Step-by-step guide to unbrick TP-Link Archer C9 v1 and revert to stock using serial recovery

Contents

1 Read first

Only follow this guide if you have tried everything else and serial recovery is your last option!

Basics
Peacock Thread-FAQ
https://www.dd-wrt.com/phpBB2/viewtopic.php?t=51486
Recover From A Bad Flash
https://www.dd-wrt.com/wiki/index.php/Recover_from_a_Bad_Flash
Serial Recovery
https://www.dd-wrt.com/wiki/index.php/Serial_Recovery
Serial Console information on Open-WRT
http://wiki.openwrt.org/doc/hardware/port.serial

TP-Link Archer C9 Threads
TP-Link Archer C9 Brick Fix (Revert To Stock Possibly)
https://www.dd-wrt.com/phpBB2/viewtopic.php?t=283784&postdays=0&postorder=asc&start=0
TP-Link Archer C9 Thread
https://www.dd-wrt.com/phpBB2/viewtopic.php?t=282831&postdays=0&postorder=asc&start=0

2 Equipment needed

USB UART TTL Interface
Check the threads above on which adapter to get. In any case, it needs to support 3.3V Tx output.
I used the following one, but any equivalent one will probably do the job:
http://www.amazon.de/gp/product/B00AFRXKFU
http://www.amazon.co.uk/gp/product/B00AFRXKFU

Connectors
To connect the cables, you can get some pin headers (https://www.google.com/search?tbm=isch&q=pin+headers) or jumper wires (https://www.google.com/search?tbm=isch&q=jumper+wires) and either solder them to the board or just temporarily insert them through the connectors.

3 Step-by-step guide

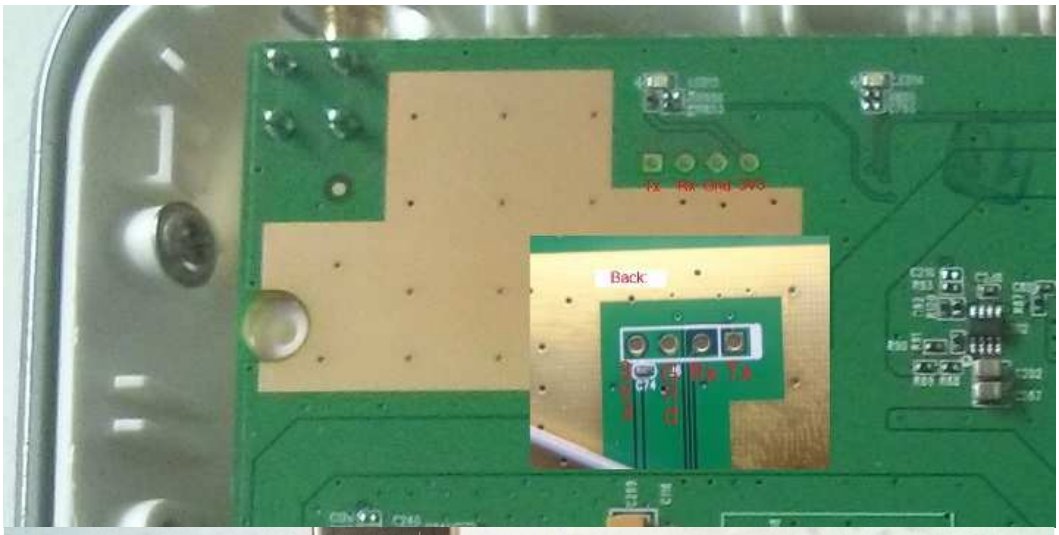
There are some variations to the order of the steps possible, but the following sequence worked for me.

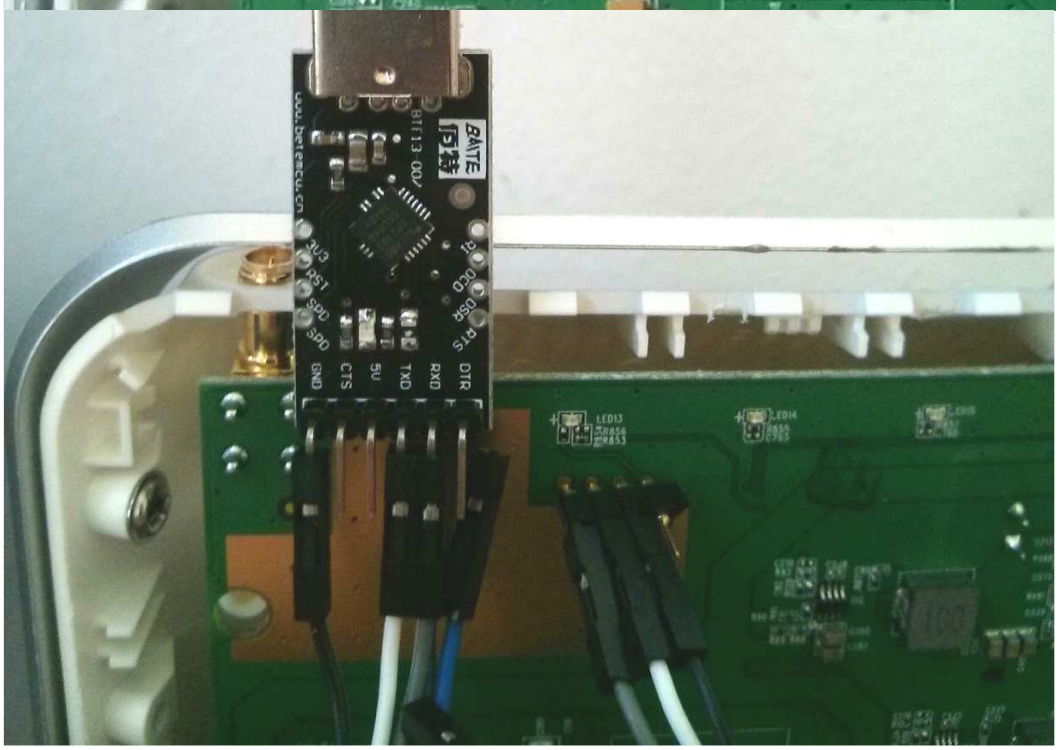
3.1 Open the case

Follow these steps:
http://wiki.openwrt.org/toh/tp-link/archer-c9#opening_the_case

3.2 Connect interface to router

Serial pinout http://wiki.openwrt.org/toh/tp-link/archer-c9#serial
Tx → Rx
Rx → Tx
Gnd → Gnd
Do NOT connect 3V3!

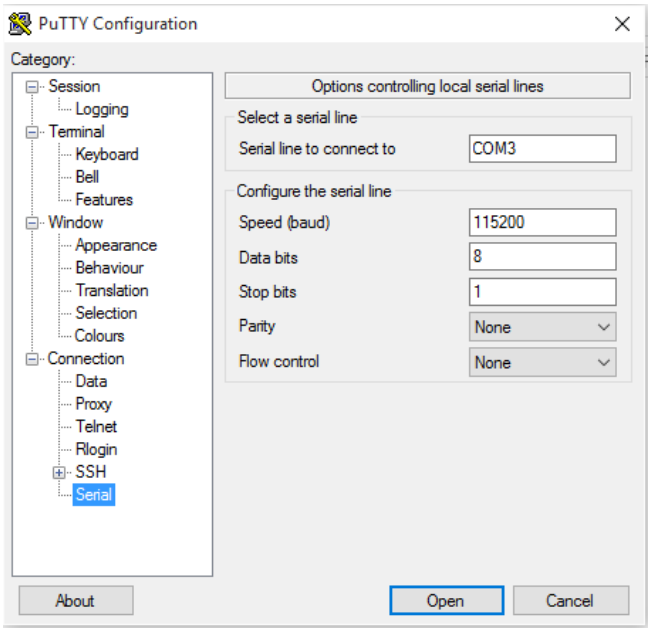




3.3 Configure Putty

You can use various terminal applications. I used Putty on Windows which you can download here: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Serial port: Check device manager for correct COM port of your adapter
Baud: 115200bps
Data bits: 8
Stop bits: 1
Parity: none
Flow control: none



3.4 Connect to router

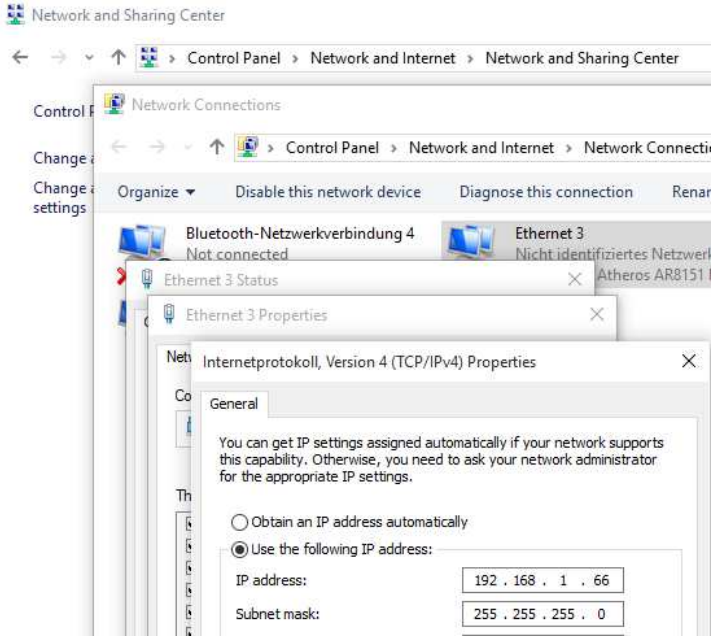
Connect the USB UART adapter to your computer, open the Putty connection and turn on the router while holding ctrl+c until CFE comes up.

Check the IP of the router with “ifconfig”:

```
CFE> ifconfig
Device eth0:  hwaddr 00-[redacted], ipaddr 192.168.1.1, mask 255.255.255.0
        gateway not set, nameserver not set
*** command status = 0
```

3.5 Configure tftp server to host firmware files

Configure your LAN interface to have one of the following static IPs depending on the router IP: 192.168.1.66 or 192.168.0.66

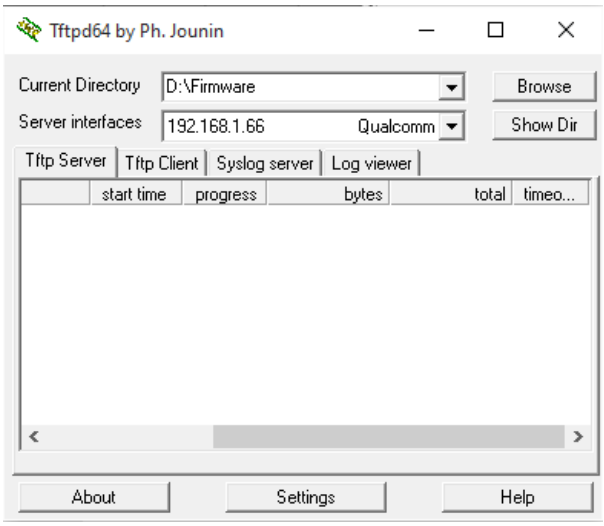


Connect your computer with a LAN cable to port 1 of the router.

Get a tftp server. I used TFTPD which you can get here:
http://tftpd32.jounin.net/tftpd32_download.html

Get the stock firmware files (check Archer C9 forum threads if links dead):
https://www.dd-wrt.com/phpBB2/viewtopic.php?p=977268#977268 or
http://www.mirrorupload.net/file/1YUCXYGZ/#!CFE-FIX.zip

Configure the server to host the folder with the firmware files on interface 192.168.1.66 or 192.168.0.66:

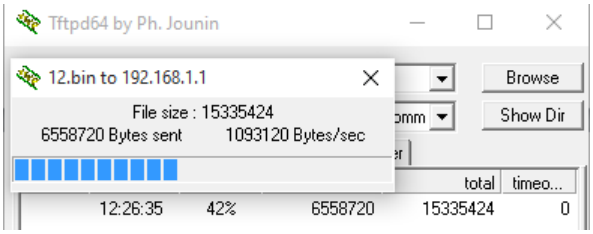


3.6 Flash stock firmware

Flash “12.bin” in the CFE console (adapt IP if necessary)

```
flash -noheader 192.168.1.66:12.bin flash0.trx
```

TFTP server should look like this:



Console like this after successful programming:

```
CFE> flash -noheader 192.168.1.66:12.bin flash0.trx
Reading 192.168.1.66:12.bin: Done. 15335424 bytes read
Programming...done. 15335424 bytes written
*** command status = 0
CFE>
```

Flash “mtd3.bin” in the CFE console (adapt IP if necessary)

```
flash -noheader -offset=0xfe0000 192.168.1.66:mtd3.bin flash0
```

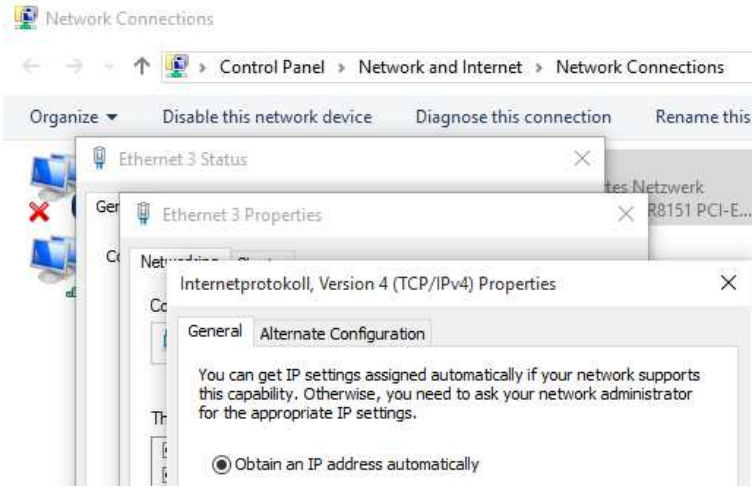
```
CFE> flash -noheader -offset=0xfe0000 192.168.1.66:mtd3.bin flash0
Reading 192.168.1.66:mtd3.bin: Done. 65536 bytes read
Programming...done. 65536 bytes written
*** command status = 0
```

Apply changes

```
go
```

After the process is finished, the router should have the default address 192.168.0.1 and the web interface should be accessible

Change your LAN adapter back to dynamically get an IP:



Load 192.168.0.1 in your browser, and log in with admin/admin

3.7 Next steps

Being now on the stock firmware you can either update to the latest official firmware or go back to DD-WRT. r27506 factory-to-ddwrt worked for me (even without 30-30-30 hard reset).

If you have UART still connected and want to dig into the OS the login info is:
user = root
pass = sohoadmin

Big Thanks to @Heinzek and @Aboshi!