

## experiència amb el hotspot del mikrotik



[1]

creat: Dll, 12/07/2010 - 00:59 — [eloi.rebes](#) [1] - actualitzat: 02/09/2013 - 10:15pm

Bé, en aquest "comesfa" recopilo els passos per muntar un hotspot molt útil en un mikrotik. Jo vaig ser l'apuntador i en Sebas qui anava configurant. Aquest hotspot es troba al Far de SantSebastià de Llafranc de Palafrugell. Situada a 1km de la platja pel que no pot ser utilitzat des de vora del mar, però sí des del mirador del Far. Oferint accés a internet durant 1h i amb un caudal de 256K per usuari, amb una mitja d'uns 10 usuaris a les primeres setmanes de l'estiu del 2010.

Els requisits per poder portar-ho a terme:

-Supernode amb mikrotik.

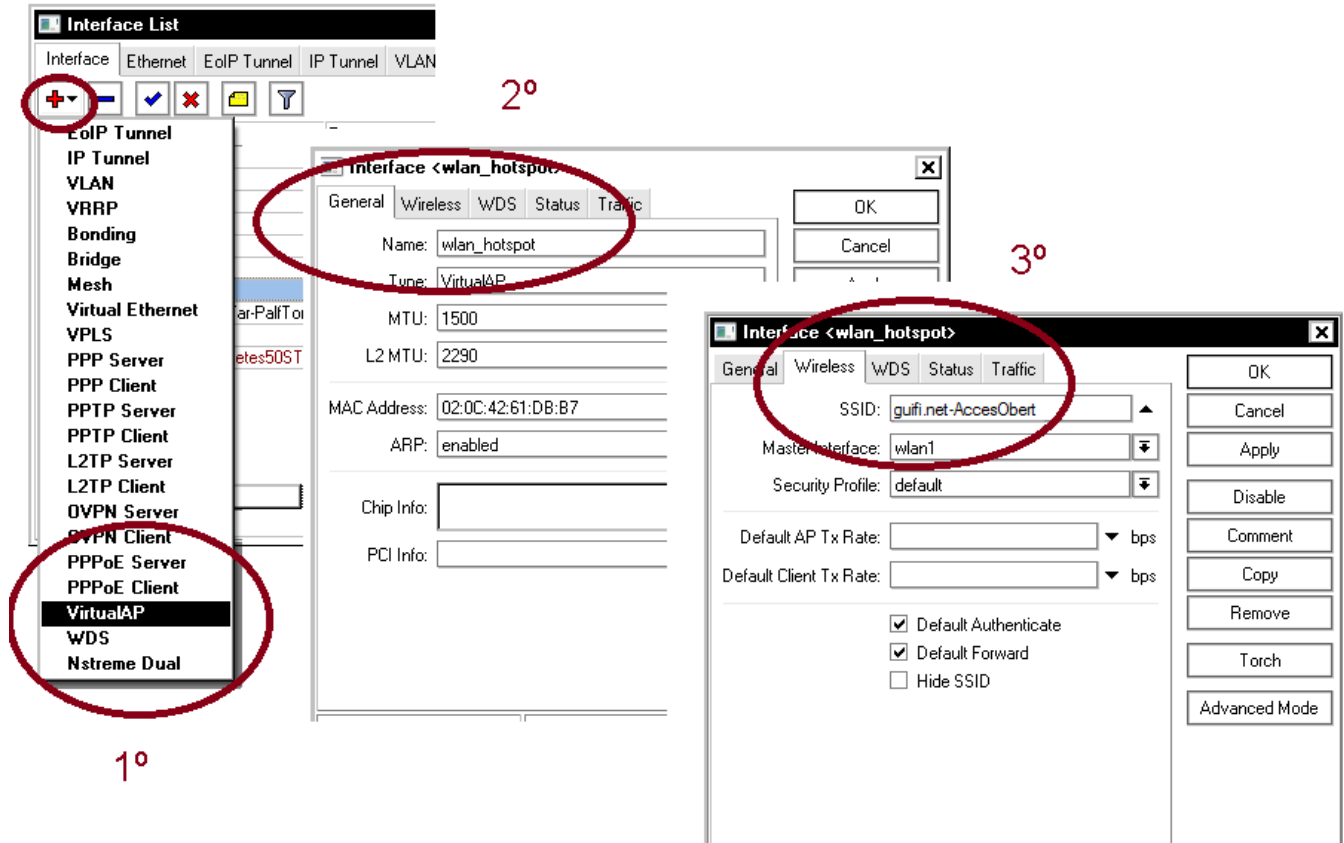
-AP sectorial a on es crearà el hotspot. No es recomana antenes omnidireccionals, al connectar un portàtil disminueix el rendiment de l'antena. (nota: si fossin 2 APs, es recomana crear un bridge amb els hotspots dels dos APs, perquè sino els usuaris tindrien 2 hotspots amb 2h al dia. Informació de com es fa... al punt 13).

-Un servidor on hi hagi un proxy federat. (Transparent no, que no permet el protocol https, el port 443. Un proxy transparent no permet el protocol https, i és necessari per veure el correu, connectar-se a les xarxes socials, etc).

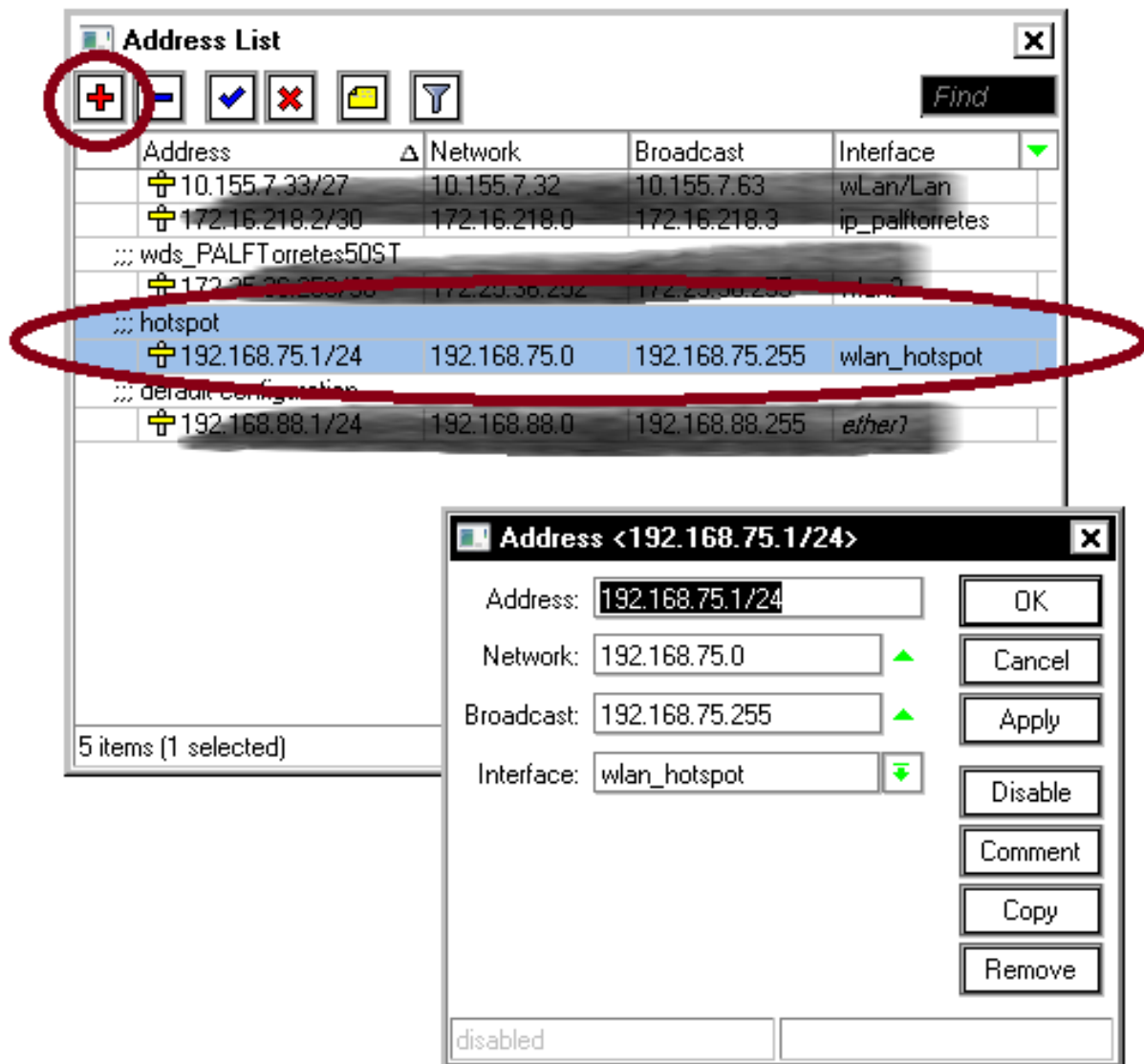
-En aquest cas s'ha utilitzat un servidor en Debian, per crear un túnel pel https. Hem de crear un túnel perquè la connexió segura (https) no pot ser redirigida.

Procés:

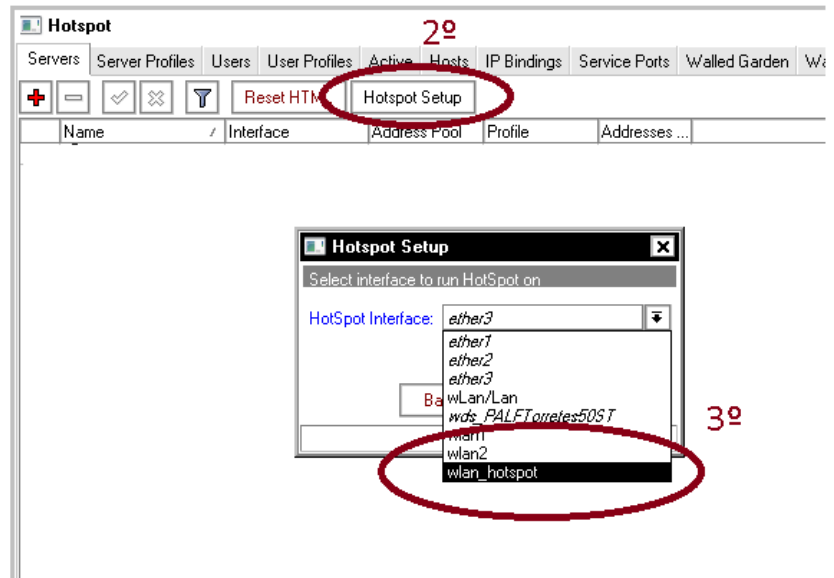
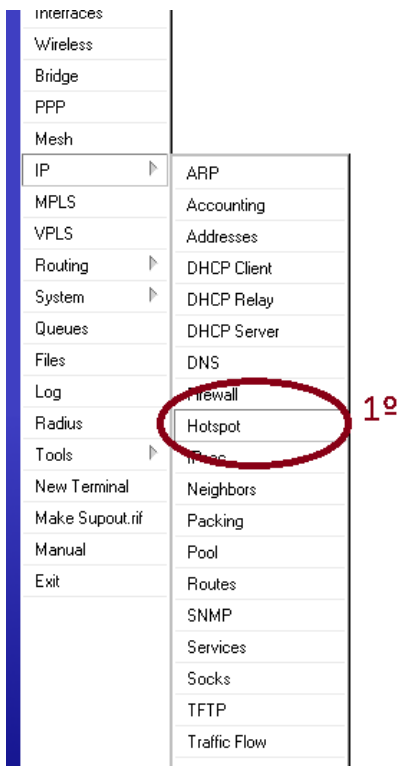
**1er- Creem la nova antena virtual: Interfaces > Afegir > VirtualAP, i l'associem a la antena on volem donar cobertura del hotspot.**



**2on- Creem un nou rang de IPs per els usuaris del hotspot... per exemple 192.168.75.1/24**



**3er- Ja podem començar amb l'assistent del hotspot: indicar el virtualAP creada, i ell solet ja ens anirà indicant els valors necessaris següents... això si, anem comprovant que corresponguin.**



nota: veureu que us ha generat regles al firewall, per poder funcionar correctament

## 4rt- L'assistent crea les dades necessàries per fer funcionar el hotspot, però cal modificar alguns valors:

**DHCP Server**

DHCP Networks Leases Options Alerts

+ - ✓ ✗ ⏏ DHCP Config DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool	Add
dhcp-wlan/Lan	wlan/Lan		3d 00:00:00	dhcp-wlan/L...	no
dhcp1	wlan_hotspo		1d 00:00:00	hs-pool-12	no

2 items (1 selected)

**DHCP Server <dhcp1>**

Name: dhcp1

Interface: wlan\_hotspot

Relay:

**Lease Time: 1d 00:00:00**

Address Pool: hs-pool-12

Src. Address:

Delay Threshold:

Authoritative: after 2s delay

Bootp Support

Add ARP For Leases

Always Broadcast

Use RADIUS

OK Cancel Apply Disable Copy Remove

modifiquem el valor de guardar la ip a 1 dia, al dhcp que ha creat l'assistent del hotspot, per coincidir la ip reservada amb la mac registrada al hotspot.

The screenshot shows the Mikrotik Hotspot configuration interface. At the top, there are tabs for Servers, Server Profiles, Users, User Profiles, Active, Hosts, IP Bindings, Service Ports, Walled Garden, and Walled Garden IP List. Below the tabs is a toolbar with icons for adding, deleting, and filtering, along with buttons for 'Reset HTML' and 'Hotspot Setup'. A table lists the configured servers:

Name	Interface	Address Pool	Profile	Addresses ...
hotspot1	wlan_hotspot	hs-pool-12	hsprof1	1

The 'Hotspot Server <hotspot1>' configuration dialog is open, showing the following settings:

- Name: hotspot1
- Interface: wlan\_hotspot
- Address Pool: hs-pool-12
- Profile: hsprof1
- Idle Timeout: 00:05:00
- Keepalive Timeout: (empty)
- Addresses Per MAC: 1
- IP of DNS Name: 0.0.0.0
- Proxy Status: running

The screenshot shows the Mikrotik Hotspot configuration interface. At the top, there are tabs for Servers, Server Profiles, Users, User Profiles, Active, Hosts, IP Bindings, and Service Ports. Below the tabs is a toolbar with icons for adding, deleting, and filtering. A table lists the configured server profiles:

Name	DNS Name	HTML Directory	Rate Limit (rx/tx)
default	hotspot	hotspot	
hsprof1	hotspot	hotspot	

The 'Hotspot Server Profile <hsprof1>' configuration dialog is open, showing the following settings:

- Name: hsprof1
- Hotspot Address: 192.168.75.1
- DNS Name: (empty)
- HTML Directory: hotspot
- Rate Limit (rx/tx): (empty)
- HTTP Proxy: 10.x.x.x
- HTTP Proxy Port: 3128
- SMTP Server: (empty)

The screenshot shows the Mikrotik Hotspot configuration interface. At the top, there are tabs for Servers, Server Profiles, Users, User Profiles, Active, Hosts, IP Bindings, and Service Ports. Below the tabs is a toolbar with icons for adding, deleting, and filtering. A table lists the configured server profiles:

Name	DNS Name	HTML Directory	Rate Limit (rx/tx)
default	hotspot	hotspot	
hsprof1	hotspot	hotspot	

The 'Hotspot Server Profile <hsprof1>' configuration dialog is open, showing the following settings:

- General tab selected
- MAC:  (circled in red)
- Cookie:  (circled in red)
- HTTP CHAP:  (circled in red)
- HTTP PAPS:  (circled in red)
- Trial:  (circled in red)
- MAC Auth. Password: (empty)
- HTTP Cookie Lifetime: 3d 00:00:00
- SSL Certificate: none
- Split User Domain:
- Trial Uptime Limit: 01:00:00 (circled in red)
- Trial Uptime Reset: 1d 00:00:00 (circled in red)
- Trial User Profile: default

a *HTTP Proxy* hi poseu un proxy a utilitzar, i també el seu port

a on posa *Trial Uptime Limit: 01:00:00* vol dir que permetrem 1h d'accés, si volem 30min posarem 00:30:00

a *Trial Uptime Reset* és el valor a coincidir amb la ip guardada del servidor dhcp (comentat 3 imatges enrera)

The screenshot shows the Mikrotik Hotspot configuration interface. At the top, there are tabs for 'Server Profiles', 'Users', 'User Profiles', 'Active', 'Hosts', 'IP Bindings', 'Service Ports', 'Walled Garden', and 'Walled Garder'. Below these are icons for adding, deleting, and filtering items. A table lists the profiles, with the 'default' profile selected and circled in red. The table has columns for Name, Session Time..., Idle Timeout, Shared U..., and Rate Limit (rx/tx). The 'default' profile has a Session Time of none, Idle Timeout of none, Shared U... of 100, and Rate Limit (rx/tx) of 256K/256K. Below the table, it says '1 item (1 selected)'. A dialog box titled 'Hotspot User Profile <default>' is open, showing configuration options for the selected profile. The dialog has tabs for 'General', 'Advertise', and 'Scripts'. The 'General' tab is active. Fields include Name (default), Address Pool (none), Session Timeout, Idle Timeout (none), Keepalive Timeout (00:02:00), Status Autorefresh (00:01:00), Shared Users (100), Rate Limit (rx/tx) (256K/256K), Address List, Incoming Filter, Outgoing Filter, Incoming Packet Mark, Outgoing Packet Mark, Open Status Page (HTTP login), and a checked 'Transparent Proxy' checkbox. The 'Shared Users' and 'Rate Limit (rx/tx)' fields are circled in red. The 'Open Status Page' dropdown is also circled in red. Buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' are on the right. The name 'default' is shown at the bottom of the dialog box.

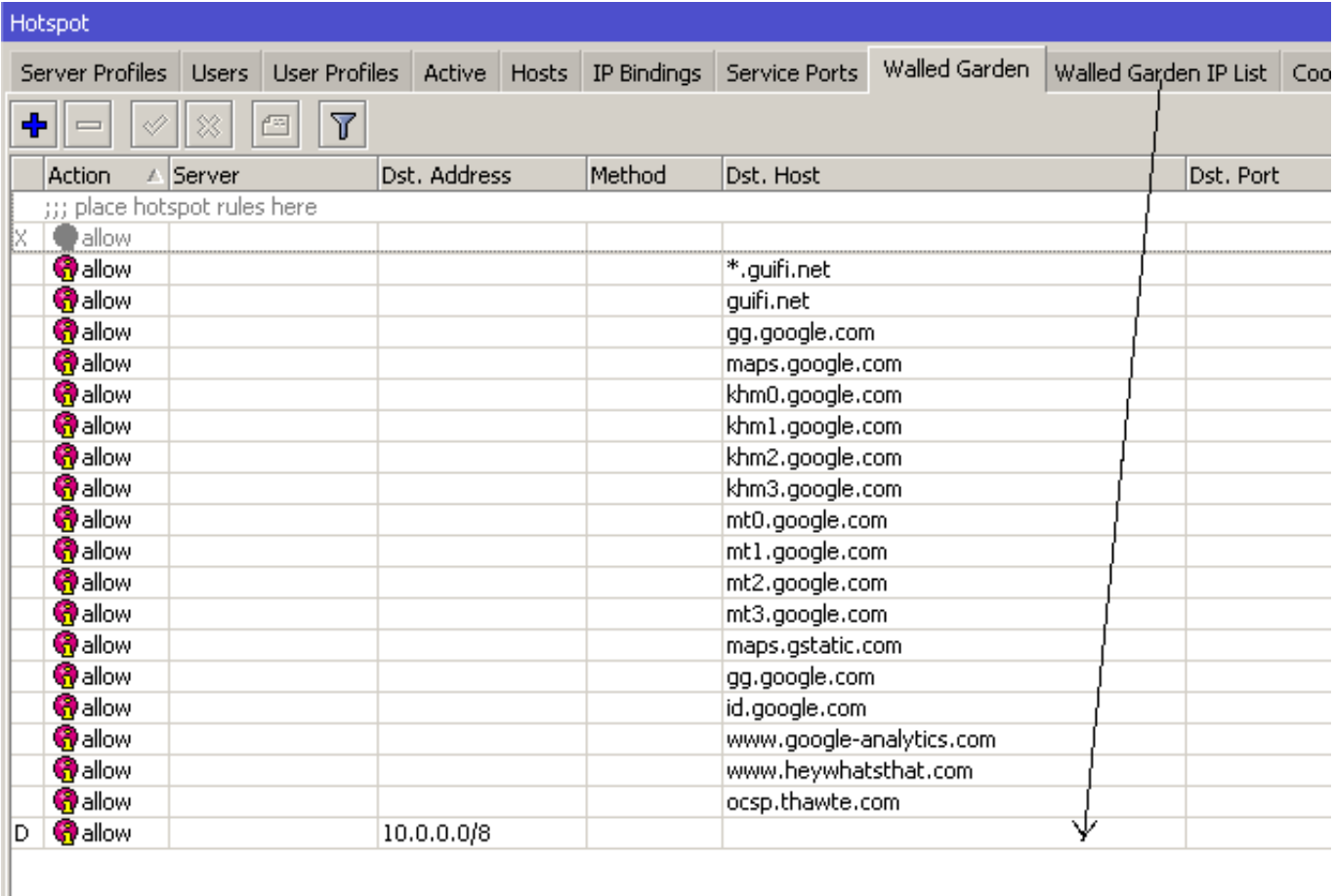
*Share Users* són els usuaris simultanis, i *Rate Límit* el caudal per usuari, si voleu posar 1 mega per usuari seria 1M/1M

(haureu de retocar la web del hotspot indicant la limitació del caudal a 1Mbps, en contes de 256Kbps)

## 5è- Exporto la llista de les pàgines blanques(=pàgines permeses sempre), per no haver de introduir una a una. Només s'ha d'enganxar a la terminal. Són les webs on sempre es podrà visitar, inclús amb la hora diària esgotada.

[codi a enganxar al terminal del mikrotik](#) [2] (podeu fer un "Anomena i desa..." o clicar i s'obrirà a una finestra nova).

quedarà així:



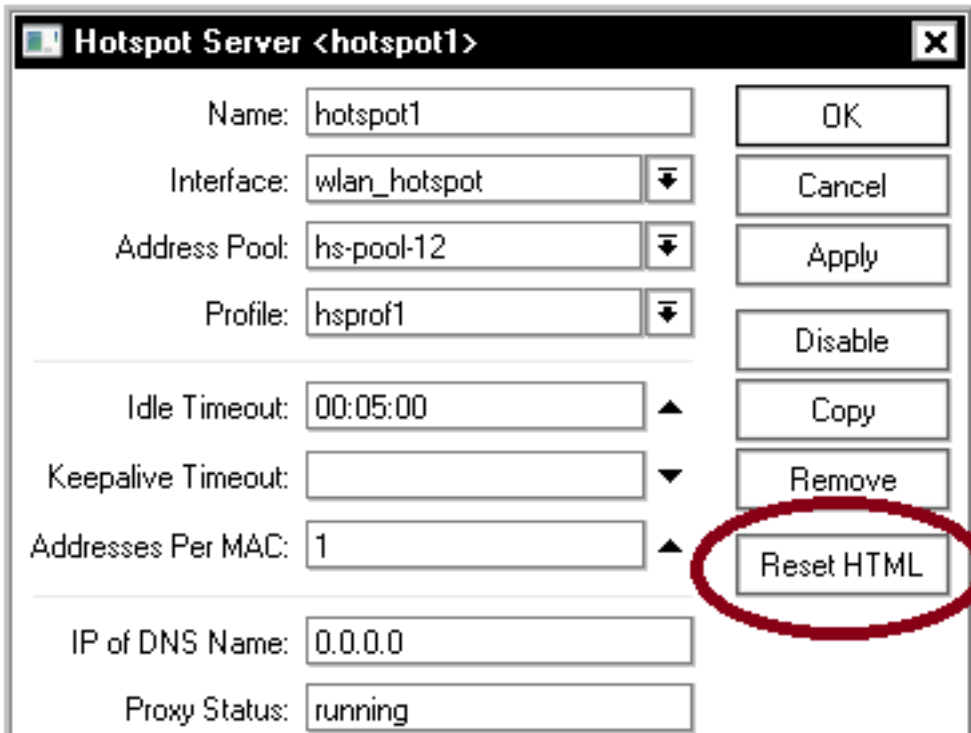
Action	Server	Dst. Address	Method	Dst. Host	Dst. Port
;;; place hotspot rules here					
X	allow				
	allow			*.guifi.net	
	allow			guifi.net	
	allow			gg.google.com	
	allow			maps.google.com	
	allow			khm0.google.com	
	allow			khm1.google.com	
	allow			khm2.google.com	
	allow			khm3.google.com	
	allow			mt0.google.com	
	allow			mt1.google.com	
	allow			mt2.google.com	
	allow			mt3.google.com	
	allow			maps.gstatic.com	
	allow			gg.google.com	
	allow			id.google.com	
	allow			www.google-analytics.com	
	allow			www.heywhatsthat.com	
	allow			ocsp.thawte.com	
D	allow	10.0.0.0/8			

la majoria d'aquests enllaços de pàgines blanques són dels mapes de google per veure'ls en la web de guifi, també l tots els dominis de guifi, i també permet accedir a qualsevol contingut de la red guifi (=10.0.0.0/8, que és molt important per donar accés a la xarxa de forma separada del sistema hotspot, és a dir, que si s'acaba el temps de connexió directe a Internet sempre tinguis accés a la xarxa de guifi, ja que per la llicència hem de garantir el lliure accés a la xarxa, com així recull la [XOLN](#) [3])

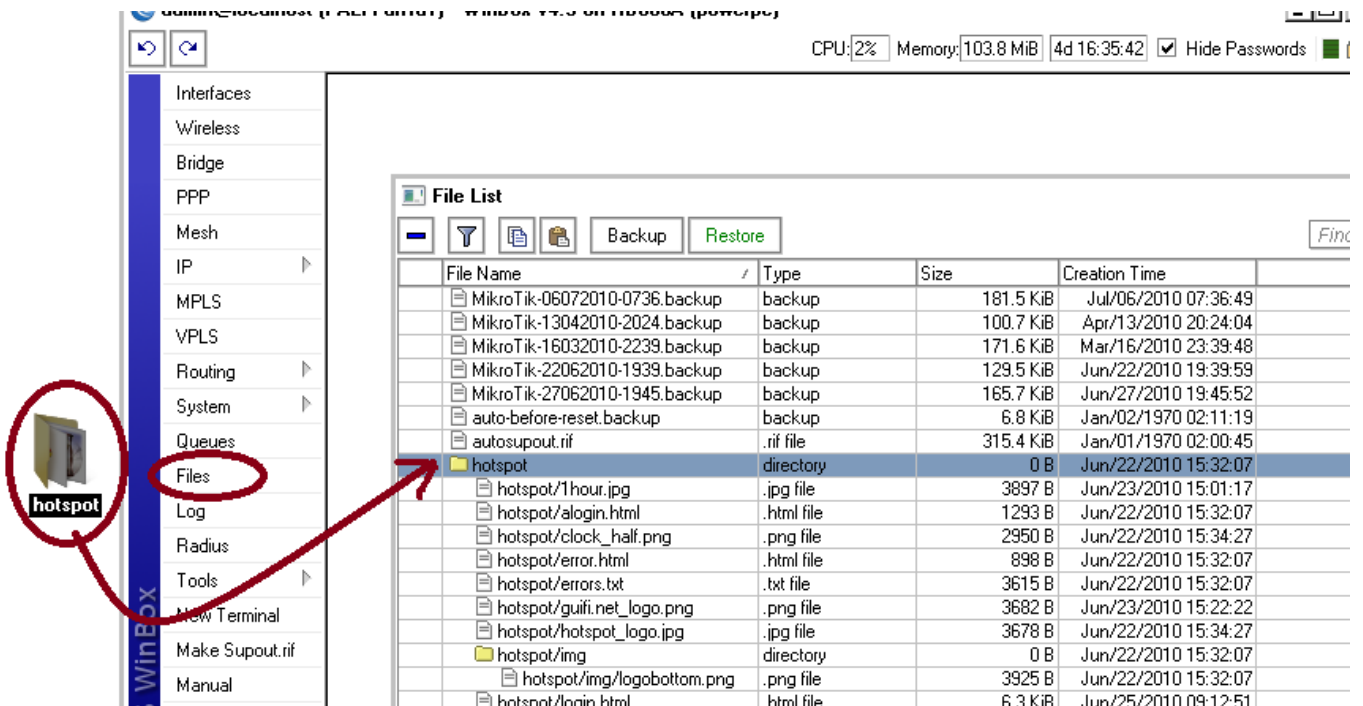
(la última linea d'aquesta llista es crea automàticament ja que el codi ho introdueix a Walled Garden IP List)

## 6è- Importem els fitxers de la web del hotspot, a la carpeta corresponent del trasto.





nota: si algú ja havia creat alguna web hotspot i vol deixar-ho de fàbrica, clicar sobre "Reset HTML"



[web hotspot \(versió 1h\)](#) [4]

[web hotspot \(versió 30min\)](#) [5]

Posem una pàgina on podeu agafar idees, o deixar-la tal com està

(el més important són els valors que necessita el mikrotik per validar l'usuari, que és el botó de "clicar per començar a navegar")

## 7è- Afegir les IPs del mikrotik i del servidor d'on hi hagi el tunel a l'ACLs del proxy

The screenshot shows two parts of the Mikrotik WinBox interface. The top part, labeled '1º', is the 'Creació d'ACL' (ACL Creation) window. It has a tab 'Adreces Client ACL' (Client IP Addresses). The 'Nom d'ACL' (ACL Name) field is set to 'hotspot'. Under 'Des de la IP' (From IP), there are two entries: '10.mikrotik' and '10.servidor'. The bottom part, labeled '2º', is the 'Control d'Accés' (Access Control) window. It has a tab 'Restriccions de proxy' (Proxy Restrictions). A table lists various actions and ACLs:

Acció	ACLs
<input type="checkbox"/> Permet	manager localhost
<input type="checkbox"/> Denega	manager
<input type="checkbox"/> Permet	purge localhost
<input type="checkbox"/> Denega	purge
<input type="checkbox"/> Denega	!Safe_ports
<input type="checkbox"/> Denega	CONNECT !SSL_ports
<input type="checkbox"/> Permet	localhost
<input type="checkbox"/> Permet	hotspot
<input type="checkbox"/> Permet	usuaris_autenticats
<input type="checkbox"/> Denega	all

- comprovem si hi ha algun problema amb les ACLs creades: > squid -k parse
- reiniciem l'Squid: > /etc/init.d/squid reload

nota: Si utilitzem un proxy federat s'han de crear amb l'accés permés a les ips del mikrotik i del propi servidor on hi haura l'altre punt del túnel, o sigui el propi proxy.

Fins aquí feta la feina del hotspot simple, o bàsicament amb el protocol http. Ara muntarem un túnel entre el mikrotik i un servidor on hi hagi un proxy, per redirigir el protocol segur https.

## 8è- Afegir el túnel al fitxer de configuració a INTERFACES, per muntar-lo en arrencar el sistema.

```
up ip_tunnel add ip_tunnel_srv mode
  ipip remote 10.x.x.x(mikrotik)
  local 10.x.x.x(servidor)

up ifconfig ip_tunnel_srv
  172.16.218.1 netmask
  255.255.255.252 up
```

```
up iptables -t nat -A POSTROUTING
-s 172.16.218.2 -j MASQUERADE

down iptables -t nat -D POSTROUTING
-s 172.16.218.2 -j MASQUERADE

down ip tunnel del ip_tunnel_srv mode
ipip remote 10.x.x.x(mikrotik) local
10.x.x.x(servidor)
```

**nota:** tot el que està en negreta és el que s'ha de canviar pel vostre cas,

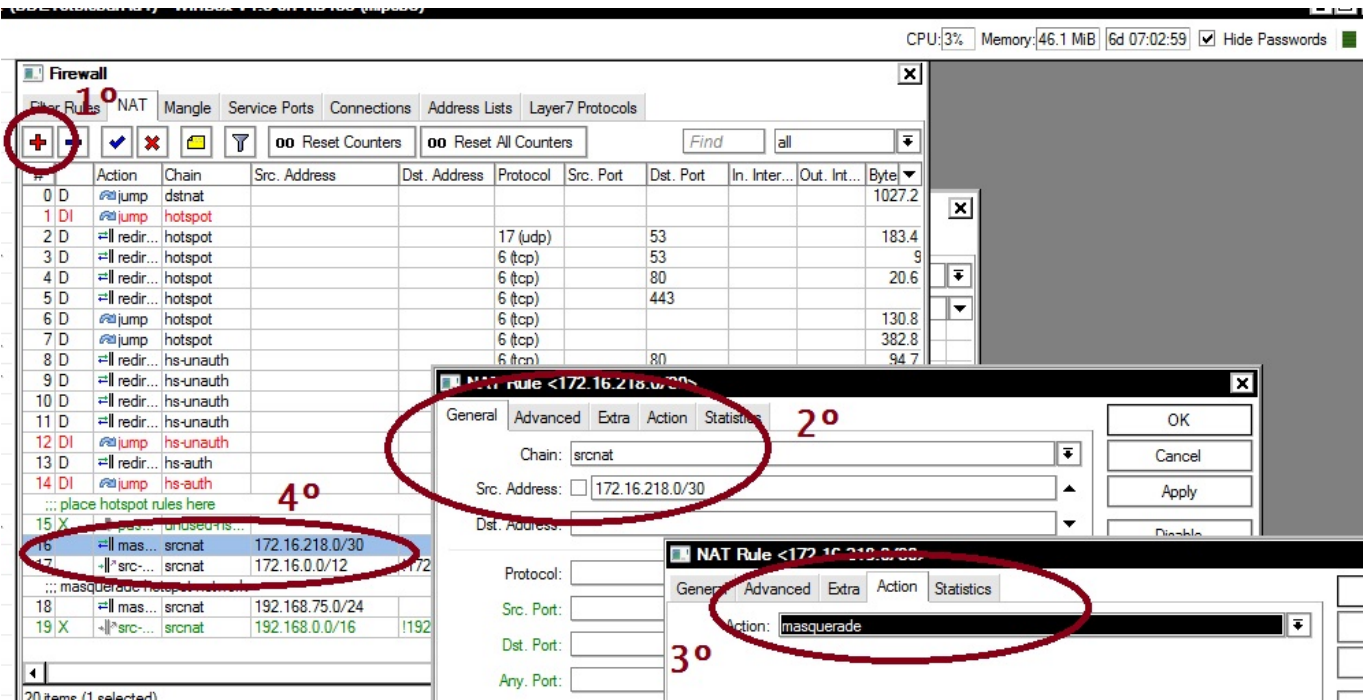
a remote posar la IP del mikrotik i a local la del servidor,

les 172.16.218.1 la ip del servidor i 172.16.218.2 la ip del mikrotik (es recomanen deixar tal com estan)

**nota:** vigileu si teniu 2 tarjes de red (normalment és així), la de guifi i la d'adsl... s'ha de posar a dins de la de guifi

## 9è- Afegir una nova regla nat al firewall

Per no interferir les IPs del tunel, que són del rang dels enllaços troncal, crearem una regla al nat únicament per què el tunel pugui arribar al servidor sense enmasquerar-se.



nota: en el 4rt punt mostra la posició de la nova regla, que ha d'estar per sobre de la regla que introdueix l'unsolclick

## 10è- Afegir l'altre punt del túnel al mikrotik

Interface List

Interface <ip\_palltorretes>

Address List

Address <172.16.218.2/30>

1º

2º

3º

4º

nota: els valors en vermell, heu de posar els vostres

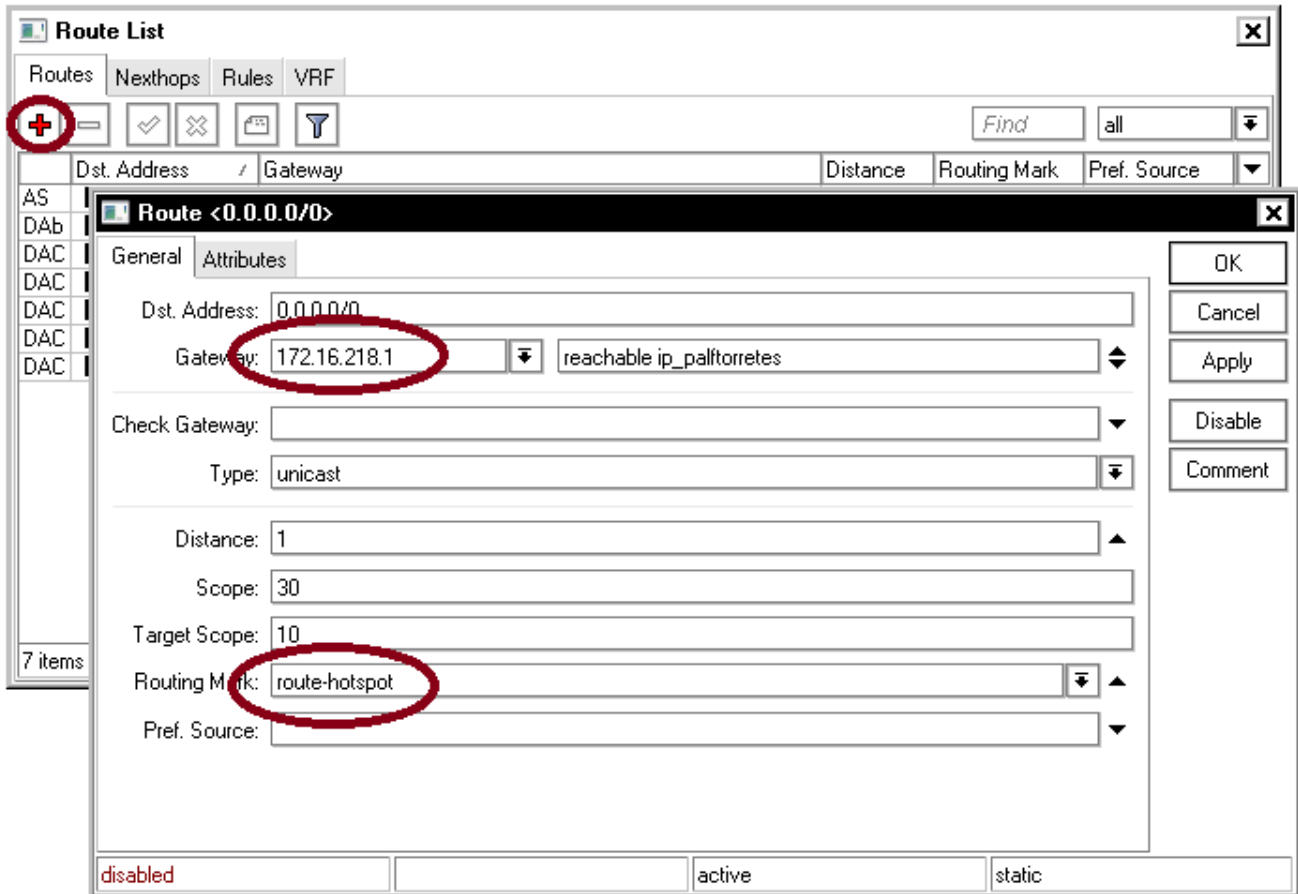
## 11è- Marcar els paquets del protocol https que surten del hotspot per redirigir-los pel túnel creat.

Firewall

Mangle Rule <192.168.75.0/24->443>

Mangle Rule <192.168.75.0/24->443>

a New Routing.Mark s'ha de crear un nom, podeu triar-lo si voleu



## 12è- Deixar passar cap a internet els paquets HTTPS que arriben del mikrotik

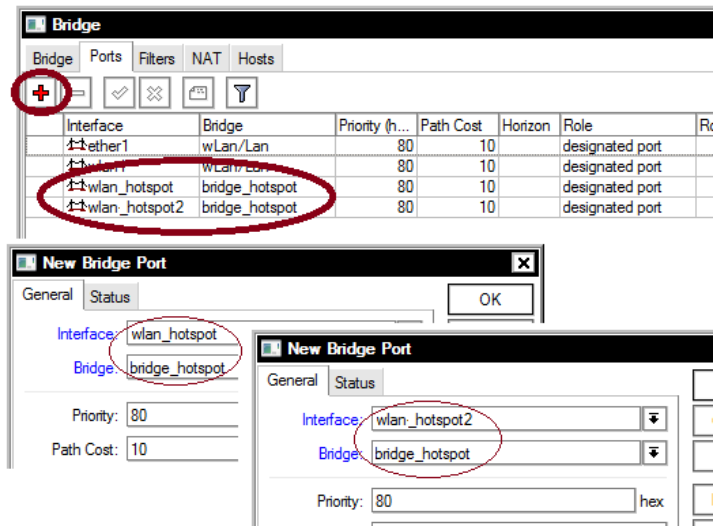
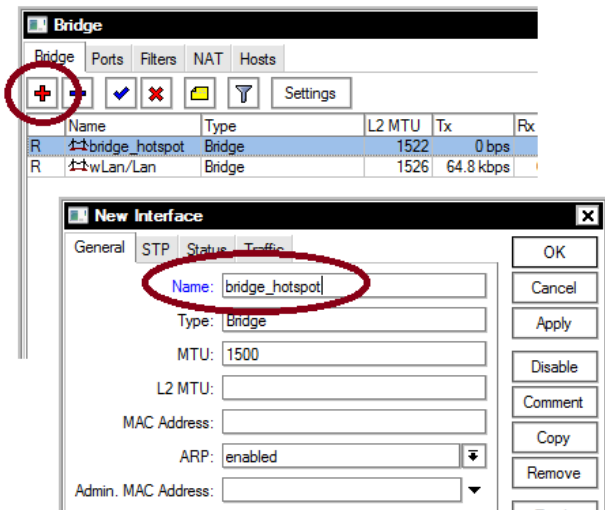
Editar l'arxiu `/etc/sysctl.conf` i descomentar la línia (treure-li el símbol #)  
`#net.ipv4.ip_forward=1`

## 13è- (opcional) Crear un bridge amb les diferents antenes possibles sobre on es faràn els hotspots.

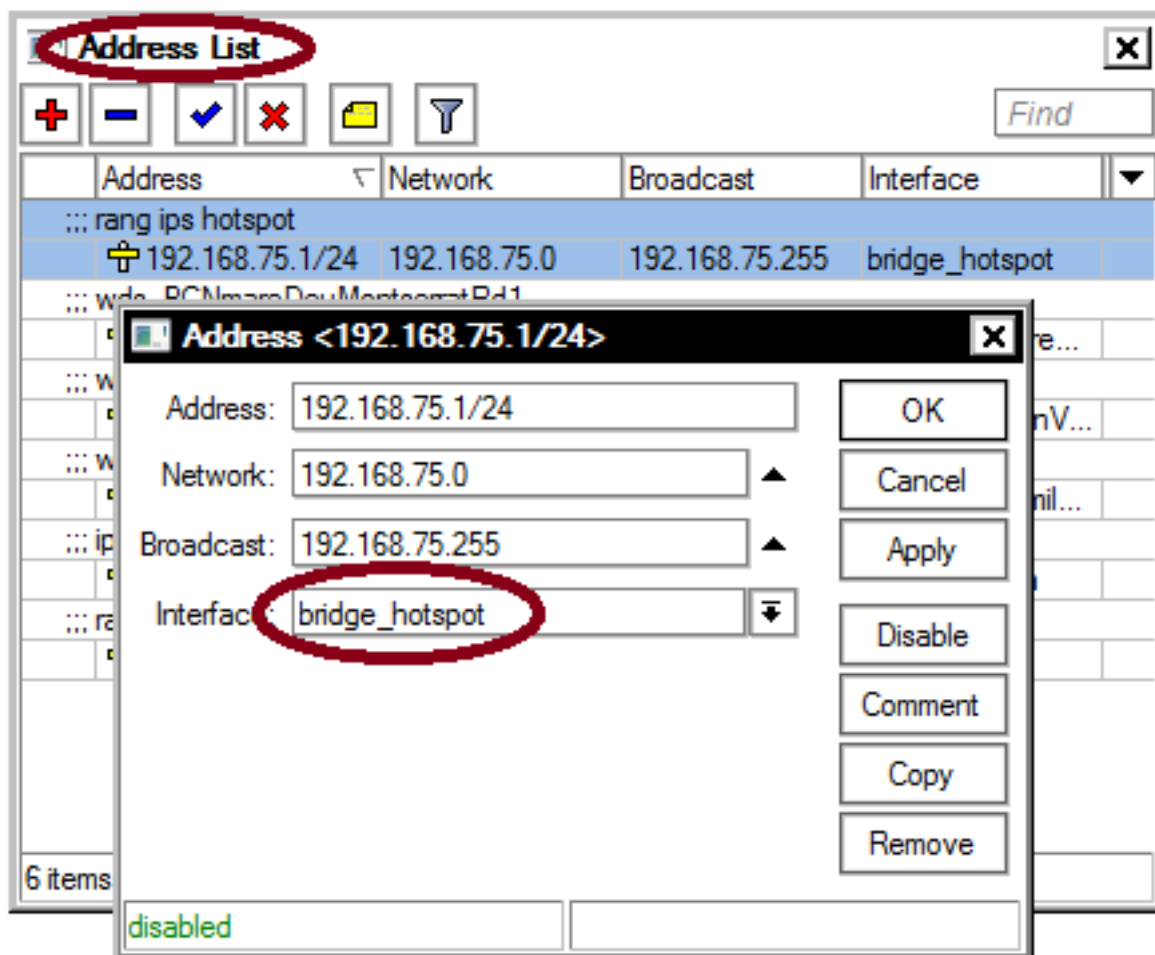
Tot aquest procés serveix per si tenim, una, dos, tres o més antenes que s'utilitzaran com a hotspot. Només s'ha de repetir el primer pas, per a cada wlan real. En comptes d'aplicar certs passos a una sola interfície, ho podem fer sobre un bridge. En aquest bridge hi podrem afegir les VirtualAPs que volguem.

Interface List						
Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP	Bonding
R	bridge_hotspot	Bridge	1522	0 bps	0 bps	
R	ether1	Ethernet	1526	71.0 kbps	9.8 kbps	
	ether2	Ethernet	1522	0 bps	0 bps	
	ether3	Ethernet	1522	0 bps	0 bps	
R	ip_tunnel	IP Tunnel		0 bps	0 bps	
R	wLan/Lan	Bridge	1526	71.0 kbps	8.1 kbps	
R	wlan1	Wireless (Atheros AR5...	2290	1410 bps	0 bps	
::: guifi.net-AccesObert						
	wlan_hotspot	VirtualAP	2290	0 bps	0 bps	
R	wlan2	Wireless (Atheros AR5...	2290	0 bps	0 bps	
::: guifi.net-AccesObert 2						
	wlan_hotspot 2	VirtualAP	2290	0 bps	0 bps	

Aquest exemple tenim 2 wlans



Aquest és el pas on hi afegim les VirtualAPs



(nota: potser modificant els valors el servidor hotspot se us posa en vermell, desactiveu i activeu aquest rang d'adreces com a últim pas.)

The screenshot shows the Mikrotik WinBox DHCP Server configuration interface. At the top, the 'DHCP Server' window is open, with tabs for 'DHCP', 'Networks', 'Leases', 'Options', and 'Alerts'. Below the tabs are several icons and buttons: a red plus sign, a blue minus sign, a blue checkmark, a red X, a funnel icon, 'DHCP Config', and 'DHCP Setup'. A table lists two DHCP servers:

Name	Interface	Relay	Lease Time	Address Pool	Ac
dhcp-wLan/Lan	wLan/Lan		1d 00:00:00	dhcp-wLan/L...	nc
dhcp_hotspots	bridge_hotspot		1d 00:00:00	hs-pool-12	nc

Below the table, a configuration dialog for 'DHCP Server <dhcp\_hotspots>' is open. The dialog contains the following fields and buttons:

- Name: dhcp\_hotspots
- Interface: bridge\_hotspot (circled in red)
- Relay: (empty)
- Lease Time: 1d 00:00:00
- Address Pool: hs-pool-12
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: after 2s delay
- Proxy Support

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Copy, and Remove.



The screenshot shows the Mikrotik WinBox interface for configuring a Hotspot. The 'Hotspot' menu is circled in red. Below it, a table lists the configured hotspot:

Name	Interface	Address Pool	Profile	Address
hotspot1	bridge_hotspot	hs-pool-12	hsprof1	

The configuration dialog box for 'Hotspot Server <hotspot 1>' is open, with the following settings:

- Name: hotspot1
- Interface: bridge\_hotspot (circled in red)
- Address Pool: hs-pool-12
- Profile: hsprof1
- Idle Timeout: 01:00:00
- Keepalive Timeout: (empty)
- Addresses Per MAC: 1
- IP of DNS Name: 0.0.0.0
- Proxy Status: running

**LLESTOS!!**

...resultat:

## ¿Què és guifi.net?



És una xarxa de telecomunicacions, oberta, lliure i neutral que es vertebrava a partir d'un acord d'interconnexió on cadascú al connectar-se esten la xarxa i obte connectivitat.

**guifi.net és de tots els seus participants.**  
+ informació a: [guifi.net/que\\_es](https://guifi.net/que_es)

## HotSpot



Aquest sistema HotSpot **guifi.net-AccesObert** permet navegar a Internet amb algunes limitacions:

- 1 hora al dia
- Caudal limitat - *256 kbps/user*

Esta dirigit a persones que necessitin un accés puntual i temporal a Internet.

Si es desitja realitzar una connexió més prolongada i lliure de limitacions, és necessari realitzar una correcta connexió a la xarxa.

Siguint els passos descrits a: [guifi.net/trespazos](https://guifi.net/trespazos)



**Pot accedir a Internet des del sistema Hotspot clicant aquí**

Adjunt

[hotspot\\_cat\\_1h\\_v1.2.zip](#) [6]

[hotspot\\_cat\\_30min\\_v1.2.zip](#) [7]

Mida

51.4 KB

51.39 KB

- [notícies guifi.net](#) [8]
- [notícies de guifi.net - Catalunya](#) [9]
- [Mig](#) [10]
- [Gestors de continguts / Portals](#) [11]

**URL d'origen:** <https://guifi.net/ca/hotspot-mikrotik>

### Enllaços:

[1] <https://guifi.net/ca/user/8771>

[2] <http://guifi.net/files/walled-garden-llista.txt>

[3] <http://guifi.net/ca/CXOLN>

[4] [http://guifi.net/files/hotspot\\_cat\\_1h\\_v1.2.zip](http://guifi.net/files/hotspot_cat_1h_v1.2.zip)

[5] [http://guifi.net/files/hotspot\\_cat\\_30min\\_v1.2.zip](http://guifi.net/files/hotspot_cat_30min_v1.2.zip)

[6] [https://guifi.net/files/hotspot\\_cat\\_1h\\_v1.2.zip](https://guifi.net/files/hotspot_cat_1h_v1.2.zip)

[7] [https://guifi.net/files/hotspot\\_cat\\_30min\\_v1.2.zip](https://guifi.net/files/hotspot_cat_30min_v1.2.zip)

[8] <https://guifi.net/ca/taxonomy/term/134>

[9] <https://guifi.net/ca/taxonomy/term/227>

[10] <https://guifi.net/ca/taxonomy/term/106>

[11] <https://guifi.net/ca/taxonomy/term/66>