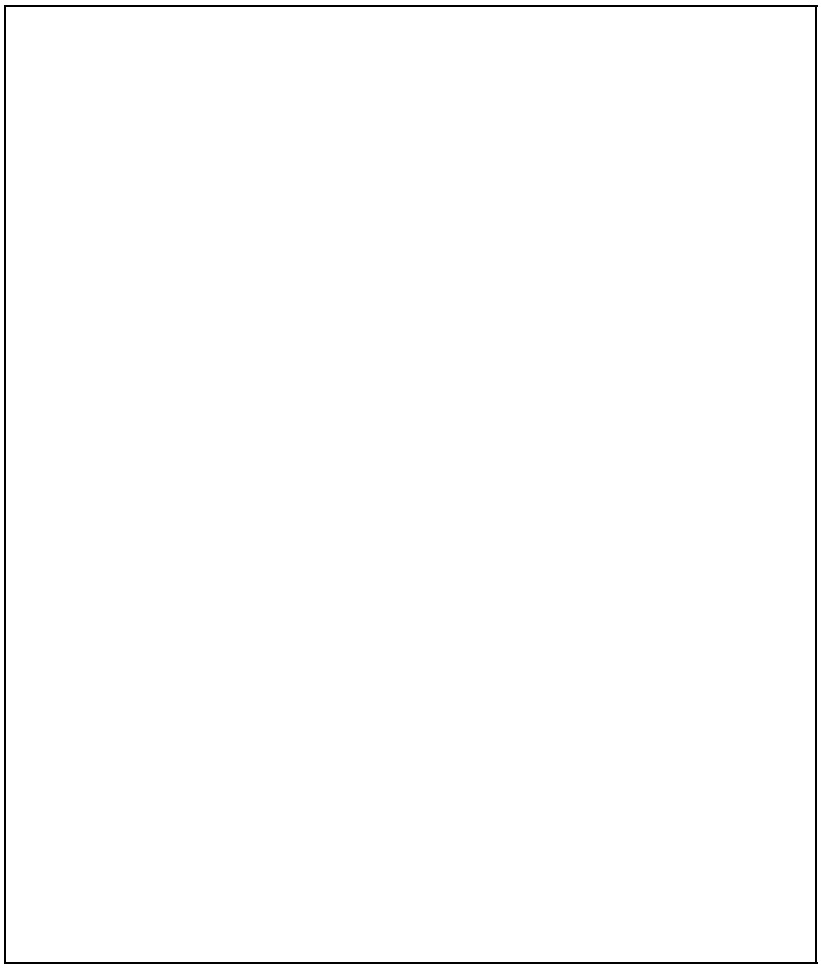
Contents

- 1 Hardware
- 2 Installation/Recovery
    - 2.1 Recovery starts from here
- 3 Revert to original firmware
- 4 FAQ
- 5 Hardware modifications
- 6 External links



Hardware

- Atheros AR5312 chipset @ 220 MHz
- 32MB RAM
- 4MB Flash
- WLAN a/b/g (ieee 802.11a/b/h/g) @ 12dBm (15mW)
- 4x LAN & 1x WAN
- Antenna detachable (reverse-sma)
- Serial port (needs a rs232 converter)
- 5V/2A PSU
- FFC ID: FDI-09101540-0
- Price: ~75?

Even though this device is called "high-powered" its reach is disappointingly low (less than WRT54G's), and its output level is fixed in hardware at 12 dBm. You may want check out FCC RADIO TEST REPORT.

Installation/Recovery

Note: This is a further "polishing" of instructions originally posted by Holgi03 in the forums. Source: [1]

Before you start, you need several things.

RedBoot_config_gdb.rom

Root.fs, lzma_vmlinuz (or newer releases)

FileZilla (For an FTP server)

PumpKIN or **TFTP@SF.net** (For a TFTP server)

Putty (For a reliable telnet client)

A **network switch/hub**, separate from your BuffaloTech WHR-HP-AG108 (to keep your computer from releasing its DHCP lease when it sees its physical link go down when the router reboots)

Create a directory on your desktop for the root.fs, lzma_vmlinuz, and RedBoot_config_gdb.rom files.

```
If your AG108 is bricked, Redboot should still be fine. Therefore:
   * Start and point your tftp program to the proper place
   * Open Putty or Terminal
   * Use command 'telnet 192.168.1.1 9000' when diagnostic red led comes on after unplug/replugin
   * Pick up the instructions at Step 9 (below), except change both IP addresses to 192.168.1.__,
      instead of 11.__

For Mac Users:
Use your Terminal program in the Applications/Utilities folder of your computer
For a tftp program, download "TftpServer" from MacUpdate.com.
   * Open TftpServer
   * Click on "Change Path" icon, navigate to and choose the folder that <br>
```

```
      the root.fs, lzma and dd-wrt files are located in.
   * Click Start TFTP icon
   * The Terminal program will control the 'load' when needed.

If you're comfortable with Unix and the command line, as an alternative to downloading TftpServer
   * sudo launchctl load -F /System/Library/LaunchDaemons/tftp.plist

When done, stop the daemon again with "sudo launchctl unload /System/Library/LaunchDaemons/tftp.p
```

Install Filezilla, create an ?anonymous? user with no password, and set its home directory to that directory.

Install PumpKIN, go to Options, and set the TFTP Filesystem Root to the path to your directory on your desktop. Tell it to give all files, and take all files.

To install DD-WRT, through the web interface, telnet, tftp, and ftp:

1. Plug a network cable into your network switch and into port 1 of your BuffaloTech router. Plug your PC into your network switch.

- This helps avoid connection problems

2. Set your PC?s ip address to: 192.168.11.10.

- Out of the box, your AG108?s IP address will be 192.168.11.1.

3. Log into the BuffaloTech router?s administration website, set the root password to 1234.

- http://192.168.11.1
- Username: root
- Password: **BLANK**
- Click the ?advanced? button at the top of the page.
- Click on the ?admin config? button on the left column of the webpage.
- Type 1234 into both administrator password fields and hit apply.
- Go ahead and log into the router again. **Now logout of the router but make sure you use the logout button**.

4. Open the following address in your web browser:

- http://192.168.11.1/cgi-bin/cgi?req=frm&frm=py-db/55debug.html
- Username: bufpy
- Password: otdpopy1234

5. Activate telnet

- Click the ?telnetd? link.
- Click the ?start? button

6. Connect via telnet to the router

- Run putty

- Select ?telnet? for connection type
- For the hostname (or IP address) put 192.168.11.1
- Click the ?open? button
- You will now be at a BusyBox prompt.
- There is no need to create a flash backup of the ROM, I have it hosted here: [2]
    - **Note:** if you use the backup provided here, your default language and default SSIDs are lost in case you want to revert to the original firmware.
- If you want you can create flash backup using following command:

```
dd if=/dev/mtdblock/0 of=/tmp/full_flash_backup.rom
```

7. Flash the redboot configuration on the router with Holgi?s redboot configuration.

- In the Putty window, type the following commands in order:

```
cd /tmp
wget ftp://192.168.11.10/RedBoot_config_gdb.rom
```

- Confirm at this point that the file transferred correctly by typing ?ls? and verifying it is in the beginning of the directory. (files with capital letters list early in the directory list)

```
dd if=/tmp/RedBoot_config_gdb.rom of=/dev/mtdblock/4
```

- Confirm that you see ?128+0 records? in and out.
- Close your putty session, and re-open putty, configure it for telnet, but use port 9000 this time.

Recovery starts from here

8. Power cycle the router and reconnect to it via telnet.

- Power cycle the router.
- While the red LED is lit, connect using putty via telnet with port 9000.
- Once you see ?== Executing boot script in?? hit CTRL-C which will interrupt the 9 second boot-wait. You should be at a **RedBoot>** prompt.

9. Connect to your TFTP server, transfer root.fs, flash it, transfer lzma_vmlinus, flash it.

- In the Putty window, type the following commands in order:

```
ip_address -l 192.168.11.1 -h 192.168.11.10
fis init
```

- This will initialize flash memory, say yes.

```
load -r -v -b 0x80041000 root.fs
```

- Make SURE you do not mistype.
- This loads the root linux filesystem into memory

```
fis create -b 0x80041000 -f 0xbe050000 -l 0x002a0000 -e 0x00000000 rootfs
```

- This writes the file to flash. Wait a while.

```
load -r -v -b 0x80100000 lzma_vmlinus
```

- This loads the linux kernel into memory.

```
fis create -r 0x80100000 -e 0x80100000 -l 0x000d0000 -f 0xbe2f0000 linux
```

- This writes the file to flash. Wait a while.

```
fis create -f 0xbe3c0000 -b 0x80041000 -l 0x00010000 -e 0x00000000 nvram
```

- This writes an empty nvram to flash. Wait a while.

```
fis list
```

- Make sure all the files are in the correct memory addresses

```
Name              FLASH addr  Mem addr    Length      Entry point
RedBoot           0xBE000000  0xBE000000  0x00050000  0x00000000
RedBoot config    0xBE3DF000  0xBE3DF000  0x00001000  0x00000000
FIS directory     0xBE3D0000  0xBE3D0000  0x0000F000  0x00000000
rootfs            0xBE050000  0xBE050000  0x002A0000  0x00000000
linux             0xBE2F0000  0x80100000  0x000D0000  0x80100000
nvram             0xBE3C0000  0xBE3C0000  0x00010000  0x00000000
```

- If these are correct, continue. If not, you may want to redownload and flash root.fs, lzma_vmlinus, and reflash the empty nvram. Don?t mistype this time.

10. Configure the bootloader

- In the Putty window, type the following commands:

```
fconfig
```

- Hit enter at ?Run script at boot: true?
- Type the following lines into the script. Hit enter after each line once.

```
fis load linux
exec
```

- Hit enter again.
- Hit enter at ?Boot script timeout ?? aka, leave it at 9.
- Hit enter nine times.

```
Boot script timeout (1000ms resolution): 9
Use BOOTP for network configuration: false
Gateway IP address: 192.168.11.254
Local IP address: 192.168.11.1
Local IP address mask: 255.255.255.0
Default server IP address: 192.168.11.10
Console baud rate: 9600
DNS server IP address: 192.168.11.254
GDB connection port: 9000
Force console for special debug messages: false
```

```
Network debug at boot time: false
```

- Type ?y? and hit enter at "Update RedBoot non-volatile configuration - continue (y/n)?"

```
reset
```

The router will now reset, and in a couple of minutes it will come back with a default DD-WRT ip address of 192.168.1.1, username of root, and password of admin.

Revert to original firmware

The revert to the original firmware is not perfect yet, but the device boots the at least.
Note:

- Your default SSIDs are no longer the ones you find on your device unless you are using your **own** flash-backup
- Login for the webinterface: user: root password: 1234

This is what the original fis table looks like, but unfortunately the last item cannot be restored. If anyone finds out why, please edit!

```
RedBoot> fis list
NameFLASH       addr        Mem  addr   Length      Entry point
RedBoot         0xBE000000  0xBE000000  0x00050000  0x00000000
RedBoot config  0xBE3DF000  0xBE3DF000  0x00001000  0x00000000
FIS directory   0xBE3D0000  0xBE3D0000  0x0000F000  0x00000000
vmlinux.bin.gz  0xBE050000  0x80002000  0x000B4B98  0x80182398
rootfs          0xBE120000  0xBE120000  0x002A0000  0x00000000
user.property   0xBE3E0000  0xBE3E0000  0x00010000  0x00000000
Radio.Config    0xBE3F0000  0xBE3F0000  0x00010000  0x00000000
```

1. Cut your firmware flash backup on your (linux) pc in pieces:

```
dd if=full_flash_backup.rom of=vmlinux.bin.gz bs=1 skip=327680 count=740248
dd if=full_flash_backup.rom of=rootfs bs=1 skip=1179648 count=2752512
dd if=full_flash_backup.rom of=user.property bs=1 skip=4063232 count=65536
dd if=full_flash_backup.rom of=Radio.Config bs=1 skip=4128768 count=65536
```

2. Put the files in your tftp root

3. Power cycle the router and reconnect to it via telnet.

```
ip_address -l 192.168.11.1 -h 192.168.11.10
fis init -f

load -r -v -b 0x80041000 rootfs
fis create -b 0x80041000 -f 0xBE120000 -l 0x002a0000 -e 0x00000000 rootfs

load -r -v -b 0x80002000 vmlinux.bin.gz
fis create -r 0x80002000 -e 0x80182398 -l 0x000B4B98 -f 0xBE050000 vmlinux.bin.gz

load -r -v -b 0x80041000 user.property
```

```
fis create -b 0x80041000 -f 0xBE3E0000 -l 0x00010000 -e 0x00000000 user.property

load -r -v -b 0x80041000 Radio.Config
fis create -b 0x80041000 -f 0xBE3F0000 -l 0x00010000 -e 0x00000000 Radio.Config
```

- **Note:** the last command is known to fail

4. Configure the bootloader

```
fconfig
```

- Hit enter at ?Run script at boot: true?
- Type the following line and hit enter twice

```
go_script
```

- Hit enter at ?Boot script timeout ?? aka, leave it at 9.
- Hit enter nine times.

```
Boot script timeout (1000ms resolution): 9
Use BOOTP for network configuration: false
Gateway IP address: 192.168.11.254
Local IP address: 192.168.11.1
Local IP address mask: 255.255.255.0
Default server IP address: 192.168.11.10
Console baud rate: 9600
DNS server IP address: 192.168.11.254
GDB connection port: 9000
Force console for special debug messages: false
Network debug at boot time: false
```

- Type ?y? and hit enter at "Update RedBoot non-volatile configuration - continue (y/n)?"

```
reset
```

FAQ

- WDS setup (2 Atheros devices): Only set one ap to "**wds ap**" and the other to "**wds station**". Put on both the same SSID. **Don´t** set the wds mac table!
- only use **one** band at the same time!
- with all atheros wlans turbo mode is only possible in a-mode at the moment
- if u have version <v.24 rc6.2 installed rc6.2 can't be flashed through the webinterface, use redboot (instruction above): pug306d's post
- v24 (release) does not work well with virtual SSIDs

Hardware modifications

Second outer antenna
Connecting JTAG

External links

Original Buffalo produkt page
Special DD-WRT WHR-HP-AG108 builds