Unlocking the
BT Openreach
VDSL2 FTTC
Huawei EchoLife HG612
modem/router

(at your own risk!)

asbokid
26 - 11 - 2011
version 1.3

The HG612 is shipped in a crippled state with no user interface.

However the device can be unlocked. Once unlocked, web access is available.

The web interface provides technical information including xDSL line statistics.

There are also configuration options for

- **firewalling**
- **http and tftp firmware upgrades**
- **restoring configuration settings**
- **diagnostic tests**
- **system logging**
- **TR-069 remote management**
- **shell access through telnet and ssh, and more.**

To unlock the modem follow these instructions carefully.

1. Power off the modem.
2. Connect your PC directly to the LAN2 socket (as in Fig. 1)

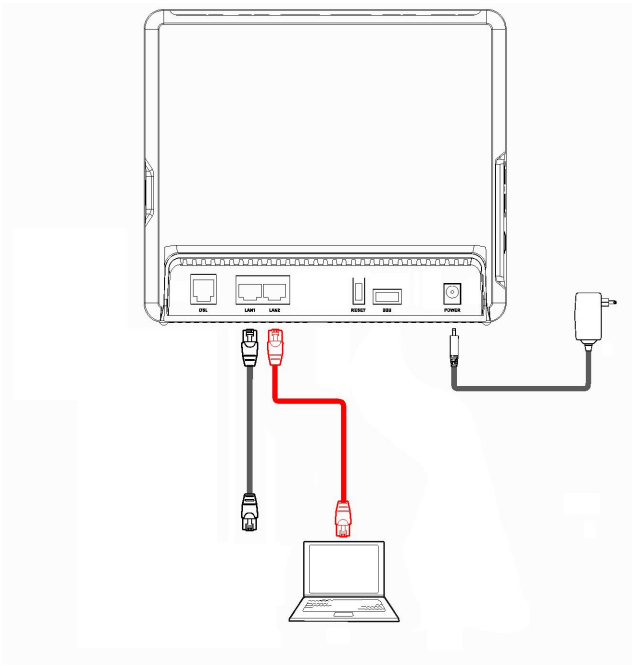

Fig. 1: Connect PC to LAN2 socket

3. Configure the ethernet NIC of your PC with IP address `192.168.1.100`.
4. Press the RESET button on the modem and keep it pressed.
5. Do not release the button yet.
6. Power on the modem.
7. Keep the RESET button pressed for a further five seconds.
8. Use your browser to visit the modem's web address http://192.168.1.1/

9. You should see this web page: (Fig. 2):

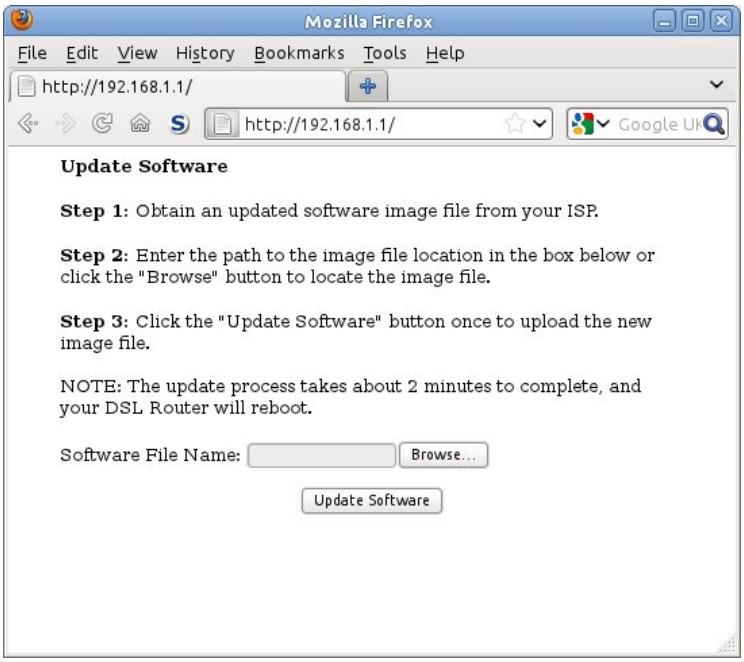

Fig. 2: Firmware Upload Web Page

10. Click the [Browse] button.

11. Select unlocked firmware from your hard drive and click Update Software.

12. You will now see this web page (Fig. 3):

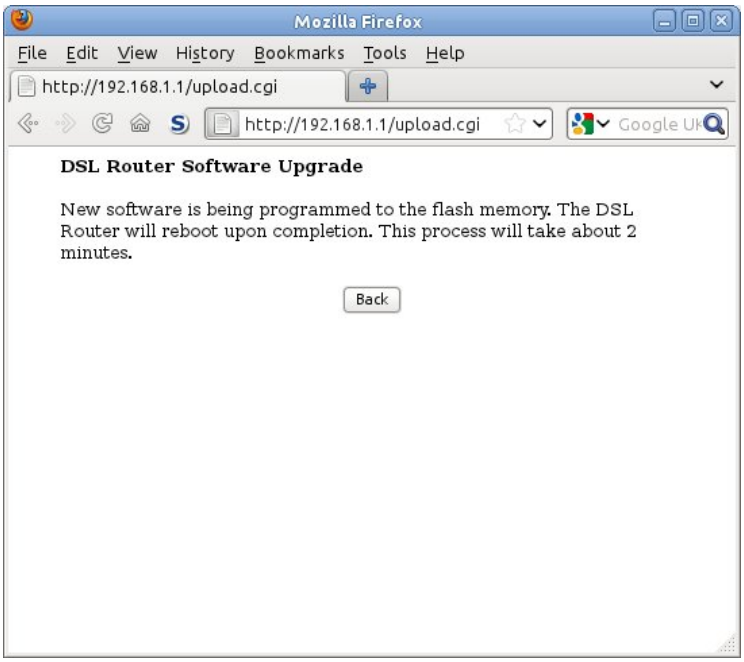

Fig. 3: Firmware Upload in progress

13. Do not turn off the modem until the new firmware is loaded and the modem has rebooted. This may take several minutes.

14. Once the modem has rebooted, visit the address http://192.168.1.1/ again.

15. You should now see this page (Fig. 4):

Fig. 4: HG612 login page

16. Enter the username '`admin`' and password '`admin`'.

17. After you have logged in, the Device Information page will load (Fig. 5):

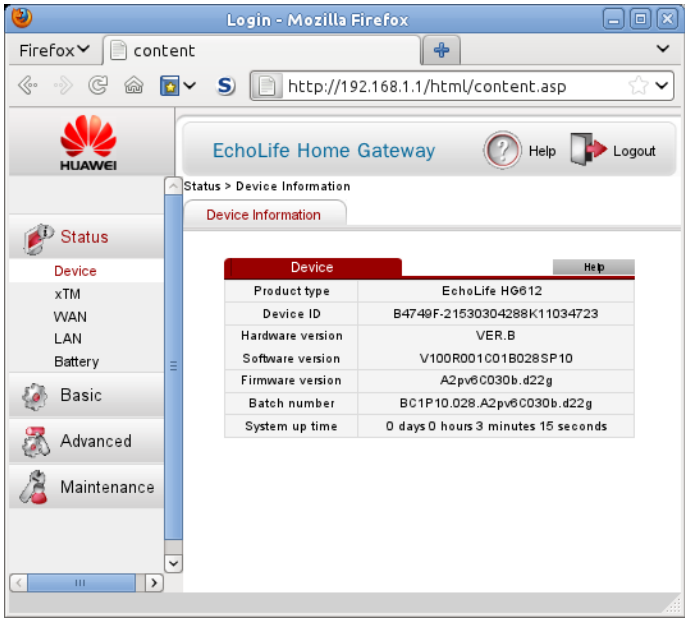

Fig. 5: Device Information Page

18. The opening of a telnet session is shown in Fig. 6.

    Log in to telnetd and sshd with username '`admin`' and password '`admin`':

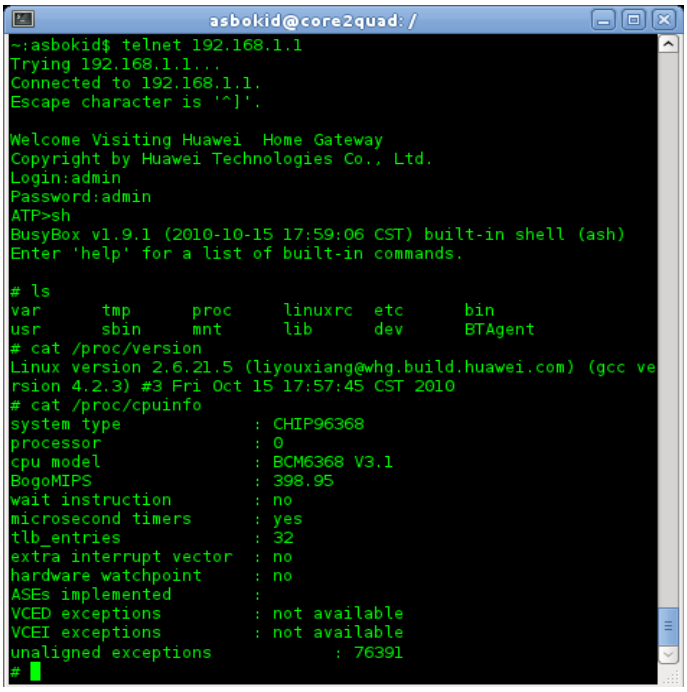

Fig. 6: Telnet access to the HG612

19. Full line statistics including Bit Depths, Quiet Line Noise and SNR for each sub-carrier can be obtained from the `xdslcmd` tool (Fig.7)

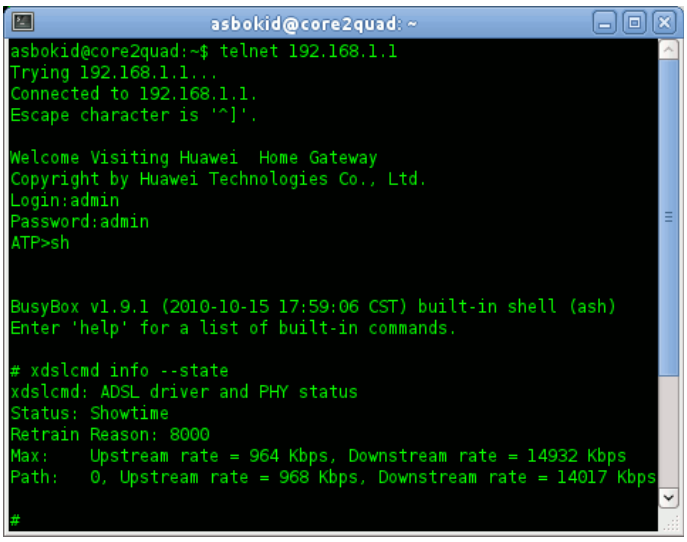

Fig. 7: Obtaining line statistics with xdslcmd tool

20. Graphs produced from line statistics data can be useful in fault diagnosis and for gauging performance.

21. The VDSL2 connection scrutinised below is poor. A Bit Loading graph highlights the reason. (Fig. 8)

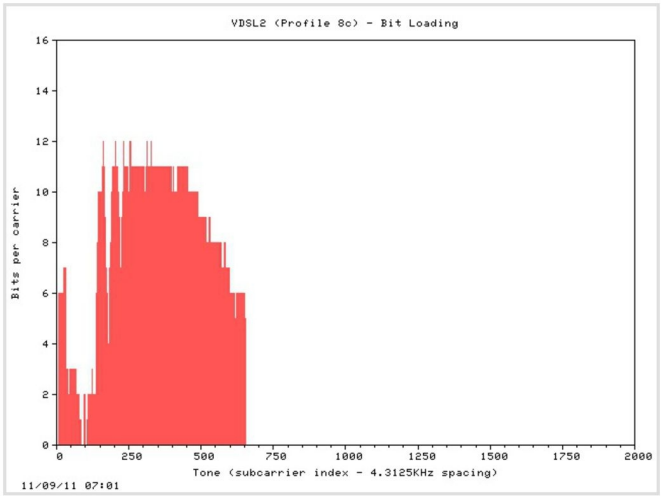

Fig. 8: Bit Loading reveals non-utilisation of Band D2

VDSL2 Profile 8c normally utilises two downstream frequency bands, D1 and D2. The second band (D2) runs from 5.1MHz – 7.0MHz and provides subcarrier tones 1192-1627.

Fig.9 reveals that Band D2 is not being utilised at all. This will result in downstream throughput that is no better than ADSL2+.

By contrast, the Bit Loading graph of Fig. 9 generated from a different line illustrates a good connection. All bands are in use and generally high bit depths are found across the spectrum of the band plan.

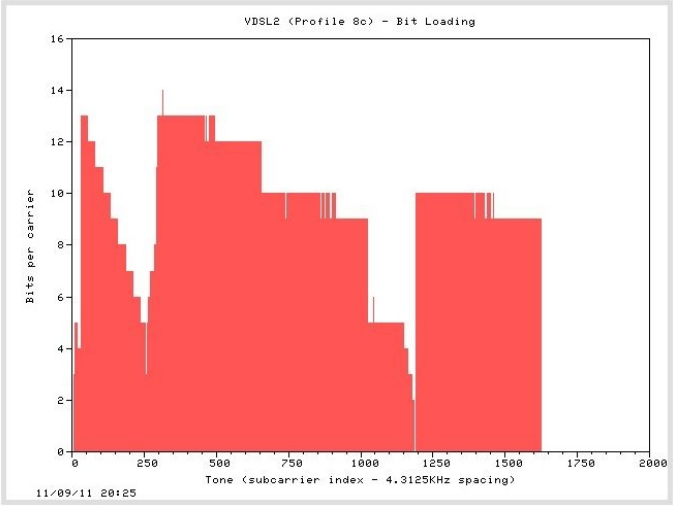

Fig. 9: Good bit depth across the band plan

Scripts that pipe all the line statistics data from `xdslcmd` to `GNUPlot`, the graphing tool, have been developed by *burakkucat* and *Little_Bird*. (Fig.10)

The scripts will run on Linux and Windows and are included with other 'hacking' tools in a Toolkit for the Huawei.

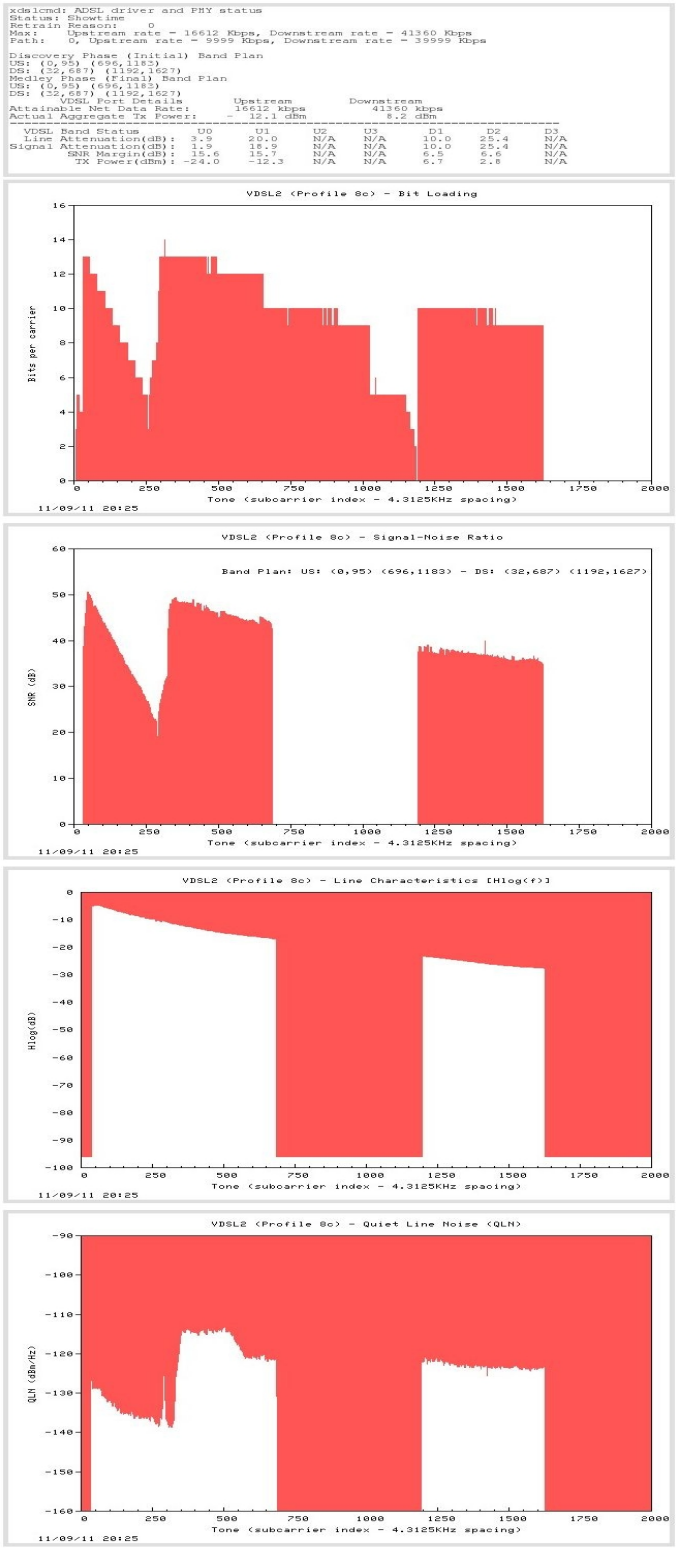

Fig. 10: Graphed Line Statistics

Notes:

- Unlocked SP10 firmware has been tested on original SP06 models, as well as the newer 2V and 2B revisions of the HG612. It apparently works on Revision 3B as well.

- There are various cabling options. In the standard setting, the home router continues to be connected to the LAN1 socket on the Huawei for 'fast bridging'. A second cable from the home router plugs into LAN2 on the Huawei. This allows internet connectivity at the same time as access to the Huawei's web interface. Different cable configurations can be selected through the web interface.

- Line Attenuation is shown as zero on the Status > WAN > xDSL page. This is a firmware bug which is present in other Broadcom-based devices. Full line statistics are available using the xdslcmd tool from telnet or ssh.

- By default, dhcpc is running on the ptm1.301 VLAN pseudo-interface for TR-069 remote management purposes.

- An Open Source toolkit for building custom firmware, and for graphing line statistics is available from http://huaweihg612hacking.wordpress.com

- The Default Configuration can always be restored with a 'Long Reset':

    - Reboot the HG612 and allow it to stabilise.

    - Check with your PC that the xDSL line has synced, and that you have internet connectivity

    - Hold in the Reset Button on the HG612 for 10+ seconds, and then release it. This causes a 'Long Reset'.

    - The modem will replace its current configuration settings with the Default Configuration.

    - Give the modem time to reboot again after the 'Long Reset'.

    - Connect your PC to the LAN2 socket on the Huawei.

    - Visit http://192.168.1.1 (the default web address of the Huawei)

    - The configuration options will now be at their default settings

Acknowledgements:

- *Burakkucat* - for his many suggestions and improvements, never-ending testing, for applying his wizardry with Unix shell scripting to the graphing scripts.

- *Bald_Eagle & Little_Bird* - for testing numerous firmware images, fault-shooting, greatly improving these instructions, and for porting the graphing scripts to Microsoft Windows.

- *WalterWilcox* – for his vigorous lobbying for fibre roll-out

- *OmegaPhil* – for sharing his automated data collection scripting

- *TomLimbo* – for scouring the world for obscure electronic components

- *MysticaMike* – for showing us limeys what a proper graph should look like

- *<paul @ sbrk.co.uk>* - for spotting and squishing a nasty mksquashfs bug.

- *Craig Heffner, Jeremy Collake, Solarflare, TexHex,* and other contributors to the *Firmware Modification Kit:* http://bitsum.com/firmware_mod_kit.htm

- many other contributors on the *thinkbroadband* and *kitz* forums who have supplied feedback, screenshots and telnet session logs.

suggestions or comments to <ballymunboy@gmail.com>