FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO Y SIMULACIÓN DE UNA RED MPLS UTILIZANDO EQUIPOS MIKROTIK Y EL EMULADOR GNS3 EN ENTORNOS PYMES.

AUTOR

DIEGO MARCELO ANDRANGO ALVARO

AÑO

2019

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO Y SIMULACIÓN DE UNA RED MPLS UTILIZANDO EQUIPOS MIKROTIK Y EL EMULADOR GNS3 EN ENTORNOS PYMES.

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones.

Profesor Guía

MSc. Edwin Guillermo Quel Hermosa

Autor

Diego Marcelo Andrango Alvaro

Año

2019

DECLARACION PROFESOR GUÍA

Declaro haber dirigido el trabajo de “DISEÑO Y SIMULACIÓN DE UNA RED MPLS UTILIZANDO EQUIPOS MIKROTIK Y EL EMULADOR GNS3 EN ENTORNOS PYMES”, a través de reuniones periódicas con el estudiante Diego Marcelo Andrango Alvaro, en el semestre 2019 - 02, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Edwin Guillermo Quel Hermosa

Magister en Gerencia de Redes y Telecomunicaciones

CI: 171872689-4

DECLARACION PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, de análisis de los aspectos técnicos del marco regulatorio para la protección de datos personales en Ecuador, de Stefan Remache Arias, en el semestre 2019 - 02, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Milton Neptalí Román Cañizares

Magister en Gerencia de Redes y Telecomunicaciones

CI: 0502163447

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

_____

Diego Marcelo Andrango Alvaro

CI: 1718547472

AGRADECIMIENTOS

Te agradezco a ti mi Dios por darme la vida y entregarme tu infinito amor.

Agradezco a toda mi familia, en especial a mis padres por todo el amor y apoyo que me brindan cada día.

A mis hermanos que siempre confiaron en mí perseverancia y me supieron dar aliento para seguir adelante en mi trabajo y en mis estudios.

DEDICATORIA

Dedico el presente trabajo de titulación a mi padre Pablo Andrango y a mi madre María Elena Alvaro, que me enseñaron a luchar y a trabajar muy duro desde pequeño para conseguir grandes cosas.

Gracias a ello y la perseverancia he conseguido este gran sueño que me propuse en la vida.

RESUMEN

El presente trabajo de titulación se basa en el diseño y simulación de una red MPLS (Multiprotocol Label Switching) utilizando equipos MikroTik y el emulador GNS3 (Graphic Network Simulation) en entornos PYMES con el objetivo de transportar datos de una manera rápida y confiable y demostrar que los equipos MikroTik pueden y tienen la misma capacidad que las marcas posicionadas en el mercado de las telecomunicaciones.

La red MPLS consta de routers MikroTik en su totalidad. En la parte de core existen dos equipos P´s (Core Provider) que permiten el reenvío de paquetes MPLS. Cabe indicar también que los equipos de core P´s y los equipos de acceso PE´s (Edge Provider) se comunican mediante el protocolo de Gateway Interior OSPF (Open Shortest Path First).

En la parte de acceso consta de tres equipos PE´s encargados de realizar en empaquetado y desempaquetado MPLS. Adicionalmente se encargan del ruteo de capa 3 mediante VPN´s L3 (Virtual Private Network), VRF´s (Virtual Routing and Forwarding) y la propagación de rutas mediante el protocolo BGP (Border Gateway Protocol).

Finalmente, los 3 routers CPE´s (Custom Premise Equipment) instalados en la parte del cliente. El primer router realiza la función de Matriz, en donde se ha configurado rutas estáticas para poder alcanzar los otros dos PE´s (Sucursales), mientras tanto en las sucursales se realizó la configuración de una ruta por defecto para que puedan alcanzar la Matriz.

ABSTRACT

The present titration work is based on the design and simulation of an MPLS (Multiprotocol Label Switching) network using MikroTik equipment and the GNS3 (Graphic Network Simulation) emulator in PYMES environments with the aim of transporting data in a fast and reliable way and demonstrating that MikroTik equipment can and has the same capacity than the brands positioned in the telecommunications area.

The MPLS network consists of MikroTik routers in their entirety. In the core part there are two P's (Core Provider) that allow the forwarding of MPLS packets. It should also be noted that the core equipment P's and the access equipment PE's (Edge Provider) communicate through the Interior Gateway protocol OSPF (Open Shortest Path First).

In the access part consists of three PE teams responsible for carrying out packaging and unpacking MPLS. Additionally, they are responsible for layer 3 routing through VPN's L3 (Virtual Private Network), VRF's (Virtual Routing and Forwarding) and the propagation of routes through the BGP protocol (Border Gateway Protocol).

Finally, there are 3 CPE´s (Custom Premise Equipment) routers installed in the client's part. The first router performs the Matrix function, where static routes have been configured to reach the other two PE's (Branches), while in the branches it was carried out the configuration of a default route so that they can reach the Matrix.

ÍNDICE

ÍNDICE DE FIGURAS

1. CAPÍTULO I. INTRODUCCIÓN.

1.1. Antecedentes

A través de los años la evolución de las redes de comunicación y tecnologías de información (TI) han permitido que las personas puedan comunicarse mediante una variedad de equipos de comunicación sean estos de gama baja, media y alta calidad. Actualmente existen un sin número de marcas posicionadas en el mercado de las redes y telecomunicaciones como son: Cisco, Huawei y Hewlett Packard (HP) entre las más renombradas. Sin embargo, en los últimos años hay una marca que está creciendo debido a su bajo costo, fiabilidad y sus grandes funcionalidades al soportar protocolos como BGP, OSPF y MPLS. Esta nueva marca es conocida como MikroTik cuyo sistema operativo es RouterOS la cual está basada en Linux.

MikroTik está enfocada en soluciones para pequeñas y medianas empresas por su bajo costo y gran rendimiento.

Por otro lado, es importante destacar el crecimiento que están teniendo las redes MPLS en pequeñas y medianas empresas con el objetivo de tener un buen desempeño, rendimiento, escalabilidad y calidad de servicio (QoS).

Finalmente, Graphical Network Simulator GNS3 es un simulador que se acerca más a la realidad, capaz de soportar y ejecutar sistemas operativos de los routers, con todas las funcionalidades que tiene un router físico lo que lo hace ideal para realizar pruebas, laboratorios y proyectos.

1.2. Alcance

El alcance del presente proyecto consiste en analizar el protocolo MPLS, el mismo que permite el diseño y simulación de una red IP utilizando equipos MiktroTik, cuya finalidad tiene la transferencia de información entre sucursales para de esta manera demostrar los múltiples beneficios de los equipos

MikroTik. La simulación se la realizará mediante el software GNS3 (Graphical Network Simulator 3) debido a su fácil instalación, manejo y entorno amigable.

Adicionalmente la solución implementada permitirá validar, si la transferencia de información entre sucursales y convergencias de los servicios fue correcta.

1.3. Justificación

El rápido desarrollo, crecimiento de las tecnologías y convergencia de servicios está afectando directa e indirectamente a las pequeñas y medianas empresas en el Ecuador las cuales están tratando de adaptarse a un costo asequible. En la actualidad existe una marca que lidera el mercado de redes y telecomunicaciones llamada CISCO con un costo considerable. Sin embargo, con el diseño y simulación de una red MPLS con equipos MikrotTik se puede conocer las ventajas y beneficios que brinda esta tecnología sobre las diferentes marcas. Por tal motivo es necesario realizar el presente proyecto y demostrar que se puede tener una red que permite transportar cada uno de los servicios del cliente como son: voz, datos y video de una manera segmentada y a un costo que sea accesible y alcanzable.

El uso del protocolo MPLS en equipos MikroTik permitirá crear un hito para futuras implementaciones de redes IP, permitiendo fomentar el estudio como una materia opcional en la Universidad de las Américas UDLA.

1.4. Objetivo General

Diseñar y simular una red MPLS utilizando equipos MikroTik y el emulador GNS3 en entornos PYMES

1.5. Objetivos específicos

1. Analizar el protocolo MPLS.
2. Analizar los equipos MikroTik para el diseño de la red MPLS.
3. Diseñar la red MPLS utilizando equipos MikroTik.

4. Simular la red MPLS mediante el software GNS3.
5. Analizar y comparar los resultados.

1.6. Metodología a utilizar

Los métodos a utilizar para el siguiente proyecto de titulación se dividirán en dos fases claramente definidas: deductivo y experimental.

El método deductivo permitirá recolectar información general mediante la investigación de trabajos relacionados acerca de la tecnología MikroTik para luego enfocarnos en lo particular, en este caso el funcionamiento de los equipos *routerOS* sobre el protocolo MPLS, mientras que por otro lado el método experimental permitirá analizar el comportamiento de tráfico entre redes LAN y definir cuáles son los equipos capaces de soportar el protocolo MPLS mediante la simulación de dicho esquema utilizando el software GNS3 el cual permite simular este tipo de redes lo más cercano a la realidad.

2. CAPÍTULO II. MARCO TEÓRICO

2.1. Multiprotocol Label Switching

2.1.1. Definición de MPLS

Multiprotocol Label Switching (MPLS) es un protocolo que fue desarrollado en los años 90, se encuentra ubicado entre la capa de enlace de datos y la capa de red del modelo OSI como se muestra en la figura 1. Adicionalmente se puede decir que toma características de ambas capas como son: conmutación de capa 2 y ruteo de capa 3 transformándose en una capa 2.5.

Figura 1. Modelo OSI que incluye el protocolo MPLS.

El objetivo principal para el cual fue diseñado este protocolo es el de unificar el transporte de datos reduciendo el procesamiento del paquete cada vez que llega a un router en la red, mejorando el desempeño de forma significativa en el reenvío de dichos paquetes y el rendimiento de los enrutadores. En la actualidad con el crecimiento de las telecomunicaciones, MPLS es capaz de transportar servicios tales como: voz, video, datos e internet. Para resumir todo lo antes expuesto podemos indicar que la palabra MULTIPROTOCOLO hace referencia a cualquier protocolo de capa 2, mientras LABEL SWITCHING es el ruteo de los paquetes mediante etiquetas. (Vélez, 2018)

2.2. Estructura MPLS.

En la figura 2 se visualiza un esquema de la cabecera MPLS haciendo relación con la capa de red y datos. En total se observa los 32 bits del paquete MPLS, 8 bits del tiempo de vida del paquete TTL (time-to-live), 1 bit que permite colocar etiquetas de manera jerárquica (S), 3 bits que sirven para identificar el tipo de servicio (EXP) y finalmente los 20 bits de la etiqueta MPLS.

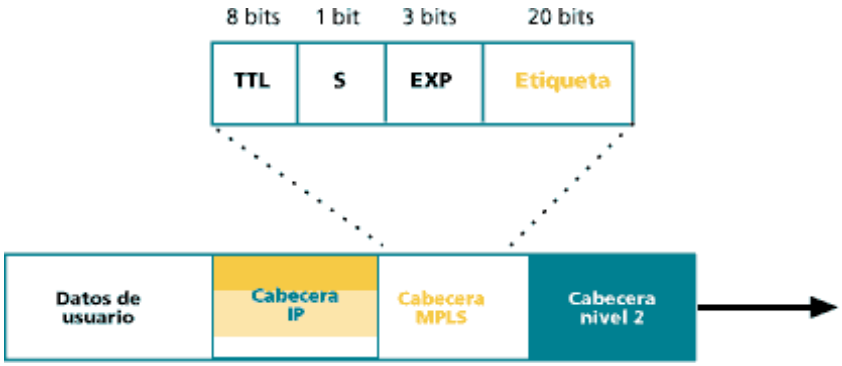


Figura 2. Cabecera MPLS.

Tomado de (Barberá, 2007)

2.3. Componentes de la red MPLS

En la figura 3 se encuentran los componentes principales de una red MPLS y su esquema de funcionamiento.

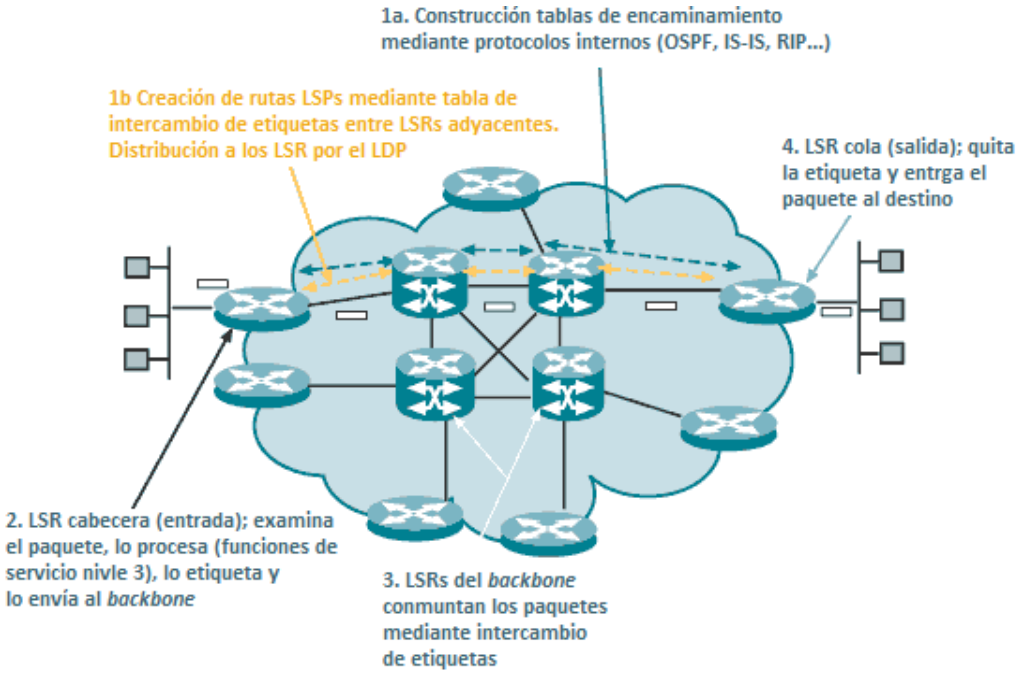


Figura 3. Elementos de una red MPLS.

Tomado de (Barberá, 2007)

1a) Tabla de enrutamiento

Está confirmada por protocolos de enrutamiento interno, tales como: OSPF (Open Shortes Path First), IS-IS (Intermediate System to Intermediate Syatem), RIP (Routing Information Protocol), etc.

1b) Creación de rutas LSP (Label Switched Path)

Es un camino o ruta virtual formada por los routers LSRs de acuerdo a su jerarquía mediante un conjunto de etiquetas utilizadas para el reenvío de paquetes en la red MPLS. Dicho camino virtual puede ser establecido a través protocolos de enrutamiento o también manualmente.

2) LSR Cabecera (Label Switch Router) o LER (Label Edge Router)

Es un router de frontera LER, encargado de crear la cabecera MPLS, insertar la etiqueta en el paquete FEC (Forwarding Equivalence Class) y lo envía al backbone MPLS.

Las etiquetas definen flujos o caminos de paquetes entre 2 puntos remotos, a esto se lo denomina FEC y cada uno es diferente de otro. Por lo tanto, los flujos tienen caminos específicos a través de los enrutadores LSR en la red.

Los FEC también tienen otra característica muy importante el cual es definir rutas mediante calidad de servicio (QoS).

3) LSRs de backbone

Son conocidos también como routers de tránsito, encargados de modificar la cabecera MPLS y reenviar el paquete al siguiente LSR. En la figura 4 se observa un ejemplo funcional de un router LSR, donde en primera instancia el paquete ingresa al router por la interfaz 3 con la etiqueta 45 luego se le asigna la etiqueta 22 y es reenviado por la interfaz 4 al siguiente LSR. (Barberá, 2007)

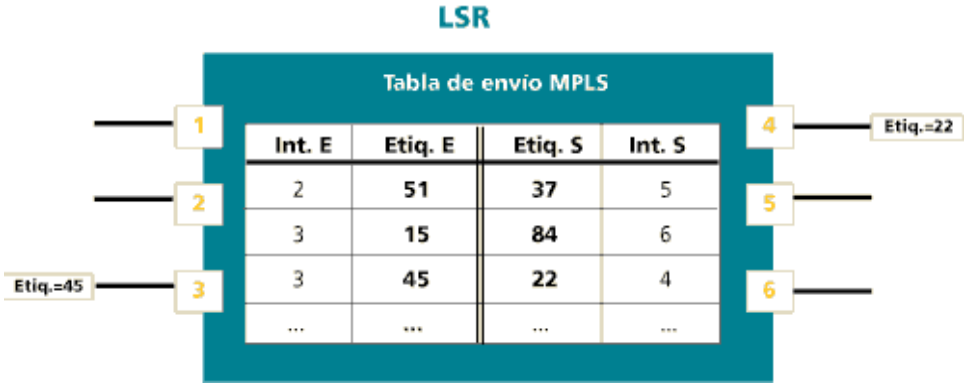


*Figura 4.*Tabla de envío MPLS en un router LSR.

Tomado de (Barberá, 2007)

LDP (Label Distribution Protocol) es un protocolo que se encarga de la distribución de etiquetas en un entorno MPLS a través de procedimientos y mensajes con los cuales los routers LSRs establecen caminos de conmutación de etiquetas LSP. Dicha conmutación la realizan mediante un mapeo de la información de enrutamiento de la capa de red (capa3) directamente a las vías o carreteras conmutadas de la capa de enlace de datos (capa 2).

4) LSR cola

Es un router de frontera de igual manera también conocido como LER encargado de retirar la cabecera MPLS y enviar el paquete a la red IP.

2.4. Arquitectura de la red MPLS

La arquitectura de la red MPLS está compuesta de elementos que cumplen un rol fundamental, dicha arquitectura puede ser visualizada en la figura 5.

A continuación, se detallan los elementos básicos de una red (MPLS):

- P o LSR.- Es un router de alta gama que trabaja en el Core del ISP realizando el reenvío de los paquetes etiquetados.

- PE o ELSR (Edge Label Switching Routing).- Tiene la función de realizar el etiquetado y el retiro de las etiquetas en los paquetes, estas funciones dependen del punto de origen del paquete.
- CE o CPE (Customer Edge).- Llamado también Equipo Local del Cliente, es un router instalado dentro de las instalaciones del cliente que tiene comunicación con el router PE de proveedor.

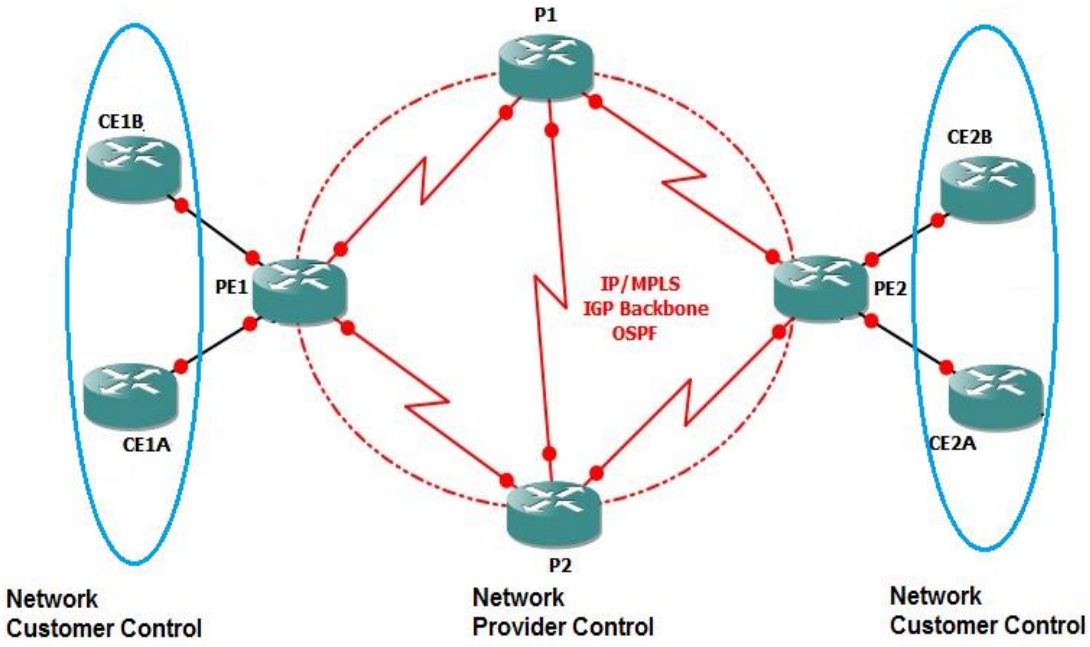


Figura 5. Arquitectura MPLS.

Una etiqueta MPLS es un identificador que se emplea localmente para definir una FEC en un ambiente MPLS. Cabe indicar que dicha etiqueta es importante localmente porque tiene la capacidad de señalar diferentes rutas o FECs en distintos routers LSRs.

2.5. Protocolos en una red MPLS

Una red MPLS generalmente utiliza los siguientes protocolos internos (IGP); Open Shortest Path First (OSPF) e Intermediate System to intermediate System (IS-IS) para conocer la topología de red, establecer los caminos de

menor costo y proporcionar información adecuada con el objetivo de calcular rutas de ingeniería de tráfico (TE). (Farrel, 2017)

2.5.1. IGP (Internal Gateway Protocol)

El Protocolo de Gateway Interior, es utilizado para intercambiar información de enrutamiento entre routers dentro de un Sistema Autónomo.

2.5.2. OSPF (Open Shortest Path First)

Conocido como protocolo del camino más corto, su métrica es el costo con el cual calcula el camino más corto entre dos nodos mediante diversos parámetros tales como la congestión de los enlaces y el ancho de banda. OSPF también tiene la ventaja de dividir los Sistemas Autónomos en áreas cuando estos son muy grandes y difíciles de administrar. Para esto utiliza LSA (Link State Advertisement) para la comunicación entre routers vecinos con el objetivo de obtener la información necesaria para formar la tabla topológica. (Vélez, 2018)

Tabla 1.

Tipos de SLA

Tipos de SLA	Descripción
1	Router LSA: Lista de interfaces, estado y costo de cada enlace, solo se publica dentro del área.
2	Network LSA: Lista de routes conectados
3y4	Sumary LSA: Se origina en el ABR hacia su propia área.
5	External SLA: Publican rutas externas.

6	Multicast OSPF LSA: Usado en multicast OSPF.
7	NSSA External LSA: similares a los LSA tipo 5 pero no propagan las rutas por toda la red.
8	External attribute LSA for Border Gateway Protocol (BGP): Para enrutar BGP dentro de OSPF.
9,10,11	Opaque LSAs: Reservados para aplicaciones específicas.

A continuación, se analizan las áreas que maneja el protocolo OSPF:

Área de Backbone.- Es también conocida como área cero, dentro de una topología OSPF es el área principal, a esta área se tienen que conectar las demás áreas de la red.

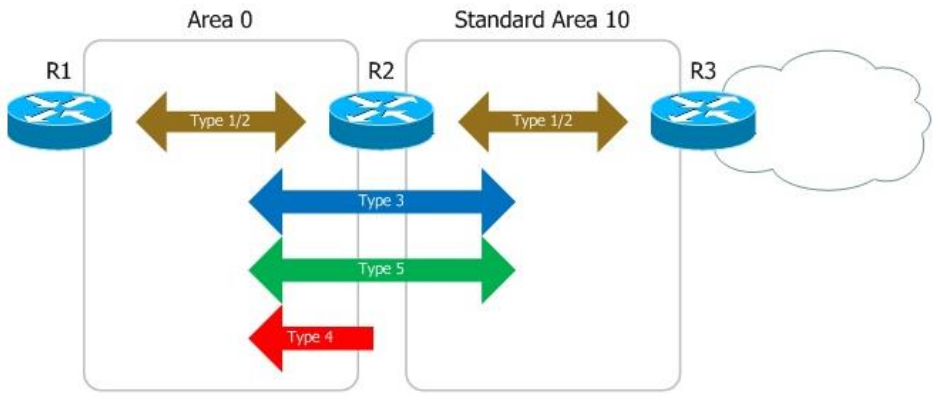


Figura 6. Área 0 y tipos de LSAs que permite.

Tomado de (Martínez, 2013)

Área Estándar.- Utiliza LSAs de tipo tres y cinco debido a que se publican rutas internas y externas. En esta área cada enrutador tiene su propia tabla de enrutamiento.

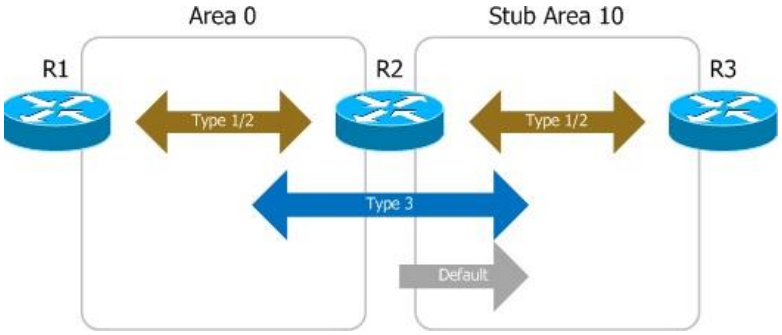


Figura 7. Área Estándar y tipos de SLAs que permite.

Tomado de: (Martínez, 2013)

Stub Área.- Esta área no permite LSA de tipo cinco, utiliza LSA de tipo tres la cual contiene una ruta por defecto o predeterminada (0.0.0.0) cuando la información proviene de un AS (sistema autónomo) diferente. Generalmente esta área es utilizada en topologías hub-and-spoke.

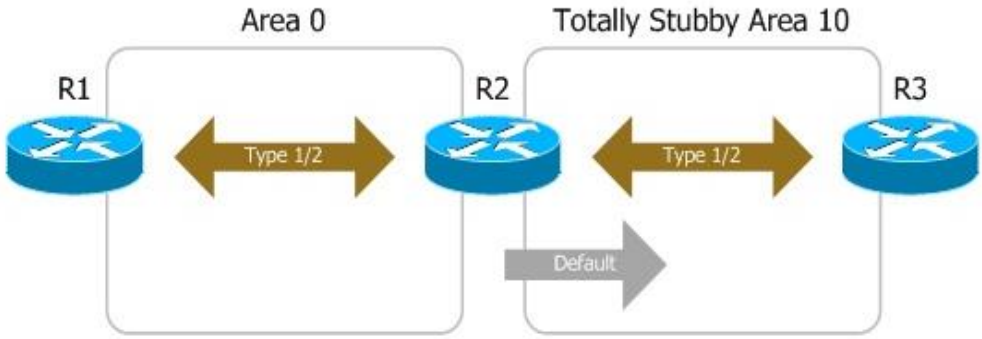


Figura 8. Stub Área y tipos de SLAs que permite.

Tomado de (Martínez, 2013)

Área Totally Stub.- Área propietaria de Cisco, no permite LSA de tipo tres, cuatro y cinco lo que quiere decir que no acepta rutas de AS externos. De igual manera que Stub Área, esta área envía una ruta por defecto (0.0.0.0) para las rutas externas y las sumarizadas.

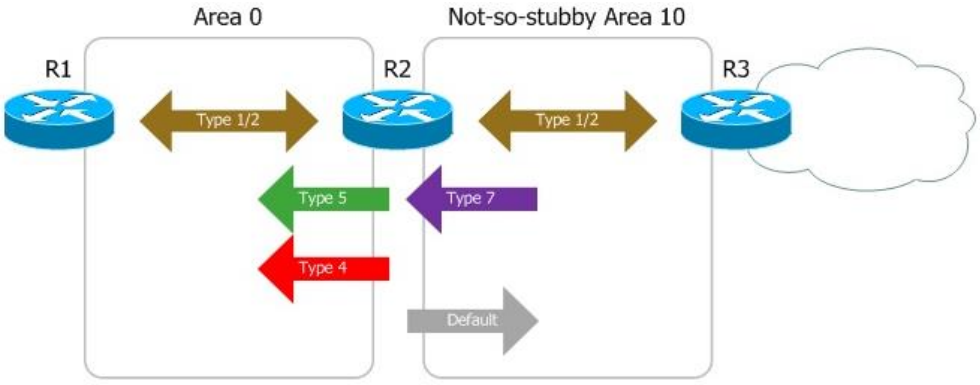


Figura 9. Área Totally Stub y tipos de SLAs que permite.

Tomado de (Martínez, 2013)

Área NSSA.- No permite LSA de tipo cuatro y cinco al igual que Stub no acepta rutas externas por lo que tiene una ruta predeterminada (0.0.0.0). Se diferencia de la Stub porque NSSA si permite que un ASBR (Autonomous System Boundary Router) se comunique con otro tipo de protocolo de enrutamiento, por lo tanto, en esta área aparecen los LSA de tipo siete para que el ABR recibe rutas dentro del área como LSA siete desde el ASBR, las traduce a cinco y las trata de forma normal.

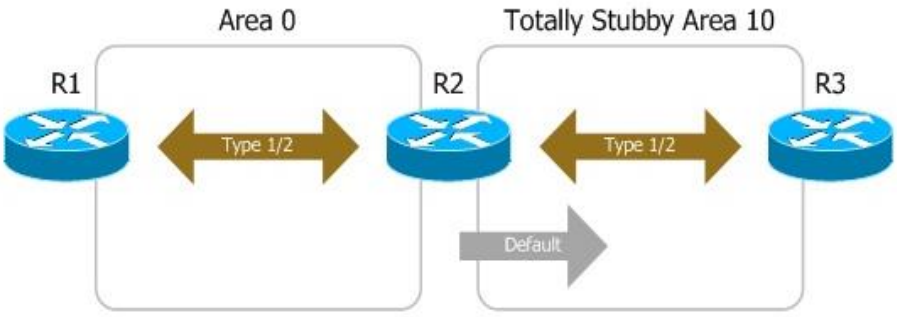


Figura 10. Área NSSA y tipos de LSAs que permite.

Tomado de (Martínez, 2013)

Totally Stubby NSSA Área.- Esta área también es propietaria de Cisco, trabaja de manera similar al área NSSA pero utilizando ASBR (Autonomous System Boundary Router) directamente.

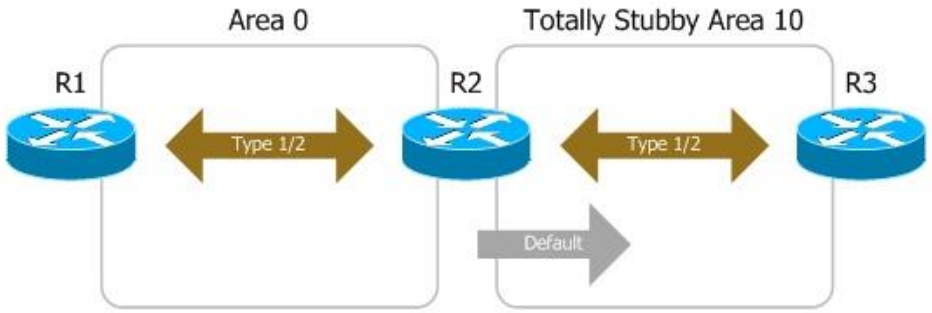


Figura 11. Totally Stubby NSSA Área y tipos de LSAs que permite.

Tomado de (Martínez, 2013)

2.5.3. BGP (Border Gateway Protocol)

BGP es un protocolo que permite intercambiar tablas de enrutamiento IP entre redes que se encuentran en sistemas autónomos diferentes (AS). Este protocolo es muy utilizado por proveedores de servicios de Internet por tener gran escalabilidad. El protocolo BGP intercambia información estableciendo sesiones de comunicación entre los routers de frontera que se encuentran en los sistemas autónomos. Este protocolo garantiza que la entrega de paquetes sea fiable al trabaja sobre el protocolo TCP con el puerto 179.

A continuación, se presenta las dos variantes que presenta el protocolo BGP:

- IBGP (Internal Border Gateway Protocol).- Este protocolo realiza el intercambio de información dentro de un sistema autónomo.
- EBGP (External Border Gateway Protocol).- Realiza el intercambio de información entre sistemas autónomos diferentes.

2.5.3.1. Tipos de mensajes BGP

BGP maneja cuatro tipos de mensajes de comunicación entre routers que se detallan a continuación:

- Open.- Se utiliza para iniciar o establecer una sesión BGP, para lo cual realiza negociaciones de parámetros y características entre routers. Un

ejemplo puede ser verificar que los router tengan la misma versión de protocolo BGP.

- Update.- Este mensaje se utiliza para actualización de nuevos prefijos y nuevas rutas establecidas.
- Keepalive.- Se utiliza para mantener viva la sesión BGP una vez que ésta ya se encuentre establecida, envía mensajes periódicamente para confirmar que el otro extremo continúa activo.
- Notification.- Este tipo de mensaje se utiliza para finalizar una sesión BGP cuando ocurre algún tipo de error.

2.5.3.2. Tipos de estados BGP

En el proceso para establecer vecindades BGP atraviesa por los siguientes estados:

- Idle.- Es el estado inicial para establecer vecindad, este estado requiere de un evento inicial para el transporte de información.
- Connect.- Se encuentra a la espera de una conexión TCP. Si se logra completar la conexión se enviará un mensaje de OPEN.
- Active.- Este estado ocurre cuando uno de los extremos no puede establecer comunicación y lo reintenta periódicamente.
- OpenSent.- El extremo envía un mensaje tipo “keepalive” o de identificación.
- OpenConfirm.- Se encuentra a la espera del mensaje “keepalive”. Si no recibe dicho mensaje el tiempo expira y pasa al estado inicial “Idle”. Pero si lo recibe pasa al siguiente estado “established”.
- Established.- En este estado la sesión está completamente activa.

2.6. Aplicaciones de MPLS y sus Beneficios

El protocolo MPLS desde su creación ha presentado diversas aplicaciones y beneficios con el objetivo de facilitar la transmisión de información de una manera rápida, segura y que sea escalable con tecnologías existentes.

A continuación, se muestra algunos aplicativos importantes donde se utiliza el protocolo MPLS.

- Ingeniería de Tráfico
- VPN (Red Privada Virtual)
- Clases de Servicios (CoS)

2.6.1. Ingeniería de Tráfico

Se entiende por Ingeniería de tráfico al proceso para asegurar que el flujo de información que cursa por una red sea eficiente y fiable, pero al mismo tiempo que el rendimiento sea óptimo.

La ingeniería de tráfico tiene como objetivo, adaptar los flujos de tráfico a los recursos físicos existentes en una red. Esto se logra utilizando de forma eficiente los recursos físicos, de tal manera que no exista saturación y tampoco cuellos de botella en ciertos puntos de la red, mientras que en otros puntos pueda existir poco flujo de tráfico.

A inicios de los años 90 los procedimientos utilizados para adaptar de manera efectiva los flujos de tráfico en una red IP eran rudimentarios. El uso del protocolo IGP, encargado de calcular el camino más corto fue bastante utilizado. Sin embargo, en casos de congestión o cuellos de botella se realizaba un aumento de la capacidad de los enlaces. La ingeniería de tráfico como se indicó previamente, consiste en ubicar ciertos flujos seleccionados por el protocolo IGP de enlaces más congestionados, a otros enlaces menos congestionados, a pesar que estos estén en una ruta con más saltos. (Barberá, 2007)

En la figura 12 se muestran dos tipos de rutas, una con el camino más corto IGP y el otro con ingeniería de tráfico que utiliza un salto adicional, pero es el camino menos congestionado.

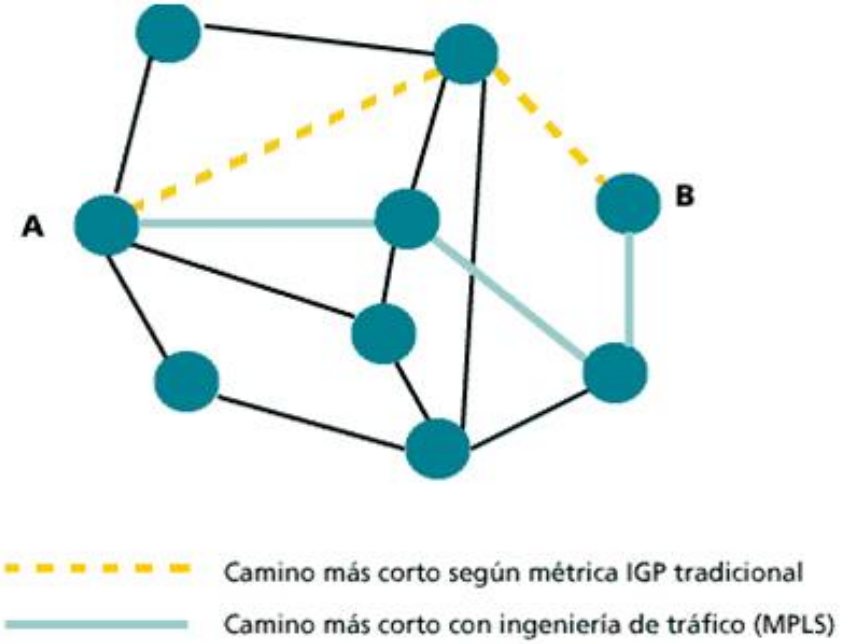


Figura 12. Comparación de ruta entre métrica IGP con Ingeniería de tráfico.

Tomado de (Martínez, 2013)

2.6.2. VPN (Red Privada Virtual)

Una Red Privada Virtual (VPN) es una red que interconecta dos o más puntos de manera permanente sobre una infraestructura compartida, posee funcionalidades y características equivalentes a una red privada. La seguridad es una característica muy importante en las VPNs ya que ninguna persona pude ingresar a la red para obtener información o utilizar recursos mientras no sea miembro de dicha red IP VPN. (Barberá, 2007)

Las VPNs se dividen en 2 tipos:

- VPNs capa 2 y
- VPNs capa 3

Las VPNs capa 2 como su nombre lo indica trabajan a nivel de capa 2 o capa de enlace de datos del modelo OSI. En este caso el Proveedor del servicio no configura o no realiza ningún tipo de ruteo a nivel de IP, esto quiere decir que el cliente es el que realiza su enrutamiento utilizando cualquier protocolo de capa

3 que desee. Con las VPN L2 se lograr tener comunicación punto–multipunto o punto–punto dentro de la red MPLS permitiendo la tercerización de servicios entre Proveedor del servicio y clientes. Las VPNs de capa 3 son aquellas cuando el router CE se encuentra instalado en el cliente y tiene conexión con el router PE mediante protocolos de capa 3. Entonces el proveedor de servicios participa en el enrutamiento con el cliente, mientras que por otro lado el cliente puede ejecutar los protocolos OSPF, EIGRP, BGP o cualquier otro protocolo de enrutamiento. Por otro lado VPNs L3 garantizan que la información de enrutamiento de un cliente esté completamente separada de otros clientes mediante una VRF (Virual Routing Forwarding) asignada para cada cliente. (Barberá, 2007)

2.6.2.1. VRF (Virtual Routing and Forwarding)

Como se mencionó anteriormente para separar el tráfico de diferentes clientes se utilizan VRF en lugar de utilizar tablas de enrutamiento. En la figura 13 se observa dos clientes conectados a la red del proveedor de servicio, los clientes A y B tienen un mismo rango de IPs pero con diferente VRF.

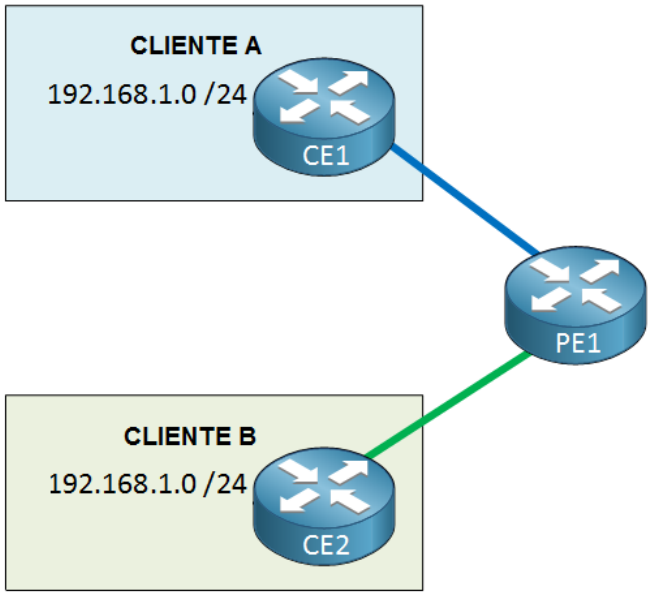


Figura 13. VPN L3 utilizando VRF para discriminar el tráfico.

Una característica importante de las VRFs es que se las configura en los routers PEs, los cuales están directamente conectados al CE.

2.6.3. Clases de Servicios (CoS)

Una red MPLS está creada para que pueda transportar servicios diferenciados, de acuerdo al Modelo DiffServ del IETF (Internet Engineering Task Force). Dicho modelo define una gran variedad de procedimientos para clasificar el tipo de tráfico en clases de servicio, con diferentes prioridades.

El modelo DiffServ permite clasificar el tráfico en un reducido número de clases de servicio que no son muy críticos como son: el correo electrónico e internet de servicios críticos que no aceptan el retardo tales como voz y video en línea. Por tal razón, se emplea el campo ToS (Type of Service) que es la técnica de calidad de servicio (QoS) para marcar los paquetes que son enviados a la red. (Barberá, 2007)

3. CAPÍTULO III. EQUIPOS MIKROTIK.

3.1. Inicios

La empresa MikroTik fue creada en Latvia (Letonia) en el año 1995 con la finalidad de proveer un sistema operativo eficiente. En el año 1997 dicho sistema operativo toma el nombre de RouterOS. La evolución de este sistema operativo conllevo a la creación de un hardware robusto, con grandes capacidades de procesamiento por sus múltiples núcleos conocido como RouterBOARD el cual tuvo su lanzamiento en el año 2002. La incursión de MikroTik en Latinoamérica comenzó hace más de una década en las empresas INDEX (México) y REICO (Costa Rica) quienes tuvieron la iniciativa de implementar soluciones basadas en software RouterOS y hardware RouterBOARD. (Roosevelt, 2016)

A través de los años MikroTik ha evolucionado con el objetivo claro de brindar equipos de comunicación que tengan fiabilidad, escalabilidad y sobre todo que se encuentren a la par de grandes marcas ya posicionadas en el mercado pero

que lamentablemente poseen un alto costo tanto para el proveedor como para el cliente final. En la actualidad MikroTik ofrece una gran variedad de equipos de comunicación como son; switches, módems 4G y como se mencionó anteriormente, antenas para enlaces de radio y routers de baja, mediana y gran capacidad.

3.2. Software

A continuación, se enlistan los 2 sistemas operativos que maneja MikroTik para sus diferentes equipos de comunicación:

- RouterOS
- SwOS

A partir del segundo semestre del año 2017, los equipos CRS3xx utilizan la función DUAL BOOT para que, cuando los switches necesiten capacidades simplificadas de conmutación los usuarios activen SwitchOS, mientras que, si necesita funciones de enrutamiento y funciones de capa 3 en algunos puertos activarán RouterOS, estas funciones pueden ser activadas desde RouterOS, SwitchOS o desde las opciones de RouterBOOT.

3.2.1. RouterOS

Es un sistema operativo Open Source, creado por MikroTik con una gran variedad de características disponibles tales como; firewall, router, switch, etc. Adicionalmente posee protocolos propietarios a nivel inalámbrico lo que lo convierte en un sistema operativo todo en uno. Sin embargo, existe una característica muy importante e innovadora el cual consiste en convertir cualquier PC en un router con las mismas características que posee un RouterOS, siendo una gran ventaja frente a sus competidores. (Roosevelt, 2016)

RouterOS dispone de varias interfaces de administración gráfica, facilitando al operador la configuración y administración del equipo.

3.2.2. SwOS

Es un Sistema Operativo que deriva del RouterOS diseñado específicamente para configurar la línea de Switches de la marca MikroTik. Al igual que el Sistema Operativo RouterOS, permite la configuración de puertos, VLan, spanning tree, mirror, velocidades en un ambiente más simplificado por lo que se considera un Sistema Operativo diseñado específicamente para la administración de productos de conmutación MikroTik. (Mikrotik, wiki.mikrotik, 2013)

SwOS es configurable desde su navegador web la cual brinda toda la funcionalidad básica para un conmutador administrado, permite administrar el reenvío de puerto a puerto, el control de tormentas de difusión, aplicar el filtro MAC, configurar las VLAN, duplicar el tráfico, aplicar la limitación de ancho de banda e incluso ajustar algunos encabezados de MAC e IP.

3.3. Hardware

A continuación, se enlistan los equipos MikroTik más utilizados en el mercado:

- Routers (RouteBoard)
- Switches (SwitchBoard)
- Sistemas inalámbricos para enlaces de exteriores
- Antenas

3.3.1. RouterBOARD

Es un router MikroTik robusto que permite trabajar en una gran cantidad de escenarios con excelentes resultados, al igual que otros routers la capacidad de servir a la red es proporcional al modelo de router instalado. Es importante indicar que el software de gestión del equipo (RouterOS) es el mismo para todos los modelos disponibles, es decir no hay ninguna diferencia en el software que se encuentra instalado en un router básico con uno más robusto. Lo que hace diferente a un router básico de un router robusto es el nivel de licenciamiento, level 4, 5 o 6, lo que define la capacidad para configurar

conexiones en el router, por ejemplo, la licencia básica que viene incluida en los routers de gama baja es level 4, esta licencia permite configurar un número máximo de conexiones, en caso de requerir un número mayor de conexiones. Se debe instalar la licencia level 5 o 6 según sea el caso. Es importante resaltar que los routers de gama alta y media ya vienen incluidos la licencia level 6 y 5 respectivamente, esto tiene mucha lógica debido a que las licencias son proporcionales a las capacidades de memoria, procesamiento e interfaces disponibles en el router.

En la figura 14 se puede observar los diferentes niveles de licenciamiento y sus diferencias. Los niveles 0 y 1 están dentro de las licencias demo, el nivel 3 es una licencia de estación inalámbrica, mientras que los niveles 4,5 y 6 son licencias comerciales que tiene su respectivo costo.

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	do not sell	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Figura 14. Cuadro de licenciamiento MikroTik.

Tomado de (Mikrotik, wiki.mikrotik, 2013)

3.3.1.1. Licenciamiento en equipos MikroTik RouterBOARD

Licencia Nivel 3.- Esta licencia está enfocada para el uso en estaciones Wireless o WISP CPE (Cliente WiFi, cliente o CPE). Para arquitecturas x86 la licencia Nivel 3 no pude ser adquirida de forma individual solos se adquieren licencias por paquetes de 100.

Licencia Nivel 4.- Está enfocada para equipos CPEs, Wireless de mediana capacidad que son utilizados especialmente por ISPs para instalación de clientes corporativos PYMES.

A continuación, se puede visualizar una descripción de un CPE MikroTik con nivel de licencia 4.

Características técnicas:

- Modelo: RB750UPr2.
- CPU núcleos: 1
- Frecuencia de CPU: 650MHz
- Sistema Operativo: RouterOS
- Nivel de licencia: 4
- Memoria RAM: 64MB
- Puertos Ethernet: 5 (El puerto 1 o POE IN puede recibir electricidad y encender el equipo, pero no proporciona electricidad).
- Puertos USB: 1
- Fuente de poder: AC/DC 12V.
- Indicadores Led: Encendido, Puertos Ethernet, Wireless (para modelos con wifi), Actividad.
- Botón de Reset.

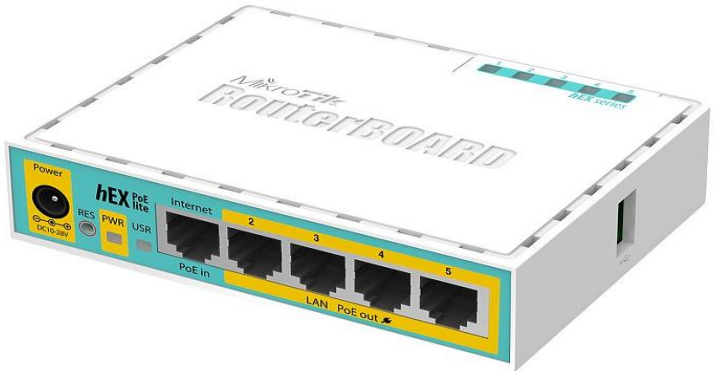


Figura 15. RouterBOARD RB750UPr2.

Tomado de (Mikrotik, MikroTik, 2019)

Licencia Nivel 5.- Este rango de licencia al igual que la anterior es utilizado por equipos Wireless pero de gran capacidad y de largo alcance, excelente para ISPs de gran capacidad.

A continuación, se muestra un equipo MikroTik con licenciamiento de nivel 5:

El RB3011 es un dispositivo multipuerto, el primero en ejecutar un CPU de arquitectura ARM para un rendimiento más alto. El RB3011 tiene diez puertos Gigabit divididos en dos grupos de conmutadores, una caja SFP y un puerto USB 3.0 SuperSpeed de tamaño completo, para agregar almacenamiento o un módem externo 3G / 4G. (Mikrotik, MikroTik, 2019)

Características técnicas:

- Modelo: RB3011UiAS-RM
- CPU núcleos: 2
- Frecuencia de CPU: 1.4GHz
- Sistema Operativo: RouterOS
- Nivel de licencia: 5
- Memoria RAM: 1G
- Puertos Ethernet 10/100/100: 10
- Puertos SFP: 1
- Puertos USB 3.0: 1

- Fuente de poder: AC/DC 12V.
- Botón de Reset.

Figura 16. RouterBOARD RB3011UiAS-RM.

Tomado de (Mikrotik, MikroTik, 2019)

Licencia Nivel 6.- Este nivel de licencia es utilizada por equipos de infraestructura interna como son; CLOUD y CORE. Los clientes frecuentes de estas licencias son ISPs de gran capacidad.

A continuación, se muestra un equipo MikroTik con licenciamiento de nivel 6:

El router RB1100AHx4 tiene una CPU Annapurna Alpine AL21400 con 4 núcleos Cortex A15 a 1.4GHz cada uno, para un rendimiento máximo de hasta 7.5Gbps. El dispositivo es compatible con la aceleración de hardware IPsec. (Mikrotik, MikroTik, 2019)

Características técnicas:

- Modelo: RB1100Dx4
- CPU núcleos: 4
- Frecuencia de CPU: 1.4GHz
- Sistema Operativo: RouterOS
- Nivel de licencia: 6
- Memoria RAM: 1G
- Puertos Ethernet 10/100/100: 13
- Puertos Sata: 2
- Puerto Serial: 1

- Puerto para MicroSD: 1
- Fuente de poder: AC/DC 12V.
- Botón de Reset.

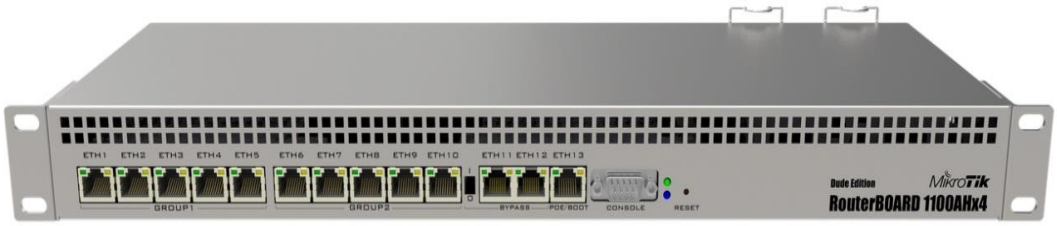


Figura 17. RouterBOARD RB1100Dx4.

Tomado de (Mikrotik, MikroTik, 2019)

MikroTik como empresa innovadora también se encuentra incursionando en la creación de equipos de core cloud.

A continuación, se muestra un equipo robusto con grandes características técnicas para soluciones cloud.

El router cloud CCR1072, está alimentado por una CPU de núcleo Tilera 72, cada núcleo tiene una velocidad de 1 GHz, y para utilizar completamente esta alimentación, el CCR1072 está equipado con ocho puertos 10G SFP + conectados de forma independiente y un solo puerto Ethernet para fines de administración. (Mikrotik, MikroTik, 2019)

Características técnicas:

- Modelo: CCR1072-1G-8S+
- CPU núcleos: 72
- Frecuencia de CPU: 1.GHz
- Sistema Operativo: RouterOS
- Nivel de licencia: 6
- Memoria RAM: 16G
- Puertos Ethernet 10/100/100: 1

- Puertos SFP: 8
- Puertos USB 3.0: 2
- Puerto Serial: 1 RJ45
- Fuente de poder: AC/DC 12V.
- Monitor de voltaje: 1
- Botón de Reset.

Figura 18. RouterBOARD CCR1072-1G-8S+

Tomado de (Mikrotik, MikroTik, 2019)

3.3.2. Métodos de Administración para MikroTik RouterOS

3.3.2.1. WebFig (WEB Browser)

Como su nombre lo indica es una interfaz de acceso basada en Web que permite; monitorear, configurar y realizar tareas de troubleshooting dentro del router. Para el acceso únicamente se requiere abrir un navegador y colocar la IP configurada por defecto 192.168.88.1 por lo que no se requiere de un software adicional previamente configurado. (Roosevelt, 2016)

A continuación, se detallan los pasos para el ingreso al equipo por Web Browser:

- Conectar un cable Ethernet en el puerto 1 del router y el otro extremo a una PC.
- Abrir un navegador (Mozilla, Chrome, Internet Explorer, etc.).
- Escribir en el browser la IP 192.168.88.1

- En la casilla de usuario colocar admin y en la casilla de contraseña queda en blanco por defecto. Como se muestra en la figura 19.

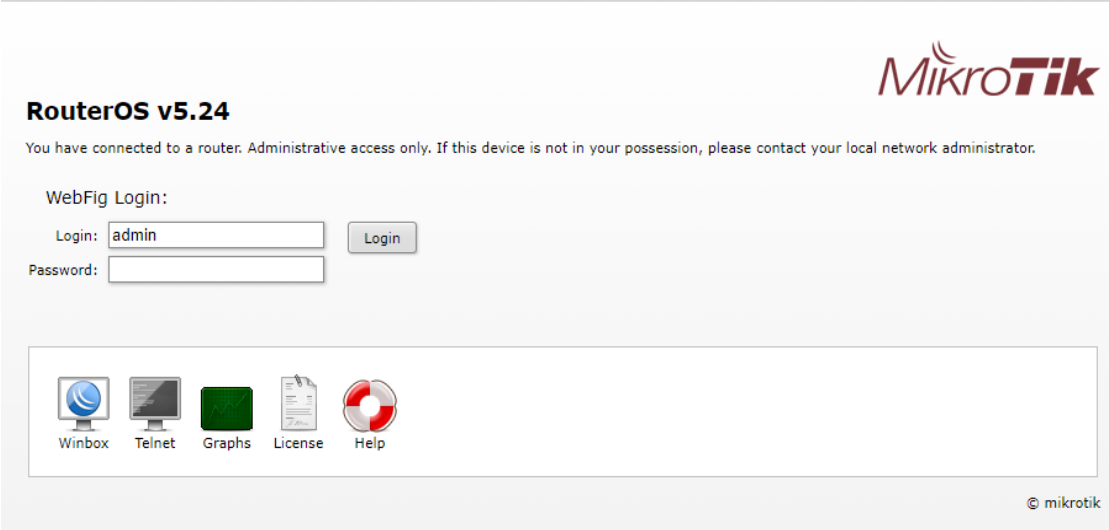


Figura 19. Entorno de ingreso al equipo por Web Browser.

Al momento de ingresar al equipo se podrá visualizar la configuración del equipo como se muestra en la figura 20.

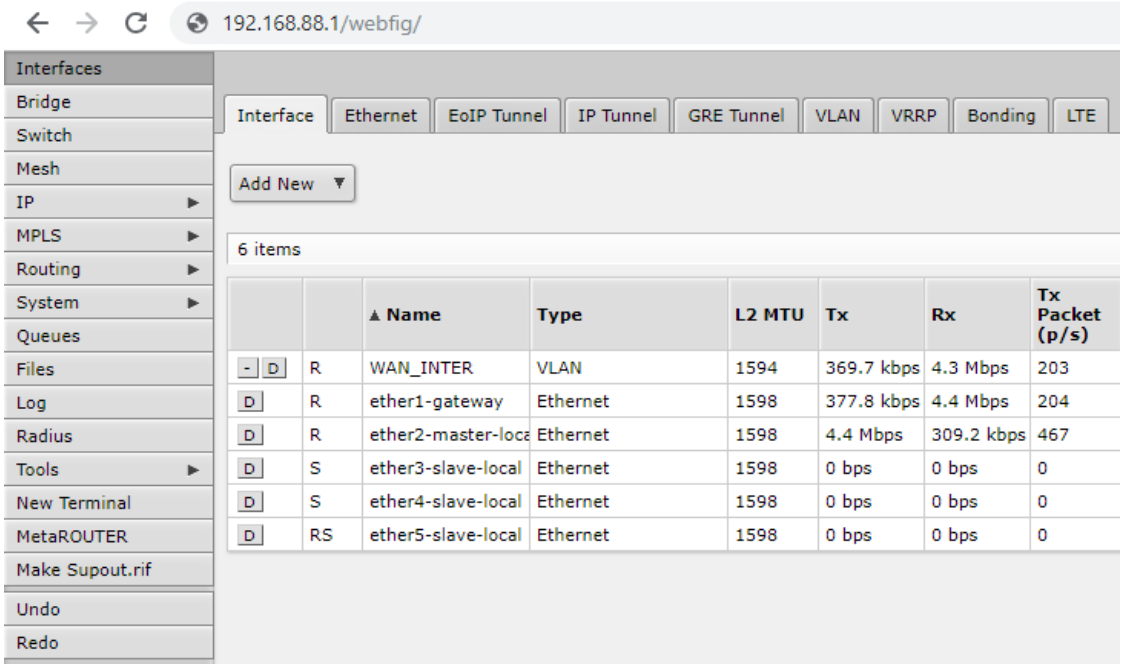


*Figura 20.*Entorno de configuración por Web Browser.

3.3.2.2. WinBox

Es un aplicativo Win32 diseñado para correr en sistemas operativos Windows, pero también tiene la capacidad de ser usado en Mac y Linux mediante wine. Fue desarrollado por MikroTik para permitir la administración de dispositivos MikroTik *RouterOS* utilizando una interfaz gráfica. Adicionalmente este software tiene la característica de ingreso al router mediante IP o Mac address, los usuarios pueden realizar conexiones vía telnet, SSH y FTP.

A continuación, se detallan los pasos para el ingreso al equipo por WinBox:

- Abrir el software WinBox.
- Ingresar la IP o la MAC del Router.
- Insertar el usuario y contraseña.
- Clic en conectar.

En la figura 21 se visualiza el loggin de acceso mediante WinBox por su dirección IP por defecto, es importante recalcar que el fabricante recomienda el ingreso usando la dirección IP en lo posible, debido a que las sesiones por MAC no son 100% seguras al utilizar broadcast de la red.

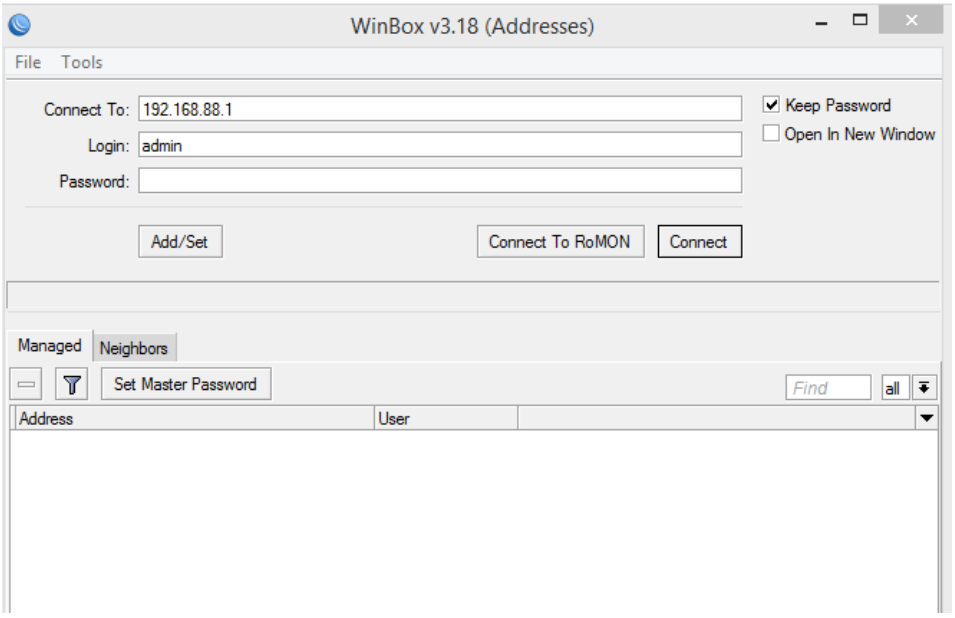


Figura 21. Ingreso al RouterOS por WinBox.

En la figura 22 se visualiza el ambiente de configuración de un RouterOS mediante el software WinBox. En la parte izquierda se encuentran las pestañas de configuración de una manera más amigable que en la presentada anteriormente con el ingreso por Web Browser.

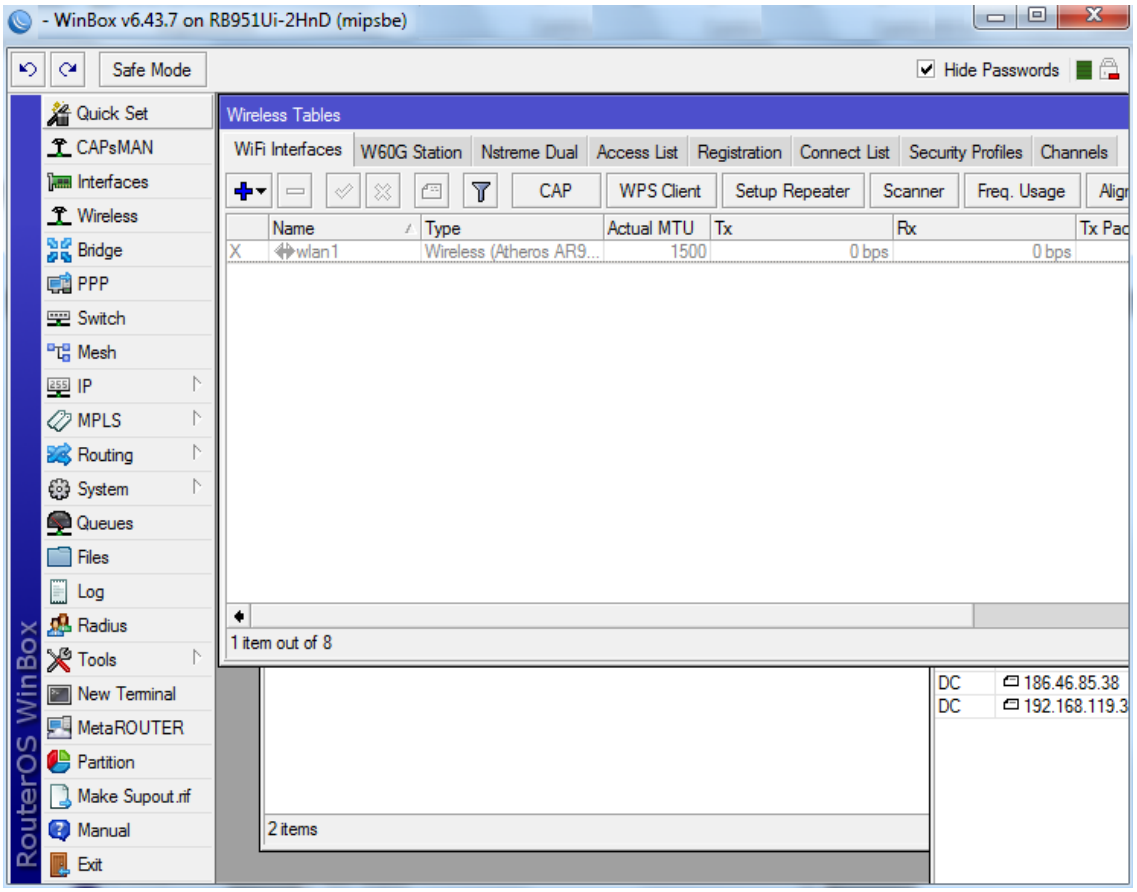


Figura 22. Entorno de configuración mediante WinBox.

Es importante mencionar que dentro de la configuración gráfica tanto vía Web y WinBox se encuentra la pestaña New Terminal que permite al usuario manejar el entorno de configuración por comandos emulando una conexión telnet o SSH como se muestra en la figura 23.

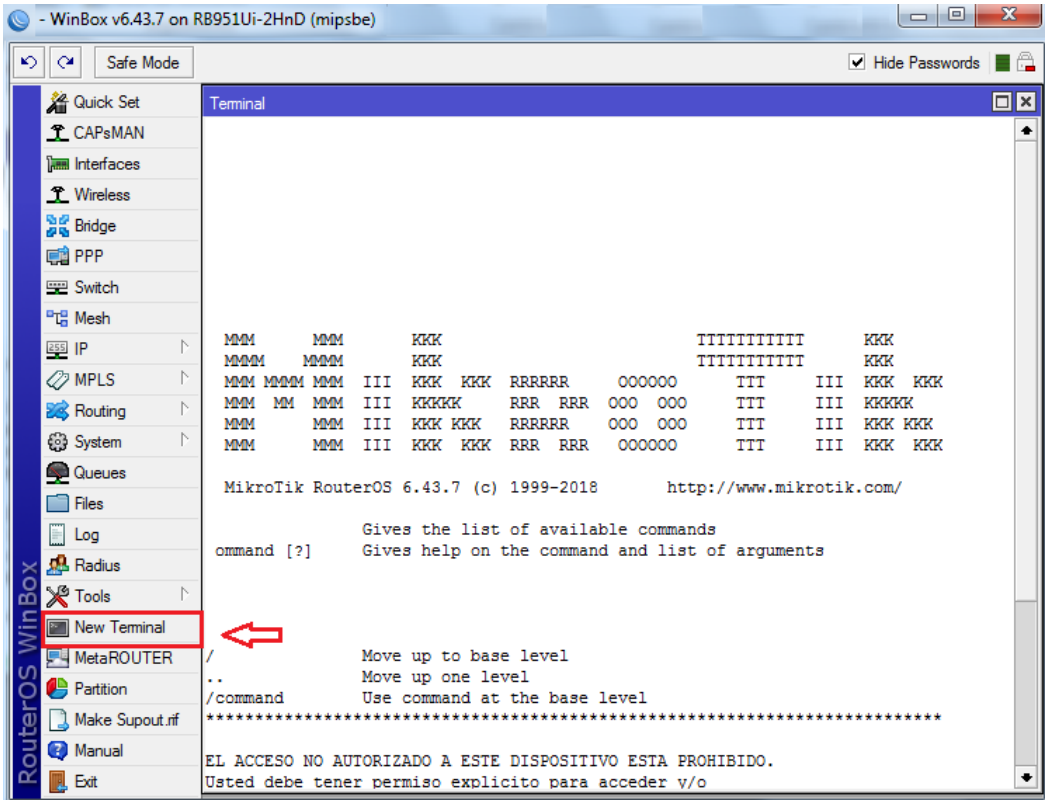


Figura 23. Entorno de configuración vía comandos dentro de WinBox.

3.3.2.3. Emulador de Terminal a través de conexión serial o puerto de consola (RS-232)

Los puertos seriales o (RS-232) fueron los primeros métodos de acceso a equipos informáticos, permitiendo el intercambio de información entre usuario y dispositivo. Es el método más utilizado para el acceso a equipos a través de interfaz de línea de comandos CLI (Command Line Interface), permite que los usuarios puedan dar instrucciones a programas informáticos por línea de texto. Este método es usado normalmente cuando se realiza el ingreso por SSH, Telnet u otros mediante los programas PuTTy, SOC, etc.

SSH y Telnet son herramientas IP estándar para el acceso a dispositivos, programas informáticos y también son formas de ingreso al MikroTik RouterOS.

- SSH: Utiliza el puerto 22/TCP, es un método seguro de ingreso a equipos que utilizan las empresas de telecomunicaciones debido a que

cifra la comunicación entre el usuario y el router. Un software disponible de código libre para acceso por SSH y telnet es la herramienta PuTTy.

- Telnet: Es una comunicación en texto plano que no utiliza cifrado el cual trabaja con el puerto 22/TCP. Al no utilizar cifrado es un método inseguro de acceso al router.

En la figura 24 se puede visualizar un típico entorno de configuración por comandos mediante PuTTY en un RouteOS.

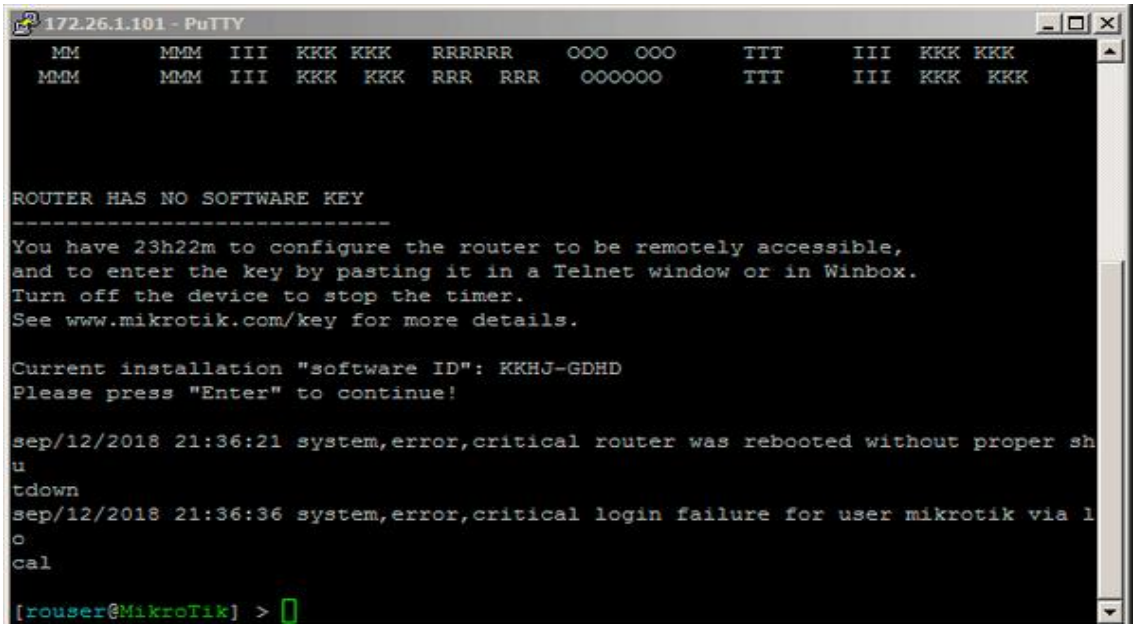


Figura 24. Entorno de configuración mediante PuTTY.

3.3.2.4. MikroTik App

Es un método de acceso implementado recientemente para facilitar al usuario la configuración de un RouterOS de manera remota a través de dispositivos móviles.

En la figura 25 se visualiza el entorno de ingreso a un RouterOS mediante MikroTik app.

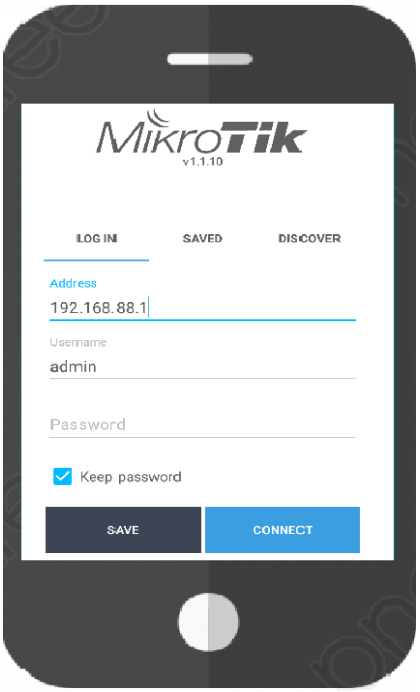


Figura 25. Ingreso al RouterOS por MikroTik App.

3.4. Características principales de un RouterOS

Existen una gran variedad de características que ofrece el dispositivo MikroTik RouterOS a pesar de no ser un equipo físicamente de grandes dimensiones, por tal razón es un dispositivo que atrae mucho a mercados que exigen grandes beneficios a un bajo costo. Entre las características más importantes están las siguientes: Firewall, Routing, VPN MPLS, WIFI, entre otras.

3.4.1. Firewall

En la actualidad, el firewall se ha convertido en una herramienta indispensable para proteger la información en una red LAN cuando se conecta a Internet. De hecho, el tener una conexión al mundo mediante Internet genera la posibilidad de múltiples ataques hacia la red interna. Para contrarrestar estos inconvenientes se generó un dispositivo llamado firewall con el objetivo de proteger la red interna.

El firewall integrado en un equipo MikroTik RouterOS provee funcionalidades de seguridad mediante un conjunto de reglas implementadas para controlar el

tráfico de la red. Conjuntamente con el NAT, crea una barrera que impide el acceso no autorizado. Adicionalmente filtra tráfico mediante IP, puertos TCP/UDP, protocolos, entre otros.

3.4.2. Routing

Es una de las funcionalidades más importantes del RouterOS ya que soporta protocolos de enrutamiento estático y dinámico tanto para IPv4 e IPv6.

- Para IPv4 soporta RIP v1 y RIP v2, OSPF v2, BGP v4
- Para IPv6 soporta RIPng, OSPFV v3 y BGP

En la figura 26 se visualiza la nomenclatura de etiquetas en las rutas más comunes de un RouterOS.

Etiqueta (Flag)	Descripción
`disabled` (X)	Regla de ruteo está deshabilitada. No tiene ningún efecto sobre las otras rutas y no se utiliza de ninguna manera para reenvío (forwarding) o protocolos de ruteo
`active` (A)	Ruta se utiliza para el reenvió de paquetes. Denota una ruta activa.
`dynamic` (D)	Regla de ruteo creada por el software y no por la interface de administración. No se exporta, y no puede ser modificado directamente.
`connect` (C)	Ruta conectada. Se genera cuando se configura una dirección IP en una interface activa
`static` (S)	Ruta estática. Ruta creada por el usuario de manera fija. Este método forzará el envío de paquetes a través de un Gateway definido por el usuario/administrador
`rip` (r)	Ruta RIP
`bgp` (b)	Ruta BGP
`ospf` (o)	Ruta OSPF
`mme` (m)	Ruta MME
`blackhole` (B)	Descarta silenciosamente el paquete reenviado por esta ruta
`unreachable` (U)	Descartar los paquetes reenviados por esta ruta. Se notifica al originador del paquete por medio de un mensaje `ICMP host unreachable` (tipo 3, código 1)
`prohibit` (P)	Descartar los paquetes reenviados por esta ruta. Se notifica al originador del paquete por medio de un mensaje `ICMP communication administratively prohibited` (tipo 3, código 13)

Figura 26. Etiquetas de rutas más comunes en un RouterOS.

Tomado de (Roosevelt, 2016)

3.4.3. VPN

MikroTik RouterOS soporta varios métodos de conexión mediante VPN, estableciendo conexiones seguras sobre redes abiertas o internet, por ejemplo: VPN MPLS, túneles de punto a punto (Open VPN, PPTP, PPPoE, L2TP), túneles simples (IPIP, EoIP), VLANs, entre otras.

3.4.3.1. VPN basada en MPLS

Los túneles MPLS RSVP TE son una forma de establecer rutas de cambio de etiquetas unidireccionales. En general, RSVP TE tiene un propósito similar al de la distribución de etiquetas mediante el protocolo LDP en equipos cisco. Establece una ruta de conmutación de etiquetas que garantiza la entrega de paquetes.

MPLS RSVP TE está basado en el protocolo RSVP con extensiones introducidas por RFC 3209 que agrega soporte para el intercambio explícito de rutas y etiquetas. (Mikrotik, wiki.mikrotik, 2013)

3.4.4. WIFI

La red inalámbrica es una de las grandes características que tiene el MikroTik RouterOS ya que con esta característica toma ventaja sobre otros fabricantes como Cisco, Huawei, Juniper entre otro.

A continuación, se enlista algunas tecnologías Wifi que soporta este dispositivo:

- Protocolo IEEE802.11a/b/g/n.
- Protocolos propietarios Nstreme y Nstreme2.
- Monitoreo de usuarios.
- Sistema de distribución inalámbrica.
- Encriptación WEP, WPA, WPA2.
- Lista de acceso a la red WIFI.
- Protocolo de ruteo inalámbrico MME.
- AP Virtual.

El protocolo Nstreme es propietario de MikroTik y permite extender el alcance y la velocidad en una conexión WIFi. Adicionalmente posee una variante de dicha tecnología conocida como Nstreme dual, que permite utilizar 2 antenas en cada extremo, la primera para recibir señal y la otra para enviar. (Roosevelt, 2016)

3.4.5. The Dude

The Dude es una aplicación gratuita de MikroTik, que puede mejorar la forma de administración de la red. Este aplicativo explora automáticamente todos los dispositivos dentro de las subredes especificadas, dibuja y diseña un mapa de sus redes, monitorea los servicios de los dispositivos y ejecuta acciones basadas en los cambios de estado del dispositivo. (Roosevelt, 2016)

Una de las características principales de este aplicativo es que se puede actualizar de forma masiva los dispositivos RouterOS en la red.

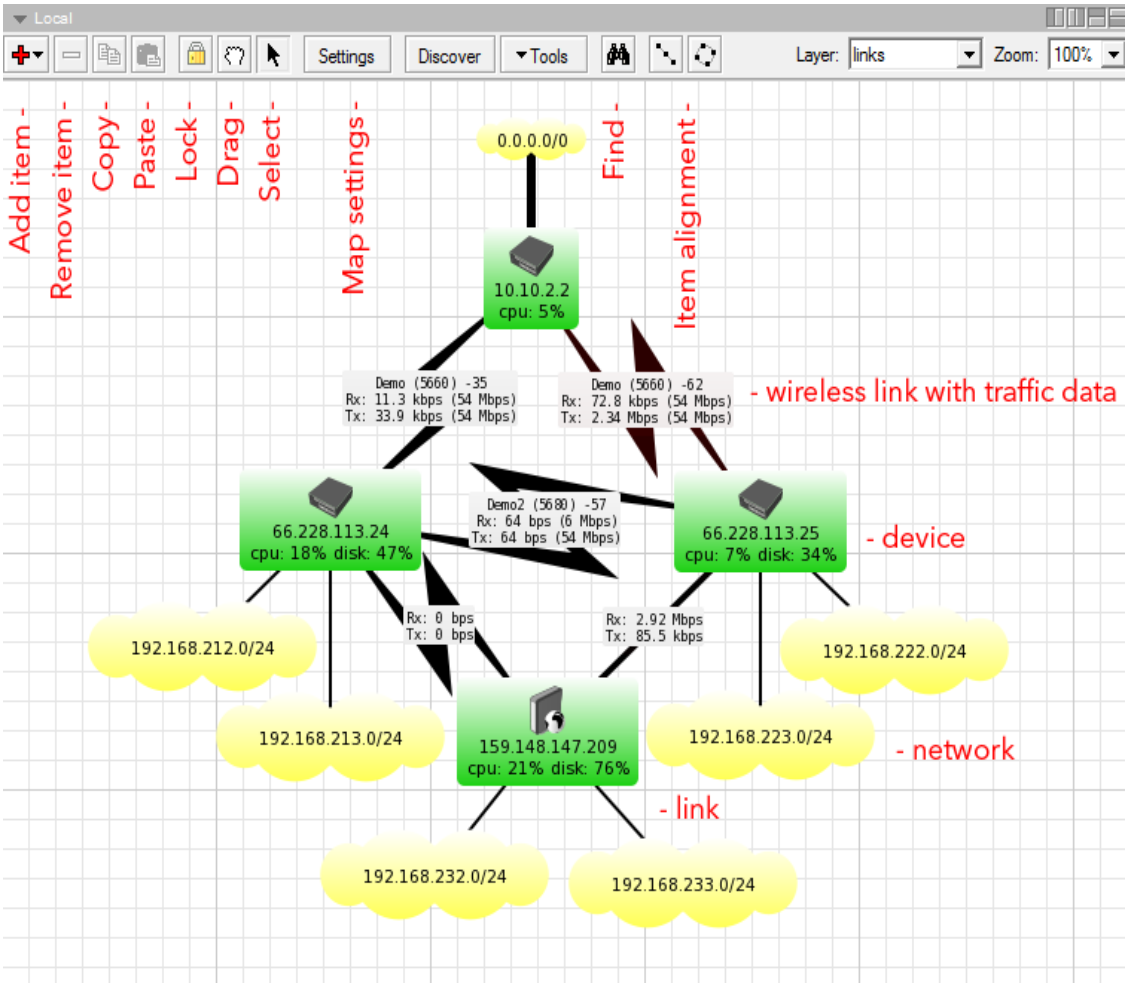


Figura 27. Ambiente de monitoreo equipos MikroTik “The Dude”

Tomado de (Mikrotik, wiki.mikrotik, 2013)

4. CAPÍTULO IV. DISEÑO DE LA RED.

En el presente proyecto de titulación se va a realizar el diseño de una red MPLS basada en equipos MikroTik para comunicar dos sucursales con matriz de la empresa virtual que llamaremos AUTOPARTES. Dicha empresa requiere contratar los servicios de Internet, Telefonía IP y un enlace de Datos en sus tres puntos. En este caso la sede o matriz se encuentra en Quito, la primera sucursal se encuentra en Guayaquil y la segunda sucursal está ubicada en la ciudad de Ambato. La contratación de los tres servicios la realiza a través del proveedor de internet FAST INTERNET que tiene cobertura en todo el Ecuador. El diseño de la red se la realizará mediante los CPEs del cliente, los mismos que se encuentran en cada sucursal, y los equipos PEs del proveedor ubicados en las localidades mencionadas anteriormente. Adicionalmente, el proveedor cuenta con 2 Routes P, el primero se encuentra en Quito (P_UIO) y el segundo en Guayaquil (P_GYE).

4.1. Análisis de la red LAN del cliente

Como primer paso se realizará un dimensionamiento de usuarios y servicios disponibles que se encuentran actualmente en cada sucursal para luego realizar una proyección de crecimiento. Con estos datos se analizará el ancho de banda que se debe asignar a cada sucursal.

- ✓ Análisis de la red Autopartes Matriz.

Para el enlace de datos en la matriz de autopartes (Quito) no se requiere cálculo para el dimensionamiento de usuarios debido a que al tratarse de una matriz no tiene restricción el ancho de banda para la conexión con las sucursales.

- ✓ Análisis de la red Autopartes Guayaquil

Como se puede observar en la tabla 2 se requiere un Ancho de Banda aproximado de 5 Megas. El dimensionamiento se realizó de acurdo a los usuarios que laboran en dicha sucursal.

Tabla 2.

Análisis Autopartes Guayaquil

Servicios	Usuarios	Ancho de banda	Sub. Total
Internet	8	512 kbps c/u	4096 Kbps
Telefonía IP	3	G.711 64 kbps	192 Kbps
Sistema de Facturación	4	128 kbps c/u	512 Kbps
		TOTAL ANCHO DE BANDA	4800 Kbps

- ✓ Análisis de la red Autopartes Guayaquil

A continuación, en la tabla 3 se puede observar se requiere un Ancho de banda aproximado de 4 Megas.

Tabla 3.

Análisis Autopartes Ambato.

Servicios	Usuarios	Ancho de banda	Sub. Total
Internet	6	512 kbps c/u	3072 Kbps
Telefonía IP	2	G.711 64 kbps	192 Kbps
Sistema de Facturación	2	128 kbps c/u	256 Kbps
		TOTAL ANCHO DE BANDA	34520 Kbps

4.2. Arquitectura de la Red

En la parte de arquitectura de red se mostrará la forma de comunicación entre los equipos que intervienen en la Red MPLS y el cliente. Como primer paso se realizará la conexión de los equipos de core mediante el protocolo de Gateway interior OSPF para luego realizar la configuración del MPLS mediante el

protocolo LDP. En lo que respecta a la comunicación lógica entre equipos PE´s, en este caso el PE_UIO, PE_GYE y PE_AMB se la realizará mediante el protocolo de enrutamiento BGP. Mientras que para conseguir comunicación entre equipos CE´s se realizará la configuración de VPNL3 en los equipos PE's la cual consiste en crear una VRF que tomará el nombre de "vrfdat01" por donde el cliente podrá enviar todo el tráfico de su red que puede res; datos, internet, telefonía, etc. Finalmente, en el equipo CE_UIO se procederá a realizar la configuración de rutas estáticas para lograr comunicarse con los diferentes CE's, mientras que dentro de los equipos CE_GYE y CE_AMB se realizará una configuración de ruta por defecto para tener comunicación hacia matriz (CE_UIO).

En la figura 28 se puede visualizar el diagrama de la red a diseñar y simular en el software GNS3 con lo descrito anteriormente. En la parte superior se visualiza el área de Core y Acceso implementada por el proveedor de servicio FAST INTERNET, mientras que en la parte inferior se puede observar la red del cliente AUTOPARTES y sus diferentes sucursales. Adicionalmente se puede observar la conexión de los equipos mediante los protocolos de enrutamiento.

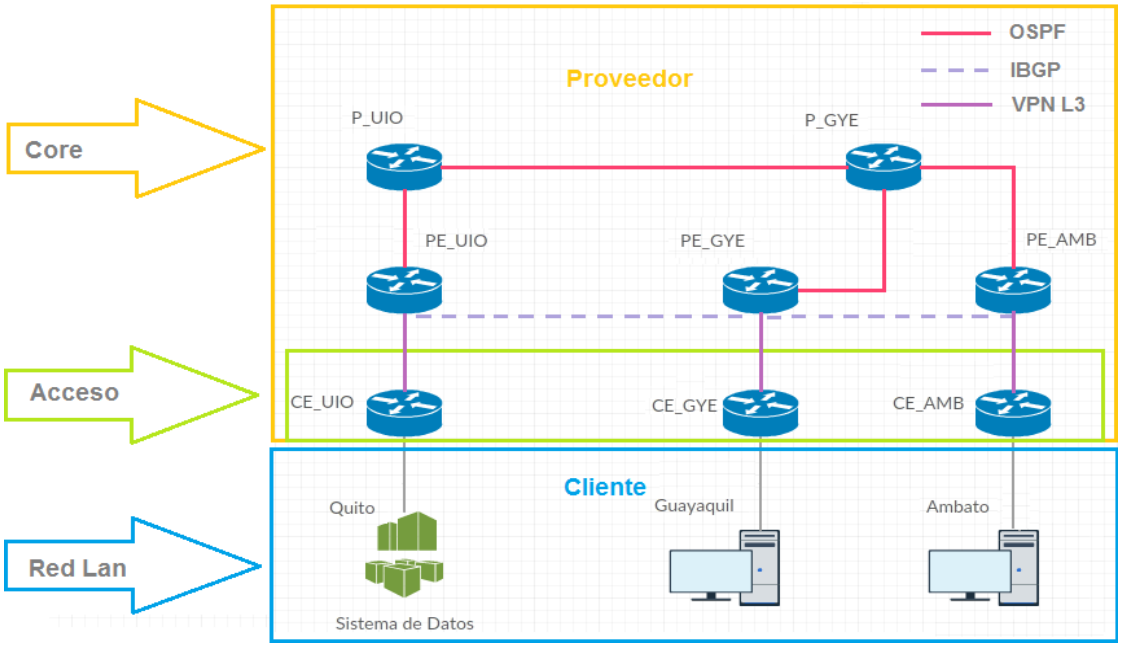


Figura 28. Diagrama de red.

4.3. Topología

La topología de la red es un elemento muy importante al momento de realizar el diseño y simulación de una red. Esto debido a que facilita la configuración de equipos, optimiza el tiempo de ejecución y nos ayuda a entender mejor de qué manera se va a ejecutar nuestro proyecto.

En la figura 29 se visualiza la topología de la red MPLS y su respectivo direccionamiento IP. Adicionalmente se puede observar la conexión de las interfaces ether.

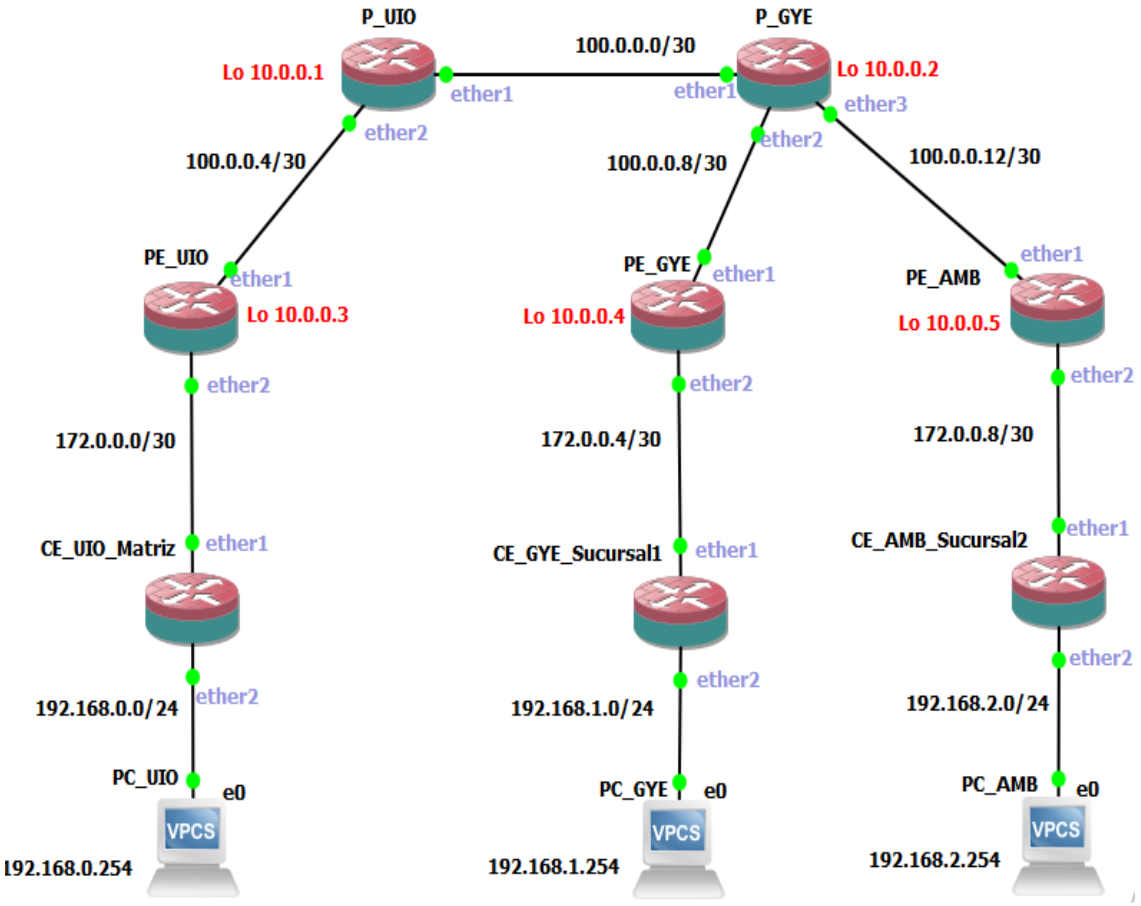


Figura 29. Topología de la red MPLS MikroTik.

A continuación, se muestra la tabla 4 que describe los equipos de backbone, loopbacks asignadas y su funcionalidad dentro del diseño de la red MPLS.

Tabla 4.

Equipos e IP´s loopbacks utilizadas en la red de backbone.

HOST NAME	IP LOOP BACK	FUNCIONALIDAD
P_UIO	10.0.0.1	Router P
P_GYE	10.0.0.2	Router P
PE_UIO	10.0.0.3	Router PE
PE_GYE	10.0.0.4	Router PE
PE_AMB	10.0.0.5	Router PE

En la tabla 5 se encuentra el listado de los equipos que formaran parte de la red a nivel de backbone y a nivel de acceso. Se puede observar la localidad a la que pertenece, el nombre del equipo, sus interfaces, hacia qué equipo se conecta y por último se muestra su direccionamiento IP.

Tabla 5.

Conexión de equipos en el backbone MPLS.

LOCALIDAD	HOSTNAME	INTERFACES	DIRECCIÓN IP
QUITO	P_UIO	Ether1 TO P_GYE	100.0.0.1/30
		Ether2 TO PE_UIO	100.0.0.5/30

	PE_UIO	Ether1 TO P_UIO	100.0.0.6/30
		Ether2 TO CE_UIO	172.0.0.1/30
	CE_UIO	Ether1 TO PE_UIO	172.0.0.2/30
		Ether2 TO RED LAN UIO	192.168.0.0/24
GUAYAQUIL	P_GYE	Ether1 TO P_UIO	100.0.0.2/30
		Ether2 TO PE_GYE	100.0.0.9/30
		Ether3 TO PE_AMB	100.0.0.13/30
	PE_GYE	Ether1 TO P_GYE	100.0.0.10/30
		Ether2 TO CE_GYE	172.0.0.5/30
	CE_GYE	Ether1 TO PE_GYE	172.0.0.6/30
		Ether2 TO RED LAN GYE	192.160.1.0/24
AMBATO	PE_AMB	Ether1 TO P_GYE	100.0.014/30
		Ether2 TO CE_AMB	172.0.0.9/30
	CE_AMB	Ether1 TO PE_AMB	172.0.0.10/30

		Ether2 TO RED LAN AMB	192.168.2.0/24

5. CAPÍTULO V. SIMULACIÓN DE LA RED.

En este capítulo se procederá a ejecutar la simulación del proyecto de titulación, el cual consiste en simular la red MPLS con el objetivo de mostrar sus características y funcionalidades para un entorno PYMES.

La simulación se la realizará con ayuda del software GNS3 (Graphic Network Simulation), el cual permite simular topologías de red avanzadas en un entorno amigable que no requiere de conocimientos avanzados para su instalación, configuración y posterior uso.

GNS3 es un software gráfico basado en Linux que permite la simulación de equipos en diferentes marcas lo que lo diferencia de otros simuladores existentes en el mercado. Entre los equipos más importantes se encuentran los siguientes; CISCO, JUNIPER, MIKROTIK entre otras. Este software es conocido por ayudar a estudiantes y profesionales a simular, implementar, ejecutar laboratorios y solucionar inconvenientes de redes. (Bombal, 2019)

5.1. Instalación del software GNS3 en Windows

Antes de empezar con la instalación se debe tomar en cuenta los requerimientos mínimos que indica el propietario del software para su buen funcionamiento.

- Compatibilidad con Windows
  - ✓ Windows 7 SP1 (64 bit)
  - ✓ Windows 8 (64 bit)
  - ✓ Windows 10 (64 bit)
  - ✓ Windows Server 2012 (64 bit)
  - ✓ Windows Server 2016 (64 bit)
- Procesador de 2 o más núcleos

- 8G de memoria RAM
- 1G disponible para su instalación

A continuación, se detalla el proceso de instalación del Software GNS3 en Windows.

✓ Descarga del Software GNS3.

El primer paso consiste en descargar el software mediante registro de usuario en la página web https://www.gns3.com/

✓ Instalación

El segundo paso consiste en ejecutar el archivo de instalación descargado previamente de la página oficial de GNS3 y continuar con los pasos de instalación propios del software.

En la figura 30 se puede visualizar la instalación completa del software sin cargar los IOS de los routers y sin conexión a la Máquina Virtual.

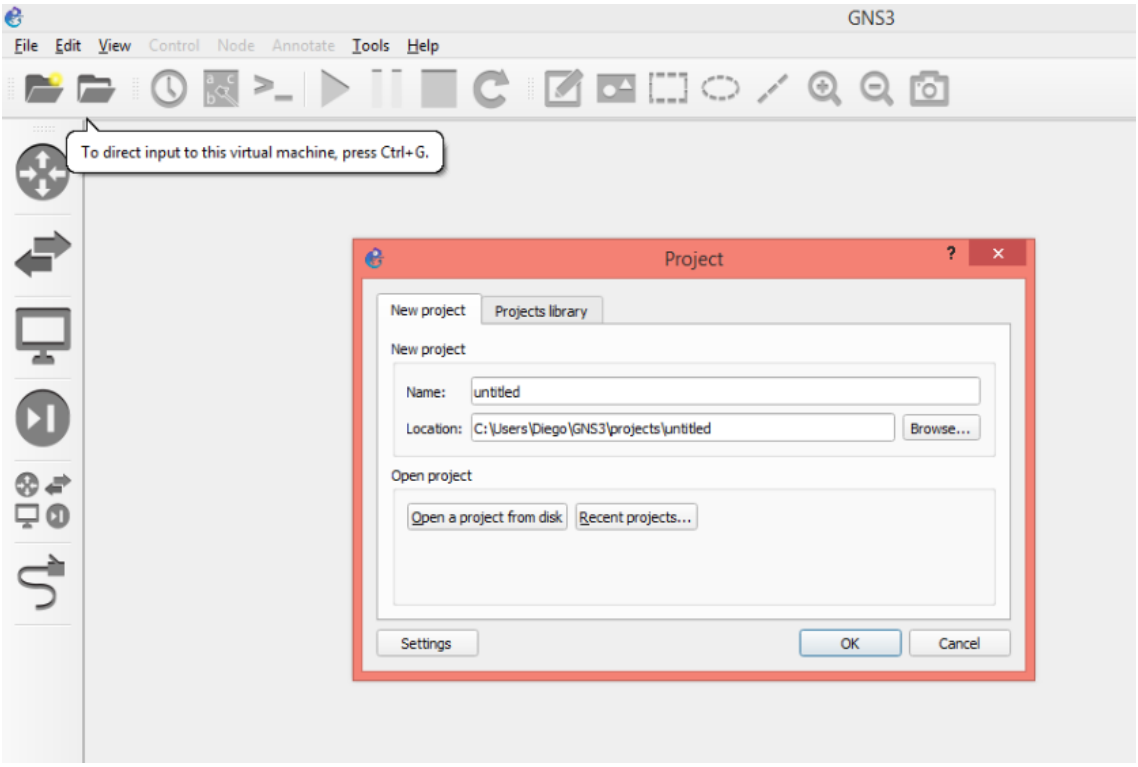


Figura 30. Entorno de software GNS3.

5.1.1. Instalación de Máquina Virtual (MV)

Para poder integrar la máquina virtual de GNS3 se debe ejecutar el Setup Wizard. Para esto se debe dar clic en el menú Help y luego en Setup Wizard como se muestra en la figura 31.

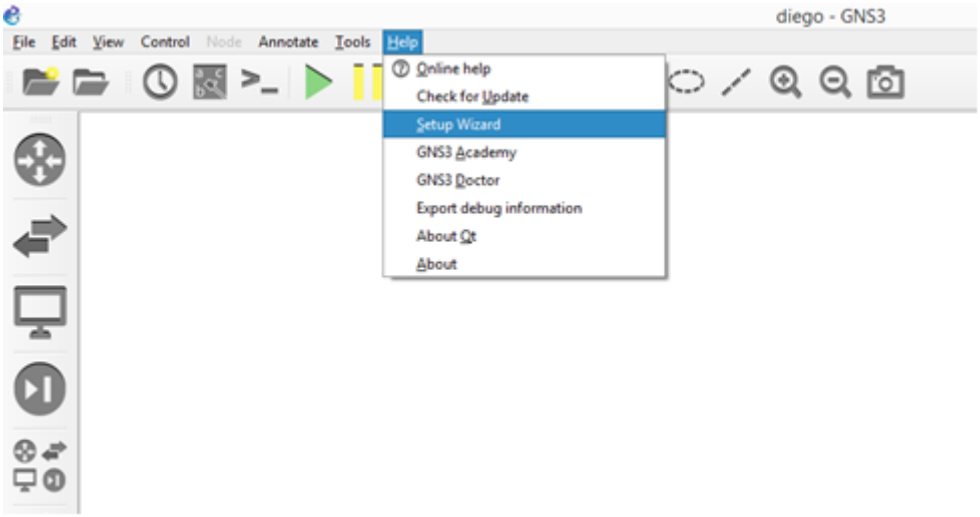


Figura 31. Paso 1 Carga de MV.

Luego se selecciona la opción “Run Modern IOS (IOSv or IOU), ASA and appliances from non Cisco manufacturers” como se muestra en la figura 32.

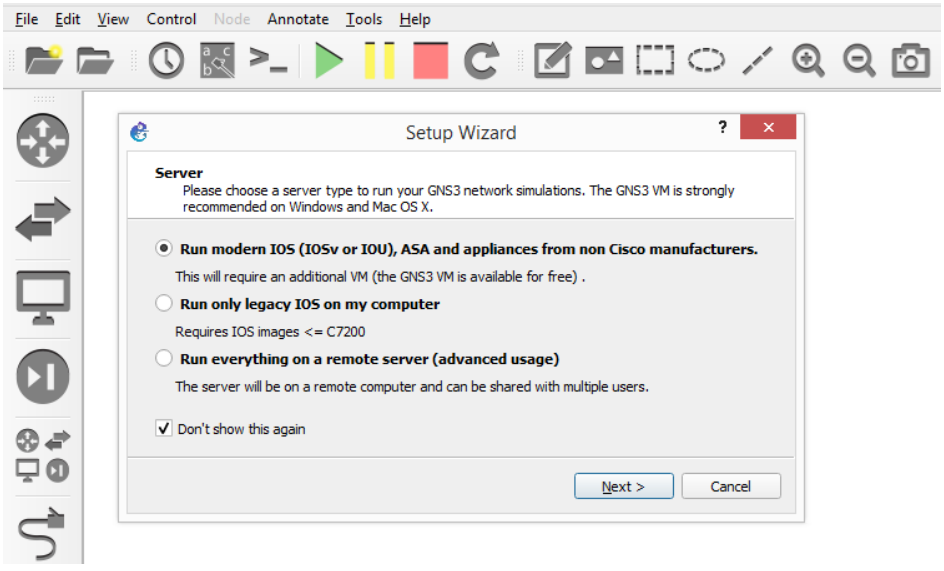


Figura 32. Paso 2 Carga MV.

Posteriormente se elige la ubicación donde se instalará el servidor local GNS3, la IP y el puerto. El fabricante recomienda colocar los siguientes parámetros que vienen por defecto tal como se muestra en la figura 33.

- Server path: Ubicación por defecto del servidor gns3server.EXE.
- Host Binding: IP 127.0.0.1 es la dirección IP de loopback configurada por defecto.
- Port: 3080 TCP

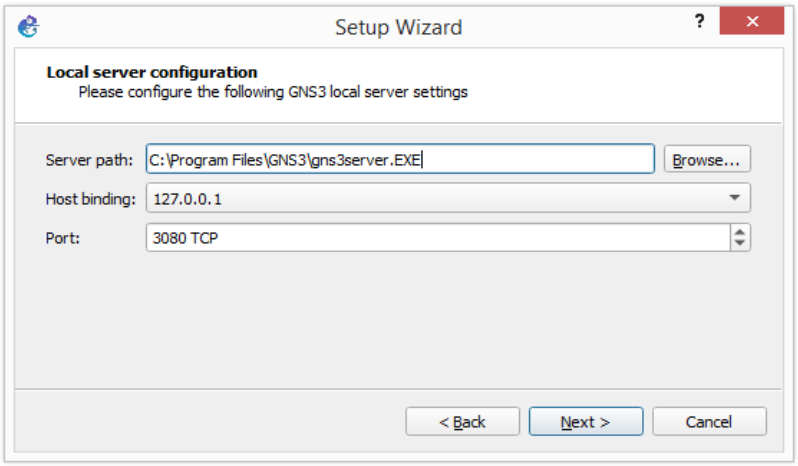


Figura 33. Paso 3 Carga MV paso.

Luego de dar en siguiente se tiene la validación del GNS3 para poder cargar la MV como se muestra en la figura 34.

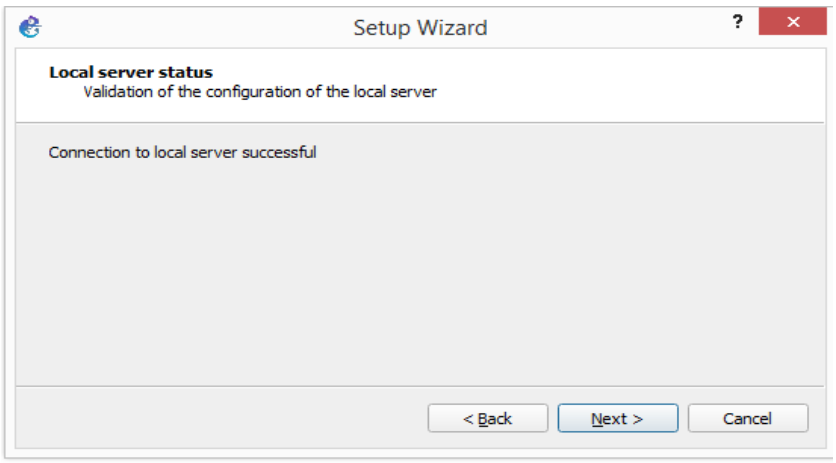


Figura 34. Paso 4 Carga MV.

En la figura 35 se visualiza las opciones de MV que soporta GNS3 que son VirtualBox y VMware, se elige la recomendada por defecto y se da clic en siguiente.

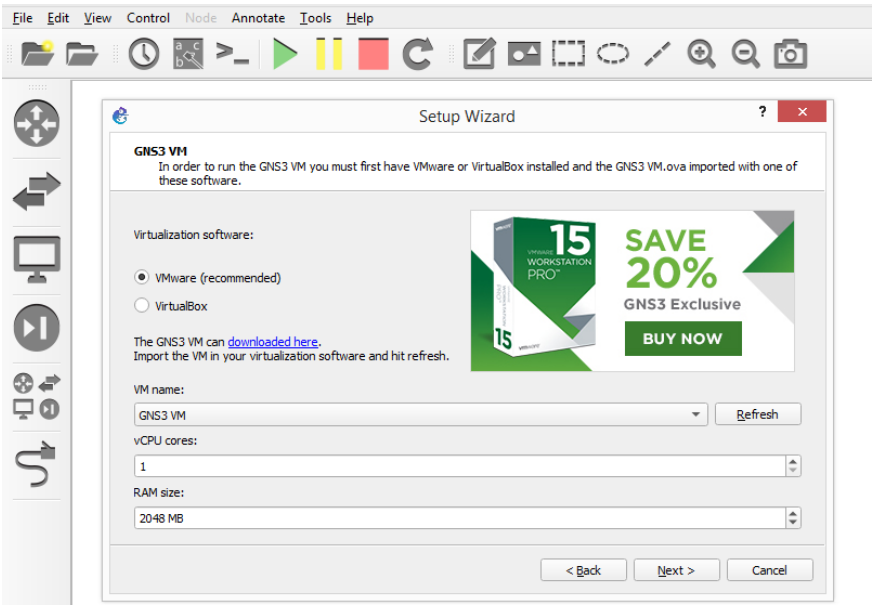


Figura 35. Paso 5 Carga MV.

Una vez cargada la MV tendremos la pantalla en Linux, donde se indica la conexión correcta de la MV con el GNS3 como se muestra en la figura 36.

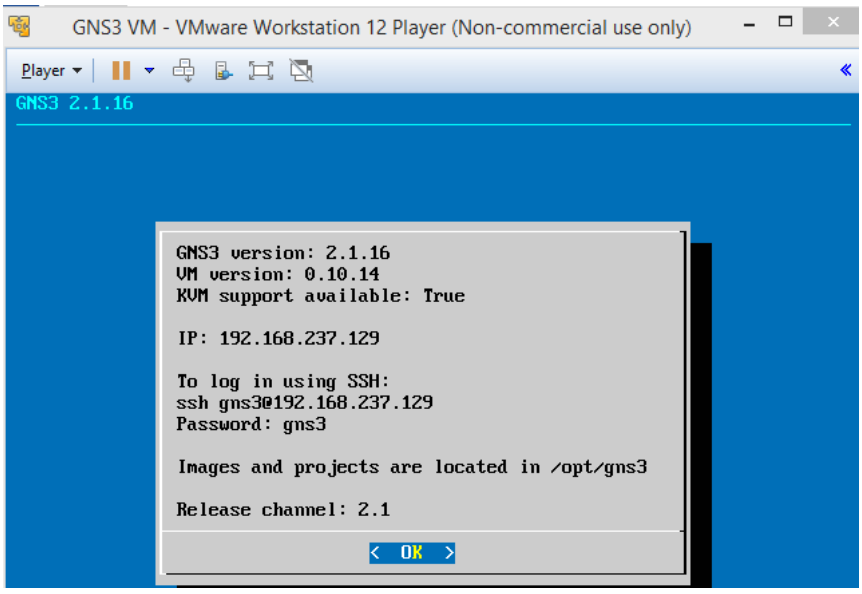


Figura 36. Conexión de MV con GNS3.

5.1.2. Carga de IOS RouterOS sobre GNS3

Como último paso para realizar las configuraciones sobre el GNS3, se requiere cargar las imágenes de los equipos. En este punto se indicará el proceso para la carga de un equipo MikroTik RouterOS. Cabe indicar que previamente ya se tiene cargado por defecto el icono del equipo router en el GNS3, lo que se va a realizar es la carga del sistema operativo. Por lo tanto como primer paso se debe descargar la imagen del equipo de la página oficial de MikroTik https://mikrotik.com/download como se muestra en la figura 37.

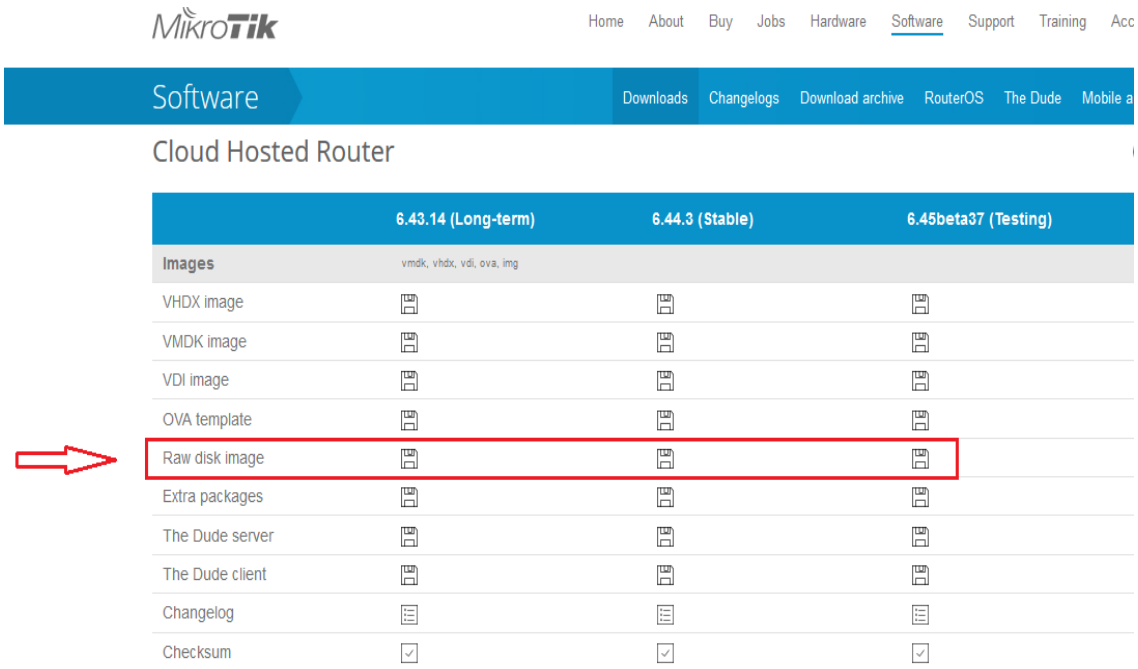


Figura 37. Descarga de IOS RouterOS.

Tomado de (Mikrotik, wiki.mikrotik, 2013)

Una vez realizada la descarga del IOS, se abre el software GNS3, se ubica en el icono del router MikroTik CHR, se da doble clic en el icono y siguiente para continuar con la instalación como se muestra en la figura 37.

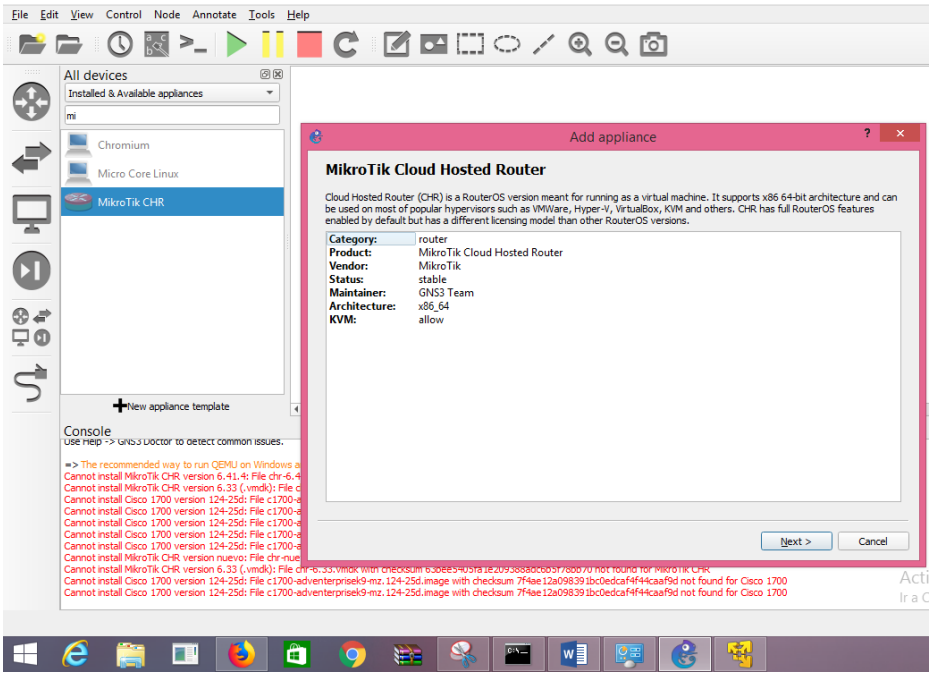


Figura 38. Paso 1 Carga de IOS RouterOS.

En el siguiente paso se elige la opción “Run the appliance on the GNS3 VM” que viene marcada por defecto, donde se realizará la cargar del IOS como se observa en la figura 39.

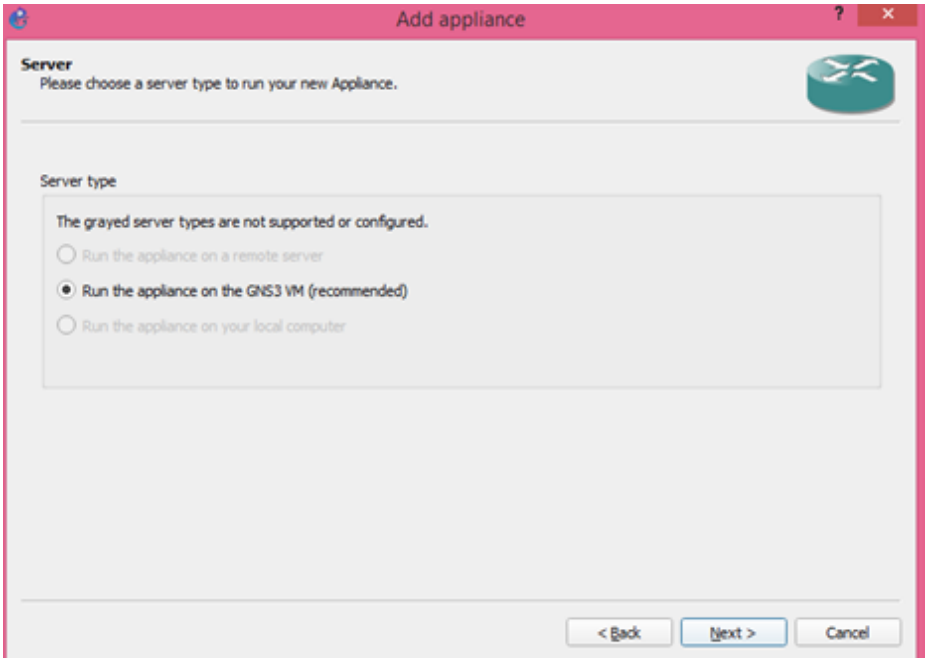


Figura 39. Paso 2 Carga de IOS RouterOS.

Luego de dar siguiente se visualiza la imagen de la figura 40, donde se debe importar la imagen IOS, esto quiere decir que debemos cargar la imagen IOS RouterOS descargada anteriormente.

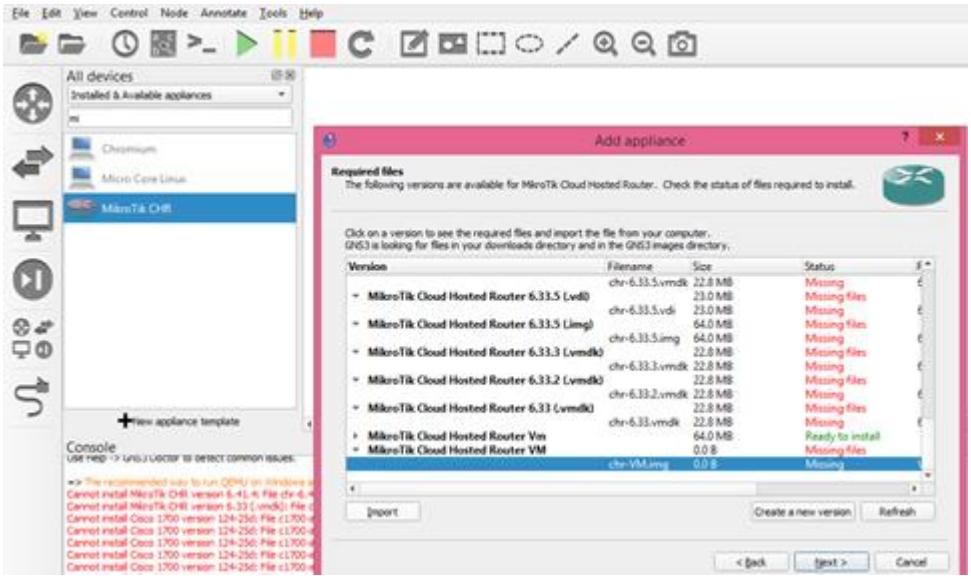


Figura 40. Paso 3 Carga de IOS RouterOS paso 3.

Para finalizar la instalación se carga el IOS en GNS3 tal como se muestra en la figura 41.

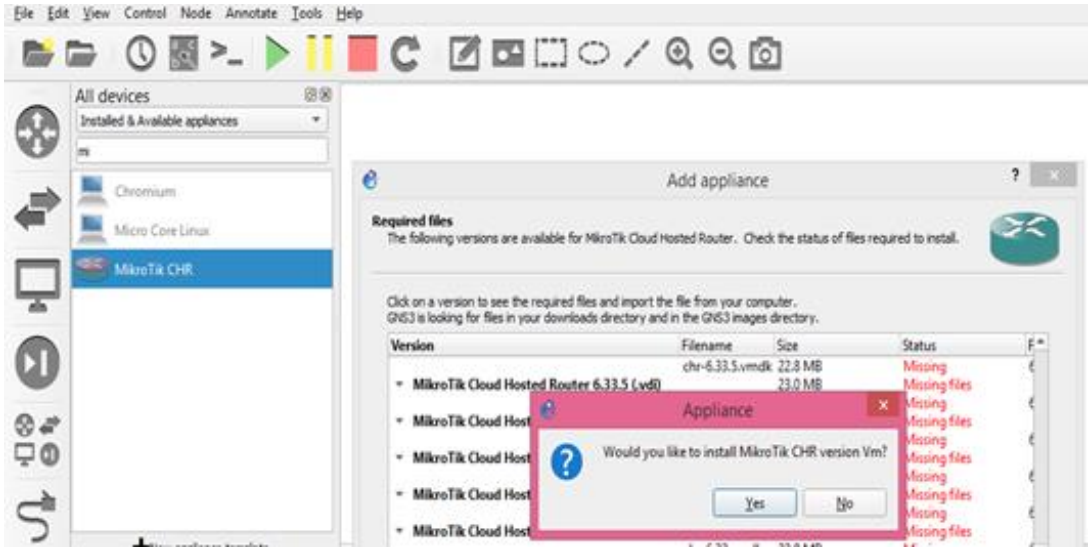


Figura 41. Paso 4 Carga de IOS RouterOS en GNS3.

5.2. Configuración de equipos RouterOS

5.2.1. Configuración básica inicial

A continuación, como primer paso se va a realizar la configuración de los siguientes parámetros en cada uno de los routers:

- ✓ Configuración de host name.
- ✓ Creación de bridge e interfaz loopback en los equipos de core (P_UIO, P_GYE, PE_UIO, PE_GYE y PE_AMB)
- ✓ Configuración de interfaces WAN.

P_UIO

```
/system identity set name=P_UIO
/interface bridge add name=loopback
/ip address add address=10.0.0.1/32 interface=loopback
/ip address add address=100.0.0.1/30 interface=ether1
/ip address add address=100.0.0.5/30 interface=ether2
```

P_GYE

```
/system identity set name=P_GYE
/interface bridge add name=loopback
/ip address add address=10.0.0.2/32 interface=loopback
/ip address add address=100.0.0.2/30 interface=ether1
/ip address add address=100.0.0.9/30 interface=ether2
/ip address add address=100.0.0.13/30 interface=ether3
```

PE_UIO

```
/system identity set name=PE_UIO
/interface bridge add name=loopback
/ip address add address=10.0.0.3/32 interface=loopback
/ip address add address=100.0.0.6/30 interface=ether1
/ip address add address=172.0.0.1/30 interface=ether2
```

PE_GYE

/system identity set name=PE_GYE
/interface bridge add name=loopback
/ip addressadd add address=10.0.0.4/32 interface=loopback
/ip addressadd address=100.0.0.10/30 interface=ether1
/ip addressadd add address=172.0.0.5/30 interface=ether2

PE_AMB

/system identity set name=PE_AMB
/interface bridge add name=loopback
/ip address add address=10.0.0.5/32 interface=loopback
/ip address add address=100.0.0.14/30 interface=ether1
/ip address add address=172.0.0.9/30 interface=ether2

CE_UIO

/system identity set name=CE_UIO_Matriz
/ip address add address=172.0.0.2/30 interface=ether1
/ip address add address=192.168.0.1/24 interface=ether2

CE_GYE

/system identity set name=CE_GYE_Sucursal1
/ip address add address=172.0.0.6/30 interface=ether1
/ip address add address=192.168.1.1/24 interface=ether2

CE_AMB

/system identity set name=CE_ABM_Sucursal2
/ip address add address=172.0.0.10/30 interface=ether1
/ip address add address= 192.168.2.1/24 interface=ether2
/quit

En este punto es muy importante verificar tramo a tramo la conectividad de los equipos a nivel WAN para posteriormente no tener problemas al momento de configurar los protocolos de enrutamiento.

Prueba de conectividad desde P_UIO hacia P_GYE

```
[MPLS@P_UIO] > ping 100.0.0.2
  SEQ HOST                          SIZE TTL TIME  STATUS
    0 100.0.0.2                     56  64 4ms
    1 100.0.0.2                     56  64 3ms
    sent=2 received=2 packet-loss=0% min-rtt=3ms avg-rtt=3ms max-
rtt=4ms
```

Prueba de conectividad desde P_UIO hacia PE_UIO

```
[MPLS@P_UIO] > ping 100.0.0.6
  SEQ HOST                          SIZE TTL TIME  STATUS
    0 100.0.0.6                     56  64 1ms
    1 100.0.0.6                     56  64 1ms

    sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-
rtt=1ms.
```

Prueba de conectividad desde P_GYE hacia PE_GYE

```
[MPLS@P_GYE] > ping 100.0.0.10
  SEQ HOST                          SIZE TTL TIME  STATUS
    0 100.0.0.10                    56  64 1ms
    1 100.0.0.10                    56  64 1ms
    sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-
rtt=1ms
```

Prueba de conectividad desde P_GYE hacia PE_AMB

```
[MPLS@P_GYE] > ping 100.0.0.14
  SEQ HOST                          SIZE TTL TIME  STATUS
    0 100.0.0.14                    56  64 1ms
```

1 100.0.0.14 56 64 1ms

2 100.0.0.14 56 64 1ms

sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-rtt=3ms

Prueba de conectividad desde PE_UIO hacia CE_UIO

[MPLS@PE_UIO] > ping 172.0.0.2

SEQ HOST SIZE TTL TIME STATUS

0 172.0.0.2 56 64 3ms

1 172.0.0.2 56 64 0ms

2 172.0.0.2 56 64 0ms

sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=2ms max-rtt=3ms

Prueba de conectividad desde PE_GYE hacia CE_GYE

[MPLS@PE_GYE] > ping 172.0.0.6

SEQ HOST SIZE TTL TIME STATUS

0 172.0.0.6 56 64 3ms

1 172.0.0.6 56 64 0ms

2 172.0.0.6 56 64 0ms

sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=2ms max-rtt=4ms

Prueba de conectividad desde PE_AMB hacia CE_AMB

[MPLS@PE_AMB] > ping 172.0.0.10

SEQ HOST SIZE TTL TIME STATUS

0 172.0.0.10 56 64 4ms

1 172.0.0.10 56 64 1ms

2 172.0.0.10 56 64 1ms

sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=3ms max-rtt=4ms

5.2.2. Configuración de OSPF

El protocolo OSPF se utiliza para formar vecindades entre los equipos P, PE's mediante loopbacks y las redes conectadas directamente como se muestra en la figura 42.

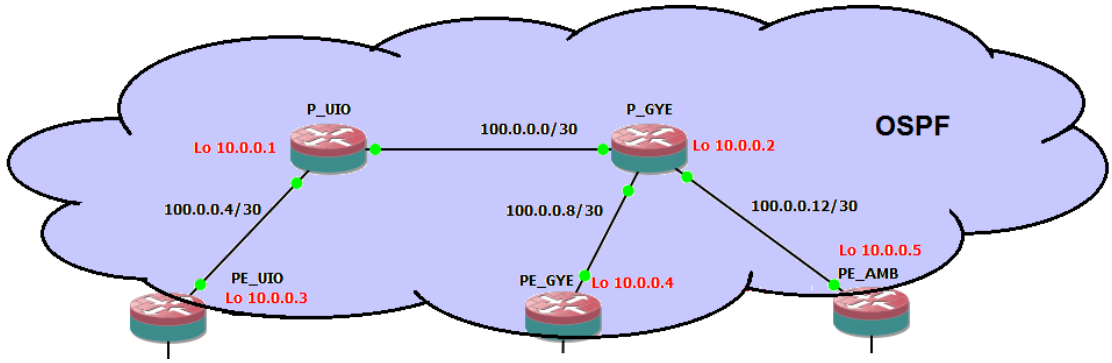


Figura 42. Nube OSPF.

A continuación, se detalla la configuración del protocolo OSPF en los equipos MikroTik: P_UIO, P_GYE, PE_UIO, PE_GYE, PE_AMB:

P_UIO

/routing ospf instance set [find default=yes] redistribute-connected=as-type-1 router-id=10.0.0.1
/routing ospf network add area=backbone network=100.0.0.4/30
/routing ospf network add area=backbone network=100.0.0.0/30
/routing ospf network add area=backbone network=10.0.0.1/32

P_GYE

/routing ospf instance set [find default=yes] redistribute-connected=as-type-1 router-id=10.0.0.2
/routing ospf network add area=backbone network=100.0.0.0/30
/routing ospf network add area=backbone network=100.0.0.8/30
/routing ospf network add area=backbone network=100.0.0.12/30
/routing ospf network add area=backbone network=10.0.0.2/32

PE_UIO

/routing ospf instance set [find default=yes] redistribute-connected=as-type-1 router-id=10.0.0.3
/routing ospf network add area=backbone network=100.0.0.4/30
/routing ospf network add area=backbone network=10.0.0.3/32

PE_GYE

/routing ospf instance set [find default=yes] redistribute-connected=as-type-1 router-id=10.0.0.4
/routing ospf network add area=backbone network=100.0.0.8/30
/routing ospf network add area=backbone network=10.0.0.4/32

PE_AMB

/routing ospf instance set [find default=yes] redistribute-connected=as-type-1 router-id=10.0.0.5
/routing ospf network add area=backbone network=100.0.0.12/30

Luego de terminar la configuración del protocolo IGP OSPF, se verifica con el comando “ip route print” las rutas aprendidas.

En la figura 43 se puede visualizar las rutas aprendidas en el equipo P_UIO mediante el protocolo OSPF con una distancia administrativa de 110 y adicionalmente las rutas conectadas directamente con una distancia administrativa de 0.

```
[MPLS@P_UIO] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.0.0.1/32        10.0.0.1        loopback                  0
 1 ADo  10.0.0.2/32                        100.0.0.2               110
 2 ADo  10.0.0.3/32                        100.0.0.6               110
 3 ADo  10.0.0.4/32                        100.0.0.2               110
 4 ADo  10.0.0.5/32                        100.0.0.2               110
 5 ADC  100.0.0.0/30       100.0.0.1       ether1                    0
 6 ADC  100.0.0.4/30       100.0.0.5       ether2                    0
 7 ADo  100.0.0.8/30                       100.0.0.2               110
 8 ADo  100.0.0.12/30                      100.0.0.2               110
 9 ADo  172.0.0.8/30                       100.0.0.2               110
```

Figura 43. Tabla de enrutamiento equipo P_UIO.

Para verificar conectividad se realiza una prueba de ping desde P_UIO hacia las loopback's y las IP WAN de los routes que no se encuentran directamente conectados.

Prueba de conectividad desde P_UIO hacia la IP WAN del equipo PE_GYE

```
[MPLS@P_UIO] > ping 100.0.0.10
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 100.0.0.10                               56  63 4ms
    1 100.0.0.10                               56  63 1ms
    2 100.0.0.10                               56  63 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-
rtt=4ms
```

Prueba de conectividad desde P_UIO hacia la loopback del equipo PE_AMB

```
 [MPLS@P_UIO] > ping 10.0.0.5
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.0.5                                 56  63 1ms
    1 10.0.0.5                                 56  63 1ms
    2 10.0.0.5                                 56  63 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-
rtt=1ms
```

5.2.3. Configuración de MPLS mediante LDP

Luego de haber realizado las validaciones de conexión en toda la red, mediante el protocolo OSPF, se configura el protocolo MPLS. Esto consiste en cambiar la dirección IP de transporte en cada router, utilizando la dirección de looback y especificando las interfaces que se encuentran conectadas al core de la red.

A continuación, se realiza la configuración de MPLS mediante el protocolo LDP.

P_UIO

```
/mpls ldp set enabled=yes lsr-id=10.0.0.1 transport-address=10.0.0.1
```

/mpls ldp interface add interface=ether1

/mpls ldp add interface=ether2

P_GYE

/mpls ldp set enabled=yes lsr-id=10.0.0.2 transport-address=10.0.0.2

/mpls ldp interface add interface=ether1

/mpls ldp interface add interface=ether2

/mpls ldp interface add interface=ether3

PE_UIO

/mpls ldp set enabled=yes lsr-id=10.0.0.3 transport-address=10.0.0.3

/mpls ldp interface add interface=ether1

PE_GYE

/mpls ldp set enabled=yes lsr-id=10.0.0.4 transport-address=10.0.0.4

/mpls ldp interface add interface=ether1

PE_AMB

/mpls ldp set enabled=yes lsr-id=10.0.0.5 transport-address=10.0.0.5

/mpls ldp interface add interface=ether1

En la figura 44 se puede observar la asignación de etiquetas para los routers de core. Se puede visualizar mediante el comando “mpls forwarding-table print” en el equipo P_UIO.

```
[MPLS@P_UIO] /mpls forwarding-table> print
Flags: H - hw-offload, L - ldp, V - vpls, T - traffic-eng
 #    IN-LABEL                    OUT-LABELS                  DESTINATION                 INTERFACE                   NEXTHOP
 0    expl-null
 1  L 16                                                      10.0.0.3/32                 ether2                      100.0.0.6
 2  L 17                                                      10.0.0.2/32                 ether1                      100.0.0.2
 3  L 19                                                      100.0.0.8/30                ether1                      100.0.0.2
 4  L 20                                                      100.0.0.12/30               ether1                      100.0.0.2
 5  L 23                        22                            172.0.0.8/30                ether1                      100.0.0.2
 6  L 24                        23                            10.0.0.5/32                 ether1                      100.0.0.2
 7  L 26                        25                            10.0.0.4/32                 ether1                      100.0.0.2
[MPLS@P_UIO] /mpls forwarding-table>
```

Figura 44. Tabla de reenvío de etiquetas MPLS.

5.2.4. Configuración BGP

A continuación, se detallan los pasos para la configuración del protocolo BGP.

- ✓ Creación de VRF.
- ✓ Configuración BGP y VPNL3

5.2.4.1. Creación de VRF

Para la conexión entre equipos PE´s y CE´s (Última Milla) se realizará la configuración de la “vrfdat01” asociando las IP´s WAN de cada router CE con el objetivo de poder discriminar el tráfico entre clientes.

A continuación, se realiza la configuración de las VRF’s en cada PE.

PE_UIO

/ip route vrf add export-route-targets=65530:1 import-route-targets=65530:1 interfaces=ether2 route-distinguisher=65530:1 routing-mark=vrfdat01

PE_GYE

/ip route vrf add export-route-targets=65530:1 import-route-targets=65530:1 interfaces=ether2 route-distinguisher=65530:1 routing-mark=vrfdat01

PE_AMB

/ip route vrf add export-route-targets=65530:1 import-route-targets=65530:1 interfaces=ether2 route-distinguisher=65530:1 routing-mark=vrfdat01

Prueba de conectividad desde PE_UIO hacia CE_UIO

```
[MPLS@PE_UIO] > ping routing-table=vrfdat01 172.0.0.2
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.0.0.2                                56  64 2ms
    1 172.0.0.2                                56  64 2ms
    sent=2 received=2 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=2ms
```

5.2.4.2. Configuración del protocolo BGP y VPNL3

Para la comunicación entre equipos PE´s se utiliza el protocolo BGP que permite la conexión VPNL3 entre sucursales asociado la vrfdat01.

A continuación, se detalla la configuración del protocolo BGP en los equipos PE´s:

PE_UIO

/routing bgp instance set default router-id=10.0.0.3

/routing bgp instance vrf add redistribute-connected=yes redistribute-static=yes routing-mark=vrfdat01

/routing bgp peer add address-families=ip,vpnv4 multihop=yes name=PE_UIO>PE_GYE nexthop-choice=force-self remote-address=10.0.0.4 remote-as=65530 ttl=default update-source=loopback

/routing bgp peer add address-families=ip,vpnv4 multihop=yes name=PE_UIO>PE_AMB nexthop-choice=force-self remote-address=10.0.0.5 remote-as=65530 ttl=default update-source=loopback

PE_GYE

/routing bgp instance set default router-id=10.0.0.4

/routing bgp instance vrf add redistribute-connected=yes redistribute-static=yes routing-mark=vrfdat01

/routing bgp peer add address-families=ip,vpnv4 multihop=yes name=PE_GYE>PE_UIO nexthop-choice=force-self remote-address=10.0.0.3 remote-as=65530 ttl=default update-source=loopback

PE_AMB

/routing bgp instance set default router-id=10.0.0.5

/routing bgp instance vrf add redistribute-connected=yes redistribute-static=yes routing-mark=vrfdat01

/routing bgp peer add address-families=ip,vpnv4 multihop=yes name=PE_AMB>PE_UIO nexthop-choice=force-self remote-address=10.0.0.3 remote-as=65530 ttl=default update-source=loopback

A continuación, se valida la conexión a nivel WAN hacia los equipos CE_GYE y CE_AMB desde en router PE_UIO.

Prueba de conectividad entre PE_UIO y CE_GYE mediante VRF

```
[MPLS@PE_UIO] > ping routing-table=vrfdat01 172.0.0.6
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.0.0.6                                56  61 4ms
    1 172.0.0.6                                56  61 2ms
    sent=2 received=2 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=4ms
```

Prueba de conectividad entre PE_UIO y CE_AMB mediante VRF

```
[MPLS@PE_UIO] > ping routing-table=vrfdat01 172.0.0.10
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.0.0.10                               56  61 3ms
    1 172.0.0.10                               56  61 2ms
    sent=2 received=2 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=3ms
```

En la figura 45 se puede observar con el comando “ip route print” las rutas aprendidas en el equipo PE_UIO mediante BGP.

```
[MPLS@PE_UIO] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf,
prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  172.0.0.0/30       172.0.0.1       ether2                    0
 1 ADb  172.0.0.4/30                       10.0.0.4                200
 2 ADb  172.0.0.8/30                       10.0.0.5                200
```

Figura 45. Rutas BGP en el router PE_UIO.

5.2.5. Configuración de rutas para conexión entre Matriz y Sucursales.

Como primer paso para la conexión de las redes LAN de la empresa Autopartes se configura rutas por defecto en todas las agencias incluyendo matriz y adicionalmente se configura rutas estáticas en el equipo CE_UIO_Matriz para alcanzar las sucursales.

A continuación, se realiza la configuración de los 3 routers CE's:

CE_UIO_Matriz

/ip route add distance=1 gateway=172.0.0.1
/ip route add distance=1 dst-address=192.168.1.0/24 gateway=172.0.0.1
/ip route add distance=1 dst-address=192.168.2.0/24 gateway=172.0.0.1

CE_GYE

/ip route add distance=1 gateway=172.0.0.5

CE_AMB

/ip route add distance=1 gateway=172.0.0.9

/quit

Luego de la configuración en los CE´s se configura una ruta por defecto en el equipo PE_UIO, para que todo el tráfico que proviene de las sucursales se direccione al equipo CE_UIO_Matriz.

/ip route add distance=1 gateway=172.0.0.2 routing-mark=vrfdat01

Finalmente, se configura rutas estáticas publicando las redes LAN de los CE's en los PE´s conectados directamente hacia las sucursales.

PE_GYE

/ip route add distance=1 dst-address=192.168.1.0/24 gateway=172.0.0.6 routing-mark=vrfdat01

PE_AMB

/ip route add add distance=1 dst-address=192.168.2.0/24 gateway=172.0.0.10 routing-mark=vrfdat01

Luego de haber realizado las configuraciones se valida conectividad entre CE_UIO_Matriz y sucursales.

Conectividad desde CE_UIO_Matriz hacia CE_GYE_Sucursal1

```
[admin@CE_UIO_Matriz] > ping 192.168.1.1 src-address=192.168.0.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.1                              56  60 8ms
    1 192.168.1.1                              56  60 4ms
    2 192.168.1.1                              56  60 5ms
    sent=3 received=3 packet-loss=0% min-rtt=4ms avg-rtt=5ms max-rtt=8ms
```

Conectividad desde CE_UIO_Matriz hacia CE_AMB_Sucursal2

```
[admin@CE_UIO_Matriz] > ping 192.168.2.1 src-address=192.168.0.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.2.1                              56  60 7ms
    1 192.168.2.1                              56  60 6ms
    sent=2 received=2 packet-loss=0% min-rtt=4ms avg-rtt=5ms max-rtt=7ms.
```

5.2.5.1. Conectividad entre sucursales

Para realizar la simulación se instaló una PC en cada sucursal para validar conectividad de la red LAN del cliente Autopartes.

A continuación, se realiza pruebas de conectividad entre sucursales:

En la figura 46 se puede observar conectividad desde Quito (Matriz) hacia las sucursales de Guayaquil con IP 192.168.1.254 y Ambato con IP 192.168.2.254.

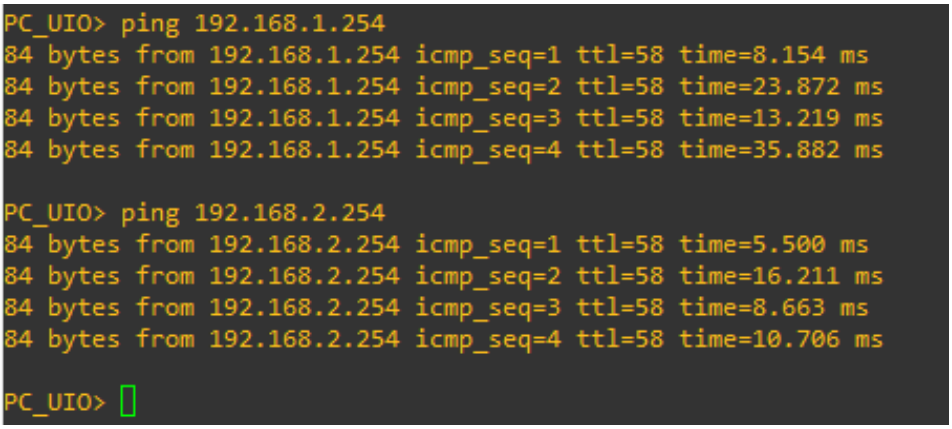


Figura 46. Prueba de conectividad desde Matriz hacia sucursales.

En la figura 47 se visualiza la prueba de conectividad desde la Sucursal de Guayaquil hacia Quito (Matriz) que tiene configurada la IP 192.168.0.254.

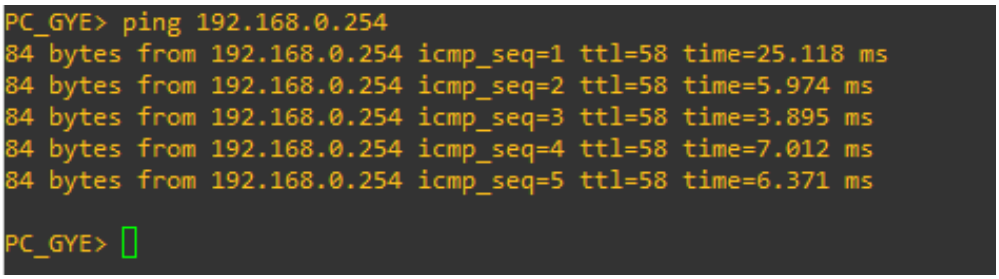


Figura 47. Prueba de conectividad desde PC_GYE hacia Matriz.

En la figura 48 se visualiza la prueba de conectividad desde la sucursal de Ambato hacia Quito (Matriz) que tiene configurada la ip 192.168.0.254.

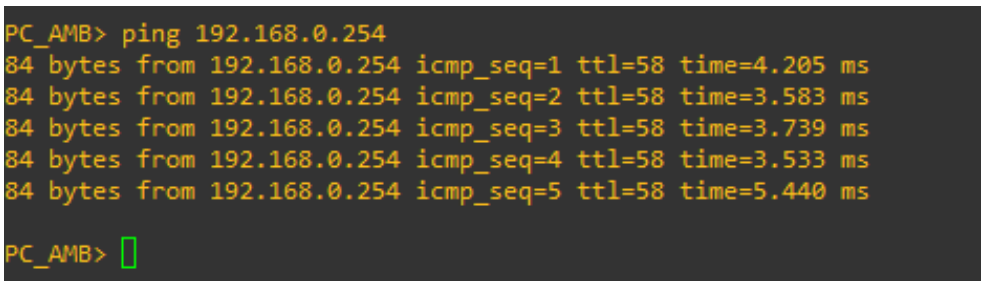


Figura 48. Prueba de conectividad desde PC_AMB hacia Matriz.

6. CONCLUSIONES Y RECOMENDACIONES.

Para finalizar el presente proyecto de titulación se tiene las siguientes conclusiones y recomendaciones que ayudaran a realizar y mejorar futuros proyectos relacionados.

6.1. Conclusiones

Como primera conclusión se puede indicar que se realizó el diseño y simulación de una red MPLS utilizando equipos MikroTik de una manera escalable para el transporte de servicios de la empresa Autopartes de manera exitosa, demostrando que estos equipos son muy confiables, robustos y con grandes funcionalidades que todavía no son explotados en su totalidad.

También se puede indicar que se logró analizar, comprender la arquitectura y los diferentes componentes que conforman una red MPLS.

Se pudo conocer el funcionamiento y el sinnúmero de características que poseen los equipos MikroTik.

En lo referente a la instalación del software GNS3 se pudo validar que es una herramienta confiable para realizar la simulación de redes mediante equipos MikroTik.

La gran ventaja del uso de equipos MikroTik es que se posee el mismo software en todos los equipos, la diferencia entre cada uno se da a nivel de licenciamiento para poder habilitar ciertas funcionalidades que no poseen ciertos equipos en el mercado.

En lo referente a la configuración de protocolos de enrutamiento utilizados, en este caso OSPF y BGP, se pudo evidenciar que el funcionamiento de los mismos no varía con referencia a cisco, pues tienen el misma lógica de configuración y el comportamiento con la gran ventaja de MikroTik que al momento de realizar configuraciones y troubleshooting la podemos realizar mediante comandos y a través de modo gráfico con el software winbox el cual ayuda a comprender de una mejor manera el funcionamiento.

6.2. Recomendaciones

Una de las principales recomendaciones para la simulación de una red mediante el software GNS3 es tener en cuenta las características mínimas requeridas recomendadas por el fabricante para la instalación.

En lo referente al diseño de la red, se recomienda iniciar el diseño de la red de manera jerarquita. Iniciar la configuración de enrutamientos y configuración de protocolos primero en los equipos de core (equipos P's) para luego enfocarse en los equipos de borde (equipos PE´s) y finalmente configurar los equipos de UM (equipos CPE's).

Se recomienda el estudio minucioso de los protocolos de configuración utilizados en MikroTik para facilitar el entendimiento y la solución de problemas de conectividad.

Es recomendable realizar la simulación de la red mediante el software GNS3 ya que es una herramienta libre de fácil uso y principalmente porque soporta la carga de IOS de varios fabricantes.

Se recomienda realizar un análisis previo antes de la implementación de una red MPLS, la jerarquía, escalabilidad y el conocimiento de los protocolos que serán utilizados.

Se recomienda realizar pruebas de conectividad tramo a tramo cuando se finalice una configuración para evitar inconvenientes futuros los cuales serán más complejos mientras va avanzando la simulación.

Referencias

Barberá, J. (2007). *RedIRIS*. Recuperado el 05 de Julio de 2018, de http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

Bombal, D. (2019). *https://www.gns3.com/*. Recuperado el 07 de Agosto de 2018

Don Jacob, T. M. (2017). *packetdesign.com*. Recuperado el 25 de Enero de 2019, de https://www.packetdesign.com/blog/quick-start-mpls-fundamentals/

Farrel, A. (2017). *ietfjournal*. Recuperado el 5 de Febrero de 2019, de https://www.ietfjournal.org/enrutamiento-por-segmentos-descubriendo-un-tesoro-de-innovacion-en-el-ietf/

Maldonado, V. (2012). *Comparación de protocolos de enrutamiento y modelos de movilidad para Redes Ad-Hoc Vehiculares usando mapas reales.* Loja: UTPL.

Martínez, A. (2013). *ospfgrupo5*. Recuperado el 3 de Septiembre de 2018, de http://ospfgrupo5.blogspot.com/p/areas.html

Mikrotik. (2013). *wiki.mikrotik*. Recuperado el 17 de Abril de 2019, de https://wiki.mikrotik.com/wiki/Manual:License

Mikrotik. (2019). *MikroTik*. (Mikrotik) Recuperado el 15 de Diciembre de 2018, de https://mikrotik.com/

Roosevelt, J. (2016). *Conceptos Fundamentales de MikroTik RouterOS v6.35.1.01.* Recuperado el 22 de Noviembre de 2018, de SCRIBD: https://es.scribd.com/document/331266566/Conceptos-Fundamentales-de-MikroTik-RouterOS-v6-35-1-01-2-pdf

Vélez, D. (2018). *DISEÑO Y SIMULACION EN GNS3 DE UNA RED MULTISERVICIOS MPLS PARA MEDIANAS EMPRESAS EN EL ECUADOR.* Guayaquil: Universidad Católica de Santiago de Guayaquil. Recuperado el 15 de Junio de 2018

ANEXOS

ANEXO 1

Equipo CPE MikroTik instalado en la red del cliente Autopartes (Sucursal y Matriz).

Specifications

Details	
Product code	RB750UPr2
Architecture	MIPSBE
CPU	QCA9531
CPU core count	1
CPU nominal frequency	650 MHz
Dimensions	113x89x28mm
License level	4
Operating System	RouterOS
Size of RAM	64 MB
Storage size	16 MB
Storage type	FLASH
Tested ambient temperature	-40°C to 70°C
Suggested price	$59.95

Powering

Details	
PoE in	Passive PoE
PoE out	Passive PoE
PoE in input Voltage	8-30 V
Number of DC inputs	2 (PoE-IN, DC jack)
DC jack input Voltage	8-30 V
Max out per port output (input < 30 V)	1 A
Max total out (A)	2 A
Max power consumption	51 W
Max power consumption without attachments	3 W

Ethernet

Details	
10/100 Ethernet ports	5

Peripherals

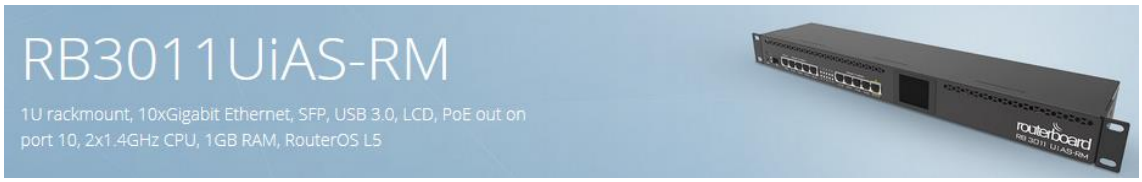
Details	
Number of USB ports	1
USB Power Reset	Yes
USB slot type	USB type A
Max USB current (A)	1

Other

Details	
Current Monitor	Yes
PCB temperature monitor	Yes
Voltage Monitor	Yes

ANEXO 2

Equipo PE MikroTik instalado en los nodos de acceso del proveedor FAST INTERNET.



Specifications

Details	
Product code	RB3011UiAS-RM
Architecture	ARM 32bit
CPU	IPQ-8064
CPU core count	2
CPU nominal frequency	1.4 GHz
Dimensions	443x92x44mm
License level	5
Operating System	RouterOS
Size of RAM	1 GB
Storage size	128 MB
Storage type	NAND
Tested ambient temperature	-20°C to 70°C
Suggested price	$179.00

Ethernet

Details	
10/100/1000 Ethernet ports	10

Powering

Details	
PoE in	Passive PoE
PoE out	Passive PoE
PoE in input Voltage	10-30 V
Number of DC inputs	2 (DC jack, PoE-IN)
DC jack input Voltage	10-30 V
Max out per port output (input < 30 V)	600 mA
Max total out (A)	600 mA
Max power consumption	30 W
Max power consumption without attachments	10 W

Fiber

Details	
SFP ports	1

Peripherals

Details	
Serial port	RJ45
Number of USB ports	1
USB Power Reset	Yes
USB slot type	USB 3.0 type A
Max USB current (A)	1

Other

Details	
PCB temperature monitor	Yes
Voltage Monitor	Yes

ANEXO 3

Equipo P MikroTik instalado en el CORE del proveedor FAST INTERNET.

Specifications

Details	
Product code	RB1100Dx4
Architecture	ARM 32bit
CPU	AL21400
CPU core count	4
CPU nominal frequency	1.4 GHz
Dimensions	444 x 148 x 47 mm
License level	6
Operating System	RouterOS
Size of RAM	1 GB
Storage size	128 MB
Storage type	NAND
Tested ambient temperature	-40°C to 70°C
Suggested price	$349.00

Ethernet

Details	
10/100/1000 Ethernet ports	13

Powering

Details	
PoE in	802.3af/at
PoE in input Voltage	20-57 V
Number of AC inputs	2
Number of DC inputs	2 (2-pin terminal, PoE-IN)
2-pin terminal input Voltage	-48, 20-57 V
Max power consumption	33 W
Max power consumption without attachments	25 W

Peripherals

Details	
Extended storage	60GB M.2 SSD included
M.2 slots	2
Memory card type	microSD
Memory Cards	1
SATA ports	2x SATA3
Serial port	RS232

Other

Details	
Current Monitor	Yes
PCB temperature monitor	Yes
Voltage Monitor	Yes