

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

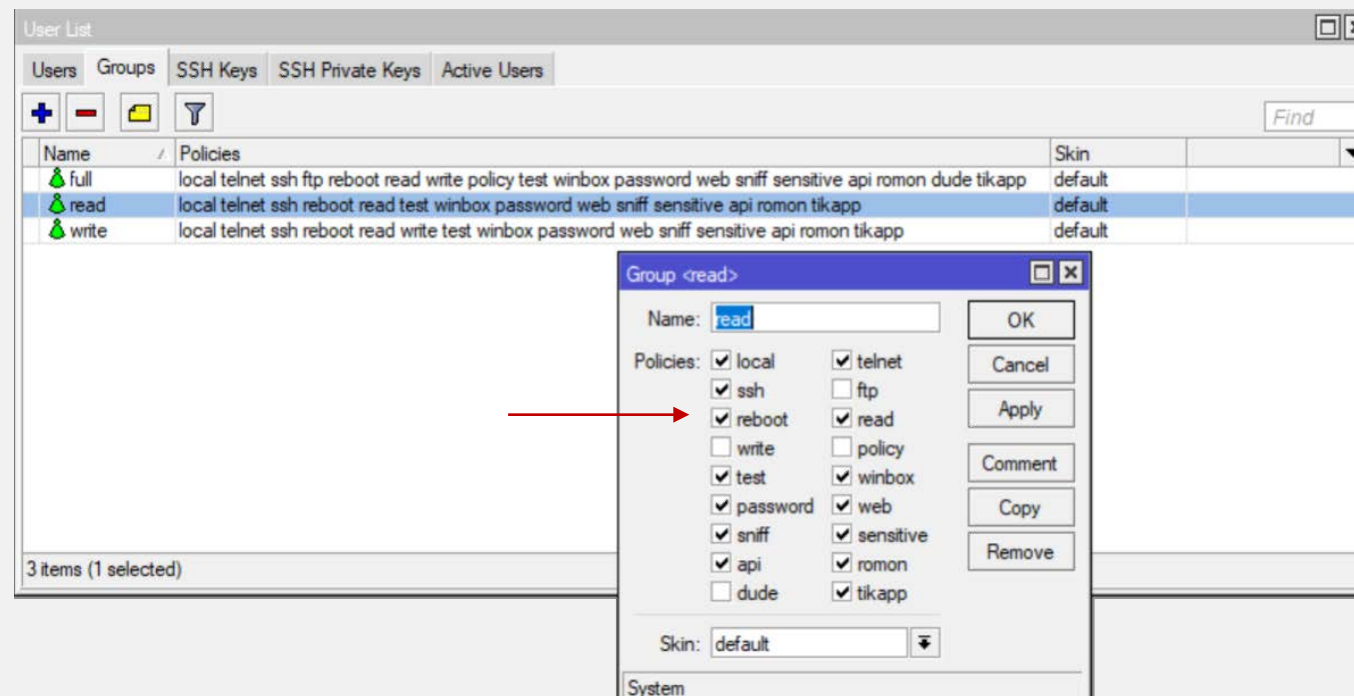
MikroTik® (RouterOS y Routerboard) nos ofrece herramientas muy poderosa y sobre todo demasiado amplias, pero como en todos los casos, hay que saber configurarlo correctamente.

- ✓ 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



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

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

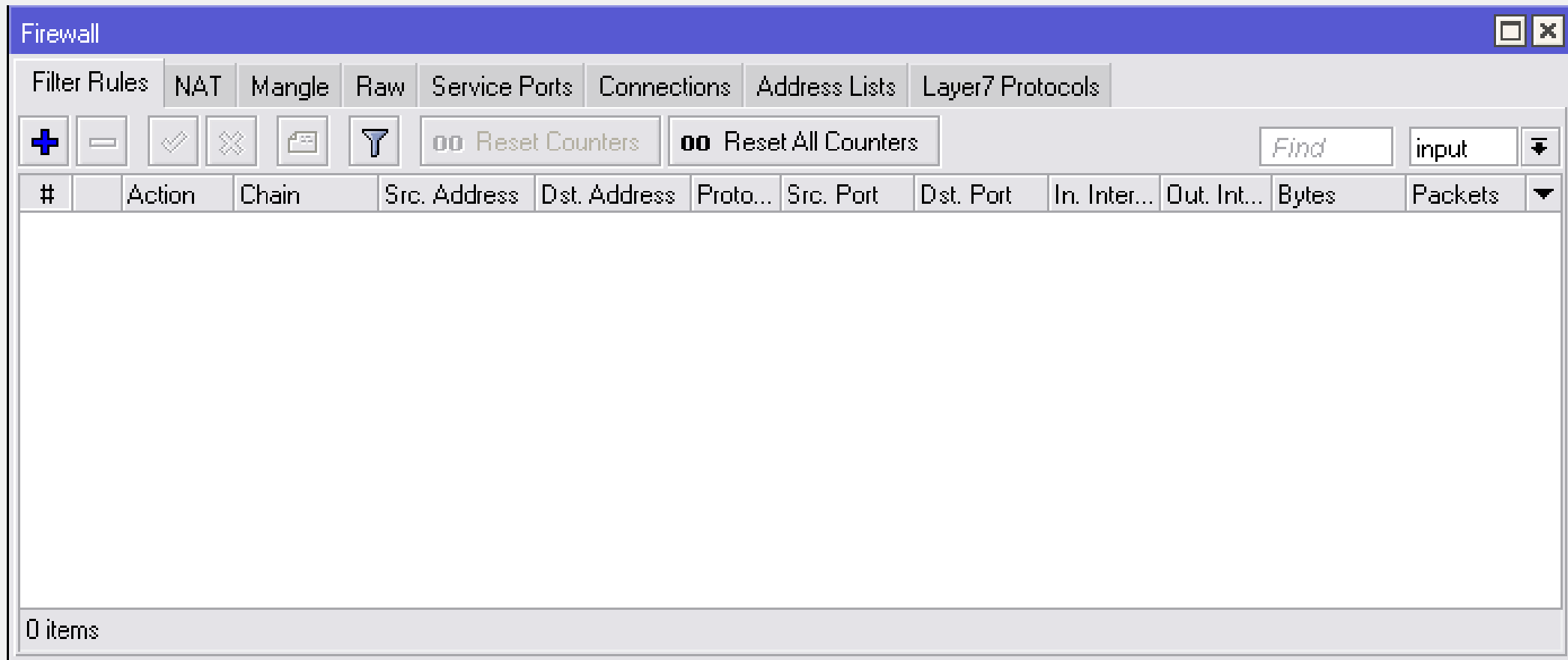
Identity: RMATICA

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** s

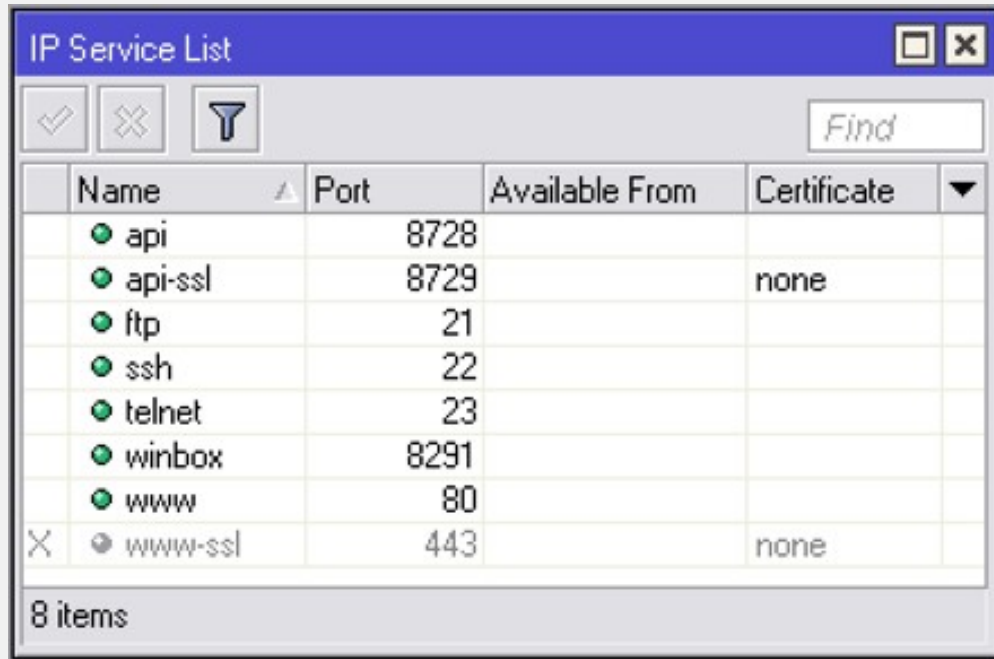
Collect
☒ Src. Address ☒ Src. Address6
☒ Dst. Address ☒ Dst. Address6
☐ MAC Protocol ☒ Port
☐ Protocol ☐ VLAN Id

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	
800 (ip)		115.238.184.125:26701	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:43549	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:16379	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:17231	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.110:20153	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:50075	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:55531	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:62555	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:34379	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:48267	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:58126	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.110:24377	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:26973	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:43181	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:48380	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:14222	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:17981	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:49099	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:9467	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:42021	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:62197	:53 (dns)		6.0 kbps	344 bps	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.

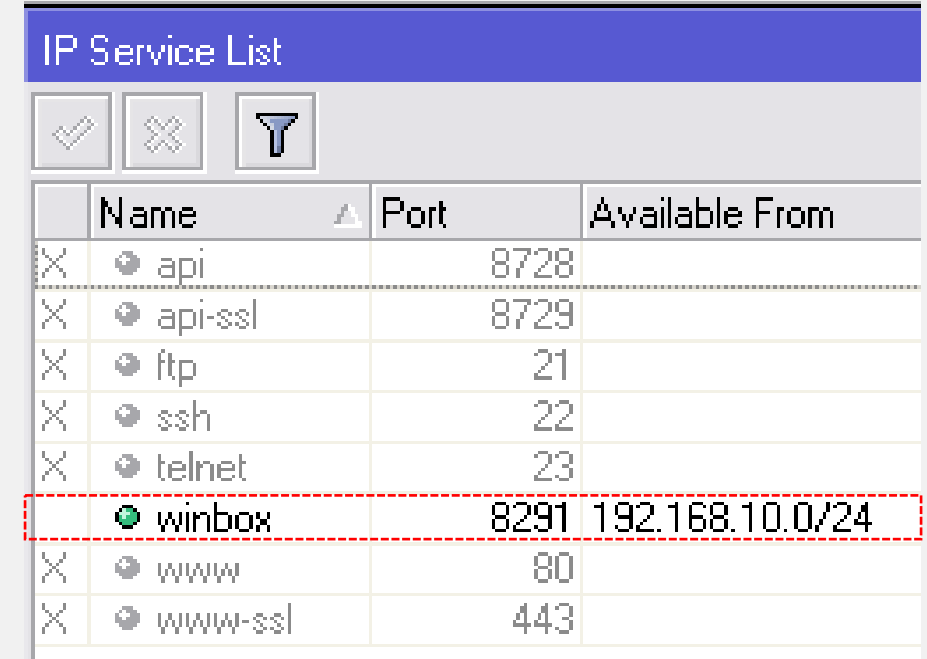
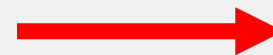


IP Service List

Find

	Name	Port	Available From	Certificate
☒	api	8728		
☒	api-ssl	8729		none
☒	ftp	21		
☒	ssh	22		
☒	telnet	23		
☒	winbox	8291		
☒	www	80		
☒	www-ssl	443		none

8 items



IP Service List

Find

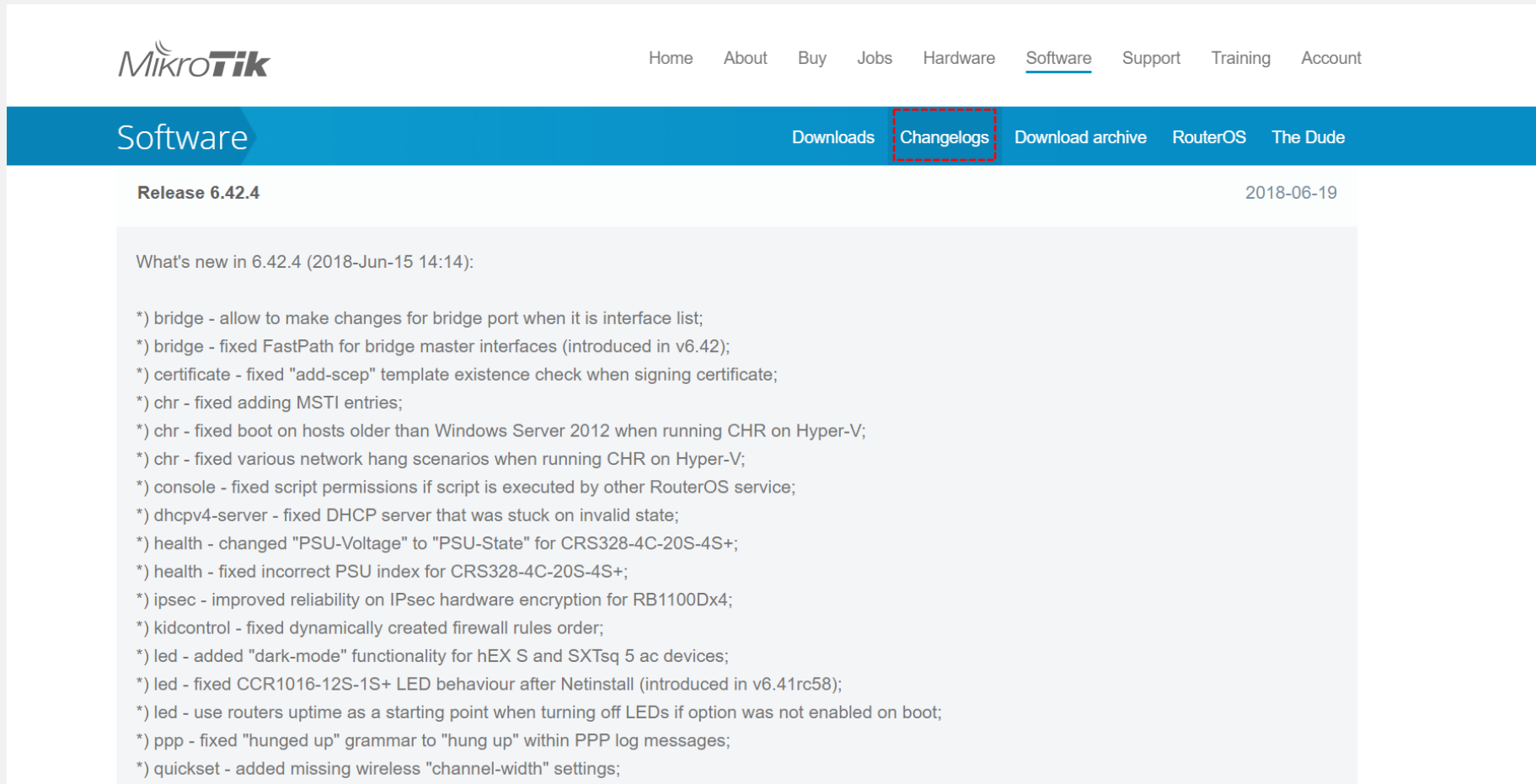
	Name	Port	Available From
☒	api	8728	
☒	api-ssl	8729	
☒	ftp	21	
☒	ssh	22	
☒	telnet	23	
☒	winbox	8291	192.168.10.0/24
☒	www	80	
☒	www-ssl	443	

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' section is displayed, dated 2018-06-19. The content lists various updates and fixes for the RouterOS software.

MikroTik Home About Buy Jobs Hardware Software Support Training Account

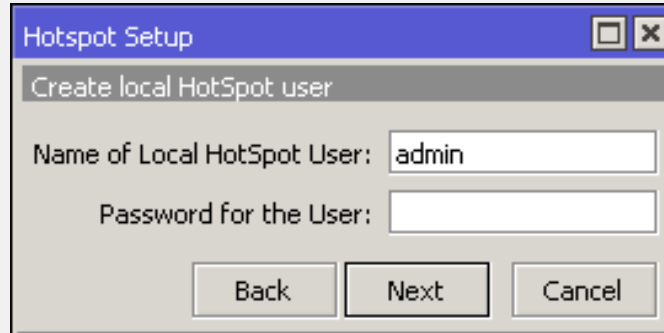
Software Downloads **Changelogs** Download archive RouterOS The Dude

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

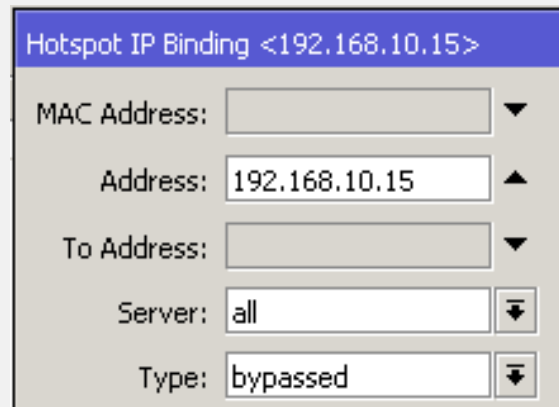
Create local HotSpot user

Name of Local HotSpot User:

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:

To Address:

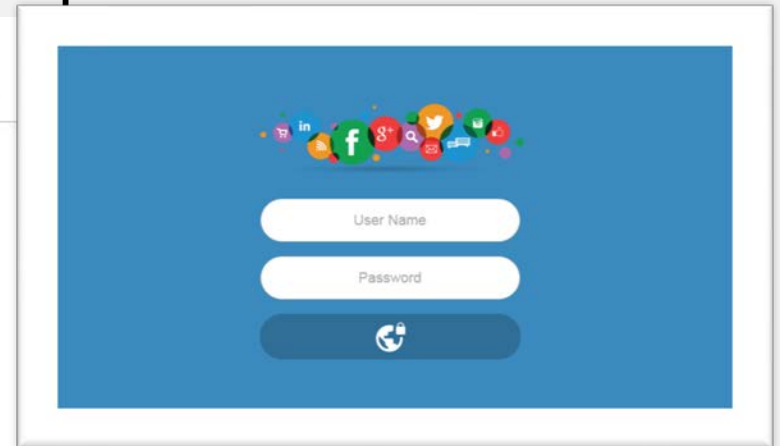
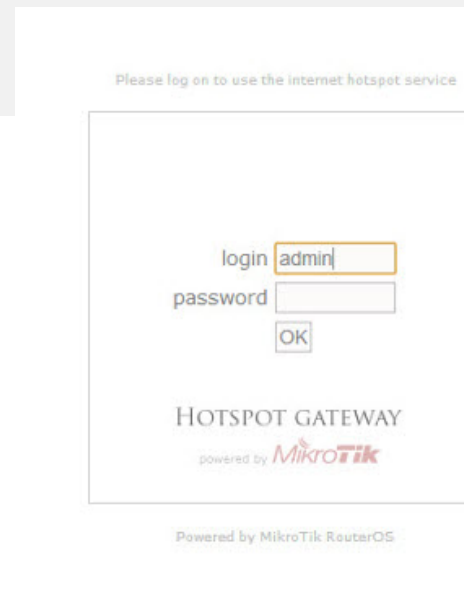
Server:

Type:

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

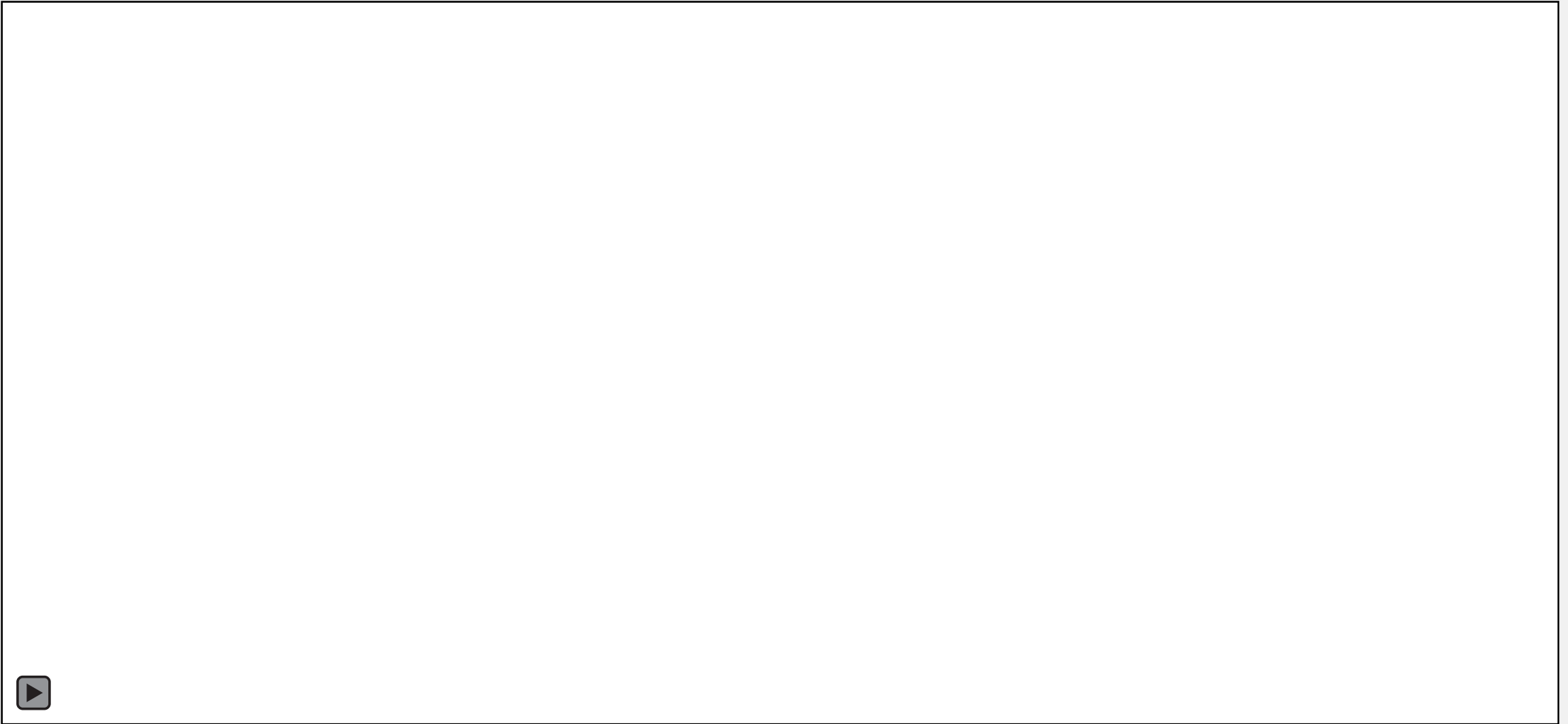
Ventajas de utilizar UserManager

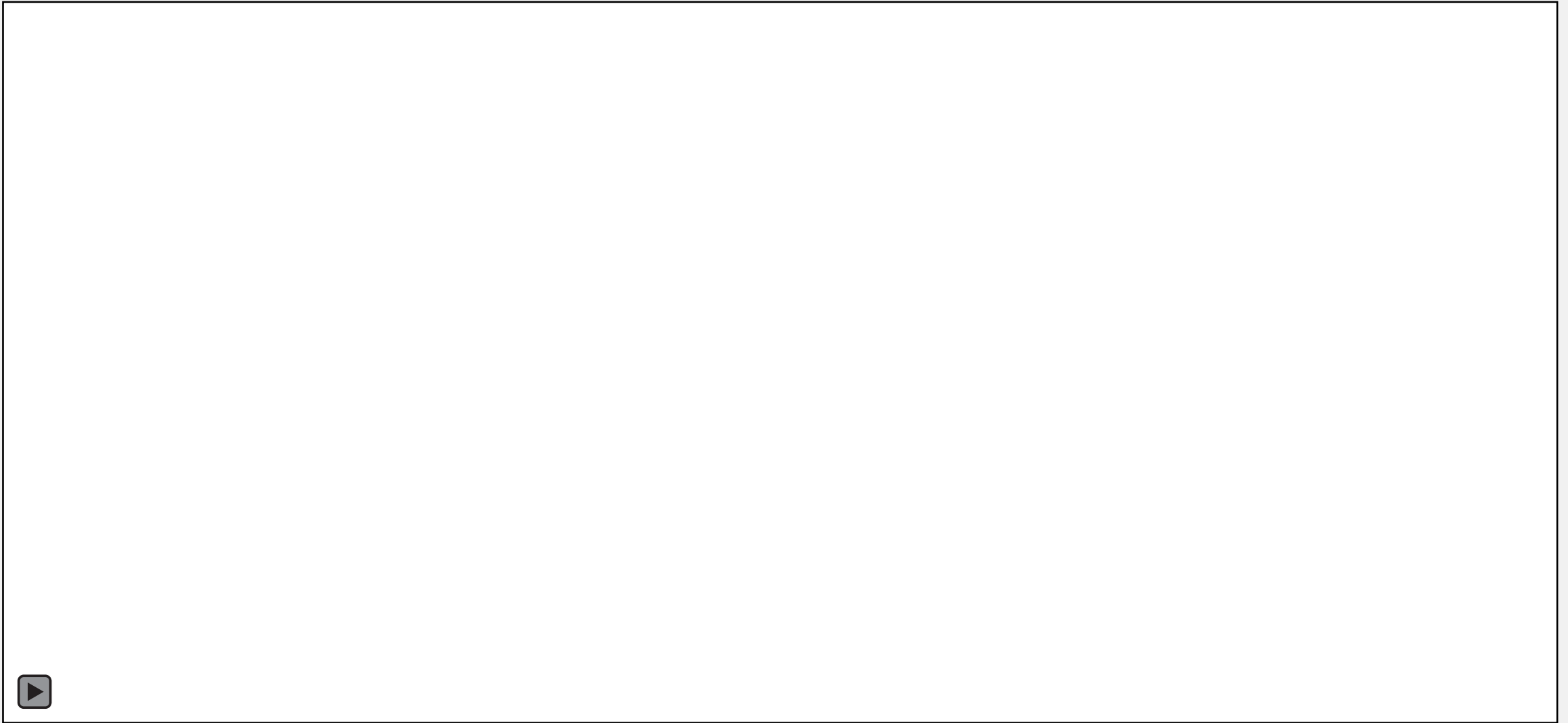
- ✓ Sin costo adicional.
- ✓ Administración centralizada de toda la red.
- ✓ Única base de datos (o réplicas) aislada de la configuración del server principal.
- ✓ Permite crear usuarios por lotes y generar Boucher o exportarlos a un archivo en CSV para una posterior impresión de tarjetas prepagas.





- ✓ 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.

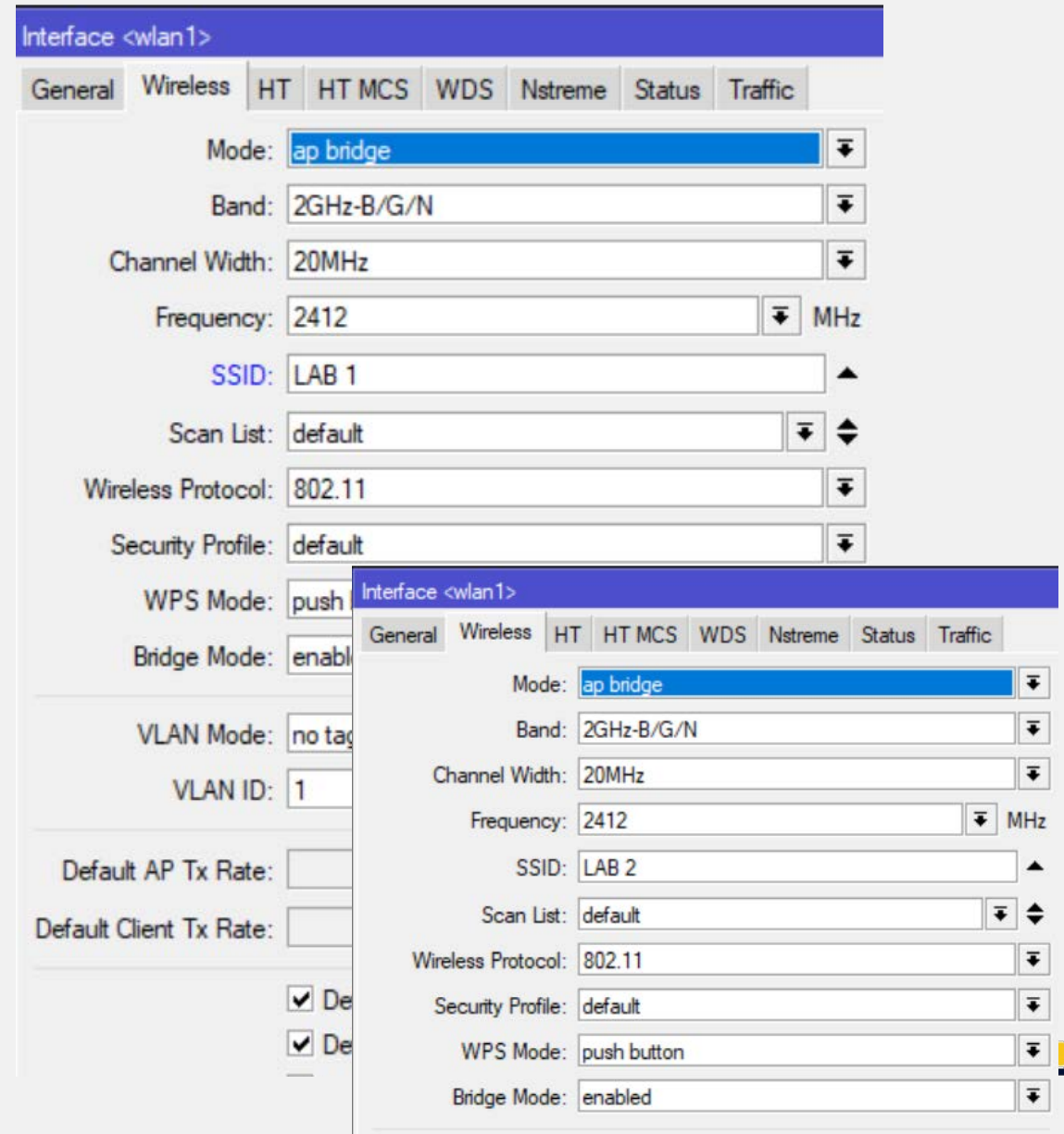






Paso 1: Configuración Básica De Wifi

- ✓ 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.



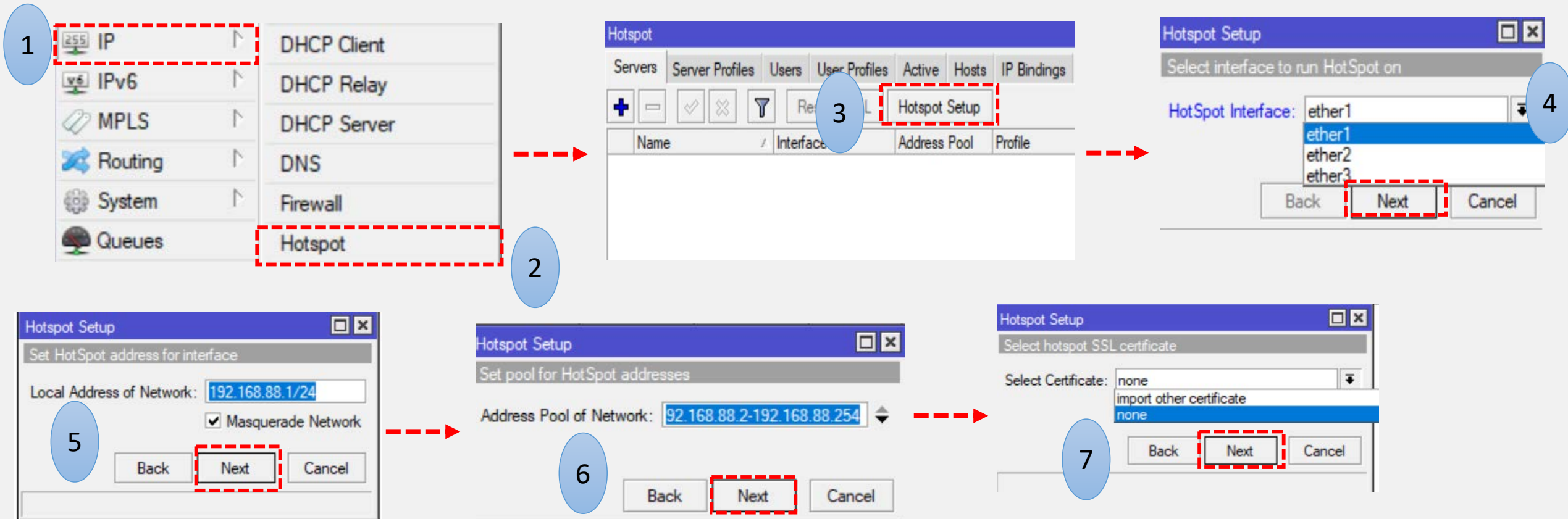
The image shows two overlapping screenshots of the Mikrotik WinBox configuration interface for wireless interfaces. The top screenshot shows the configuration for 'Interface <wlan1>' with the following settings:

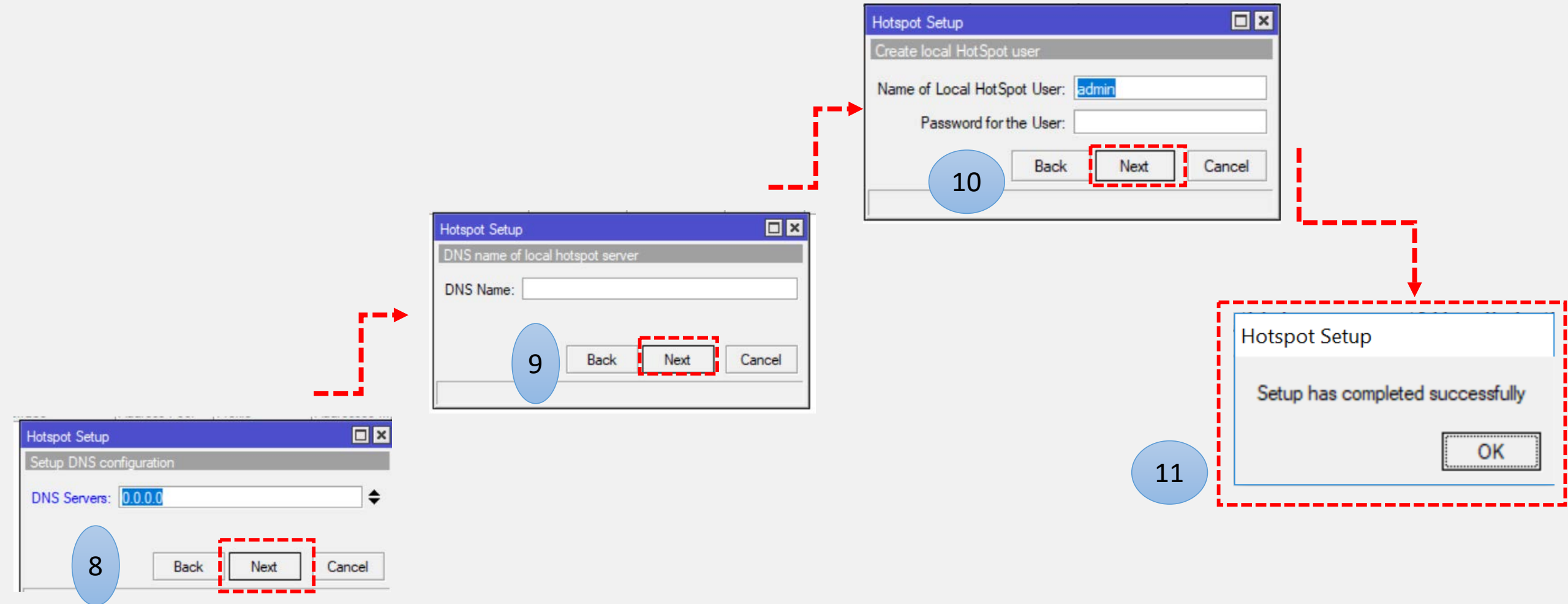
- Mode: ap bridge
- Band: 2GHz-B/G/N
- Channel Width: 20MHz
- Frequency: 2412 MHz
- SSID: LAB 1
- Scan List: default
- Wireless Protocol: 802.11
- Security Profile: default
- WPS Mode: push button
- Bridge Mode: enabled
- VLAN Mode: no tag
- VLAN ID: 1
- Default AP Tx Rate: (empty)
- Default Client Tx Rate: (empty)
- Checkboxes: ☒ De (partially visible)
- Checkboxes: ☒ De (partially visible)

The bottom screenshot shows the configuration for 'Interface <wlan2>' with the following settings:

- 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)

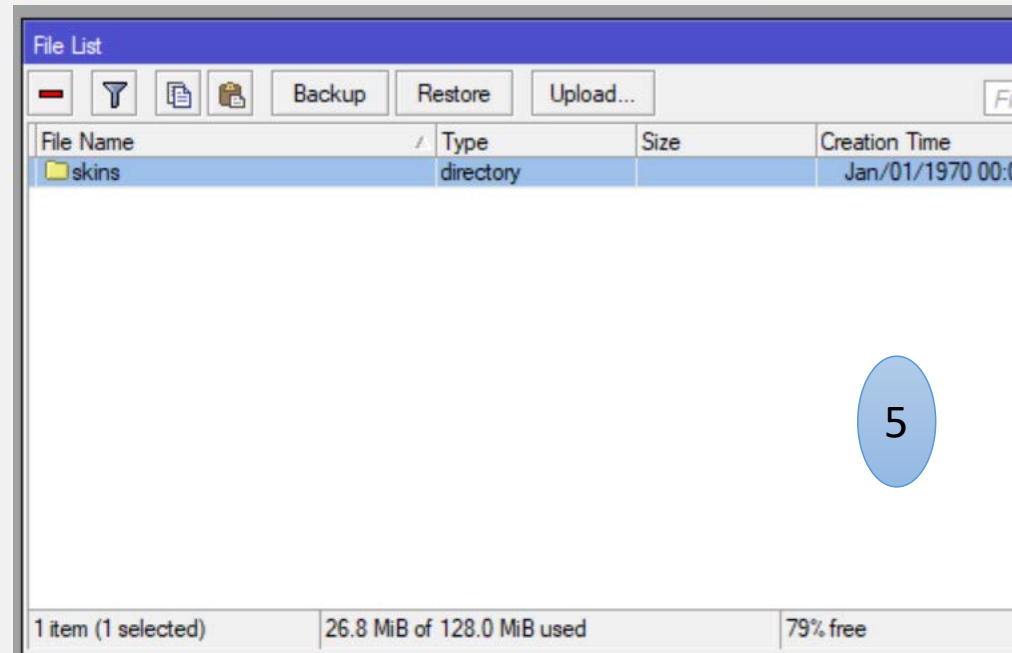
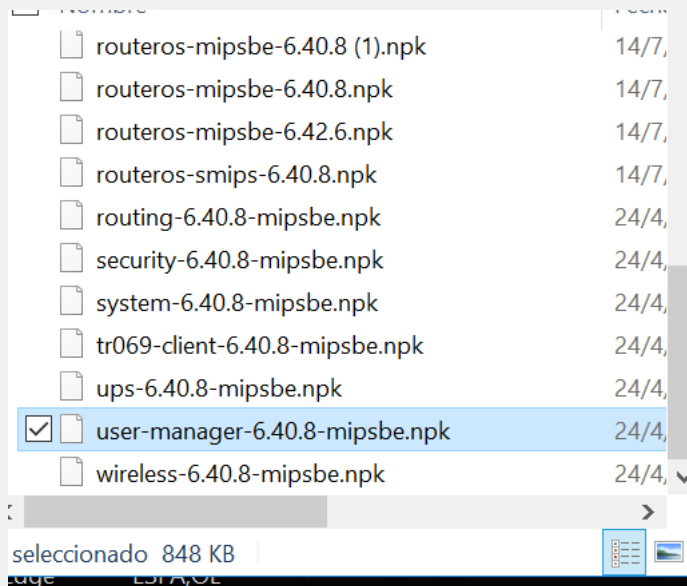
1

<https://mikrotik.com/download>

2

[admin@AULA] > system reboot

6



Paso 4: Configuración del Hostpot y User manager

IP 192.168.87.1

IP 192.168.87.2

RADIUS 192.168.88.1

Diagram illustrating the configuration steps for the Radius server:

1. Select **Radius** from the menu.
2. Click the **+** button to add a new Radius server.
3. Configure the **Radius Server <192.168.88.1>** dialog box.

The **Radius Server <192.168.88.1>** dialog box shows the following configuration:

- General** tab:
 - 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
- Status** tab:
 - Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Status

Diagram illustrating the configuration steps for the Hotspot server profile:

1. Select **hsprof1** from the **Hotspot** list.
2. Configure the **Hotspot Server Profile <hsprof1>** dialog box.

The **Hotspot Server Profile <hsprof1>** dialog box shows the following configuration:

- General** tab:
 - ☒ Use RADIUS
 - Default Domain:
 - Location ID:
 - Location Name:
- Login** tab:
 -
- RADIUS** tab:
 -

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 success ☒ Authorization failure ☐ Accounting success ☐ Accounting failure

Router details

▲ Main

Name: SALA 1

Owner: admin

IP address:

Shared secret:

Time zone: Parent time zone

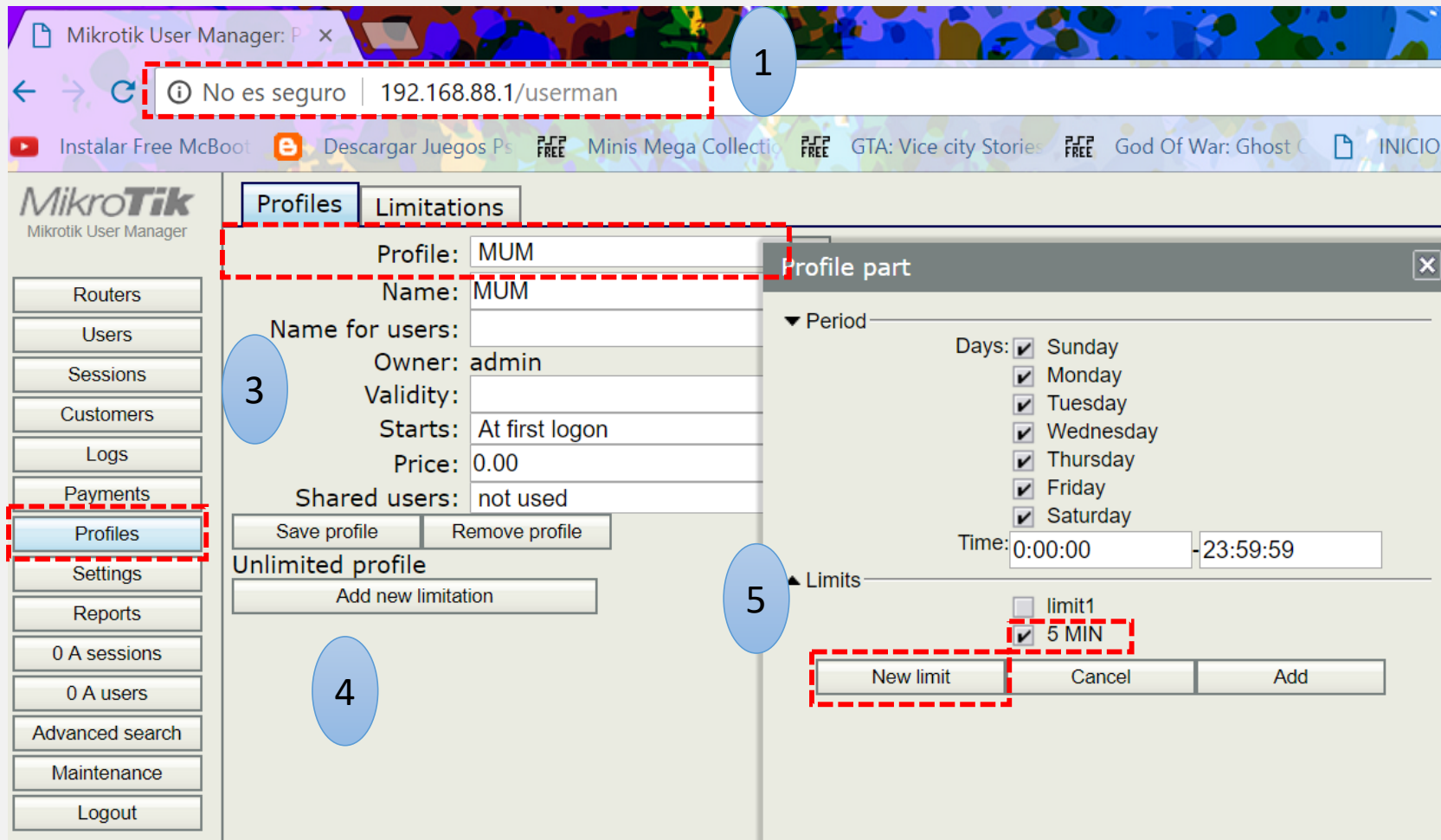
Disabled: ☐

Log events: ☐ Authorization success ☒ Authorization failure ☐ Accounting success ☐ Accounting failure

1

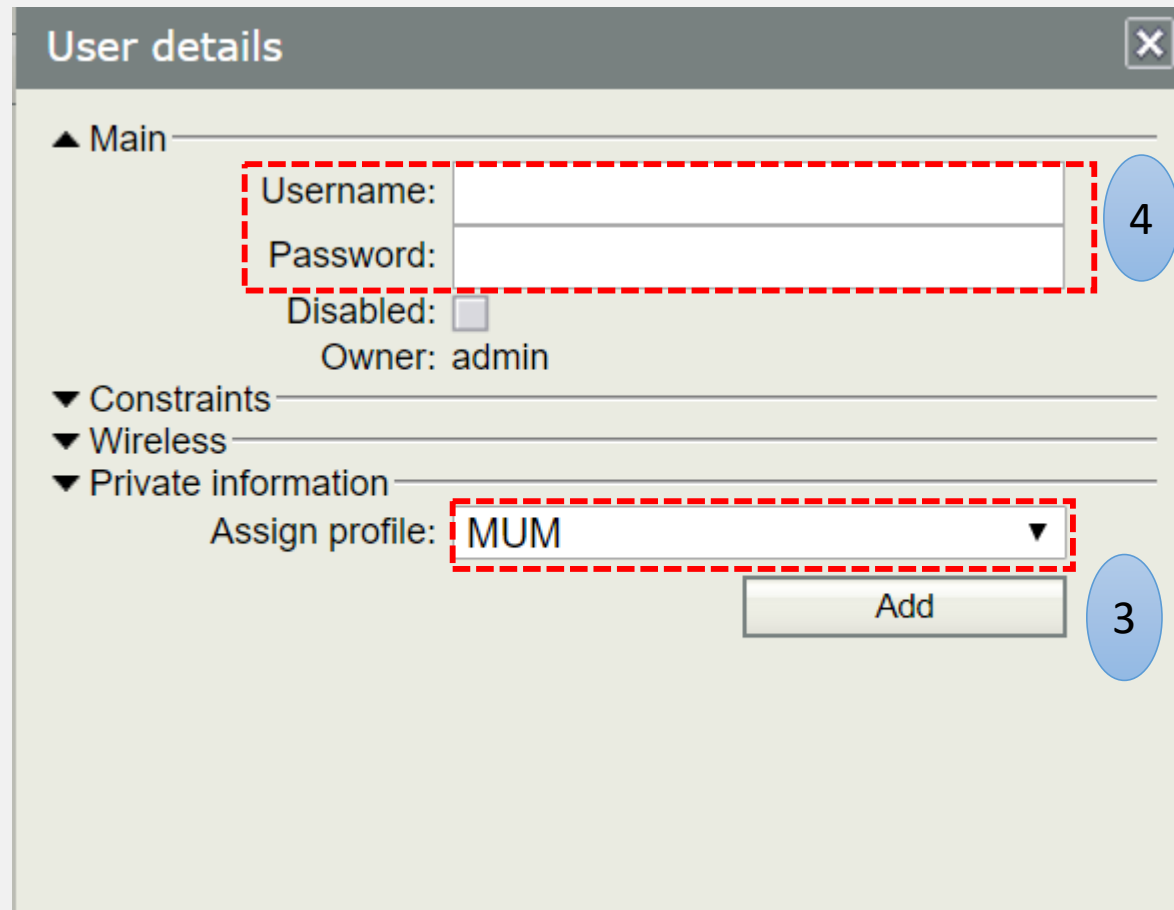
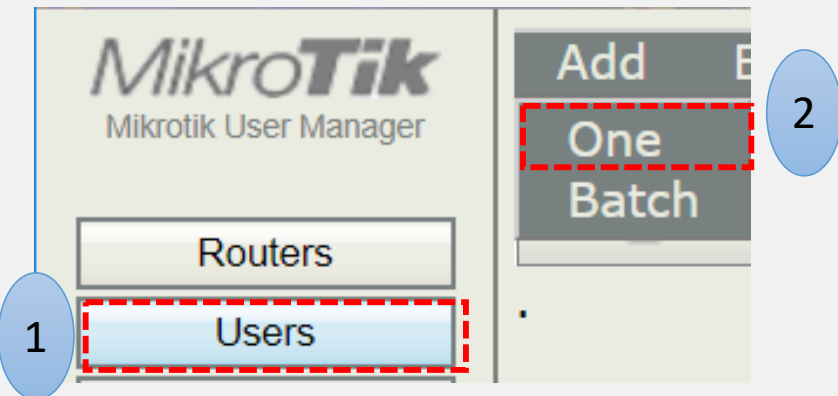
LADO SERVIDOR

Paso 5: Configuración User manager (PERFIL)



The screenshot displays the Mikrotik User Manager web interface. The browser address bar shows the URL `192.168.88.1/userman` (Step 1). The left sidebar contains a menu with options: Routers, Users, Sessions, Customers, Logs, Payments, Profiles (highlighted with a red dashed box and labeled 2), Settings, Reports, 0 A sessions, 0 A users, Advanced search, Maintenance, and Logout. The main content area has two tabs: Profiles and Limitations. The Profiles tab is active, showing a form for creating a new profile named 'MUM' (Step 3). The form fields include: Name (MUM), Name for users (empty), Owner (admin), Validity (empty), Starts (At first logon), Price (0.00), and Shared users (not used). Below the form are buttons for 'Save profile', 'Remove profile', and 'Add new limitation' (labeled 4). A 'Profile part' dialog box is open, showing the 'Period' section with days of the week selected (Sunday through Saturday) and a time range from 00:00:00 to 23:59:59. The 'Limits' section shows a checkbox for 'limit1' and a radio button for '5 MIN' (labeled 5). At the bottom of the dialog are buttons for 'New limit', 'Cancel', and 'Add'.

Paso 6 : Configuración User manager (Usuarios)



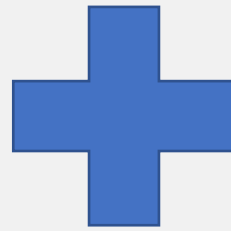
The 'User details' form is shown with the following fields and options:

- Main:**
 - Username:
 - Password:
 - Disabled: ☐
 - Owner: admin
- Constraints:** (collapsed)
- Wireless:** (collapsed)
- Private information:**
 - Assign profile:

An 'Add' button is located at the bottom right of the form, highlighted with a red dashed box and a blue circle labeled '3'.

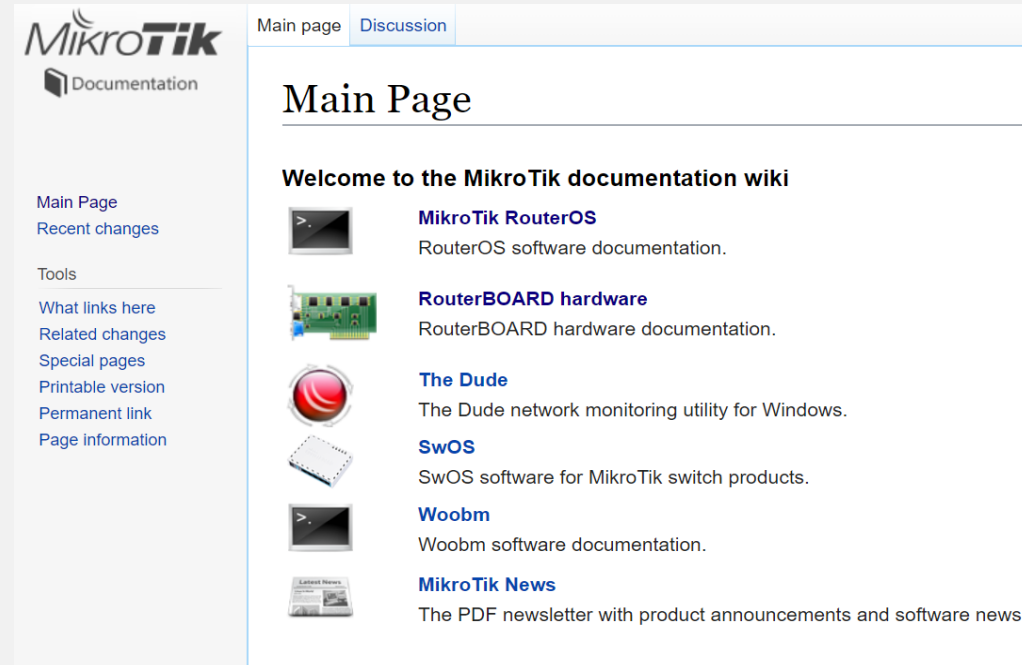


DUDE

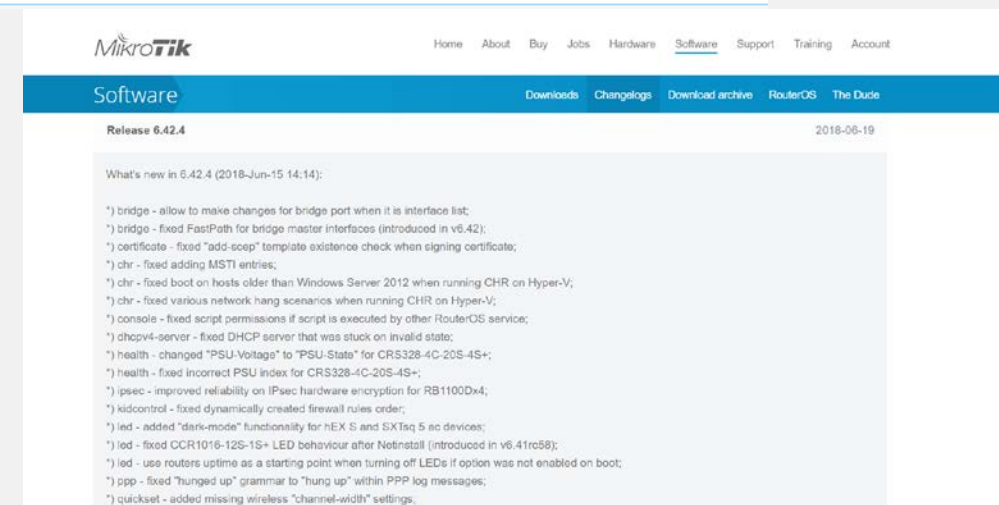


Virtual Private Network

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



The screenshot shows the MikroTik Documentation website. On the left is a sidebar with links: Main Page, Recent changes, Tools, What links here, Related changes, Special pages, Printable version, Permanent link, and Page information. The main content area is titled 'Main Page' and includes a welcome message: 'Welcome to the MikroTik documentation wiki'. Below this are several links with icons: MikroTik RouterOS (RouterOS software documentation), RouterBOARD hardware (RouterBOARD hardware documentation), The Dude (The Dude network monitoring utility for Windows), SwOS (SwOS software for MikroTik switch products), Woobm (Woobm software documentation), and MikroTik News (The PDF newsletter with product announcements and software news).



The screenshot shows the MikroTik Software page for Release 6.42.4. The page has a navigation bar with links: Home, About, Buy, Jobs, Hardware, Software, Support, Training, and Account. The main content area is titled 'Software' and includes a sub-header 'Release 6.42.4' with the date '2018-06-19'. Below this is a section 'What's new in 6.42.4 (2018-Jun-15 14:14):' followed by a list of changes:

- *) 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 SXTq 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 "hung up" grammar to "hung up" within PPP log messages;
- *) quickset - added missing wireless "channel-width" settings;

¿PREGUNTAS?

¡MUCHAS GRACIAS!

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

Armando Cartagena
ITDES

MUM HONDURAS 2018