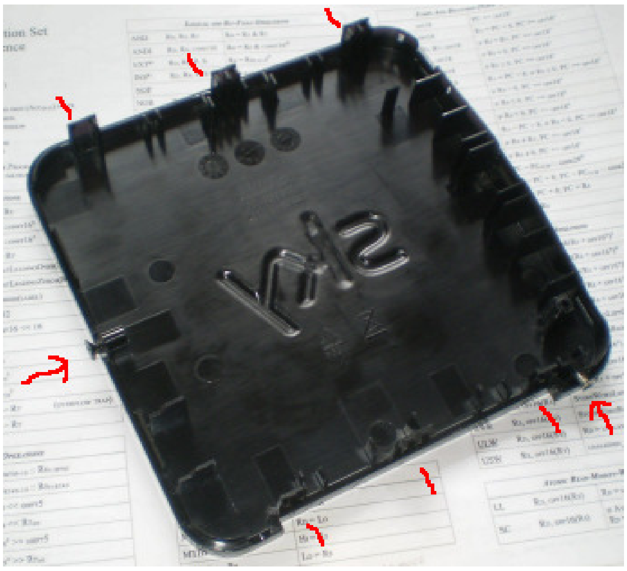
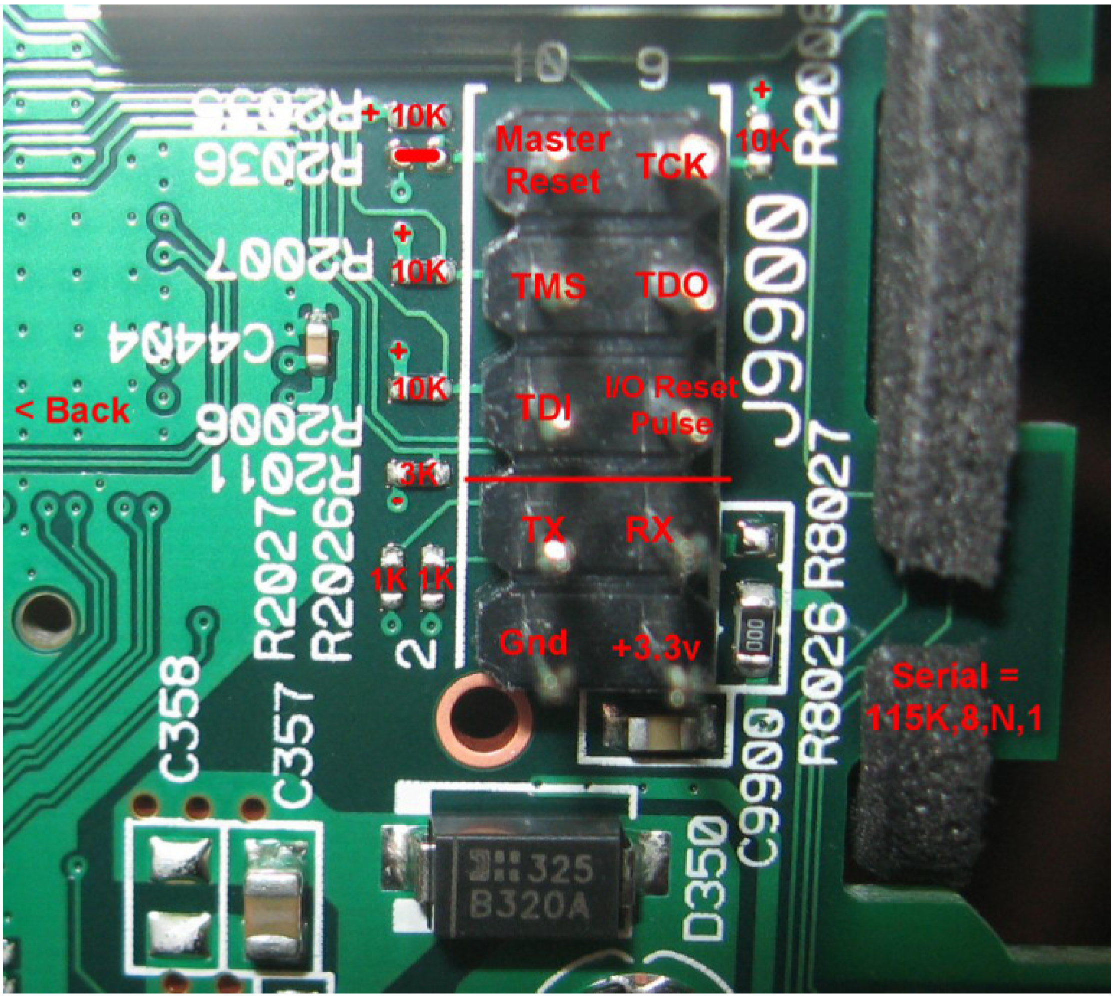
Here are some steps/ideas to Install the adjusted Sky SR102 Firmware

Some requirements are:
Soldering Iron or Header connector or Fine tape
Serial Port (or some USB gadget equivalent)
A mini HTTP server or mini FTP server software

Remove the case of the box via the **2** screws, and the row of push clips along the top and bottom.



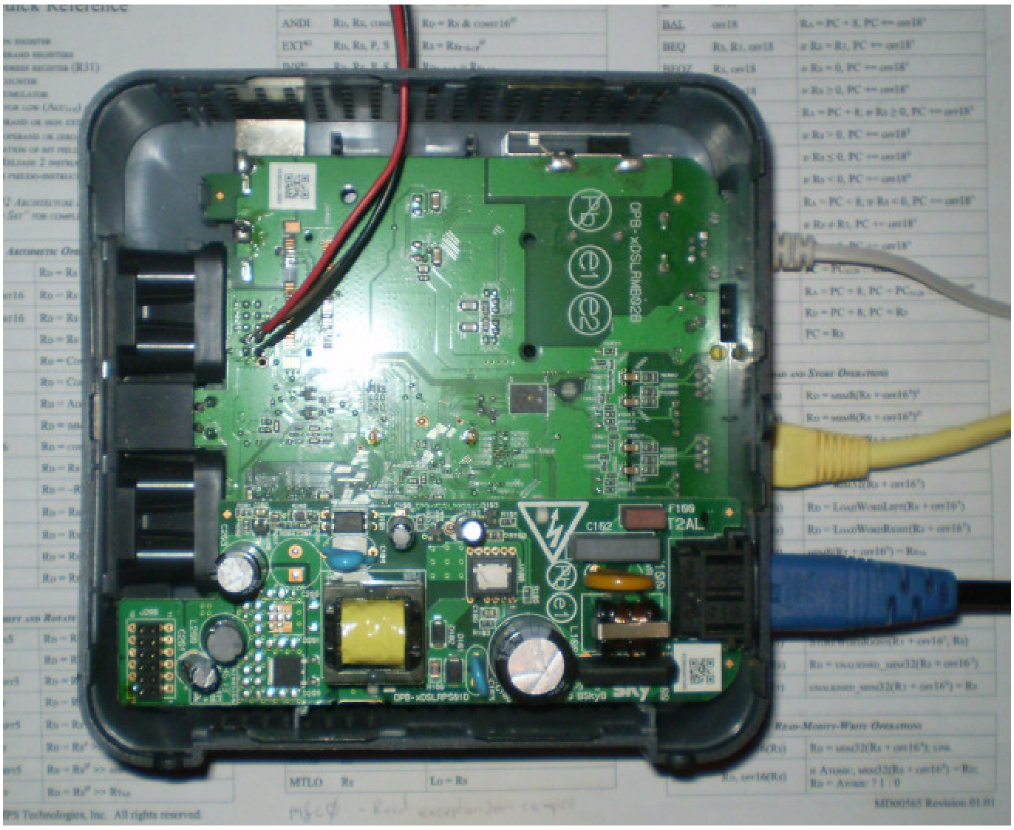
Its awkward, but remove the PCB and you will see the pin header on the right.



The top part of the header is the JTAG, only use it if you have a 3.3v Parallel Port (or another similar device). You can re-flash the boot-loader if you corrupt it. https://drive.google.com/open?id=0B4-Ln6UubyEeRGFDUXphTW1RVWc

Focus on the bottom 4 Serial / UART pins.

Alternatively you can solder onto the pins from the other side of the board:



It’s handy for future access. But don’t hurt yourself on the PSU high volts   ☺

Serial Port

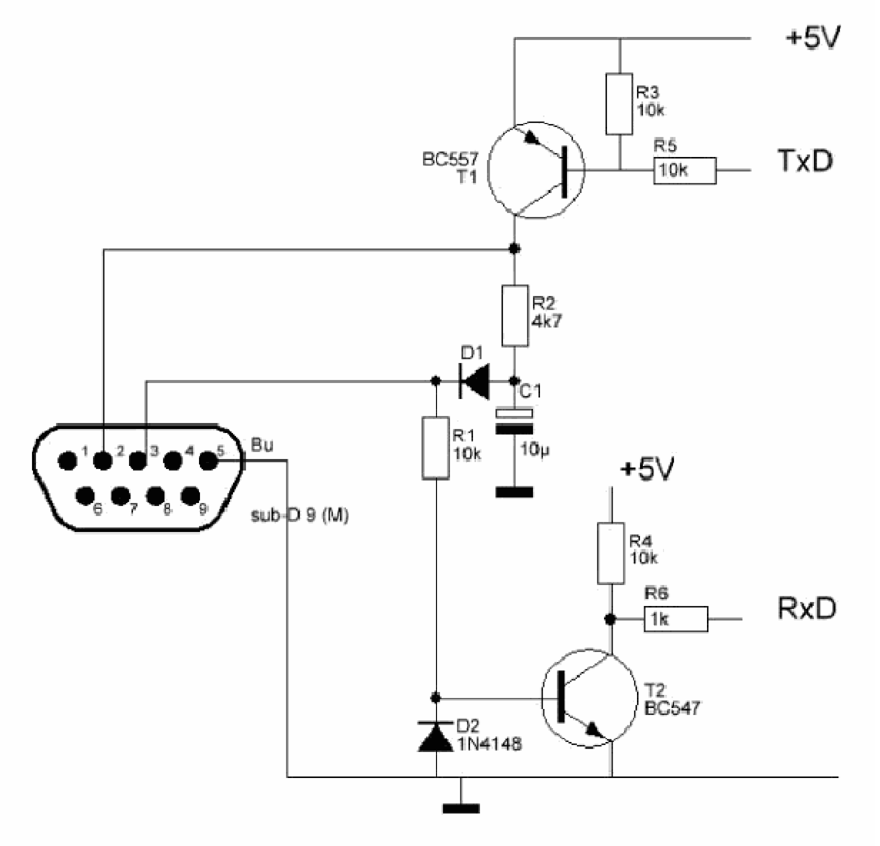
It requires TTL Serial @ 115K200 Baud. There are USB gadgets to do that, but its more interesting to build your own.

Info: https://www.google.co.uk/#q=convert+rs232+to+ttl

You might be lucky and use an old USB mobile phone connector. Sometimes they are built for this purpose, and use a fancy proprietary connector on the end.

But I prefer to use this diagram for a simple converter:

Copied from https://arduinodiy.wordpress.com/2012/03/ (slightly fancier version)



There is no need to use the exact transistors, generally speaking any-old NPN and PNP transistors will do (due to the slow speed). Also don't use 5v here, use the 3.3v from pin 1 of the PCB header.

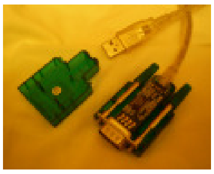
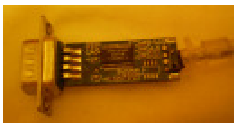
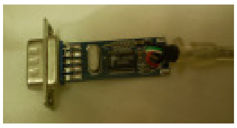
There are simpler versions available, but I prefer the capacitor (for full duplex) and the clamping diode at the bottom.

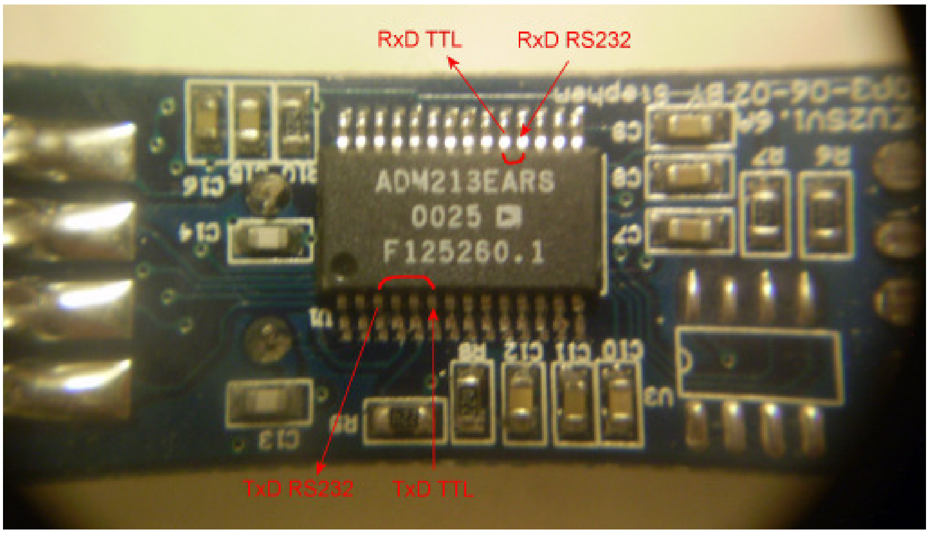
Also, if you have a USB to RS232 converter. It is (some times) possible to hijack the pins inside the converter. If it has 2 or more chips: you should be able to get the signal after the USB chip and before the single conversion chip – probably a MAX232 chip. (aka EIA-232 Drivers/Receivers)

If you Google the chip numbers. I'm sure you will be able to download a datasheet.

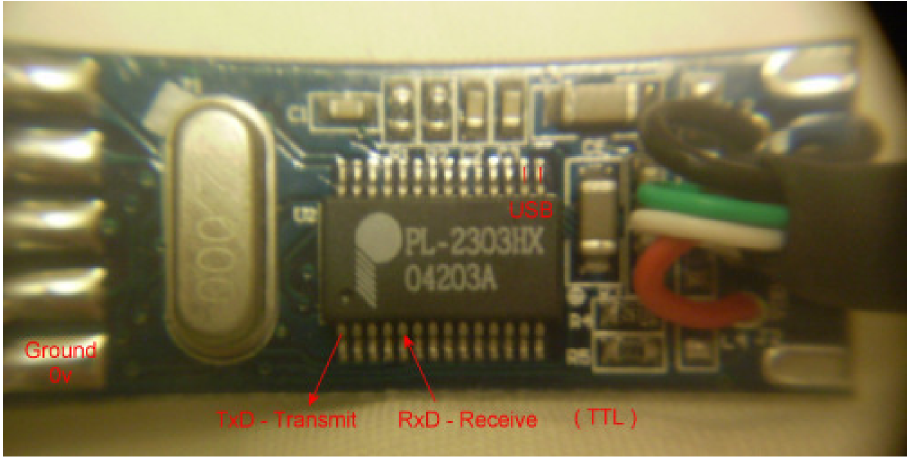
More Serial Stuff   (Bad example)

Here's the inside of a USB to Serial adapter:

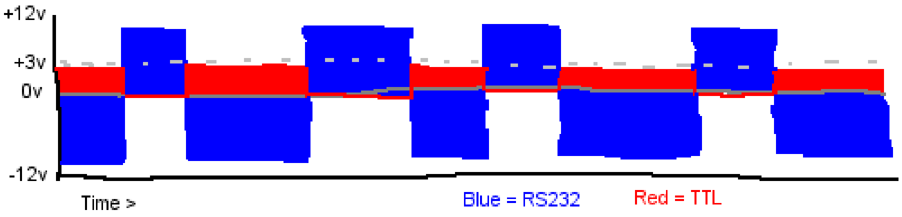






Found these Chip Datasheets on Google

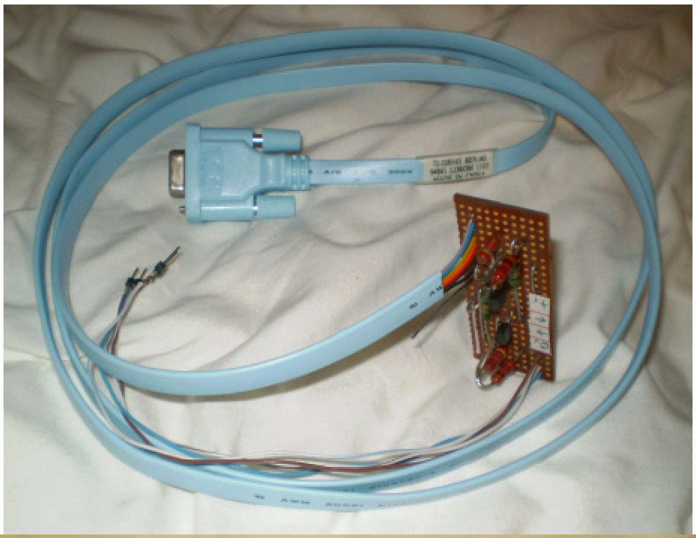


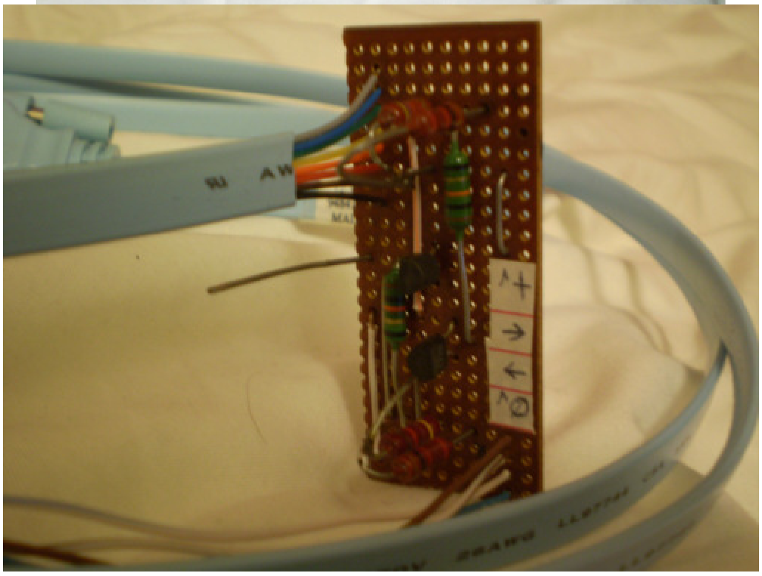
This adapter does not have a easy-to-remove link/resistor between the Chips.
I can use the TxD Transmit Pin, But I can not use the RxD Receive Pin. So I could completely remove the ADM213 chip, but its better to cut off the power line instead.
* But I want to save this adapter *

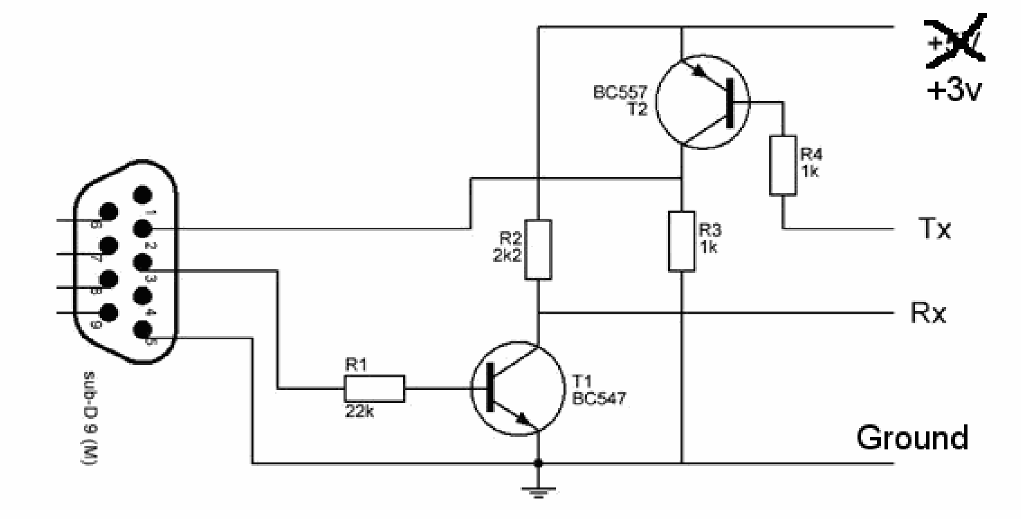


More Serial Stuff (Simple adapter)

This is probably the simplest home made adapter:



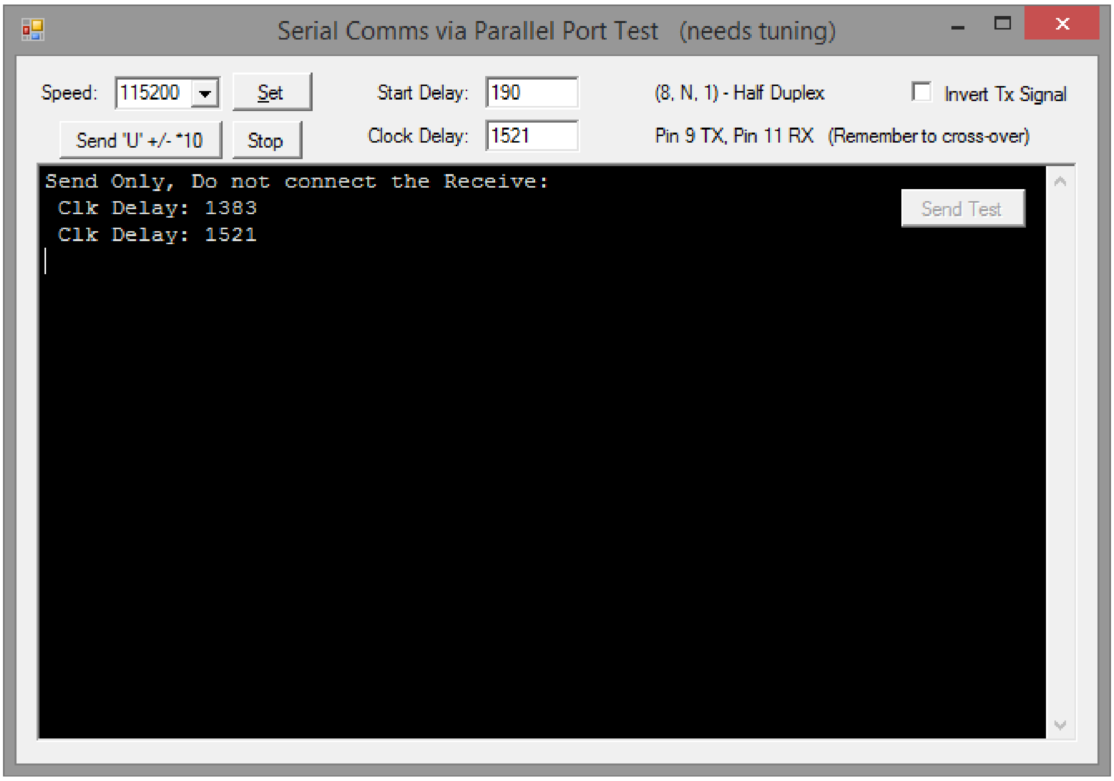




This circuit it prone to errors, and you may have to fiddle the values of the resistors.

Parallel Port Attempt   (why am I suggesting this?)

This crude idea will attempt to use your Parallel port to send some Serial data. Without the need to solder anything.
https://drive.google.com/open?id=0B4-Ln6UubyEeU0dMZkFzS3dRV3c



Serial Comms via Parallel Port Test   (needs tuning)

Speed: 115200 | Set | Start Delay: 190 | (8, N, 1) - Half Duplex | □ Invert Tx Signal

Send 'U' +/- *10 | Stop | Clock Delay: 1521 | Pin 9 TX, Pin 11 RX   (Remember to cross-over)

```
Send Only, Do not connect the Receive:
 Clk Delay: 1383
 Clk Delay: 1521
```

(Because of the 1K resistors on the router, 5 volt Parallel ports are ok)

Connect Pin 9 of the Parallel Port to the Receive Pin of the Router.
Connect a Ground pin (18 to 25) to the Ground Pin of the Router too.
This program can not Receive correctly, so do not connect it.

Click the 'Set' button twice, so its guesses a 'Clock Delay' speed based off your PC's speed. Then type the following to see if it reboots….

```
<Enter>
admin  <Enter>
sky    <Enter>
sh     <Enter>
reboot <Enter>
```

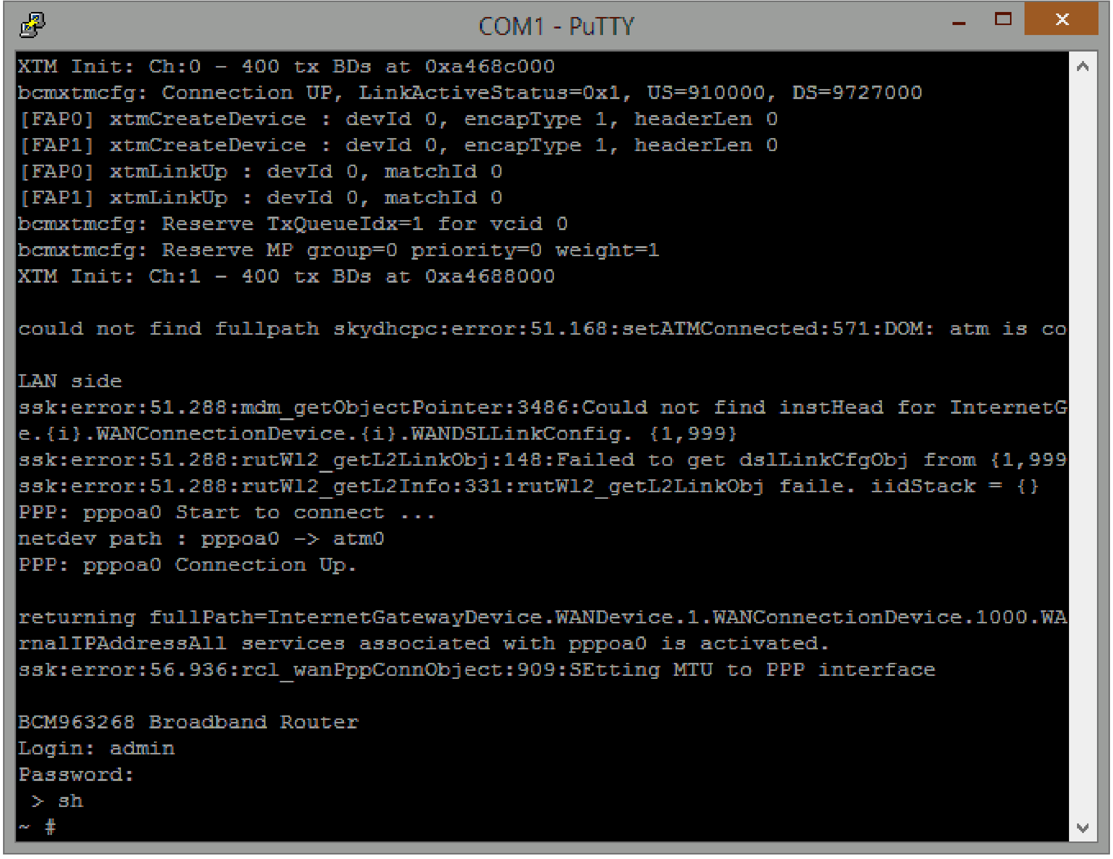
If you are lucky and it reboots. You can try to type in blind commands after the 'sh' command. Perhaps you can try to upload a telnet program.

Suggestion: change your web login password to 'admin' as well. So you can type 'admin' lots of times, then try 'sh' & 'reboot' ?

Communication

Download something like PUTTY, when you got the Serial connected:

(Please ignore the test output)



```
XTM Init: Ch:0 - 400 tx BDs at 0xa468c000
bcmxtmcfg: Connection UP, LinkActiveStatus=0x1, US=910000, DS=9727000
[FAP0] xtmCreateDevice : devId 0, encapType 1, headerLen 0
[FAP1] xtmCreateDevice : devId 0, encapType 1, headerLen 0
[FAP0] xtmLinkUp : devId 0, matchId 0
[FAP1] xtmLinkUp : devId 0, matchId 0
bcmxtmcfg: Reserve TxQueueIdx=1 for vcid 0
bcmxtmcfg: Reserve MP group=0 priority=0 weight=1
XTM Init: Ch:1 - 400 tx BDs at 0xa4688000

could not find fullpath skydhcpc:error:51.168:setATMConnected:571:DOM: atm is co

LAN side
ssk:error:51.288:mdm_getObjectPointer:3486:Could not find instHead for InternetG
e.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig. {1,999}
ssk:error:51.288:rutWl2_getL2LinkObj:148:Failed to get dslLinkCfgObj from {1,999
ssk:error:51.288:rutWl2_getL2Info:331:rutWl2_getL2LinkObj faile. iidStack = {}
PPP: pppoa0 Start to connect ...
netdev path : pppoa0 -> atm0
PPP: pppoa0 Connection Up.

returning fullPath=InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1000.WA
rnalIPAddressAll services associated with pppoa0 is activated.
ssk:error:56.936:rcl_wanPppConnObject:909:SEtting MTU to PPP interface

BCM963268 Broadband Router
Login: admin
Password:
 > sh
~ #
```

```
Login: admin
Password: sky   (default)
> sh
```

And that’s root access.

If you are having some communication errors with your adapter, you can lower the baud rate with this command:

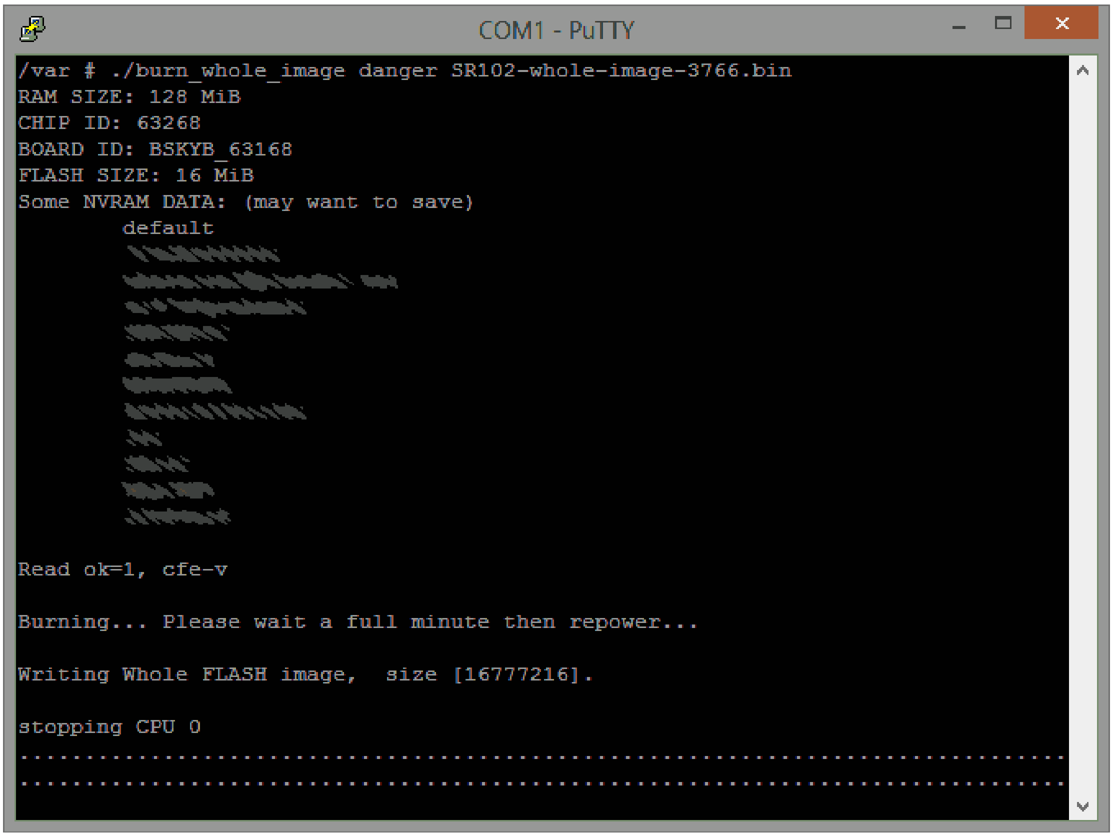
```
stty -F /dev/ttyS0 9600
```

<u>Transfer Firmware</u>

Download a mini http server, so you can use the ‘wget’ command from the PC to the router.

```
cd /var
wget http://192.168.0.2:8000/SR102-whole-image-3766.bin
wget http://192.168.0.2:8000/burn_whole_image
chmod 0777 ./burn_whole_image
./burn_whole_image danger SR102-whole-image-3766.bin
```

These commands copy over the firmware and burn it.
Just after you paste the last command, it will show you some serialisation data from your box, which you might want to save (just in case).



```
/var # ./burn_whole_image danger SR102-whole-image-3766.bin
RAM SIZE: 128 MiB
CHIP ID: 63268
BOARD ID: BSKYB_63168
FLASH SIZE: 16 MiB
Some NVRAM DATA: (may want to save)
        default
        [redacted]


Read ok=1, cfe-v

Burning... Please wait a full minute then repower...

Writing Whole FLASH image,  size [16777216].

stopping CPU 0
................................................................................
................................................................................
```

Recovery Mode

The normal recovery mode (boot-loader): Hold the WPS button while you power on. Within a few seconds you will have access to the basic web interface to re-flash the stock firmware. http://192.168.0.1/

If you delete/change an important boot-up file. You can erase the JFFS2 partition during boot-up.

The additional recovery mode: Hold the WPS button starting between 5 to 25 seconds after you power on. When the SkyHD led turns on, it will erase the R/W partition & reboot.

Good Luck – Matt Goring, July 2015

Change Log

Revision 3766:

Implemented UnionFS (read unionFSnotes.txt)
Added Bridge Mode & Fake Bridge Mode (Advanced > Extras)
Enabled NFS
Removed tcpdump

Revision 3765:

Restored original Busybox version - due to knock-on BUG
Added option to change LAN MAC Address
Added 'DslDiagD' binary for Detailed Line Diagnostics
Enabled a few other options (in buildconfig.cfg)

Revision 3764:

Added new Web page for changing DSL line Username/Password (Advanced > Extras)
Enabled Broadcom Web Interface (some options do not work)
Enabled Telnet
Disables WAN ping & port 30005
~~Replaced BusyBox~~
Added MTD blocks - CFE, NVRAM, ~~Spare 4MB~~, Full Flash - for better access
Added UnionFS - Currently not implemented
~~Auto executes file '/var/auxfs/init2.sh' for custom startup scripts, e.g. Overlay spare MTD block~~.
Disabled signature validation for GUI firmware uploading
Removed tr69c (Remote management)
Removed fus (Firmware Upgrade)
Removed factory
Removed tinyproxy

Revision 3763:

Just released Binaries, similar to Rev 3764

Revision 3761:

Original GLP Source from SKY