

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE SEGURIDADES, SERVICIOS Y PROTOCOLOS DE REDES EN EQUIPOS *MIKROTIK*

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

EDISON RODRIGO ARRIETA SUCUZHAÑAY

edison.arrieta@epn.edu.ec

DIEGO FERNANDO GUALLPA CAGUANA

diego.guallpa@epn.edu.ec

DIRECTORA: ING. MÓNICA VINUEZA RHOR

monica.vinueza@epn.edu.ec

QUITO, FEBRERO 2021

DECLARACIÓN

Nosotros, Edison Rodrigo Arrieta Sucuzhañay y Diego Fernando Guallpa Caguana, manifestamos bajo juramento que el presente proyecto es de nuestra autoría, que no ha sido antes expuesto en ningún grado o calificación profesional y que se ha consultado las referencias bibliográficas que se adjunta en este documento.

Sin quebranto de los derechos declarados en el párrafo I del artículo 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación -COESC-, somos titulares de la obra en mención y otorgamos una licencia gratuita, intransferible y no exclusiva de uso con fines académicos a la Escuela Politécnica Nacional. Entregaremos toda la información técnica pertinente. En el caso de que hubiese una explotación comercial de la obra por parte de la EPN, se negociará los porcentajes de los beneficios conforme lo establece la normativa nacional vigente.



Edison Rodrigo Arrieta Sucuzhañay



Diego Fernando Guallpa Caguana

CERTIFICACIÓN

Certifico que el siguiente trabajo fue realizado por Edison Rodrigo Arrieta Sucuzhañay y Diego Fernando Guallpa Caguana, bajo mi supervisión.

Ing. Mónica Vinueza Rhor MSc.

DIRECTORA DE PROYECTO

AGRADECIMIENTO

Un gran y profundo agradecimiento a mi DIOS y CREADOR por haberme dado la vida y por permitirme contar con mis queridos padres Carlos Arrieta y Carmita Sucuzhañay que con su amor han sido los brazos que me han sostenido, han sido mi guía y la lámpara en mi caminar, con su sabiduría me han enseñado de sus valores y han inculcado como ser una buena persona para la sociedad.

A mis queridos hermanos Verónica, Daniel, Mery y Brayan le estoy tan agradecido por su cariño, comprensión, ayuda y compañía.

No puedo dejar de mencionar la gran labor de cada uno de mis profesores, que con sus conocimientos y experiencias permitieron enriquecerme de habilidades y objetivos en mi vida. Han sido quienes me han permitido encaminar en mi vida laboral.

Para mis amigos de curso, con los cuales compartí buenos momentos y por estar presente en este momento muy importante de mi vida.

Como no dar un reconcomiendo y agradecimiento especial para nuestra directora de tesis Ing. Mónica Vinueza MSc, por su gran ayuda y consejos para terminar con éxito este proyecto.

Edison Rodrigo Arrieta Sucuzhañay

AGRADECIMIENTO

Gracias a Dios, que a él le debo este triunfo y mi crecimiento profesional, a mis padres María y Segundo que siempre me han dado su apoyo a pesar de cada obstáculo han estado ahí a mi lado dándome lo mejor con su arduo trabajo y dedicación. Es a quienes dedico esto por darme una formación académica e inculcarme valores que me han servido a lo largo de mi vida académica para ellos es este triunfo y para ellos todos mis agradecimientos.

Para mis mejores amigos con los cuales compartí hermosos momentos, por apoyarme y ayudarme y regalarme una buena experiencia a lo largo de mi carrera académica han sido tantas risas a carcajadas y tantos momentos de tensión que me llevo como un recuerdo para toda mi vida gracias, amigos por ustedes se pudo culminar esta etapa en la carrera profesional.

Para mis hermanos Jonathan, William y Clara que me han brindado su apoyo y consejo que luchan por superarse que sueñan grande que de eso se trata la vida a pesar de cada obstáculo que se nos presente seguir adelante como nos han enseñado nuestros padres.

Para mi directora de tesis Ing. Mónica Vinueza MSc, por tenernos paciencia y la confianza al apoyarnos en este periodo para la culminación de la carrera y formación académica.

Diego Fernando Guallpa Caguana

ÍNDICE DE CONTENIDO

❖	DECLARACIÓN.....	I
❖	CERTIFICACIÓN.....	II
❖	AGRADECIMIENTO.....	III
❖	RESUMEN.....	X
❖	ABSTRACT.....	XI
1.	INTRODUCCIÓN.....	1
1.1	Marco teórico.....	2
❖	<i>MikroTik</i>	2
❖	<i>MikroTik RouterOS</i>	2
❖	<i>MikroTik SwOS</i>	2
❖	<i>WinBox</i>	2
❖	CLI (<i>Command Line Interface</i>).....	2
❖	GUI (<i>Graphical User Interface</i>).....	3
❖	MAC (<i>Media Access Control</i>).....	3
❖	IP (<i>Internet Protocol</i>).....	3
❖	ARP (<i>Address Resolution Protocol</i>).....	3
❖	NAT (<i>Network Address Translation</i>).....	4
❖	Enrutamiento estático.....	4
❖	Enrutamiento dinámico.....	4
❖	BGP (<i>Border Gateway Protocol</i>).....	4
❖	<i>Firewall</i>	5
❖	DHCP (<i>Dynamic Host Configuration Protocol</i>).....	5
❖	DNS (<i>Domain Name System</i>).....	5
❖	VLAN (<i>Virtual LAN</i>).....	5
❖	Colas simples.....	5
❖	PuTTY.....	6
❖	Telnet (<i>Telecommunication Network</i>).....	6
❖	SSH (<i>Secure Shell</i>).....	6
❖	CMD (<i>CoMmanD prompt</i>).....	6
2.	METODOLOGÍA.....	7
3.	RESULTADOS Y DISCUSIÓN.....	8
3.1	Requerimientos de los equipos.....	8

❖	Análisis de los equipos	8
3.2	Modos de configuración de los equipos <i>MikroTik</i>	14
❖	<i>WinBox</i>	14
❖	Configuración vía <i>web</i>	15
❖	<i>PuTTY</i>	17
❖	<i>CMD</i>	18
3.3	Implementación de topologías de red	19
❖	Configuración de las diferentes topologías de red	19
3.4	Pruebas de funcionamiento de diferentes topologías de red	38
4	CONCLUSIONES Y RECOMENDACIONES.....	44
4.1	Conclusiones	44
4.2	Recomendaciones.....	45
5	Bibliografía.....	46
6	ANEXOS.....	49
❖	ANEXO A: Hojas guías de prácticas para profesores.....	50
❖	ANEXO B: Hojas guías de prácticas para estudiantes.....	168
❖	ANEXO C: Manual de Usuario.....	185

ÍNDICE DE FIGURAS

Figura 3.1	Página oficial de <i>routers MikroTik</i> .	8
Figura 3.2	<i>Router hEX lite RB750r2</i> .	9
Figura 3.3	<i>RouterBOARD RB951G-2HnD</i> de <i>MikroTik</i> .	9
Figura 3.4	<i>RB951Ui-2HnD</i> de <i>MikroTik</i> .	10
Figura 3.5	<i>RB750UPr2</i> de <i>MikroTik</i> .	11
Figura 3.6	Página oficial de <i>swicths MikroTik</i> .	12
Figura 3.7	<i>Cloud Switch CRS326-24G-2S</i> de <i>MikroTik</i> .	12
Figura 3.8	<i>Cloud Switch CSS326-24G-2S</i> de <i>MikroTik</i> .	13
Figura 3.9	Modo de configuración <i>MikroTik</i> .	14
Figura 3.10	Interfaz gráfica de <i>WinBox</i> .	15
Figura 3.11	Interfaz de línea de comando de <i>WinBox</i> .	15
Figura 3.12	Credenciales de acceso vía <i>web</i> .	16
Figura 3.13	Página de configuración vía <i>web</i> .	17
Figura 3.14	<i>Software PuTTY</i> para configuración de equipos <i>MikroTik</i> .	18
Figura 3.15	Configuración mediante <i>CMD (Telnet)</i> .	19
Figura 3.16	Ingreso al <i>router</i> .	19
Figura 3.17	Configuración de políticas de grupo.	20
Figura 3.18	Creación de usuarios.	21
Figura 3.19	Configuración de interfaces.	22
Figura 3.20	Configuración de rutas estáticas.	22
Figura 3.21	Configuración <i>DHCP</i> .	23
Figura 3.22	Configuración amarre <i>IP/MAC</i> .	24
Figura 3.23	Configuración <i>DHCP relay</i> .	25
Figura 3.24	Configuración <i>DHCP client</i> .	26
Figura 3.25	Configuración <i>DNS server</i> .	27
Figura 3.26	Configuración <i>DNS</i> transparente.	28
Figura 3.27	Configuración de ruta de salida.	29
Figura 3.28	Configuración de enmascaramiento.	29
Figura 3.29	Configuración enrutamiento <i>BGP</i> .	30
Figura 3.30	Configuración <i>Address lists</i> .	31
Figura 3.31	Configuración <i>Address lists</i> .	32
Figura 3.32	Configuración de acceso y restricción a internet.	33
Figura 3.33	Configuración de colas padre.	34
Figura 3.34	Configuración de colas hijos.	34
Figura 3.35	Configuración de ráfagas de velocidad.	35

Figura 3.36 Configuración de <i>bridge</i> .	36
Figura 3.37 Creación y levantamiento de interfaces <i>VLANs</i> en <i>router</i> .	37
Figura 3.38 Creación de <i>VLANs</i> en <i>switch</i> .	38
Figura 3.39 Lista de políticas de grupo.	39
Figura 3.40 Conectividad entre equipos.	39
Figura 3.41 Configuración de <i>DHCP</i> en <i>bridge</i> .	40
Figura 3.42 Tabla <i>DNS cache</i> .	41
Figura 3.43 Filtro de direcciones privadas en <i>BGP</i> .	41
Figura 3.44 Bloqueo de página <i>Netflix</i> .	42
Figura 3.45 Desactivación de colas simples por horario.	42
Figura 3.44 Bloqueo de página <i>Netflix</i> .	43
Figura 3.46 Conectividad entre <i>VLANs</i> .	43

ÍNDICE DE TABLAS

Tabla 3.1 Características del <i>router RB951G-2HnD</i> y <i>RB750r2</i>	10
Tabla 3.2 Características del <i>router RB951Ui-2HnD</i> y <i>RB750UPr2</i>	11
Tabla 3.3 Características de <i>switch CRS326-24G-2S</i> y <i>CSS326-24G-2S</i>	13

RESUMEN

Este proyecto es implementado con el objetivo de estudiar dispositivos de red ,tanto sus funciones usos y aplicaciones con la finalidad de adquirir conocimientos en la configuración ,administración y uso de estos equipos ,y así implementar prácticas de topologías de red, con equipos *Router* y *Switch* de la marca *MikroTik*, realizando un previo estudio de los equipos que cumplan con las características para llevar a cabo estas topología y de esa manera estudiantes y profesores puedan implementar de manera física cada topología estudiada y así desarrollar habilidades que los irán preparando para el diseño y construcción de redes y el mercado laboral afín.

En este proyecto se abarca conceptos de seguridades de acceso, creación de usuarios, filtros de *MAC/IP*, protocolos de enrutamiento estático y dinámico (*BGP*), control de tráfico (*Firewall*), servicio como *DHCP*, *DNS*, colas simples y *VLANs* para la implementación de 8 topologías de red cada una con su práctica de laboratorio, de manera que con la dotación de equipos *MikroTik* tanto para el uso de estudiantes como profesores de la ESFOT, puedan aplicar el conocimiento adquirido en el aula, y complementarlo de manera física, y con esto adiestrar y preparar de mejor manera a los profesionales.

La metodología en que se basó este proyecto es exploratoria, debido al uso de diferentes temas en el ámbito de redes y especialmente aplicado a equipos *MikroTik*, como resultado de este proyecto se pudo reforzar conocimientos de suma importancia en el área de redes, familiarizándose con las configuraciones de esta marca y generando la posibilidad de llegar con una mayor ventaja en el mundo laboral al estudiante. De esta manera se elaboró un manual básico de manejo de dichos equipos, detallando toda la configuración en cada tema, mediante el uso de línea de comandos como interfaz gráfica con la ayuda de hojas guía tanto para estudiante como para profesores.

Finalmente se determinó las conclusiones y recomendaciones como resultado del desarrollo de cada etapa de este proyecto.

ABSTRACT

This project is implemented with the objective of studying network devices, both their functions, uses and applications in order to acquire knowledge in the configuration, administration and use of these equipment, and thus implement practices of network topologies, with Router and Switch equipment. of the MikroTik brand, carrying out a prior study of the equipment that meets the characteristics to carry out these topologies and in this way students and teachers can physically implement each studied topology and thus develop skills that will prepare them for the design and building networks and the related labor market.

This project covers concepts of access security, user creation, MAC / IP filters, static and dynamic routing protocols (BGP), traffic control (Firewall), services such as DHCP, DNS, simple queues and VLANs for the implementation of 8 network topologies each with its laboratory practice, so that with the provision of MikroTik equipment both for the use of students and teachers of the ESFOT, they can apply the knowledge acquired in the classroom, and complement it physically, and with this, train and prepare professionals in a better way.

The methodology on which this project was based is exploratory, due to the use of different topics in the field of networks and especially applied to MikroTik equipment, as a result of this project it was possible to reinforce knowledge of great importance in the area of networks, becoming familiar with the configurations of this brand and generating the possibility of reaching the student with a greater advantage in the world of work. In this way, a basic manual for handling said equipment was prepared, detailing all the configuration in each subject, using the command line as a graphical interface with the help of guide sheets for both students and teachers.

Finally, the conclusions and recommendations were determined as a result of the development of each stage of this project.

1. INTRODUCCIÓN

Desde la aparición de las telecomunicaciones y el incesante avance de la tecnología, ha logrado que el sector de las Tecnologías de la Información y Comunicación (*TIC*) se convierta en el motor de las sociedades debido a su presencia en cada una de las actividades humanas.

Es por tal motivo que la demanda de servicios de telecomunicaciones ha crecido significativamente en los últimos tiempos. Todo esto ha provocado que surjan nuevos tipos de fabricantes que ofrezcan equipos de conectividad con bajos costos, menor consumo de energía, mínimos tiempos de inactividad y una fácil administración de la red.

La Escuela Politécnica Nacional es una institución que está a la vanguardia en la educación, que tiene como misión formar profesionales con conciencia ética y con la capacidad de proponer soluciones innovadoras a los problemas que los nuevos tiempos demandan.

La Escuela de Formación de Tecnólogos (ESFOT) de la Escuela Politécnica Nacional tiene un déficit de infraestructura adecuada que proporcionen ambientes de aprendizaje práctico convenientes para impartir los procesos de enseñanza necesarios para la formación de profesionales calificados.

Ante tal situación se propone la implementación y manejo de equipos *MikroTik* en el ámbito de seguridades y protocolos de enrutamiento como área de enseñanza para los estudiantes de la ESFOT.

1.1 Marco teórico

❖ MikroTik

Es una empresa letona creada en 1996 con el objetivo de ser una compañía proveedora de hardware de red (*routers* y *switch*), *software* de red (*RouterOS* y *SwOS*), sistemas ISP inalámbricos. *MikroTik* en la actualidad proporciona equipos de conectividad a Internet en la mayoría de los países a nivel mundial [1].

❖ MikroTik RouterOS

Es un sistema operativo independiente desarrollado en el núcleo Linux de *hardware MikroTik RouterBOARD*, el cual admite instrumentos de configuración tales como: *PUTTY*, *Tera Term*, *WinBox*, interfaz de configuración basado en *web* simple. *RouterOS* se lo puede instalar en un computador y convertir al ordenador en un enrutador con todas las características necesarias como son: *firewall*, puerta de enlace de punto de acceso, VPN, enrutamiento [2].

❖ MikroTik SwOS

Es un sistema operativo creado con el propósito de gestionar los equipos de conmutación *MikroTik*. *SwOS* es administrable desde un navegador web y brinda una funcionalidad básica, es decir, permite aplicar filtro *MAC*, configurar *VLAN*, regulación de ancho de banda, control de tormentas de transmisión, ajuste de encabezados *MAC* e *IP* y reenvío de puerto a puerto [3].

❖ WinBox

Es una aplicación ejecutable para *Windows*, *Linux* y *OSX* creada por *MikroTik* con el objetivo de administrar el *software RouterOS* empleando una interfaz gráfica (*GUI*) o mediante comandos (*CLI*). *WinBox* permite acceder a una gran variedad de configuraciones de una forma amigable y otorga a los usuarios la posibilidad de realizar comunicaciones mediante *Telnet* y *SSH* [4].

❖ CLI (*Command Line Interface*)

Es la interface de comandos, el cual es un programa que permite el ingreso y ejecución de comandos sobre un sistema operativo, es decir, *CLI* es un interpretador de comandos que requiere un cierto nivel de conocimientos en programación por parte del usuario. A

diferencia de la interfaz gráfica que contiene menús y botones, *CLI* acepta líneas de texto y los convierte en funciones en un sistema operativo [5].

❖ **GUI (*Graphical User Interface*)**

Es una interfaz de usuario gráfica que contiene imágenes, menús y botones y se caracteriza por el desarrollo de elementos gráficos, que permite al usuario tener una mayor y mejor interacción con el sistema operativo, siendo más amigable, dinámica e intuitivo. La principal función es la de generar un entorno visual que permite la comunicación con el sistema operativo de un ordenador [6].

❖ **MAC (*Media Access Control*)**

Una dirección *MAC*, también conocido como dirección física es un identificador único que los fabricantes de dispositivos de red lo asignan a los equipos. Este identificador está conformado por 48 bits representados en seis grupos de dos caracteres hexadecimales, los tres primeros octetos permiten identificar al fabricante (*OUI*), mientras los 3 siguientes octetos son un identificador del equipo o producto (*UAA*). La dirección *MAC* tiene presencia en el modelo OSI, específicamente en la capa de enlace [7].

❖ **IP (*Internet Protocol*)**

Es el protocolo que permite establecer conexiones de red mediante el proceso de envío y recepción de paquetes de información. Las direcciones *IP* es parte de la capa de red del modelo *OSI* y está compuesto de 32 bits expresados de manera decimal o hexadecimal para facilitar su uso y lectura. Las direcciones *IP* se encuentran en cada dispositivo que tiene acceso a Internet como son: *routers*, teléfonos, televisores, ordenadores, etc. La asignación de direcciones *IP* se lo puede realizar de forma estática o *dinámica* [8].

❖ **ARP (*Address Resolution Protocol*)**

Es el protocolo de resolución de direcciones que permite asociar una dirección *MAC* de un dispositivo con una dirección *IP* conectado a la red. La asociación entre *IP* y *MAC* se realiza cuando el protocolo *ARP* averigua a cada dispositivo de red sobre sus direcciones físicas y luego crea una tabla donde se registra cada dirección física con su correspondiente dirección lógica [9].

❖ **NAT (*Network Address Translation*)**

Es el servicio que se encarga de traducir direcciones de red privadas a direcciones públicas. *NAT* permite que los dispositivos de una red privada reutilicen direcciones *IP* públicas creando un cuadro de conexiones que pasan por *Internet Gateway* para asignar aleatoriamente un número de puerto para identificar cada conexión, aunque se emplee la misma dirección *IP* cuando. Esto ayuda a preservar la cantidad de direcciones *IPv4* que son limitadas cuando son incompatibles la *IP* de origen y destino, es decir, entre redes privadas y redes públicas [10].

❖ **Enrutamiento estático**

Es un método manual que permite determinar el camino que debe seguir un paquete de datos hasta alcanzar su destino, para ello se debe indicar explícitamente en cada dispositivo (*router*) las redes que pueden ser alcanzadas y el camino para alcanzar dichas redes. El enrutamiento estático se emplea en redes pequeñas que no necesitan escalabilidad, siendo sencilla su configuración para crear las tablas de enrutamiento de un equipo. Esta información debe ser proporcionada por el administrador de la red [11].

❖ **Enrutamiento dinámico**

Conocido también como enrutamiento adaptativo, es un método que tiene gran escalabilidad y que permite decidir el trayecto más eficiente por donde un paquete de datos deber ir a través de la red hacia un destino determinado. El enrutamiento dinámico para determinar las mejores rutas emplea algoritmos, protocolos y estos son sujetos a cambios que existan en una topología de red. Este método es empleado para redes de grandes extensiones [12].

❖ **BGP (*Border Gateway Protocol*)**

Es el protocolo de puerta de enlace de frontera que utilizan los diferentes sistemas autónomos (AS) para comunicarse entre sí y de esta manera poder transferir grandes cantidades de información mediante el intercambio de prefijos de rutas en forma dinámica. *BGP* tiene como objetivo encontrar la ruta más eficiente entre los nodos para garantizar un correcto flujo de la información en Internet. *BGP* es un protocolo que funciona sobre *TCP* por el puerto 179 [13].

❖ Firewall

Es un sistema que permite administrar todo el tráfico que ingresa y sale entre una red interna (*LAN*) y una red externa (Internet). *Firewall* también conocido como cortafuegos funciona como una barrera de protección para las redes privadas ante los ingresos no autorizados de terceros que pueden robar o suplantar datos confidenciales, denegar servicios o pérdida de información sensible. *Firewall* se puede implementar como un equipo (*hardware*) o un programa (*software*) [14].

❖ DHCP (*Dynamic Host Configuration Protocol*)

Es un protocolo de configuración de dispositivos que permite que se pueda asignar de forma dinámica direccionamiento *IP* para cada equipo que se conecta a una red o a la Internet. *DHCP* tiene como objetivo simplificar la administración de la red mediante la distribución de direcciones *IP* y fue desarrollada para reducir en gran medida los errores que produce el arrendamiento de direcciones *IP* de manera manual en redes de grandes dimensiones [15].

❖ DNS (*Domain Name System*)

Es un sistema que permite traducir de forma fácil los nombres de dominio que son conocidos por las personas a direcciones *IP* utilizadas por los computadores. *DNS* es un intermediario que vincula los nombres de sitios *web* con las direcciones lógicas de *host* dentro de una base de datos. De esta manera *DNS* permite una navegación amigable para los usuarios [16].

❖ VLAN (*Virtual LAN*)

Es una red de área local virtual que se encarga de agrupar equipos de manera lógica dentro de una red física, es decir, que se puede crear diferentes *VLAN* dentro de una misma red *LAN*. *VLAN* permite crear redes que lógicamente son independientes pero que necesitan intercambiar datos o información entre sí. De esta forma, el administrador podrá disponer de varias *VLAN* dentro de un mismo equipo *switch* y *router* [17].

❖ Colas simples

Es un método sencillo para limitar el consumo de recursos de red como regular el ancho de banda en cada cliente mediante la combinación de reglas que se ejecutan una a la vez, implementar características de calidad de servicio (*QoS*), controlar el tráfico en direcciones

IP o usuarios. Las colas simples permiten controlar el flujo de datos en la red mediante la delimitación del ancho de banda para evitar congestiones de tráfico [18].

❖ **PuTTY**

Es un *software* ejecutable de terminal gratuito y de código abierto para sistemas *Windows* y *UNIX*. Emplea varios protocolos de administración de red como *SSH*, *Telnet*, *Rlogin*, *Raw* y soporta conexiones de puerto serial local. *PuTTY* brinda una interfaz gráfica de configuración muy amigable con el usuario y que permite iniciar sesión de consola en sistemas remotos [19].

❖ **Telnet (*Telecommunication Network*)**

Es un protocolo estándar de la arquitectura *TCP/IP* que permite acceder a un equipo de forma remota solo en modo comandos trabajando en el puerto 23. *Telnet* se ejecuta en línea de comandos del ordenador. Las conexiones remotas no cuentan con cifrado, es decir, no cuenta con ningún nivel de *encriptación*. Es empleado generalmente por los administradores de sistemas informáticos en el área de las redes [20].

❖ **SSH (*Secure Shell*)**

Es un protocolo de red que permite a los usuarios tener el acceso seguro a un equipo o un servidor de forma remota para realizar la función de copia y transferencia de datos. *SSH* fue desarrollado para reemplazar métodos antiguos de conexión remota como *Telnet*. Este protocolo emplea una arquitectura cliente/servidor y emplea técnicas de cifrado que ayuda a encriptar la información que se genera por cada sesión haciendo imposible que algún tercero pueda acceder a las contraseñas. *SSH* trabaja en el puerto 22 [21].

❖ **CMD (*Command prompt*)**

El Símbolo del Sistema es un programa traductor de comandos desarrollado por *Windows* que utiliza el mismo sistema operativo para el ingreso, interpretación y ejecución de comandos. *CMD* es empleado para realizar varias tareas de forma rápida, las cuales también podrían ser realizadas desde un entorno gráfico del sistema operativo. El programa se ejecuta en modo texto y no es tan intuitivo y amigable con el usuario como si lo es la interfaz gráfica [22].

2. METODOLOGÍA

Este proyecto tuvo su base en la investigación exploratoria y aplicada. La investigación exploratoria se aplicó para realizar un acercamiento hacia la problemática que representa el déficit de equipos de red que permitan un aprendizaje práctico con el fin de llevar a cabo las fases de instrucción necesarios para la formación de profesionales calificados en la carrera de Tecnología en Electrónica y Telecomunicaciones. Una de las marcas de equipos de conectividad que están en auge en la actualidad es la marca *MikroTik*, por ello se realizó un análisis entre la gama de equipos de conectividad que ofrece dicha marca y se identificó 4 *Routers* y 4 *Switchs* que permitan realizar los diferentes tipos de configuraciones que se requiere para solventar el aprendizaje de los estudiantes.

La investigación aplicada fue usada con el objetivo de resolver el problema antes planteado. Para ello se procedió con la adquisición de los equipos con un estudio de mercado previo referente a costos. De esta manera se da solución al déficit de equipos de red. Un complemento de esta solución fue la implementación de 8 topologías de red que permita crear prácticas de laboratorio para reforzar y fortalecer el conocimiento teórico. Las prácticas de laboratorio de acuerdo con las topologías de red implementadas contienen configuraciones de seguridad como son contraseñas de acceso a equipos, filtrado por *MAC* e *IP*, bloqueo de puertos, *firewall*, enrutamiento estático, enrutamiento dinámico (*BGP*), *DHCP*, *DNS*, *VLAN* y colas simples mediante *CLI* y *GUI*.

Adicionalmente, se implementó un manual del uso de los equipos, en el cual se detalla las diferentes configuraciones de las topologías.

3. RESULTADOS Y DISCUSIÓN

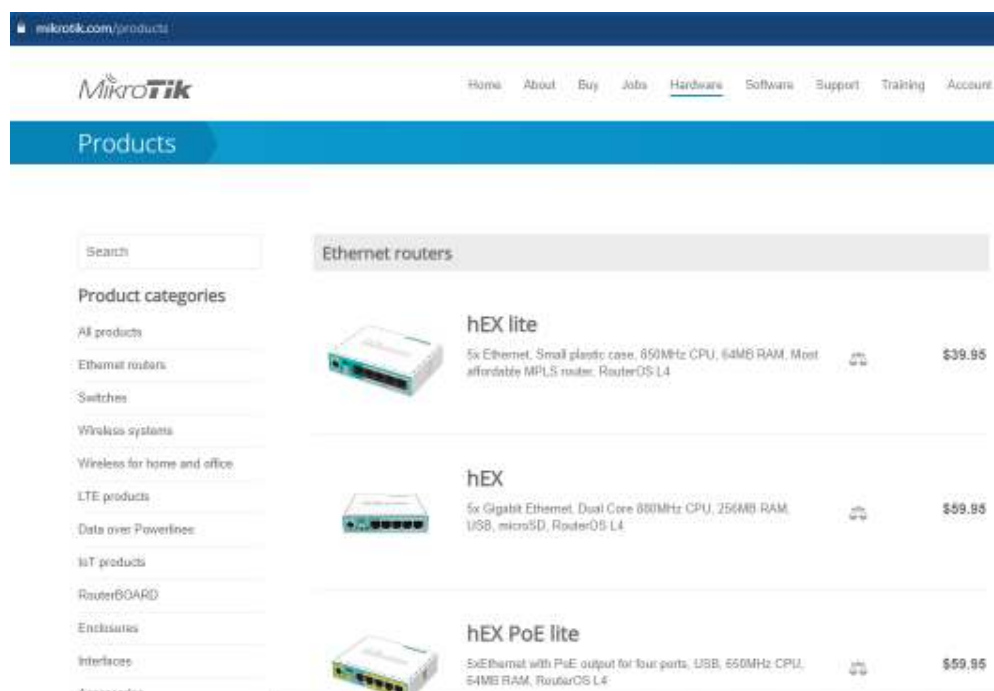
3.1 Requerimientos de los equipos

En esta primera etapa se ha realizado un estudio de los equipos que brinden los requerimientos necesarios para ser empleados en este proyecto.

❖ Análisis de los equipos

Se efectuó un análisis sobre los requerimientos que necesita el *router* para la implementación de este proyecto y se determinó que el equipo debe tener las siguientes características: 5 puertos Ethernet RJ45 con velocidades de 10/100 Mbps que es compatible con cualquier red *Ethernet*. Memoria RAM de 128 MB para enrutamiento *IP* y cache *ARP*. *Wireless* de 2.4 GHz con velocidad de 300 Mbps que es compatible con todos los dispositivos independientemente si cuentan con *Wi-Fi 802.11b*, *802.11g* o *802.11n*. Puerto USB tipo A para respaldar y cargar *backups* de configuración. *Software RouterOS* para configurar vía línea de comandos o interfaz gráfica el equipo.

Una vez determinado las características, se procedió a obtener información de equipos que cumplan con dichos requerimientos, ver figura 3.1.



The image shows a screenshot of the MikroTik website's product page for Ethernet routers. The page features a search bar, a navigation menu with 'Hardware' selected, and a list of product categories on the left. The main content area displays three router models: hEX lite, hEX, and hEX PoE lite, each with a small image, a brief description of its specifications, and its price.

Product Name	Specifications	Price
hEX lite	5x Ethernet, Small plastic case, 850MHz CPU, 64MB RAM, Most affordable MPLS router, RouterOS L4	\$39.95
hEX	5x Gigabit Ethernet, Dual Core 880MHz CPU, 256MB RAM, USB, microSD, RouterOS L4	\$59.95
hEX PoE lite	5x Ethernet with PoE output for four ports, USB, 650MHz CPU, 64MB RAM, RouterOS L4	\$59.95

Figura 3.1 Página oficial de *routers MikroTik*

Se escogió algunos modelos que ofrece *MikroTik* en *routers* y entre ellos se tiene:

- *Router hEX lite RB750r2*
- *RouterBOARD RB951Ui-2HnD*
- *RouterBOARD RB951G-2HnD*
- *RouterBOARD RB750UPr2*

A continuación, se procedió a realizar un cuadro comparativo con las características técnicas de cada equipo para determinar cuál de ellos cumple los requerimientos.

Los primeros equipos en ser comparados fueron el *Router hEX lite RB750r2*, ver figura 3.2 y el *Router RB951G-2HnD*, ver figura 3.3. Se elaboró un cuadro comparativo, ver tabla 3.1, en el que se detalla las características de los *routers* antes mencionados para analizar si posee las especificaciones técnicas.

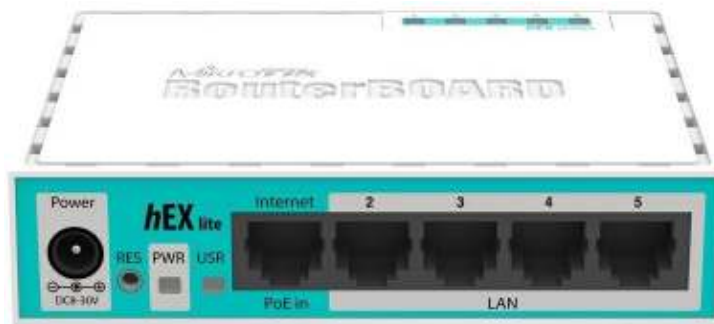


Figura 3.2 Router *hEX lite* RB750r2



Figura 3.3 RouterBOARD RB951G-2HnD de MikroTik

Tabla 3.1 Características del *router RB951G-2HnD* y *RB750r2*

CARACTERÍSTICAS TÉCNICAS DE <i>ROUTER MIKROTIK</i>		
MARCA	<i>MikroTik</i>	
MODELO	<i>RB951G-2HnD</i>	<i>RB750r2</i>
PARÁMETROS TÉCNICOS SOLICITADOS		
Sistema Operativo <i>RouterOS</i>	✓	✓
4 puertos <i>Ethernet</i> 10/100 Mbps	✓	✓
Puerto <i>PoE</i>	✓	✓
Memoria <i>RAM</i> 128 MB	✓	
Puerto <i>USB</i> tipo A	✓	
Soporta enrutamiento estático y dinámico	✓	✓
<i>Wireless</i> 2.4 GHz de 300 Mbps	✓	

El equipo *RouterBOARD RB951G-2HnD* cuenta con todas las características técnicas solicitadas en el proyecto. El *router hEX lite RB750r2* dispone de una memoria *RAM* de menor capacidad a las requeridas, necesarios para el almacenamiento de las tablas de enrutamiento *IP* y cache *ARP*. Además, no cuenta con tecnología inalámbrica. Por tales motivos el equipo queda descartado del proyecto.

Los siguientes equipos analizados fueron el *RB951Ui-2HnD*, ver figura 3.4 y *RB750UPr2*, ver figura 3.5. Se elaboró un cuadro comparativo, ver tabla 3.2, en el que se detalló las características del *router* para analizar si dispone de las especificaciones técnicas antes mencionadas.



Figura 3.4 *RB951Ui-2HnD* de *MikroTik*



Figura 3.5 RB750UPr2 de MikroTik

Tabla 3.2 Características del router RB951Ui-2HnD y RB750UPr2

CARACTERÍSTICAS TÉCNICAS DE ROUTER MIKROTIK		
MARCA	MikroTik	
MODELO	RB951Ui-2HnD	RB750UPr2
PARÁMETROS TÉCNICOS SOLICITADOS		
Sistema Operativo RouterOS	✓	✓
4 puertos Ethernet 10/100 Mbps	✓	✓
Puerto PoE	✓	✓
Memoria RAM 128 MB	✓	
Puerto USB tipo A	✓	
Soporta enrutamiento estático y dinámico	✓	✓
Wireless 2.4 GHz de 300 Mbps	✓	

El router RB951Ui-2HnD posee todas las especificaciones técnicas que requiere para la implementación de este proyecto.

Por tanto, se llegó a la conclusión que los equipos RB951G-2HnD y RB951Ui-2HnD tiene todos los requerimientos solicitados para la implementación de cada topología de red propuesta en este proyecto. En el mercado no se pudo encontrar la cantidad necesaria de equipos en un solo modelo, pero el análisis realizado anteriormente permitió la posibilidad de adquirir routers de los 2 modelos que cumplen con los requerimientos necesarios.

A continuación, se efectuó un análisis sobre los requerimientos que necesita el switch para en este proyecto y se determinó los siguientes requisitos: 24 puertos RJ45 de 10/100/1000 Mbps administrable o inteligente, es decir que cuente con SwOS para la implementación

de VLAN, SNMP, enrutamiento IP, QoS. Una vez determinado las características del switch se procedió a obtener información de equipos *MikroTik* que cumplan con dichos requerimientos, ver figura 3.6.

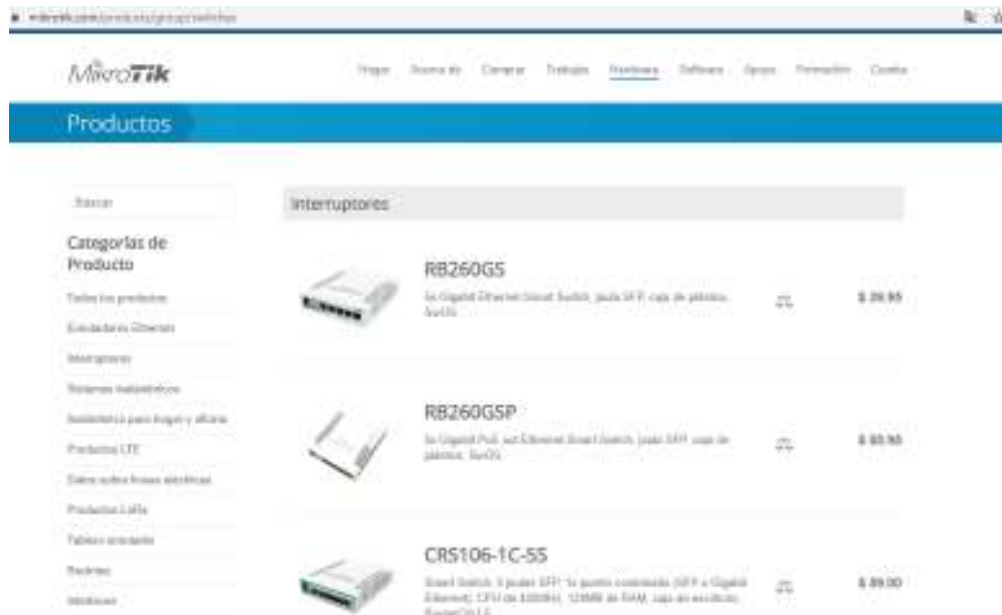


Figura 3.6 Página oficial de swiths *MikroTik*

Una vez identificado las características del switch, se identificó posibles modelos que ofrece *MikroTik* y entre ellos se tiene:

- *Cloud Switch CRS326-24G-2S*
- *Cloud Switch CSS326-24G-2S*

Con las características de los equipos *Cloud Switch CRS326-24G-2S*, ver figura 3.7 y *CSS326-24G-2S*, ver figura 3.8. Se elaboró un cuadro comparativo, ver tabla 3.3.



Figura 3.7 *Cloud Switch CRS326-24G-2S* de *MikroTik*



Figura 3.8 Cloud Switch CSS326-24G-2S de MikroTik

Tabla 3.3 Características de switch CRS326-24G-2S y CSS326-24G-2S

CARACTERISTICAS TÉCNICAS DE SWITCH MIKROTIK		
MARCA	MikroTik	
MODELO	CRS326-24G-2S	CSS326-24G-2S
PARÁMETRO TÉCNICO SOLICITADO		
Sistema Operativo SwOS	✓	✓
24 puertos 10/100/1000 Mbps	✓	✓
VLAN	✓	✓
Enrutamiento IP	✓	✓
QoS	✓	✓

Una vez, realizado el análisis de los equipos se llegó a la siguiente conclusión, los dos modelos de *switchs* cuentan con todas las características técnicas indispensables para la implementación desarrollo de este proyecto.

Después de identificar los equipos (*routers* y *switchs*) para el proyecto se procedió con la búsqueda de empresas proveedoras de dispositivos de conectividad como:

- FIS Solutions
- Aire Wireless and Security Solutions
- ALTALA The Network Company

Se solicitó proformas a cada uno de estos proveedores y una vez definidos los precios de los equipos se procedió con la compra de estos.

3.2 Modos de configuración de los equipos *MikroTik*

MikroTik desarrollo una aplicación llamado *WinBox* para el acceso y configuración de equipos de esta marca. Dicho *software* se lo puede descargar directamente de la página oficial de *MikroTik*, pero no es el único *software* que permite acceder y configurar los equipos, sino que además existe otros *softwares* como son: *Putty* (*Telnet/SSH*), *CMD(Telnet)*. Adicional existe una forma de configurar los equipos sin la necesidad de un *software* como lo es vía *web*, ver figura 3.9.

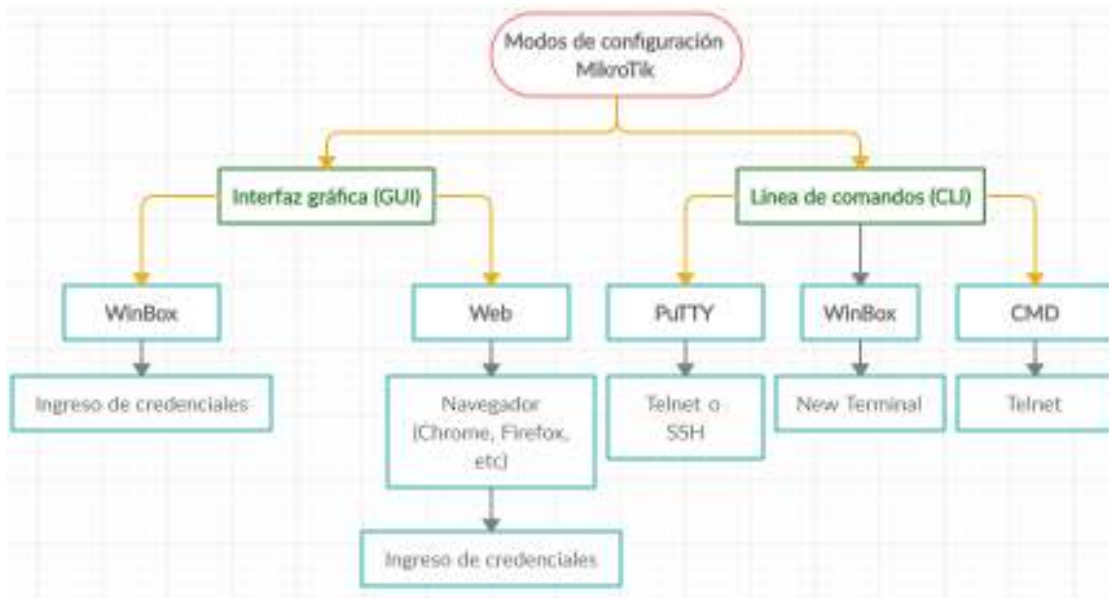


Figura 3.9 Modo de configuración *MikroTik*

❖ WinBox

WinBox es una aplicación utilizada en los entornos *OSX*, *Windows* y *Linux* desarrollada por *MikroTik* para que los usuarios tengan la posibilidad de administrar *RouterOS* mediante la interfaz gráfica (*GUI*) o la interfaz de comandos (*CLI*). *GUI* es una interfaz gráfica, ver figura 3.10, el cual contiene menús, casilleros con opciones, permitiendo al usuario realizar configuraciones de forma amigable, intuitivas y dinámicas.

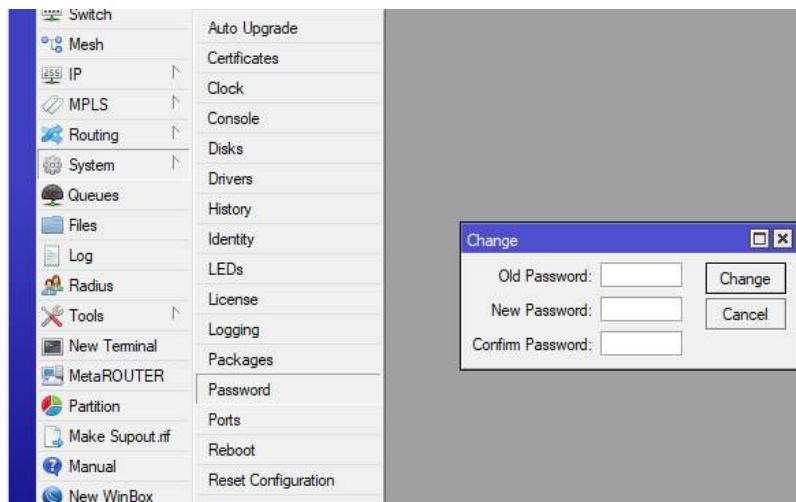


Figura 3.10 Interfaz gráfica de WinBox

Mientras que para acceder a la interface de comandos (CLI) en WinBox, ver figura 3.11, se elige en la barra de menú la opción *New Terminal* la misma que despliega una ventana que permite el ingreso de comandos para la configuración del equipo.

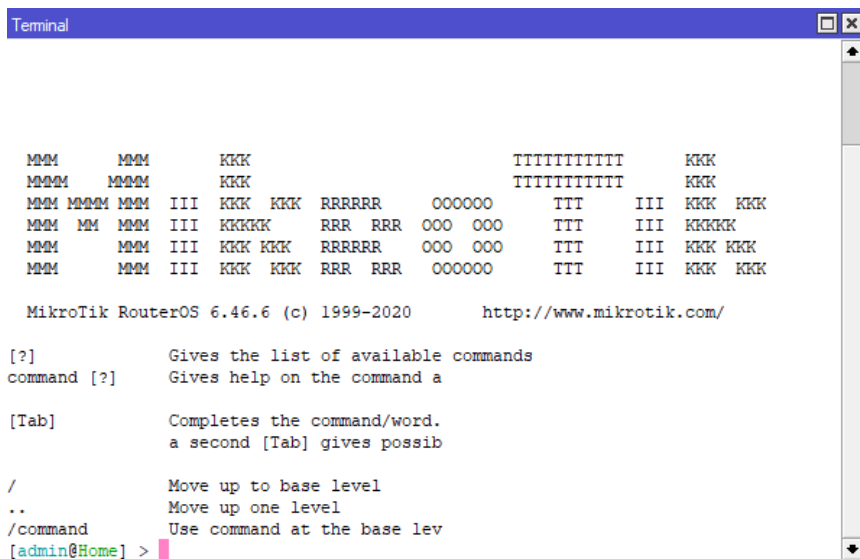


Figura 3.11 Interfaz de línea de comando de WinBox

❖ Configuración vía web

MikroTik permite al administrador ingresar mediante cualquier navegador *web* para realizar configuraciones de los equipos. Para ello es necesario realizar una conexión física y una lógica. Para realizar la conexión física se necesita un ordenador, en el que su tarjeta de red esté conectado directamente al equipo *MikroTik* en uno de sus puertos mediante un *Patch Cord RJ45*. Para la conexión lógica es necesario que el ordenador este dentro de la misma

red del equipo *MikroTik*. Por *default* los equipos *MikroTik* tiene la dirección 192.168.88.1/24 y en este caso se configuró la interface de red (NIC) del computador con la dirección IP 192.168.88.2/24. A continuación, se abre un explorador web (*Mozilla*, *Chrome*, *Internet Explorer*, *Opera*) y se coloca en el navegador la dirección IP del equipo *MikroTik*. Se desplegará una ventana que solicita el ingreso de un usuario (*Login*) y una contraseña (*Password*), ver figura 3.12.

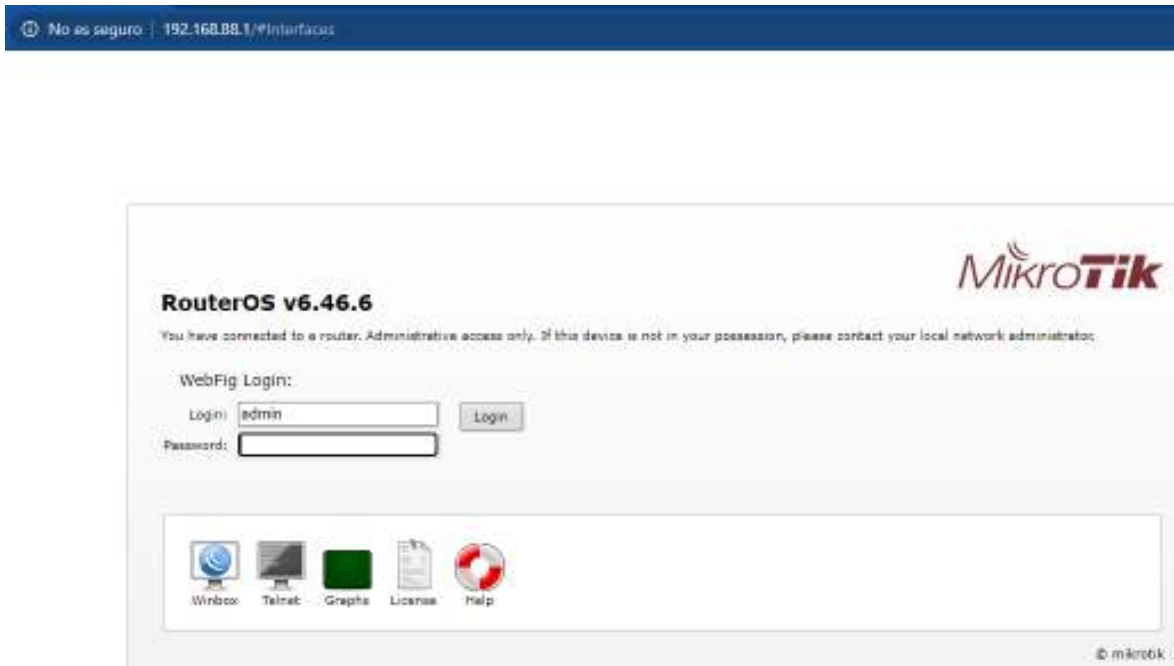


Figura 3.12 Credenciales de acceso vía web

Por *default* el usuario es *admin* y no cuenta con contraseña. Una vez ingresado las credenciales de seguridad se ingresará a la página de configuraciones *MikroTik* por web, ver figura 3.13.

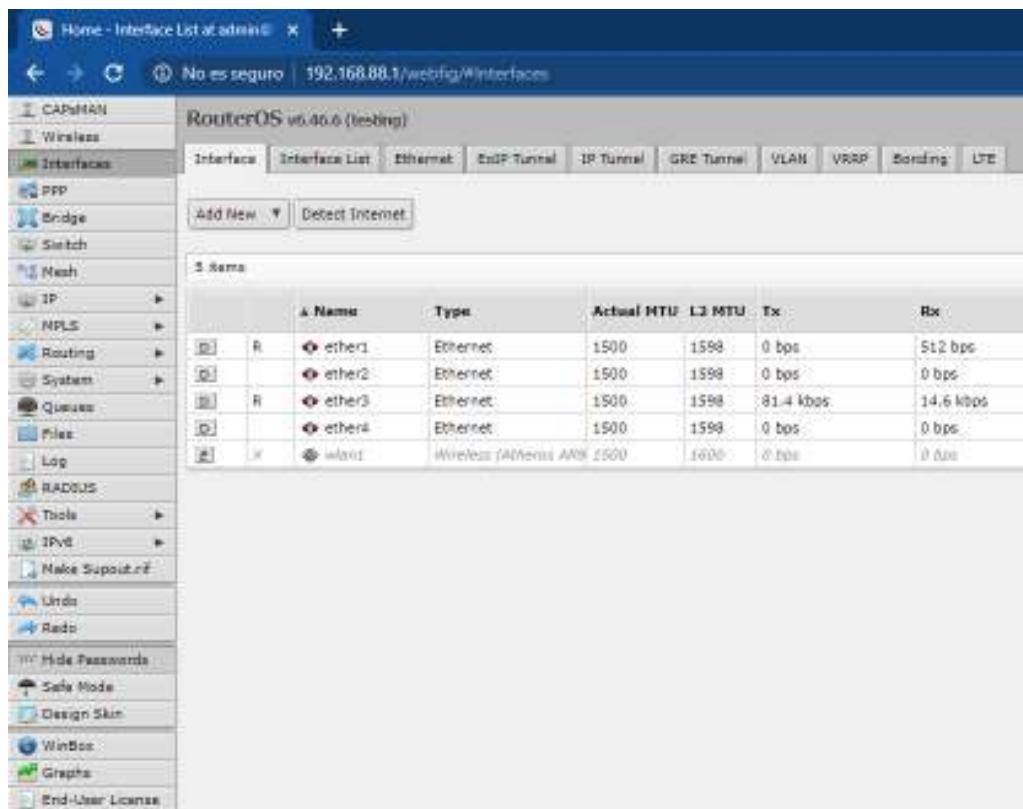


Figura 3.13 Página de configuración *vía web*

❖ PuTTY

Para la administración de equipos *MikroTik* mediante *PuTTY*, es necesario descargar el *software* directamente de su página oficial (<https://www.putty.org/>). A continuación, se procede a ejecutar el *software* ya que no necesita ser instalado. Se coloca la dirección *IP* del equipo *MikroTik* y se selecciona el protocolo *SSH* o *Telnet* según sea la necesidad del administrador, ver figura 3.14. Luego se elige la opción *Open* y se despliega el terminal del equipo *MikroTik*, en donde se ingresan los comandos para realizar las configuraciones.

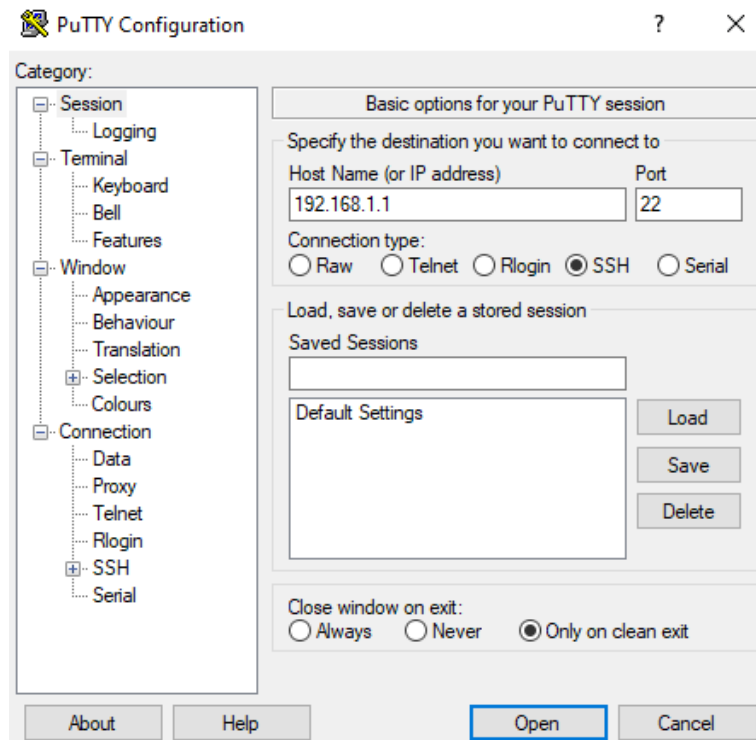


Figura 3.14 Software PuTTY para configuración de equipos MikroTik

❖ CMD

El símbolo de sistema permite el ingreso, interpretación y ejecución de comandos para realizar configuraciones. Para acceder a equipos *MikroTik* mediante *CMD* es necesario emplear el protocolo de acceso *Telnet*, por ello una vez ingresado a *CMD* es necesario escribir el comando *telnet* seguido de la dirección *IP* que tiene el equipo una vez ingresado el comando se despliega una ventana que solicita credenciales de autenticación. Una vez colocada las respectivas credenciales el usuario ingresará al sistema *RouterOS* donde podrá realizar las configuraciones, ver figura 3.15.

```

Telnet 192.168.88.1
sword:

MMM      MMM      KKK      TTTTTTTTTTT      KKK
MMMM    MMMM     KKK      TTTTTTTTTTT      KKK
MMM MMMM MMM III  KKK KKK RRRRRR   000000   TTT   III  KKK  KKK
MMM MM  MMM III  KKKKK  RRR  RRR  000 000   TTT   III  KKKKK
MMM     MMM III  KKK KKK RRRRRR   000 000   TTT   III  KKK  KKK
MMM     MMM III  KKK KKK RRR  RRR  000000   TTT   III  KKK  KKK

MikroTik RouterOS 6.46.1 (c) 1999-2019      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

```

Figura 3.15 Configuración por medio CMD (Telnet)

3.3 Implementación de topologías de red

Los temas propuestos en este proyecto son de mucho valor para obtener un mayor nivel de conocimientos en la administración de topologías.

❖ Configuración de las diferentes topologías de red

Acceso a un router

Para ingresa por primera vez al router sea mediante WinBox o Webfig, este cuenta con un usuario por defecto llamado *admin* y sin contraseña, ver figura 3.16.



Figura 3.16 Ingreso al router

Creación de políticas de grupo

Permitir el acceso al *router* es de gran importancia para mantener una red de datos segura, es uno de los niveles de seguridad que debe contar toda topología. En el caso del sistema operativo *RouterOS* que maneja *MikroTik*, posee políticas de seguridad que permite al administrador de red asignar los permisos o privilegios a cada usuario. Mediante *WinBox* es posible crear nuevas políticas de grupo.

```
- [admin@MikroTik] > user group add name=write
policy=telnet,read,local,ssh,write,test,winbox,web,sniff,api,romon,
dude,tikapp
```

De forma gráfica se ingresa al menú *System, Users* y la pestaña *Group*, ver figura 3.17.

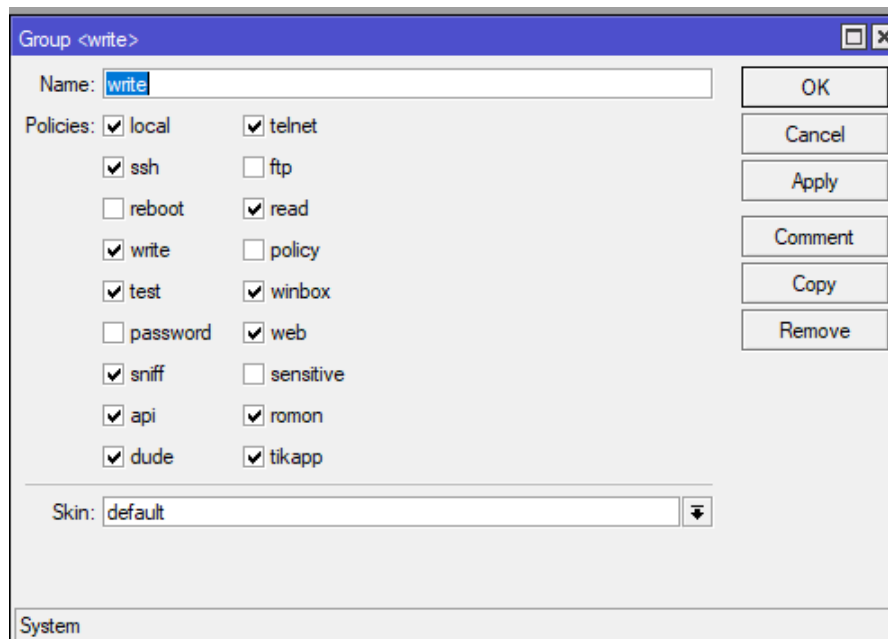


Figura 3.17 Configuración de políticas de grupo

Creación de usuarios

La creación de nuevos usuarios para el acceso al *router* es una de las configuraciones más importantes para la red en temas de seguridad. Es necesario asociar cada usuario con un grupo en específico de acuerdo a las necesidades de cada usuario. Para ello se debe ingresar los siguientes comandos:

```
- [admin@Router_LAN] > user add group=read name=Consultor_externo
password=Ce123456
```


De forma gráfica para la creación de usuarios se ingresa al menú a la pestaña *Users*, ver figura 3.18.



Figura 3.18 Creación de usuarios

Configuración de interfaces

Dentro de las configuraciones en una red es necesario el levantamiento de interfaces para permitir una conectividad entre equipos. Para ello se define las rutas de encaminamiento donde se debe saber la ruta destino, *gateway* y se emplea los siguientes comandos para su configuración:

- [admin@R1] > `IP route add distance=1 dst-address=172.16.128.0/18 gateway=10.0.0.62 comment=Gateway_LAN`

Para su configuración de forma gráfica se selecciona la opción *IP/Addresses*, ver figura 3.19.

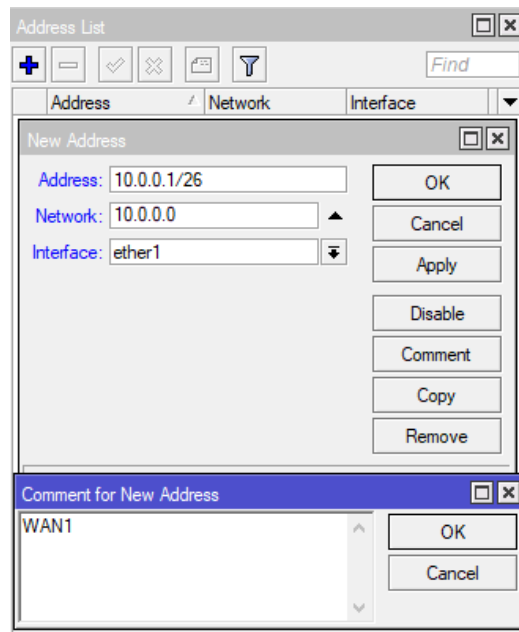


Figura 3.19 Configuración de interfaces

Configuración de rutas estáticas

Para la configuración de rutas estáticas se coloca la distancia administrativa (*Distance*), para una red estática la distancia administrativa es 1, se especifica el Gateway (*Gateway*) para alcanzar las redes que no se encuentran conectadas directamente en cada *router*.

Para ello se debe ingresar los siguientes comandos:

- [admin@R1] > IP route add distance=1 dst-address=10.0.0.64/26 gateway=10.0.0.62 comment=Gateway_WAN2

De manera gráfica se configura ingresando al menú *IP/Route*, ver figura 3.20.

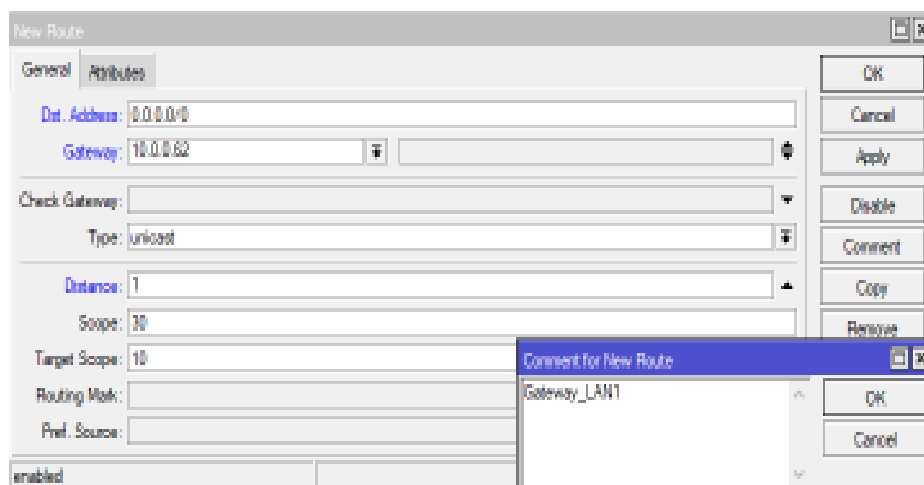


Figura 3.20 Configuración de rutas estáticas

Configuración de *DHCP*

DHCP se emplea como un protocolo de configuración en topologías de gran cantidad de equipos de conectividad y *hosts*, donde se requiere una aleatoria asignación de direcciones *IP*. Para su configuración es necesario saber la dirección de red, *gateway*, rango de direcciones a ser distribuidas, tiempo de prestación de la dirección dinámica y se ingresa los siguientes comandos:

```
[admin@Router] > IP DHCP-server setup
Select interface to run DHCP server on
DHCP server interface: DCHP1
Select network for DHCP addresses
DHCP address space: 192.168.2.0/24
Select gateway for given network
gateway for DHCP network: 192.168.2.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.2.2-192.168.2.254
Select DNS servers
dns servers: 8.8.8.8
Select lease time
```

Para la configuración de *DHCP* por medio de la interfaz gráfica se ingresa al menú *IP/DHCP* setup, ver figura 3.21.

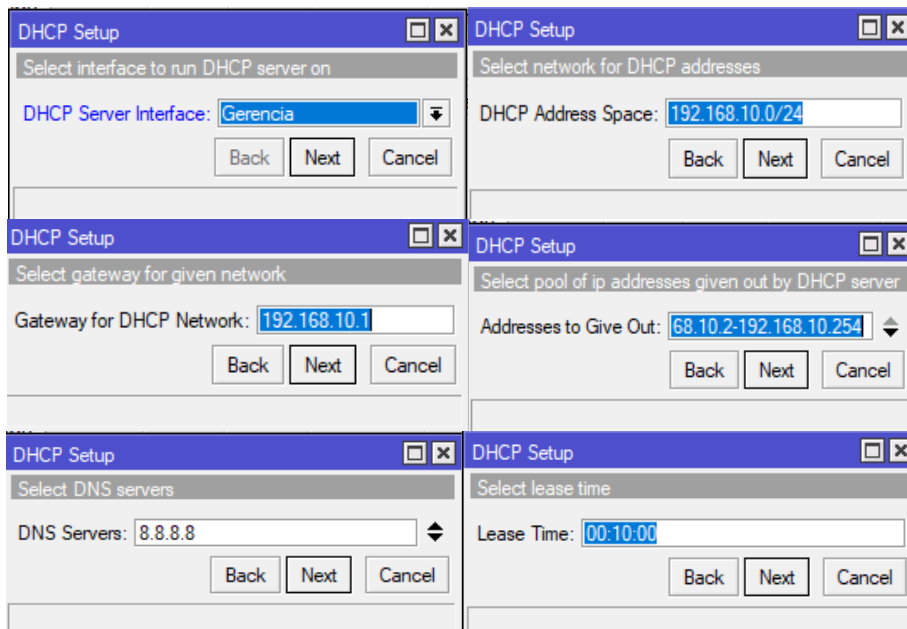


Figura 3.21 Configuración *DHCP*

Configuración de amarre *IP/MAC*

La reserva de determinada dirección *IP* es una herramienta muy útil al momento de configurar dispositivos que son estáticos y es necesario que no varíe la dirección *IP*. Para reservar determinada dirección *IP* por medio de la dirección *MAC* se ingresa los siguientes comandos:

- [admin@Router] > IP DHCP-server lease add address=192.168.2.77 mac-address=38:60:77:b0:ee:ae server=DHCP_WAN2 comment=impresora

Para la configuración de amarre *IP/MAC* por medio de la interfaz gráfica se ingresa al menú *IP/DHCP server* y (+), ver figura 3.22.

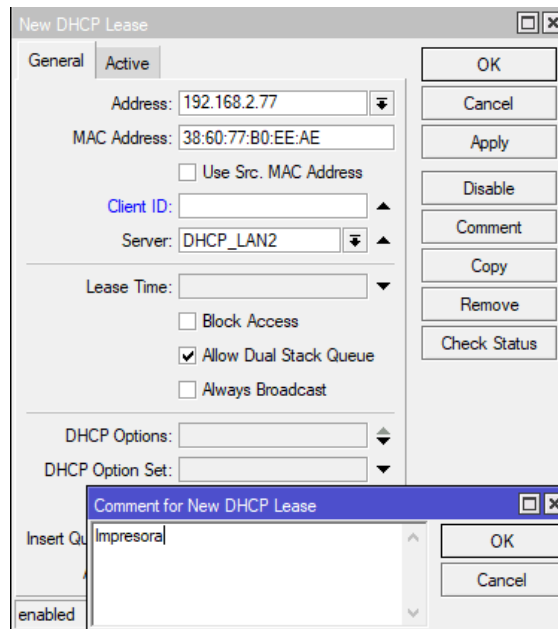


Figura 3.22 Configuración amarre *IP/MAC*

Configuración de *DHCP relay*

DHCP relay tiene la capacidad de recibir una solicitud *DHCP* y reenviar dicha solicitud a un servidor *DHCP* real. Para la configuración es necesario conocer la interfaz, *DHCP server* y *gateway* de la red. Para ello se ingresa los siguientes comandos:

- [admin@R2] > IP DHCP-relay add name=DHCP_LAN1 interface=ether2 DHCP-server=10.0.1.1 local-address=192.168.1.1 disable=no

Para su configuración gráfica selecciona en el menú la opción *IP/DHCP Relay* y se selecciona la opción (+), ver figura 3.23.

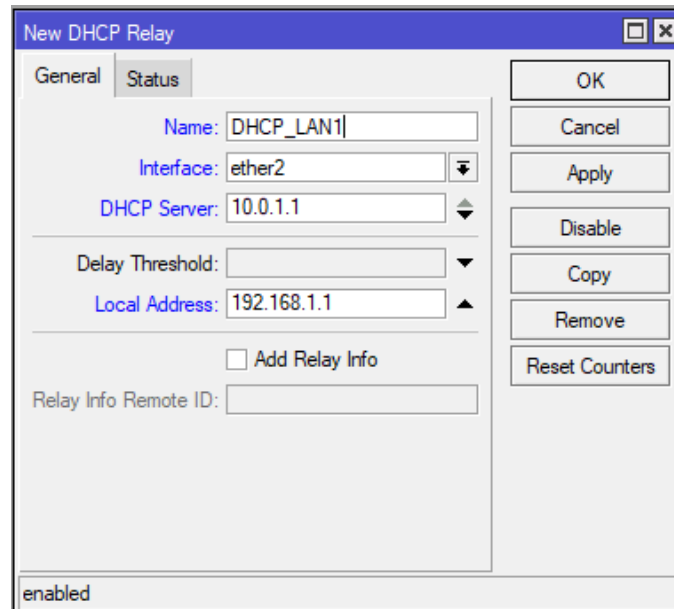


Figura 3.23 Configuración *DHCP relay*

Configuración de *DHCP client*

DHCP client es uno de los servicios que permite que una interfaz pueda solicitar una dirección *IP* de acuerdo a las configuraciones realizadas por el administrador de la red. Se debe definir la interfaz que va a recibir la dirección *IP* y para ello se ingresa los siguientes comandos:

```
- [admin@Router] > IP DHCP-client add interface=ether1  
comment=DHCP_client
```

Para la configuración gráfica de *DHCP client* se selecciona en el menú la opción *IP/DHCP client* y a continuación se selecciona la opción (+), ver figura 3.24.

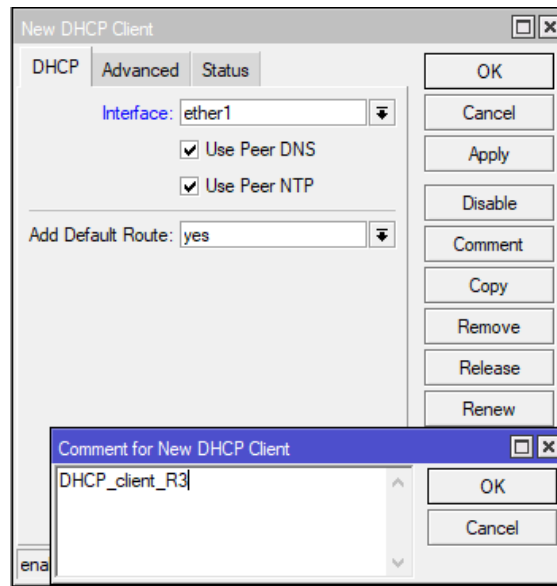


Figura 3.24 Configuración *DHCP client*

Configuración de *DNS server* y *cache*

DNS server es un servicio esencial para la navegación en Internet ya que es parte del directorio primario de Internet. Este servicio provee de una resolución de nombres en internet, la cual permite realizar la traducción de nombres llamados dominios a direcciones IP. Entre las funciones más recomendadas es la utilización del *cache* que crea una tabla de páginas web con sus respectivas dirección *IP*, esto evita un alto consumo en el ancho de banda, por ello es necesario en algún momento realizar una limpieza del *cache*, debido a que hay páginas que con el pasar del tiempo no se vuelven a utilizar. Para ello se emplea el siguiente comando.

Para su configuración se determina la dirección *IP* del servidor DNS al que va apuntar para este servicio y se ingresa los siguientes comandos:

- [admin@Router_LAN] > IP dns set servers=8.8.8.8,8.8.4.4 allow-remote-requests=yes

Para su configuración gráfica se selecciona en el menú la opción *IP/DNS*, ver figura 3.25.

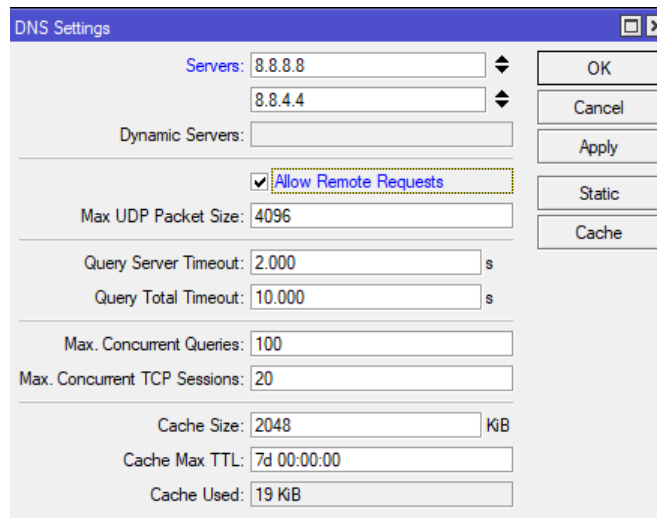


Figura 3.25 Configuración DNS server

Configuración de DNS transparente

DNS transparente permite que el *router* re direccionar el DNS del computador para utilizar el cache generado para evitar la salida del usuario hacia el Internet para obtener la traducción de dirección IP a dominio. Para ello se ingresa los siguientes comandos.

- [admin@Router_LAN] > IP firewall nat add chain=dstnat protocol=tcp dst-port=53 action=redirect to-ports=53
- [admin@Router_LAN] > IP firewall nat add chain=dstnat protocol=udp dst-port=53 action=redirect to-ports=53
-

Para la configuración de direcciones dinámicas por medio de la interfaz gráfica se ingresa al menú *IP DHCP setup*, ver figura 3.26.

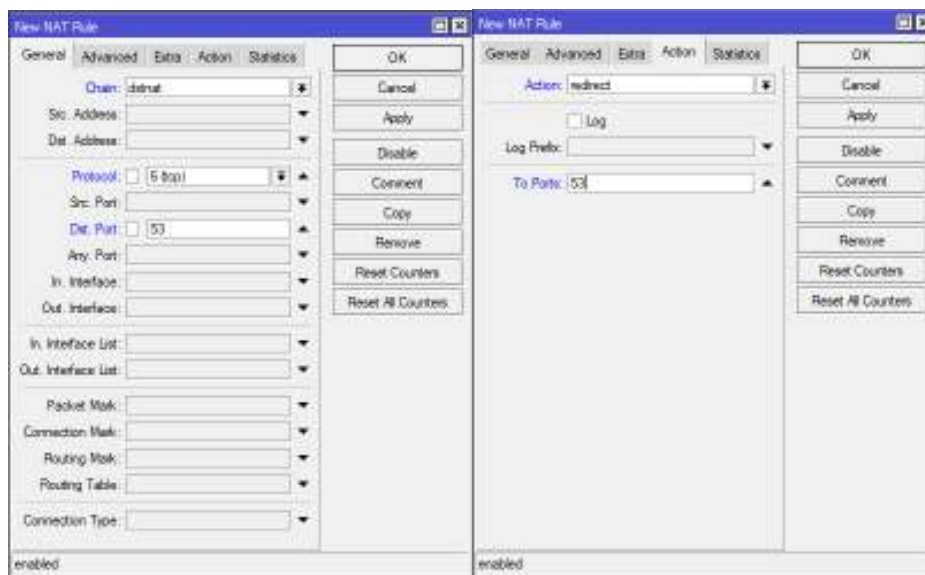


Figura 3.26 Configuración *DNS* transparente

Configuración de acceso a Internet

Para el acceso a Internet es necesario crear una ruta para la salida de paquetes, para ello se crea una ruta por defecto que por lo general es 0.0.0.0/0. Para su configuración se ingresa los siguientes comandos:

- [admin@Router_LAN] > `IP route add distance=1 dst-address=0.0.0.0/0 gateway=192.168.0.1`

Ahora es necesario configurar el enmascaramiento de los paquetes de la red *LAN*.

- [admin@Router_LAN] > `IP firewall nat add action=masquerade chain=srcnat out-interface=ether1`

Para su configuración gráfica selecciona la opción *IP/Routes* y se selecciona la opción (+), ver figura 3.27 y figura 3.28.

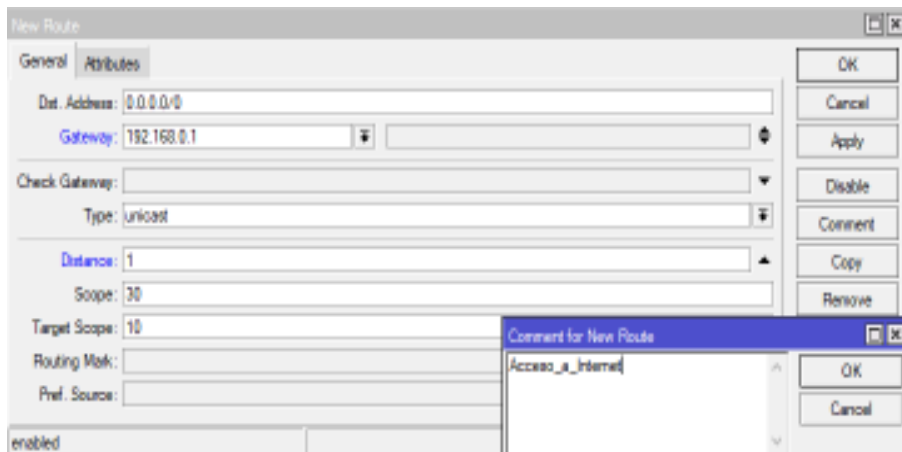


Figura 3.27 Configuración de ruta de salida

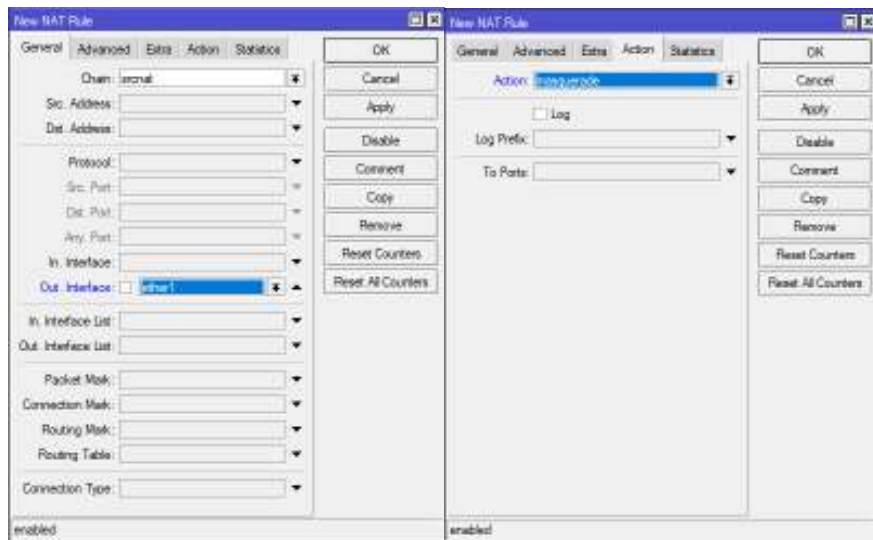


Figura 3.28 Configuración de enmascaramiento

Enrutamiento *BGP*

El protocolo de enrutamiento *BGP* fue creado con el propósito de interconectar redes administradas por distintas entidades es decir permite el enrutamiento entre diferentes sistemas autónomos. Este protocolo funciona sobre *TCP* en el puerto 179, para ello es necesario definir la numeración de los sistemas autónomos y se ingresa los siguientes comandos:

- [admin@R2] > routing *BGP* peer add name=R2-R1 instance=AS200_R1 remote-address=10.10.10.1 remote-as=100 in-filter=AS200

Para su configuración gráfica se ingresa a la opción *Routing/BGP*, ver figura 3.29.

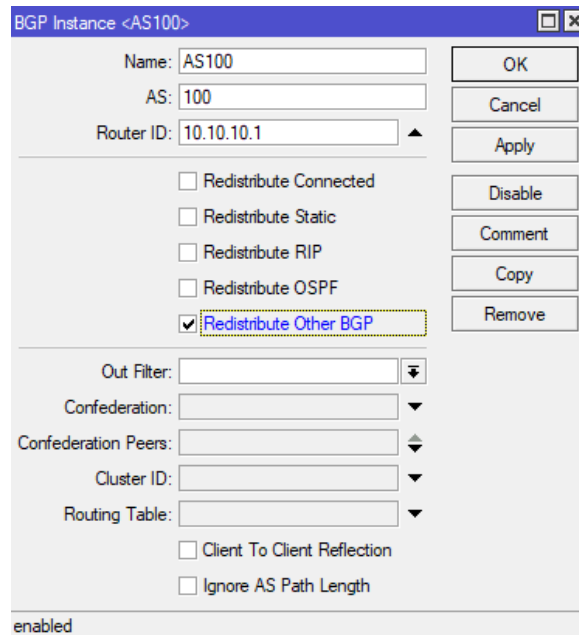


Figura 3.29 Configuración enrutamiento BGP

Configuración de *firewall*

Firewall es una de las herramientas más indispensables al momento de proteger la información de nuestros equipos cuando se conectan a internet. Dentro de una empresa juega un rol muy importante como barrera para la protección de la información, así como tener un control de páginas web a las que acceden los usuarios, debido a que existen páginas que pueden representar un peligro para la red o páginas que demandan un mayor ancho de banda.

Creación de *Address Lists*

La creación de listas de direcciones es necesario para tener un control de acceso o bloqueo a los servicios que presta el *router* a los usuarios. Para ello se ingresa los siguientes comandos:

- [admin@Router] > IP firewall address-list add address=192.168.10.25 list=IP_con_restricciones
- [admin@Router] > IP firewall address-list add address=192.168.10.125 list=IP_sin_restricciones

Para la configuración gráfica de la lista de direcciones se elige la opción *IP/Firewall*, ver figura 3.30.

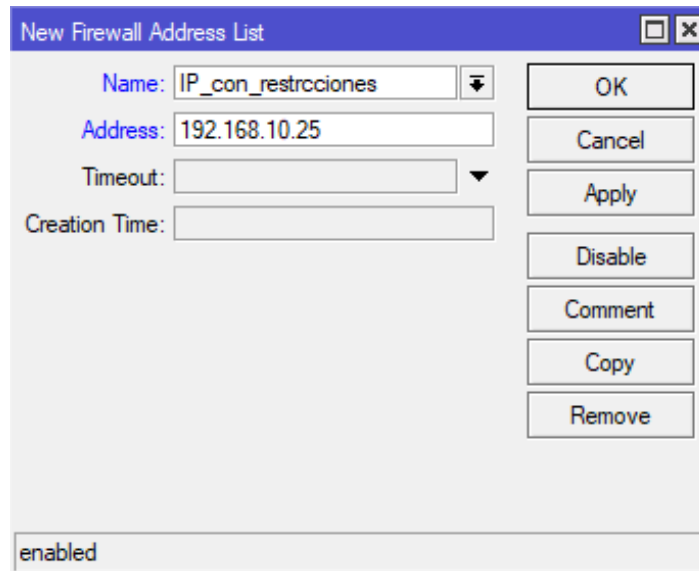


Figura 3.30 Configuración Address lists

Configuración de bloqueo servicios de acceso al *router*

En una red es necesario configurar el bloqueo de puertos como por ejemplo *Ping*, *SSH*, *Telnet* con determinada lista de direcciones *IP* para evitar riesgos en la red. Para ello se ingresa los siguientes comandos:

- [admin@Router] > `IP firewall filter add action=drop chain=input comment=Bloqueo_PING protocol=icmp scr-address-list=IP_con_restricciones`
- [admin@Router] > `IP firewall filter add action=drop chain=input comment=Bloqueo_SSH protocol=tcp dst-port=22 scr-address-list=IP_con_restricciones`
- [admin@Router] > `IP firewall filter add action=drop chain=input comment=Bloqueo_Telnet protocol=tcp dst-port=23 scr-address-list=IP_con_restricciones`

Para el bloque de servicios por interfaz gráfica se ingresa al menú *IP/Firewall*, en la pestaña *Address lists*, ver figura 3.31.



Figura 3.31 Configuración Address lists

Configuración de acceso y restricción a páginas en Internet

Para bloquear páginas web como por ejemplo *Whatsapp, Facebook, Twitter, Instagram* es necesario trabajar en la capa 7 del modelo OSI, donde se ingresará una expresión regular (*regex*), la cual es una secuencia de caracteres que permite definir un patrón de búsqueda. Para ello se ingresan los siguientes comandos:

- [admin@Router_LAN] > IP firewall layer7-protocol add
name=Bloqueo_redes_sociales regex=^(.*(facebook|twitter
|whatsapp|instagram)[.]+.*\$
- [admin@Router_LAN] > IP firewall filter add action=drop
chain=forward layer7-protocol=Bloqueo_redes_sociales
comment=Bloqueo_de_redes_sociales scr-address-
list=IP_con_restricciones
- [admin@Router_LAN] > IP firewall filter add action=accept
chain=forward
comment=Permitir_conexiones_establecidas_relacionadas_internet
connection-state=established,related
- [admin@Router_LAN] > IP firewall filter add action=drop
chain=forward comment=Rechazar_conexiones_invalidas_intenet
connection-state=invalid
- [admin@Router_LAN] > IP firewall filter add action=accept
chain=forward comment=Permitir_navegacion_IPs

Para la configuración de acceso y restricción a páginas en Internet se dirige a la opción *Layer7 Protocols* en el menú *IP/Firewall filter*, ver figura 3.32.

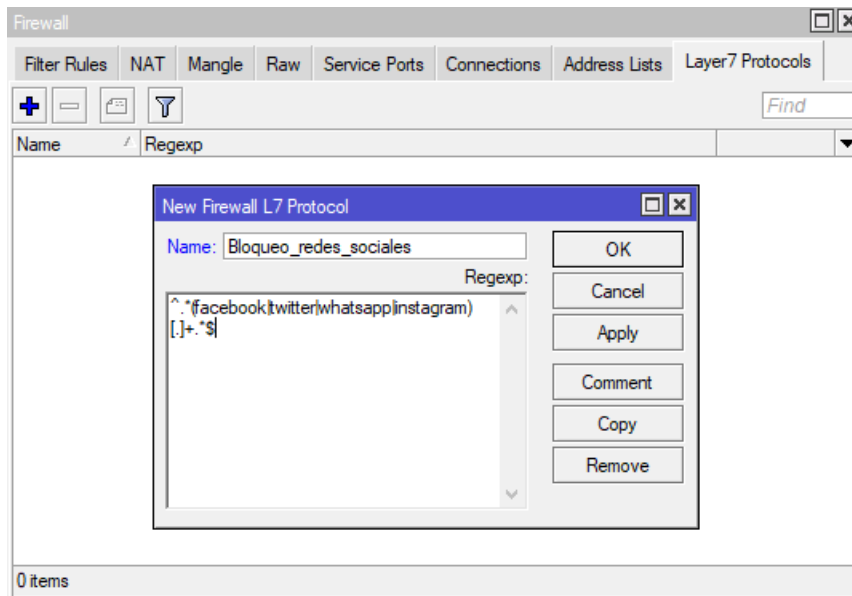


Figura 3.32 Configuración de acceso y restricción a Internet

Configuración de colas simples

Las colas simples se emplean por lo general para la limitación de tráfico de forma simétrica o asimétrica a los usuarios de una red. Las colas simples están basadas en HTB, la cual permite crear una relación entre colas padre-hijo o hijo-hijo y una estructura jerárquica entre colas que se ejecutan en un orden secuencial. Entre las configuraciones de colas simples se tiene la implementación de horarios de programación por horas o días para la desactivación de colas simples.

Configuración de colas padre

Esta configuración es útil para liberar ancho de banda para los usuarios en determinado tiempo. Para ello es necesario determinar la dirección *IP* a delimitar, el ancho de banda a asignar y ejecutar la siguiente línea de comandos:

```
- [admin@Router] > queue simple add name=Padre_LAN
target=192.168.10.0/24 max-limit=1M/1M
```

Mientras para su configuración por medio de interfaz gráfica se ingresa al menú *Simple Queues* y en la opción (+), ver figura 3.33.

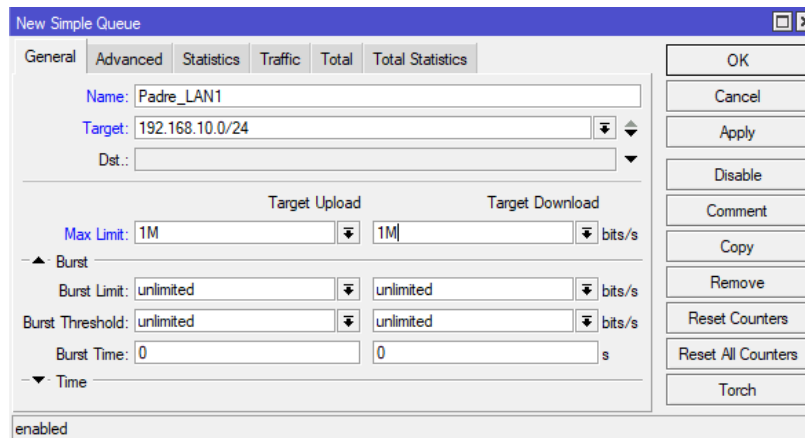


Figura 3.33 Configuración de colas padre

Configuración de colas hijos

Las colas hijos son aquellas que van a consumir el tráfico que las colas padres ofrecen, es por ello que las colas hijos logran satisfacer el primer *limit-at* y luego las colas padres reparten el tráfico restante. Para su configuración se define la dirección *IP*, el ancho de banda y se ingresa los siguientes comandos:

- [admin@Router] > queue simple add name=Host1 target=192.168.10.254 max-limit=1M/1M limit-at=512k/512k parent=Padre_LAN

Mediante interfaz gráfica se ingresa al menú *Queue simple*, ver figura 3.34.

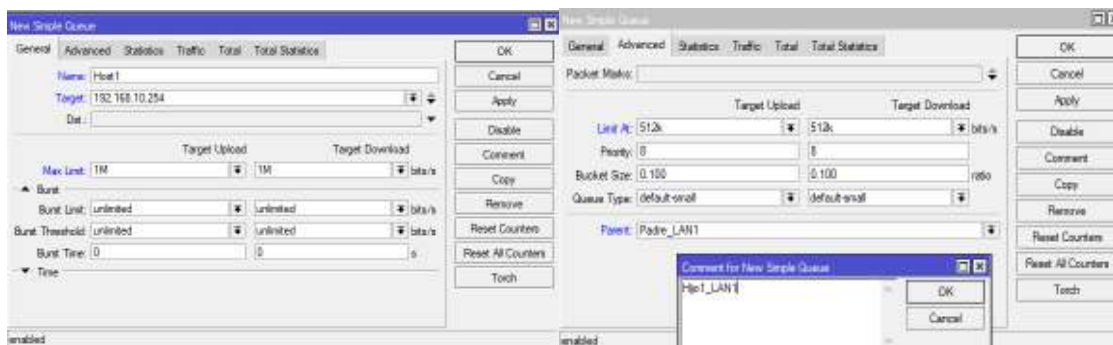


Figura 3.34 Configuración de colas hijos

Configuración de ráfagas de velocidad

Las ráfagas o *burst* de *MikroTik* permiten brindar un mayor ancho de banda al establecido durante un tiempo determinado. Esto permite que el usuario final tenga un mejor desempeño en la red al inicio. Para ello se debe ingresar los siguientes comandos:

- [admin@Router] > queue simple add name=Host target=192.168.20.254 max-limit=1M/1M burst-limit=2M/2M burst-threshold=512k/512k burst-time=16/16

Para su configuración gráfica se elige en el menú *Queue simple* y la opción (+), ver figura 3.35.

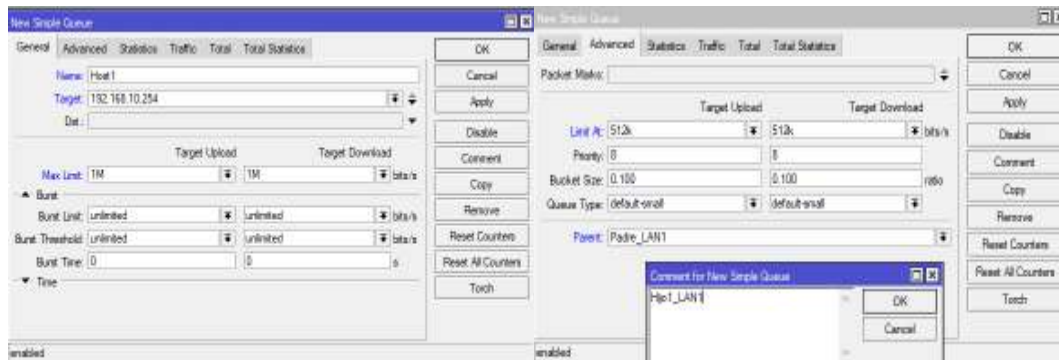


Figura 3.35 Configuración de ráfagas de velocidad

Configuración de VLANs

VLANs es un método que permite crear redes y subredes que físicamente se encuentran dentro de una misma red pero que lógicamente son independientes, de esta forma el administrador de una topología podrá disponer de varias redes dentro de un mismo *switch* y dentro de una misma interfaz de *router*. Entre sus aplicaciones se puede encontrar en empresas donde se necesita independizar las redes de conectividad de cada departamento y área que lo conforman.

Configuración de *bridge*

Para ello se crea un *bridge* en la que se agrupa interfaces de forma lógica y se ingresa los siguientes comandos:

- [admin@Router] > interface bridge add name=Bridge_VLAN
- [admin@Router] > interface bridge port add interface=ether2 bridge=Bridge_VLAN
- admin@Router] > interface bridge port add interface=ether3 bridge=Bridge_VLAN

Mediante interfaz gráfica se configura seleccionando *Bridge* y la opción (+), ver figura 3.36.

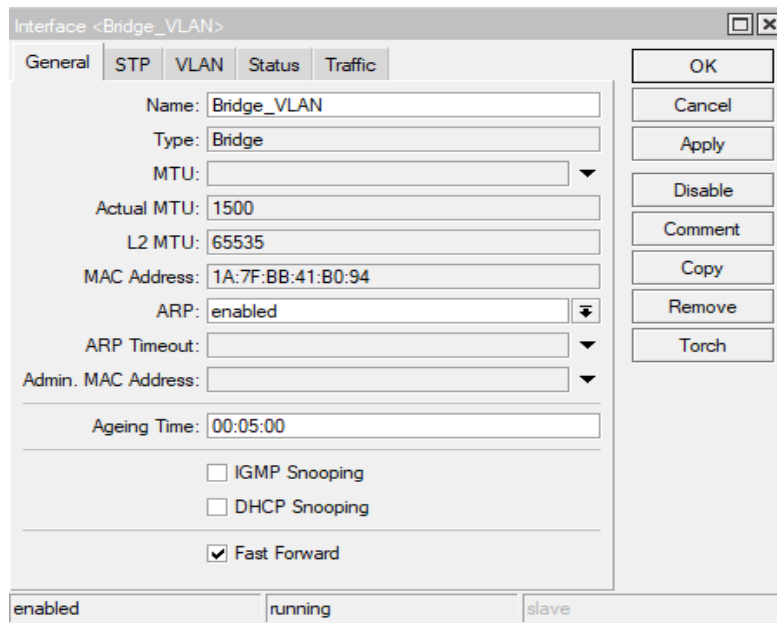


Figura 3.36 Configuración de *bridge*

Creación y levantamiento de interfaces *VLANs* en *router*

Para la creación y configuración de interfaces *VLANs* se ingresa los siguientes comandos:

- [admin@Router] > interface vLAN add name=VLAN10 vLAN-id=10
interface=Bridge_VLAN
- [admin@Router] > interface vLAN add name=VLAN10 vLAN-id=10
interface=Bridge_VLAN

Para su creación de *VLANs* se ingresa a la opción *Interface*, mientras para el levantamiento de las interfaces de forma gráfica se selecciona la opción *Address lists*, ver figura 3.37.

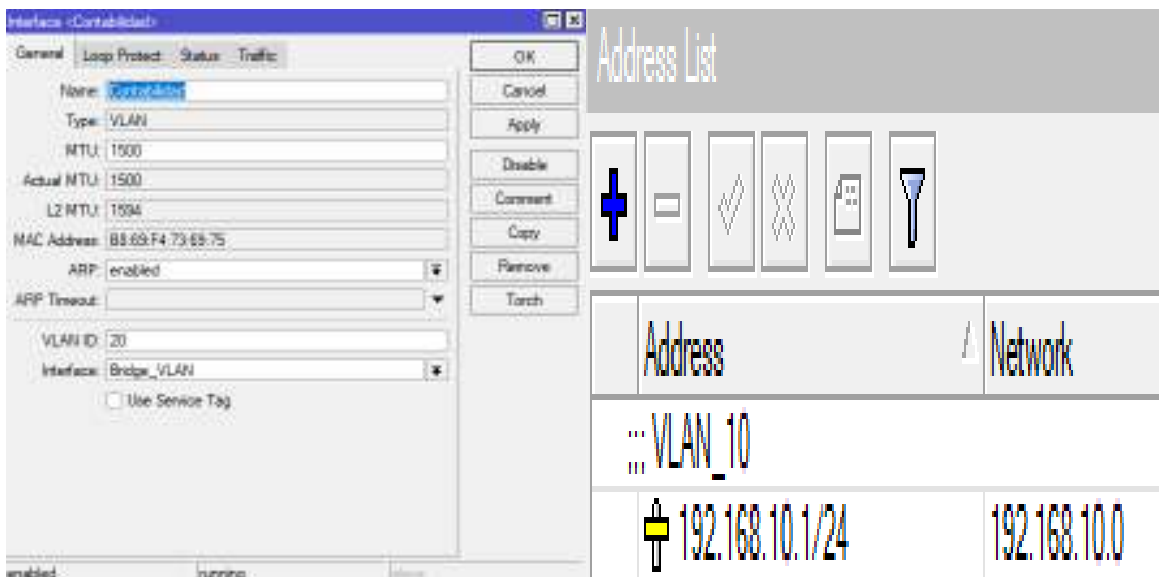


Figura 3.37 Creación y levantamiento de interfaces VLANs en router

Creación de VLANs en switch

Para ingresar a un switch se utiliza un navegador de acuerdo a la forma de configuración web. Para el ingreso a un switch por vez primera es necesario realizar un cambio de dirección IP del computador para que este dentro de la red que viene por default 192.168.88.0/24. Una vez ingresado al menú VLAN donde se coloca el nombre de cada red virtual asociada a los diferentes puertos, ver figura 3.38.

User List				
Users	Groups	SSH Keys	SSH Private Keys	Active Users
+	-			
Name	Policys	Skin		
full	local telnet ssh ftp reboot read write policy test winbox passw...	default		
read	local telnet ssh reboot read test winbox password web sniff s...	default		
reinicio	local telnet reboot read	default		
write	local telnet ssh reboot read write test winbox password web ...	default		

Figura 3.39 Lista de políticas de grupo

Enrutamiento estático

Para comprobar el correcto funcionamiento del enrutamiento estático se revisa la lista de rutas estáticas configuradas en el *router* para determinar si el equipo cuenta con los encaminamientos para llegar a las diferentes redes WAN y LAN no conectadas directamente como se observa en la parte izquierda de la figura 3.40. En la figura 3.40 lado derecho se emplea *CMD* y el comando *ping* para verificar la conectividad entre redes, en este caso se realiza una prueba entre la red *LAN 2* y *LAN 4*, ver figura 3.40.

The screenshot displays two windows. On the left, the 'Route List' window shows a table of static routes:

	Det. Address	Gateway
DAC	10.0.0.0/26	ether1 reachable
DC	10.0.0.192/26	ether2 unreachable
DAC	172.16.0.0/18	ether3 reachable
::: Gateway1_LAN3		
AS	172.16.128.0/18	10.0.0.62 reachable ether1
::: Gateway2_LAN3		
S	172.16.128.0/18	10.0.0.193 unreachable

On the right, a command prompt window shows the configuration of two Ethernet adapters and the execution of a ping command:

```

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión...:
  Dirección IPv4...: 172.16.63.254
  Máscara de subred...: 255.255.192.0
  Puerta de enlace predeterminada...: 172.16.8.1

Adaptador de Ethernet vEthernet (Default Switch):
  Sufijo DNS específico para la conexión...:
  Vínculo: dirección IPv6 local...: fe80::74ab:8162:334a:aed7%28
  Dirección IPv4...: 172.17.14.17
  Máscara de subred...: 255.255.255.248
  Puerta de enlace predeterminada...:

C:\Users\FARSUC>ping 172.16.128.1

Haciendo ping a 172.16.128.1 con 32 bytes de datos:
Respuesta desde 172.16.128.1: bytes=32 tiempo=10ms TTL=64
Respuesta desde 172.16.128.1: bytes=32 tiempo=10ms TTL=64
Respuesta desde 172.16.128.1: bytes=32 tiempo=10ms TTL=64
Respuesta desde 172.16.128.1: bytes=32 tiempo=10ms TTL=64

Estadísticas de ping para 172.16.128.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 8ms, Máximo = 8ms, Media = 8ms
  
```

Figura 3.40 Conectividad entre equipos

DHCP server

Para comprobar el correcto funcionamiento de un servidor DHCP se conecta al *router* hosts configurados previamente como DHCP *client* para solicitar una dirección *IP* de forma automática. Una vez conectados los equipos se procede a verificar por medio de la opción

DHCP server de WinBox las direcciones IP dadas para arrendamiento a los hosts. En la imagen se observa la tabla con la dirección IP, dirección MAC correspondiente a cada equipo. La letra D al lado izquierdo de la imagen indica que el arrendamiento IP es dinámico, ver figura 3.41.

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address
D	192.168.2.253	38:60:77:B0:EE:AE	1:38:60:77:b0:ee:....	dhcp1	192.168.2.253	38:60:77:B0:EE:AE
D	192.168.2.254	B8:69:F4:73:6B:8B	1:b8:69f4:73:6b:8b	dhcp1	192.168.2.254	B8:69:F4:73:6B:8B

Figura 3.41 Configuración de DHCP en bridge

DNS cache

Para la comprobación del servicio DNS cache como se observa en la figura 3.42 parte izquierda es necesario utilizar un navegador e ingresar alguna página. De esta manera empieza a generar tráfico que se va registrando en la memoria cache del router. Por medio de la opción DNS cache de WinBox como se observa en la parte derecha de la figura 3.42 se verifica todos los datos de navegación que pasan por el router, figura 3.42.

#	NAME	TYPE	DATA	TTL
0	dev...	CNAME	device.south.xboxlive.com.akadns.net	36m18s
1	tit...	CNAME	title.auth.xboxlive.com.akadns.net	32m58s
2	cli...	CNAME	wns.notify.windows.com.akadns.net	17m38s
3	arc...	CNAME	arc.man.com.nsatc.net	17m22s
4	ria...	CNAME	ria-prod.trafficmanager.net	18m54s
5	cti...	CNAME	au-ig-stim.trafficmanager.net	17m4s
6	su...	CNAME	su.download.windowsupdate.nesco.net	17m6s
7	cri...	CNAME	ms9.wa.phicdn.net	36m20s
8	cs9...	A	192.168.8.8	17m18s
9	ww...	CNAME	a-0001.a-afentry.net.trafficmanager.net	17m27s
10	sel...	CNAME	global.asimov.events.data.trafficmanag...	17m39s
11	a-0...	CNAME	aca-office.a-0005.a-msedge.net	19m36s
12	ea...	CNAME	a-0006.a-msedge.net	8s
13	ev...	CNAME	evobs-windowservices-tas-msedge-net.e...	20m18s
14	ev...	CNAME	e-0006.e-msedge.net	12s
15	a-0...	A	13.107.9.88	52s
16	upd...	A	172.217.30.195	1m19s
17	log...	CNAME	login.ms.msidentity.com	1m12s
18	log...	CNAME	www.tm.lg.prod.asdmsa.akadns.net	1m4s
19	che...	CNAME	wd-prod-us.trafficmanager.net	19m18s

Figura 3.42 Tabla DNS cache

Enrutamiento BGP

Para la comprobación del enrutamiento BGP se aplicó filtros que permite la no publicación y el no aprendizaje de redes privadas en este protocolo, esto implica que, si en una red existen subredes, están no sean reflejadas en las tablas de enrutamiento. Por medio de la opción *Router Filters* de WinBox se procede a verifica los resultados de estas reglas y como se observa en la figura de las tablas de enrutamiento que las redes de aprendizaje solo corresponden a sistemas autónomos, ver figura 3.43.

#	Chain	Prefix	Prefix Length	Protocol	BGP AS Path	Action
0	AS200	192.168.0.0/16	16-32			discard

Figura 3.43 Filtro de direcciones privadas en BGP

Firewall

Para realizar el bloque a ciertas páginas web se emplea la regla de *Drop* que niega el acceso como se observa en la figura 3.44 lado izquierdo. Por medio de esta regla el usuario está limitada su navegación. Para la comprobación de las seguridades configuradas en *Firewall* se empleó un navegador web para intentar ingresar a una de las paginas bloqueadas en el *Firewall* a nivel de capa 7 como es *Netflix*. Al lado derecho de la figura 3.44 se observa el intento negado al navegador para acceder a esta página, así como sus subdominios que contenga este sitio, ver figura 3.44.

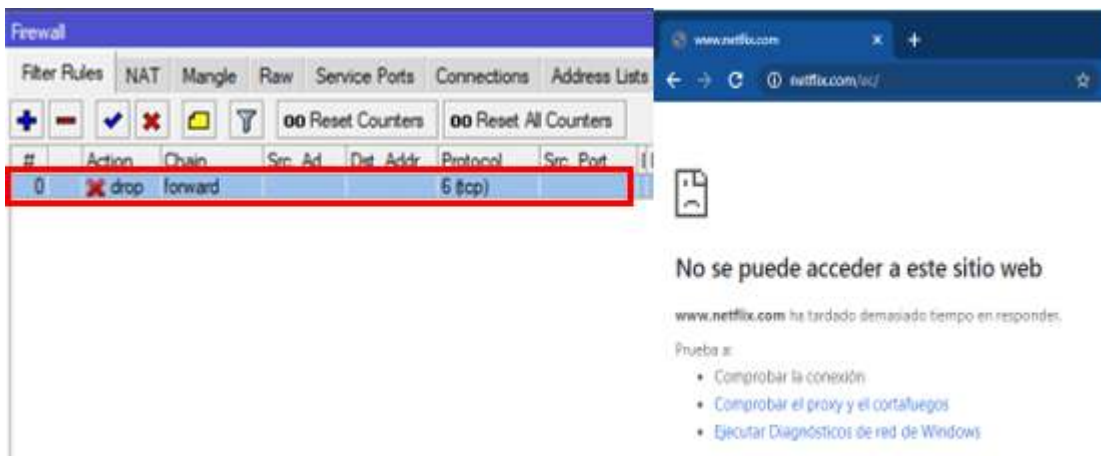


Figura 3.44 Bloqueo de página *Netflix*

Colas simples

Para verificar la restricción del ancho de banda por horarios se ingresó a la opción *Queue List* de *WinBox* y se observa la cola simple creada, la cual cuenta con un horario y dirección *IP* de restricción. Para realizar la comprobación de las colas se observa que la regla se encuentra desactivada al colocarse de color rojo, esto es debido a que la regla no está en uso porque esta fuera del horario en el que fue configurado, caso contrario la regla debería esta de color negro, ver figura 3.45.

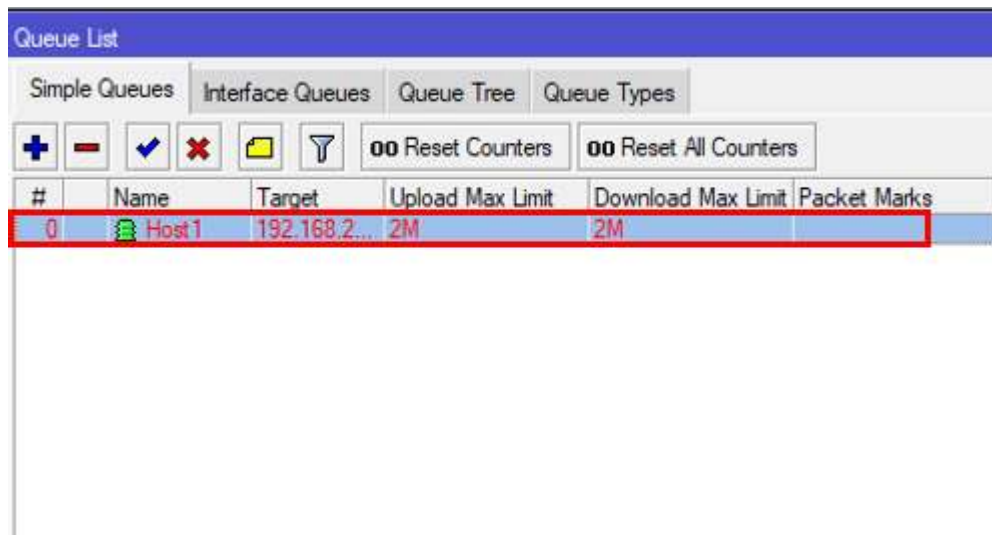


Figura 3.45 Desactivación de colas simples por horario

VLANs

Para la verificación de VLANs se procedió a emplear el *CMD* de *Windows* y por medio del comando *ping* se comprueba la conectividad entre las de diferente subred, se puede observar en la figura como se recibe una contestación entre subredes, ver figura 3.46.

```

Configuración IP de Windows

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Dirección IPv4. . . . . : 192.168.20.253
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 192.168.20.1

Adaptador de Ethernet vEthernet (Default Switch):
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::d4b0:a95c:94e2:cecc%20
  Dirección IPv4. . . . . : 172.17.14.17
  Máscara de subred . . . . . : 255.255.255.240
  Puerta de enlace predeterminada . . . . . :

C:\Users\FARSUC>ping 192.168.40.253

Haciendo ping a 192.168.40.253 con 32 bytes de datos:
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 192.168.40.253:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:

```

Figura 3.46 Conectividad entre VLANs

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- *MikroTik* cuenta con una interfaz gráfica llamada *WinBox*, la cual es muy amigable con el usuario para la configuración y administración de los equipos. Dentro de esta interfaz tiene un apartado para realizar configuración vía comandos llamado *Terminal*.
- *MikroTik* ofrece varias herramientas para la administración de *routers* así como permisos de acceso a las configuraciones e información sensible de los equipos como son los *backups*. Estas herramientas de administración están ligadas a las políticas de grupo que maneja los equipos.
- En el enrutamiento estático para alcanzar otras redes se configura en las tablas de enrutamiento las redes que no se encuentran conectadas directamente, se elige un sentido sea este horario o antihorario para el tráfico, esto evita que se generen lazos entre interfaces.
- El servicio de *DNS* forma parte importante en la administración de una red debido a que este servicio permite registrar información de navegación de la red, asociando direccionamiento *IP* con nombres de dominio. Con este servicio se evita el uso innecesario de ancho de banda dentro de una red porque las consultas de navegación se direccionan al *router*.
- *MikroTik* cuenta con una guía de configuración rápida para la creación de servidores *DHCP* en interfaces (*DHCP Server Setup*). Esta opción predetermina los posibles valores para pool de direcciones en arrendamiento, puerta de enlace, *DNS* y el tiempo de arrendamiento de las direcciones *IP*.
- *BGP* es uno de los protocolos de enrutamiento que se maneja a nivel de sistemas autónomos, los cuales son administrados por un mismo operador y están compuestos de varias subredes, que permite el intercambio de tablas de rutas a nivel de sistemas autónomos, esto implica que no se refleje rutas de subredes.
- Las ráfagas de velocidad en colas simples permiten tener un ancho de banda adicional al configurarlo para satisfacer la demanda de ancho de banda que normalmente se requiere cuando un usuario está empezando una nueva conexión web.
- Una herramienta importante que permite el *firewall* de *MikroTik* es crear un *Address List* con el uso de un *Firewall filter* con el cual se puede crear una lista de direcciones

IP y poner una regla para cada una de ellas y así tener más seguridad en la red con el cual se usa el comando *IP firewall filter* que permite bloquear ciertas páginas y asignar un horario para ingresar en ellas, así como bloquear unos usuarios.

- *MikroTik* cuenta con un sistema operativo para la configuración de *switch* llamado *SwOS*, el cual se accede desde un navegador web y ofrece todas las funcionalidades para administrar estos equipos.

4.2 Recomendaciones

- *MikroTik* cuenta con herramientas de monitoreo y configuración para los equipos, por lo que se debe tener en cuenta estas herramientas al momento de dar permisos o credenciales a los usuarios para ingresar a los equipos.
- En la configuración de servicios *DNS* para conseguir una respuesta rápida con una menor utilización de ancho de banda es recomendable emplear el cache *DNS* que usa la memoria interna del equipo para almacenar las páginas web con su respectiva dirección *IP*.
- En las configuraciones de Firewall es recomendable la no desactivación del *Connection Tracking*, debido que permite hacer un seguimiento de las conexiones *UDP* y al desactivarse se deshabilitan servicios como *NAT* y *Firewall*.
- Se recomienda mantener actualizado el *Firmware* del *router* para eliminar vulnerabilidades, resolver fallos que posea el equipo y a la vez recibir nuevas funciones y características que el fabricante haya desarrollado en nuevas versiones siempre previa realización de una copia de seguridad en evitar pérdida de configuraciones.
- Para realizar configuraciones de forma no presencial, de forma remota o si el administrador no está seguro de su implementación, es recomendable emplear el modo seguro (*Safe Mode*), este modo permite que todos los cambios realizados en modo seguro sean eliminados de forma automática si la sesión finaliza de manera anormal o si se desea deshacer las configuraciones.
- Se recomienda verificar el tráfico de la red y en caso de que exista lentitud provocada por el congestionamiento, revisar que usuario es para desconectarlo de la red y bloquearlo mediante la *MAC Address* en caso de que no exista a la empresa y si pertenece a esta darle ciertos privilegios.
- Se recomienda en el caso de que ha olvidado la contraseña de su equipo *MikroTik* reinstale el sistema operativo *RouterOs* con la herramienta *Netinstall* o regresarlo a su configuración de fábrica.

5 Bibliografía

- [1] SN, «*MikroTik*,» *MikroTik*, [En línea]. Available: <https://MikroTik.com/aboutus>. [Último acceso: 10 Febrero 2020].
- [2] SN, «*RouterOS*,» Pondi, [En línea]. Available: <https://www.MikroTik-routeros.net/routeros.aspx>. [Último acceso: 10 Febrero 2020].
- [3] SN, «*SwOS*,» *MikroTik*, 12 Junio 2019. [En línea]. Available: <https://wiki.MikroTik.com/wiki/SwOS>. [Último acceso: 10 Febrero 2020].
- [4] F. Pugliese. [En línea]. Available: https://eva.udelar.edu.uy/pluginfile.php/422873/mod_resource/content/1/Introducc%C3%B3n%20a%20MikroTik.pdf. [Último acceso: 10 Febrero 2020].
- [5] M. Rivas, «Línea de comandos: Qué es y para qué se utiliza,» NeoGuías, 27 Mayo 2019. [En línea]. Available: <https://www.neoguias.com/interprete-de-una-linea-de-comando/>. [Último acceso: 10 Febrero 2020].
- [6] M. Rouse, «GUI (interfaz gráfica de usuario),» SearchDataCenter, 14 Marzo 2017. [En línea]. Available: <https://searchdatacenter.techtarget.com/es/definicion/GUI-interfaz-gráfica-de-usuario>. [Último acceso: 10 Febrero 2020].
- [7] T. Cabanas, «Qué es y para qué sirve la dirección MAC,» MC, 04 Marzo 2019. [En línea]. Available: <https://www.muycomputer.com/2019/03/04/direccion-mac/>. [Último acceso: 10 Febrero 2020].
- [8] M. Wilke, «Direcciones *IP*: para qué sirven y cómo funcionan,» HostGator, 16 Septiembre 2019. [En línea]. Available: <https://www.hostgator.mx/blog/que-es-una-direccion-IP/>. [Último acceso: 10 Febrero 2020].
- [9] C. Villagomez, «El protocolo ARP,» CCM, 20 Octubre 2017. [En línea]. Available: <https://es.ccm.net/contents/260-el-protocolo-arp>. [Último acceso: 10 Febrero 2020].

- [10] V. González, «Traducción de direcciones de red (NAT),» 12 Septiembre 2016. [En línea]. Available: <https://w3.ual.es/~vruiz/Docencia/Apuntes/Networking/Protocols/Level-3/03-NAT/index.html>. [Último acceso: 10 Febrero 2020].
- [11] SN, «RUTEO DINÁMICO,» MIKRO WAYS, 05 Septiembre 2010. [En línea]. Available: <https://www.mikroways.net/2010/09/05/ruteo-estatico-frente-a-ruteo-dinamico/>. [Último acceso: 10 Febrero 2020].
- [12] M. Rouse, «Enrutamiento adaptativo (enrutamiento dinámico),» SearchDataCenter, Abril 2017. [En línea]. Available: <https://searchdatacenter.techtarget.com/es/definicion/Enrutamiento-adaptativo-enrutamiento-dinamico>. [Último acceso: 10 Febrero 2020].
- [13] A. Riveiro, «¿Qué es el protocolo *BGP?*,» EL PAÍS, 27 Agosto 2008. [En línea]. Available: https://elpais.com/tecnologia/2008/08/27/actualidad/1219825686_850215.html. [Último acceso: 10 Febrero 2020].
- [14] J. Carles, «Que es y para que sirve un firewall,» geekLAND, 06 Julio 2013. [En línea]. Available: <https://geekLAND.eu/que-es-y-para-que-sirve-un-firewall/>. [Último acceso: 10 Febrero 2020].
- [15] C. Villagómez, «El protocolo *DHCP*,» CCM, 08 Marzo 2017. [En línea]. Available: <https://es.ccm.net/contents/261-el-protocolo-DHCP>. [Último acceso: 10 Febrero 2020].
- [16] M. Luis, «Qué es un servidor DNS y cómo solucionar problemas habituales,» webempresa, 22 Febrero 2019. [En línea]. Available: <https://www.webempresa.com/blog/servidor-dns-como-solucionar-problemas-habituales.html>. [Último acceso: 10 Febrero 2020].
- [17] C. Villagómez, «*VLAN* - Redes virtuales,» CCM, 13 Septiembre 2017. [En línea]. Available: <https://es.ccm.net/contents/286-vLAN-redes-virtuales>. [Último acceso: 10 Febrero 2020].

- [18] E. Merino, «*MikroTik* QoS pLAN: queue trees + simple queues + PCQ,» Medium, 22 Abril 2017. [En línea]. Available: <https://medium.com/@emerino/MikroTik-qos-pLAN-queue-trees-simple-queues-pcq-2dbc831b39e>. [Último acceso: 10 Febrero 2020].
- [19] J. Valle, «¿Qué es Putty?,» Proyecto-TIC, [En línea]. Available: <https://www.proyecto-tic.es/que-es-putty/>. [Último acceso: 10 Febrero 2020].
- [20] V. Carlos, «Protocolo Telnet,» CCM, 29 Septiembre 2017. [En línea]. Available: <https://es.ccm.net/contents/283-protocolo-telnet>. [Último acceso: 10 Febrero 2020].
- [21] R. Cabrera, «¿QUÉ ES SSH Y CÓMO FUNCIONA?,» desafiohosting, 06 Marzo 2020. [En línea]. Available: <https://desafiohosting.com/que-es-ssh/>. [Último acceso: 10 Marzo 2020].
- [22] J. Ranchal, «Guía *CMD*: los mejores trucos y comandos para manejar la consola de *Windows*,» MCPRO, 24 Abril 2018. [En línea]. Available: <https://www.muycomputerpro.com/2018/04/24/consola-de-Windows>. [Último acceso: 10 Marzo 2020].

ANEXOS

ANEXO A: Hojas guías de prácticas para profesores

❖ Práctica N°1

Tema: Acceso de usuarios a *router*

Objetivo general: Creación y configuración de usuarios con acceso a *router MikroTik*

Objetivos específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*.
- Configurar políticas de administración para los grupos de usuarios.
- Crear los usuarios con sus respectivas contraseñas.
- Asignar a los usuarios a los grupos de acuerdo con la lista de usuarios.
- Configurar las interfaces y direcciones *IP* en *routers* y *hosts*.
- Probar las políticas de administración de cada usuario.

Implementación de topología

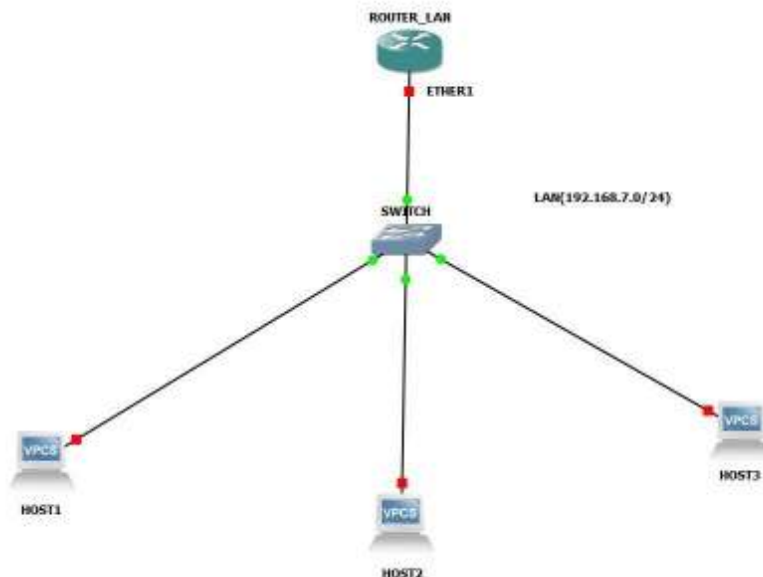


Figura 3.47 Topología de acceso de usuarios al *router*

Asignación de direcciones *IP* para cada equipo, interfaz y *host*

A continuación, se muestra en la tabla 3.4 se indica las direcciones *IP*, *máscara*, *Gateway* para cada equipo y *host*.

Tabla 3.4 Direccionamiento *IP* para equipos

Equipo	Usuario	Dirección <i>IP</i>	Mascara	Gateway	Interfaz
<i>Router</i>	-----	192.168.7.1	/24	-----	ether2
<i>Host1</i>	Jefe_de_infraestructura	192.168.7.254	/24	192.168.7.1	ether switch
<i>Host2</i>	Soporte_tecnico	192.168.7.253	/24	192.168.7.1	ether switch
<i>Host3</i>	Consultor_externo	192.168.7.252	/24	192.168.7.1	ether switch

Lista de usuarios

A continuación, se muestra en la tabla 3.5 la lista de usuarios a ser creados para el ingreso al *router*, siendo de gran importancia para mantener una red segura, para ello es necesario la configuración de usuarios con distintas prioridades.

Tabla 3.5 Usuarios de acceso

Usuario	Password	Grupo	Políticas	<i>IP</i> permitida
Jefe_de_infraestructura	Ji123456	Full	local/telnet/ssh/ftp/reboot/read/ write/policy/test/ <i>WinBox</i> /password/ web/sniff/sensitive/api/romon/ dude/tikapp	
Soporte_tecnico	St123456	Write	local/telnet/ssh/read/write/test/ <i>WinBox</i> / /web/sniff/tikapp	
Consultor_externo	Ce123456	Read	local/telnet/ssh/read/test/ <i>WinBox</i> / web/tikapp	192.168.7.252

Configuración vía interfaz gráfica

Acceso al router

Para ingresar por primera vez al *router* sea mediante *WinBox* o *Webfig*, este cuenta con un usuario por defecto llamado *admin*, pero este usuario no tiene contraseña. Para ello se inicia el software *WinBox* y su acceso puede ser por dirección *MAC* (capa 2) o por dirección *IP* (capa 3) 192.168.88.1, ver figura 3.48.

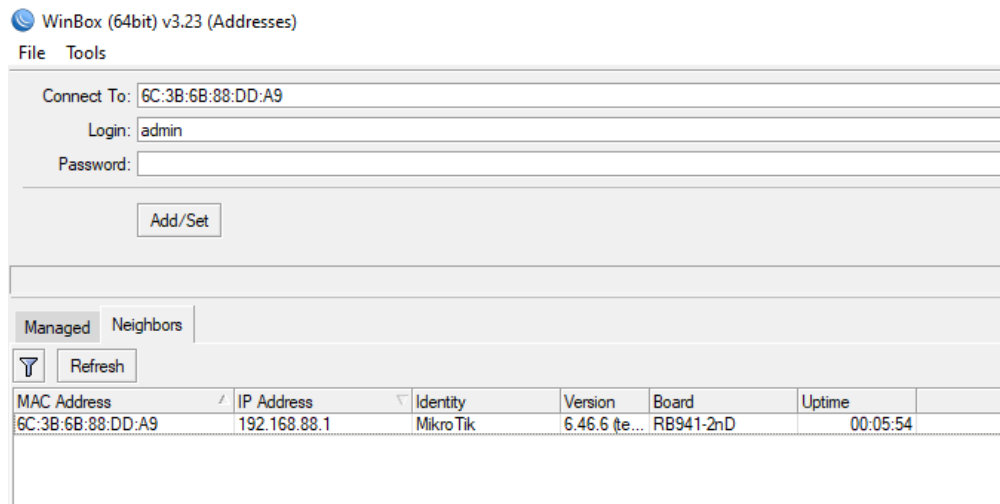


Figura 3.48 Acceso al router

Cambio de nombre a router

Para la configuración del equipo se ingresa en el menú a *System/Identity*, ver figura 3.49.

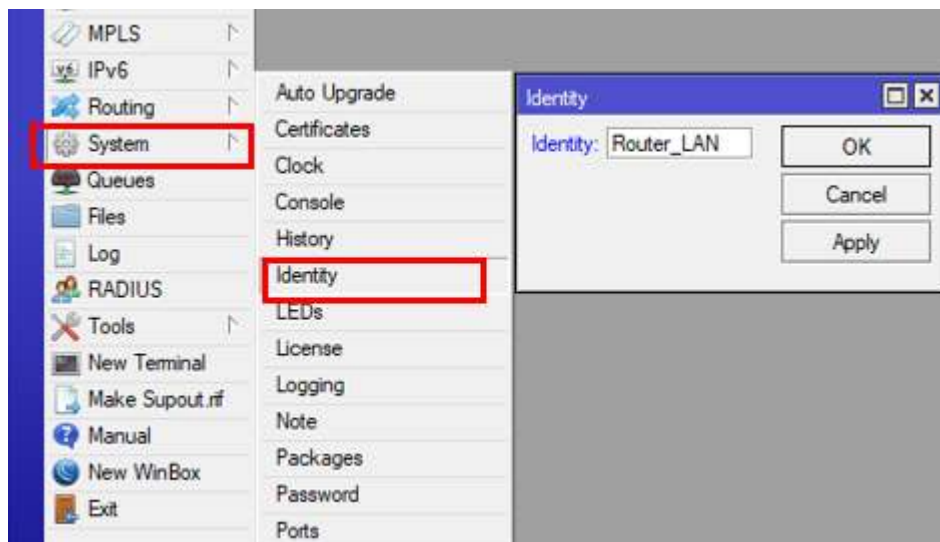


Figura 3.49 Identificación de router

Configuración de políticas de grupo

Para la configuración de las políticas de grupos se selecciona la opción *System, Users*. A continuación, se elige la opción *Groups*, por defecto están creados los grupos *full*, *read* y *write* con sus respectivas políticas. Por temas de seguridad en la red es necesario reconfigurar las políticas de grupo de *full*, *read* y *write* de acuerdo con la lista de usuarios, ver figura 3.50.

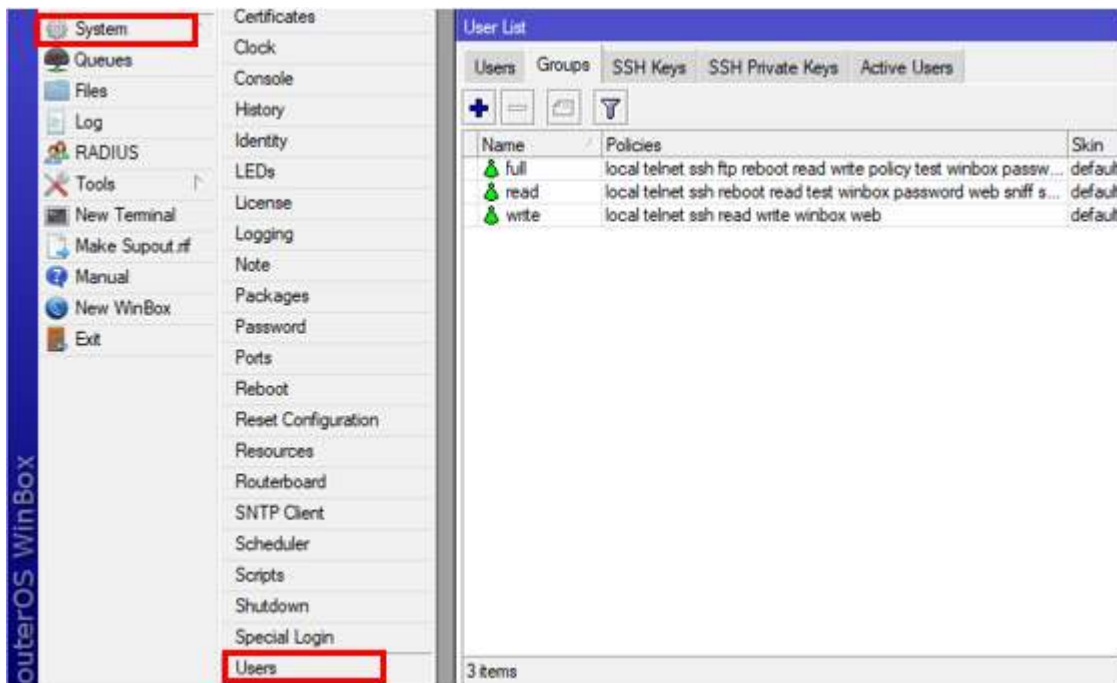


Figura 3.50 Grupos por defecto en MikroTik

Para la configuración del grupo *read*, se selecciona las siguientes políticas: *local*, *telnet*, *ssh*, *read*, *test*, *WinBox*, *web*, *tikapp*. A continuación, se coloca *Apply* y *OK*, ver figura 3.51. Esta política de grupo es creada para no permitir la creación, modificación o eliminación interfaces, direcciones *IP*, contraseñas de usuarios, políticas de grupos, *backups*. No permite el reinicio (*reboot*) ni el *reset* del equipo (*reset configuration*). Permite el ingreso por *telnet*, *ssh*, *WinBox*, *web*, *tikapp*, la visualización de interfaces y direcciones *IP*.

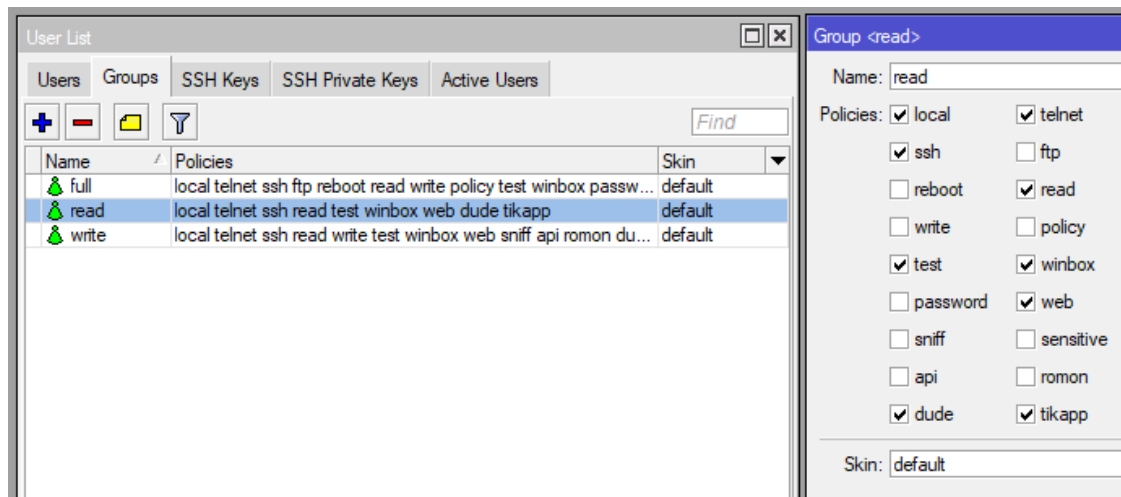


Figura 3.51 Configuración del grupo *read*

Para la configuración del grupo *write*, se selecciona las siguientes políticas: *local*, *telnet*, *ssh*, *read*, *write*, *test*, *WinBox*, *web*, *sniff*, *tikapp*. A continuación, se coloca *Apply* y *OK*, ver figura 3.52. Esta política de grupo es creada para no permitir la creación, modificación o eliminación de contraseñas de usuarios, políticas de grupos, *backups*. No permite el reinicio (*reboot*) ni el *reset* del equipo (*reset configuration*). Permite el ingreso por *telnet*, *ssh*, *WinBox*, *web*, *tikapp*, la creación, modificación, eliminación de interfaces y direcciones *IP*.

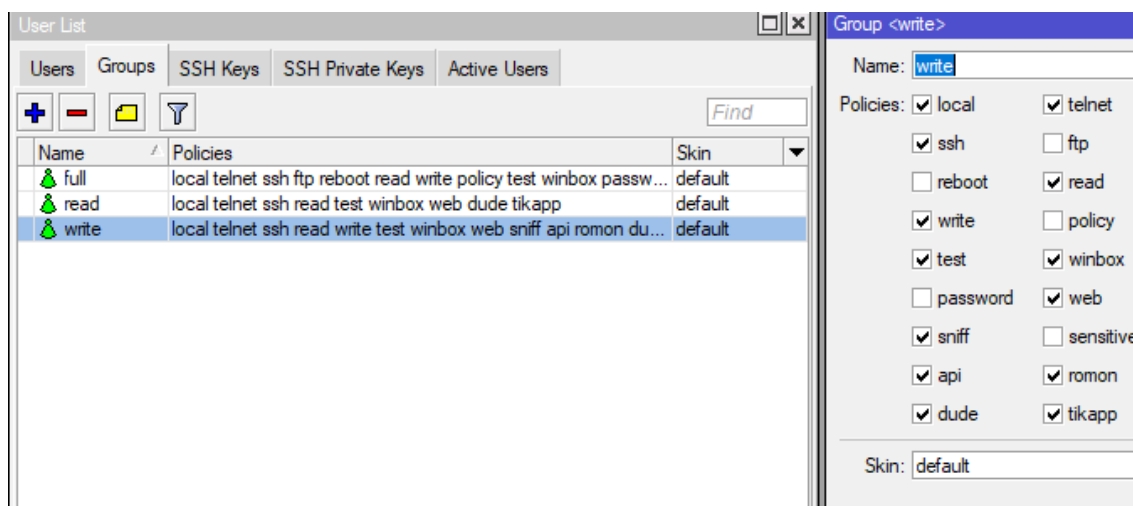


Figura 3.52 Configuración del grupo *write*

Para la configuración del grupo *full*, se selecciona las siguientes políticas: *local, telnet, ssh, ftp, reboot, read, write, policy, test, WinBox, password, web, sniff, sensitive, api, romon, tikapp, dude*. A continuación, se coloca *Apply* y *OK*, ver figura 3.53. Esta política de grupo es creada para tener la administración total del equipo, esto conlleva la creación, modificación o eliminación de usuarios y contraseñas, políticas de grupos, *backups*. Permite el reinicio (*reboot*), *reset* del equipo (*reset configuration*), monitoreo y control de la red (*dude*). Permite el ingreso por *telnet, ssh, WinBox, web, tikapp, RoMon*, la creación, modificación, eliminación de interfaces y direcciones *IP*.

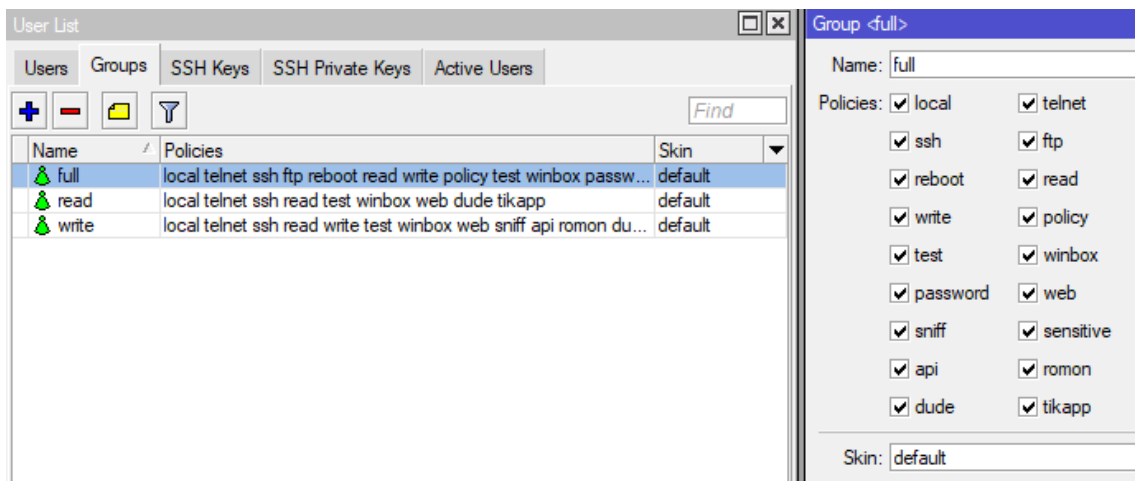


Figura 3.53 Configuración del grupo *full*

Usuario por defecto en *router MikroTik*

Para ver lo usuario por defecto se selecciona el casillero *Users*, como se observa existe un usuario por defecto llamado *admin* que cuenta con todas las políticas de administración. *Admin* no puede ser eliminado hasta que no exista otro usuario que cuente con todas las políticas de administración, ver figura 3.54.

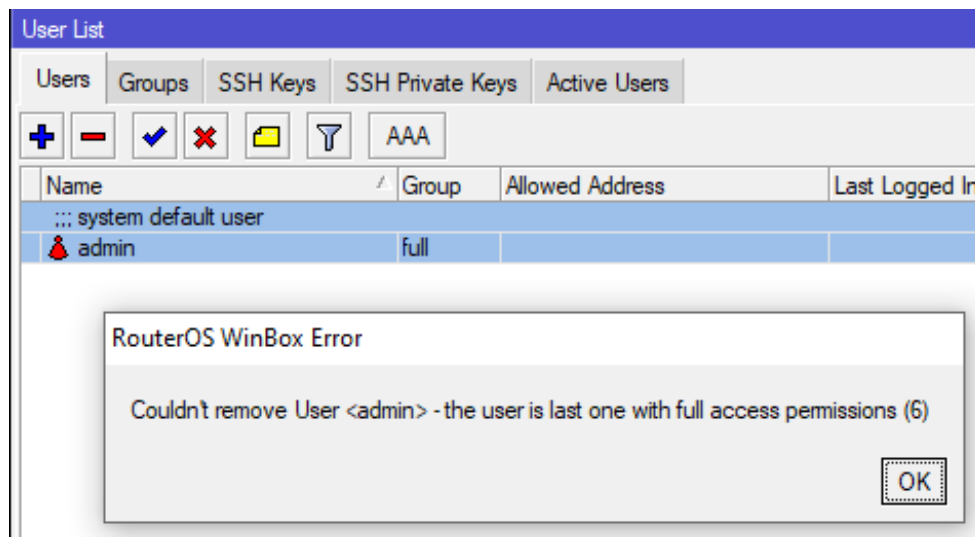


Figura 3.54 Usuario por defecto en *router MikroTik*

Creación de nuevos usuarios

Ahora para la creación de los nuevos usuarios se selecciona la opción (+), se despliega una ventana donde se ingresa el nombre del usuario, grupo al que pertenece, dirección *IP* permitida para ingresar al *router* y la contraseña de acuerdo con la lista de usuarios, ver figura 3.55.

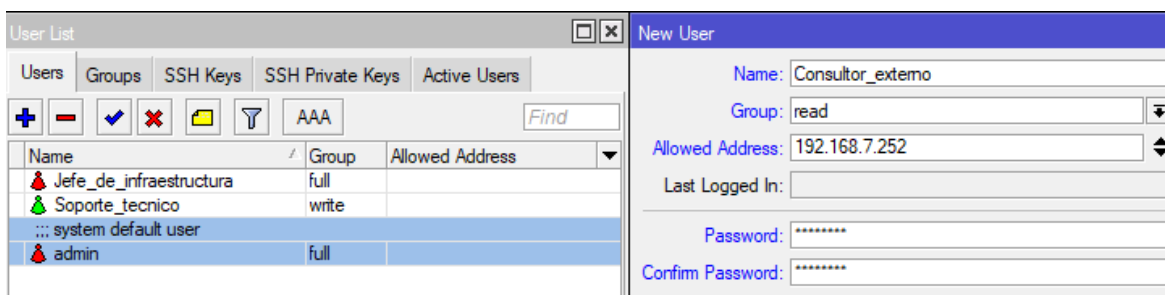


Figura 3.55 Creación y configuración de nuevos usuarios

Una vez creado todos los usuarios, por seguridad es necesario eliminar el usuario *admin* seleccionando el usuario y eligiendo en la opción (-). A continuación, se observa la lista de usuarios creados con sus respectivos grupos, ver figura 3.56.

Name	Group	Allowed Address
Consultor_externo	read	192.168.7.252
Jefe_de_infraestructura	full	
Soporte_tecnico	write	

Figura 3.56 Lista de usuarios creados

Configuración de interfaz ether 2

Para la configuración de la interfaz del *router* se ingresa en la opción *IP/Addresses*, se despliega una ventana, elegimos la opción (+). A continuación, se despliega otra ventana donde se ingresa la dirección *IP (Address)* con su máscara, la red (*Network*) y su interfaz (*Interface*), ver figura 3.57.

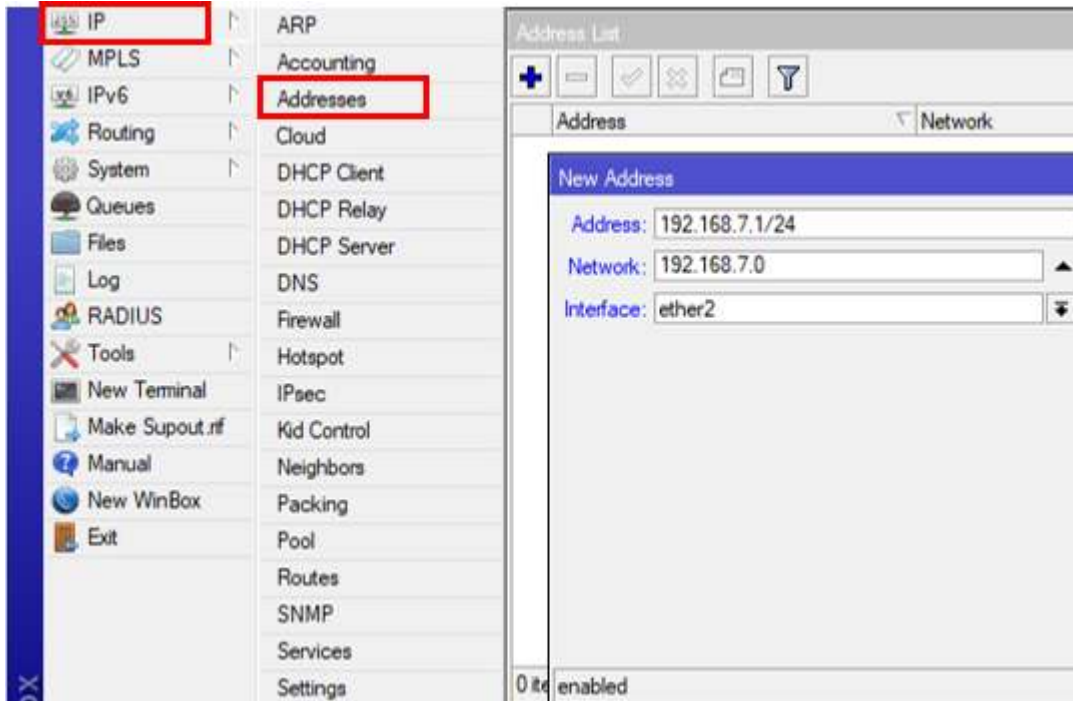


Figura 3.57 Configuración de interfaz

Una vez configurado la interfaz, la dirección *IP* se despliega en la ventana *Address List*, ver figura 3.58.

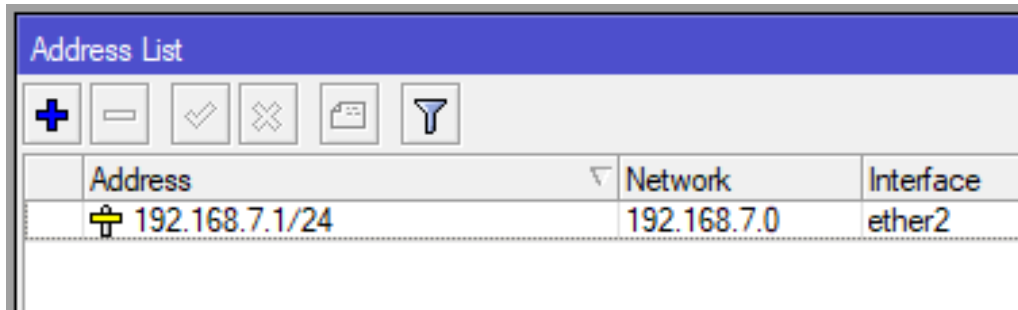


Figura 3.58 Interfaz configurado en *router*

Configuración de direcciones *IP* en *host*

Ahora es necesario realizar la configuración en cada *host* de acuerdo con la lista de usuarios, para ello es necesario ir a las *Propiedades del Protocolo de Internet versión 4 (TCP/IPv4)* del computador y se ingresa la dirección *IP*, máscara y *gateway*. A continuación, se selecciona la opción *Aceptar*, ver figura 3.59.

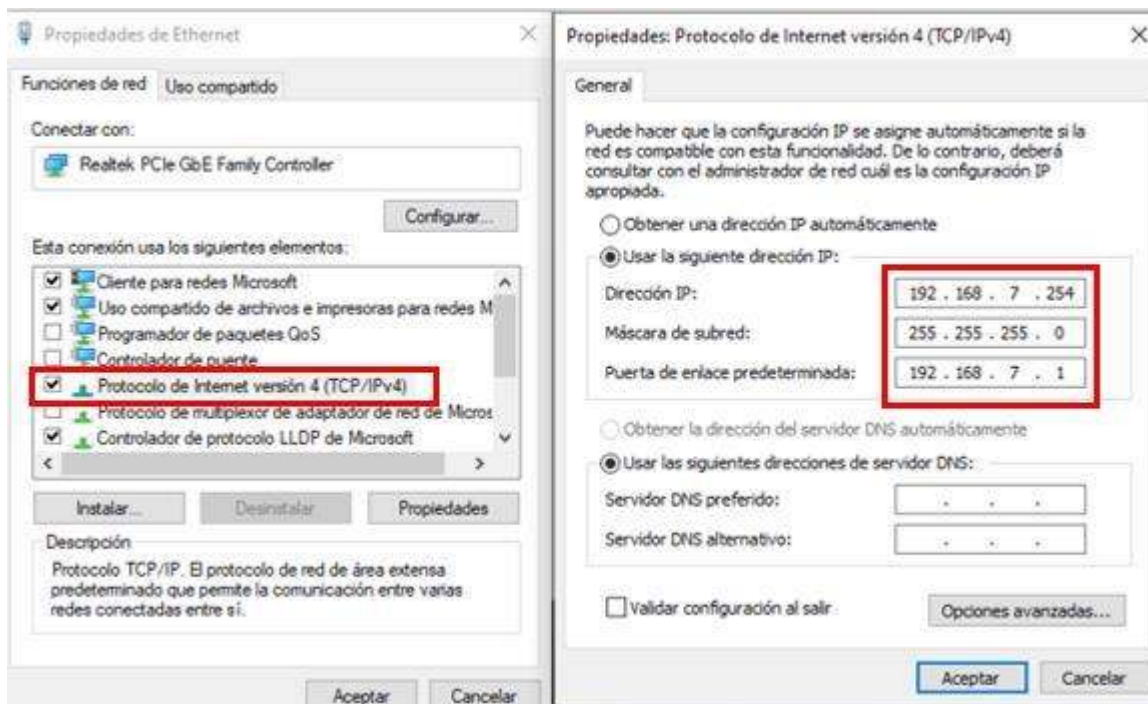


Figura 3.59 Configuración de dirección *IP* en computador

Configuración vía comandos

Configuración de nombre a *router*

Para el cambio de nombre al equipo se ingresa el comando *system identity*

- [admin@MikroTik] > system identity set name=Router_LAN

Configuración de políticas de grupo

Para la configuración de las políticas de grupo *read* se ingresa los siguientes comandos:

- [admin@Router_LAN] > user group set read
policy=local,telnet,ssh,read,test,WinBox,web,tikapp,!ftp,!reboot,!write,!policy,!password,!sniff,!sensitive,!api,!romon,!dude

Para la configuración de las políticas de grupo *write* se ingresa los siguientes comandos:

- [admin@Router_LAN] > user group set write
policy=local,telnet,ssh,read,write,test,WinBox,web,sniff,tikapp,!ftp,!reboot,!policy,!password,!sensitive,!api,!romon,!dude

Para la configuración de las políticas de grupo *full* se ingresa los siguientes comandos:

- [admin@Router_LAN] > user group set full
policy=local,telnet,ssh,read,write,test,WinBox,web,sniff,tikapp,ftp, reboot,policy,password,sensitive,api,romon,dude

Creación de nuevos usuarios

Para la creación de nuevos usuarios se ingresa el comando *user* y se ingresa el nombre, grupo y *password* de cada usuario.

- [admin@Router_LAN] > user add group=full
name=Jefe_de_infraestructura password=Ji123456
- [admin@Router_LAN] > user add group=write name=Soporte_tecnico
password=St123456
- [admin@Router_LAN] > user add group=read name=Consultor_externo
password=Ce123456

Para la eliminación del usuario por defecto *admin*, es necesario iniciar nuevamente sesión con otro usuario que cuente con todas las políticas de grupo y se ingresa los siguientes comandos:

- [admin@Router_LAN] > user remove admin

Configuración de interfaz *ether 2*

```
[admin@Router_LAN] > IP address add address=192.168.7.1/24  
interface=ether2
```

Pruebas de políticas administrativas de cada grupo

Para ver el desempeño de las políticas de grupo de cada usuario se realizó las siguientes pruebas:

La primera prueba realizada es en el usuario *Consultor_externo*, entre sus autorizaciones se tiene la visualización de interfaces. Entre los impedimentos se tiene el no permitir resetear el equipo y el no ingreso al equipo desde otra dirección *IP* que no sea la autorizada en la configuración (192.168.7.252), ver figura 3.60.

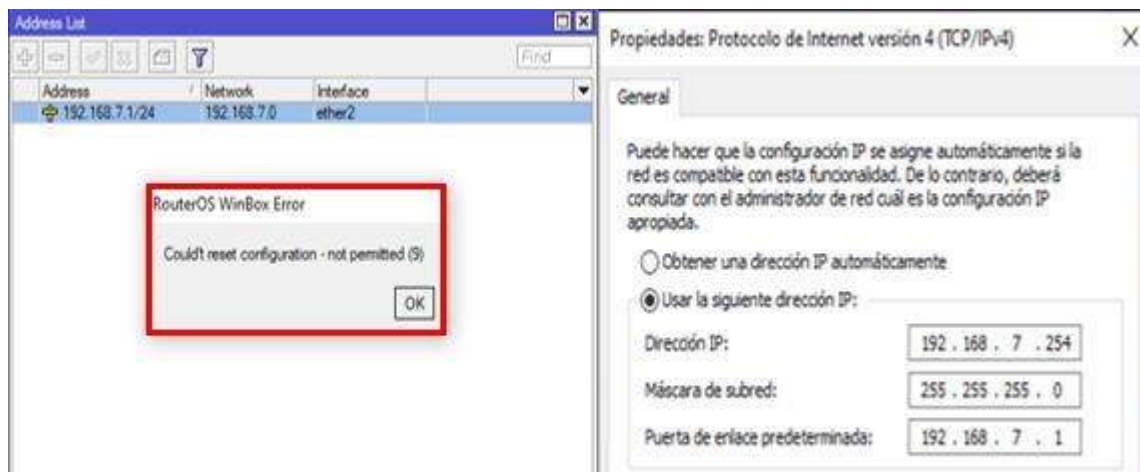


Figura 3.60 Pruebas de usuario *Consultor_externo*

La segunda prueba realizada es en el usuario *Soporte_tecnico*, entre sus autorizaciones se tiene la visualización, creación, modificación y eliminación de interfaces. Entre los impedimentos se tiene el no permitir la modificación de las políticas de grupo, ver figura 3.61.

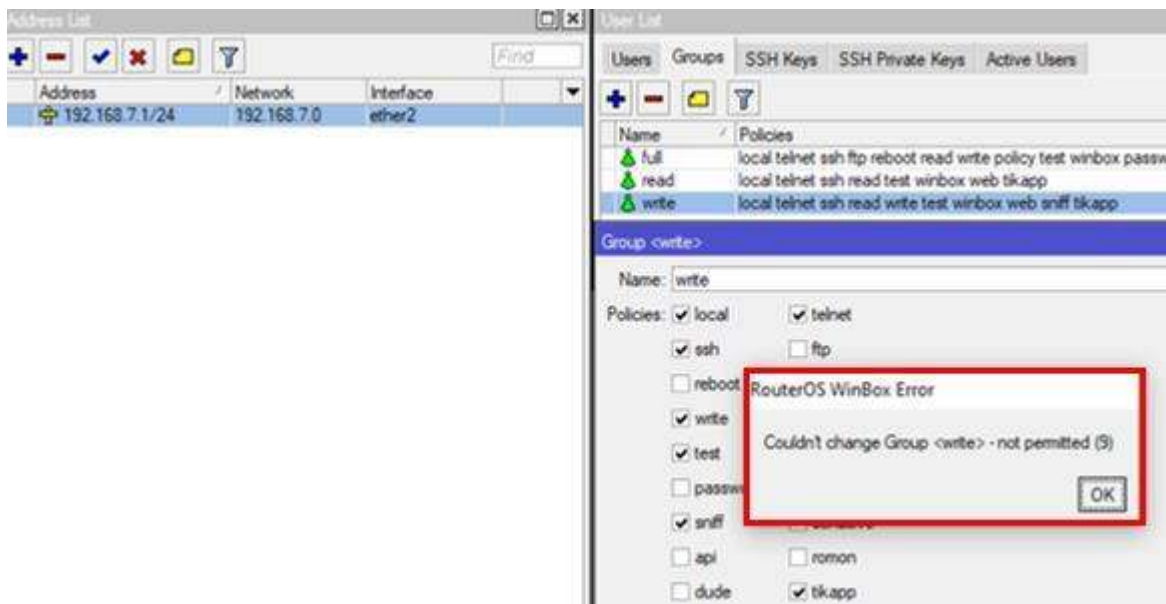


Figura 3.61 Pruebas de usuario Soporte_técnico

La tercera prueba realizada es en el usuario Jefe_de_infraestructura. Este usuario cuenta con todas las autorizaciones de administrar el equipo, entre ellas se tiene el crear, eliminar y descargar *backups*, ver figura 3.62.

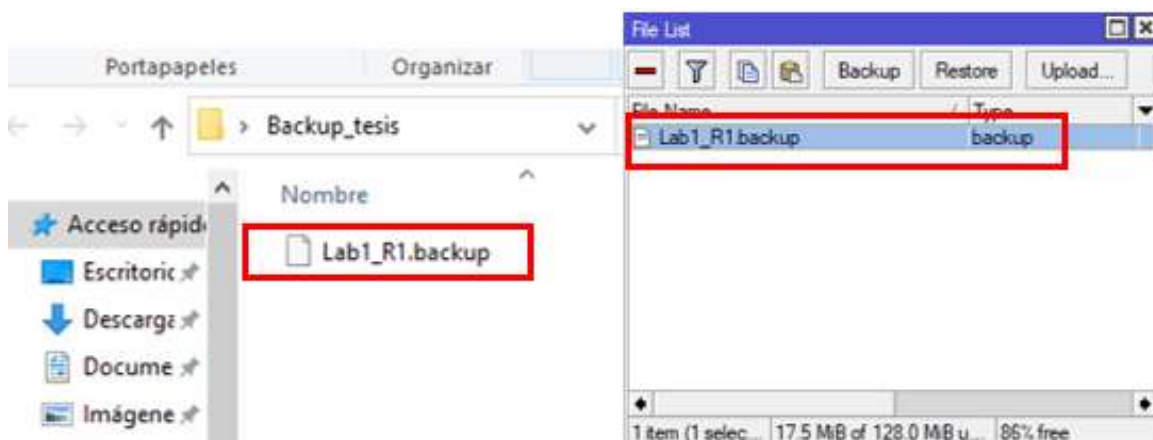


Figura 3.62 Pruebas de usuario Jefe_de_infraestructura

❖ Práctica N°2

Tema: Enrutamiento estático

Objetivo general: Configuración de enrutamiento estático en *routers MikroTik*.

Objetivos específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*.
- Configurar las interfaces de los *routers MikroTik*
- Configurar las rutas *WAN* y *LAN* de cada equipo
- Comprobar conectividad entre equipos *MikroTik* y *hosts*.

Implementación de topología

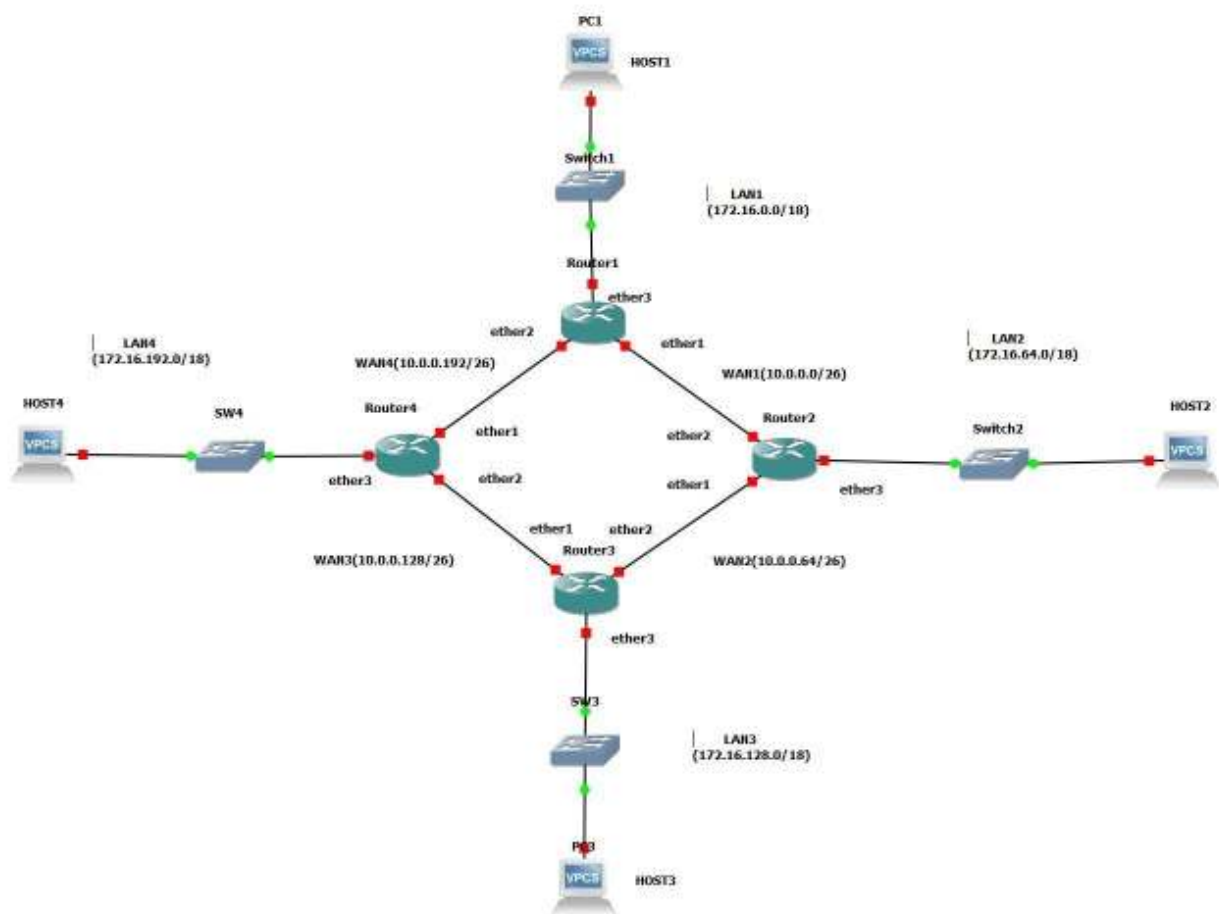


Figura 3.63 Topología de enrutamiento estático

Asignación de direcciones *IP* para cada equipo e interfaces

A continuación, se muestra la tabla 3.6 la distribución de redes *WAN*. Se utiliza la red 10.0.0.0/24 para la creación de 4 subredes *WAN* de máscara fija. Para cada subred *WAN* creada se empleó la primera *IP* válida en *Ether1* mientras para *Ether2* se utiliza la última *IP* válida.

Tabla 3.6 Direccionamiento *IP* de subredes *WAN*

Nombre Subred	Subred	Máscara	Rango de direcciones validas	Broadcast
WAN1	10.0.0.0	/26	10.0.0.1 – 10.0.0.62	10.0.0.63
WAN2	10.0.0.64	/26	10.0.0.65 – 10.0.0.126	10.0.0.127
WAN3	10.0.0.128	/26	10.0.0.129 – 10.0.0.190	10.0.0.191
WAN4	10.0.0.192	/26	10.0.0.193 – 10.0.0.254	10.0.0.255

A continuación, se muestra la tabla 3.7 de distribución de redes *LAN*. Se utiliza la red 172.16.0.0/16 para la creación de 4 subredes *LAN* de máscara fija. Para cada subred *LAN* creada se empleó la primera *IP* válida en *Ether3*, mientras para el *host* se coloca la última *IP* válida.

Tabla 3.7 Direccionamiento *IP* de subredes *LAN*

Nombre subred	Subred	Máscara	Rango de direcciones válidas	Broadcast
LAN1	172.16.0.0	/18	172.16.0.1 – 172.16.63.254	172.16.63.255
LAN2	172.16.64.0	/18	172.16.64.1 – 172.16.127.254	172.16.127.255
LAN3	172.16.128.0	/18	172.16.128.1 – 172.16.191.254	172.16.191.255
LAN4	172.16.192.0	/18	172.16.192.1 – 172.16.255.254	172.16.255.255

Configuración vía interfaz gráfica

Cambio de nombre de cada *router*

Para cambiar el nombre del *router* se selecciona la opción *System/Identify*, ver figura 3.64.

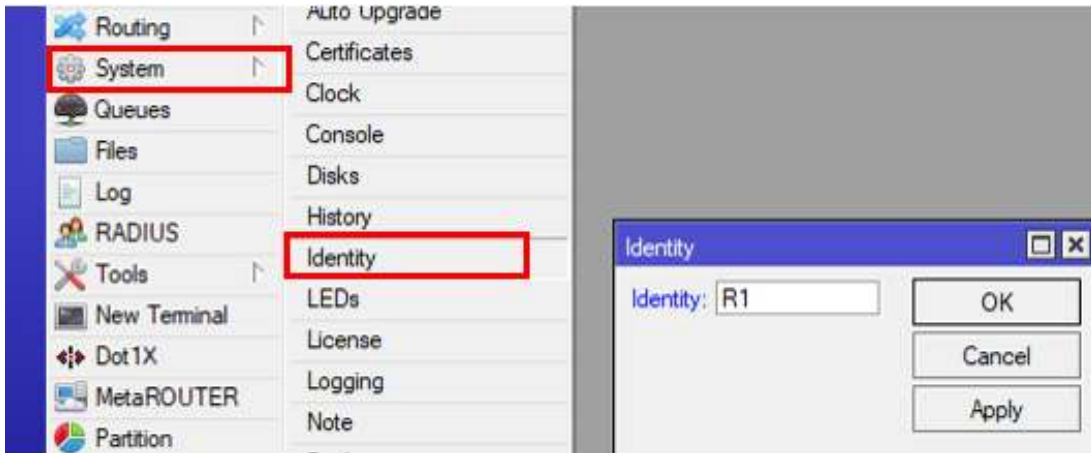


Figura 3.64 Cambio de nombre de equipo *MikroTik*

Configuración de interfaces *WAN* y *LAN*

Para la configuración de cada red se selecciona la opción *IP/Addresses* y a continuación se elige la opción (+). Se ingresa las direcciones *IP (Address)* con su máscara de acuerdo con cada red *WAN* y *LAN*, la red (*Network*) y la interfaz (*Interface*). Todo es necesario para levantar las interfaces de cada equipo *MikroTik* con su respectivo comentario (*Comment*).

Configuración en *R1*

Se configura las interfaces de *ether 1, 2, 3* para *WAN1, WAN4* y *LAN1*, ver figura 3.65.

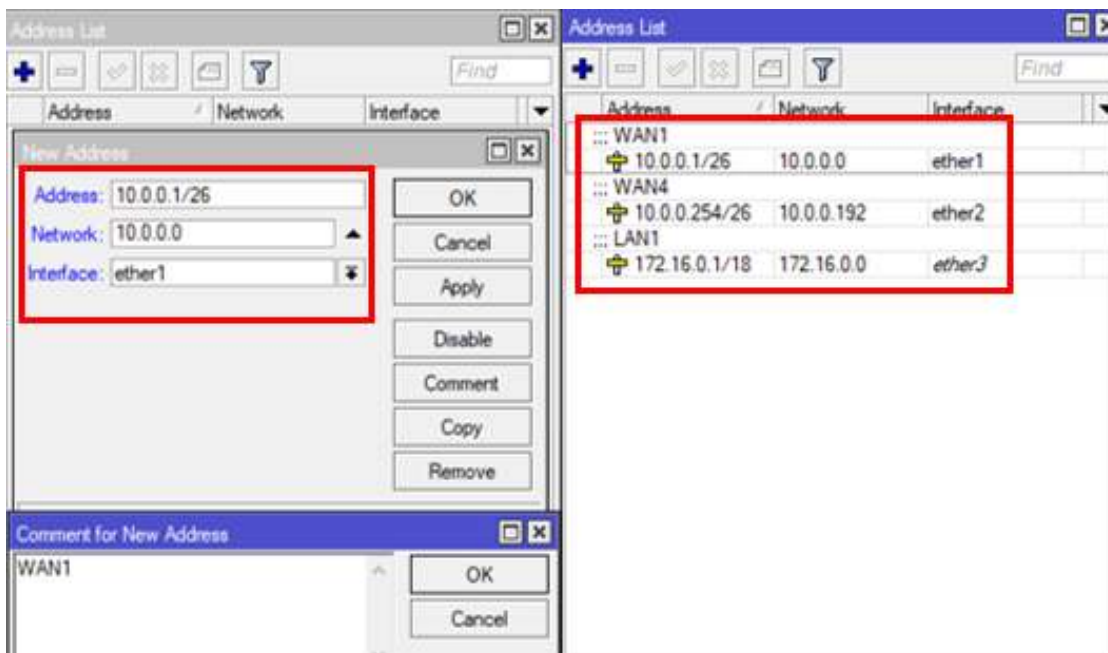


Figura 3.65 Configuración de interfaces WAN y LAN en R1

Configuración en R2

Se configura las interfaces de ether 1, 2, 3 para WAN1, WAN2 y LAN2, ver figura 3.66.

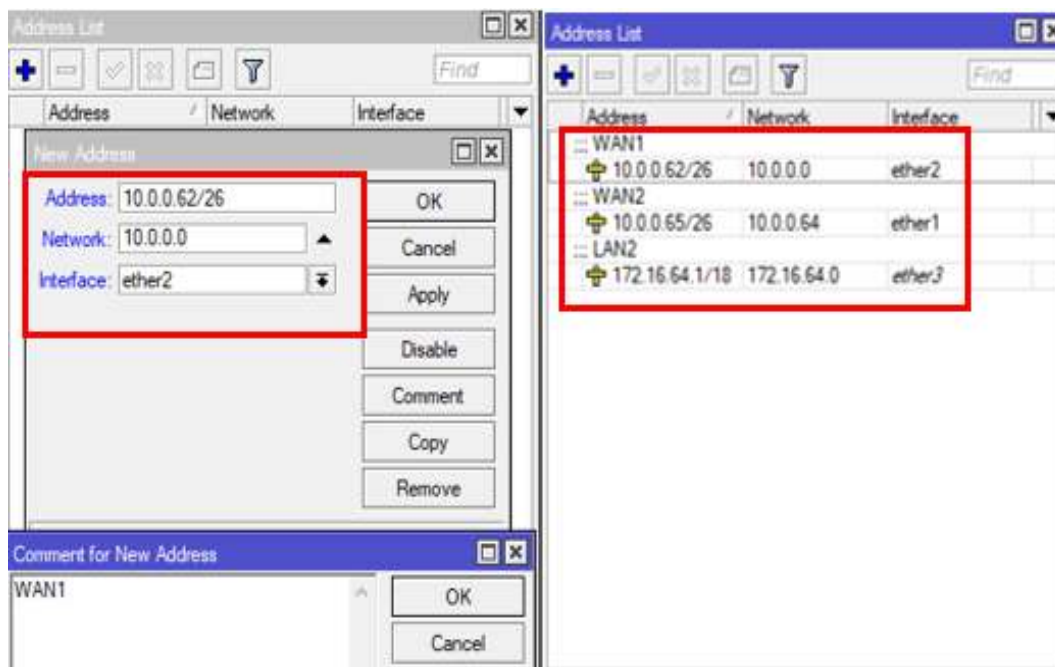


Figura 3.66 Configuración de interfaces WAN y LAN en R2

Configuración en R3

Se configura las interfaces de *ether* 1, 2, 3 para *WAN2*, *WAN3* y *LAN3*, ver figura 3.67.

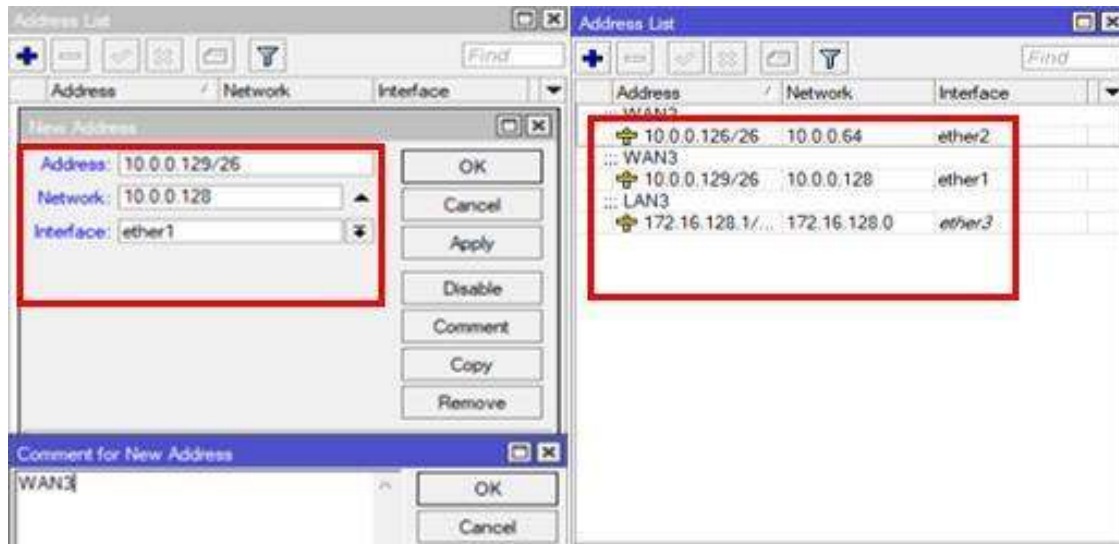


Figura 3.67 Configuración de interfaces WAN y LAN en R3

Configuración en R4

Se configura las interfaces de *ether* 1, 2, 3 para *WAN3*, *WAN4* y *LAN4*, ver figura 3.68.

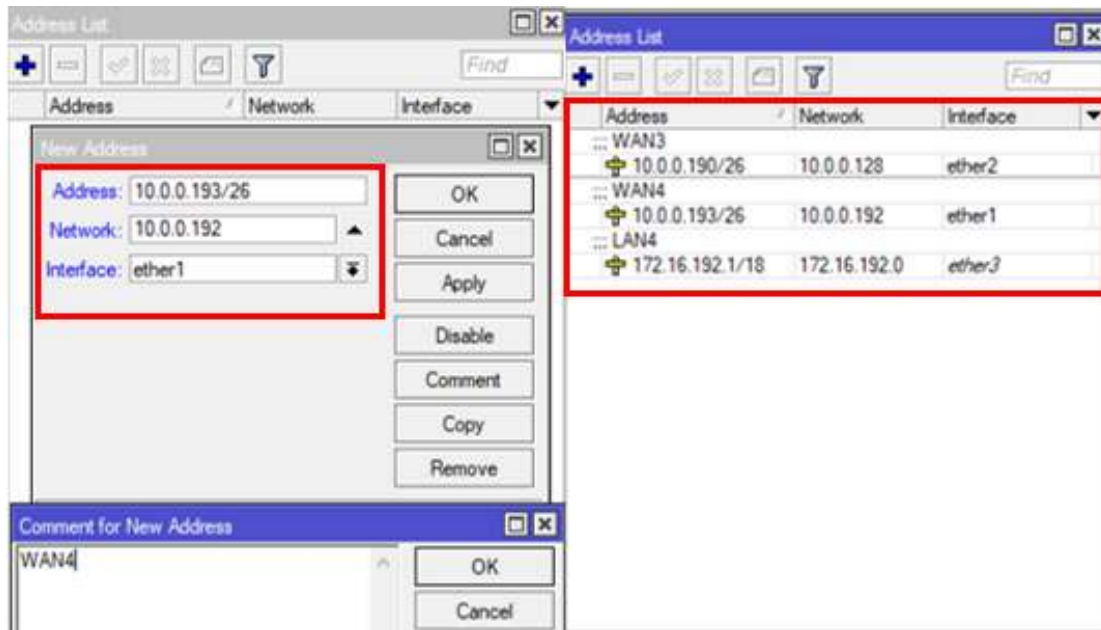


Figura 3.68 Configuración WAN y LAN en R4

Configuración de enrutamiento estático

Para la configuración de enrutamiento estático se especifica el sentido del tráfico, en este caso se lo define en sentido horario, para ello se elige la opción *IP/Routes*, ver figura 3.66. A continuación, se elige la opción (+), donde se ingresa la red que vamos a alcanzar (*Dst. Address*), se especifica el *gateway* (*Gateway*) para alcanzar las redes que no se encuentran conectadas directamente en cada *router*, se coloca la distancia administrativa (*Distance*), en este caso para una red estática la distancia administrativa es 1. Esto debe ir acompañado de un comentario (*Comment*). Adicional para configurar la salida de tráfico de cada red *LAN* se coloca la ruta por default 0.0.0.0/0 con el *gateway* correspondiente a cada *router*.

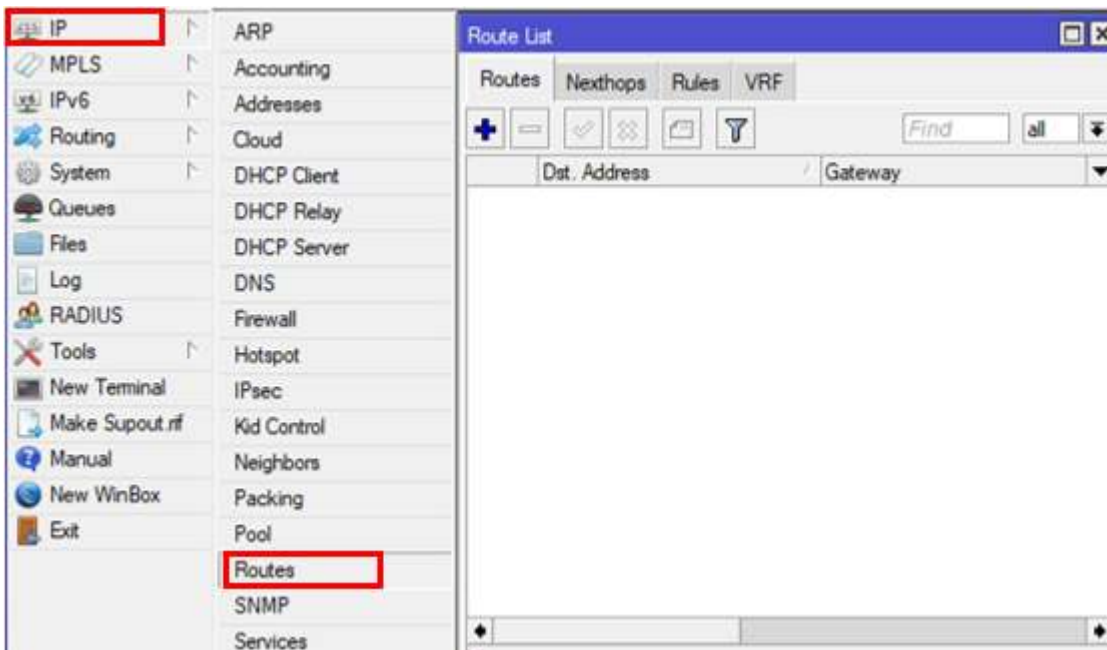


Figura 3.69 Acceso a Router

R1

Se configura las rutas estáticas para *WAN2*, *WAN3* y *LAN1*, ver figura 3.70.

New Route		Dst. Address	Gateway	Distance
General	Attributes			
Dst. Address: 10.0.0.64/26		DAC	172.16.0.0/18 ether3 reachable	0
Gateway: 10.0.0.62		DAC	10.0.0.192/26 ether2 reachable	0
Check Gateway:		DAC	10.0.0.0/26 ether1 reachable	0
Type: unicast		::: Gateway_LAN1		
Distance: 1		AS	0.0.0.0/0 10.0.0.62 reachable ether1	1
Scope: 30		::: Gateway_WAN2		
Target Scope: 10		AS	10.0.0.64/26 10.0.0.62 reachable ether1	1
Routing Mark:		::: Gateway_WAN3		
Pref. Source:		AS	10.0.0.128/26 10.0.0.62 reachable ether1	1

Figura 3.70 Configuración de rutas WAN y LAN en R1

R2

Se configura las rutas estáticas para WAN3, WAN4 y LAN2, ver figura 3.71.

New Route		Dst. Address	Gateway
General	Attributes		
Dst. Address: 10.0.0.128/26		DAC	172.16.64.0/18 ether3 reachable
Gateway: 10.0.0.126		DAC	10.0.0.0/26 ether2 reachable
Check Gateway:		DAC	10.0.0.64/26 ether1 reachable
Type: unicast		::: Gateway_WAN4	
Distance: 1		AS	10.0.0.192/26 10.0.0.126 reachable ether1
Scope: 30		::: Gateway_WAN3	
Target Scope: 10		AS	10.0.0.128/26 10.0.0.126 reachable ether1
Routing Mark:		::: Gateway_LAN2	
Pref. Source:		AS	0.0.0.0/0 10.0.0.126 reachable ether1

Figura 3.71 Configuración de rutas WAN y LAN en R2

R3

Se configura las rutas estáticas para WAN1, WAN4 y LAN3, ver figura 3.72.

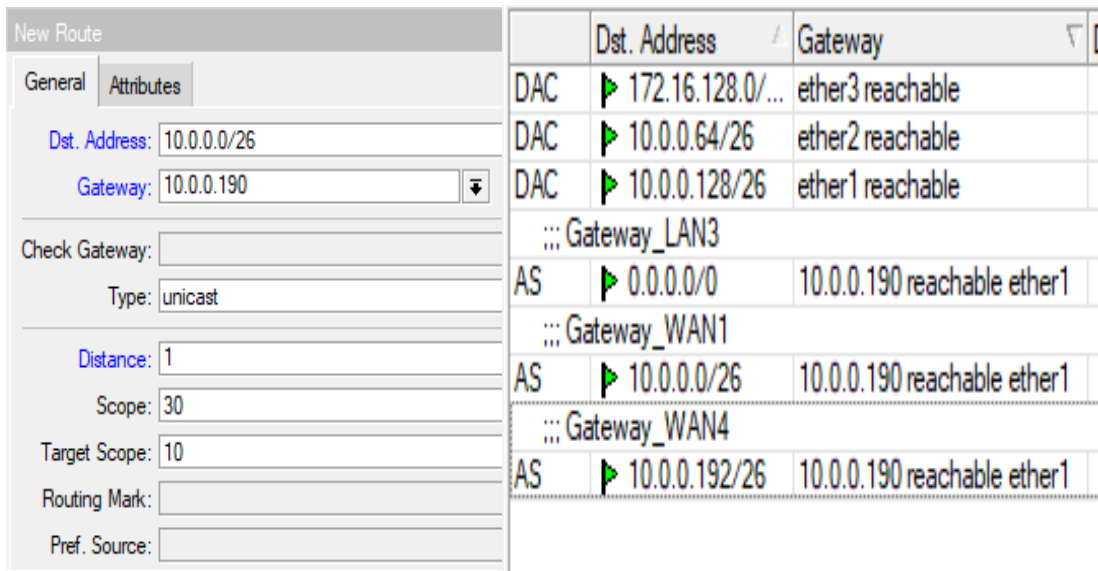


Figura 3.72 Configuración de rutas WAN y LAN en R3

R4

Se configura las rutas estáticas para WAN1, WAN2 y LAN4, ver figura 3.73.

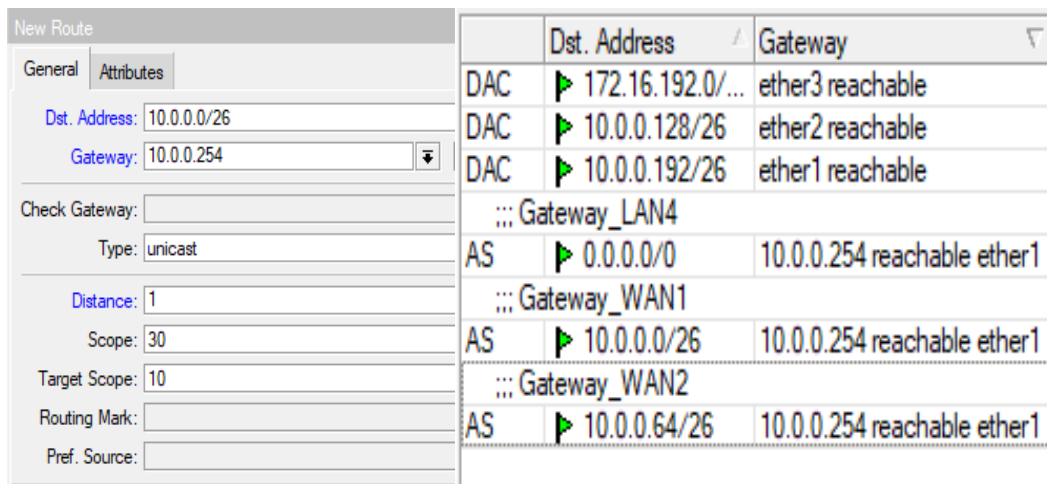


Figura 3.73 Configuración de rutas WAN y LAN en R4

Configuración de host de cada red LAN

Para la configuración de cada *host* se ingresa a las Propiedades del *Protocolo de Internet versión 4 (TCP/IPv4)* del computador e ingresamos la dirección *IP*, máscara y *gateway*. A continuación, se selecciona la opción *Aceptar*, ver figura 3.74.

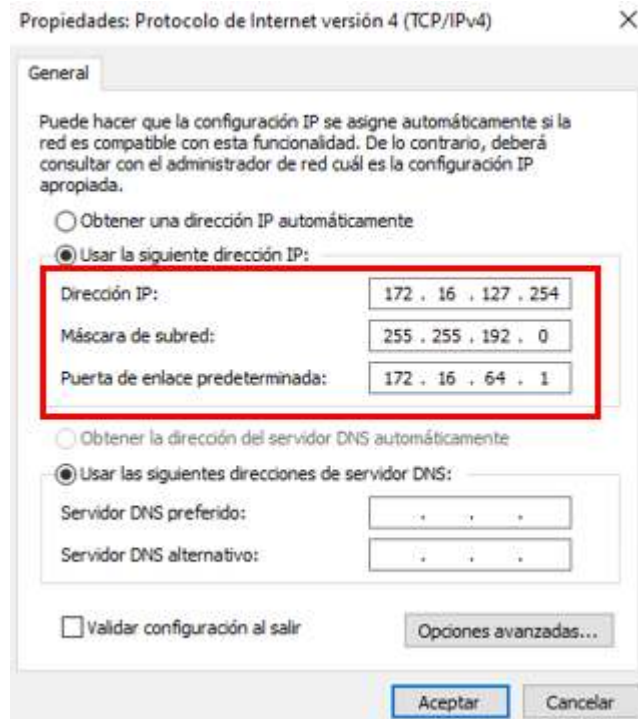


Figura 3.74 Configuración de *host* en LAN2

Configuración vía comandos

Cambio de nombre de cada *router*

- [admin@MikroTik] > system identity set name=R1

Configuración de interfaces *WAN* y *LAN*

Para la configuración de cada red se ingresa el comando *IP route*.

R1

- [admin@R1] > IP address add address=10.0.0.1/26 comment=WAN1 interface=ether1
- [admin@R1] > IP address add address=10.0.0.254/26 comment=WAN4 interface=ether2
- [admin@R1] > IP address add address=172.16.0.1/18 comment=LAN1 interface=ether3

R2

- [admin@R2] > IP address add address=10.0.0.65/26 comment=WAN2 interface=ether1

- [admin@R2] > IP address add address=10.0.0.62/26 comment=WAN1
interface=ether2
- [admin@R2] > IP address add address=172.16.64.1/18 comment=LAN2
interface=ether3

R3

- [admin@R3] > IP address add address=10.0.0.129/26 comment=WAN3
interface=ether1
- [admin@R3] > IP address add address=10.0.0.126/26 comment=WAN2
interface=ether2
- [admin@R3] > IP address add address=172.16.128.1/18 comment=LAN3
interface=ether3

R4

- [admin@R4] > IP address add address=10.0.0.193/26 comment=WAN4
interface=ether1
- [admin@R4] > IP address add address=10.0.0.190/26 comment=WAN3
interface=ether2
- [admin@R4] > IP address add address=172.16.192.1/18 comment=LAN4
interface=ether3

Configuración de enrutamiento estático

Para la configuración se ingresa el comando *IP route*, donde se especifica el *gateway* para alcanzar las redes que no se encuentran conectadas directamente en cada *router*.

R1

- [admin@R1] > IP route add distance=1 dst-address=10.0.0.64/26
gateway=10.0.0.62 comment=Gateway_WAN2
- [admin@R1] > IP route add distance=1 dst-address=10.0.0.128/26
gateway=10.0.0.62 comment=Gateway_WAN3
- [admin@R1] > IP route add distance=1 dst-address=0.0.0.0/0
gateway=10.0.0.62 comment=Gateway_LAN1

R2

- [admin@R2] > IP route add distance=1 dst-address=10.0.0.128/26
gateway=10.0.0.126 comment=Gateway_WAN3
- [admin@R2] > IP route add distance=1 dst-address=10.0.0.192/26
gateway=10.0.0.126 comment=Gateway_WAN4
- [admin@R2] > IP route add distance=1 dst-address=0.0.0.0/0
gateway=10.0.0.126 comment=Gateway_LAN2

R3

- [admin@R3] > IP route add distance=1 dst-address=10.0.0.0/26 gateway=10.0.0.190 comment=Gateway_WAN1
- [admin@R3] > IP route add distance=1 dst-address=10.0.0.192/26 gateway=10.0.0.190 comment=Gateway_WAN4
- [admin@R3] > IP route add distance=1 dst-address=0.0.0.0/0 gateway=10.0.0.190 comment=Gateway_LAN3

R4

- [admin@R4] > IP route add distance=1 dst-address=10.0.0.0/26 gateway=10.0.0.254 comment=Gateway_WAN1
- [admin@R4] > IP route add distance=1 dst-address=10.0.0.64/26 gateway=10.0.0.254 comment=Gateway_WAN2
- [admin@R4] > IP route add distance=1 dst-address=0.0.0.0/0 gateway=10.0.0.254 comment=Gateway_LAN4

Pruebas de conectividad entre equipos y hosts

Se realizó las pruebas de conectividad en toda la red por medio de la utilización del comando ping, para ello es necesario ingresar al *CMD* de *Windows*.

La primera prueba realizada es la conectividad entre el *host* de *LAN2* y la interfaz *ether 1* de *R4*, ver figura 3.75.

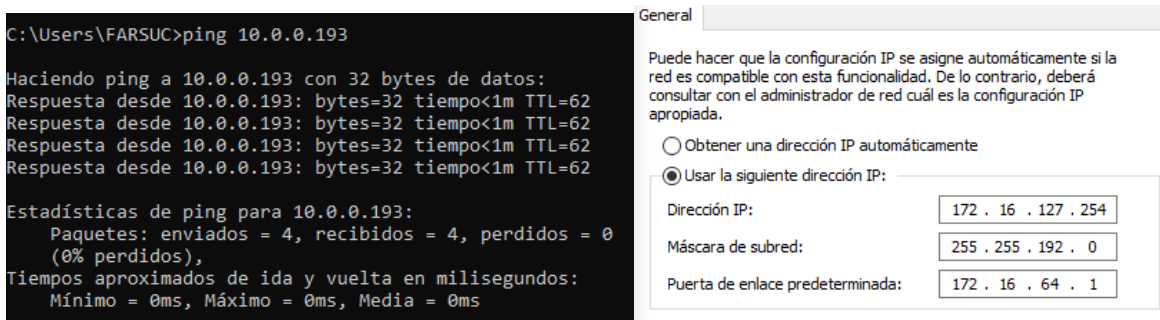


Figura 3.75 Prueba de conectividad en la red

La segunda prueba realizada es la conectividad entre el *host* de *LAN3* y el *gateway* de *LAN1*, ver figura 3.76.

C:\Users\FARSUC>ping 172.16.0.1

Haciendo ping a 172.16.0.1 con 32 bytes de datos:
 Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=62
 Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=62
 Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=62
 Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=62

Estadísticas de ping para 172.16.0.1:
 Paquetes: enviados = 4, recibidos = 4, perdidos = 0
 (0% perdidos),
 Tiempos aproximados de ida y vuelta en milisegundos:
 Mínimo = 0ms, Máximo = 0ms, Media = 0ms

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

Figura 3.76 Prueba de conectividad en la red

La tercera prueba realizada es la conectividad entre el *host* de LAN1 y *host* de LAN3, ver figura 3.77.

C:\Users\FARSUC>ping 172.16.191.254

Haciendo ping a 172.16.191.254 con 32 bytes de datos:
 Respuesta desde 172.16.191.254: bytes=32 tiempo=114ms TTL=61
 Respuesta desde 172.16.191.254: bytes=32 tiempo=120ms TTL=61
 Respuesta desde 172.16.191.254: bytes=32 tiempo=124ms TTL=61
 Respuesta desde 172.16.191.254: bytes=32 tiempo=11ms TTL=61

Estadísticas de ping para 172.16.191.254:
 Paquetes: enviados = 4, recibidos = 4, perdidos = 0
 (0% perdidos),
 Tiempos aproximados de ida y vuelta en milisegundos:
 Mínimo = 11ms, Máximo = 124ms, Media = 92ms

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

Figura 3.77 Prueba de conectividad en la red

❖ Práctica N°3

Tema: *DHCP server, client, relay*

Objetivo: Configuración de *DHCP* en *router MikroTik*.

Objetivos Específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*
- Configuración de interfaces *WAN* y *LAN*
- Configuración de *pool* de direcciones para *DHCP server*
- Configuración de *DHCP server, relay* y *client*
- Configuración de rutas estáticas entre redes *WAN* y *LAN*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

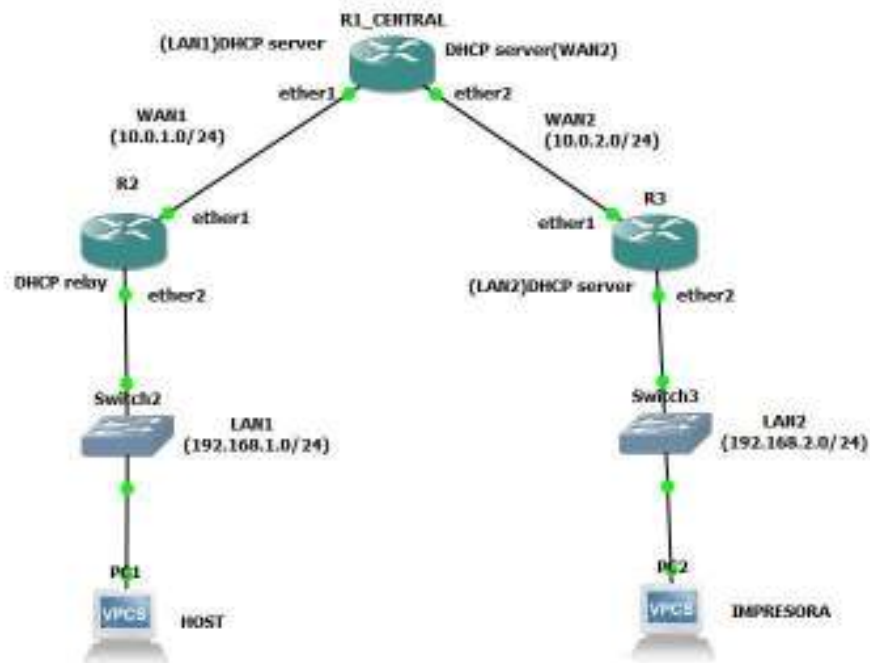


Figura 3.78 Topología de *DHCP server, client, relay*

Tabla de direcciones IP

A continuación, se muestra la tabla 3.8 de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Tabla 3.8 Direccionamiento *IP* en redes *WAN*, *LAN* y *hosts*

Nombre de red	Red	Máscara	Interfaz	Dirección <i>IP</i>	Máscara
WAN1	10.0.1.0	/24	<i>Ether1</i> (R1_central)	10.0.1.1	/24
			<i>Ether1</i> (R2)	10.0.1.2	/24
WAN2	10.0.2.0	/24	<i>Ether2</i> (R1_central)	10.0.2.1	/24
			<i>Ether1</i> (R3)	<i>DHCP</i>	<i>DHCP</i>
LAN1	192.168.1.0	/24	<i>Ether2</i> (R2)	192.168.1.1	/24
			<i>Host</i>	<i>DHCP</i>	<i>DHCP</i>
LAN1	192.168.1.0	/24	<i>Ether2</i> (R3)	192.168.2.1	/24
			Impresora	192.168.2.77	/24

Pool de direcciones *IP*

A continuación, se muestra la tabla 3.9 de rangos de direcciones *IP* de las redes *WAN2*, *LAN1* y *LAN2*.

Tabla 3.9 *Pool* de direcciones *IP* en redes *WAN* y *LAN*

Nombre de red	Red	Máscara	<i>Pool</i> de direcciones <i>IP</i>	<i>Broadcast</i>
WAN2	10.0.2.0	/24	10.0.2.2 – 10.0.2.254	10.0.2.255
LAN1	192.168.1.0	/24	192.168.1.2 – 192.168.1.254	192.168.1.255
LAN2	192.168.2.0	/24	192.168.2.2 – 192.168.2.254	192.168.2.255

Configuración vía interfaz gráfica

Cambio de nombre de cada *router*

Para definir el nombre del *router* se selecciona la opción *System/Identify*, ver figura 3.79.

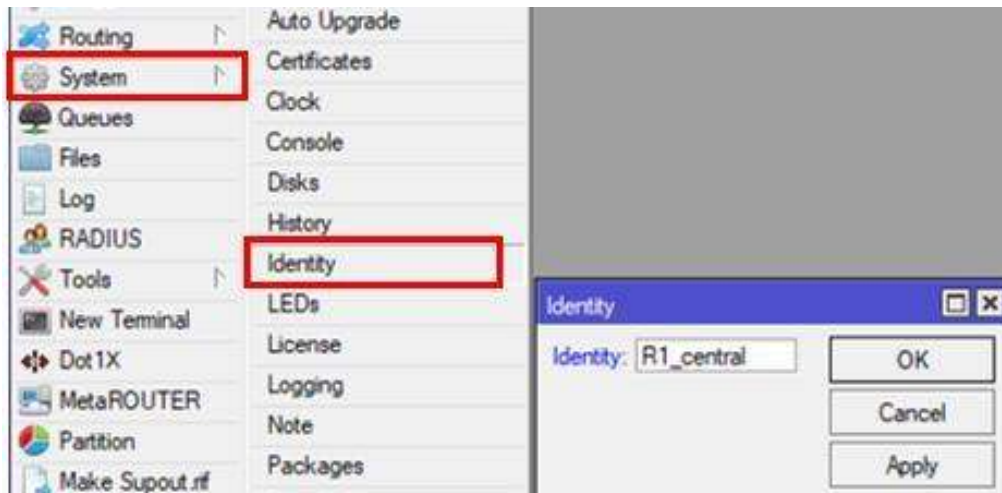


Figura 3.79 Cambio de nombre de equipo MikroTik

Configuración de interfaces WAN y LAN

Para la configuración se selecciona en el menú la opción *IP/Addresses* y se ingresa las direcciones *IP* en cada equipo.

R2

Se configura las interfaces de *ether 1* y *2* para *WAN1* y *LAN1*, ver figura 3.80.



Figura 3.80 Configuración de interfaces en R2

R3

Se configura las interfaces de *ether 2* para *LAN2*, ver figura 3.81.

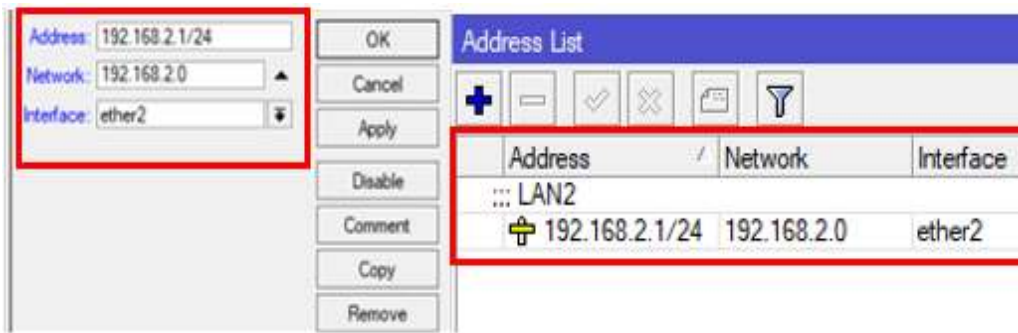


Figura 3.81 Configuración de interfaces en R3

R1_central

Se configura las interfaces de *ether 1* y *2* para *WAN1* y *WAN2*, ver figura 3.82.

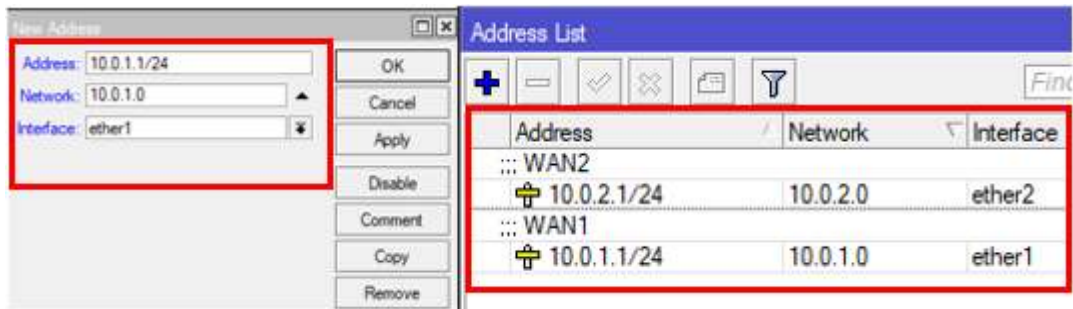


Figura 3.82 Configuración de interfaces en R1_central

Creación de pool de direcciones

Para la creación se selecciona en el menú la opción *IP/Pool* y se selecciona la opción (+), ver figura 3.83. A continuación, se coloca un nombre (*Name*) y el rango de direcciones de la red (*Addresses*) de acuerdo con la tabla de pool de direcciones.

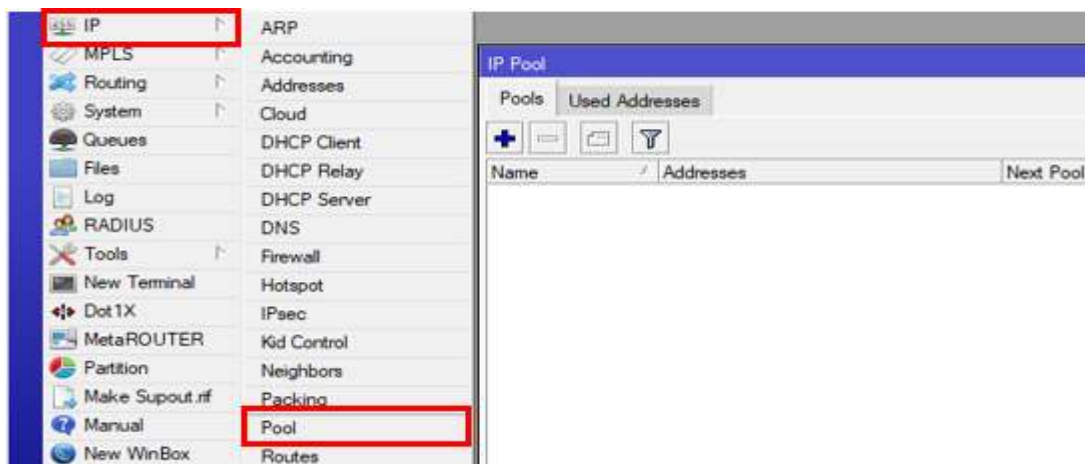


Figura 3.83 Acceso a pool

R3

Se crea un pool de direcciones con el rango 192.168.2.2 – 192.168.2.254 para el *DHCP server* de LAN2, ver figura 3.84.



Figura 3.84 Creación de *pool* de direcciones en R3

R1_central

Se crea un pool de direcciones con el rango 192.168.1.2 – 192.168.1.254 para la *DHCP relay* de LAN1 y se crea el rango 10.0.2.2 – 10.0.2.254 para el *DCHP server* de WAN2, ver figura 3.85.

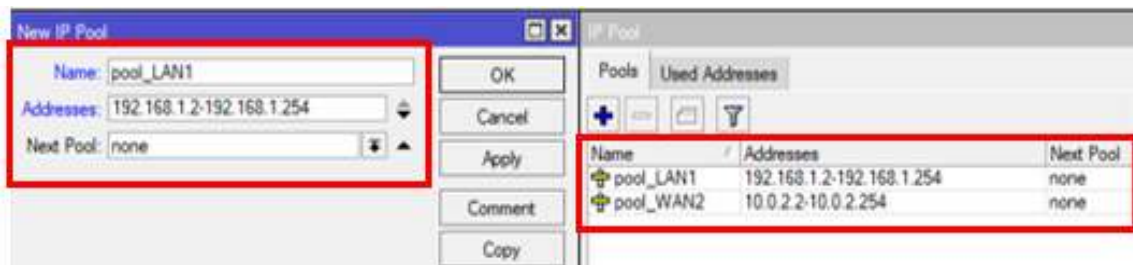


Figura 3.85 Configuración de interfaces en R1_central

Configuración de *DCHP server*

Para la configuración se selecciona en el menú la opción *IP/DHCP server* y se selecciona la opción (+), ver figura 3.86. A continuación, se coloca un nombre (*Name*), la interfaz donde se configura el *DHCP server* (*Interface*), el tiempo de arrendamiento de direcciones *IP* (*Lease Time*) y se selecciona el pool creado para esta red (*Address Pool*). En la opción de *Networks* se elige la opción (+) y a continuación se ingresa la dirección de la red (*Address*) y el *gateway* de la red (*gateway*) con su respectivo comentario.

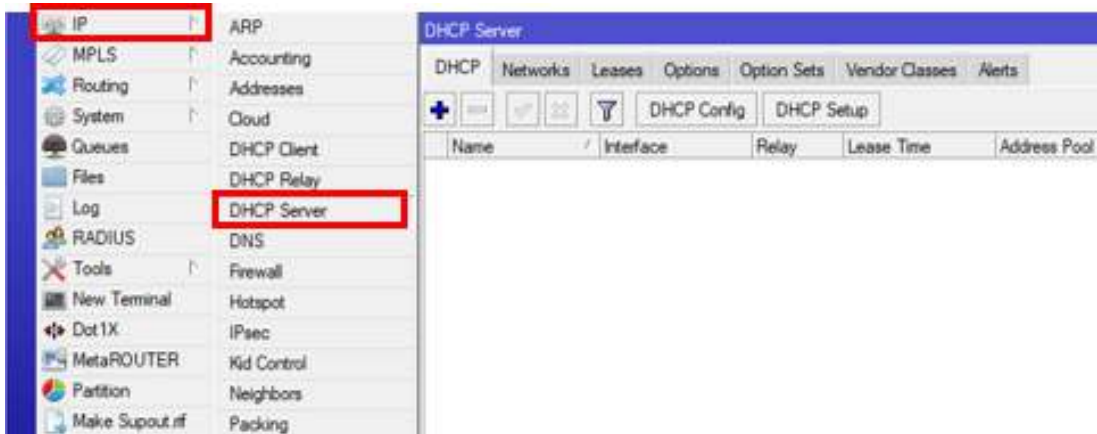


Figura 3.86 Acceso a *DHCP server*

R3

Se configura el *DCHP server* para *LAN2* en *ether 2* con *pool_LAN2*, ver figura 3.87.

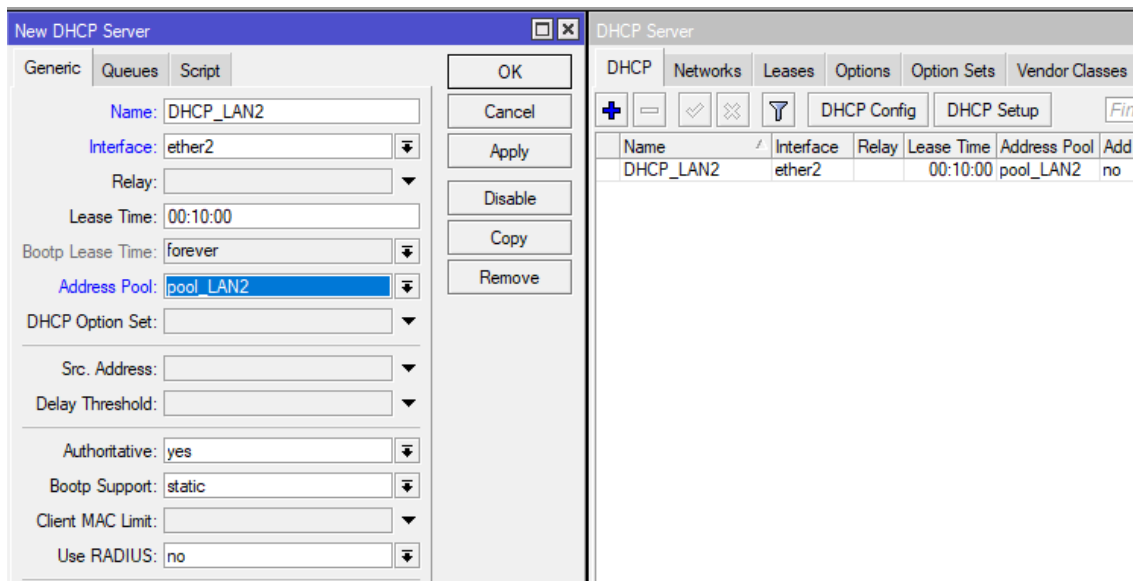


Figura 3.87 Configuración de *DHCP server*

Ahora se configura la red 192.168.2.0/24 para LAN2, ver figura 3.88.

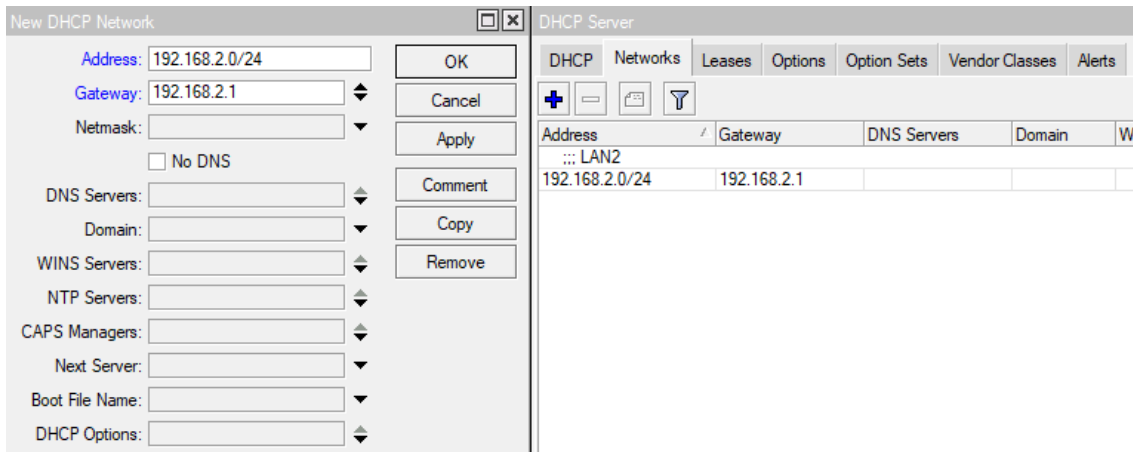


Figura 3.88 Configuración de red LAN2 en R3

R1_central

Se configura el *DCHP* server para WAN2 en ether 2 con *pool_WAN2*, ver figura 3.89.

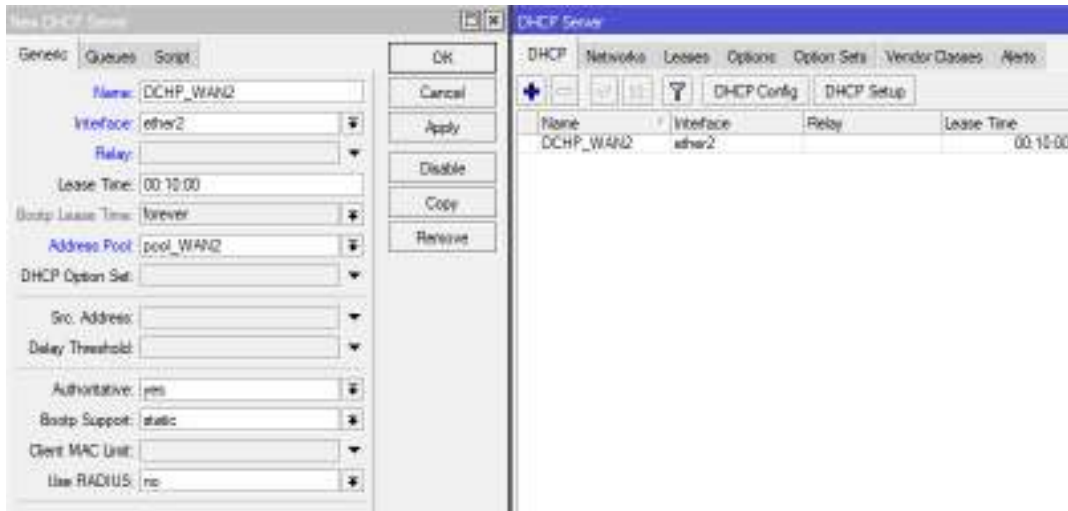


Figura 3.89 Configuración de *DHCP* server en R1_central

Se configura el *DCHP* server de LAN1 con *pool_LAN1*, donde se coloca la dirección *IP* de *Ether1* del R2 (*relay*) para habilitar el *DHCP* relay, ver figura 3.90.

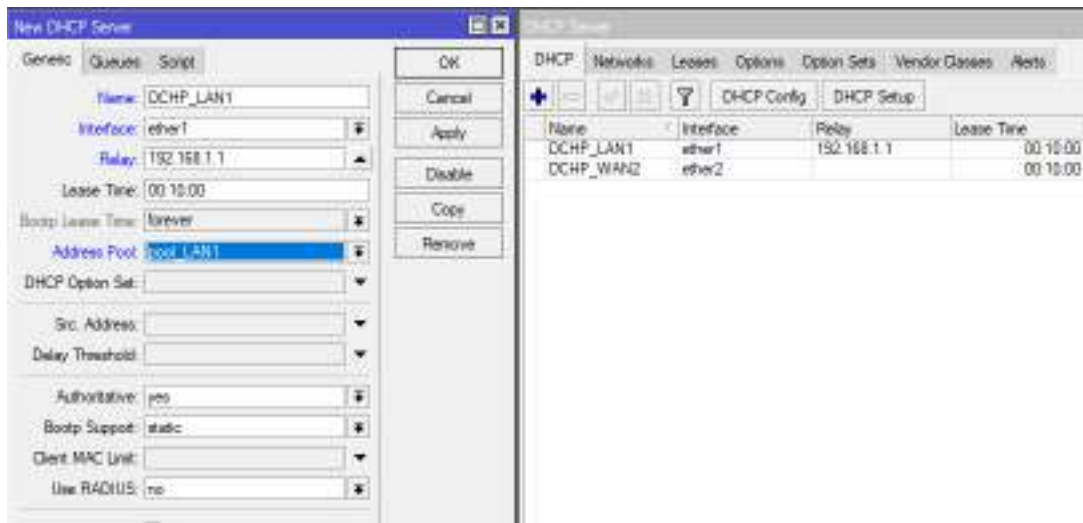


Figura 3.90 Configuración de DHCP server para DHCP relay

Ahora se configura la red 10.0.1.0/24 para WAN1 y a la red 192.168.1.0/24 para LAN1, ver figura 3.91.

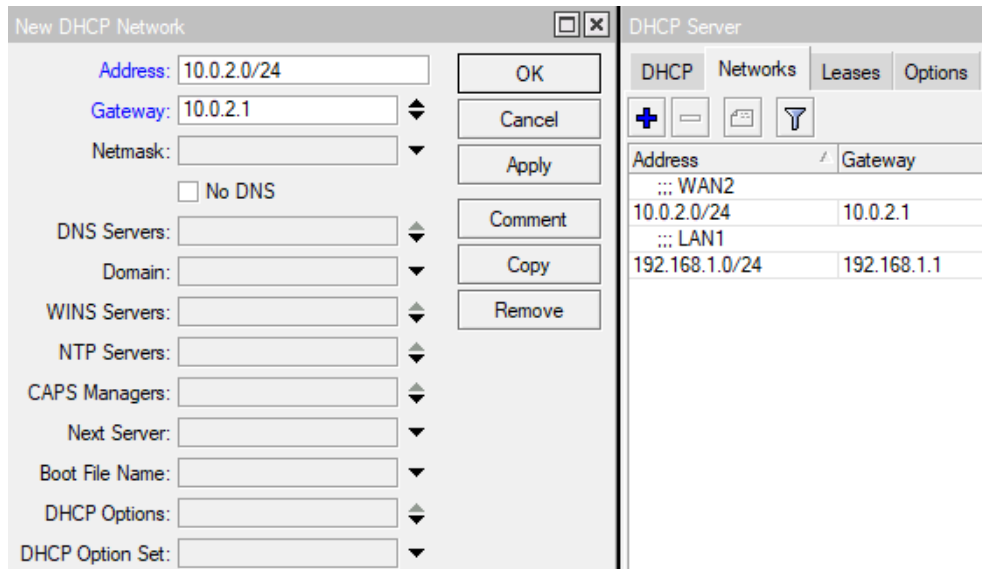


Figura 3.91 Configuración de red LAN2 en R3

Configuración de amarre IP/MAC

Para reservar la dirección IP por medio de la dirección MAC se selecciona en el menú la opción IP/DHCP server, después se escoge la opción Lease y la opción (+), ver figura 3.92. A continuación, se ingresa la dirección IP a reservar (Address), la dirección MAC (MAC Address) del host y se selecciona el DHCP server de la red (server) con su respectivo comentario.

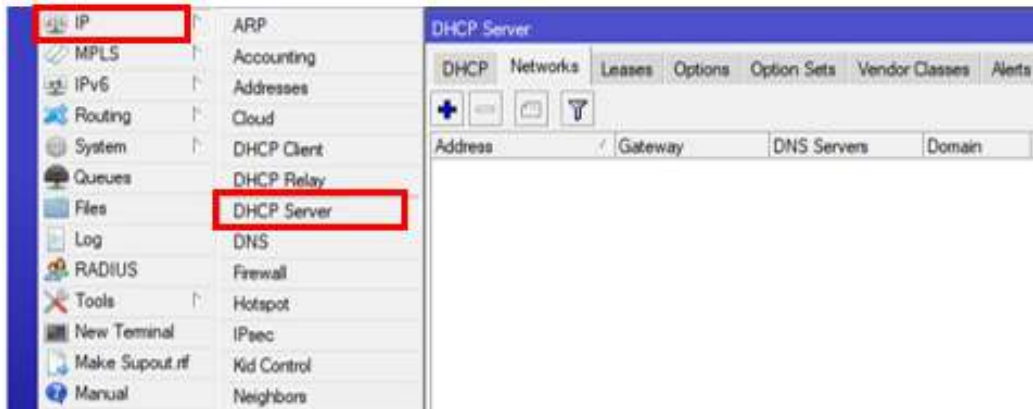


Figura 3.92 Acceso a Lease

R3

Se configura la IP 192.168.2.77 de LAN2 como reserva al host impresora, ver figura 3.93.

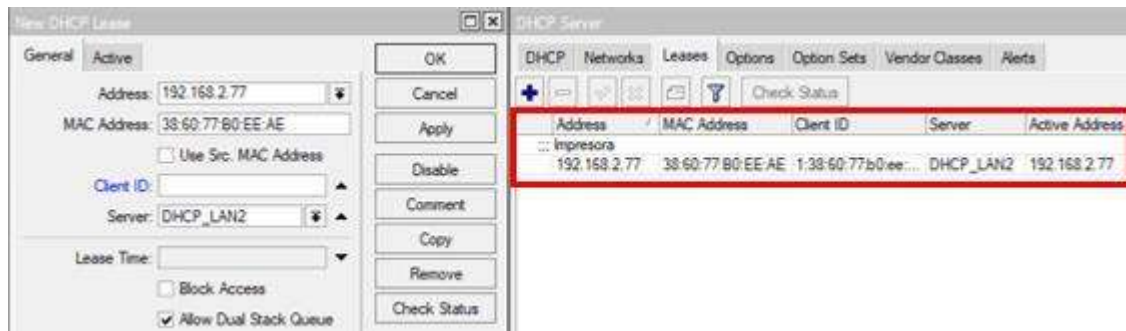


Figura 3.93 Configuración de amarre de IP/MAC en R3

Configuración de DHCP relay

Para la configuración se selecciona en el menú la opción *IP/DHCP Relay* y se selecciona la opción (+), ver figura 3.94. A continuación, se coloca un nombre (*Name*), la interfaz destino del *DHCP relay* (*Interface*), dirección *IP* del *DHCP server* origen (*DHCP server*) y la dirección *IP* de la interfaz destino del *DHCP relay* (*Local Address*).

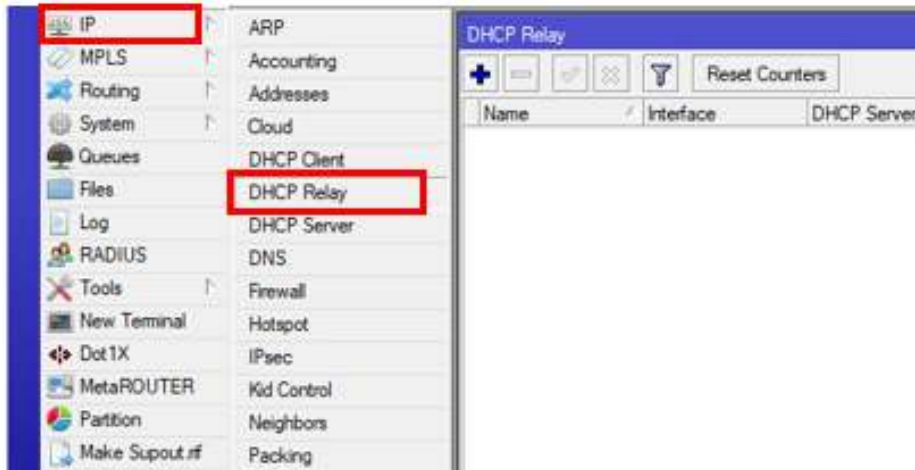


Figura 3.94 Acceso a *DCHP Relay*

R2

A continuación, se muestra la configuración de *DHCP relay* de *LAN1*, ver figura 3.95.

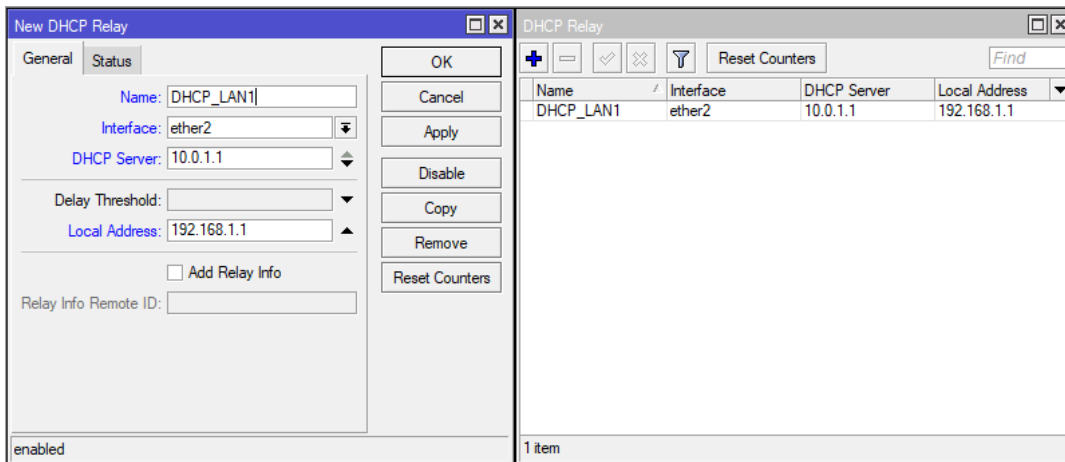


Figura 3.95 Configuración de *DHCP relay* en R2

Configuración de *DHCP client*

Para la configuración se selecciona en el menú la opción *IP/DHCP client* y a continuación se selecciona la opción (+), ver figura 3.96. Para configurar *DCHP client* se selecciona la interfaz que necesita obtener una dirección *IP* (*Interface*).

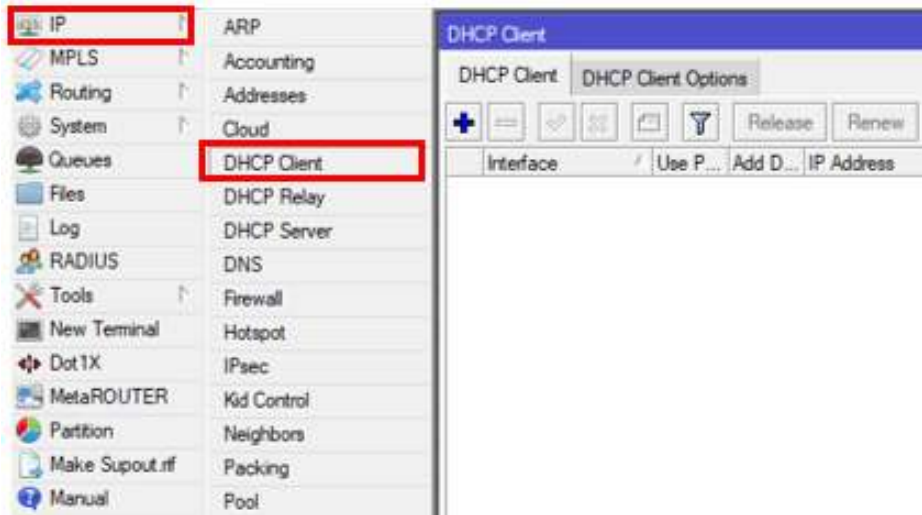


Figura 3.96 Acceso a *DHCP client*

R3

A continuación, se muestra la configuración de *DHCP client* en R3 donde se observa en este caso que la dirección *IP* 10.0.2.254/24 ha sido asignada del *DHCP server*, ver figura 3.97.



Figura 3.97 Configuración de *DHCP client* en R3

Configuración de rutas estáticas

Para la configuración se selecciona en el menú la opción *IP/Routes* y se ingresa las rutas estáticas para cada red *LAN* y *WAN* que no se encuentra conectada directamente a cada equipo.

R2

Se configura las rutas para alcanzar las redes *WAN2* y *LAN2* en R2, ver figura 3.98.

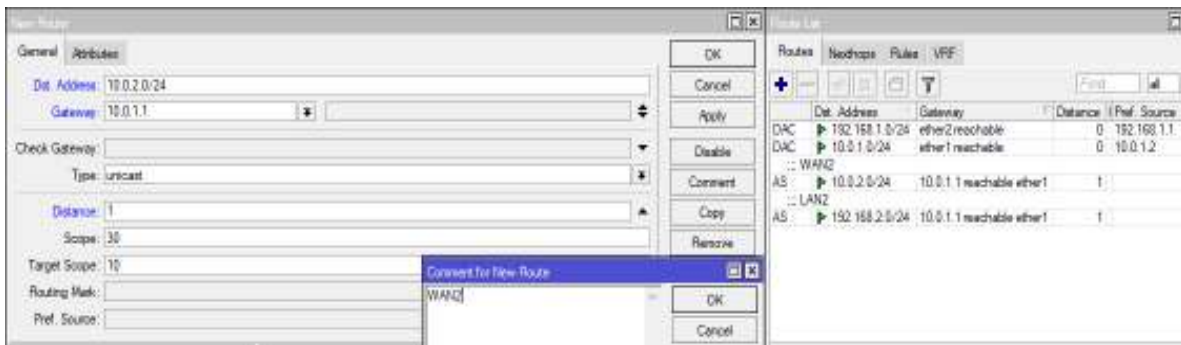


Figura 3.98 Configuración de rutas estáticas en R2

R3

Se crea una ruta por defecto con IP 0.0.0.0/0 con salida por la IP 10.0.2.1/24 ya que se implementó en este *router* el servicio de *DHCP client*, pero es necesario configurar las rutas para alcanzar las redes *WAN1* y *LAN1*. Para ello se elimina la ruta por defecto y se configura las respectivas rutas, ver figura 3.99.

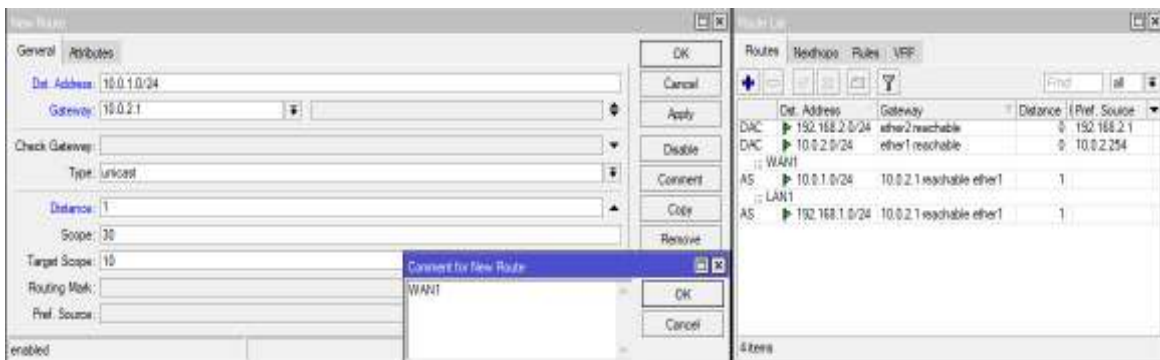


Figura 3.99 Configuración de rutas estáticas en R3

R1_central

Para la configuración es necesario verificar en la opción *Lease* la IP de arrendamiento dada por *DHCP server* al R3, en este caso la IP asignada fue 10.0.2.254/24, ver figura 3.100.

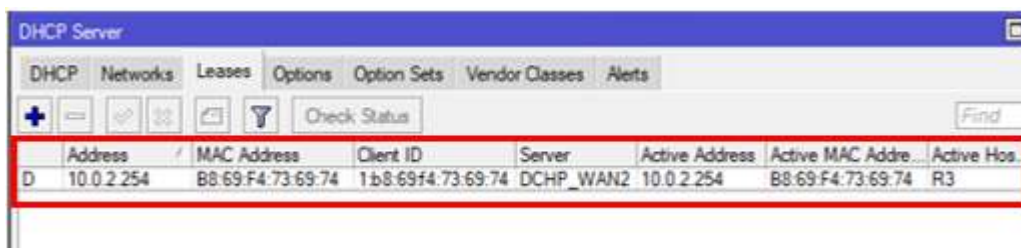


Figura 3.100 IP de arrendamiento asignada para R3

A continuación, se configura las rutas para alcanzar las redes *LAN1* y *LAN2*, ver figura 3.101.

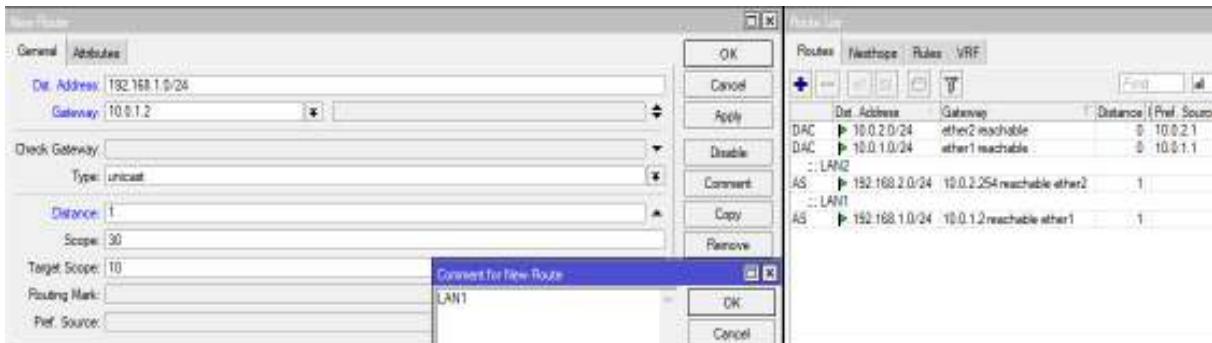


Figura 3.101 Configuración de rutas estáticas en R1_central

Configuración vía comandos

Cambio de nombre de cada *router*

- [admin@MikroTik] > system identity set name=R1_central

Configuración de interfaces *WAN* y *LAN*

Para las configuraciones de las interfaces *WAN* y *LAN* se ingresa el comando *IP address*.

R2

- [admin@R2] > IP address add address=10.0.1.2/24 comment=WAN1 interface=ether1
- [admin@R2] > IP address add address=192.168.1.1/24 comment=LAN1 interface=ether2

R3

- [admin@R3] > IP address add address=192.168.2.1/24 comment=LAN2 interface=ether2

R1_central

- [admin@R1_central] > IP address add address=10.0.1.1/24 comment=WAN1 interface=ether1
- [admin@R1_central] > IP address add address=10.0.2.1/24 comment=WAN2 interface=ether2

Creación de pool de direcciones

Para la configuración del rango de direcciones se ingresa el comando *IP pool*.

R3

- [admin@R3] > *IP pool add name=pool_LAN2 ranges=192.168.2.2-192.168.2.254*

R1_central

- [admin@R1_central] > *IP pool add name=pool_LAN1 ranges=192.168.1.2-192.168.1.254*
- [admin@R1_central] > *IP pool add name=pool_WAN2 ranges=10.0.2.2-10.0.2.254*

Configuración de DHCP server

Para la configuración de *DHCP server* se ingresa el comando *IP DHCP-server*.

R3

- [admin@R3] > *IP DHCP-server add name=DHCP_LAN2 interface=ether2 address-pool=pool_LAN2 lease-time=00:10:00*

Ahora se configura la red para *LAN2* en *DHCP server*.

- [admin@R3] > *IP DHCP-server network add address=192.168.2.0/24 gateway=192.168.2.1 comment=LAN2*

R1_central

- [admin@R1_central] > *IP DHCP-server add name=DHCP_WAN2 interface=ether2 address-pool=pool_WAN2 lease-time=00:10:00*

Para la configuración de *DHCP server* con la habilitación de *DHCP relay* para *LAN1*.

- [admin@R1_central] > *IP DHCP-server add name=DHCP_LAN1 interface=ether1 relay=192.168.1.1 address-pool=pool_LAN1 lease-time=00:10:00 disable=no*

Ahora se configura la red para *WAN2* y *LAN1* en *DHCP server*.

- [admin@R1_central] > *IP DHCP-server network add address=10.0.2.0/24 gateway=10.0.2.1 comment=WAN2*
- [admin@R1_central] > *IP DHCP-server network add address=192.168.1.0/24 gateway=192.168.1.1 comment=LAN1*

Configuración de amarre IP/MAC

Para configurar la reserva de *IP/MAC* se ingresa el comando *IP DHCP-server lease*.

R3

- [admin@R3] > `IP DHCP-server lease add address=192.168.2.77 mac-address=38:60:77:b0:ee:ae server=DHCP_WAN2 comment=impresora`

Configuración de DHCP relay

Para la configuración de *DHCP relay* se ingresa el comando

R2

- [admin@R2] > `IP DHCP-relay add name=DHCP_LAN1 interface=ether2 DHCP-server=10.0.1.1 local-address=192.168.1.1 disable=no`

Configuración de DHCP Client

Para la configuración *DHCP Client* se ingresa el comando *IP DHCP-client*

R3

- [admin@R3] > `IP DHCP-client add interface=ether1 comment=DHCP_client_R3`

Configuración de rutas estáticas

Para la configuración se ingresa el comando *IP route*.

R2

- [admin@R2] > `IP route add distance=1 dst-address=10.0.2.0/24 gateway=10.0.1.1 comment=WAN2`
- [admin@R2] > `IP route add distance=1 dst-address=192.168.2.0/24 gateway=10.0.1.1 comment=LAN2`

R3

- [admin@R3] > `IP route add distance=1 dst-address=10.0.1.0/24 gateway=10.0.2.1 comment=WAN1`
- [admin@R3] > `IP route add distance=1 dst-address=192.168.1.0/24 gateway=10.0.2.1 comment=LAN1`

R1_central

- [admin@R1_central] > `IP route add distance=1 dst-address=192.168.1.0/24 gateway=10.0.1.2 comment=LAN1`
- [admin@R1_central] > `IP route add distance=1 dst-address=192.168.2.0/24 gateway=10.0.2.254 comment=LAN2`

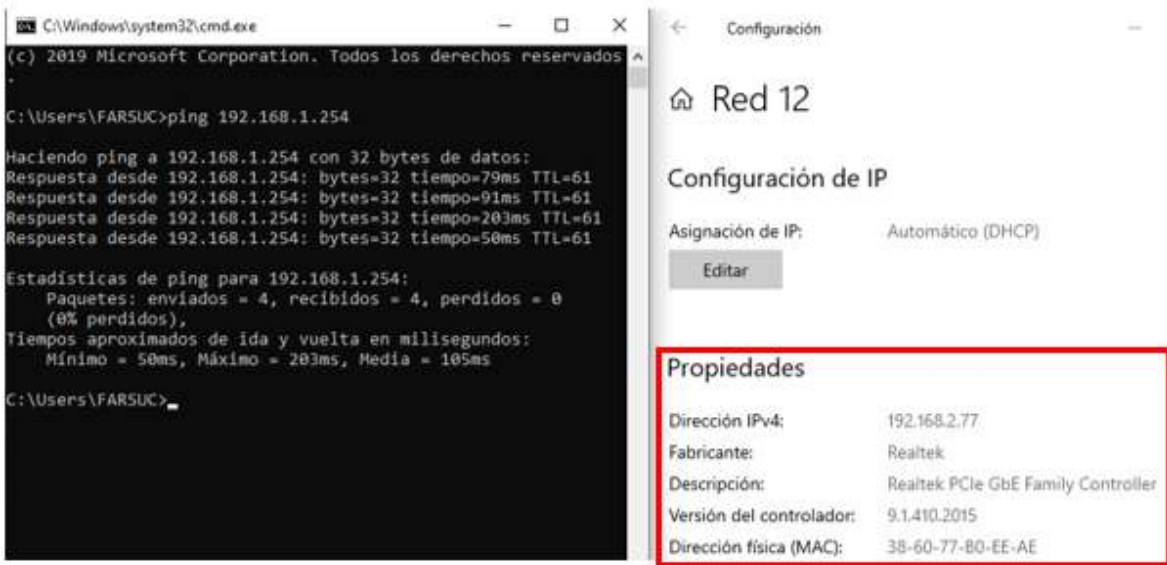


Figura 3.104 Prueba de conectividad entre LAN1 y LAN2

❖ Práctica N°4

Tema: *DNS server, cache, transparente*

Objetivo: Configuración de *DNS* en *router MikroTik*.

Objetivos Específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*
- Configuración de interfaces *WAN* y *LAN*
- Configuración de *DNS server, cache* y *transparente*
- Configuración de acceso a internet
- Configuración de *DHCP Server*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

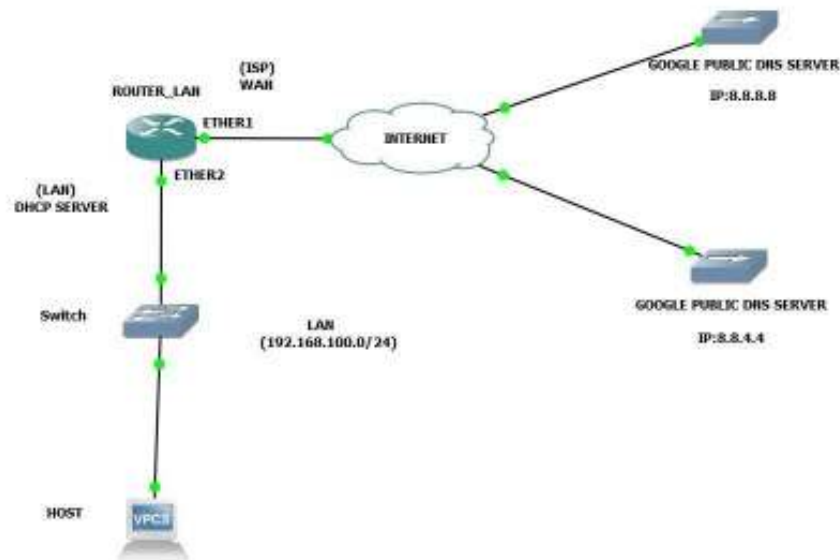


Figura 3.105 Topología de *DNS server, cache* y *transparente*

Tabla de direcciones *IP*

A continuación, se muestra la tabla 3.10 de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Tabla 3.10 Direccionamiento IP en redes WAN, LAN y hosts

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
WAN	ISP	ISP	R1(Ether1)	ISP	ISP
LAN	192.168.100.0	/24	R1(Ether2)	192.168.100.1	/24

Configuración vía interfaz gráfica

Cambio de nombre en el router

Para el cambio de nombre ingresamos *System/Identity*, ver figura 3.106.

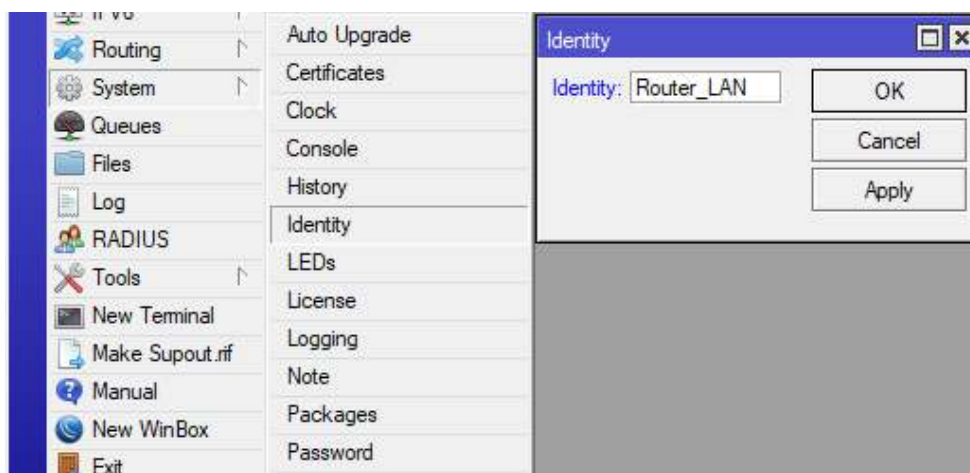


Figura 3.106 Identificación de router

Configuración de interfaces WAN y LAN

Para la configuración se selecciona en el menú la opción *IP/Addresses* y se ingresa las direcciones IP en cada equipo. Se configura las interfaces de ether 1 y 2 para WAN y LAN, ver figura 3.107.

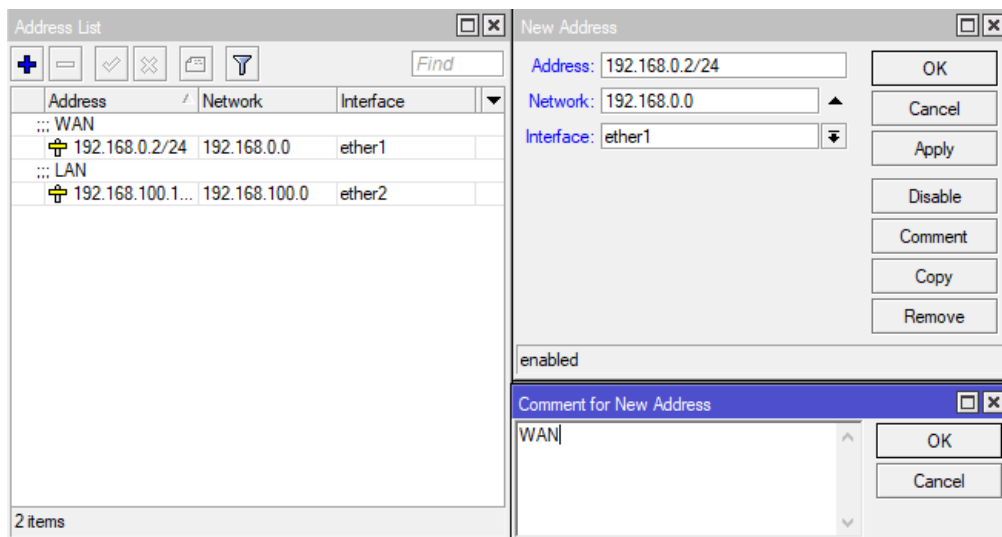


Figura 3.107 Configuración de interfaces en router

Configuración de DNS Server y Cache

Para la configuración se selecciona en el menú la opción *IP/DNS*, ver figura 3.108.

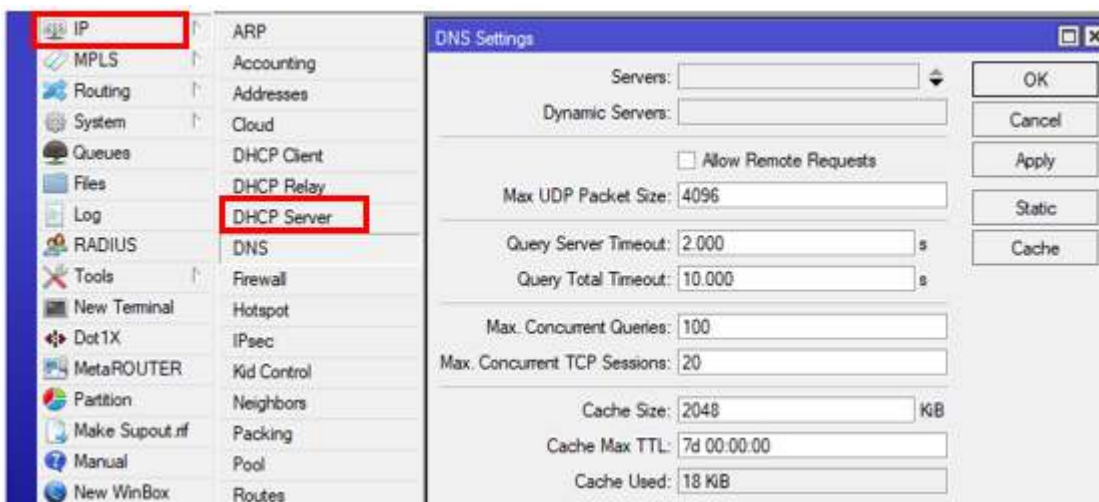


Figura 3.108 Acceso a DNS Server

A continuación, se coloca la *DNS* primaria 8.8.8.8 y secundaria 8.8.4.4 que corresponden a las *Google Public DNS* server y se activa la opción *Allow Remote Request* para habilitar el *DNS Cache*. Se da en *Apply* y *OK*, ver figura 3.109.

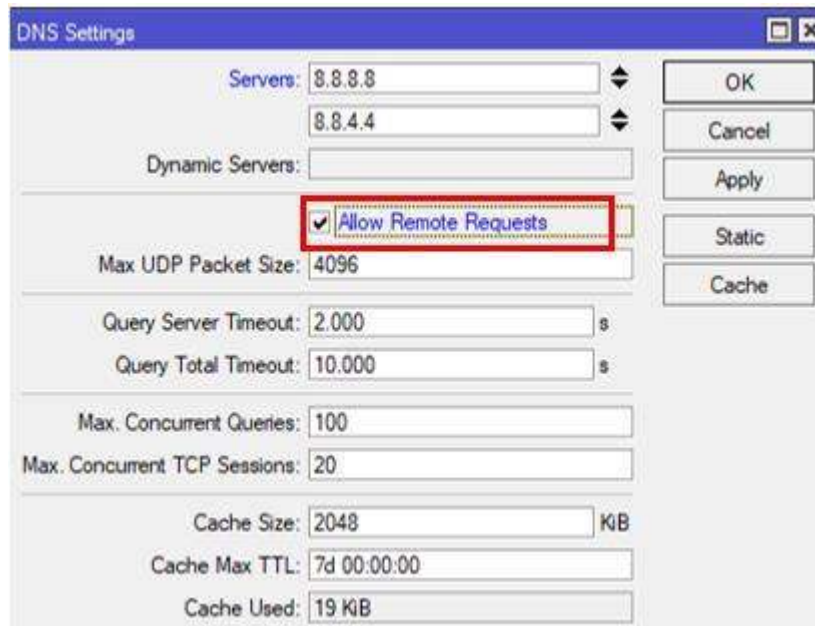


Figura 3.109 Configuración de *DNS server* y *cache*

Configuración de *DNS* transparente

Para la configuración de *DNS* transparente es necesario ingresar a la opción *IP/Firewall*, ver figura 3.110.

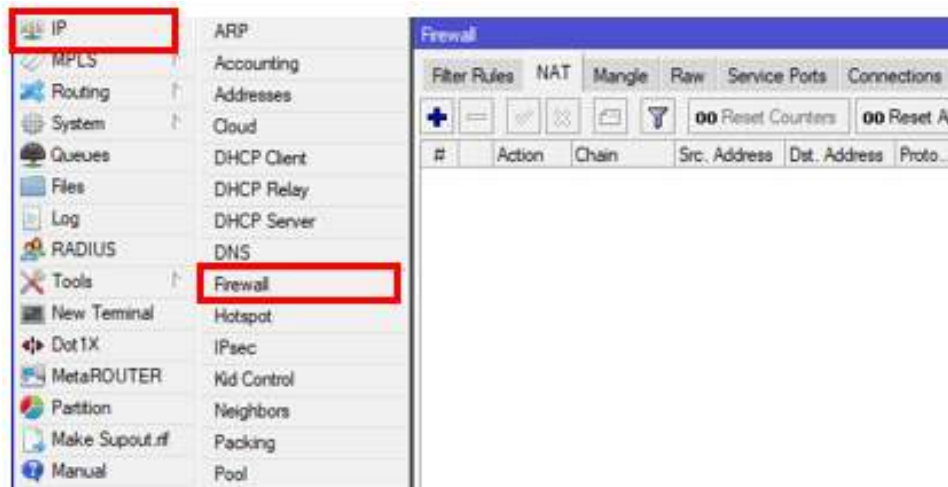


Figura 3.110 Acceso a *Firewall*

A continuación, se ingresa a la opción *NAT* y se elige la opción (+). En *General* en el casillero *Chain* se coloca *dstnat* que indica los paquetes que tiene como destino una red *LAN*. En el casillero *Protocolo* se selecciona el protocolo con el que trabaja *DNS*. *DNS* utiliza los protocolos *UDP* y *TCP* para responder las consultas. En el casillero *Dst. Port* se ingresa el puerto en que trabaja *DNS* el cual es el número 53. En *Action* en el

casillero *Action* se elige la opción *redirect* que indica que se va a redireccionar las peticiones *DNS* y en el casillero *To Ports* se coloca el puerto 53. Configuración para el protocolo *UDP*, ver figura 3.111.

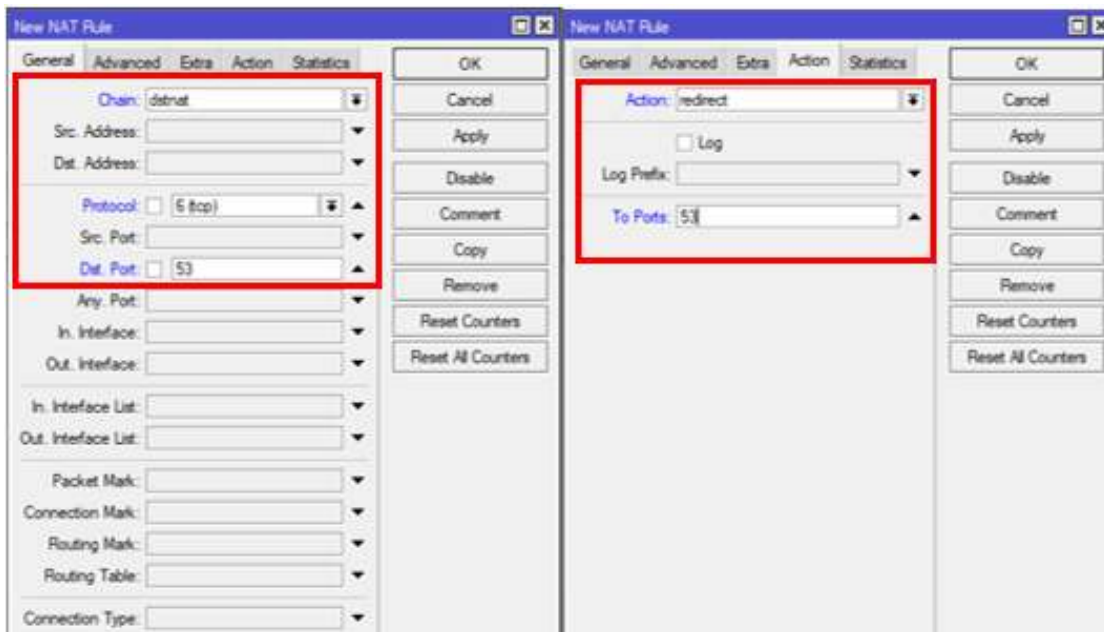


Figura 3.111 Configuración de protocolo *TCP*

Configuración para el protocolo *TCP*, ver figura 3.112.

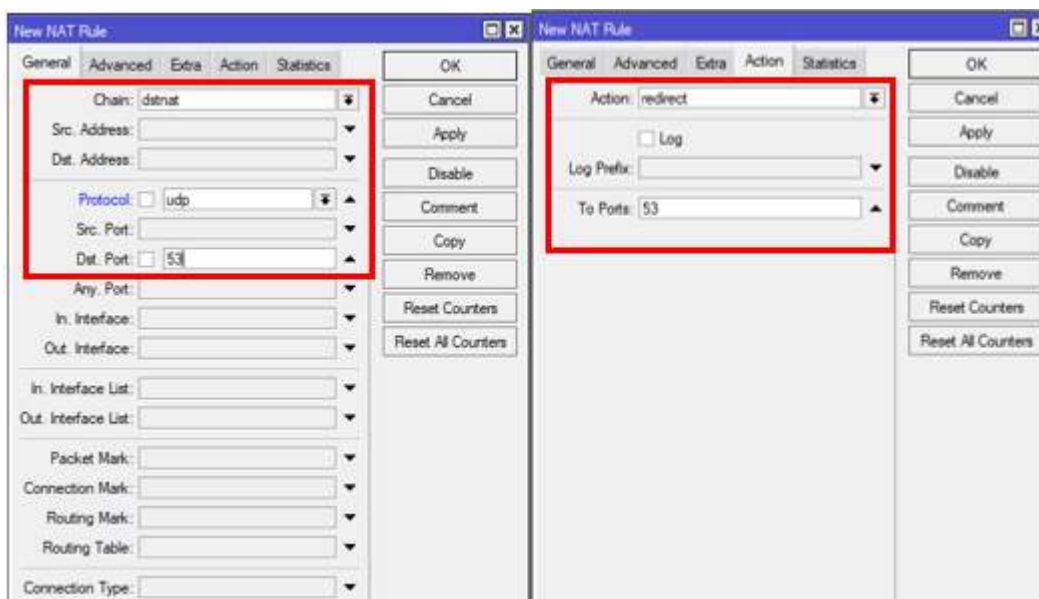


Figura 3.112 Configuración de protocolo *UDP*

Una vez configurado los protocolos *UDP* y *TCP* se registra una lista en *NAT*, ver figura 3.113.

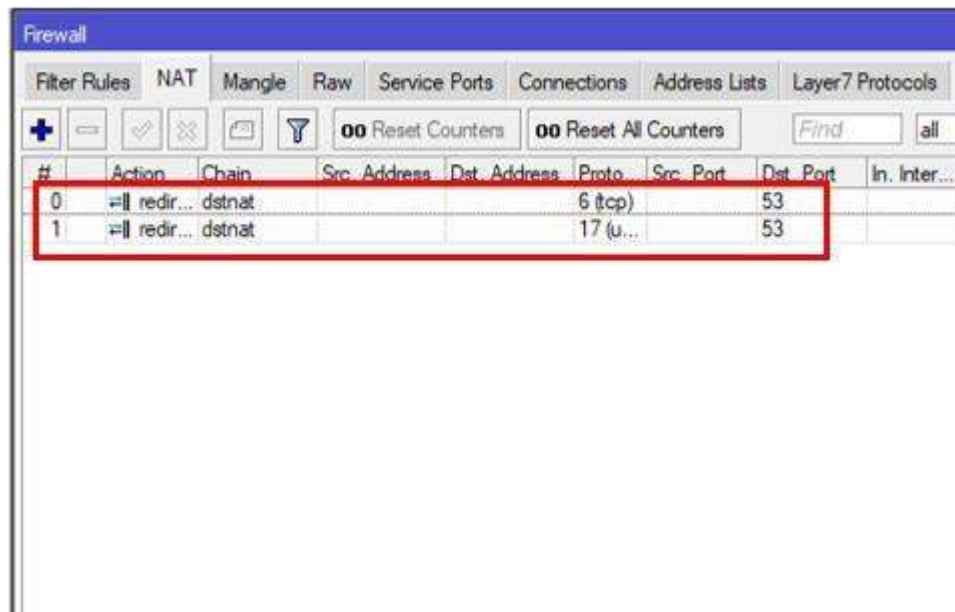


Figura 3.113 Configuración de *DNS* Transparente

Configuración de acceso a Internet

Para tener acceso a Internet se selecciona la opción *IP/Routes* y se selecciona la opción (+). A continuación, es necesario crear una ruta para la salida de paquetes, para ello se crea una ruta por defecto *0.0.0.0/0* (*Dts. Address*) y una *IP* de salida (*gateway*). En este caso el enlace *WAN* en el extremo del *ISP* tiene la dirección *IP* *192.168.0.1/24*, ver figura 3.114.



Figura 3.114 Configuración de ruta para acceso a Internet

Ahora se debe realizar el enmascaramiento de nuestra red local LAN para tener salida a Internet. Para ello es necesario ir a *IP/Firewall* y en la opción de *NAT* en *General*, en el casillero *Chain* colocamos *srcnat* que indica los paquetes originados en la red LAN. En el casillero *Out. Interface* se coloca la interfaz que está conectada con la red WAN, que es la salida a Internet. En *Action* en el casillero *Action* se elige la opción *masquerade*, ver figura 3.115.

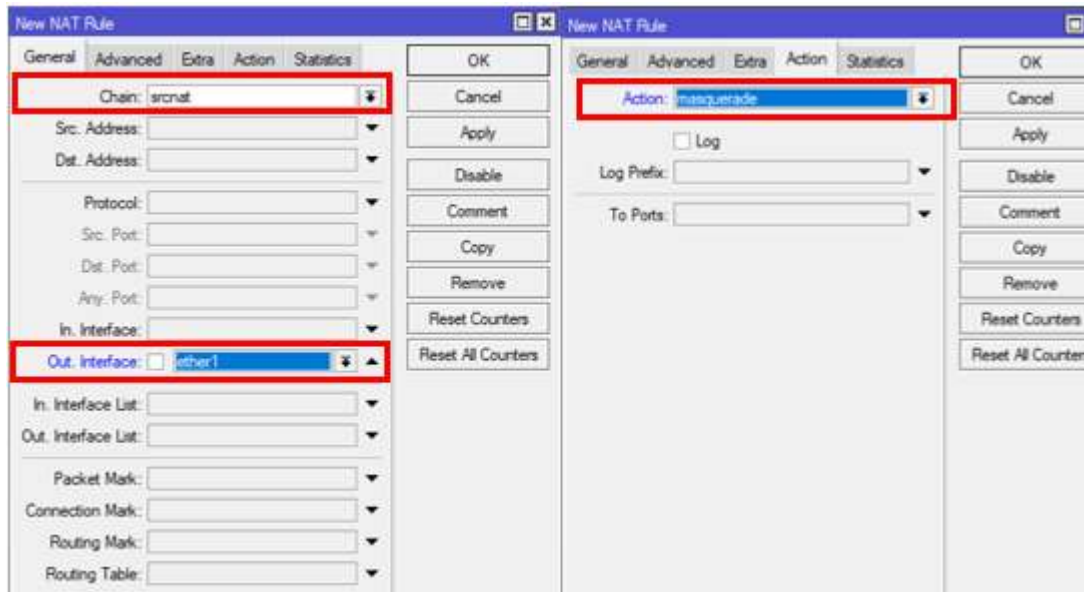


Figura 3.115 Configuración de enmascaramiento

Ahora se observa la lista de configuraciones realizadas en *NAT*, ver figura 3.116.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	redir...	dstnat			6 (tcp)		53		
1	redir...	dstnat			17 (u...)		53		
2	mas...	srcnat							ether1

Figura 3.116 Lista de configuración NAT

Configuración *DHCP* server

Para la configuración de *DHCP* server se ingresa a *IP/DHCP* server. *WinBox* da una opción de configuración rápida para el servidor *DHCP*, para ello se elige la opción *DHCP Setup*, ver figura 3.117.

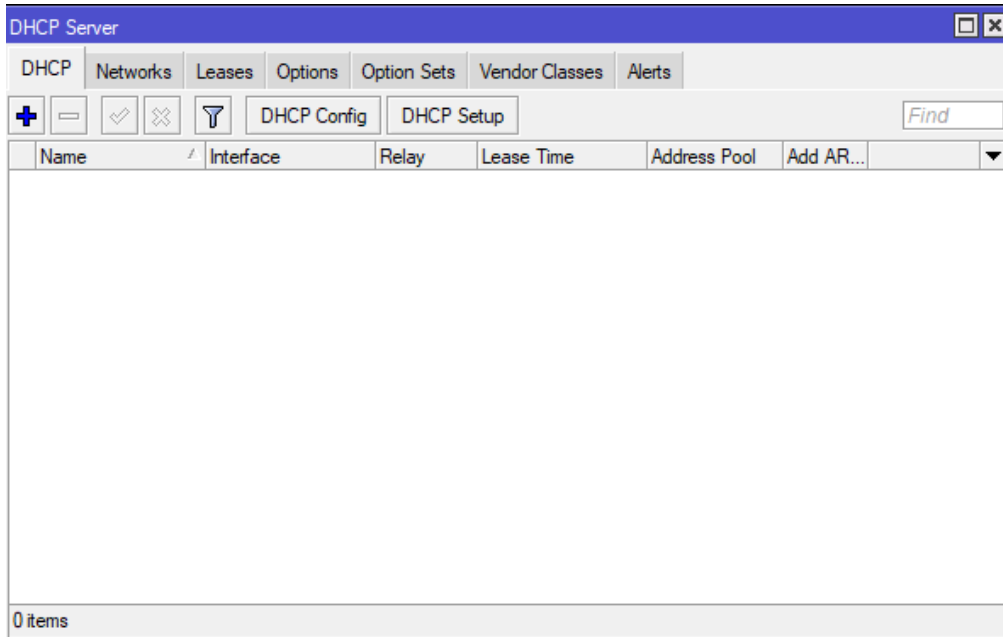


Figura 3.117 Acceso a *DHCP Setup*

A continuación, se visualiza una nueva ventana donde se ingresa la interfaz donde se va a implementar el servidor *DHCP* (*DHCP Server Interface*), en este caso se coloca la interfaz de la red *LAN*, ver figura 3.118.

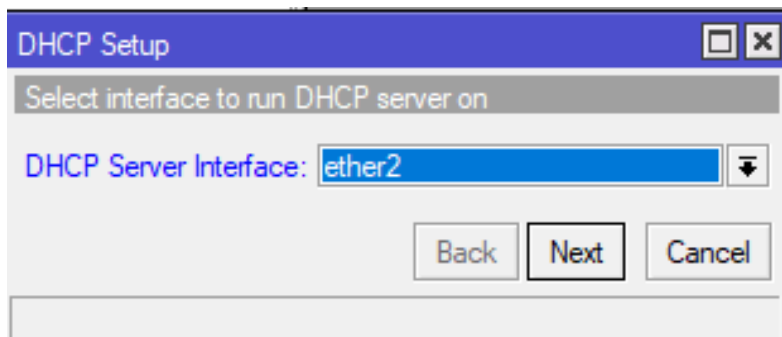


Figura 3.118 Interfaz de red *LAN*

Luego se ingresa la *IP* 192.168.100.0/24 que pertenece a la red *LAN* (*DHCP Address Space*), ver figura 3.119.

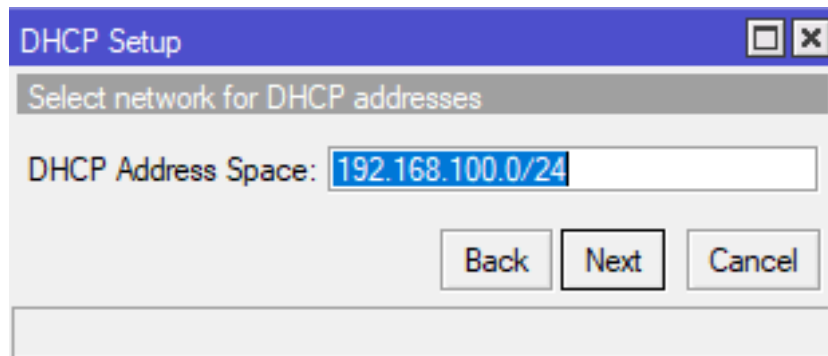


Figura 3.119 IP de red LAN

Ahora se ingresa la dirección IP 192.168.100.1 que corresponde a la interfaz de la red LAN (Gateway for DHCP Network), ver figura 3.120.

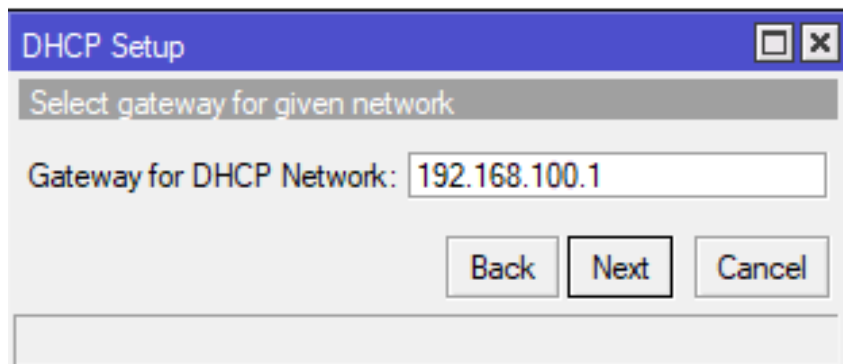


Figura 3.120 IP de interfaz de red LAN

A continuación, se ingresa el rango de direcciones IP que va a arrendar el servidor DHCP, en este caso se coloca desde la dirección 192.168.100.2 hasta 192.168.100.254, ve figura 3.121.

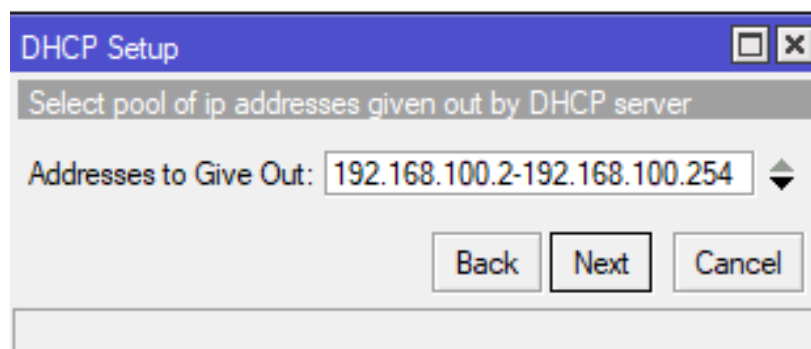


Figura 3.121 Rango de direcciones IP

Luego se visualiza una ventana donde *DHCP setup* toma las *DNS* configuradas previamente en *DNS server*, ver figura 3.122.

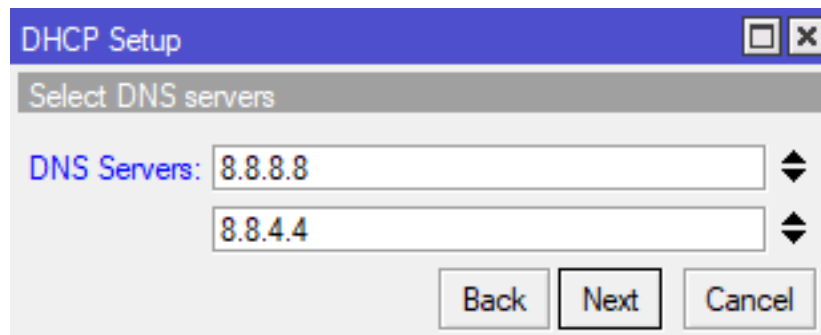


Figura 3.122 Configuración *DNS*

Y por último se ingresa el tiempo de arrendamiento de direcciones *IP* (*Lease Time*), ver figura 3.223.

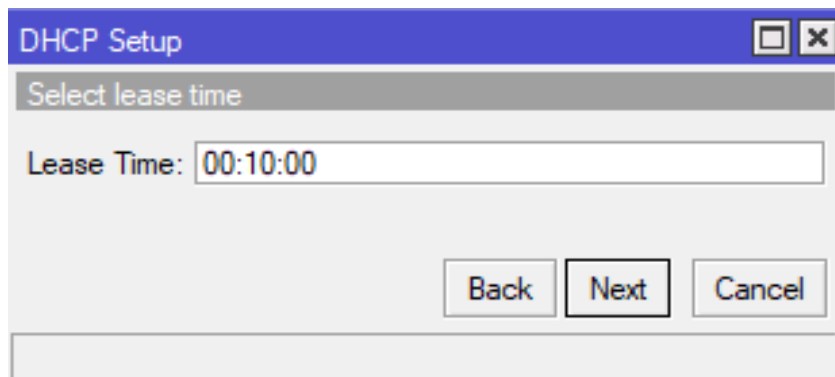


Figura 3.223 Tiempo de arrendamiento de direcciones *IP*

Configuración vía comandos

Cambio de nombre de cada *router*

- [admin@Router_LAN] > system identity set name=Router

Configuración de interfaces *WAN* y *LAN*

Para su configuración se ingresa el comando *IP address*

- [admin@Router_LAN] > IP address add address=192.168.0.2/24
comment=WAN interface=ether1
- [admin@Router_LAN] > IP address add address=192.168.100.1/24
comment=LAN interface=ether2

Configuración de DNS Server y Cache

Para la configuración de *DNS server* y *cache* se ingresa el comando *IP dns*.

- [admin@Router_LAN] > IP dns set servers=8.8.8.8,8.8.4.4 allow-remote-requests=yes

Configuración de DNS transparente

Para la configuración de *DNS transparente* se ingresa el comando *IP firewall*.

- [admin@Router_LAN] > IP firewall nat add chain=dstnat protocol=tcp dst-port=53 action=redirect to-ports=53
- [admin@Router_LAN] > IP firewall nat add chain=dstnat protocol=udp dst-port=53 action=redirect to-ports=53

Configuración de acceso a Internet

Para el acceso a Internet se crea una ruta por defecto ingresando el comando *IP route*.

- [admin@Router_LAN] > IP route add distance=1 dst-address=0.0.0.0/0 gateway=192.168.0.1 comment=Acceso_a_Internet

Ahora se ingresa el comando *IP firewall* para el enmascaramiento de los paquetes de la red *LAN*.

- [admin@Router_LAN] > IP firewall nat add action=masquerade chain=srcnat out-interface=ether1

Configuración DHCP Server

Para la configuración de *DHCP Server* se ingresa el comando *IP DHCP-server*.

- [admin@Router_LAN] > IP DHCP-server setup
- Select interface to run DHCP server on
- DHCP server interface: ether2
- Select network for DHCP addresses
- DHCP address space: 192.168.100.0/24
- Select gateway for given network
- gateway for DHCP network: 192.168.100.1
- Select pool of IP addresses given out by DHCP server
- addresses to given out: 192.168.100.2-192.168.100.254
- Select DNS servers
- dns servers: 8.8.8.8,8.8.4.4

- Select lease time
- lease time: 10m

Pruebas de conectividad en equipos y *hosts*

Se realizó las pruebas de conectividad en toda la red por medio de la utilización del comando *ping*, para ello es necesario ingresar al *CMD* de *Windows*.

La primera prueba realizada es la verificación de arrendamiento de una *IP* en el *host* y la redirección de las peticiones *DNS* hacia el *router* por medio del comando *IPconfig /all* en *CMD*, ver figura 3.124.

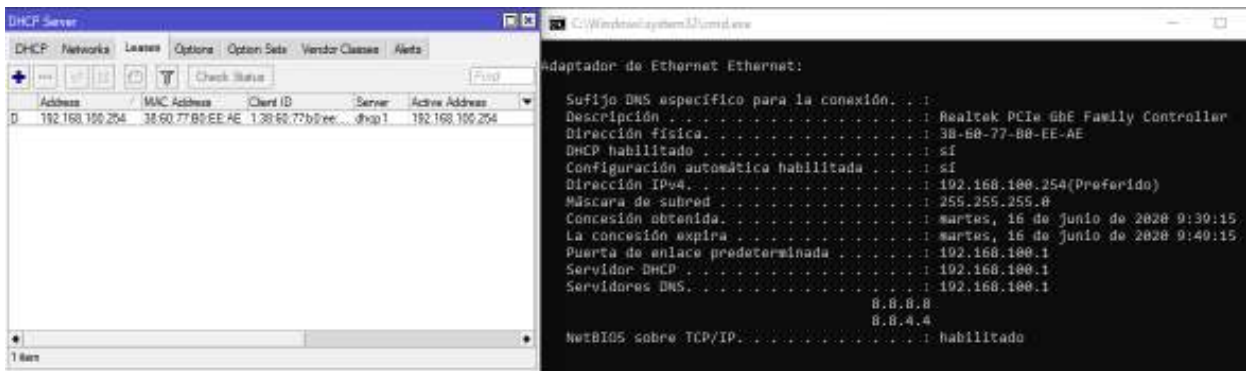


Figura 3.124 Prueba de arrendamiento de *IP* en *host*

La segunda prueba realizada es el cambio manual de la *DNS* en el *host*, en esta ocasión se ingresa el valor 1.2.3.4 y aunque tenga una dirección *DNS* no válida va a tener acceso al *host* a internet debido a que toda petición generada en el computador se redirige al *router*, ver figura 3.125.

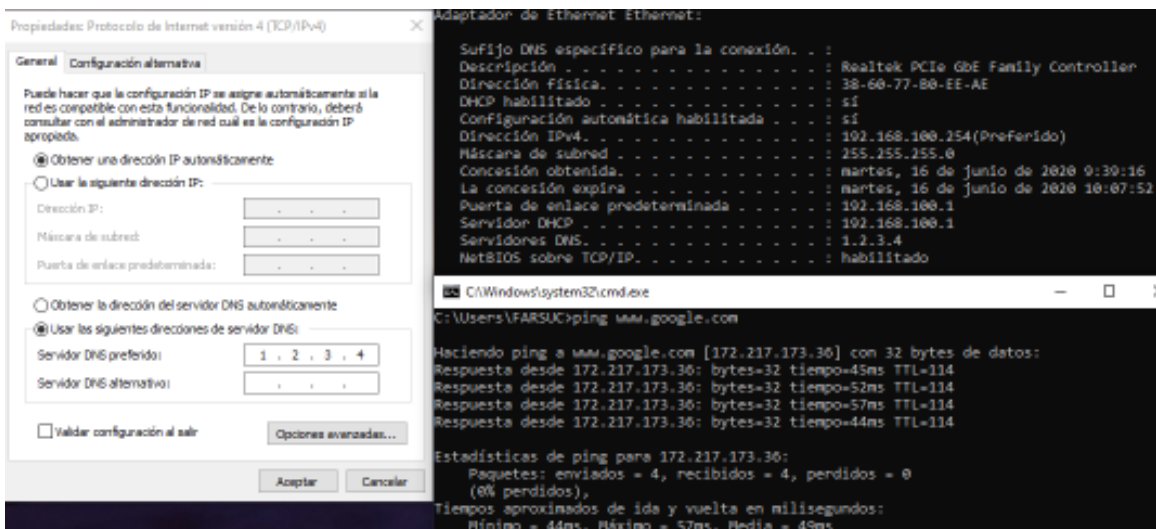


Figura 3.125 Prueba de cambio de DNS en *host*

La tercera prueba realizada es la generación del *DNS cache* cada vez que se realice *ping* a una página *web* ver figura 3.126.

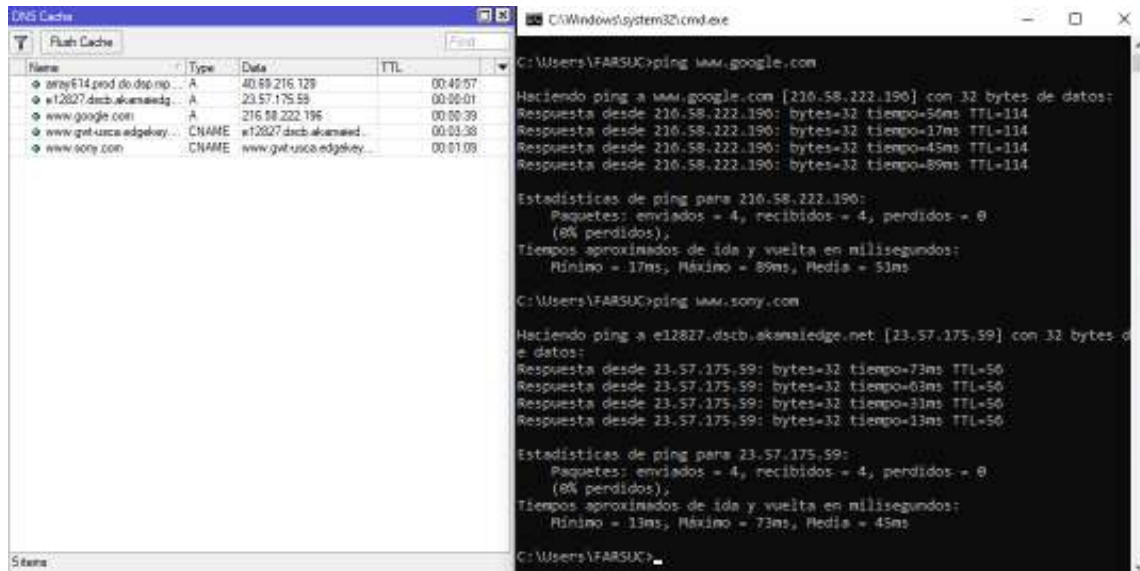


Figura 3.126 Prueba de conectividad entre *LAN1* y *LAN2*

❖ Práctica N°5

Tema: Protocolo de enrutamiento *BGP*

Objetivo: Configuración de protocolo de enrutamiento *BGP* en *routers MikroTik*

Objetivos Específicos:

- Diseñar una topología de red con equipos *MikroTik*
- Configuración de interfaces *WAN* y *LAN*
- Configuración de *BGP*
- Configuración *DHCP* en interfaces *LAN*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

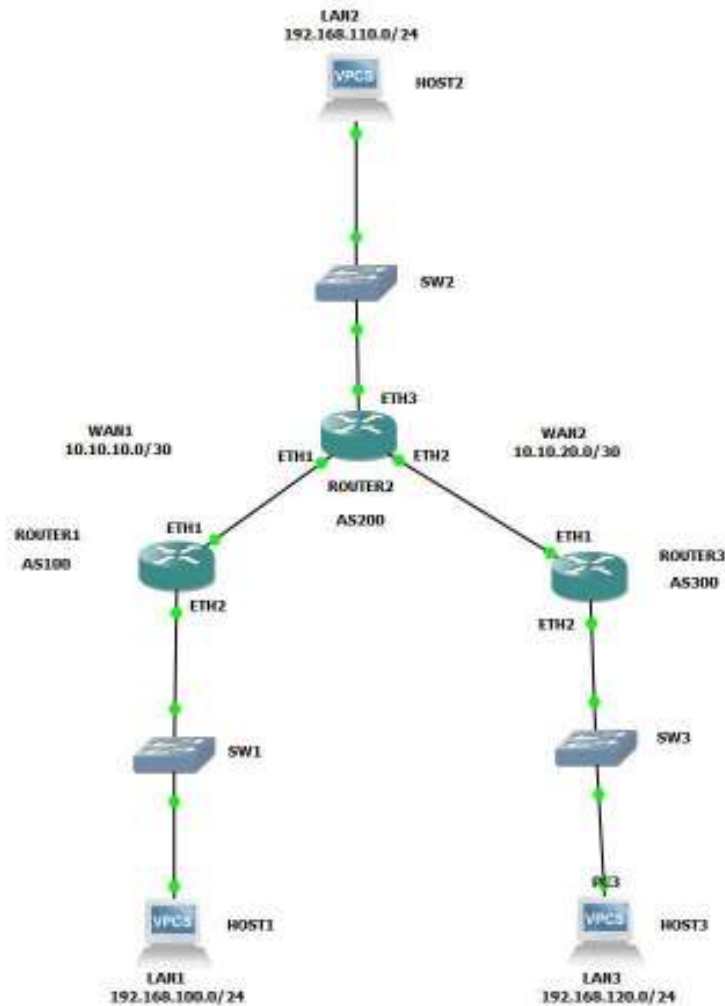


Figura 3.127 Topología de *BGP*

Tabla de direcciones *IP*

A continuación, se muestra la tabla 3.11 de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Tabla 3.11 Direccionamiento *IP* en redes *WAN*, *LAN*

Nombre de red	Red	Máscara	Interfaz	Dirección <i>IP</i>	Máscara
<i>WAN1</i>	10.10.10.0	/30	R1(Ether1)	10.10.10.1	/30
			R2(Ether1)	10.10.10.2	/30
<i>WAN2</i>	10.10.20.0	/30	R2(Ether2)	10.10.20.1	/30
			R3(Ether1)	10.10.20.2	/30
<i>LAN1</i>	192.168.100.0	/24	R1(Ether2)	192.168.100.1	/24
<i>LAN2</i>	192.168.110.0	/24	R2(Ether3)	192.168.110.1	/24
<i>LAN3</i>	192.168.120.0	/24	R3(Ether2)	192.168.120.1	/24

Tabla de sistemas autónomos

A continuación, se muestra la tabla 3.12 de sistemas autónomos en *routers*.

Tabla 3.12 Tabla de sistemas autónomos

Nombre	<i>Router</i>
AS100	R1
AS200_R1	R2
AS200_R3	R2
AS300	R3

Configuración vía interfaz gráfica

Cambio de nombre en el router

Para el cambio de nombre ingresamos *System/Identity*, ver figura 3.128.

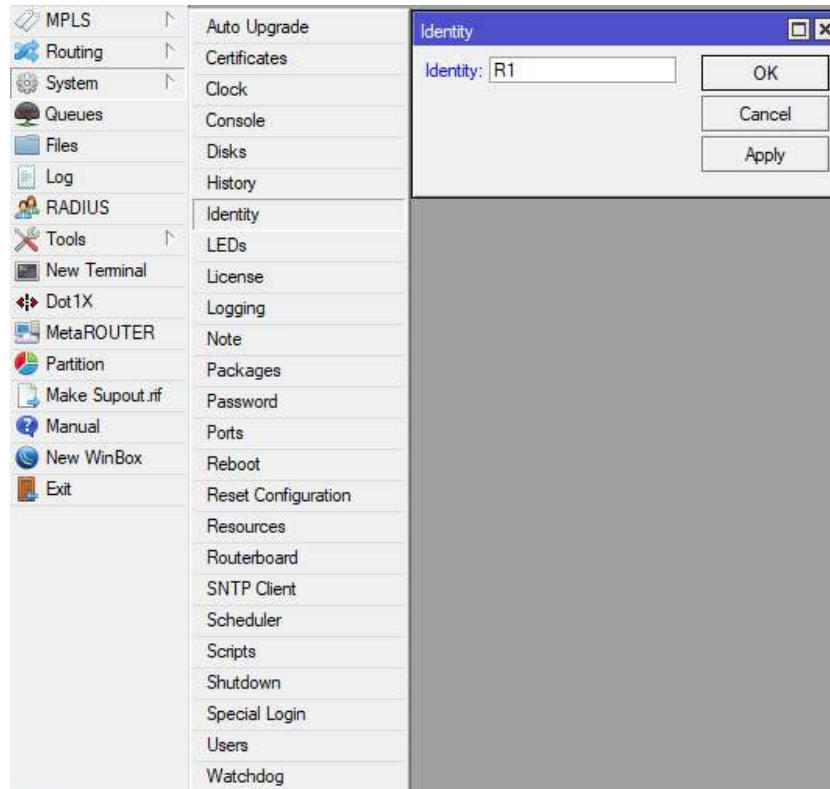


Figura 3.128 Identificación de *router*

Configuración de interfaces WAN y LAN.

Para la configuración se selecciona en el menú la opción *IP/Addresses* y se ingresa las direcciones *IP* de cada interfaz *WAN* y *LAN* con su respectivo comentario.

R1

Se levanta la interfaz *WAN1* con la dirección 10.10.10.1/30 y *LAN1* con la dirección 192.168.100.1/24, ver figura 3.129.

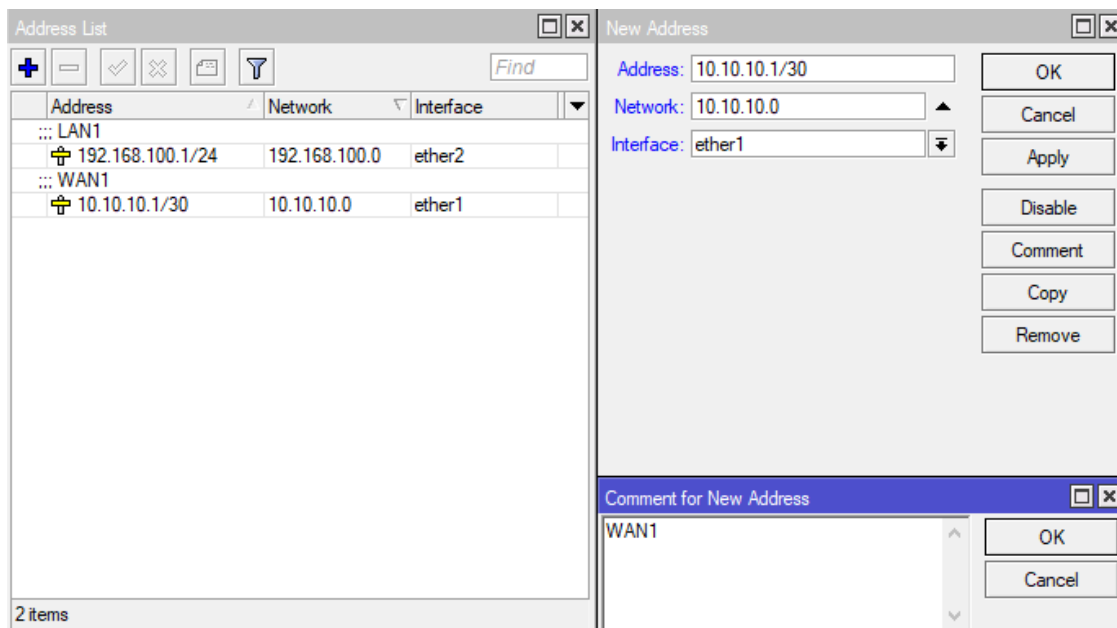


Figura 3.129 Configuración de interfaces en R1

R2

Se levanta la interfaz *WAN1* con la dirección 10.10.10.2/30, *WAN2* con la dirección 10.10.20.1/30 y *LAN2* con la dirección 192.168.110.1/24, ver figura 3.130.

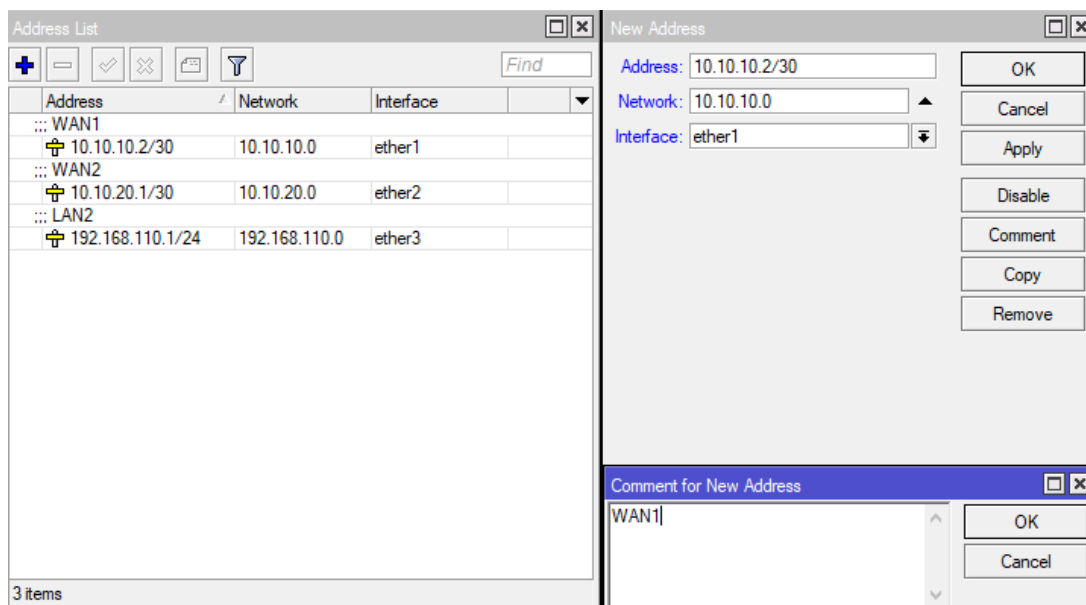


Figura 3.130 Configuración de interfaces en R2

R3

Se levanta la interfaz *WAN2* con la dirección 10.10.20.2/30 y *LAN3* con la dirección 192.168.120.1/24, ver figura 3.131.

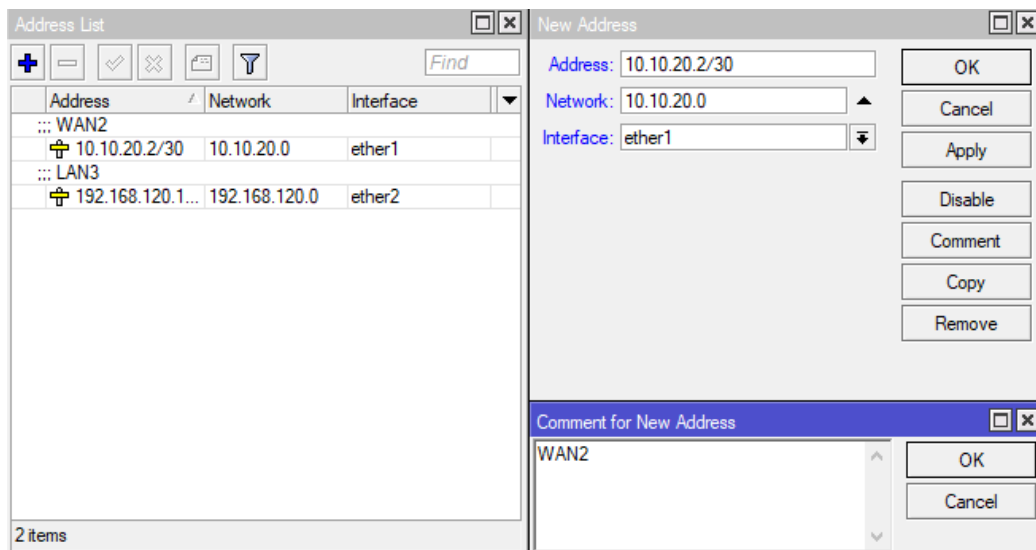


Figura 3.131 Configuración de interfaces en R3

Configuración de BGP

El protocolo *BGP* se encarga del intercambio de información de enrutamiento entre sistemas autónomos. Para la configuración de *BGP* se selecciona en el menú la opción *Routing/BGP*. En el casillero *Instances* viene predefinido un sistema autónomo por default, el cual no puede ser eliminado, por lo que se lo deshabilita y se crea uno nuevo. Ahora se elige la opción (+) y se ingresa el nombre (*Name*), el valor del sistema autónomo (*AS*) y la interfaz *WAN* de cada *router* (*Router ID*).

R1

Se ingresa el nombre del sistema autónomo AS100, el valor del sistema autónomo 100 y la dirección *IP* 10.10.10.1 que comunica con *WAN1*, ver figura 3.132.

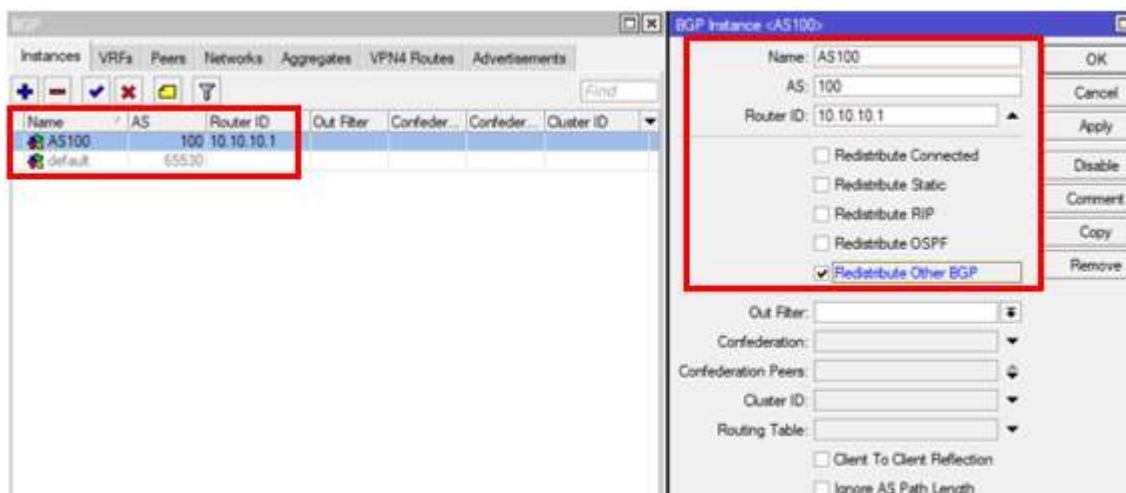


Figura 3.132 Configuración del sistema autónomo en R1

R2

Se ingresa el nombre del sistema autónomo AS200_R1, el valor del sistema autónomo 200 y la dirección IP 10.10.10.2 que comunica con WAN1, ver figura 3.133.

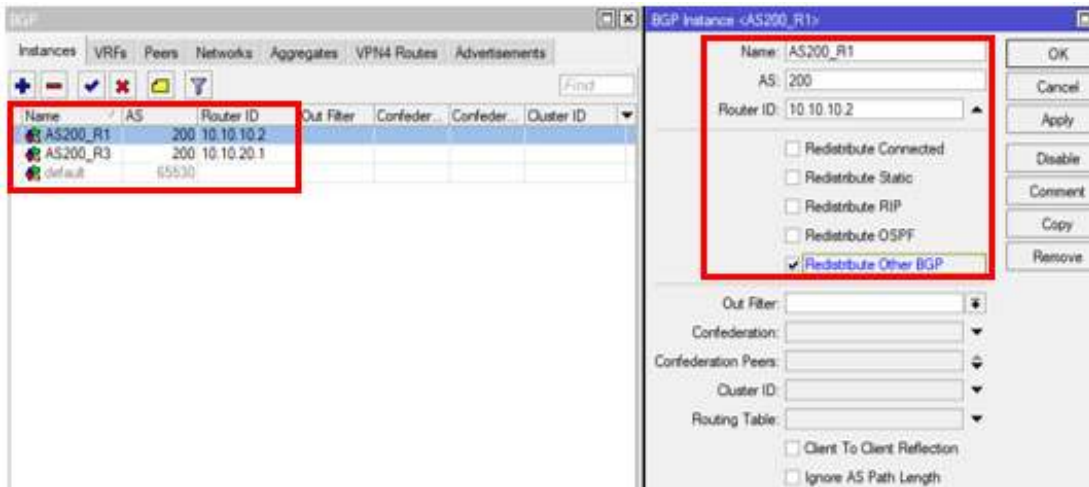


Figura 3.133 Configuración del sistema autónomo en R2 para R1

Ahora se crea un nuevo sistema autónomo con el nombre AS200_R3, el mismo valor del sistema para R2 y la dirección IP 10.10.20.1 que comunica con WAN2, ver figura 3.134.

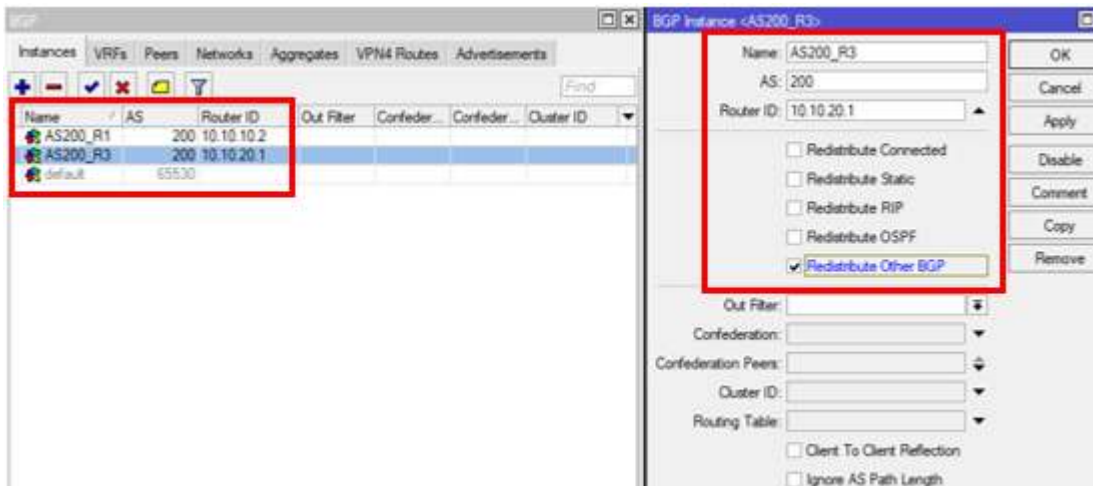


Figura 3.134 Configuración del sistema autónomo en R2 para R3

R3

Se ingresa el nombre del sistema autónomo AS300, el valor del sistema autónomo 300 y la dirección IP 10.10.20.2 que comunica con WAN2, ver figura 3.135.

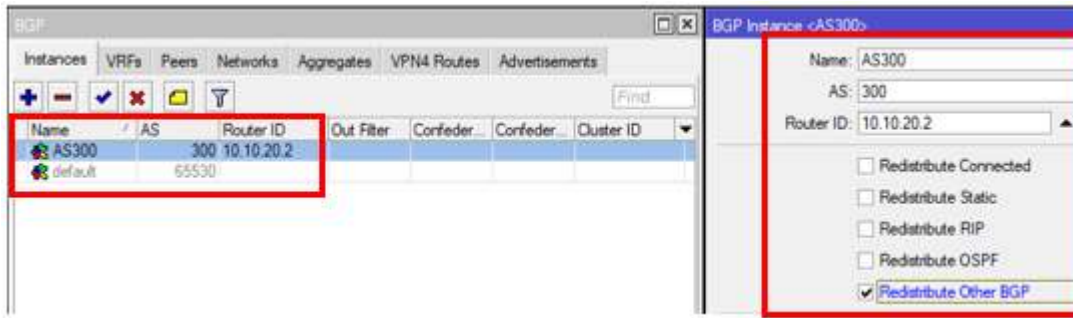


Figura 3.135 Configuración del sistema autónomo en R3

A continuación, en el casillero *Peers* se selecciona la opción (+) donde se aprecia una nueva ventana donde se configurará la comunicación entre sistemas autónomos. Para ello ingresa el nombre de relación par entres *routers* (*Name*), se selecciona la instancia anteriormente configurada que corresponde al *router* (*Instance*), se ingresa la dirección *IP* correspondiente a la interfaz del *router* vecino donde se está realizando la relación par (*Remote Address*). Ahora se ingresa el valor del sistema autónomo del *router* vecino de la relación par (*Remote AS*).

R1

Se ingresa el nombre de la relación par R1-R2 (*Name*), se selecciona la instancia AS100 (*Instance*), se ingresa la dirección *IP* 10.10.10.2 (*Remote Address*) y se ingresa el valor 200 (*Remote AS*), ver figura 3.136.

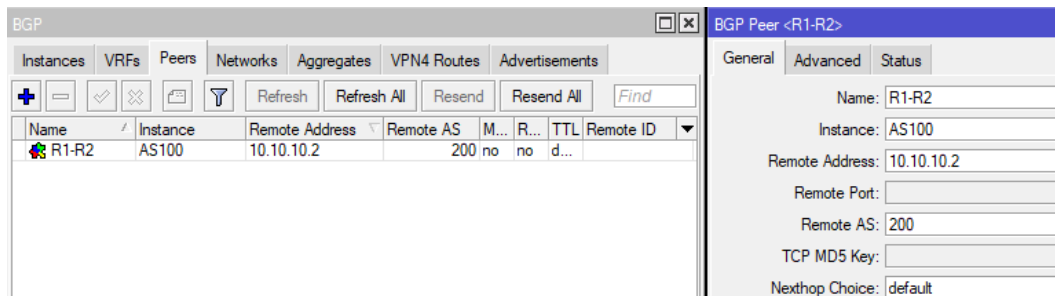


Figura 3.136 Configuración de relación par entre R1 y R2

R2

Se ingresa el nombre de la relación par R2-R1 (*Name*), se selecciona la instancia AS200_R1 (*Instance*), se ingresa la dirección *IP* 10.10.10.1 (*Remote Address*) y se ingresa el valor 100 (*Remote AS*), ver figura 3.137.

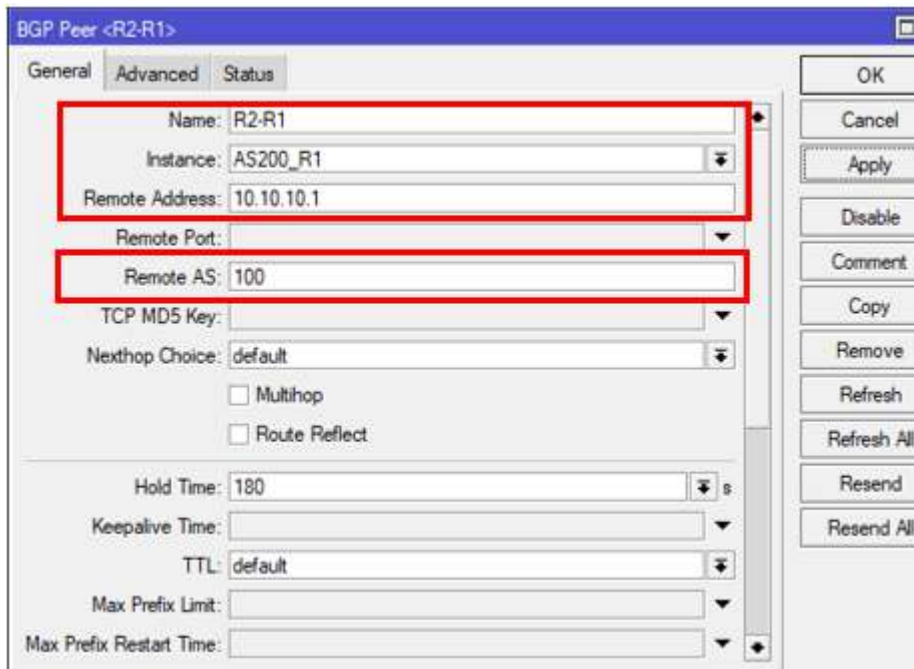


Figura 3.137 Configuración de relación par entre R2 y R1

Ahora se ingresa el nombre de la relación par R2-R3 (*Name*), se selecciona la instancia AS200_R3 (*Instance*), se ingresa la dirección IP 10.10.20.2 (*Remote Address*) y se ingresa el valor 300 (*Remote AS*), ver figura 3.138.

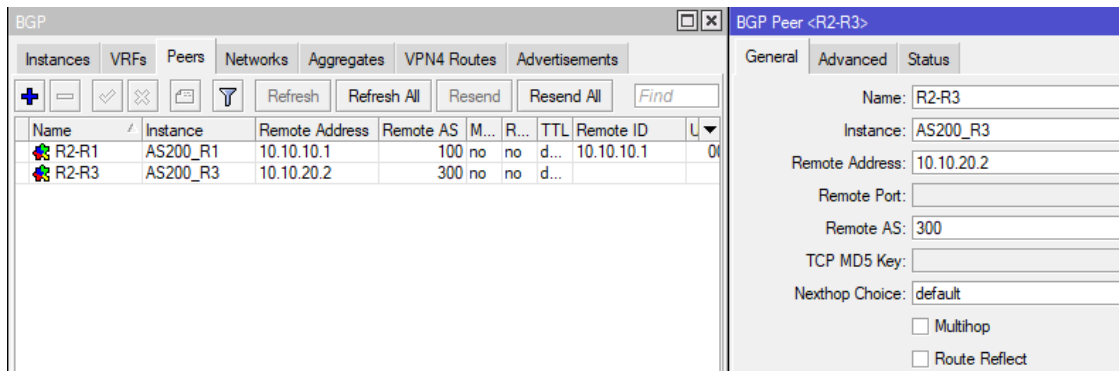


Figura 3.138 Configuración de relación par entre R2 y R3

R3

Se ingresa el nombre de la relación par R3-R2 (*Name*), se selecciona la instancia AS300 (*Instance*), se ingresa la dirección IP 10.10.20.1 (*Remote Address*) y se ingresa el valor 200 (*Remote AS*), ver figura 3.139.

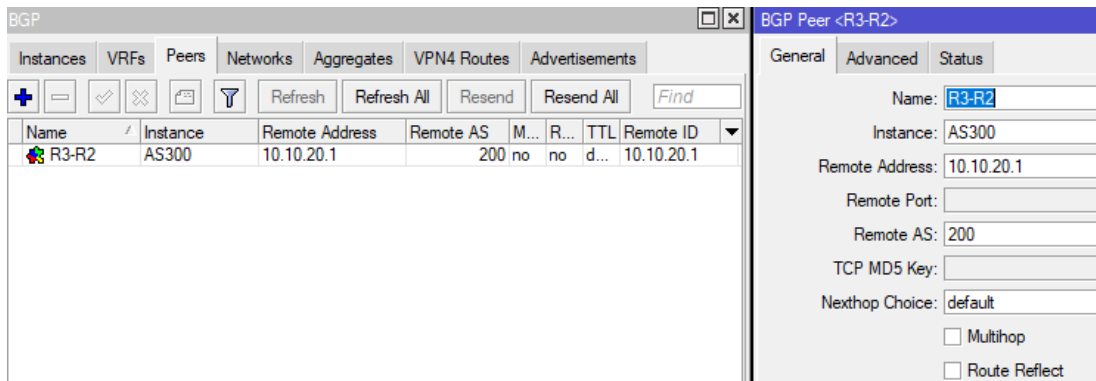


Figura 3.139 Configuración de relación par entre R3 y R2

Ahora se debe configurar la publicación de las redes LAN en cada router. Para ello se selecciona el casillero *Networks* y se elige la opción (+) donde se observa una nueva ventana. Se ingresa la red LAN directamente conectada de acuerdo con cada router (*Network*) y su respectivo comentario.

R1

Se ingresa la red de LAN1 192.168.100.0/24, ver figura 3.140.

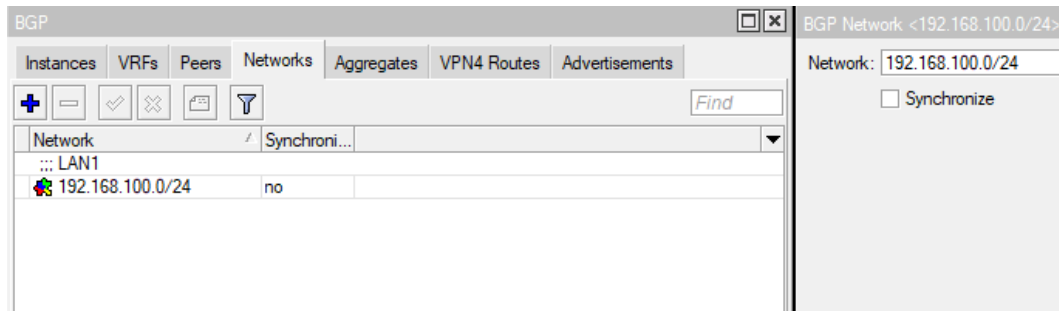


Figura 3.140 Configuración de publicación de red LAN1 en R1

R2

Se ingresa la red de LAN2 192.168.110.0/24, ver figura 3.141.

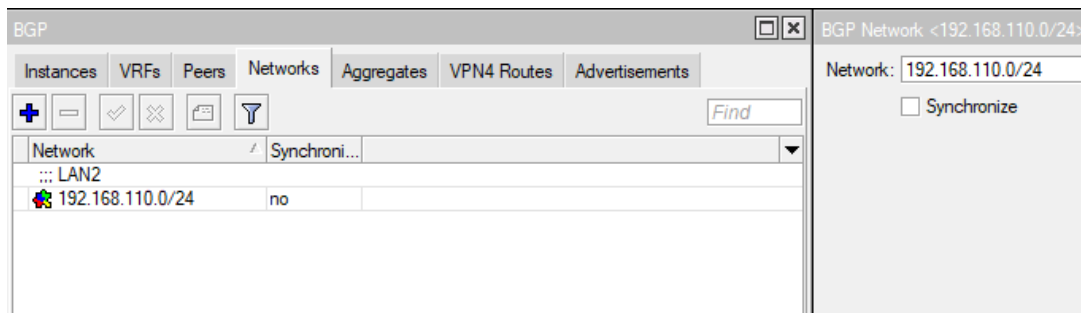


Figura 3.141 Configuración de publicación de red LAN2 en R2

R3

Se ingresa la red de LAN3 192.168.120.0/24, ver figura 3.142.

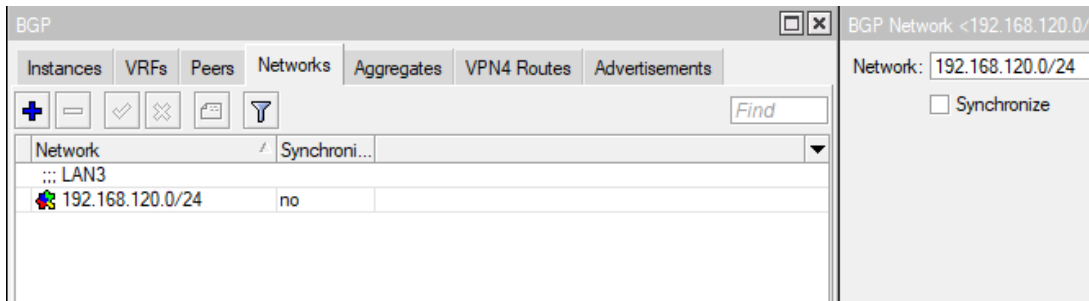


Figura 3.142 Configuración de publicación de red LAN3 en R3

Configuración DHCP en interfaces LAN

Para la configuración del servidor DHCP se selecciona en el menú la opción *IP/DHCP Server*. En el casillero DHCP se selecciona la opción *DHCP Setup*. Ahora se aprecia una nueva ventana donde se elige la interfaz a configurar el servidor (*DHCP Server Interface*), se ingresa la red LAN (*DHCP Address Space*), se ingresa la puerta de enlace de la red LAN (*Gateway for DHCP Network*), se ingresa el rango de direcciones para arrendar en la red LAN (*Addresses to Give Out*) y el tiempo de arrendamiento de las direcciones IP (*Lease Time*).

R1

Se selecciona le interfaz ether2, se ingresa la red LAN1, se ingresa el Gateway de LAN1 192.168.100.1, se ingresa el rango de direcciones 192.168.100.2-192.168.100.254 y un tiempo de arredramiento de 10 minutos. ver figura 3.143.

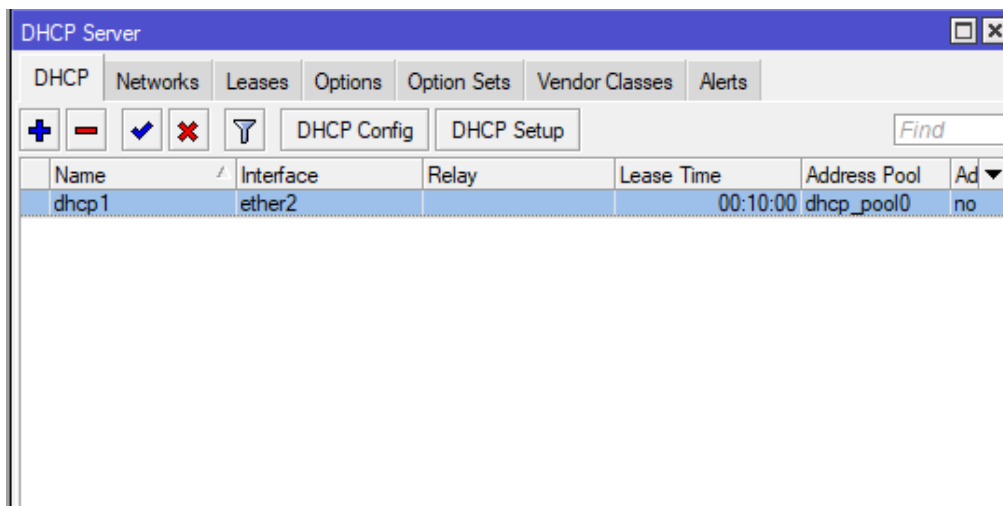
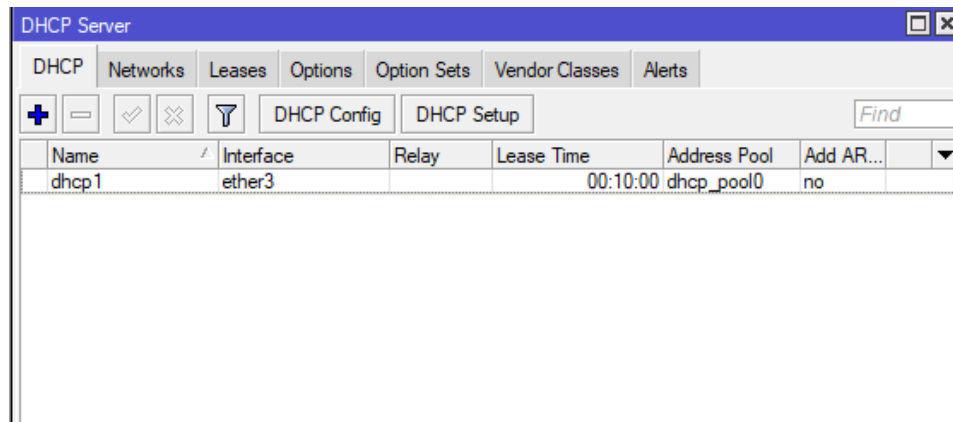


Figura 3.143 Configuración de DHCP en R1

R2

Se selecciona le interfaz ether3, se ingresa la red LAN2, se ingresa el Gateway de LAN2 192.168.110.1, se ingresa el rango de direcciones 192.168.110.2-192.168.110.254 y un tiempo de arredramiento de 10 minutos. ver figura 3.144.

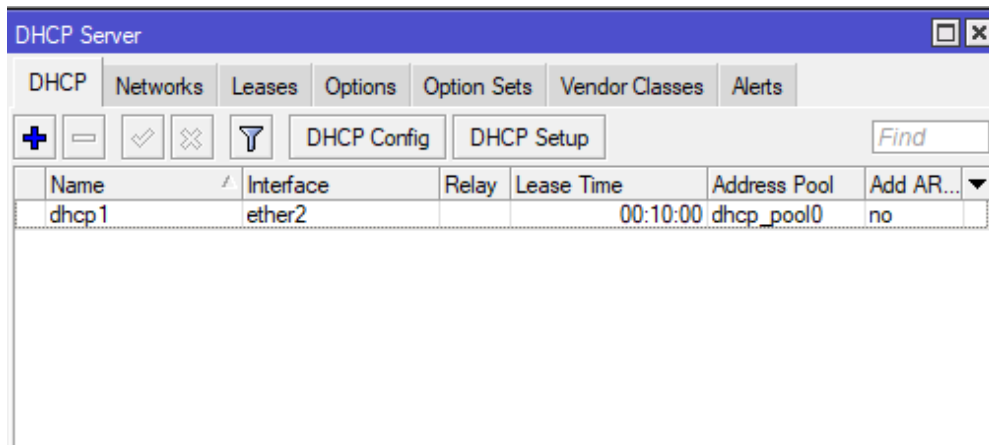


Name	Interface	Relay	Lease Time	Address Pool	Add AR...	
dhcp1	ether3		00:10:00	dhcp_pool0	no	

Figura 3.144 Configuración de DHCP en R2

R3

Se selecciona le interfaz ether2, se ingresa la red LAN3, se ingresa el Gateway de LAN3 192.168.120.1, se ingresa el rango de direcciones 192.168.120.2-192.168.120.254 y un tiempo de arredramiento de 10 minutos. ver figura 3.145.



Name	Interface	Relay	Lease Time	Address Pool	Add AR...	
dhcp1	ether2		00:10:00	dhcp_pool0	no	

Figura 3.145 Configuración de DHCP en R3

A continuación, se ingresa al menú *IP/Routes* donde se muestra la tabla de rutas del equipo aprendidas por *BGP* en R1, R2 y R3, ver figura 3.146.

The image shows three overlapping windows of the Mikrotik WinBox interface, each displaying a BGP routing table. The windows are titled 'Route List'.

The top-left window shows the routing table for R1:

Dest. Address	Gateway	Distance	Pref. Source
DAC ▶ 10.10.10.0/30	ether1 reachable	0	10.10.10.1
DAC ▶ 192.168.100.0/24	ether2 reachable	0	192.168.100.1
DAb ▶ 192.168.110.0/24	10.10.10.2 reachable ether1	20	
DAb ▶ 192.168.120.0/24	10.10.10.2 reachable ether1	20	

The top-right window shows the routing table for R2:

Dest. Address	Gateway	Distance	Pref. Source
DAC ▶ 192.168.110.0/24	ether3 reachable	0	192.168.110.1
DAC ▶ 10.10.20.0/30	ether2 reachable	0	10.10.20.1
DAC ▶ 10.10.10.0/30	ether1 reachable	0	10.10.10.2
DAb ▶ 192.168.120.0/24	10.10.20.2 reachable ether2	20	
DAb ▶ 192.168.100.0/24	10.10.10.1 reachable ether1	20	

The bottom window shows a filtered view of the routing table for R3:

Dest. Address	Gateway	Distance	Pref. Source
DAC ▶ 192.168.120.0/24	ether2 reachable	0	192.168.120.1
DAC ▶ 10.10.20.0/30	ether1 reachable	0	10.10.20.2
DAb ▶ 192.168.100.0/24	10.10.20.1 reachable ether1	20	
DAb ▶ 192.168.110.0/24	10.10.20.1 reachable ether1	20	

Figura 3.146 Tabla de enrutamiento por *BGP*

Configuración vía comandos

Cambio de nombre en el *router*

Para su configuración se ingresa el comando *system/identity*.

- [admin@MikroTik] > system identity set name=R1

Configuración de interfaces *WAN* y *LAN*

Para su configuración se ingresa el comando *IP address*

R1

- [admin@R1] > IP address add address=10.10.10.1/30 comment=WAN1 interface=ether1
- [admin@R1] > IP address add address=192.168.100.1/24 comment=LAN1 interface=ether2

R2

- [admin@R2] > IP address add address=10.10.10.2/30 comment=WAN1 interface=ether1
- [admin@R2] > IP address add address=10.10.20.1/30 comment=WAN2 interface=ether2
- [admin@R2] > IP address add address=192.168.110.1/24 comment=LAN2 interface=ether3

R3

- [admin@R3] > IP address add address=10.10.20.2/30 comment=WAN2 interface=ether1
- [admin@R3] > IP address add address=192.168.120.1/24 comment=LAN2 interface=ether2

Configuración de BGP

Para el acceso a la configuración del protocolo *BGP* en cada *router* se ingresando el comando *routing BGP*.

R1

- [admin@R1] > routing BGP instance add name=AS100 as=100 router-id=10.10.10.1 redistribute-other-BGP=yes

R2

- [admin@R2] > routing BGP instance add name=AS200_R1 as=200 router-id=10.10.10.2 redistribute-other-BGP=yes
- [admin@R2] > routing BGP instance add name=AS200_R3 as=200 router-id=10.10.20.1 redistribute-other-BGP=yes

R3

- [admin@R3] > routing BGP instance add name=AS300 as=300 router-id=10.10.20.2 redistribute-other-BGP=yes

Ahora se configura las relaciones pares entre *routers*, para ello se ingresa el comando *routing BGP peer*.

R1

- [admin@R1] > routing BGP peer add name=R1-R2 instance=AS100 remote-address=10.10.10.2 remote-as=200

R2

- [admin@R2] > routing BGP peer add name=R2-R1 instance=AS200_R1 remote-address=10.10.10.1 remote-as=100
- [admin@R2] > routing BGP peer add name=R2-R3 instance=AS200_R3 remote-address=10.10.20.2 remote-as=300

R3

- [admin@R3] > routing BGP peer add name=R3-R2 instance=AS300 remote-address=10.10.20.1 remote-as=200

A continuación, se configura la publicación de las redes *LAN*, para ello se ingresa el comando *routing BGP peer*.

R1

- [admin@R1] > routing BGP network add network=192.168.100.0/24
comment=LAN1 synchronize=no

R2

- [admin@R2] > routing BGP network add network=192.168.110.0/24
comment=LAN2 synchronize=no

R3

- [admin@R3] > routing BGP network add network=192.168.120.0/24
comment=LAN3 synchronize=no

Configuración *DHCP* en interfaces *LAN*

Para la configuración de *DHCP* Server en cada interfaz *LAN* se ingresa el comando *IP DHCP-server*.

R1

- [admin@Router_R1] > IP DHCP-server setup
Select interface to run DHCP server on
DHCP server interface: ether2
Select network for DHCP addresses
DHCP address space: 192.168.100.0/24
Select gateway for given network
gateway for DHCP network: 192.168.100.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.100.2-192.168.100.254
Select lease time
lease time: 10m

R2

- [admin@Router_R1] > IP DHCP-server setup
Select interface to run DHCP server on
DHCP server interface: ether3
Select network for DHCP addresses
DHCP address space: 192.168.110.0/24
Select gateway for given network
gateway for DHCP network: 192.168.110.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.110.2-192.168.110.254
Select lease time
lease time: 10m

R3

- [admin@Router_R1] > IP DHCP-server setup
 Select interface to run DHCP server on
 DHCP server interface: ether2
 Select network for DHCP addresses
 DHCP address space: 192.168.120.0/24
 Select gateway for given network
 gateway for DHCP network: 192.168.120.1
 Select pool of IP addresses given out by DHCP server
 addresses to given out: 192.168.120.2-192.168.120.254
 Select lease time
 lease time: 10m

Pruebas de conectividad en equipos y hosts

Se realizó las pruebas de conectividad en toda la red, para ello es necesario ingresar al CMD de Windows.

La primera prueba realizada es la conectividad entre un host de LAN1 y un host de LAN2 por medio del comando ping, ver figura 3.147.

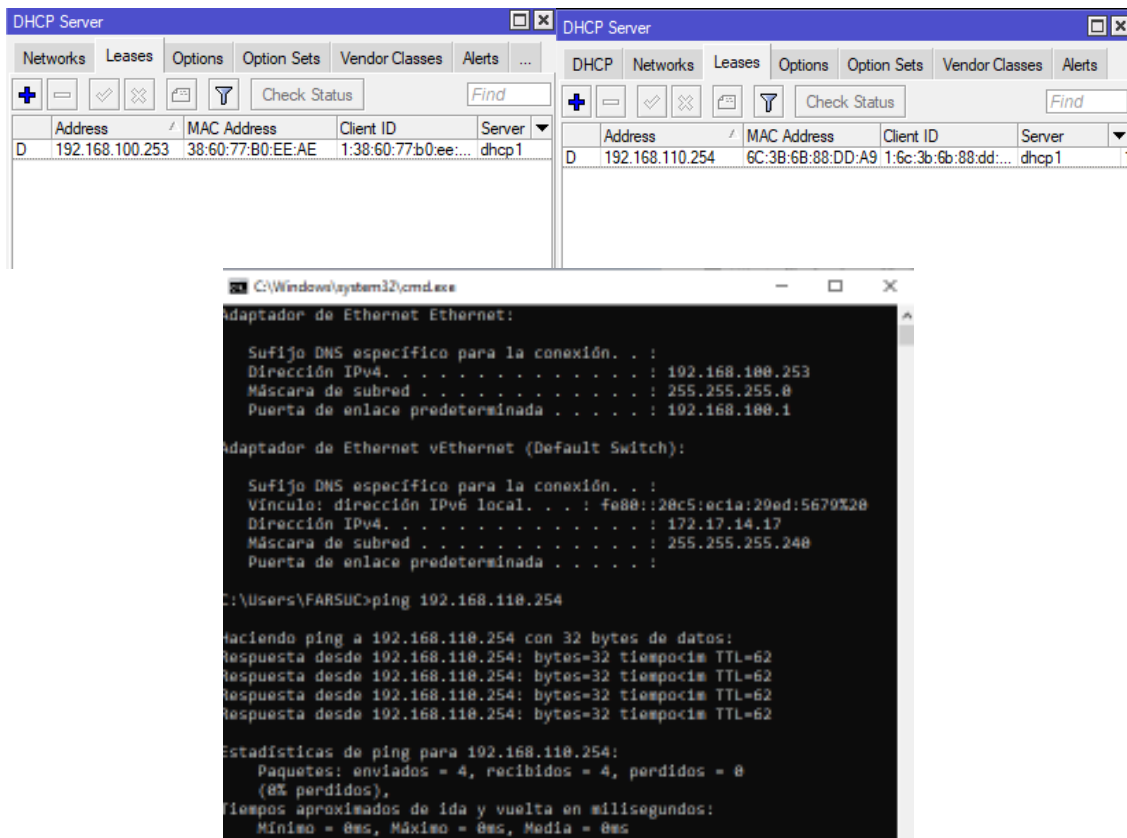


Figura 3.147 Prueba de conectividad entre LAN1 y LAN2

La segunda prueba realizada es la conectividad entre un *host* de LAN1 y un *host* de LAN3 por medio del comando *ping*, ver figura 3.148.

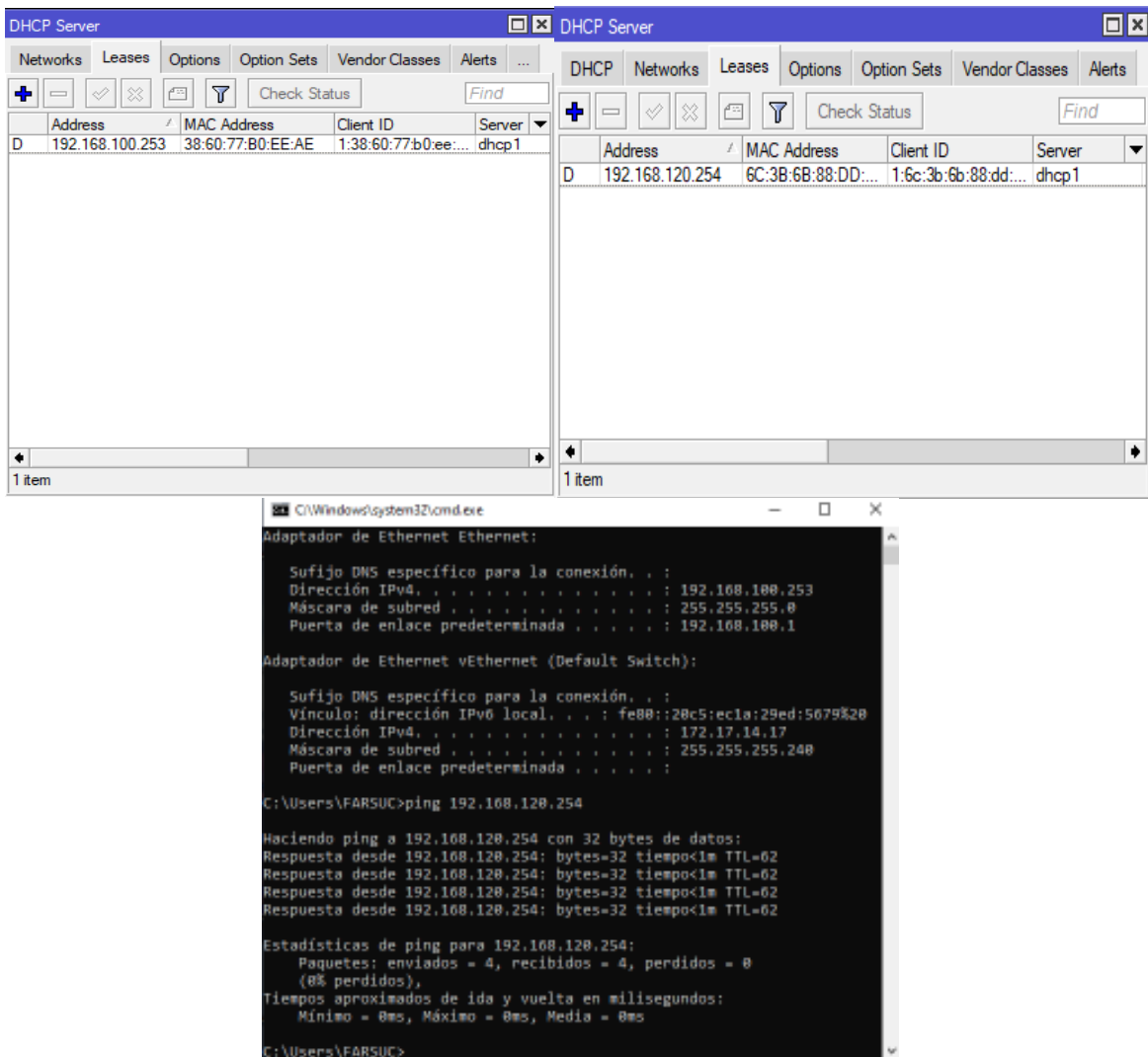


Figura 3.148 Prueba de conectividad entre LAN1 y LAN3

La tercera prueba realizada es la conectividad entre un *host* de LAN2 y un *host* de LAN3 por medio del comando *ping*, ver figura 3.149.

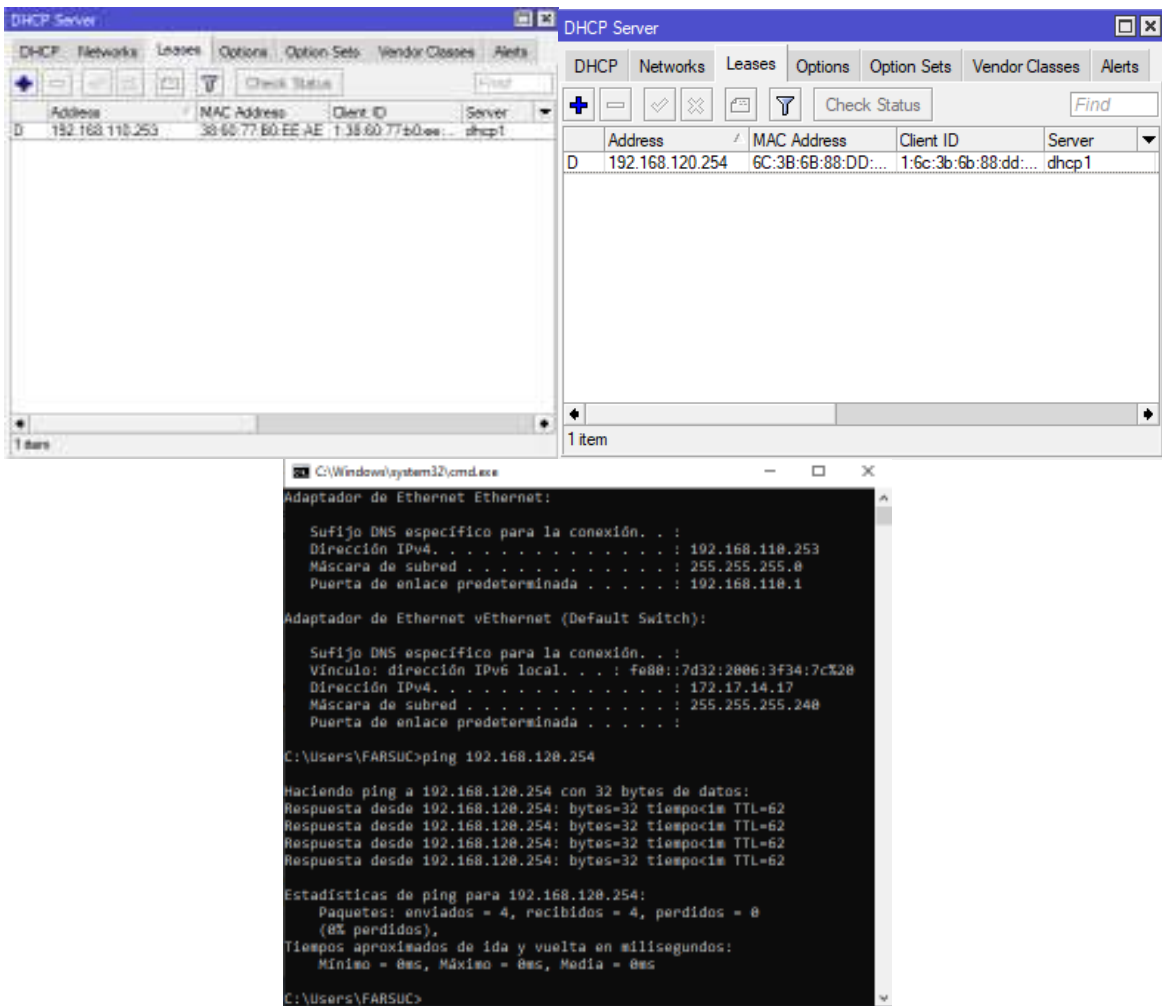


Figura 3.149 Prueba de conectividad entre LAN2 y LAN3

❖ Práctica N°6

Tema: *Firewall* básico

Objetivo: Configuración de Firewall básico en *router MikroTik*

Objetivos Específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*
- Configuración de interfaces *WAN* y *LAN*
- Configuración de *bridge* en *Ether2* y *Ether3*
- Configuración de acceso a internet
- Configuración de *firewall*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

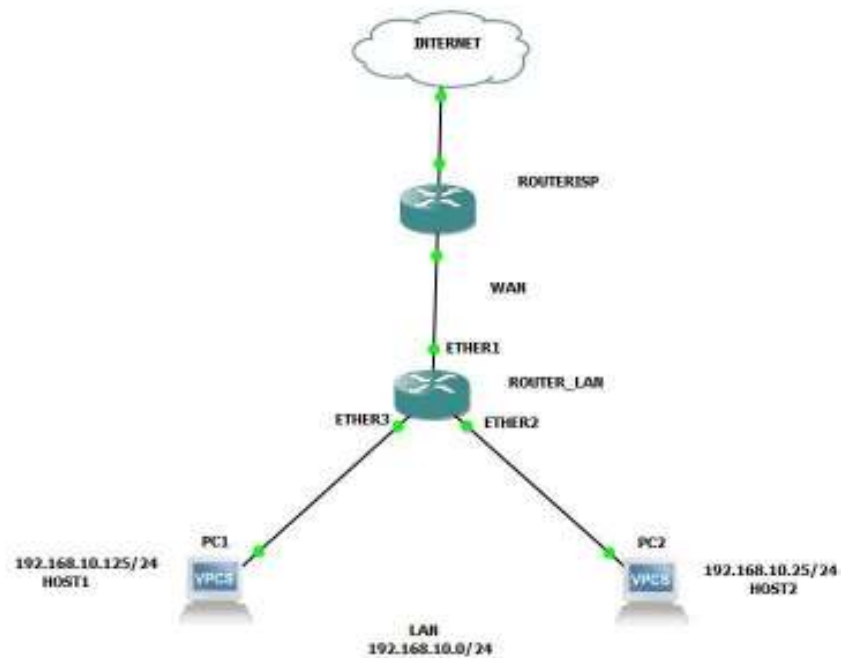


Figura 3.150 Topología de *firewall* básico

Tabla de direcciones IP

A continuación, se muestra la tabla 3.13 de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Tabla 3.13 Direccionamiento IP en redes WAN, LAN y hosts

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
WAN	ISP	ISP	R1(Ether1)	ISP	ISP
LAN	192.168.10.0	/24	R1(Ether2-3)	192.168.10.1	/24

Tabla de reglas en hosts

A continuación, se muestra la tabla 3.14 de reglas *firewall* para cada *host*.

Tabla 3.14 Tabla de filtros en *hosts*

Nombre	Dirección IP	Máscara	Reglas
Host1	192.168.10.125	/24	Acceso al <i>router</i> / Acceso SSH-Ping-Telnet / Acceso a internet sin restricciones
Host2	192.168.10.25	/24	No acceso al <i>router</i> / Bloqueo SSH-Ping-Telnet / Acceso a internet con restricciones a redes sociales

Configuración vía interfaz gráfica

Cambio de nombre en el *router*

Para el cambio de nombre ingresamos *System/Identity*, ver figura 3.151.

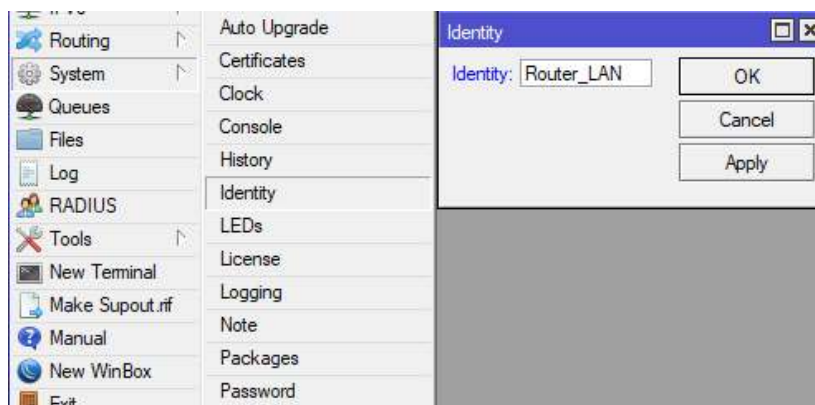


Figura 3.151 Identificación de router

Configuración de bridge en ether2 y ether3

Para la configuración se selecciona en el menú la opción *Bridge*, y se selecciona la opción (+). A continuación, en General se coloca un nombre al *bridge* (*Name*) y luego se da en *Apply/Ok*, ver figura 3.152.

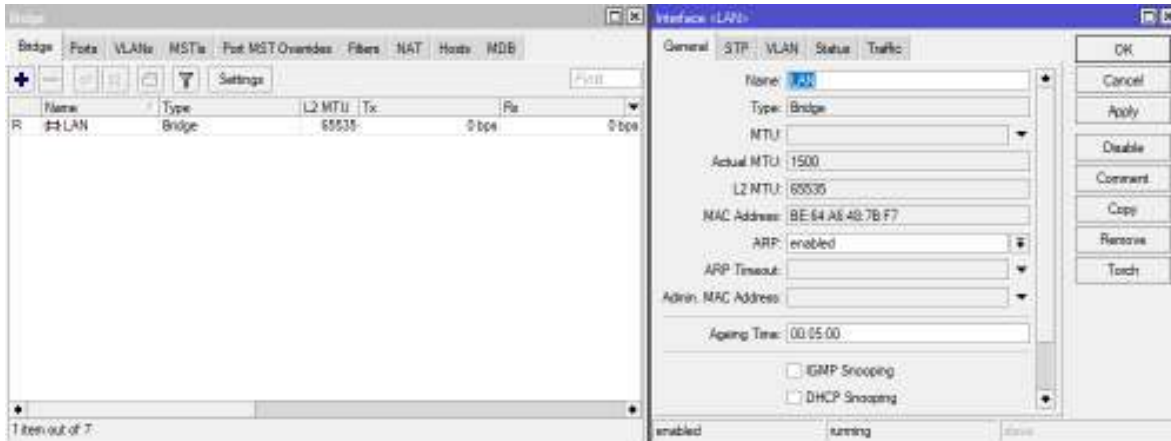


Figura 3.152 Configuración de nombre al bridge

En *Ports* se elige la opción (+) y se ingresa las interfaces que van a pertenecer al bridge (*Interface*). En *Bridge* se selecciona el nombre dado al bridge y luego se da elige *Apply/Ok*, ver figura 3.153.

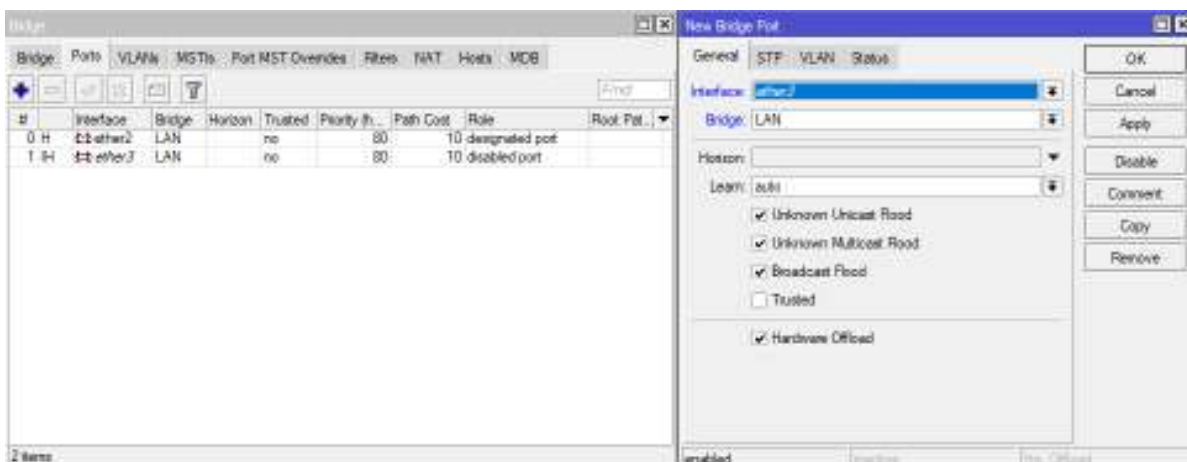


Figura 3.153 Configuración de interfaces del bridge

Configuración de interfaces WAN y LAN

Para la configuración se selecciona en el menú la opción *IP/Addresses* y se ingresa las direcciones *IP* de cada interfaz. Se configura las interfaces de *ether 1* y *2* para *WAN* y *LAN*, ver figura 3.154.

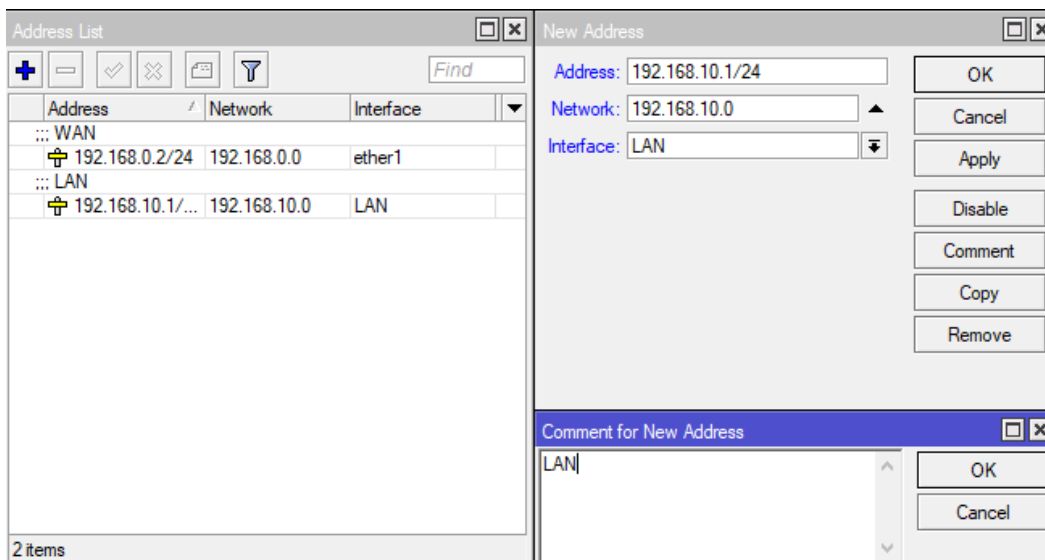


Figura 3.154 Configuración de interfaces en router

Configuración de acceso a Internet

Para tener acceso a Internet se selecciona la opción *IP/Routes* y se selecciona la opción (+). A continuación, es necesario crear una ruta para la salida de paquetes, para ello se crea una ruta por defecto 0.0.0.0/0 (*Dst. Address*) y una *IP* de salida (*Gateway*). En este caso el enlace *WAN* en el extremo del ISP tiene la dirección *IP* 192.168.0.1/24, ver figura 3.155.

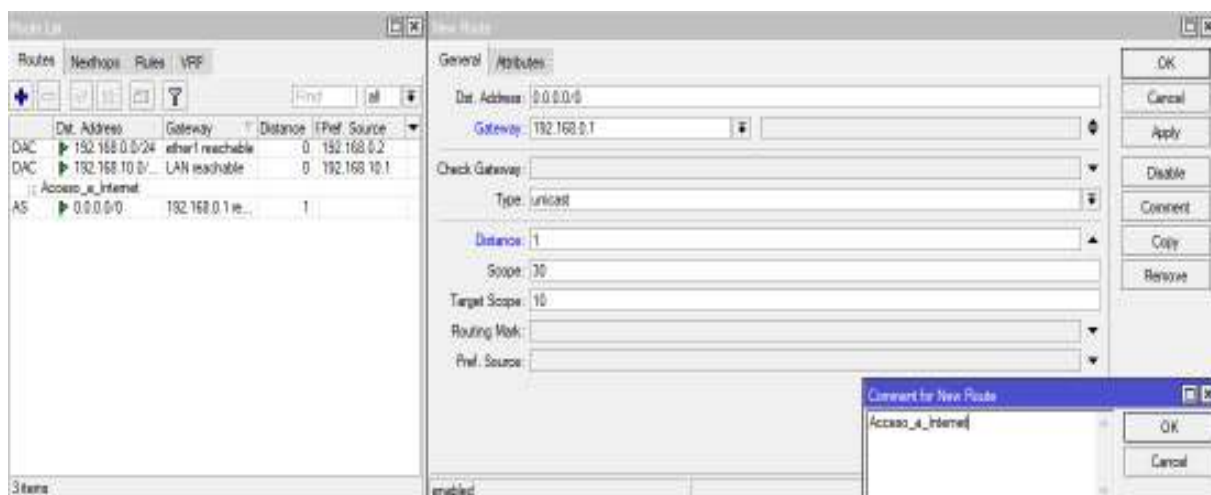


Figura 3.155 Configuración de ruta para acceso a Internet

Ahora se debe realizar el enmascaramiento de nuestra red local *LAN* para tener salida a Internet. Para ello es necesario ir a *IP/Firewall* y en la opción de *NAT* en General, en el casillero *Chain* colocamos *srcnat* que indica los paquetes originados en la red *LAN*. En el casillero *Out. Interface* se coloca la interfaz que está conectada con la red *WAN*, que es la

salida a Internet. En *Action* en el casillero *Action* se elige la opción *masquerade*, ver figura 3.156.

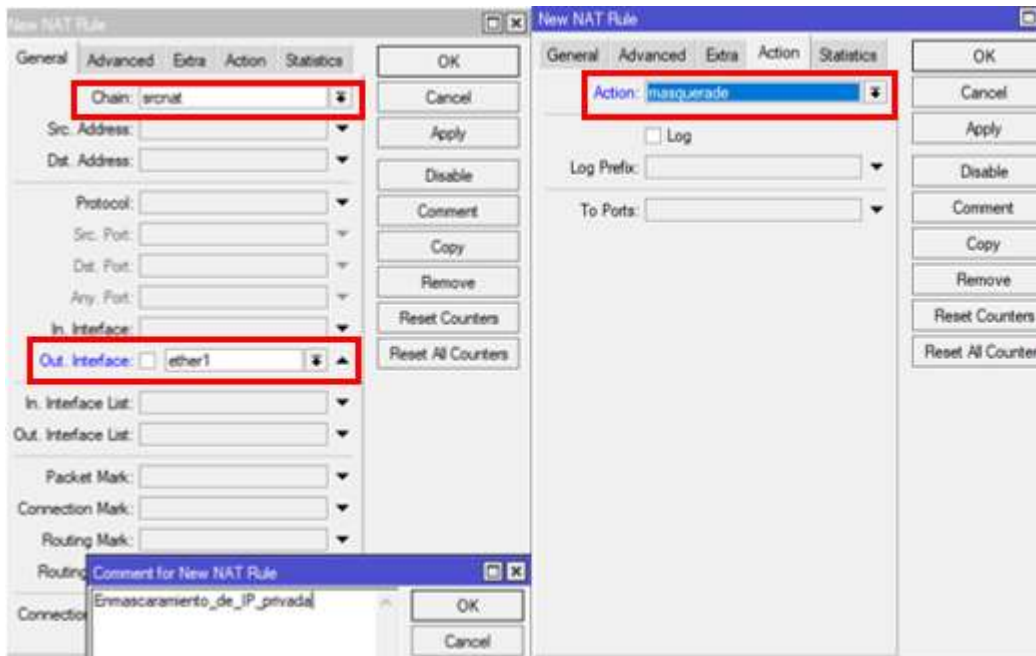


Figura 3.156 Configuración de enmascaramiento

Ahora se observa la lista de configuraciones realizadas en *NAT*, ver figura 3.157.

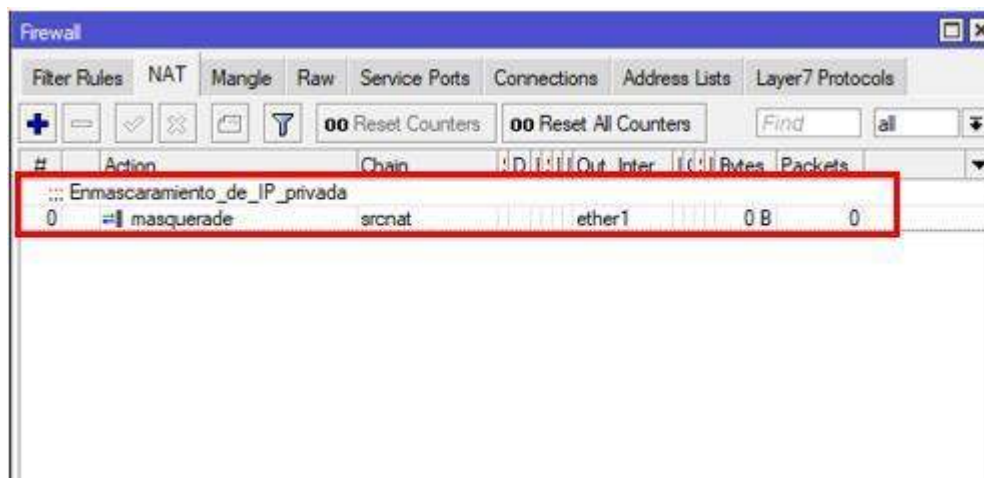


Figura 3.157 Lista de configuración NAT

Configuración de *firewall* básico

Creación de *Address Lists*

Para la creación de direcciones *IP* se selecciona la opción *IP/Firewall*. En el casillero *Address Lists* se escoge la opción (+) y se ingresa el nombre que se identificara a la dirección *IP* (*Name*). Luego se ingresa la dirección *IP* (*Address*) y se elige *Apply* y *Ok*, ver figura 3.158.

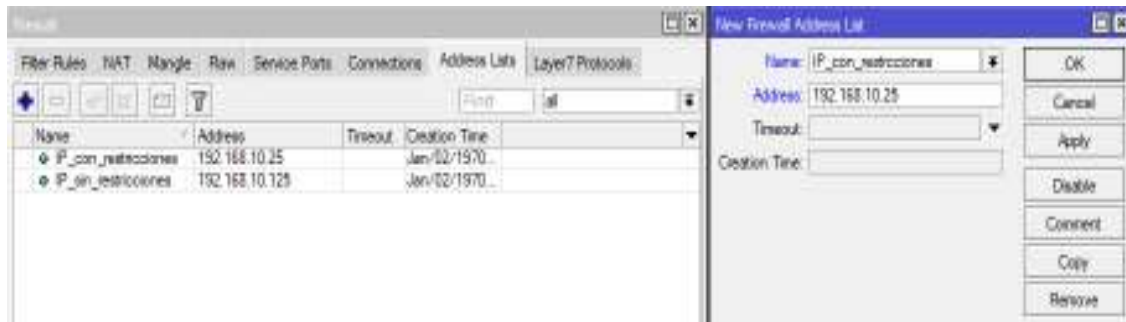


Figura 3.158 Creación de *Address Lists*

Configuración de acceso y bloqueo al *router*

En el casillero *Filter Rules* se selecciona la opción (+). A continuación, en el casillero *General*, en *Chain* se ingresa la opción *input*. En *Connection State* se selecciona las opciones *established* y *related*. En el casillero *Action*, en *Action* se selecciona la opción *accept* y se ingresa su respectivo comentario de identificación, ver figura 3.159.

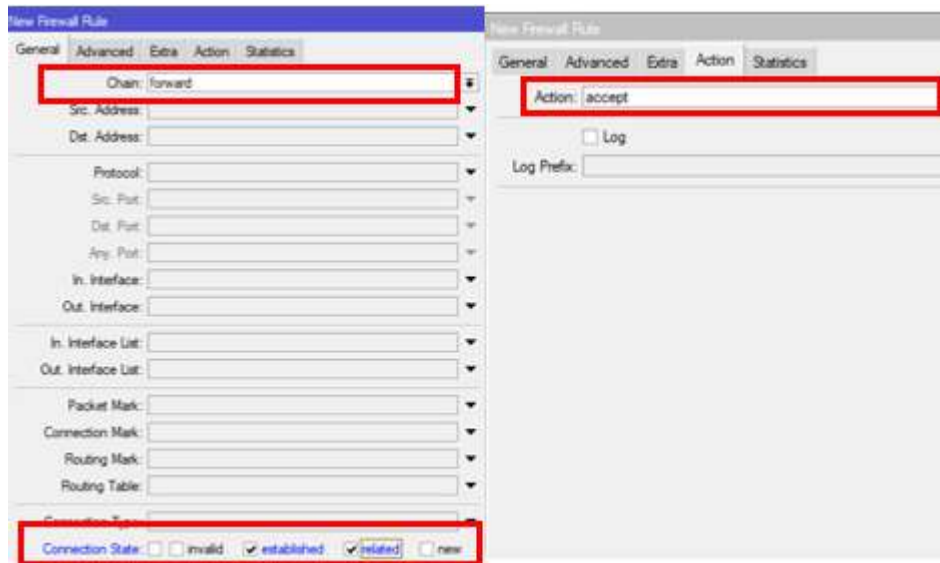


Figura 3.159 Regla de permiso de conexiones válidas *INPUT*

Ahora para negar conexiones invalidas se crea una nueva regla en *Filter Rules*. En el casillero *General*, en *Chain* ingresa la opción *input*. En *Connection State* se selecciona la opción *invalid*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.160.

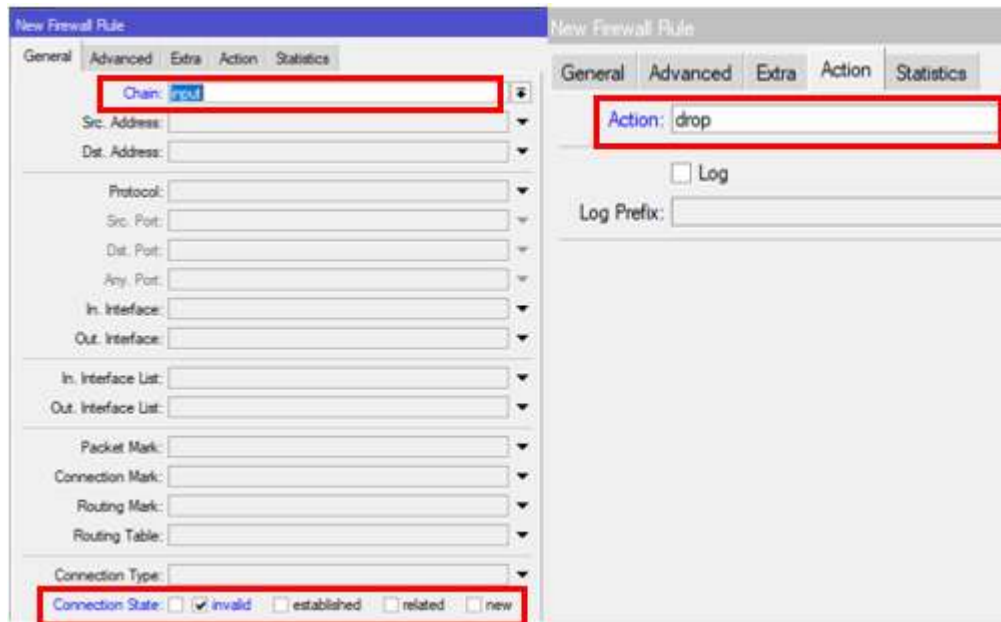


Figura 3.160 Regla de negación de conexiones inválidas *INPUT*

A continuación, para aceptar el acceso de la dirección *IP* de acuerdo con la tabla de reglas se crea un nuevo filtro en *Filter Rules*. En el casillero *General*, en *Chain* se ingresa la opción *input*. En el casillero *Advanced*, en *Src. Address Lists* se selecciona la *IP* con el nombre *IP_sin_restricciones*. En el casillero *Action*, en *Action* se selecciona la opción *accept* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.161.

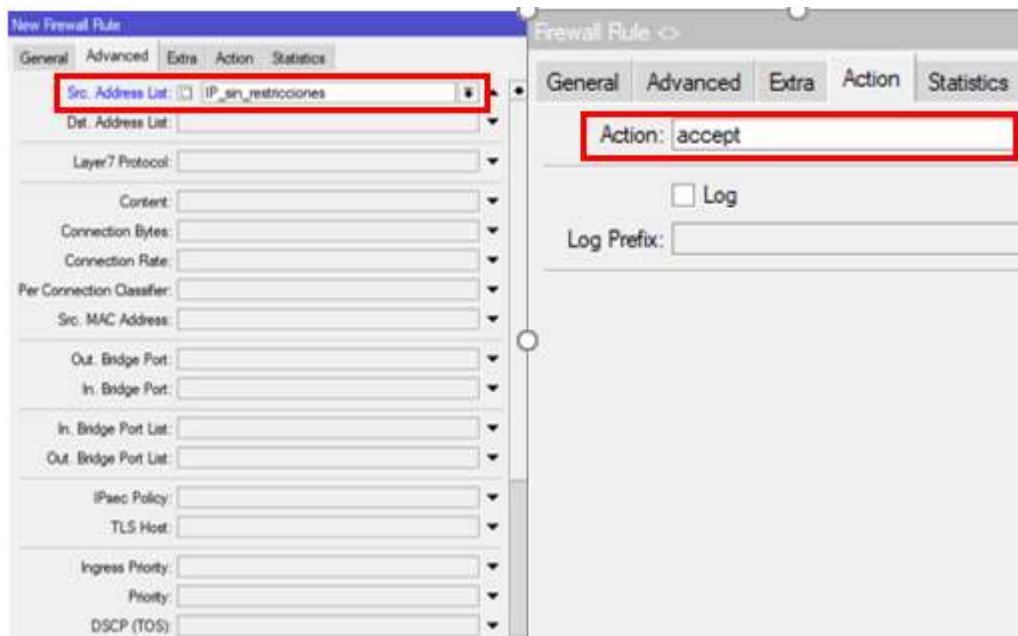


Figura 3.161 Regla de acceso al router

A continuación, para negar el acceso de una dirección IP se crea una nueva regla *Filter Rules*. En el casillero *General*, en *Chain* se ingresa la opción *input*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.162.

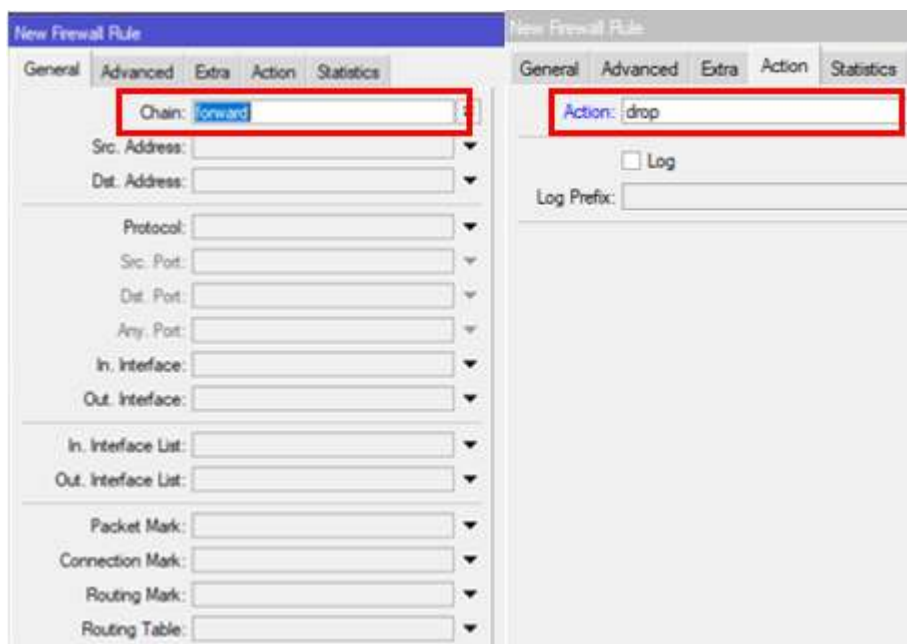


Figura 3.162 Regla de negación de acceso al router

Configuración de bloqueo servicios de acceso al *router*

Ahora para realizar el bloqueo de *PING* de cierta dirección *IP* hacia el *router* se crea una nueva regla *Filter Rules*. En el casillero *General*, en *Chain* se ingresa la opción *input*, en *Protocol* se coloca *icmp*. En el casillero *Advanced*, en *Src. Address Lists* se selecciona la *IP* con el nombre *IP_con_restricciones*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.163.

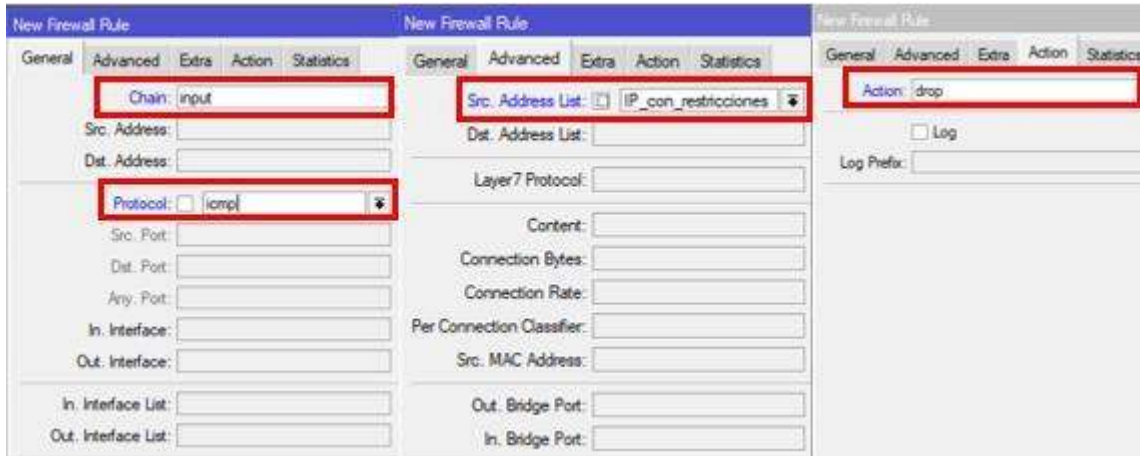


Figura 3.163 Configuración de bloqueo *PING*

A continuación, para realizar el bloqueo de *SSH* de cierta dirección *IP* hacia el *router* se crea la siguiente regla en *Filter Rules*. En el casillero *General*, en *Chain* se ingresa la opción *input*, en *Protocol* se coloca *tcp*, en *Dst. Port* se ingresa el número de puerto 22. En el casillero *Advanced*, en *Src. Address Lists* se selecciona la *IP* con el nombre *IP_con_restricciones*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.164.

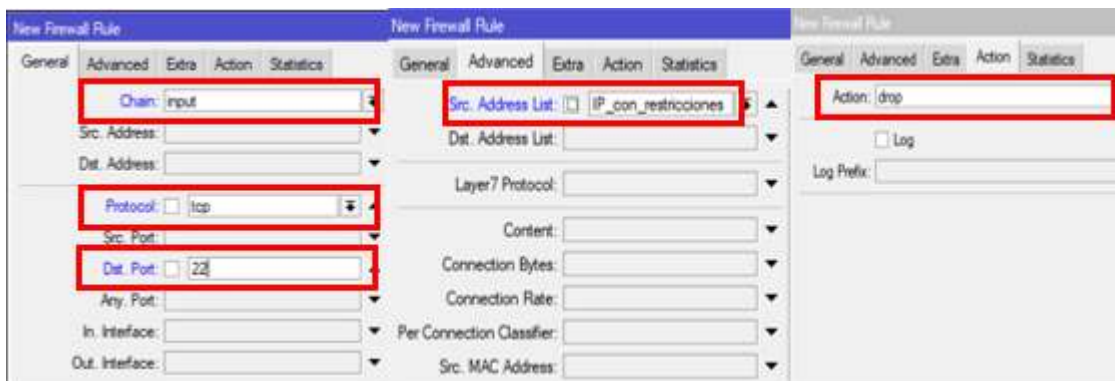


Figura 3.164 Configuración de bloqueo *SSH*

Ahora para realizar el bloqueo de *Telnet* en cierta dirección *IP* hacia el *router* se crea la siguiente regla. En el casillero General, en *Chain* se ingresa la opción *input*, en *Protocol* se coloca *tcp*, en *Dst. Port* se ingresa el número de puerto 23. En el casillero *Advanced*, en *Src. Address Lists* se selecciona la *IP* con el nombre *IP_con_restricciones*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.165.

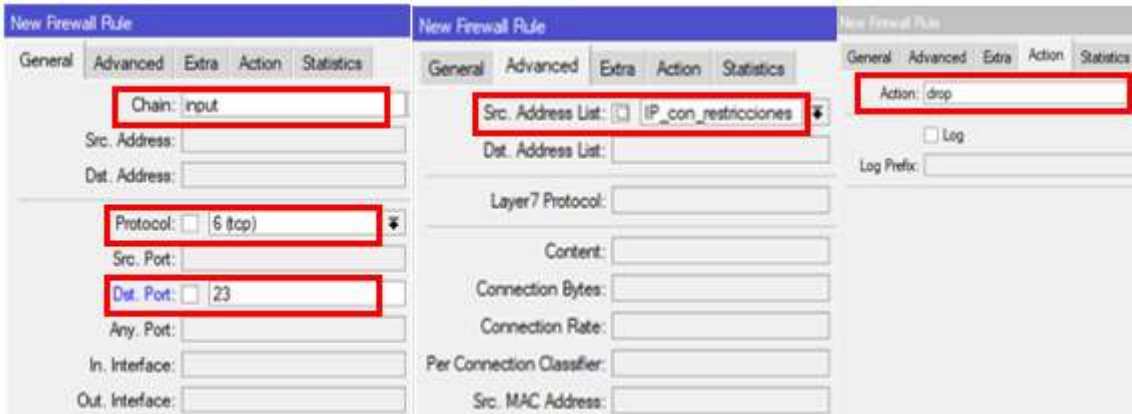


Figura 3.165 Configuración de bloqueo *Telnet*

Configuración de acceso y restricción a Internet

Para bloquear ciertas páginas web se trabaja en la capa 7 del modelo OSI, En el casillero *Layer7 Protocols* se elige la opción (+), se coloca un nombre a la regla (*Name*) y en *Regexp* se ingresa una expresión regular para su configuración, ver figura 3.166.

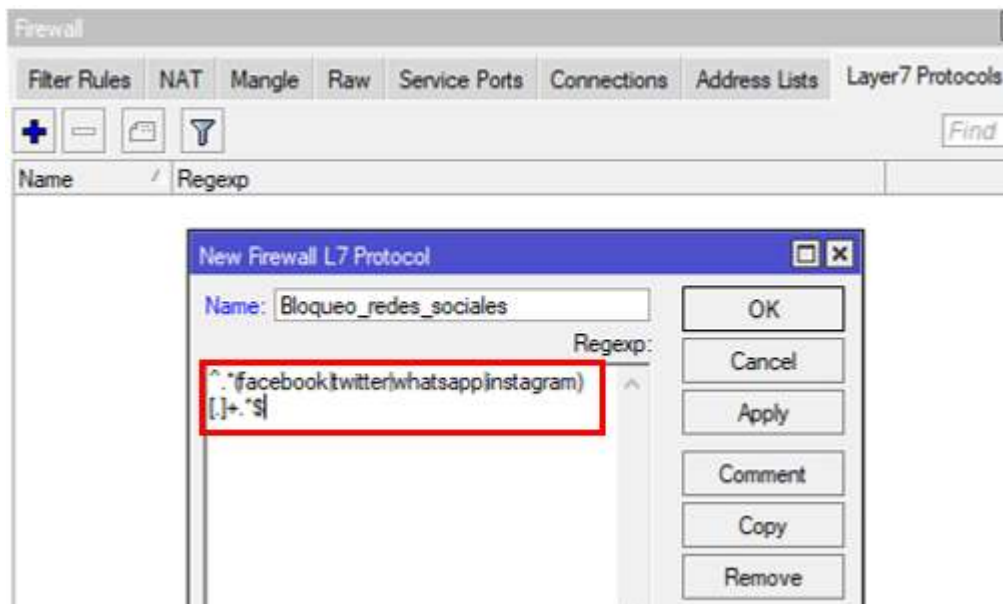


Figura 3.166 Configuración de *Layer7 Protocol*

A continuación, se crea la siguiente regla en *Filter Rules*. En el casillero *General*, en *Chain* se ingresa la opción *forward*. En el casillero *Advanced*, en *Src. Address Lists* se selecciona la *IP* con el nombre *IP_con_restricciones*, en *Layer7 Protocol* se selecciona la regla *Bloqueo_redes_sociales*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.167.

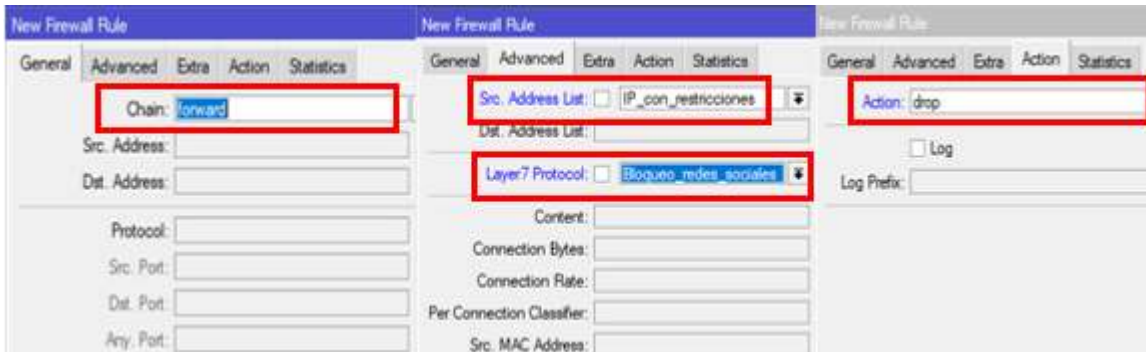


Figura 3.167 Configuración de *Layer7 Protocol*.

Ahora para aceptar conexiones validas en internet se crea una nueva regla en *Filter Rules*. En el casillero *General*, en *Chain* ingresa la opción *forward*. En *Connection State* se selecciona la opción *established* y *related*. En el casillero *Action*, en *Action* se selecciona la opción *accept* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.168.

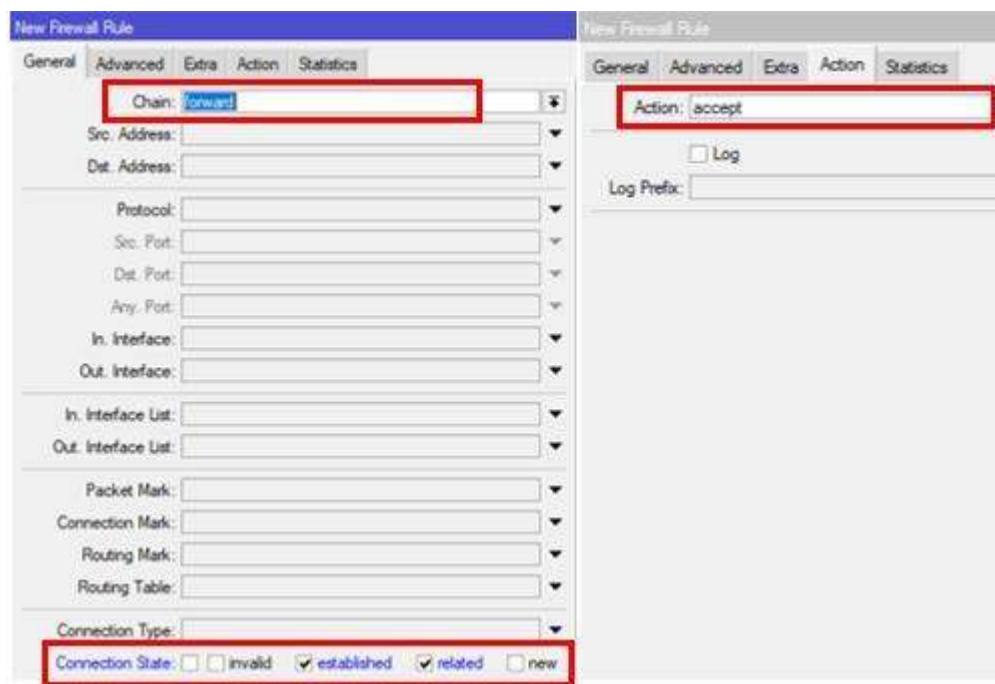


Figura 3.168 Regla de permiso de conexiones válidas *FORWARD*

Ahora para negar conexiones invalidas en internet se crea una nueva regla en *Filter Rules*. En el casillero *General*, en *Chain* ingresa la opción *forward*. En *Connection State* se selecciona la opción *invalid*. En el casillero *Action*, en *Action* se selecciona la opción *drop* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.169.

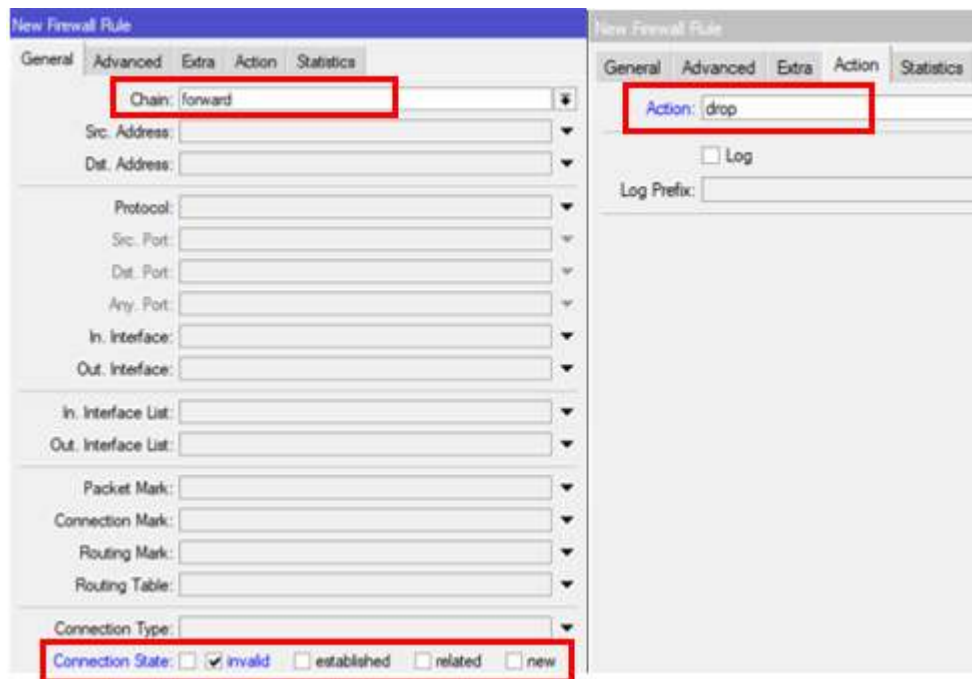


Figura 3.169 Regla de negación de conexiones inválidas *FORWARD*

A continuación, para permitir la navegación a internet de las direcciones *IP* se crea una nueva regla en *Filter Rules*. En el casillero *General*, en *Chain* ingresa la opción *forward*. En el casillero *Action*, en *Action* se selecciona la opción *accept* y se ingresa su respectivo comentario de identificación. Luego se coloca en *Apply* y *Ok*, ver figura 3.170

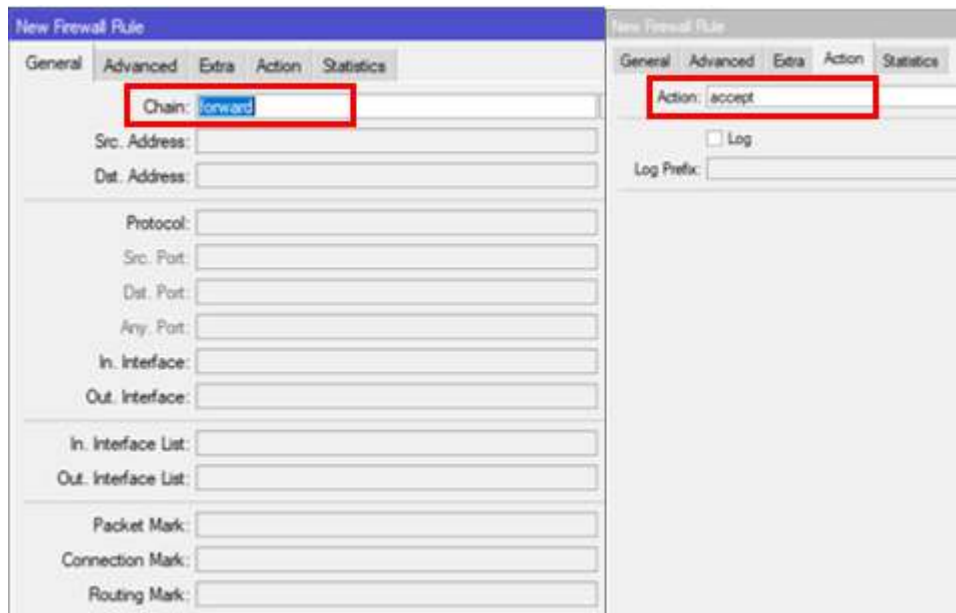


Figura 3.170 Regla para acceder a Internet

Se muestra la lista de reglas configuradas en *firewall*, ver figura 3.171.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Src. Address List
::: Permitir conexiones establecidas relacionadas router										
0	✓ acc...	input								
::: Rechazar conexiones invalidas										
1	✗ drop	input								
::: IP permitida acceso router										
2	✓ acc...	input								IP_sin_restricciones
::: IP negar acceso router										
3	✗ drop	input								
::: Bloqueo_PING										
4	✗ drop	input			1 (icmp)					IP_con_restricciones
::: Bloqueo_SSH										
5	✗ drop	input			6 (tcp)		22			IP_con_restricciones
::: Bloqueo_Telnet										
6	✗ drop	input			6 (tcp)		23			IP_con_restricciones
::: Bloqueo_de_redes_sociales										
7	✗ drop	forward								IP_con_restricciones
::: Permitir conexiones establecidas relacionadas internet										
8	✓ acc...	forward								
::: Rechazar conexiones invalidas internet										
9	✗ drop	forward								
::: Permitir navegacion IPs										
10	✓ acc...	forward								

Figura 3.171 Lista de regla *firewall*

Configuración de *hosts*

Para la configuración de *host* se ingresa a las propiedades de la tarjeta de red y se coloca las *IPs*, ver figura 3.172.

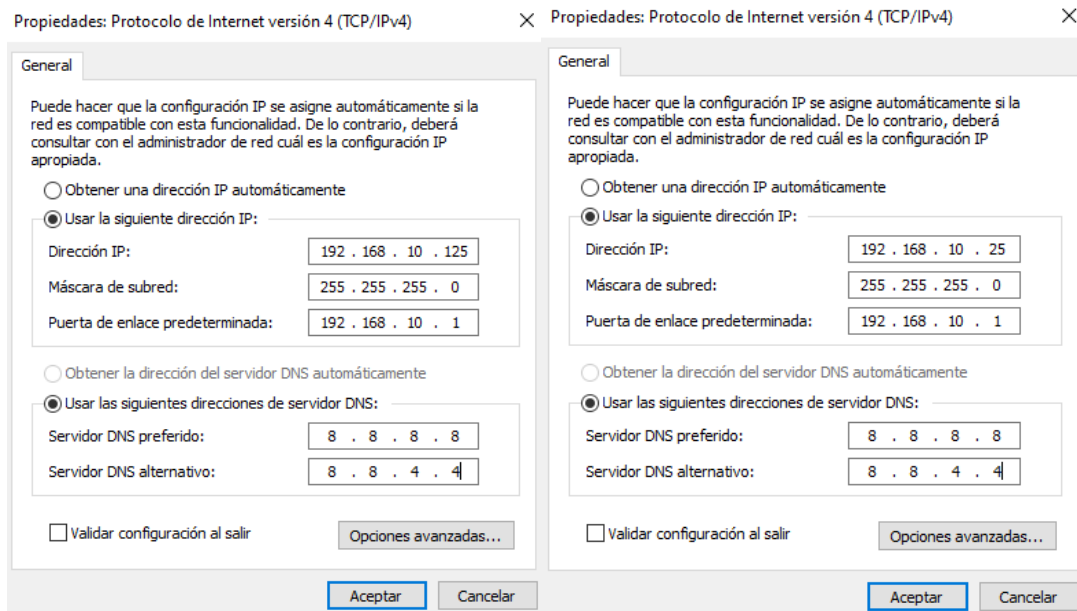


Figura 3.172 Configuración de tarjeta de red en *hosts*

Configuración vía comandos

Cambio de nombre en el *router*

Para su configuración se ingresa el comando *system/identity*.

```
- [admin@MikroTik] > system identity set name=Router_LAN
```

Configuración de bridge en *ether1* y *ether2*

Para su configuración se ingresa el comando *interface bridge*.

```
- [admin@Router_LAN] > interface bridge add name=LAN
- [admin@Router_LAN] > interface bridge port add interface=ether2
  bridge=LAN
- admin@Router_LAN] > interface bridge port add interface=ether3
  bridge=LAN
```

Configuración de interfaces *WAN* y *LAN*

Para su configuración se ingresa el comando *IP address*

```
- [admin@Router_LAN] > IP address add address=192.168.0.2/24
  comment=WAN interface=ether1
- [admin@Router_LAN] > IP address add address=192.168.10.1/24
  comment=LAN interface=ether2
```

Configuración de acceso a Internet

Para el acceso a Internet se crea una ruta por defecto ingresando el comando *IP route*.

- [admin@Router_LAN] > IP route add distance=1 dst-address=0.0.0.0/0 gateway=192.168.0.1 comment=Acceso_a_Internet

Ahora se ingresa el comando *IP firewall* para el enmascaramiento de los paquetes de la red LAN.

- [admin@Router_LAN] > IP firewall nat add action=masquerade chain=srcnat out-interface=ether1

Configuración de *firewall* básico

Creación de *Address Lists*

Para la creación de lista de direcciones *IP* se ingresa el comando *IP firewall*.

- [admin@Router_LAN] > IP firewall address-list add address=192.168.10.25 list=IP_con_restricciones
- [admin@Router_LAN] > IP firewall address-list add address=192.168.10.125 list=IP_sin_restricciones

Configuración de acceso y bloqueo al *router*

Para la creación de lista de direcciones *IP* se ingresa el comando *IP firewall filter*.

- [admin@Router_LAN] > IP firewall filter add action=accept chain=input comment=Permitir_conexiones_establecidas_relacionadas_router connection-state=established,related
- [admin@Router_LAN] > IP firewall filter add action=drop chain=input comment=Rechazar_conexiones_invalidas connection-state=invalid
- [admin@Router_LAN] > IP firewall filter add action=accept chain=input comment=Permitir_acceso_router src-address-list=IP_sin_restricciones
- [admin@Router_LAN] > IP firewall filter add action=drop chain=input comment=IP_negar_acceso

Configuración de bloqueo servicios de acceso al *router*

Para la creación de lista de direcciones *IP* se ingresa el comando *IP firewall filter*.

- [admin@Router_LAN] > IP firewall filter add action=drop chain=input
comment=Bloqueo_PING protocol=icmp scr-address-
list=IP_con_restricciones
- [admin@Router_LAN] > IP firewall filter add action=drop chain=input
comment=Bloqueo_SSH protocol=tcp dst-port=22 scr-address-
list=IP_con_restricciones
- [admin@Router_LAN] > IP firewall filter add action=drop chain=input
comment=Bloqueo_Telnet protocol=tcp dst-port=23 scr-address-
list=IP_con_restricciones

Configuración de acceso y restricción a Internet

Para bloquear ciertas paginas se ingresa el comando *IP firewall layer7-protocol*.

- [admin@Router_LAN] > IP firewall layer7-protocol add
name=Bloqueo_redes_sociales regexp=^(.*(facebook|twitter
|whatsapp|instagram)[.]+.*\$

Para el bloque o acceso a páginas web con determinada dirección IP se ingresa el comando *IP firewall filter*.

- [admin@Router_LAN] > IP firewall filter add action=drop
chain=forward layer7-protocol=Bloqueo_redes_sociales
comment=Bloqueo_de_redes_sociales scr-address-
list=IP_con_restricciones
- [admin@Router_LAN] > IP firewall filter add action=accept
chain=forward
comment=Permitir_conexiones_establecidas_relacionadas_internet
connection-state=established,related

- [admin@Router_LAN] > IP firewall filter add action=drop chain=forward comment=Rechazar_conexiones_invalidas_intenet connection-state=invalid
- [admin@Router_LAN] > IP firewall filter add action=accept chain=forward comment=Permitir_navegacion_IPs

Pruebas de conectividad en equipos y *hosts*

Se realizó las pruebas de acceso y restricciones en la red por medio de la utilización del comando *PING* y *SSH*, para ello es necesario ingresar al *CMD* de *Windows*.

La primera prueba realizada es la negación de la dirección *IP* 192.168.10.25 para hacer *PING* al *router*, ver figura 3.173.

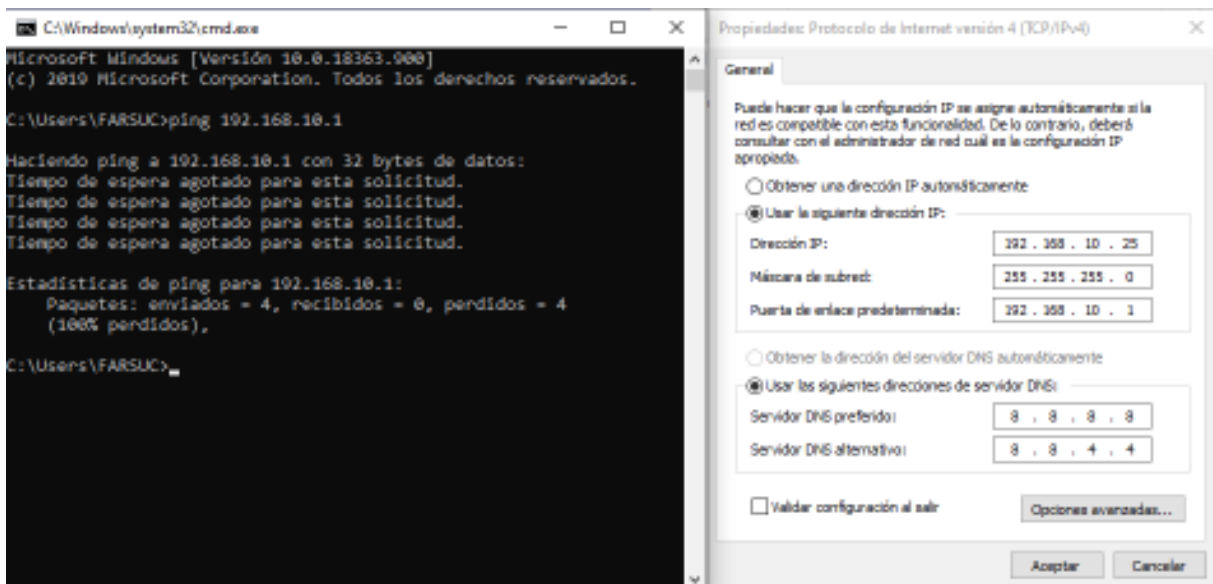


Figura 3.173 Prueba de bloqueo PING al *router*

La segunda prueba realizada es el bloqueo o la restricción de la página de *Facebook* para la *IP* 192.168.10.25 de acuerdo con las reglas *firewall*, ver figura 3.174.

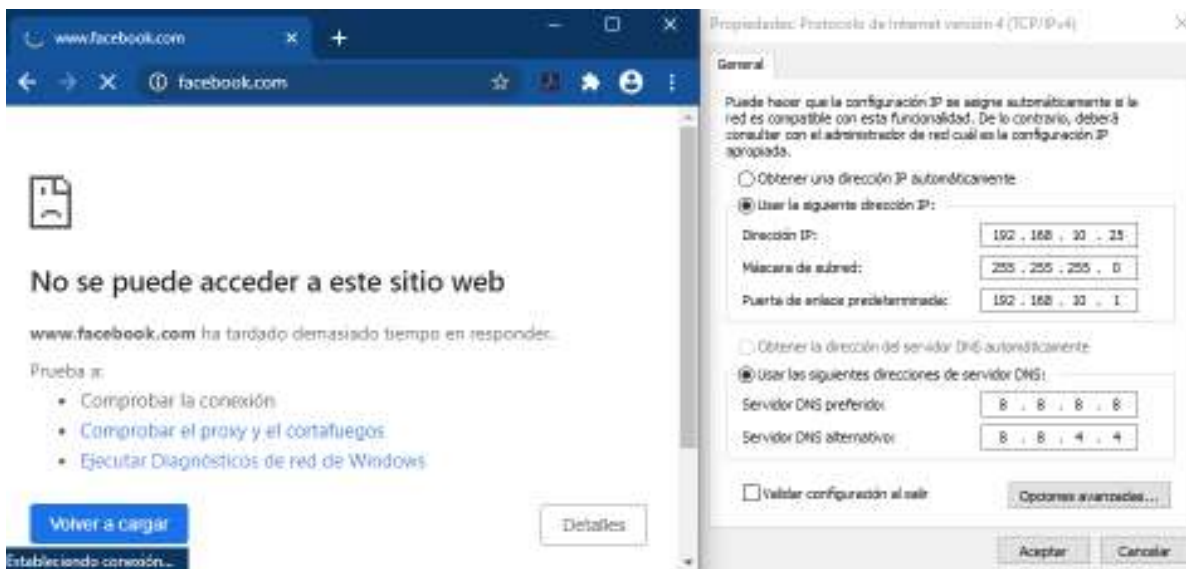


Figura 3.174 Prueba de bloqueo de página Facebook

La tercera prueba realizada es el bloqueo de la dirección IP 192.168.10.25 para acceder al router por medio de SSH. Para ello se utiliza el software PuTTY, ver figura 3.175.



Figura 3.175 Prueba de bloqueo por SSH al router

❖ Practica N°7

Tema: Colas simples

Objetivo: Configuración de colas simples en *router MikroTik*

Objetivos Específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*
- Configuración de interfaces *WAN*, *LAN1* y *LAN2*
- Configuración de brigde en Ether2 y Ether3
- Configuración de acceso a internet
- Configuración de colas padre e hijos en *LAN1*
- Configuración de ráfagas de velocidad en *LAN2*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

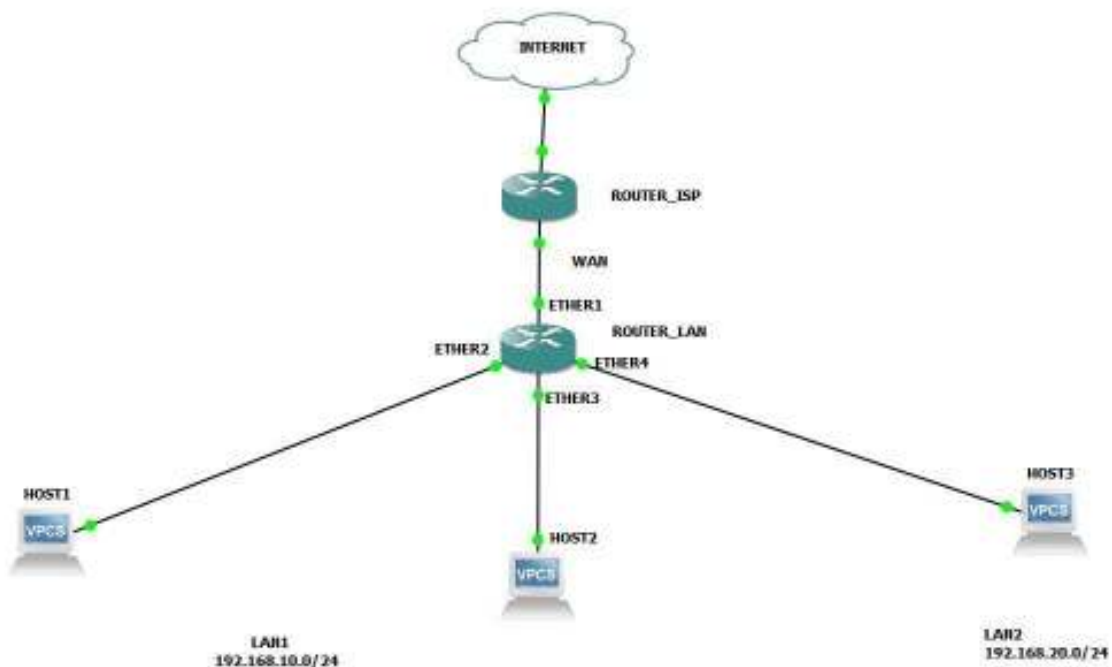


Figura 3.176 Topología de colas simples

Tabla de direcciones IP

A continuación, se muestra la tabla 3.15 de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Tabla 3.15 Direccionamiento IP en redes WAN, LAN y hosts

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
WAN	ISP	ISP	R1(Ether1)	ISP	ISP
LAN1	192.168.10.0	/24	R1(Ether2-3)	192.168.10.1	/24
LAN2	192.168.20.0	/24	R1(Ether4)	192.168.20.1	/24

Tabla de reglas en hosts

A continuación, se muestra la tabla 3.16 de anchos de banda para cada host.

Tabla 3.16 Tabla de anchos de banda en hosts

Nombre	Dirección IP	Máscara	Reglas
Host1	192.168.10.254	/24	Max-Limit: 1M (up) / 1M (down) Limit at: 512K (up) / 512K (down)
Host2	192.168.10.253	/24	Max-Limit: 1M (up) / 1M (down) Limit at: 512K (up) / 512K (down)
Host2	192.168.20.254	/24	Max-Limit: 1M (up) / 1M (down) Burst limit: 2M (up) / 2M (down) Burst threshold: 512K (up) / 512K (down) Burst time: 16 s (up) / 16 s (down)

Configuración vía interfaz gráfica

Cambio de nombre en el router

Para el cambio de nombre ingresamos *System/Identity*, ver figura 3.177.

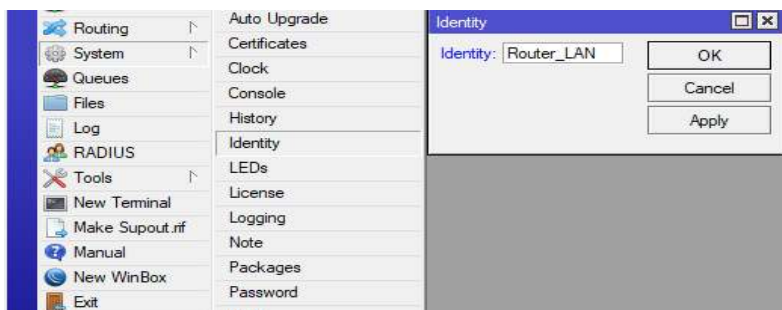


Figura 3.177 Identificación de *router*

Configuración de *bridge* en *LAN1*

Para la configuración se selecciona en el menú la opción *Bridge*, y se selecciona la opción (+). A continuación, en *General* se coloca un nombre al bridge (*Name*) y luego se da en *Apply/Ok*, ver figura 3.178.

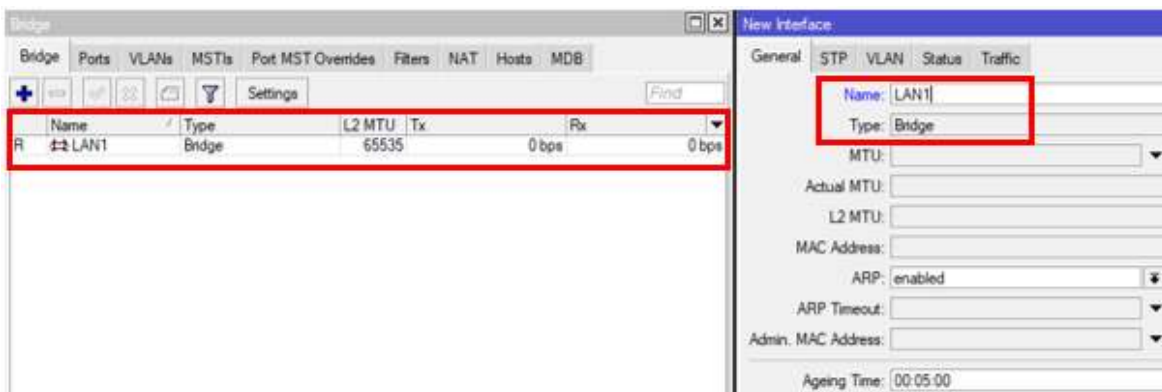


Figura 3.178 Configuración de nombre al *bridge*

En *Ports* se elige la opción (+) y se ingresa las interfaces que van a pertenecer al bridge (*Interface*). En *Bridge* se selecciona el nombre dado al bridge y luego se da elige *Apply/Ok*, ver figura 3.179.

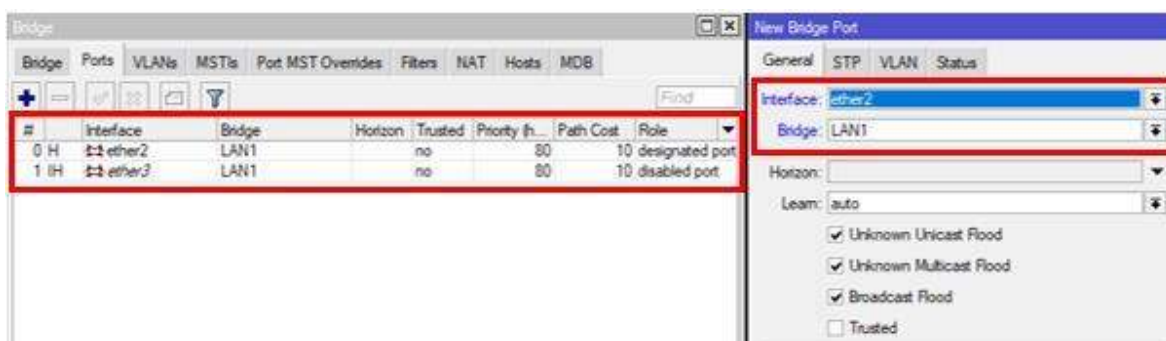


Figura 3.179 Configuración de interfaces del *bridge*

Configuración de interfaces *WAN*, *LAN1* y *LAN2*

Para la configuración se selecciona en el menú la opción *IP/Addresses* y se ingresa las direcciones *IP* de cada interfaz. Se configura las interfaces de ether 1, 2 y 4 para *WAN*, *LAN1* y *LAN2* respectivamente. Se ingresa su respectivo comentario de identificación, ver figura 3.180.

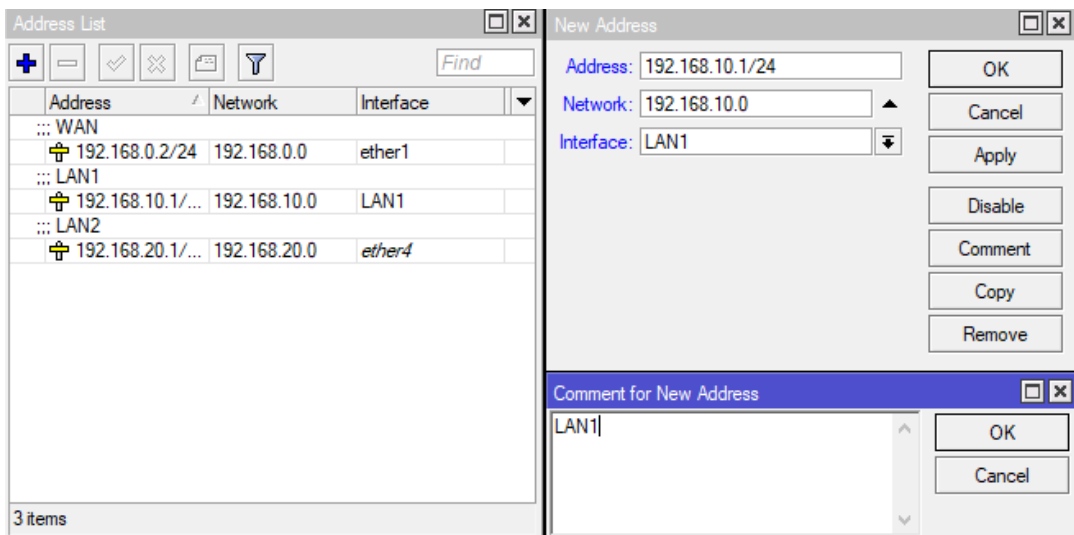


Figura 3.180 Configuración de interfaces en router

Configuración de acceso a Internet

Para tener acceso a Internet se selecciona la opción *IP/Routes* y se selecciona la opción (+). A continuación, es necesario crear una ruta para la salida de paquetes, para ello se crea una ruta por defecto 0.0.0.0/0 (*Dts. Address*) y una *IP* de salida (*Gateway*). En este caso el enlace *WAN* en el extremo del *ISP* tiene la dirección *IP* 192.168.0.1/24 y se ingresa su respectivo comentario de identificación, ver figura 3.181.

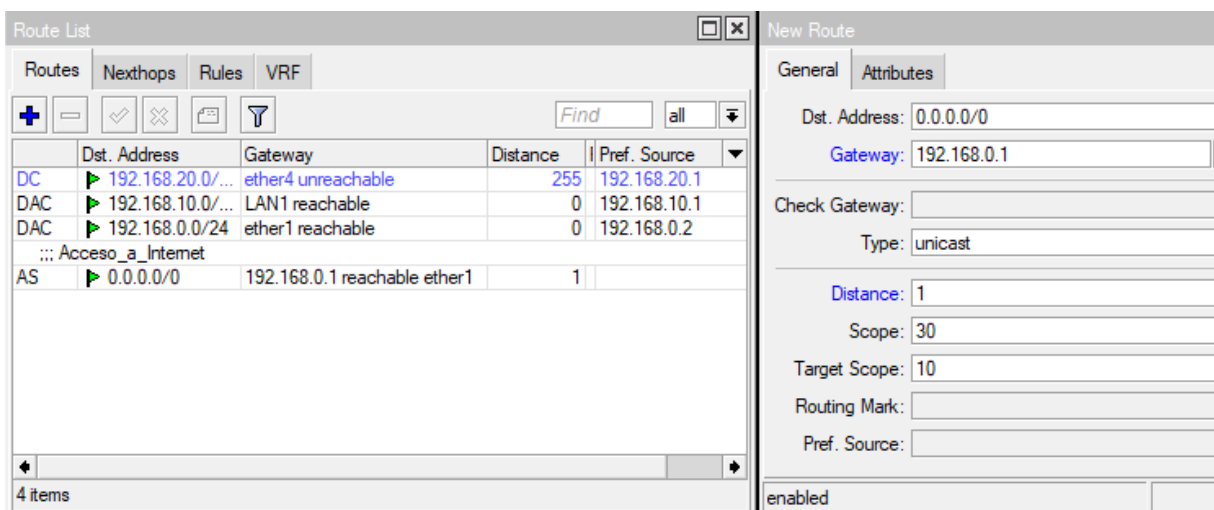


Figura 3.181 Configuración de ruta para acceso a Internet

Ahora se debe realizar el enmascaramiento de nuestra red local *LAN* para tener salida a internet. Para ello es necesario ir a *IP/Firewall* y en la opción de *NAT* en General, en el casillero *Chain* colocamos *srcnat* que indica los paquetes originados en la red *LAN*. En el casillero *Out. Interface* se coloca la interfaz que está conectada con la red *WAN*, que es la

salida a internet. En *Action* en el casillero *Action* se elige la opción *masquerade* y se ingresa su respectivo comentario de identificación, ver figura 3.182.

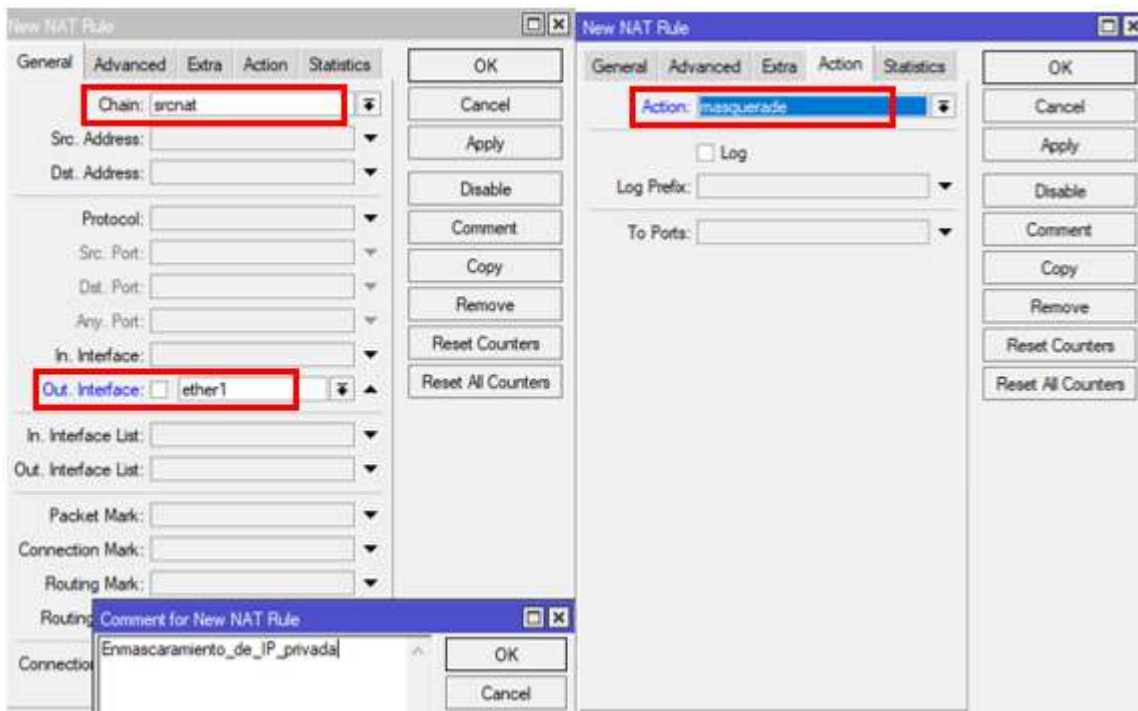


Figura 3.182 Configuración de enmascaramiento

Ahora se observa la lista de configuraciones realizadas en *NAT*, ver figura 3.183.

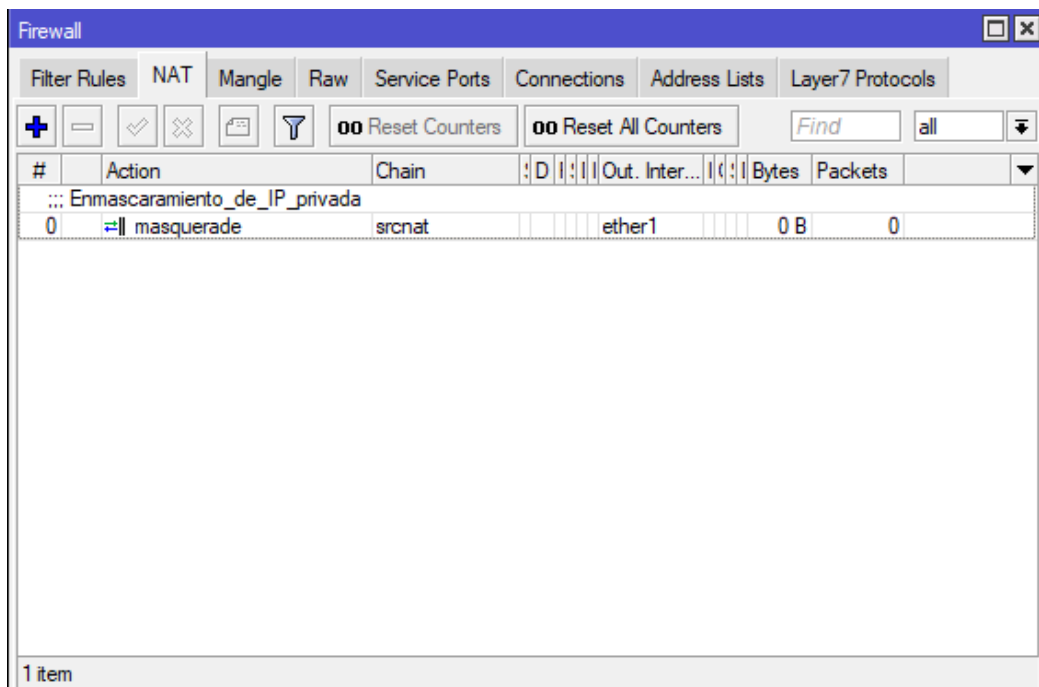


Figura 3.183 Lista de configuración NAT

Configuración de colas padre e hijos en LAN1

Configuración de cola padre

Para la creación de la cola padre se selecciona la opción *Queues*. En el casillero *Simple Queues* se escoge la opción (+) y se ingresa el nombre que se identificara a la cola simple (*Name*). Luego se ingresa la dirección *IP* o red a la que pertenecerá la cola padre (*Target*), A continuación, se ingresa ancho de banda máximo a otorgar tanto en carga como en descarga (*Max Limit*). Se ingresa su respectivo comentario de identificación y se elige *Apply* y *Ok*, ver figura 3.184.

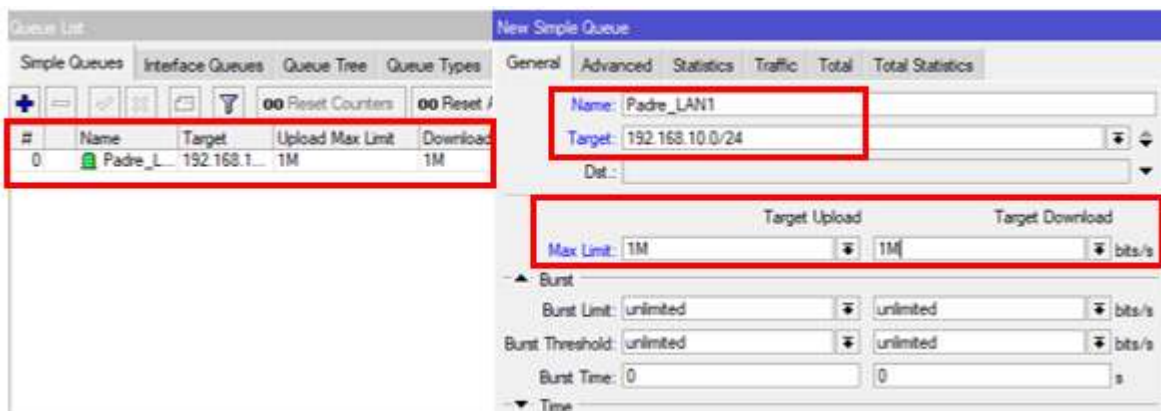


Figura 3.184 Configuración de cola padre

Configuración de colas hijos en LAN1

En el casillero *Simple Queues* se selecciona la opción (+) y se ingresa el nombre que se identificara a la cola simple (*Name*). Luego se ingresa la dirección *IP* que corresponde a la cola hijo (*Target*), A continuación, se ingresa ancho de banda máximo a otorgar tanto en carga como en descarga (*Max Limit*), en el casillero *Advanced* en la opción *Limit AT*: se ingresa el ancho de banda mínimo que debe tener cada *host*. En la opción *Parent* se selecciona el nombre de la cola padre a la que pertenece la cola hijo. Se ingresa su respectivo comentario de identificación se elige *Apply* y *Ok*, ver figura 3.185.

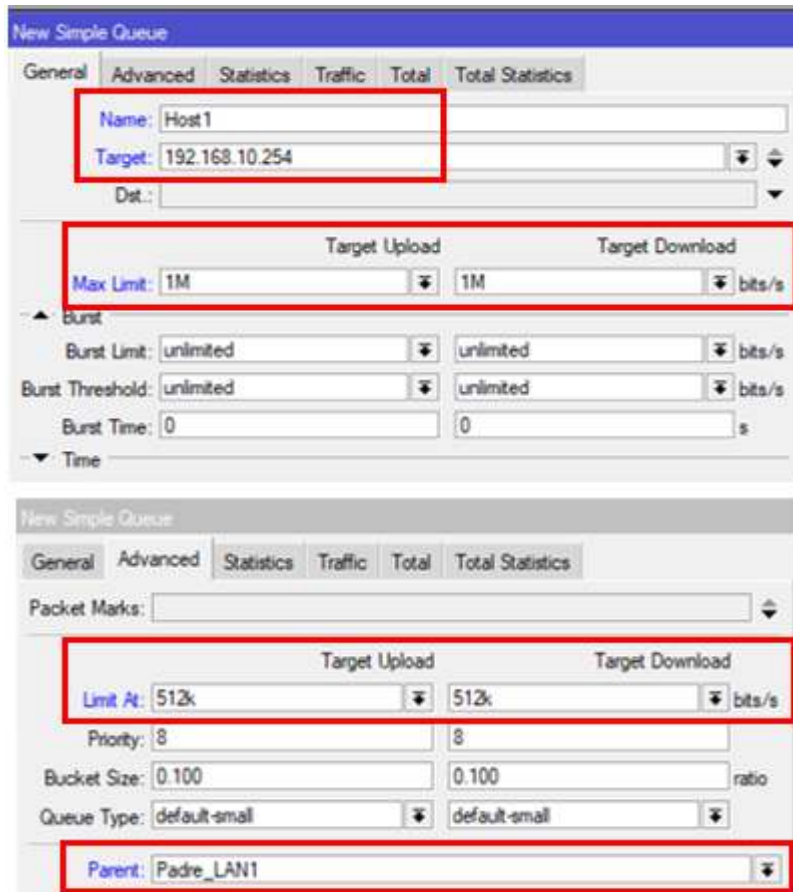


Figura 3.185 Configuración de cola hijo

A continuación, se presenta la lista de colas configuradas, ver figura 3.186.

#	Name	Target	Upload Max Limit	Download Max Limit
0	Padre_LAN1	192.168.10.0/24	1M	1M
	::: Hijo1_LAN1			
1	Host1	192.168.10.254	1M	1M
	::: Hijo2_LAN1			
2	Host2	192.168.10.253	1M	1M

3 items 0 B queued 0 packets queued

Figura 3.186 Lista de configuración de colas padre e hijos

Configuración de ráfagas de velocidad en LAN2

En el casillero *Simple Queues* se selecciona la opción (+) y se ingresa el nombre que se identificara a la cola simple (*Name*). Luego se ingresa la dirección *IP* que corresponde a la ráfaga de velocidad (*Target*), A continuación, se ingresa ancho de banda máximo a otorgar tanto en carga como en descarga (*Max Limit*), en la opción *Burst Limit* se ingresa el ancho de banda que va alcanzar la ráfaga, en *Burst Threshold* se ingresa el ancho de banda donde se activara la ráfaga, en *Burst Time* se ingresa el tiempo de muestreo en el que se obtiene la velocidad promedio. Se ingresa su respectivo comentario de identificación y se elige *Apply* y *Ok*, ver figura 3.187.

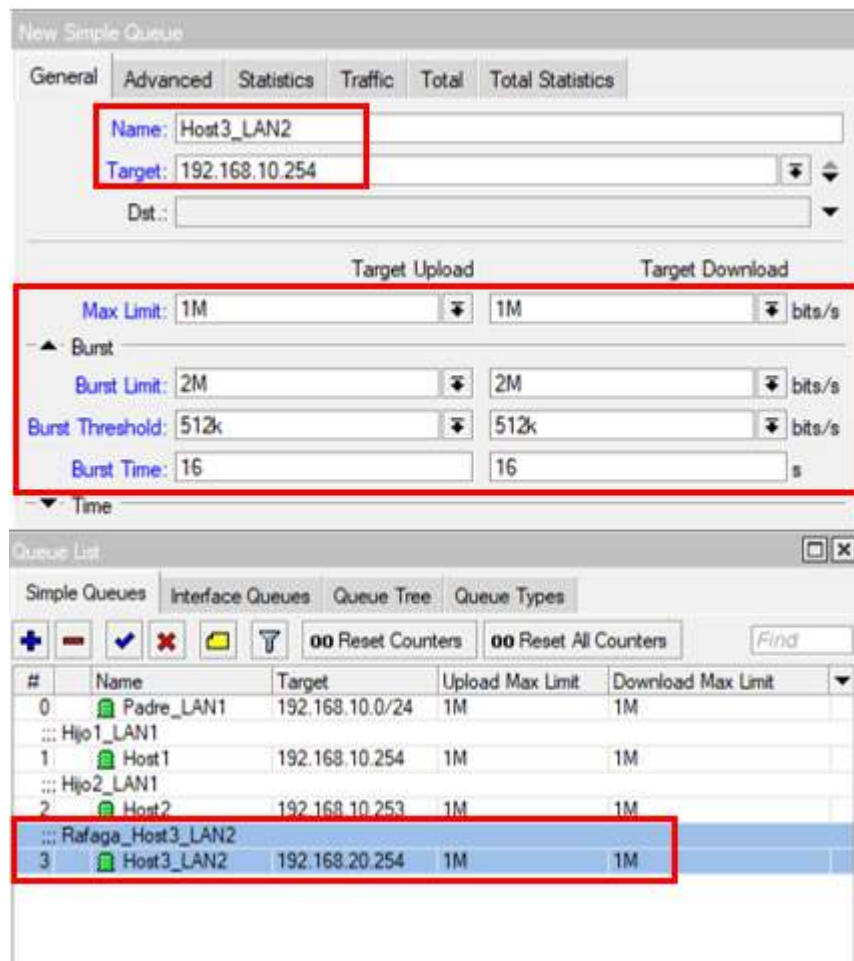


Figura 3.187 Configuración de ráfagas en LAN2

Configuración de hosts

Para la configuración de *host* se ingresa a las propiedades de la tarjeta de red y se coloca las *IPs* correspondientes, ver figura 3.188.

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

Servidor DNS alternativo:

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

Servidor DNS alternativo:

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

Servidor DNS alternativo:

Figura 3.188 Configuración de tarjeta de red en *hosts*.

Configuración vía comandos

Cambio de nombre en el *router*

Para su configuración se ingresa el comando *system/identity*

```
- [admin@MikroTik] > system identity set name=Router_LAN
```

Configuración de *bridge* en LAN1

Para su configuración se ingresa el comando *interface bridge*

```
- [admin@Router_LAN] > interface bridge add name=LAN1
```


- [admin@Router_LAN] > interface brigde port add interface=ether2
brigde=LAN1
- admin@Router_LAN] > interface brigde port add interface=ether3
brigde=LAN1

Configuración de interfaces *WAN, LAN1 y LAN2.*

Para su configuración se ingresa el comando *IP address*

- [admin@Router_LAN] > IP address add address=192.168.0.2/24
comment=WAN interface=ether1
- [admin@Router_LAN] > IP address add address=192.168.10.1/24
comment=LAN interface=LAN1
- [admin@Router_LAN] > IP address add address=192.168.20.1/24
comment=LAN interface=ether4

Configuración de acceso a Internet

Para el acceso a Internet se crea una ruta por defecto ingresando el comando *IP route*.

- [admin@Router_LAN] > IP route add distance=1 dst-address=0.0.0.0/0
gateway=192.168.0.1 comment=Acceso_a_Internet

Ahora se ingresa el comando *IP firewall* para el enmascaramiento de los paquetes de la red *LAN*.

- [admin@Router_LAN] > IP firewall nat add action=masquerade
chain=srcnat out-interface=ether1

Configuración de colas padre e hijos en *LAN1*

Configuración de cola padre

Para la configuración de colas padre se ingresa el comando *queue simple*.

- [admin@Router_LAN] > queue simple add name=Padre_LAN1
target=192.168.10.0/24 max-limit=1M/1M

Configuración de colas hijos en *LAN1*

Para la creación de lista de direcciones IP se ingresa el comando *queue simple*.

- [admin@Router_LAN] > queue simple add name=Host1
target=192.168.10.254 max-limit=1M/1M limit-at=512k/512k
parent=Padre_LAN1 comment=Hijo1_LAN1

```

- [admin@Router_LAN] > queue simple add name=Host2
target=192.168.10.253 max-limit=1M/1M limit-at=512k/512k
parent=Padre_LAN1 comment=Hijo2_LAN1

```

Configuración de ráfagas de velocidad en LAN2

```

- [admin@Router_LAN] > queue simple add name=Host3_LAN2
target=192.168.20.254 max-limit=1M/1M burst-limit=2M/2M burst-
threshold=512k/512k burst-time=16/16 comment=Rafaga_Host3_LAN2

```

Pruebas de conectividad en equipos y hosts

Se realizó las pruebas de control de ancho de banda en *hosts* por medio de test de velocidad.

La primera prueba realizada es la velocidad de navegación en *Host1* donde el ancho de banda no debe superar el *Max Limit* de la cola padre, ver figura 3.189.

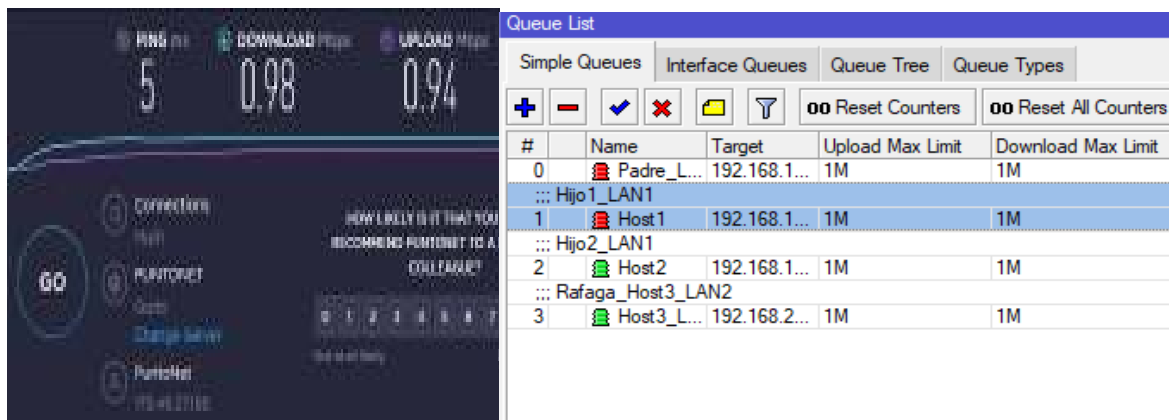


Figura 3.189 Prueba de ancho de banda en *Host1*

La segunda prueba realizada es la velocidad de navegación en *Host2* donde el ancho de banda no debe superar el *Max Limit* de la cola padre, ver figura 3.190.

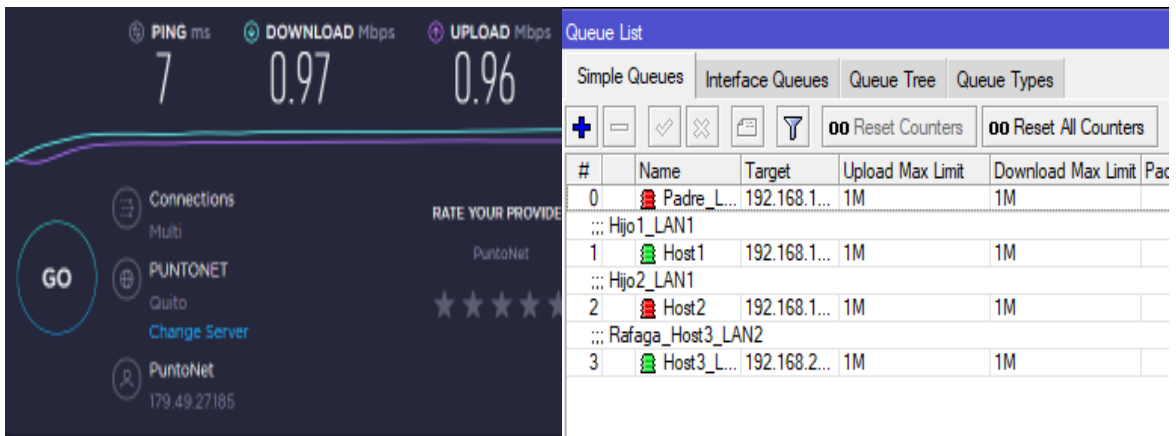


Figura 3.190 Prueba de ancho de banda en Host2

La tercera prueba realizada es la ráfaga de velocidad permitida en Host3, ver figura 3.191.

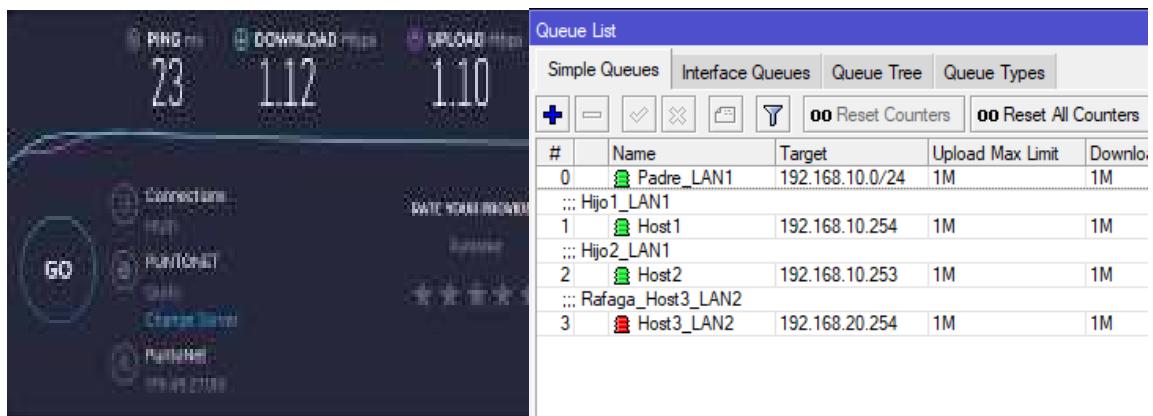


Figura 3.191 Prueba de ráfaga de velocidad en Host3

❖ Practica N°8

Tema: VLANs

Objetivo: Configuración de VLANs en *routers* y *switchs MikroTik*

Objetivos Específicos:

- Diseñar una topología de red con *routers* y *switchs MikroTik*
- Configuración de brigde en Ether2 y Ether3
- Configuración de VLANs en *router*
- Configuración de *DHCP* en VLANs y acceso a internet
- Configuración de VLANs en *switch*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

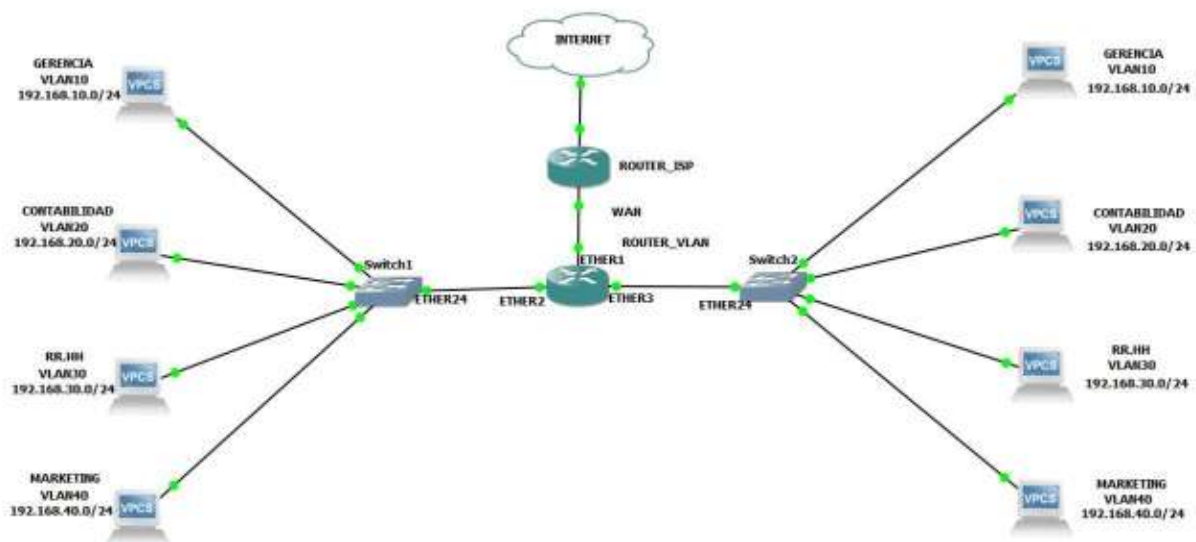


Figura 3.192 Topología de VLANs

Tabla de direcciones IP en VLANs

A continuación, se muestra la tabla 3.17 de distribución de direcciones IP para VLANs.

Tabla 3.17 Direccionamiento IP para VLANs

Nombre de VLAN	VLAN ID	Red	Máscara	IP en router	Interfaces switch
Gerencia	10	192.168.10.0	/24	192.168.10.1	Ether1-Ether5
Contabilidad	20	192.168.20.0	/24	192.168.20.1	Ether6-Ether10
RR.HH	30	192.168.30.0	/24	192.168.30.1	Ether11-Ether15
Marketing	40	192.168.40.0	/24	192.168.40.1	Ether16-Ether20

Configuración vía interfaz gráfica

Cambio de nombre en el router

Para el cambio de nombre ingresamos *System/Identity*, ver figura 3.193.

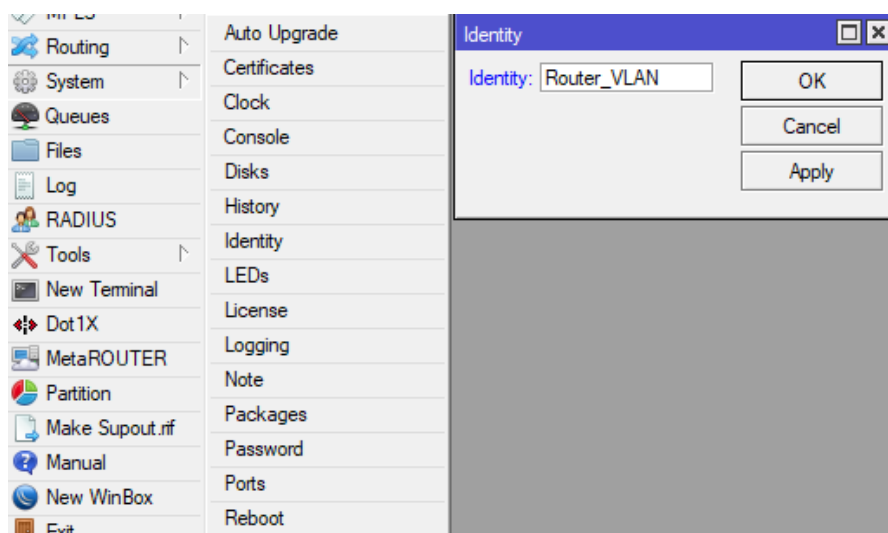


Figura 3.193 Identificación de router

Configuración de bridge

Para la configuración se selecciona en el menú la opción *Bridge*, y se selecciona la opción (+). A continuación, en *General* se coloca un nombre al bridge (*Name*) y luego se da en *Apply/Ok*, ver figura 3.194.

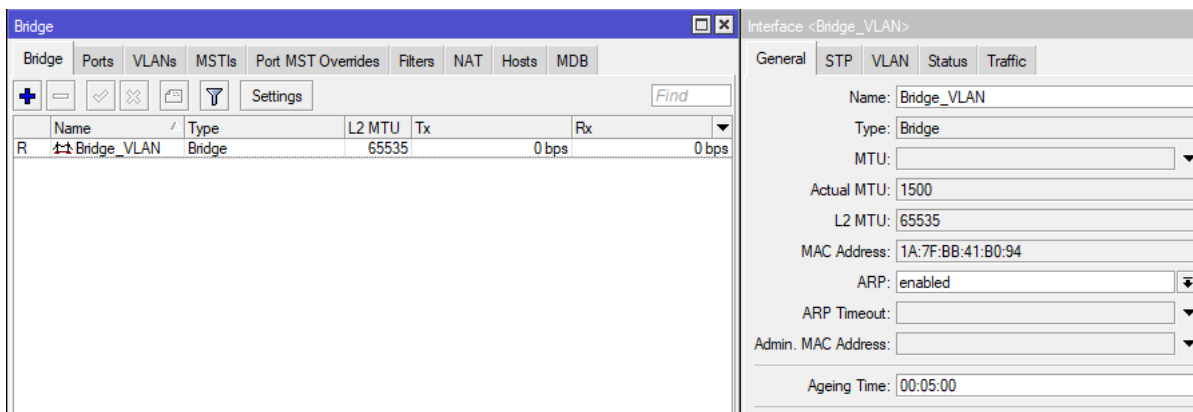


Figura 3.194 Configuración de nombre al *bridge* para VLANs

En Ports se *elige la opción (+)* y se ingresa las interfaces que van a pertenecer al bridge (*Interface*). En *Bridge* se selecciona el nombre dado al bridge y luego se da *elige Apply/Ok*, ver figura 3.195.

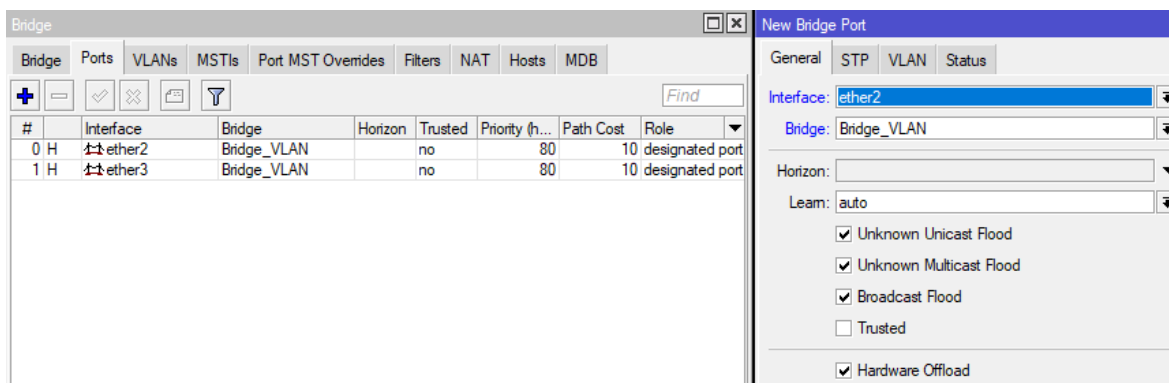


Figura 3.195 Configuración de interfaces del *bridge*

Configuración de VLANs en *router*

Para la configuración se selecciona en el menú la opción *Interface* y a continuación se elige la opción (+) donde se despliega un menú. En este menú se selecciona la opción *VLAN*, ver figura 3.196.

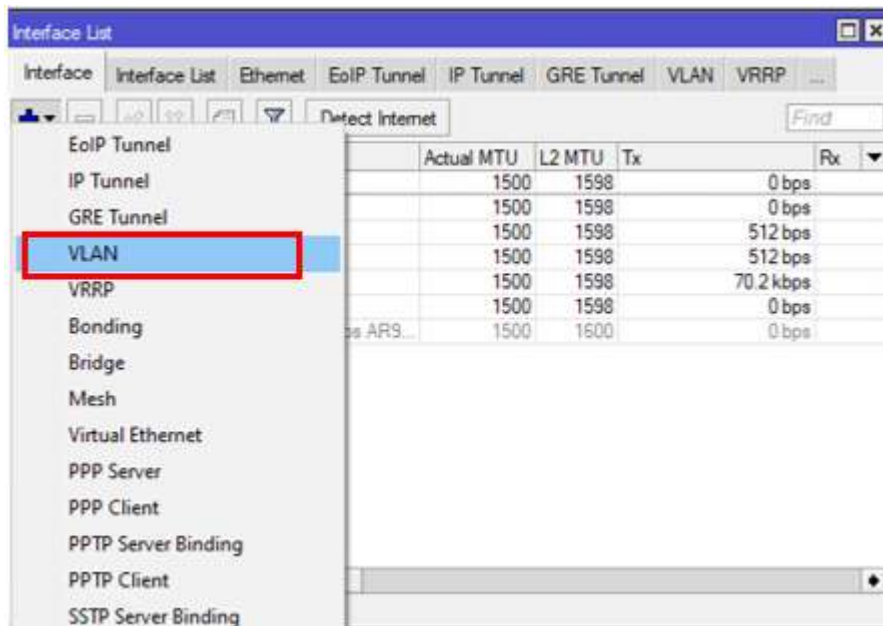


Figura 3.196 Ingreso a configuración VLANs

A continuación, se aprecia una nueva ventana donde se ingresa el nombre asignado a cada VLAN (*Name*), el valor de cada LAN Virtual (*VLAN ID*) y la interfaz a la que estará conectada (*Interface*). ver figura 3.197.

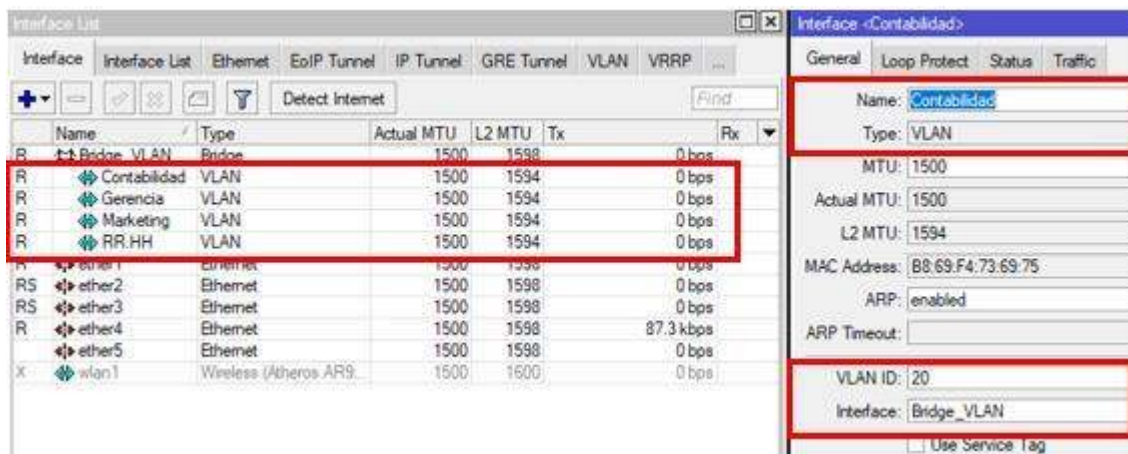


Figura 3.197 Configuración de VLANs

Para la asignación de un direccionamiento *IP* a las *VLANs* se selecciona en el menú la opción *IP/Addresses* y se ingresa las direcciones *IP* para cada *VLAN*. Se ingresa su respectivo comentario de identificación, ver figura 3.198.

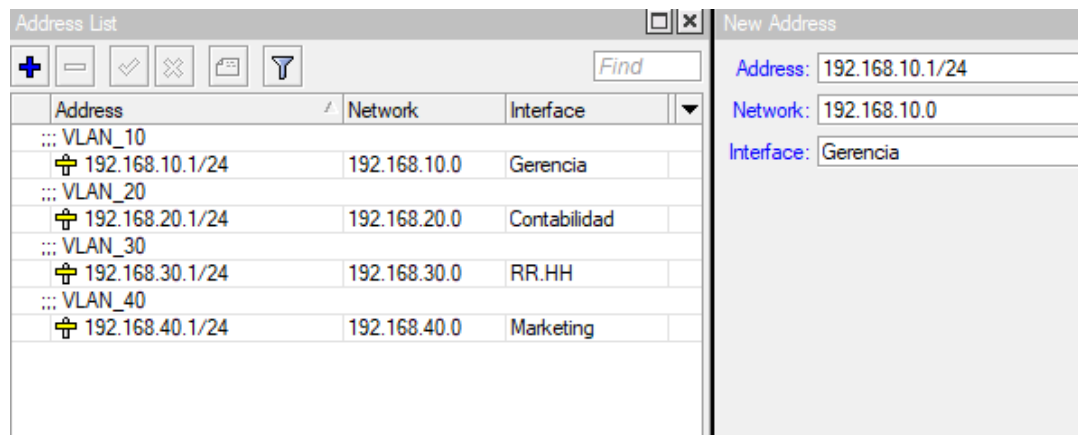


Figura 3.198 Configuración de interfaces en VLANs

Configuración de *DHCP* en *VLANs* y acceso a Internet

Para la configuración de *DHCP* en *VLANs* se configura el DNS del equipo, para ello en el menú se selecciona la opción *IP/DNS*, en la opción *Servers* se coloca la dirección *IP* de los servidores *DNS*, ver figura 3.199.

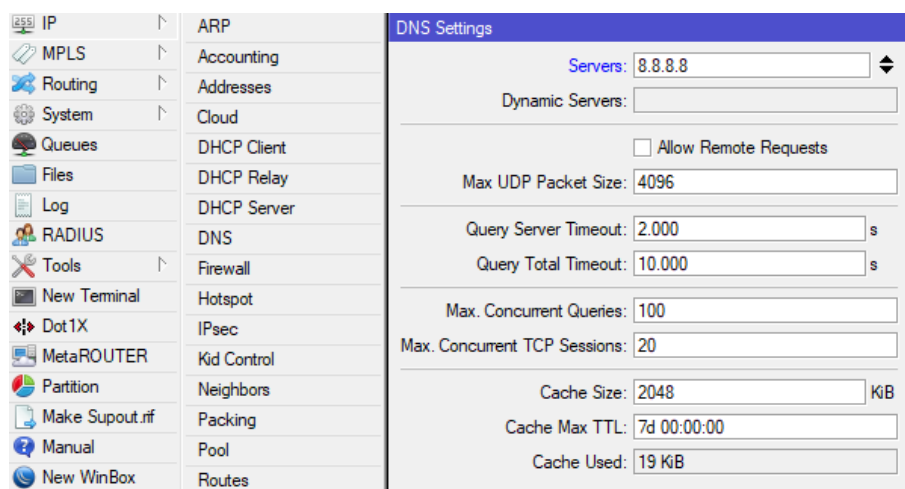


Figura 3.199 Configuración de *DNS*

Ahora se ingresa a la opción *IP/DHCP Server*, se selecciona la opción *DHCP Setup* donde se elige las *VLANs* que entregaran direcciones *IP* de forma dinámica, ver figura 3.200.

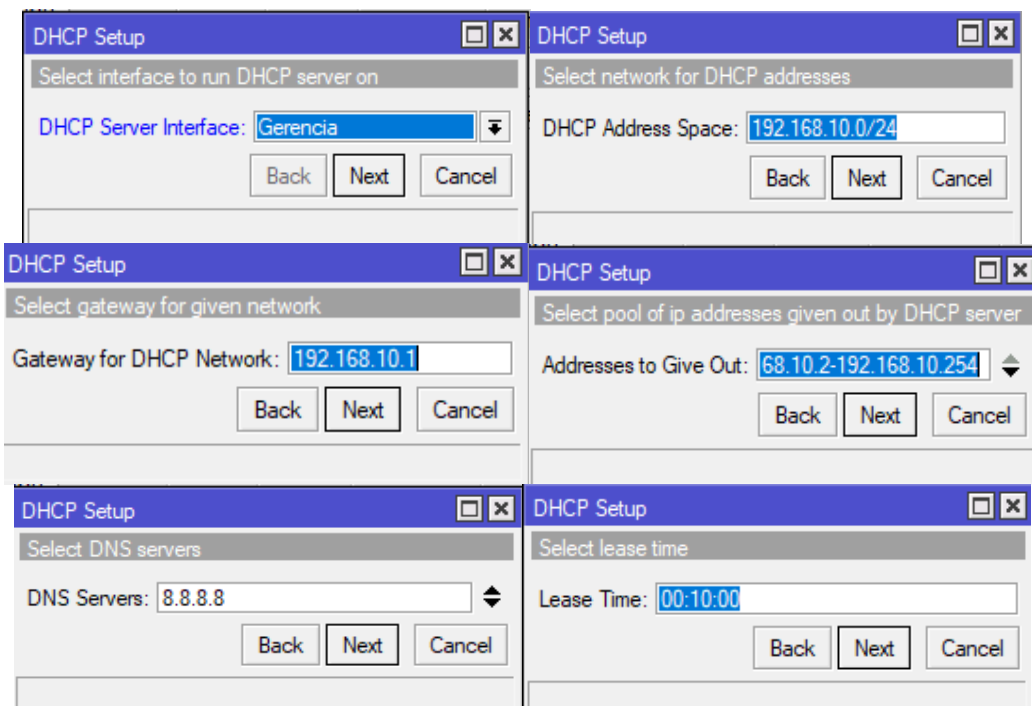


Figura 3.200 Configuración de *DHCP server*

A continuación, se muestra la lista de configuración de *DHCP Server*, ver figura 3.201.

The screenshot shows the DHCP Server configuration window with the following data in the DHCP Config tab:

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	Gerencia		00:10:00	dhcp_pool0	no
dhcp2	Contabilidad		00:10:00	dhcp_pool1	no
dhcp3	RR.HH		00:10:00	dhcp_pool2	no
dhcp4	Marketing		00:10:00	dhcp_pool3	no

4 items

Figura 3.201 Lista de configuraciones de *DHCP server*

Para tener acceso a Internet se levanta la interfaz *ether1* del *router* de acuerdo con el direccionamiento *IP* del *ISP*. En este caso el *ISP* tiene la red 192.168.0.0/24 y se coloca la dirección 192.168.0.2/24 para levantar la interfaz, ver figura 3.202.

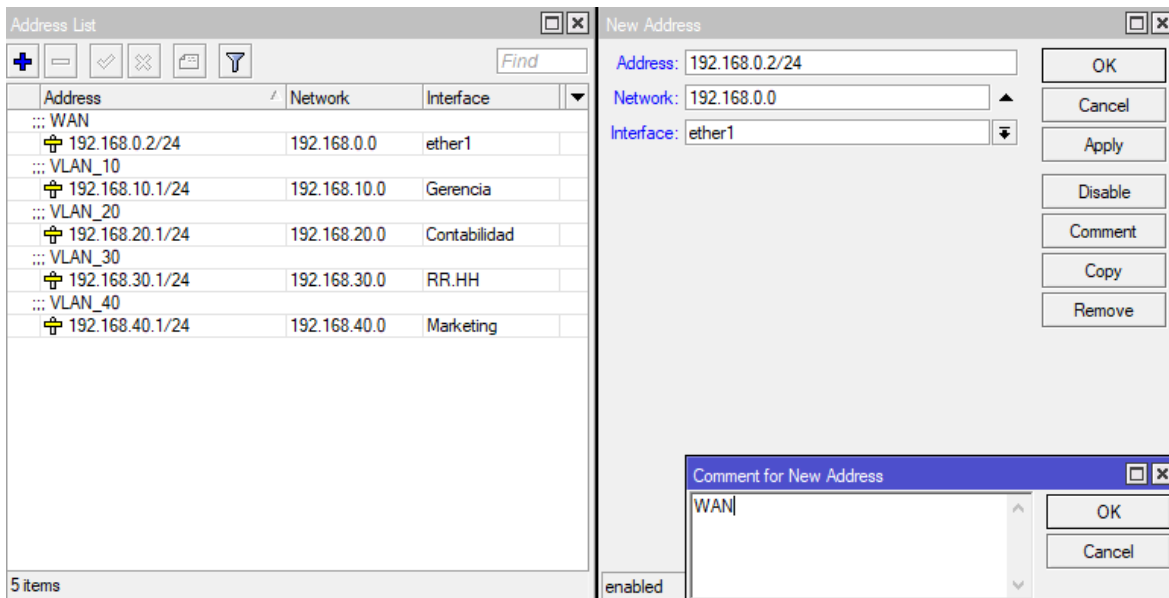


Figura 3.202 Configuración de enlace WAN

Ahora se selecciona la opción *IP/Routes* y se selecciona la opción (+). A continuación, es necesario crear una ruta para la salida de paquetes, para ello se crea una ruta por defecto 0.0.0.0/0 (*Dts. Address*) y una *IP* de salida (*Gateway*). En este caso el enlace *WAN* en el extremo del *ISP* tiene la dirección *IP* 192.168.0.1/24 y se ingresa su respectivo comentario de identificación, ver figura 3.203.

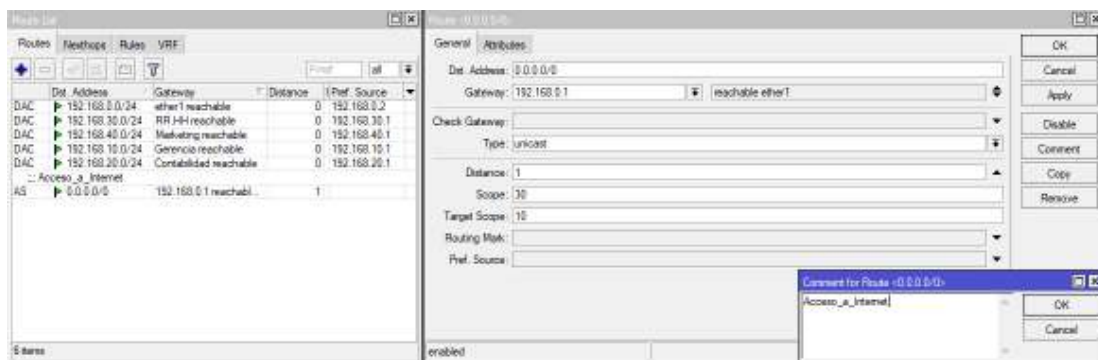


Figura 3.203 Configuración de ruta para acceso a Internet

Ahora se debe realizar el enmascaramiento de nuestra red local *LAN* para tener salida a Internet. Para ello es necesario ir a *IP/Firewall* y en la opción de *NAT* en *General*, en el casillero *Chain* colocamos *srcnat* que indica los paquetes originados en la red *LAN*. En el casillero *Out. Interface* se coloca la interfaz que está conectada con la red *WAN*, que es la salida a internet. En *Action* en el casillero *Action* se elige la opción *masquerade* y se ingresa su respectivo comentario de identificación, ver figura 3.204.

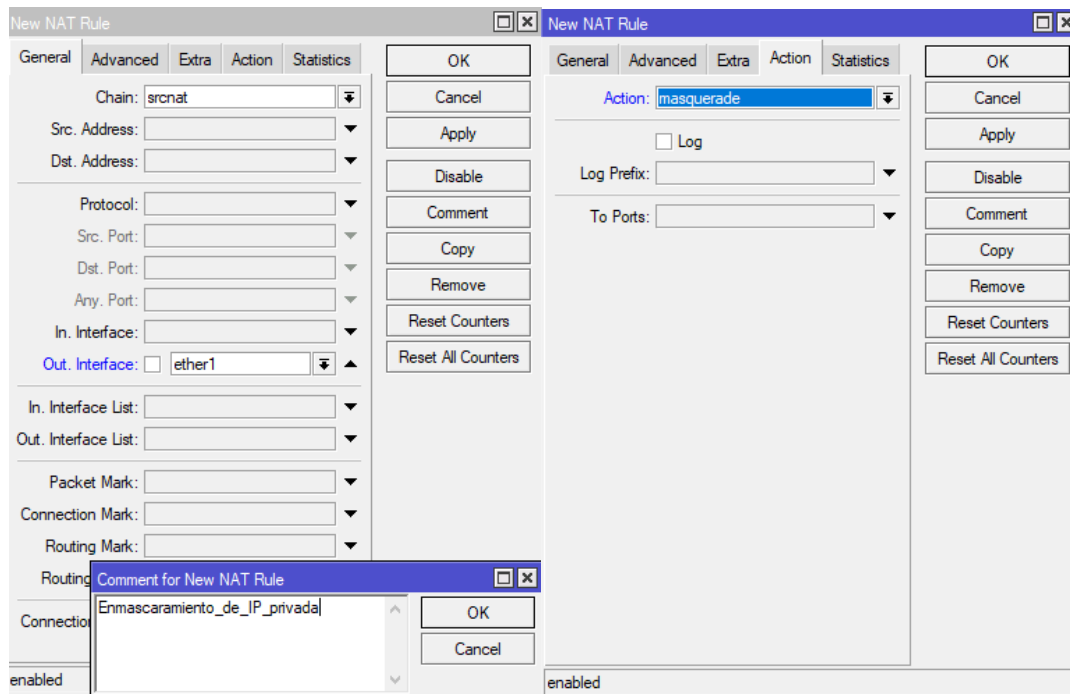


Figura 3.204 Configuración de enmascaramiento

Ahora se observa la lista de configuraciones realizadas en NAT, ver figura 3.205.

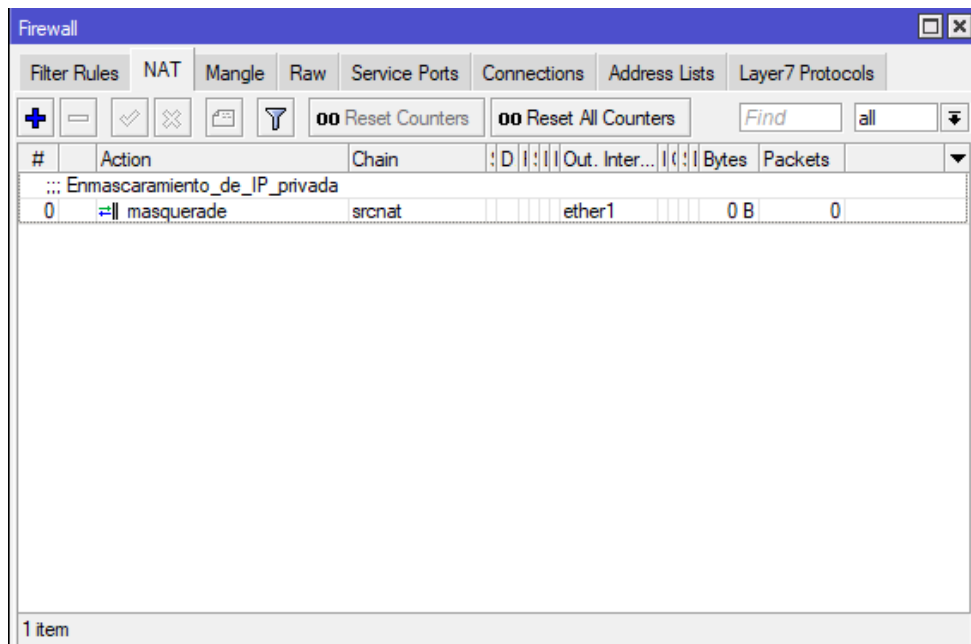


Figura 3.205 Lista de configuración NAT

Configuración de VLANs en switch1 y switch2

Para la configuración de VLANs en switch1 y switch2 es necesario cambiar la dirección IP del computador para que este dentro de la red 192.168.88.0/24, ver figura 3.206.

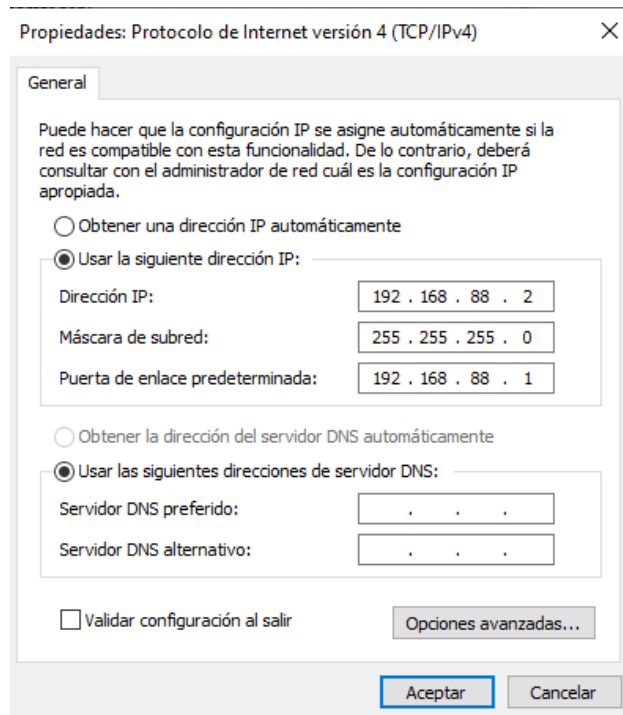


Figura 3.206 Cambio de dirección *IP* en computador

Ahora se ingresa a cualquier navegador y se coloca la dirección *IP* 192.168.88.1. A continuación, se ingresa el usuario y contraseña, al ser un equipo nuevo el usuario es *admin* y no cuenta con contraseña, ver figura 3.207.

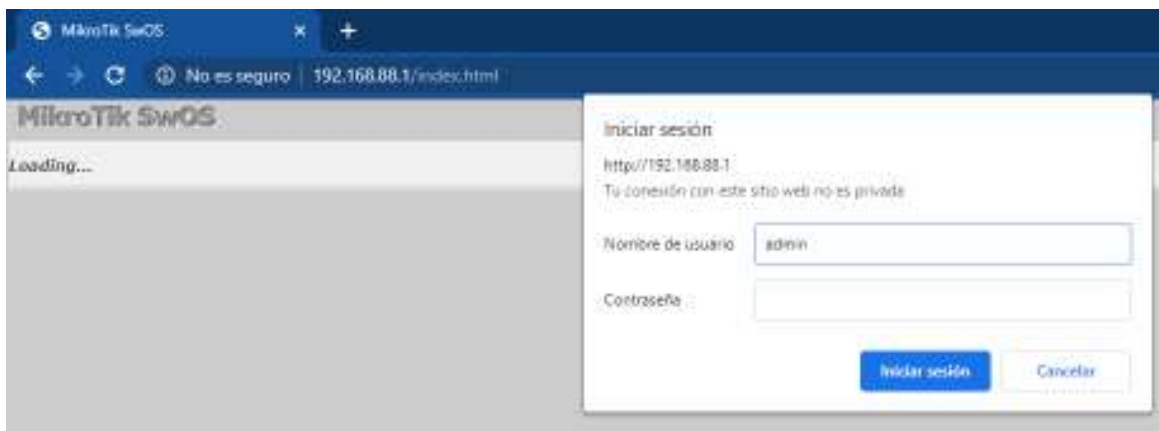


Figura 3.207 Ingreso a SwOS

Una vez ingresado al SwOS, en el casillero *VLANs*, se elige la opción *Append* para crear las *VLANs* creadas en el *router*, para ello se ingresa el valor de cada *VLAN* (*VLAN ID*), en la opción *Members* se selecciona los puertos que corresponden a cada *VLAN* y el puerto 24 como puerto troncal para llevar todo el tráfico. Después se selecciona la opción *Apply All* para guardar las configuraciones realizadas, figura 3.208.

Ahora es necesario configurar un puerto troncal que permite transportar todo el tráfico de las VLANs Gerencia, Contabilidad, RR.HH, *Marketing*, para ello se selecciona el puerto 24 y en opción *VLAN Mode* se selecciona la opción *strict* y en *VLAN Receive* se elige la opción *only tagged*. Después se selecciona la opción *Apply All* para guardar las configuraciones realizadas, ver figura 3.210.

Port5	strict	only untagged	10	<input type="checkbox"/>
Port6	strict	only untagged	20	<input type="checkbox"/>
Port7	strict	only untagged	20	<input type="checkbox"/>
Port8	strict	only untagged	20	<input type="checkbox"/>
Port9	strict	only untagged	20	<input type="checkbox"/>
Port10	strict	only untagged	20	<input type="checkbox"/>
Port11	strict	only untagged	30	<input type="checkbox"/>
Port12	strict	only untagged	30	<input type="checkbox"/>
Port13	strict	only untagged	30	<input type="checkbox"/>
Port14	strict	only untagged	30	<input type="checkbox"/>
Port15	strict	only untagged	30	<input type="checkbox"/>
Port16	strict	only untagged	40	<input type="checkbox"/>
Port17	strict	only untagged	40	<input type="checkbox"/>
Port18	strict	only untagged	40	<input type="checkbox"/>
Port19	strict	only untagged	40	<input type="checkbox"/>
Port20	strict	only untagged	40	<input type="checkbox"/>
Port21	optional	any	1	<input type="checkbox"/>
Port22	optional	any	1	<input type="checkbox"/>
Port23	optional	any	1	<input type="checkbox"/>
Port24	strict	only tagged	1	<input type="checkbox"/>
SFP1	optional	any	1	<input type="checkbox"/>
SFP2	optional	any	1	<input type="checkbox"/>

Figura 3.210 Configuración de puerto troncal para VLANs

Configuración de *hosts*

Ahora es necesario configurar la tarjeta de red del computador para obtener una dirección *IP* de forma automática de acuerdo con cada *VLAN*, ver figura 3.211.

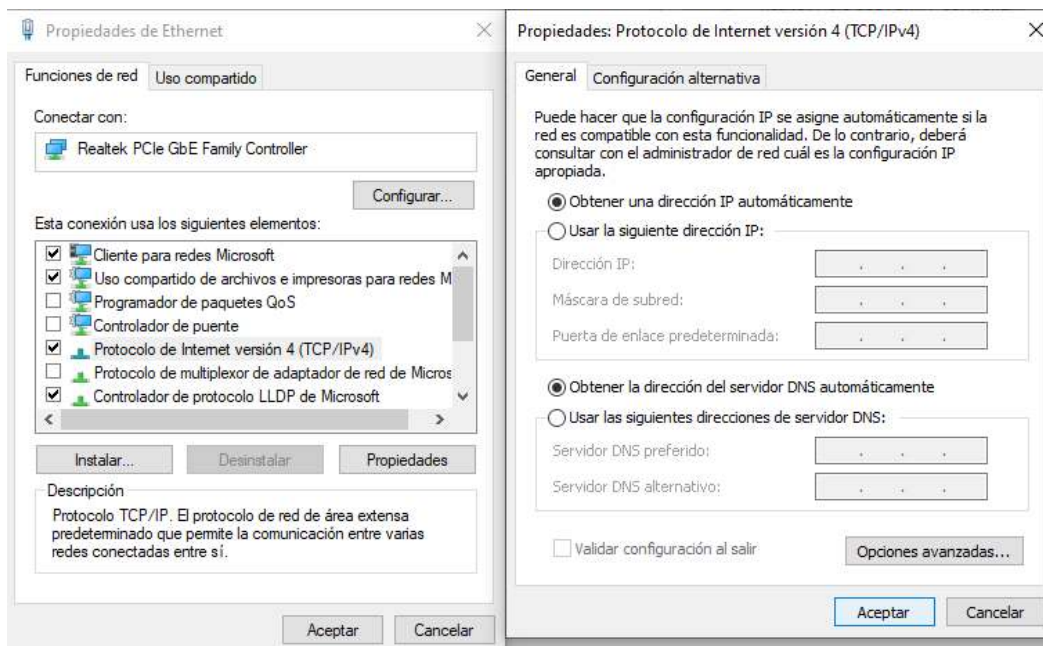


Figura 3.211 Configuración de tarjeta de red en *hosts*.

Configuración vía comandos

Cambio de nombre en el *router*

Para su configuración se ingresa el comando *system/identity*

- [admin@MikroTik] > system identity set name=Router_VLAN

Configuración de *bridge* en *LAN1*

Para su configuración se ingresa el comando *interface bridge*.

- [admin@Router_VLAN] > interface bridge add name=Bridge_VLAN
- [admin@Router_VLAN] > interface bridge port add interface=ether2
bridge=Bridge_VLAN
- admin@Router_VLAN] > interface bridge port add interface=ether3
bridge=Bridge_VLAN

Configuración de *VLANs* en *router*

Para su configuración de *VLANs* se ingresa el comando *interface VLAN*

- [admin@Router_VLAN] > interface vLAN add name=Gerencia vLAN-id=10
interface=Bridge_VLAN

- [admin@Router_VLAN] > interface vLAN add name=Contabilidad vLAN-id=20 interface=Bridge_VLAN
- [admin@Router_VLAN] > interface vLAN add name=RR.HH vLAN-id=30 interface=Bridge_VLAN
- [admin@Router_VLAN] > interface vLAN add name=Marketing vLAN-id=40 interface=Bridge_VLAN

Para la configuración de interfaces VLANs se ingresa el comando *IP address*

- [admin@Router_VLAN] > IP address add address=192.168.10.1/24 comment=VLAN_10 interface=Gerencia
- [admin@Router_VLAN] > IP address add address=192.168.20.1/24 comment=VLAN_20 interface=Contabilidad
- [admin@Router_VLAN] > IP address add address=192.168.30.1/24 comment=VLAN_30 interface=RR.HH
- [admin@Router_VLAN] > IP address add address=192.168.40.1/24 comment=VLAN_40 interface=Marketing

Configuración de DHCP en VLANs y acceso a Internet

Para la configuración de *DHCP* es necesario configurar DNS, para ello se ingresa el comando *IP dns*

- [admin@Router_VLAN] > IP dns set servers=8.8.8.8

Para la configuración de *DHCP* Server en cada VLAN se ingresa el comando *IP DHCP-server*.

- [admin@Router_VLAN] > IP DHCP-server setup
Select interface to run DHCP server on
DHCP server interface: Gerencia
Select network for DHCP addresses
DHCP address space: 192.168.10.0/24
Select gateway for given network
gateway for DHCP network: 192.168.10.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.10.2-192.168.10.254
Select DNS servers
dns servers: 8.8.8.8
Select lease time
lease time: 10m
- [admin@Router_VLAN] > IP DHCP-server setup


```

Select interface to run DHCP server on
DHCP server interface: Contabilidad
Select network for DHCP addresses
DHCP address space: 192.168.20.0/24
Select gateway for given network
gateway for DHCP network: 192.168.20.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.20.2-192.168.20.254
Select DNS servers
dns servers: 8.8.8.8
Select lease time
- [admin@Router_VLAN] > IP DHCP-server setup
Select interface to run DHCP server on
DHCP server interface: RR.HH
Select network for DHCP addresses
DHCP address space: 192.168.30.0/24
Select gateway for given network
gateway for DHCP network: 192.168.30.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.30.2-192.168.30.254
Select DNS servers
dns servers: 8.8.8.8
Select lease time
- [admin@Router_VLAN] > IP DHCP-server setup
Select interface to run DHCP server on
DHCP server interface: Marketing
Select network for DHCP addresses
DHCP address space: 192.168.40.0/24
Select gateway for given network
gateway for DHCP network: 192.168.40.1
Select pool of IP addresses given out by DHCP server
addresses to given out: 192.168.40.2-192.168.40.254
Select DNS servers
dns servers: 8.8.8.8
Select lease time

```

Para el acceso a Internet se levanta el enlace WAN, para ello se ingresa el comando *IP interface*.

```

- [admin@Router_VLAN] > IP address add address=192.168.0.2/24
comment=WAN interface=ether1

```

A continuación, se crea una ruta por defecto ingresando el comando *IP route*.

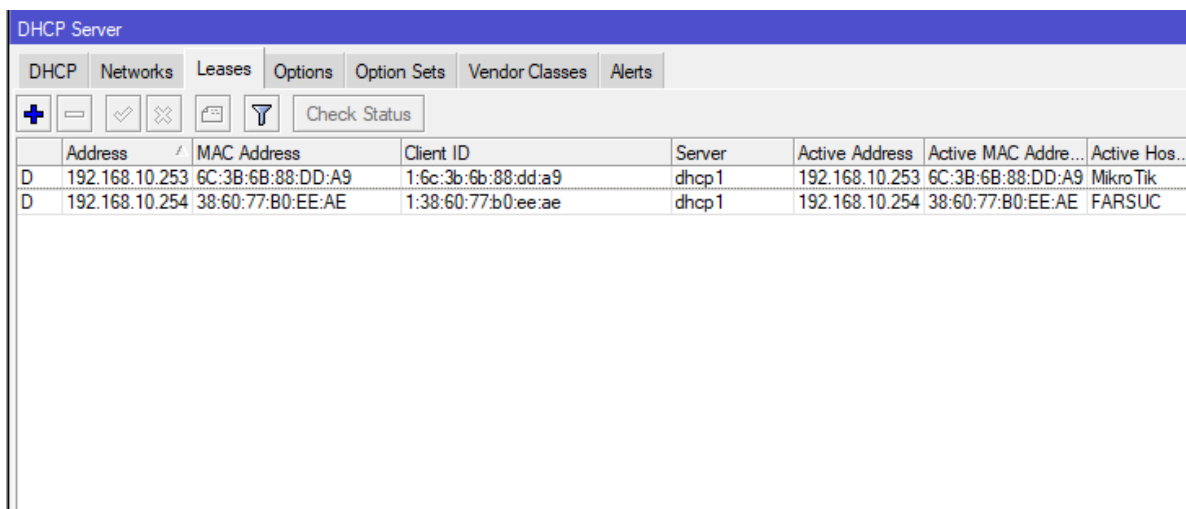
```
[admin@Router_VLAN] > IP route add distance=1 dst-address=0.0.0.0/0
gateway=192.168.0.1 comment=Acceso_a_Internet
```

Ahora se ingresa el comando *IP firewall* para el enmascaramiento de los paquetes de la red LAN.

```
[admin@Router_VLAN] > IP firewall nat add action=masquerade
chain=srcnat out-interface=ether1
```

Pruebas de conectividad en equipos y hosts

La primera prueba realizada es la entrega de direccionamiento *IP* en la *VLAN10* de Gerencia en *switch1* y *switch2*, ver figura 3.212.



The screenshot shows the DHCP Server configuration window in Mikrotik WinBox, specifically the Leases tab. The table below displays the active leases for the DHCP server.

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Hostname
D	192.168.10.253	6C:3B:6B:88:DD:A9	1:6c:3b:6b:88:dd:a9	dhcp1	192.168.10.253	6C:3B:6B:88:DD:A9	MikroTik
D	192.168.10.254	38:60:77:B0:EE:AE	1:38:60:77:b0:ee:ae	dhcp1	192.168.10.254	38:60:77:B0:EE:AE	FARSUC

Figura 3.212 Direccionamiento *IP* en arrendamiento *VLAN10*

La segunda prueba es la conectividad entre las *VLAN20* (Contabilidad) y *VLAN40* (Marketing), ver figura 3.213.

```
C:\Users\FARSUC>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.20.253
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.20.1

Adaptador de Ethernet vEthernet (Default Switch):

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::d4b0:a95c:94e2:cecc%20
    Dirección IPv4. . . . . : 172.17.14.17
    Máscara de subred . . . . . : 255.255.255.240
    Puerta de enlace predeterminada . . . . . :

C:\Users\FARSUC>ping 192.168.40.253

Haciendo ping a 192.168.40.253 con 32 bytes de datos:
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.40.253: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 192.168.40.253:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
```

Figura 3.213 Prueba de conectividad entre VLAN20 y VLAN40

La tercera prueba realizada es el acceso a Internet desde VLAN30 (RR.HH), ver figura 3.214.

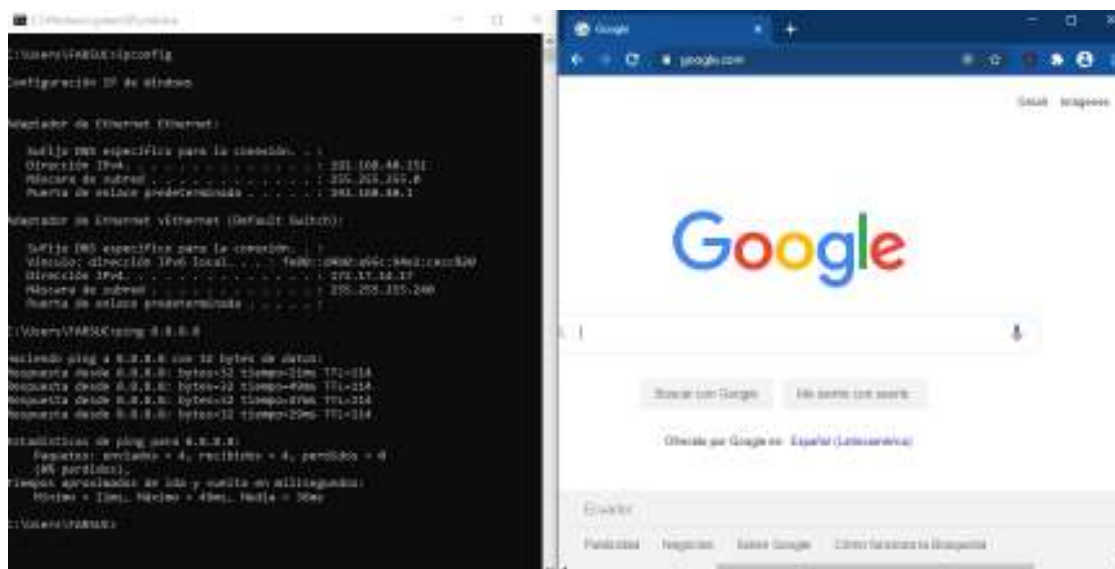


Figura 3.214 Acceso a Internet de VLAN30

ANEXO B: Hojas guías de prácticas para estudiantes

❖ Práctica N°1

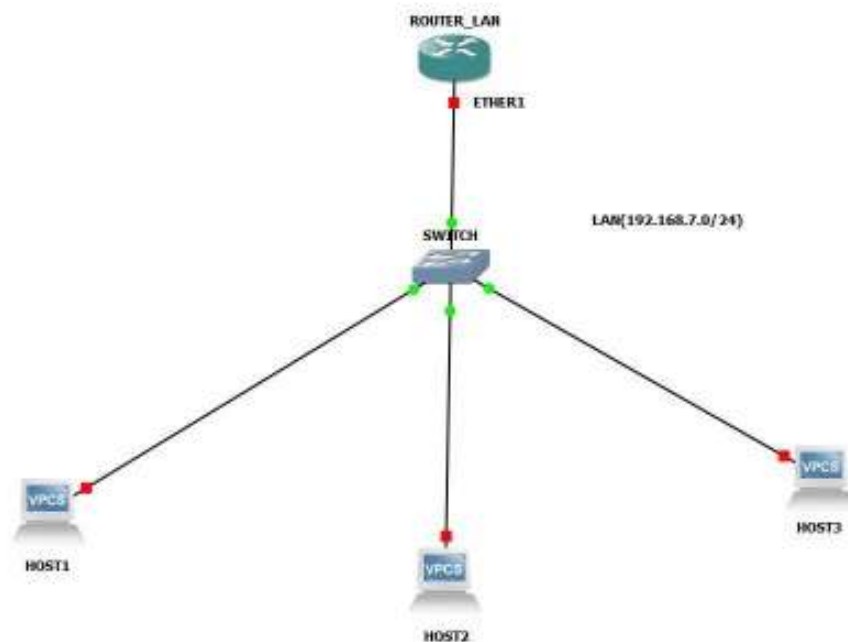
Tema: Acceso de usuarios a *router MikroTik*

Objetivo General: Creación y configuración de usuarios con acceso a *router MikroTik*

Objetivos Específicos:

- Configurar políticas de administración para los grupos de usuarios.
- Crear los usuarios con sus respectivas contraseñas.
- Asignar a los usuarios a los grupos de acuerdo con la lista de usuarios.
- Configurar las interfaces y direcciones *IP* en *routers* y *hosts*.
- Probar las políticas de administración de cada usuario.
- Configurar las interfaces y direcciones *IP* en *routers* y *hosts*.
- Probar las políticas de administración de cada usuario.

Implementación de topología



Asignación de direcciones *IP* para cada equipo, interfaz y *host*

A continuación, se muestra la tabla en donde se indica las direcciones *IP*, máscara, Gateway para cada equipo y *host*.

Equipo	Usuario	Dirección IP	Máscara	Gateway	Interfaz
<i>Router</i>	-----	192.168.7.1	/24	-----	ether2
<i>Host1</i>	Jefe_de_infraestructura	192.168.7.254	/24	192.168.7.1	ether <i>switch</i>
<i>Host2</i>	Soporte_tecnico	192.168.7.253	/24	192.168.7.1	ether <i>switch</i>
<i>Host3</i>	Consultor_externo	192.168.7.252	/24	192.168.7.1	ether <i>switch</i>

Lista de usuarios

A continuación, se muestra la tabla que contiene la lista de usuarios a ser creados para el ingreso al *router*, siendo de gran importancia para mantener una red segura, para ello es necesario la configuración de usuarios con distintas prioridades.

Usuario	Password	Grupo	Políticas	IP permitida
Jefe_de_infraestructura	Ji123456	Full	local/telnet/ssh/ftp/reboot/read/ write/policy/test/ <i>WinBox</i> /password/ web/sniff/sensitive/api/romon/ dude/tikapp	
Soporte_tecnico	St123456	Write	local/telnet/ssh/read/write/test/ <i>WinBox</i> / /web/sniff/tikapp	
Consultor_externo	Ce123456	Read	local/telnet/ssh/read/test/ <i>WinBox</i> / web/tikapp	192.168.7.252

Cuestionario:

- Investigar el usuario por defecto para el acceso a un *router MikroTik*.
- Consultar como realizar la configuración de políticas de grupo.
- Consultar como realizar la creación y configuración de usuarios.
- Determinar la conexión total de la topología implementada.

❖ Practica N°2

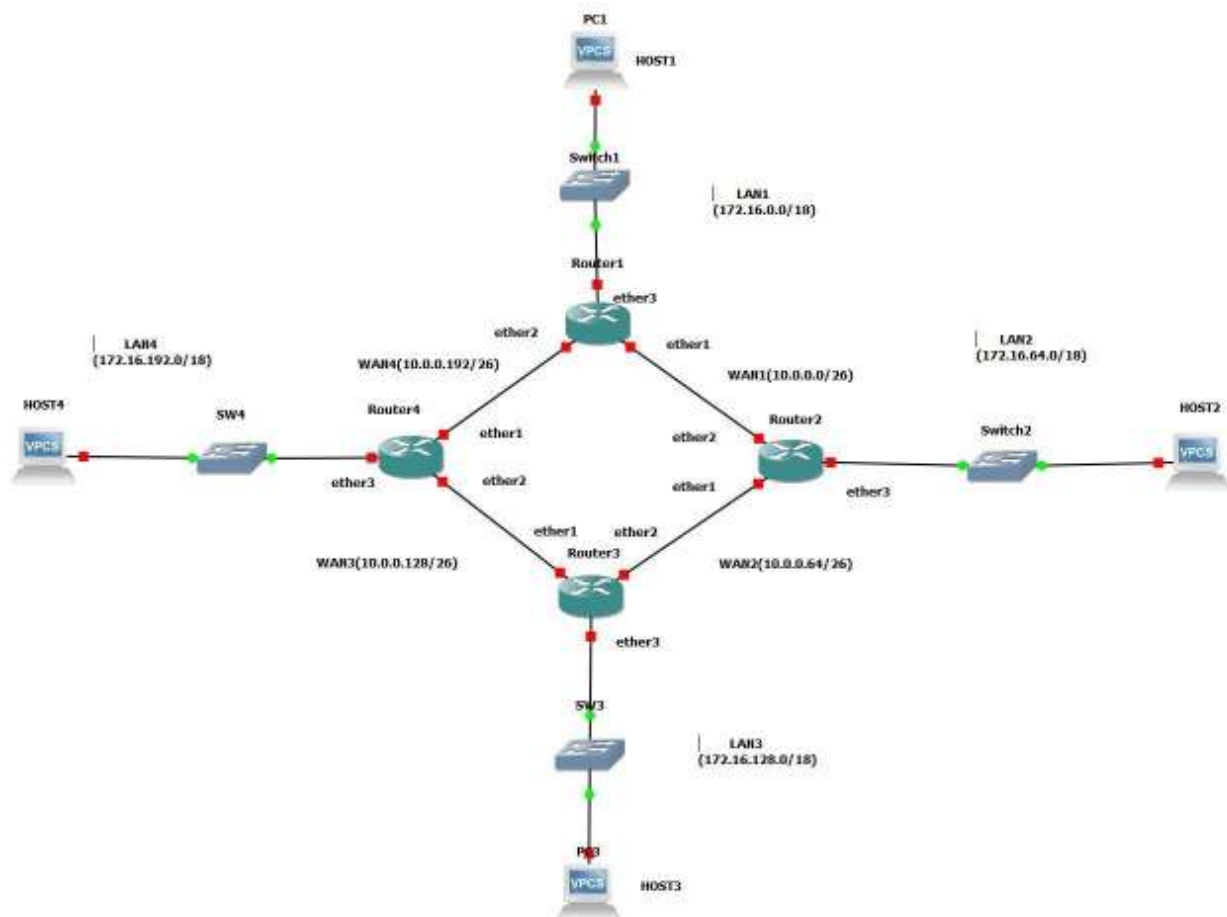
Tema: Enrutamiento estático

Objetivo general: Configuración de enrutamiento estático en *routers MikroTik*.

Objetivos específicos:

- Configurar las interfaces de los *routers MikroTik*
- Configurar las rutas *WAN* y *LAN* de cada equipo
- Comprobar conectividad entre equipos *MikroTik* y *hosts*.

Implementación de topología



Asignación de direcciones *IP* para cada equipo e interfaces

A continuación, se muestra la tabla de distribución de redes *WAN*. Se utiliza la red 10.0.0.0/24 para la creación de 4 subredes *WAN* de máscara fija. Para cada subred *WAN*

creada se empleó la primera *IP* válida en Ether1 mientras para Ether2 se utiliza la última *IP* válida.

Nombre subred	Subred	Máscara	Rango de direcciones válidas	Broadcast
WAN1				
WAN2				
WAN3				
WAN4				

A continuación, se muestra la tabla de distribución de redes *LAN*. Se utiliza la red 172.16.0.0/16 para la creación de 4 subredes *LAN* de máscara fija. Para cada subred *LAN* creada se empleó la primera *IP* válida en Ether3, mientras para el *host* se coloca la última *IP* válida.

Nombre subred	Subred	Máscara	Rango de direcciones válidas	Broadcast
LAN1				
LAN2				
LAN3				
LAN4				

Cuestionario:

- Investigar sobre el funcionamiento del enrutamiento estático.
- Consultar como configurar(levantar) interfaces en *routers*.
- Consultar como configurar enrutamiento estático en *routers*.
- Determinar la conexión total de la topología implementada.

❖ Practica N°3

Tema: *DHCP server, client, relay*

Objetivo: Configuración de *DHCP* en *router MikroTik*.

Objetivos Específicos:

- Configuración de interfaces *WAN* y *LAN*
- Configuración de pool de direcciones para *DHCP* server
- Configuración de *DHCP* server, relay y client
- Configuración de rutas estáticas entre redes *WAN* y *LAN*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

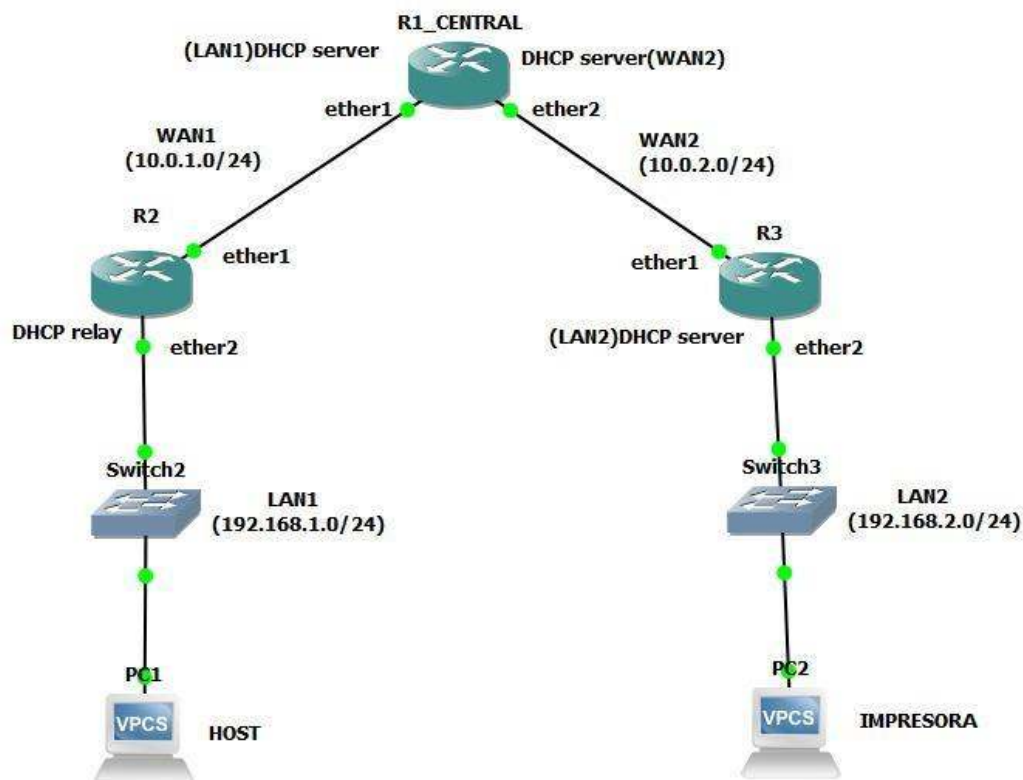


Tabla de direcciones *IP*

A continuación, se muestra la tabla de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
WAN1	10.0.1.0	/24	Ether1 (R1_central)	10.0.1.1	/24
			Ether1 (R2)	10.0.1.2	/24
WAN2	10.0.2.0	/24	Ether2 (R1_central)	10.0.2.1	/24
			Ether1 (R3)	<i>DHCP</i>	<i>DHCP</i>
LAN1	192.168.1.0	/24	Ether2 (R2)	192.168.1.1	/24
			<i>Host</i>	<i>DHCP</i>	<i>DHCP</i>
LAN1	192.168.1.0	/24	Ether2 (R3)	192.168.2.1	/24
			Impresora	192.168.2.77	/24

Pool de direcciones IP

A continuación, se muestra la tabla de rangos de direcciones *IP* de las redes *WAN2*, *LAN1* y *LAN2*.

Nombre de red	Red	Máscara	Pool de direcciones IP	Broadcast
WAN2	10.0.2.0	/24	10.0.2.2 – 10.0.2.254	10.0.2.255
LAN1	192.168.1.0	/24	192.168.1.2 – 192.168.1.254	192.168.1.255
LAN2	192.168.2.0	/24	192.168.2.2 – 192.168.2.254	192.168.2.255

Cuestionario:

- Investigar el funcionamiento y aplicaciones del servidor *DHCP*.
- Consultar como realizar la configuración de *DHCP* Server.
- Consultar como realizar la configuración de *DHCP* Client.
- Consultar como realizar la configuración de *DHCP* Relay.
- Consultar como realizar la configuración de amarre *MAC/IP*.
- Determinar la conexión total de la topología implementada.

❖ Practica N°4

Tema: DNS server, cache, transparente

Objetivo: Configuración de *DNS* en *router MikroTik*.

Objetivos Específicos:

- Configuración de interfaces *WAN* y *LAN*
- Configuración de DNS server, cache y transparente
- Configuración de acceso a internet
- Configuración de *DHCP* server
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

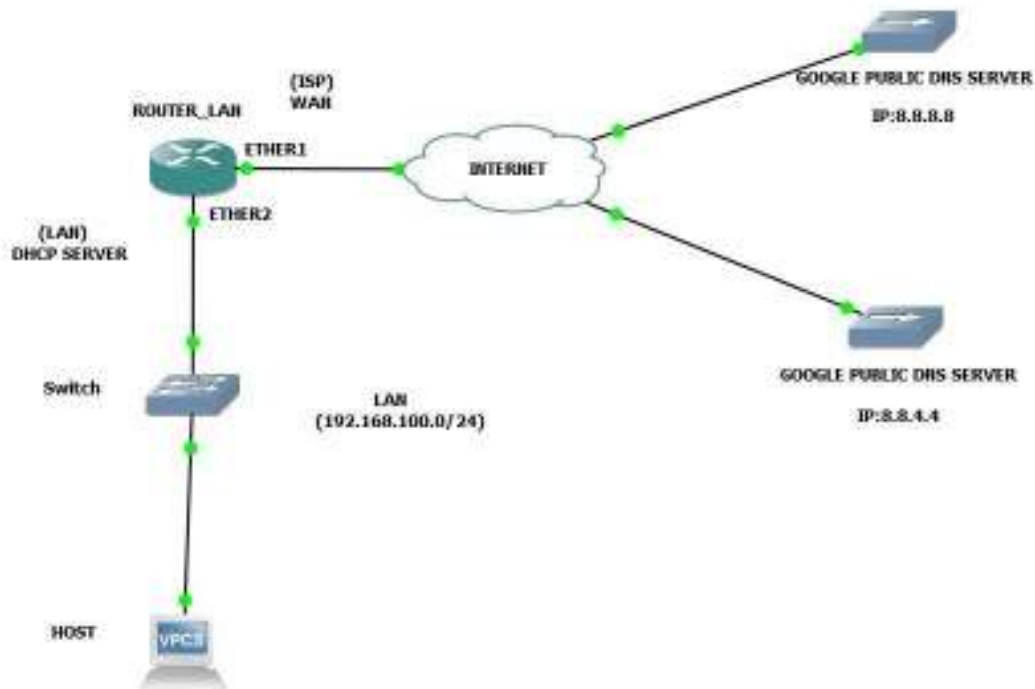


Tabla de direcciones *IP*

A continuación, se muestra la tabla de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
<i>WAN</i>	ISP	ISP	R1(Ether1)	ISP	ISP
<i>LAN</i>	192.168.100.0	/24	R1(Ether2)	192.168.100.1	/24

Cuestionario:

- Investigar el funcionamiento y aplicaciones del servidor DNS.
- Consultar como realizar la configuración de DNS Server.
- Consultar como realizar la configuración de DNS Cache.
- Consultar como realizar la configuración de DNS Transparente.
- Determinar la conexión total de la topología implementada.

❖ Practica N°5

Tema: Protocolo de enrutamiento *BGP*

Objetivo: Configuración de protocolo de enrutamiento *BGP* en *routers MikroTik*

Objetivos Específicos:

- Configuración de interfaces *WAN* y *LAN*
- Configuración de *BGP*
- Configuración *DHCP* en interfaces *LAN*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

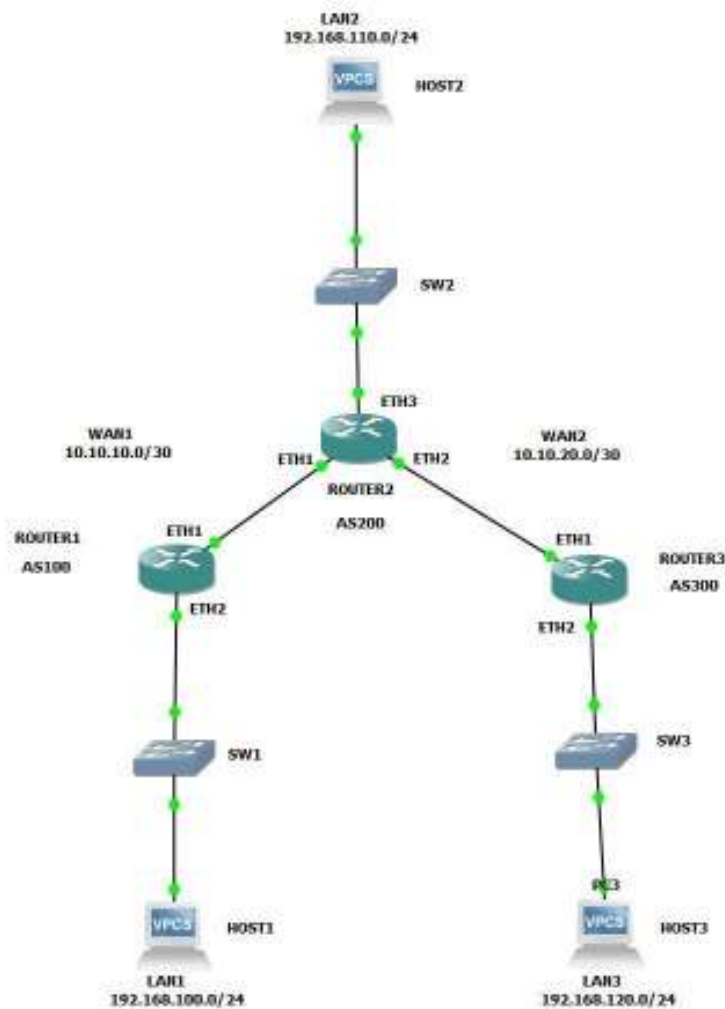


Tabla de direcciones IP

A continuación, se muestra la tabla de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Nombre de red	Red	Máscara	Interfaz	Dirección <i>IP</i>	Máscara
<i>WAN1</i>	10.10.10.0	/30	R1(Ether1)	10.10.10.1	/30
			R2(Ether1)	10.10.10.2	/30
<i>WAN2</i>	10.10.20.0	/30	R2(Ether2)	10.10.20.1	/30
			R3(Ether1)	10.10.20.2	/30
<i>LAN1</i>	192.168.100.0	/24	R1(Ether2)	192.168.100.1	/24
<i>LAN2</i>	192.168.110.0	/24	R2(Ether3)	192.168.110.1	/24
<i>LAN3</i>	192.168.120.0	/24	R3(Ether2)	192.168.120.1	/24

Tabla de sistemas autónomos

A continuación, se muestra la tabla de sistemas autónomos en *routers*.

Nombre	<i>Router</i>
AS100	R1
AS200_R1	R2
AS200_R3	R2
AS300	R3

Cuestionario:

- Investigar el funcionamiento del protocolo *BGP*.
- Consultar que son los sistemas autónomos.
- Consultar que son las relaciones peers en *BGP*.
- Determinar la conexión total de la topología implementada.

❖ Practica N°6

Tema: Firewall básico

Objetivo: Configuración de Firewall básico en *router Mikrotik*

Objetivos Específicos:

- Configuración de interfaces *WAN* y *LAN*
- Configuración de brigde en Ether1 y Ether2
- Configuración de acceso a Internet
- Configuración de Firewall
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

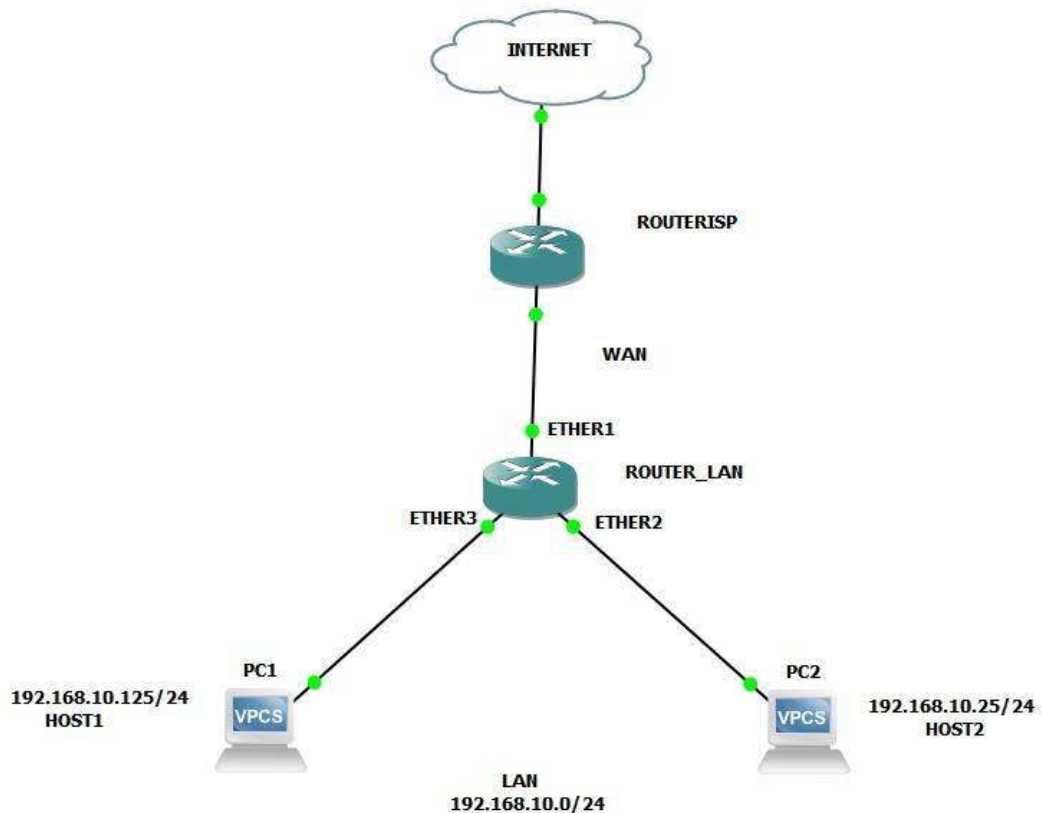


Tabla de direcciones *IP*

A continuación, se muestra la tabla de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
WAN	ISP	ISP	R1(Ether1)	ISP	ISP
LAN	192.168.10.0	/24	R1(Ether2)	192.168.10.1	/24

Tabla de reglas en *hosts*

A continuación, se muestra la tabla de reglas firewall en *hosts*.

Nombre	Dirección IP	Máscara	Reglas
<i>Host1</i>	192.168.10.125	/24	Acceso al <i>router</i> / Acceso SSH-Ping-Telnet / Acceso a internet sin restricciones
<i>Host2</i>	192.168.10.25	/24	No acceso al <i>router</i> / Bloqueo SSH-Ping-Telnet / Acceso a internet con restricciones a redes sociales

Cuestionario:

- Investigar el funcionamiento y aplicaciones de *firewall*.
- Consultar que es un *Bridge* y como funciona.
- Consultar como funciona *INPUT*, *OUTPUT* y *FORWARD*.
- Consultar como realizar la configuración básica de *firewall*.
- Determinar la conexión total de la topología implementada.

❖ Practica N°7

Tema: Colas simples

Objetivo: Configuración de colas simples en *router MikroTik*

Objetivos Específicos:

- Configuración de interfaces *WAN*, *LAN1* y *LAN2*
- Configuración de brigde en Ether2 y Ether3
- Configuración de acceso a internet
- Configuración de colas padre e hijos en *LAN1*
- Configuración de ráfagas de velocidad en *LAN2*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

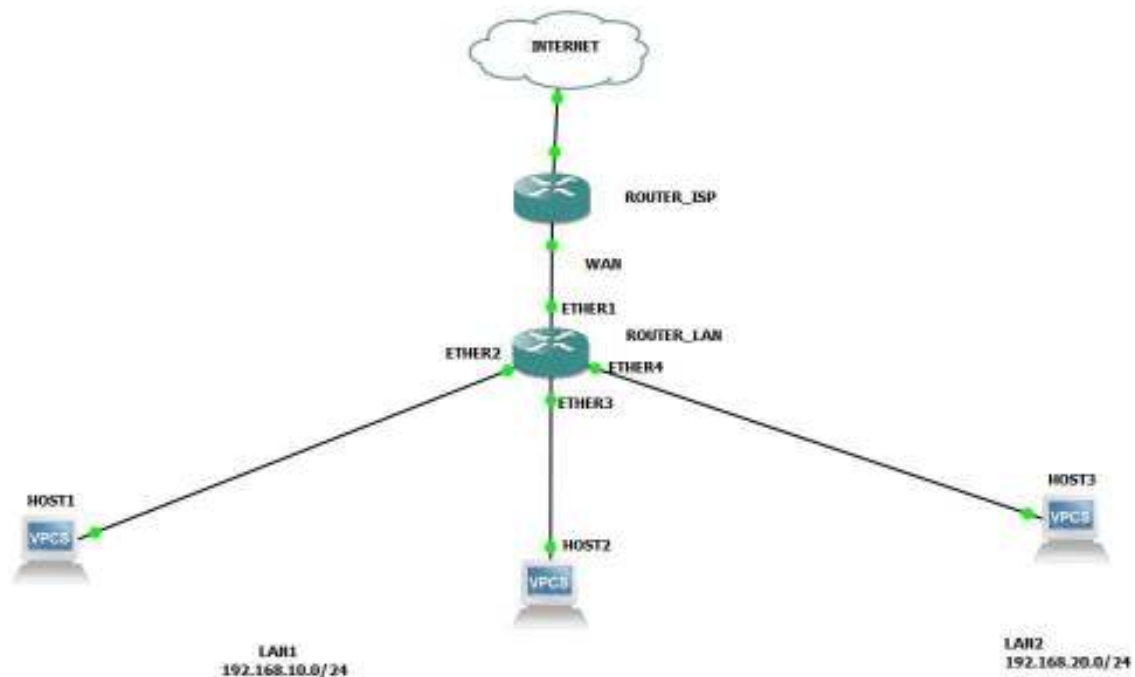


Tabla de direcciones IP

A continuación, se muestra la tabla de distribución de direcciones *IP* para redes *WAN*, *LAN* y *hosts*.

Nombre de red	Red	Máscara	Interfaz	Dirección IP	Máscara
WAN	ISP	ISP	R1(Ether1)	ISP	ISP
LAN1	192.168.10.0	/24	R1(Ether2-3)	192.168.10.1	/24
LAN2	192.168.20.0	/24	R1(Ether4)	192.168.20.1	/24

Tabla de reglas en *hosts*

A continuación, se muestra la tabla de anchos de banda para cada *host*.

Nombre	Dirección IP	Máscara	Reglas
<i>Host1</i>	192.168.10.254	/24	Max-Limit: 1M (up) / 1M (down) Limit at: 512K (up) / 512K (down)
<i>Host2</i>	192.168.10.253	/24	Max-Limit: 1M (up) / 1M (down) Limit at: 512K (up) / 512K (down)
<i>Host2</i>	192.168.20.254	/24	Max-Limit: 1M (up) / 1M (down) Burst limit: 2M (up) / 2M (down) Burst threshold: 512K (up) / 512K (down) Burst time: 16 s (up) / 16 s (down)

Cuestionario:

- Investigar el funcionamiento y aplicaciones de colas simples.
- Consultar qué es y cómo funciona una cola padre y colas hijos.
- Consultar qué es y cómo funciona ráfagas de velocidad.
- Determinar la conexión total de la topología implementada.

❖ Practica N°8

Tema: VLANs

Objetivo: Configuración de VLANs en *routers* y *switchs MikroTik*

Objetivos Específicos:

- Configuración de brigde en Ether2 y Ether3
- Configuración de VLANs en *router*
- Configuración de *DHCP* en VLANs y acceso a internet
- Configuración de VLANs en *switch*
- Comprobar conectividad entre equipos y *hosts*

Implementación de topología

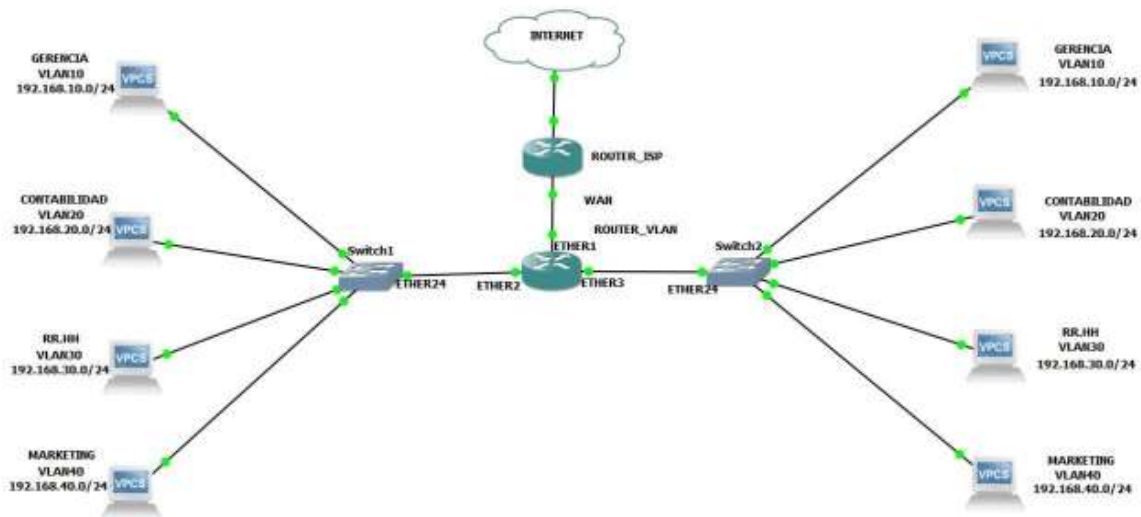


Tabla de direcciones IP en VLANs

A continuación, se muestra la tabla de distribución de direcciones IP para VLANs.

Nombre de VLAN	VLAN ID	Red	Máscara	IP en router	Interfaces switch
Gerencia	10	192.168.10.0	/24	192.168.10.1	Ether1-Ether5
Contabilidad	20	192.168.20.0	/24	192.168.20.1	Ether6-Ether10
RR.HH	30	192.168.30.0	/24	192.168.30.1	Ether11-Ether15
Marketing	40	192.168.40.0	/24	192.168.40.1	Ether16-Ether20

Cuestionario:

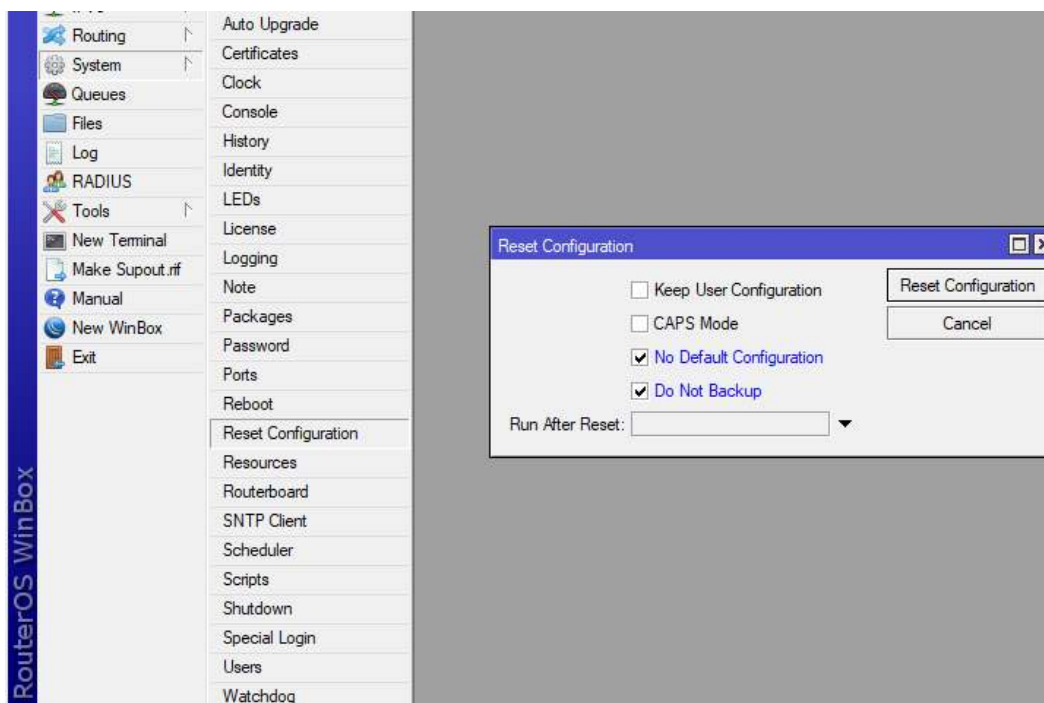
- Investigar el funcionamiento y aplicaciones de VLANs.
- Consultar sobre los puertos de acceso y puertos troncales.
- Consultar sobre los tipos de VLANs
- Determinar la conexión total de la topología implementada.

ANEXO C: Manual de Usuario

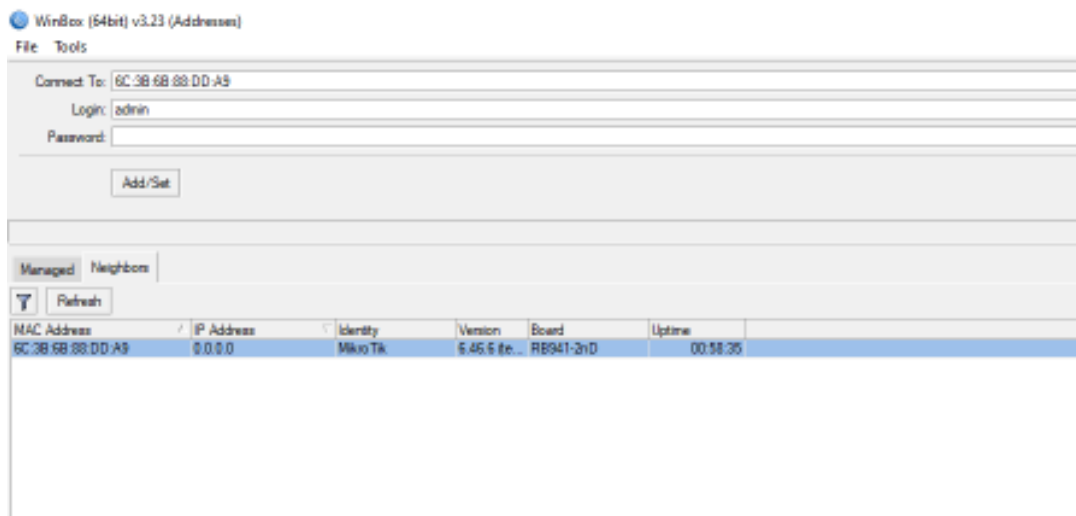
❖ Eliminación de configuraciones de fábrica en *router*

Configuración vía interfaz gráfica

Los equipos *MikroTik* cuentan con una configuración de fábrica, por lo que es necesario borrar para que no exista reglas ni configuraciones preestablecidas que puedan dar conflictos de operación o no se pueda comportar correctamente los equipos *MikroTik* al momento de realizar nuestras configuraciones. Para ello se selecciona la opción *System / Reset Configuration*. A continuación, se despliega una ventana donde se selecciona los casilleros *No Default Configuration* y *Do Not Backup* y se elige la opción *Reset Configuration*,



Una vez borrado las preconfiguraciones de fabrica en el *router*, se procede al ingreso del equipo, el *router* cuenta con una dirección *IP* 0.0.0.0, con un usuario predeterminado *admin* sin contraseña.



Configuración vía comandos

Eliminación de configuraciones de fabrica en *router*

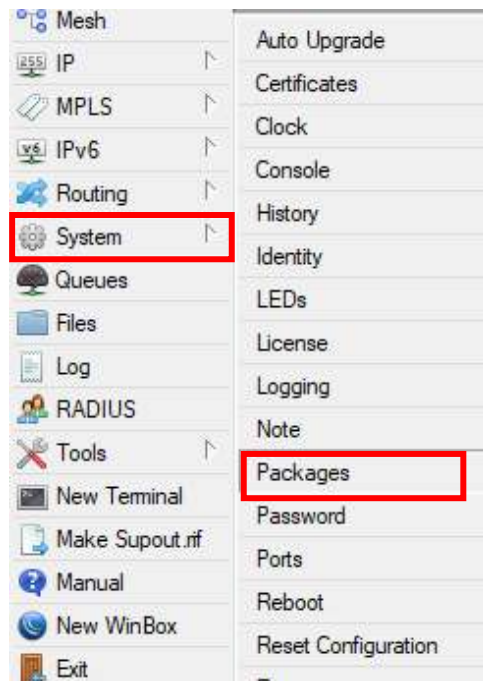
Para borrar las configuraciones de fabrica se ingresa los siguientes comandos:

- [admin@MikroTik] > system reset-configuration no-defaults=yes
skIP-backup=yes

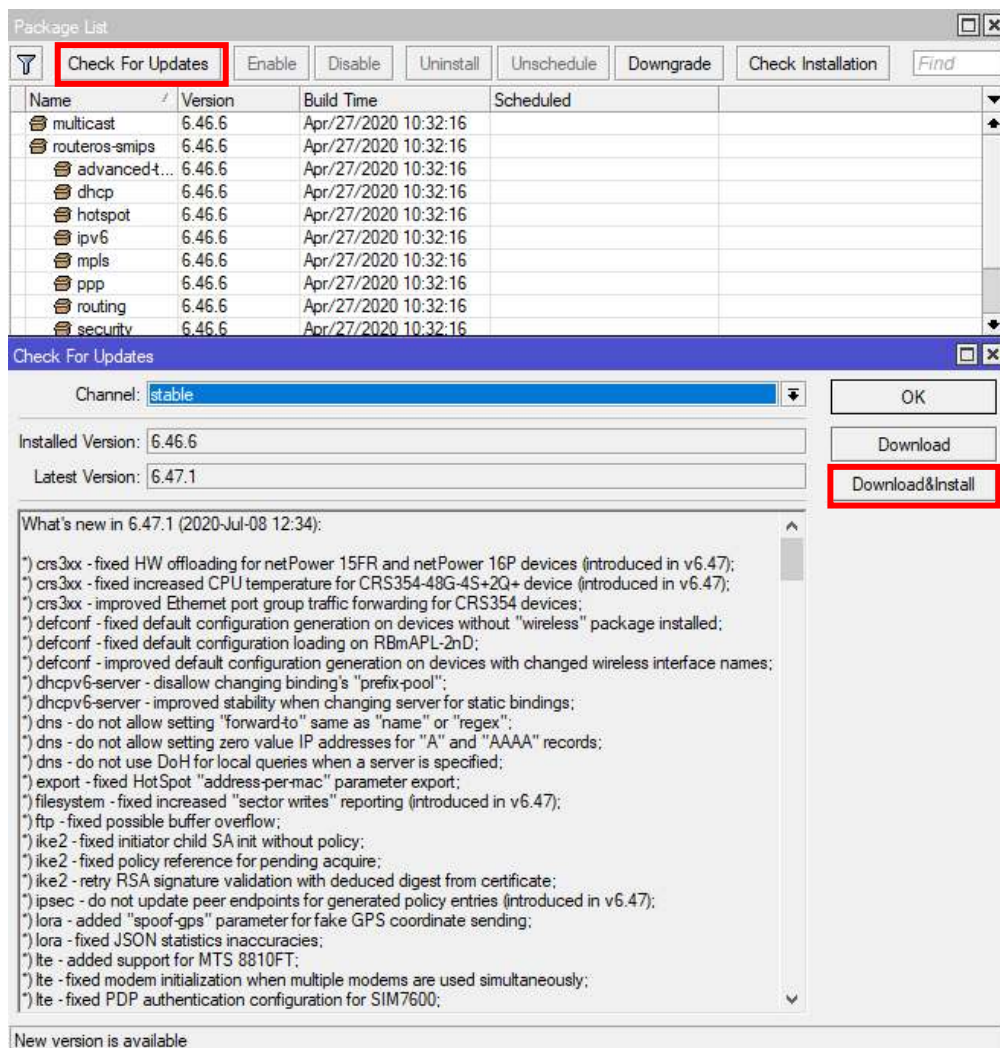
❖ Actualización de firmware en equipo *MikroTik*

Configuración vía interfaz gráfica

Es necesario tener siempre actualizado el Firmware debido a que los fabricantes suelen trabajar en modificaciones del *software* que permite un mejor funcionamiento de los componentes hardware. Estas modificaciones pueden añadir nuevas funcionalidades a las originales del componente o pueden corregir fallos que hubieran aparecido en el equipo. Para ello se elige en el menú la opción *System/Packages*.



A continuación, aparece una ventana donde se elige la opción *Check For Updates* para comprobar si existe actualizaciones recientes. Ahora se observa una nueva ventana donde indica la versión instalada y si existe una versión más reciente. Si hay una nueva versión se selecciona la opción *Download&Install* para descargar e instalar la última versión en el equipo.



Configuración vía comandos

Para actualizar el firmware del equipo se ingresa el comando *system package*

- [admin@MikroTik] > system package update check-for-updates
channel: stable
installed-version: 6.46.6
latest-version: 6.47.1
status: New version is available
- [admin@MikroTik] > system package update install