

Resurrección de un MikroTik wAP AC

Instalación de OpenWrt en un RBwAPG-5HacD2HnD mediante programador SPI (CH341A) — cuando el bootloader no coopera

Autor:

Matías (zhack) — itServicios / matt.ar

Dispositivo:

MikroTik wAP AC (RBwAPG-5HacD2HnD) r3

Fecha:

Junio 2026

Estado:

✓ Completado

TL;DR: Este documento detalla el proceso completo para instalar OpenWrt en un MikroTik wAP AC cuando los métodos oficiales (TFTP y Netinstall) fallan. Se emplea un programador CH341A para leer y escribir la flash SPI, combinando el bootloader original con una imagen sysupgrade de OpenWrt. Incluye comandos, advertencias y lecciones aprendidas.

1. El problema

El MikroTik wAP AC (RBwAPG-5HacD2HnD) es un dispositivo compatible con OpenWrt, pero su bootloader (RouterBOOT) puede presentar incompatibilidades con versiones de RouterOS modernas. En mi caso, el router venía con `factory-firmware: 6.44.6` y `current-firmware: 6.45.9`. Tras hacer un downgrade a 6.44.6 mediante Netinstall, el método TFTP seguía sin funcionar: el router no solicitaba el archivo `vmlinux`.



Bootloader incompatible: El bootloader de RouterOS v7 no es compatible con OpenWrt. Si tienes RouterOS v7, debes degradar a v6 (versión igual o superior a la

de fábrica). Mi versión de fábrica era 6.44.6, por lo que instalé esa versión.

2. Hardware utilizado

- **Programador SPI:** CH341A (con adaptador SOIC-8).
- **Chip de memoria:** Winbond W25Q128.V..M (16 MB, encapsulado WSON-8).
- **Estación de aire caliente** para desoldar/soldar el chip (opcional, pero recomendado).
- **PC con Ubuntu 24.04** y herramientas `flashrom`, `dd`, `binwalk`.

3. Extracción de la flash original

Antes de cualquier modificación, se debe hacer una copia de seguridad completa de la flash. Esto permitirá restaurar el estado original si algo sale mal.

3.1 Conexión del CH341A

Se desoldó el chip WSON-8 y se colocó en el zócalo del programador, asegurando la orientación correcta (pin 1 alineado).

3.2 Lectura con flashrom

```
sudo flashrom -p ch341a_spi -c "W25Q128.V..M" -r backup_original.bin
```

El archivo resultante debe tener un tamaño de 16.777.216 bytes (16 MB).

✓ **Verificación:** `ls -l backup_original.bin` → `-rw-r--r-- 1 root root 16777216`

4. Construcción de la imagen combinada

La imagen `sysupgrade` de OpenWrt no contiene el bootloader. Para que el router arranque, debemos mantener el bootloader original de MikroTik y escribir OpenWrt a

partir de una posición determinada. Se extrae el bootloader (primeros 1 MB) y se concatena con la imagen sysupgrade.

```
# Extraer bootloader (1 MB)
dd if=backup_original.bin of=bootloader.bin bs=1M count=1

# Crear archivo de 16 MB con ceros
dd if=/dev/zero of=imagen_completa.bin bs=16M count=1

# Escribir bootloader al inicio
dd if=bootloader.bin of=imagen_completa.bin conv=notrunc

# Escribir OpenWrt a partir del offset 1 MB
dd if=openwrt-25.12.4-ipq40xx-mikrotik-mikrotik_wap-ac-squashfs-sysupgrade.bin of=imagen_com
```

 **Nota:** El offset de 1 MB puede variar según el modelo. Para este dispositivo, el bootloader ocupa exactamente 1 MB. En otros modelos puede ser 256 KB o 512 KB.

5. Escritura de la imagen en la flash

```
sudo flashrom -p ch341a_spi -c "W25Q128.V..M" -w imagen_completa.bin
```

El proceso tarda unos minutos. Al finalizar, se muestra el mensaje `VERIFIED`.

✓ **Resultado:** Erase/write done from 0 to fffffff → Verifying flash...
`VERIFIED.`

6. Soldadura del chip y primer arranque

Se soldó el chip de nuevo en la placa del router (con orientación correcta). Al encender el router, se obtuvo respuesta a ping en `192.168.1.1` y acceso SSH sin contraseña (usuario `root`).

 **¡OpenWrt funcionando!** El router arrancó correctamente con OpenWrt 25.12.4.

7. Configuración básica post-instalación

7.1 Establecer contraseña de root

```
passwd
```

7.2 Conectar el router a Internet (WiFi como cliente)

Para que el router tenga acceso a Internet y pueda instalar paquetes, se configuró la interfaz WiFi interna como cliente (STA) conectándose a una red existente.

```
# Activar la radio (si está deshabilitada)
uci set wireless.radio0.disabled='0'
uci commit wireless
wifi reload

# Crear interfaz cliente
uci set wireless.sta=wifi-iface
uci set wireless.sta.device='radio0'
uci set wireless.sta.mode='sta'
uci set wireless.sta.ssid='nombre_de_tu_red'
uci set wireless.sta.encryption='psk2'
uci set wireless.sta.key='tu_contraseña'
uci set wireless.sta.network='wan'
uci commit wireless
wifi reload

# Configurar WAN como DHCP
uci set network.wan=interface
uci set network.wan.proto='dhcp'
uci set network.wan.device='wlan0'
uci commit network
/etc/init.d/network restart
```

 **Problema conocido con apk:** Al intentar instalar paquetes, puede aparecer `wgetSSL verify error: unknown error`. Esto se debe a que la fecha del sistema es incorrecta. Se debe corregir con `date MMDDhhmmYYYY` (ej. `date 062522302026` para el 25 de junio de 2026 a las 22:30).

8. Instalación de herramientas para el slot mini PCIe

El router tiene un slot mini PCIe (soldado posteriormente). Para verificar dispositivos PCIe y USB:

```
# Instalar herramientas
apk add pciutils usbutils

# Listar dispositivos PCIe
lspci -v

# Listar dispositivos USB
lsusb
```

 **Nota sobre el slot mini PCIe:** En este modelo, el slot mini PCIe no está conectado al bus PCIe, solo a USB (para módems 3G/4G). Por lo tanto, `lspci` no muestra ningún dispositivo. Para usar una tarjeta WiFi, se debe conectar un adaptador mini PCIe a USB o una tarjeta con interfaz USB.

9. Lecciones aprendidas

- **El TFTP no siempre funciona:** Aunque el bootloader sea compatible, algunos modelos tienen limitaciones o requieren nombres de archivo específicos (`vmlinux` , `kernel.bin` , etc.).
- **Netinstall no acepta imágenes de OpenWrt:** Solo archivos `.npk` . No se puede usar directamente para flashear OpenWrt.
- **El CH341A es una herramienta poderosa:** Permite leer y escribir la flash directamente, evitando las limitaciones del bootloader.
- **La imagen combinada (bootloader + sysupgrade) funciona:** Mantener el bootloader original y escribir OpenWrt a partir del offset correcto es la clave.
- **La fecha del sistema afecta a `apk` :** Si la fecha es incorrecta, los certificados SSL fallan. Corregir la fecha antes de instalar paquetes.

10. Archivos utilizados

- `backup_original.bin` — Volcado completo de la flash original (16 MB).
- `openwrt-25.12.4-ipq40xx-mikrotik-mikrotik_wap-ac-squashfs-sysupgrade.bin` — Imagen sysupgrade de OpenWrt para el wAP AC.
- `imagen_completa.bin` — Imagen combinada (bootloader + OpenWrt) para escribir en la flash.

11. Enlaces de interés

- [Página oficial de OpenWrt para el MikroTik wAP AC](#)
- [Procedimientos comunes para MikroTik RouterBoard](#)
- [Página oficial de flashrom](#)

12. Conclusión

Se ha logrado instalar OpenWrt en un MikroTik wAP AC que se negaba a cooperar por los métodos tradicionales. La combinación de un programador CH341A, la extracción del bootloader y la escritura de una imagen combinada ha demostrado ser una solución fiable y repetible. Este documento sirve como guía para otros entusiastas que enfrenten el mismo desafío.

 Licencia: CC BY-NC-ND 4.0 — Puede redistribuirse libremente con fines educativos y defensivos.

 Canal Telegram

 @mattzhack

 matt.ar

 GitHub

 Uso exclusivamente con fines educativos y de autogestión. No me hago responsable del mal uso de esta información.