16th December 2014

Tftp secret of TL-WR740N uncovered

I've found out that even this particular entry level router [http://wiki.openwrt.org/toh/tp-link/tl-wr740n] supports anti-bricking, so there's no need for soldering, unless of course you are modding. The method I used is the following:

1. Set up a tftp server [http://wiki.openwrt.org/doc/howto/generic.flashing.tftp] on your PC and verify if it works correctly (configuration, permissions, firewalls, etc.)
2. Rename your target firmware to **wr740v4_tp_recovery.bin** and copy it to your base folder (by default /tftpboot). I tested with openwrt-ar71xx-generic-tl-wr740n-v4-squashfs-factory.bin r43602.
3. Set up the following static IP for your PC: **192.168.0.66**/255.255.255.0. If you're not sure about the firmware name on a different model, start a packet sniffer on your PC (*tcpdump -i eth0 -n -l*) and look for the name in the RRQ message.
4. Preferably disconnect WAN from the router
5. Connect the PC to a LAN port
6. Power off the router
7. Press and hold the reset button
8. Power on the router
9. *After the leftmost (power) LED and the rightmost (padlock) LED turn on alone in a few seconds, release the reset button*
10. The router will now identify as 192.168.0.86, finish upgrading using its built-in tftp client and reboot in less than half a minute. In case of failure, it retries multiple times and gives up in about 5-10 seconds to resume normal booting. No configuration is erased, so it's safe to experiment. OpenWRT will need to finish initialization on first/second startup if that's what you are installing

I was preparing to replace the factory default U-Boot with an alternative that supports recovery measures to save you from bricking: web failsafe [https://code.google.com/p/wr703n-uboot-with-web-failsafe/] or pepe2k mod [https://github.com/pepe2k/u-boot_mod] . This is a must have if you are experimenting with OpenWRT/DD-WRT a lot and don't want to solder serial port or JTAG on your board. I found this out after trial and error and fiddling a bit with tcpdump. By the way, in my opinion, tftp is a much cleaner solution for mass router flashing compared to scripting the web interface.

For future reference, I share some information for identification below.

On the box it says ver: **4.27**.

On the updated version of the stock firmware the web interface said:

```
Firmware Version:
3.17.0 Build 140520 Rel.75075n
Hardware Version:
WR740N v4 00000000
```

Some lines from dmesg:

```
Linux version 3.14.26 (openwrt@gb-17) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r43602) ) #1 Thu Dec 11 07:13:50 UTC 2014
CPU0 revision is: 00019374 (MIPS 24Kc)
SoC: Atheros AR9330 rev 1
Kernel command line:  board=TL-WR741ND-v4 console=ttyATH0,115200 rootfstype=squash
fs,jffs2 noinitrd
Memory: 28456K/32768K available (2517K kernel code, 122K rwdata, 516K rodata, 228K init, 191K bss, 4312K reserved)
Clocks: CPU:400.000MHz, DDR:400.000MHz, AHB:200.000MHz, Ref:25.000MHz
Calibrating delay loop... 265.42 BogoMIPS (lpj=1327104)
MIPS: machine is TP-LINK TL-WR741ND v4
m25p80 spi0.0: found s25sl032p, expected m25p80
m25p80 spi0.0: s25sl032p (4096 Kbytes)
eth0: Atheros AG71xx at 0xba000000, irq 5, mode:GMII
eth1: Atheros AG71xx at 0xb9000000, irq 4, mode:MII
eth0: link up (1000Mbps/Full duplex)
```

I have found a report in the dd-wrt forum from the user 'kar200' about similar findings [http://www.dd-wrt.com/phpBB2/viewtopic.php?p=784826&sid=36286d66a7d699db4c215936e8faf159#784826] .

I wouldn't be surprised if this finding would generalize to the similar chipsets including tl-wr703n [http://wiki.openwrt.org/toh/tp-link/tl-wr703n#failsafe_mode] ("*If the button is pushed immediately after powering on, the single blue LED will start blinking, supposedly indicating some failsafe firmware recovery mody [sic] of the embedded bootloader (not yet discovered how to use it)*"), WR741ND, WR841ND, MR3020, etc.

Please leave a comment (and/or update the respective wiki page) if you succeed in reproducing this hidden recovery mode in any other version or model.

edit: many more router models confirmed to have the same recovery [http://bkil.blogspot.com/2014/12/hidden-tftp-of-tp-link-routers.html] (fixed link)
edit #2: here's a video to show you the process [https://www.youtube.com/watch?v=J83CHqw6kxM]

Posted 16th December 2014 by bkil

Labels: 740n, boot, bricked, dd-wrt, failed, firmware, fix, flash, openwrt, repair, reset, restore, router, stock, tftp, tp-link, unbrick, upgrade, without soldering

View comments