

MODULO 5

Configuraciones inalámbricas Wi-Fi en MikroTik

1. Configuración Wireless.

Antes de empezar a configurar una red inalámbrica Wifi en los Router MikroTik hay que tener en cuenta si el modelo cuenta con esa característica de forma física y real ya que dentro del sistema RouterOS si vamos a contar con la opción Wireless, aunque el router no cuente con la característica física.

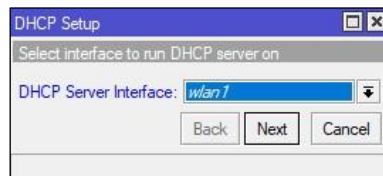
1.1. Creación de la subred destinada al Wireless.

En IP -> Addresses creamos una nueva subred para las conexiones inalámbricas indicando la dirección en formato CIDR e indicando la interface donde la vamos a crear.



1.2. Habilitar el servidor DHCP para la interface inalámbrica

En IP -> DHCP-Server, hacemos clic en el botón DHCP-Setup para configurar en servidor dhcp en la interface WLAN1. estableciendo todos los parámetros como ya lo habíamos visto anteriormente.



1.3. Creación del perfil de seguridad

El perfil de seguridad será el punto de seguridad donde configuramos el tipo de encriptación y el password de la red inalámbrica.

En Wireless, dentro de la pestaña SecurityProfile vamos a crear un nuevo perfil de seguridad muy aparte del perfil por defecto que ya tiene MikroTik de la siguiente forma.

Name	: Nombre del perfil de seguridad
Mode	: Dynamic keys
Authentication Types	: WPA2-PSK (es el protocolo de encriptación más robusto)
Unicast Ciphers	: aes ccm (usado por el nuevo protocolo wpa2)
	tkip (método de cifrado antiguo usado por wpa)
Group Ciphers	: aes ccm
WPA2 Pre-Shared Key	: Password de seguridad de la red wifi

1.4. Creación del perfil inalámbrico.

El perfil inalámbrico es la configuración donde se establecerá el nombre del perfil, el nombre SSID de la red inalámbrica y la selección del perfil de seguridad.

En Wireless, dentro de la pestaña Wifi-Interfaces vamos crear un nuevo perfil inalámbrico o podemos modificar el perfil que viene por defecto.

GENERAL

WIRELESS

MODULO 6

Copias de seguridad y restauración

1. Configuración de copias de seguridad.

1.1. Tipos de Backup

1.1.1. Binarios.

Son seguros y no son legibles ni editables además de que crea Backup en general

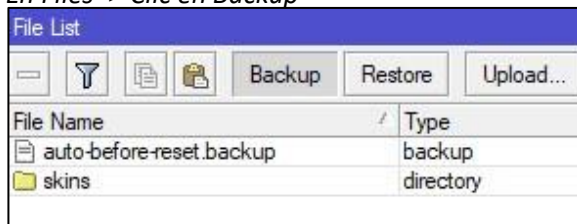
1.1.2. Export.

Son inseguros, son legibles y editables además se puede elegir que partes hacer backup.

1.2. Creación de un Backup binario (GUI)

Crear un backup binario

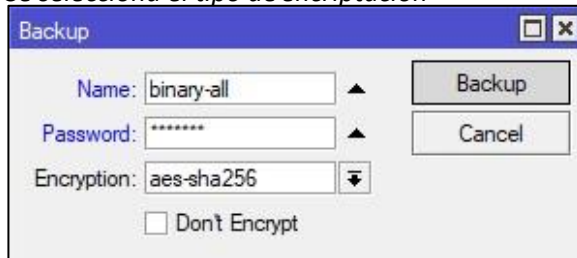
En Files -> Clic en Backup



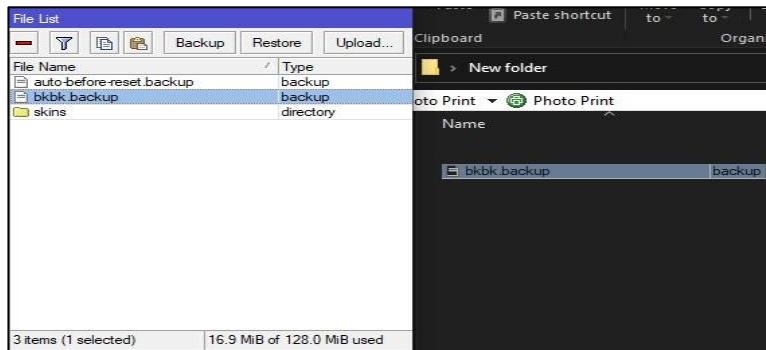
Se pone el nombre

Se configura el password

Se selecciona el tipo de encriptación



Hacemos un Drag and Drop (Arrastrar y soltar) a una ubicación local y segura, para no llenar la memoria del MikroTik.



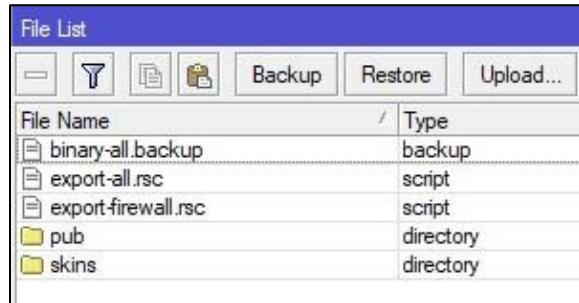
1.3. Creación de un export (CLI)

Para exportar todas las configuraciones a partir de la raíz

```
[admin@mikrotik] > export file=export-all
```

Para exportar configuraciones en específico a partir de la ubicación

```
[admin@mikrotik] > /ip firewall [admin@mikrotik] /ip firewall> export  
file=export-firewall
```

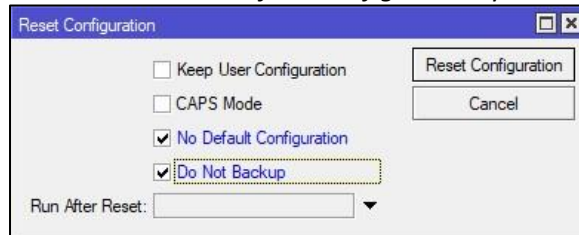


File Name	Type
binary-all.backup	backup
export-all.rsc	script
export-firewall.rsc	script
pub	directory
skins	directory

1.4. Resetear el router a valores de fábrica.

En System -> Reset Configuration

Seleccionamos *no default configuration* y *do not backup* luego clic en *reset configuration*



1.5. Probar ambos métodos de restaurado.

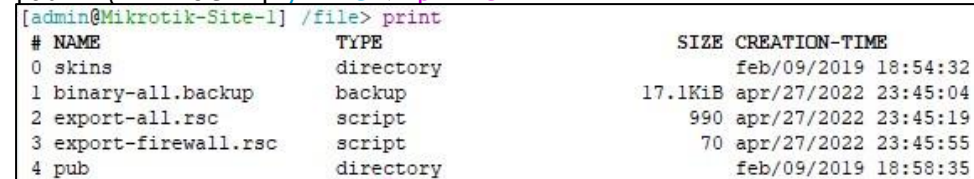
1.5.1. Restaurar Backup binario (CLI) Ingresar

a una terminal -> ingresar a file

```
[admin@mikrotik] >  
[admin@mikrotik] > /file  
[admin@mikrotik] /file >
```

Verificamos que nuestro backup está en file

```
[admin@mikrotik] /file > print
```



#	NAME	TYPE	SIZE	CREATION-TIME
0	skins	directory		feb/09/2019 18:54:32
1	binary-all.backup	backup	17.1KiB	apr/27/2022 23:45:04
2	export-all.rsc	script	990	apr/27/2022 23:45:19
3	export-firewall.rsc	script	70	apr/27/2022 23:45:55
4	pub	directory		feb/09/2019 18:58:35

Volvemos a raíz

```
[admin@mikrotik] /file > /
```

Ingresamos a system backup

```
[admin@mikrotik] > / system backup  
[admin@mikrotik] /system backup >
```

Dentro de system backup digitamos el siguiente comando **(si el backup NO tiene password)**

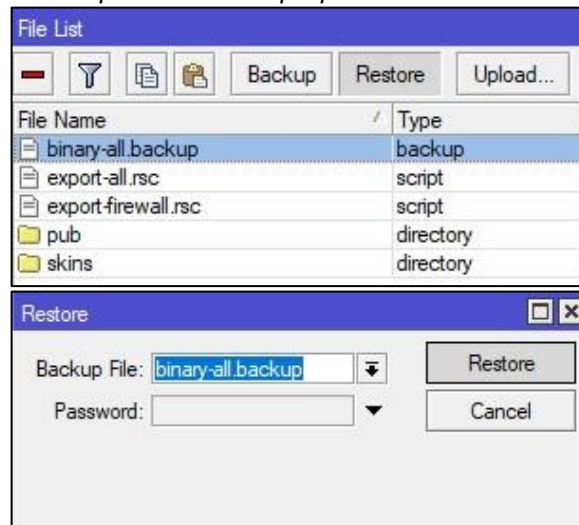
```
[admin@mikrotik] /system backup > load name=binary-all.backup
```

Dentro de system backup digitamos el siguiente comando **(si el backup tiene password)**

```
[admin@mikrotik] /system backup > load name=binary-all.backup  
password=1234567
```

1.5.2. Restaurar Backup binario (GUI)

En Files -> seleccionamos el backup que queremos restaurar y damos clic en Restore, si tuviera password se lo proporcionamos



1.5.3. Restaurar un export (CLI)

Ingresar a una terminal -> nos posicionamos en la raíz

```
[admin@mikrotik] >
```

Digitamos el comando import y con doble TAB podemos ver las opciones export que deseamos restaurar

```
[admin@mikrotik] > import  
[admin@Mikrotik-Site-1] > import  
export-all.rsc export-firewall.rsc
```

A diferencia de un backup binario, un export no requiere que el router se reinicie además podemos ver el proceso de recuperación con simples comandos

[admin@mikrotik] > **import** export-all.rsc **verbose=yes**

```
[admin@MikroTik] > import export-all.rsc verbose=yes
#line 1
! apr/27/2022 23:45:19 by RouterOS 6.43.8
#line 2
! software id =
#line 3
!
#line 4
!
#line 5
!
#line 6
/interface ethernet
#line 7
set [ find default-name=ether1 ] disable-running-check=no
#line 8
set [ find default-name=ether2 ] disable-running-check=no
#line 9
set [ find default-name=ether3 ] disable-running-check=no
#line 10
set [ find default-name=ether4 ] disable-running-check=no
#line 11
set [ find default-name=ether5 ] disable-running-check=no
#line 12
set [ find default-name=ether6 ] disable-running-check=no
#line 13
set [ find default-name=ether7 ] disable-running-check=no
#line 14
set [ find default-name=ether8 ] disable-running-check=no
#line 15
/interface wireless security-profiles
#line 16
set [ find default=yes ] supplicant-identity=MikroTik
#line 17
/ip address
#line 18
add address=10.0.1.254/24 interface=ether4 network=10.0.1.0
#line 19
add address=10.200.1.1/30 interface=ether2 network=10.200.1.0
#line 20
add address=10.200.2.1/30 interface=ether3 network=10.200.2.0
#line 21
/ip dhcp-client
#line 22
add disabled=no interface=ether1
failure: dhcp-client on that interface already exists
```

Pero, vemos que nos acaba de mostrar un error y que no se ha podido realizar el restaurado, debido que existe una configuración DHCP

Para solucionar ese error vamos a borrar la configuración DHCP existente

[admin@mikrotik] > /ip dhcp-client

[admin@mikrotik] /ip dhcp-client > print

```
[admin@MikroTik] /ip dhcp-client> print
Flags: X - disabled, I - invalid, D - dynamic
#  INTERFACE  USE-PEER-DNS  ADD-DEFAULT-ROUTES
0  ether1      yes           yes
```

Eliminamos la configuración DHCP

[admin@mikrotik] /ip dhcp-client > remove numbers=0

Volvemos a intentar el restaurado

[admin@mikrotik] > **import** export-all.rsc **verbose=yes**

```
[admin@mikrotik] > import export-all.rsc verbose=yes
#line 1
# apr/27/2022 23:45:19 by RouterOS 6.43.8
#line 2
# software id =
#line 3
#
#line 4
#
#line 5
#
#line 6
/interface ethernet
#line 7
set [ find default-name=ether1 ] disable-running-check=no
#line 8
set [ find default-name=ether2 ] disable-running-check=no
#line 9
set [ find default-name=ether3 ] disable-running-check=no
#line 10
set [ find default-name=ether4 ] disable-running-check=no
#line 11
set [ find default-name=ether5 ] disable-running-check=no
#line 12
set [ find default-name=ether6 ] disable-running-check=no
#line 13
set [ find default-name=ether7 ] disable-running-check=no
#line 14
set [ find default-name=ether8 ] disable-running-check=no
#line 15
/interface wireless security-profiles
#line 16
set [ find default=yes ] supplicant-identity=MikroTik
#line 17
/ip address
#line 18
add address=10.0.1.254/24 interface=ether4 network=10.0.1.0
#line 19
add address=10.200.1.1/30 interface=ether2 network=10.200.1.0
#line 20
add address=10.200.2.1/30 interface=ether3 network=10.200.2.0
#line 21
/ip dhcp-client
#line 22
add disabled=no interface=ether1
#line 23
/ip service
#line 24
set www-ssl disabled=no
#line 25
/system identity
#line 26
set name=Mikrotik-Site-1
```

Finalizo el restaurado
correctamente

NOTA: si en algún momento quisiéramos restaurar configuraciones de un MikroTik con 24 puertos ethernet a un MikroTik con 5 puertos ethernet, por el método binario jamás funcionaría. debido a que en el MikroTik grande tenemos muchas bocas de canal ethernet y en el MikroTik pequeño no, para poder realizar esa acción es completamente necesario hacer el restaurado por el método import ya que un archivo export es editable y podemos modificar las bocas de canales ethernet a nuestro gusto, es un trabajo que requiere mucha atención.

1.5.4. Restaurar un export (GUI) No se puede realizar, es imposible.

MODULO 7

DNS

2. Configuraciones DNS

2.1. Configurar DNS estática

En IP -> DNS, Podemos ver las configuraciones de DNS, ahí dentro tendremos la posibilidad de agregar direcciones DNS a gusto y solo podremos ver las direcciones DNS dinámicas las cuales usa desde la configuración de DHCP Client

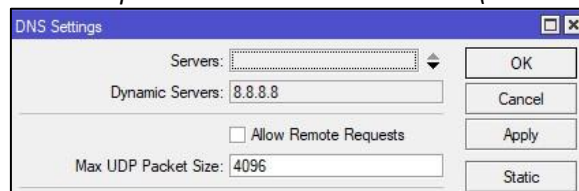
2.2. Aceptar o rechazar peticiones DNS desde LAN

En IP -> DNS, podemos aceptar o rechazar la resolución de peticiones DNS a PC's que estén dentro de la LAN en cada mikrotik.

Primero debemos obligar a la PC conectada al mikrotik que se resuelvan los nombres de dominio a través del Gateway del mikrotik de la siguiente forma:

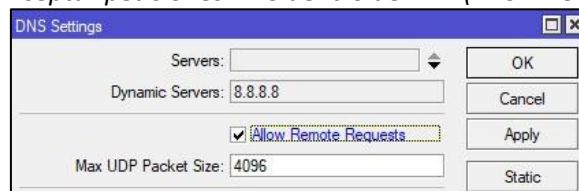
```
PC-1> ip dns 10.0.1.254
```

Rechazar peticiones DNS dentro de LAN (Allow Remote Request - DESHABILITADO)



```
PC-1> ping google.com
Cannot resolve google.com
```

Aceptar peticiones DNS dentro de LAN (Allow Remote Request - HABILITADO)



```
PC-1> ping google.com
google.com resolved to 142.250.0.102

84 bytes from 142.250.0.102 icmp_seq=1 ttl=56 time=58.120 ms
84 bytes from 142.250.0.102 icmp_seq=2 ttl=56 time=58.433 ms
84 bytes from 142.250.0.102 icmp_seq=3 ttl=56 time=60.983 ms
```

2.3. Almacenar o guardar resoluciones DNS estáticas

En IP -> DNS Setting -> Static, Podemos agregar de forma manual resoluciones DNS de forma permanente



New DNS Static Entry

Name:

Regexp:

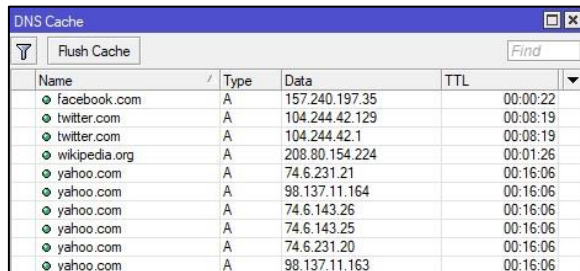
Address:

TTL: s

OK Cancel Apply Disable

2.4. Limpiar cache

Mikrotik guarda todas las resoluciones DNS en memoria para no tener que resolverlas nuevamente



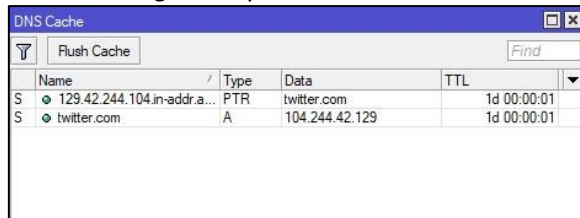
DNS Cache

Flush Cache Find

Name	Type	Data	TTL
facebook.com	A	157.240.197.35	00:00:22
twitter.com	A	104.244.42.129	00:08:19
twitter.com	A	104.244.42.1	00:08:19
wikipedia.org	A	208.80.154.224	00:01:26
yahoo.com	A	74.6.231.21	00:16:06
yahoo.com	A	98.137.11.164	00:16:06
yahoo.com	A	74.6.143.26	00:16:06
yahoo.com	A	74.6.143.25	00:16:06
yahoo.com	A	74.6.231.20	00:16:06
yahoo.com	A	98.137.11.163	00:16:06

imagínense una empresa de muchos empleados que visitan varias páginas... la memoria cache se llenaría bastante, para limpiar la memoria simplemente debemos ingresar a IP -> DNS Settings -> Cache, dar clic en flush Cache.

Los únicos registros que no se borrarán serán las que agregamos de forma manual



DNS Cache

Flush Cache Find

Name	Type	Data	TTL
S 129.42.244.104.in-addr.a...	PTR	twitter.com	1d 00:00:01
S twitter.com	A	104.244.42.129	1d 00:00:01

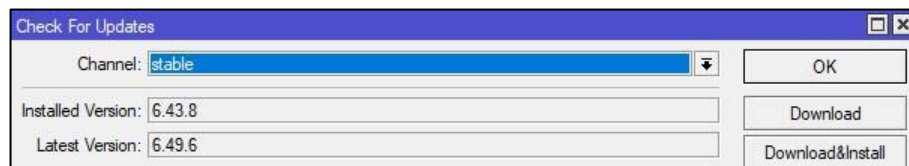
MODULO 8

MikroTik Update

3. Configuraciones de Update para el MikroTik.
 - 3.1. Actualizar el Firmware de nuestro MikroTik.
 - 3.1.1. METODO 1: mediante WinBox.

En System -> Packages, hacemos clic en Check For Updates para verificar si hay alguna versión mas reciente.

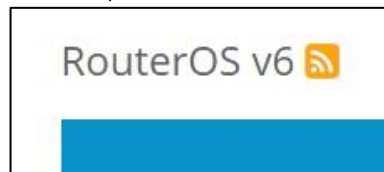
Como observamos en la siguiente imagen, existe una versión mas reciente, para actualizar hacemos clic en Download&Install.













MikroTik se actualizará automáticamente usando la red actual de conexión.

- 3.1.2. METODO 2: Desde la página oficial mikrotik.com.

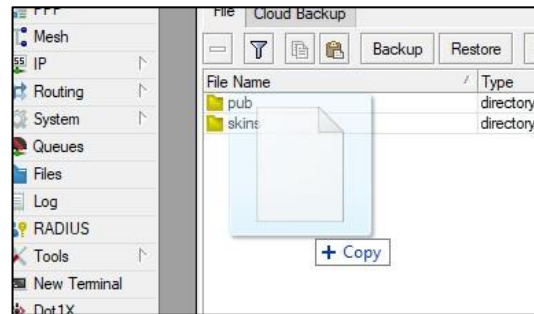
En la página www.mikrotik.com en la sección de Downloads buscamos la versión deseada, en este caso RouterOS V6.



Buscamos la arquitectura x86_64 y descargamos MainPackage de la versión más estable.

X86		
Main package		
Extra packages		
CD Image		
Install image		
The Dude server		

Subimos el archivo descargado a la sección FILES de MikroTik.



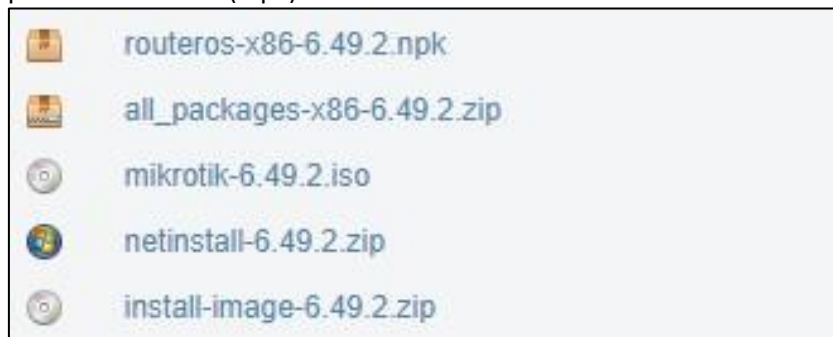
Luego de subir el fichero reiniciamos el sistema para que se efectuó el update.

3.2. Realizar un Down grade a una versión anterior.

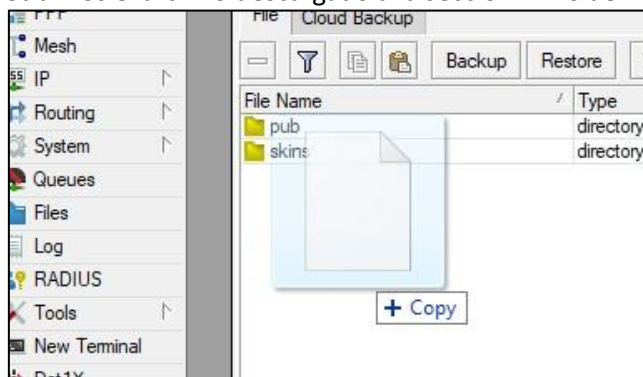
En la pagina www.mikrotik.com en la sección Download archive buscamos la sección Stable Release Tree



Hacemos clic en la versión que deseamos y nos mostrara varias opciones y seleccionamos el primero de la lista (.npk)



Subimos el archivo descargado a la sección FILES de MikroTik.



Luego de subir el fichero reiniciamos el sistema para que se efectuó el downgrade.

3.3. Actualizar el Firmware de nuestro MikroTik por consola.

Para poder actualizar nuestro MikroTik mediante CLI de la consola, verificamos si tenemos nuevas versiones con el siguiente comando.

`/system package update check-for-updates`

```
[admin@Mikrotik-Site-2] > /system package update check-for-updates
channel: stable
installed-version: 6.43.8
latest-version: 6.49.6
status: New version is available
```

Iniciamos la descarga con el siguiente comando:

`/system package update download`

```
[admin@Mikrotik-Site-2] > /system package update download
channel: stable
installed-version: 6.43.8
latest-version: 6.49.6
status: downloading...
-- [Q quit|D dump|C-z pause]
```

```
[admin@Mikrotik-Site-2] > /system package update download
channel: stable
installed-version: 6.43.8
latest-version: 6.49.6
status: Downloaded, please reboot router to upgrade it
```

Luego reiniciamos el router.

```
[admin@Mikrotik-Site-2] > /system reboot
Reboot, yes? [y/N]:
Y
system will reboot shortly
```

Verificamos que el sistema ya no tiene actualizaciones pendientes.

```
[admin@Mikrotik-Site-2] > /system package update check-for-updates
channel: stable
installed-version: 6.49.6
latest-version: 6.49.6
status: System is already up to date
```

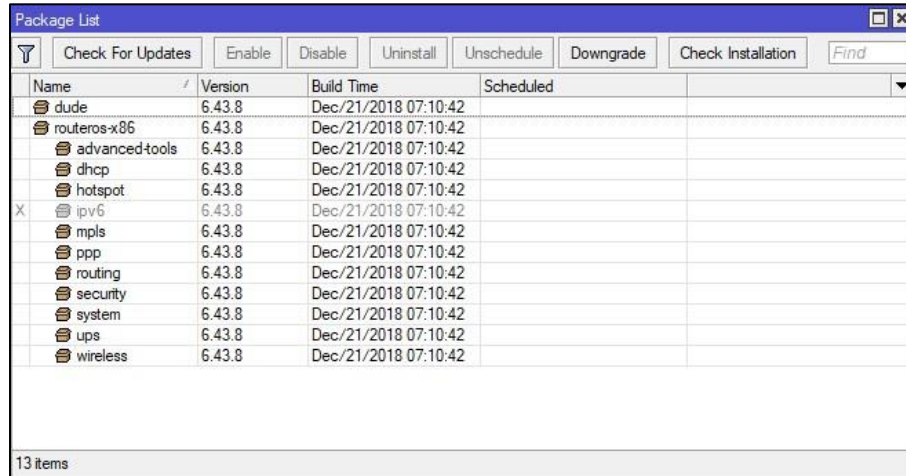
MODULO 9

Paquetes y servicios

4. Configuraciones de ajuste en paquetes y servicios.

4.1. Entendiendo cada paquete que viene por defecto en MikroTik.

En system -> Packages, podemos ver todos los paquetes que vienen por defecto en MikroTik.



Name	Version	Build Time	Scheduled
dude	6.43.8	Dec/21/2018 07:10:42	
routeros-x86	6.43.8	Dec/21/2018 07:10:42	
advanced-tools	6.43.8	Dec/21/2018 07:10:42	
dhcp	6.43.8	Dec/21/2018 07:10:42	
hotspot	6.43.8	Dec/21/2018 07:10:42	
ipv6	6.43.8	Dec/21/2018 07:10:42	
mpls	6.43.8	Dec/21/2018 07:10:42	
ppp	6.43.8	Dec/21/2018 07:10:42	
routing	6.43.8	Dec/21/2018 07:10:42	
security	6.43.8	Dec/21/2018 07:10:42	
system	6.43.8	Dec/21/2018 07:10:42	
ups	6.43.8	Dec/21/2018 07:10:42	
wireless	6.43.8	Dec/21/2018 07:10:42	

13 items

RouterOS-x86, Es el paquete principal es de donde los demás paquetes van a derivar en pocas palabras el kernel del sistema.

Advanced-tools, son herramientas avanzadas que podemos encontrar en la sección de tools (Recomendable NO QUITARLO).

DHCP, Nos permite realizar configuraciones dhcp que podemos encontrar en la sección IP. (recomendable ANALIZAR EL USO DE ESTAS FUNCIONES DE ACUERDO A LA INSTALACION).

Hotspot, Habilita la función hotspot que encontramos en la sección IP->hotspot. (recomendable HABILITAR O DESHABILITAR de acuerdo al USO).

Ipv6, Viene desactivado por defecto (PODEMOS HABILITARLO DE ACUERDO A LA NECESIDAD DE LA RED).

MPLS, nos permite crear redes de tipo mpls. Si lo deshabilitamos no sufriremos ningún cambio.

PPP, Nos permite configurar redes VPN, podemos deshabilitar si es conveniente para la red.

Routing, hace referencia al ruteo dinámico (si deshabilitamos perdemos la opción de hacer ruteo dinámico, pero no perderemos la opción de ruteo estático que es la que más usamos).

Security, tenemos la parte de Login y otras opciones avanzadas (recomendable NO QUITAR)

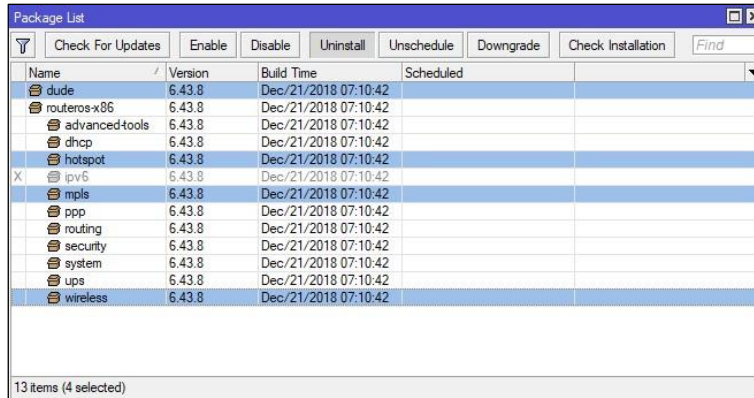
System, Es un paquete integrado en el CORE de RouterOS (NO QUITAR)

UPS, Permite realizar configuraciones UPS (Recomendable QUITARLO o analizar el caso de uso).

Wireless, Nos permite configurar redes inalámbricas (QUITARLO si el dispositivo no tiene una salida Wireless física).

4.2. Desactivar paquetes que no vamos a usar para optimizar recursos.

Para desinstalar paquetes que no nos sirvan, debemos seleccionar un paquete y dar clic en para que se programe su desinstalación en el próximo reinicio del router.



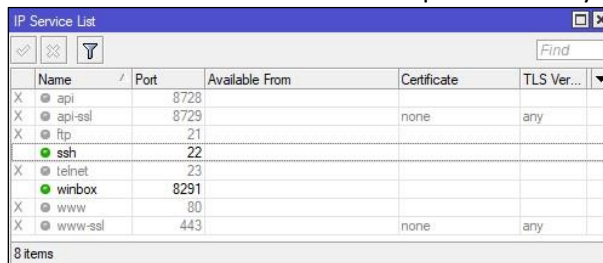
Name	Version	Build Time	Scheduled
dude	6.43.8	Dec/21/2018 07:10:42	
routeros-x86	6.43.8	Dec/21/2018 07:10:42	
advanced-tools	6.43.8	Dec/21/2018 07:10:42	
dhcp	6.43.8	Dec/21/2018 07:10:42	
hotspot	6.43.8	Dec/21/2018 07:10:42	
ipv6	6.43.8	Dec/21/2018 07:10:42	
mpls	6.43.8	Dec/21/2018 07:10:42	
ppp	6.43.8	Dec/21/2018 07:10:42	
routing	6.43.8	Dec/21/2018 07:10:42	
security	6.43.8	Dec/21/2018 07:10:42	
system	6.43.8	Dec/21/2018 07:10:42	
ups	6.43.8	Dec/21/2018 07:10:42	
wireless	6.43.8	Dec/21/2018 07:10:42	

13 items (4 selected)

Luego de marcar Uninstall debemos reiniciar el MikroTik para que surtan efectos.

4.3. Cambiar puertos de servicio para la administración.

En IP -> Services, desactivamos todos los servicios de administración que no vamos a usar para la administración del MikroTik exceptuando SSH y WinBox.



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

8 items

por seguridad podemos cambiar el puerto de acceso a puertos poco conocidos y no seas los por defecto.



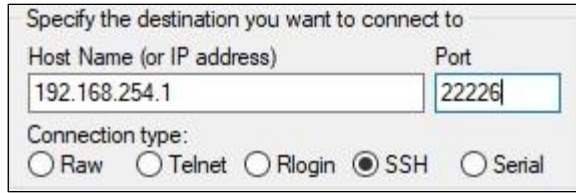
Name	Port	Available From	Certificate	TLS Ver...
api	8728			
api-ssl	8729		none	any
ftp	21			
ssh	22226			
telnet	23			
winbox	8998			
www	80			
www-ssl	443		none	any

8 items (2 selected)

Para ingresar por WinBox con el nuevo puerto de administración, debemos hacerlo de la siguiente forma ya que WinBox viene con la configuración de puertos por defecto, con dirección MAC seguiremos ingresando normal.

Connect To:	192.168.254.1:8998
Login:	admin
Password:	

Acceso de administración CLI con Putty.



Specify the destination you want to connect to

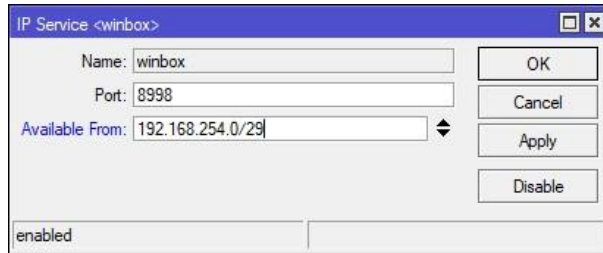
Host Name (or IP address) Port

192.168.254.1 22226

Connection type:

☐ Raw ☐ Telnet ☐ Rlogin ☒ SSH ☐ Serial

Para incrementar la seguridad podemos establecer una dirección única o una subred completa para la administración.



IP Service <winbox>

Name: winbox

Port: 8998

Available From: 192.168.254.0/29

enabled

OK Cancel Apply Disable

Con este método estamos restringiendo el acceso a la administración para que solo las direcciones dentro de esa red puedan tener acceso al MikroTik, el ingreso por dirección MAC seguirá siendo normal.

MODULO 10

Grupos y usuarios

5. Administración de grupos y usuarios.
- 5.1. Creación y administración de grupos.

En System -> Users, en la pestaña Groups podemos administrar los grupos con diferentes roles y accesos.

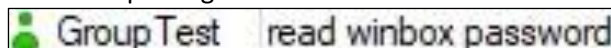
User List		
Users Groups SSH Keys SSH Private Keys Active Users		
Name	Policies	Skin
S full	local telnet ssh ftp reboot read write polic...	default
S read	local telnet ssh reboot read test winbox p...	default
S write	local telnet ssh reboot read write test win...	default

Los grupos Full, Read y Write son grupos predeterminados de MikroTik.

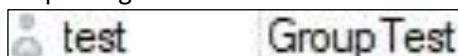
Podríamos crear un nuevo grupo de administración teniendo en cuenta las siguientes políticas:

<i>local</i>	<i>= nos permite iniciar sesión localmente por consola</i>
<i>ssh</i>	<i>= permite conexión ssh</i>
<i>reboot</i>	<i>= permite reinicia el router</i>
<i>write</i>	<i>= permite escribir configuraciones en el router</i>
<i>test</i>	<i>= Permite realizar diferentes testeos dentro de Mikrotik</i>
<i>password</i>	<i>= permite cambiar su propio password</i>
<i>sniff</i>	<i>= capturar tráfico de la red para luego ser analizado por WireShark</i>
<i>api</i>	<i>= conexión al router mediante api o app de móvil</i>
<i>dude</i>	<i>= permite al usuario conectarse al servidor dude si lo tuviéramos</i>
<i>telnet</i>	<i>= permite conexión por telnet</i>
<i>ftp</i>	<i>= Permite comunicación FTP (Protocolo de Transferencia de Archivos)</i>
<i>read</i>	<i>= permisos de lectura de la configuración del router</i>
<i>policy</i>	<i>= permite manejar las políticas de usuarios</i>
<i>winbox</i>	<i>= permite conexión por WinBox</i>
<i>web</i>	<i>= permite conexión por web</i>
<i>sensitive</i>	<i>= permite tomar Backup por ambos métodos</i>
<i>romon</i>	<i>= permite al usuario conectarse al router para administración remota</i>
<i>tikapp</i>	<i>= app oficial para MikroTik para celulares</i>
<i>permisos mínimos (permiso de acción y permiso de conexión)</i>	

Vamos a crear un nuevo grupo llamado GroupTest solo con algunos privilegios tomando en cuenta los privilegios mínimos de acción.



Luego vamos a crear un usuario test al cual lo relacionamos con el grupo GroupTest para ver si sus privilegios funcionan.



5.2. Verificación de permisos.

ejemplo al ingresar con el usuario nuevo

