Contents

Einführung

Falls man sich sein Gerät kaputt geflasht hat, ist es praktisch so wie blockiert. Die POWER-LED blinkt nur noch, und er reagiert nicht mehr auf Pings oder Zugriffsversuche über den Browser. Abhilfe schafft da ggf. ein sogenannter JTAG-Adapter. Dieser wird an vorgesehene Pins am WRT und an einen parallelen 25poligen Anschluss am PC angeschlossen. Nun ist es einfach möglich über eine Software ganz gezielt bestimmte Bereiche (CFE, Kernel und NVRAM) des Intel-Flash-Chips zu sichern, löschen oder neu zu beschreiben.

Aufbau

Für den Aufbau benötigt man folgende Teile:

- 4x 100Ohm Widerstände
- 1x 25pol.D-SUB-Stecker (für an den Parallel-Port des PCs)
- 1x D-SUB-Kappe für den Stecker
- etwas Kabel/Flachbandkabel
- nach Wunsch Wannenstecker und Pfostenbuchse fürs Flachbandkabel
- Lötkolben usw.

Schaltplan:

```
D-SUB-Stecker JTAG (JP2 am WRT)
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
```

Wer keine 100 Ohm Widerstände zu Hand hat, kann sie u.U. auch weglassen: Die Eingänge der JTAG Schnittstelle sind ohnehin mit 4,7 KOhm Widerständen beschaltet. So war das zumindest bei meinem WRT54G v5, also bei anderen Versionen lieber nochmal nachschauen. Achtung: Bei dem Modell WRT54G v.3.1 fehlen die SMD-Widerstände RH4 - RH9 (PullUp) und RG4 (PullDown).

Vorsicht! Die Beschriftung der Anschlußfelder kann variieren. Auf manchen Platinen ist das JTAG mit "JP1" und der COM-Anschluß mit "JP2"beschriftet. Grade die Nummerrierung am COM-Anschluß ist etwas verwirrend. Aber: JTAG hat 12 Kontakte, der COM-Anschluß 10 Kontakte. Bei WRT54G 1.0 , 1.1 und WRT54GS 1.0 sind zwei COM-Anschlüsse vorgesehen und das Anschlußfeld ist 20-polig. Fazit: den 12poligen benutzen ;-)

Verwendung des Adapters

Nachdem man den Adapter gebaut hat und alle Kontakte überprüft sind, muss der WRT geöffnet werden. Dazu den blauen vorderen Bereich von dem zweigeteilten hinteren Bereich entfernen. Geht etwas schwer anfangs.

Nun die Kabelenden bzw. den Wannenstecker entsprechend dem Schaltplan anlöten und mit dem Adapter verbinden.

Nun den Adapter an den PC anschliessen. (WRT ist dabei stromlos!)

In der Konsole nun folgende Zeile eintippen aber noch nicht ausführen:

```
./wrtjtag –erase:nvram
```

Jetzt erst den WRT mit Strom versorgen und gleich dannachbinnerhalb von 0,5s bis 2,0s nach der Stromzufuhr Enter drücken und das Programm ausführen. Es wird nun der NVRAM-Bereich gelöscht. Nach erfolgreichem Löschen den WRT wieder stromlos machen und obiges Spielchen mit folgender Zeile wiederhohlen:

```
./wrtjtag –erase:kernel
```

Wenn nun auch der Kernel erfolgreich gelöscht wurde, sollte der WRT auf eine neue Firmware warten. Diese kann man mittels TFTP an die IP 192.168.1.1 an den WRT senden (sollte unter 2,8MB sein):

```
tftp –i 192.168.1.1 PUT Firmware.bin
```

Der WRT erhält durch das Löschen automatisch die IP 192.168.1.1.

http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=33

cfe.bin Datei Lonewolf von Sveasoft betreibt eine Seite wo man die verschiedenen Versionen runterladen kann.