

[router](#), [mikrotik](#)

Configurar Router Mikrotik

Conexión inicial

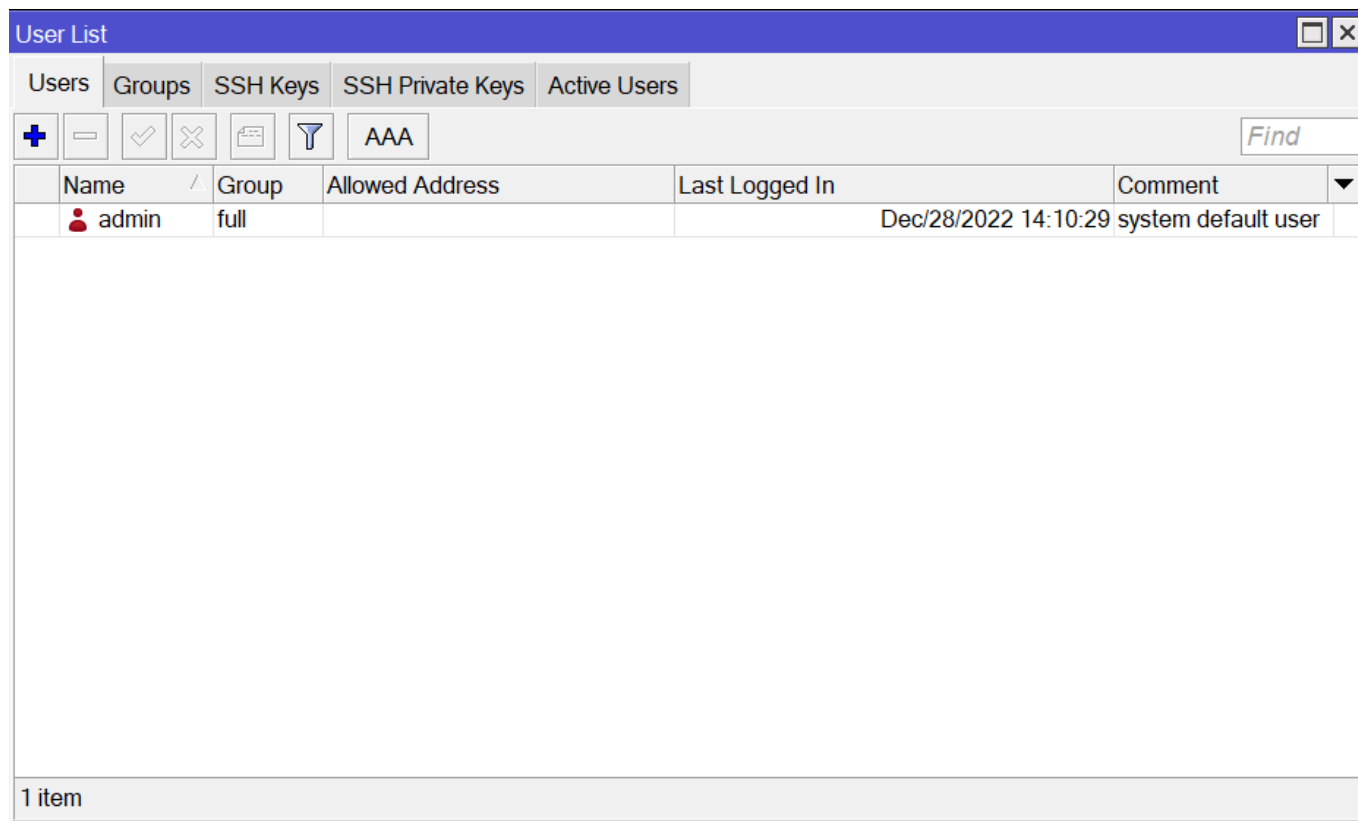
- Conectamos la boca Eth 1 del mikrotik a la misma red a la que estemos conectados . La boca 1 tiene un cliente de DHCP y cogerá una ip automáticamente.
- Usando el programa Winbox previamente descargado de la página de Mikrotik, nos conectamos o bien por ip o usando la MAC mediante la pestaña Neightbords para configurarlo

usuario: admin
password : no tiene

Cambiar la contraseña del usuario admin

por defecto el usuario admin viene sin contraseña, por lo que debemos asignarle una contraseña:

Vamos a system/users



Actualizar Firmware

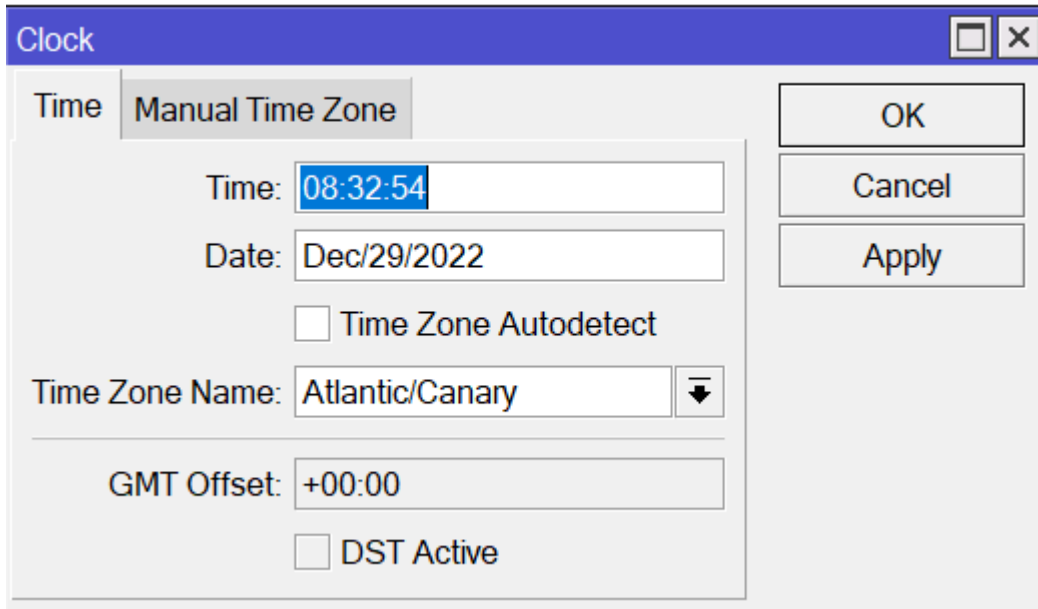
1. Desde la página de Mikrotik nos bajamos la última versión estable del firmware de nuestro router
2. Abrimos una conexión con nuestro router, pulsamos en la pestaña Files y arrastramos el fichero

con la actualización a dicha ventana

3. Reiniciamos el router para que instale la versión del firmware que hemos copiado

Sincronizar hora

se cambia la zona horaria a Atlantic/Canary. Vamos a System/Clock



The image shows a screenshot of the 'Clock' configuration window in Mikrotik WinBox. The window has a blue title bar with the text 'Clock' and standard window control buttons. Below the title bar, there are two tabs: 'Time' and 'Manual Time Zone', with 'Manual Time Zone' being the active tab. The main area contains several input fields and checkboxes: 'Time' is set to '08:32:54', 'Date' is 'Dec/29/2022', 'Time Zone Name' is 'Atlantic/Canary' (selected from a dropdown menu), and 'GMT Offset' is '+00:00'. There are also two unchecked checkboxes: 'Time Zone Autodetect' and 'DST Active'. On the right side of the window, there are three buttons: 'OK', 'Cancel', and 'Apply'.

Activamos el cliente de ntp del router en → system/sntp client

SNTP Client

Enabled

Mode: unicast

Primary NTP Server: hora.roa.es

Secondary NTP Server: 0.0.0.0

Server DNS Names:

Dynamic Servers:

Poll Interval: 128 s

Active Server: 150.214.94.5

Last Update From: 150.214.94.5

Last Update: 00:00:52 ago

Last Adjustment: 5 065 us

Last Bad Packet From:

Last Bad Packet:

Last Bad Packet Reason:

OK

Cancel

Apply

Cambiamos el identificador del router

Vamos a → System/Identity

Identity

Identity: ROU0001

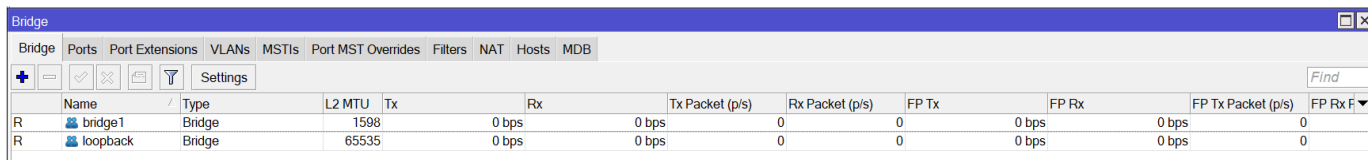
OK

Cancel

Apply

Creamos un Bridge

En el menú /BRIDGE vamos a crear dos bridges, uno para aplicar la configuración a los puerto eth1 al eth5, el otro lo llamamos loopback pero no tiene asociado ningún interfaz

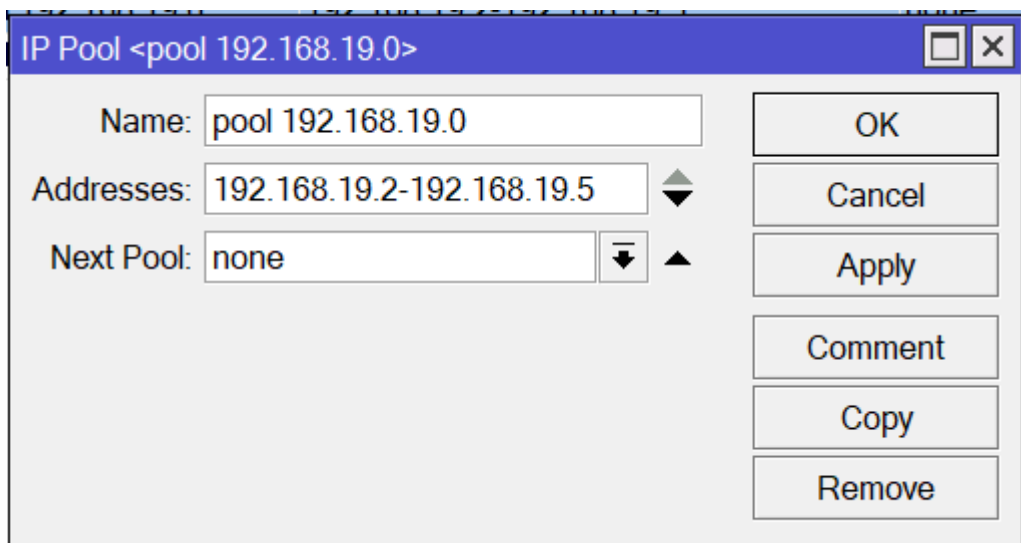


Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx F
bridge1	Bridge	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	
loopback	Bridge	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	

Configuración del DHCP

Paso 1

Se crea un DHCP Pool → IP/pool



IP Pool <pool 192.168.19.0>

Name: pool 192.168.19.0

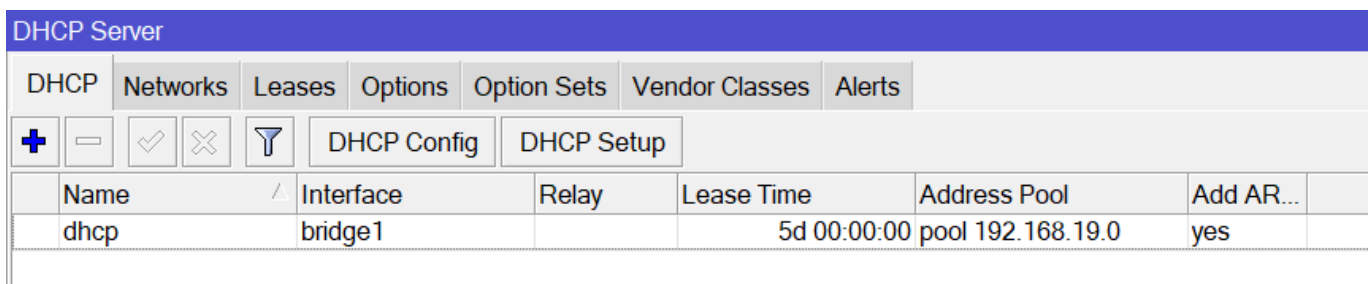
Addresses: 192.168.19.2-192.168.19.5

Next Pool: none

Buttons: OK, Cancel, Apply, Comment, Copy, Remove

Paso 2

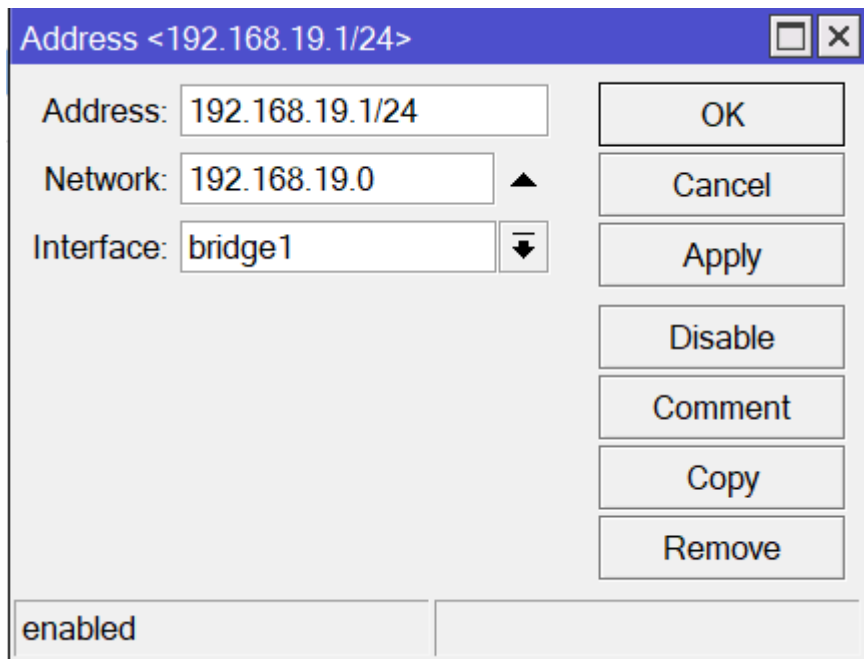
Se crea un DHCP Server



Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp	bridge1		5d 00:00:00	pool 192.168.19.0	yes

Paso 3

Le asignamos al bridge la ip 1 para que actúe como gateway → /IP/Address



Paso 4

Creamos reglas de filtrado → IP/Firewall/Filter Rules

Como mínimo

#	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Interface	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Action	Bytes	Packets	Comment
0	forward												accept	750.4 MiB	1 303 109	Conexiones establecidas y relacionadas
1	forward												drop	0 B	0	Conexiones invalidas
2	input												accept	451.9 MiB	704 692	Input Conexiones establecidas y relac...
3	input												drop	0 B	0	Trafico invalido
4	output												accept	218.8 MiB	550 395	Output Conexiones establecidas y rel...
5	output												drop	0 B	0	
6	input			6 (tcp)		22,8291					lte1		accept	156 B	3	administración desde WAN
7	input			6 (tcp)		22,8291					bridge1		accept	0 B	0	administración desde LAN

Paso 5

Configuramos el NAT → IP/Firewall/Nat

#	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets	Comment
0	accept	srcnat												85.1 KiB	1 676	
1	masquerade	srcnat									lte1			153.9 KiB	2 248	

Paso 6

Habilitamos DDNS → IP /Cloud

Cloud□ ×

DDNS Enabled

OK

DDNS Update Interval: ▼

Cancel

Update Time

Apply

Public Address:

Force Update

Public IPv6 Address:

DNS Name: sn.mynetname.net

Use Local Address

updated

Router is behind a NAT. Remote connection ...

Paso 7

Pasamos a crear los túneles IPSEC

Paso 8

Configuramos el envío de avisos y backup por correo → /Tools/Email

Paso 9

Bastionamos → [Proceso de Bastionado](#)

Referencias

- <https://soporte.syscom.mx/es/articles/2381987-mikrotik-configuracion-modem-lte>
- <https://soporte.syscom.mx/es/articles/1439423-mikrotik-configuracion-firewall-basico>
- <https://soporte.syscom.mx/es/articles/2673203-mikrotik-administracion-de-respaldos-backup-de-las-configuraciones>
- <https://soporte.syscom.mx/es/articles/3840228-mikrotik-activar-el-ip-cloud-ddns-de-mikrotik>

From:
<http://wiki.intrusos.info/> - LCWIKI

Permanent link:
<http://wiki.intrusos.info/doku.php?id=hardware:mikrotik:configuracion>

Last update: **242023/02/ 11:09**



