

1 Edimax WAP1750

From:

https://openwrt.org/toh/devolo/devolo_wifi_pro_1750e

¹ The devolo WiFi pro 1750e is a wall mountable access point with:
Dual band 2.4 and 5 GHz WiFi (3 by 3 IEEE 802.11n 450Mbps,
3 by3 IEEE 802.11ac 1299Mbps)

- 2x 1Gbit ethernet ports (with Power over Ethernet support)
- 1x USB 2.0 port
- External serial console port (Currently unsupported but internal 4-pin internal Dupont connector is functional)
- 1x GPIO attached piezo beeper

The access point is manufactured by OEM Acelink Technologies Co., Ltd. as a EW-7679WAC and was originally sold by Edimax as a WAP1750. The Edimax unit was reviewed by SmallNetBuilder.

¹Always type out full URL in links. Don't put hyperlinks. This is done, so that when you print out a webpage, the URLs are still readable.

1.1 Flashing Openwrt on to the WAP1750

At the moment, this page:

https://openwrt.org/toh/devolo/devolo_wifi_pro_1750e discusses flashing new firmware via SSH. However, the WAP1750 has a custom console, and while it's running GPLv2 GNU Linux, somehow it managed to lock down the software, so that simply shelling into it, is no longer possible. I'm sure that is a sin. GPLv2 does not mean people can take it and then abuse it for commercial use. It's a community good.

None the less, it can be turned into an upgradeable router via the following means:

- Teardown enclosure
- Remove flash chip by desoldering with hot air
- Read flash with appropriate tool (Flashrom, TL866A).
- Patch existing image sysupgrade for Devolo 1700 series.
- Write flash with new image
- Resolder chip to board
- Access board via FTDI / USB-Serial chip

Simple enough, right? It is simple. But it's not simple. At least 5 years of hobbyist electronics and I'm able to do this, but for the layman... Only with a guide. And let's also talk about the issues that arose during the above steps. It's never as easy as it would be in a normal world. Earth is not normal. Earth is tilted.

1.2 Teardown Enclosure

The first time, I went careful with a plastic spudger. This device is actually well designed as far as teardowns go. The second time, I got angry and snapped off the front plate with a screwdriver. In fact, the screwdriver approach (here) was superior. Much faster. Although scratches are left. Scratches only hurt those who favor form over function. Fools.

1.3 Remove Flash chip by desoldering with hot air

Once you teardown into the board, you'll examine the ICs. The flash is nowhere to be seen. Is it onboard the CPU? No, it's on the bottom of the board. So it must be lifted out of the enclosure. With hot air desoldering, you must also use lead solder first on the pins. This guide is not a tutorial on hot air soldering. I assume you know this kind of stuff. I won't go into it, unless notable.

Not all tweezers can grab these large chips easy. I have one pair that fits them, and about 3 that don't. Can't have enough tweezers, it seems.

1.4 Read flash with appropriate tool

I have a new rule. Every EE should have a toolbox of flash reading / writing equipment. It's necessary.

My weapon of choice for this project was the Beaglebone black with flashrom. A TL866A could also work. Flashrom is compatible with lots of hardware. An RPI can be used. Doesn't matter, but you must set it up. And when you have the chip, you will need:

- Breakout boards for the IC, as those clips are useless ²
- Soldering Iron
- Hot Air station
- Lead solder
- Tweezers
- Experience to not damage pins during the operation
- Short wires between breakout and BBB
- Proper connecting of wires to BBB

²I have two of those flash-in-place clips. Pomona used to sell them for \$40 each, then China came in and sells them for less than 12 dollars each now. Some for 5. They can work, but the one I had barely reached to all the pins. It wasn't big enough. Not worth it. Get breakout pcbs unless you do this a lot.

I got a tote/toolbox of a few pages of documentation on flashing via BBB, and also the pinouts of the P8 and P9 headers of the BBB. Printouts help.

A guide on the BBB flashrom setup is here:

BBB SRM manual has the P8 and P9 headers.

Since I've used flashrom in the past to flash Libreboot, this was not new territory for me. Experience with this helps. ³

1.5 Patch existing image sysupgrade for Devolo 1700 series.

This was easy enough (what I tried worked the first time). Based on this link on the forum for tp link devices <https://forum.openwrt.org/t/debricking-tl-wr1043nd-v4-hard-way-by-external-flashing-solved/7675/6> So the command was similar.

```
sudo dd if=lede-17.01.4-ar71xx-generic-tl-wr1043nd-v4-squashfs-sys
```

Except I knew the proper directory was at 0x70000 on my chip, thanks to the partition map at the devolo page, and also the partitions page here which explains all this:

³Such as, keep wires short, make multiple reads, and compare with md5sum afterwards, don't fry chip.