ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Automatización de procesos de asignación de recursos en una red de proveedor de servicios de internet mediante simulación

Proyecto Integrador

Previo la obtención del Título de:

INGENIERO EN TELECOMUNICACIONES

Presentado por:

Patricio Darío Sellan Fajardo

Jeniffer Judith Urquiza Olivo

Guayaquil-Ecuador

Año 2022

DEDICATORIA

Este proyecto de titulación en primer lugar va dedicado a Dios quien es mi refugio y guía, a mi madre Jeniffer Olivo quien ha creído en mí desde siempre, me ha brindado su apoyo incondicional y me ha enseñado a luchar por mis sueños. A mi padre Norman y mis abuelitas Aurea y Olga, mi tía Ivonne, mis hermanas que a la distancia me llenaron de amor y me motivaron a seguir adelante.

Finalmente, una dedicatoria especial a Brayan y a mis amigos que hicieron de esta etapa llamada universidad más amena y son partícipes también de este logro alcanzado.

Jeniffer Judith Urquiza Olivo

Dedico este proyecto de titulación, en primer lugar, a Dios del cual proviene toda sabiduría y a mi abuelita, Angela Parra Vargas, ya que nunca ha salido de mi mente y corazón la promesa que le hice, y ha sido la principal motivación de llegar hasta este momento. En vida siempre me llenó de amor y me incentivó a ser un profesional. No se muere quién se va, solo se muere el que se olvida; por esta razón le dedico mi trabajo, en ofrenda a su cuidado y amor.

Patricio Darío Sellan Fajardo

AGRADECIMIENTO

Agradezco a mi profesor Ph.D. Francisco Novillo y mi tutora Mg. Verónica Soto quienes me guiaron y acompañaron durante el desarrollo de este proyecto y son parte fundamental del mismo. De igual manera a mi compañero Patricio Sellan por su responsabilidad y entrega para poder culminar con éxito lo propuesto.

Finalmente, un agradecimiento especial a mi madre por confiar en mí y ser mi acompañante durante estos años de estudio.

Jeniffer Judith Urquiza Olivo

AGRADECIMIENTO

En primer lugar, agradezco a Dios por haberme acompañado en toda mi carrera universitaria, a pesar de lo difícil que ha sido el camino, su mano y dirección nunca me desamparó durante este proceso. Un agradecimiento a mis Padres, Patricio Sellan y Juanita Fajardo, por nunca dejar de creer en mí y ser mi apoyo incondicional durante todo este tiempo; sus oraciones, sacrificios y paciencia me han ayudado a llegar hasta este momento.

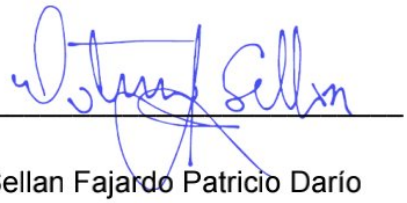
Gracias a mi amada, Martha Llerena, por recordarme siempre que se debe luchar hasta el final; ella es pilar fundamental y ha sido un soporte en el desarrollo de mi vida como estudiante. A mi amiga Ana Clara y a mis compañeros de trabajo quienes me apoyaron y motivaron a realizar este proyecto con éxito.

Finalmente, agradezco a mi profesor Ph.D. Francisco Novillo y mi Tutora Mg. Verónica Soto quienes me guiaron y acompañaron durante el desarrollo de este proyecto. Además, de ser parte fundamental del mismo. Al igual que mi compañera Jeniffer Urquiza por su gran esfuerzo, dedicación y responsabilidad para poder finalizar lo propuesto.

Patricio Darío Sellan Fajardo

DECLARACIÓN EXPRESA

"Los derechos de titularidad y explotación, nos corresponde conforme al reglamento de propiedad intelectual de la institución; Sellan Fajardo Patricio Darío y Urquiza Olivo Jeniffer Judith damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Sellan Fajardo Patricio Darío

Urquiza Olivo Jeniffer Judith

EVALUADORES

Firmado electrónicamente por:
FRANCISCO
VICENTE NOVILLO
PARALES

Ph.D. Francisco Novillo Parales

PROFESOR DE LA MATERIA

Firmado electrónicamente por:
VERONICA
ALEXANDRA SOTO
VERA

Mg. Verónica Soto

PROFESOR TUTOR

RESUMEN

Debido a la pandemia Covid-19 el uso de internet es indispensable para poder trabajar o estudiar, es por esto que el número de proveedores de internet ha crecido aproximadamente 21 veces a nivel nacional, como consecuencia existe una alta competencia en calidad, garantía de servicio y atención al cliente.

Los proveedores de servicio de internet buscan mejorar la experiencia del usuario atendiendo de forma oportuna los reclamos de los mismos, para esto es necesario una buena distribución del tiempo dentro del departamento de redes. Por ello se propone automatizar las tareas repetitivas realizadas al ejecutar el enrutamiento para proveer de internet al usuario y resolver conflictos de red que se dan por el crecimiento de la misma.

Una vez identificadas las tareas repetitivas por medio de un lenguaje de programación y la plataforma denominada RouterOS se automatiza estas tareas para posteriormente ser cargadas en el servidor del ISP, de tal manera que el tiempo de ejecución disminuya y el departamento de redes invierta este tiempo ahorrado en casos puntuales como la demanda de soporte técnico y mejorar la atención al cliente. Esto permitirá que el proveedor de servicios de internet gane eficiencia y competitividad dentro del mercado.

Palabras Claves: Covid-19, automatizar, tareas repetitivas, programación, ISP, usuarios, competitividad, tiempo, ahorro.

ABSTRACT

Due to the Covid-19 pandemic, the use of the internet is essential to be able to work or study, which is why the number of internet providers has grown approximately 21 times nationwide, due to this there is high competition in quality, guarantee of Service and customer support.

Internet service providers seek to improve the user experience by responding in a timely manner to user complaints, for this a good distribution of time within the network department is necessary. For this reason, it is proposed to automate the repetitive tasks carried out when executing the routing to provide the user with internet and resolve network conflicts that occur due to network growth.

Once the repetitive tasks have been identified by means of a programming language and the platform called RouterOS, these tasks are automated to later be uploaded to the ISP server, in such a way that the execution time decreases and the network department invests this saved time in specific cases such as the demand for technical support and improving customer service. This will allow the internet service provider to gain efficiency and competitiveness in the market.

Keywords: Covid-19, automate, repetitive tasks, programming, ISP, users, competitiveness, time, savings.

ÍNDICE GENERAL

ABREVIATURAS

ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
AS	Sistema Autónomo
BGP	Border Gateway Protocol (Protocolo puerta de enlace)
FTP	File Transfer Protocol (Protocolo de transferencia de archivos)
GPON	Gigabit Passive Optical Network (Red óptica pasiva Gigabit)
IP	Internet Protocol (Protocolo de internet)
IGRP	Interior Gateway Routing Protocolo (Protocolo vector distancia)
ISP	Internet Service Provider (Proveedor de servicios de internet)
NAT	Network Address Translation (Traductor de direcciones de red)
NOS	Network Operating System (Sistema de red operativo)
OSPF	Open Shortest Path First
PBR	Policy-Based Routing (Enrutamiento basado en políticas)
RIP	Protocolo de información de enrutamiento
TCP	Transfer Control Protocol (Protocolo de control de transmisión)
VLAN	Virtual Local Area Network (Red de área local virtual)
VPN	Virtual Private Network (Re d virtual privada)
VS	Versus

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

CAPÍTULO 1

1.1 Introducción

Ecuador consta de una población cercana a los 17.777 millones de habitantes, de los cuales el 57 % es decir un aproximado de 10.128 millones de habitantes tienen acceso a internet [1] además, se debe tomar en cuenta que la prestación de este servicio ha ido en aumento en el último año debido a la demanda que existe a causa de la pandemia COVID-19. Según la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) el número de proveedores de internet ha crecido aproximadamente 21 veces a nivel nacional, lo que ocasiona una alta competencia en calidad, garantía de servicio, atención al cliente, entre otros [2].

Debido a la alta competencia existente entre proveedores de servicio de internet, las empresas dedicadas a esto buscan mejorar la experiencia del usuario y así ganar competitividad en el mercado [3]. La empresa In.planet ubicada en la ciudad de Milagro tiene como principal objetivo dar soluciones a reclamos en el menor tiempo posible, de forma primordial a las quejas por soporte técnico suscitadas dentro del departamento de redes.

El presente proyecto de titulación tiene como objetivo automatizar los procesos de asignación de recursos en una red de proveedor de servicios de internet, esto se logra mediante la identificación de tareas reiterativas que ocurren dentro del departamento de redes [2], de esta manera se busca reducir el tiempo que el departamento dedica al proceso de enrutamiento y mantenimiento de la red para posteriormente ser usado en la demanda de soporte técnico y atención al cliente, mejorando la eficiencia y competitividad de la empresa [4].

El proyecto se ha dividido en cuatro capítulos, en el primer capítulo se expone la identificación del problema y la propuesta de solución. En el segundo capítulo se detalla el marco teórico donde se explican las definiciones más relevantes dentro del proceso de enrutamiento y los diferentes programas usados en la simulación. En el tercer capítulo se indica el proceso y algoritmos usados para lograr la automatización de las tareas reiterativas. Finalmente, en el capítulo cuatro se presentan los resultados y en base a esto las conclusiones obtenidas del proyecto.

1.2 Definición del problema

La empresa In.Planet, es un proveedor de internet residencial que presta servicios a la provincia de Guayas y Los Ríos, en esta empresa dentro del departamento de redes se realizan actividades como PBR (Policy- based routing), mantenimiento de la red y brindar soporte técnico al usuario [5]. Al momento de realizar el enrutamiento y dar mantenimiento a la red se realizan tareas reiterativas, las cuales se detallan a continuación:

- Creación de nuevos usuarios en los routers.
- Cambio de ruta o cargar PBR.
- Creación de un nuevo nodo.
- Consultas acerca de los módulos sfp+ en cada router.

Estas tareas repetitivas en conjunto con el crecimiento de la red al agregar nuevos usuarios, provocan que la respuesta al requerimiento de los mismos sea ineficiente, además, de generar conflictos en la red dando como resultado que la empresa pierda competitividad ante la demanda que representa el mercado dentro de la ciudad.

1.3 Justificación del problema

El crecimiento de los proveedores de internet ha hecho que las empresas dedicadas a prestar este servicio estén obligadas a mejorar la experiencia del usuario para ganar competitividad [2].

El objetivo de la empresa In.planet es dar soluciones a reclamos de los usuarios en el menor tiempo posible, de forma primordial a las quejas por soporte técnico suscitadas dentro del departamento de redes, tratando de reducir al máximo las actividades repetitivas que se realizan al momento de ejecutar el enrutamiento para proveer de internet, dar mantenimiento y evitar conflictos de red ante el crecimiento de la misma.

La empresa requiere una herramienta que le permita automatizar las tareas reiterativas para disminuir el tiempo que el departamento de redes ocupa en las mismas y que también le ayude a resolver los conflictos suscitados dentro de la red [6]. De esta manera con el tiempo ahorrado

pueda cubrir casos puntuales como solventar de manera eficiente la demanda de soporte técnico y mejorar la atención al cliente.

1.4 Objetivos

1.4.1 Objetivo general

Implementar los algoritmos mediante el servidor de la empresa In.Planet para automatizar las tareas reiterativas.

1.4.2 Objetivos específicos

- Identificar las tareas reiterativas que existen dentro de la empresa In.planet.
- Simular el escenario de la red.
- Elaborar algoritmos para automatización de tareas reiterativas de la empresa.

1.5 Metodología

En primer lugar, se identifican las tareas que más se repiten dentro del departamento de redes de la empresa In.planet y se registra el tiempo que toma hacerlas de forma actual es decir, sin automatización.

` Una vez identificadas estas tareas se procede a investigar qué lenguaje de programación es el más fiable para usar en conjunto con el servidor que maneja la empresa antes mencionada.

Posteriormente se realiza la simulación de la red con características similares a las que tiene la empresa In.planet y se crean algoritmos que permiten automatizar las tareas que al desempeñarlas de forma repetitiva demandan mayor tiempo y puedan crear conflicto en la red. Finalmente, estos algoritmos son implementados dentro de la red por medio de un servidor para luego poder realizar pruebas, comprobar la automatización de tareas y presentar los resultados obtenidos.

1.6 Resultados esperados

Una vez simulada la red con características similares a las de la empresa In.planet e implementados los algoritmos que permiten automatizar las tareas, es decir las tareas que se hacían de forma repetitiva ahora mediante los algoritmos se realizarán de forma automática. Con la automatización de tareas se espera que existan menos conflictos de red suscitados por el crecimiento de la misma y reducción del tiempo que se emplea en ejecutarlas. De esta manera el departamento de redes podrá asistir de forma eficaz la demanda de soporte técnico, permitiendo que la empresa gane competitividad.

CAPÍTULO 2

2.1 Marco teórico

2.1.1 Proveedor de servicios de internet (ISP)

ISP (Internet Service Provider) son empresas u organizaciones que empezaron a surgir a inicio de 1990 las cuales se dedican a dar acceso a internet por medio de distintos protocolos [7]. Un ISP se encarga de proveer de internet a varios clientes como se presenta en la figura 2.1 además, parten de un sistema jerárquico el cual se basa en la conectividad que existe al backbone de internet es decir, que los niveles inferiores se conectarán a un nivel superior del ISP mediante el backbone [8].

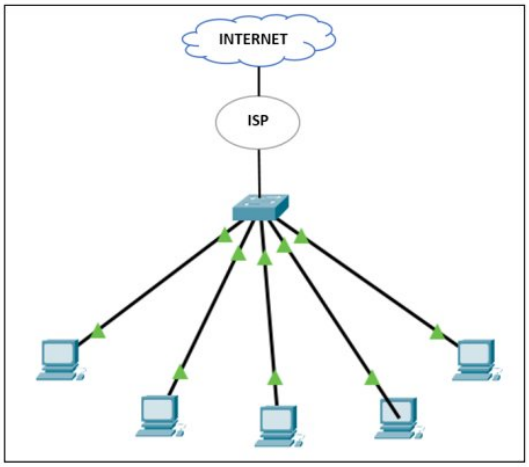


Figura 2.1 Ejemplo de ISP

A continuación, se enlistan algunos tipos de ISP:

- ISP de acceso: Son aquellos que usan distintas tecnologías para agilizar la conexión de los clientes. Dentro de estas tecnologías están conexión por línea conmutada o banda ancha, cable compuesto, conexión por fibra entre otros.
- ISP de buzón de correo: Los ISP que se dedican a buzón de correo también son proveedores de acceso, pero estos específicamente se dedican a ofrecer servidores de buzón para email los cuales se encargan de enviar y recibir mensajes.

- ISP de servidores: Su oferta es más amplia ya que dentro de esta se encuentra el protocolo de Transferencia de archivos (FTP), máquinas virtuales, servidores cloud y físicos.
- ISP de tránsito: Entregan un ancho de banda más amplio el cual es primordial para conectar los ISP de servidores y tener acceso en conjunto a los mismos.
- ISP virtuales: Son aquellos que compran servicios a diferentes ISP y así pueden ofrecer a sus clientes acceso a internet.
- ISP gratuitos: Aquellos a los que se acceden de forma gratuita pero que para prestar el servicio constantemente enseñan anuncios.

2.1.2 Protocolos de enrutamiento

La creación de rutas estáticas genera conflictos cuando la red empieza a expandirse debido a que, el administrador de la misma debe reconfigurar cada uno de los routers ante posibles cambios dentro de la red. Por esta razón lo más factible es usar el enrutamiento dinámico el cual se adapta a los cambios de la red y se actualiza de forma constante [9]. Los protocolos de enrutamiento son aquellos que se encargan de mantener actualizadas las tablas de encaminamiento y además, ayudan a determinar la mejor ruta para enviar paquetes. Dentro de este proyecto se usa el protocolo de enrutamiento BGP y OSPF. A continuación, se explican los protocolos de enrutamiento que se usan con más frecuencia:

- RIP: Rounting Information Protocol, es un protocolo de enrutamiento dinámico que usa un algoritmo de vector-distancia el cual determina la mejor ruta para enviar el paquete al destino deseado, este protocolo maneja una lista que contiene la información sobre las rutas la misma que es compartida entre los routers vecinos en un lapso de 30 segundos [10].
- IGRP: Interior Gateway Routing Protocol es un protocolo de enrutamiento patentado por Cisco, al igual que RIP también es considerado como un protocolo de métrica vector-distancia. El IGRP se basa en métricas compuestas en donde se considera el ancho de banda, la carga, el retardo y la confiabilidad. Se envía un mensaje de las actualizaciones realizadas en la red cada 90 segundos [11].
- OSPF: Open Shortest Path First es un protocolo que usa un algoritmo tipo enlace, este protocolo es óptimo para ser usado en redes de gran tamaño debido a que

trabaja con sistemas autónomos los cuales pueden mantenerse separados y de esta forma disminuir el tráfico transmitido. Una de las mayores ventajas de OSPF es la facilidad con la que puede recalcular las rutas si la topología de red presenta algún cambio [10].

- BGP: Border Gateway Protocol permite el enrutamiento basado en políticas. Es conocido por su escalabilidad y por el uso de sistemas autónomos para poder intercambiar información. Usa directivas de enrutamiento para elegir entre varios caminos hasta lograr llegar al destino y de esta forma controla la distribución de la información.

2.1.3 Protocolos de red

Los protocolos de red son aquellas reglas que hacen posible la comunicación entre los dispositivos que pertenecen o están conectados a una red. Estás reglas contienen instrucciones las cuales les permite a los dispositivos entrar en comunicación sin ningún conflicto, existe también la conocida regla de formateo la cual se basa en verificar si los datos fueron recibidos, rechazados o tuvieron algún problema para poder completar con éxito la transferencia de información [12]. Los protocolos de red que son necesarios saber dentro de este proyecto de titulación son los siguientes:

- IP: Internet Protocol es un estándar que contiene todas las especificaciones necesarias y reglas que ayudan al funcionamiento de los dispositivos que se encuentran conectados a internet.
- TCP: Transmission Control Protocol se asocia con IP debido a que se encarga de garantizar que los datos se transmiten adecuadamente a través de Internet. La función principal es respecto a la seguridad ya que, se encarga de asegurar que el tráfico llegue a su destino sin que exista pérdida de información. [12].
- DNS: El sistema de nombres de dominio es el encargado de traducir e interpretar nombres de dominio a direcciones IP. Adicionalmente se tiene que tener en cuenta que cada proveedor de servicios de internet cuenta con sus propios nombres de dominio y son estos los que proveen al momento de usar el servicios sin embargo, es posible utilizar DNS alternativos.

Además, dentro de los protocolos de red es importante mencionar a los sistemas autónomos (AS) los cuales se conocen como una colección de prefijos del protocolo IP

asociados con una política de enrutamiento claramente definida que gobierna cómo el AS intercambia información de enrutamiento con otros sistemas autónomos [13]. Esto quiere decir que un AS puede considerarse como un grupo conectado de redes IP administradas por una sola entidad, cabe mencionar que dentro de la configuración de los equipos es necesario usar AS en la red que trabaja con BGP.

2.1.4 Sistema operativo de red

Un sistema operativo de red es capaz de soportar estaciones de trabajo como computadoras, terminales o algún dispositivo que esté conectado a una red local. El software de un sistema operativo de red o Network Operating System (NOS) es indispensable ya que, permite que todos los dispositivos que comparten una red se puedan comunicar entre sí [14]. En este caso el estudio del sistema operativo de red se centrará en RouterOS el cual es un software que funciona como un sistema operativo que hace posible que una computadora o placa Mikrotik pueda convertirse en un router virtual es decir, cumplirá las funciones de un router real pero el costo será inferior adicionalmente se encuentra en constantes actualizaciones. Las aplicaciones dentro de RouterOS son: balanceo de conexiones de red de banda amplia (WAN) y enlaces punto a punto que permiten alcanzar zonas más grandes de cobertura logrando ofrecer mejor calidad y ampliar progresivamente el ISP [15].

2.1.5 Plataformas de automatización

Las plataformas de integración y automatización de tareas o del flujo de trabajo facilitan la realización de procesos complejos o que puedan demandar mucho tiempo, además, existen plataformas que se pueden conectar con la nube de internet ampliando el campo de aplicaciones. La automatización da como resultado la optimización del trabajo repetitivo ahorrando tiempo y dinero. Existen diversas plataformas de automatización como Zapier, Integromat, Ansible en esta última se centra este proyecto [16].

Ansible es de acceso libre, se centra en la infraestructura ya que, automatiza los procesos referentes a construcción de redes. Se encarga de gestionar configuraciones, organizar sistemas, crear programas entre otros procedimientos de telecomunicaciones [17]. Ansible tiene una conexión directa con los nodos y les inserta pequeños programas

a los cuales se los llama módulos estos a su vez permiten llevar a cabo tareas de automatización en la plataforma. Luego ejecuta los programas que funcionan como modelos de recursos del estado deseado de los sistemas y al finalizar la tarea los retira. Por medio del protocolo SSH (Secure SHell) encargado del acceso remoto, puede conectarse a los servidores y ejecutar las tareas, una de las ventajas de la plataforma de automatización es que el administrador de red o programador puede crear módulos de su autoría en varios lenguajes, en este caso el lenguaje a usar es el de Python.

2.1.6 Redes ópticas pasivas

Las redes ópticas pasivas (PON) son redes compuestas por fibra óptica en donde los componentes son en su mayoría pasivos dentro de la red de distribución es decir fuera de la central y domicilio del cliente [18]. Es un tipo de red conocida y caracterizada porque tiene una gran variedad de aplicaciones. Además, es recursiva debido a que permite compartir una misma fibra entre varios usuarios. Dentro de esta tecnología la máxima distancia se establece entre un terminal de línea óptica (OLT) y un equipo de unidad de red óptica (ONU) el cual es un dispositivo encargado de convertir las señales ópticas que pasan a través de la fibra en señales eléctricas, una red debe tener no más de 20 Km para que la red óptica pasiva sea operativa. Con las redes Ethernet activas este límite cambia y aumenta la distancia a más 80 Km desde el punto de distribución hasta el usuario adicionalmente del equipamiento activo durante el trayecto. El objetivo que tiene este tipo de sistema es eliminar todos los componentes activos que puedan existir entre el servidor y el cliente y reemplazarlos por componentes ópticos pasivos para dirigir el tráfico por la red, cuyo elemento principal es el dispositivo divisor óptico el cual se lo conoce como splitter [19].

La utilización de estos sistemas pasivos son de mucha ayuda a nivel económico ya que, reduce considerablemente los costes y son utilizados en las redes FTTX (Fiber to the x) [20]. Además, es importante mencionar que el ancho de banda no es dedicado, sino multiplexado en una misma fibra existen varios usuarios.

2.1.7 Componentes de la red

- Router: Es un dispositivo conocido y usado para la conmutación de redes, el cual se encarga de enrutar paquetes de red, según sus direcciones, a otras redes o dispositivos. Se utilizan principalmente para el acceso a Internet, acoplar redes o para conectar sucursales a una oficina central a través de VPN (Red Privada Virtual) [21].
- Switch: Es el encargado de reenviar paquetes de datos entre dispositivos, opera en la capa 2 es decir, en la capa de enlace de datos por lo tanto admite cualquier tipo de protocolos de paquetes. El conmutador perteneciente a capa 2 también se lo conoce como puente, cumple con la función de enviar tramas que contienen paquetes de datos entre nodos o segmentos de una red.
- Nodo: es un punto donde empieza la redistribución de información o un punto donde termina. La definición de un nodo siempre dependerá de la red donde se desarrolle y a la capa a la que pertenece. Un nodo es capaz de crear, recibir o transmitir información por medio de un canal de comunicación [22].
- Vlan: Son redes de área local las cuales permiten crear redes lógicas independientes dentro de una misma red física. Una vlan se usa principalmente para segmentar la red de forma adecuada lo cual ayuda a usar cada subred de forma diferente. Según las necesidades una vlan puede permitir o denegar el tráfico entre ellas dentro de la red.
- PBR: Enrutamiento basado en políticas es una técnica que permite reenviar y enrutar paquetes de datos según políticas o filtros. Los administradores de redes pueden aplicar políticas según las necesidades de la red proporcionando parámetros específicos, como la dirección IP de origen o destino, el puerto de origen o destino, la clase de tráfico, los protocolos, el tamaño de paquete y así lograr enrutar los paquetes en rutas definidas por el usuario. Teniendo como principal objetivo hacer la red más ágil y poder encontrar la mejor ruta de forma más eficaz [23].

CAPÍTULO 3

3.1 Descripción del escenario

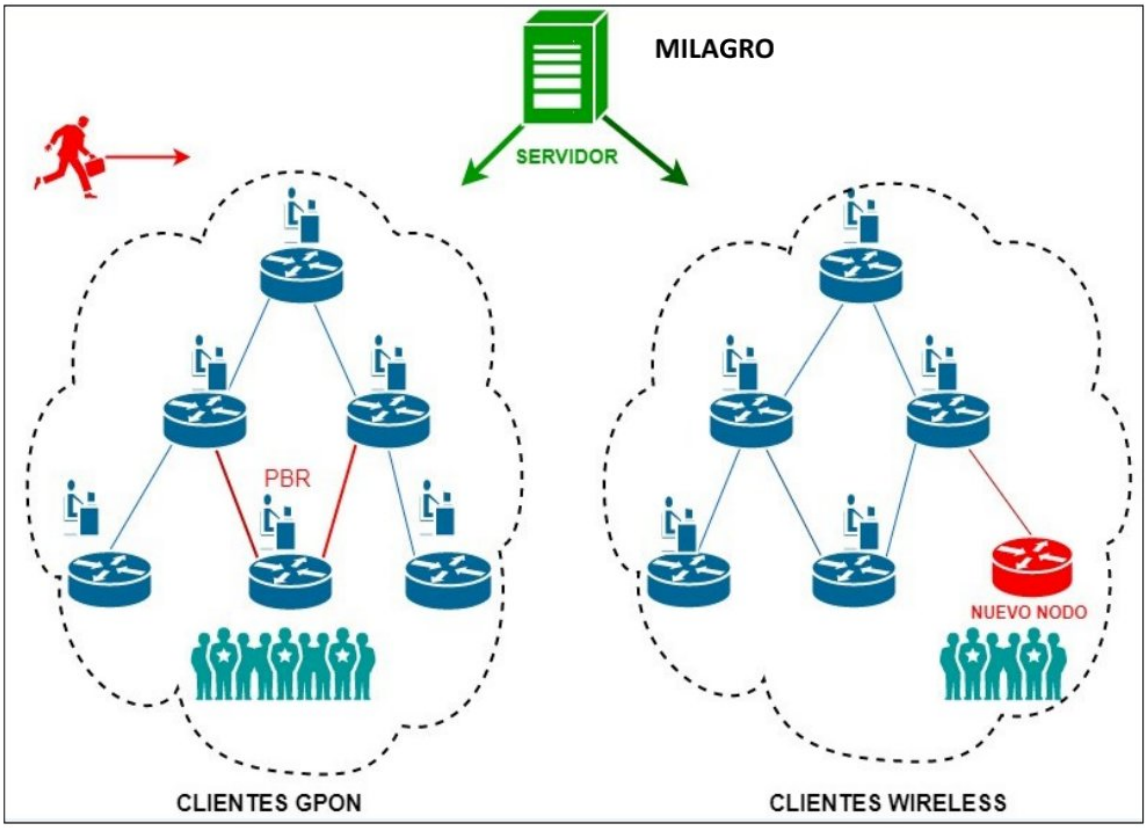


Figura 3.1 Descripción del escenario

El escenario del proyecto de titulación se visualiza en la figura 3.1 donde se muestra como está divida la red del proveedor de servicios de internet la cual se encuentra ubicada en la ciudad de Milagro. El ISP se encarga de brindar internet por medio de fibra óptica a distintas ciudades de la provincia de Guayas y Los Ríos. Esta red se divide en dos, una parte identificada como clientes GPON y la otra como clientes Wireless. Debido al crecimiento que existe dentro de la red ocasionado por el aumento en la demanda de clientes, existen tareas que se realizan de forma repetitiva como: creación de un nodo, cambio de ruta o PBR, consultas sfp y creación de usuarios, en estas tareas se invierte mucho tiempo y al no realizarlas de forma correcta pueden causar indisponibilidad de la red o conflictos en la misma haciendo que el ISP pierda competitividad y eficacia ante los usuarios.

3.2 Desarrollo de tareas de forma actual

El ISP para llevar a cabo las tareas repetitivas utiliza la consola de MikroTik la cual se presenta en la figura 3.2.

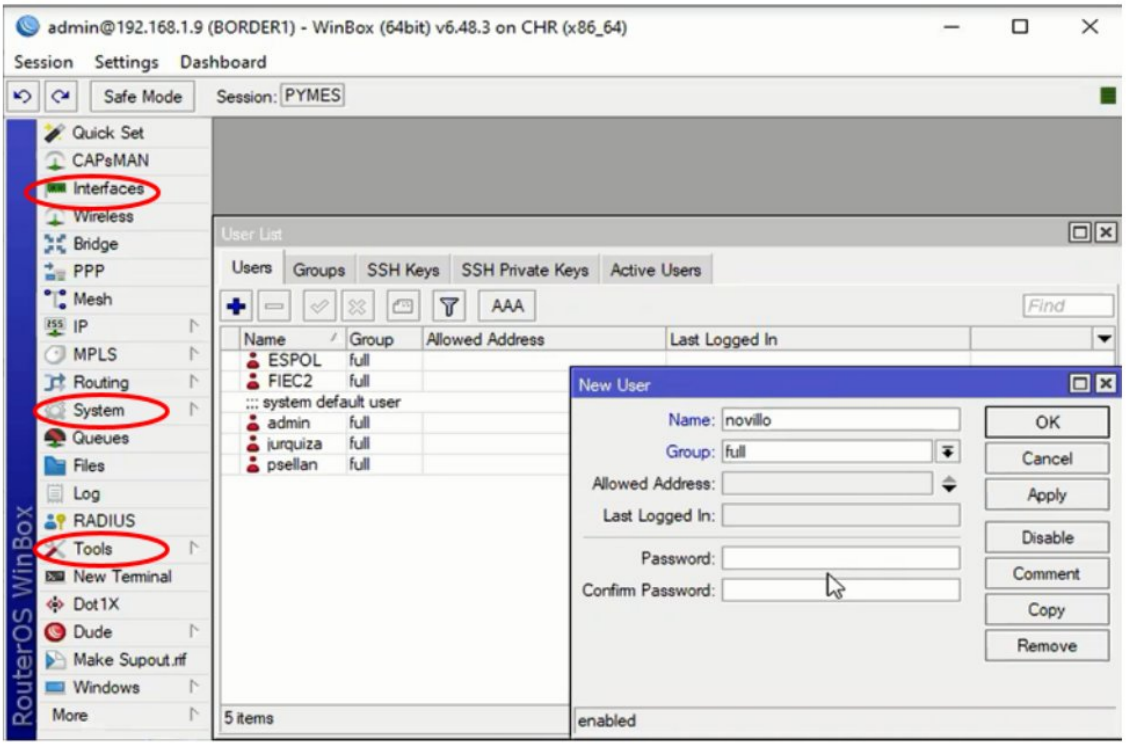


Figura 3.2 Entorno de MikroTik

Dentro de este entorno existen pestañas de gran utilidad como System, Tools, Interfaces, entre otras señaladas dentro de la figura 3.2, por lo que el administrador de red debe identificar y conocer el funcionamiento de cada una, de esta manera podrá desarrollar los procesos necesarios para las distintas tareas que se desempeñan dentro del ISP. En este caso sólo se ha enfocado la atención a las tareas que más se repiten y aquellas que ayuden a resolver algún conflicto de red para poder automatizarlas y así reducir el tiempo que se invierte en ellas. Es conveniente efectuar un análisis de las tareas que se hacen de forma actual es decir sin automatización dentro del ISP y evaluar el tiempo invertido para posteriormente realizar una comparación con las tareas automatizadas y poder obtener resultados.

3.2.1 Creación de usuario de forma actual

Para crear un usuario de forma actual se debe seguir los pasos que me muestran en el diagrama de bloques de la figura 3.3 como se explicó anteriormente se lo realiza por medio de consola de MikroTik.

Figura 3.3 Pasos para crear un usuario de forma actual

Este diagrama consta de ocho pasos y la mayoría de estos se desarrollan dentro la pestaña system. Asignar usuario hace referencia a colocar el nombre con el que se reconocerá al mismo, mientras que el tipo de usuario indica los permisos que se le conceden al nuevo usuario dentro de la red, estos pueden ser leer, escribir, full siendo el último el que cuente con todos los permisos para realizar cambios en la red.

Cabe mencionar que de esta forma se crea el usuario solo en el router que se haya elegido, para que el administrador tenga acceso al resto de routers pertenecientes a la red con el nuevo usuario este deberá ser creado en cada uno de los routers repitiendo los pasos que se muestran en la figura 3.3 así sea asignado como usuario full.

Al realizar este proceso el administrador se demora aproximadamente 60 segundos en crear un usuario por router, es decir que si la red tiene 10 routers, el tiempo invertido aumenta 10 veces más.

3.2.1 Cargar PBR o cambio de ruta de forma actual

Uno de los problemas recurrentes dentro de un ISP es el crecimiento de la red ya que, debido a esto pueden existir diversos colapsos de la misma que pueden ocasionar pérdidas de paquetes, por esta razón se busca cargar PBR o realizar cambio de rutas en la red cuando sea necesario. Con esto el administrador de red aplica ciertas políticas para enrutar los paquetes en rutas que estén definidas.

A continuación, en la figura 3.4 se muestra el escenario de un nodo colapsado y posteriormente la inhabilitación de red.

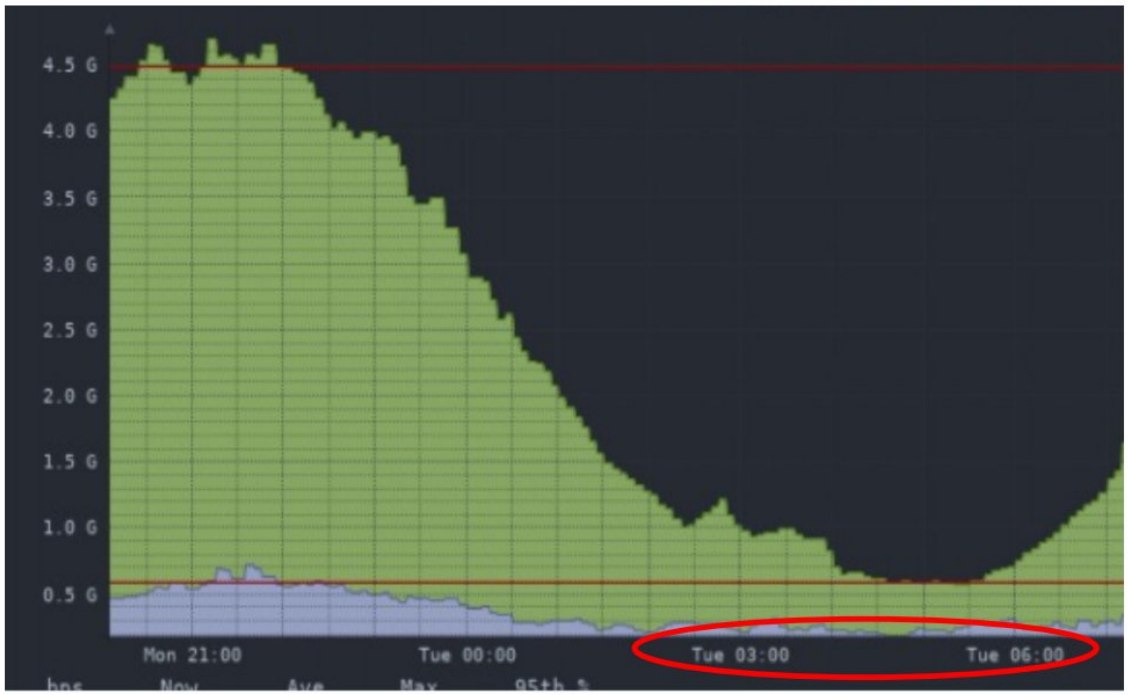


Figura 3.4 Nodo colapsado y posterior caída

Existen dos escenarios que se manejan dentro del ISP al momento que ocurre la caída de red, el escenario sencillo es cuando el administrador de red realiza el cambio de ruta por medio de la consola es decir, se ha identificado hacia qué ruta se puede enviar el tráfico bajo la premisa de prueba y error, este proceso lleva un tiempo

aproximado de 240 segundos, mientras que el escenario más complejo es cuando el administrador de red no encuentra la mejor ruta para desviar el tráfico y se debe ir al lugar del inconveniente dando como resultado una indisponibilidad de servicios de red aproximada de 3 horas como se visualiza en la figura 3.4 la cual evidencia que el tráfico ha disminuido en gran medida desde las 3 hasta las 6.

Para cambiar de ruta por medio de consola se deben seguir los pasos mostrados en la figura 3.5 la cual describe el número de pasos necesarios para llevar a cabo dicha tarea.

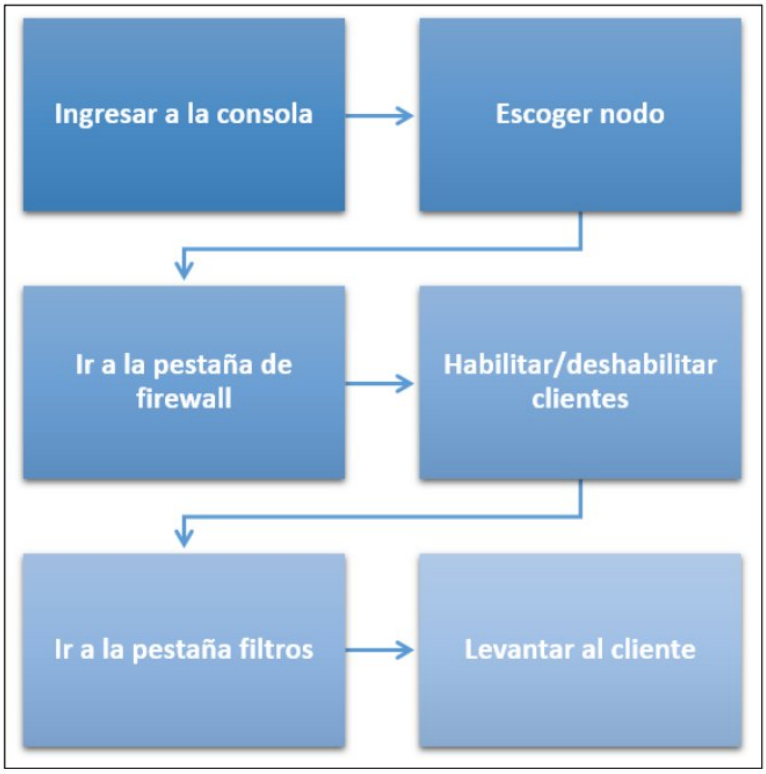


Figura 3.5 Pasos para realizar cambio de ruta de forma actual

Como se muestra en la figura 3.5 se necesita identificar el nodo del problema además, tener conocimiento de los clientes que se encuentran en la lista de direcciones del firewall y cuáles deben ser habilitados o deshabilitados para poder aplicar filtros y posteriormente levantar el cliente. Con este método la forma sencilla de cargar PBR o cambiar ruta se realiza en 6 pasos y un aproximado de 240 segundos.

3.2.3 Creación de nodo de forma actual

Debido al incremento de la demanda de usuarios de internet, los ISP se ven obligados a extender la red por lo que es necesario crear nodos y de esta manera proveer el servicio a nuevos usuarios.

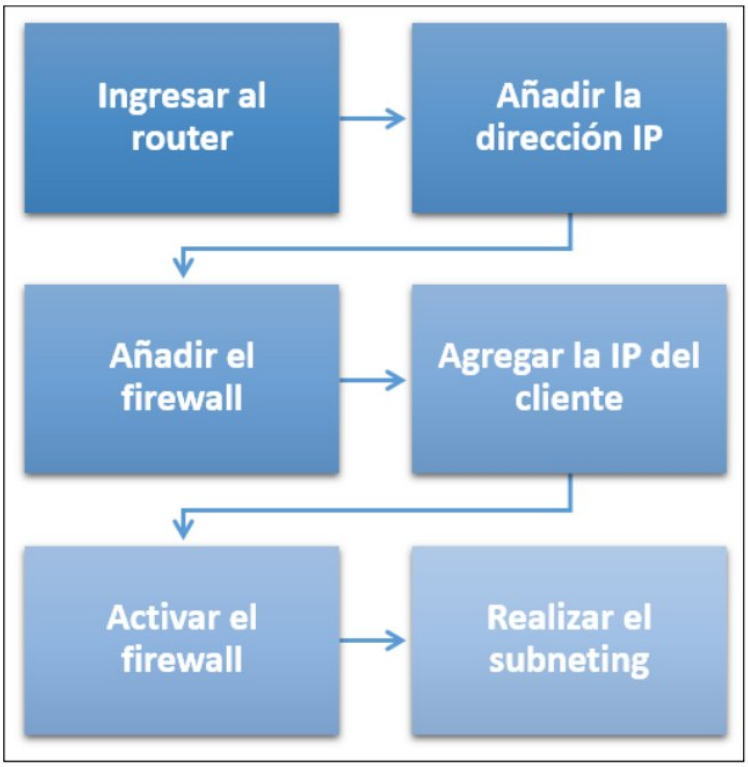


Figura 3.6 Pasos para la creación de un nodo de forma actual

En la figura 3.6 se observan los pasos para poder realizar la creación de un nodo de forma actual, para esto se deben ejecutar 6 pasos, en primer lugar el administrador de red debe ingresar al router, agregar la dirección IP que desee añadir, colocar la puerta de enlace (gateway), escribir la dirección del cliente con el que hará nat es decir, tener salida a internet mediante una IP pública y activar el firewall, aquí es importante acotar que se debe realizar un subneteo para saber con qué direcciones IP se trabajará en ese nodo. Llevar a cabo esta tarea de forma actual toma un tiempo aproximado de 600 segundos.

3.2.4 Consultas de SFP+ en cada router de forma actual

Para llevar un control de los nodos y evitar que estos colapsen se deben realizar de forma constante consultas de spf en cada una de las interfaces de los routers. En este caso se lo realiza mediante la ventana denominada PuTTY con el usuario y contraseña del administrador de red, se realizan los 4 pasos mostrados en la figura 3.7.

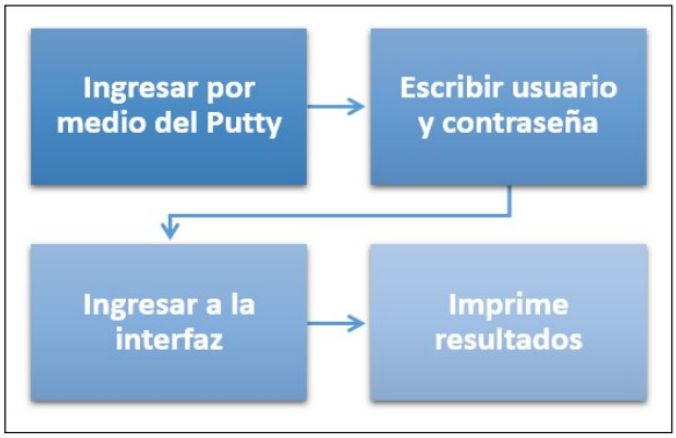


Figura 3.7 Consultas sfp en los routers

La información que brinda las consultas de spf se puede apreciar en la figura 3.8 la cual proyecta la cantidad de paquetes que se envían por segundo, la transmisión de datos, los errores entre otros, este proceso se debe repetir a partir del paso 3 mostrado en la figura 3.7 para cada una de las interfaces del router, en este caso los routers cuenta aproximadamente con 13 interfaces, es decir que el tiempo invertido en esta tarea es aproximadamente de 30 segundos por interfaz, por lo tanto para consultar el estado de todas las interfaces el tiempo empleado sería 13 veces más o dependerá de la cantidad de interfaces que exista en cada router.

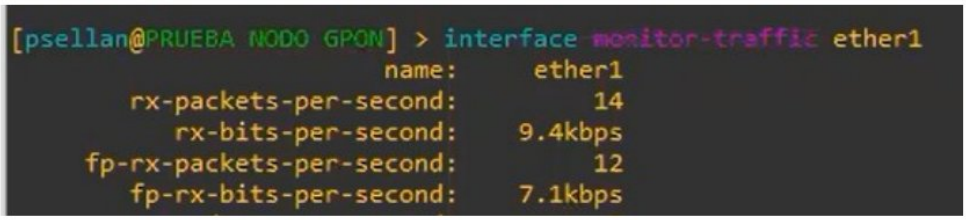


Figura 3.8 Información de la interfaz brindada por sfp

3.3 Simulación de la red

Para lograr automatizar las tareas que se repiten, es necesario simular la red correspondiente al ISP. En la figura 3.9 se muestra la topología de red usada para automatizar las tareas identificadas como repetitivas por medio del servidor encerrado de color naranja y la adición de un nuevo nodo debido al crecimiento de la red.

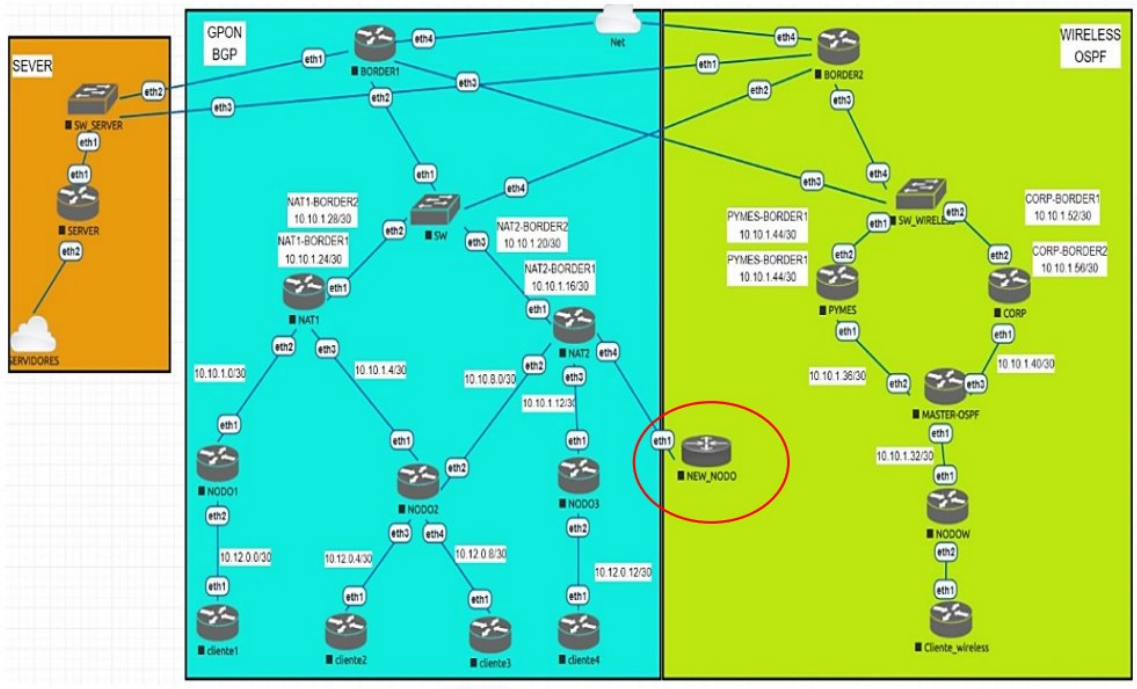


Figura 3.9 Topología de la red del ISP

La topología de la red correspondiente al ISP se desarrolló en un software de acceso libre, cuenta con servidores, switches y routers los cuales necesitan distintas configuraciones para poder estar conectados entre sí y además, tener acceso a internet. Esta red se divide en 3 partes, en la parte izquierda se encuentran los servidores, la red encerrada en un cuadro turquesa es la denominada red GPON la cual usa el protocolo de enrutamiento BGP mientras que la parte delimitada por el cuadro verde es la red Wireless que usa el protocolo OSPF para el enrutamiento. Posteriormente sobre esta topología se realizarán las respectivas pruebas para analizar el funcionamiento de la red con las tareas automatizadas.

3.3.1 Asignación de direccionamiento IP de la red

Una vez construida la topología es necesario crear un direccionamiento IP para poder configurar los equipos, verificar las conexiones entre sí y comprobar el acceso a internet.

Tabla 3.1 Direccionamiento IP red GPON

/30	
ROUTER	**IP**
NODO1-NAT1	**10.10.1.0**
NAT1	10.10.1.1
NODO1	10.10.1.2
Broadcast	10.10.1.3
NODO2-NAT1	**10.10.1.4**
NAT2	10.10.1.5
NODO2	10.10.1.6
Broadcast	10.10.1.7
NODO2-NAT2	**10.10.1.8**
NAT2	10.10.1.9
NODO2	10.10.1.10
Broadcast	10.10.1.11
NODO3-NAT2	**10.10.1.12**
NAT2	10.10.1.13
NODO3	10.10.1.14
Broadcast	10.10.1.15
NAT2-BORDER1	**10.10.1.16**
BORDER1	10.10.1.17
NAT2	10.10.1.18
Broadcast	10.10.1.19
NAT2-BORDER2	**10.10.1.20**
BORDER2	10.10.1.21
NAT2	10.10.1.22
Broadcast	10.10.1.23
NAT1-BORDER1	**10.10.1.24**
BORDER1	10.10.1.25
NAT1	10.10.1.26
Broadcast	10.10.1.27
NAT1-BORDER2	**10.10.1.28**
BORDER2	10.10.1.29
NAT1	10.10.1.30
Broadcast	10.10.1.31

Como se explicó anteriormente en la topología de red mostrada en la figura 3.9, la red denominada GPON está compuesta por routers, switches que han sido configurados con el pool de direcciones que se presenta en la tabla 3.1 la cual indica las direcciones IP correspondientes para cada uno de los dispositivos, los cuales van a ser alcanzables desde el router server para lograr conectividad entre ellos. Mientras que la red Wireless tiene el direccionamiento que se muestra en la tabla 3.2 denominada direccionamiento IP de la red Wireless mostrada a continuación:

Tabla 3.2 Direccionamiento IP de la red Wireless

/30	
Router	**Ip**
NODOW-MOSPF	**10.10.1.32**
MOSPF	10.10.1.33
NODOW	10.10.1.34
Broadcast	10.10.1.35
MOSPF-PYMES	**10.10.1.36**
PYMES	10.10.1.37
MOSPF	10.10.1.38
Broadcast	10.10.1.39
MOSPF-CORP	**10.10.1.40**
CORP	10.10.1.41
MOSPF	10.10.1.42
Broadcast	10.10.1.43
PYMES-BORDER1	**10.10.1.44**
BORDER1	10.10.1.45
PYMES	10.10.1.46
Broadcast	10.10.1.47
PYMES-BORDER2	**10.10.1.48**
BORDER2	10.10.1.49
PYMES	10.10.1.50
Broadcast	10.10.1.51
CORP-BORDER1	**10.10.1.52**
BORDER1	10.10.1.53
CORP	10.10.1.54
Broadcast	10.10.1.55
SERVER-BORDER2	**10.10.1.64**
BORDER2	10.10.1.65
SERVER	10.10.1.66
Broadcast	10.10.1.67

Las tablas 3.1 y 3.2 muestran las direcciones IP más importantes que se usaron dentro de la configuración de la red, si desea más información sobre las direcciones usadas se adjuntan las tablas completas en el anexo B, el cual muestra a detalle las direcciones IP usadas para cada componente de la red visualizada en la figura 3.9.

3.3.2 Configuración de la red

Una vez que se creó el pool de direcciones IP se procede a configurar cada uno de los equipos que pertenecen a la red. Se presenta como ejemplo la configuración del router Border 1 el cual se encuentra en la parte superior de la figura 3.9. Se configuraron las interfaces del router las cuales tienen su respectiva sub-interfaz y vlan como se muestra en la figura 3.10, la nomenclatura empleada es la que usa generalmente el ISP.

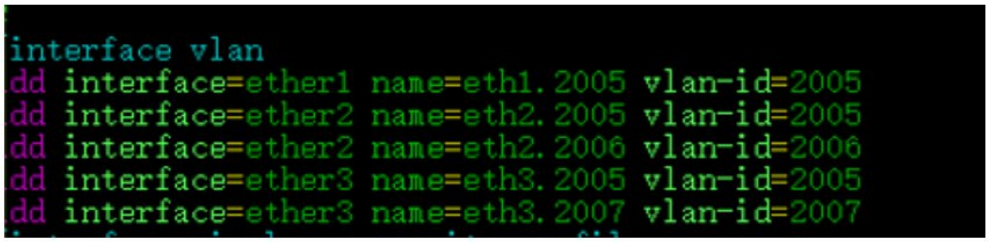


Figura 3.10 Creación de Vlan en Border 1

Dentro del router Border 1 también se configuraron las direcciones IP que este administra, en la figura 3.11 se muestra a detalle la asignación de direccionamiento con el nombre correspondiente y la interfaz a la que corresponde. Además, se indican las direcciones de los routers: Corp, Nat 1, Nat 2 entre otros.

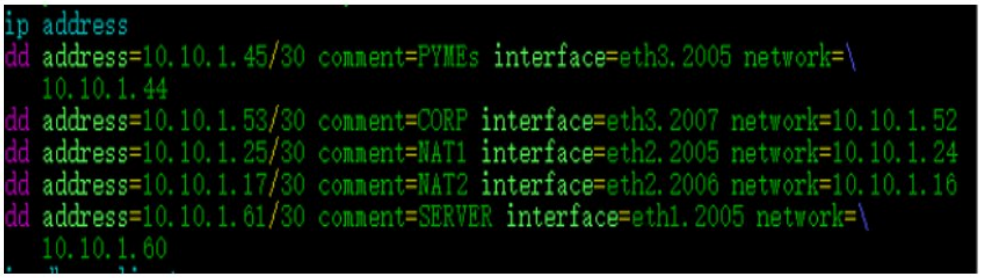


Figura 3.11 Asignación de direccionamiento IP

BGP que es el protocolo de enrutamiento a usarse para la red denominada GPON también debe ser configurado dentro del router Border 1 como se muestra en la figura 3.12 además, se puede observar que este protocolo trabaja con el sistema autónomo denominado 65535.

```
routing bgp instance
dd as=65535 name=BORDER1 redistribute-connected=yes redistribute-other-bgp=\
   yes redistribute-static=yes router-id=1.1.1.1
```

Figura 3.12 Configuración de BGP dentro de Border 1

En la red Wireless los dispositivos encargados de hacer Nat, es decir traduce las IP privadas en públicas para poder tener conexión son los routers: Pymes, Border 1 y Border 2 presentados en la figura 3.13, estos routers tienen salida directa con el proveedor de internet. En el anexo A se puede observar otras configuraciones importantes realizadas en los dispositivos restantes para poder lograr la automatización de las tareas repetitivas cabe recalcar que para cada router se usó básicamente la misma configuración presentada con anterioridad.

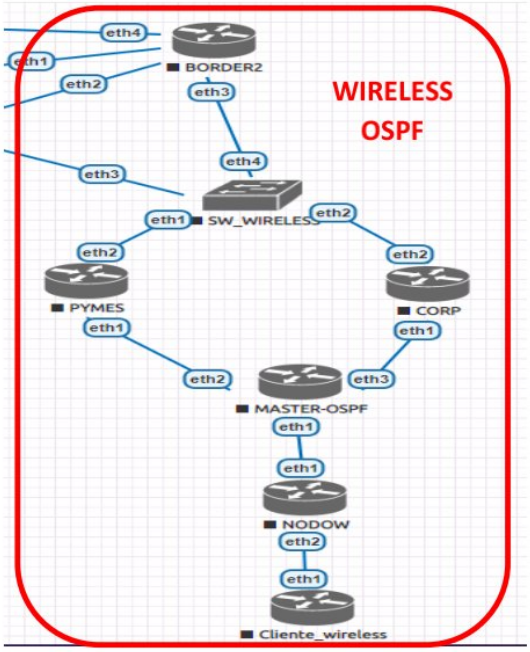


Figura 3.13 Red Wireless

3.4 Automatización de tareas

Una vez configurada la red y los respectivos dispositivos se empieza a realizar la programación correspondiente para automatizar las tareas identificadas como repetitivas y poder ser implementadas mediante el servidor del ISP, para esto se usa RouterOS, la cual permite usar las librerías de Python por medio de la interfaz de Mikrotik, de forma específica se usa la librería de Python RouterOS, la misma que ya ha sido usada en anteriores ocasiones por los administradores de red del ISP. El programa realizado mediante Python contiene un menú principal donde el administrador de la red debe elegir entre 4 opciones la tarea que desea automatizar y conforme avance se le presenta las distintas opciones que existen como se puede apreciar en la figura 3.14.

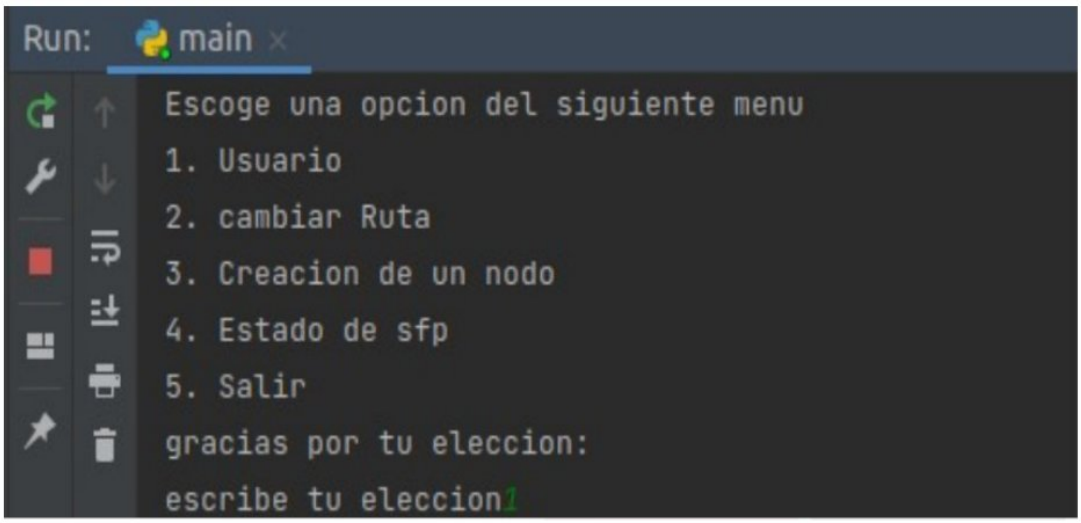


Figura 3.14 Menú principal de la automatización de tareas

El menú principal para la automatización de las tareas repetitivas se realiza con el fin de que el programa desarrollado tenga un entorno amigable y entendible. De esta manera cualquier persona puede interactuar de forma sencilla y rápida sin tener que abrir varias pestañas como se lo hace sin automatización por medio de la consola de MikroTik y así poder ahorrar el mayor tiempo además, reducir los errores que se pueden cometer. Adicionalmente es importante mencionar que el programa realizado mediante Python y RouterOS es cargado por medio del servidor del ISP para poder ejecutarlo.

3.4.1 Creación de un nuevo usuario en los routers

La automatización de tareas en primera instancia reduce los pasos a seguir debido a que todo se realiza dentro de un solo entorno sin la necesidad de tener que abrir otras pestañas y esperar que las mismas se carguen. En la figura 3.15 se presenta un diagrama de bloques el cual indica los pasos necesarios para crear un usuario mediante automatización.

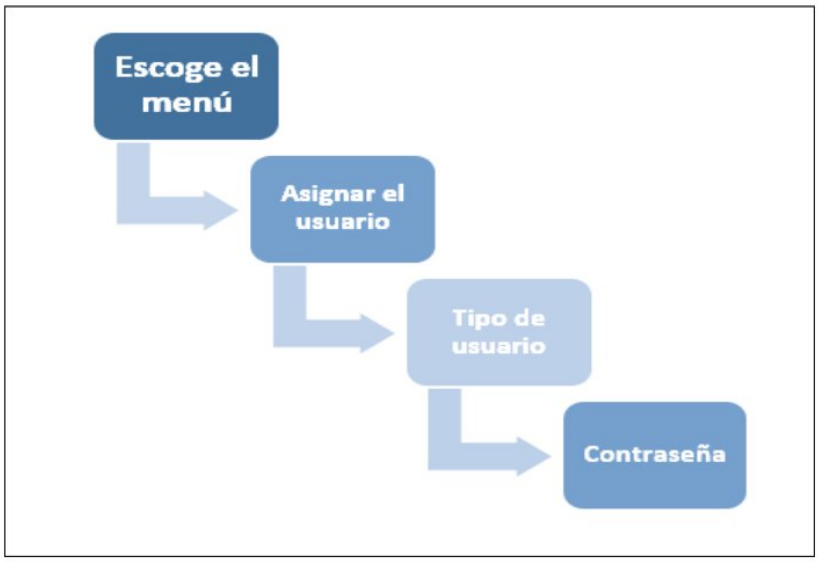


Figura 3.15 Pasos a seguir para crear un usuario de forma automatizada

Al realizar una comparación entre la figura 3.3 y 3.15 visualmente se puede apreciar que los pasos se redujeron ya que, el administrador de forma actual o sin automatización debe realizar 8 pasos mientras que de forma automatizada solo 4 pasos. Otra de las ventajas de la automatización de esta tarea es que el usuario se crea de forma rápida en todos los routers que pertenecen a la red y no se tendrá que crear el nuevo usuario en cada uno de los routers de forma repetitiva para obtener acceso.

Se automatiza la creación de usuarios para evitar el error humano, como colocar de forma errada la autenticación o credenciales dentro del router. Y de esta forma mejorar el tiempo de respuesta ante un requerimiento.

3.4.2 Cargar PBR o cambio de ruta

Una vez automatizado el cambio de ruta el administrador debe seguir los pasos mostrados en el diagrama de bloques de la figura 3.16, son pasos que guían al administrador de red para realizar un cambio de ruta rápido y sencillo. Adicionalmente se debe mencionar que se debe tener conocimiento de la red para poder desviar el tráfico y que no exista un colapso en la misma.

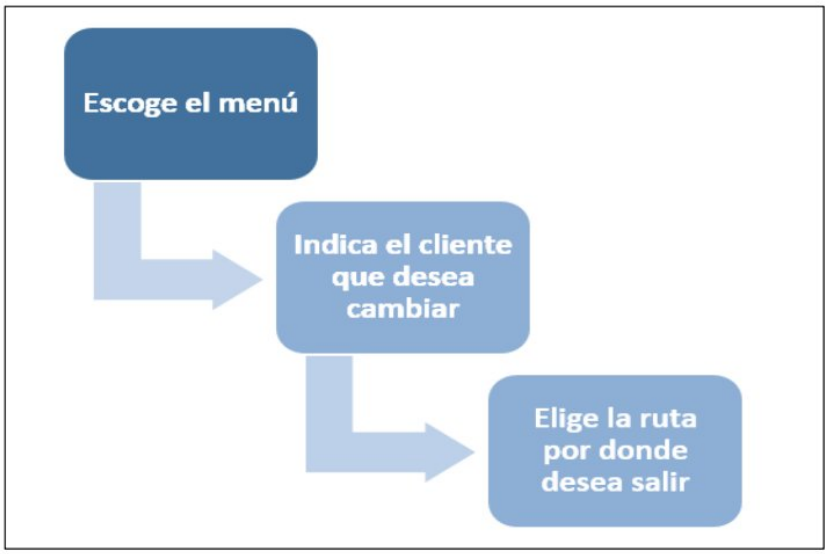


Figura 3.16 Cambio de ruta automatizada

Nuevamente como ha ocurrido en la automatización de otras tareas aquí también se reducen los pasos para poder cambiar de ruta. Sin la automatización de esta tarea se necesitaban 6 pasos mientras que de forma automatizada estos pasos se reducen en un 50 %. Para poder realizar esto el administrador de red debe tener en claro las políticas de enrutamiento establecidas por medio de PBR y la ruta por donde quiere enviar el tráfico para evitar el colapso de la red. Cabe recalcar que este cambio se da en un tiempo aproximado de 30 segundos ya no de 240 segundos o de 3 horas como se demostró en la figura 3.4 al realizar la misma tarea.

3.4.3 Creación de un nuevo nodo

Se automatiza la creación de usuarios para poder extender la red de forma rápida y eficiente, evitando algún error debido al subneteo que se debe realizar para llevar a cabo esta tarea. Al realizar la automatización de esta tarea se reducen los pasos en un 66 % y el tiempo de ejecución es de 30 segundos. En la figura 3.17 se muestra un diagrama de bloques con los pasos a seguir para poder crear un nuevo nodo de forma automatizada.

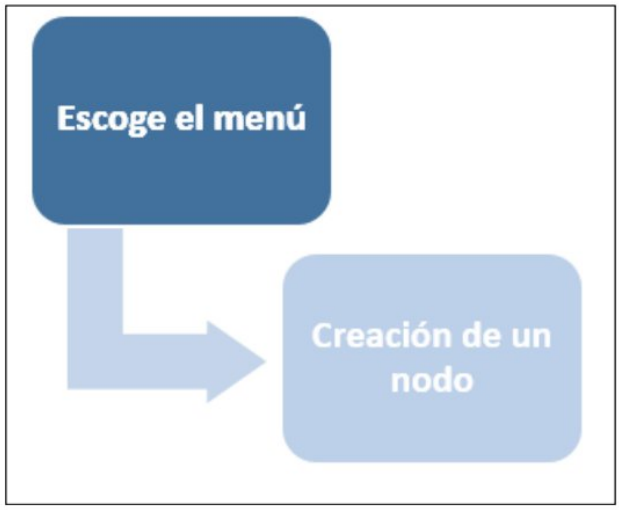


Figura 3.17 Creación de un nodo de forma automática

Son dos pasos sencillos realizados en el mismo entorno, donde le da la posibilidad al administrador de red que elija el cliente que desea cambiar y la ruta que desea seguir.

3.4.4 Consultas de SFP+ en cada router

Realizar consultas sfp de forma rápida es necesario para poder llevar un control de la interfaz y como consecuencia de cada router denominado nodo. En este caso los pasos a seguir una vez que se automatiza esta tarea son 2 como se aprecia en la figura 3.18.

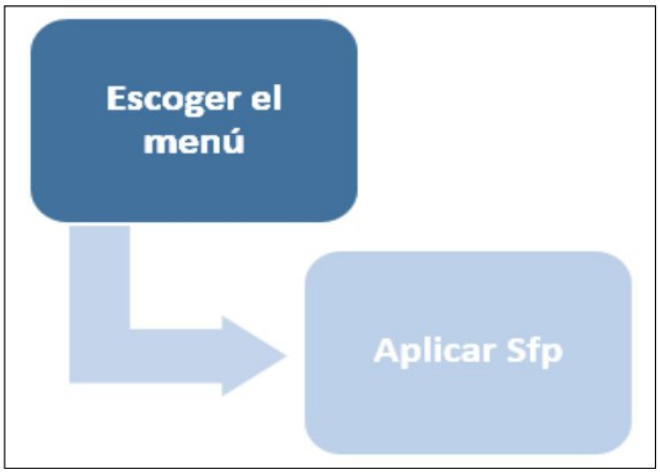


Figura 3.18 Consultas módulos sfp de forma automática

Una vez automatizada esta tarea se pueden consultar los módulos spf dentro del menú principal, en este caso no sólo aparecerá la información de una sola interfaz sino de todas aquellas que pertenezcan al router, logrando que el administrador de red evite repetir estos pasos para consultar cada interfaz como se realizaba anteriormente. El tiempo que se emplea en esta tarea una vez automatizada es de 30 segundos logrando que se simplifique el proceso de consulta y de esta forma el administrador de red pueda tomar precauciones ante posibles colapsos o conflictos de red. Los pasos en comparación con la figura 3.7 se redujeron en un 50%.

CAPÍTULO 4

4.1 Pruebas del funcionamiento de la automatización de tareas repetitivas

En este capítulo se muestra cada una de las tareas repetitivas una vez que el programa realizado mediante Python y RouterOS fue cargado en el servidor de la red, es decir se realizó la automatización de estas tareas. Además, se ejecuta cada una para comprobar su correcto funcionamiento.

4.1.1 Creación de usuarios

Como se observa en la figura 4.1 se muestra la creación de un usuario en el programa para la automatización de tareas, para esta comprobación se creó un nuevo usuario denominado integradora el cual fue designado como usuario full es decir que cuenta con todos los permisos tanto de lectura como escritura para realizar modificaciones dentro de la red.

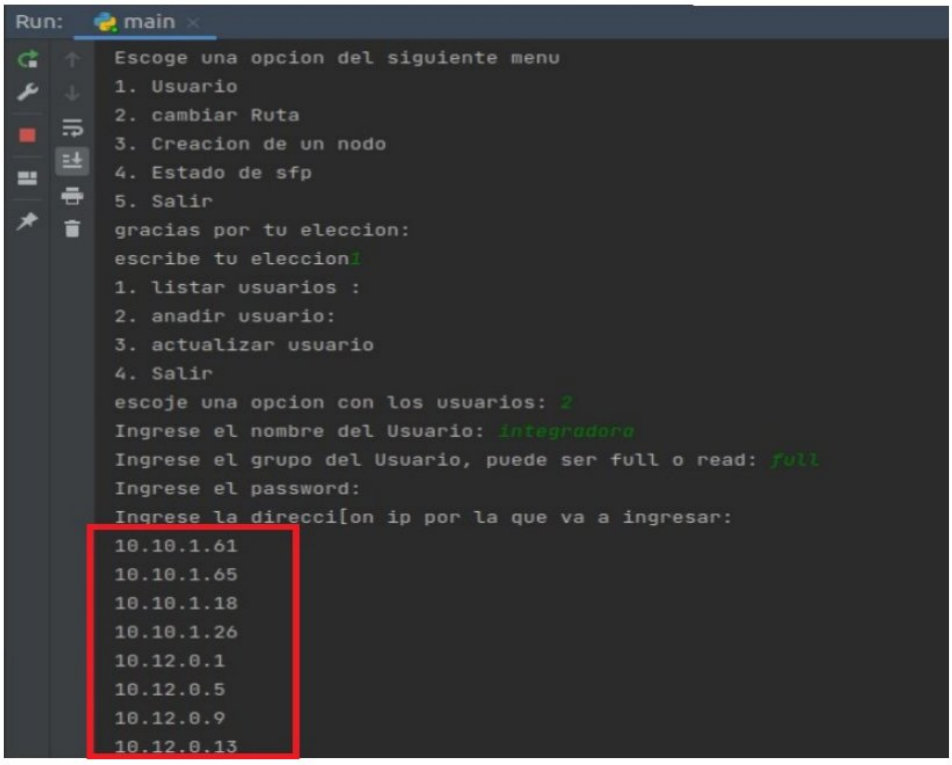


Figura 4.1 Creación de usuario denominado Integradora

Además, las direcciones IP encerradas dentro del recuadro rojo en la figura 4.1 indica las direcciones de los routers donde se creó este usuario de forma automática evitando que los pasos se repitan innecesariamente en cada uno de los routers donde se desee tener acceso con el nuevo usuario.

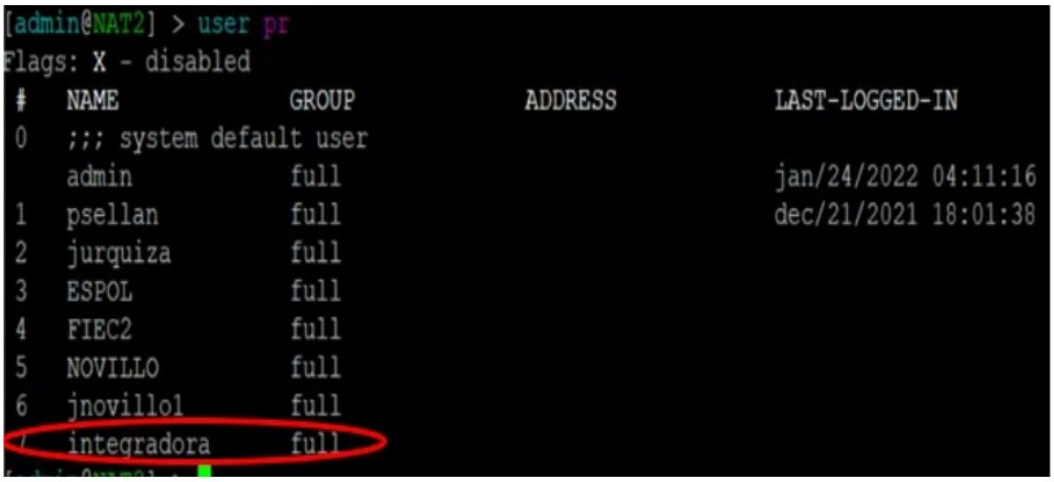


Figura 4.2 Verificación de la creación del usuario Integradora dentro del router Nat 2

Para la verificación de la correcta creación del usuario se ingresó por medio de consola al router Nat 2 como se muestra en la figura 4.2 la cual indica todos los usuarios creados en la red en especial, el usuario denominado integradora, la ejecución de esta tarea mediante la automatización se realiza en un tiempo aproximado de 30 segundos.

4.1.2 Cambio de ruta o cargar PBR

Una vez que se eligió la opción denominada cambio de ruta, se debe identificar el nodo y además, la Nat donde se requiere enviar el tráfico en este caso como se visualiza en la figura 4.3 se eligió la opción 2 es decir, cambio de ruta y luego se debe escribir en mayúscula el cambio que el administrador de red desea realizar.

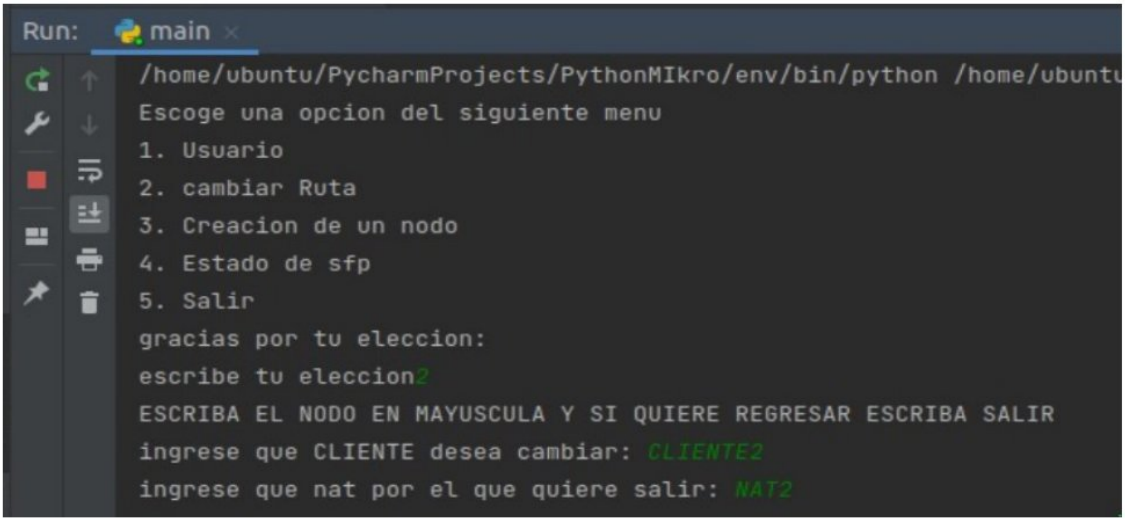


Figura 4.3 Prueba de cambio de ruta

En la figura 4.4 se muestra el cambio de ruta efectuado de forma exitosa. Antes de hacer el cambio de ruta los paquetes del cliente2 salían por la dirección 10.12.0.5 la cual está encerrada en el círculo 1 al ejecutar el programa y elegir la mejor ruta inmediatamente el mismo cliente2 cambia su tráfico a otra ruta que es la 10.10.1.9 como lo indica el círculo 2. De esta manera se evita que existan pérdidas de paquetes y se reduce el tiempo de indisponibilidad de la red. La automatización de esta tarea hace posible que se pueda ser desarrollada en un tiempo aproximado de 30 segundos.

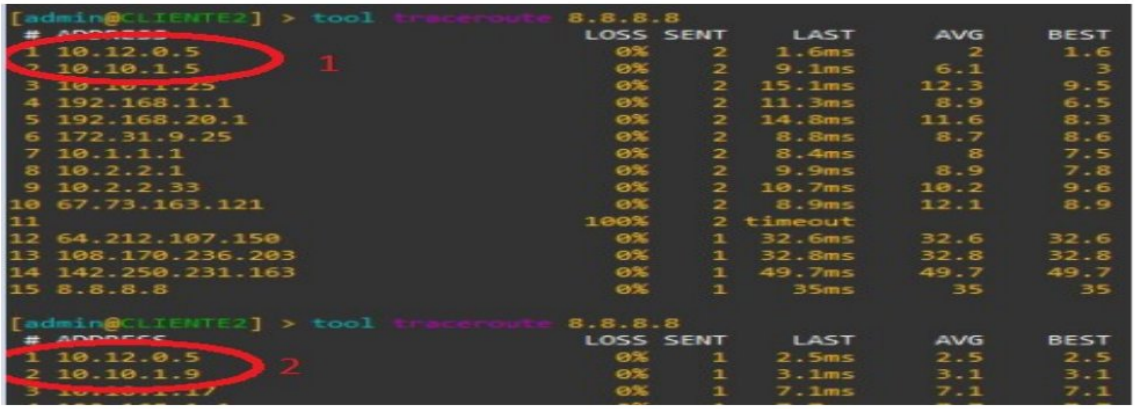


Figura 4.4 Comprobación del cambio de ruta

4.1.3 Creación de un nodo

Al escoger la opción de crear un nodo en el menú principal el programa automáticamente indica la IP con la que se identificará al nuevo nodo que corresponde a la última dirección disponible en este caso es la 10.10.1.69 y adicional a esto también indica la IP que le corresponde al cliente 10.23.0.16 tal cual aparece en la figura 4.5.

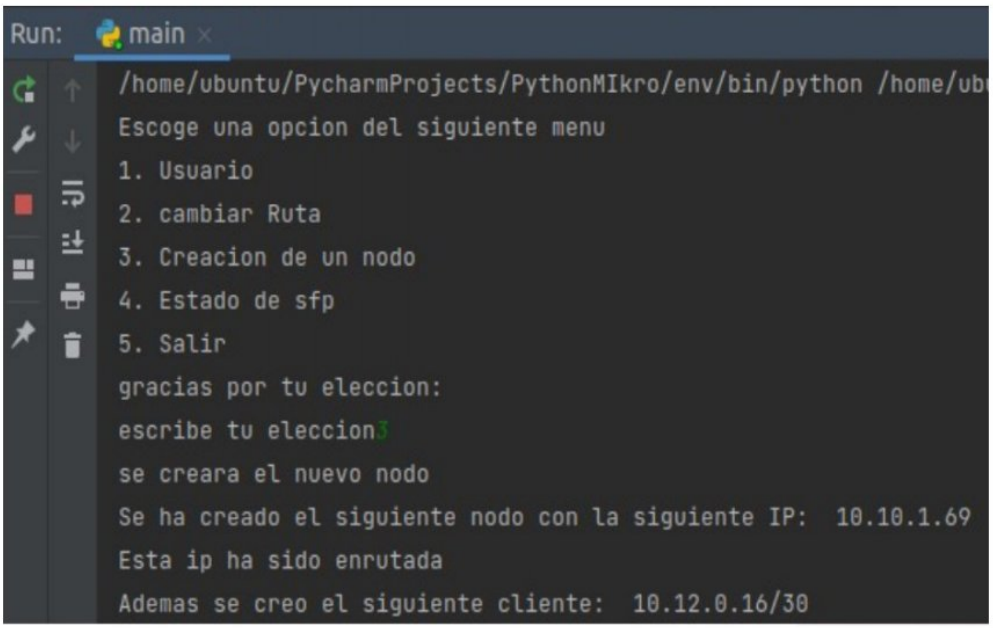


Figura 4.5 Prueba para la creación de un nodo

En las figuras 4.6 y 4.7 se muestra como la creación del nodo se realizó con éxito y además usan las mismas direcciones IP mostradas en el programa de automatización de tareas como se puede observar en la figura 4.5, ejecutar esta tarea por medio del programa toma un tiempo aproximado de 30 segundos y se evita hacer las divisiones de red de forma manual disminuyendo al máximo los errores que se pueden cometer y evitando los conflictos de red que se pueden suscitar a causa de alguna dirección IP errónea.

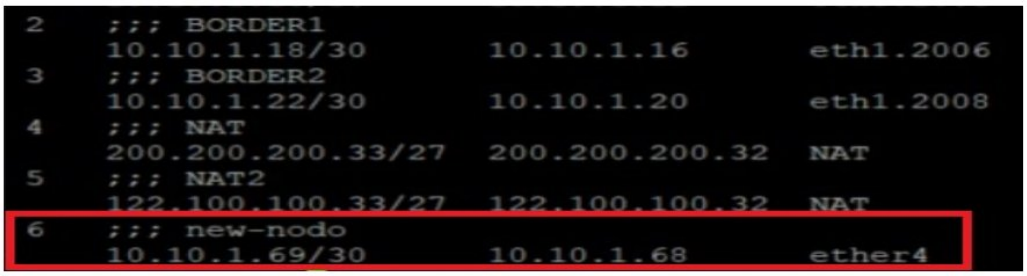


Figura 4.6 Verificación de la creación de nodo

Figura 4.7 Verificación de la creación del cliente

4.1.4 Consultas sfp

Al elegir la opción 4 del menú principal es decir consultas spf se despliega una lista con las principales características de cada interfaz que pertenece al router en una sola ventana como se indica en la figura 4.8. El tiempo invertido en esta tarea una vez automatizada es de 30 segundos y con esto se evita realizar la búsqueda de cada interfaz de forma individual.

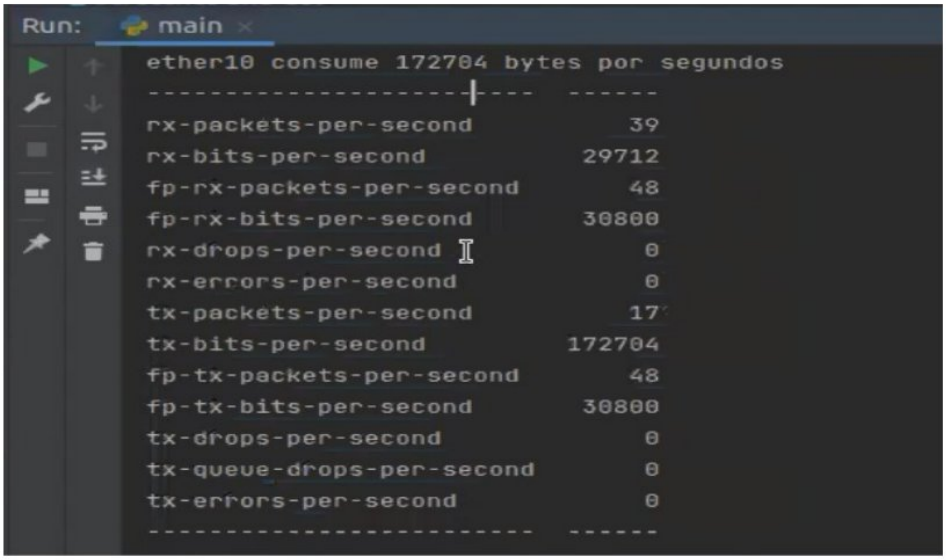


Figura 4.8 Pruebas para consultas sfp

4.2 Análisis de resultados

Para poder realizar un análisis comparativo entre las tareas repetitivas realizadas de forma actual y las tareas realizadas por medio de automatización se tuvo que simular la ejecución de las mismas y medir el tiempo aproximado que se invertía en cada una.

- Crear un usuario de forma actual en un solo router toma un tiempo aproximado de 60 segundos, en este caso en la red existen 8 routers en los cuales es necesario crear dicho usuario es decir, el tiempo aumenta 8 veces más dando un total aproximado de 480 segundos al realizarlo una sola vez en cambio, al crear un usuario de forma automatizada el tiempo total sólo es de 60 segundos para los 8 routers. Adicionalmente al automatizar esta tarea se observó una reducción de pasos del 50 %.
- Para realizar cambios de ruta de forma actual dentro del ISP se invierte un tiempo aproximado de 300 segundos, teniendo en cuenta que se tomó el escenario más sencillo mientras que de forma automatizada la misma tarea se la puede realizar en 30 segundos y con una reducción de pasos del 50%.
- La creación de un nodo es una de las tareas que más tiempo necesita para ser desarrollada de forma actual, debido a las constantes búsquedas de direccionamiento IP o divisiones de red que se debe realizar para ejecutar la creación por lo que, se invierte un tiempo aproximado de 600 segundos mientras que al automatizar está tarea sólo se emplea un tiempo de 30 segundos debido a que las direcciones IP ya vienen cargadas dentro del programa. También existe una reducción de pasos del 66%.
- Las consultas de módulos spf de forma actual para una sola interfaz se realizan en un tiempo de 30 segundos, para ver el estado del nodo es necesario verificar cada una de las interfaces, en este caso son aproximadamente 13 es por esto que el tiempo aproximado invertido es de 390 segundos. Al automatizar esta tarea las consultas de las 13 interfaces se realizan en 30 segundos y los pasos se reducen en un 50%.

Tabla 4.1 Tiempo invertido en tareas sin automatizar y automatizadas

	Sin automatizar		Automatizado	
Tarea	**Tiempo total (s)**	**Número de pasos**	**Tiempo total (s)**	**Número de pasos**
Creación de usuario	480	8	60	4
Cambio de ruta	300	6	30	3
Creación de nodo	600	6	30	2
Consultas de módulos sfp	390	4	30	2

La tabla 4.1 muestra los resultados obtenidos, los cuales indican que al implementar el programa de automatización por medio del servidor del ISP los pasos que se usaban para ejecutar las tareas se reducen en un 50 % además, el tiempo invertido en las misma disminuye logrando que tareas en las cuales se invertía más de 5 minutos ahora se las logre realizar en menos de 1 minuto.

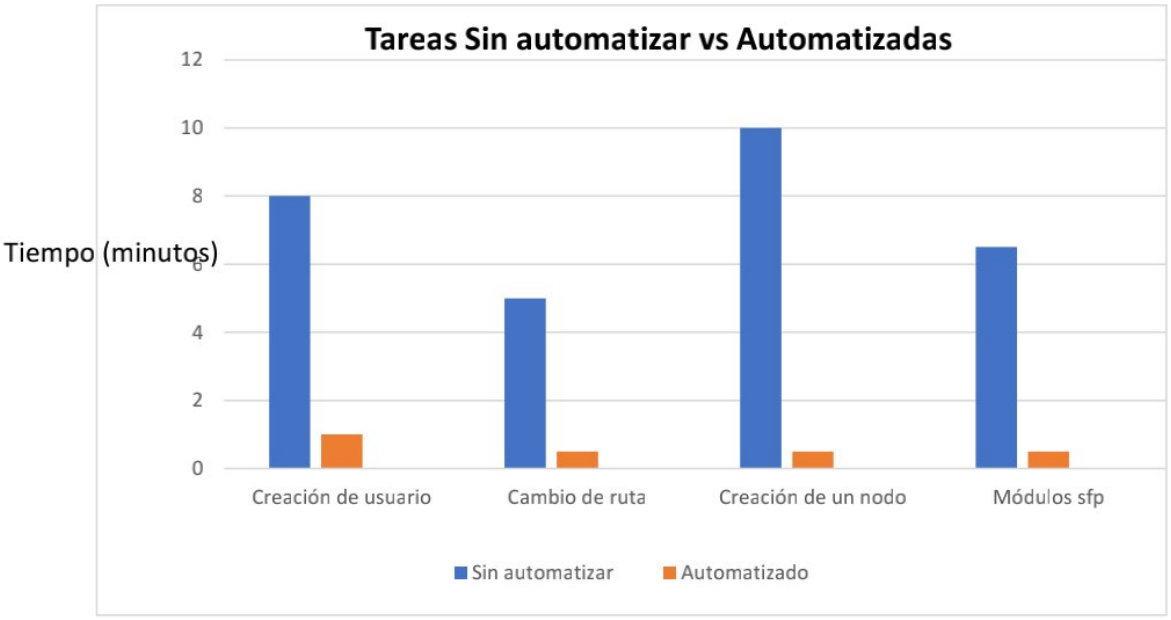


Figura 4.9 Comparación entre las tareas sin automatizar vs las tareas automatizadas en minutos

En la figura 4.9 se expone una gráfica en donde se realiza una comparación del tiempo invertido entre las tareas repetitivas antes y después de la automatización logrando una disminución del tiempo considerable y notorio. Se logró está disminución debido a que, se creó un programa de fácil manejo en donde los procesos de asignación de recursos se realizan dentro de un solo entorno además, disminuye la probabilidad de cometer errores. Los módulos de programación poseen la información necesaria para ejecutar las tareas sin necesidad de realizar los pasos de forma repetitiva dando como resultado que las 4 tareas identificadas como repetitivas se puedan realizar en intervalos de tiempo de entre 30 y 60 segundos.

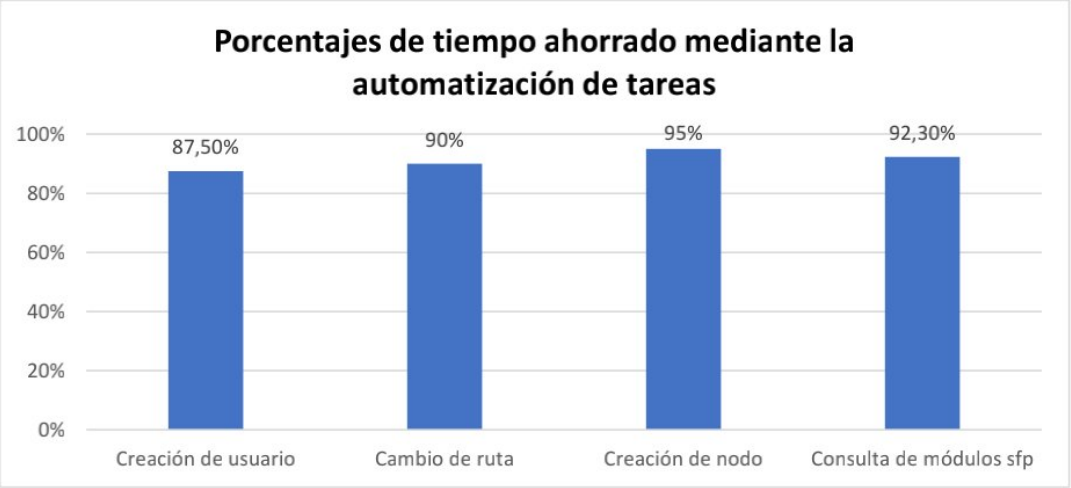


Figura 4.10 Porcentaje de ahorro mediante automatización de tareas

Finalmente, como se puede observar en la figura 4.10 el porcentaje del tiempo ahorrado mediante la automatización de tareas es alto, de forma general se ahorra más del 85% por tarea, lo que hace que el ISP gane competitividad dentro del mercado y este tiempo ahorra pueda ser invertido en solventar las demandas del servicio al cliente de forma eficaz. La tarea que más porcentaje de tiempo ahorra es la creación de un nodo con un 95% debido a que es la tarea que más tiempo invierte al hacerla sin automatización.

CONCLUSIONES

- Se logró implementar el programa de automatización en el servidor del ISP, a través de Python en conjunto con el sistema operativo RouterOS y automatizar las 4 tareas identificadas como repetitivas con éxito.
- La simulación de la red del proveedor de servicios de internet sirve para futuras pruebas y de esta manera realizar cambios de forma virtualizada que después se puedan implementar en la misma sin tener que afectar a los usuarios.
- Con la automatización de las tareas repetitivas dentro del ISP, se tuvo un ahorro de tiempo mayor al 85% de forma general y además, se ve una disminución de pasos al ejecutar cada tarea de aproximadamente 50%.
- Es recurrente que existan errores humanos dentro del desarrollo de las tareas repetitivas que pueden causar conflictos en la red, por medio de la automatización estos errores disminuyen.
- El programa creado para la automatización de tareas repetitivas es versátil, debido a que se puede adaptar a las necesidades de cualquier proveedor de servicios de internet siempre y cuando brinden la información requerida de su red.

RECOMENDACIONES

- Se aconseja tener un equipo con las características necesarias ya que, al simular la red se usa un router virtualizado lo cual requiere consumo de recursos.
- Al implementar el programa es necesario tener una base de datos con todas las direcciones IP que se hayan creado para así poder ingresar y escribir sobre ellos las funciones realizadas con Python.
- Se necesita que el servidor sea alcanzable en toda la red del ISP para así poder escribir sobre ellos adicionalmente, como tema de seguridad se puede realizar un certificado de autenticación tanto en routers como en el servidor.

ANEXOS

Anexo A: Configuraciones implementadas en los routers principales.

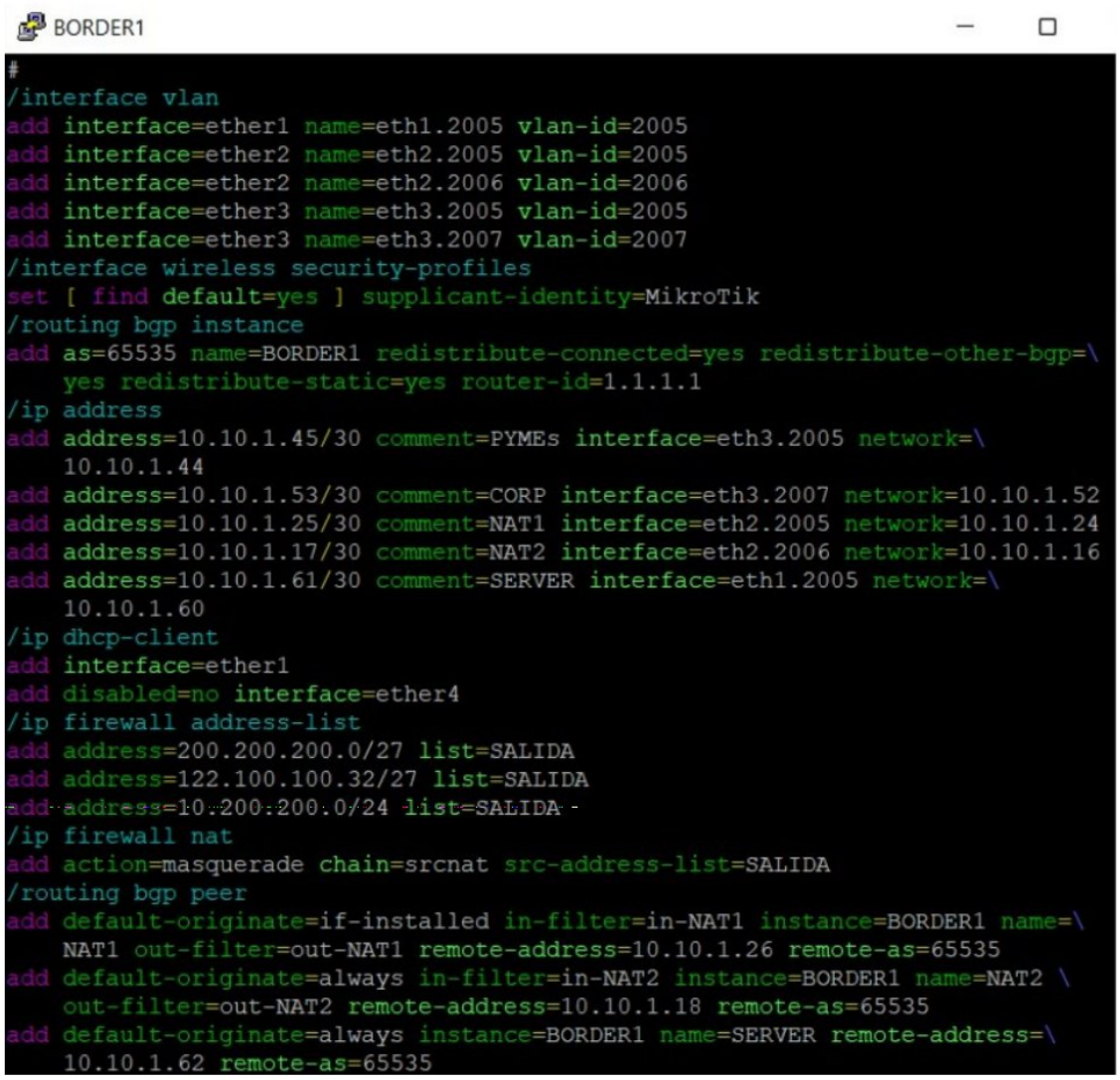
```
/interface bridge
add name=NAT1
/interface vlan
add interface=ether1 name=eth1.2005 vlan-id=2005
add interface=ether1 name=eth1.2007 vlan-id=2007
add interface=ether2 name=eth2.2005 vlan-id=2005
add interface=ether3 name=eth3.2005 vlan-id=2005
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
add as=65535 name=NAT1 redistribute-connected=yes redistribute-other-bgp=yes \
    router-id=1.1.1.3
/ip address
add address=10.10.1.1/30 comment=NODO1 interface=eth2.2005 network=10.10.1.0
add address=10.10.1.5/30 comment=NODO2 interface=eth3.2005 network=10.10.1.4
add address=10.10.1.26/30 comment=BORDER1 interface=eth1.2005 network=\
    10.10.1.24
add address=10.10.1.30/30 comment=BORDER2 interface=eth1.2007 network=\
    10.10.1.28
add address=200.200.200.1/27 comment=NAT interface=NAT1 network=200.200.200.0
add address=200.200.200.2/27 comment=NAT interface=NAT1 network=200.200.200.0
add address=122.100.100.1/27 comment=PUBLICAS2 interface=NAT1 network=\
    122.100.100.0
/ip dhcp-client
add disabled=no interface=ether1
/ip firewall address-list
add address=200.200.200.0/27 list=PUBLICAS
add address=10.12.0.0/30 list=CLIENTE1
add address=10.12.0.8/30 list=CLIENTE1
/ip firewall nat
add action=src-nat chain=srcnat src-address-list=CLIENTE1 to-addresses=\
    200.200.200.1
/routing bgp network
add network=200.200.200.0/27 synchronize=no
add network=122.100.100.0/27 synchronize=no
add network=10.10.1.0/30 synchronize=no
add network=10.12.0.0/30 synchronize=no
/routing bgp peer
add in-filter=in-BORDER1 instance=NAT1 name=BORDER1 out-filter=out-BORDER1 \
    remote-address=10.10.1.25 remote-as=65535
add in-filter=in-BORDER2 instance=NAT1 name=BORDER2 out-filter=out-BORDER2 \
    remote-address=10.10.1.29 remote-as=65535
add default-originate=always instance=NAT1 name=NODO1 remote-address=\
    10.10.1.2 remote-as=65535
add default-originate=always instance=NAT1 name=NODO2 remote-address=\
```

Anexo A.1 Configuración de Nat 1

NAT2

```
/interface bridge
add name=NAT
/interface vlan
add interface=ether1 name=eth1.2006 vlan-id=2006
add interface=ether1 name=eth1.2008 vlan-id=2008
add interface=ether2 name=eth2.2005 vlan-id=2005
add interface=ether3 name=eth3.2005 vlan-id=2005
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
add as=65535 name=NAT2 router-id=1.1.1.4
/ip address
add address=10.10.1.9/30 comment=NODO2 interface=eth2.2005 network=10.10.1.8
add address=10.10.1.13/30 comment=NODO3 interface=eth3.2005 network=\
    10.10.1.12
add address=10.10.1.18/30 comment=BORDER1 interface=eth1.2006 network=\
    10.10.1.16
add address=10.10.1.22/30 comment=BORDER2 interface=eth1.2008 network=\
    10.10.1.20
add address=200.200.200.33/27 comment=NAT interface=NAT network=\
    200.200.200.32
add address=122.100.100.33/27 comment=NAT2 interface=NAT network=\
    122.100.100.32
add address=10.10.1.69/30 comment=new-nodo interface=ether4 network=\
    10.10.1.68
/ip dhcp-client
add disabled=no interface=ether1
/ip firewall address-list
add address=10.12.0.12/30 comment=CLIENTE4 list=cliente
add address=10.12.0.4/30 comment=CLIENTE2 list=cliente
add address=10.12.0.8/30 comment=CLIENTE3 list=cliente
add address=10.12.0.16/30 comment="NEW NODO" list=cliente
/ip firewall nat
add action=src-nat chain=srcnat log=yes src-address-list=cliente \
    to-addresses=122.100.100.32/27
add action=src-nat chain=srcnat log=yes src-address-list=cliente \
    to-addresses=122.100.100.32/27
/routing bgp network
add network=122.100.100.32/27 synchronize=no
add network=200.200.200.32/27 synchronize=no
add network=10.12.0.8/30 synchronize=no
add network=10.12.0.4/30 synchronize=no
add network=10.12.0.12/30 synchronize=no
```

Anexo A.2 Configuración de Nat 2



Anexo A.3 Configuración de Border 1

```
[admin@SERVER] > export
# feb/02/2022 05:15:28 by RouterOS 6.48.3
# software id =
#
#
#
/interface vlan
add interface=ether1 name=eth1.2005 vlan-id=2005
add interface=ether1 name=eth1.2007 vlan-id=2007
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
add as=65535 name=SERVER router-id=1.2.3.1
/ip address
add address=10.10.1.62/30 comment=BORDER1 interface=eth1.2005 network=\
    10.10.1.60
add address=10.10.1.66/30 comment=BORDER2 interface=eth1.2007 network=\
    10.10.1.64
add address=10.200.200.4/24 interface=ether2 network=10.200.200.0
/ip dhcp-client
add interface=ether2
/ip route
add disabled=yes distance=1 gateway=eth1.2005
/routing bgp network
add network=10.200.200.0/24 synchronize=no
/routing bgp peer
add instance=SERVER name=BODER1 remote-address=10.10.1.61 remote-as=65535
/system identity
set name=SERVER
/tool romon
set enabled=yes
[admin@SERVER] >
```

Anexo A.4 Configuración del Server

Anexo B: Direccionamiento IP usado en las configuraciones de la red.

/30	
Router	**Ip**
NODO1-NAT1	**10.10.1.0**
NAT1	10.10.1.1
NODO1	10.10.1.2
Broadcast	10.10.1.3
NODO2-NAT1	**10.10.1.4**
NAT2	10.10.1.5
NODO2	10.10.1.6
Broadcast	10.10.1.7
NODO2-NAT2	**10.10.1.8**
NAT2	10.10.1.9
NODO2	10.10.1.10
Broadcast	10.10.1.11
NODO3-NAT2	**10.10.1.12**
NAT2	10.10.1.13
NODO3	10.10.1.14
Broadcast	10.10.1.15
NAT2-BORDER1	**10.10.1.16**
BORDER1	10.10.1.17
NAT2	10.10.1.18
Broadcast	10.10.1.19
NAT2-BORDER2	**10.10.1.20**
BORDER2	10.10.1.21
NAT2	10.10.1.22
Broadcast	10.10.1.23
NAT1-BORDER1	**10.10.1.24**
BORDER1	10.10.1.25
NAT1	10.10.1.26
Broadcast	10.10.1.27
NAT1-BORDER2	**10.10.1.28**
BORDER2	10.10.1.29
NAT1	10.10.1.30
Broadcast	10.10.1.31
NODOW-MOSPF	**10.10.1.32**
MOSPF	10.10.1.33
NODOW	10.10.1.34
Broadcast	10.10.1.35

MOSPF-PYMES	**10.10.1.36**
PYMES	10.10.1.37
MOSPF	10.10.1.38
Broadcast	10.10.1.39
MOSPF-CORP	**10.10.1.40**
CORP	10.10.1.41
MOSPF	10.10.1.42
Broadcast	10.10.1.43
PYMES-BORDER1	**10.10.1.44**
BORDER1	10.10.1.45
PYMES	10.10.1.46
Broadcast	10.10.1.47
PYMES-BORDER2	**10.10.1.48**
BORDER2	10.10.1.49
PYMES	10.10.1.50
Broadcast	10.10.1.51
CORP-BORDER1	**10.10.1.52**
BORDER1	10.10.1.53
CORP	10.10.1.54
Broadcast	10.10.1.55
CORP-BORDER2	**10.10.1.56**
BORDER2	10.10.1.57
CORP	10.10.1.58
Broadcast	10.10.1.59
SERVER-BORDER1	**10.10.1.60**
BORDER1	10.10.1.61
SERVER	10.10.1.62
Broadcast	10.10.1.63
SERVER-BORDER2	**10.10.1.64**
BORDER2	10.10.1.65
SERVER	10.10.1.66
Broadcast	10.10.1.67

Anexo B.1 Tabla de direccionamiento IP usada en los routers

/30	
clienteW	**ip**
clienteW-nodoW	**10.6.0.0**
nodoW	10.6.0.1
clienteW	10.6.0.2
Broadcast	10.6.0.3

Anexo B.2 Direccionamiento IP de cliente W

/30	
ClienteGPON	**ip**
cliente1-nodo1	**10.12.0.0**
nodo1	10.12.0.1
cliente1	10.12.0.2
Broadcast	10.12.0.3
cliente2-nodo2	**10.12.0.4**
nodo2	10.12.0.5
Cliente2	10.12.0.6
Broadcast	10.12.0.7
cliente3-nodo2	**10.12.0.8**
nodo2	10.12.0.9
cliente3	10.12.0.10
Broadcast	10.12.0.11
cliente4-nodo3	**10.12.0.12**
nodo3	10.12.0.13
cliente4	10.12.0.14
Broadcast	10.12.0.15

Anexo B.3 Direccionamiento IP usado en Cliente GPON

/29	
enlace	**ip**
enlace_cliente1	**172.22.0.0**
BRN_CLIENTE1	172.22.0.1
STN_CLIENTE1	172.22.0.2
RB_CLIENTE1	172.22.0.3
-	172.22.0.4
-	172.22.0.5
-	172.22.0.6
Broadcast	172.22.0.7

Anexo B.4 Direccionamiento IP usado dentro de la red

/28 o /29	
aps	**ip**
aps_clientew1	**172.18.0.0**
ap1	172.18.1.1
ap2	172.18.1.2
ap3	172.18.1.3
ap4	172.18.1.4
ap5	172.18.1.5
ap6	172.18.1.6
Broadcast	172.18.1.7

Anexo B.5 Direccionamiento IP usado en ClienteW1

BIBLIOGRAFÍA

[1] M.Starri, «DIGITAL 2021-I DATI DI LUGLIO,» *WE ARE SOCIAL,* 2021.

[2] ARCOTEL, «SERVICIO DE ACCESO A INTERNET,» Quito , 2020.

[3] D. B. Innovation, «¿El servicio de internet o telefonía en Ecuador es competitivo para las empresas?,» *DATTA,* 2020.

[4] J. T. C. P.-. M. E. R. Loja, «Propuesta para la medicion de la calidad de servicio de internet en la zona urbana,» Universidad Politécnica Salesiana, Cuenca, 2013.

[5] D.J.G.Meza, «Cobertura de los servicios de internet de la empresa In.Planet SA en la ciudad de Babahoyo y su afectación en la rentabilidad,» Babahoyo, 2017.

[6] V. Muñoz, «TECNOLOGÍAS PARA AUTOMATIZARTécnologías para automatizar la gestión de abonados de un proveedor de servicios de internet.,» *BandaLibre,* 2021.

[7] O. S. Figueroa Alemán y V. E. Masache Narváez, «Análisis de tecnologías de un centro de operaciones de ciberseguridad para un proveedor de servicios de internet,» Universidad de las Américas, 2018.

[8] L. H. V. A.-. J. A. V. VIVAS, «Diseño e implementación de un ISP con acceso inalámbrico para soportar servicios de interner y telefonía IP en e Laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente.,» Universidad autónoma de Occidente, 2013.

[9] J. Castro, «Protocolos de enrutamiento para una red de un proveedor de servicios de internet.,» ACADEMIA, 2018.

[10] L. L. Modesto González, «Enrutamiento Dinámico RIP-OSPF establecidos en una red de internet.».

[11] G. E. A. A. Almanza G., «Fundamentos de redes y entutamiento básico,» Universidad tencológica de Bolívar, 2004.

[12] T. Gabriel, «Protocolos de Red y Modelo Osi,» 2020.

[13] R. Sheldon, «Redes y Sistemas Autónomos».

[14] W. STALLINGS, Sistemas Operativos, Quinta Edición, Pearson- Prentice Hall, 2015.

[15] D. M. Siguenza Suscal y J. P. Jiménez Pesantez, «Estudio e implementación de la nueva arquitectura física y lógica de la red de datos, servicios utilizando RouterOS y tecnologías Open Source de bajo costo, integradas a un sistema de

administración Web para control de abonados y gestión de planes.,» Universidad Politécninca Salesiana, Guayaquil, 2014.

[16] A. L. Quiroga, «Propuesta de planeación estratégica para automatización de procesos en el sector de telecomunicaciones,» Universidad Militar Nueva Granada, 2018.

[17] L. Dominguez Quintero y M. Vargas Lombardo, «Tool infrastructure as code: ansible, terrafom, chef, puppet,» Universidad Tecnológica de Panamá, 2021.

[18] A. Osorio, «Redes GPON-FTTH, evolución y puntos críticos para su respectivo despliegue.,» Instituto Tecnológico de Buenos Aires, Buenos Aires, 2016.

[19] M. A. Ibañez, Ingeniería de Fibras Ópticas, ISBN.

[20] J. O. Famer, The Book on FTTX: : A Practical Guide to FTTX infraestructure.

[21] O. O. Armas Espinoza, «Diseño y simulación de una red MPLS para ESP Completion Technologies LLC,» Pontificia Universidad Católica del Ecuador , 2017.

[22] C. F. Cordero Vizhñay y P. L. Gallegos Segovia, «Diseño y despliegue de Funciones de Red Virtualizadas (NFV) usando Redes Definidas por Software (SDN) dentro de una infraestructura virtual, aplicando balanceo de carga y seguridad distribuida en IPv6,» Universidad Politécnica Salesiana, Guayaquil, 2017.

[23] G. D. Salazar Chacón y G. X. Chafla Altamirano, «Empleo de path-control tools en una red empresarial moderna mediante políticas de enrutamiento,» Pontificia Universidad Católica del Ecuador.