

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.

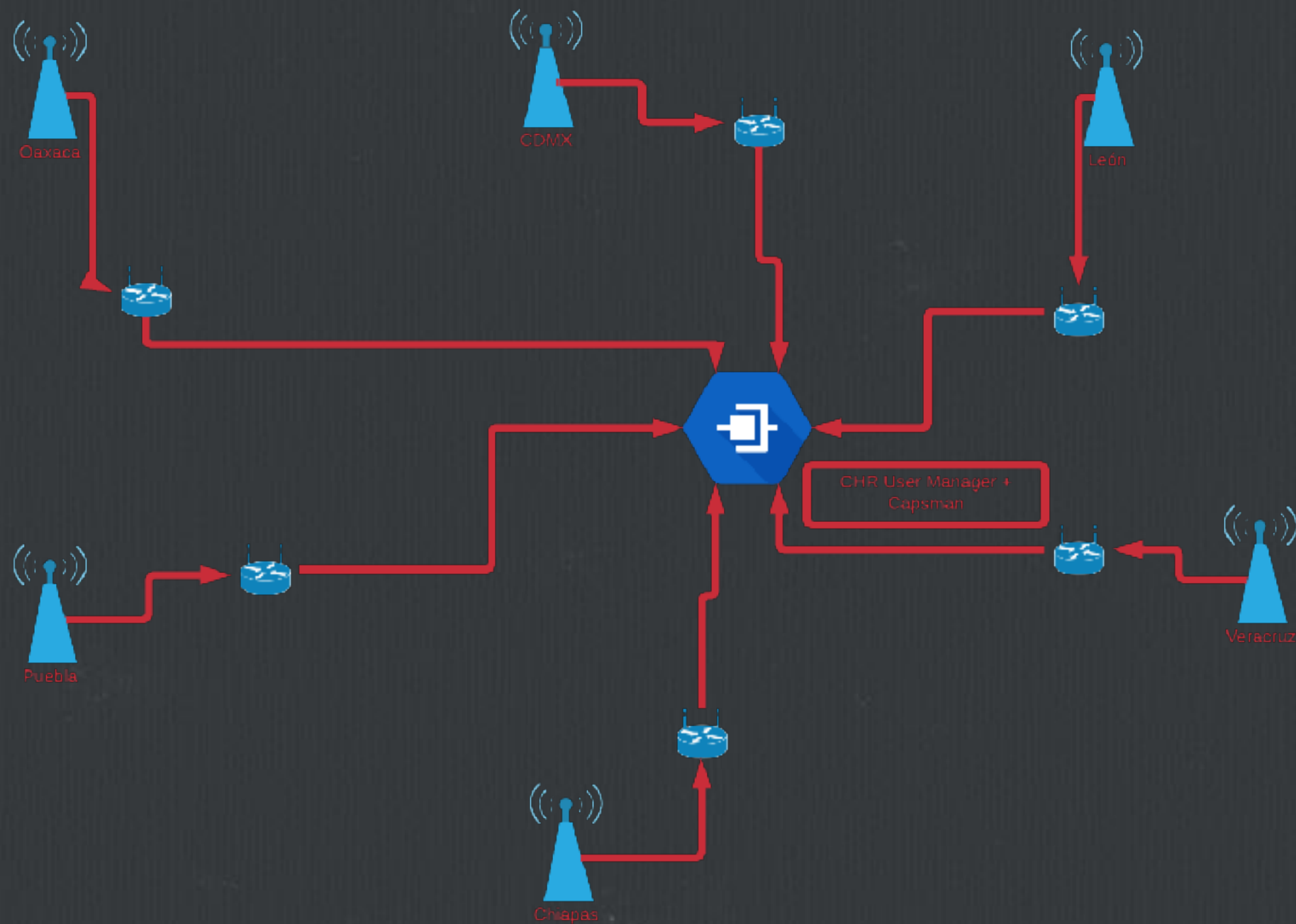
Qué es VPN

- **“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?



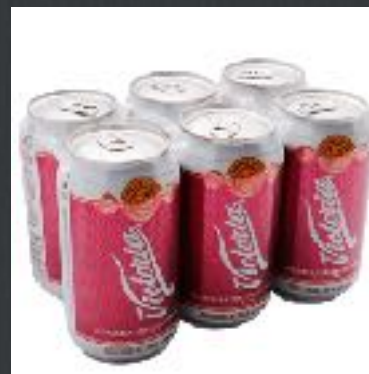
Licencia



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



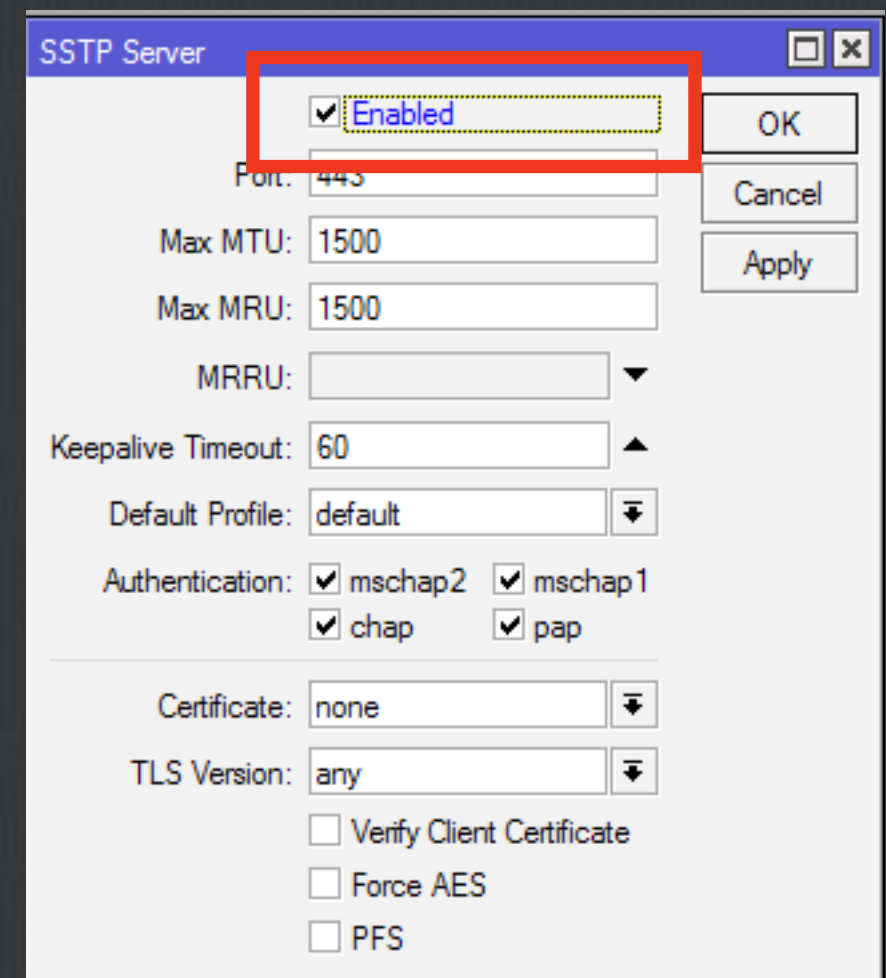
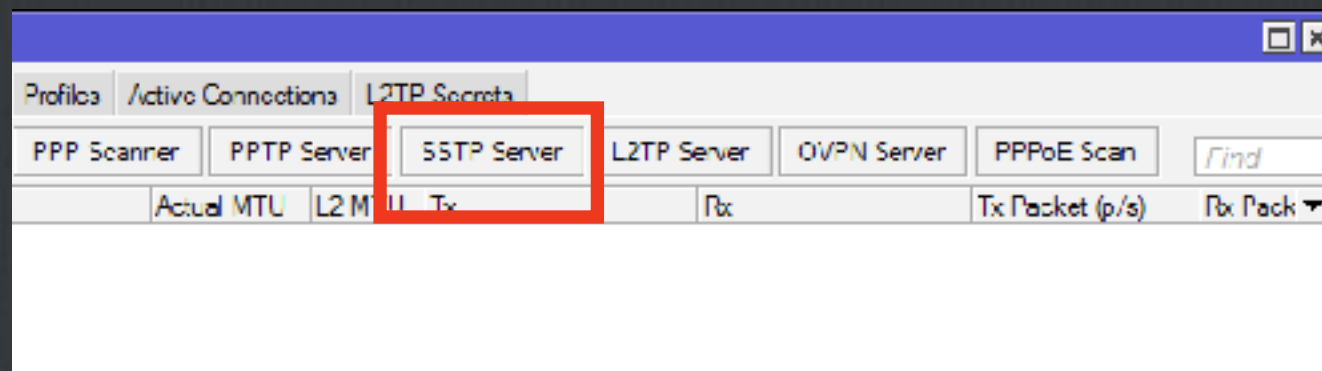
Instalamos RouterOS

- ☐ **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

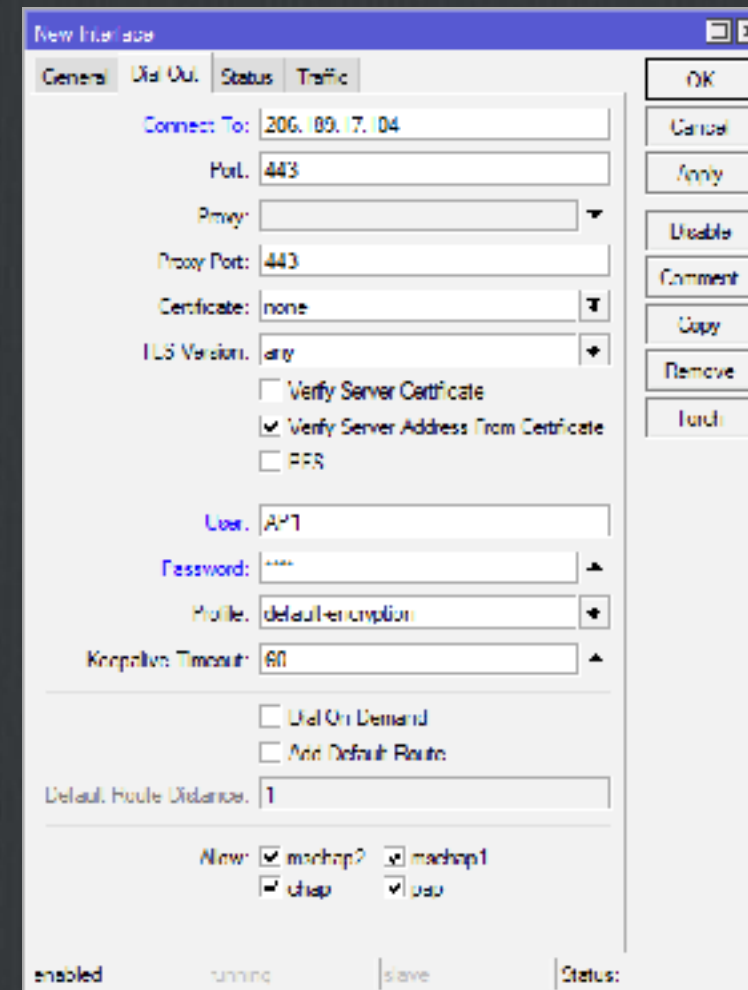
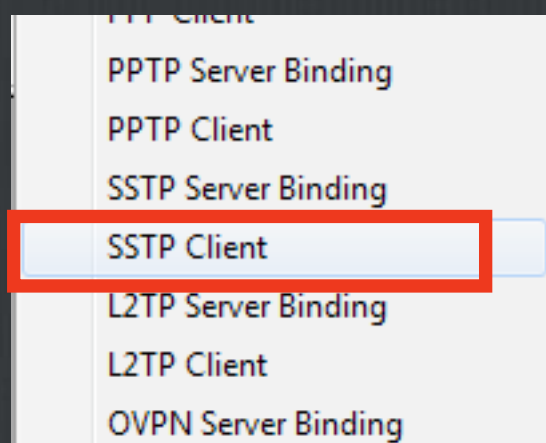
PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting

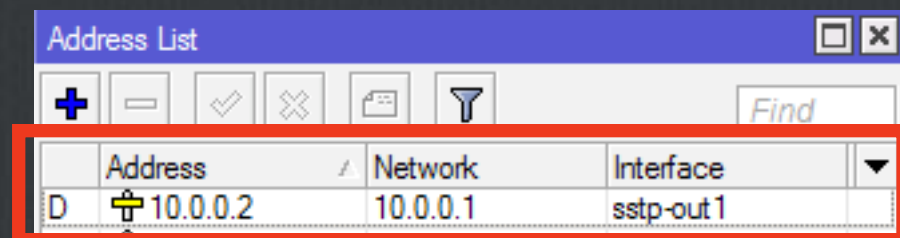
Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
AP1	AP1#	sstp		default	10.0.0.1	10.0.0.2	

Establecemos VPN (cliente)



	ether3	Ethernet	1500	1538	0 bps	0 bps	0	0	0 b
	ether4	Ethernet	1500	1538	0 bps	0 bps	0	0	0 b
	ether5	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. It features a toolbar with icons for adding, deleting, and filtering addresses. A table below contains one entry with a red border. The entry has a checkbox, an address field with a cross icon, a network field, and an interface field.

	Address	Network	Interface
☒	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

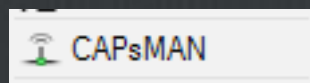
Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

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

CAP Interface Provisioning Configurations Channels **Datapaths** Security Cfg. Access List

+ - ✓ ✗ [Icon] Reselect Channel **Manager** AAA

Name	Type	MTU	Actual MTU	L2 MTU	Tx
------	------	-----	------------	--------	----

CAPs Manager

☒ **Enabled**

Certificate: [Dropdown]

CA Certificate: [Dropdown]

☐ Require Peer Certificate

Generated Certificate: [Text Box]

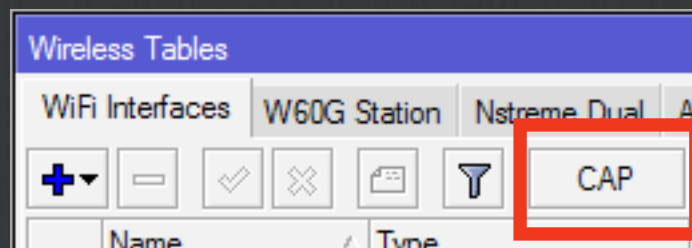
Generated CA Certificate: [Text Box]

Package Path: [Text Box]

Upgrade Policy: none [Dropdown]

OK Cancel Apply Interfaces

Configuramos CAP



The 'CAP' configuration dialog box is shown with the following fields and options:

- ☒ Enabled
- Interfaces: wlan1
- Certificate: none
- Discovery Interfaces:
- ☐ Lock To CAPsMAN
- CAPsMAN Addresses: 10.0.0.1
- CAPsMAN Names:
- CAPsMAN Certificate Common Names:
- Bridge: none
- ☐ Static Virtual
- Requested Certificate:
- Locked CAPsMAN Common Name:

Buttons: OK, Cancel, Apply

Establecemos conexión y personalizamos

CAPsMAN										
CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table										
+ - ✓ ✗ [Icon] [Icon] Reselect Channel Manager AAA Find										
	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 Datapath 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:

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

enabled running slave master bound inactive

CAPs Configuration: General

Wireless Channel Rates Datapath Security

Name: General

Mode:

SSID: InternetMovil

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 Info Advanced Security Status Tools

Channel:

Frequency: 2442

Channel Width:

Band: 2ghz b/g/n

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Refresh

Scan

Reselect Channel

enabled running slave master bound inactive

Interface <cap1>

General Mode Advanced Security Status Tools

Configuration: General

Mode: ad

SSID: InternetMovil

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Refresh

Scan ...

Reselect Channel

Load Balancing Group:

Distance:

HTW Retries:

HTW Protection Mode:

Frame Lifetime:

Disconnect Timeout:

Keepalive Frames:

Country:

Max Station Count:

Multicast Helper:

HT Tx Chains: ☒ 0 ☒ 1 ☐ 2

HT Rx Chains: ☒ 0 ☒ 1 ☐ 2

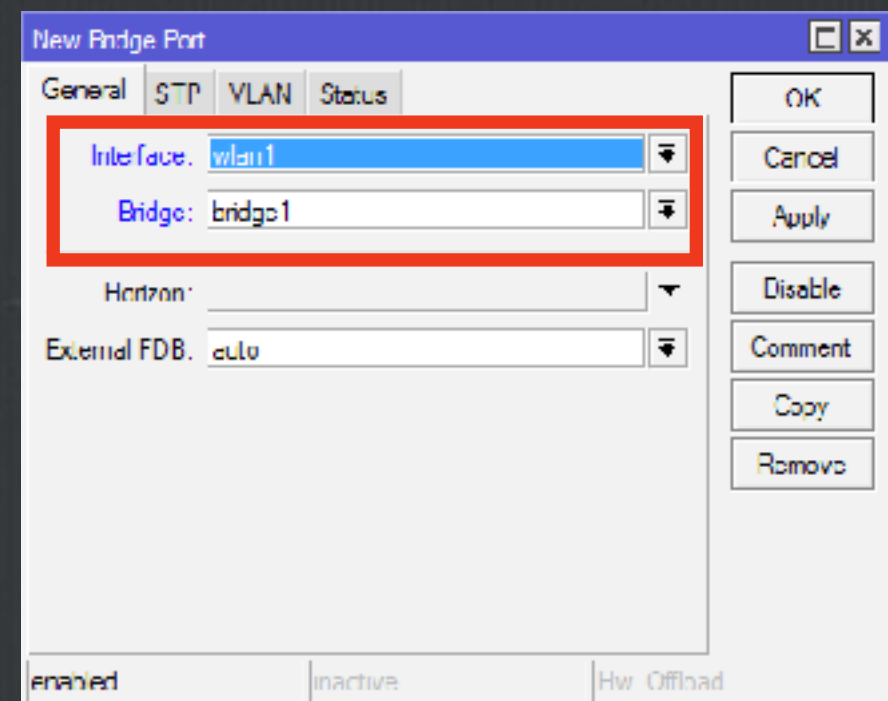
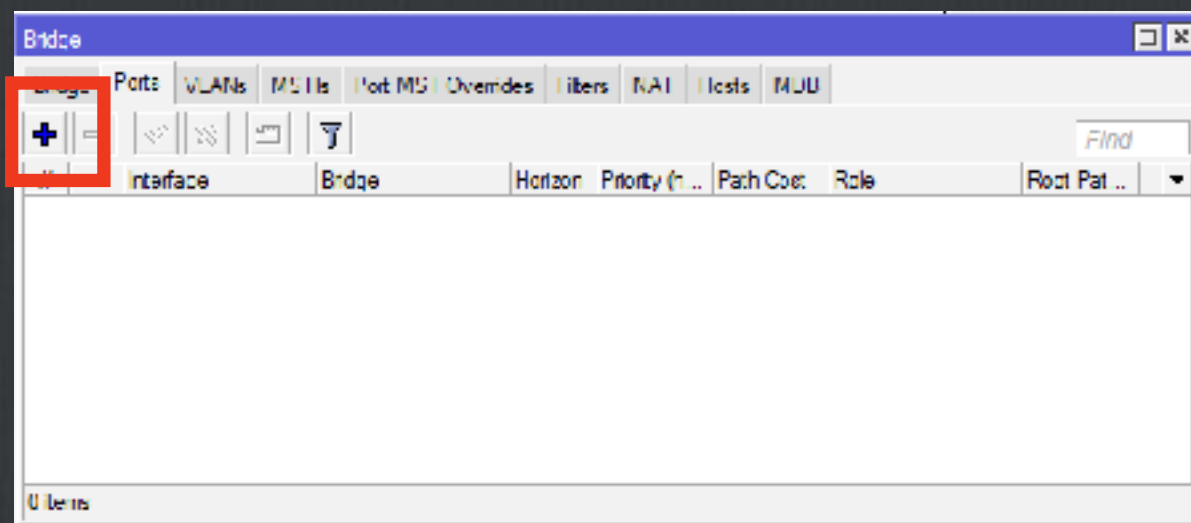
HT Guard Interval:

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 ☒ hotspot ☐ login ☐ 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 [X]

▲ Main

Login: admin

Password: [REDACTED]

Parent: admin

Permissions: Owner

Public ID:

Public host:

Backup allowed: ☒

▼ Access

▼ Private information

▼ Signup options

▼ Format

Save

Router details [X]

▼ 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:

Mega

Owner:

admin

▼ Limits

Download:

1M

Upload:

128K

Transfer:

0B

Uptime:

1h

▼ Rate limits

▼ Constraints

Save

Profile part

▼ Period

Days:

☒ Sunday

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

Time:

0:00:00

-

23:59:59

▲ Limits

☒ Mega

New limit

Cancel

Add

Hotspot creamos perfil

Profiles	Limitations
Profile: Test1	
Name: Test1	
Name for users:	
Owner: admin	
Validity: 1h	
Starts: At first upon	
Price: 0.00	
Shared users: not used	
Save profile Remove profile	
Profile limitations	
☐	Active
☐	Always
Constraints	
Download limit: 1024.0 KiB	
Upload limit: 128.0 KiB	
Uptime Limit: 1h	
Add new limitation Remove selected limitation	

User details

▼ Main

Username:

Password:

Disabled: ☐

Owner: admin

▼ Constraints

▼ Wireless

▼ Private information

▼ All profiles

▼ Actual profile

Hotspot

Usamos RADIUS en hs

Hotspot

Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service Ports ...

+ - Filter Find

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

2 items

Hotspot Server Profile <hsprof1>

General Location **RADIUS**

☒ Use RADIUS

Default Domain:

Location ID:

Location Name:

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

☒ Accounting

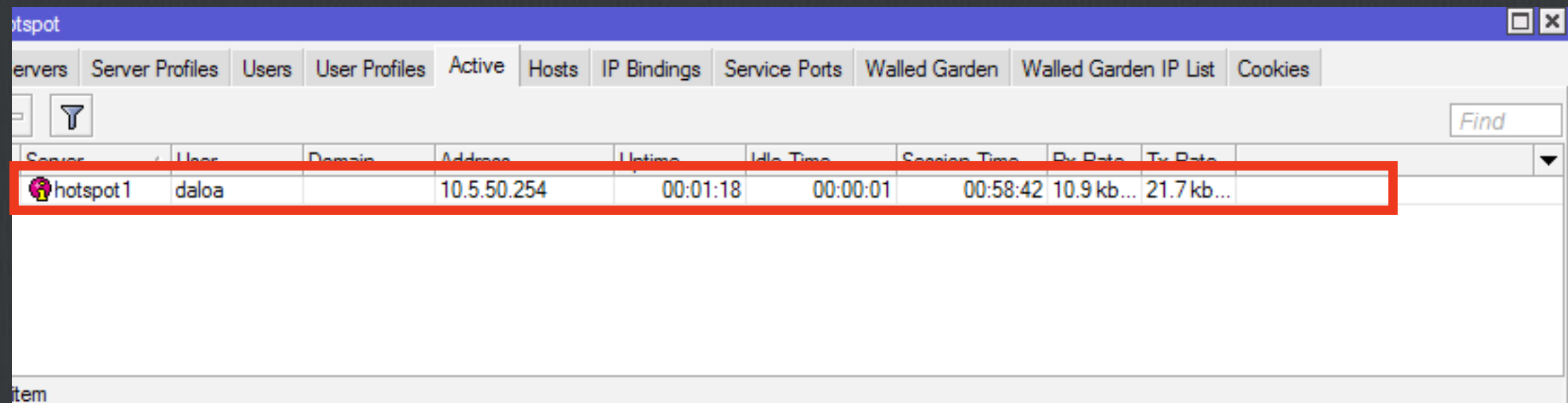
Interim Update:

NAS Port Type: 19 (wireless-802.11)

OK Cancel Apply Copy Remove

default

Hotspot



The screenshot shows the Mikrotik WinBox interface for the Hotspot Manager. The 'Active' tab is selected, displaying a table of active users. The first row is highlighted with a red border. The table columns are: Server, User, Domain, Address, Uptime, Idle Time, Session Time, Rx Rate, and Tx Rate. The first row contains the following data: hotspot1, daloa, (empty), 10.5.50.254, 00:01:18, 00:00:01, 00:58:42, 10.9 kb..., and 21.7 kb....

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?

