

## Firmware flashen mit tools/push\_firmware.sh

Eine Firmware zu flashen mit diesem Werkzeug, ist einfach und hat diverse Vorteile gegenüber der AVM-Weboberfläche oder dem Firmware-Update-Button in der DS-Mod-Oberfläche:

- Es funktioniert bei jeder Box, also auch bei Speedports, die sich über AVM-Web nicht umflashen lassen. Der Firmware-Update-Button steht ja erst zur Verfügung, wenn der DS-Mod bereits installiert ist.
- Es erscheint keine Meldung bzgl. Nicht-Original-Firmware.
- Da es über den EVA-Bootloader läuft, wird das Update nicht durch laufende Prozesse gestört, die evtl. zu viel Speicherplatz im RAM belegen und erst beendet werden müßten.
- Der Vorteil eines „normalen“ Updates, daß die Einstellungen im TFFS (/var/flash/\*) erhalten bleiben, geht nicht verloren, das ist hier ebenso der Fall.
- Downgrades sind ebenfalls ohne Fehlermeldung möglich, wobei man hier jedoch aufpassen muß, daß die alte Version nicht so alt ist, daß Änderungen der Original-Firmware bzw. des DS-Mod inzwischen die Syntax der jeweiligen Konfigurationsdateien geändert haben. Sollte dies der Fall sein, müßte man erst mal das TFFS löschen, um nach dem Downgrade mit einem sauberen Stand weitermachen zu können.
- Wenn die Box nach einem problematischen Firmware-Update oder einem fatalen Konfigurationsfehler nicht mehr hochfährt, man also nicht mehr via Web flashen kann, geht push\_firmware immer noch.

### Voraussetzungen

Das Skript ist entweder unter Linux aufzurufen oder via Cygwin unter Windows. Cygwin ist nicht offiziell unterstützt, funktioniert aber, wenn die passenden Pakete installiert sind (siehe weiter unten). Folgende Sachverhalte sollen geprüft bzw. sichergestellt werden, damit das Werkzeug funktioniert:

- Die Box muß über Ethernet-Kabel mit dem Quell-Rechner verbunden sein, WLAN geht nicht. Am besten bitte das Kabel an den ersten LAN-Port anschließen, obwohl es auch mit anderen Ports funktionieren könnte. Aber sicher ist sicher.
- Die Boot-IP der zu flashenden Box muß bekannt sein. Standardmäßig versucht das Skript die AVM-typische Standard-IP 192.168.178.1, aber diese kann abweichen und auch manuell geändert werden, sodaß man sie per optionalem Parameter mit übergeben muß, falls dies der Fall ist. Über Telnet läßt sich die Boot-IP wie folgt bestimmen:  
  

```
cat /proc/sys/urlader/environment | grep my_ip
```

  

```
my_ipaddress      192.168.178.100
```
- Achtung: Die Boot-IP ist nicht zwangsläufig identisch mit einer evtl. in den AVM-Einstellungen vergebenen IP, die nach dem Hochfahren der Box gilt. Die Boot-IP kann nur über Bootloader-FTP geändert werden.
- Der Rechner, von wo aus der Flash-Vorgang initiiert soll, sollte - zumindest temporär - eine feste IP-Adresse aus dem Subnetz der Boot-IP zugewiesen bekommen, denn DHCP greift zu dem frühen Zeitpunkt, wenn wir auf den Bootloader zugreifen, noch nicht. Falls also die Boot-IP z.B. 192.168.178.1 wäre, könnte man sich die 192.168.178.111 aussuchen, im Falle 192.168.2.1 könnte man die 192.168.2.111 nehmen usw.
- Sofern man von einem Windows-Rechner aus agiert (auch bei Verwendung von Linux in einem VMware-Gastsystem unter Windows), hilft es, das DHCP-Mediasensing dauerhaft oder zumindest temporär auszuschalten. Das ist das, was das AVM-Recover.exe tut, bevor es den Rechner neu startet. Dauerhaft ausschalten kann man es dann, wenn der entsprechende PC nicht ständig zwischen mehreren DHCP-Servern hin und her wechselt und dies automatisch erkennen soll (z.B. Notebook abwechselnd in Firma und zu Hause). Wie das Mediasensing ausgeschaltet wird über die Windows-Registry, beschreibe ich im Forum, wo auch entsprechende Registry-Dateien zum Download bereit stehen, um das Ganze einfacher und ohne Regedit zu erledigen.

### Cygwin

Unter Cygwin müssen noch weitere Voraussetzungen erfüllt sein. Ich zitiere aus dem Quellcode-Kommentar des Skripts (aktuelle Änderungen bitte ggf. dort selbst nachlesen):

```
# Cygwin users note:

# 1. There is NO guarantee whatsoever that this will work on Cygwin, even

#    though it does on my box (kriegaex). Provided as is.

# 2. For FTP you need the 'ncftp' cygwin package (category 'net').

# 3. You need the 'ping' command from Windows (tested on XP), NOT from the

#    'ping' cygwin package (please uninstall or change path so Windows

#    version is found first), because the cygwin version has no timeout

#    parameter as of today (2007-07-11).

# 4. For 'hexdump' you need the 'util-linux' cygwin package (category

#    'utils').
```

### Ablauf des Updates

Ich beschreibe den Ablauf mit den entsprechenden Meldungen der aktuellen Entwickler-Version für ds26-15.3, aber bei 15.2 lauten die Meldungen gleich oder ähnlich, so daß es damit keine Verständnisprobleme geben sollte. Syntax `push_firmware`

Das ausführbare Skript wird am besten vom DS-Mod-Basisverzeichnis aus gestartet und liegt unter `tools/push_firmware`. Ruft man es ohne Parameter auf, erhält man folgende Hilfe:

```
Usage: tools/push_firmware <firmware> [ -f ] [ <ip> ]

firmware    firmware file to flash (mostly kernel.image)

-f          disable safety prompt

ip          bootloader IP address (default: 192.168.178.1)
```

Im einfachsten Fall ruft man das Skript also mit nur einem Parameter auf, nämlich dem Pfadnamen der Datei `kernel.image`, welche man flashen möchte. Achtung, kein komplettes Firmware-Image mit dem Namen `<Boxname>-blabla.image`, also z.B. `7170_04.40-ds26-15.2.de_20071119-120711.image` flashen. Komplette Firmware-Images sind einfache Tar-Archive, welche mittels `tar xvf dateiname` entpackt werden können. Das gesuchte `kernel.image` befindet sich unterhalb `var/tmp`. Sollte man doch versehentlich ein komplettes Image flashen wollen, so erhält man in der aktuellen Version des Skripts folgende Fehlermeldung:

```
Error: file is not a valid image to be written to mtd1. Please use a
hidden root 'kernel.image' containing both Linux kernel and file system.

Hint: file seems to be a full firmware image archive in 'tar' format
containing the 'kernel.image' you are looking for. Please extract the archive
by means of 'tar xf', then call this script again upon the extracted
'kernel.image'
```

Der zweite Parameter “-f“ bewirkt, wenn er angegeben wird, daß folgende Sicherheitsabfrage unterdrückt wird:

```
!!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!

!!!   THERE IS NO WARRENTY AT ALL !!! USE AT YOU OWN RISK   !!!

Are you sure, that you want to flash <pfad>/kernel.image directly to mtd1?

proceed (y/n)
```

Der dritte Parameter bezeichnet die Boot-IP der Box, falls diese von 192.168.178.1 abweicht.

Die Reihenfolge der Parameter ist übrigens wichtig, `push_firmware` erwartet sie in dieser Reihenfolge, sofern sie angegeben werden.

Ein Aufruf könnte also z.B. so lauten:

```
tools/push_firmware build/modified/firmware/var/tmp/kernel.image -f 192.168.2.1
```

## Ablauf-Schritte

Bei obigem Aufruf passiert im Erfolgsfall Folgendes:

\* You should now reboot your box.

Waiting for box to shut down. Tip: switch off, if reboot is not detected because it happens too quickly

Man erhält also die Anweisung, die Box neu zu starten. Solange weiter die Pünktchen auf die Konsole geschrieben werden, bedeutet das, daß die Box unter der Boot-IP momentan erreicht werden kann. Dies ist der Fall, falls die Boot-IP auch der Laufzeit-IP der Box entspricht. Andernfalls (oder falls die Box bereits ausgeschaltet bzw. der Stecker gezogen wurde) würde diese Meldung schnell übersprungen und die nächste (siehe unten) würde erscheinen. Es ist also egal, ob Sie den Vorgang bei noch laufender oder ausgeschalteter Box beginnen.

Nun führen Sie entweder einen Neustart (Reboot) der Box durch oder ziehen, wie gesagt, den Stecker, falls Sie nicht bereits mit gezogenem Stecker begonnen haben, was am einfachsten wäre. Bei einem Software-Reboot könnte es sein, daß die Box so schnell neu startet, daß das Skript gar nicht bemerkt, daß die Box zwischendurch nicht mehr

erreichbar war und somit bei obiger Meldung verharret, während die Box schon wieder neu hochfährt. Deshalb arbeiten Sie einfach gewohnheitsmäßig mit dem Netzstecker bzw. Ausschalter, falls Ihre Box einen hat (z.B. Speedport W701V). Dann läuft das Skript in jedem Falls direkt weiter zur nächsten Meldung:

```
* No reply from box. Assuming switch-off or restart.
```

```
Trying to re-detect box.
```

Diese Meldung ist also erwünscht und kein Fehler!

Sobald die Box wieder eingeschaltet wird und über ping unter der Boot-IP erreichbar ist, erscheint:

```
* Box is back up again.
```

```
Initiating transfer.
```

```
Tip: switch off/on box several times, if FTP client cannot log in ...
```

Jetzt versucht das Skript sofort, sich via FTP beim Bootloader anzumelden, um die Firmware hochzuladen. Falls folgendes Protokoll so oder ähnlich nicht innerhalb weniger Sekunden zu erscheinen beginnt, tun Sie, was oben steht und schalten Sie im Fünf-Sekunden-Takt immer wieder die Box aus und ein bzw. ziehen Sie immer wieder den Netzstecker, bis es klappt. Meist sind nur wenige Versuche notwendig, sofern Sie die Hinweise zur festen IP im selben Subnetz wie die Boot-IP am Anfang des Artikels beachtet und Mediasensing unter Windows deaktiviert haben. Die Boot-IP muß auch stimmen, das ist klar.

Der Rest der Sitzung läuft in etwa so ab:

```
Debugging on (debug=1).
```

```
----> TYPE I
```

```
----> MEDIA FLSH
```

```
ftp: setsockopt (ignored): Permission denied
```

```
----> PASV
```

```
----> STOR mtd1
```

```
----> REBOOT
```

```
----> QUIT
```

Der Upload-Vorgang sollte einige Sekunden dauern, je nach Größe der Firmware. Falls zwischen STOR und REBOOT nur wenige (0-5) Sekunden vergehen, könnte etwas schief gelaufen und das Update gar nicht erfolgt sein. Andernfalls sollte das Firmware-Update erfolgreich gewesen sein und die Box unmittelbar mit der neuen Firmware neu hochfahren.

Es ist übrigens eine gute Idee, immer eine Kopie einer zuvor funktionierenden Firmware bereit zu halten, um notfalls auf diesen Stand zurück gehen zu können, und zwar ebenfalls mittels push\_firmware. Einfach wie oben beschrieben das Firmware-Image (Tar-Datei) entpacken und das funktionierende kernel.image flashen.

### Problembehebung / Troubleshooting

Sollte trotz der o.g. vorbereitenden Maßnahmen die Box in mehreren Anläufen nicht gefunden werden, sollte man manuell von derselben Kommandozeile aus, wo man auch push\_firmware startet, testen, ob ein ping-Befehl auf die bekannte oder vermutete Boot-IP direkt nach dem Einschalten der Box erfolgreich ist. Falls nicht, kann das Update auch nicht funktionieren. Allerdings setzt ja push\_firmware selbst auch ping-Befehle in zwei Phasen ab (siehe Ablauf-Beschreibung im vorigen Abschnitt), so daß dieser Test im Grunde nicht nötig sein sollte.

Was aber noch wichtig ist, ist, daß auf dem Ausgangs-PC keine Dienste laufen, welche die Netzwerk-Kommunikation behindern. Im Zweifel bitte für den Zeitraum des Updates evtl. laufende Firewall- und Virens Scanner-Dienste sowie sonstige Sicherheitspakete wie Anti-Spyware etc. komplett beenden - nicht nur auf inaktiv setzen, wirklich beenden, bei mir hat das einmal einen Unterschied gemacht. Wenn es dann geht, kann man immer noch die Software so konfigurieren, daß sie die entsprechenden Kommunikationskanäle auch im laufenden Betrieb wieder durchlässig macht. (Das würde den Rahmen dieses Artikels aber sprengen.)

Falls Sie aus einer Linux-VM, z.B. aus VMware heraus, das Update durchführen möchten, ist dafür zu sorgen, daß das Netzwerk entsprechend konfiguriert ist. Am einfachsten geht es mit dem sog. Bridged Networking, aber auch in der NAT-Konfiguration kann man push\_firmware zum Laufen bringen, wenn die Konfiguration entsprechend paßt. Falls man also schon aus der VM heraus nicht ins Internet bzw. sauber ins LAN kommt, wird es vermutlich auch nichts mit dem Flash-Update.

#### Einstellungen im TFFS komplett löschen

Sollte nach dem Flash-Up-/Downgrade die Box nicht mehr sauber starten, könnte es an inkompatiblen AVM- oder DS-Mod-Einstellungen liegen. Hierbei ist die Wahrscheinlichkeit für Probleme höher bei AVM- als bei DS-Mod-Einstellungen und höher bei Downgrades als bei Upgrades, aber sicher ist das nicht, da es zu viele mögliche Kombinationen von Vorher-Nachher-Situationen gibt. In der Regel sollte es keine Probleme geben, aber falls doch, ist es einen Versuch wert, einmal die Einstellungen komplett zu löschen und die Box anschließend komplett neu zu konfigurieren.

Einschub: Es gibt auch die Möglichkeit, nur die AVM- oder die DS-Mod-Einstellungen zurückzusetzen und die jeweils anderen beizubehalten, aber diese Möglichkeiten beschreibe ich hier nicht. Nur ganz kurz folgende Hinweise: Für die AVM-Einstellungen gibt es im Web-Menü den sog. Werks-Reset (Einstellungen → System → Zurücksetzen → Werkseinstellungen), für den DS-Mod gibt es die Möglichkeit, moduninstall all-mods über Telnet aufzurufen und anschließend den Stecker zu ziehen.

Daß man vor jeglicher Rücksetzungs-Maßnahme von der Möglichkeit Gebrauch machen kann, die funktionierenden Einstellungen zu sichern - entweder nur die AVM-Einstellungen (Einstellungen → System → Einstellungen sichern) oder alles komplett, also AVM + DS-Mod über die DS-Mod-Oberfläche (Sichern/Wiederherstellen), sollte klar sein. Ebenso sollte klar sein, daß man gerade durch das Zurückspielen einer Sicherung, die auf einer anderen Box gemacht wurde, die eine Box abschießt und zum Recover-Fall macht. Gleiches kann - mit geringerer Wahrscheinlichkeit - passieren, wenn man eine Sicherung zurückspielt, die bei einem anderen Firmware- bzw. DS-Mod-Stand gemacht wurde.

Nun aber zum eigentlichen Thema: Wie wird das TFFS (Tiny Flash Filesystem, oft auch Transaction Filesystem genannt), also alle sichtbaren und unsichtbaren Dateien unterhalb des Verzeichnisses /var/flash, komplett gelöscht? Dazu benötigt man eine Telnet-Konsole (Rudi-Shell oder SSH geht selbstverständlich auch), wo man folgende aus dem AVM-Firmware-Update-Skript entnommene Code-Sequenz eingibt:

```
echo "Force: factorysettings ..."

#####

# factorysettings non-tffs

#####

# TAM

if [ -d /data ] ; then

    if [ -d /data/tam ] ; then

        rm -f /data/tam/config

        rm -f /data/tam/meta*

    fi

fi

# DECT (Swissvoice)

if [ -x /bin/dectwe ] ; then

    /bin/dectwe

fi

#####

# factorysettings tffs
```

```
#####

echo "Force: factorysettings ..."

id=$((0x10))

while [ $id -le 255 ] ; do

    echo "clear_id $id" >/proc/tffs

    id=$((id + 1))

done

id=$((0x400))

while [ $id -le $((0x4040)) ] ; do

    echo "clear_id $id" >/proc/tffs

    id=$((id + 1))

done

id=$((0x4400))

while [ $id -le $((0x4440)) ] ; do

    echo "clear_id $id" >/proc/tffs

    id=$((id + 1))

done

echo "Force: factorysettings done."
```

Danach bitte den Stecker ziehen!

Anmerkung zu den Nicht-TFFS-Teilen: Der TAM-Abschnitt wird meines Wissens nur für Phone-Labor bzw. die aktuelle 7170-Beta sowie für 7270 benötigt, der DECT-Abschnitt nur für 7270, aber aufgrund der If-Abfragen sollte das kein Problem sein, man kann den Code mit ausführen.

Quelle <http://wiki.ip-phone-forum.de/>