

WiFi

CONCEPTOS

ESTANDARES

SOLUCION DE PROBLEMAS

SEGURIDAD

En las redes sin hilos tenemos los estándares de:

Estándar	Ancho de canal	Vel. Teórica Máx.	Banda
802.11	22Mhz	2Mbits	2.4Ghz
802.11b	22Mhz	11Mbits	2.4Ghz
802.11g	20Mhz	54Mbits	2.4Ghz
802.11a	20Mhz	54Mbits	5Ghz
802.11n	20Mhz	300Mbits	2.4 y 5Ghz
802.11ac	160Mhz	6Mibts	5Ghz
802.11ad	2Mhz	7Mbits	60Ghz

- Mikrotik soporta todos los estándares anteriores.
- Depende de los modelos de Mikrotik
- Hay con banda dual de 2.4 y 5Ghz
- Se configuran dentro del Menú *Wireless*.

- En estándar a utilizar se configura dentro de las propiedades del interfaz inalámbrico.
- **Para poder establecer la conexión, la banda y el estándar debe coincidir en ambos extremos.**
- Si definimos 2Ghz-B/G/N significa que:
 - ✓ La banda es 2Ghz.
 - ✓ Podemos conectar con el estándar B, G ó N.

Interface <wlan1>

General Wireless Data Rates Advanced HT HT MCS WDS ...

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 2GHz-B

Frequency: 2GHz-only-N

SSID: 2GHz-B/G/N

Radio Name: CC2DE022AD21

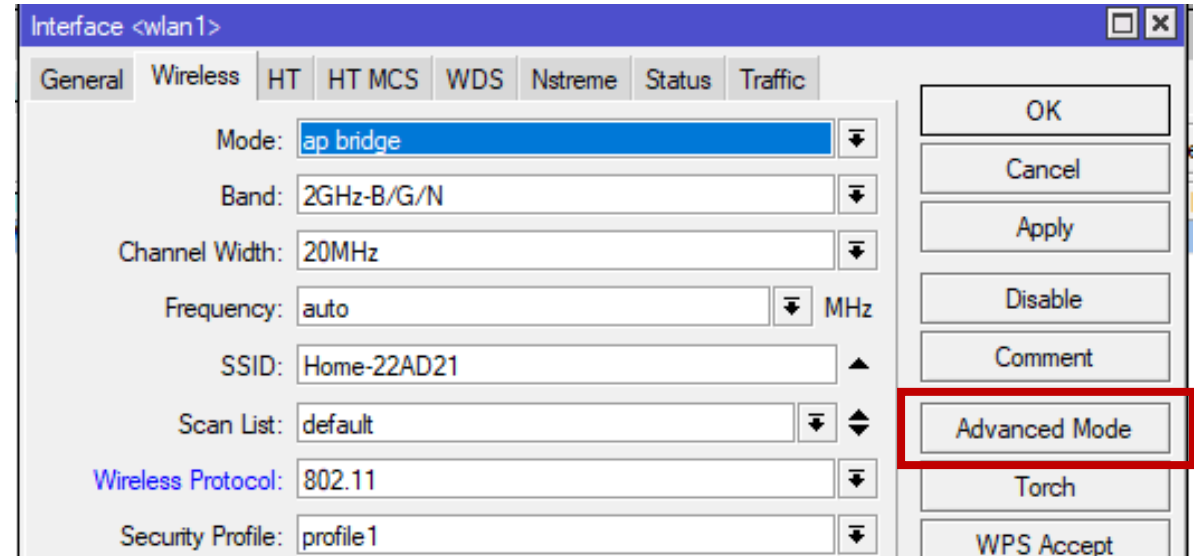
Scan List: default

Wireless Protocol: 802.11

Security Profile: profile 1

WPS Mode: disabled

- Tened en cuenta que para poder ver todas las opciones de configuración del interfaz inalámbrico hemos de pulsar el botón *Advanced Mode*.



- El ancho de canal, nos va ha definir la velocidad máxima de transferencia que vamos a poder obtener.
- **Para poder establecer la conexión, el ancho de canal debe coincidir en ambos extremos.**
- Si definimos 20/40Mhz Ce significa que tenemos dos opciones:
 - ✓ Utilizar un ancho de canal de 20Mhz.
 - ✓ Utilizar dos canales de 20Mhz con el canal de Datos en el siguiente canal al canal principal .

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 5MHz

SSID: 10MHz

Scan List: 20/40MHz Ce

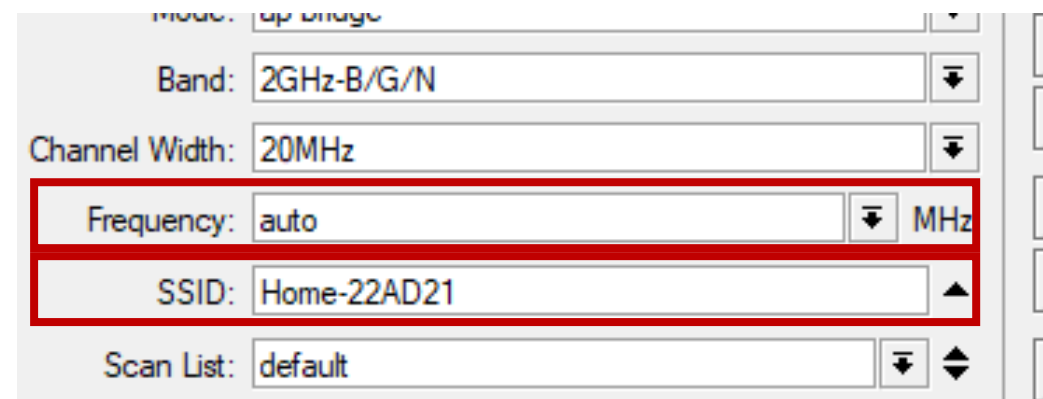
Wireless Protocol: 20/40MHz eC

20MHz

default

802.11

- La frecuencia nos va a indicar donde está emitiendo el punto de acceso.
- El SSID nos indica el nombre de la red a la que me conecto.
- **Para poder establecer la conexión, el SSID debe coincidir en ambos extremos.**
- Si definimos *Frequency* en *Auto*, significa que el Punto de Acceso elige la mejor frecuencia disponible para la transmisión.
- En el cliente siempre busca al AP.



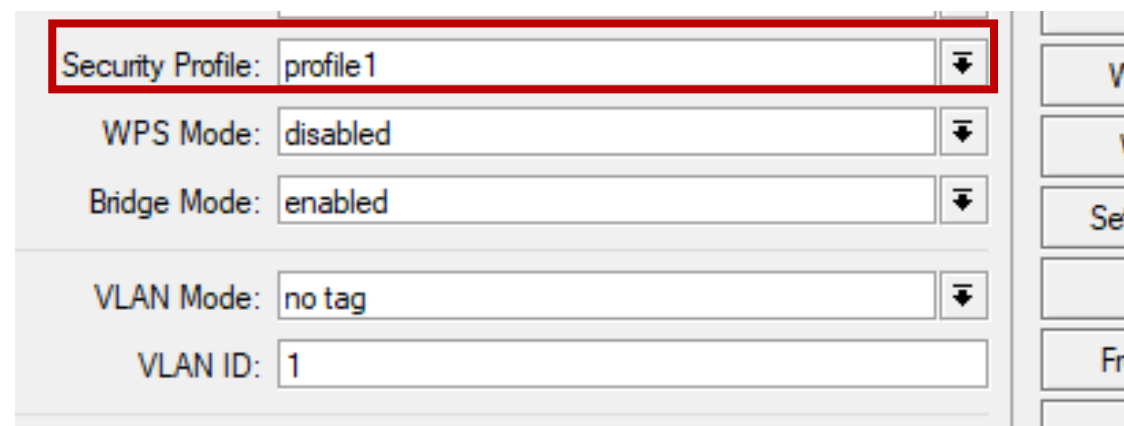
A screenshot of a MikroTik configuration interface. The settings shown are: Mode: up bridge, Band: 2GHz-B/G/N, Channel Width: 20MHz, Frequency: auto MHz, SSID: Home-22AD21, and Scan List: default. The 'Frequency' and 'SSID' fields are highlighted with a red rectangular border.

- La lista de frecuencias nos va a indicar que canales voy a utilizar dentro de los canales disponibles en el país.
- **Para poder establecer la conexión, la lista de canales de ambos extremos debe de tener al menos un canal común.**
- Si definimos *Scan List* en *Auto*, significa que la radio utiliza todas frecuencias disponibles según la normativa del país.

The image shows a portion of the MikroTik WinBox configuration interface for a wireless network. The following settings are visible:

- Mode: ap bridge
- Band: 2GHz-B/G/N
- Channel Width: 20MHz
- Frequency: auto MHz
- SSID: Home-22AD21
- Scan List: default** (This field is highlighted with a red rectangle)

- El perfil de seguridad nos define la contraseña de la red.
- **Para poder establecer la conexión, el perfil de seguridad debe coincidir en ambos extremos.**
- El perfil default que viene por defecto es un perfil sin seguridad, por lo que estoy configurando una red abierta.



The screenshot shows a configuration window with several settings. The 'Security Profile' dropdown menu is highlighted with a red rectangle and is set to 'profile 1'. Other settings include 'WPS Mode' set to 'disabled', 'Bridge Mode' set to 'enabled', 'VLAN Mode' set to 'no tag', and 'VLAN ID' set to '1'. On the right side of the window, there are buttons for 'W', 'V', 'Setu', and 'Fre'.

Security Profile:	profile 1	↓
WPS Mode:	disabled	↓
Bridge Mode:	enabled	↓
VLAN Mode:	no tag	↓
VLAN ID:	1	

- WPS nos va a permitir el conectarnos al punto de acceso sin conocer la contraseña.
- **El WPS aunque es cómodo no es un método seguro de conectarse a una red.**
- Mikrotik nos brinda la opción de los botones virtuales, por si no queremos pulsar el botón físico.
 - *WPS Accept* en el caso de un Punto de Acceso.
 - *WPS Cliente* en el caso de un cliente.

Scan List: default

Wireless Protocol: 802.11

Security Profile: profile1

WPS Mode: disabled

Frequency Mode: push button, virtual push button only

Torch

WPS Accept

WPS Client

Setup Repeater

Scan...

- WPS nos va a permitir el conectarnos al punto de acceso sin conocer la contraseña.
- **El WPS aunque es cómodo no es un método seguro de conectarse a una red.**
- Mikrotik nos brinda la opción de los botones virtuales, por si no queremos pulsar el botón físico.
 - *WPS Accept* en el caso de un Punto de Acceso.
 - *WPS Cliente* en el caso de un cliente.

Scan List: default

Wireless Protocol: 802.11

Security Profile: profile1

WPS Mode: disabled

Frequency Mode: push button, virtual push button only

Torch

WPS Accept

WPS Client

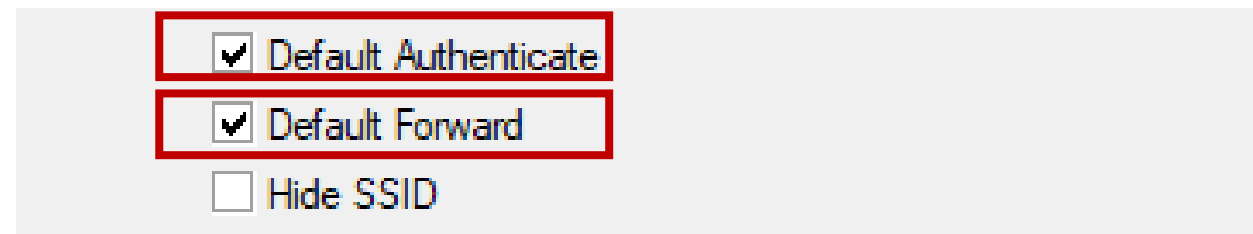
Setup Repeater

Scan...

- El país nos va a determinar la lista de frecuencias disponibles y su potencia de transmisión.
- **Para poder establecer la conexión, el país debe coincidir en ambos extremos. Hay que poner el país correctamente para cumplir normativa.**
- Puede pasar que aunque sean países diferentes la lista de canales coincida.
- **El *Antenna Gain* es importante poner el correcto para cumplir normativa.**

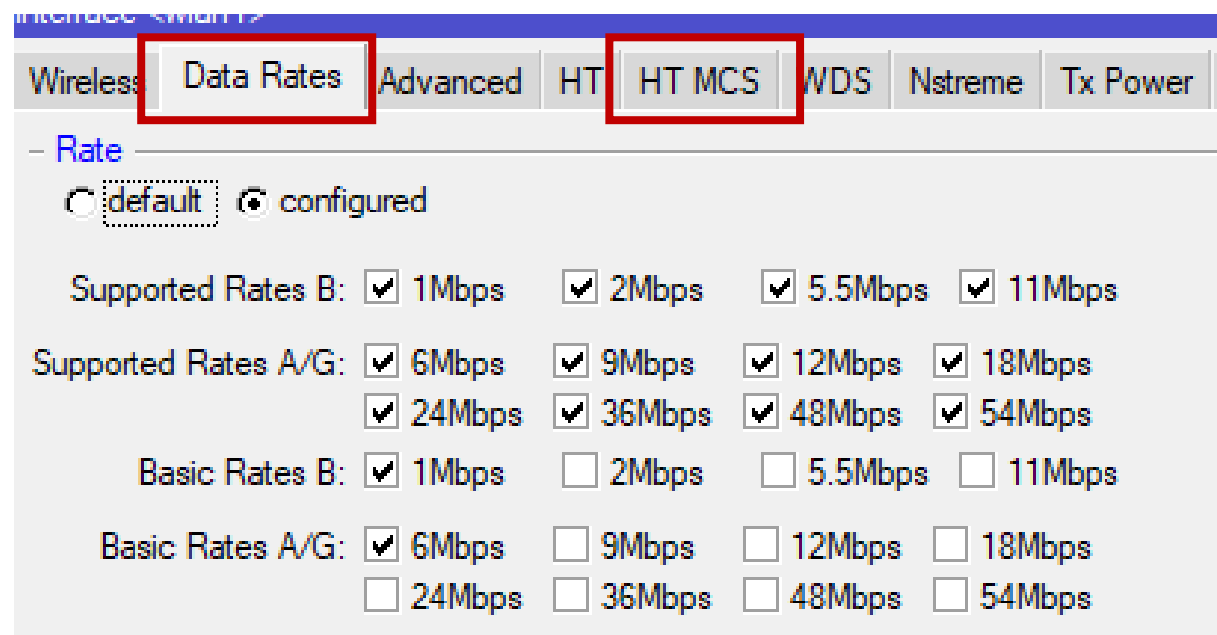
Frequency Mode:	regulatory-domain	▼
Country:	spain	▼
Antenna Gain:	0	dBi

- **Default Authenticate** nos va a indicar si:
 - El punto de acceso acepta las conexiones de todos los clientes.
 - El cliente se conecta al punto de acceso.
- *Default Forward* nos va a indicar si el Punto de acceso permite L2 entre lo clientes.
- **No es obligatorio que coincidan en ambos extremos. En este caso dependerá de las lista de acceso/conexión.**



☒	Default Authenticate
☒	Default Forward
☐	Hide SSID

- Los Data Rates (b/g/a) y los HTMCS (n/ac) nos van a indicar las velocidades a negociar.
- **Para establecer la conexión han de coincidir al menos en uno en ambos extremos.**
- **Para establecer la conexión, los Basic Rates han de estar incluidos en los Supported.**



interf: wlan1

Wireless **Data Rates** Advanced HT **HT MCS** WDS Nstreme Tx Power

– Rate

☐ default ☒ configured

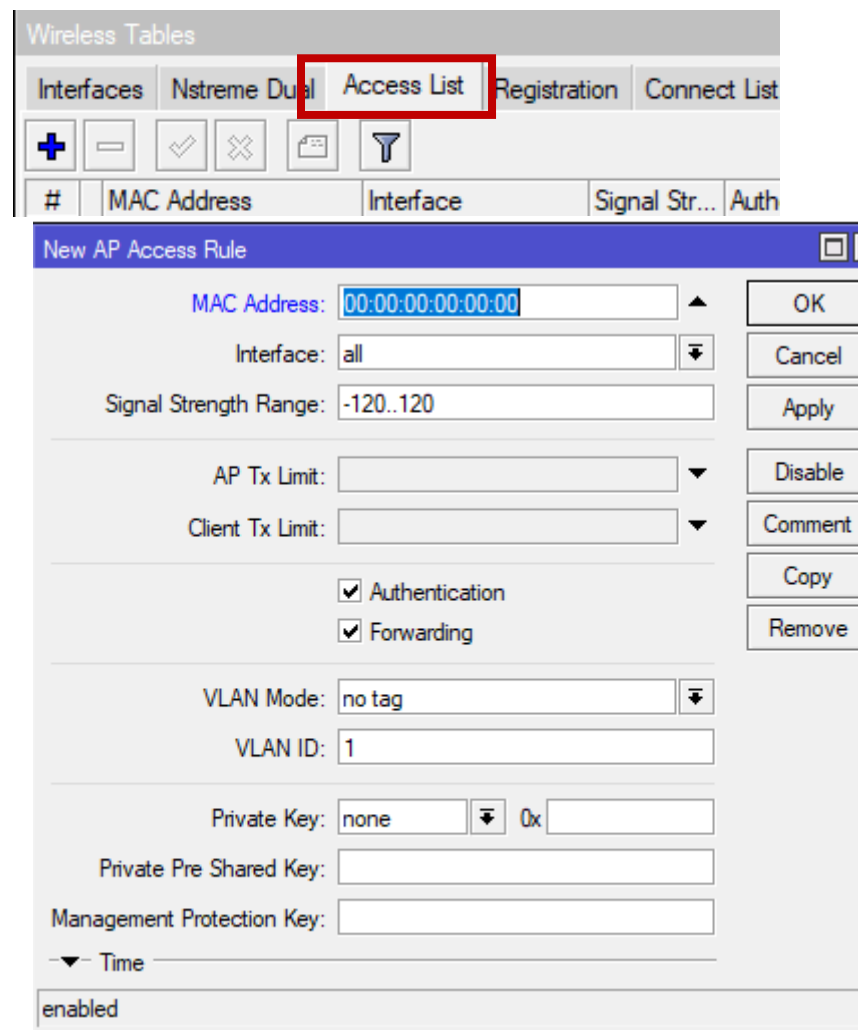
Supported Rates B: ☒ 1Mbps ☒ 2Mbps ☒ 5.5Mbps ☒ 11Mbps

Supported Rates A/G: ☒ 6Mbps ☒ 9Mbps ☒ 12Mbps ☒ 18Mbps
☒ 24Mbps ☒ 36Mbps ☒ 48Mbps ☒ 54Mbps

Basic Rates B: ☒ 1Mbps ☐ 2Mbps ☐ 5.5Mbps ☐ 11Mbps

Basic Rates A/G: ☒ 6Mbps ☐ 9Mbps ☐ 12Mbps ☐ 18Mbps
☐ 24Mbps ☐ 36Mbps ☐ 48Mbps ☐ 54Mbps

- La lista de acceso nos permite parametrizar la conexión de un cliente en particular (si especifico su MAC) o la de todos.
- Si defino una regla de acceso para un cliente, los parámetros que defina deben coincidir en la configuración del cliente.



Wireless Tables

Interfaces Nstreme Dual **Access List** Registration Connect List

+ - ✓ ✗ [icon] [icon]

#	MAC Address	Interface	Signal Str...	Auth
---	-------------	-----------	---------------	------

New AP Access Rule

MAC Address: 00:00:00:00:00:00

Interface: all

Signal Strength Range: -120..120

AP Tx Limit: [dropdown]

Client Tx Limit: [dropdown]

☒ Authentication

☒ Forwarding

VLAN Mode: no tag

VLAN ID: 1

Private Key: none [dropdown] 0x [text]

Private Pre Shared Key: [text]

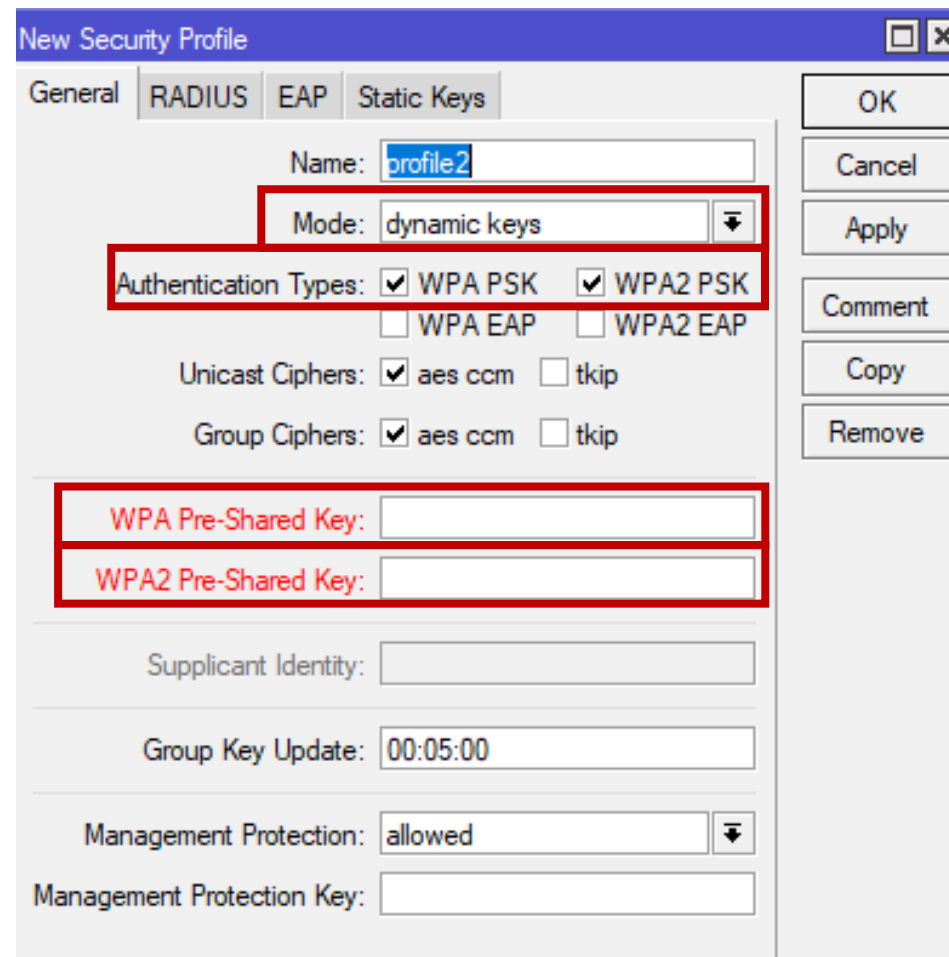
Management Protection Key: [text]

Time [dropdown]

enabled

OK Cancel Apply Disable Comment Copy Remove

- El perfil de seguridad nos permite definir la contraseña de nuestra red.
- **El perfil de seguridad debe coincidir en ambos extremos.**
- **O bien que un extremo tenga el perfil de seguridad incluido en el otro.**
- **Management Protection Key es una opción específica**



New Security Profile

General | RADIUS | EAP | Static Keys

Name: profile2

Mode: dynamic keys

Authentication Types: ☒ WPA PSK ☒ WPA2 PSK
☐ WPA EAP ☐ WPA2 EAP

Unicast Ciphers: ☒ aes ccm ☐ tkip

Group Ciphers: ☒ aes ccm ☐ tkip

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Supplicant Identity:

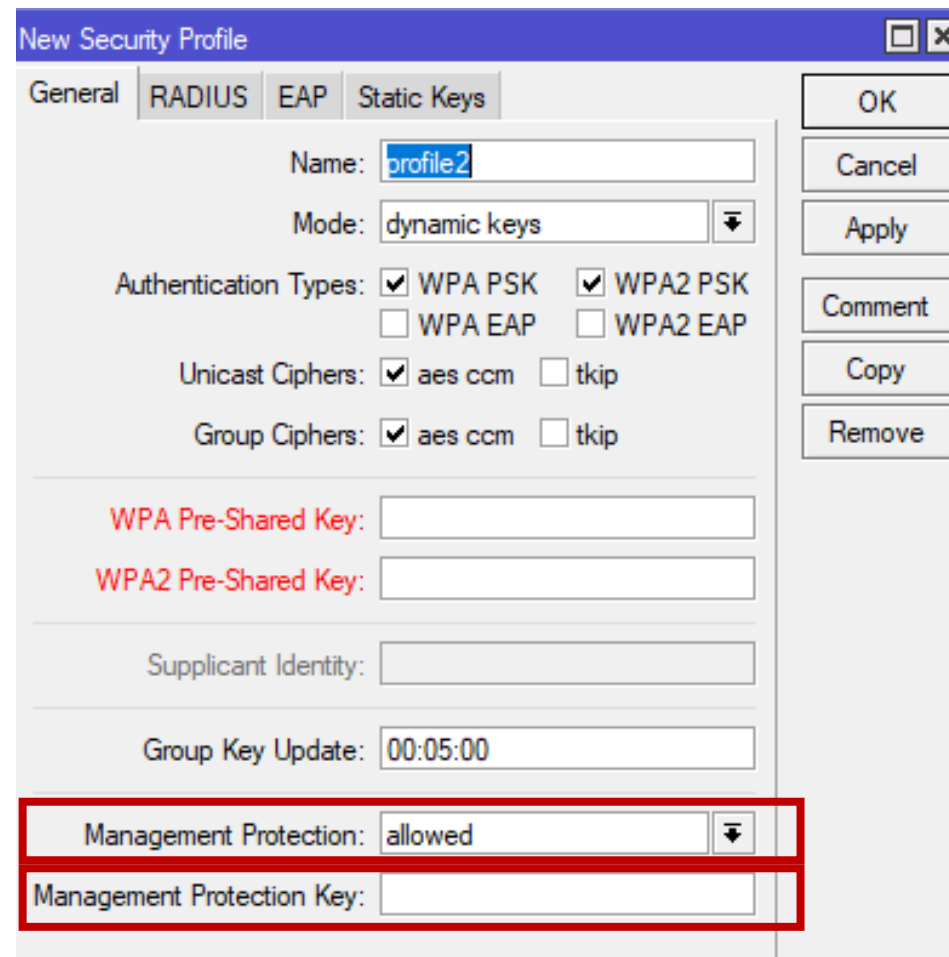
Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

OK Cancel Apply Comment Copy Remove

- Management Protection es una opción específica de mikrotik que nos permite ser menos vulnerables a los rogue AP.
- **La clave de protección debe coincidir en ambos extremos para que se establezca la conexión.**
- **No es compatible con otros fabricantes.**



New Security Profile

General | **RADIUS** | EAP | Static Keys

Name: profile2

Mode: dynamic keys

Authentication Types: ☒ WPA PSK ☒ WPA2 PSK
☐ WPA EAP ☐ WPA2 EAP

Unicast Ciphers: ☒ aes ccm ☐ tkip

Group Ciphers: ☒ aes ccm ☐ tkip

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Supplicant Identity:

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

OK Cancel Apply Comment Copy Remove