English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Contents

Intro

What is JTAG? JTAG is a communication/debug interface to access flash chips directly even when the OS is corrupted or not installed.

If you have bricked (nice story) your device by flashing it with incorrect firmware, interrupting the flashing process, etc., you can use JTAG to bring your device back to life! You can also use JTAG to make backups of your existing flash content. This is very useful for porting.

All you need is a short adapter cable, a piece of software, and of course a JTAG header on your device's circuit board. The JTAG header is usually located near the flash chip. In most cases it is a 12 to 14 pin header which must be assembled with 2,54mm pins.

JTAG software is available from Tornado a DD-WRT developer. His current builds for windows and the source files for linux can be found in the DD-WRT download section in the "others->tornado" folder.

Building the Cable

Building the cable is quite easy. You will need some parts you can get at every electronic store in your area, some soldering skills and a voltage/resistance meter.

Parts:

- 4x 100Ohm resistors
- 1x 25pol.D-SUB-Plug (PC Parallel-Port)
- 1x D-SUB-case for the plug
- 12 to 14 ping ribbon cable or single wires
- 1x Pfostenbuchse (i dont know how its called in english. its the header pin which gets soldered to the board)
- 1x Wannenstecker (i dont know how its called in english, too. its the plug which fits to the header on the board)

Circuit:

```
D-SUB-Plug JTAG
Pin 2  -------[100Ohm]------- Pin 3
D0                            TDI

Pin 3  -------[100Ohm]------- Pin 9
D1                            TCK

Pin 4  -------[100Ohm]------- Pin 7
D2                            TMS

Pin 13 -------[100Ohm]------- Pin 5
Select                        TD0

Pin 20 ---+------------------ Pin 6
GND       |                   GND
          |
Pin 25 ---+
GND
```

Using the Cable

install the software, connect your device to the cable and the cable to your pc. leave the psu unplugged. open a cli, go to the folder where the jtag software is stored.
Always do a backup of your existing flash state before doing something else! This is necessary for recovering to the pre flash state and for testing that everything is working fine!
Always let the software auto neg the right settings first.

The flash areas you can modify are cfe (the broadcom bootloader), nvram (the system nonvolatile ram), kernel(the system) and wholeflash (takes a very long time). The switches which can be used are -erase (purging the flash area), -backup and -flash.

If you have a brick caused by a bad flash the easiest way to debrick is to erase the kernel and nvram. After a powercycling the router it will wait for a Tftp_flash firmware flash. You can upload the new firmware via JTAG, too, but this will take hours!
In a standard bricked situation you will never have to erase the cfe! Hands OFF!!

Some examples:
This console commands are for linux Backup:

```
./wrtjtag -backup:kernel
```

Erase Kernel

```
./wrtjtag -erase:kernel
```

These are for windows (maybe the .exe is called different):
Backup:

```
wrtjtag -backup:kernel
```

Erase Kernel

```
wrtjtag -erase:kernel
```