

MikroTik - 6 Consejos de Seguridad

Una de las partes mas importantes de la Red es la seguridad, y para apoyar con este tema se muestra este artículo. Una vez instalado un nuevo Router es de vital importancia tomar en cuenta los siguientes consejos.

1. Usuarios y contraseñas

Estas credenciales vienen de fabrica el Usuario Admin y sin contraseña, Lo que puede hacer es entrar y sustituirlo por uno mas seguro o bien ponerle una contraseña mas segura, para realizar esto puede ver el siguiente artículo.

MikroTik - Poner contraseña de Administrador para acceder al equipo

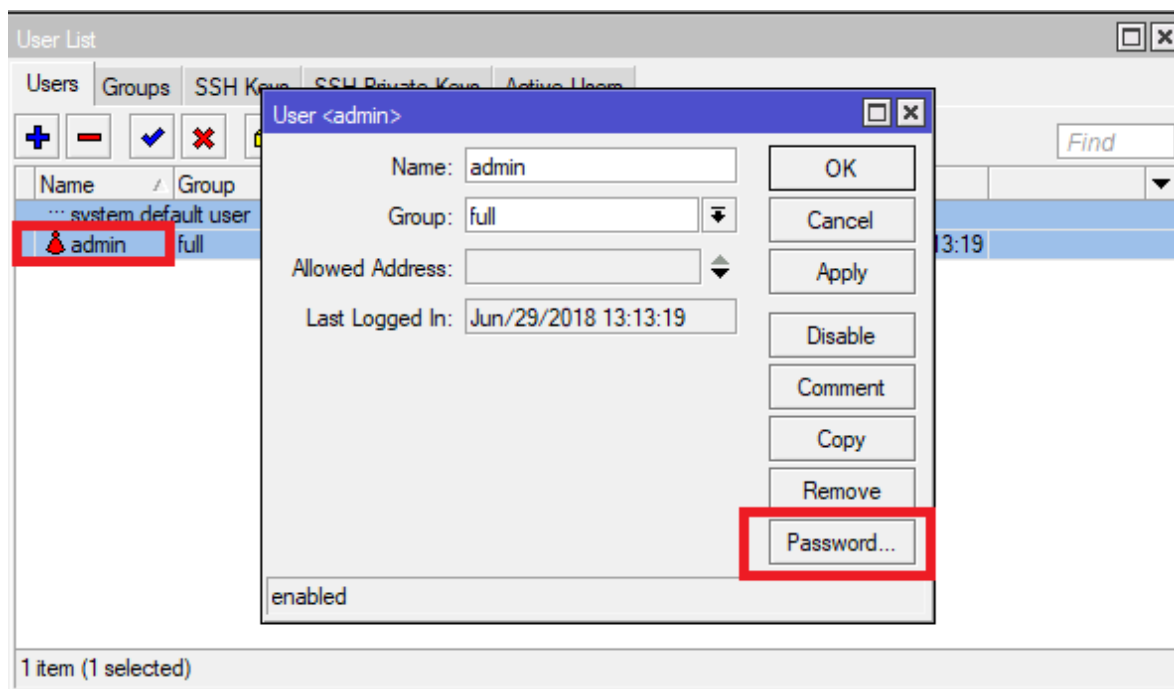
Este artículo se muestra como podemos ponerle una contraseña para la administración del equipo MikroTik de esta manera esta menos vulnerable a ataques, que puedan acceder a el o borrar información etc...

Cuando se abre la herramienta Winbox detecta todos los equipos MikroTik que estén conectados a la red. Cuando detecta todos los equipos, primero seleccionamos el indicado después solo damos en connect para entrar a configurar.

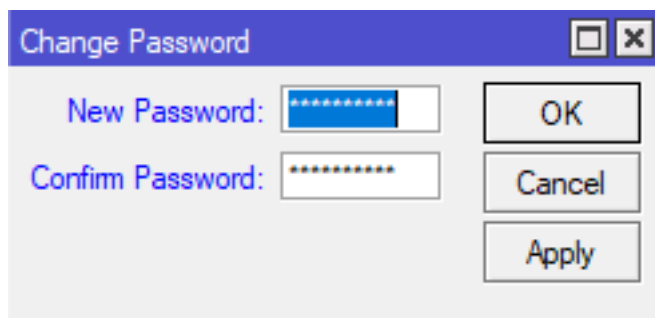
The screenshot shows the Winbox interface. At the top, there is a 'Connect To' dialog with a text field containing '64:D [redacted] E:D4', a 'Login' field with 'admin', and a 'Password' field. Below these fields is an 'Add/Set' button. Below the dialog, there are two tabs: 'Managed' and 'Neighbors'. The 'Managed' tab is active, showing a table of detected devices. The table has columns for 'MAC Address', 'IP Address', 'Identity', 'Version', and 'Board'. The first row shows a device with MAC address '64:D [redacted] E:D4', IP address '192.168.5.1', Identity 'MikroTik', Version '6.41.3 (stable)', and Board 'RB750Gr3'. There is also a 'Refresh' button and a filter icon.

MAC Address	IP Address	Identity	Version	Board
64:D [redacted] E:D4	192.168.5.1	MikroTik	6.41.3 (stable)	RB750Gr3

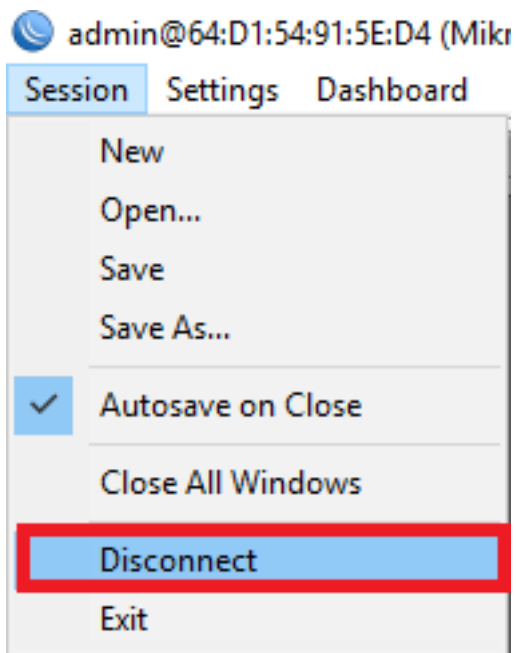
Una vez dentro de la interfaz en opción de System -> Users entramos a esa lista y damos doble click en el usuario admin para editar esté, del lado derecho muestra varios botones selecciona password.



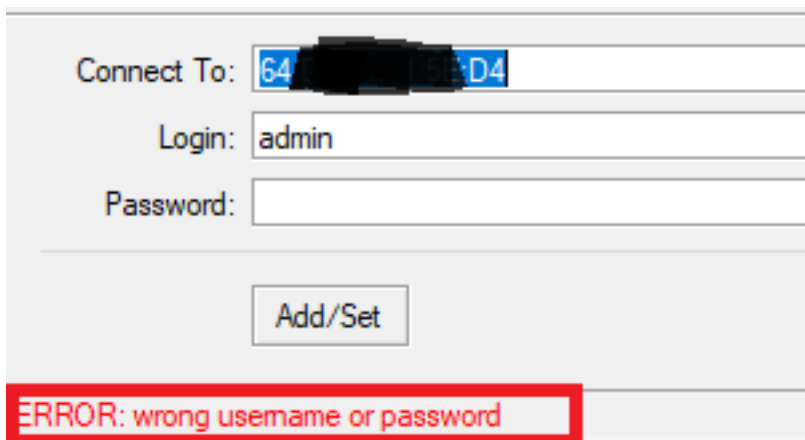
Ahora ponemos las nuevas credenciales.



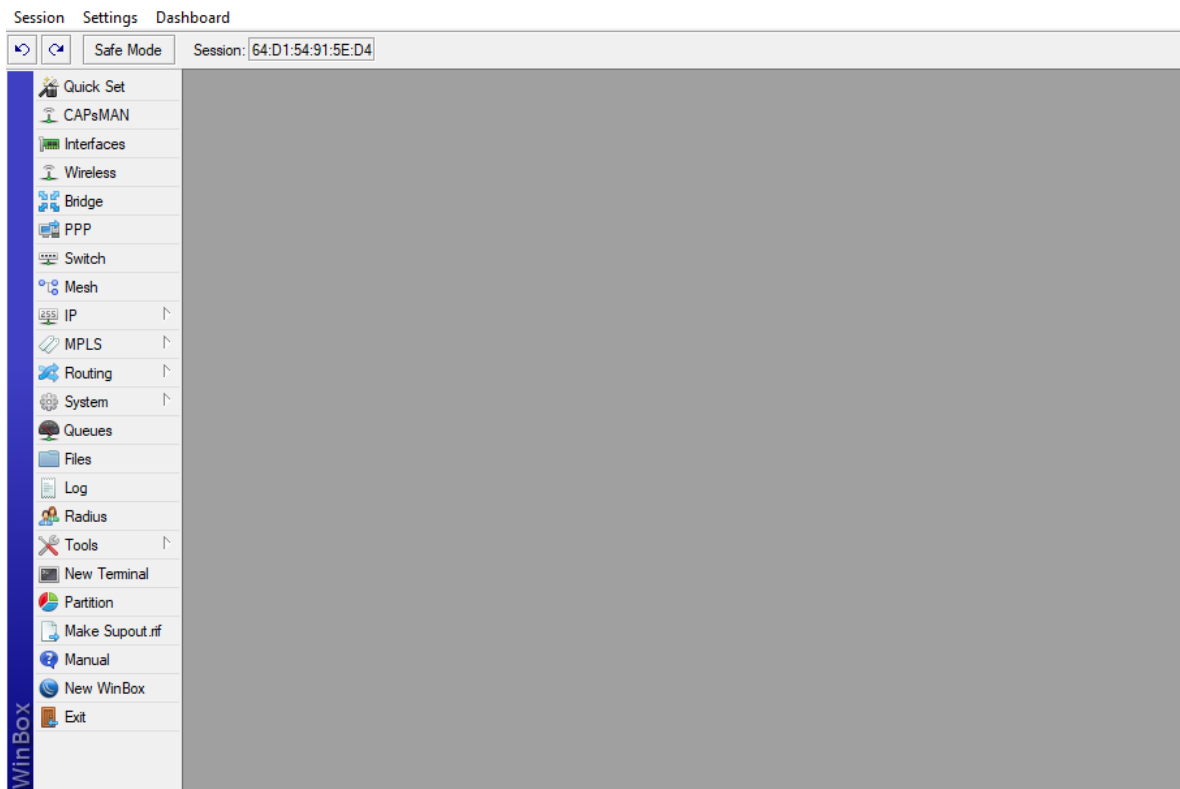
Luego nos desconectamos de la sesión con el equipo.



Intentamos de nuevo conectar y debe mostrar un error (sin poner las credenciales).



Eso fue solo para confirmar que efectivamente nos solicite las credenciales para poder entrar a el equipo. Ahora ingrese las credenciales correctamente y debe permitir entrar a la interfaz.



2. Actualizar el Firmware

Es importante tener actualizado el Firmware ya que estos siempre traen mejoras y si Mikrotik se da cuenta de algún error o debilidad, sacan una nueva versión y puede revisar las mejoras [AQUÍ](https://mikrotik.com/download/changelogs). <https://mikrotik.com/download/changelogs>

Para actualizar puede ver lo siguiente:

MikroTik – Actualizar RouterOS

Nivel: Básico

En este artículo se explicará la forma de actualizar el Sistema Operativo del RouterBoard.

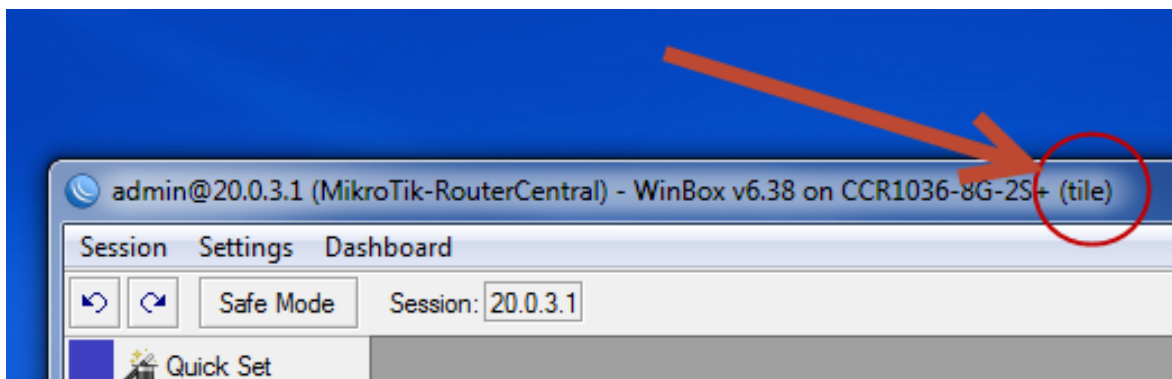
Si por algún motivo elegimos el archivo de alguna arquitectura diferente, no pasará nada ya que el Router identificará que el archivo no está diseñado para su arquitectura.

1. Identificando la arquitectura del Router

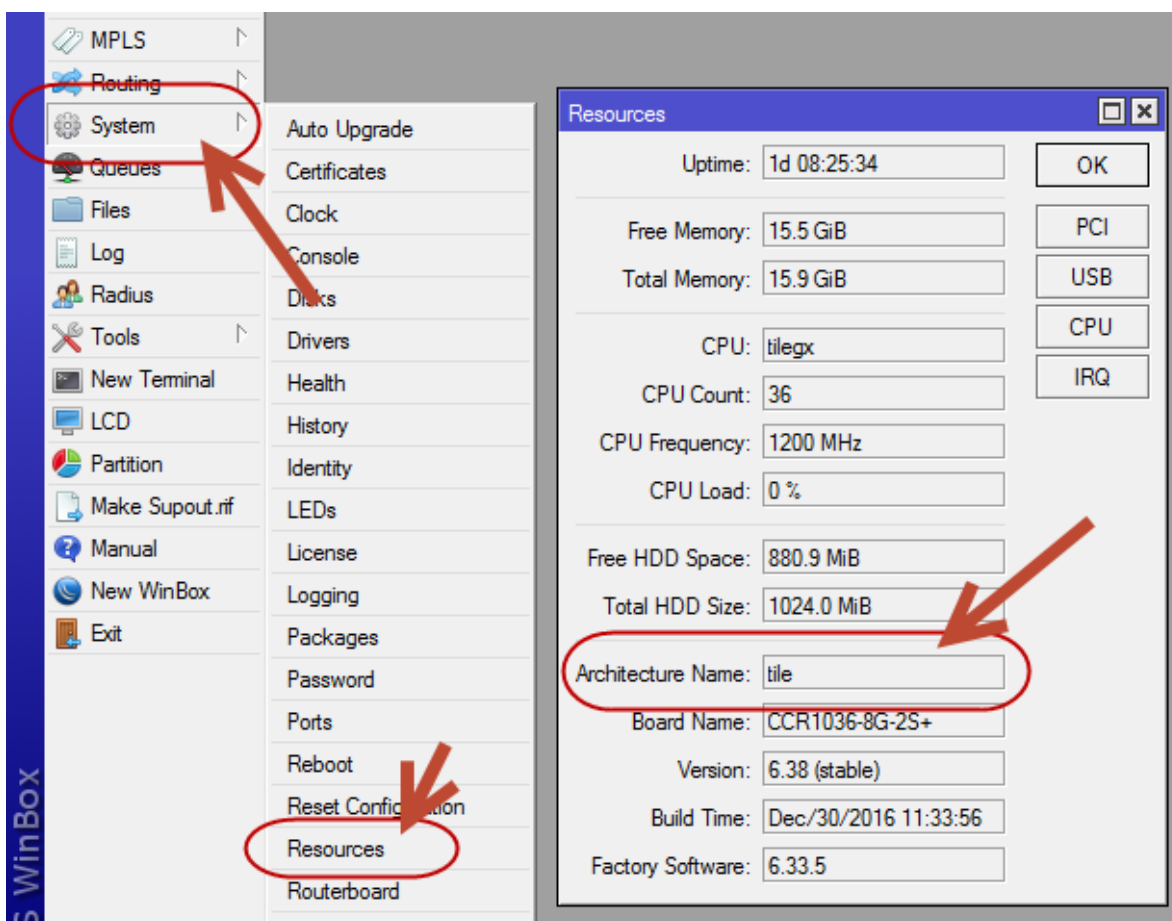
Lo primero que tenemos que hacer para poder actualizar es identificar la arquitectura de nuestro router, para conocer qué versión de archivo es que tenemos que descargar.

Existen varias formas de identificar la arquitectura de nuestro router:

a. En el encabezado de nuestra aplicación “Winbox” se muestra al final la arquitectura que tiene el equipo al que estamos conectados como se ve en la imagen



2. Otra forma de ver la información de la arquitectura es en el Menú Principal en **System > Resources**, como se ve en la imagen



3. Si estamos conectados por Consola o Terminal se escribe el siguiente comando:

```
/system resources print
```

Como se ve en la imagen

```
MMM      MMM      KKK
MMMM     MMMM     KKK
MMM MMMM MMM III KKK KKK RRRRRR  OOOOOO  TTT TTT III KKK KKK
MMM MM  MMM III KKKKK RRR RRR  OOO  OOO  TTT TTT III KKKKK
MMM      MMM III KKK KKK RRRRRR  OOO  OOO  TTT TTT III KKK KKK
MMM      MMM III KKK KKK RRR RRR  OOOOOO  TTT TTT III KKK KKK

MikroTik RouterOS 6.38 (c) 1999-2016      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
[admin@MikroTik-RouterCentral] > system resource print
              uptime: 1d8h27m7s
              version: 6.38 (stable)
              build-time: Dec/30/2016 11:33:56
factory-software: 6.33.5
free-memory: 15.5GiB
total-memory: 15.9GiB
cpu: tilegx
cpu-count: 36
cpu-frequency: 1200MHz
cpu-load: 0%
free-hdd-space: 880.9MiB
total-hdd-space: 1024.0MiB
architecture-name: tile
board-name: CCR1036-8G-2S+
platform: MikroTik
[admin@MikroTik-RouterCentral] > 
```

2. Descargar el Main Package

Ya que se identifico la arquitectura se accede a la pagina donde MikroTik tiene publicadas las actualizaciones del RouterOS, en: www.mikrotik.com/download













































En la columna se encuentra la versión Current que viene siendo la versión completa y la ultima liberada, se busca la arquitectura que corresponde al router en cuestión y se descarga el archivo Main Package


[Home](#)
[Buy](#)
[About](#)
[Jobs](#)
[Hardware](#)
[Software](#)
[Support](#)
[Training](#)
[Account](#)

Software

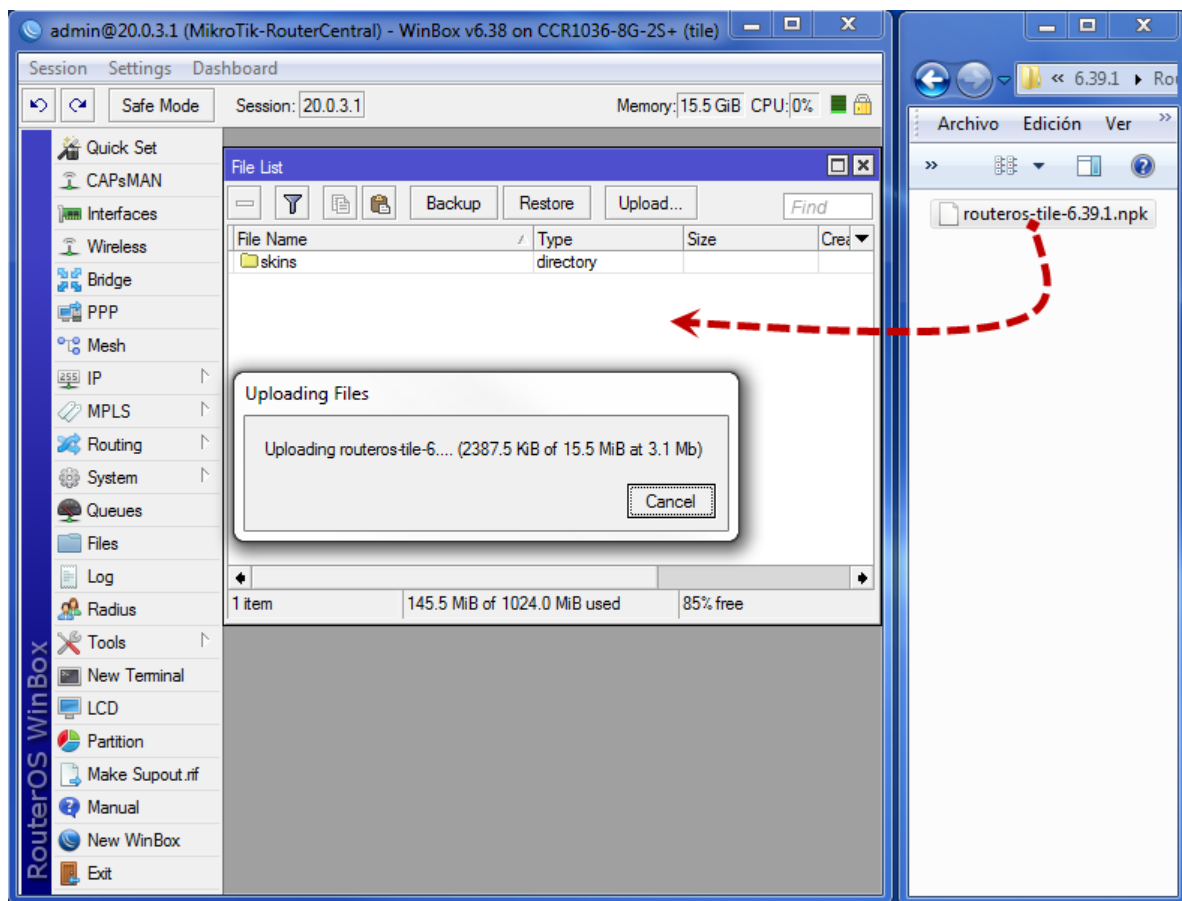
[Downloads](#)
[Changelogs](#)
[Download archive](#)
[RouterOS](#)
[The Dude](#)

RouterOS

	6.37.5 (Bugfix only)	6.39.1 (Current)	5.26 (Legacy)	6.40rc8 (Release candidate)
MIPSBE	CRB, DISC, LDF, LHG, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mANTBox, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package				
Extra packages				
SMIPS	hAP lite			
Main package			-	
Extra packages			-	
TILE	CCR			
Main package			-	
Extra packages			-	
The Dude server			-	
PPC	RB3xx, RB600, RB8xx, RB1100AHx2			
Main package				
Extra packages				
ARM	RB3011, RB1100AHx4			
Main package			-	
Extra packages			-	
The Dude server			-	
X86	RB230, X86			
Main package				

3. Cargar la actualización al Router

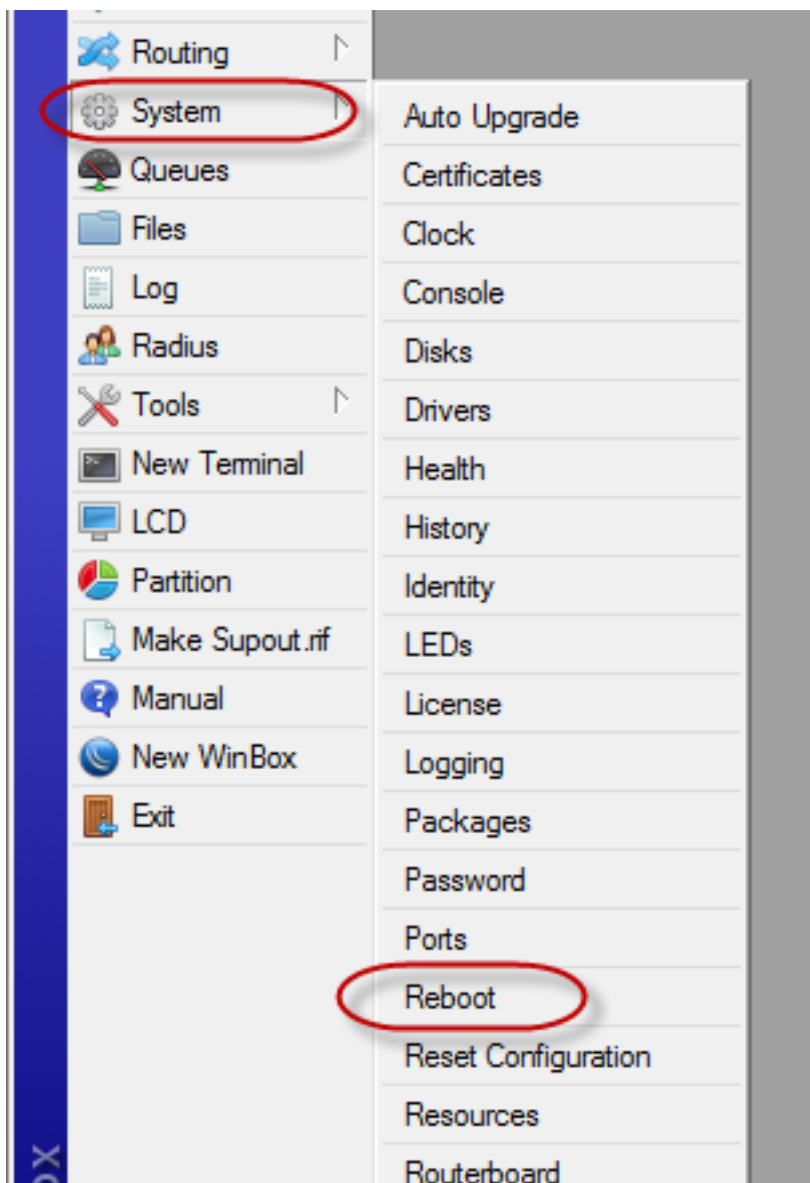
Una vez que descargamos el package y lo tenemos en una carpeta de nuestra computadora lo que tenemos que hacer es entrar al router por winbox y copiar el archivo al winbox, automáticamente despliega la ventana “File List” como se ve en la imagen



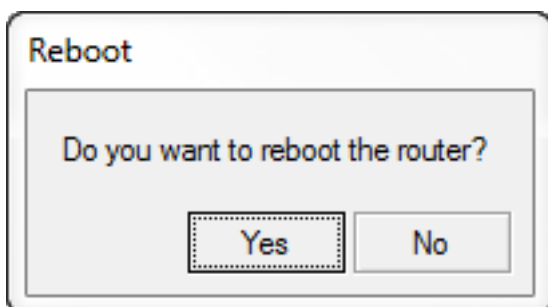
4. Aplicar la actualización

Por ultimo lo único que requerimos es reiniciar nuestro router.

Para ello hay que ir a **System > Reboot** como se ve en la imagen



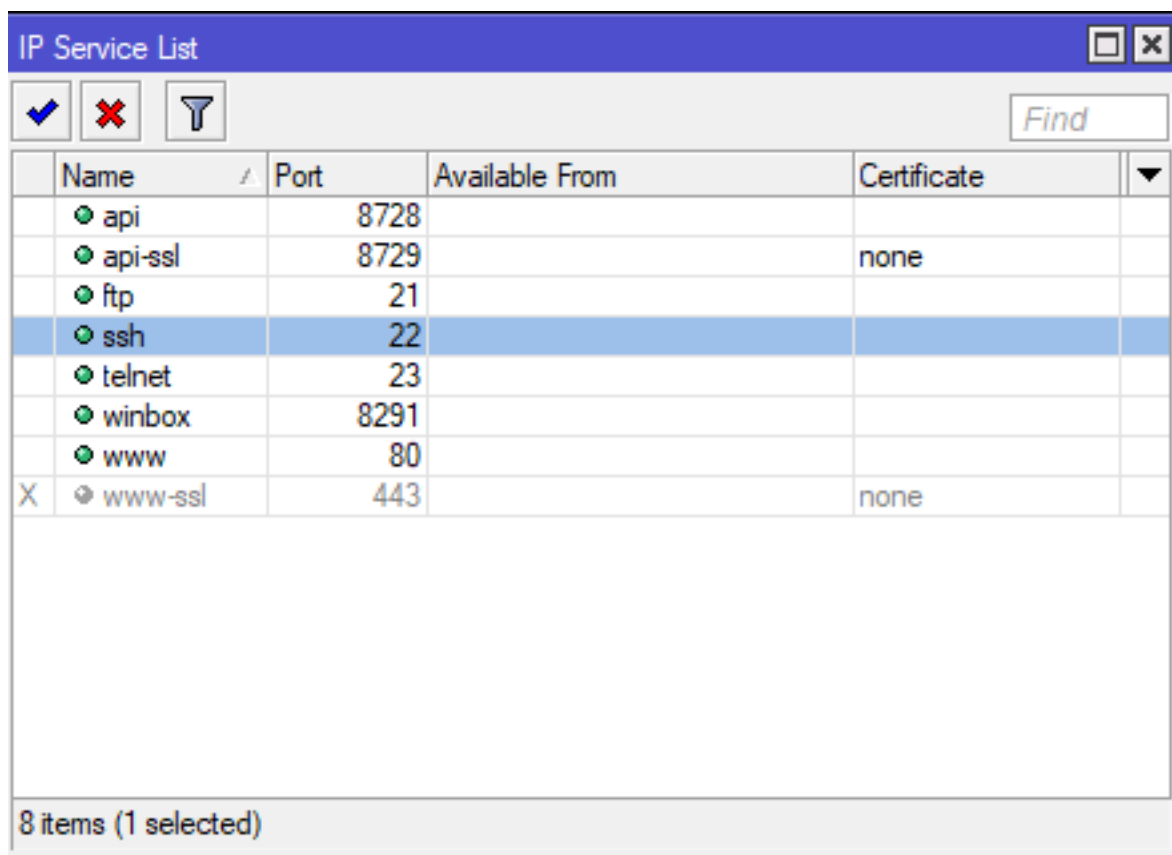
Ya por ultimo el sistema nos pedirá la confirmación de reiniciar como se se ve en la imagen:



3. Puertos de Acceso

Como con cualquier dispositivo conectado a Internet, la ejecución de los servicios en sus puertos por defecto es una invitación a ser hackeado. La primera, y más segura opción es desactivar cualquier servicio que no se va a utilizar. ¿Utiliza FTP para subir o descargar archivos a su RouterBOARD? Si no, entonces apagarlo. Lo mismo va para telnet, ssh y la API Winbox.

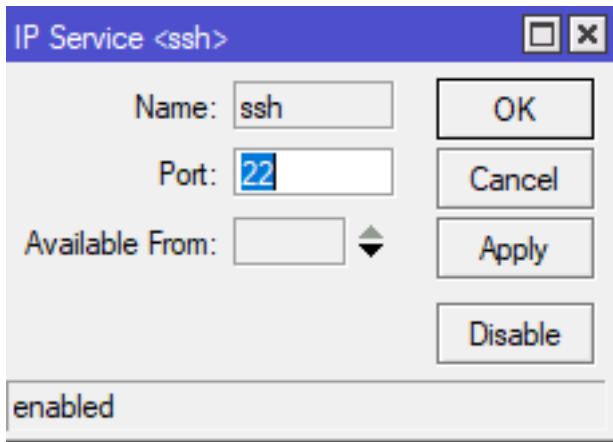
Para deshabilitar estos puertos o bien modificarlos entra en IP -> Services entonces abre la ventana que la siguiente imagen muestra y ahí puede deshabilitarlos.



	Name	Port	Available From	Certificate	
	api	8728			
	api-ssl	8729		none	
	ftp	21			
	ssh	22			
	telnet	23			
	winbox	8291			
	www	80			
X	www-ssl	443		none	

8 items (1 selected)

para cambiar el puerto simplemente da doble click, lo modifica, aplica y presiona OK.



4. Reglas de Firewall

Estas reglas son vitales ya que con esto se tiene un mejor control de lo que entra o sale de nuestra Red y para apoyarse puede seguir el siguiente artículo.

- Artículo: “[MikroTik – Configuración Firewall Básico](#)”.(ya lo hizo en practica anterior, no hacer)

5. Utilizar VPN

Es difícil Saber quien se encuentra husmeando en la red. así que tratamos de cifrar a conexión que exista con estos equipos y para realizar alguna configuración VPN puede ver los siguientes artículos.

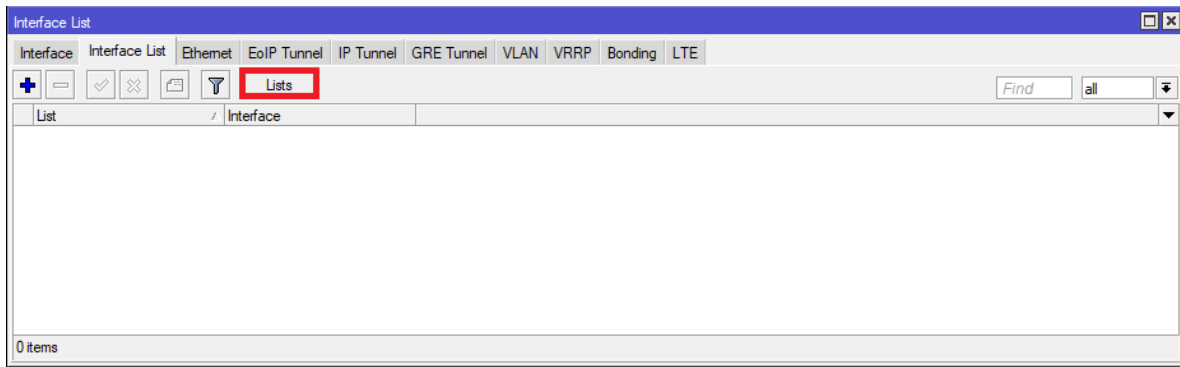
- Artículo: “[MikroTik – Configuración de VPN con Tunnel PPTP](#)”. No realizar
- Artículo: “[MikroTik - Configuración de VPN con Tunnel IPSEC](#)”. No realizar
- Artículo: “[MikroTik - Configuración de VPN con Tunnel L2TP-IPsec](#)”. No realizar

6. Desactivar la Función Neighbor discovery

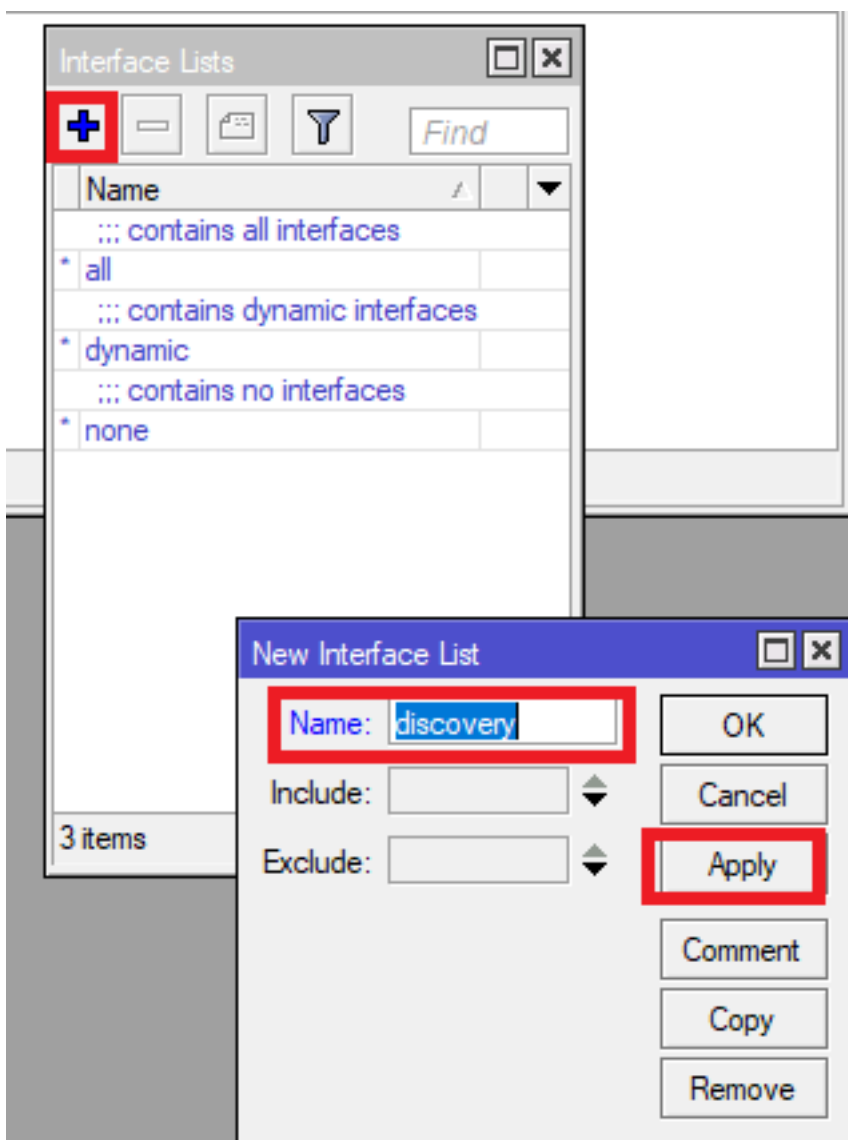
Esta función se puede utilizar para cuando usted no quiere que su equipo MikroTik sea visualizado en la Red o bien para seleccionar por que interface desea que se conecte el equipo vía winbox.

Lo primero que se debe hacer es crear una lista para permitir el discovery por ejemplo y solo permitiremos la conexión por una sola interface del equipo MikroTik.

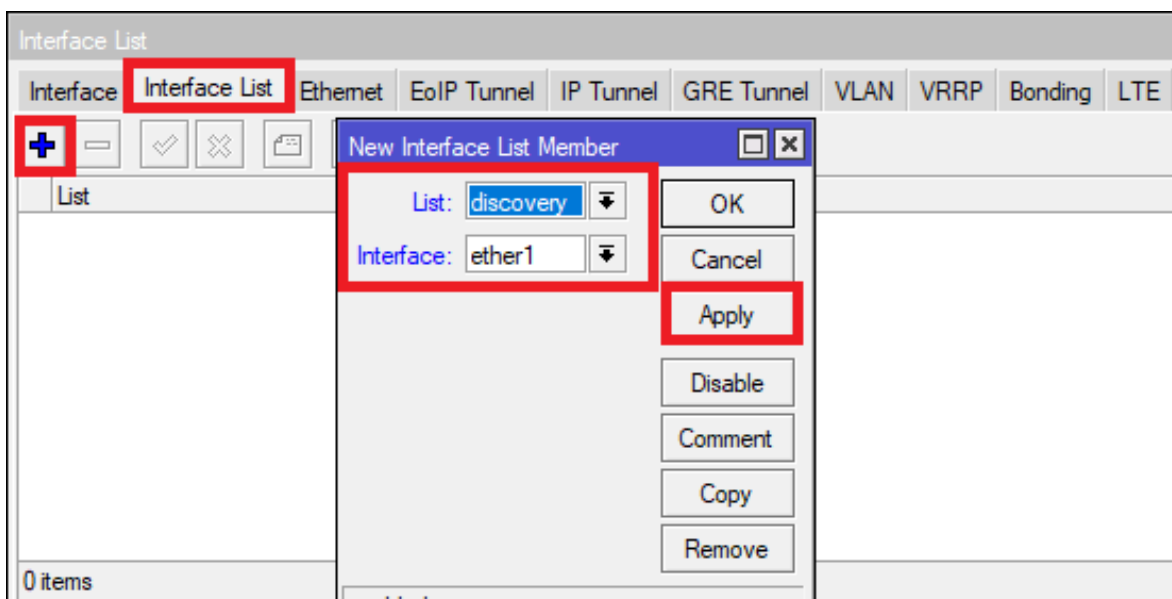
En el menú principal esta **Interfaces** luego en el botón **List**



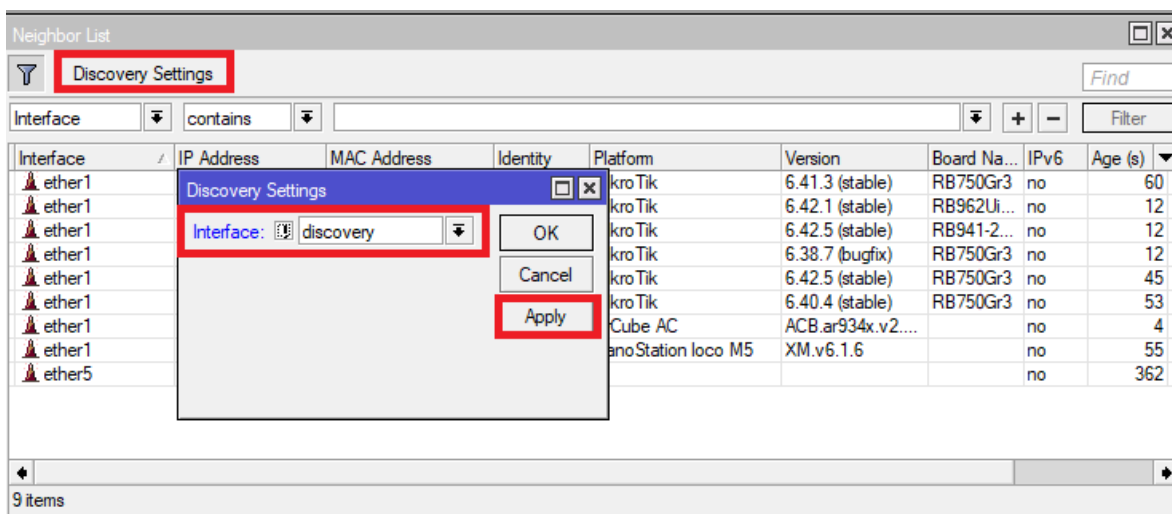
Una vez dentro muestra las siguientes ventanas y agregamos una lista nueva que en este ejemplo fue de nombre "discovery".



Ahora que ya esta creada la Lista vamos a la segunda pestaña que dice **Interface List** agregamos una nueva y luego se selecciona la Lista que fue creada anteriormente y seleccionamos por que Interface pueda ser visualizado nuestro equipo.





Después que ya esta creado lo anterior, ahora vamos a **IP -> Neighbor List -> Discovery Settings** y dentro de este menú seleccionamos la lista de nombre "discovery".



o bien podemos seleccionar "none" para que no pueda ser escaneado y solo se acceda a el sabiendo los datos de este equipo. Si por alguna razón se pierden estos datos obligatoria mente tendrá que regresar a valores de fabrica.

Discovery Settings □ ✕

Interface:  none 

OK

Cancel

Apply