

CAPsMAN gestionando todas las WiFi de un ISP

Ramón Fernández Rego

Sobre mi

- Ramón Fernández Rego
 - Ingeniero de Telecomunicación (Colegiado nº 18.269)
 - MikroTik MTCNA, MTCWE, MTCTCE, MTCRE, MTCUME, MTCINE

Objetivos

- Mostraremos cómo poder gestionar de forma centralizada con CAPsMAN, todas las redes WiFi y servicios asociados a ellas, que actualmente un ISP suele desplegar en los dispositivos (CPE) de sus clientes.
- Veremos una simulación de la red de un ISP, con CPEs gestionados por CAPsMAN, y con varias redes WiFi provisionadas.

CAPsMAN

Breve introducción

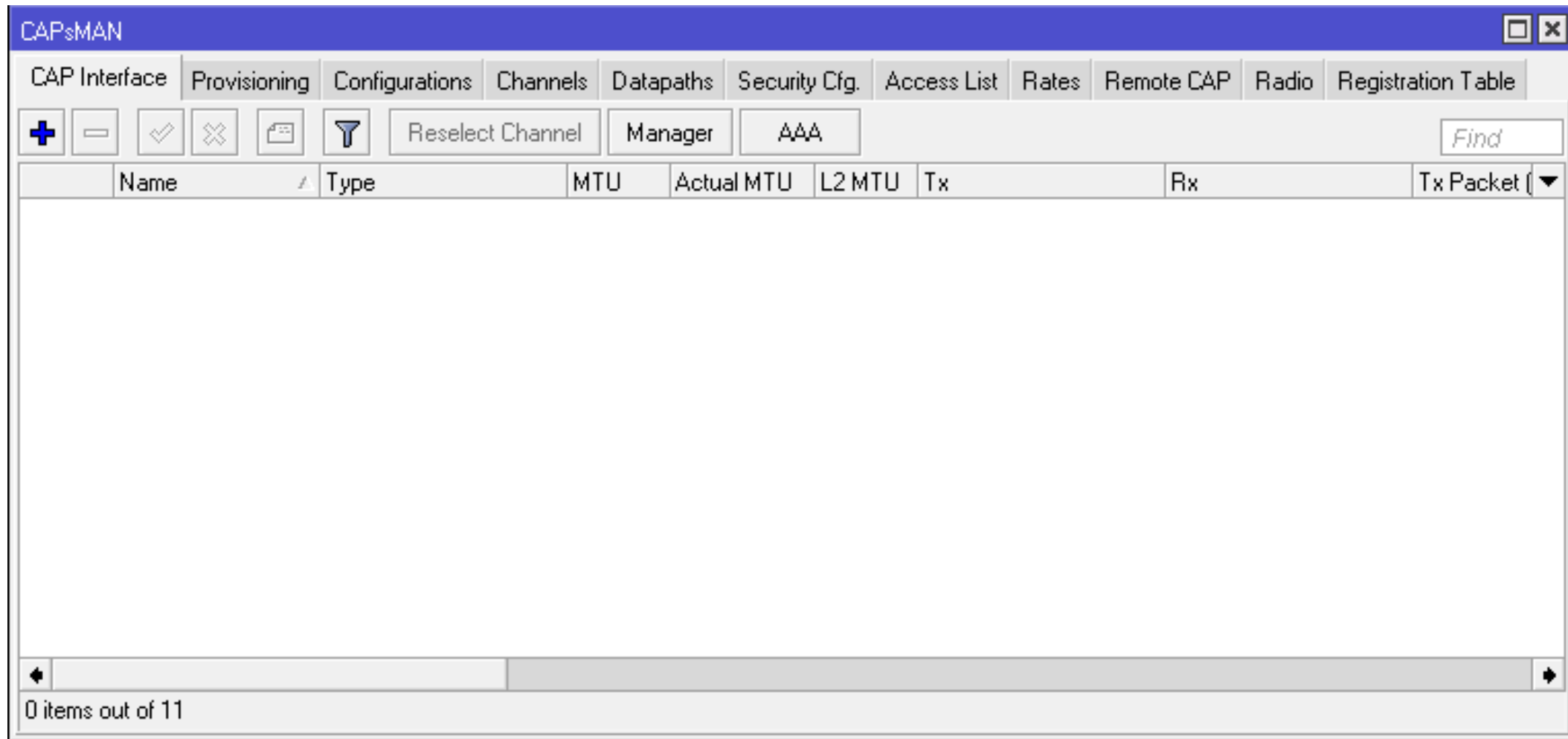
¿Qué es CAPsMAN?

- Sistema Gestor de Puntos de Acceso Controlados “Controlled Access Point system MANager” (CAPsMAN).
- Permite la centralización de la gestión de redes inalámbricas y, si es necesario, el procesamiento de los datos que las atraviesan.

¿Qué es CAPsMAN?

- Cuando un AP es controlado por un CAPsMAN, sólo necesita un mínimo de configuración.
- Las funciones wireless que normalmente gestiona el AP, ahora son ejecutadas por CAPsMAN.
- Los datos de las redes inalámbricas pueden ser redirigidos al CAPsMAN, o pueden ser redirigidos localmente para que el propio CAP tome las decisiones sobre ese tráfico.

Menú CAPsMAN



Requisitos de CAPsMAN

- CAPsMAN v2 funciona desde v6.22rc7.
- No es necesario que tenga interfaces wireless.
- Puede gestionar un número ilimitado de CAPs.
- Conectividad en L2 o L3 entre CAPs y CAPsMAN.
- Si el CAP pierde la comunicación con su CAPsMAN, pierde la configuración de sus interfaces wireless.

Funcionalidades en CAPsMAN

- Permite usar certificados para autenticar la conexión entre CAPs y CAPsMAN.
- CAPsMAN puede pedir actualizar la versión RouterOS del CAP.

The screenshot shows the CAPsMAN interface with the 'CAPs Manager' dialog box open. The dialog box has the following fields and options:

- ☒ Enabled
- Certificate: auto
- CA Certificate: auto
- ☐ Require Peer Certificate
- Generated Certificate: CAPsMAN-64D1542AAF14
- Generated CA Certificate: CAPsMAN-CA-64D1542AAF14
- Package Path: (empty field)
- Upgrade Policy: suggest same version

The background interface shows a table of CAPs:

Name	Type	MTU	Actual MTU
RSMB R3-SOTANO-1	CAP Interface	1500	1500
SB R3-SOTANO-1-1	CAP Interface	1500	1500
RSMB R2-HABITACION-1	CAP Interface	1500	1500
SB R2-HABITACION-1-1	CAP Interface	1500	1500
RSMB R1-ENTRADA-1	CAP Interface	1500	1500
SB R1-ENTRADA-1-1	CAP Interface	1500	1500

Funcionalidades en CAPsMAN

- Protocolo seguro de conexión entre CAPs y CAPsMAN.
- Fijación del CAP a un determinado CAPsMAN.

The screenshot displays the Mikrotik WinBox interface for configuring CAPsMAN. The 'CAP' configuration window is the primary focus, showing various settings for a specific CAP. The 'Enabled' checkbox is checked, indicating the CAP is active. The 'Interfaces' field is set to 'wlan1'. The 'Certificate' field is set to 'CAP-64D15426FE62'. The 'Discovery Interfaces' field is set to 'bridge-GESTION'. The 'Lock To CAPsMAN' checkbox is checked. The 'CAPsMAN Addresses' field is empty. The 'CAPsMAN Names' field is empty. The 'CAPsMAN Certificate Common Names' field is set to 'CAPsMAN-64D1542A'. The 'Bridge' field is set to 'none'. The 'Static Virtual' checkbox is unchecked. The 'Requested Certificate' field is set to 'CAP-64D15426FE62'. The 'Locked CAPsMAN Common Name' field is set to 'CAPsMAN-64D1542AAF14'. The background shows the 'Wireless Tables' window with a list of wireless interfaces.

WiFi y Servicios de un ISP

Introducción a los Servicios WiFi de un ISP

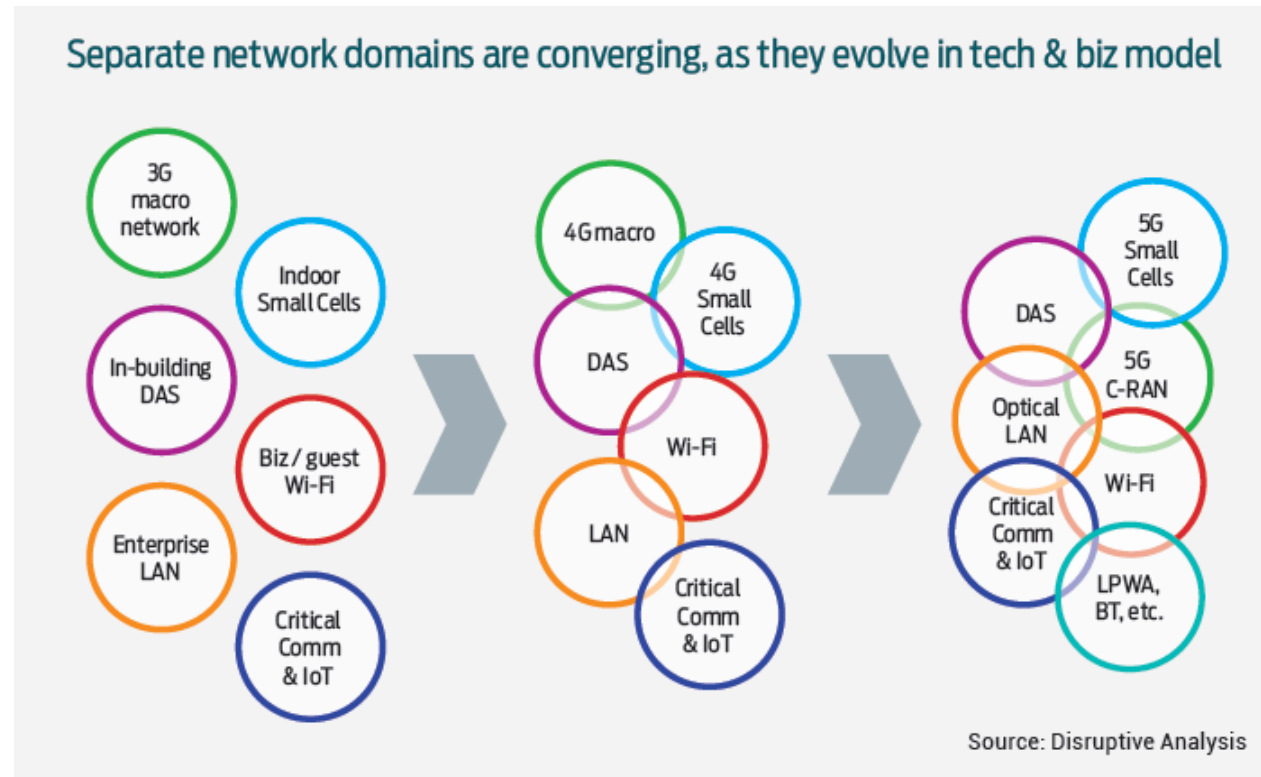
Situación actual:

- Todos los clientes quieren WiFi.
- Si falla, el ISP “sufre” sus incidencias.
- Hay muchos Servicios que ofrecer con estas redes a los clientes.
- WaaS (WiFi como Servicio).

Introducción a los Servicios WiFi de un ISP

Tendencia:

- Convergencia de las redes Wireless.



WiFi del cliente

- La WiFi principal que un ISP despliega en sus CPE, es la del propio cliente.
- En entorno residencial, suele ser suficiente que tenga seguridad WPA2 de clave compartida (WPA2-PSK)
- En entorno empresarial, puede requerirse WPA2 “Enterprise” (WPA2-EAP)

WiFi para visitantes

- Normalmente los clientes (sean empresa o residencial), prefieren tener una WiFi para sus invitados antes de darles acceso a la suya
- En el caso de clientes empresa, suele interesarles regular ese acceso con un portal cautivo (HotSpot) en esta WiFi de cortesía.

WiFi para abonados del ISP

- Cada vez más ISPs despliegan este tipo de WiFi, porque les permite:
 - Que sus abonados puedan conectarse a Internet a través de la WiFi de otros abonados.
 - Aumentar cobertura de acceso a Internet a sus abonados
 - Disminuir el tráfico de datos a través de sus redes 3G/4G
- Para este tipo de WiFi, implementamos seguridad WPA2-Enterprise

Necesidad de una gestión centralizada

- Todas estas WiFis suponen un incremento considerable en la complejidad de la implantación y monitorización de los equipos del cliente, por lo que se hace imprescindible una gestión centralizada de las mismas.
- CAPsMAN facilita esa gestión centralizada, añadiendo funcionalidades que otros Controladores Wireless no tienen.

Escenario real de un ISP

Servicios provisionados en los CPE

Nuestro ISP necesitaba provisionar y gestionar los siguientes servicios a sus clientes (empresas/residencial):

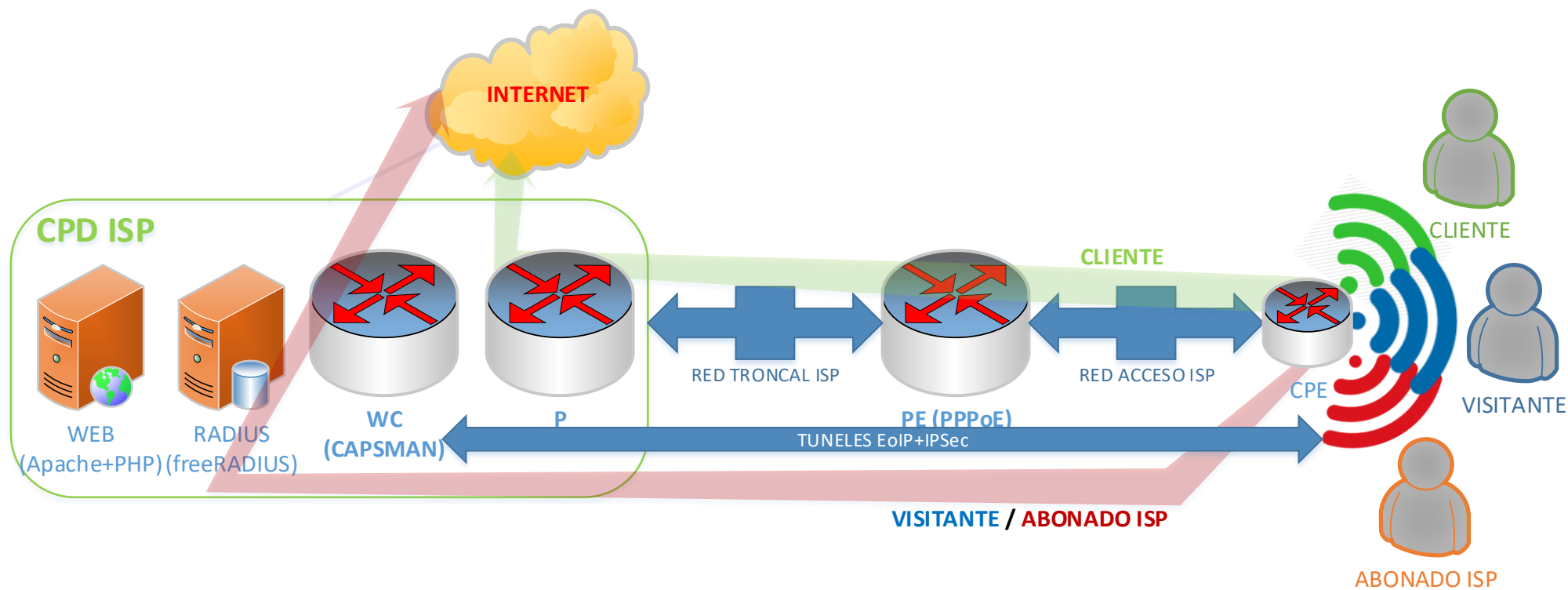
- Acceso a Internet.
- Red WiFi del propio cliente y gestionada por él (perfil **no** técnico).
- Red WiFi para los visitantes del cliente.
- Red WiFi para los abonados del ISP.

Servicios asociados a la provisión

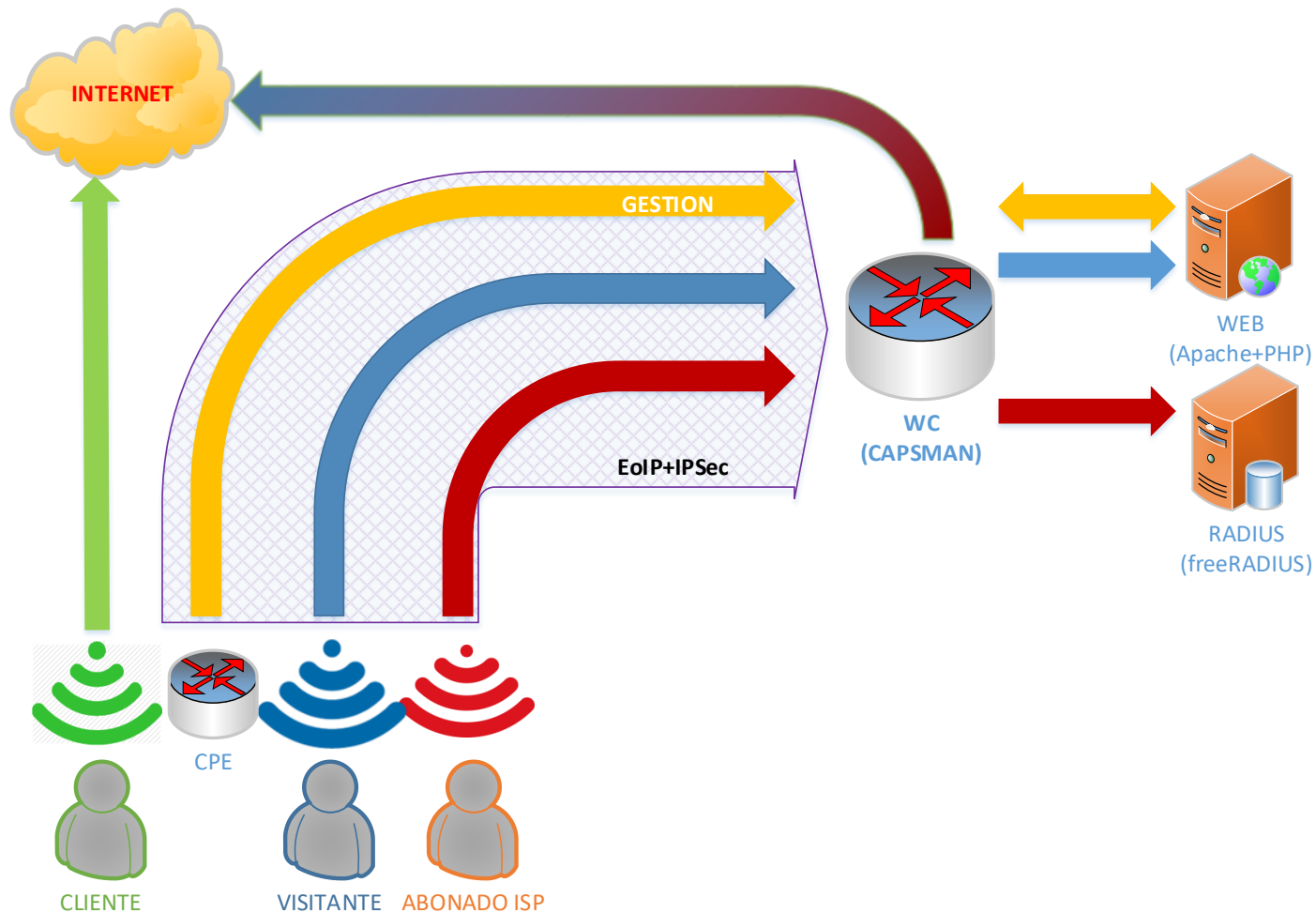
Para cada cliente:

- Portal web de gestión en la nube.
- Portal cautivo (HotSpot) para sus visitas.

Esquema de la solución



Esquema lógico



Configuración de CAPsMAN

- Servicios principales:
 - CAPsMAN
 - Concentrador túneles EoIP
 - Servidor DHCP redes ABONADOS y VISITANTES
 - HotSpot redes VISITANTES

Configuración de CAPsMAN

CAPs Manager

☒ Enabled

OK

Cancel

Apply

Interfaces

Certificate: CAPsMAN-4318B03499C8

CA Certificate: CAPsMAN-CA-4318B03499C8

☒ Require Peer Certificate

Generated Certificate: CAPsMAN-4318B03499C8

Generated CA Certificate: CAPsMAN-CA-4318B03499C8

Package Path:

Upgrade Policy: none

Interface <eoip-tunnel-CPE_A01>

General

Loop Protect

Status

Traffic

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Torch

Name: eoip-tunnel-CPE_A01

Type: EoIP Tunnel

MTU:

Actual MTU: 1408

L2 MTU: 65535

MAC Address: 02:8F:3C:F6:A0:3C

ARP: enabled

ARP Timeout:

Local Address: 10.253.0.2

Remote Address: 10.0.1.1

Tunnel ID: 1001

IPsec Secret:

Keepalive: 00:00:10 , 10

DSCP: inherit

Dont Fragment: no

☒ Clamp TCP MSS

☐ Allow Fast Path

enabled

running

slave

Configuración de los CAPs

Interface <eoip-tunnel-CAPsMAN>

General

Loop Protect

Status

Traffic

Name: eoip-tunnel-CAPsMAN

Type: EoIP Tunnel

MTU:

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:8B:5D:C2:EC:2A

ARP: enabled

ARP Timeout:

Local Address: 10.0.1.1

Remote Address: 10.253.0.2

Tunnel ID: 1001

IPsec Secret:

xxxxxxx

Keepalive: 00:00:10

10

DSCP: inherit

Dont Fragment: no

☒ Clamp TCP MSS
 ☐ Allow Fast Path

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Torch

enabled

running

slave

CAP

☒ Enabled

Interfaces: wlan1

wlan2

Certificate: CAP-242F4387EB5C

Discovery Interfaces: eoip-tunnel-CAPsMAN

☒ Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names: CAPsMAN-4318B03499C8

Bridge: none

☐ Static Virtual

Requested Certificate: CAP-242F4387EB5C

Locked CAPsMAN Common Name:

OK

Cancel

Apply

Configuración de Seguridad (Security)

CAPs Security Configuration <SEC-CLIENTE-A>	CAPs Security Configuration <SEC-CLIENTE-B>
Name: SEC-CLIENTE-A	Name: SEC-CLIENTE-B
Authentication Type: ☐ WPA PSK ☒ WPA2 PSK ☐ WPA EAP ☐ WPA2 EAP ▲	Authentication Type: ☐ WPA PSK ☒ WPA2 PSK ☐ WPA EAP ☐ WPA2 EAP ▲
Encryption: ☒ aes ccm ☐ tkip ▲	Encryption: ☒ aes ccm ☐ tkip ▲
Group Encryption:	Group Encryption:
Group Key Update:	Group Key Update:
Passphrase: 12345678	Passphrase: 87654321
Disable PMKID:	Disable PMKID:
EAP Methods:	EAP Methods:
EAP Radius Accounting:	EAP Radius Accounting:
TLS Mode:	TLS Mode:
TLS Certificate:	TLS Certificate:
OK Cancel Apply Comment Copy Remove	OK Cancel Apply Comment Copy Remove

Configuración de Seguridad (Security)

- **¡IMPORTANTE!**: muchas opciones de configurar WPA2-Enterprise

The image displays two side-by-side screenshots of the Mikrotik WinBox interface, specifically the 'CAPs Security Configuration' window. The left window is titled 'CAPs Security Configuration <SEC-ABONADOS>' and the right window is titled 'CAPs Security Configuration <SEC-VISITANTES>'. Both windows show a form for configuring security settings. In the left window, the 'Name' field is 'SEC-ABONADOS', 'Authentication Type' is 'WPA2 EAP' (checked), 'Encryption' is 'aes ccm' (checked), and 'EAP Methods' is 'passthrough'. The right window shows the same form for 'SEC-VISITANTES', but the 'Authentication Type' and 'Encryption' fields are empty. Both windows have buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

Field	SEC-ABONADOS	SEC-VISITANTES
Name	SEC-ABONADOS	SEC-VISITANTES
Authentication Type	☒ WPA PSK ☐ WPA2 PSK ☐ WPA EAP ☒ WPA2 EAP	☐ WPA PSK ☐ WPA2 PSK ☐ WPA EAP ☐ WPA2 EAP
Encryption	☒ aes ccm ☐ tkip	☐ aes ccm ☐ tkip
Group Encryption		
Group Key Update		
Passphrase		
Disable PMKID		
EAP Methods	passthrough	
EAP Radius Accounting		
TLS Mode		
TLS Certificate		

Rutas de datos (Datapaths)

- **¡IMPORTANTE!**: “Local Forwarding” vs. “Manager Forwarding”

CAPs Datapath Configuration <DAT-CLIENTE>

Name:	DAT-CLIENTE	OK
MTU:		Cancel
L2 MTU:		Apply
ARP:		Comment
Bridge:		Copy
Bridge Cost:		Remove
Bridge Horizon:		
Local Forwarding:	☒	▲
Client To Client Forwarding:	☒	▲
VLAN Mode:		▼
VLAN ID:		▼
Interface List:		▼

Rutas de datos (Datapaths)

CAPs Datapath Configuration <DAT-ABONADOS>	CAPs Datapath Configuration <DAT-VISITANTES-A>	CAPs Datapath Configuration <DAT-VISITANTES-B>
Name: DAT-ABONADOS	Name: DAT-VISITANTES-A	Name: DAT-VISITANTES-B
MTU:	MTU:	MTU:
L2 MTU:	L2 MTU:	L2 MTU:
ARP:	ARP:	ARP:
Bridge: ABONADOS	Bridge: VISITANTES-A	Bridge: VISITANTES-B
Bridge Cost:	Bridge Cost:	Bridge Cost:
Bridge Horizon:	Bridge Horizon:	Bridge Horizon:
Local Forwarding: ☐	Local Forwarding: ☐	Local Forwarding: ☐
Client To Client Forwarding: ☐	Client To Client Forwarding: ☐	Client To Client Forwarding: ☐
VLAN Mode:	VLAN Mode:	VLAN Mode:
VLAN ID:	VLAN ID:	VLAN ID:
Interface List:	Interface List:	Interface List:

Combinación de Configuraciones (Configurations)

CAPsMAN

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

+ - [Icon] [Icon] Find

Name	SSID	Datapath	Security	
ABONADOS	AEROWI-ABONADOS	DAT-ABONADOS	SEC-ABONADOS	
CLIENTE-A	EMPRESA-A	DAT-CLIENTE	SEC-CLIENTE-A	
CLIENTE-B	EMPRESA-B	DAT-CLIENTE	SEC-CLIENTE-B	
CLIENTE-C	EMPRESA-C	DAT-CLIENTE	SEC-CLIENTE-C	
VISITANTES-A	EMPRESA-A-CORTESIA	DAT-VISITANTES-A	SEC-VISITANTES	
VISITANTES-B	EMPRESA-B-CORTESIA	DAT-VISITANTES-B	SEC-VISITANTES	
VISITANTES-C	EMPRESA-C-CORTESIA	DAT-VISITANTES-C	SEC-VISITANTES	

Provisión de CAPs (Provisioning)

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

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

Hw. Supported Modes:

Identity Regexp: CPE_A*

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: CLIENTE-A

Slave Configuration: VISITANTES-A

ABONADOS

Name Format: prefix identity

Name Prefix:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Interfaces de CAP

CAPsMAN									
CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table									
+ - ✓ ✗ 📄 🔍 Reselect Channel Manager AAA Find									
	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	
DMB	↔ CPE_A01-1	CAP Interface	1500	1500	1600	0 bps	0 bps	0	
DSB	↔ CPE_A01-1-1	CAP Interface	1500	1500	1600	0 bps	0 bps	0	
DSB	↔ CPE_A01-1-2	CAP Interface	1500	1500	1600	0 bps	0 bps	0	
DMB	↔ CPE_A01-2	CAP Interface	1500	1500	1600	0 bps	0 bps	0	
DSB	↔ CPE_A01-2-1	CAP Interface	1500	1500	1600	0 bps	0 bps	0	
DSB	↔ CPE_A01-2-2	CAP Interface	1500	1500	1600	0 bps	0 bps	0	

Configuración del resto de Servicios: Portal Cautivo

13:00

Iniciar sesión en EMPRESA-A-C...
empresa-a.local

WC01

aerowi
solucions sen fies

Please log on to use the hotspot service.

Login

Login

Password

Password

OK

13:03

empresa-a.local/status

WC01

aerowi
solucions sen fies

Welcome ramon!

IP address:	172.17.255.254
bytes up/down	1885.2 KiB / 1287.7 KiB
connected:	2m10s
status refresh	1m



Configuración del resto de Servicios: Portal Gestión

wiBox CPE

← → ↻ 🏠 ⓘ No es seguro | 192.168.180.10/cpe-a01/pages/index.html

☆ 📄 👤

wiBox CPE

Buscar...

🔍

🏠 Cuadro de Mando

🔧 Configuración

🔒 Seguridad

📊 Gráficas

📄 Información del Sistema

IP Pública	83.165.239.234
Nombre DDNS	92f20917e7fd.sn.mynetname.net
Nombre	CPE_A01
Modelo	RBD52G-5HacD2HnD
Número de Serie	92F20917E7FD
RouterBOARD	6.42.1
RouterOS	6.42.7 (stable)
Tiempo encendido	35m30s
Tipo CPU	ARMv7
Uso CPU	0%
Memoria libre	202MB
Disco Duro libre	3MB

🔔 Soporte wiBox

🐦 https://twitter.com/aerowi

✉ helpdesk@aerowi.es

📄 Red (IP)

IP LAN: 192.168.11.1/24

WIFI LAN: EMPRESA-A

Contraseña WIFI: 12345678

IP LAN	MAC	HOSTNAME
192.168.0.254	04:B1:67:00:D7:31	

IP WAN: 10.0.1.1/32

GW WAN: pppoe-PE01

RUTA DESTINO	GW	DISTANCIA	ESTADO
0.0.0.0/0	pppoe-PE01	1	pppoe-PE01 reachable

Configuración del resto de Servicios: Portal Gestión

RouterOS 6.42.7 (stable)

Tiempo encendido 35m30s

Tipo CPU ARMv7

Uso CPU 0%

Memoria libre 202MB

Disco Duro libre 3MB

Contraseña WiFi: 12345678

IP LAN	MAC	HOSTNAME
192.168.0.254	04:B1:67:00:D7:31	

IP WAN: 10.0.1.1/32

GW WAN: pppoe-PE01

ruta destino	GW	distancia	estado
0.0.0.0/0	pppoe-PE01	1	pppoe-PE01 reachable
10.0.255.254/32	pppoe-PE01	0	pppoe-PE01 reachable
192.168.11.0/24	bridge-LAN	0	bridge-LAN reachable

Filtrado Web

NIVEL DE PROTECCION ACTUAL: DESACTIVADO

Control Parental

DISPOSITIVOS ACTUALMENTE BLOQUEADOS: 0

USUARIO	DISPOSITIVO	MAC
---------	-------------	-----

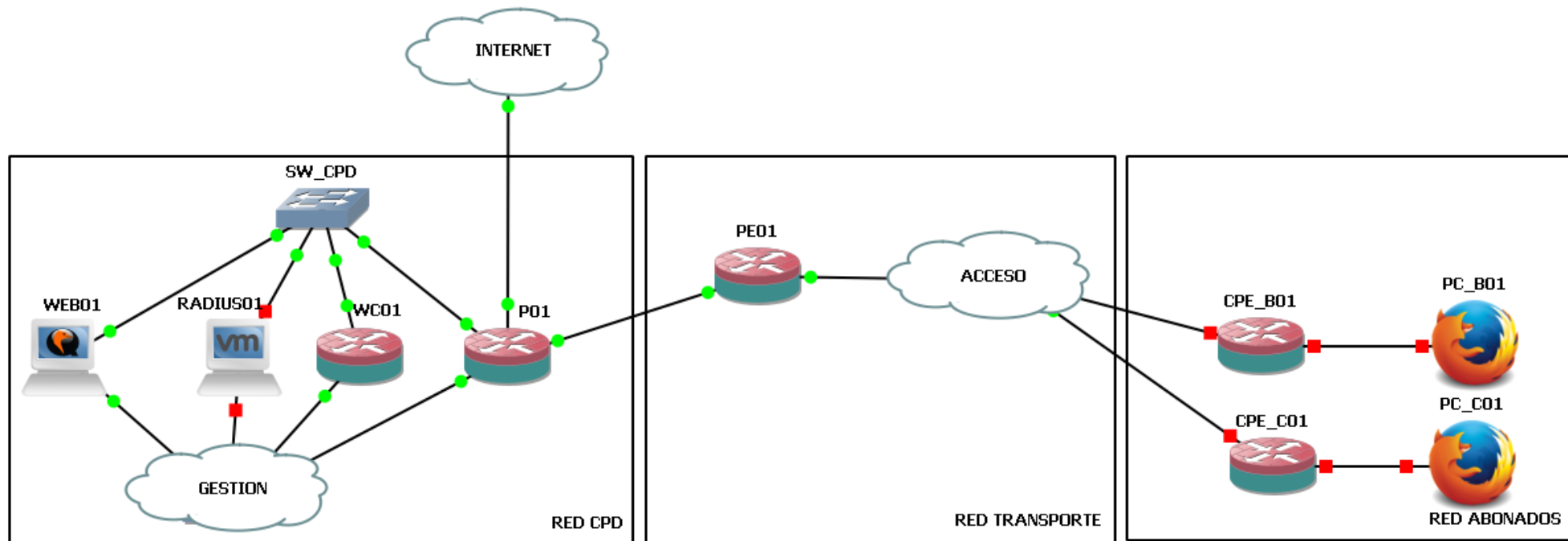
Dispositivos (ARP)

MAC	IP	INTERFAZ
-----	----	----------

Interfaces

Interfaz	MAC	Conectada?
ether1	B8:69:F4:33:ED:DA	true
ether2	B8:69:F4:33:ED:DB	false
ether3	B8:69:F4:33:ED:DC	false
ether4	B8:69:F4:33:ED:DD	false
ether5	B8:69:F4:33:ED:DE	false

- Provisión de un equipo MikroTik gestionado por CAPsMAN, con tres WiFi: cliente, visitantes y abonados del ISP.
- Infraestructura y Servicios del ISP simulados con GNS3



Contacto

Ramón Fernández Rego
moncho.rego@aerowi.es
<http://www.aerowi.es>