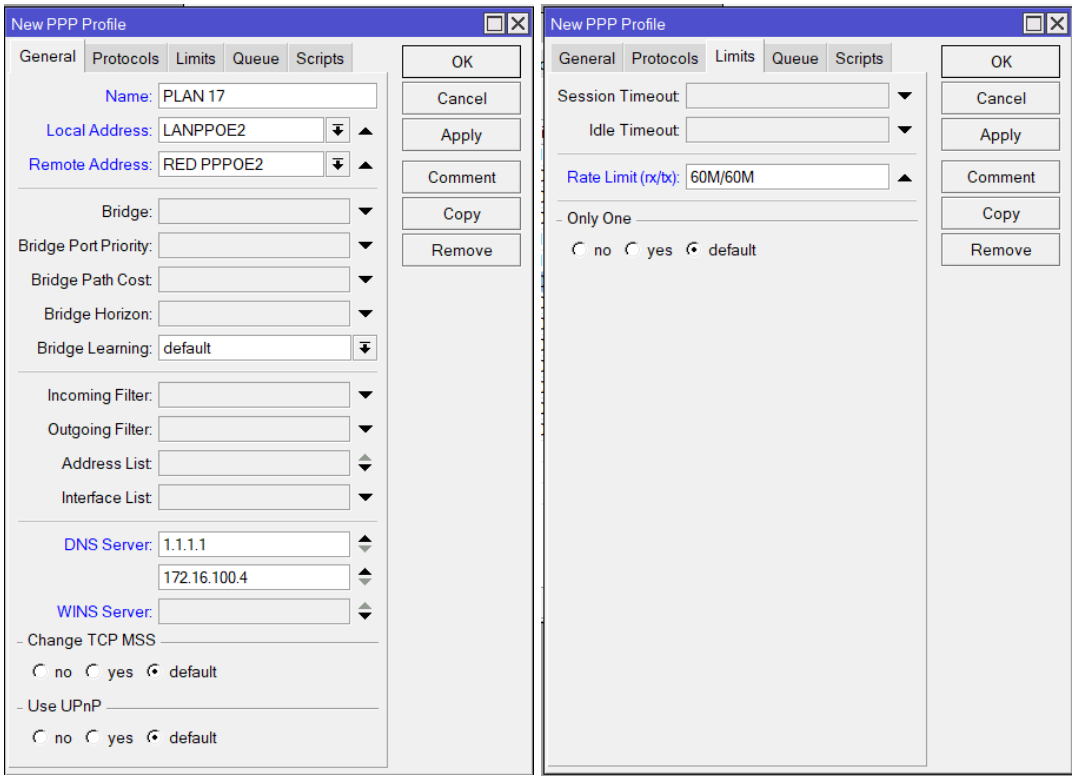
Nota. Asociar este Pool con la interfaz correspondiente asegura una distribución ordenada y automatizada de direcciones IP a los dispositivos de la LAN Remota, en este caso se asigna el nombre Remote LAN1 PPPoE y el rango de direcciones que se usarán es desde la 10.10.11.10 hasta 10.10.11.250.

En el presente contexto, se procede a la configuración de los perfiles de usuario, tal como se muestra en la Figura 19., denominados como Planes de Prestación de Servicios, los cuales constituyen las ofertas de servicios proporcionadas por la empresa. En esta fase, se lleva a cabo la creación minuciosa de dichos perfiles, caracterizados por la definición y asignación precisa del ancho de banda correspondiente a cada plan. Este proceso resulta fundamental en la estructuración y gestión eficiente de la prestación de servicios, al establecer criterios específicos

que regulan la distribución de recursos de conectividad, procurando así una experiencia óptima y personalizada para cada usuario en función del plan adquirido.

Figura 19

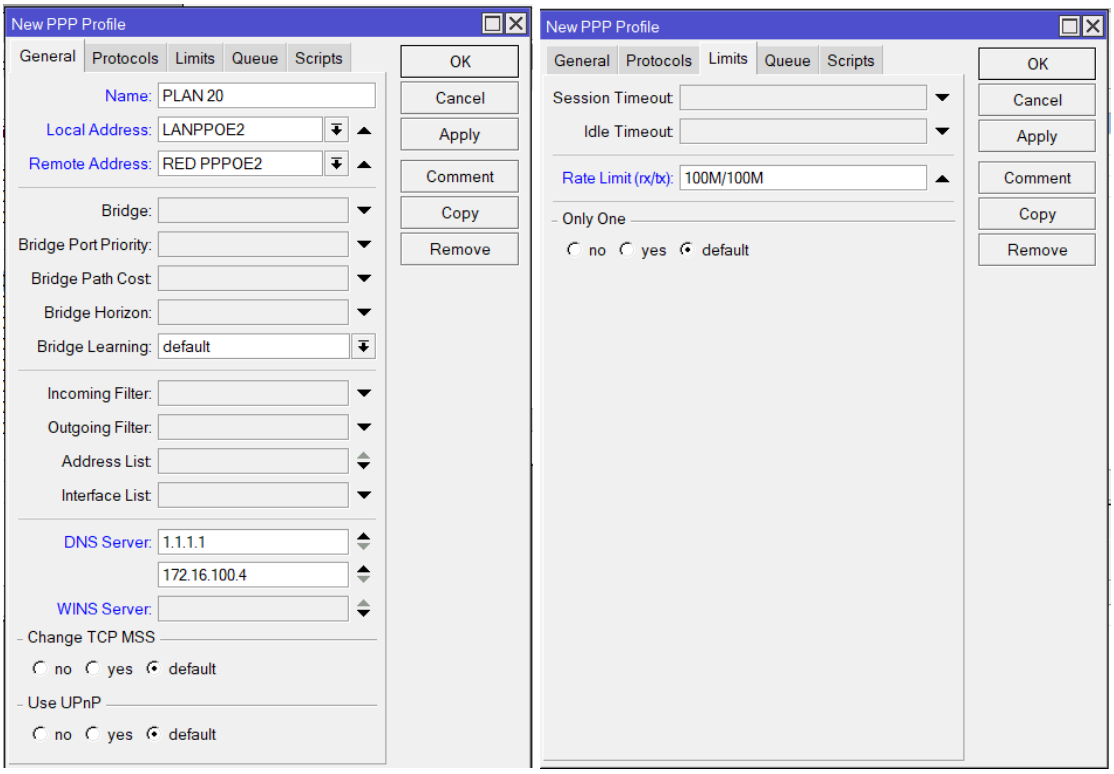
Creación de Perfil Plan 17



Nota. En el perfil denominado "Plan 17", la configuración incluye la dirección local como "LANPPOE2" y la dirección remota como "RED PPPOE2". Los servidores DNS utilizados son 1.1.1.1 y 172.16.100.4. Se ha asignado un límite de velocidad de 60 megabits por segundo tanto en la dirección ascendente como en la descendente. Esta configuración define la experiencia de conectividad para los usuarios que optan por el mencionado plan.

Figura 20

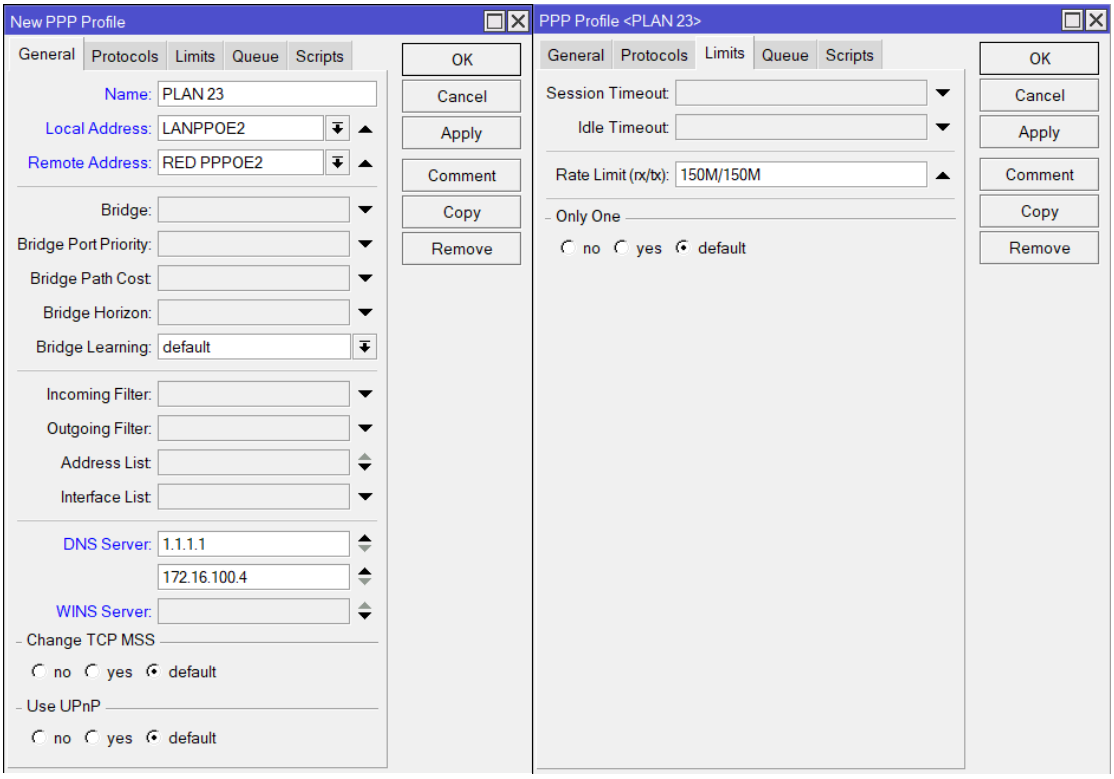
Creación de Perfil Plan 20



Nota. En el perfil denominado "Plan 20", la configuración incluye la dirección local como "LANPPOE2" y la dirección remota como "RED PPPOE2". Los servidores DNS utilizados son 1.1.1.1 y 172.16.100.4. Se ha asignado un límite de velocidad de 100 megabits por segundo tanto en la dirección ascendente como en la descendente. Esta configuración define la experiencia de conectividad para los usuarios que optan por el mencionado plan.

Figura 21

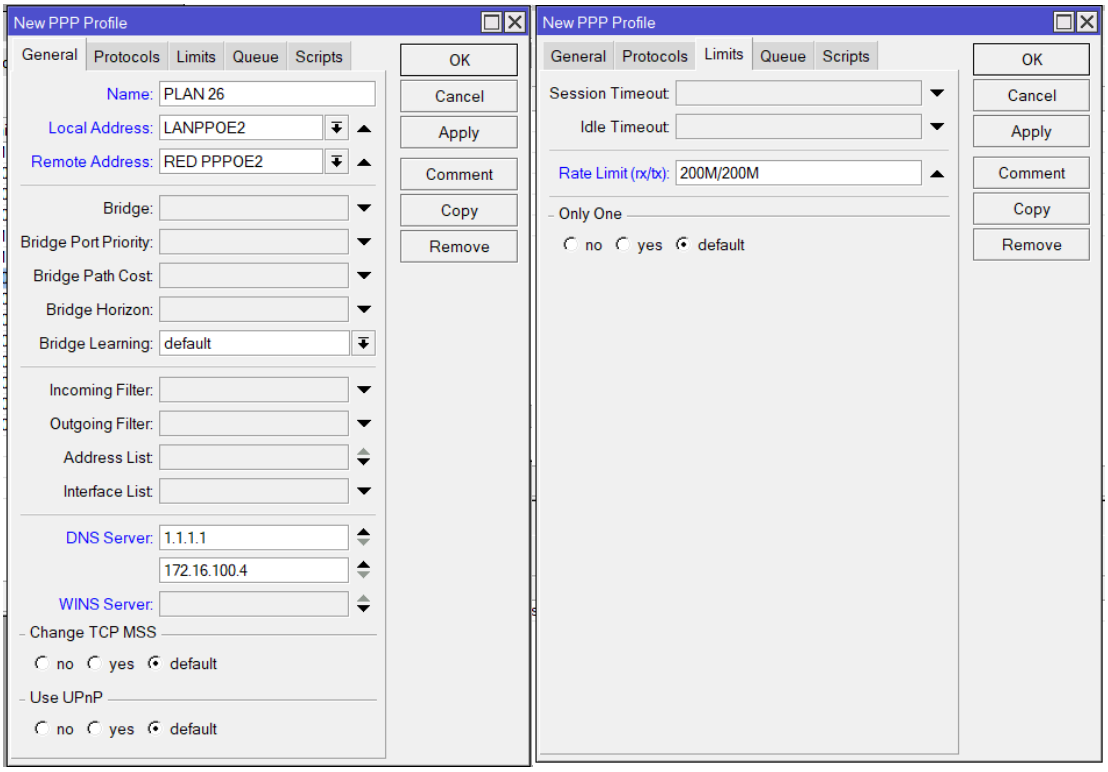
Creación de Perfil Plan 23



Nota. En el perfil denominado "Plan 23", la configuración incluye la dirección local como "LANPPOE2" y la dirección remota como "RED PPPOE2". Los servidores DNS utilizados son 1.1.1.1 y 172.16.100.4. Se ha asignado un límite de velocidad de 150 megabits por segundo tanto en la dirección ascendente como en la descendente. Esta configuración define la experiencia de conectividad para los usuarios que optan por el mencionado plan.

Figura 22

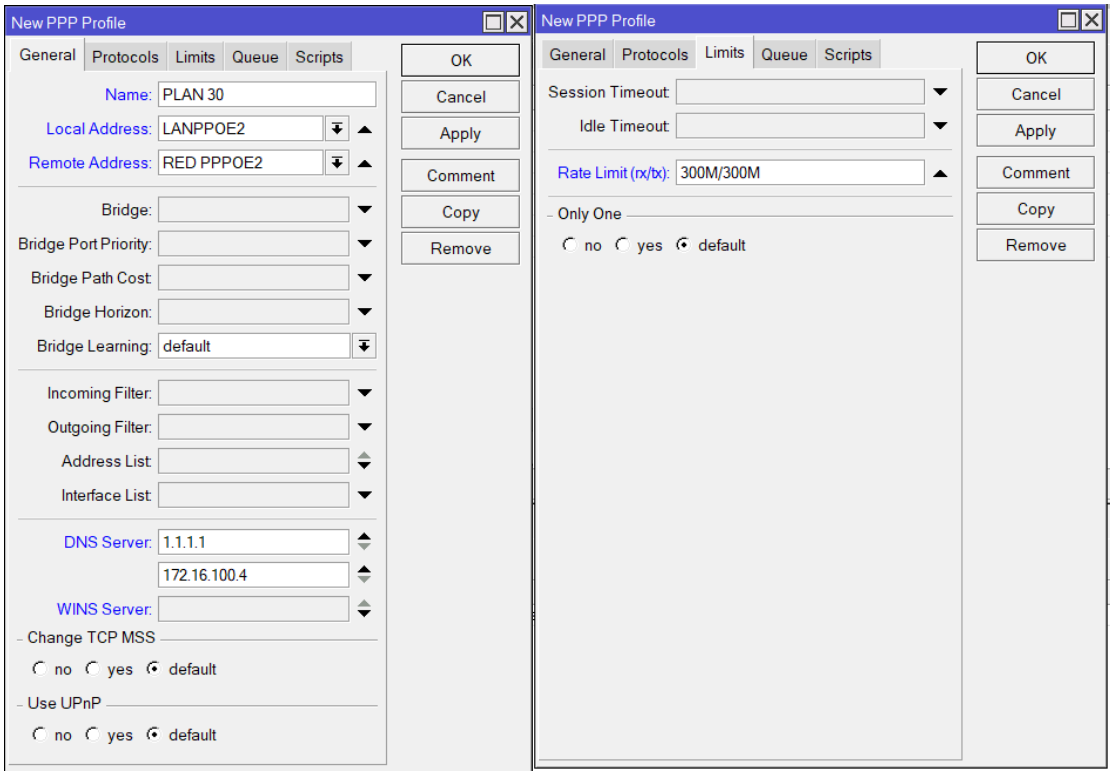
Creación de Perfil Plan 26



Nota. En el perfil denominado "Plan 26", la configuración incluye la dirección local como "LANPPOE2" y la dirección remota como "RED PPPOE2". Los servidores DNS utilizados son 1.1.1.1 y 172.16.100.4. Se ha asignado un límite de velocidad de 200 megabits por segundo tanto en la dirección ascendente como en la descendente. Esta configuración define la experiencia de conectividad para los usuarios que optan por el mencionado plan.

Figura 23

Creación de Perfil Plan 30



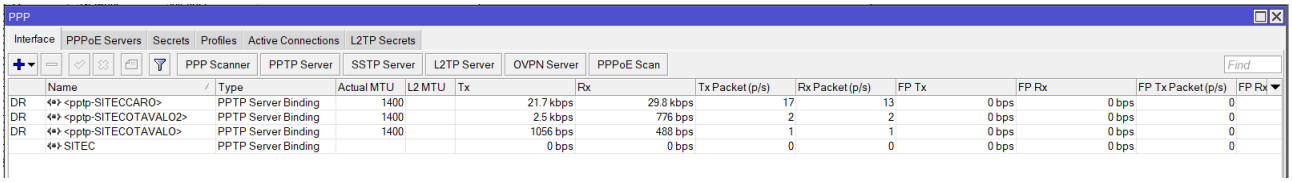
Nota. En el perfil denominado "Plan 30", la configuración incluye la dirección local como "LANPPOE2" y la dirección remota como "RED PPPOE2". Los servidores DNS utilizados son 1.1.1.1 y 172.16.100.4. Se ha asignado un límite de velocidad de 300 megabits por segundo tanto en la dirección ascendente como en la descendente. Esta configuración define la experiencia de conectividad para los usuarios que optan por el mencionado plan.

La fase de implementación de "Usuarios Iniciales por PPTP" implica la creación y configuración de cuentas de usuario destinadas a la autenticación mediante el protocolo PPTP, como se muestra en la Figura 24. En esta etapa, los administradores del sistema asignan credenciales específicas, tales como nombres de usuario y contraseñas, a los usuarios autorizados para acceder de manera remota a través de conexiones PPTP. Paralelamente, se configura el

servidor PPTP para recibir y gestionar estas conexiones, definiendo parámetros de seguridad y la interfaz de red a la que los usuarios tendrán acceso.

Figura 24

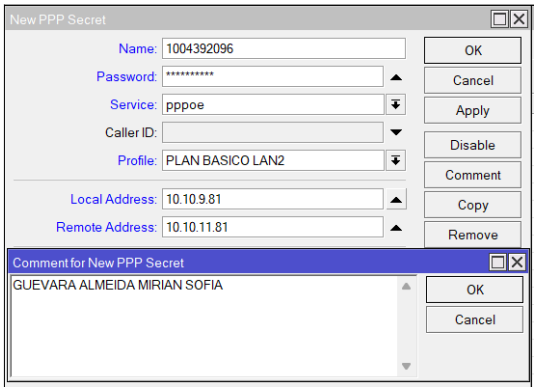
Usuarios Iniciales por PPTP



En el contexto de servicios de conectividad, se lleva a cabo un proceso esencial para la incorporación de nuevos usuarios mediante autenticación PPPoE. Se configuran el nombre de usuario, contraseña, tipo de autenticación, y se asocian con un perfil específico (Plan de Servicio), que define características como límites de ancho de banda. Además, se establecen las direcciones local y remota para la conexión PPPoE, como se muestra en la Figura 25.

Figura 25

Creación de Usuario para PPPoE



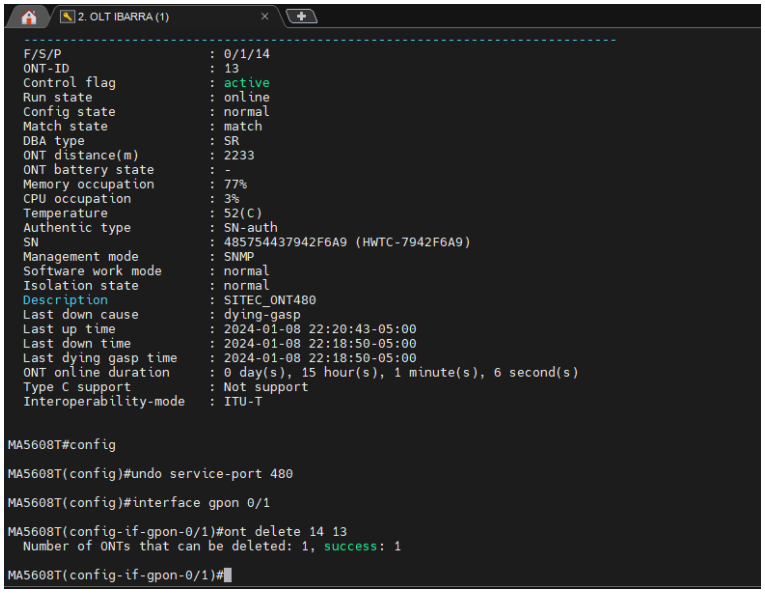
Nota. En la creación del nuevo perfil, se establece el número de cédula como el nombre de usuario, mientras que la contraseña se asigna conforme a los registros almacenados en la base de

datos de clientes. Se configura el servicio como PPPoE y se aplica la autenticación correspondiente. El perfil asociado es el "Plan 17", caracterizado por sus atributos específicos, como límites de ancho de banda y otras configuraciones predefinidas. Las direcciones local y remota se definen como 10.10.9.81 y 10.10.11.81, respectivamente. A modo de comentario adicional, se añade el nombre completo del cliente.

Mediante la aplicación Mobaxterm, se establece una conexión remota con la OLT (Optical Line Terminal). A través de la utilización de comandos en la interfaz de línea de comandos, se procede a la eliminación de la ONT (Optical Network Terminal) previamente configurada en la OLT, como se muestra en la Figura 26. Este proceso de supresión se lleva a cabo con el propósito de realizar una reconfiguración de la ONT, incorporando información actualizada y ajustada a los requerimientos específicos.

Figura 26

Borrado de ONT de la OLT



Nota. En la imagen se puede visualizar detalles de la ONT y los comandos que se utilizan para borrar la ONT de la OLT para realizar la nueva configuración.

Durante esta conexión, se lleva a cabo la adición de la ONT (Optical Network Terminal) del usuario a la VLAN correspondiente mediante el uso de comandos específicos. En primer lugar, se accede a la OLT a través de Mobaxterm, lo que permite la interacción con la interfaz de línea de comandos del dispositivo, tal como se muestra en la Figura 27. Una vez autenticado, se ejecutan comandos para agregar la ONT del usuario a la VLAN deseada.

Figura 27

Agregar ONT a la VLAN 150

Nota. En la representación gráfica proporcionada, se observan los comandos de configuración específicos destinados a la inclusión de la Optical Network Terminal (ONT) en la VLAN 150. Estos comandos son distinguidos por la utilización del número de serie asociado al enrutador y el identificador asignado al cliente, representado por un número específico en la ONT. La ejecución precisa de estos comandos es esencial para establecer la conexión de la ONT dentro del contexto de la VLAN 150.

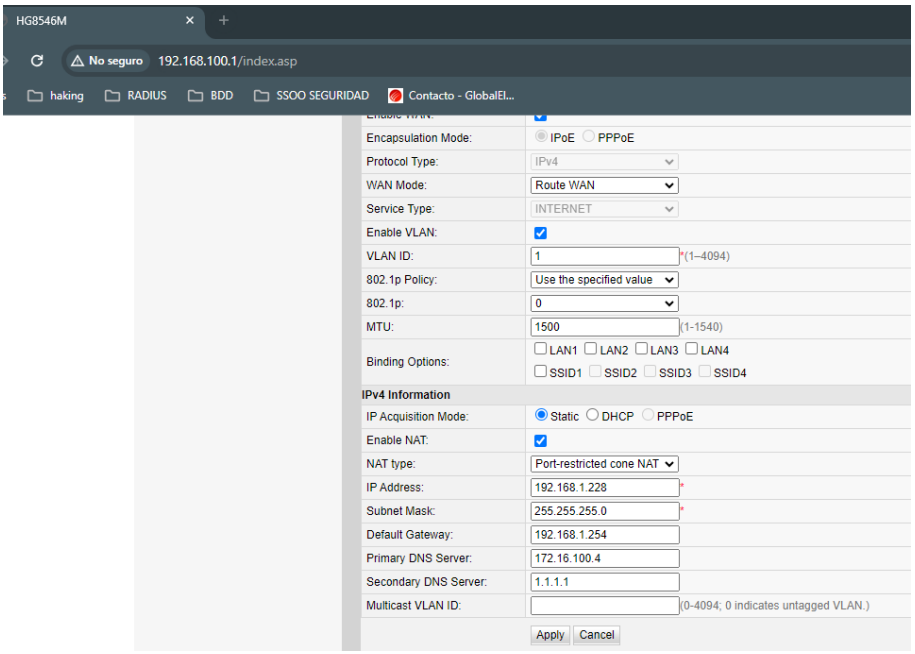
4.1.6 Configuración en la ONU

Dentro de las configuraciones actuales del Router se destaca que el método utilizado para obtener la dirección IP se configura como estático y se le asigna una dirección ip de acuerdo con

el rango anteriormente utilizado, esta información se verifica en la Figura 28. La visualización detallada de la configuración actual del router es esencial para comprender y gestionar la transición hacia un nuevo entorno o configuración, en este caso, la migración en curso.

Figura 28

Configuración Actual en el router

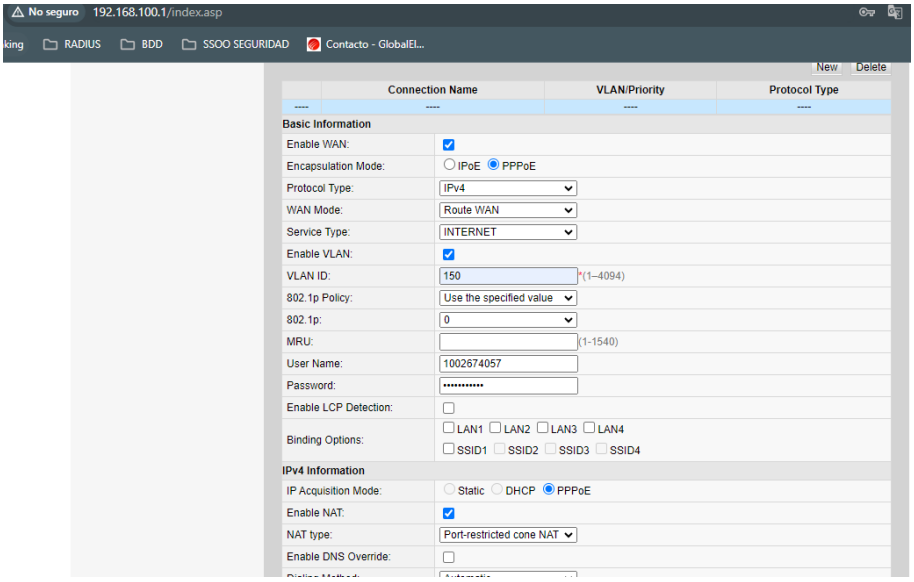


Nota. Se presenta la configuración actual del router perteneciente al usuario destinatario de la migración.

En la configuración actual del dispositivo final, se asigna un juego de credenciales que incluye un usuario y una contraseña específicos. Estas credenciales se utilizan para autenticar al cliente durante el proceso de conexión. El método de autenticación seleccionado es PPPoE, y la obtención de la dirección sigue el mismo protocolo, PPPoE. Con esta configuración, se completa la migración, resaltando la transición desde el método estático anterior hacia el enfoque dinámico encapsulado por PPPoE, como se muestra en la Figura 29.

Figura 29

Creación WAN de dispositivo final

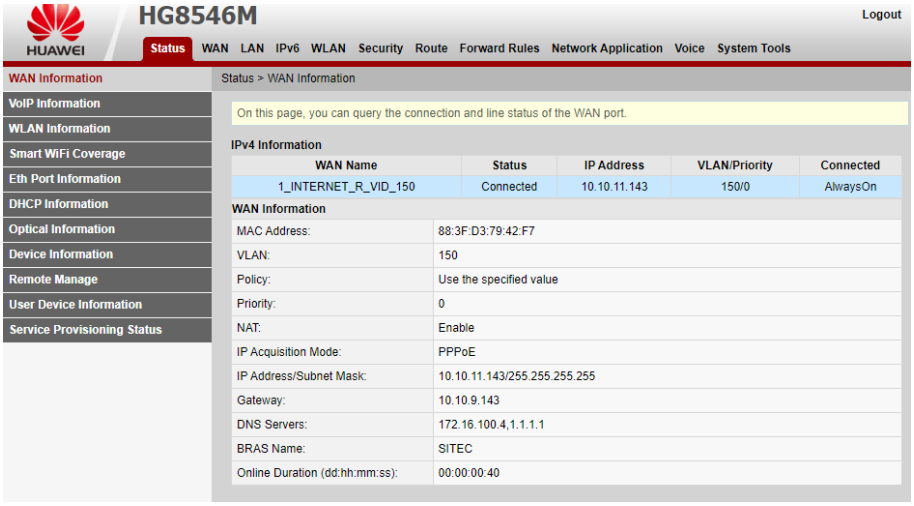


Nota. La imagen revela la configuración final aplicada al router, evidenciando la implementación del modo de encapsulación PPPoE, el cual se utiliza para establecer la conexión a través del Protocolo Punto a Punto sobre Ethernet.

Como paso final se realiza la revisión de las configuraciones realizadas al dispositivo, como en la Figura 30, esta configuración final refleja la culminación de un proceso técnico que asegura la integración exitosa del cliente en la infraestructura de red, específicamente en el contexto de la VLAN 150. La validación de la dirección IP a través del protocolo PPPoE añade un nivel adicional de seguridad y autenticación, garantizando así una conexión estable y eficiente para el cliente.

Figura 30

Estado de WAN y Parámetros de dispositivo final

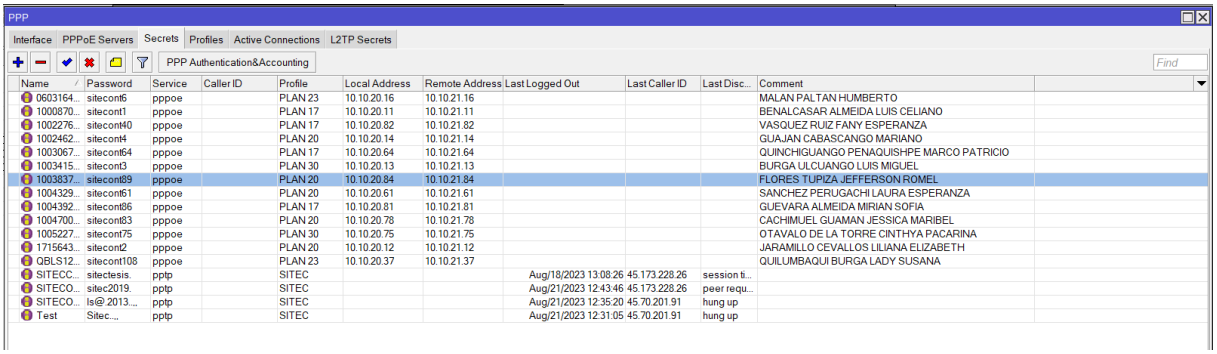


Nota. Se presentan las configuraciones finales del cliente, cuya conexión se encuentra asociada a la VLAN 150. La implementación de este escenario se consolida con la validación de la dirección IP mediante el protocolo PPPoE.

Finalmente, se verifica que el servicio PPPoE ha sido implementado con éxito en MikroTik, y cada cliente se autentica y opera mediante este protocolo, como se muestra en la Figura 31. Cada cliente cuenta con credenciales únicas, asociadas al Plan de Servicio seleccionado, y se le asigna una dirección IP dentro del rango predefinido. Este enfoque garantiza un acceso seguro y personalizado para cada usuario, facilitando la gestión y la entrega eficiente de servicios según las especificaciones del plan contratado.

Figura 31

Servicio PPPoE levantado en Mikrotik



Nota. Se visualiza el funcionamiento tras la configuración y provisión del servicio PPPoE en un enrutador MikroTik, con el propósito de ofrecer a los usuarios una conexión segura y personalizada.

En caso de existir un cliente con varios contratos registrados con un mismo número de cédula se asignará el identificativo después del número de cédula asignado como usuario al nombre de usuario PPPoE, se detalla un ejemplo en la Tabla 5.

Tabla 5

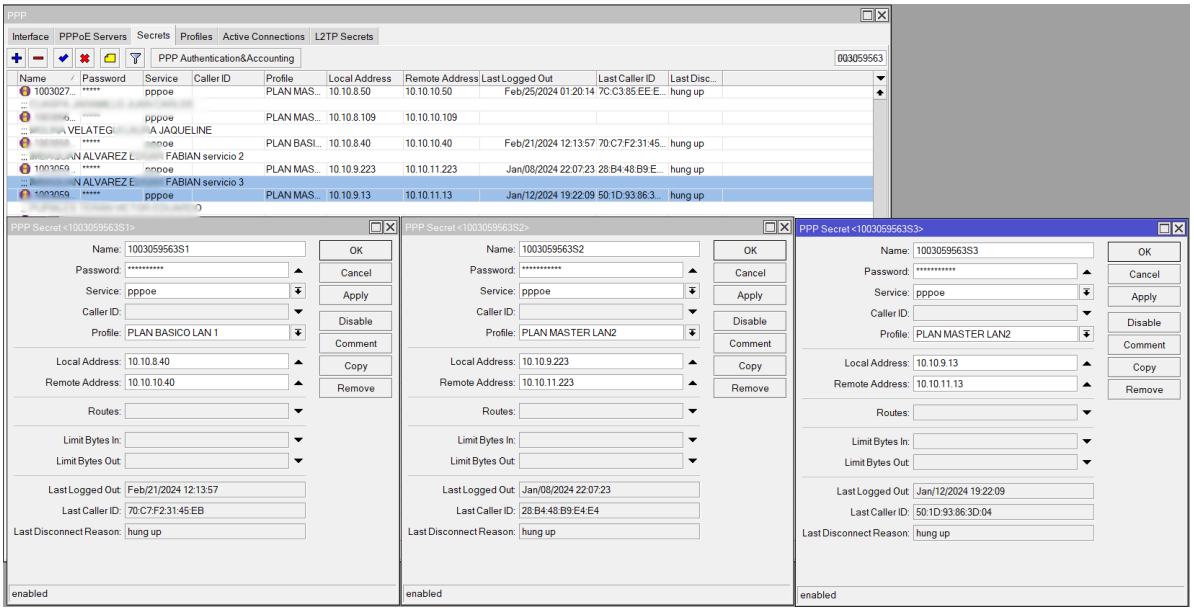
Parámetros de asignación de usuario

N° Servicio	Número de cédula	Formato de Nombre Asignado
S1	1003886163	1003886163
S2	1003886163	1003886163S2
S3	1003886163	1003886163S3

Como se observa en el ejemplo para la asignación del usuario en un cliente con varios contratos se opta por agregar un identificativo al final del número de cédula a partir del segundo contrato, la letra “S” de servicio y el número de servicio. En la Figura 32., se visualiza un cliente el cual se ha realizado esta asignación de usuario añadido el identificativo pues se tiene 3 contratos con el mismo número de cédula.

Figura 32

Usuario con identificativo de número de servicio



Nota. Se visualiza el cliente registrado con el mismo número de cédula 3 veces.

4.1.7 Registro y Control de Actividad de administradores

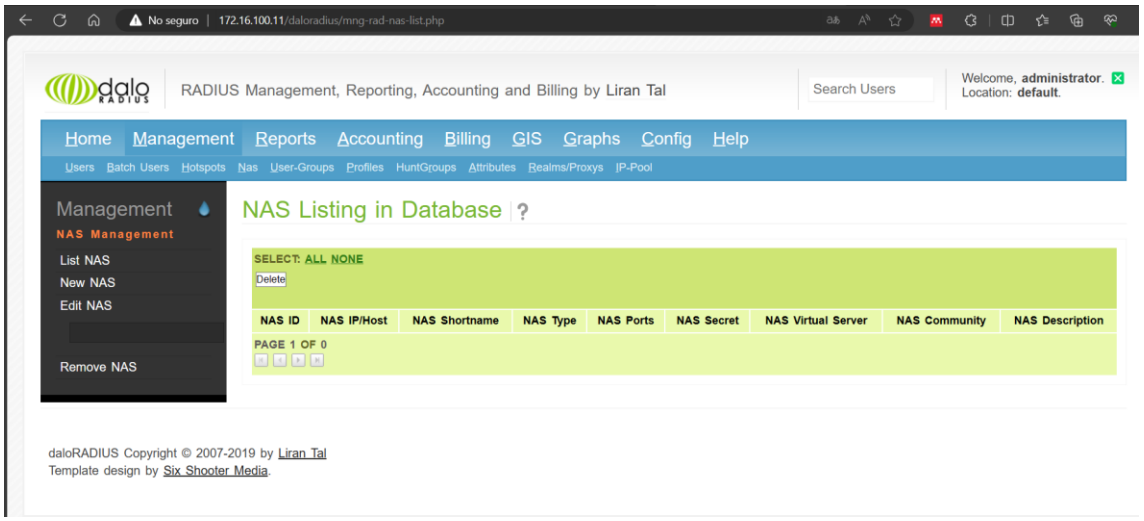
Dentro de la plataforma Daloradius, se lleva a cabo la creación de usuarios administrativos, los cuales serán habilitados con acceso a los equipos y podrán realizar configuraciones de acuerdo con los permisos otorgados. Esta acción se encuadra en la gestión centralizada de usuarios y privilegios, permitiendo establecer roles específicos y responsabilidades dentro del entorno de red. La creación de usuarios administrativos en Daloradius facilita una administración eficaz y segura de los equipos, garantizando que solo personal autorizado tenga acceso a funciones específicas de configuración y gestión.

La primera configuración que se lleva a cabo es la creación de Network Access Servers (NAS), como se muestra en la Figura 33. Esta acción implica la incorporación de servidores y

dispositivos de red a la plataforma, estableciendo una conexión centralizada y unificada con los equipos que forman parte de la infraestructura de red. La creación de NAS es un paso esencial para la gestión efectiva de la red, ya que permite identificar y administrar cada dispositivo que forma parte del entorno, facilitando así la aplicación de políticas, control de accesos y supervisión integral desde la plataforma Daloradius.

Figura 33

Creación de NAS



Nota. Para la creación de la NAS únicamente se ingresa en New NAS.

Se establece la dirección del Network Access Server (NAS), se definen las credenciales correspondientes y se asigna un nombre al equipo al cual se va a anclar, tal como se muestra en la Figura 34. Este conjunto de acciones permite una integración precisa del NAS con la plataforma Daloradius, asegurando una identificación clara y segura del servidor o dispositivo de red.

Figura 34

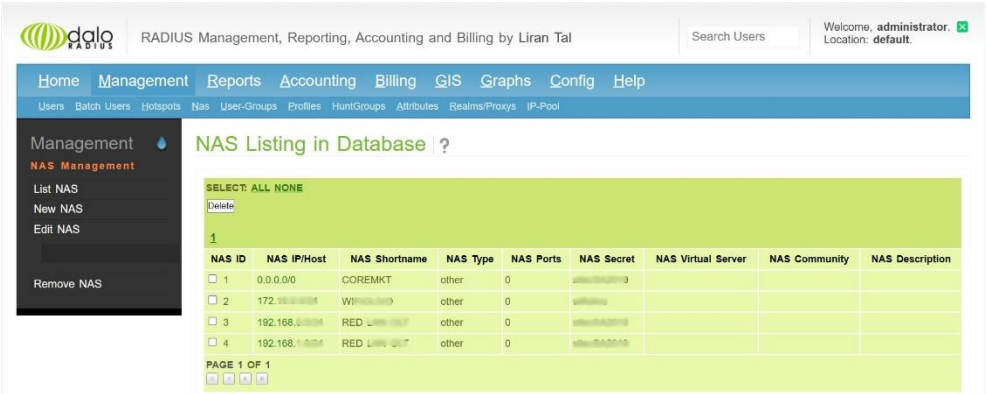
Configuración de NAS

Nota. En la imagen se visualiza los parámetros que se configuran dentro del Daloradius para las NAS creada.

En la opción List NAS se puede visualizar todas las NAS que han sido creadas dentro de la base de datos, como se visualiza en la Figura 35.

Figura 35

Lista de NAS

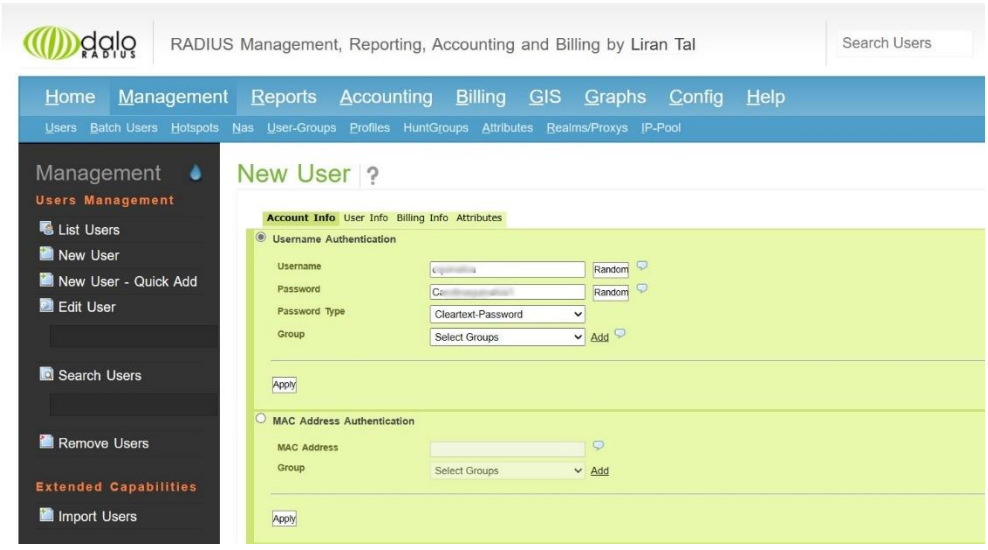


Nota. En la imagen se muestra la NAS creada, en este caso, hay únicamente la NAS con el nombre COREMKT.

Tras la creación exitosa de la Network Access Server (NAS), se procede a la creación del usuario administrativo en Daloradius, como se evidencia en la Figura 36. A este usuario se le asignan credenciales de autenticación, como nombre de usuario y contraseña, además de ser integrado a un grupo específico de Radius al que pertenecerá. El formato de asignación de nombres de usuario se establece con la Inicial del primer nombre y el Apellido, en caso de que existan persona con la misma inicial de nombre y el mismo apellido se tomará la segunda letra del nombre. Para la asignación de la contraseña se ha establecido un formato de consta de 2 credenciales propias del usuario, un número y un caracter especial. Esta acción configura un perfil de acceso para el usuario administrativo, estableciendo así los parámetros necesarios para su autenticación y determinando su afiliación a un grupo de Radius particular.

Figura 36

Creación De Usuario

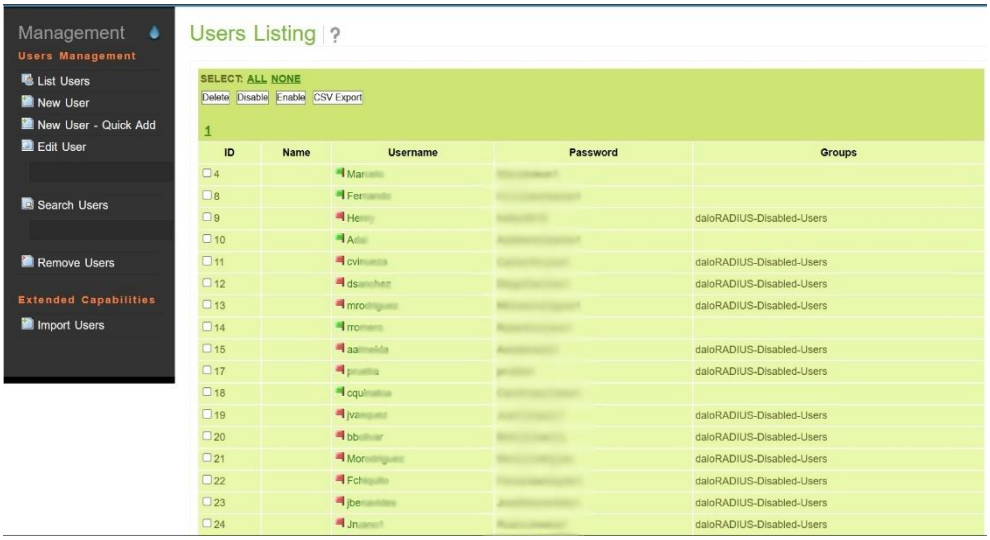


Nota. El nuevo usuario tendrá como un nombre y se le asignará una contraseña que serán las credenciales con las cuales va a acceder al equipo.

Para verificar el usuario creado, se ingresa en la opción List Users, como se evidencia en la Figura 37, esta opción muestra la lista de los usuarios que han sido configurados dentro de esta base de datos. Estos usuarios pertenecen a la lista de administradores.

Figura 37

Usuarios Creados



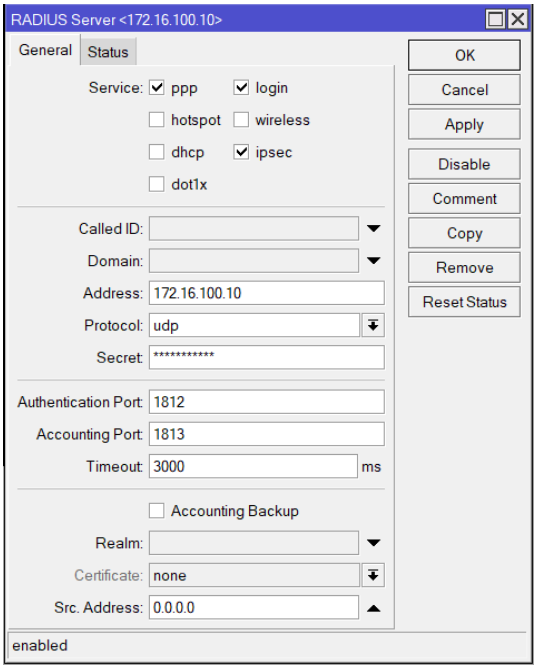
Nota. Se evidencia a los usuarios creados y se verifica que los que se encuentran habilitados poseen bandera verde.

La conexión entre el Core y el servidor Radius se lleva a cabo en Mikrotik mediante la configuración de un nuevo servidor Radius. En la opción "New Radius Server", se establecen los parámetros necesarios para facilitar la conexión efectiva entre ambos componentes, como se muestra en la Figura 38. Estos parámetros incluyen información clave como la dirección IP del

servidor Radius, el puerto de conexión, así como las credenciales necesarias para autenticar la conexión. Esta configuración permite una comunicación segura y eficiente entre el Core y el servidor Radius, asegurando que la autenticación y la autorización de los usuarios se realicen de manera efectiva a través del servidor Radius centralizado.

Figura 38

Conexión entre Core y Radius



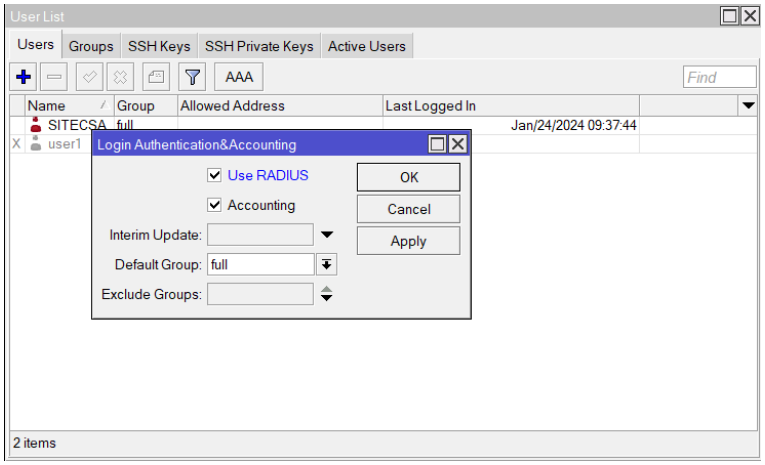
Nota. Para esta verificación se realiza la selección de varios servicios como PPP, Login, Ipsec, la dirección ip en este caso es 172.16.100.10, a través de protocolo UDP y la contraseña de acceso.

Para verificar la implementación del Protocolo AAA (Autenticación, Autorización y Contabilidad), se procede a habilitar el ingreso por AAA en la configuración. Esta acción asegura que el sistema esté configurado para utilizar el Protocolo AAA para la autenticación de usuarios, la autorización de accesos y la contabilidad de actividades. Al habilitar el ingreso por

AAA, se confirma que el sistema seguirá los principios del Protocolo AAA para gestionar de manera integral la seguridad y la administración de accesos en la red, tal como la Figura 39.

Figura 39

Activación Protocolo AAA



Nota. Se visualiza la configuración del Protocolo AAA en la lista de usuarios

4.2 Pruebas de Funcionamiento de la Arquitectura

En este apartado de la tesis, se llevan a cabo las pruebas de rendimiento de la arquitectura implementada, la verificación de su cumplimiento se visualiza en el Anexo D. Estas pruebas se dividen en dos secciones fundamentales: las pruebas básicas, que se centran en la verificación del correcto funcionamiento de los servidores, y las pruebas específicas, que ofrecen un análisis detallado del proceso de configuración de la autenticación PPPoE basada en el protocolo AAA. Estas evaluaciones exhaustivas buscan garantizar tanto la estabilidad general del sistema como la eficacia y precisión en la implementación de las funciones de autenticación y autorización, en la Tabla 4., se detalla la lista de pruebas a realizarse.

Tabla 6

Pruebas Realizadas

Tipo de Prueba	Descripción	Resultado
Pruebas básicas	Diseño de proceso y arquitectura del proyecto	Se verifica que se ha realizado el diseño paso a paso de la implementación del proyecto y la arquitectura que se maneja en este.
	Funcionamiento Radius	A través de comandos se verifica que el servidor Radius se encuentre activo.
	Funcionamiento Servicio web	A través de comandos se verifica que el Servicio Web se encuentre activo.
	Funcionamiento Firewall	A través de comandos se verifica que el firewall se encuentre activo.
	Verificación Base de Datos	A través de comandos se verifica que la base de datos haya sido creada.
	Verificación de usuarios en base de datos	A través de comandos se verifica que los usuarios se encuentren registrados en la base de datos.
Pruebas Específicas	Digitalización de Contratos y Creación de Base de datos	Se verifica que los contratos fueron digitalizados y la base de datos en Excel fue creada y se registra los clientes en esta.
	Levantamiento de servidor Radius	Se verifica el proceso de levantamiento del servidor Radius para clientes en el MikroTik
	Creación de usuario PPPoE	Se verifica la creación de un nuevo usuario que se autentica por PPPoE
	Configuración nuevo usuario en OLT	Se verifica la configuración del dispositivo final del usuario dentro de la OLT
	Configuración PPPoE en Dispositivo Final	Se verifica las configuraciones realizadas dentro del dispositivo final para que la autenticación se realice por PPPoE
	Verificación de autenticación de Usuario a la red por PPPoE	Se verifica que el usuario se encuentre activo dentro de la red a través de Winbox
	Configuración Daloradius	Se verifica la configuración del DaloRadius para los usuarios administrativos
	Creación de Usuario Administrador	Se verifica la creación de un nuevo usuario con permisos de administración

	Conexión Daloradius con Winbox	Se verifica la conexión entre el servidor de administración y servidor de clientes, a través del DaloRadius y el Winbox
	Verificación de autenticación de Administrador por PPPoE	Se verifica que el usuario administrador tiene acceso por PPPoE al Mikrotik a través de Winbox.

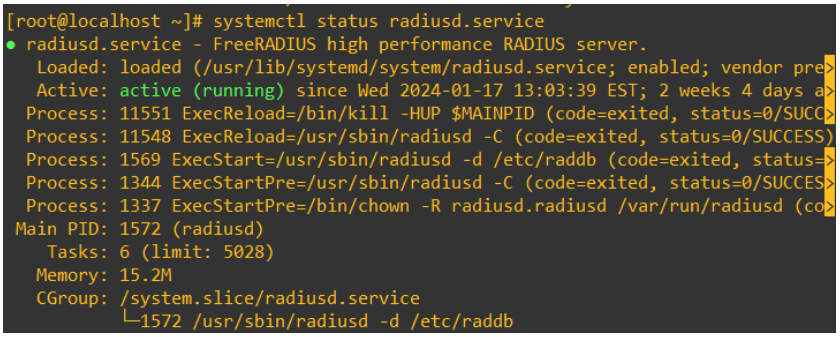
4.2.1 Pruebas Básicas

En esta sección, se presenta una exhaustiva documentación de las pruebas básicas llevadas a cabo para evaluar la robustez y eficiencia de la implementación. Se aborda detalladamente el funcionamiento del servidor Radius, analizando su capacidad para gestionar las solicitudes de autenticación de manera efectiva. Además, se examina el servicio web asociado, evaluando su accesibilidad y rendimiento. Se profundiza en la base de datos creada específicamente para el almacenamiento de datos relevantes, verificando su integridad y capacidad para gestionar la información de manera eficaz. Asimismo, se documenta el proceso de autenticación del usuario administrador mediante comandos, destacando la seguridad y eficacia de este procedimiento.

En esta fase de la investigación, se lleva a cabo la exhaustiva verificación del rendimiento y funcionalidad del servidor Radius implementado en el sistema operativo Debian 11, como se muestra en la Figura 40.

Figura 40

Funcionamiento Radius

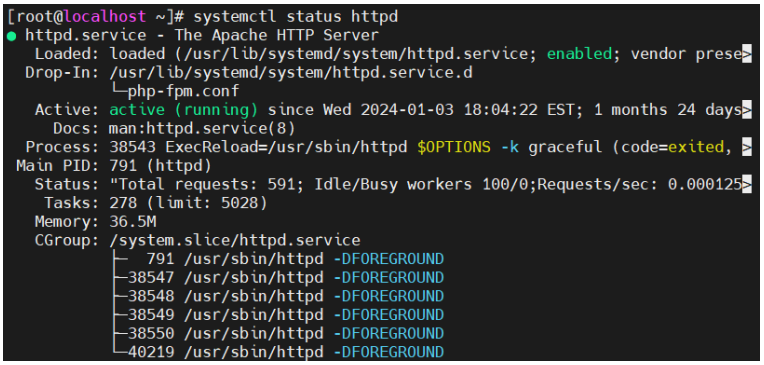


Nota. En la imagen se muestra la evaluación que se realiza meticulosamente mediante la consola del sistema, permitiendo una supervisión detallada de cada aspecto operativo del servidor.

En esta etapa del proceso, se procede a la verificación exhaustiva del servicio web, como se muestra en la Figura 41., fundamental para la operatividad de Daloradius dentro del sistema. La evaluación se lleva a cabo meticulosamente para asegurar la correcta disponibilidad y funcionamiento del servicio que respalda la interfaz web de Daloradius. Se exploran aspectos cruciales, como la accesibilidad, la capacidad de respuesta y la integración efectiva con la base de datos, asegurando así que Daloradius pueda desplegarse y operar de manera óptima.

Figura 41

Funcionamiento Servicio web

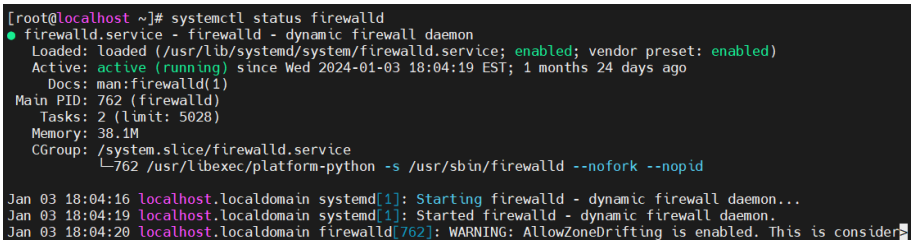


Nota. En la imagen se verifica el funcionamiento y se asegura la correcta disponibilidad y funcionamiento del servicio web.

Durante esta fase del proceso, se realiza una exhaustiva verificación del estado operativo del servicio de firewall en el sistema, como se muestra en la Figura 42. Se asegura de manera minuciosa que el firewall esté activo y funcionando correctamente, desempeñando su papel crucial en la protección y seguridad de la red.

Figura 42

Funcionamiento Firewall

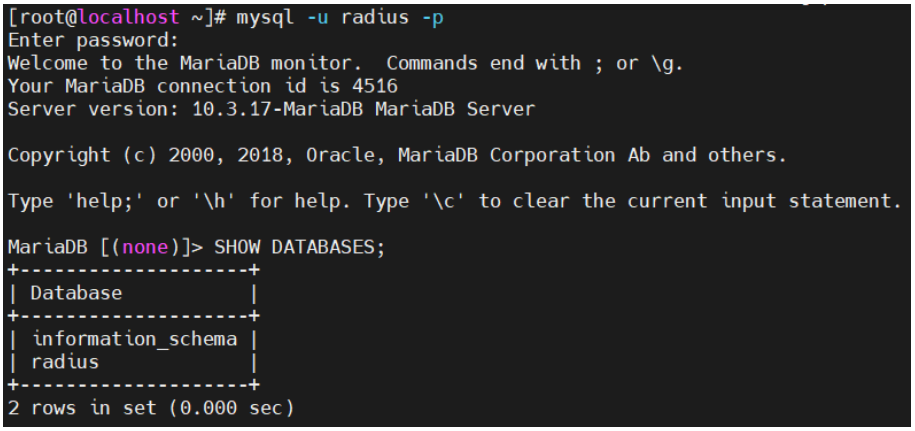


Nota. En la imagen se puede verificar que el servicio de firewall se encuentra habilitado y funcionando.

En esta etapa esencial del proceso, se procede a la meticulosa verificación de la creación de la base de datos destinada a almacenar la información vital de los usuarios generados mediante Daloradius, como se evidencia en la Figura 43. La validación de esta base de datos constituye un paso crítico para asegurar que Daloradius pueda interactuar de manera efectiva con la infraestructura de almacenamiento, proporcionando una sólida base para la gestión y autenticación de usuarios.

Figura 43

Verificación Base de Datos

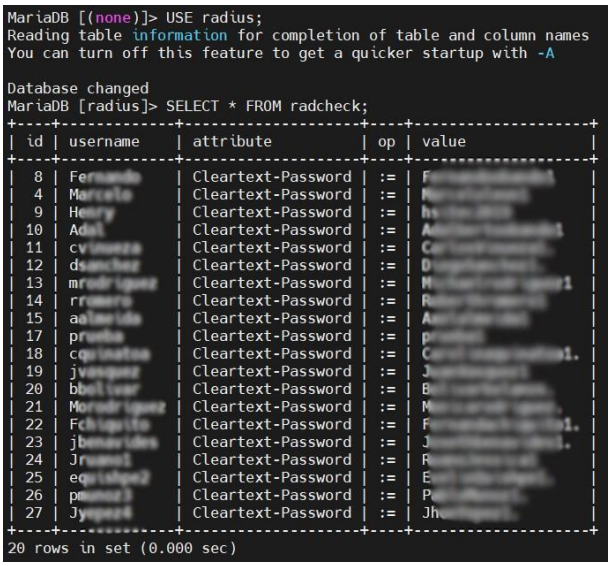


Nota. En la imagen se puede verificar que la base de datos que almacena los usuarios de administración se encuentra creada.

En este punto crucial del proceso de verificación, se lleva a cabo la meticulosa revisión de la presencia y correcta incorporación de usuarios dentro de la base de datos, como se muestra en la Figura 44. Utilizando comandos específicos, se verifica la integridad de la información almacenada, asegurando que cada usuario creado a través de Daloradius sea correctamente registrado en la base de datos. Este paso es esencial para garantizar la coherencia entre la interfaz de gestión, Daloradius, y la base de datos subyacente, estableciendo una conexión fluida y confiable entre ambas entidades. La verificación exhaustiva de los usuarios en la base de datos consolida la solidez del sistema implementado y sienta las bases para un funcionamiento óptimo en la gestión de accesos y autenticación.

Figura 44

Verificación de usuarios en base de datos



Nota. En la imagen se muestra los usuarios que se encuentran dentro de la base de datos de Daloradius.

4.2.2 Pruebas Específicas

En esta sección de pruebas específicas, se aborda detalladamente la situación actual de autenticación de los usuarios en la red de la empresa SITEC, focalizándose en aspectos cruciales como la interrupción del servicio debido a falta de pago por parte de los usuarios. La autenticación mediante el protocolo PPPoE es sometida a rigurosas pruebas para evaluar su eficacia y robustez. Se lleva a cabo una evaluación exhaustiva del funcionamiento de la autenticación, junto con la implementación de medidas de bloqueo para contrarrestar posibles ataques por parte de los usuarios, asegurando así la integridad y seguridad del sistema. Este

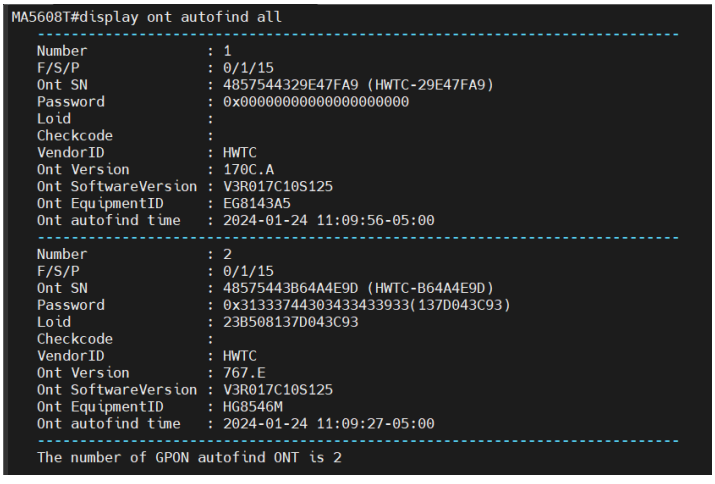
capítulo se enfoca en demostrar la eficiencia y confiabilidad de las soluciones implementadas en el marco de la arquitectura AAA y el protocolo PPPoE con equipos MikroTik.

Situación Actual de autenticación del usuario en la red. Las configuraciones presentadas a continuación permiten evidenciar el proceso de reconocimiento de un usuario en la red. Cada parámetro refleja la implementación de medidas de seguridad y procedimientos de identificación que son fundamentales en el establecimiento de una conexión.

La conexión a la Optical Line Terminal (OLT) se lleva a cabo de manera eficiente mediante el protocolo Secure Shell (SSH), facilitando la ejecución de configuraciones específicas en las Optical Network Terminals (ONT). Este procedimiento es esencial en la gestión y administración de redes de fibra óptica, permitiendo un acceso remoto seguro a la infraestructura central. La elección del protocolo SSH garantiza la protección integral de la transmisión de datos, asegurando la confidencialidad y la integridad de la información durante el proceso de configuración. Todas las configuraciones por realizarse se llevan a cabo a través de comandos como se puede visualizar en la Figura 45.

Figura 45

Reconocimiento de ONT cercanas

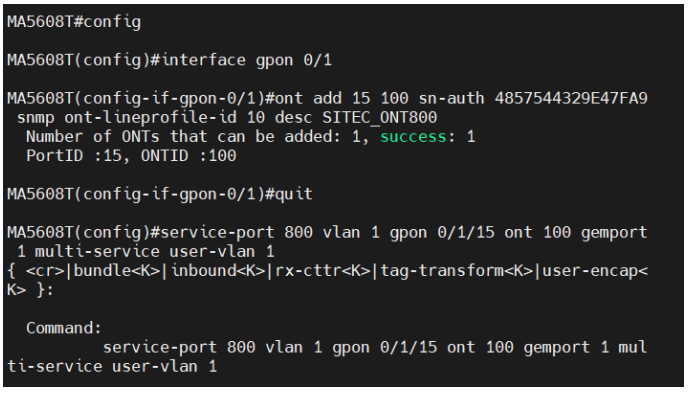


Nota. En la imagen se puede visualizar el comando que permite detectar de forma automática las ONT cercanas y la información básica de estas.

La incorporación de una Optical Network Terminal (ONT) en la Optical Line Terminal (OLT) se lleva a cabo mediante la ejecución de comandos específicos, que se muestran en la Figura 46. Este proceso se inicia al acceder a la interfaz GPON, donde se asignan valores identificativos cruciales, tales como el puerto de conexión, la interfaz correspondiente, el número de serie único de la ONT, su identificación (ID) y un nombre distintivo que facilita su reconocimiento en la red. Posteriormente, se implementan comandos adicionales destinados a la inclusión del dispositivo en una VLAN específica. Estos comandos adicionales aseguran la correcta segmentación y asignación de recursos dentro de la red, contribuyendo así a una administración eficiente y organizada. Este enfoque basado en líneas de comandos destaca la importancia de una configuración precisa y detallada para garantizar la integración exitosa de la ONT en la OLT, elemento fundamental en el despliegue y gestión de redes de fibra óptica.

Figura 46

Configuración de la ONT dentro de la OLT



Nota. En la imagen se visualiza la configuración para esa ONT que habilita la interfaz de conexión 15, se asigna un ID 100 y el puerto de conexión será el 800.

Tras la exitosa incorporación de la Optical Network Terminal (ONT), se procede con la configuración del dispositivo final. Para ello, se accede a dicho dispositivo a través de una dirección IP predeterminada, se verifica la página principal en la Figura 47. Durante este proceso, se lleva a cabo la autenticación a través de un nombre de usuario y la contraseña de acceso correspondientes.

Figura 47

Ingreso de usuario y contraseña

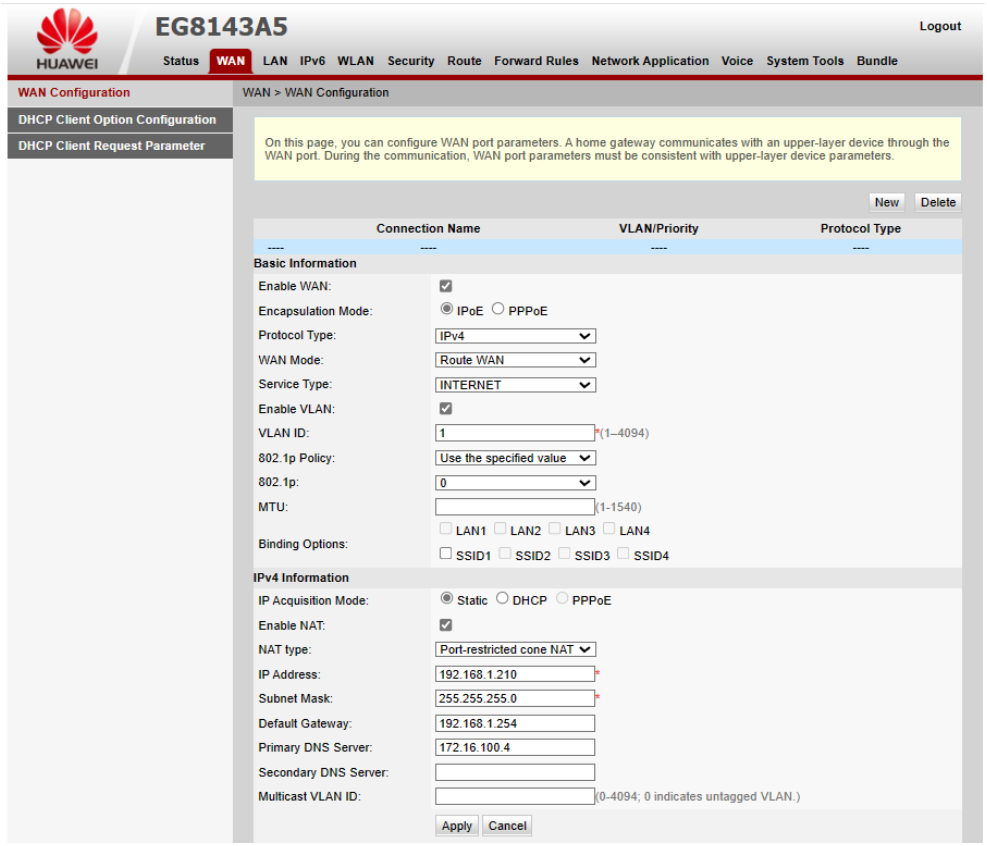
Nota. En la imagen se visualiza la página principal de ingreso hacia el dispositivo, al cual se accede a través de la dirección ip 192.168.100.1.

En el dispositivo final, la primera configuración que se lleva a cabo es la Wide Area Network (WAN). En esta sección, se establecen parámetros fundamentales para la conectividad, tales como la encapsulación, asignación de VLAN, modo de obtención de la dirección IP, dirección IP del dispositivo, máscara de subred, gateway predeterminado y servidores DNS, mismas que se pueden visualizar en la Figura 48. La encapsulación define cómo se envían los

datos a través de la red, la VLAN facilita la segmentación lógica, mientras que el modo de obtención de IP puede ser configurado para asignar direcciones de forma dinámica o estática. La asignación de una dirección IP, máscara y gateway son esenciales para la identificación y enrutamiento eficiente del dispositivo en la red. Además, se especifican los servidores DNS, fundamentales para la resolución de nombres de dominio. Esta configuración integral de la WAN establece las bases para la conectividad del dispositivo final en la red, asegurando una comunicación eficaz y segura.

Figura 48

Configuración WAN

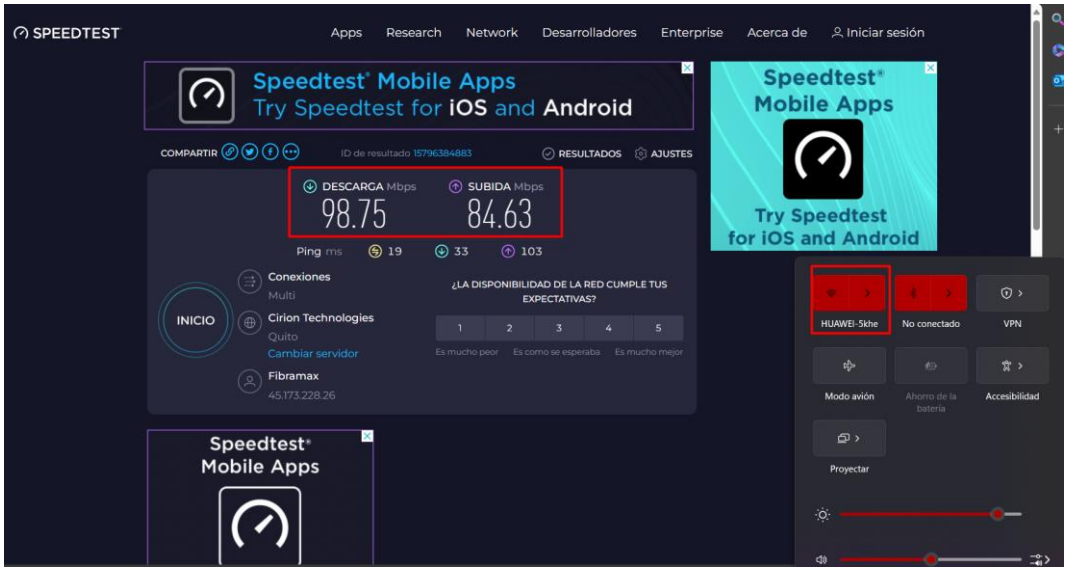


Nota. En la imagen anterior se puede visualizar que el modo de encapsulación es por IPoE, la dirección IP del cliente, en este caso 192.168.1.210, la máscara de subred 255.255.255.0, el Gateway por defecto 192.168.1.254 y el servidor DNS primario 172.16.100.4.

Como parte del proceso de verificación del servicio y la velocidad contratada, se lleva a cabo un test de velocidad, como se observa en la Figura 49. Este procedimiento implica la medición de la velocidad de conexión de la red para asegurar que coincide con la velocidad especificada en el contrato del servicio. Durante el test, se evalúa la velocidad de descarga y carga, proporcionando una evaluación precisa del rendimiento de la conexión. Este paso es esencial para garantizar que el usuario final reciba la calidad de servicio esperada y para identificar posibles problemas en la red que puedan afectar la velocidad.

Figura 49

Test de Velocidad



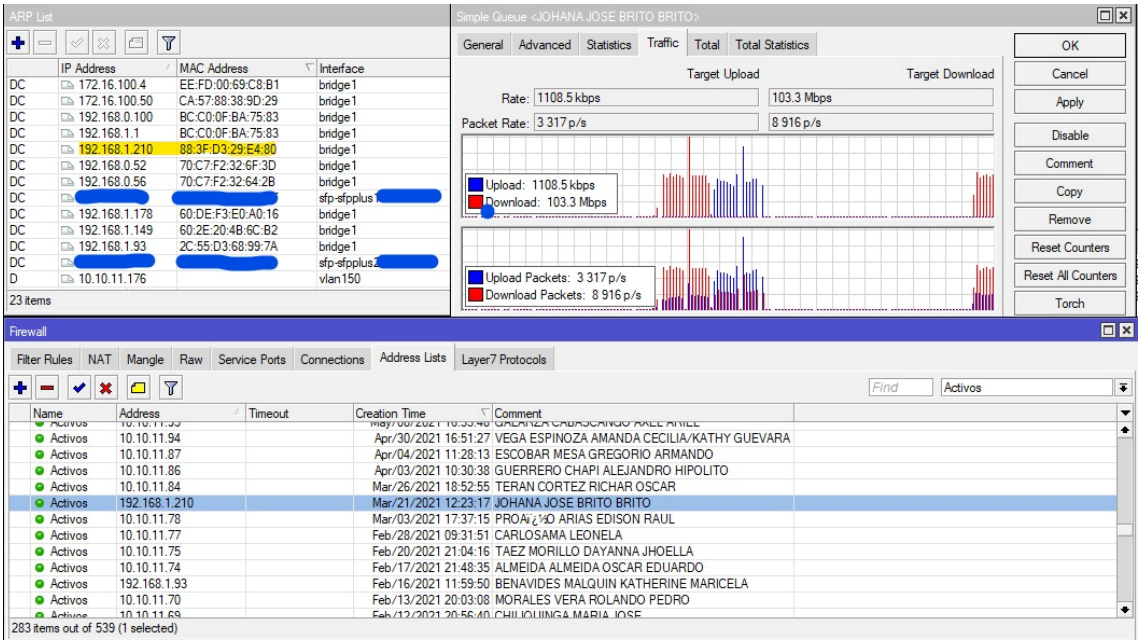
Nota. En la imagen se puede comprobar que el cliente posee el servicio de internet habilitado y saber la velocidad de descarga y subida con la que está trabajando.

A través de la interfaz de Winbox, se analizan detalladamente los datos recopilados durante el test, incluyendo las velocidades de descarga y carga, latencia y otros parámetros significativos, como se muestra en la Figura 50. La visualización de estos resultados permite una

evaluación directa de la calidad y rendimiento de la conexión a Internet del usuario. Este enfoque de monitoreo en Winbox constituye un método efectivo para validar y respaldar la funcionalidad activa del servicio de Internet para el usuario final.

Figura 50

Monitoreo en Winbox



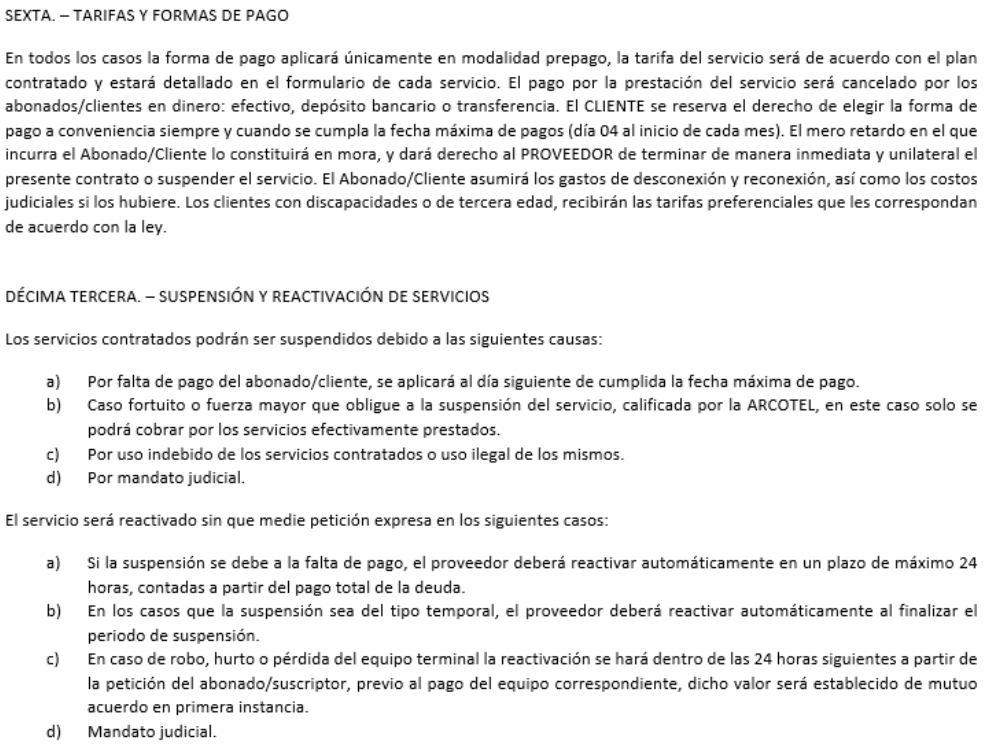
Nota. Se puede visualizar al cliente activo en la lista del Firewall, en la lista de ARP se observa la dirección IP y la dirección MAC del cliente y la ventana donde se analiza el test de velocidad realizado anteriormente.

Corte del servicio al usuario por falta de pago. La falta de pago por parte de los clientes se presenta como uno de los motivos fundamentales que conduce a la ejecución de un corte de servicio de Internet, el contrato completo se puede visualizar en el Anexo C. En esta instancia, se

procede a suspender de manera temporal el acceso del usuario al servicio, como medida disciplinaria y en cumplimiento de los términos del contrato, como se especifica en la Figura 51.

Figura 51

Cláusulas del contrato



SEXTA. – TARIFAS Y FORMAS DE PAGO

En todos los casos la forma de pago aplicará únicamente en modalidad prepago, la tarifa del servicio será de acuerdo con el plan contratado y estará detallado en el formulario de cada servicio. El pago por la prestación del servicio será cancelado por los abonados/clientes en dinero: efectivo, depósito bancario o transferencia. El CLIENTE se reserva el derecho de elegir la forma de pago a conveniencia siempre y cuando se cumpla la fecha máxima de pagos (día 04 al inicio de cada mes). El mero retardo en el que incurra el Abonado/Cliente lo constituirá en mora, y dará derecho al PROVEEDOR de terminar de manera inmediata y unilateral el presente contrato o suspender el servicio. El Abonado/Cliente asumirá los gastos de desconexión y reconexión, así como los costos judiciales si los hubiere. Los clientes con discapacidades o de tercera edad, recibirán las tarifas preferenciales que les correspondan de acuerdo con la ley.

DÉCIMA TERCERA. – SUSPENSIÓN Y REACTIVACIÓN DE SERVICIOS

Los servicios contratados podrán ser suspendidos debido a las siguientes causas:

a) Por falta de pago del abonado/cliente, se aplicará al día siguiente de cumplida la fecha máxima de pago.
b) Caso fortuito o fuerza mayor que obligue a la suspensión del servicio, calificada por la ARCOTEL, en este caso solo se podrá cobrar por los servicios efectivamente prestados.
c) Por uso indebido de los servicios contratados o uso ilegal de los mismos.
d) Por mandato judicial.

El servicio será reactivado sin que medie petición expresa en los siguientes casos:

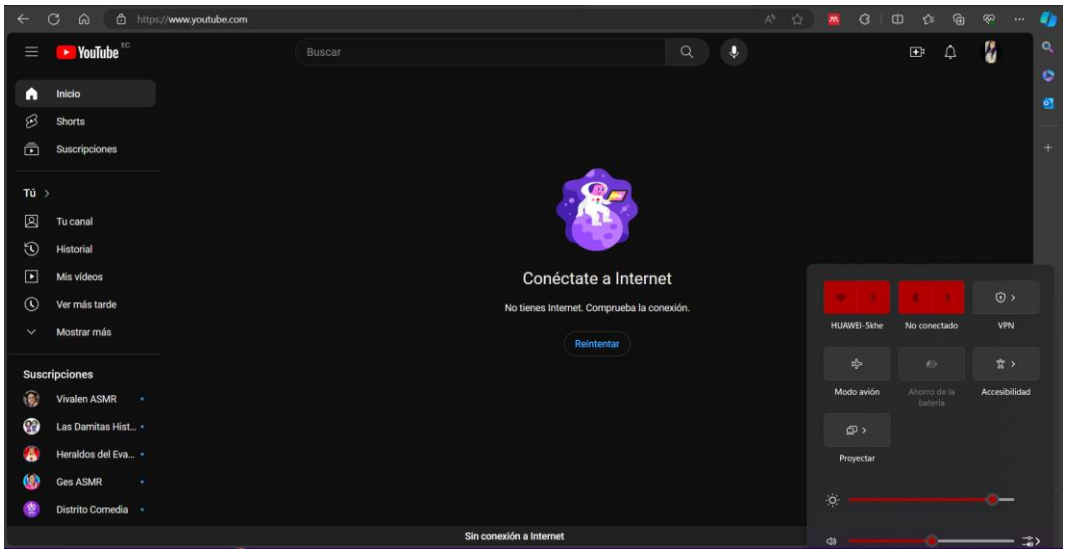
a) Si la suspensión se debe a la falta de pago, el proveedor deberá reactivar automáticamente en un plazo de máximo 24 horas, contadas a partir del pago total de la deuda.
b) En los casos que la suspensión sea del tipo temporal, el proveedor deberá reactivar automáticamente al finalizar el periodo de suspensión.
c) En caso de robo, hurto o pérdida del equipo terminal la reactivación se hará dentro de las 24 horas siguientes a partir de la petición del abonado/suscriptor, previo al pago del equipo correspondiente, dicho valor será establecido de mutuo acuerdo en primera instancia.
d) Mandato judicial.

Nota. En la imagen se detallan las cláusulas que especifican y justifican el corte del servicio por incumplimiento en el pago.

Se realiza una verificación adicional para confirmar que el usuario efectivamente ha perdido el acceso, como se muestra en la Figura 52.

Figura 52

Usuario sin acceso a Internet

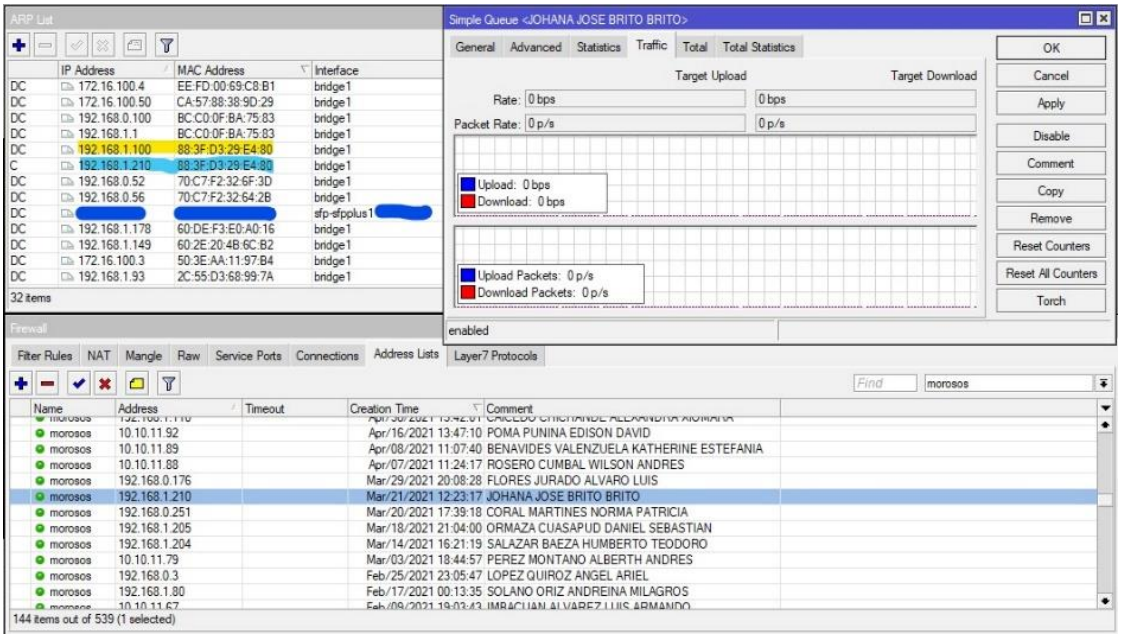


Nota. En la imagen se muestra que el corte de servicio se hizo efectivo, el usuario no tiene acceso a las páginas que funcionan con internet.

La observación revela que el cliente en cuestión no está generando tráfico en la red, como se muestra en la Figura 53, debido a su inclusión en la lista de usuarios a los cuales se les ha suspendido el servicio por falta de pago. Esta medida restrictiva, implementada como consecuencia del incumplimiento en los pagos correspondientes, ha resultado en la inactividad de la conexión del cliente. La suspensión del servicio por motivos financieros se refleja claramente en la ausencia de actividad de red por parte de dicho usuario.

Figura 53

Usuario en Lista de Suspensión del servicio



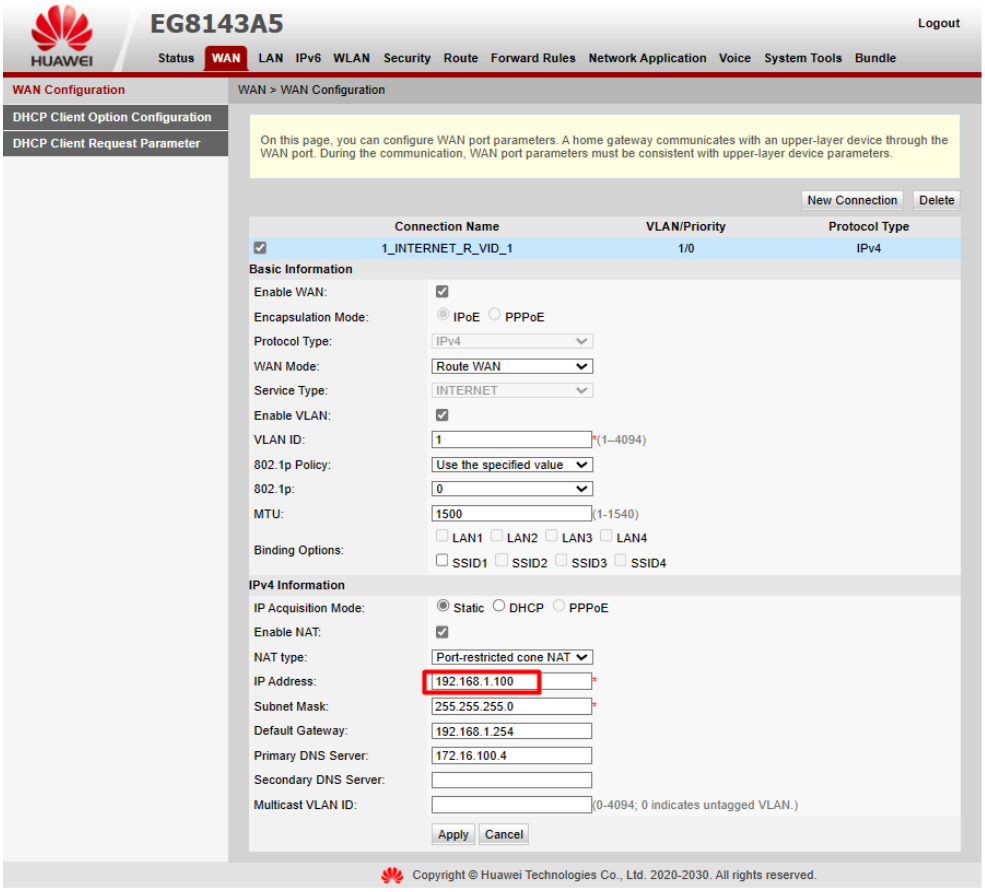
Nota. En la imagen se puede visualizar al usuario dentro de la lista de morosos, por lo cual el servicio de internet se encuentra suspendido.

El anclaje de la dirección MAC a una dirección IP es una medida de seguridad comúnmente utilizada para controlar el acceso a la red. Sin embargo, es importante reconocer que, aunque esta práctica puede proporcionar cierto nivel de seguridad, no garantiza una protección absoluta en todos los escenarios. La vinculación de la dirección MAC a una dirección IP se basa en asociar de manera exclusiva una dirección física única (MAC) a una dirección lógica (IP) en la red.

Verificación de cambio de dirección por parte del usuario. La capacidad del usuario para modificar su dirección IP dentro del pool de direcciones asignadas al servicio de Internet presenta un desafío significativo en términos de seguridad y control de acceso, como se evidencia en la Figura 54. Esto permite al usuario eludir restricciones y volver a conectarse sin haber cumplido con los requisitos de pago establecidos.

Figura 54

Nueva configuración de dirección ip del cliente

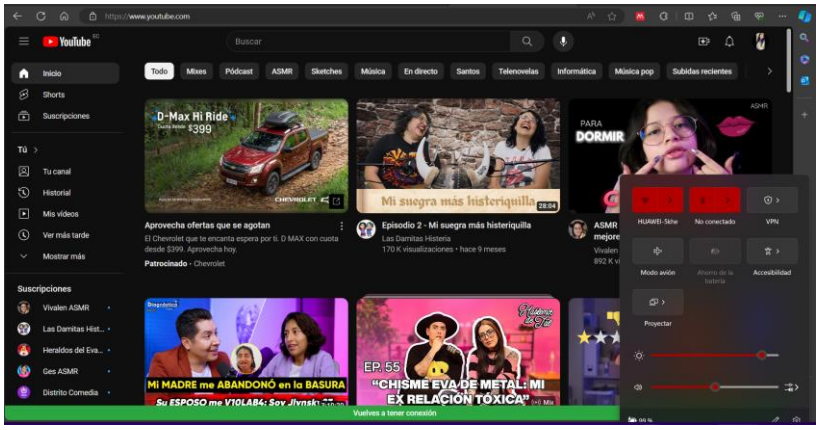


Nota. En la imagen se visualiza la nueva dirección ip del cliente, en este caso será la 192.168.1.100 que se encuentra dentro del pool de direcciones que acceden al servicio de internet.

Al realizar el cambio de ip el usuario vuelve a tener conexión al servicio de internet y puede acceder a los servicios que brinda, como se muestra en la Figura 55.

Figura 55

Reconexión del servicio

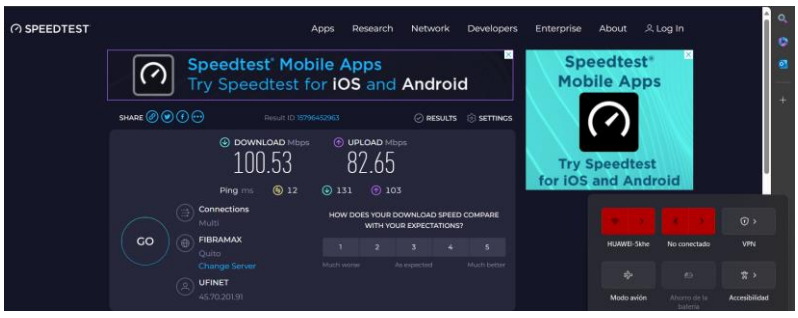


Nota. En la figura se muestra que el usuario puede acceder nuevamente a los servicios que brinda internet.

Se puede corroborar la reconexión a través de un test de velocidad de la red, que muestra la velocidad que posee el cliente, como se muestra en la Figura 56.

Figura 56

Test de velocidad de la reconexión



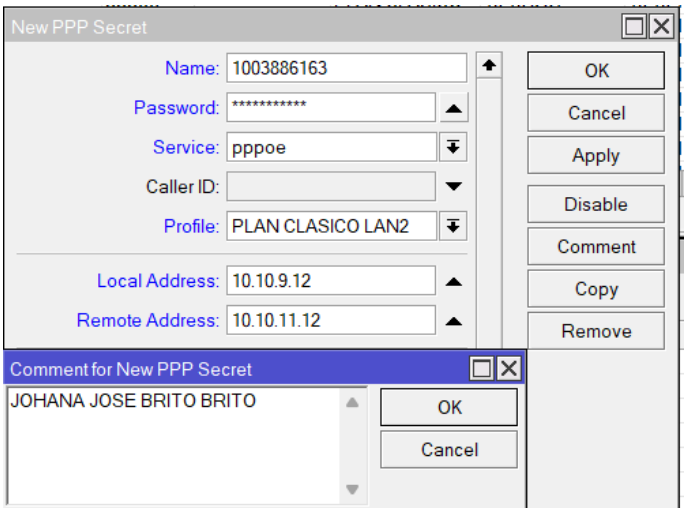
Nota. En la imagen se visualiza el test de velocidad que brinda información sobre la velocidad de descarga y subida de la red.

Autenticación por PPPoE del usuario. Como solución al problema identificado, se opta por llevar a cabo la migración del usuario hacia un método de autenticación más seguro, específicamente mediante el Protocolo de Punto a Punto sobre Ethernet (PPPoE). Esta migración implica la implementación de un sistema de autenticación más robusto, donde cada usuario se autentica de manera individualizada mediante un nombre de usuario y una contraseña. Al adoptar el PPPOE, se refuerza la seguridad al tiempo que se establece un mayor control sobre el acceso a la red. Este cambio no solo fortalece las medidas de seguridad, sino que también brinda una mayor capacidad para gestionar las conexiones de los usuarios, asegurando así un entorno más protegido y confiable en el servicio de Internet.

Como parte de la Gestión de Usuarios y Credenciales, las configuraciones iniciales se llevan a cabo a través de la plataforma Winbox, donde se inicia la creación de un nuevo perfil PPP secreto, como se muestra en la Figura 57. Este perfil está compuesto por un conjunto de parámetros esenciales, entre los que se incluyen un nombre de usuario y una contraseña para la autenticación, la especificación del servicio (en este caso, el protocolo PPP), la asignación de un perfil que corresponde al plan contratado de servicio de Internet y la definición de dos direcciones, una para la LAN local y otra para la LAN remota. Además, se incluye un comentario que proporciona información adicional, como el nombre del usuario.

Figura 57

Configuración Perfil PPP Secret



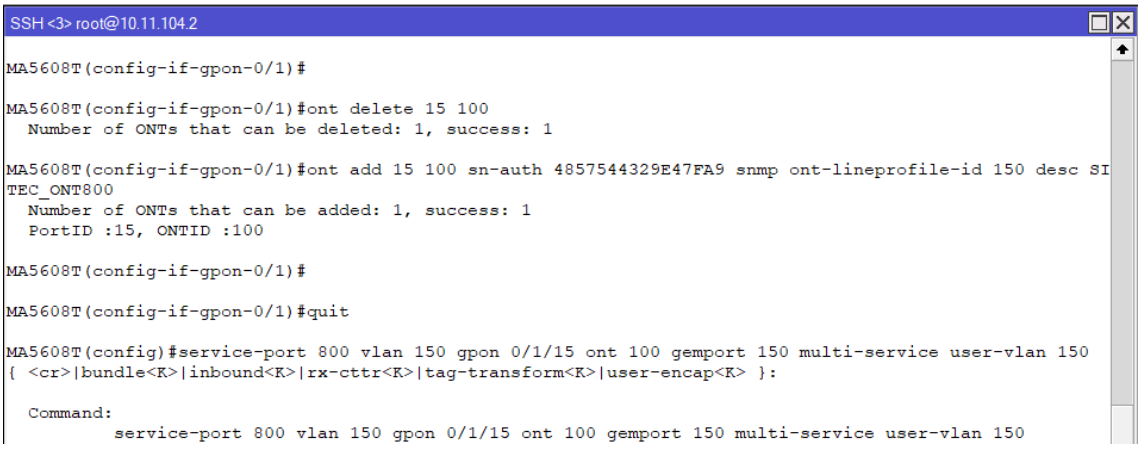
Nota. En la imagen se muestra las configuraciones del nuevo perfil, en este caso la información del cliente será las credenciales de acceso, como nombre usuario se asigna el número de cédula, la contraseña se asigna en la base de datos que se almacena a los clientes, se especifica que el servicio será PPPoE, el plan de servicio PLAN CLÁSICO LAN2, la dirección local y remota se encuentran en un nuevo pool de direcciones y como comentario, el nombre del cliente para identificación.

Para el proceso de configuración de Punto de Acceso con Equipos MikroTik se implementa el siguiente proceso, cuando es necesario actualizar o modificar la configuración de una ONT en la OLT, se opta por realizar un procedimiento que implica primero eliminar la ONT existente para luego agregarla nuevamente con los nuevos datos. Los comandos específicos utilizados para llevar a cabo esta tarea se encuentran detallados en la Figura 58. La conexión hacia la OLT se establece mediante el protocolo SSH desde la plataforma Winbox. Este enfoque

permite realizar ajustes precisos en la configuración de la ONT, garantizando que los cambios se implementen de manera efectiva.

Figura 58

Configuración en OLT

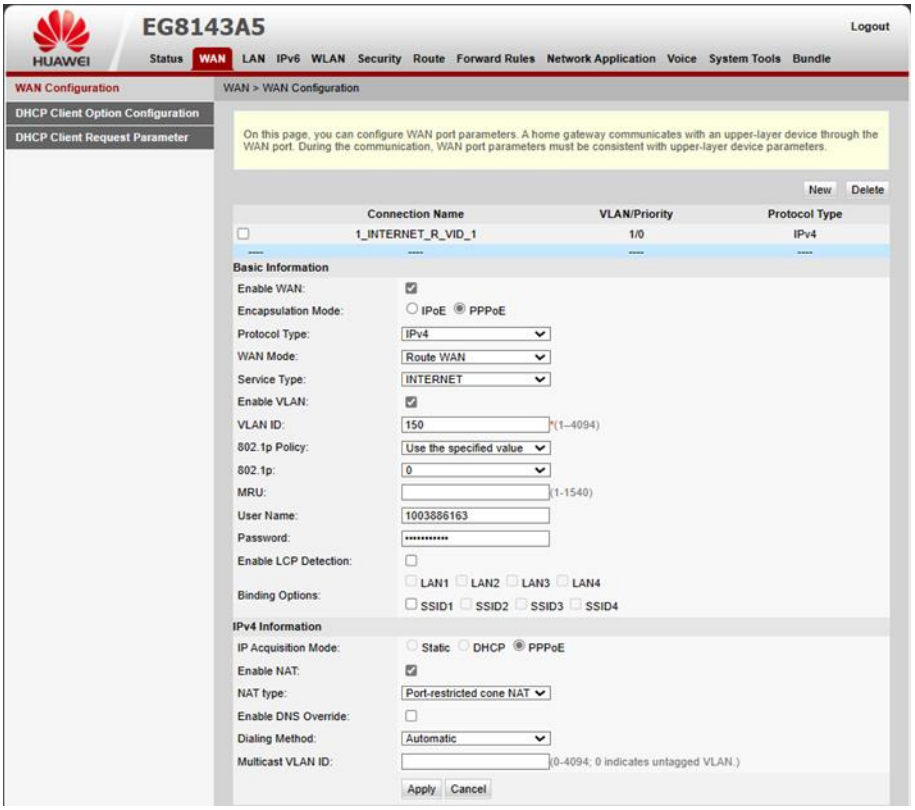


Nota. En la imagen se muestra la nueva configuración de la ONT, la cual consta de un cambio en la VLAN de la 1 a la 150.

Dentro del parámetro de configuración de la ONU en la arquitectura se implementa la autenticación por PPPoE a través de la configuración del tipo de encapsulación en este modo, la VLAN a la que se le asigna, el nombre de usuario y contraseña que se configuró previamente el Winbox que serán las credenciales de acceso, como se detalle en la Figura 59. Para esta configuración cabe destacar que no se puede asignar una dirección ip en el dispositivo final, únicamente el administrador puede hacerlo desde Winbox.

Figura 59

Configuración PPPoE de Dispositivo Final



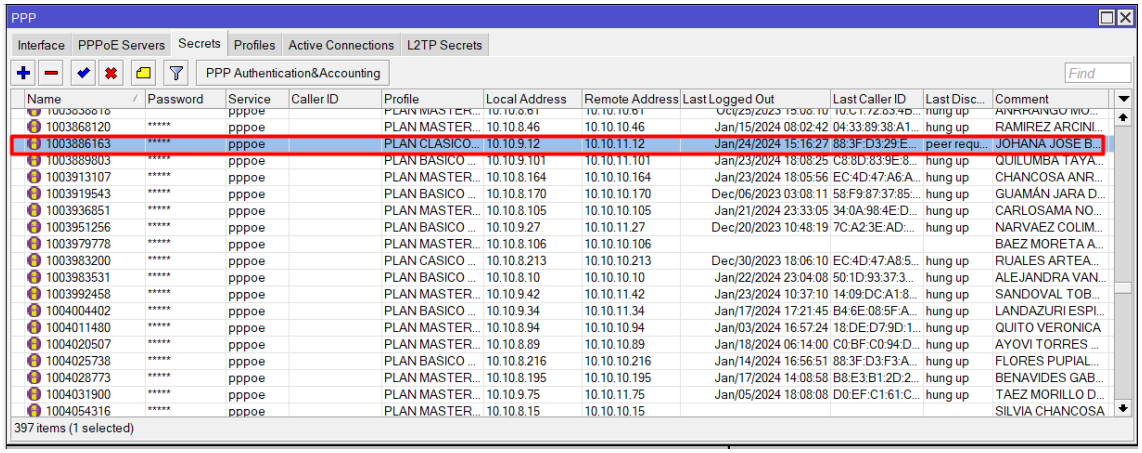
Nota. En la imagen se visualiza las configuraciones del dispositivo final donde se especifica que el modo de Encapsulación que será PPPoE, la VLAN a la que pertenece es la 150, el usuario y contraseña serán los asignados anteriormente.

Verificación del funcionamiento de la autenticación. En la interfaz de Winbox, se posibilita la verificación de la conexión del usuario a la red mediante PPPoE, esto forma parte del Registro y Control de Actividad de los usuarios. En esta ventana, se presentan detalladamente los atributos asociados al usuario, incluyendo su nombre y contraseña de autenticación, el tipo de servicio al que está suscrito, el plan de servicio asignado, así como las direcciones de red local y remota, se verifica esto en la Figura 60. Además, se brinda la capacidad de administrar la

conexión del usuario, lo que implica la posibilidad de realizar ajustes y gestionar eficazmente los parámetros de la conexión.

Figura 60

Usuario conectado por PPPoE

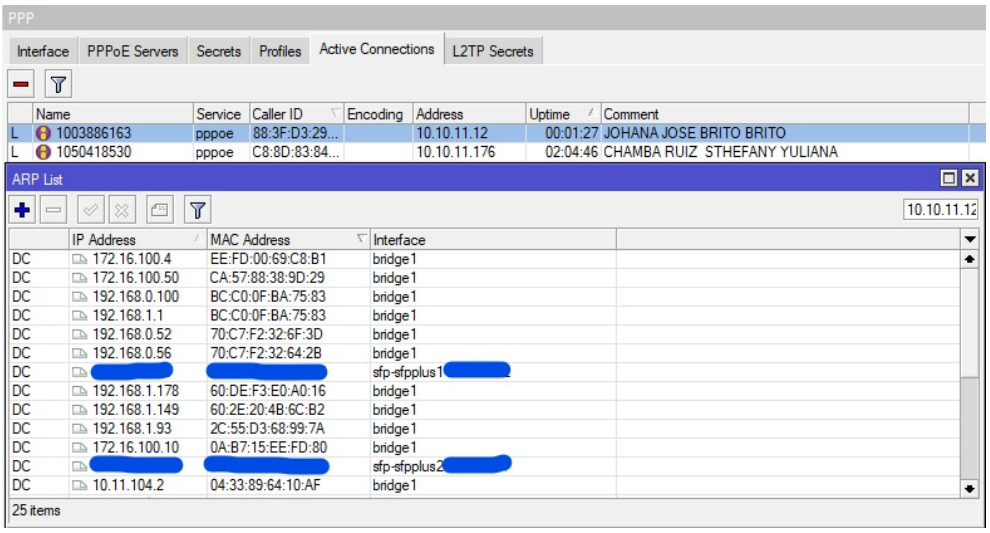


Nota. En la imagen se visualiza los usuarios que se encuentran autenticados a la red por PPPoE, en esta ventana se puede realizar la gestión de conexiones y credenciales.

Además, se realiza una verificación adicional en el listado de las conexiones activas en el Protocolo de Punto a Punto (PPP) en esta parte se puede evidenciar el Monitoreo y Resolución de Problemas, donde se identifica la presencia del nuevo usuario asociado al cliente, como se muestra en la Figura 61. Este listado proporciona un panorama completo de las conexiones PPP activas en la red, permitiendo así confirmar de manera específica la incorporación exitosa del usuario recientemente configurado, al mismo tiempo se comprueba que ya no existe registro de este usuario en la lista de ARP.

Figura 61

Usuario Activo

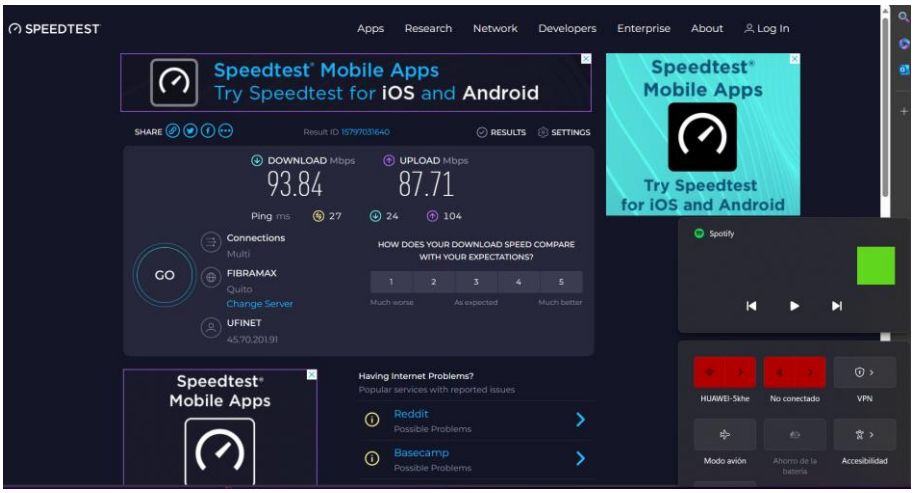


Nota. En la figura se puede visualizar que el usuario fue registrado correctamente y se visualiza los datos configurados.

Para verificar la conectividad del cliente, se lleva a cabo un test de velocidad que evalúa la capacidad de transferencia de datos de la conexión, como se muestra en la Figura 62. Este procedimiento no solo confirma la existencia de la conectividad, sino que también proporciona información valiosa sobre el rendimiento de la conexión a Internet. Una vez completado el test de velocidad, se verifica que el usuario efectivamente tiene acceso a Internet, asegurando así la funcionalidad y operatividad exitosa de la conexión recientemente configurada.

Figura 62

Test de Velocidad

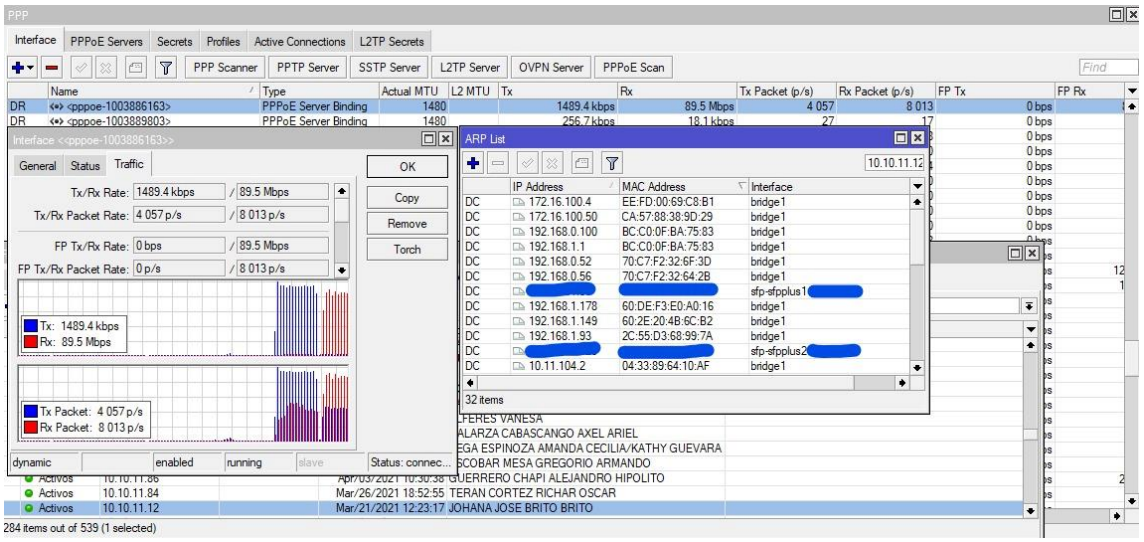


Nota. En la imagen se observa que la velocidad de descarga y de subida que el usuario posee, esto permite verificar que la conexión a internet es buena.

Cuando se verifica la activación de la dirección IP en la conexión PPPoE y se observa su ausencia en la tabla de resolución de direcciones ARP, se confirma que el proceso de autenticación del usuario se ha llevado a cabo de manera integral y exitosa. Este escenario indica que el usuario ha completado satisfactoriamente la autenticación, obteniendo así la asignación de una dirección IP válida mediante el protocolo PPPoE, esto se puede verificar en la Figura 63. La ausencia de la dirección IP en la tabla ARP sugiere que el sistema ha realizado un proceso de autenticación completo, permitiendo al usuario acceder a la red y obtener una conexión activa este proceso forma parte del Monitoreo y Resolución de Problemas.

Figura 63

Verificación de Usuario activo

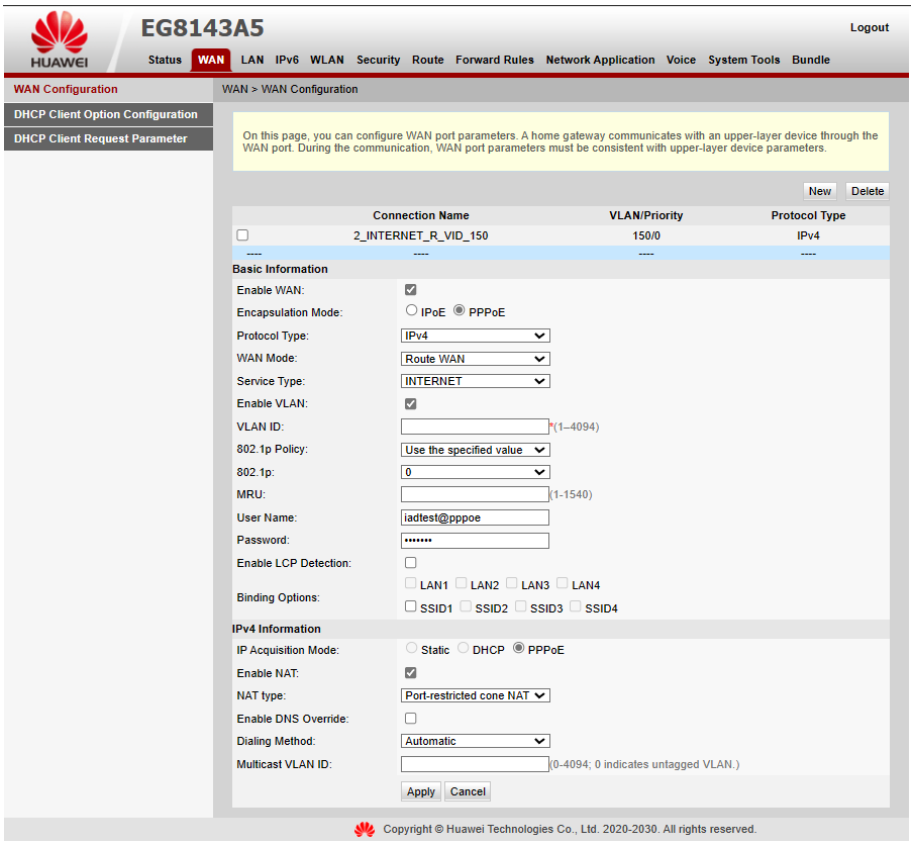


Nota. En la imagen se visualiza las gráficas del tráfico que genera el usuario y se comprueba que se encuentra activo en la lista se conexiones PPP.

La configuración del dispositivo final se encuentra protegida contra manipulaciones no autorizadas por parte del cliente debido a las restricciones inherentes al protocolo PPPoE, se puede verificar en la Figura 64. Esta limitación impide que el cliente realice cambios directos en la configuración, como agregar direcciones IP o modificar la dirección del usuario. La información esencial para la conexión, incluyendo las direcciones IP y los detalles del usuario, está exclusivamente almacenada en Winbox, centralizando así la gestión y control de la red.

Figura 64

Configuraciones Dispositivo Final



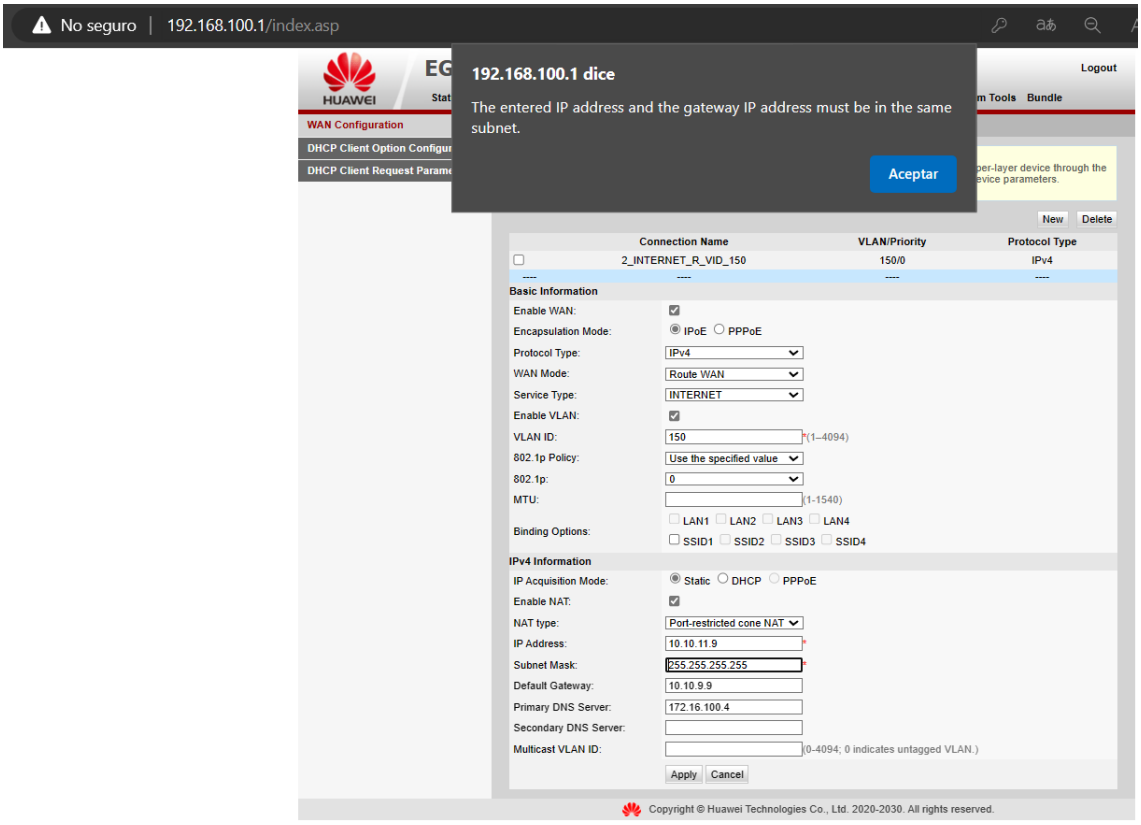
Nota. En la imagen se visualiza los parámetros que el protocolo PPPoE permite configurar, a diferencia del IPoE.

La tentativa de crear un nuevo perfil con el propósito de asignar una dirección IP, replicando los datos ya asignados al usuario, resulta infructuosa debido a las limitaciones inherentes a la configuración PPPoE, como se evidencia en la Figura 65. Este protocolo no permite realizar este tipo de modificaciones o configuraciones directas en los perfiles de usuario. La naturaleza restrictiva del PPPoE asegura la integridad de la asignación de direcciones IP y

otros parámetros, evitando cambios no autorizados que podrían afectar la estabilidad y seguridad de la red.

Figura 65

Configuración No válida



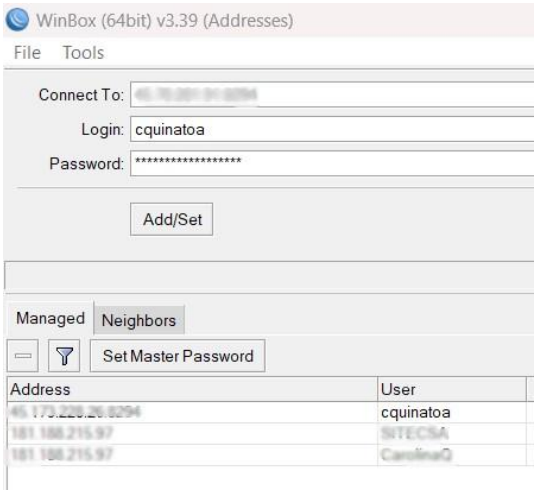
Nota. En la imagen ser visualiza que no se puede configurar una nueva dirección al usuario, el sistema rechaza este tipo de configuraciones pues el protocolo en funcionamiento es PPPoE.

Como parte del despliegue del protocolo PPPoE y la arquitectura AAA en la infraestructura de la empresa y el Registro y Control de Actividad de la arquitectura, se llevan a cabo pruebas fundamentales para verificar la funcionalidad de la autenticación, tanto para usuarios administrativos como para la conexión exitosa del servidor Radius con el servicio

PPPoE. Después de crear un nuevo usuario para propósitos administrativos, se ejecuta una verificación meticulosa para asegurar que dicho usuario tenga acceso al equipo MikroTik, como se ilustra en la Figura 66. Este paso reviste una importancia significativa al confirmar la efectividad de la creación del perfil administrativo y garantizar que el recién creado usuario pueda acceder al equipo MikroTik de acuerdo con los parámetros y permisos establecidos. Esta validación asegura la coherencia entre la configuración del perfil administrativo y el acceso real al equipo, consolidando así la implementación exitosa de la autenticación y la conexión PPPoE en el entorno de la empresa.

Figura 66

Validación de Usuario

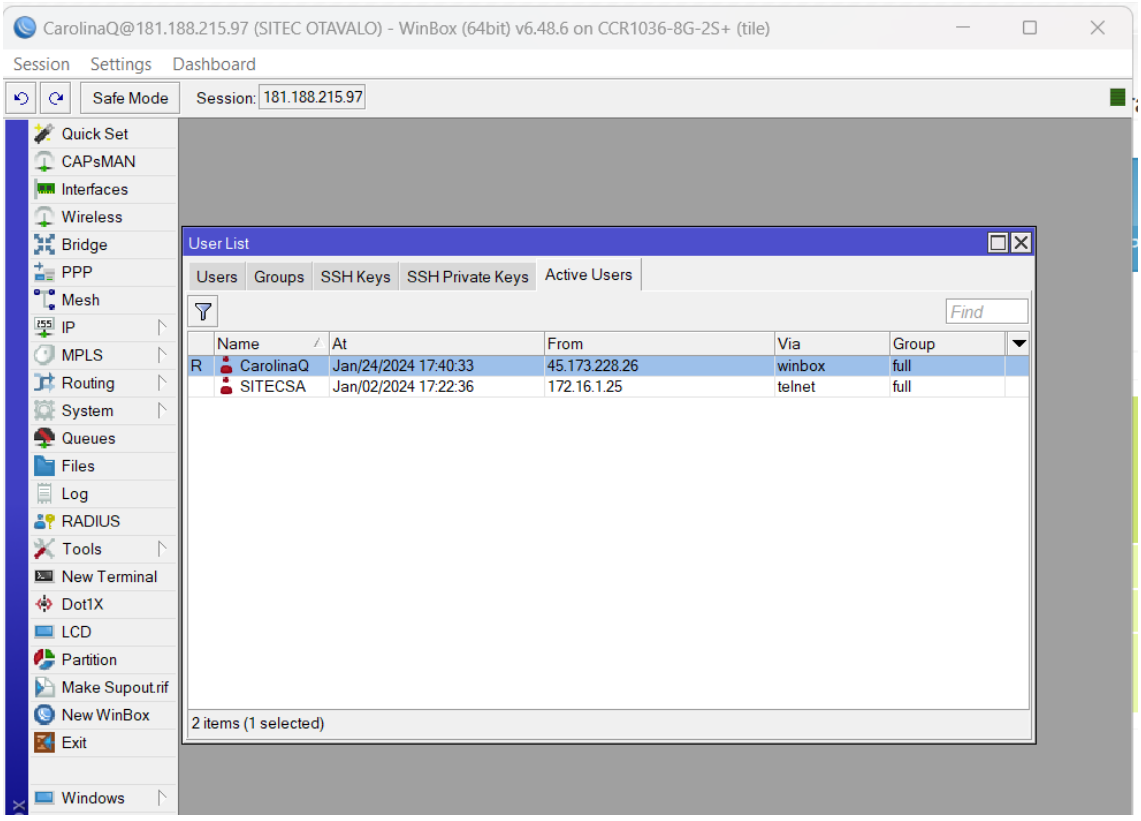


Nota. En la imagen se visualiza la autenticación del usuario como administrador del equipo Mikrotik, el usuario cquinatoa y se le asigna una contraseña que serán las credenciales para el acceso.

Una vez que se logra acceder al equipo, se procede a visualizar el ingreso del usuario mediante las listas de usuarios, donde se obtiene información detallada como las fechas de acceso y los permisos específicos que el usuario posee, como se visualiza en la Figura 67. Esta función proporciona una visión exhaustiva del historial de acceso del usuario, permitiendo una supervisión efectiva de las actividades y privilegios asignados, esto asegura un control riguroso sobre el acceso y la gestión de configuraciones en el equipo Mikrotik.

Figura 67

Verificación de Ingreso del usuario

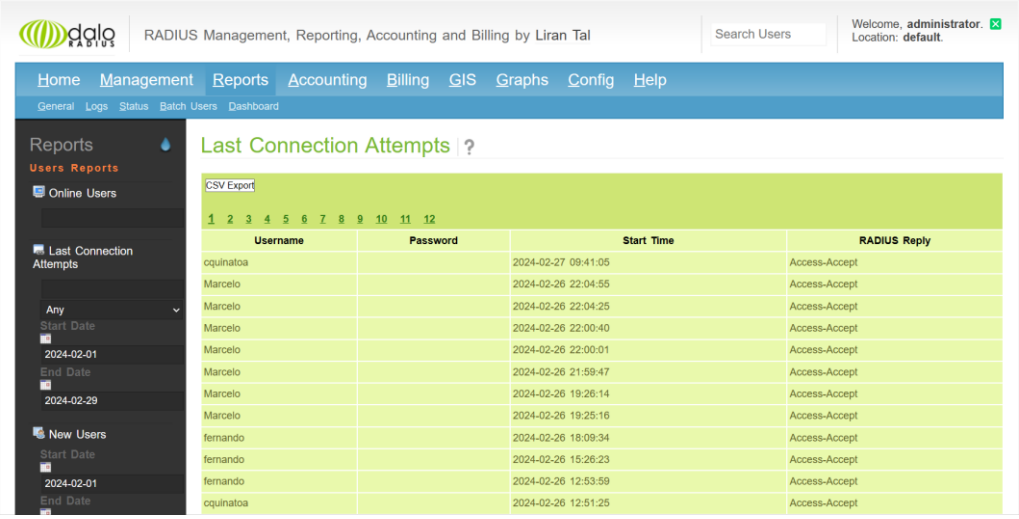


Nota. La imagen muestra la información que el usuario realizó una autenticación y obtuvo el acceso al equipo.

Esta herramienta proporciona la capacidad de monitorear los ingresos de personas autorizadas, registrando de manera detallada la fecha y la hora de cada acceso. A través de este monitoreo, se obtiene un registro preciso y cronológico de las actividades de los usuarios autorizados, como se visualiza en la Figura 68., lo que facilita la supervisión efectiva de la red.

Figura 68

Conexiones Realizadas



Nota. Se puede visualizar en la imagen los intentos de acceso de los usuarios con las credenciales y la fecha de acceso.

Conclusiones y Recomendaciones

Conclusiones

- La exploración en profundidad de la gestión de servicios de Internet en la empresa SITEC ha revelado la necesidad crítica de un cambio de modelo en los mecanismos de control de acceso y autenticación de usuarios. La dependencia actual del control de acceso basado en IP ha demostrado ser susceptible de ser evadido por los usuarios, lo que ha provocado la necesidad de una solución más robusta y segura.
- La implementación propuesta de la arquitectura AAA y el protocolo PPPoE, utilizando equipos MikroTik, surge como una respuesta estratégica a los problemas detectados como es el cambio de dirección ip del cliente y la falta de control de acceso del personal dentro de la red. La integración de la arquitectura AAA no sólo mejora la autenticación de usuarios a través de servidores Radius, sino que también introduce un enfoque sistemático para la autorización y la auditoría. Este enfoque multifacético promete un sistema de gestión de usuarios más seguro y eficaz.
- Los objetivos planteados describen una estrategia integral para el despliegue de AAA y PPPoE en la infraestructura de red de la empresa SITEC. La utilización de servidores Radius para la autenticación de usuarios se alinea con los estándares actuales y las mejores prácticas de la industria, garantizando una solución robusta y adaptable.
- La implementación de la arquitectura AAA y el protocolo PPPoE para controlar el acceso a Internet de los usuarios de la empresa SITEC de Ibarra permitió realizar una cuidadosa planificación y pruebas exhaustivas que dieron como resultado un sistema robusto y fiable que cumple eficazmente las normas de autenticación, autorización y registro.

- Los resultados previstos de esta tesis abarcan una postura de seguridad mejorada, una administración racionalizada de los servicios de Internet y una reducción de las vulnerabilidades asociadas con el actual sistema de control de acceso centrado en IP. La migración prevista del control basado en IP a la autenticación centrada en el usuario representa un paso fundamental hacia la consolidación de la integridad general de la red y la fiabilidad del servicio en la empresa SITEC.

Recomendaciones

- Asegurarse de tener conocimiento básico de los programas que se utilizan, incluidos los routers, Daloradius, Proxmox y MikroTik. Esta familiaridad contribuirá a un funcionamiento más fluido y a una resolución de problemas eficaz.
- Priorizar el uso de las últimas versiones estables del software. Asegúrese de que todos los instaladores tienen acceso a las versiones más recientes y estables junto con los parches necesarios. Esto ayuda a prevenir complicaciones durante la instalación y garantiza un rendimiento óptimo.
- Documentar exhaustivamente la solución implementada, incluidos los ajustes de configuración, las políticas de seguridad y los procedimientos de solución de problemas. Facilitar la transferencia de conocimientos dentro de la empresa para capacitar a los administradores en la gestión y el mantenimiento eficaces de la nueva infraestructura.
- Definir y aplicar políticas de control de acceso dentro de la red. Asigne permisos y privilegios específicos a los administradores en función de sus funciones y responsabilidades. Esto garantiza que sólo el personal autorizado pueda acceder a la información sensible, mejorando la seguridad de la red.

Bibliografía

ARCOTEL. (diciembre de 2019). *ARCOTEL*. Obtenido de Boletín Estadístico: https://www.arcotel.gob.ec/wp-content/uploads/2015/01/boletin-febrero-2020-.pdf

Ashley. (27 de noviembre de 2022). *What is Winbox and How to Use it*. Obtenido de OperaVPS: https://operavps.com/docs/what-is-winbox/

Caicedo, A. (10 de agosto de 2013). *ADMINISTRACIÓN DE REDES DE COMPUTADORES Conceptos Generales.* Recuperado el 31 de enero de 2023, de https://www.academia.edu/11531163/ADMINISTRACI%C3%93N_DE_REDE

Calvete, F. (25 de noviembre de 2020). *Xdoc.m.* Obtenido de Seguridad en el acceso: https://xdoc.mx/preview/aaa-arquitectura-metodos-de-autenticacion-username-y-password-5c10199cd6a3c

Cepeda, C., & Proaño, P. (2007). *Diseño e Implementación de un cliente radius en Linux.* Quito: Escuela Politécnica Nacional.

Charlene. (23 de junio de 2020). *FS Community.* Obtenido de ¿Cuál es la diferencia entre PPPoE y DHCP:?: https://community.fs.com/es/blog/pppoe-vs-dhcp-what-is-the-difference.html

Debian.org. (2004). *Cumplir los requisitos mínimos de hardware*. Obtenido de Debian: https://www.debian.org/releases/stable/s390x/ch03s04.es.html

Ecuador, R. (13 de septiembre de 2019). *RUC Ecuador*. Obtenido de Información Básica de la Empresa: https://rucecuador.com/rucsri/servicio-internet-telecomunicaciones-sitec-sitec-1091784498001

EMIS. (21 de agosto de 2019). *EMIS.* Obtenido de SERVICIO DE INTERNET Y TELECOMUNICACIONES SITEC S.A. (ECUADOR):

https://www.emis.com/php/company-profile/EC/Servicio_de_Internet_y_Telecomunicaciones_Sitec_SA_es_9651009.html

Fernández, P. (2014). *Estudio de un sistema centralizado de autenticación, autorización y Accounting (AAA) que facilite la provisión de políticas de calidad para los servicios de banda ancha de la Corporación Nacional de Telecomunicaciones E.P.* Quito.

Firch, J. (23 de septiembre de 2022). *Purplesec*. Obtenido de Common Types Of Network Security Vulnerabilities: https://purplesec.us/common-network-vulnerabilities/#:~:text=Operating%20System%20Misconfigurations-,What%20Is%20A%20Network%20Vulnerability%3F,result%20in%20a%20security%20breach.

Hashemi, M. (14 de junio de 2022). *What is Winbox and How you can connect to your Mikrotik VPS by it.* Obtenido de https://ded9.com/what-is-winbox-and-how-you-can-connect-to-your-mikrotik-vps-by-it/

Hassel, J. (2002). *RADIUS: Authentication and Accounting.* O REILLY & ASSOCIATES.

Hellberg, C., Greene, D., & Boyes, T. (2006). *Broadband Network Architectures: Designing and Deploying Triple-Play.*

Hoxha, D. (2017). *Managing Internet Connections with PPPoE, Mikrotik and Radius.*

Huerta, A. (2002). *Seguridad en Unix y Redes.*

Kumar, S. (20 de abril de 2023). *Tutorialspoint*. Obtenido de A Fresh Installation of Debian 11 Bullseye: https://www.tutorialspoint.com/a-fresh-installation-of-debian-11-bullseye#:~:text=Before%20you%20start%20installation%20process,GB%20of%20free%20disk%20space.

Mikrotik. (2023). *Mikrotik*. Obtenido de CCR1036-12G-4S: https://mikrotik.com/product/CCR1036-12G-4S-149

Molero, L., Villaruel, M., Aguirre, E., & Martínez, Á. (2010). *Planificación y Gestión de Redes.* Maracaibo: Universidad "Dr. Rafael Belloso Chacín".

Murray, L. (28 de agosto de 2023). *Imperva.* Obtenido de Information Security: The Ultimate Guide: https://www.imperva.com/learn/data-security/information-security-infosec/

Nakhjiri, M., & Nakhjiri, M. (2005). *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility.* Wiley.

NetworkRadius. (2021). *Hardware Requirements for FreeRADIUS.* Obtenido de NetworkRadius: https://networkradius.com/articles/2023/02/07/hardware-requirements.html

Proxmox. (2023). *Proxmox*. Obtenido de Proxmox Virtual Environment: https://www.proxmox.com/en/proxmox-virtual-environment/overview

Raj, V. (2022). *CloudRadius*. Obtenido de 2022 Security Analysis of PEAP-MSCHAPv2: https://www.cloudradius.com/security-of-peap-mschapv2/

Shami, A., & Maier, M. (2008). *Broadband Access Networks: Introduction Strategies and Technologies.* Springer-Science+Business Media.

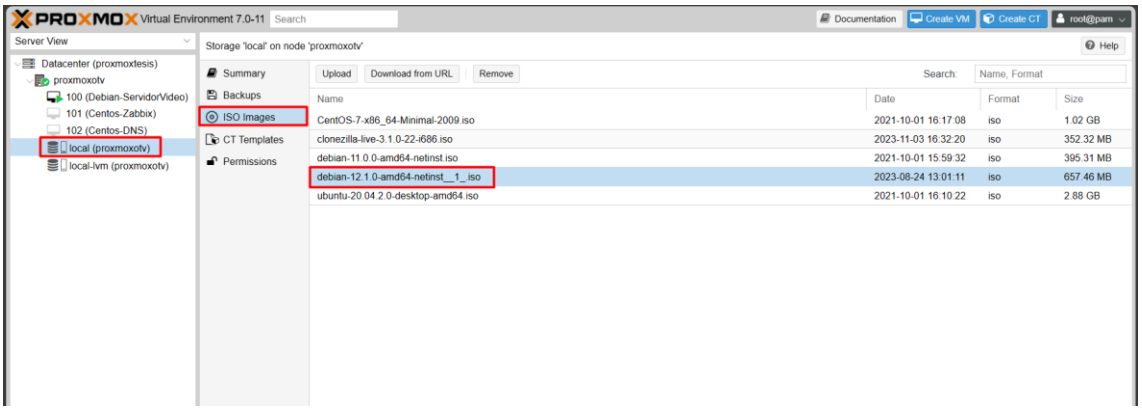
SITEC S.A. (septiembre de 2023). *SITEC Navega Sin Límites*. Obtenido de SITEC Navega Sin Límites: https://sitec.ec/

Tal, L. (4 de noviembre de 2021). *DaloRadius*. Obtenido de GitHub: https://github.com/lirantal/daloradius

ANEXOS

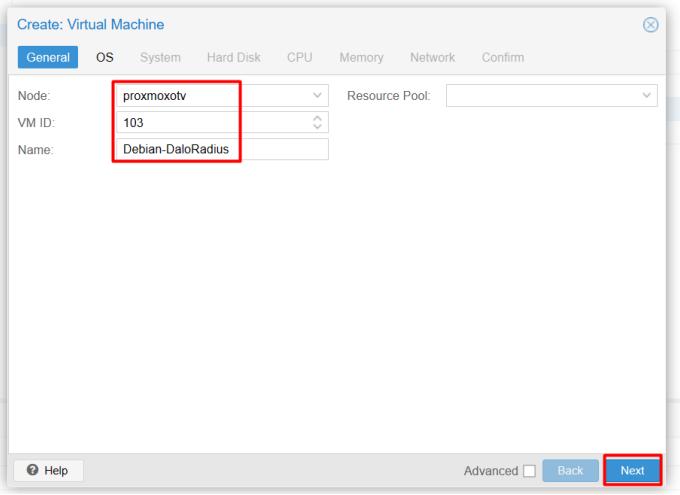
Anexo A: Instalación Debian 11 en Proxmox

Carga de Imagen ISO en Proxmox

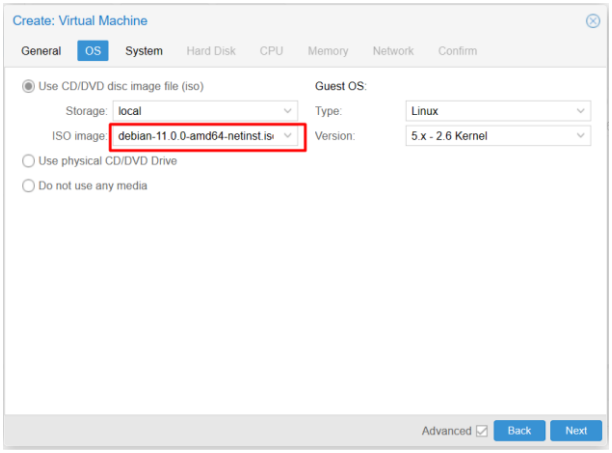


Tras cargar la imagen ISO en Proxmox, se inicia la creación de la máquina virtual para instalar el sistema operativo. Durante este proceso, se elige el nodo "proxmoxtv", se le asigna el identificador 103 y se nombra la máquina virtual como "Debian-Daloradius" para facilitar su identificación.

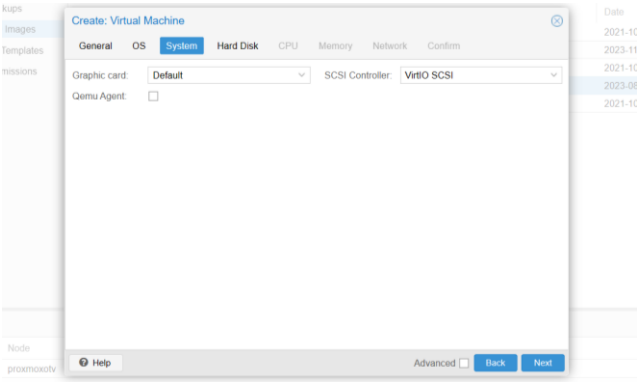
Configuración General para Máquina Virtual



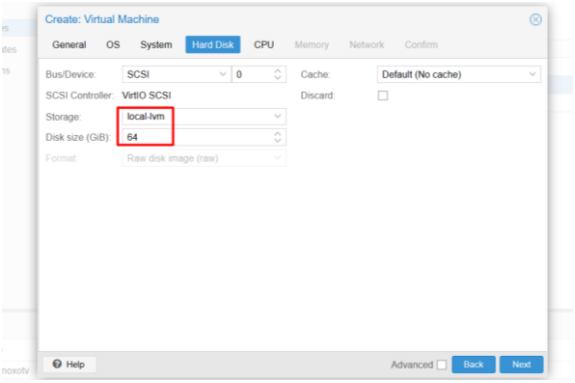
Durante este procedimiento, se selecciona la imagen ISO previamente cargada con el fin de instalar el sistema operativo. En este caso específico, se opta por instalar Debian 11 utilizando el archivo de disco en formato ISO como si fuera un CD/DVD.



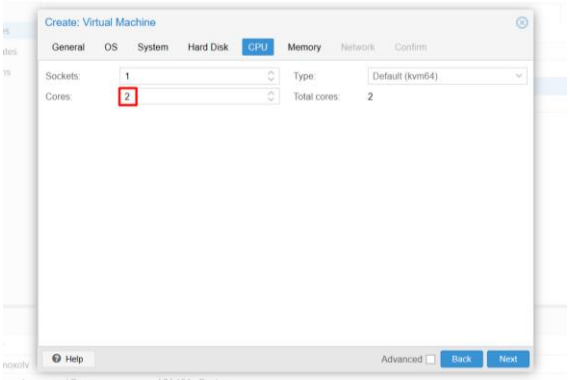
En este caso la configuración será por defecto



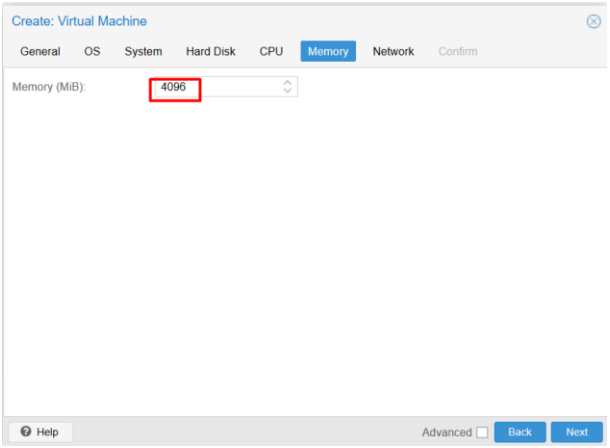
Para la selección del disco, se elige el disco local, y se le asigna un espacio requerido.



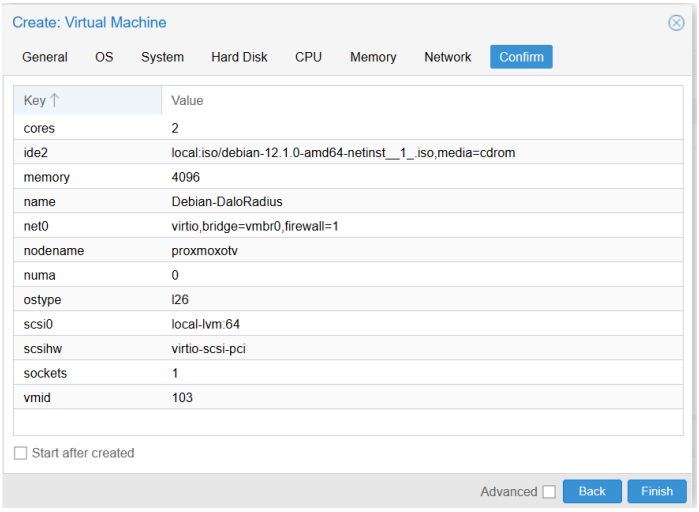
El número de CPU que se le asigna es de 2 para un correcto funcionamiento



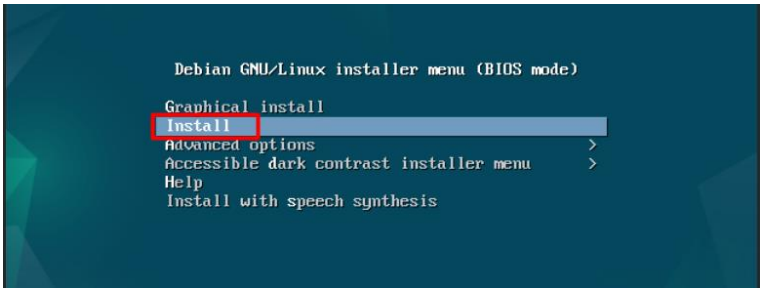
El espacio de memoria asignada de es de 4096 MB



Se visualiza el resumen de los parámetros configurados para la máquina Debian



Para el levantamiento del sistema operativo Debian se realiza una instalación con requisitos mínimos



En este caso selecciona la opción de instalación mínima del sistema

En el siguiente enlace se asigna un video como recurso para la instalación correcta del sistema operativo Debian 11

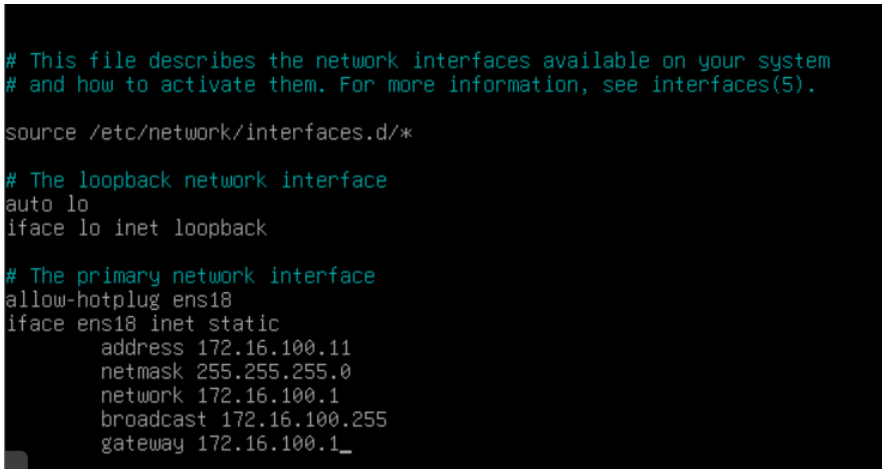
(10) Linux Debian 11 - Instalación Mínima paso a paso [V284] - YouTube

Anexo B: Instalación Daloradius en Debian 11

Para la instalación de DaloRadius se realiza el siguiente proceso. Principalmente se realiza la configuración de los parámetros de red con el siguiente comando.

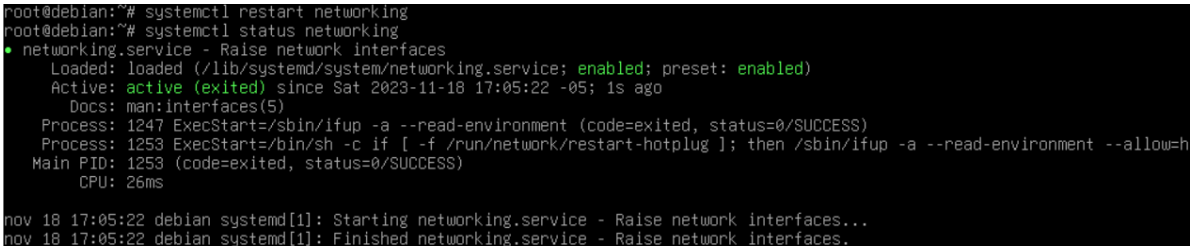
nano /etc/network/interfaces

- address
- netmask
- network
- broadcast
- gateway

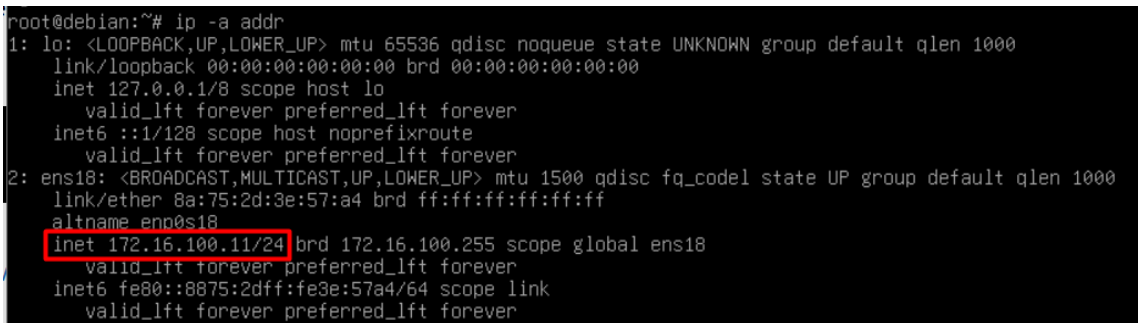


Verificar que la red esté activa y realizar la consulta de los parámetros de red para verificar que los cambios se han realizado de manera correcta.

systemctl status networking



ip -a addr



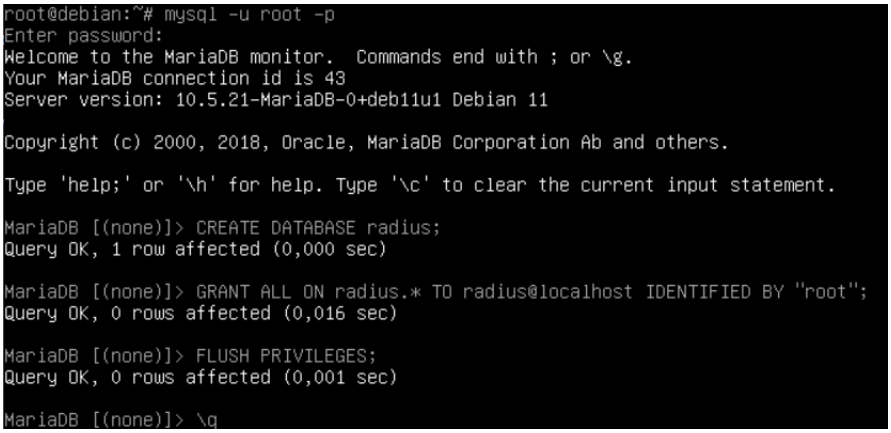
Se procederá con la actualización y aprovisionamiento del sistema operativo mediante los comandos apt update y sudo apt -y upgrade. Posteriormente, se llevará a cabo la instalación de un servidor de bases de datos. En este caso, se empleará MariaDB, aunque se puede optar por cualquier otro servidor de bases de datos compatible.

apt -y install mariadb-server mariadb-client.

mysql_secure_installation

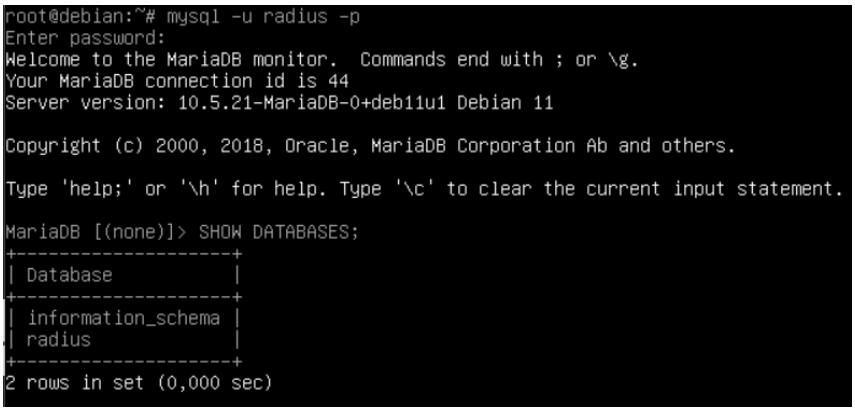
Después de finalizar la instalación, se llevará a cabo la creación de una base de datos y de un usuario específicamente destinados para FreeRADIUS/daloRADIUS.

mysql -u root -p



Garantizar la accesibilidad del usuario "radius" a la base de datos requiere la ejecución de ciertos procedimientos.

mysql -u radius -p



Con el siguiente comando se realiza la instalación del servidor web Apache2 y PHP

apt -y install apache2

apt -y install php libapache2-mod-php php-{gd,common,mail,mail-mime,mysql,pear,mbstring,xml,curl}

pear install DB

Para confirmar una instalación exitosa, se recomienda verificar la versión de PHP instalada. Esto se puede lograr ejecutando el siguiente comando:

php -v

Este comando proporcionará información detallada sobre la versión de PHP instalada en el sistema.

Los paquetes FreeRADIUS están disponibles en los repositorios de Debian de manera predeterminada. La instalación se realiza de manera sencilla mediante el siguiente comando:

apt -y install freeradius freeradius-mysql freeradius-utils

Este procedimiento instalará FreeRADIUS junto con sus dependencias.

Después de la instalación, se debe ejecutar el servicio para que entre en funcionamiento. Esto se realiza con el siguiente comando:

systemctl enable --now freeradius.service

```
root@debian:~# systemctl enable --now freeradius.service
Synchronizing state of freeradius.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable freeradius
```

Para verificar el estado actual del servicio FreeRADIUS, puede utilizar el siguiente comando:

systemctl status freeradius

```
root@debian:~# systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-11-20 19:15:00 -05; 57s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
   Main PID: 3796 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 4661)
     Memory: 81.1M (limit: 2.0G)
        CPU: 232ms
     CGroup: /system.slice/freeradius.service
             └─3796 /usr/sbin/freeradius -f
```

Este comando proporcionará información detallada sobre el estado actual del servicio, permitiendo confirmar si se está ejecutando correctamente.

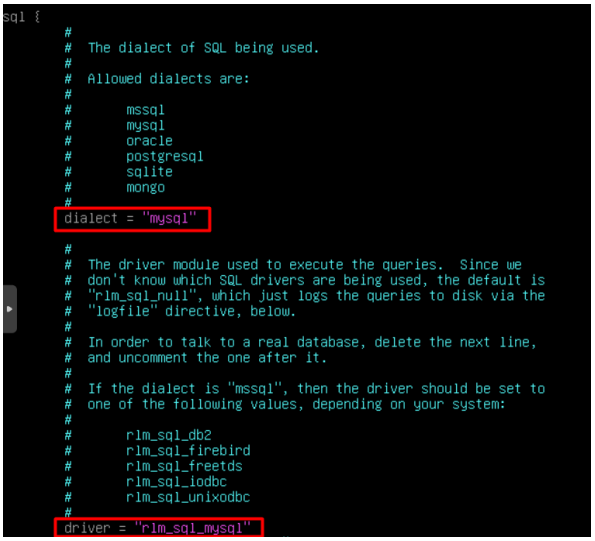
Para configurar FreeRADIUS para utilizar MariaDB, se deben seguir los siguientes pasos:

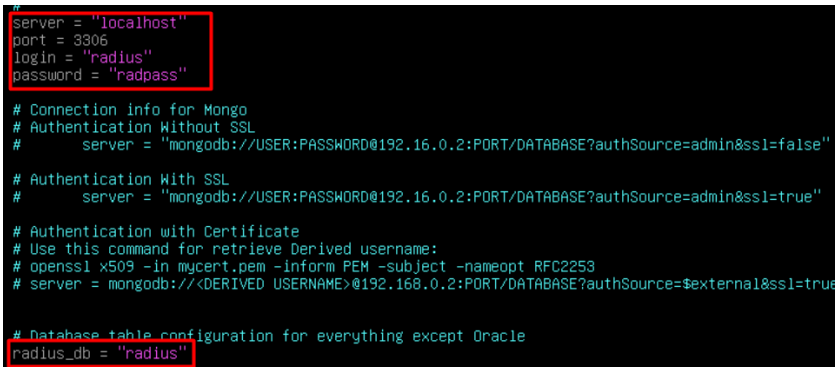
Importe el esquema de la base de datos Radius para poblar la base de datos Radius. Este paso implica la carga de la estructura de la base de datos necesaria para el funcionamiento de FreeRADIUS.

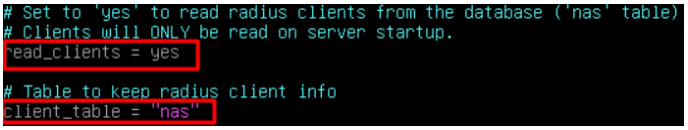
mysql -u root -p radius </etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql

ln -s /etc/freeradius/3.0/mods-available/sql /etc/freeradius/3.0/mods-enabled/

vim /etc/freeradius/3.0/mods-enabled/sql







Esta línea realiza el cambio del grupo del archivo o enlace simbólico ubicado en /etc/freeradius/3.0/mods-available/sql al grupo freerad.

chgrp -h freerad /etc/freeradius/3.0/mods-available/sql

Esta línea cambia el propietario y grupo de todos los archivos y subdirectorios dentro de /etc/freeradius/3.0/mods-enabled/sql al usuario y grupo freerad.

chown -R freerad:freerad /etc/freeradius/3.0/mods-enabled/sql

Al finalizar las configuraciones, se reinicia el servicio y está listo para ser utilizado.

systemctl restart Freeradius

Anexo C: Contrato de Prestación de Servicios

CONTRATO DE PRESTACIÓN DE SERVICIOS DE INTERNET No: ____

Ibarra, ___ de _____ del ____, comparecen a la celebración del presente contrato, por una parte, el ABONADO/SUSCRIPTOR: _____ con cédula/RUC: _____, email: _____, teléfono: _____, con domicilio en: _____, parroquia:_____, cantón: _____, ciudad: _____, provincia: _____ que para efectos de este contrato se lo denominará CLIENTE. Dirección donde será prestado el servicio: _____

El abonado es de la Tercera edad o con discapacidad:

SI ◯

NO ◯

Por otra parte, la señora Susana del Rocío León Gudiño en calidad de Representante Legal de SITEC S.A. con R.U.C. Nro. 1091784498001 a quien en adelante se llamará el "PROVEEDOR,", quienes libre y voluntariamente convienen celebrar el presente contrato, contenido en las siguientes cláusulas:

PRIMERA. - ANTECEDENTES

En base a la NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES emitida por la Agencia de Regulación y Control de las Telecomunicaciones, actualmente vigente, El PROVEEDOR como empresa privada con fin de lucro enfoca sus servicios en la compra/venta, importación/exportación de hardware y software necesarios para la prestación de servicios de telecomunicaciones en general. El mismo que propone unilateralmente la definición de este contrato de adhesión, así como también de cada una de sus cláusulas.

El objeto del permiso otorgado a SITEC S.A para la prestación de servicios de telecomunicaciones anticipa que el PROVEEDOR se encuentra en capacidad de suscribir el presente contrato para la prestación de Servicios de Internet, Valor Agregado, u otros afines al área de Informática y Telecomunicaciones en general, y proporcionará al CLIENTE los servicios que este pidiera a través de las respectivas órdenes de servicio. Así mismo acogiéndose a los derechos del cliente otorgados en la Ley Orgánica de Telecomunicaciones que establece en el artículo 22, como derecho de los abonados, clientes y usuarios: "*18. A acceder a cualquier aplicación o servicio permitido disponible en la red de internet. Los prestadores no podrán limitar, bloquear, interferir, discriminar, entorpecer ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos de red, siempre que sean legales. Se exceptúan aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, aplicaciones, desarrollos o servicios disponibles, o por disposición de autoridad competente. Los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas, para efectos de garantizar el servicio." (Subrayado fuera del texto original).*

Valiendo mencionar que el PROVEEDOR debe precautelar la privacidad del CLIENTE para cumplimiento de su derecho a la Intimidad establecido en el artículo 66, numeral 20 de la Constitución de la República, sin embargo, no se garantiza la privacidad debido a factores externos no imputables al prestador.

SEGUNDA. - OBJETO DEL CONTRATO

El PROVEEDOR se compromete a proporcionar al ABONADO/SUSCRIPTOR el o los servicios de:

Acceso a Internet ◯

Portador ◯

Para lo cual el prestador del servicio dispone de los correspondientes títulos habilitantes otorgados por la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL.

El PROVEEDOR brindará el servicio objeto de este contrato dentro del marco legal general definido por el mismo y el ámbito legal regido por el Código Civil, Ley Especial de Telecomunicaciones, Ley de Propiedad Intelectual, Ley de Compañías, Ley de Arbitraje y Mediación y ordenamiento jurídico vigente; con el alcance, condiciones y demás características establecidos y detallados en el presente contrato.

TERCERA. - PLAZO

La duración del contrato es de 12 meses, su vigencia iniciará a partir de la instalación y activación del servicio contratado. Sin prejuicio de lo anteriormente señalado, el Cliente pueda dar por terminado el contrato para ello se deberán seguir las condiciones contenidas en las leyes vigentes y en la cláusula decimoquinta del mismo documento.

El abonado acepta la renovación automática sucesiva del contrato en las mismas condiciones de este contrato, independientemente de su derecho a terminar la relación contractual conforme a la legislación vigente y la cláusula decimotercera del presente contrato.

SI ◯

NO ◯

CUARTA. - CLAUSULA DE PERMANENCIA MÍNIMA

Sin perjuicio de la cláusula anterior, sí el cliente deseara contratar el servicio objeto del presente contrato, con beneficios mismos que se aplican mediante promoción, deja expresa y válida constancia de que el presente Contrato tiene un tiempo mínimo de permanencia de 12 meses sucesivos contados a partir del momento la activación del servicio, y que en caso de terminar el contrato antes de cumplirse el tiempo mínimo de permanencia, tendrá que pagar a la empresa el valor correspondiente a la instalación como se detallará en el ANEXO 1, así como también la devolución de los equipos instalados en el mismo estado en el que se encontraban al momento de la instalación.

El abonado se acoge al periodo mínimo de permanencia

SI ◯

NO ◯

QUINTA. -RECLAMOS Y SOPORTE TÉCNICO,

En caso de necesitar soporte técnico mediante vía telefónica SITEC tiene disponibilidad las 24 horas al día, los 7 días de la semana y se puede comunicar a los números 096 945 3071 o 098 6641487. Si existiese un fallo o interrupción del servicio, el Abonado/Cliente deberá notificarlo inmediatamente de detectado al PROVEEDOR, quien se compromete a reportar al Abonado/Cliente sobre las causas del problema y proceder a su inmediata reparación con un tiempo máximo de respuesta para atención al Abonado/Cliente. El "PROVEEDOR no será sujeto de sanción o responsabilidad alguna por la aparición de cualquier daño directo, indirecto incidental, consecuencial, especial o de cualquier otro tipo que pueda acontecer al Abonado/Cliente, de sus dependientes, terceros, bienes, operaciones y/o negocios, en razón o con ocasión de los servicios que contrata, siempre que estos no se produzcan por negligencia, imprudencia, impericia, culpa o dolo del PROVEEDOR o sus dependientes, pues de ser así será responsable de aquellos. En el caso de incumplimiento o violaciones de los derechos de los abonados/clientes, reclamos o quejas que no han sido atendidos por el prestador del servicio, en relación con la calidad del servicio, facturación de servicios no contratados, pagos indebidos o en general por cualquier irregularidad en relación con el servicio contratado. Los abonados/clientes pueden presentar sus quejas o denuncias ante la ARCOTEL por los siguientes canales de atención: Atención presencial (Oficinas Coordinaciones Zonales de la ARCOTEL), PBX-Directo Matriz; Coordinaciones Zonales y oficinas técnicas, Call Center (llamadas gratuitas al número 1800-567567 o al número que designe la ARCOTEL), Correo Electrónico o Correo tradicional(oficios), Página web de la ARCOTEL:

(http://reclamoconsumidor.arcotel.gob.ec/osTicket/)

SEXTA. – TARIFAS Y FORMAS DE PAGO

En todos los casos la forma de pago aplicará únicamente en modalidad prepago, la tarifa del servicio será de acuerdo con el plan contratado y estará detallado en el formulario de cada servicio. El pago por la prestación del servicio será cancelado por los abonados/clientes en dinero: efectivo, depósito bancario o transferencia. El CLIENTE se reserva el derecho de elegir la forma de pago a conveniencia siempre y cuando se cumpla la fecha máxima de pagos (día 04 al inicio de cada mes). El mero retardo en el que incurra el Abonado/Cliente lo constituirá en mora, y dará derecho al PROVEEDOR de terminar de manera inmediata y unilateral el presente contrato o suspender el servicio. El Abonado/Cliente asumirá los gastos de desconexión y reconexión, así como los costos judiciales si los hubiere. Los clientes con discapacidades o de tercera edad, recibirán las tarifas preferenciales que les correspondan de acuerdo con la ley.

SÉPTIMA. - IMPUESTOS

De acuerdo con la legislación ecuatoriana, el PROVEEDOR incorporará al precio respectivo los impuestos que se causen por concepto de la prestación de servicios materia de este Contrato. Por consiguiente, la facturación reflejará el establecimiento de cualquier nuevo gravamen y los ajustes que se decreten en los existentes, en especial, toda modificación del impuesto al valor agregado (IVA) o Impuesto de Consumos Especiales (ICE) si fuese necesario.

NOVENA. — USO DE INFORMACION PERSONAL

Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora, salvo autorización y consentimiento expreso del abonado/suscriptor el que constara como instrumento separado y distinto el presente contrato de prestación de servicios a través de los medios físicos y electrónicos. En dicho documento se debe dejar constancia expresa de los datos personales o información que están expresamente

autorizados, el plazo de autorización y el objetivo que esta utilización persigue, conforme lo dispuesto en el artículo 121 del reglamento general a la Ley Orgánica de Telecomunicaciones

DÉCIMA. – RESPONSABILIDAD QUE NO ASUME EL PROVEEDOR

El PROVEEDOR no asume responsabilidad alguna en los siguientes eventos:

a) Por los daños y perjuicios que directa o indirectamente puedan ocasionar al Abonado/Cliente, la utilización de los programas, equipos y líneas de comunicación del PROVEEDOR.
b) Si uno, varios o todos los proveedores de equipos, líneas, servicios o información, de los que se vale el PROVEEDOR para el cumplimiento de este contrato, suspenden temporal o definitivamente, o total o parcialmente, tales equipos, líneas, servicios de información.
c) Si por reformas a las leyes, reglamentos, tarifas o por circunstancias de fuerza mayor o caso fortuito, el PROVEEDOR se ve impedido de continuar prestando sus servicios al Abonado/Cliente.
d) De las interceptaciones por terceros de la información encriptada o no encriptada que se maneje por las redes u otros mecanismos de comunicación y
e) De los virus informáticos o pestes que puedan transmitirse a través de redes. El abonado/Cliente no tendrá derechos o acciones de indemnización de daños y perjuicios, de pasado, presente o futuro, que reclamar o intentar en contra del PROVEEDOR.

DÉCIMA PRIMERA. – RESTRICCIONES DEL CLIENTE

Se deja expresa constancia que el PROVEEDOR no asume responsabilidad alguna por el uso que el Abonado/Cliente dé al servicio, aclarando que el Abonado/Cliente se hace responsable no sólo de sus propios actos sino de los de sus dependientes, agentes, familiares o terceros. Abonado/Cliente deja expresa constancia de que conoce la Ley Orgánica de Telecomunicaciones, Ley de Derechos de Autor, Ley de Propiedad Intelectual, y otras leyes conexas, así como los Reglamentos y Resoluciones vigentes sobre la materia, y de que está ilustrado sobre las facultades, impedimentos y prohibiciones determinados en estos cuerpos jurídicos, por lo que utilizará el servicio del PROVEEDOR ciñéndose estrictamente a los mismos. En consecuencia, el PROVEEDOR no asume responsabilidad alguna, ni directa ni indirecta, solidaria o subsidiaria, sobre las eventuales infracciones a las referidas disposiciones por parte del solicitante, quien para efectos de esta obligación contractual asume el deber de informarse permanentemente sobre las leyes y sus reformas que se “relacionen con el servicio que se brinda. Igualmente queda expresamente prohibido el acceso de personas no autorizadas al SISTEMA del PROVEEDOR que no sea por personal técnico calificado del mismo. Abonado/Cliente se hace responsable por el mal uso del plan contratado y asumirá las consecuencias económicas, civiles y penales a que hubiere lugar.

DÉCIMA SEGUNDA. – EVENTUALIDADES EN CASOS ESPECIALES

En el caso de que el Abonado/Cliente sea parte actora o demandada en cualquier juicio, litigio o controversia con los proveedores de información, o con cualquier otra persona natural o jurídica que tenga relación con las redes de información, se compromete a mantener indemne de tales juicios o litigios al PROVEEDOR. Además, el Abonado/Cliente se compromete a respetar y acatar todas las normas sobre derechos de propiedad o derechos de autor, especialmente los que rigen los programas de software y bases de datos vigentes en el Ecuador y en todos los países enlazados por el servicio.

DÉCIMA TERCERA. – SUSPENSIÓN Y REACTIVACIÓN DE SERVICIOS

Los servicios contratados podrán ser suspendidos debido a las siguientes causas:

a) Por falta de pago del abonado/cliente, se aplicará al día siguiente de cumplida la fecha máxima de pago.

b) Caso fortuito o fuerza mayor que obligue a la suspensión del servicio, calificada por la ARCOTEL, en este caso solo se podrá cobrar por los servicios efectivamente prestados.
c) Por uso indebido de los servicios contratados o uso ilegal de los mismos.
d) Por mandato judicial.

El servicio será reactivado sin que medie petición expresa en los siguientes casos:

a) Si la suspensión se debe a la falta de pago, el proveedor deberá reactivar automáticamente en un plazo de máximo 24 horas, contadas a partir del pago total de la deuda.
b) En los casos que la suspensión sea del tipo temporal, el proveedor deberá reactivar automáticamente al finalizar el periodo de suspensión.
c) En caso de robo, hurto o pérdida del equipo terminal la reactivación se hará dentro de las 24 horas siguientes a partir de la petición del abonado/suscriptor, previo al pago del equipo correspondiente, dicho valor será establecido de mutuo acuerdo en primera instancia.
d) Mandato judicial.

DÉCIMA CUARTA. – TERMINACIÓN DEL CONTRATO

El presente contrato podrá darse por terminado por cualquiera de las siguientes causas:

Por el prestador del servicio:

a) Si el Abonado/Cliente utiliza los servicios contratados para fines distintos de los convenidos o si los utiliza en prácticas contrarias a la ley.
b) Con previa notificación al Abonado/Cliente escrita con 30 días de anticipación si terceros que le proveen equipos, líneas o servicios los suspenden temporal o definitivamente, total o parcialmente.
c) Si el Abonado/Cliente está en desacuerdo con los nuevos valores que implemente la empresa a los servicios podrá dar por terminado este contrato.
d) Por vencimiento del plazo de vigencia del contrato, cuando no exista renovación.
e) En caso de que se reformen las leyes, reglamentos o tarifas en el Ecuador o en el exterior, o las instituciones competentes, nacionales o extranjeras dicten resoluciones que impidan al PROVEEDOR continuar brindando sus servicios.
f) Inmediatamente con notificación escrita, en caso de que el Abonado/cliente incumpla expresa o tácitamente cualquiera de las cláusulas consignadas en este contrato.
g) Por circunstancias de fuerza mayor o caso fortuito que obligue al proveedor a suspender temporal o definitivamente los servicios. Si el PROVEEDOR se encontrase impedido de prestar el servicio debido al caso fortuito o por causa de fuerza mayor debidamente comprobada el Contrato podrá ser terminado inmediatamente por cualquiera de las Partes mediante simple comunicación escrita cursada con 48 horas de anticipación sin incurrir en ninguna responsabilidad legal. Bajo esta circunstancia el PROVEEDOR no se responsabilizará por el lucro cesante.
h) Por injurias graves o amenazas irrogadas al PROVEEDOR o a los empleados del mismo que le representen.
i) Por falta de pago.
j) Por las demás causas previstas en el Ordenamiento Jurídico Vigente.

Por parte del Abonado/Cliente también podrá dar por terminado unilateralmente el contrato

a) En cualquier tiempo previa notificación por escrito con al menos 7 días de anticipación por cualquier medio físico o electrónico sin que para ello esté obligado a cancelar multas o recargas de valores de ninguna naturaleza, salvo saldos pendientes por servicios recibidos o solicitados hasta la terminación del contrato, esto es el valor proporcional a los 7 días siguientes a la notificación que el Abonado/Cliente aún tendrá servicio y previo pago del valor de instalación o beneficios de promoción tal como se manifiesta en la cláusula cuarta.
b) Por vencimiento del plazo de vigencia del contrato, cuando no exista renovación.
c) El Abonado/Cliente se compromete a prestar todas las facilidades para retirar el o los equipos utilizados para prestar este servicio, en caso de no hacerlo el PROVEEDOR se reserva el derecho de judicialmente demandar el acceso y retiro a dichos equipos o reclamar el pago por parte del Abonado/Cliente del valor de 250,00 (Doscientos cincuenta dólares americanos con 00/100) por el consto de los mismos. En consecuencia, se deja expresa constancia de que el presente contrato se constituye en un título ejecutivo de conformidad con el Código General de Procesos toda vez que contiene obligaciones claras, puras y determinadas entre las partes.
d) El contrato se extingue en caso de que el Abonado/Cliente fallece y se justifique su deceso.

DÉCIMA QUINTA. – CONTROVERSIAS

Este Contrato se rige por la legislación ecuatoriana. Para el caso de controversias en su aplicación o interpretación se observarán las siguientes disposiciones: Si el accionante fuere el CLIENTE, queda a su facultad privativa y discrecional el sujetarse a la Ley de Arbitraje y Mediación o al trámite verbal sumario ante los jueces competentes de la ciudad de Ibarra o de la ciudad en que el CLIENTE suscribe este documento. Por otra parte, si el accionante fuere el PROVEEDOR, queda a su facultad privativa y discrecional el sujetarse a la Ley de Arbitraje y

Mediación o al trámite verbal sumario ante los jueces competentes de la ciudad de Ibarra o de la ciudad en que el CLIENTE suscribe este documento.

Sea que el CLIENTE y/o el PROVEEDOR optaren por sujetarse a la Ley de Arbitraje y Mediación, se observarán las siguientes precisiones:

a) El proceso se llevará en la ciudad de Ibarra, ante la Cámara de Comercio de Ibarra, conforme su reglamentación interna.
b) El tribunal se constituirá con un solo árbitro, quien habrá de resolver en derecho.
a) El árbitro queda expresamente facultado para dictar medidas cautelares y para solicitar el auxilio que fuere necesario para ejecutar dichas medidas, en los términos previstos en el Art. 9 de la Ley de Arbitraje y Mediación.
b) Los costos y gastos en que se incurra, incluidos los honorarios profesionales pactados razonablemente, serán cubiertos por la Parte que fuere vencida. A pedido de la Parte, antes de dictar el respectivo laudo, el Tribunal tendrá facultades para regular dichos honorarios, si es que le parecieren considerablemente excesivos o exiguos, en consideración a la cuantía y circunstancias del caso que deban resolver.
c) Las Partes se comprometen a aceptar el Laudo Arbitral. Sin perjuicio del derecho conferido por la Ley ecuatoriana para que la Parte afectada pueda demandar la nulidad del laudo, en los casos taxativamente permitidos por dicha Ley, las Partes acuerdan que la Parte que dedujere un recurso de nulidad que fuere resuelto negativamente para ella, deberá cancelar a la otra Parte, a más de todas las obligaciones pendientes o generadas a esa fecha y de aquellas otras obligaciones que, por disposición de la ley, se generasen como efecto de dicha resolución negativa, una indemnización equivalente a la máxima tasa de interés convencional que hubieren generado la suma de todas las citadas obligaciones, desde la fecha de expedición del laudo impugnado, hasta la fecha de pago efectivo. Esta suma será mandada a pagar por el respectivo órgano o juez ejecutor.
d) De ser requerido, el respectivo laudo será ejecutado ante los jueces competentes de la ciudad de Ibarra o de la ciudad donde el CLIENTE suscribe la Solicitud de Servicio o del lugar en que se encontraren los bienes del ejecutado.

Las Partes declaran que las estipulaciones que anteceden constituyen un convenio arbitral, en los términos exigidos por la Ley de Arbitraje y Mediación y que, por tanto, no cabrá excepción alguna para el caso en que una de las Partes o ambas, decidan resolver sus controversias por medio de arbitraje.

DÉCIMA SEXTA. – CONSTANCIA Y RATIFICACIÓN.

Los comparecientes o quienes los representen legal y debidamente autorizados, una vez inteligenciados en el contenido y efectos del presente instrumento, libre y voluntariamente y por convenir a sus respectivos intereses, se ratifican en el para fe y constancia de lo cual suscriben a continuación en dos ejemplares de igual valor y contenido.

_____ _____

Representante Legal SITEC S.A.
Susana del Rocío León Gudiño
RUC: 1091784498001

SUSCRIPTOR
_____
C.I./RUC:_____

SERVICIO DE ACCESO A INTERNET

ANEXO 1

Fecha de suscripción del anexo:	De	De

Nombre de plan:

Red de Acceso:

Par de cobre		Fibra optica	
Coaxial		Inalambrico	

Tipo de cuenta

Residencial		Cibercafé	
Corporativo			

Velocidad (Kbps) (si existe velocidad máxima para acceso a internet en servidores internacionales y a travez del NAP local, se debe especificar):

Comercial de bajada		Comercila de subida	
Minima efectiva de bajada		Mínima efectiva de subida	

Nivel de compartición (1:1, 2:1, 4:1, 8:4)

El contrato incluye permanencia mínima	**Si**	**No**	**Tiempo**

Beneficios por permanencia mínima

Servicios adicionales que se ofrece:	**Si**	**No**	**Descripción**
Cuentas de correo electrónico			

Tarifas (*)

Valores a pagar por una sola vez

Valor instalación	USD
Plazo para instalar/activar el servicio (horas, días)	

Valores pago mensual

	Valor USD
Valor mensual	
Valor total	

Detalle otros valores

Ítem	**Valor USD**
Total otros valores	

Correo electrónico web para consulta de tarifas	Sitec.ec.sa@gmail.com
Correo electrónico para consulta calidad de servicio	Sitec.ec.sa@gmail.com

Notas (*) Las tarifas no incluyen impuestos de ley

Prestador **Abonado suscriptor**

Anexo D: Tabla de resumen de actividades realizadas

TEMA: Administración de las conexiones a Internet de los usuarios de la Empresa SITEC de la Ciudad de Ibarra en base a la Arquitectura AAA y el Protocolo PPPoE utilizando equipos Mikrotik

OBJETIVO	CUMPLIDO	NO CUMPLIDO
Diseño de proceso y arquitectura del proyecto	X	
Digitalización de Contratos y Creación de Base de datos	X	
Levantamiento de servidor Radius	X	
Creación de usuario PPPoE	X	
Configuración nuevo usuario en OLT	X	
Configuración PPPoE en Dispositivo Final	X	
Verificación de autenticación de Usuario a la red por PPPoE	X	
Configuración Daloradius	X	
Creación de Usuario Administrador	X	
Conexión Daloradius con Winbox	X	
Verificación de autenticación de Administrador por PPPoE	X	

Ing. Fernando Obando

Gerente SITEC S.A

Eliana Carolina Quinatoa Aguirre

Autor