

Hotspot + CAPsMAN + VPN en la nube

MTI David Ricardo López Aldret

MUM México 2018

Acerca de mí

- Mágister IT**
- Mikrotik MTCNA, MTCTCE, MTCWE, MTCRE certified**
- Ubiquiti UAC certified**
- Microsoft MCSE, MCSA, MCP certified**
- Cambium Networks ePMP, PtP 650 certified**
- CompTIA A+, Security+, Network+, Server+ certified**
- ETA-I CST, CNST certified**
- Access Data ACE certified**
- Denwa DeECP certified**

Acerca de mí



Objetivo

- Mostrar de una forma clara lo sencillo que es implementar uno o múltiples hotspots que sean controlados en la nube mediante herramientas propias de Mikrotik (RouterOS, User Manager y CAPsMAN) y accesibles a través de una VPN.**
- Se omiten configuraciones obvias y personalizadas.**

Qué es CAPsMan

- **Es un controlador Wireless, a través de el, los AP's que se encuentren registrados en el, serán administrados y manejados de forma centralizada. Permite despliegues masivos de equipos inalámbricos con configuraciones homogéneas.**

Qué es Hotspot

- Sencillamente, es un servicio que ofrece conexión a internet a través de una red inalámbrica, pueden ser gratuitos o de paga.

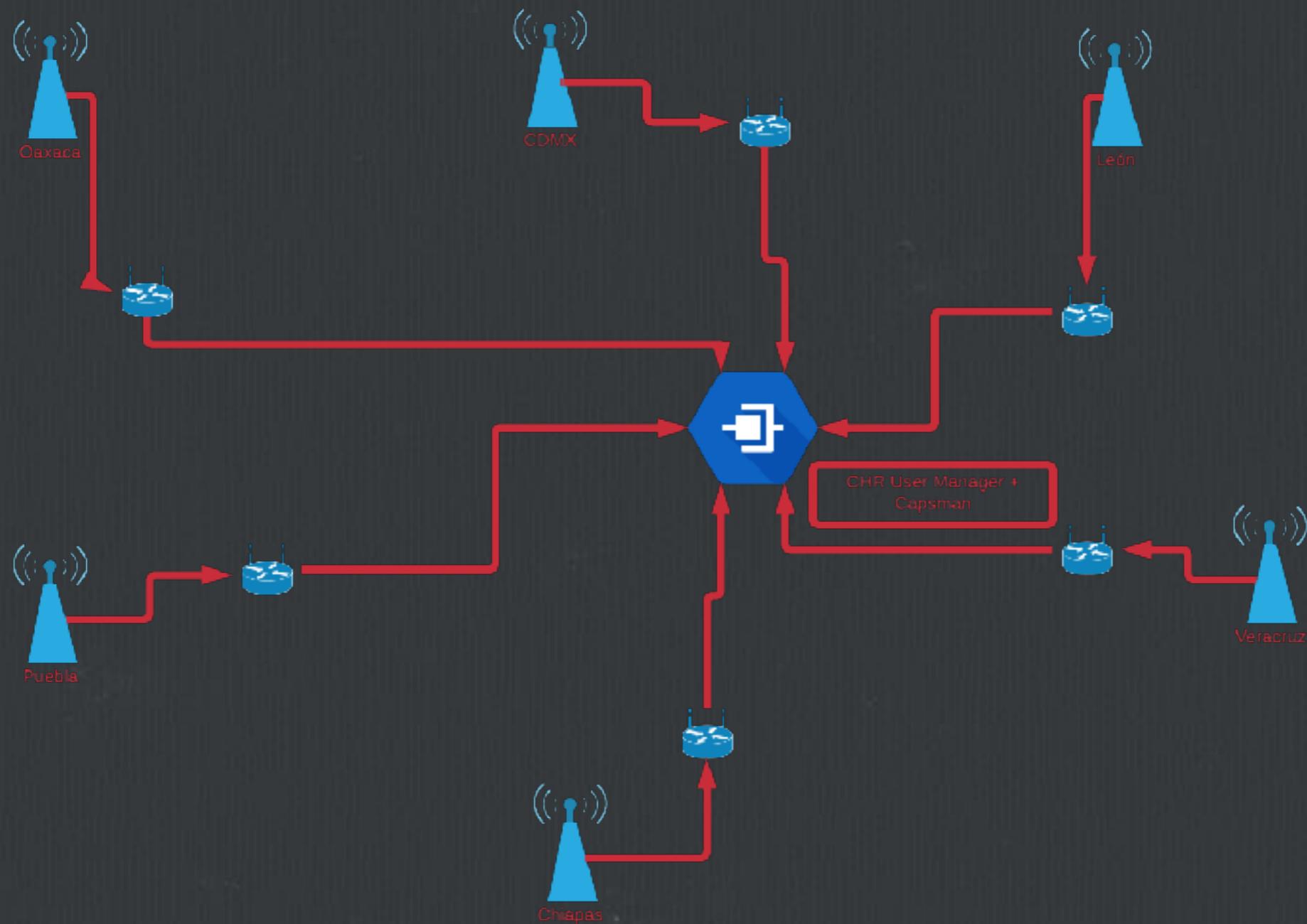
Qué es VPN

- **“Red privada virtual”** , permite una conexión segura entre dos puntos distantes entre si y que permiten interactuar como si se tratara de una red local. Existen varios tipos de VPN que han surgido con los años.

Qué es UserManager

- **Es una aplicación RADIUS desarrollada por Mikrotik que cumple con los estándares de AAA (Autorización, Autenticación y Contabilización). A través de el es posible administrar servicios PPP, Hotspot, DHCP, Wireless y RouterOS**

Escenario



Ventajas de un escenario así

- Cada Cap+Hotspot tiene una salida propia a internet**
- Cada Cap+Hotspot está centralizado a un solo CAPsMAN y UserManager, ergo, solo es una generación de vouchers**
- Roaming de usuarios con el mismo voucher**
- Cambios en caliente en toda la red**

Desventajas

- CAPsMAN se encuentra estacionado a nivel de desarrollo, no han habido mejoras ni agregados.**

Desventajas

- ¿Se cayó EL CHR? eso es algo malo, malo....malo



¿Qué necesitamos?



Licencia



VPS



AP



Instalamos RouterOS

- <https://www.digitalocean.com/community/questions/installing-mikrotik-routers>
- Creamos un droplet y pegamos el script

Droplets

Search by Droplet name

Droplets

Volumes

Name	IP Address	Created	Tags
 Dude 1 GB / 30 GB Disk / NYC3 - Ubuntu 16.04.2 x64	104.131.19.75	1 year ago	More

Choose an image

Distributions Containers



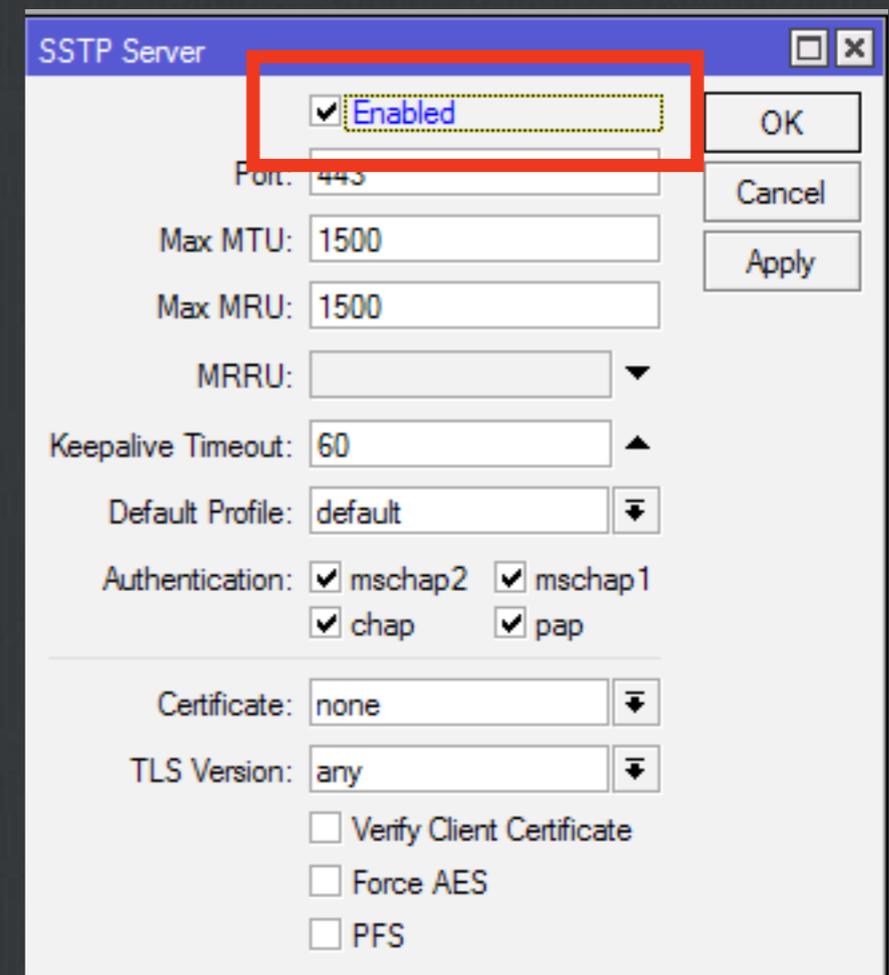
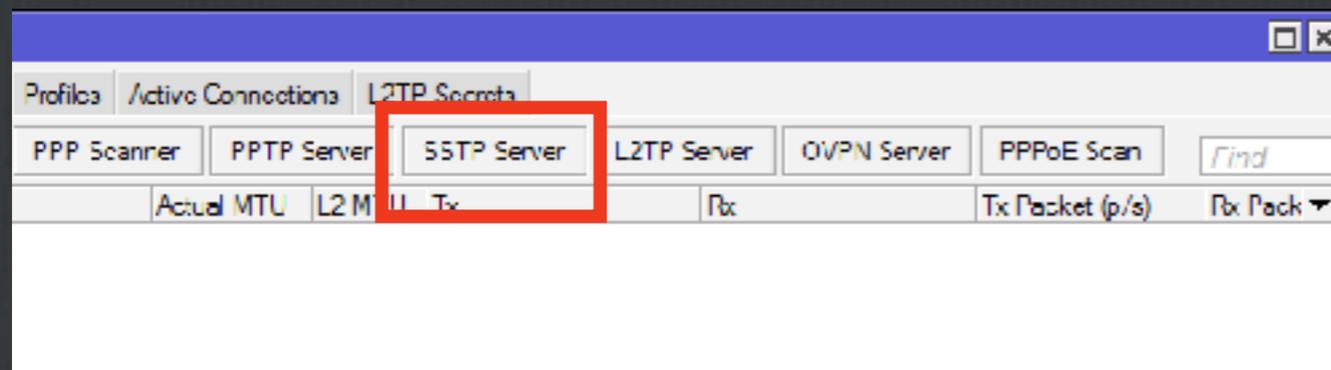
Instalamos RouterOS

- Usuario: root y contraseña: xxxxxx**
- Upgradeamos**
- Realizamos las configuraciones básicas (cambio de password, dns, etc)**
- Descargamos el paquete UserManager y lo instalamos**

Configuramos nuestros AP's

- Damos salida a internet (DNS, Gateway, IP, etc)
- Actualizamos y aseguramos nuestro RouterOS
- Personalizamos

Establecemos VPN (server)



Establecemos VPN (server)

New PPP Secret

Name: AP1

Password: AP1#

Service: sstp

Caller ID:

Profile: default

Local Address: 10.0.0.1

Remote Address: 10.0.0.2

OK

Cancel

Apply

Disable

Comment

Copy

Remove

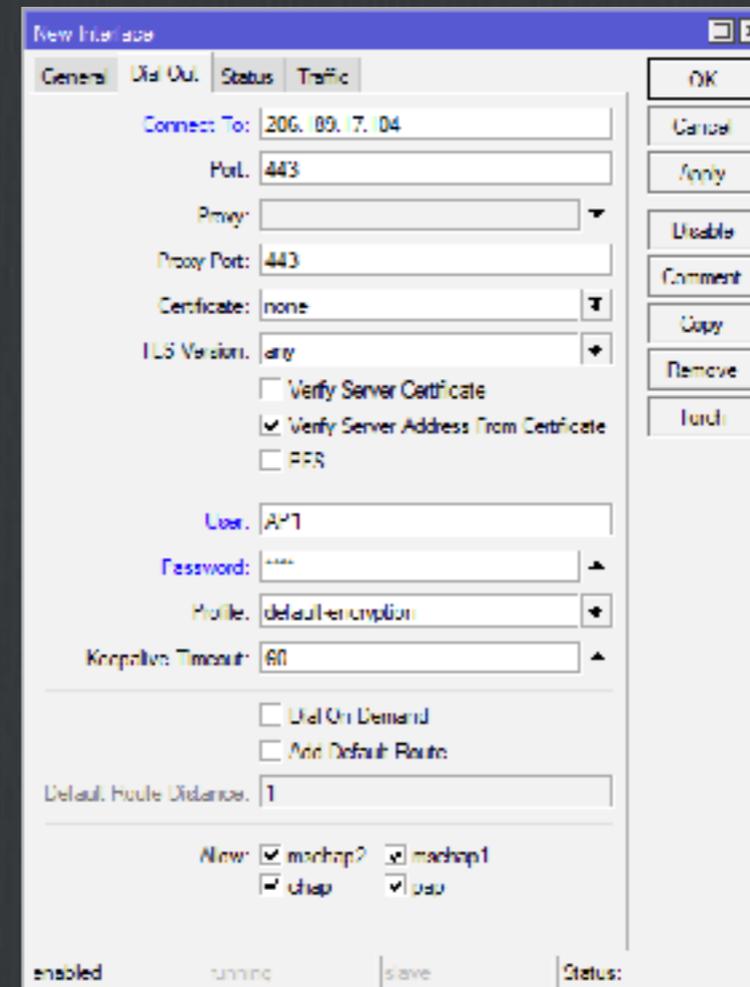
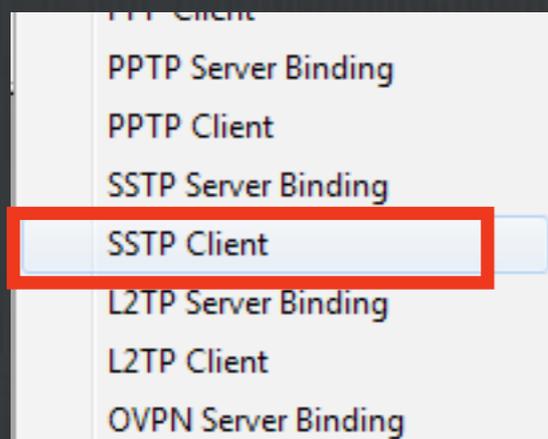
PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting Find

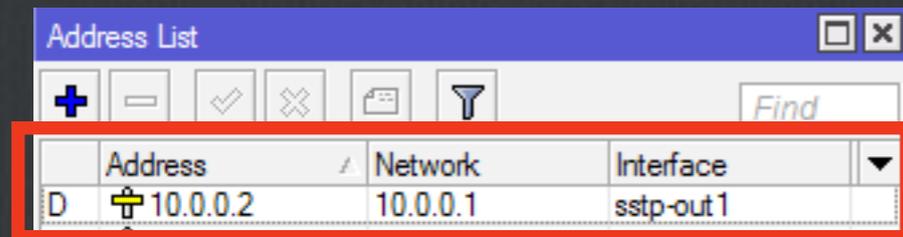
Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
AP1	AP1#	sstp		default	10.0.0.1	10.0.0.2	

Establecemos VPN (cliente)



	ethernet3	Ethernet	1500	1538	0 bps	0 bps	0	0	0 b
	ethernet4	Ethernet	1500	1538	0 bps	0 bps	0	0	0 b
	ethernet5	Ethernet	1500	1538	0 bps	0 bps	0	0	0 b
R	sstp-out1	SSTP Client	1500		0 bps	0 bps	0	0	0 b
X	wlan1	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0 b

Establecemos VPN (cliente)



The screenshot shows the 'Address List' window in Mikrotik WinBox. The window title is 'Address List'. Below the title bar is a toolbar with icons for adding (+), deleting (-), checking (✓), unchecking (✗), printing (🖨), and filtering (🔍), along with a 'Find' search box. The main area contains a table with the following data:

	Address	Network	Interface	
D	10.0.0.2	10.0.0.1	sstp-out1	▼

```
[admin@MikroTik] > ping 10.0.0.1
  SEQ HOST                      SIZE TTL TIME  STATUS
  0 10.0.0.1                      56  64 156ms
  1 10.0.0.1                      56  64 160ms
  2 10.0.0.1                      56  64 159ms
sent=3 received=3 packet-loss=0% min-rtt=156ms avg-rtt=158ms max-rtt=160ms
```

Establecemos VPN (server)

New PPP Secret

Name: AP1

Password: AP1#

Service: sstp

Caller ID:

Profile: default

Local Address: 10.0.0.1

Remote Address: 10.0.0.2

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections | L2TP Secrets

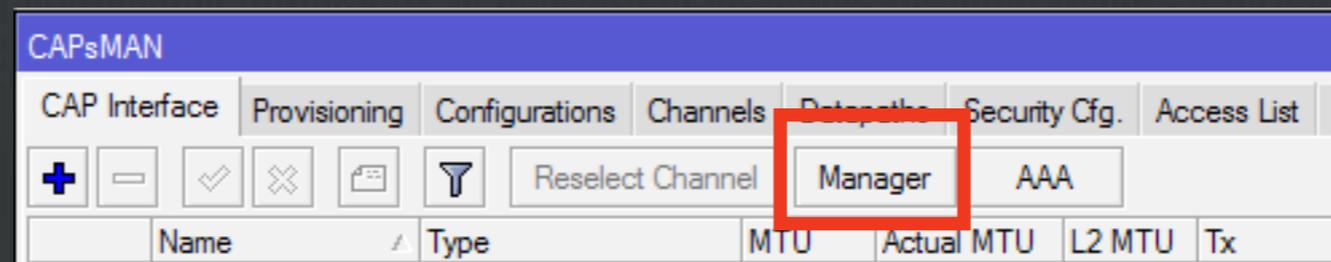
PPP Authentication&Accounting

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
AP1	AP1#	sstp		default	10.0.0.1	10.0.0.2	

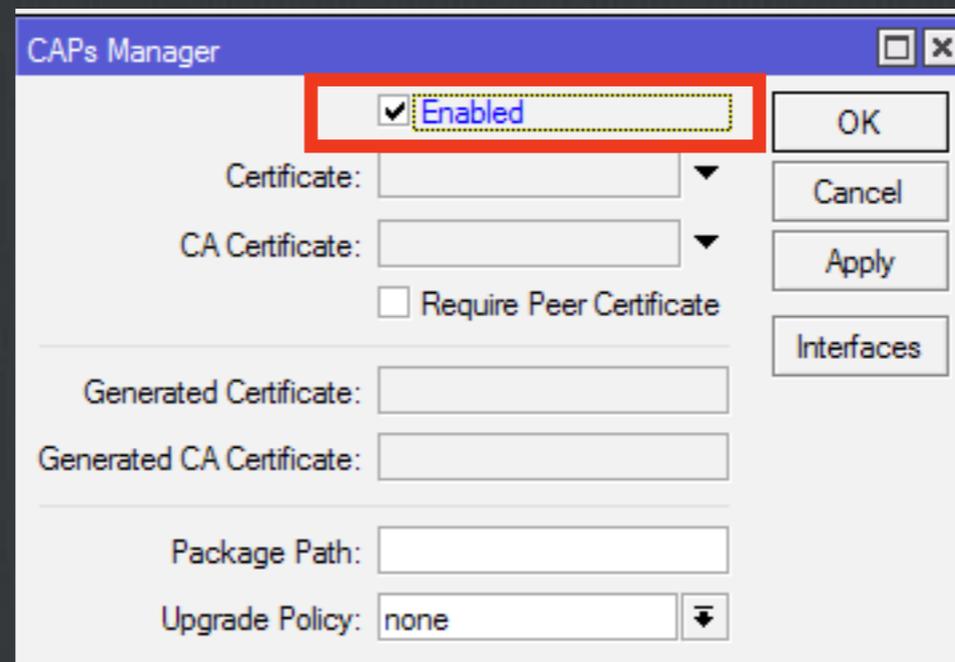
1 item

Configuramos CAPsMAN (VPS)

CAPsMAN



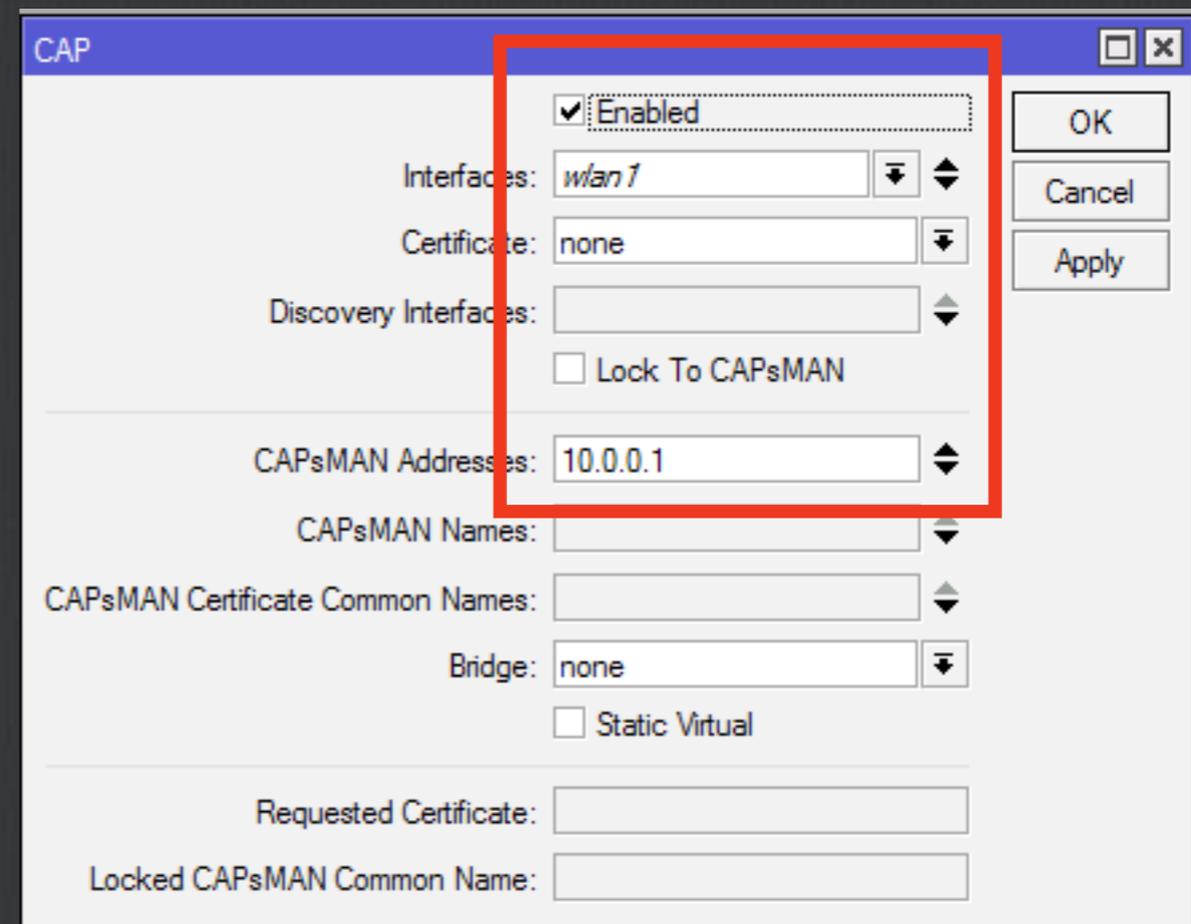
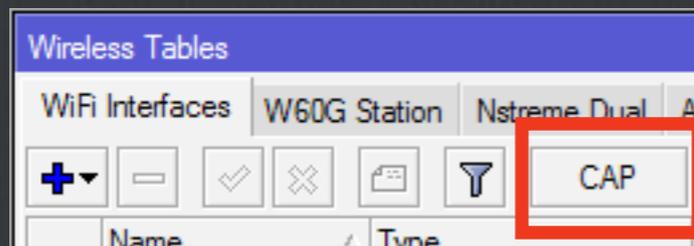
The screenshot shows the CAPsMAN configuration window with the following tabs: CAP Interface, Provisioning, Configurations, Channels, Data Paths, Security Cfg., and Access List. The Manager tab is highlighted with a red box. Below the tabs are several icons and buttons: a plus sign, a minus sign, a checkmark, a cross, a document icon, a funnel icon, a 'Reselect Channel' button, a 'Manager' button (highlighted with a red box), and an 'AAA' button. Below these is a table with columns: Name, Type, MTU, Actual MTU, L2 MTU, and Tx.



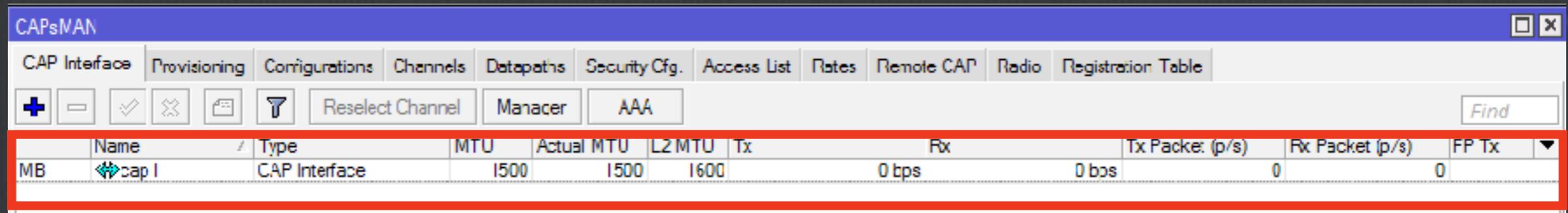
The screenshot shows the CAPs Manager dialog box with the following fields and controls:

- Enabled (highlighted with a red box)
- OK button
- Cancel button
- Apply button
- Interfaces button
- Certificate: [dropdown menu]
- CA Certificate: [dropdown menu]
- Require Peer Certificate
- Generated Certificate: [text field]
- Generated CA Certificate: [text field]
- Package Path: [text field]
- Upgrade Policy: none [dropdown menu]

Configuramos CAP



Establecemos conexión y personalizamos



The screenshot shows the CAPsMAN configuration window with the 'CAP Interface' tab selected. The table below lists the configured CAP interfaces.

	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
MB	cap 1	CAP Interface	1500	1500	1600		0 bps	0 bps	0	0

Establecemos conexión y personalizamos

Interface: wlan1

General Wireless Channel Rates Data Path Security Status ..

Configuration:

Mode:

SSID:

Hide SSID:

Load Balancing Group:

Distance:

Hw. Retries:

Hw. Protection Mode:

Frame Lifetime:

Disconnect Timeout:

Keepalive Frames:

Country:

Max Station Count:

Multicast Helper:

HT Tx Chains:

HT Rx Chains:

HT Guard Interval:

enabled running slave master bound inactive

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Touch
Scan ...
Reconnect Channel

CAPs Configuration (General)

Wireless Channel Rates Data Path Security

Name:

Mode:

SSID:

Hide SSID:

Load Balancing Group:

Distance:

Hw. Retries:

Hw. Protection Mode:

Frame Lifetime:

Disconnect Timeout:

Keepalive Frames:

Country:

Max Station Count:

Multicast Helper:

HT Tx Chains:

HT Rx Chains:

HT Guard Interval:

OK
Cancel
Apply
Comment
Copy
Remove

Establecemos conexión y personalizamos

Interface <cap1>

Wireless Channel

Channel: []

Frequency: 2442

Channel Width: []

Band: 2ghz b/g/n

Tx Power: []

Save Selected: []

Reselect Interval: []

Skip DFS Channels: []

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Refresh

Reselect Channel

enabled running slave master bound inactive

Interface <cap1>

General

Configuration: General

Mode: ad

SSID: Internet/Movl

Load Balancing Group: []

Distance: []

HTW Retries: []

HTW Protection Mode: []

Frame Lifetime: []

Disconnected Timeout: []

Keepalive Frames: []

Country: []

Max Station Count: []

Multicast Helper: []

HT Tx Chains: 0 1 2

HT Rx Chains: 0 1 2

HT Guard Interval: []

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Refresh

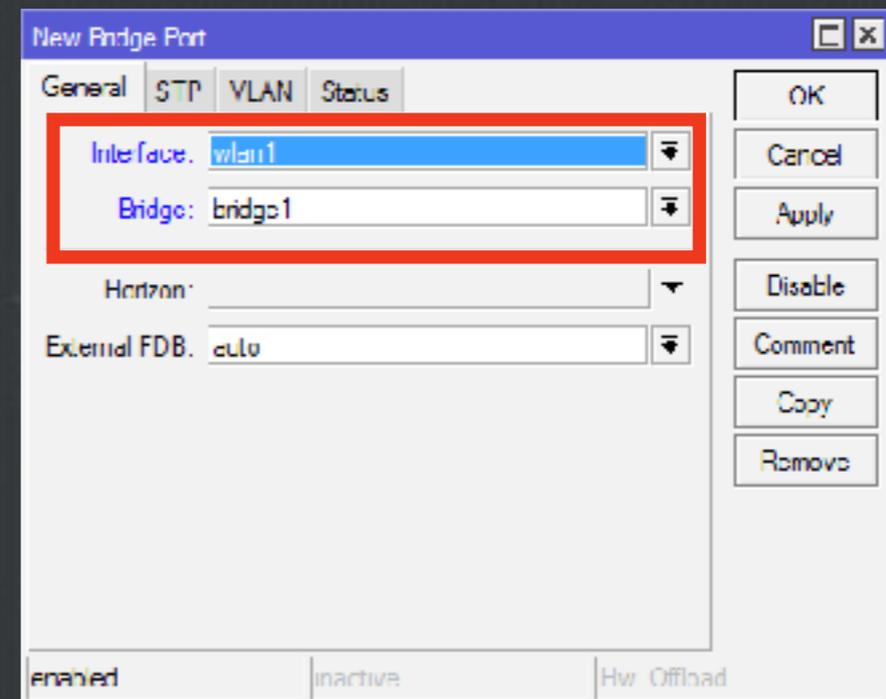
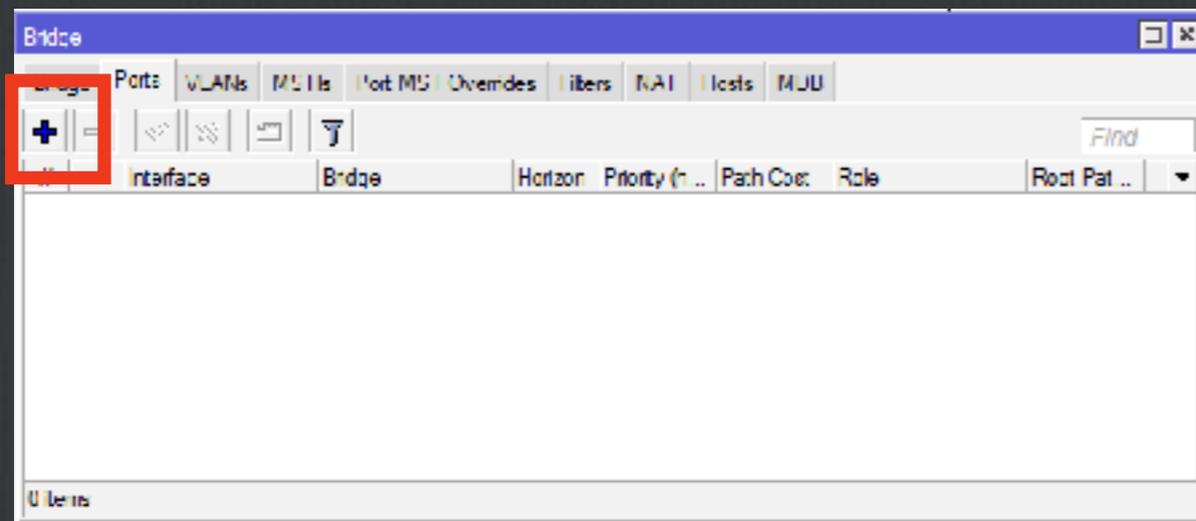
Reselect Channel

enabled running slave master bound inactive

Hotspot

- MUY IMPORTANTE:**
- La configuración del HS **DEBE** hacerse sobre un BRIDGE**
- Al ser la interfaz Wlan esclava del CAPsMAN no permitirá crearse ahí.**

Hotspot



Hotspot

- Generamos hotspot**
- Upgradeamos**
- Realizamos las configuraciones básicas (cambio de password, dns, etc)**
- Descargamos el paquete UserManager y lo instalamos**

Hotspot vinculamos RADIUS

New Radius Server

General Status

Service ppp login
 hotspot wireless
 dhcp ipsec

Called ID:

Domain:

Address: 10.0.0.1

Secret:

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

Accounting Backup

Realm:

Src. Address:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

enabled

Hotspot vinculamos router a RADIUS

Customer details

▲ Main

Login: admin

Password:

Parent: admin

Permissions: Owner

Public ID:

Public host:

Backup allowed:

▼ Access

▼ Private information

▼ Signup options

▼ Format

Save

Router details

▼ Main

Name: HS1

Owner: admin

IP address: 10.0.0.2

Shared secret: radius

Time zone: Parent time zone

Disabled:

Log events:

Authorization success

Authorization failure

Accounting success

Accounting failure

▼ Radius incoming

Save

Hotspot Creamos perfil

Limitation details ✕

▼ Main

Name:
Owner:

▼ Limits

Download:
Upload:
Transfer:
Uptime:

▼ Rate limits
▼ Constraints

Profile part ✕

▼ Period

Days: Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Time: -

▲ Limits

Mega

Hotspot creamos perfil

Profiles	Limitations
Profile: <input type="text" value="test1"/>	
Name: <input type="text" value="test1"/>	
Name for users: <input type="text"/>	
Owner: <input type="text" value="admin"/>	
Validity: <input type="text" value="1h"/>	
Starts: <input type="text" value="At first login"/>	
Price: <input type="text" value="0.00"/>	
Shared users: <input type="text" value="not used"/>	
<input type="button" value="Save profile"/> <input type="button" value="Remove profile"/>	
Profile limitations	
<input type="checkbox"/> Active	
<input type="checkbox"/> Always	
Constraints	
Download limit: 1024.0 KiB	
Upload limit: 128.0 KiB	
Uptime Limit: 1h	
<input type="button" value="Add new limitation"/>	<input type="button" value="Remove selected limitations"/>

User details

▼ Main

Username:

Password:

Disabled:

Owner: admin

▼ Constraints

▼ Wireless

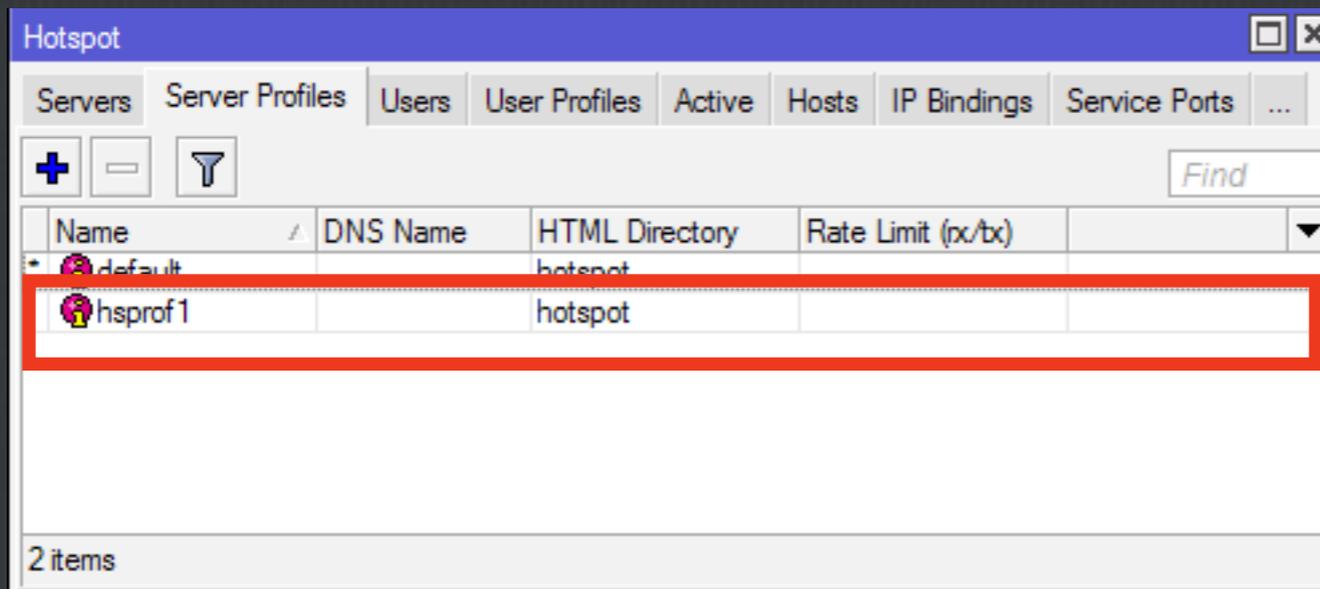
▼ Private information

▼ All profiles

▼ Actual profile

Hotspot

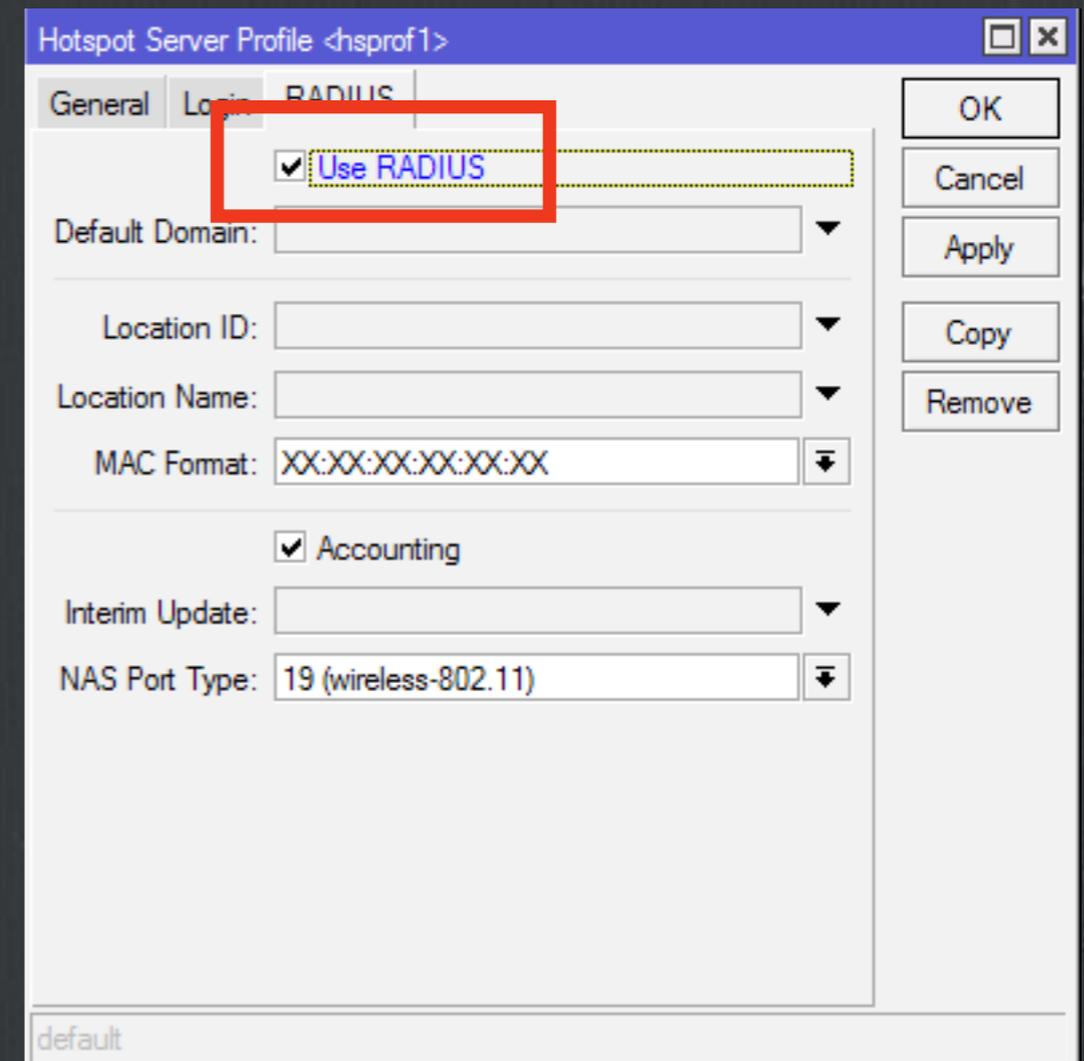
Usamos RADIUS en hs



The screenshot shows the 'Hotspot' application window with the 'Server Profiles' tab selected. A table lists two server profiles: 'default' and 'hsprof1'. The 'hsprof1' profile is highlighted with a red border.

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

2 items



The screenshot shows the 'Hotspot Server Profile <hsprof1>' configuration dialog box, specifically the 'RADIUS' tab. The 'Use RADIUS' checkbox is checked and highlighted with a red box. Other settings include 'Accounting' checked, 'Interim Update' set to an empty field, and 'NAS Port Type' set to '19 (wireless-802.11)'. The 'Default Domain', 'Location ID', and 'Location Name' fields are empty.

Hotspot Server Profile <hsprof1>

General Location **RADIUS**

Use RADIUS

Default Domain:

Location ID:

Location Name:

MAC Format: XX:XX:XX:XX:XX:XX

Accounting

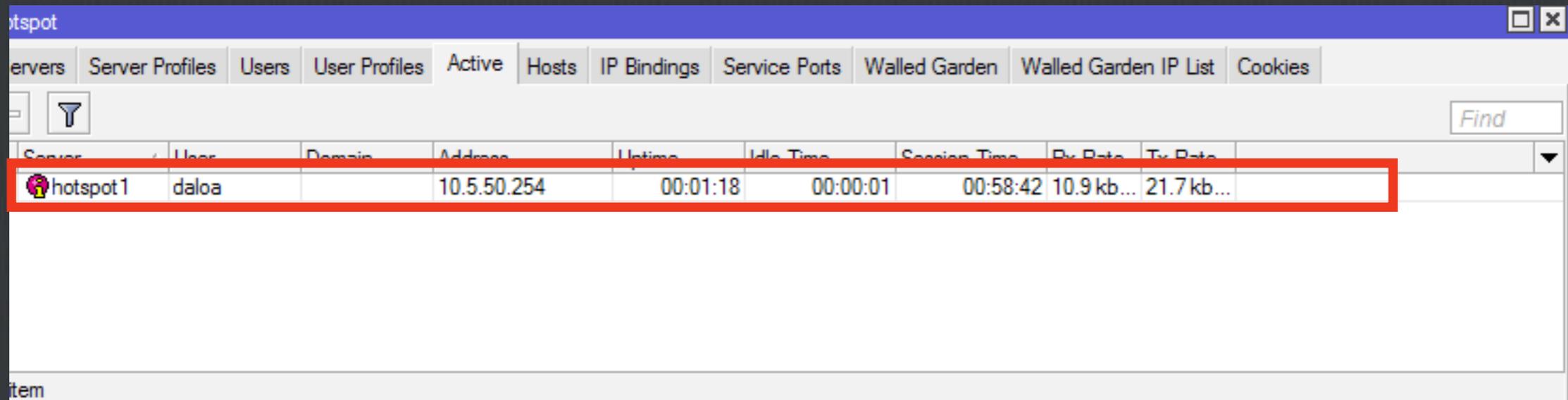
Interim Update:

NAS Port Type: 19 (wireless-802.11)

OK
Cancel
Apply
Copy
Remove

default

Hotspot



The screenshot shows a web-based interface for managing a hotspot. The title bar reads "Hotspot". Below the title bar is a navigation menu with tabs: Servers, Server Profiles, Users, User Profiles, Active, Hosts, IP Bindings, Service Ports, Walled Garden, Walled Garden IP List, and Cookies. The "Active" tab is selected. Below the navigation menu is a search bar with a "Find" button. The main content area is a table with the following columns: Server, User, Domain, Address, Uptime, Idle Time, Session Time, Rx Rate, and Tx Rate. The first row of the table is highlighted with a red box and contains the following data: Server: hotspot1, User: daloa, Domain: (empty), Address: 10.5.50.254, Uptime: 00:01:18, Idle Time: 00:00:01, Session Time: 00:58:42, Rx Rate: 10.9 kb..., and Tx Rate: 21.7 kb... Below the table, there is a label "Item" followed by a dropdown arrow.

Server	User	Domain	Address	Uptime	Idle Time	Session Time	Rx Rate	Tx Rate
hotspot1	daloa		10.5.50.254	00:01:18	00:00:01	00:58:42	10.9 kb...	21.7 kb...

¡Listo!



¿Dudas?

