

Tips para Principiantes + HotSpot (Seguridad, User Manager)

Armando Cartagena
ITDES



23 de Julio de 2018

Tegucigalpa

Honduras



- ✓ Nombre: Jose Armando Cartagena Mendoza.
- ✓ Pasante Universitario.
- ✓ Estudiante del Instituto Técnico Departamental “Espíritu del Siglo”. (2011-2017)
- ✓ Experiencia desde 2015.



Cartagenam13



@Cartagenam13



+504 9511-5263



Cartagenam13@gmail.com



- ✓ Fundado en 1930.
- ✓ Institución Pública.
- ✓ 65 Docentes.
- ✓ Colegio - Técnico Insignia Del Departamento De Colon.
- ✓ Oferta Educativa:
 - 5 BTP Y 1 BCH.
 - Ciclo Básico Técnico.





Tips Básicos-Principiante

MikroTik® (RouterOS y Routerboard) nos ofrece herramientas muy poderosa y sobre todo demasiado amplias, pero como en todos los casos, hay que saber configurarlo correctamente.

- ✓ Mostrar los descuidos mas comunes.
- ✓ Demostrar que con unos pocos pasos se pueden mejorar las configuraciones, incrementando la seguridad y reduciendo las posibles fallas.



✓ Descuidos en los accesos por defecto, dejando la puerta completamente abierta para ingresar al router con las credenciales por defecto.

Usuario	Contraseña
Admin	
Admin	1234
User1	

✓ Casos en que a User1 le otorgamos permiso solo de lectura y Admin con permisos Full

The screenshot shows the Mikrotik WinBox interface. The 'User List' window is open, displaying a table of users and their policies. The 'read' user is selected. A 'Group <read>' configuration dialog is also open, showing the 'Policies' section with a red arrow pointing to the 'read' policy checkbox, which is checked.

Name	Policies	Skin
full	local telnet ssh ftp reboot read write policy test winbox password web sniff sensitive api romon dude tikapp	default
read	local telnet ssh reboot read test winbox password web sniff sensitive api romon tikapp	default
write	local telnet ssh reboot read write test winbox password web sniff sensitive api romon tikapp	default

Group <read> configuration:

Name: read

Policies:

- local
- telnet
- ssh
- ftp
- reboot
- read
- write
- policy
- test
- winbox
- password
- web
- sniff
- sensitive
- api
- romon
- dude
- tikapp

Skin: default



admin@08:00:27:B8:17:16 (LABORATORIO DE INFORMATICA) - WinBox v6.40.8 on x86 (x86)

Session Settings Das Auto Upgrade

Safe Mode

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- Dude
- KVM

- Auto Upgrade
- Certificates
- Clock
- Console
- Disks
- Drivers
- GPS
- Health
- History
- Identity
- LCD
- LEDs
- License
- Logging
- NTP Client
- NTP Server
- Packages
- Password
- Ports
- Reboot
- Reset Configuration
- Resources
- Routerboard

Identity

Identity: RMATICA

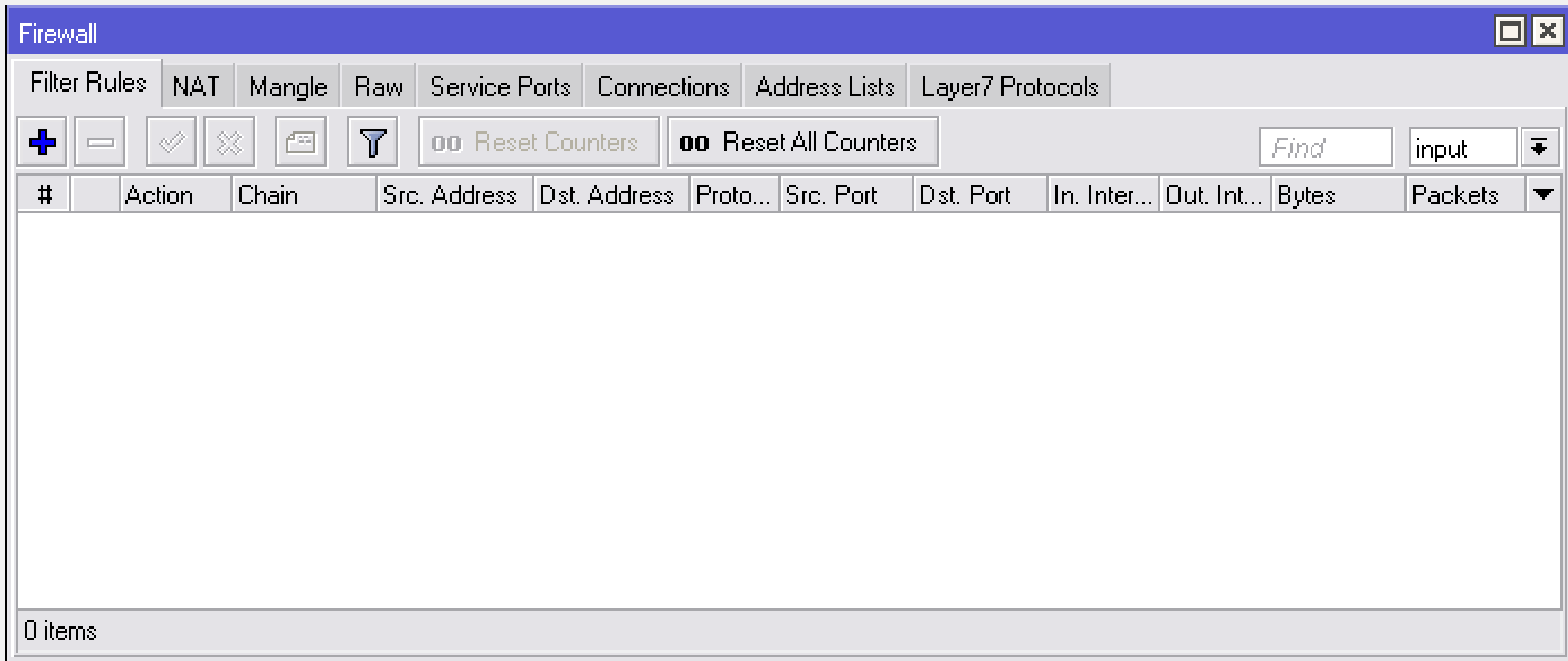
OK

Cancel

Apply



- ✓ Una de las primeras acciones a realizar en todo equipo es poner al menos un pequeño firewall para prevenir los ataques más comunes.





Los ataques tienen principalmente 2 objetivos:

- ✓ Tomar el control del router.
- ✓ Provocar una denegación de servicios (CPU 100%, consumo de todo el ancho de banda, etc.)

Principales problemas:

- ✓ Ataques por Fuerza Bruta
- ✓ Ataque al DNS

Ataque por Fuerza Bruta

```
rcaire@suyai /home/rcaire]% python3 mkbrutus.py -t 192.168.0.11 -d dictionary2.txt

Mikrotik RouterOS Bruteforce Tool 1.0.0
Ramiro Caire (@rcaire) & Federico Massa (@fgmassa)

[*] Starting bruteforce attack...
-----
[-] Trying with default credentials on RouterOS...

[-] Default RouterOS credentials were unsuccessful, trying with user's password list...

[-] Trying User: admin Password: 1234
[-] Trying User: admin Password: 12345
[-] Trying User: admin Password: 123456
[-] Trying User: admin Password: 1234567
[-] Trying User: admin Password: 12345678
[-] Trying User: admin Password: porsche
[-] Trying User: admin Password: dragon
[-] Trying User: admin Password: qwerty
[-] Trying User: admin Password: 696969
[-] Trying User: admin Password: mustang
[-] Trying User: admin Password: letmein
[-] Trying User: admin Password: baseball
[-] Trying User: admin Password: master
[-] Trying User: admin Password: michael
[-] Trying User: admin Password: football
[-] Trying User: admin Password: shadow
[-] Trying User: admin Password: monkey
[-] Trying User: admin Password: abc123
[-] Trying User: admin Password: jordan
[-] Trying User: admin Password: pass
[-] Trying User: admin Password: password
[-] Trying User: admin Password: P@ssw0rd
[+] Login successful!!! User: admin Password: P@ssw0rd
```

Ataque por DNS

Torch (Running)

Basic: Interface: wan, Entry Timeout: 00:00:03

Collect: Src. Address, Dst. Address, MAC Protocol, Protocol, Src. Address6, Dst. Address6, Port, VLAN Id

Filters: Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Src. Address6: ::/0, Dst. Address6: ::/0, MAC Protocol: all, Protocol: any, Port: dns, VLAN Id: any

Et...	Prot...	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx Pack
800 (ip)		115.238.184.126:12633	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:26701	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:43549	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:16379	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:17231	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.110:20153	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:50075	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:55531	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:62555	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:34379	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:48267	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:58126	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.110:24377	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:26973	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:43181	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:48380	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:14222	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:17981	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:49099	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:9467	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:42021	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:62197	:53 (dns)		6.0 kbps	344 bps	0	0

Total Tx: 724.7 kbps | Total Rx: 176.6 kbps | Total Tx Packet: 2 | Total Rx Packet: 2



- ✓ Deshabilita Servicios innecesarios, y proteger los demás con reglas de *firewall* o especificar.

	Name	Port	Available From	Certificate
<input checked="" type="checkbox"/>	api	8728		
<input checked="" type="checkbox"/>	api-ssl	8729		none
<input checked="" type="checkbox"/>	ftp	21		
<input checked="" type="checkbox"/>	ssh	22		
<input checked="" type="checkbox"/>	telnet	23		
<input checked="" type="checkbox"/>	winbox	8291		
<input checked="" type="checkbox"/>	www	80		
<input checked="" type="checkbox"/>	www-ssl	443		none

	Name	Port	Available From
<input checked="" type="checkbox"/>	api	8728	
<input checked="" type="checkbox"/>	api-ssl	8729	
<input checked="" type="checkbox"/>	ftp	21	
<input checked="" type="checkbox"/>	ssh	22	
<input checked="" type="checkbox"/>	telnet	23	
<input checked="" type="checkbox"/>	winbox	8291	192.168.10.0/24
<input checked="" type="checkbox"/>	www	80	
<input checked="" type="checkbox"/>	www-ssl	443	

Puerto	Protocolo	Comentario
20,21	TCP	FTP
22	TCP	SSH, SFTP
23	TCP	TELNET
53	TCP/UDP	DNS
80	TCP	HTTP
123	UDP	NTP
161,162	UDP	SNMP
179	TCP	BGP
443	TCP	HTTPS //(HotSpot)

Puerto	Protocolo	Comentario
2000	TCP	Bandwidth Server
3128,8080	TCP	WebProxy
5678	UDP	Neighbour Discovery
8291	TCP	WinBox
8728	TCP	API
1701	UDP	L2tP
1723	TCP	PPTP
1812,1813	UDP	User Manager



✓ NUNCA actualizar solo porque si

✓ Leé

The screenshot shows the MikroTik website's 'Software' section. The 'Changelogs' link is highlighted with a red dashed box. Below it, the 'Release 6.42.4' page is displayed, dated 2018-06-19. The page content includes a list of changes for this release.

Release 6.42.4 2018-06-19

What's new in 6.42.4 (2018-Jun-15 14:14):

- *) bridge - allow to make changes for bridge port when it is interface list;
- *) bridge - fixed FastPath for bridge master interfaces (introduced in v6.42);
- *) certificate - fixed "add-scep" template existence check when signing certificate;
- *) chr - fixed adding MSTI entries;
- *) chr - fixed boot on hosts older than Windows Server 2012 when running CHR on Hyper-V;
- *) chr - fixed various network hang scenarios when running CHR on Hyper-V;
- *) console - fixed script permissions if script is executed by other RouterOS service;
- *) dhcpv4-server - fixed DHCP server that was stuck on invalid state;
- *) health - changed "PSU-Voltage" to "PSU-State" for CRS328-4C-20S-4S+;
- *) health - fixed incorrect PSU index for CRS328-4C-20S-4S+;
- *) ipsec - improved reliability on IPsec hardware encryption for RB1100Dx4;
- *) kidcontrol - fixed dynamically created firewall rules order;
- *) led - added "dark-mode" functionality for hEX S and SXTsq 5 ac devices;
- *) led - fixed CCR1016-12S-1S+ LED behaviour after Netinstall (introduced in v6.41rc58);
- *) led - use routers uptime as a starting point when turning off LEDs if option was not enabled on boot;
- *) ppp - fixed "hunged up" grammar to "hung up" within PPP log messages;
- *) quickset - added missing wireless "channel-width" settings;



- ✓ No dejar el usuario como “admin” en el HotSpot sin contraseña

Hotspot Setup

Create local HotSpot user

Name of Local HotSpot User: admin

Password for the User:

Back Next Cancel

- ✓ El bypass oculta el HotSpot, pero no controla el ancho de banda!

Hotspot IP Binding <192.168.10.15>

MAC Address:

Address: 192.168.10.15

To Address:

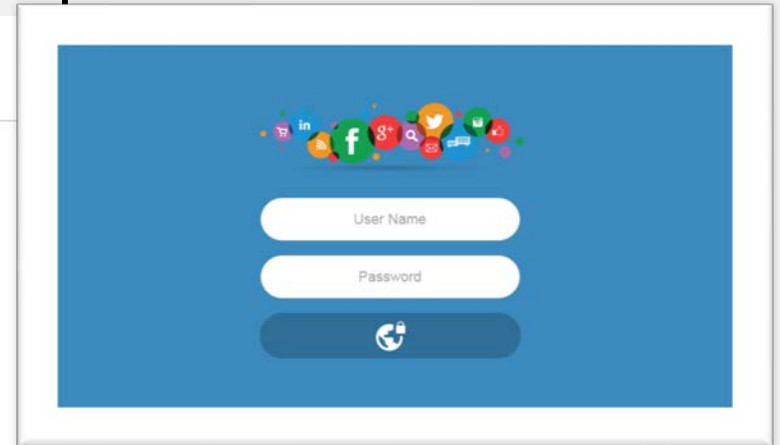
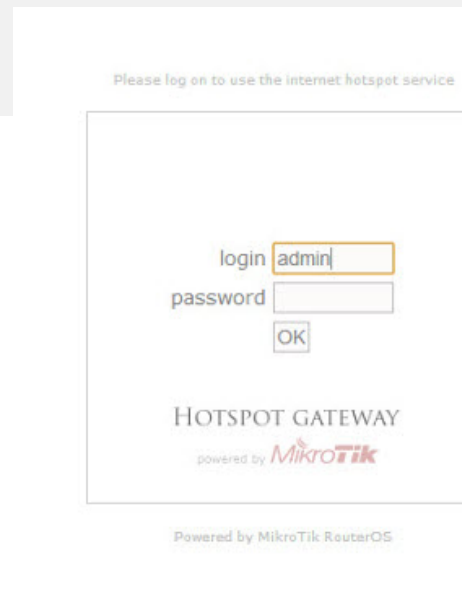
Server: all

Type: bypassed

Integración de HotSpot con User Manager

¿Que es un HotSpot?

- ✓ Sistema de autenticación de clientes mayormente por un USUARIO Y CONTRASEÑA al abrir el navegador.
- ✓ Comúnmente utilizados para dar acceso en lugares públicos.





¿Que es UserManager ?

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

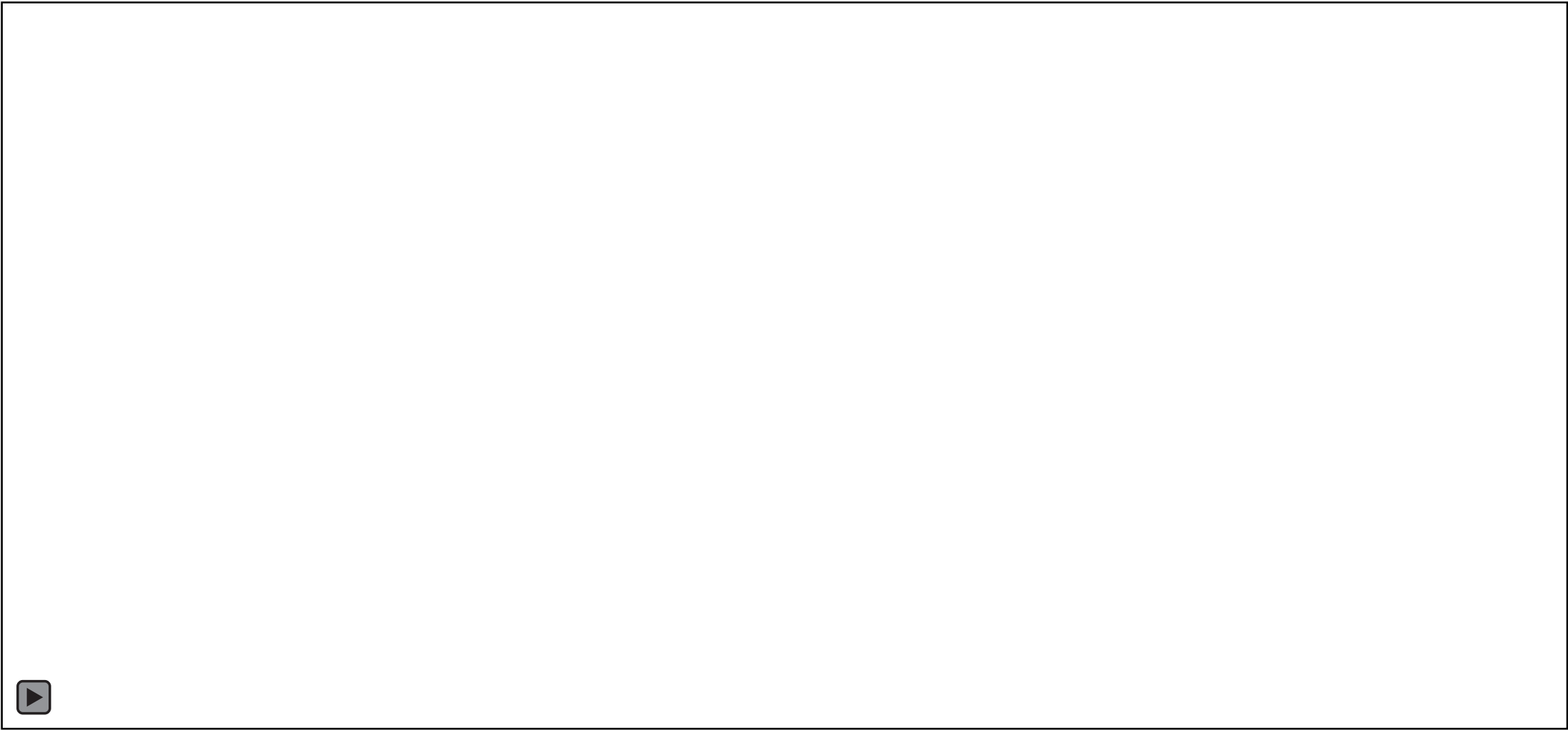
Ventajas de utilizar UserManager

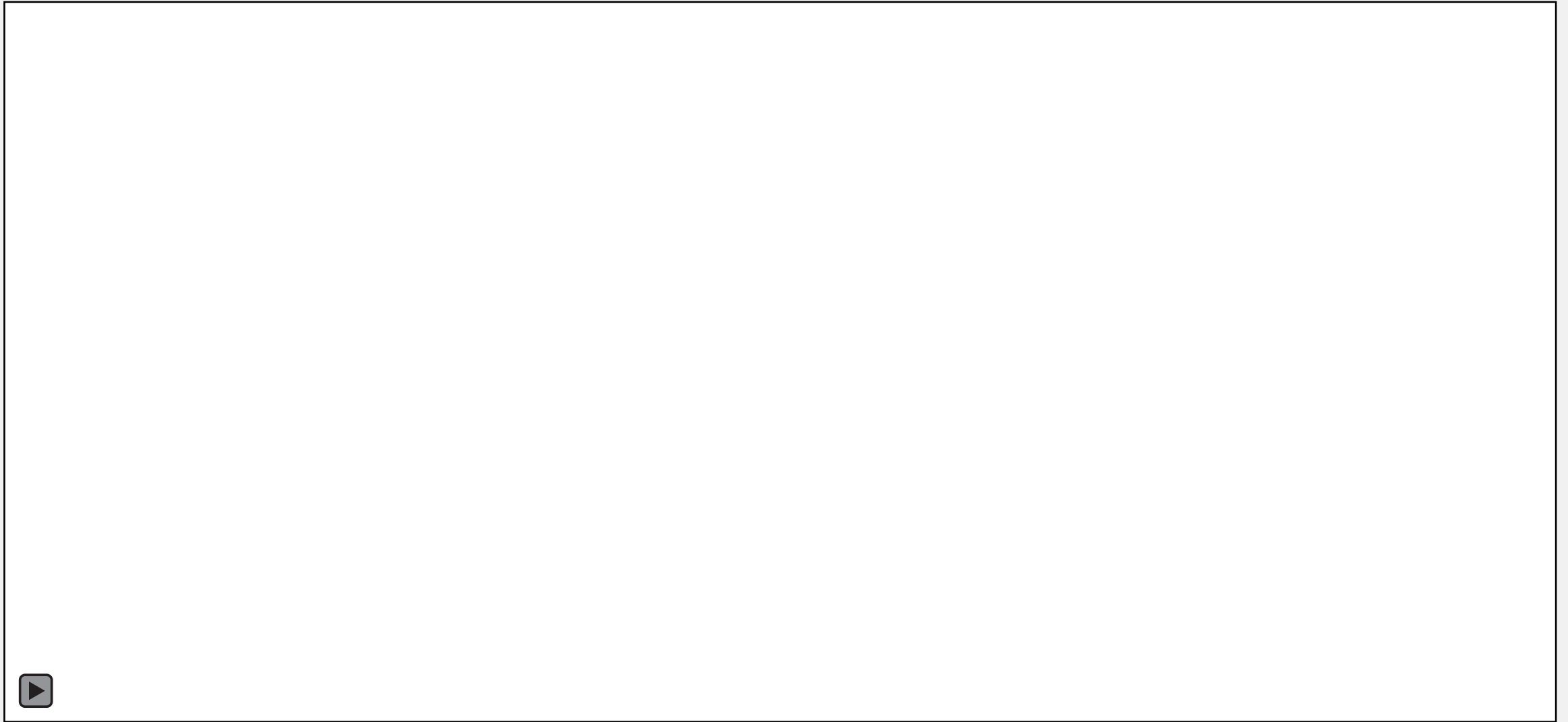
- ✓ Sin costo adicional.
- ✓ Administración centralizada de toda la red.
- ✓ Única base de datos (o réplicas) aislada de la configuración del server principal.
- ✓ Permite crear usuarios por lotes y generar Boucher o exportarlos a un archivo en CSV para una posterior impresión de tarjetas prepagas.





- ✓ Se debe tener la misma versión de RouterOS y del paquete UserManager.
- ✓ Funciona en arquitectura X86, MIPS, PowerPC y Tile.
- ✓ Hardware Mínimo: 32MB de RAM y 2MB de HDD.
- ✓ Software: RouterOS.
- ✓ Licencia MikroTik RouterOS de UserManager.
 - Nivel 3: 10 sesiones activas.
 - Nivel 4: 20 sesiones activas.
 - Nivel 5: 50 sesiones activas.
 - Nivel 6: sesiones ilimitadas.









Paso 1: Configuración Básica De Wifi

- ✓ Después de crear nuestra red WIFI, configuramos de la misma **AP1 LAB 1 Y AP2 LAB**, configuramos de la misma forma, de tal manera que no tenga que pedir autenticación (Password) al momento de registrarnos.

The image shows two screenshots of the Mikrotik Router configuration interface for the wlan1 interface. The top screenshot shows the configuration for AP1 LAB 1, and the bottom screenshot shows the configuration for AP2 LAB.

Interface <wlan1>

General | **Wireless** | HT | HT MCS | WDS | Nstreme | Status | Traffic

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: LAB 1

Scan List: default

Wireless Protocol: 802.11

Security Profile: default

WPS Mode: push

Bridge Mode: enable

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate:

Default Client Tx Rate:

De

De

Interface <wlan1>

General | **Wireless** | HT | HT MCS | WDS | Nstreme | Status | Traffic

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: LAB 2

Scan List: default

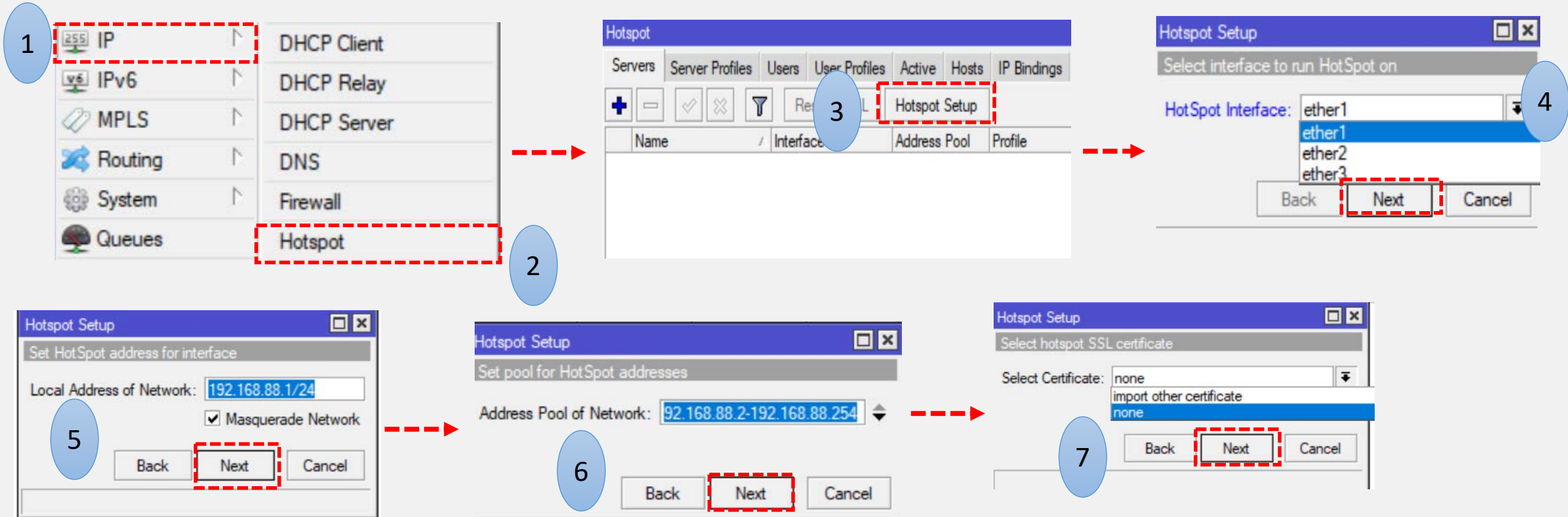
Wireless Protocol: 802.11

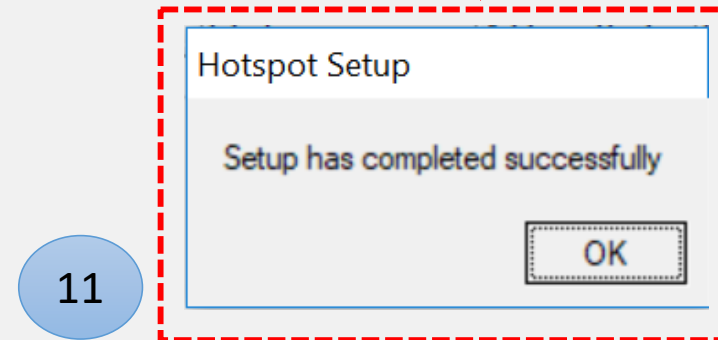
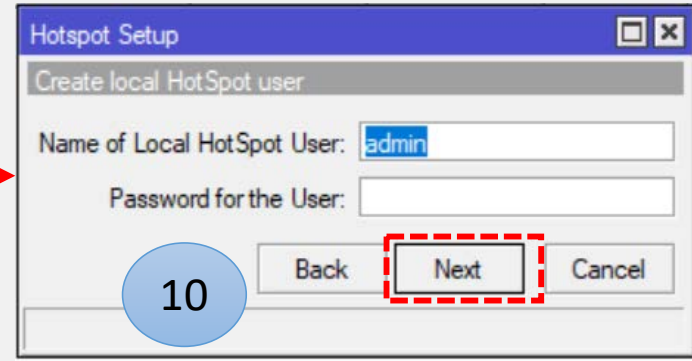
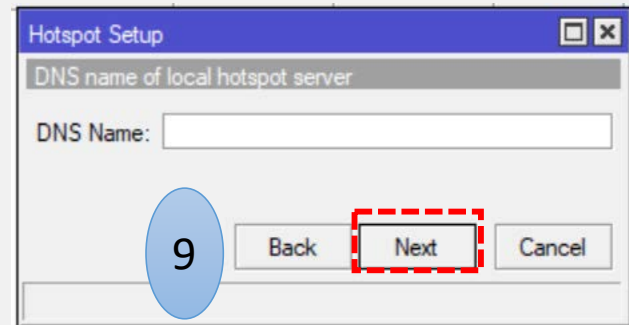
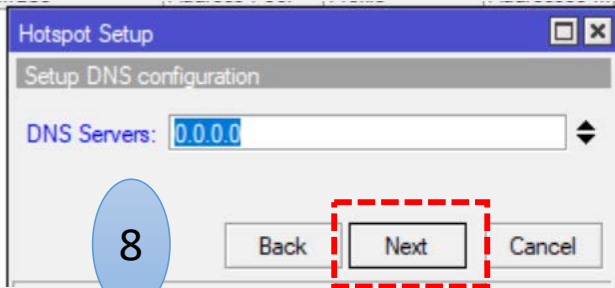
Security Profile: default

WPS Mode: push button

Bridge Mode: enabled

Paso 2: Configuración Básica De HotSpot







Paso 3: Configuración del User Manager

admin@4C:5E:0C:60:5A:8D (MikroTik) - WinBox v6.40.8 on RB750 (mipsbe)

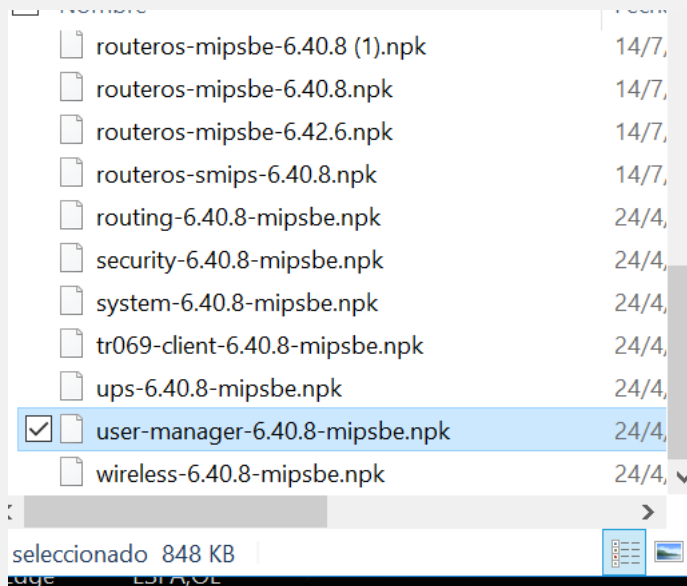
1

<https://mikrotik.com/download>

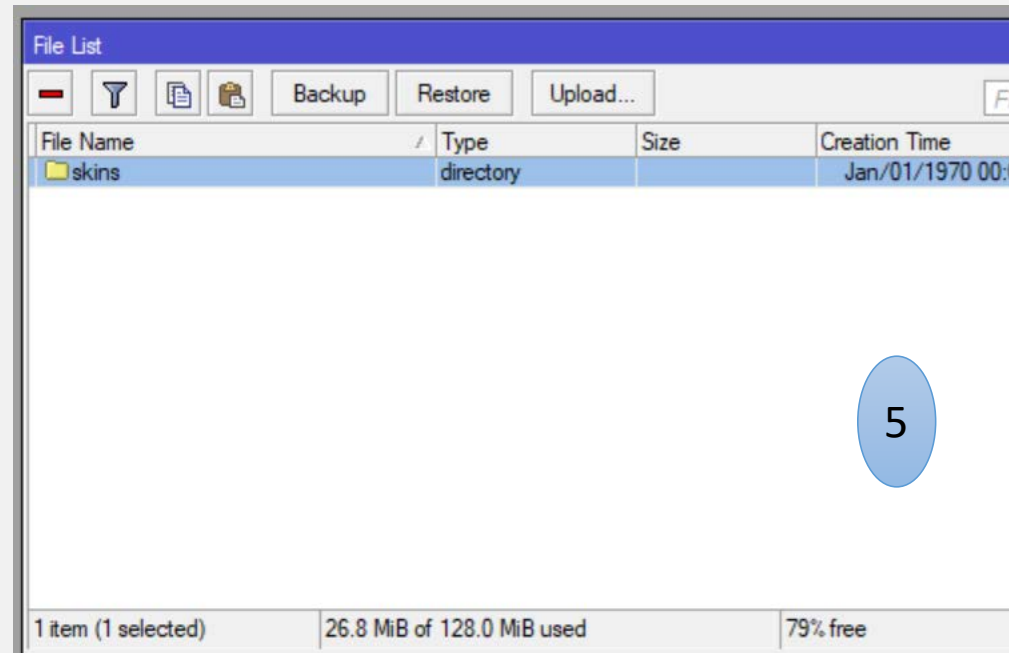
2

```
[admin@AULA ] > system reboot
```

6



4



5

Paso 4: Configuración del Hostpot y User manager

IP 192.168.87.1

IP 192.168.87.2

RADIUS 192.168.88.1

1

2

3

Radius

#	Service

Radius Server <192.168.88.1>

General Status

Service: ppp login
 hotspot wireless
 dhcp ipsec

Called ID:
 Domain:
 Address: 192.168.88.1
 Secret: ****

Authentication Port: 1812
 Accounting Port: 1813
 Timeout: 300 ms

Accounting Backun

OK
 Cancel
 Apply
 Disable
 Comment
 Copy
 Remove
 Reset Status

Hotspot

Servers Server Profiles Users User

+ - Filter

Name	DNS Name
* default	
hsprof1	

Hotspot Server Profile <hsprof1>

General Login RADIUS

Use RADIUS

Default Domain:
 Location ID:
 Location Name:



Paso 4: Configuración del Hostpot y User manager

Router details

▲ Main

Name: SALA 2

Owner: admin

IP address:

Shared secret:

Time zone: Parent time zone

Disabled:

Log events: Authorization suc
 Authorization failu
 Accounting succe
 Accounting failure

1

Router details

▲ Main

Name: SALA 1

Owner: admin

IP address:

Shared secret:

Time zone: Parent time zone

Disabled:

Log events: Authorization success
 Authorization failure
 Accounting success
 Accounting failure

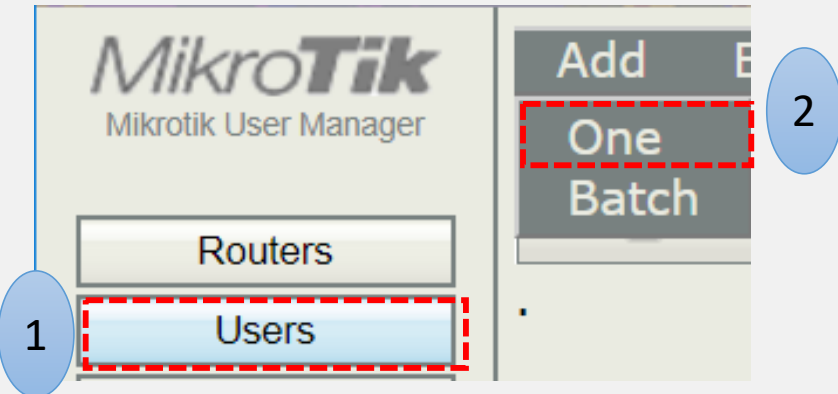
LADO SERVIDOR

Paso 5: Configuración User manager (PERFIL)

The screenshot shows the Mikrotik User Manager web interface. The browser address bar (1) displays '192.168.88.1/userman'. The left sidebar (2) has the 'Profiles' menu item highlighted. The main content area shows the 'Profiles' configuration page (3) for a profile named 'MUM'. The profile details include: Name: MUM, Owner: admin, Starts: At first logon, Price: 0.00, and Shared users: not used. Below these details are buttons for 'Save profile' and 'Remove profile'. A 'Limits' dialog box (5) is open, showing a 'Period' of all days and a 'Time' range from 0:00:00 to 23:59:59. Under 'Limits', the '5 MIN' option is selected (4), and the 'New limit' button is highlighted.



Paso 6 : Configuración User manager (Usuarios)



User details

▲ Main

Username:

Password:

Disabled:

Owner: admin

▼ Constraints

▼ Wireless

▼ Private information

Assign profile: MUM

Add

3

4



DUDE



Virtual Private Network



- ✓ Leer!
- ✓ Implementar
- ✓ Fallar
- ✓ Volver a Leer
- ✓ Corregir
- ✓ Testear
- ✓ Documentar.

¿PREGUNTAS?

¡MUCHAS GRACIAS!

“El verdadero progreso es el que pone la tecnología al alcance de todos” ... Henry Ford

Armando Cartagena
ITDES

MUM HONDURAS 2018

