

MikroTik User Meeting en Bolivia



Controlando el Wi-Fi a nivel nacional, de una cadena de Farmacias por CAPsMAN.

**Por: José Alfredo García D.
Writel Bolivia S.R.L**



Acerca de Mí



- * Nombre.: José Alfredo García D.
 - * Profesión.: Ing. en Redes y Telecomunicaciones
 - * CEO Writel Bolivia S.R.L.
 - * CEO Academy Xperts Bolivia
-
- Coordinador Academia MikroTik
 - Experiencia con MikroTik RouterOS desde 2012
 - Consultor y Entrenador MikroTik.....
 - Certificaciones MTCNA-MTCTCE-MTCWE-MTCUME
MTCRE-MTCINE
 - Participaciones MikroTik User Meeting MUM
Lima - Perú ; Santa Cruz - Bolivia ; Buenos Aires - Argentina

Presentación de la Empresa

Ventas e Importaciones

- Distribuidor mayorista oficial MikroTik.
- Garantías extendidas
- Licencias RouterOS
- Distribuidor mayorista en equipos de seguridad y domótica

Capacitaciones

- Entrenamientos Privados y Públicos
- Convenios Internacionales
- Academia de Entrenamientos
- Academy Xperts Bolivia

Proyectos

- Consultorías
- Soluciones Llave en Mano
- Monitoreos de Redes alámbricas e inalámbricas

Soportes

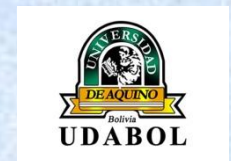
- Pre-Venta y Post-Ventas
- Soportes en Sitio u Online 24,7 ; 8,5
- Soportes Mensual / Anual
- ISP / Wisp

Productos que ofrecemos



MikroTik en BOLIVIA

- Se han realizado implementaciones exitosas en Bolivia, algunos clientes que destacan **utilizando MikroTik** son



Conociendo CAPsMAN

- El Administrador de sistemas de puntos de accesos controlado (**CAPsMAN**) permite la centralización de la gestión de redes inalámbricas , con la capacidad de administrar interfaces de otros dispositivos (CAP). **CAPsMAN** gestiona la configuración de los APs, con o sin interfaces inalámbricas , también se encarga de provisionar configuraciones a todo **CAP(APs)** que lo necesite.
- El Manager opcionalmente puede hacer reenvío de tráfico , puede estar trabajado como Router de Borde y con el controlador (MANAGER) activo al mismo tiempo sin afectarse en nada. También es posible agregar certificados de seguridad en el controlador.
- **CAP** , son equipos con interfaces inalámbricas , sean simple o dual band , que tienen por objetivo dar conectividad inalámbrica a los usuarios finales. Los CAP son configurados por el MANAGER y no así localmente. Es posible obtener configuraciones del CAPsMAN por capa 2 o capa 3.

Conociendo CAPsMAN

- **CAPsMAN** , a pesar que llego un poco tarde , llegó con mucha fuerza y para quedarse por mucho tiempo , siempre en constante mejora y actualización. No trae nada oculto , vale decir no requiere ningún tipo de licenciamiento , ningún hardware extra , tan solo es suficiente trabajar en cualquier ROUTERBOARD MikroTik que posea el S.O RouterOS desde el LEVEL 4 en adelante.



Resumiendo CAPsMAN y CAP

- ✓ Gestión y administración centralizada
- ✓ El CAPsMAN (Manager) no requiere interfaz inalámbrica
- ✓ Comunicación por Layer 2(MAC) y Layer 3 (IP)→DHCP para los CAP con opción de MANAGER
- ✓ Aprovisionamiento de Aps (CAP)
- ✓ Soporta simple y dual band (2Ghz , 5Ghz)
- ✓ Soporta Ap Virtuales
- ✓ 32 Interfaces virtuales por interfaz física
- ✓ Los CAPs al menos deben contar con al menos una interfaz inalámbrica y licencia L4 para proveer acceso a múltiples clientes
- ✓ CAPsMAN Soporta: Autenticación MAC vía RADIUS , Autenticación vía WPA/WPA2 y cifrado TKIP / AES
- ✓ Soporta local forwarding , CAPsMAN forwarding

Situación Problemática Inicial

Antecedentes



- ☐ La Cadena de Farmacias **** contaba solamente con Wi-Fi en su oficina central. Son 2 equipos que se administran de manera individual para dar la cobertura en un Edificio de 3 pisos.
- ☐ Se busca una solución que sea administrable , de bajos costos , de manera centralizada, que permite cambiar las configuraciones del Wi-Fi de manera rápida y sencilla.
- ☐ No se contaba con un control de calidad online sobre sus servicios o productos que ofrecen.

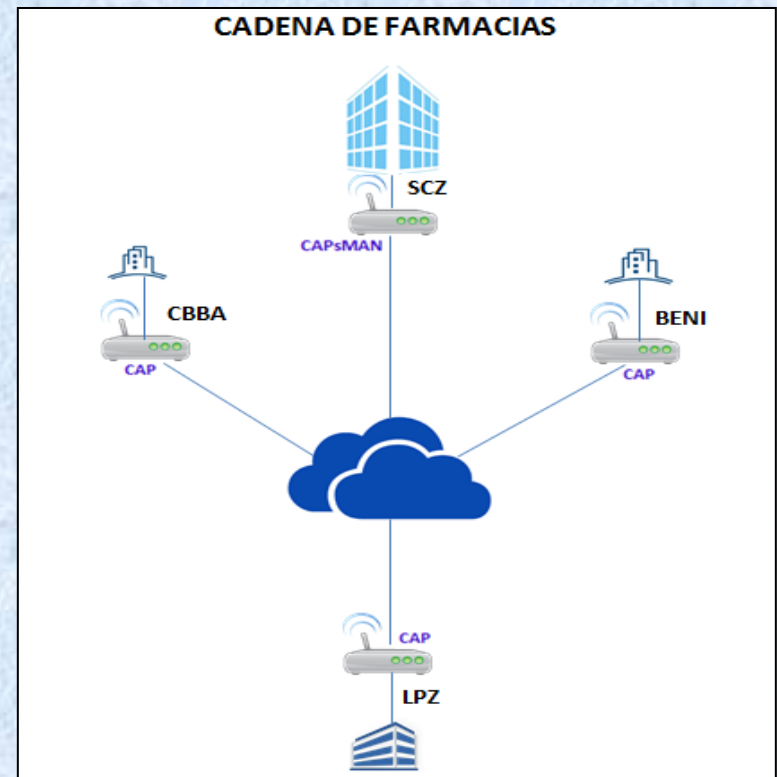
Propuesta

El presente proyecto tiene como alcance la implementación de:

- ✓ Configuración de un router de Borde como Wireless Controller (CAPsMAN).
- ✓ Configuración de 40 Access Point (CAP) inicialmente.
- ✓ Tener la misma red (SSID) para permitir la movilidad del personal en todas las sucursales.
- ✓ Permitir y denegar ciertas conexiones Wi-Fi (Address List).

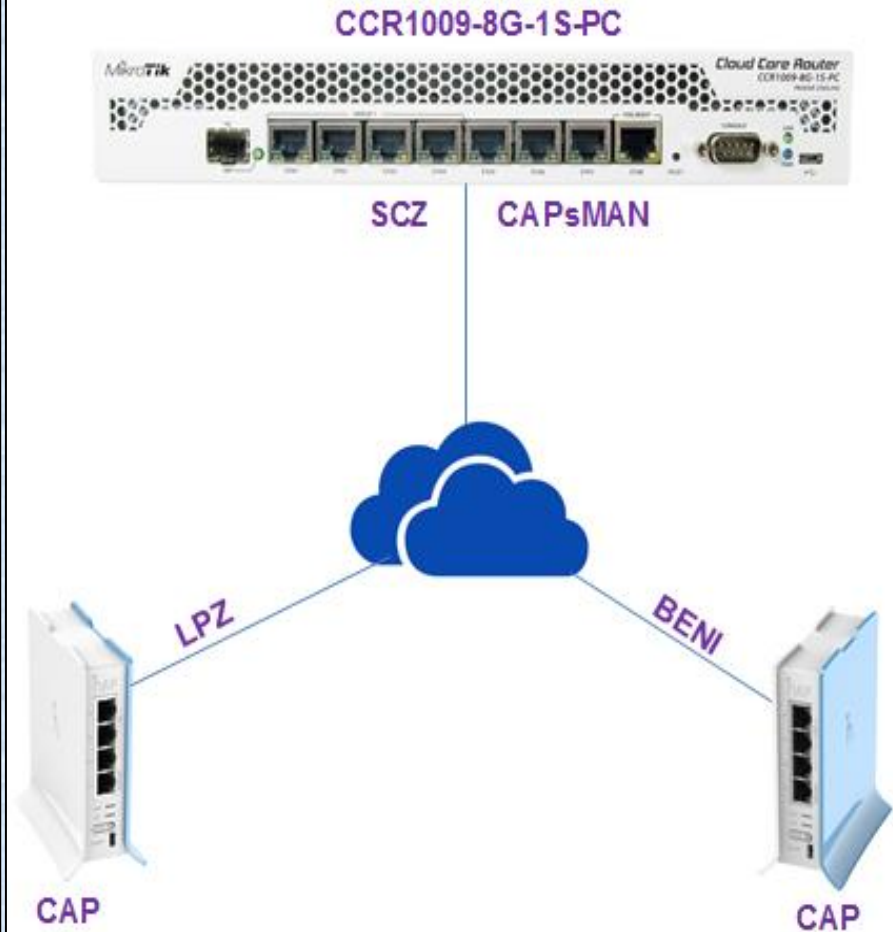
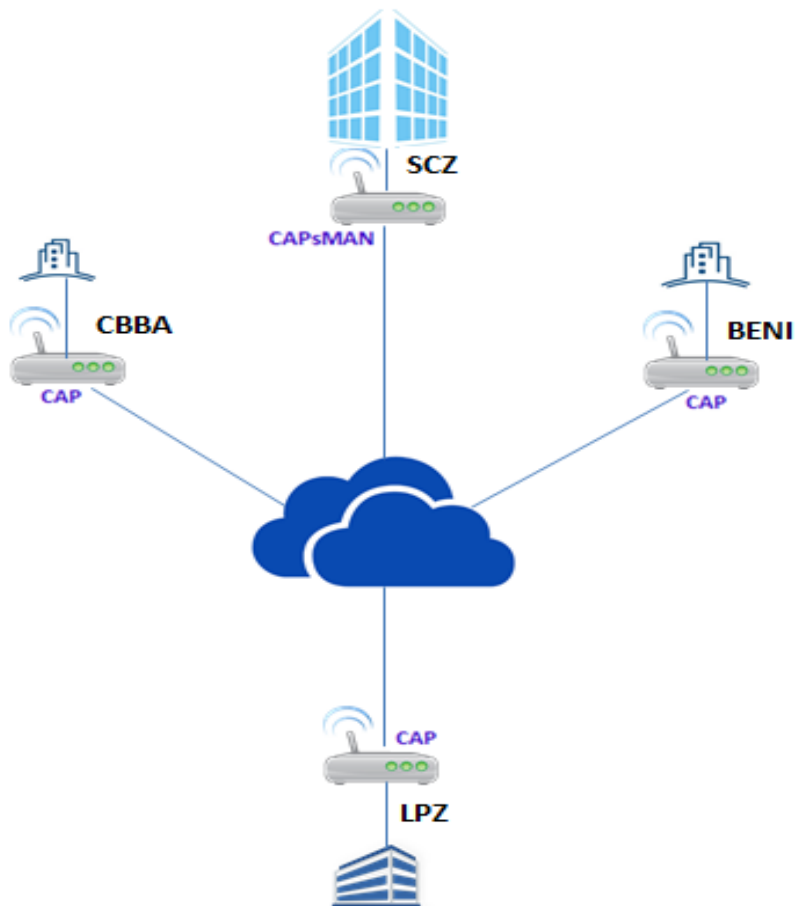
Implementación de CAPsMAN

- ✓ Crear un bridge (Farmacia)
- ✓ Crear un DHCP Server en la interfaz bridge.
- ✓ Activar CAPsMAN en Router Central (Santa Cruz)
- ✓ Conf. el aprovisionamiento de APs (Conf. potencia del radio)
- ✓ Crear un túnel PPTP
- ✓ Configurar los CAP (L3) y registrarse en CAPsMAN
- ✓ Enrutamiento
- ✓ Crear reglas de Access List



Escenario

CADENA DE FARMACIAS



Estaciones Registradas en CAPsMAN

CAPsMAN									
Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table									
Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Packets	Tx/Rx Bytes
cap12	Rey Charles Pc	70:77:81:0F:91:7D	54Mbps...	135Mbps...	0	-55	01:50:30...	1 415 713/918 250	1090.4 MB/484.3...
cap166	Dr. David	1C:3E:84:6C:4C:13	65Mbps...	135Mbps...	0	-62	02:24:11....	1 749/1 360	75.0 KB/165.2 KB
cap166	Leo Mac	80:E6:50:25:3C:0A	52Mbps...	6Mbps	0	-68	01:53:14....	105 022/96 127	131.7 MiB/6.4 MiB
cap166	Negrita Laptop	48:D2:24:EE:E1:FD	11Mbps	108Mbps...	0	-53	00:15:55....	76/209	3122 B/22.9 KiB
cap166	Salinas Laptop	B0:C0:90:55:73:28	26Mbps...	1Mbps	0	-91	00:10:39....	278/952	41.5 KiB/105.1 KiB
cap166	Leonardo S.	28:A0:2B:F1:C3:9F	1Mbps	65Mbps...	0	-76	00:00:45....	6/57	438 B/8.5 KiB
cap166	Linkser Banzer	00:12:54:04:B9:06	1Mbps	5.5Mbps	0	-85	00:00:24....	38/24	4045 B/8.0 KiB
cap232	Inventario Deicy	4C:BB:58:A4:2C:66	65Mbps...	65Mbps...	0	-43	01:51:03....	68 826/72 300	37.8 MiB/10.8 MiB
cap264	Tablet Sis 1	54:EF:92:6A:E8:CE	108Mbps...	13.5Mbps...	0	-61	3d 21:37....	170 071/65 767	109.7 MiB/7.6 MiB
cap264	Tablet Sistemas	54:EF:92:38:E7:2F	121.5Mbps...	13.5Mbps...	0	-64	3d 21:32....	77 013/9 004	9.2 MiB/1185.2 KiB
cap264	Tablet Sis 5	54:EF:92:C5:8E:CF	108Mbps...	13.5Mbps...	0	-70	1d 17:31....	32 794/2 892	1380.4 KiB/421.7...
cap264	Saul	F0:27:65:4F:39:2A	48Mbps	26Mbps...	0	-73	01:37:36....	2 193/1 982	577.2 KiB/285.4...
cap264	Salinas	60:6C:66:1C:C9:9C	65Mbps...	104Mbps...	0	-69	01:24:56....	36 765/20 808	45.5 MiB/2361.5...
cap264	Tablet Sistema	54:EF:92:BF:19:CF	108Mbps...	13.5Mbps...	0	-72	00:36:36....	1 585/1 702	825.1 KiB/481.0...
cap264	Tablet Sis 12	54:EF:92:CA:BC:87	121.5Mbps...	135Mbps...	0	-58	00:35:44....	127 417/62 602	170.8 MiB/4809.9...
cap264	Tablet Sis 10	54:EF:92:54:62:DA	135Mbps...	13.5Mbps...	0	-60	00:34:42....	15 249/8 918	19.3 MiB/1050.8...
cap264	Tablet Sis 3	54:EF:92:88:34:B1	135Mbps...	13.5Mbps...	0	-57	00:34:18....	49 623/22 803	64.9 MiB/2171.0...
cap264	Ariel Avatech Cell	F8:A9:D0:84:24:F6	48Mbps	19.5Mbps...	0	-76	00:34:10....	7 503/4 483	10.0 MiB/548.8 KiB
28 items									

Tabla de Registro del CAPsMAN



Bloqueando conexiones a la red Wi-Fi por medio de Access List

CAPsMAN								
Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table								
#	MAC Address	MAC Mask	Interface	Signal Ra...	Action	Client To Clie...	VLAN Mo...	VLAN ID
...	Desconocido 31				reject			
97	00:08:22:4C:87:FF				reject			
...	Desconocido 27				reject			
88	00:4D:5F:1C:2B:04				reject			
...	Desconocido 22				reject			
78	00:DB:DF:24:4F:BE				reject			
...	Desconocido 45				reject			
119	00:EB:2D:E9:6B:E0				reject			
...	Desconocido 49				reject			
125	04:F7:E4:91:F2:0A				reject			
...	Desconocido 4				reject			
59	08:3D:88:85:87:03				reject			
...	Leydi Cell				reject			
105	08:3D:88:E9:DA:3C				reject			
...	Desconocido 17				reject			
72	08:EC:A9:92:60:28				reject			
...	Rey Charles Cell				reject			
54	08:EE:8B:92:1E:4F				reject			
...	Padilla cell				reject			
37	0C:B3:19:5D:19:55				reject			
...	Desconocido 57				reject			
147	0C:E7:25:B9:14:F8				reject			
...	Willy el escocés				reject			
135	10:66:75:53:3D:26				reject			
...	Desconocido 54				reject			
139	10:D3:8A:BC:8D:...				reject			
...	Desconocido 9				reject			
64	10:D5:42:7B:C2:F6				reject			
...	Desconocido 48				reject			
124	14:A3:64:68:CD:00				reject			
...	Desconocido 47				reject			
122	18:21:95:0E:07:36				reject			
...	Desconocido 46				reject			
120	18:22:7E:5F:91:9C				reject			
...	Desconocido 10				reject			
65	18:F6:43:83:75:0B				reject			
163 items								



Configuración de direcciones MAC rechazadas.

CAPs Access Rule <6E:3B:6B:09:8F:3F>

MAC Address: 6E:3B:6B:09:8F:3F

MAC Mask:

Interface:

SSID Regexp:

Signal Range:

Time

Action: reject

AP Tx Limit:

Client Tx Limit:

Private Passphrase:

Client To Client Forwarding:

RADIUS Accounting:

VLAN Mode:

VLAN ID:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Utilizando esta regla (reject) se rechaza únicamente las estaciones no deseadas.

Listado de equipos Hap lite registrados en el CAPsMAN

CAPsMAN					
Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table					
T Provision					
	Radio MAC	Remote CAP Name	Remote CAP Identi...	Interface	
P	E4:8D:8C:E8:1B:EE	[E4:8D:8C:E8:1B:EE]		cap12	
P	E4:8D:8C:4E:46:B4	[E4:8D:8C:4E:46:B4]		cap142	
P	E4:8D:8C:64:B5:B7	[E4:8D:8C:64:B5:B7]		cap166	
P	E4:8D:8C:31:AF:E6	[E4:8D:8C:31:AF:E6]		cap173	
P	E4:8D:8C:4E:BB:BF	[E4:8D:8C:4E:BB:BF]		cap19	
P	E4:8D:8C:E0:68:5F	[E4:8D:8C:E0:68:5F]		cap214	
P	E4:8D:8C:E8:20:62	[E4:8D:8C:E8:20:62]		cap232	
P	E4:8D:8C:50:6D:07	[E4:8D:8C:50:6D:07]		cap234	
P	E4:8D:8C:CB:80:61	[E4:8D:8C:CB:80:61]		cap264	
P	E4:8D:8C:E8:01:08	[E4:8D:8C:E8:01:08]		cap265	
P	E4:8D:8C:4D:47:7D	[E4:8D:8C:4D:47:7D]		cap271	
P	E4:8D:8C:E8:02:7F	[E4:8D:8C:E8:02:7F]		cap272	
P	E4:8D:8C:4D:48:A4	[E4:8D:8C:4D:48:A4]		cap273	
P	E4:8D:8C:E8:20:EE	[E4:8D:8C:E8:20:EE]		cap286	
P	E4:8D:8C:50:63:66	[E4:8D:8C:50:63:66]		cap292	
P	6C:3B:6B:23:61:F2	[6C:3B:6B:23:61:F2]		cap301	
P	6C:3B:6B:04:3E:83	[6C:3B:6B:04:3E:83]		cap307	
P	6C:3B:6B:09:86:03	[6C:3B:6B:09:86:03]		cap308	
P	E4:8D:8C:4E:09:E8	[E4:8D:8C:4E:09:E8]		cap31	
P	6C:3B:6B:23:71:B5	[6C:3B:6B:23:71:B5]		cap310	
P	E4:8D:8C:4E:BB:CE	[E4:8D:8C:4E:BB:CE]		cap317	
P	6C:3B:6B:22:C5:3A	[6C:3B:6B:22:C5:3A]		cap326	
P	6C:3B:6B:23:62:4C	[6C:3B:6B:23:62:4C]		cap327	
P	6C:3B:6B:1F:4E:E6	[6C:3B:6B:1F:4E:E6]		cap329	
P	6C:3B:6B:22:D1:BC	[6C:3B:6B:22:D1:BC]		cap330	
P	6C:3B:6B:23:62:47	[6C:3B:6B:23:62:47]		cap331	
P	E4:8D:8C:4E:00:10	[E4:8D:8C:4E:00:10]		cap332	
P	E4:8D:8C:50:6C:E4	[E4:8D:8C:50:6C:E4]		cap333	
P	E4:8D:8C:4E:09:D4	[E4:8D:8C:4E:09:D4]		cap334	
P	E4:8D:8C:50:63:57	[E4:8D:8C:50:63:57]		cap335	
P	E4:8D:8C:65:73:85	[E4:8D:8C:65:73:85]		cap336	
P	E4:8D:8C:4E:00:06	[E4:8D:8C:4E:00:06]		cap337	
P	E4:8D:8C:50:6C:A3	[E4:8D:8C:50:6C:A3]		cap338	
P	E4:8D:8C:50:63:4D	[E4:8D:8C:50:63:4D]		cap339	
P	E4:8D:8C:50:6C:F8	[E4:8D:8C:50:6C:F8]		cap340	
P	E4:8D:8C:E0:63:7D	[E4:8D:8C:E0:63:7D]		cap341	
41 items					

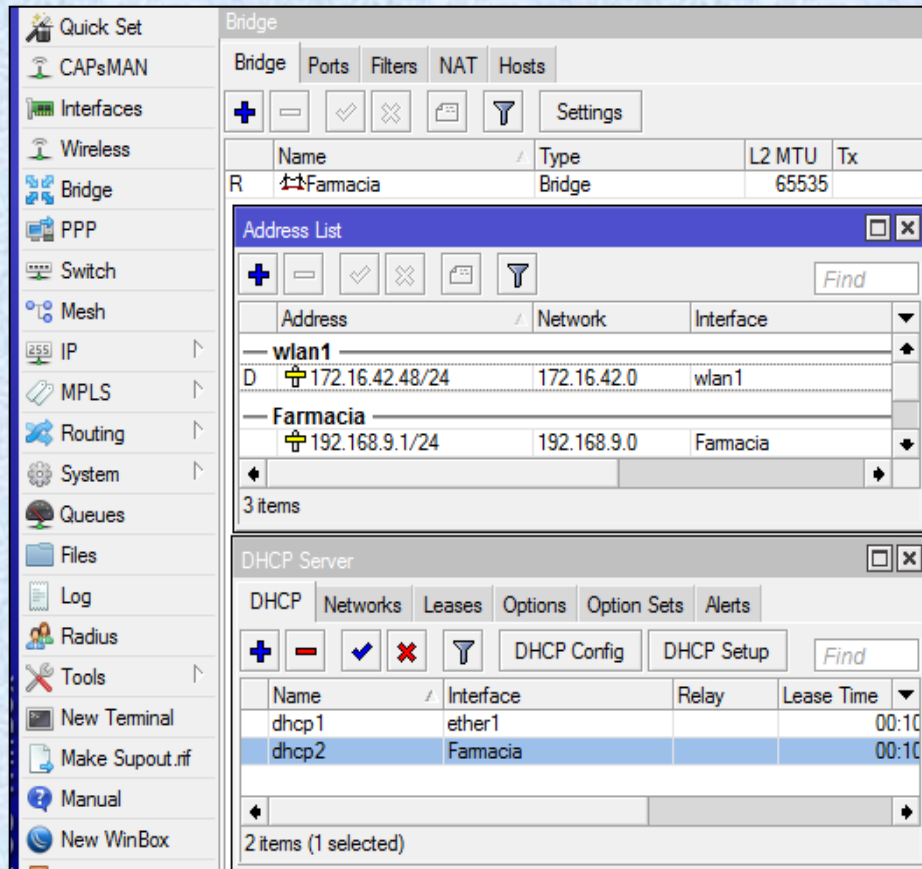
Routers instalados en cada sucursal a nivel nacional



hAP lite RB941-2nD-TC.

Demostración

1.- Condiciones para CAPsMAN



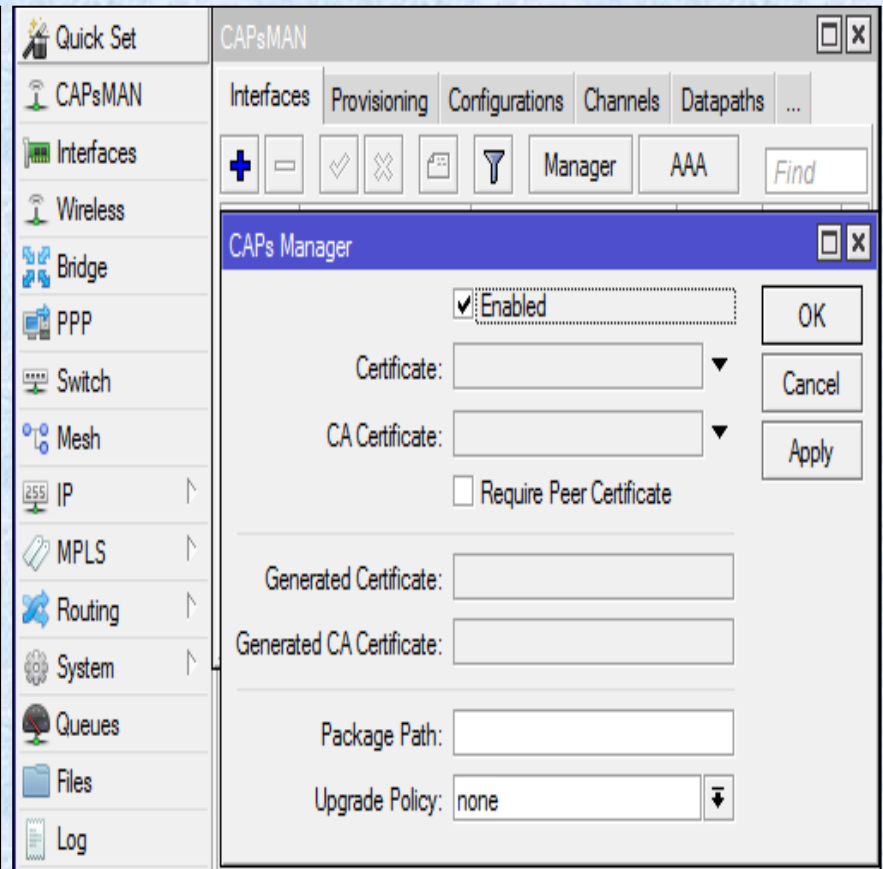
The screenshot shows the MikroTik WinBox interface. The left sidebar contains various configuration menus. The main window is divided into two panes. The top pane is titled 'Bridge' and shows a table of bridge interfaces. The bottom pane is titled 'DHCP Server' and shows a table of DHCP servers.

Name	Type	L2 MTU	Tx
R Farmacia	Bridge	65535	

Address	Network	Interface
wlan1		
D 172.16.42.48/24	172.16.42.0	wlan1
Farmacia		
D 192.168.9.1/24	192.168.9.0	Farmacia

Name	Interface	Relay	Lease Time
dhcp1	ether1		00:10
dhcp2	Farmacia		00:10

2.- Activando CAPsMAN



The screenshot shows the MikroTik WinBox interface with the CAPsMAN configuration window open. The 'CAPs Manager' tab is selected, and the 'Enabled' checkbox is checked. The 'Certificate' and 'CA Certificate' fields are empty. The 'Require Peer Certificate' checkbox is unchecked. The 'Generated Certificate' and 'Generated CA Certificate' fields are empty. The 'Package Path' field is empty. The 'Upgrade Policy' is set to 'none'.

Configurando CAPsMAN

Quick Set CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

Wireless

Name	Mode	SSID	C.F.	Tx. Power	Datapath	Bridge	Local Forwarding	Security	Authenticatio...	Encryption
Farmacia	ap	Farmacia		10		Farmacia	yes		WPA2 PSK	aes ccm tkip

3.- Configuraciones

4.- Provisionando

CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00

Hw. Supported Modes:

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: Farmacia

Slave Configuration:

Name Format: cap

Name Prefix:

enabled

OK Cancel Apply Disable Comment Copy Remove

5.- Access List

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates

#	MAC Address	MAC Mask	Interface	Signal Ra...	Action
Gerente de Ventas					
0	6C:3B:6B:7F:49:9C				accept
Block Cel.					
1	6C:3B:6B:1F:49:3B				reject
Block Tableta					
2	6C:3B:6B:1F:49:3C				reject
Block Laptop javier					
3	8C:3B:6B:1F:49:3C				reject

Configuración de CAPs en las Sucursales

5.- CAP → hacia CAPsMAN / Esperando aprovisionamiento

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Chanr

+ - ✓ ✗ CAP WPS Client Setup Repeater Scann

Name	Type	Actual MTU	Tx	Rx
--- managed by CAPsMAN				
--- channel: 2442/20-Ce/gn(10dBm), SSID: Farmacia, local forwarding				
RS wlan1	Wireless (Atheros AR9...	1500	0 bps	

CAP

☒ Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: wlan1

☐ Lock To CAPsMAN

CAPsMAN Addresses: 192.168.33.1

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: bridge1

Requested Certificate:

Locked CAPsMAN Common Name:

OK Cancel Apply

Bridge

Bridge Ports Filters NAT Hosts

+ - ✓ ✗ Settings Find

Name	Type	L2 MTU	Tx	Rx
R bridge1	Bridge	1600	0 bps	

1 item out of 6

DHCP Client

DHCP Client DHCP Client Options

+ - ✓ ✗ Release Renew Find

Interface	Use P...	Add D...	IP Address	Expires After	Stat
ether4	yes	yes	192.168.33.252/24	00:07:29	bound

1 item

Recomendaciones

- Usar el paquete wireless-cm2 / wireless en la 6.37.1 (Wireless repetidor / CAPsMAN).
- Realizar reglas de filtrado por niveles de señal.
- Crear aprovisionamientos personalizados.
- Realizar en lo posible local forwarding , mas aun si se tiene cantidad de equipos CAPs conectados al Manager.

¿PREGUNTAS?

Muchas Gracias!

