

# Configuración de un router mikrotik para una red local

*Trabajo de fin de grado*



**Antonio Manuel Rueda Guijarro**



<b>INTRODUCCIÓN</b>	<b>3</b>
<b>Configuración del router mikrotik desde winbox</b>	<b>4</b>
<b>Acceso a router</b>	<b>6</b>
<b>Nombre del router</b>	<b>7</b>
<b>Configuración del router para dhcp</b>	<b>7</b>
<b>Copia de seguridad</b>	<b>14</b>
<b>Firewall - Filtrar tráfico entrante</b>	<b>15</b>
Permitir SSH	15
Permitir WinBox	16
<b>Firewall - Filtrar tráfico saliente</b>	<b>17</b>
Permitir servicios esenciales	17
Bloquear tráfico no autorizado	18
<b>Crear Reglas de Firewall para Mitigar DDoS</b>	<b>19</b>
<b>Configuración de Reglas Adicionales para Mitigar DDoS</b>	<b>22</b>
Limitar el número de conexiones por puerto o protocolo	22
¿Por qué vamos a limitar conexiones por puerto?	22
Activar el Registro (Logging) de Reglas de Firewall	23
<b>Monitoreo de tráfico</b>	<b>24</b>
Habilitar SNMP	24
Habilitamos touch	25
<b>Crear 3 subredes con Bridges y servidores DHCP</b>	<b>26</b>
Configurar reglas de firewall para aislar subredes	28
Crear los servidores DHCP para cada subred:	28
<b>Creación de una regla nat para acceder a un equipo de la subred C</b>	<b>30</b>
<b>¿Qué estamos haciendo?</b>	<b>30</b>
Desglose de los parámetros:	30
<b>Crear una regla de Firewall para permitir acceso</b>	<b>31</b>
¿Qué estamos haciendo?	31
Desglose de los parámetros:	32
<b>Creación de un Script que genere y envíe por email: el backup binario y el Export completo</b>	<b>33</b>
Crear el Script	33
<b>Configurar el Servidor de Correo</b>	<b>34</b>
<b>Crear el Evento Diario</b>	<b>35</b>
<b>Configurar VLANs en MikroTik</b>	<b>37</b>
Asignar una IP a la VLAN	38
Configuración de un Bridge (Puente) para VLANs	38
Añadir Interfaces al Bridge	39

Configurar el Bridge para VLANs	40
Verificación de Configuración	41
¿Qué se puede verificar con estos comandos?	41
<b>Conclusión del Proyecto de Configuración y Optimización de un Router MikroTik</b>	<b>42</b>
<b>Bibliografía</b>	<b>43</b>

## Introducción del proyecto

Este proyecto tiene como objetivo la configuración y optimización de un router MikroTik para mejorar la gestión y el rendimiento de una red local. A través de la implementación de varias herramientas y técnicas, me encargaré de administrar de manera eficiente los dispositivos conectados a la red, asignar direcciones IP automáticamente mediante el servicio de DHCP, agregar capas de seguridad utilizando cortafuegos para proteger la red contra accesos no autorizados y asegurar un acceso a internet rápido y confiable para todos los usuarios.

El enfoque de este proyecto está orientado a redes locales en diversos entornos, tales como empresas, organizaciones y hogares, proporcionando soluciones de conectividad robustas, seguras y escalables. Además de las tareas básicas de administración y asignación de IPs, también se llevará a cabo una configuración avanzada de la red, ajustando parámetros específicos de calidad de servicio (QoS) para optimizar el uso del ancho de banda, implementando reglas de firewall para prevenir amenazas cibernéticas y garantizando una conectividad fluida y estable.

El router MikroTik, conocido por su versatilidad y funcionalidad, se utilizará como la pieza central de este proyecto para ofrecer un control preciso sobre el tráfico de datos y la seguridad de la red. Con esta configuración, se espera mejorar la eficiencia operativa, reducir riesgos de seguridad y asegurar una experiencia de usuario satisfactoria dentro de la red local.

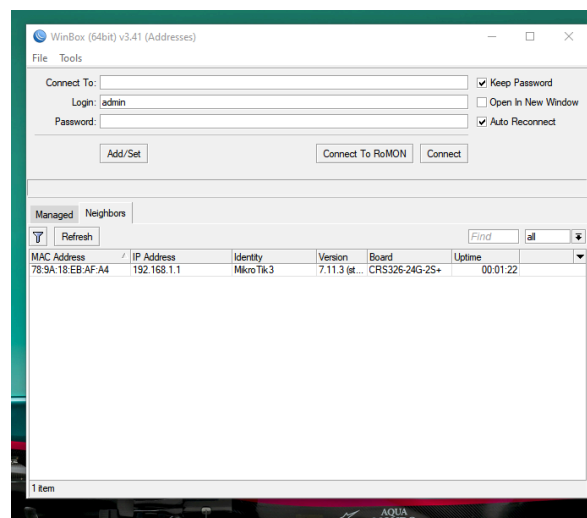
## Configuración del router mikrotik desde winbox

Primero que nada vamos a instalar la aplicación para la gestión del router mikrotik, para ello nos vamos a ir a google y vamos a descargarla

Desde el siguiente enlace vamos a poder descargarnos la aplicación

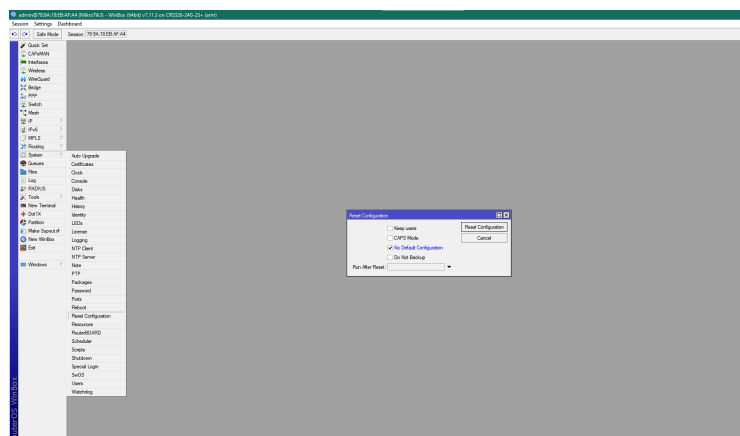
<https://mikrotik.com/download>

La ejecutamos y nos va a salir lo siguiente



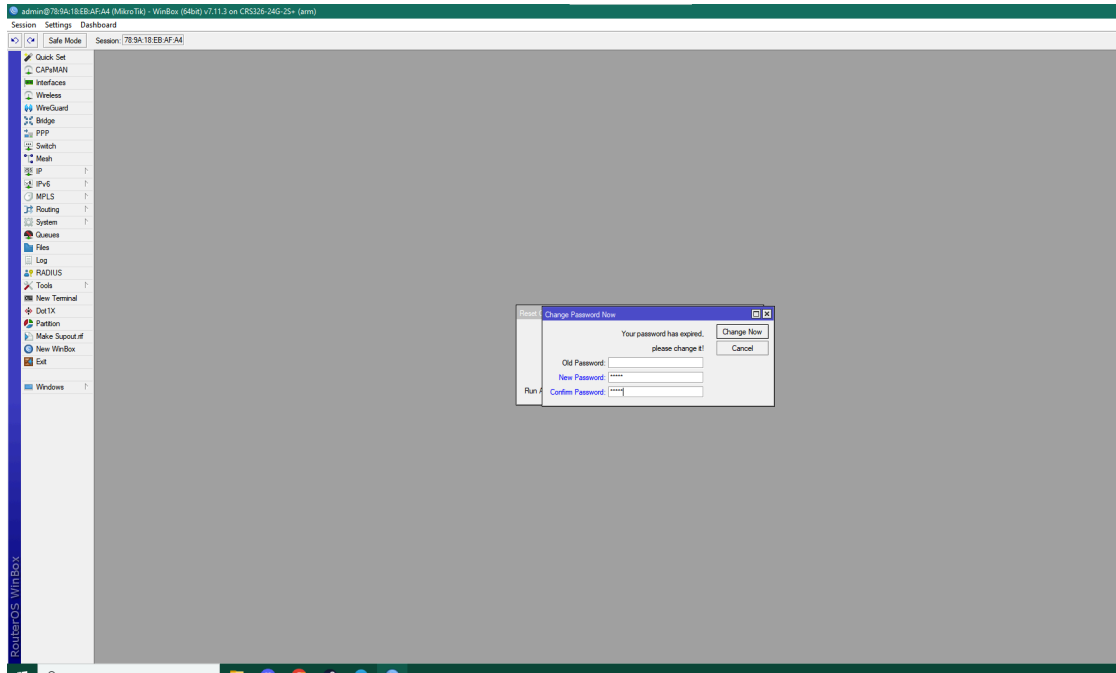
Para acceder al router la primera vez el usuario es admin sin contraseña

Una vez dentro vamos a restaurarlo de fabrica



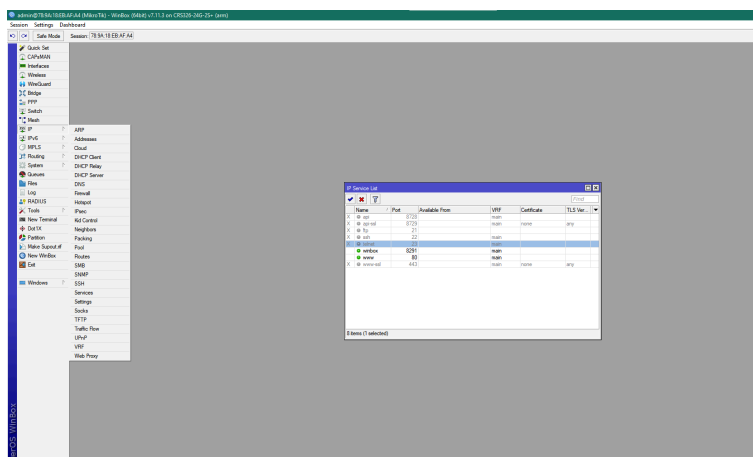
Para restaurar un router MikroTik, accede a System > Reset Configuration y

selecciona la opción "no default configuration". Esto eliminará toda la configuración actual y dejará el router completamente vacío, sin ninguna configuración personalizada. Luego, el router se reiniciará y, al acceder nuevamente con el usuario admin (sin contraseña), te pedirá que cambies la contraseña por una nueva para asegurar el dispositivo.



## Acceso a router

Ahora vamos a deshabilitar alguna de las maneras de acceso al router para que tenga un poco mas de seguridad



Para aumentar la seguridad y controlar cómo se accede a la configuración del router Mikrotik, debemos ir a **"IP > Services"** en la interfaz de administración. Allí veremos una lista de servicios que permiten el acceso remoto al router, como Telnet, SSH, FTP, entre otros. Para asegurarnos de que solo se pueda acceder mediante **Winbox** y **WWW**, necesitamos desactivar todos los demás servicios.

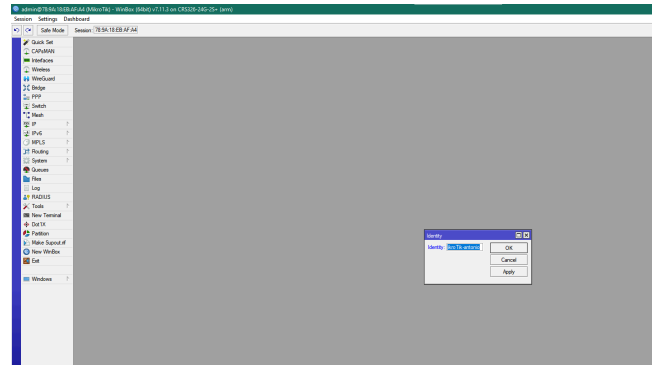
Primero, accedemos a **IP > Services** desde Winbox o WebFig. Luego, localizamos los servicios habilitados, como Telnet, FTP, SSH, API, etc. Desactivamos cada uno de estos servicios haciendo clic en **Disable**. Finalmente, nos aseguramos de que solo **Winbox** y **WWW** estén habilitados, ya que son los métodos que queremos usar para la administración del router.

De este modo, restringimos el acceso al router exclusivamente a través de **Winbox** y **WWW**, mejorando la seguridad al reducir las opciones de acceso remoto.

## Nombre del router

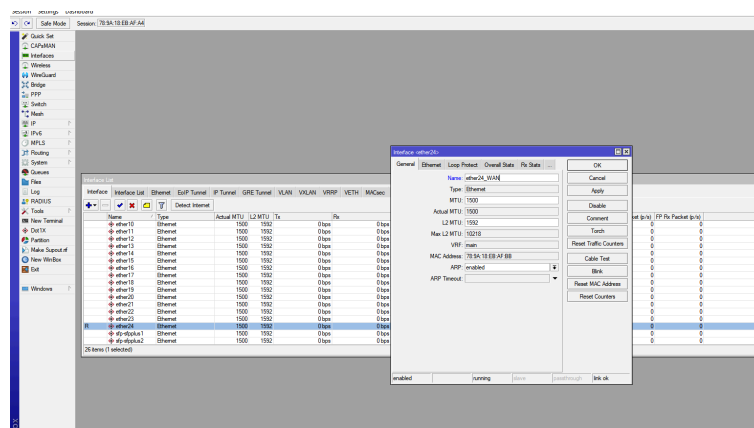
Ahora vamos a cambiarle el nombre al router

Para ello vamos a irnos a “system → identity” y vamos a ponerle un nombre para poder identificarlo más fácilmente



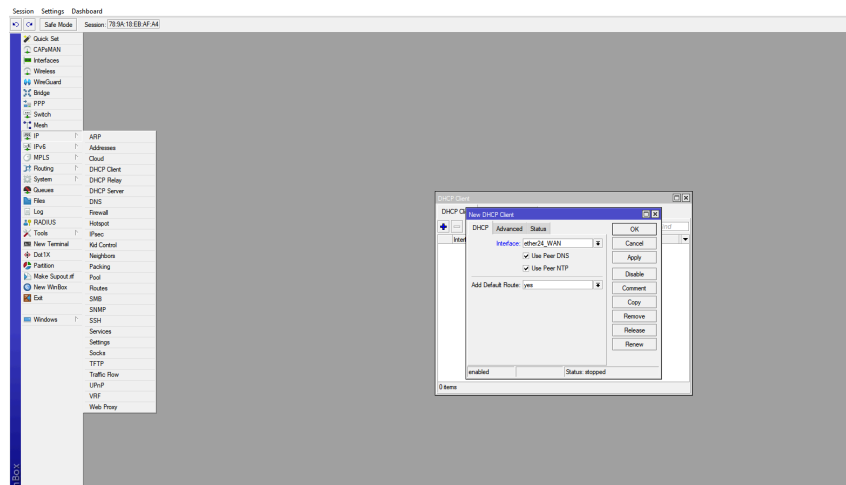
## Configuración del router para dhcp

Para configurar el puerto que usaremos para la salida a internet, accedemos a **"Interfaces > Ethernet"** en MikroTik y buscamos el **puerto 24**. Una vez localizado, hacemos clic sobre él para editar su configuración y cambiamos el nombre a algo más descriptivo, como **"WAN"**. Esto nos ayudará a identificar fácilmente esta interfaz como la conexión a la red externa, mejorando la organización de la configuración del router.

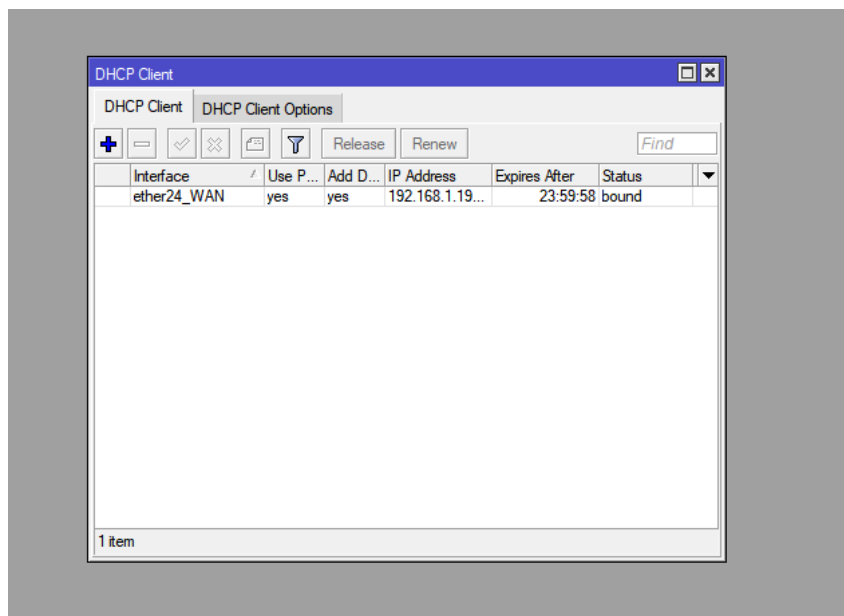




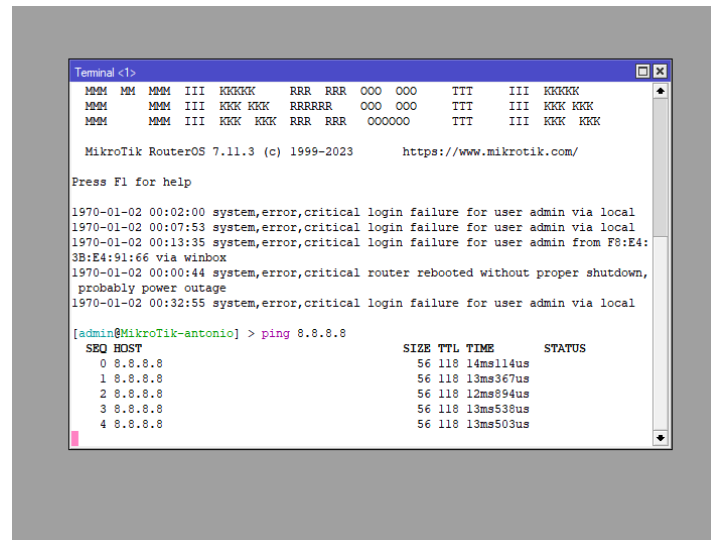
Para habilitar un cliente DHCP en la interfaz WAN, primero debemos acceder a **"IP > DHCP Client"** en la interfaz de administración de MikroTik. Una vez dentro, hacemos clic en el símbolo "+" para agregar un nuevo cliente DHCP. Luego, seleccionamos la interfaz WAN (la que hemos renombrado previamente) de la lista de interfaces disponibles. Después de elegir la interfaz, hacemos clic en **"Aplicar"** para que el cliente DHCP se active en la interfaz WAN, permitiendo que el router obtenga automáticamente una dirección IP desde el servidor DHCP del proveedor de internet.



Una vez le hemos dado a aplicar podemos ver como se ha creado



Para confirmar que el MikroTik tiene acceso a internet, abre el **Terminal** desde la interfaz de administración. Luego, ejecuta el siguiente comando para hacer un ping a la dirección IP pública de Google (8.8.8.8):



```
Terminal <1>
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK

MikroTik RouterOS 7.11.3 (c) 1999-2023 https://www.mikrotik.com/

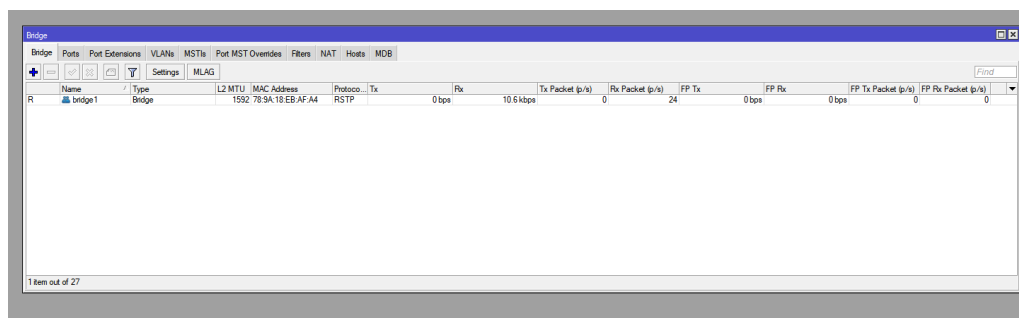
Press F1 for help

1970-01-02 00:02:00 system,error,critical login failure for user admin via local
1970-01-02 00:07:53 system,error,critical login failure for user admin via local
1970-01-02 00:13:35 system,error,critical login failure for user admin from F8:E4:
3B:E4:91:66 via winbox
1970-01-02 00:00:44 system,error,critical router rebooted without proper shutdown,
probably power outage
1970-01-02 00:32:55 system,error,critical login failure for user admin via local

[admin@MikroTik-antonio] > ping 8.8.8.8
  SEQ HOST                      SIZE TTL TIME          STATUS
  ---
0 8.8.8.8                56 118 14ms114us
1 8.8.8.8                56 118 13ms367us
2 8.8.8.8                56 118 12ms894us
3 8.8.8.8                56 118 13ms539us
4 8.8.8.8                56 118 13ms503us
```

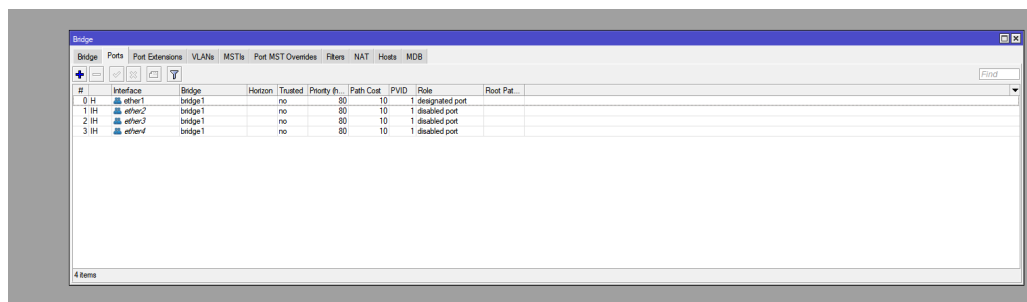
Si el router recibe respuestas (es decir, los paquetes son respondidos), eso indica que la conexión a internet está funcionando correctamente y que el MikroTik ha logrado obtener una dirección IP a través del cliente DHCP. Si no recibes respuestas, es posible que haya un problema con la configuración de la interfaz WAN o con la conexión a tu proveedor de internet.

Para crear un puente en MikroTik, ve a Bridge y haz clic en "Agregar". Asigna un nombre al puente, como "bridge1", y luego agrega las interfaces que deseas combinar bajo este puente. Esto permitirá la comunicación entre las interfaces seleccionadas.



Una vez creado el puente, dirígete a la pestaña "**Ports**" dentro de la sección

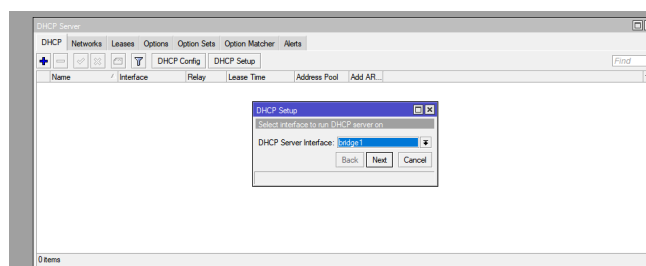
**"Bridge"**. Allí, hacemos clic en **"Agregar"** y selecciona los puertos del router que deseas añadir al puente. Esto permitirá que las interfaces seleccionadas se comuniquen entre sí a través del puente.



Para crear un servidor DHCP en el puente y que asigna automáticamente direcciones IP a los dispositivos conectados a los puertos de ese puente, sigue estos pasos:

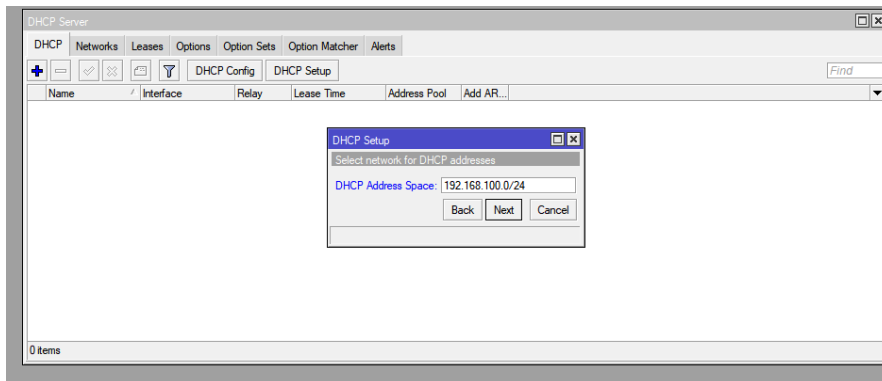
1. Dirígete a "IP > DHCP Server" en la interfaz de administración de Mikrotik.
2. Una vez allí, haz clic en la opción "DHCP Setup".
3. Se abrirá una ventana donde podrás seleccionar la interfaz sobre la cual deseas configurar el servidor DHCP. Selecciona el puente que has creado (por ejemplo, bridge1).
4. Luego, el asistente de configuración de DHCP nos guiará a través de los pasos para configurar el rango de direcciones IP que el servidor DHCP asignará, la puerta de enlace predeterminada y otros parámetros necesarios.

Esto permitirá que los dispositivos conectados a los puertos del puente reciban automáticamente una dirección IP, facilitando la configuración de la red local.

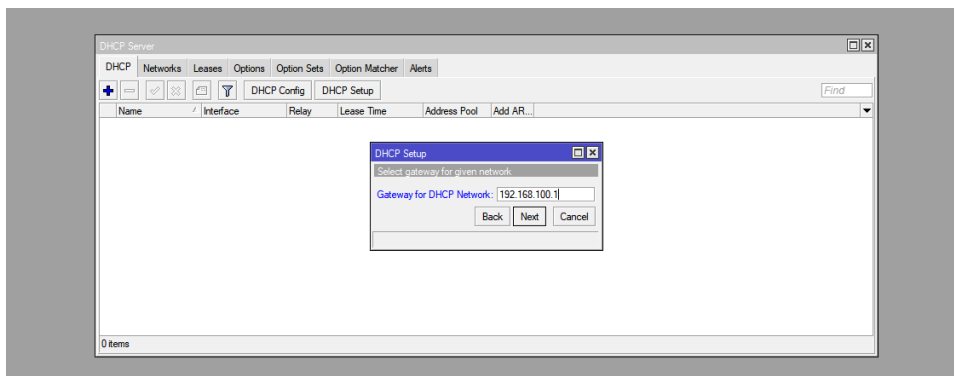


Le damos a siguiente

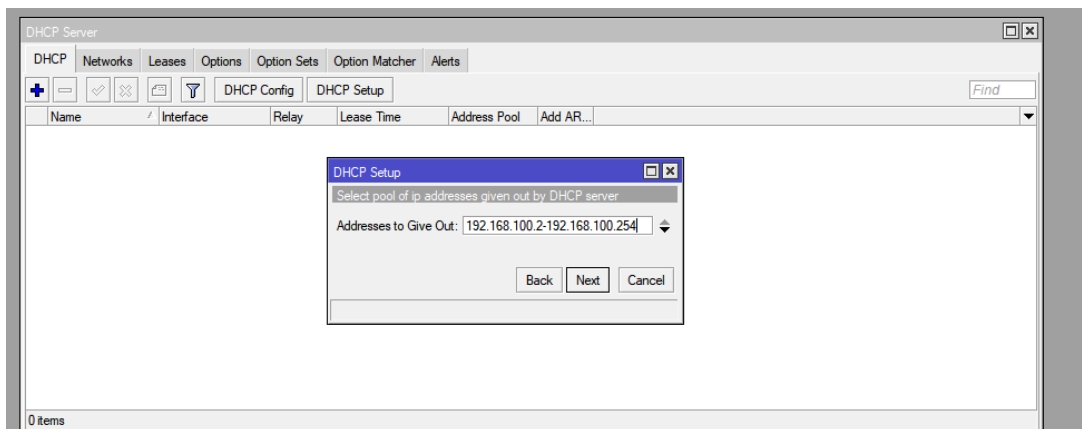
Se nos rellenará automáticamente la ip ya que la definimos anteriormente



Ahora una vez le damos a siguiente, se nos rellenará automáticamente la puerta de enlace y le daremos a siguiente

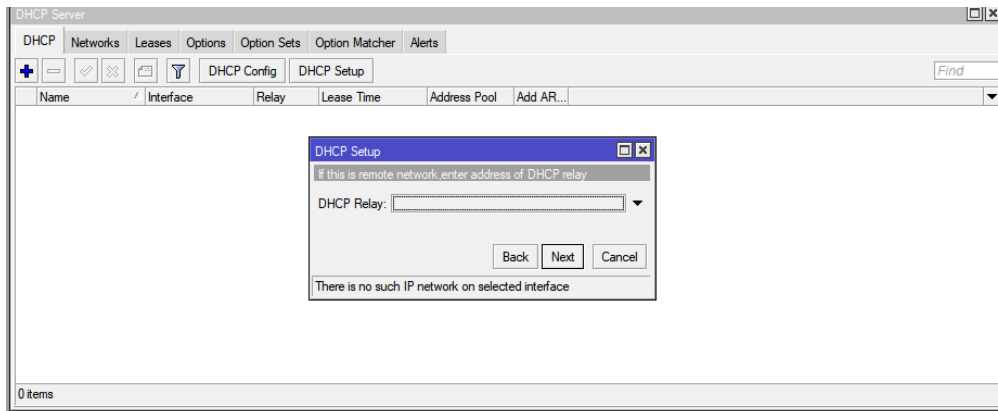


Aquí asignaremos el rango de ip que queremos que tenga el bridge

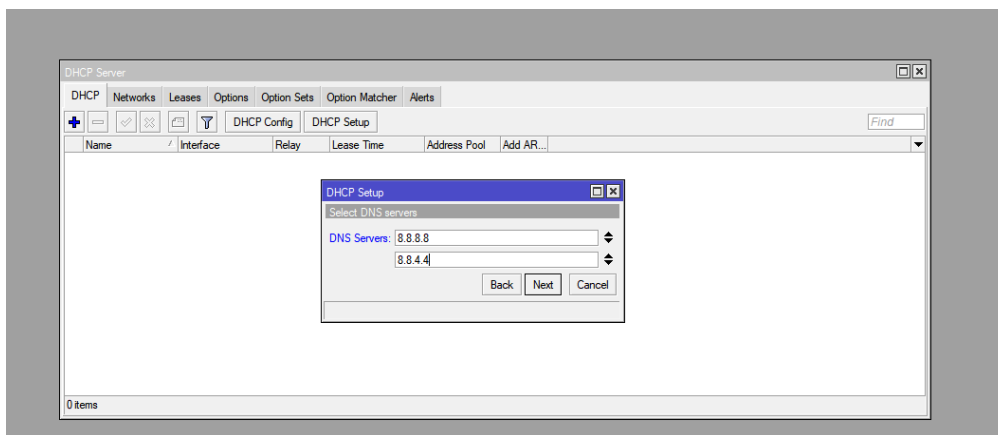


Aquí nos aseguraremos que se quede vacío el parámetro relay ya que es

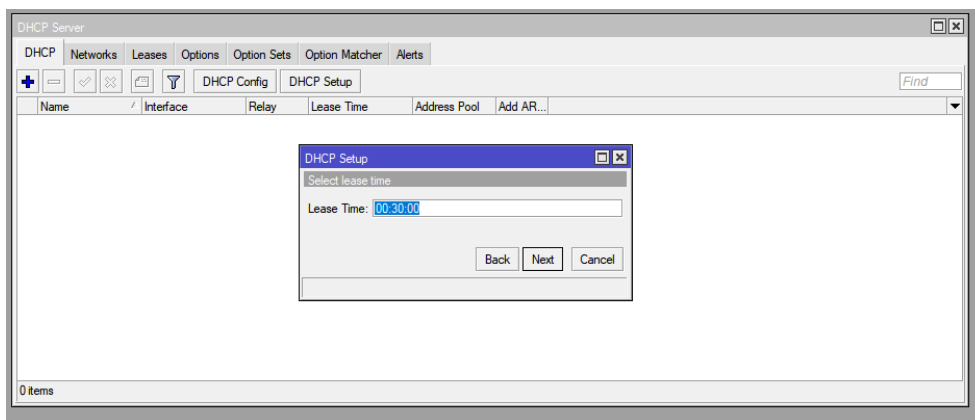
importante



A continuación definiremos los DNS que tendrá el SERVIDOR DHCP



Aquí asignaremos el tiempo de refrescos que tendrá el servidor DHCP



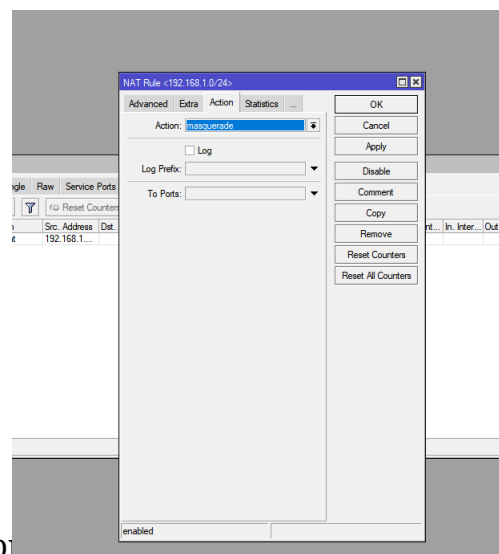
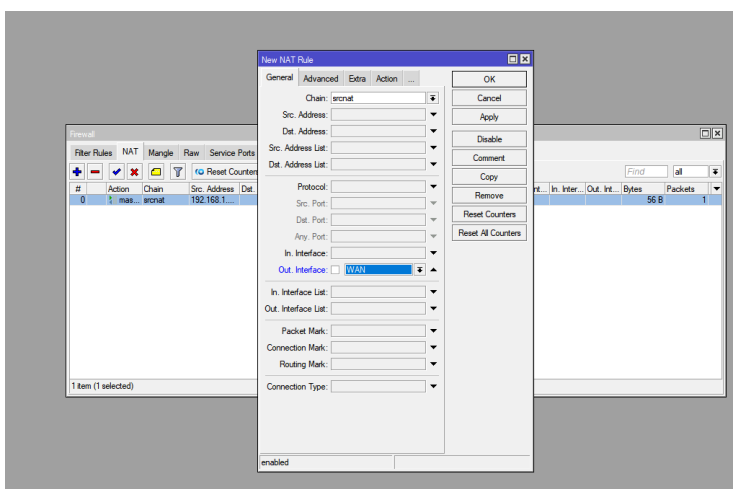
Para que los dispositivos conectados al router puedan acceder a internet, necesitamos crear una regla NAT (Traducción de Direcciones de Red). Esta regla hace que el tráfico de la red local (LAN) se “enmascara” con la dirección IP pública de la interfaz WAN del router. Aquí te explico cómo hacerlo paso a paso:

Primero, vamos a IP > Firewall en la interfaz de administración de MikroTik. Ahí, seleccionamos la pestaña NAT.

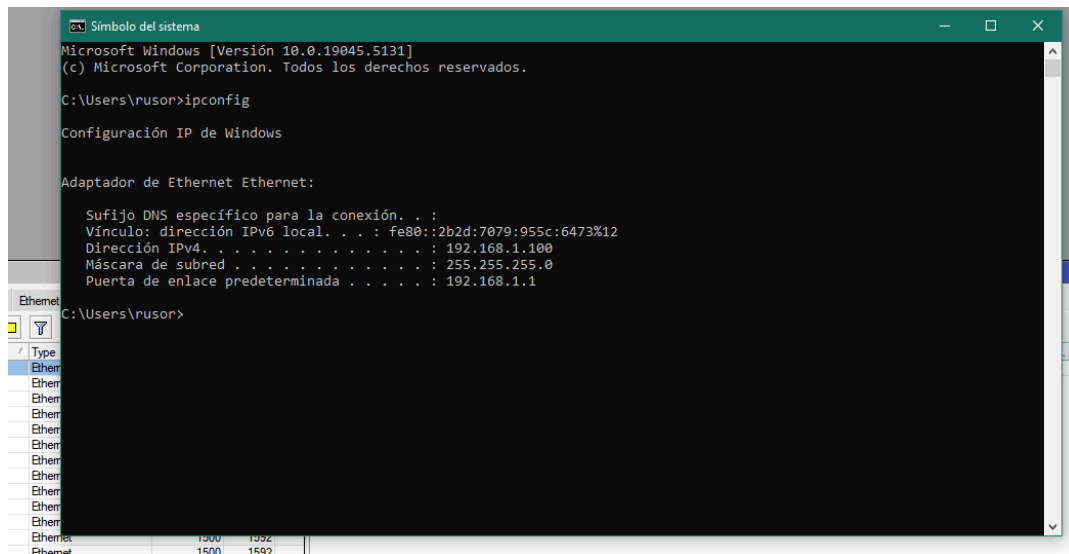
Luego, damos clic en el botón "+" para agregar una nueva regla NAT. Ahora, tenemos que configurar los parámetros de esta nueva regla:

1. En Chain, seleccionamos srcnat. Esto hace que la regla se aplique al tráfico saliente de la LAN hacia internet.
2. En Out Interface, seleccionamos WAN. Esto indica que la regla solo se aplicará al tráfico que sale por la interfaz WAN (la que está conectada al proveedor de internet).
3. En Action, elegimos masquerade. Esto permite que las direcciones IP privadas de nuestra LAN se cambien por la IP pública del router. Lo bueno de esta opción es que funciona con redes que usan una IP dinámica, ya que se ajusta automáticamente si la dirección pública cambia.

Con esto, ya tendrás configurado el acceso a internet para los dispositivos conectados a la red local, utilizando la IP pública del router.



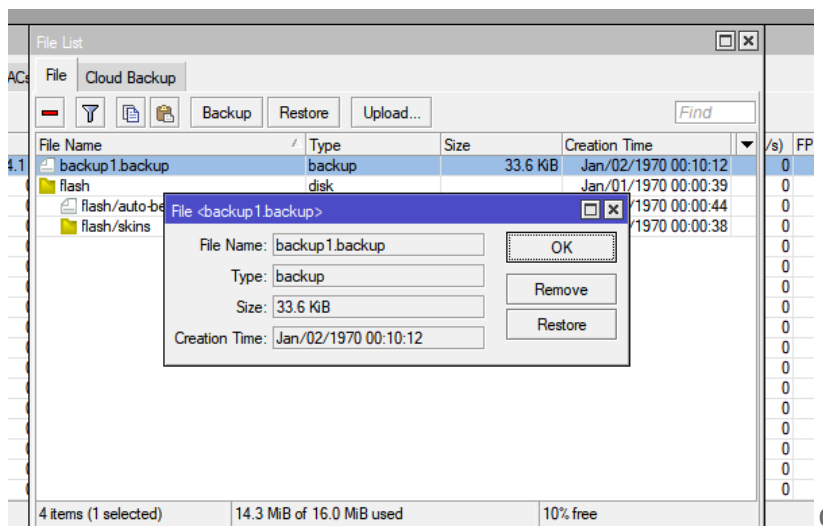
Ahora vamos a comprobar que todo funciona. La IP dentro del rango que le damos, y también que nos da acceso a internet



Y comprobamos que nos da una ip que tenemos en el rango

## Copia de seguridad

Vamos a hacer una copia de seguridad de lo que llevamos por si en cualquier circunstancia nos diera un error y tendremos que volver a restaurarla para ello nos vamos a File → Backup → y le ponemos el nombre que queremos



## Firewall - Filtrar tráfico entrante

## Vamos a crear algunas reglas para que el router sea más seguro

## Permitir SSH

La regla está configurada en el *firewall* del router, específicamente en la *chain* (cadena) Input. Esta cadena controla el tráfico que llega directamente al router, es decir, no el tráfico que atraviesa el router hacia otros dispositivos.

Permitir que los administradores puedan acceder al router de forma remota utilizando el protocolo SSH. Este tipo de acceso remoto es útil para tareas como:

Configuración inicial.

### Solución de problemas.

## Actualización de configuraciones.

- ## 1. Chain: Input

Esto indica que la regla se aplica al tráfico destinado al propio router, no al tráfico que se enruta hacia otros dispositivos.

2. Action: Accept

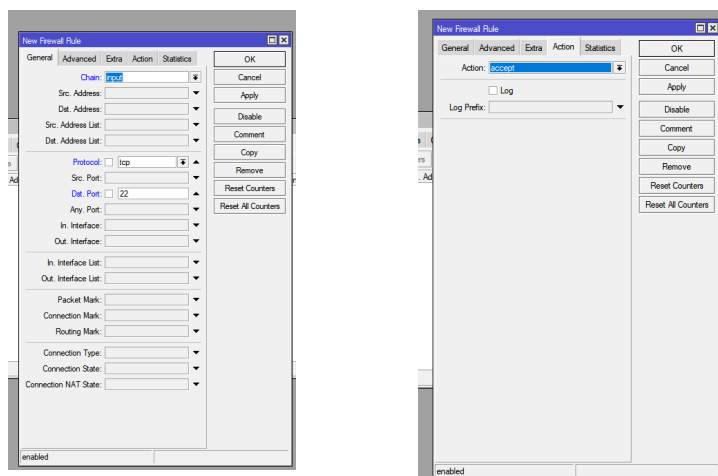
El tráfico que coincide con esta regla será permitido. Esto significa que el router aceptará las conexiones entrantes de SSH.

- ### 3. Protocol: TCP

SSH opera sobre el protocolo TCP, que es orientado a conexión y confiable.

4. Dst. Port: 22

El puerto 22 es el predeterminado para SSH. Si en algún momento se cambia el puerto de SSH, esta regla necesitaría ser actualizada para reflejar el nuevo puerto.





## Permitir WinBox

Esta regla se ha diseñado para permitir que los administradores puedan acceder al router a través de la interfaz gráfica de WinBox. Esta interfaz es útil para tareas como:

Configuración visual y más amigable del router.

Diagnóstico y mantenimiento.

Supervisión en tiempo real de las configuraciones y el estado del sistema.

### 1. Chain: Input

La regla se aplica al tráfico dirigido al propio router. Esto significa que permite las conexiones a la interfaz de administración gráfica del router.

### 2. Action: Accept

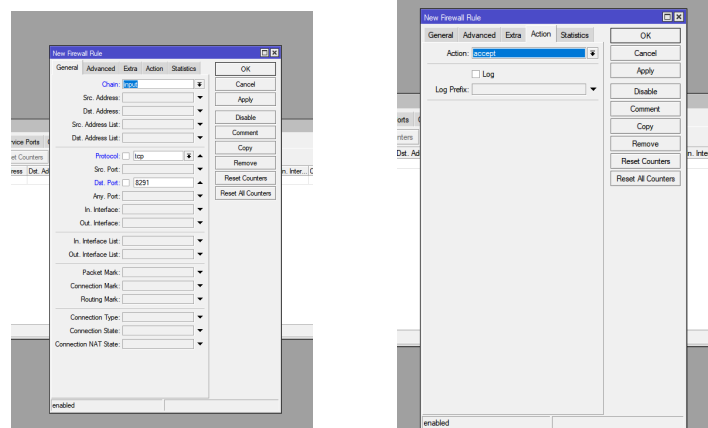
El tráfico que coincida con esta regla será aceptado y procesado. El router permitirá las conexiones entrantes al puerto utilizado por WinBox.

### 3. Protocol: TCP

WinBox utiliza el protocolo TCP, que garantiza una conexión estable y confiable.

### 4. Dst. Port: 8291

El puerto 8291 es el predeterminado para las conexiones de WinBox. Si en algún momento se cambia este puerto en la configuración del router, la regla deberá ajustarse para reflejar el nuevo número de puerto.



## Firewall - Filtrar tráfico saliente

### Permitir servicios esenciales

Esta regla tiene como propósito permitir que el tráfico saliente del router hacia servicios esenciales, como DNS, sea procesado. Esto es necesario para que el router pueda realizar ciertas operaciones básicas de conectividad.

#### 1. Chain: Output

La regla aplica al tráfico saliente generado por el propio router. Esto no afecta al tráfico que el router enruta entre otras redes, sino sólo al tráfico originado directamente por el router.

#### 2. Action: Accept

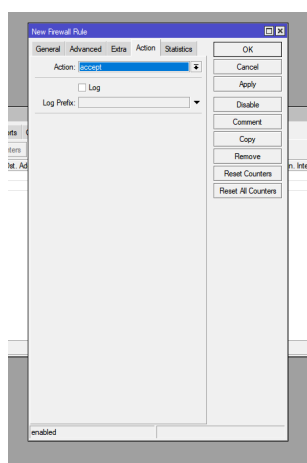
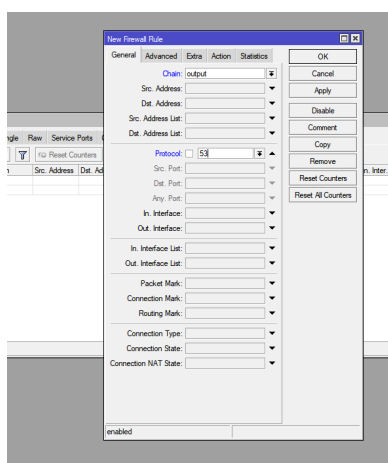
Este tráfico será permitido, lo que significa que el router podrá enviar y recibir paquetes relacionados con el servicio DNS.

#### 3. Protocol: DNS

El DNS (Sistema de Nombres de Dominio) usa el protocolo UDP para consultas normales y ocasionalmente TCP para transferencias de zona o respuestas más largas.

#### 4. Dst. Port: 53

El puerto 53 es el predeterminado para DNS. Este es el puerto al que se dirigen las consultas DNS para resolver nombres de dominio en direcciones IP.



## Bloquear tráfico no autorizado

Esta regla tiene el objetivo de bloquear cualquier tráfico saliente no autorizado desde el router hacia internet. Esto forma parte de una estrategia de seguridad para limitar las actividades del router únicamente a aquellas que sean estrictamente necesarias, minimizando riesgos.

### 1. Chain: Output

Esta regla afecta el tráfico saliente generado por el propio router. Específicamente, controla las comunicaciones que el router inicia hacia otras redes o hacia internet.

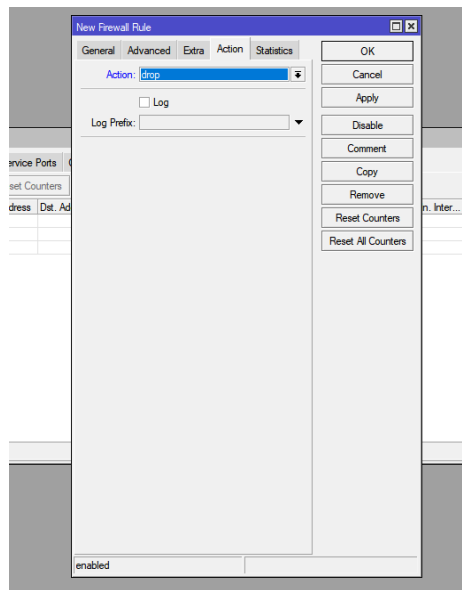
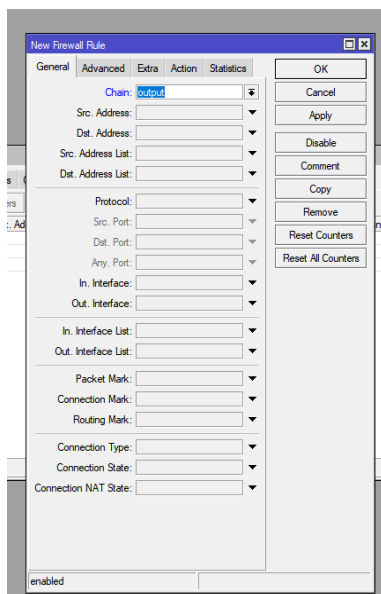
### 2. Action: Drop

Todo tráfico que coincida con esta regla será bloqueado. Los paquetes no serán enviados ni procesados más allá de esta regla.

### 3. Propósito principal

La regla actúa como un mecanismo de seguridad:

- Prevención de tráfico innecesario: El router no podrá generar tráfico hacia internet a menos que existan reglas específicas que lo permitan (como la regla de DNS mencionada antes).
- Reducción de vectores de ataque: Al limitar las conexiones salientes, se evita que el router se conecte a destinos no confiables, lo que podría ser explotado por malware o ataques dirigidos.



## Beneficios de esta regla

1. Control estricto del tráfico del router
  - Garantiza que el router no realice comunicaciones imprevistas o no autorizadas, mejorando la seguridad general de la red.
2. Minimización de riesgos de malware
  - Si el router está comprometido, esta regla puede limitar la capacidad del atacante de comunicarse con servidores de comando y control (C2).
3. Aumento de la eficiencia y confiabilidad
  - Al reducir el tráfico innecesario, se mejora el uso de recursos y se evitan problemas derivados de conexiones malintencionadas.

## Crear Reglas de Firewall para Mitigar DDoS

El *Connection Tracking* es una función que permite al firewall de un router MikroTik llevar un registro detallado de todas las conexiones que pasan a través de él. Esta herramienta:

- Supervisa y registra el estado de las conexiones activas en tiempo real.
- Permite saber cuántas conexiones tiene abiertas cada IP.
- Clasifica las conexiones según su estado, como nuevas, establecidas o cerradas.

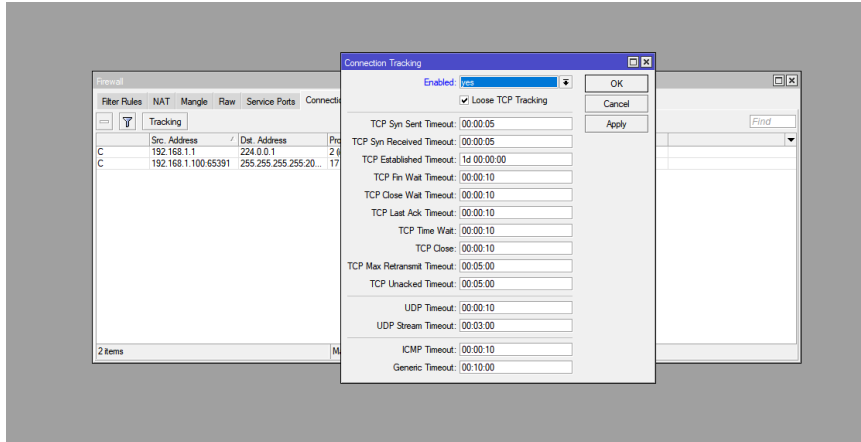
Gracias a esta capacidad, el router puede identificar comportamientos sospechosos, como una IP que intenta abrir demasiadas conexiones al mismo tiempo, algo típico de ataques DDoS.

Es fundamental habilitar el "Connection Tracking"

Monitoreo preciso: Ayuda al router a identificar IPs que generan un número inusual de conexiones simultáneas.

Necesario para configuraciones avanzadas: Muchas reglas avanzadas de seguridad en el firewall requieren esta función activa para contar y limitar conexiones.

Protección frente a ataques: Facilita la detección y bloqueo de tráfico anómalo o excesivo, evitando que el router se sobrecargue durante un ataque DDoS.



Ahora, vamos a crear una regla de firewall que limite el número de conexiones simultáneas permitidas por una IP. Si una IP supera el umbral, se bloqueará automáticamente.

Configurar los parámetros de la regla:

Chain: Selecciona input si estás protegiendo el tráfico hacia el router o forward si estás protegiendo el tráfico que pasa a través del router.

Protocol: Deja como all o selecciona un protocolo específico (por ejemplo, TCP o UDP).

Src. Address List: No es necesario configurarlo, ya que vamos a bloquear por número de conexiones.

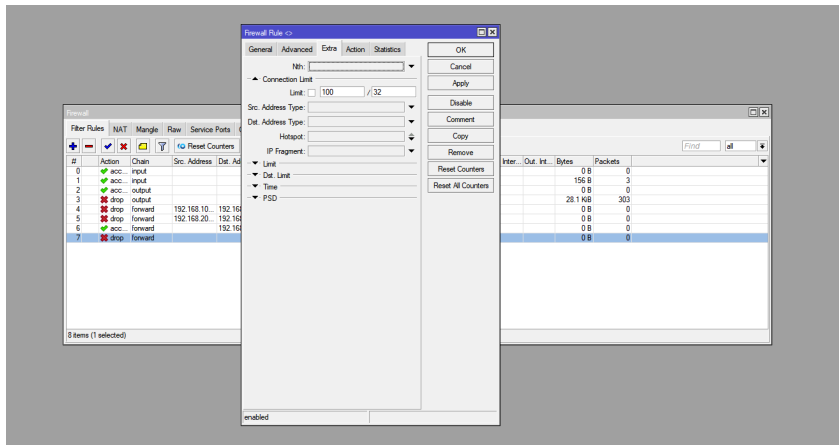
Connection Limit: Aquí es donde puedes establecer el número máximo de conexiones permitidas por IP. Por ejemplo, para permitir solo 100 conexiones simultáneas:

Connection Limit: 100,32 (esto significa que una IP podrá tener 100 conexiones activas, pero se bloqueará después de 100 conexiones).

Action: Selecciona drop, para que se descarten las conexiones cuando se sobrepase el límite.

```
[admin@MikroTik Antonio] > /ip firewall filter add chain=forward connection-limit=100,32 action=drop
```

Aquí podemos ver que la regla se ha creado correctamente



## Configuración de Reglas Adicionales para Mitigar DDoS

Esta configuración está diseñada para proteger tu router MikroTik contra ataques que abusen de los paquetes **SYN**. Estos paquetes son usados para iniciar conexiones TCP y, en un ataque, podrían inundar el sistema con solicitudes falsas, agotando los recursos del router.

- **Chain::** Elige **forward** si quieres proteger el tráfico que pasa a través del router hacia otros dispositivos de la red.
- **Protocol :** Seleccionamos **tcp**, ya que los paquetes SYN pertenecen a este protocolo.
- **TCP Flags:** Marcamos la casilla **SYN** para filtrar solo los paquetes SYN, que son los utilizados para iniciar conexiones.
- **Connection State:** Configuramos esta opción como **new**, para actuar solo sobre nuevas conexiones que están en proceso de ser establecidas.
- **Action :** Selecciona **drop**, para que el router descarte los paquetes que coincidan con la regla. Esto bloquea los intentos de inundar el sistema con solicitudes SYN.

```
[admin@MikroTik Antonio] > /ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new action=drop
```

### Limitar el número de conexiones por puerto o protocolo

#### ¿Por qué vamos a limitar conexiones por puerto?

**Objetivo de un ataque DDoS dirigido:** En un ataque DDoS, los atacantes pueden concentrarse en un puerto específico, como el 80 (HTTP), para intentar inutilizar servicios web o aplicaciones.

**Solución:** Establecer un límite máximo de conexiones simultáneas hacia ese puerto. Si una IP intenta exceder ese límite, el router bloqueará esas conexiones automáticamente.

## Configuración de la Regla de Firewall:

- **Chain:** forward para proteger el tráfico que pasa a través del router.
- **Protocol:** Selecciona el protocolo específico (por ejemplo, TCP o UDP) según el ataque.
- **Dst. Port:** Especifica el puerto a proteger (por ejemplo, 80 para HTTP, 443 para HTTPS, o 22 para SSH).
- **Connection Limit:**
  - Define el límite máximo de conexiones simultáneas por IP, como 50, 32, lo que permite hasta 50 conexiones antes de bloquear.
- **Action:**
  - Selecciona drop para descartar las conexiones que excedan el límite.

```
[admin@MikroTik Antonio] > /ip firewall filter add chain=forward protocol=tcp dst-port=80 connection-limit=20,32 action=drop
```

## Activar el Registro (Logging) de Reglas de Firewall

Es útil habilitar el registro de las reglas para observar qué IPs están siendo bloqueadas y así ajustar las reglas según sea necesario.

```
[admin@MikroTik Antonio] > /ip firewall filter add chain=forward protocol=tcp connection-limit=100,32 action=drop log=yes  
[admin@MikroTik Antonio] > █
```



## Monitoreo de tráfico

### Habilitar SNMP

Habilitar SNMP en un router MikroTik permite que el dispositivo proporcione datos a herramientas de monitoreo externas.

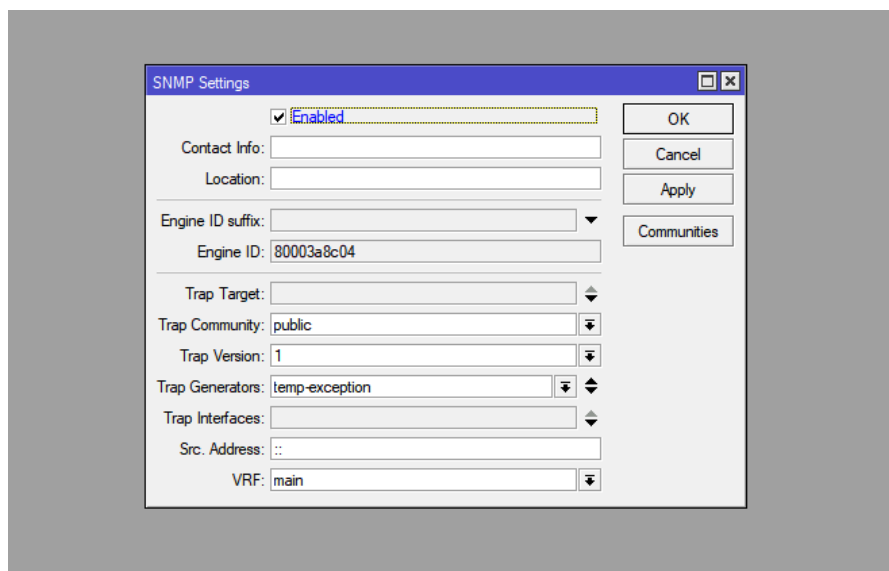
Ve a IP > SNMP

Accedemos al menú de configuración de SNMP en el MikroTik. Esta opción permite habilitar y configurar cómo el router responde a las solicitudes SNMP.

Marcamos Enabled

Esto activa el protocolo SNMP en el router. Una vez activado, el MikroTik puede enviar datos solicitados por herramientas externas que soportan SNMP.

Configuramos un trap community y lo ponemos por ejemplo en público y aplicamos y guardamos



## Habilitamos touch

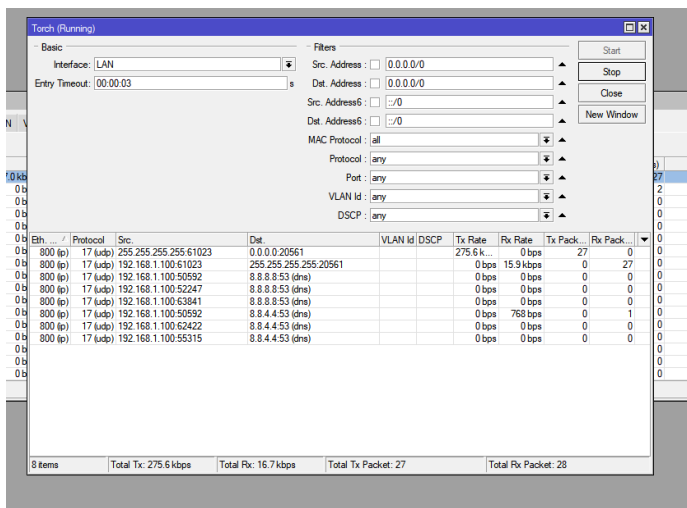
**Torch** es una herramienta muy útil en MikroTik para observar el tráfico de la red en tiempo real. Permite ver en detalle qué dispositivos están usando más ancho de banda y qué protocolos están siendo utilizados en cada interfaz.

1. Ve a **Tools > Torch** en la interfaz de MikroTik.
2. Elige la interfaz que quieres monitorear, como la **WAN** o la **LAN**.
3. Haz clic en **Start** para comenzar a capturar el tráfico de esa interfaz.
4. Puedes aplicar filtros por **IP** o **Protocolos** si deseas ver solo el tráfico específico que te interesa.

Una vez que esté activo, verás estadísticas en vivo, tales como:

- **Ancho de banda por IP:** Qué cantidad de datos está enviando o recibiendo cada dispositivo en la red.
- **Protocolo utilizado:** Qué protocolos están siendo usados (por ejemplo, TCP, UDP, etc.).
- **Puertos y tasas de transferencia:** Qué puertos están en uso y las tasas de transferencia asociadas a cada uno.

Esta herramienta es ideal para detectar posibles problemas de red, como dispositivos que consumen demasiado ancho de banda o identificar cuellos de botella en el tráfico.



The screenshot shows the MikroTik Torch interface with the 'Basic' tab selected. The 'Interface' is set to 'LAN'. The 'Filters' section shows various criteria like Src. Address, Dst. Address, Src. Address6, Dst. Address6, MAC Protocol, Protocol, Port, VLAN Id, and DSCP, all set to 'any' or 'all'. The 'Start' button is highlighted. Below the filters, a table displays real-time traffic statistics for 8 items.

Seq.	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pack.
800 (ip)	17 (udp)	255.255.255.61023	0.0.0.0:20561			275.6 kbps	0 bps	27	0
800 (ip)	17 (udp)	192.168.1.100:61023	255.255.255.255:20561			0 bps	15.9 kbps	0	27
800 (ip)	17 (udp)	192.168.1.100:50592	8.8.8.8:53 (dns)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.1.100:52247	8.8.8.8:53 (dns)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.1.100:53041	8.8.8.8:53 (dns)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.1.100:50592	8.8.4.4:53 (dns)			0 bps	768 bps	0	1
800 (ip)	17 (udp)	192.168.1.100:62422	8.8.4.4:53 (dns)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.1.100:55315	8.8.4.4:53 (dns)			0 bps	0 bps	0	0

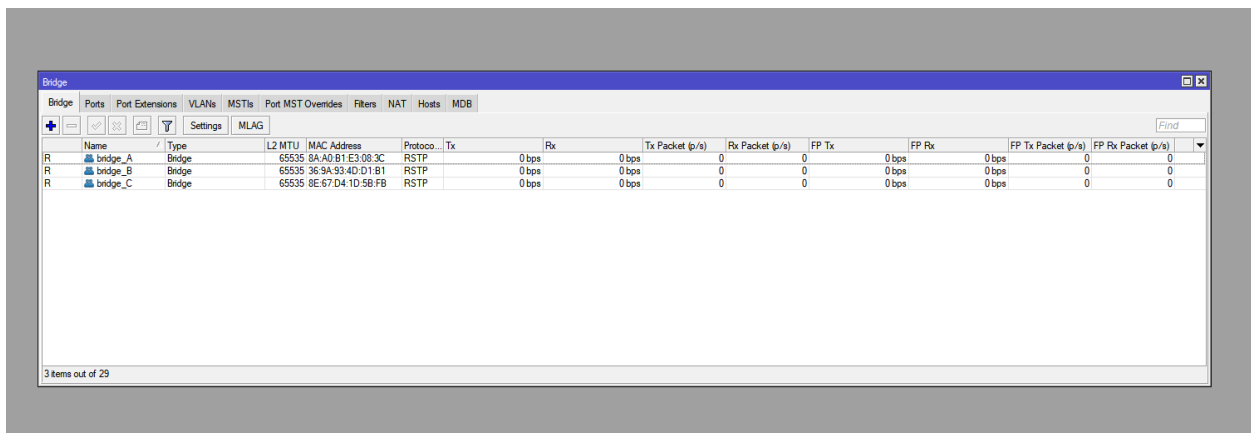
Summary statistics at the bottom:

8 items	Total Tx: 275.6 kbps	Total Rx: 16.7 kbps	Total Tx Packet: 27	Total Rx Packet: 28
---------	----------------------	---------------------	---------------------	---------------------

## Crear 3 subredes con Bridges y servidores DHCP

Para la creación de las subredes vamos a crear 3 bridges. Cada subred (A, B y C) funcionará como una red independiente, con sus propias IPs y servicios, separadas lógicamente entre sí.

Creemos los bridges y los llamamos A,B y C



Cada subred necesita uno o más puntos físicos de conexión (los puertos Ethernet del Mikrotik). Al asignar puertos Ethernet específicos a cada Bridge, estamos definiendo físicamente dónde los dispositivos se pueden conectar para ser parte de una subred específica.

Ejemplo:

Si conectamos un cable al puerto 3 o 4 (asignado a Bridge\_A), el dispositivo será parte de la subred A.

Esto segmenta las conexiones físicas, haciendo que las subredes no se mezclen.

Le asignaremos el puerto 3 y 4 al bridge A, el puerto 4 y 5 al bridge B , el puerto 6 y 7 al bridge C

#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	PVID	Role	Root Pat...
0 IH	ether3	bridge_A	no		80	10	1	disabled port	
1 IH	ether4	bridge_A	no		80	10	1	disabled port	
2 I	ether5	bridge_B	no		80	10	1	disabled port	
3 I	ether6	bridge_B	no		80	10	1	disabled port	
4 I	ether7	bridge_C	no		80	10	1	disabled port	
5 I	ether8	bridge_C	no		80	10	1	disabled port	

Al configurar IPs para cada Bridge en IP → Addresses, estamos asignando una dirección IP a cada bridge para que:

Cada subred tenga un gateway (puerta de enlace):

Las direcciones IP asignadas (192.168.10.1, 192.168.20.1, 192.168.30.1) serán las puertas de enlace predeterminadas para los dispositivos conectados a cada bridge.

El router pueda comunicarse con las subredes:

Estas IPs permiten que el router identifique y gestione las conexiones entre dispositivos en cada subred.

Por ejemplo, un equipo conectado a Bridge-A puede enviar solicitudes a Bridge-C a través del router.

Address	Network	Interface
192.168.1.1/24	192.168.1.0	LAN
192.168.1.216/24	192.168.1.0	WAN
192.168.10.1/24	192.168.10.0	bridge_A
192.168.20.1/24	192.168.20.0	bridge_B
192.168.30.1/24	192.168.30.0	bridge_C

## Configurar reglas de firewall para aislar subredes

El firewall actúa como un sistema de control que permite o bloquea el tráfico entre diferentes partes de la red según reglas que se defina

Bloquear comunicación entre A y B:

Estas reglas aseguran que los dispositivos en la subred A no puedan comunicarse con los dispositivos en la subred B, y viceversa. Esto es útil si quieres aislar redes para mayor seguridad o privacidad (por ejemplo, una red de visitantes y una red interna).

Permitir acceso a la subred C:

La subred C queda accesible desde las subredes A y B. Esto significa que los dispositivos en A y B pueden enviar datos a dispositivos en C (y recibir respuestas). Puede ser útil para recursos compartidos, como impresoras o servidores.

```
[admin@MikroTik Antonio] > /ip firewall filter add chain=forward src-address=192.168.10.0/24 dst-address=192.168.20.0/24 action=drop

[admin@MikroTik Antonio] > /ip firewall filter add chain=forward src-address=192.168.20.0/24 dst-address=192.168.10.0/24 action=drop
```

## Crear los servidores DHCP para cada subred:

DHCP\_A será el servidor DHCP que asigna direcciones IP dentro del rango 192.168.10.10 - 192.168.10.254 a los dispositivos conectados a bridge\_A.

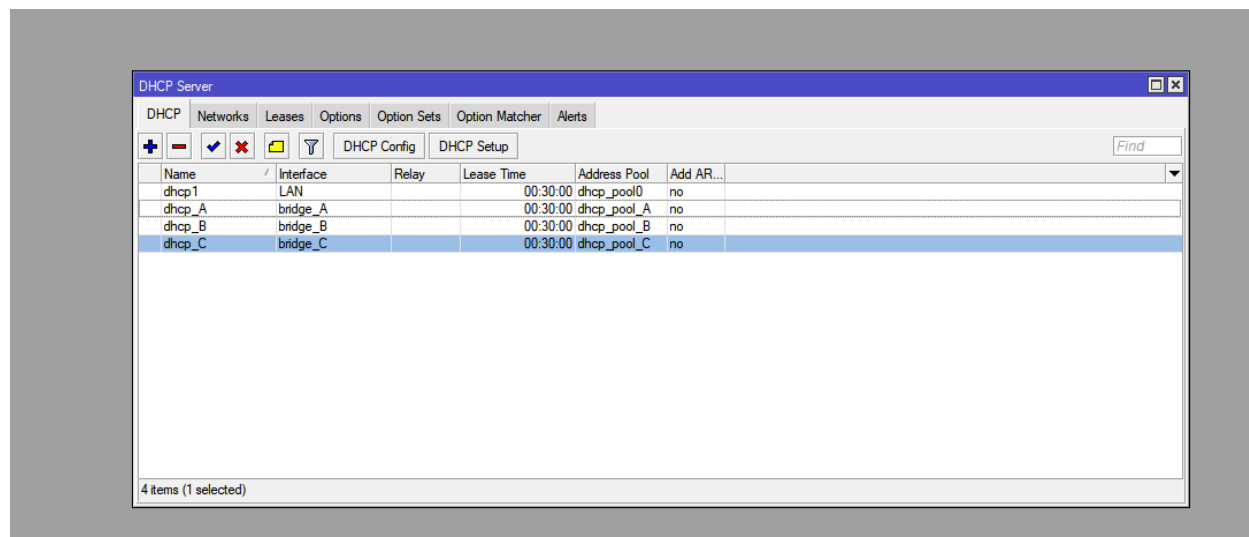
DHCP\_B hará lo mismo con el rango 192.168.20.10 - 192.168.20.254 en bridge\_B.

DHCP\_C manejará el rango 192.168.30.10 - 192.168.30.254 en bridge\_C.

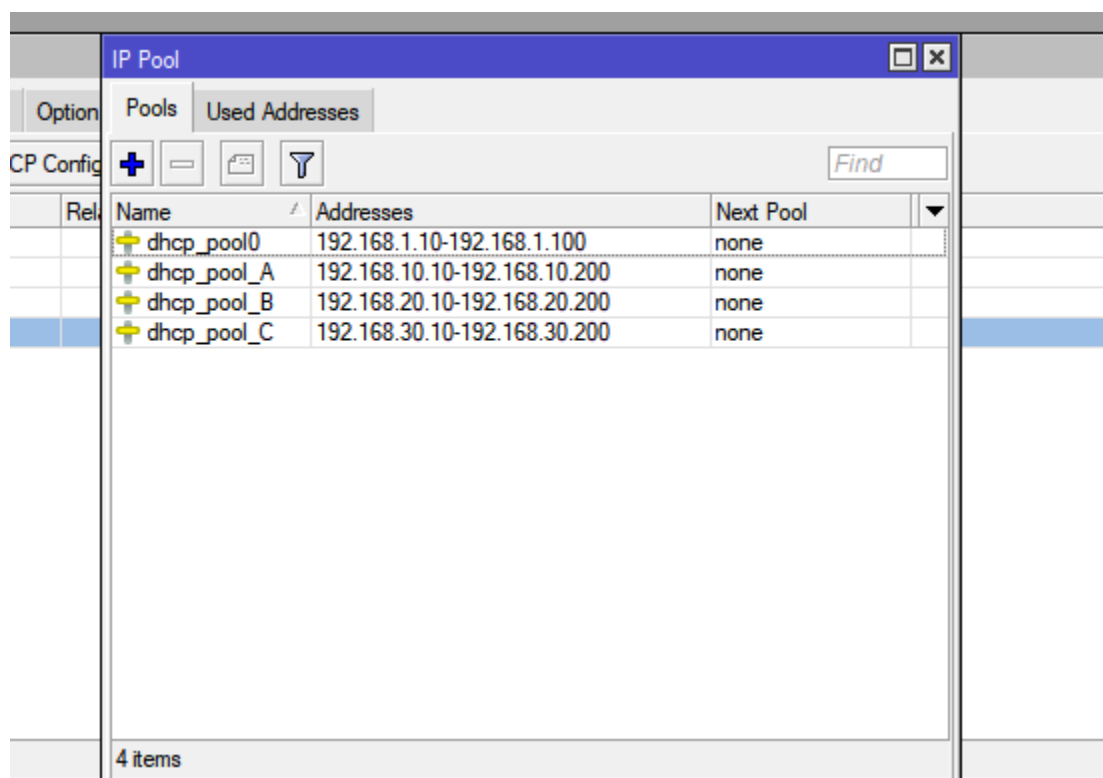
Asociar cada servidor DHCP con su bridge:

El servidor DHCP se configura para trabajar únicamente en el bridge al que está asignado.

Esto garantiza que los dispositivos en cada subred reciban IPs dentro del rango correspondiente y no de otra subred.



Aquí podemos comprobar los rangos de ip que tienen cada bridge



## Creación de una regla nat para acceder a un equipo de la subred C

### ¿Qué estamos haciendo?

Configuramos una regla de NAT de destino (dst-nat) que redirige el tráfico que llega desde Internet a la dirección IP pública fija (tu router) hacia un servidor web ubicado en la subred C (192.168.30.100).

Específicamente, cualquier conexión entrante al puerto 80 (HTTP) de la IP pública será redirigida al puerto 80 del servidor interno.

### Desglose de los parámetros:

Chain: dstnat

Indica que esta regla se aplica al tráfico entrante que necesita ser redirigido.

Dst. Address: Tu IP pública fija.

Especifica que esta regla se activa solo cuando alguien accede a tu IP pública.

Protocol: tcp

Limita la regla a conexiones TCP (usadas por servicios como HTTP).

Dst. Port: 80

Filtra el tráfico que llega específicamente al puerto 80 (HTTP).

Action: dst-nat

Indica que el tráfico debe ser redirigido.

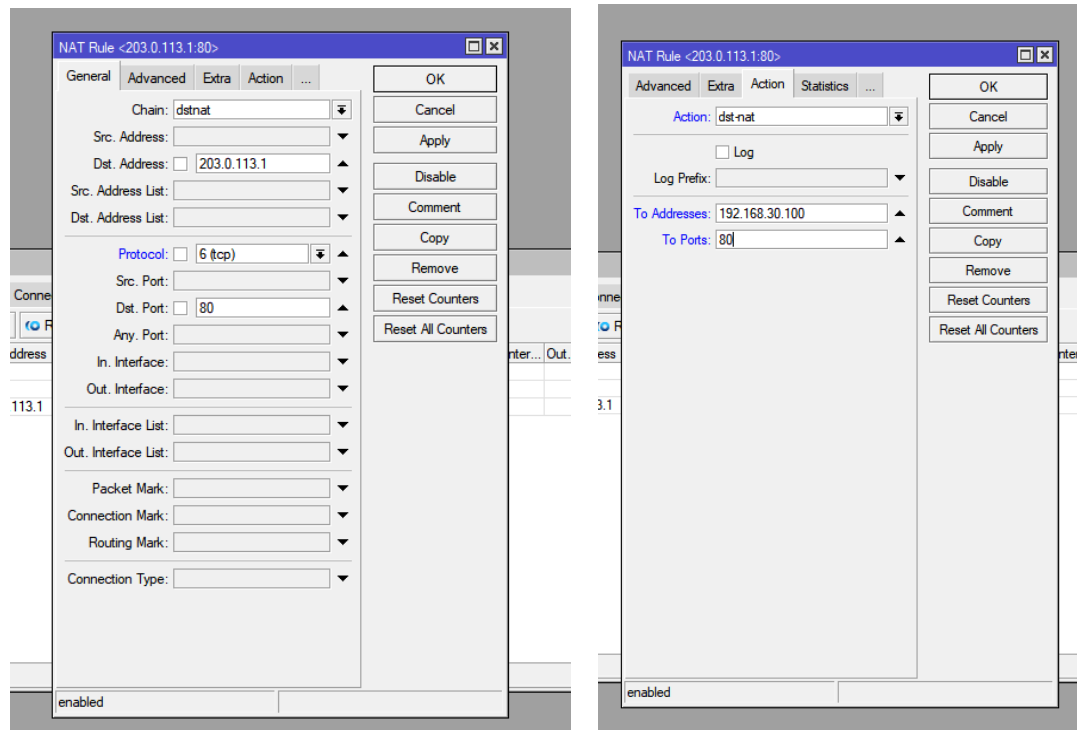
To Address: IP del servidor interno (192.168.30.x)

Especifica que el tráfico debe ser reenviado a esta dirección dentro de la red

local.

To Ports: 80

Asegura que el tráfico sea enviado al puerto 80 del servidor interno.



## Crear una regla de Firewall para permitir acceso

### ¿Qué estamos haciendo?

Configuramos una regla en el Firewall para permitir que el tráfico redirigido (gracias a la regla NAT) pueda llegar al servidor web en la subred C.

Esto es necesario porque el firewall de Mikrotik bloquea por defecto cualquier tráfico que no sea permitido explícitamente.



### Desglose de los parámetros:

Chain: forward

Indica que esta regla afecta al tráfico que pasa a través del router (de Internet hacia una red interna, en este caso).

Dst. Address: IP del servidor (192.168.30.x)

Filtra solo el tráfico destinado a este servidor específico.

Protocol: tcp

Se limita a conexiones TCP, usadas por HTTP.

Dst. Port: 80

Permite únicamente tráfico hacia el puerto 80 del servidor web.

Action: accept

Indica que este tráfico debe ser permitido.

The screenshot shows the 'General' tab of the 'Firewall Rule <192.168.30.100:80>' configuration window. The 'Chain' is set to 'forward'. The 'Dst. Address' is '192.168.30.100'. The 'Protocol' is '6 (tcp)'. The 'Dst. Port' is '80'. The 'In. Interface' and 'Out. Interface' are both set to 'eth0'. The 'Packet Mark', 'Connection Mark', and 'Routing Mark' are all empty. The 'Connection Type', 'Connection State', and 'Connection NAT State' are also empty. The 'enabled' checkbox is checked.

The screenshot shows the 'Action' tab of the 'Firewall Rule <192.168.30.100:80>' configuration window. The 'Action' is set to 'accept'. The 'Log' checkbox is unchecked. The 'Log Prefix' is empty. The 'enabled' checkbox is checked.

## Creación de un Script que genere y envíe por email: el backup binario y el Export completo

### Crear el Script

¿Qué estamos haciendo?

Creamos un script en el router MikroTik que automatiza el proceso de realizar un backup binario, exportar la configuración completa del router, y enviar ambos archivos por correo electrónico.

Desglose de acciones en el script:

Backup binario:

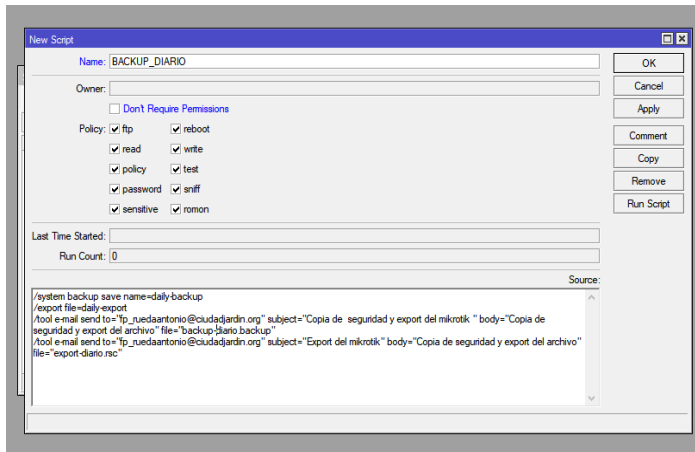
El comando `/system backup save name=daily_backup` genera un archivo binario con la configuración completa del router, incluidas contraseñas encriptadas. Este archivo se puede restaurar fácilmente en el mismo modelo de router.

Export completo:

El comando `/export file=daily_export` genera un archivo de texto (.rsc) con toda la configuración del router. Este archivo es útil para auditar o replicar configuraciones en otros dispositivos.

Enviar por correo:

El comando `/tool e-mail send` envía ambos archivos a un correo electrónico especificado. Esto asegura que los backups estén disponibles fuera del router, incluso en caso de fallo del hardware.



## Configurar el Servidor de Correo

¿Qué estamos haciendo?

Configuramos el router MikroTik para que utilice los servidores de Gmail (u otro proveedor) para enviar correos electrónicos.

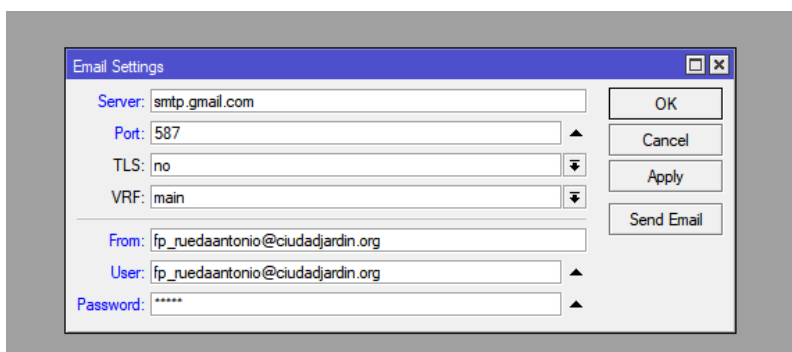
Esto incluye especificar:

Servidor SMTP: smtp.gmail.com para Gmail.

Puerto: 587, que es el puerto estándar para conexiones seguras usando TLS.

Credenciales: Dirección de correo y contraseña (o clave de aplicación en caso de que 2FA esté activado).

TLS: Activamos la seguridad para cifrar las comunicaciones con el servidor de correo.



## Crear el Evento Diario

¿Qué estamos haciendo?

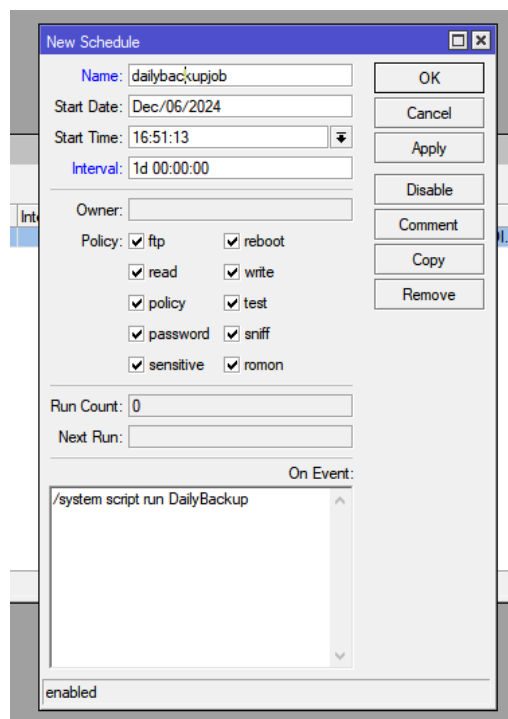
Creamos un evento programado (Scheduler) para ejecutar automáticamente el script de backup todos los días.

Configuramos los siguientes parámetros:

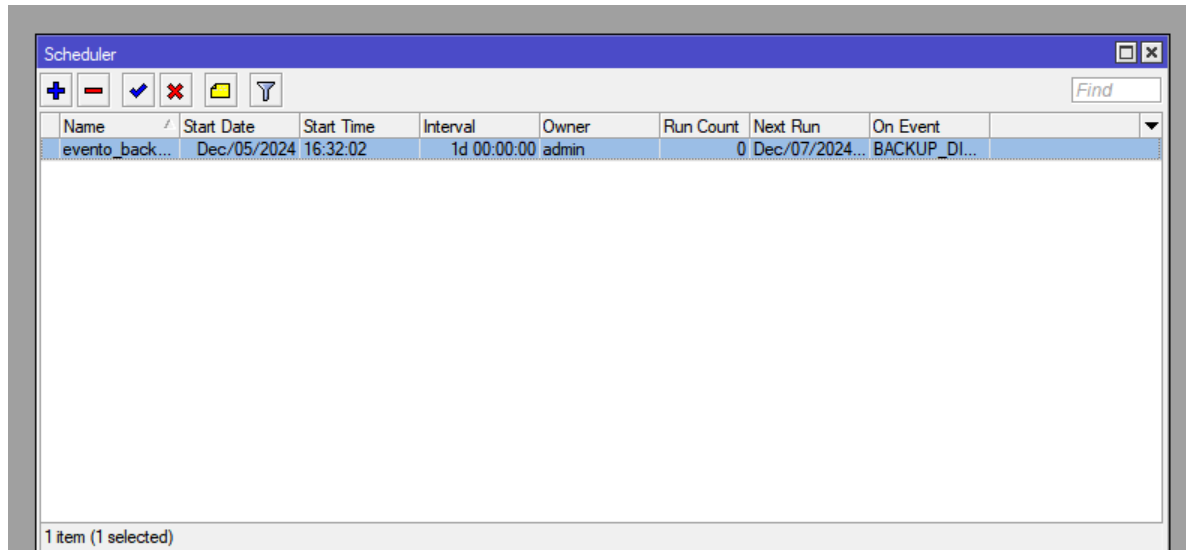
Intervalo: 1d, lo que significa que el evento se ejecutará cada 24 horas.

Hora de inicio: La hora específica en la que se ejecutará el script (por ejemplo, 03:00:00).

Comando: /system script run DailyBackup, que ejecuta el script creado previamente.



Aquí podemos ver el evento creado con toda la información necesaria configurada según lo explicado anteriormente. Todos los parámetros, condiciones y acciones están completos y listos. Esto asegura que la configuración esté correcta y lista para ser ejecutada.



The screenshot shows the Mikrotik Scheduler application window. It has a blue title bar with the text 'Scheduler'. Below the title bar is a toolbar with icons for adding, deleting, enabling, disabling, and filtering tasks, along with a 'Find' search box. The main area is a table with the following columns: Name, Start Date, Start Time, Interval, Owner, Run Count, Next Run, and On Event. A single task is listed in the table.

Name	Start Date	Start Time	Interval	Owner	Run Count	Next Run	On Event
evento_back...	Dec/05/2024	16:32:02	1d 00:00:00	admin	0	Dec/07/2024...	BACKUP_DI...

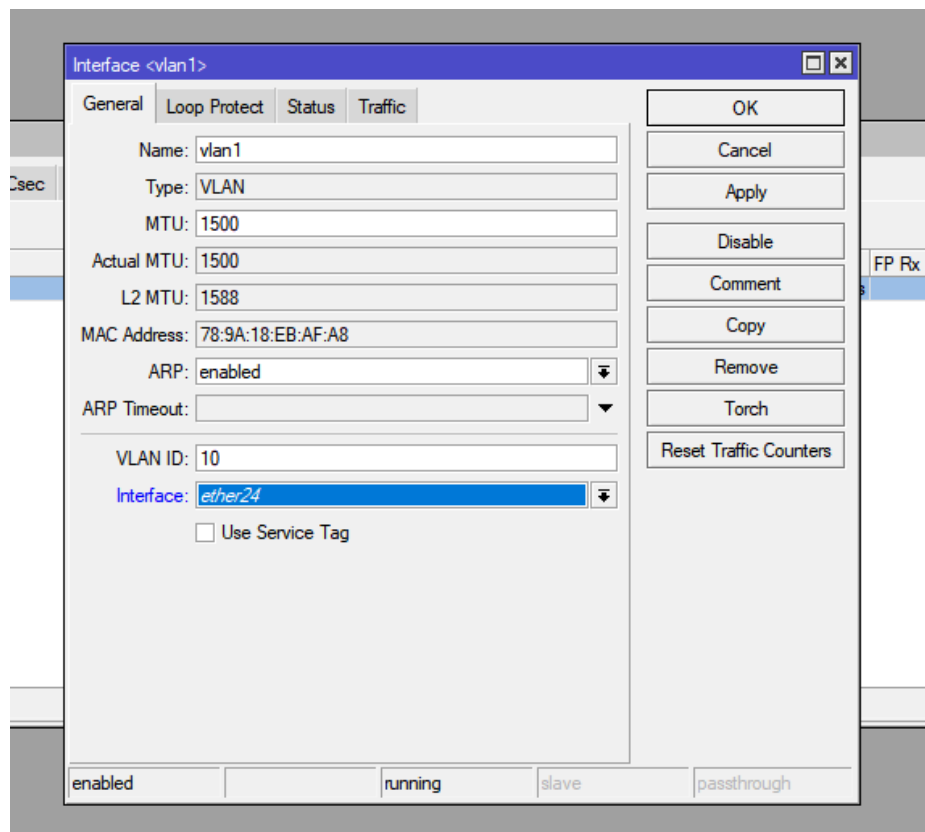
1 item (1 selected)

## Configurar VLANs en MikroTik

Las VLANs (Virtual LANs) son una herramienta para dividir una red física en varias subredes lógicas. Esto permite segmentar el tráfico de forma más eficiente, mejorando el rendimiento, la seguridad y la organización de la red.

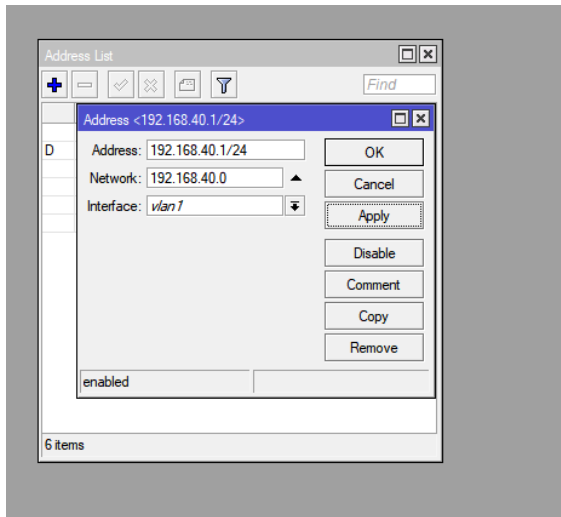
Configuración de los parámetros necesarios:

- Name (Nombre):
  - Asigna un nombre descriptivo a la VLAN.
- VLAN ID:
  - Este es el identificador único de la VLAN dentro de la red.
- Interface (Interfaz física):
  - Especifica la interfaz física o puente (bridge) donde funcionará la VLAN.



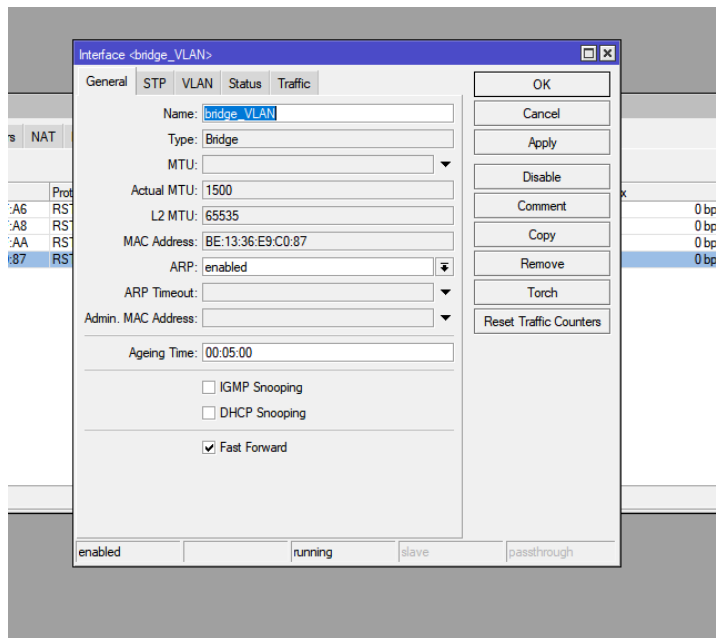
### Asignar una IP a la VLAN

Para que se pueda enrutar el tráfico entre VLANs o conectarnos a la VLAN, necesitaremos asignar una dirección IP a la interfaz VLAN.



### Configuración de un Bridge (Puentes) para VLANs

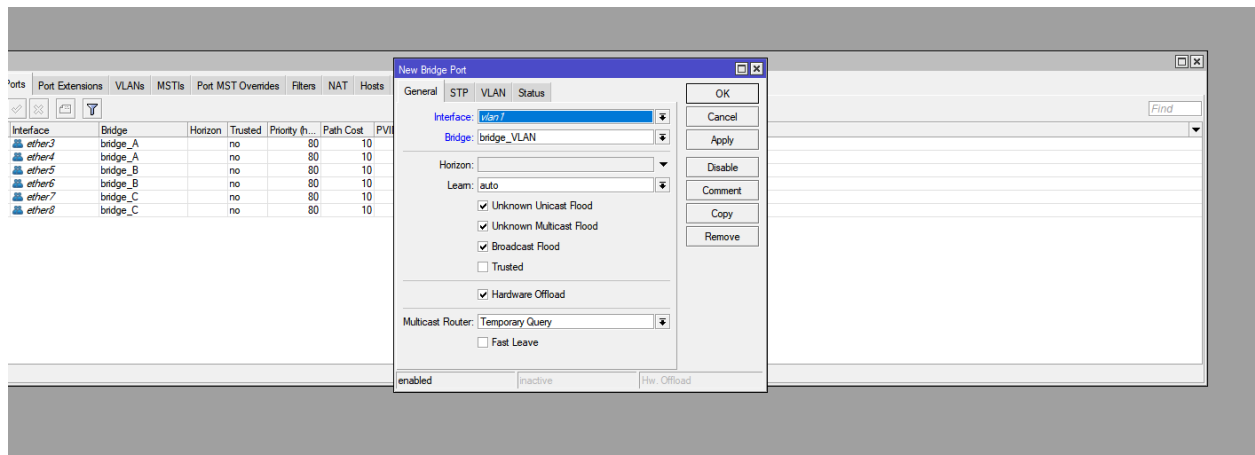
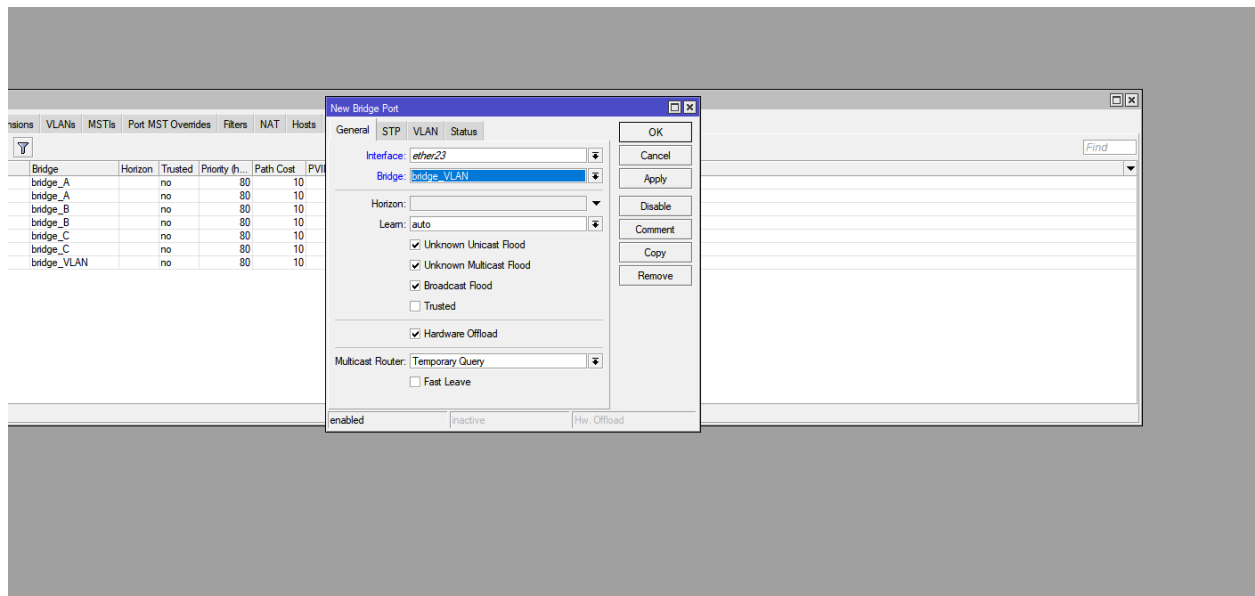
Le asignamos un nombre al bridge que permite que las VLANs compartan el mismo segmento de red y puedan comunicarse entre sí como si estuvieran directamente conectadas.



### Añadir Interfaces al Bridge

Aquí lo que estamos haciendo es **añadir interfaces físicas o VLANs a un puente (bridge)** en MikroTik, lo que permite combinar varias interfaces de red en una sola red lógica. Esto facilita la comunicación entre las interfaces que forman parte del mismo puente, ya que compartirán la misma red.



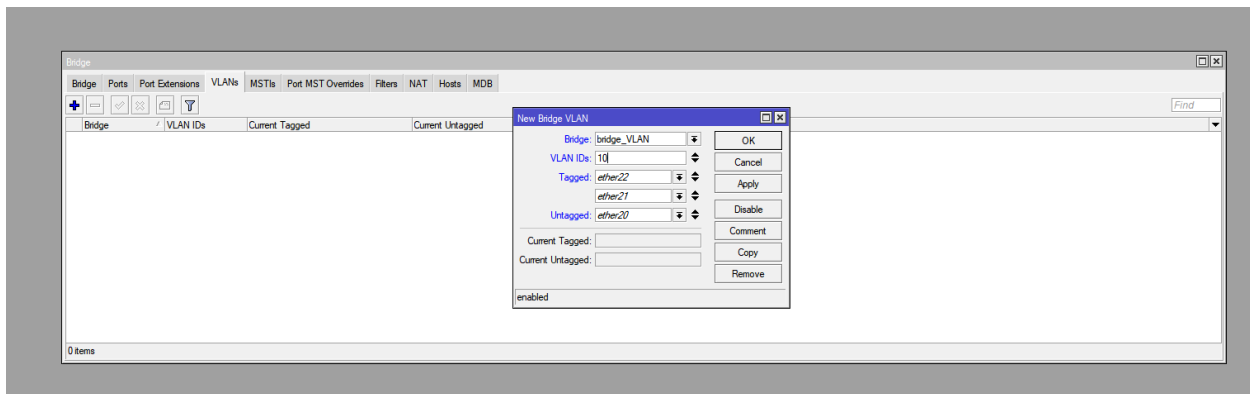


Al agregar estas interfaces al puente, ambas (la VLAN y el puerto físico) compartirán la misma red lógica, lo que significa que los dispositivos conectados a esas interfaces podrán comunicarse entre sí como si estuvieran en la misma red local.

## Configurar el Bridge para VLANs

Cuando trabajamos con **VLANs** (Redes de Área Local Virtuales) y un **Bridge** (puente) en MikroTik, es importante configurar correctamente cómo se maneja el tráfico entre estas VLANs. Existen dos formas de manejar este tráfico:

- **Tagged (Etiquetado):** Esto significa que los paquetes de datos que viajan por la red llevan una "etiqueta" que indica a qué VLAN pertenece. Es como si el paquete tuviera una identificación que lo clasifica en una VLAN específica.
- **Untagged (Sin Etiqueta):** En este caso, los paquetes no llevan una etiqueta. El dispositivo receptor los trata como parte de una VLAN predeterminada, sin necesidad de saber a qué VLAN originalmente pertenecían.



## Verificación de Configuración

Para asegurarte de que las **VLANs** y su configuración en el **Bridge** están funcionando correctamente en Mikrotik, puedes usar ciertos comandos en la **CLI** (línea de comandos) para verificar el estado de las configuraciones.

```
[admin@MikroTik Antonio] > /interface vlan print
Columns: NAME, MTU, ARP, VLAN-ID, INTERFACE
# NAME    MTU  ARP    VLAN-ID  INTERFACE
0 vlan1  1500  enabled    10    ether24
[admin@MikroTik Antonio] > /interface bridge vlan print
Columns: BRIDGE, VLAN-IDS
# BRIDGE    VLAN-IDS
0 bridge_VLAN    10
[admin@MikroTik Antonio] >
```

### **/interface vlan print**

Este comando te dará una lista de todas las VLANs configuradas en el router, mostrando detalles como el nombre de la interfaz, el ID de la VLAN, la interfaz física asociada, entre otros. Aquí podrás verificar si las VLANs están correctamente creadas y si están asociadas a las interfaces correspondientes.

### **/interface bridge vlan print**

Este comando muestra cómo se han configurado las VLANs dentro del Bridge. Te dará información sobre qué interfaces están etiquetadas (tagged) y cuáles están sin etiquetar (untagged) para cada VLAN. También verás el ID de la VLAN y cómo las interfaces están relacionadas con el Bridge.

### **¿Qué se puede verificar con estos comandos?**

- **Interfaces VLAN:** Asegúrate de que todas las VLANs estén correctamente configuradas con sus IDs y asociadas a las interfaces correctas.
- **Puente y VLANs:** Verifica que las interfaces dentro del **Bridge** estén correctamente configuradas como **tagged** o **untagged** según lo que necesites, y que el tráfico se esté manejando correctamente entre las VLANs.

## **Conclusión del Proyecto de Configuración y Optimización de un Router MikroTik**

En este proyecto, configuré y optimicé un router MikroTik para mejorar la gestión, rendimiento y seguridad de una red local. Implementé reglas de firewall estrictas para bloquear accesos no autorizados y mitigar riesgos de malware, además de configuraciones avanzadas para supervisar y limitar conexiones sospechosas, protegiendo contra ataques DDoS.

Para optimizar el rendimiento, segmenté la red en subredes lógicas usando VLANs y Bridges, lo que permitió una comunicación más eficiente entre dispositivos, garantizando estabilidad incluso bajo tráfico intenso. También configuré NAT para proporcionar acceso confiable a internet y ajusté el servicio DHCP para simplificar la asignación de direcciones IP.

Automatiza respaldos regulares mediante scripts, asegurando la disponibilidad de configuraciones críticas, y utilicé herramientas como Torch y SNMP para monitorear en tiempo real, detectando posibles problemas de manera oportuna.

Finalmente, la segmentación lógica incrementó la seguridad al aislar subredes y controlar accesos a recursos compartidos. Estas mejoras convirtieron al router MikroTik en una solución robusta y escalable, ideal para redes pequeñas y medianas, preparada para desafíos futuros y fácil de administrar.

## Bibliografía

<https://blog.wifire.me/como-configurar-una-red-en-el-router-mikrotik-winbox/>

<https://mikrotik.com/>

<https://engelausmetall.blogspot.com/2015/04/configuracion-de-equipo-mikrotik-para.html>

[https://mum.mikrotik.com/presentations/HN20/presentation\\_7422\\_1580111784.pdf](https://mum.mikrotik.com/presentations/HN20/presentation_7422_1580111784.pdf)

<https://www.mikrotiklabs.com/2019/07/18/creacion-de-vlan-con-mikrotik/>

<https://abcxperts.com/tipos-de-ataques-de-denegacion-de-servicio-distribuido-ddos/>

<https://abcxperts.com/docs/se-puede-hacer-backup-automaticos-y-mandarlos-a-un-ftp-o-tftp/>

<https://drive.google.com/drive/u/2/home>