



Ok Guys and Gals I decided to put all the tutorials together kind of like a Haynes Manual to modem hacking. Everything that's covered within is available separately for download on the various forums that are about.

This guide was put together by

[Cableguy69](#)



Guides / images from the following are included (sorry if anyone is missed):
(These are not listed in any particular order)

[Cableguy69](#)

[Viiiper](#)

[Cleric](#)

[LLAADD](#)

[Jim Rose](#)

[JimboTheHo](#)

[Boltar](#)

[Astra](#)

[Cashmere](#)

[666](#)

[Koevoet](#)

[Witchy2K1](#)

[Granty](#)

[NoOne](#)

[R3V3NG3R](#)

[Dshocker \(of TCNISO\)](#)

Thanks to all of you for your hard work.

The guide was re-organised, corrected, re-worded, updated and converted by

[LLAADD](#)

(If any of you disagree with any these changes, please PM him [unlocker-forums])

Contents

1. Cable Modem Basics	4
2. Sniffing for MAC Address'	5
2a. Cable Modem & UBR Gateway	5
2b. Sniffing for new MAC Addresses using DHCP Force	6
2c. Mac Swap Tutorial	9
2d. Know your DOCSIS	11
NTL: Franchise Areas (Pure & Ex-C&W)	11
Telewest: Network Map.....	12
2e. Config file Database, accurate on: 03/06/2007	13
NTL.....	13
Telewest.....	14
3. Spoofing Your NIC (Network Interface Card)	15
3a. Changing your NIC MAC	15
4. IP Address	16
5. MAX 232 & 233.....	17
5a. MAX232.....	17
5b. MAX233.....	18
5c. Pre Manufactured Max Cables	18
Chartmans Max 232.....	18
TMC Max 232	18
Jabs Place Max 233.....	19
Wayneeboy19117	19
5d. Webstar Max cable adapter.....	19
6. Ambit 200	20
6a. Changing the MAC Address of the Ambit 200	20
6b. Communicating with your modem	21
6c. Telewest (TW) Stream.....	24
6d. Programming Ambit Chips, with Willem 4.5.....	26
6e. Ambit 200 Firmware Downgrading via Ethernet	30
6f. Latest release for the Ambit 200.....	34
6g. Restoring a Compatible Bootloader.....	41
6h. Ambit 120 Tutorial	43
7. Ambit 250 - Guide to Hacking v2	52
7a. Updating Ambit 250 to hacked firmware.....	52
7b. Force modem to use the 10mb config file.....	56
7c. Finding your TFTP IP.....	57
7d. 250 configurator guide.....	61
Troubleshooting.....	63
8. Motorola SB3100	65

9. Motorola SB4100 & SB4200	68
9a. Change Firmware on Surfboard Modem - 1 PC Method	68
9b. Modems from America or Japan.....	70
10. Hacked Firmware	71
10a. Fibercoax.....	71
How To Use It.....	71
Flags.....	71
FAQ	72
Status Page.....	73
10b. Hackware	74
11. SB4100/SB4200 using a MAX232/MAX233 serial cable	75
11a. SB4100.....	75
11b. SB4100 - Rev a	75
11c. SB4101.....	76
11d. SB4200.....	76
11e. SB5100.....	76
11e. "bootp referenced but not included" Error (SB3100/SB4100/SB4200)	79
SBxx00 TELNET COMMAND LINE.....	80
To get into Telnet:.....	80
12. Blackcat	81
12a. SN74LS244N Version	81
12b. Chipless version	81
12c. Making a Chipless Blackcat.....	82
12d. Soldering a pin header	84
13. SB5100 Tutorial with Broadcom Commands	88
13a. USB JTAG ON A SB5100 USING FERCSA`S X2 STEALTH13.5.....	97
14. Motorola SB5101	102
14a. Method 1	102
14b. Method 2	103
15. Webstar DPC2100, EPC2100.....	106
16. Baseline Privacy (BPI) Hack	109
17. Directly install SB5000 Series modems to PC and run off PC PSU.....	110
18. Secret MIB's & Secret way to upgrade cable modem via BITFILE	113
18a. Factory Mode.....	113
18b. Bit Files.....	113
18c. Enable Factory MIB	114
18d. Factory mode OID list for Motorola cable modems.....	115
Links.....	119

1. Cable Modem Basics

Ok I'll leave out as much jargon as possible.

A cable modem is identified by the cable company by its Mac address which can usually be found on the underneath of the modem on a sticker with bar codes. This Mac is known as the HFC (Hybrid Fiber Coax) Mac Address. How it works is by using a method know as handshaking, When you boot your modem (Switch it on), the modem will perform some tasks. Firstly the modem will send out a signal saying, "Hey I'm Mac address 00.11.22.AA.BB.CC" (Or whatever the Mac address is). The cable co. then check the Mac address against there data base the Mac address must be known by the cable co. or the modem will not be able to synchronize with the cable co network.

Once the Mac is recognized by the cable co. it will then be assigned a config file. Now a config file is what determines the speed the modem will run at so the config you will be looking to use is the one with the fastest speeds available. So basically the modem says hello I'm Mac Address whatever, the cable co then say yes we know who you are, and this what speed we want you to run at, once all this has been done, you get assigned an IP address and away you go.

Cloning works by copying the Mac address of a modem that is legitimately paid for by a subscriber. This will allow you to receive the same level of service as the paying customer. Now here's the catch, you are able to sniff out Mac address' from any PC that is connected to a cable modem with a valid IP address, but the Mac address' you sniff out will be of no use to you. The cable companies divide their networks into gateways, if two identical Macs appear on the same gateway it'll cause a conflict as the cable co. will not know which modem to assign an IP to, so the two modems will go into a reboot loop where both modems continually reboot each other, giving you very little, if any internet access. Another detail which is very important when buying a modem is it's DOCSIS (Data over cable service interface specification) standard. There are 2 DOCSIS standards "International" & "European". Pure NTL & TW use International DOCSIS whereas EXCW areas use European DOCSIS.

If you live in an I DOCSIS area you will need one of the following:

Ambit 200

Motorola SB4100i, SB4200i or SB5100i

If you live in an E DOCSIS area you will need one of the following:

Ambit 200

Motorola SB4100e, SB4200e or SB5100e

The Ambit 200 will work in either of the areas as it is capable of both DOCSIS standards.

2. Sniffing for MAC Address'

The first thing you need to understand is UBR's (Gateways).

The following text was put together by

Viiiper



2a. Cable Modem & UBR Gateway

Cloned modems can only work in a different segment of the cable network from the original cable modem

All Cable modems login to the cable network with there unique MAC address. Think of your town/ city as segmented like an orange. We all live in a certain segment and no two MAC addresses are the same. A cloned modem comes online, as long as it is in a different segment of the network from the original, it will work this is because the network primarily checks the cable modems Mac address and does NOT ALLOW 2 identical Mac's to be online [registered on the network] in the same segment.

So when you are all requesting Mac's for trade you should actually be asking for Mac's from a different Cable network segment. You may think this obvious but the network does not necessarily follow the physical layout of your town/ city.

The segments of the cable network [like the orange are separated], in the case of cable the separation is done by ROUTER GATEWAYS, known as UBR's [**Universal Broadband Router**].

FINDING YOUR UBR is easy

The link given goes to the GRC [Gibson Research Corporation] website [a bit like who is]

<https://www.grc.com/x/ne.dll?bh0bkyd2>

When you initiate the page it will return your full UBR address [Bottom (4th) box between the "Proceed" Buttons]

xxx.xxx.xxx.xxx.cable.ubrxx.shef.blueyonder.co.uk

xxx is replacing actual numbers [you won't see xxx on the result]

The information address follows the following format:-

YOU'RE INTERNET I.P / NETWORK TYPE / UBR SEGMENT / YOUR CITY
ACRONYM / PROVIDER DOMAIN NAME

For example if it returned a UBR05 this means you're in segment 05 of your town/city

So for MAC trading purposes you need to trade with anyone outside UBR05, for example UBR01. Areas/ cities are normally segmented into approx 10 segments depending on size

You should supply TOWN/ CITY ACRONYM & UBR SEGMENT
i.e.: SHEF.UBR05

All the Best, Viiiper

2b. Sniffing for new MAC Addresses using DHCP Force

Now we know about UBR's, lets talk about Sniffing out Macs. There's a few programs out there that will suit your needs, the most popular is DHCP Force, others include CM Sniff and Mac Reaper. I'll cover DHCP Force as it's most commonly covered and a tutorial is already written.

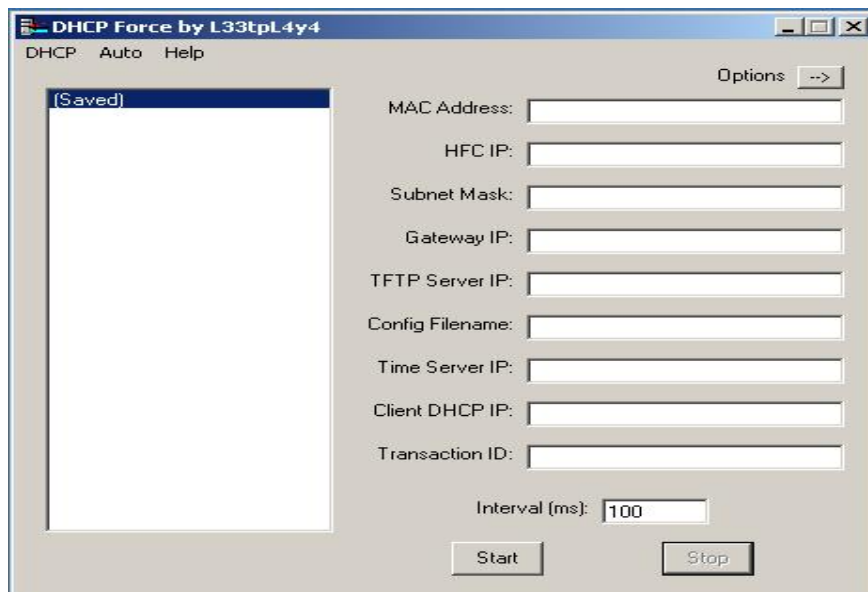
The following screen shots and text were put together by
Cleric



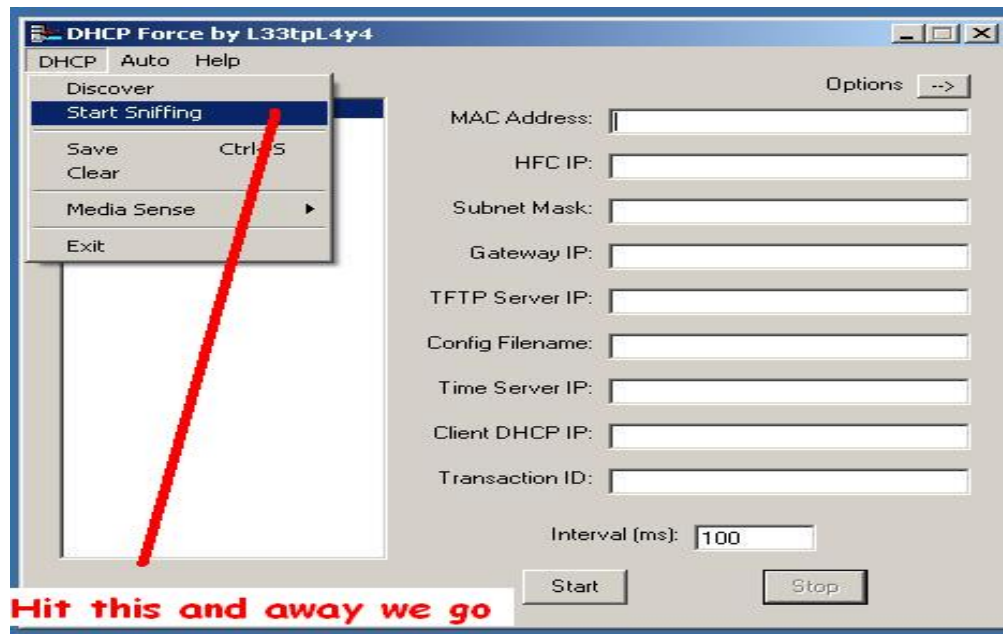
In this section I am going to tell you how I search for and find new Mac addresses using DHCP Force.

First off you need the program this can be found in most forums.

When you 1st run the program this is the screen you should have in front of you:



Once you have this screen up all you have to do to start sniffing for Mac addresses on your gateway is go to DHCP and select start sniffing as seen in next screen:

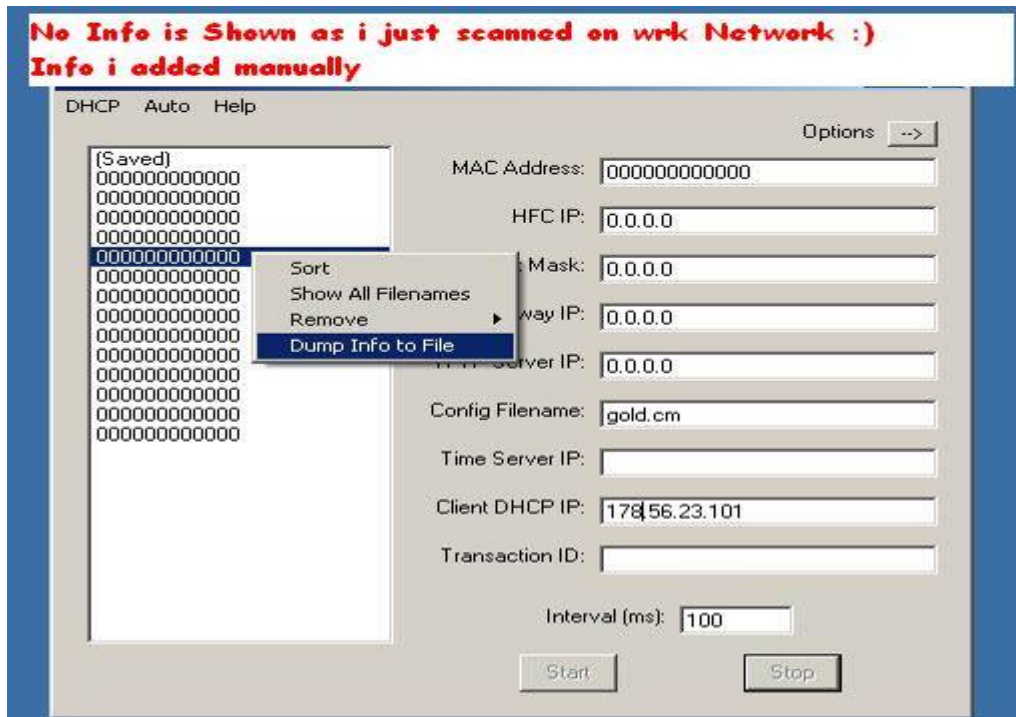


Once you have hit the start sniffing button it becomes a case of sit back and wait for it to scan your gateway and find any Macs available, this is time consuming and slow and at present seems to take a day or two of constant scanning so just get on with summit else while you wait ☺

One point I will make when scanning for Macs is that you must not be connected to a Router or have a firewall enabled, you will just get back blank results as a few peeps from forums have found out, it can be done but its best just to unplug modem from router and do the scan.

The other thing you have got to consider is once you have all your Macs you are going to have to trade Macs with someone in your surrounding area as you cant use the Macs from your gateway as the network will see two people with the same Mac address and start kicking each of you off all the time, this is the reason you need to find someone in your area that is on a different gateway, swap Macs and then use the new Mac to clone a modem. Most forums that deal with cable have a Mac swapping thread.

Once finished sniffing you should have a picture like this with address and Macs in etc:



You can save these addresses by right clicking on the addresses and selecting Dump info to file as in picture, this file is saved were you run your DHCP Force program from.

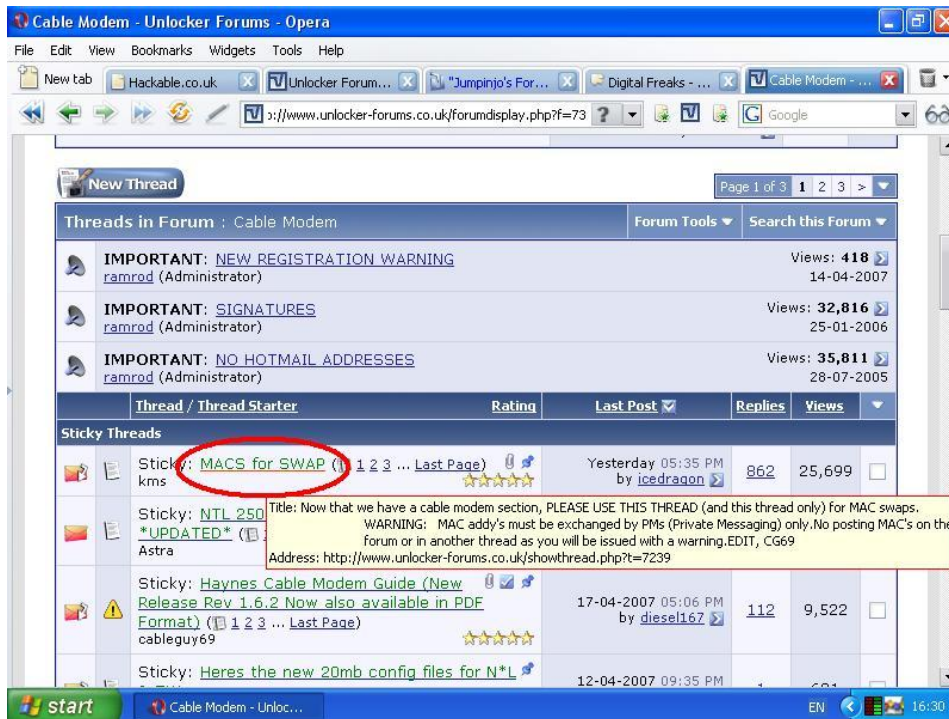
The thing I always do as well is get rid of all the slower config files cause you no you will never use them so there is no point in having a list of them ☺

Only keep your mid and high ones, there is also a 10meg at min as well.

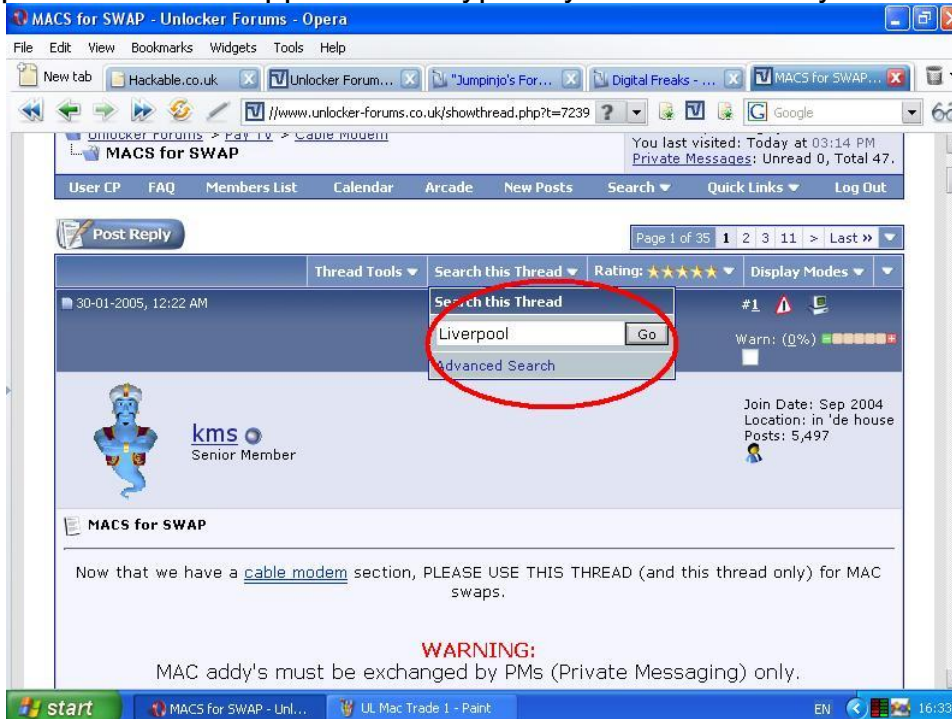
2c. Mac Swap Tutorial

There seems to be loads of people struggling to get their heads round the Mac Trade Threads, so I've put this together to help.

1. Go to the Mac Trade thread



2. Once in the Mac Trade thread, click the tab that says "Search this thread". A drop down box will appear. Now type in your Town or City and click "Go".



- Now you will have a list of everybody who's posted a request in your Town / City. Note down the names of the people who've posted requests and send them a polite PM asking for a trade.



Now if you haven't already posted in the Mac Trade thread, do so now, the reason being, so other members, who may need Macs in the future, can go through the same process.

This is however by no means always going to work. You'll still have to rely on other people to be generous and send you Macs and you may also find nobody from your area has posted. The only other option then is to go to a mates or family members and scan from there if they live outside your UBR but within the server limits. Another way is to go out with a wireless laptop and see if you can get into somebody's wireless network and bring up the web interface of their cable modem and get a Mac like that, although you'll need to check the UBR address first to make sure it's compatible for you.

If you don't know your UBR click one of these links to find it.

<https://www.grc.com/x/ne.dll?bh0bkyd2>

http://www.dslzoneuk.net/ip_checker.php

2d. Know your DOCSIS

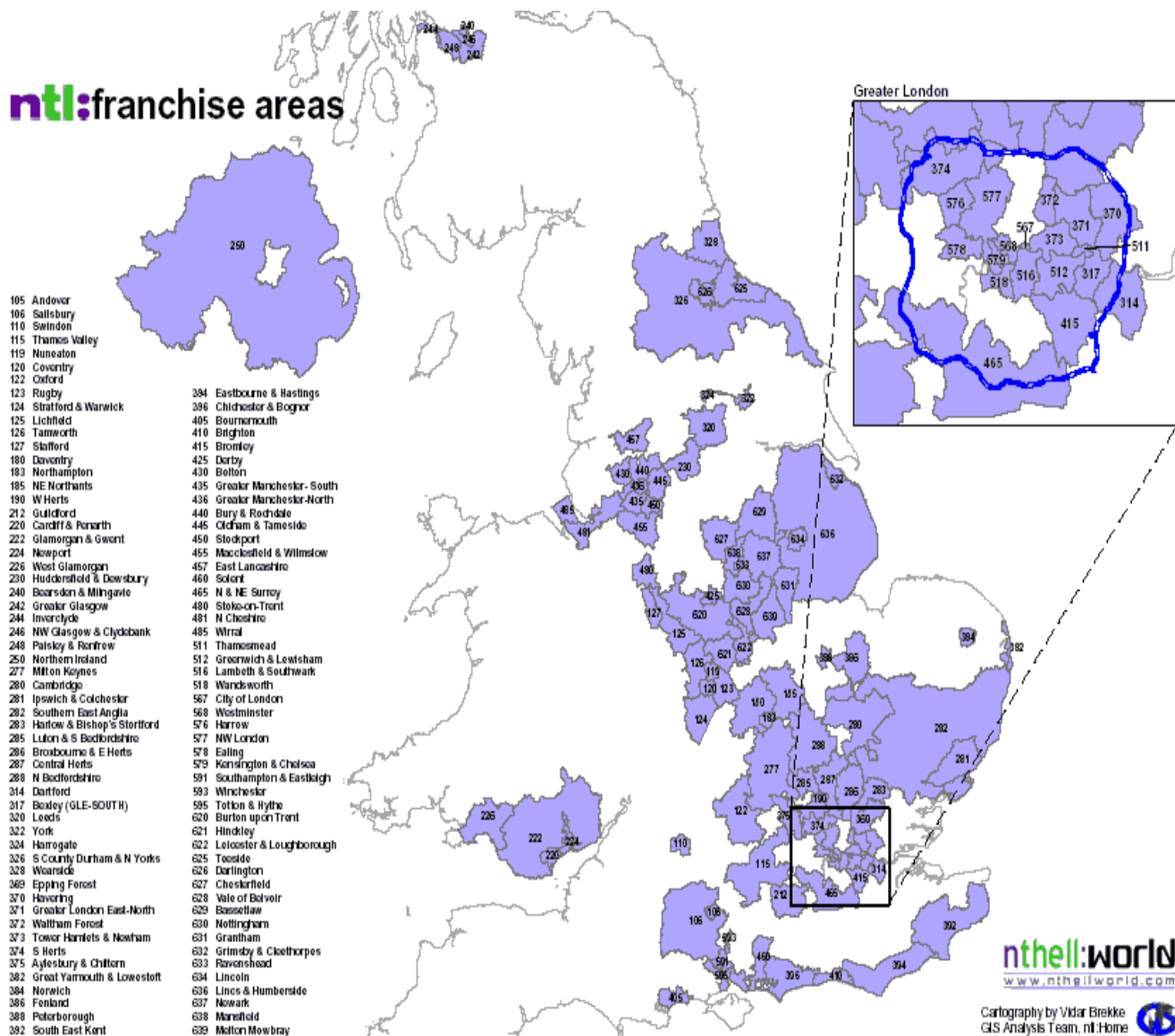
If your area on the map starts with:

1, 2 or 6; Then you are in a Pure NTL area: International DOCSIS.

3, 4 or 5; Then you are in an ex C&W area: European DOCSIS

If you are in the TW area, then that's an International DOCSIS area.

NTL: Franchise Areas (Pure & Ex-C&W)



To find out if you're in pure NTL or ex C&W area, go to the link below and enter your postal code:

http://www.dslzoneuk.net/ntl_region.php

Telewest: Network Map

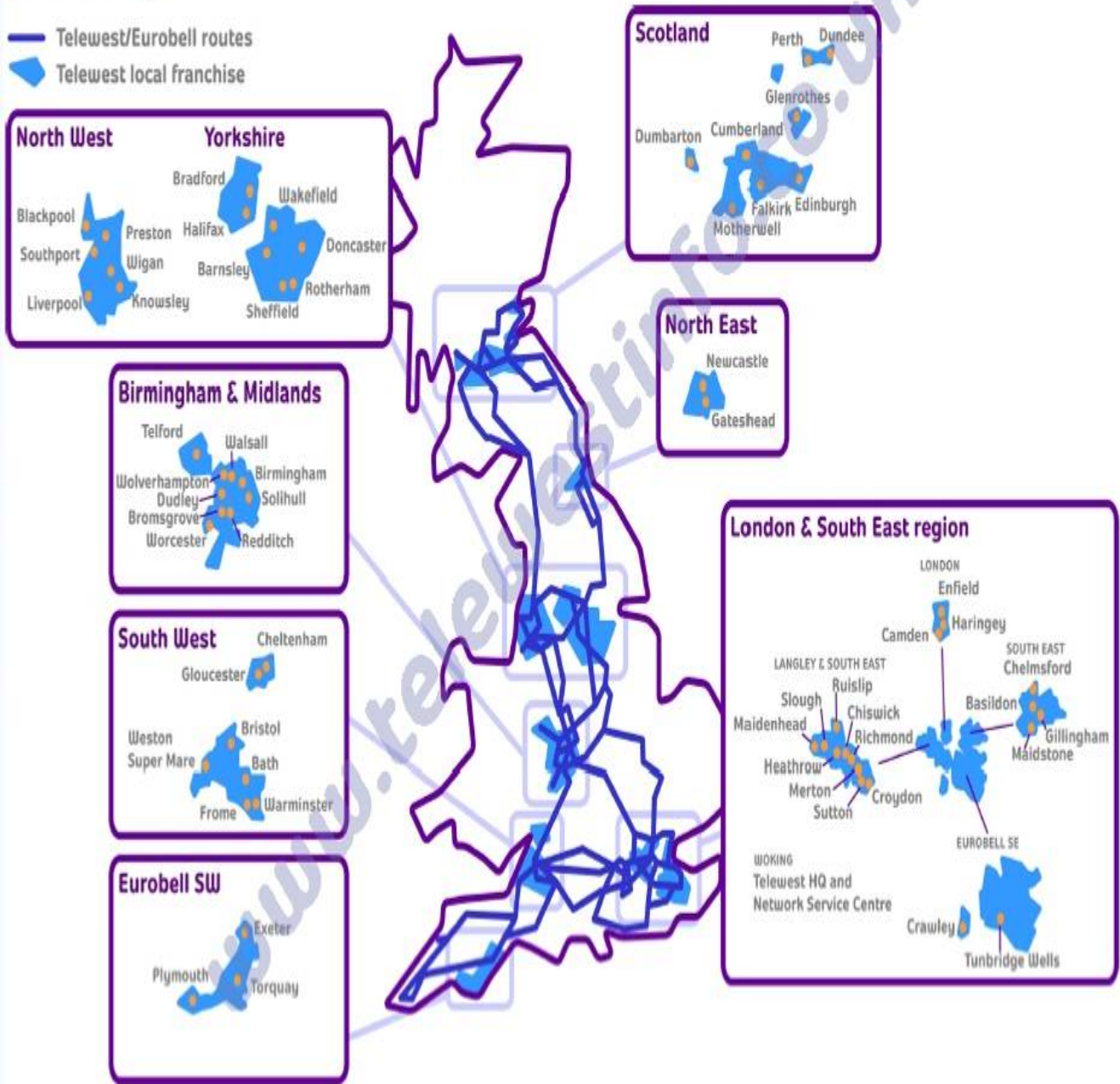
At a glance August 2002

www.telewestinfo.co.uk



Network map

- Telewest/Eurobell routes
- Telewest local franchise



I DOCSIS Modems will only work in Pure NTL & TW areas.

E DOCSIS Modems will work in all areas, i.e.: ex C&W, Pure NTL & TW areas.

2e. Config file Database, accurate on: 03/06/2007

Warning!!! This Database could change at any moment, config files are constantly being reviewed and updated by Virgin Media, this list is accurate on the day of posting.

NTL

Config File Name	Down Speed	Up Speed	Notes
noserv.cm	-	-	No internet access at all
unreg.cm	-	-	No internet access at all
cmreg-mota4100-light.cm	1Mb	128kb	
cmreg-mota4100-mid.cm	2Mb	256kb	
cmreg-mota4100-midxbox.cm	2Mb	256kb	2 IP Address's
cmreg-mota4100-mid-ps2.cm	2Mb	256kb	2 IP Address's
cmreg-mota4100-high.cm	4Mb	256kb	
cmreg-mota4100-highxbox.cm	4Mb	256kb	2 IP Address's
cmreg-mota4100-high-ps2.cm	4Mb	256kb	2 IP Address's
cmreg-mota4100-bund03.cm	10Mb	512kb	20Mb if area has been upgraded
cmreg-mota4100-bund03xbox.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmreg-mota4100-bund03-ps2.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmwsi-mota4100-2048-aol.cm	2Mb	256kb	
cmreg-mota4100-unltd01.cm	512kb	76kb	
cmreg-ntlhm100-light.cm	1Mb	128kb	
cmreg-ntlhm100-mid.cm	2Mb	256kb	
cmreg-ntlhm100-midxbox.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm100-mid-ps2.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm100-high.cm	4Mb	256kb	
cmreg-ntlhm100-highxbox.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm100-high-ps2.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm100-bund03.cm	10Mb	512kb	20Mb if area has been upgraded
cmreg-ntlhm100-bund03xbox.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmreg-ntlhm100-bund03-ps2.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmwsi-ntlhm100-2048-aol.cm	2Mb	256kb	
cmreg-ntlhm100-unltd01.cm	512kb	76kb	
cmreg-ntlhm120-light.cm	1Mb	128kb	
cmreg-ntlhm120-mid.cm	2Mb	256kb	
cmreg-ntlhm120-midxbox.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm120-mid-ps2.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm120-high.cm	4Mb	256kb	
cmreg-ntlhm120-highxbox.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm120-high-ps2.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm120-bund03.cm	10Mb	512kb	20Mb if area has been upgraded
cmreg-ntlhm120-bund03xbox.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmreg-ntlhm120-bund03-ps2.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmwsi-ntlhm120-2048-aol.cm	2Mb	256kb	
cmreg-ntlhm120-unltd01.cm	512kb	76kb	
cmreg-ntlhm200-light.cm	1Mb	128kb	
cmreg-ntlhm200-mid.cm	2Mb	256kb	

Continued on next page

NTL (Continued)

Config File Name	Down Speed	Up Speed	Notes
cmreg-ntlhm200-midxbox.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm200-mid-ps2.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm200-high.cm	4Mb	256kb	
cmreg-ntlhm200-highxbox.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm200-high-ps2.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm200-bund03.cm	10Mb	512kb	20Mb if area has been upgraded
cmreg-ntlhm200-bund03xbox.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmreg-ntlhm200-bund03-ps2.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmwsi-ntlhm200-2048-aol.cm	2Mb	256kb	
cmreg-ntlhm200-unltd01.cm	512kb	76kb	
cmreg-ntlhm250-light.cm	1Mb	128kb	
cmreg-ntlhm250-mid.cm	2Mb	256kb	
cmreg-ntlhm250-midxbox.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm250-mid-ps2.cm	2Mb	256kb	2 IP Address's
cmreg-ntlhm250-high.cm	4Mb	256kb	
cmreg-ntlhm250-highxbox.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm250-high-ps2.cm	4Mb	256kb	2 IP Address's
cmreg-ntlhm250-bund03.cm	10Mb	512kb	20Mb if area has been upgraded
cmreg-ntlhm250-bund03xbox.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmreg-ntlhm250-bund03-ps2.cm	10Mb	512kb	2 IP Address's & 20Mb if area has been upgraded
cmwsi-ntlhm250-2048-aol.cm	2Mb	256kb	
cmreg-ntlhm250-unltd01.cm	512kb	76kb	

Telewest

Config File Name	Down Speed	Up Speed	Notes
dtv-only.cm	-	-	No internet access but can be forced to use another config
hsi.cm	1Mb	128kb	
midband.cm	256kb	128kb	
platinum.cm	1Mb	256kb	
sa-dtv-only.cm	256kb	64kb	
sa-hsi.cm	1Mb	128kb	2 IP Address's
sa-midband.cm	256kb	128kb	2 IP Address's
cm-1024-128	1Mb	128kb	
cm-2048-256	2Mb	256kb	
cm-2048-512	2Mb	512kb	
cm-2148-256	2Mb	256kb	
cm-4096-384	4Mb	384kb	
cm-4096-512	4Mb	512kb	
cm-10240-384	10Mb	384kb	
cm-10240-769	10Mb	769kb	
cm-20480-768	20Mb	768kb	
cm-cpe2-1024-128	1Mb	128kb	2 IP Address's
cm-cpe2-2148-256	2Mb	256kb	2 IP Address's
cm-cpe2-4096-384	4Mb	384kb	2 IP Address's
cm-cpe2-10240-384	10Mb	384kb	2 IP Address's
cm-cpe2-20480-768	20Mb	768kb	2 IP Address's

3. Spoofing Your NIC (Network Interface Card)

Now the above is not essential but if you have a subscribed modem which is recommended, and you plan to connect your clone to the same network card (Ethernet Card also known as NIC & Network Interface Card) you should take some precautions as the cable companies can see your NIC and can log the against your modems Mac address. So for example you connect your subscribed modem to your PC through your NIC then you connect a cloned modem to the same pc using the same NIC then the cable co. will know you've used a clone on your PC and you'll get the dreaded knock on the door. All of this of course is theoretical and I've never heard of anybody getting caught using a clone like, to be honest I've never heard of any body getting caught using a clone but that's another topic all together.

The following screen shots and text were put together by [Cleric](#)



3a. Changing your NIC MAC

This is a simple procedure, download SMAC from one of the various forums, run it and enter the Mac address you want in the boxes as shown bellow and hit update Mac, restart pc and your done.



PUT THE MAC ADDRESS YOU WANT IN THESE BOXES AND YOUR DONE

I personally recommend you only change the last two or three digits of the NIC Mac as completely changing the Mac can cause your PC to not detect a network connection. Also if you have never connected a subscribed modem to the NIC you are going use your clone on then there will be no need to spoof the NIC Mac address. If you have never used Ethernet and only used USB or just plan to use your clone via USB then you will not need to spoof the NIC as it will not be getting used.

4. IP Address

Here's some very simple and quite helpful fault finding information. If you don't know how to check your IP address, do the following.

Windows 95, 98 & Millennium

- 1) Click Start>Run
- 2) Type: [winipcfg](#) and hit Enter
- 3) In the drop down box click on your connection (If you connect through Ethernet highlight your network card, if you connect through USB highlight the cable modem).

For Windows 2000 & XP

- 1) Click Start>run
- 2) Type: [cmd](#) and hit Enter
- 3) In the new dos window type: [ipconfig](#) and hit enter.

If the IP starts **192** then the modem is either receiving no signal via the cable feed or the Mac address isn't recognized by the cable co.

If the IP starts **169** then you've got a connection problem between your modem and PC theirs quite a few possible causes, Firewalls, SMAC, Virus, Faulty USB or Ethernet Cable the list goes on.

5. MAX 232 & 233

Two really easy circuits to build the Max 233, is probably the easiest of the two and more reliable. If you're a bit of lazy Tw*t you can buy these circuits ready made. My favorite stockiest is Tailor Made Circuits and can be found at this address.

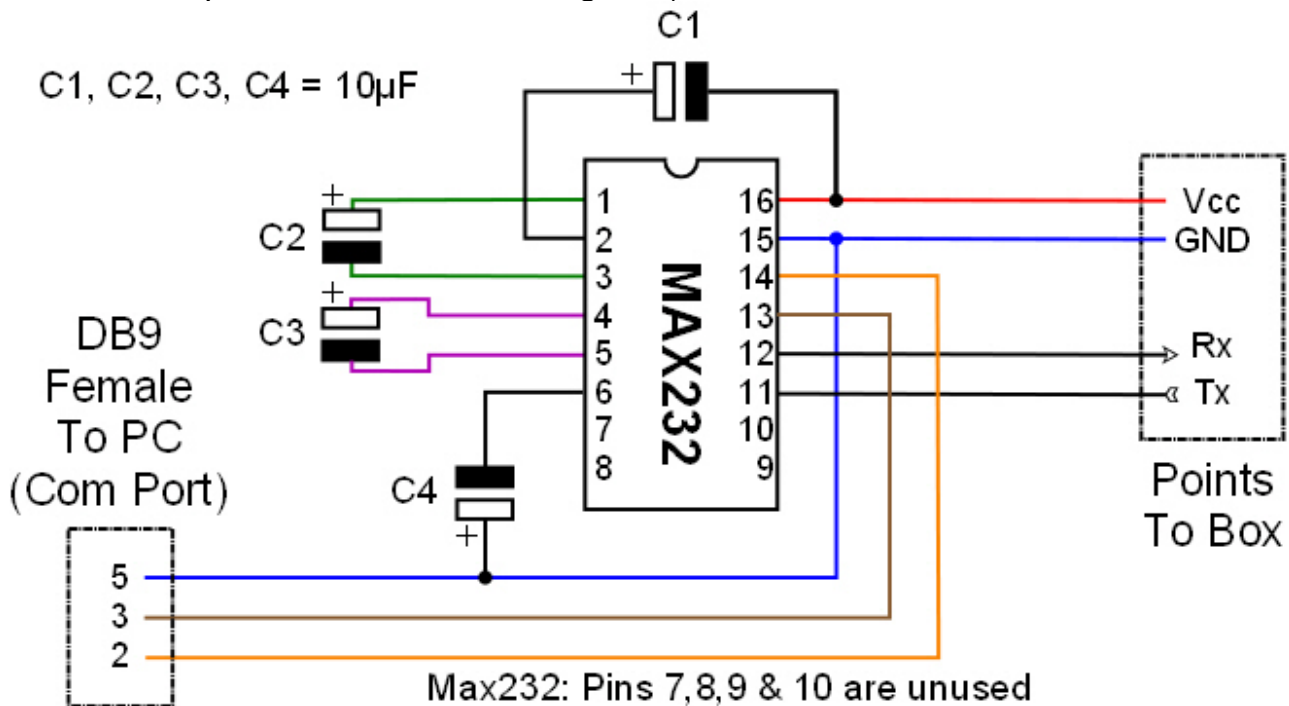
www.tailor-madecircuits.com

The following text and images were from LLAADD.

5a. MAX232

The voltage tolerance of the capacitor should not matter; anything over 12v should work fine.

Make sure you use electrolytic capacitors, & put them the correct way, as shown (White side is positive, black side is negative):



Parts List

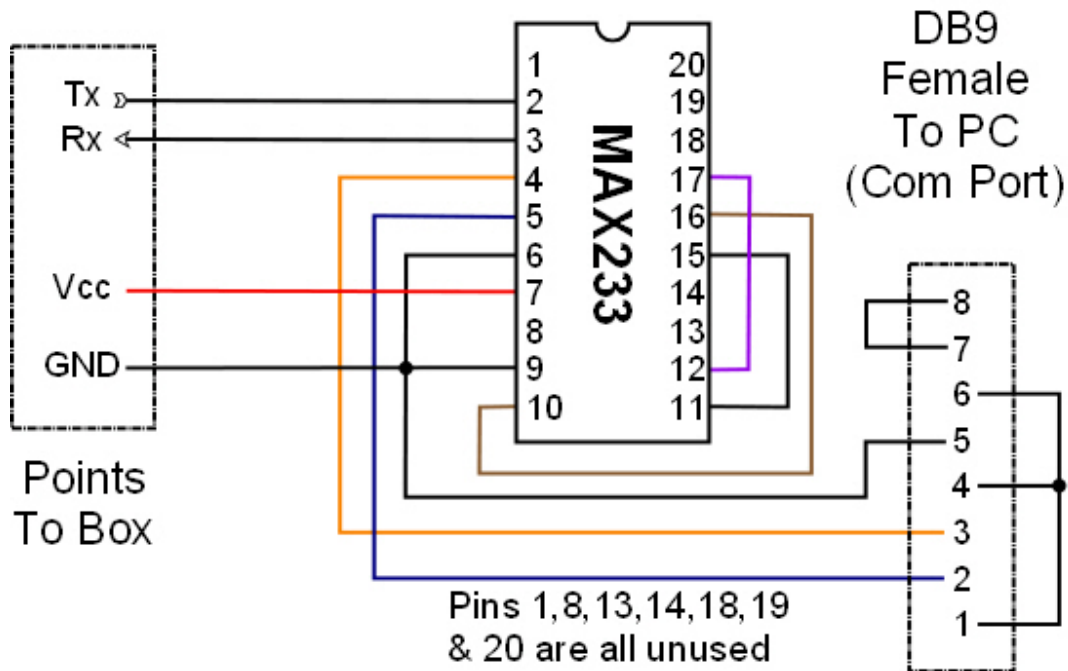
- 4 x 10 μ F Capacitors
- 1 x MAX232 Microchip
- 1 x 9pin DB9 Female Serial Cable

Optional Parts

- 1 x 16 Pin Microchip Holder (allows easy replacement of IC)
- 1 x 4 Pin internal PC Audio connector (Female)

5b. MAX233

This one is simple to put together.



Parts List

- 1 x MAX233 Microchip
- 1 x 9pin DB9 Female Serial Cable

Optional Parts

- 1 x 20 Pin Microchip holder (allows easy replacement of IC)
- 1 x 4 Pin internal PC Audio connector (Female)

5c. Pre Manufactured Max Cables

Chartmans Max 232



- Pin 1. TXD
- Pin 2. RXD
- Pin 3. GND
- Pin 4. VCC

http://www.fleetcomputersystems.co.uk/product_info.php?products_id=35

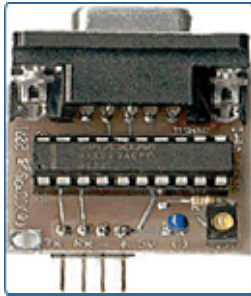
TMC Max 232



- TXD =1 Red
- RXD =2 Yellow
- VCC =3 Blue
- GND =4 Black

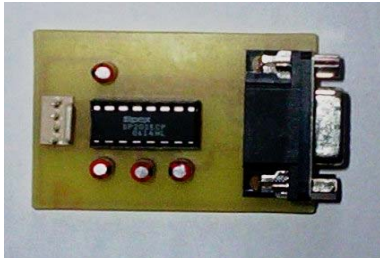
http://www.tailor-madecircuits.com/rs232_max.htm

Jabs Place Max 233



PIN 3: TX
PIN 4: RX
PIN 5: POWER (-)
PIN 6: POWER (+)

Wayneeboy19117



VCC = RED
GND = BLACK
RXD = YELLOW
TXD = GREEN

[You'll need to PM Wayneeboy19117 on Digital Worldz.](#)
[Don't worry he is a trusted member of that forum and very reliable.](#)

5d. Webstar Max cable adapter

All screenshots and text were compiled by

Breed



Your max lead won't just plug into the Webstar like it does on a 250, it's a different plug and wiring order. You just need to make a small adapter to plug into the Webstar.



6. Ambit 200

Ok I've left out the Ambit 100 & 120 for the same reasons as Cleric and here's another great tutorial by the man himself.

The following screen shots and text were put together by

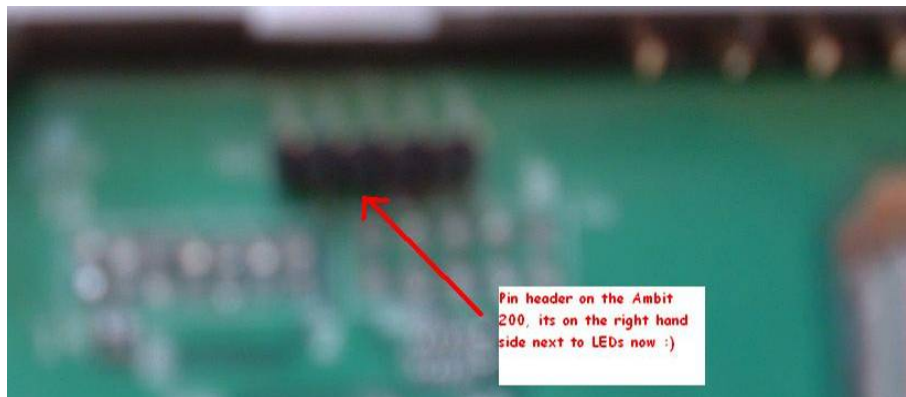
[Cleric](#)



6a. Changing the MAC Address of the Ambit 200

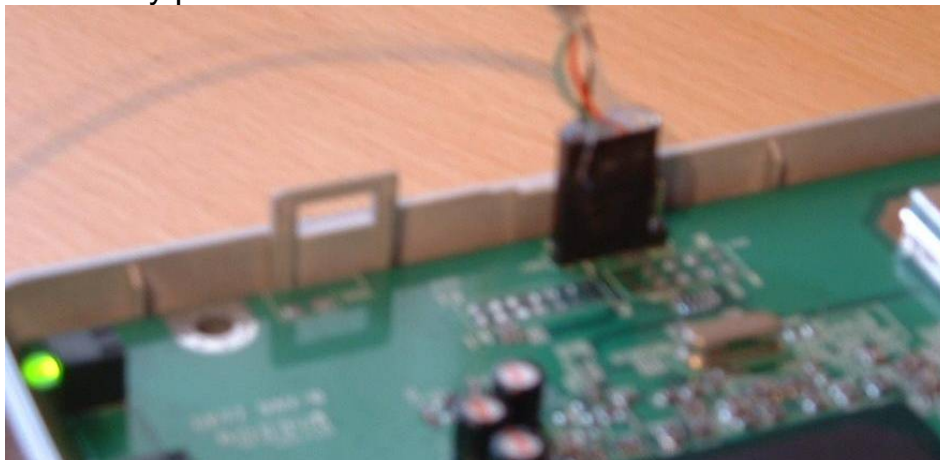
First things first ☺ , you will need to open your modem this is done by locating the rubber feet underneath your modem it's the back two you want to lift, once you have removed the rubber feet you need to remove the two screws, which will then allow you to unclip the cover, be careful as the clips are fragile and break easily.

Once you're inside your modem you need to locate a 5 pin header, you can see this in the photo below:



The pin header is on the Right hand side of the board on the ambit 200 modems. You will see that they are labeled: **GND, TXD, 3.3v, RXD & GND**, you will only be using one of the grounds and that is the one next to TXD.

Now you need to attach your audio clip onto the pin header as shown below, it should fit perfectly without any problems:



Once this is done attach the serial end to your computer in COM1, don't plug the power into your modem yet.

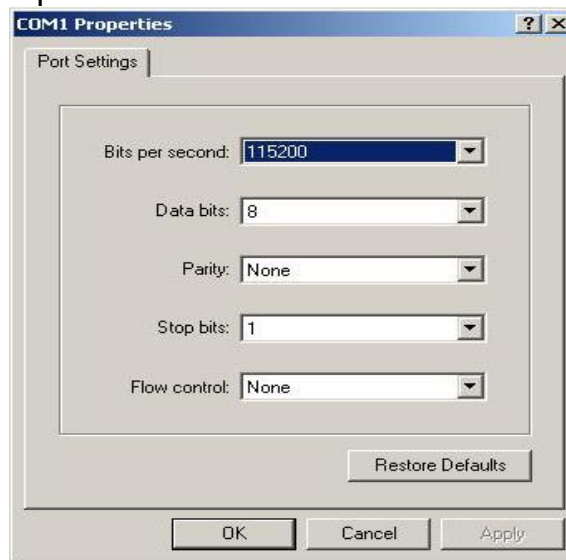
6b. Communicating with your modem

Next comes the setting up of your computer to talk to the modem, this can be done in two ways either using **HyperTerminal** or **Teraterm** (download available from the shack under cable modem download section), for the purpose of this tutorial I am using hyper terminal.

Open up hyper terminal by going to

Start > Programs > Accessories > Communications > HyperTerminal

Click this to open up the program you will be asked to choose a name for the session, you can choose whatever you like, I just normally put in NTL, press ok, you will then need to configure your port I like to do this manually as I think it works better, the settings should be like the picture below:



Once you have set these hit ok, and you will see the next screen like in the picture below with the phone icon active:



But still don't plug the cable feed in yet!

The modem will not lock on so the data will keep running in HyperTerminal window this is fine

Now enter the non update command:

```
cd non-vol\nsnmp
max_dload_tries 0
write
cd \
reset
```

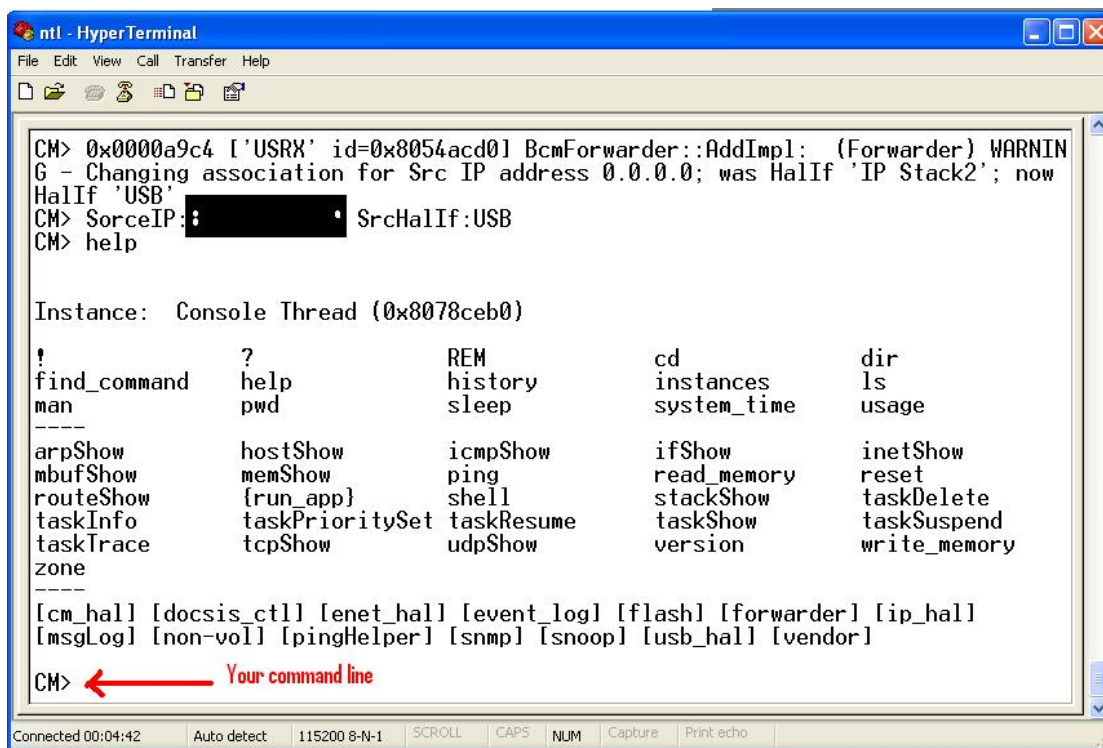
Now unplug the modem from the power lead and connect the cable feed

You should have the HyperTerminal window still open.

And now power the modem up again

And leave it to boot fully this time should take 30 sec's to a minute

But when complete you will see the picture below in HyperTerminal window



```
ntl - HyperTerminal
File Edit View Call Transfer Help

CM> 0x0000a9c4 ['USRX' id=0x8054acd0] BcmForwarder::AddImpl: (Forwarder) WARNIN
G - Changing association for Src IP address 0.0.0.0; was HalIf 'IP Stack2'; now
HalIf 'USB'
CM> SorceIP: [redacted] SrcHalIf:USB
CM> help

Instance: Console Thread (0x8078ceb0)

!          ?          REM          cd          dir
find_command  help      history     instances  ls
man          pwd       sleep       system_time  usage
-----

arpShow      hostShow  icmpShow    ifShow      inetShow
mbufShow     memShow   ping        read_memory  reset
routeShow    {run_app} shell       stackShow   taskDelete
taskInfo     taskPrioritySet taskResume  taskShow    taskSuspend
taskTrace    tcpShow   udpShow     version     write_memory
zone
-----

[cm_hal] [docsis_ctl] [enet_hal] [event_log] [flash] [forwarder] [ip_hal]
[msgLog] [non-vol] [pingHelper] [snmp] [snoop] [usb_hal] [vendor]

CM> ← Your command line

Connected 00:04:42  Auto detect  115200 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

What I always do is enter the non update again

This is as follows:

```
cd non-vol\nsnmp
max_dload_tries 0
write
cd \
reset
```

The modem will reset this time and just wait until you see the command line again.

This is now at the point we enter the new Mac in to the modem.

Once you're at the command line type the following:

Cd non-vol **press Enter**
Cd halif **press Enter**

Once you have done the above all you need to do now is enter the command for changing your Mac address which is as follows:

mac_address 1 00:00:00:00:00:00

This command sets HFC mac address (this is the cable modem mac address). Replace the 0's with your relevant numbers.

After you have entered your new mac address, type the following:

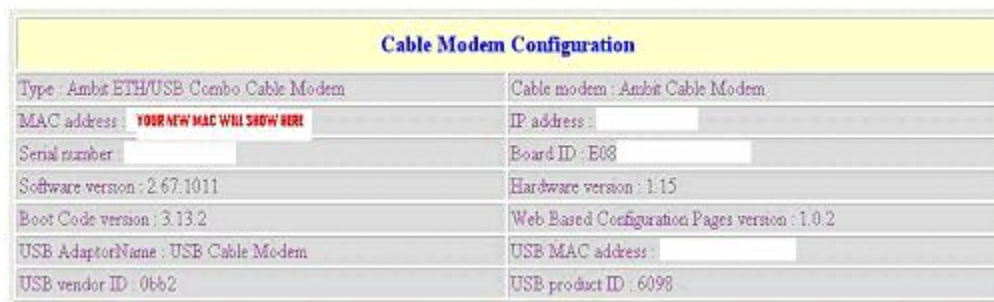
Write

This command writes the information you changed to the nvram, once this is done reset your modem by unplugging power and re plug back in.

That should be your Ambit 200 modem cloned with a new Mac address.

The next bit is to go into Internet explorer and type in <http://192.168.100.1>, this is the root address of the modem, you will be asked for a username and password they are both the same and it is **root**.

You should then see in the centre of your internet explorer the following information; this I hope will show you your new Mac address ☺



Cable Modem Configuration	
Type : Ambit ETH/USB Combo Cable Modem	Cable modem : Ambit Cable Modem
MAC address : YOUR NEW MAC WILL SHOW HERE	IP address :
Serial number :	Board ID : E08
Software version : 2.67.1011	Hardware version : 1.15
Boot Code version : 3.13.2	Web Based Configuration Pages version : 1.0.2
USB AdaptorName : USB Cable Modem	USB MAC address :
USB vendor ID : 06b2	USB product ID : 6098

You can now give yourself a pat on the back for cloning your 1ST Mac address

The Final thing you need to do is remove your max232 / max233 from your PC and your modem pin header connection, turn of modem, unplug cables and put modem back together with screws and sticky feet.

6c. Telewest (TW) Stream

Now as I've already mentioned the NTL Ambits can be used on a TW stream to do this you must do the following as put together by me,

[Cableguy69](#)



Enter 192.168.100.1 into your web browser you will be asked for username and password both are root once you have entered these details you will be presented with this screen:

Cable Modem Configuration	
Type : Ambit ETH/USB Combo Cable Modem	Cable modem : Ambit Cable Modem
MAC address : 00:20: [REDACTED] F2	IP address : 10 [REDACTED] 249
Serial number : 0041 [REDACTED] 19	Board ID : E08C [REDACTED]
Software version : 2.67.1011	Hardware version : 1.15
Boot Code version : 3.13.2	Web Based Configuration Pages version : 1.0.2
USB AdaptorName : USB Cable Modem	USB MAC address : 00:02:8A [REDACTED]
USB vendor ID : 0bb2	USB product ID : 6098

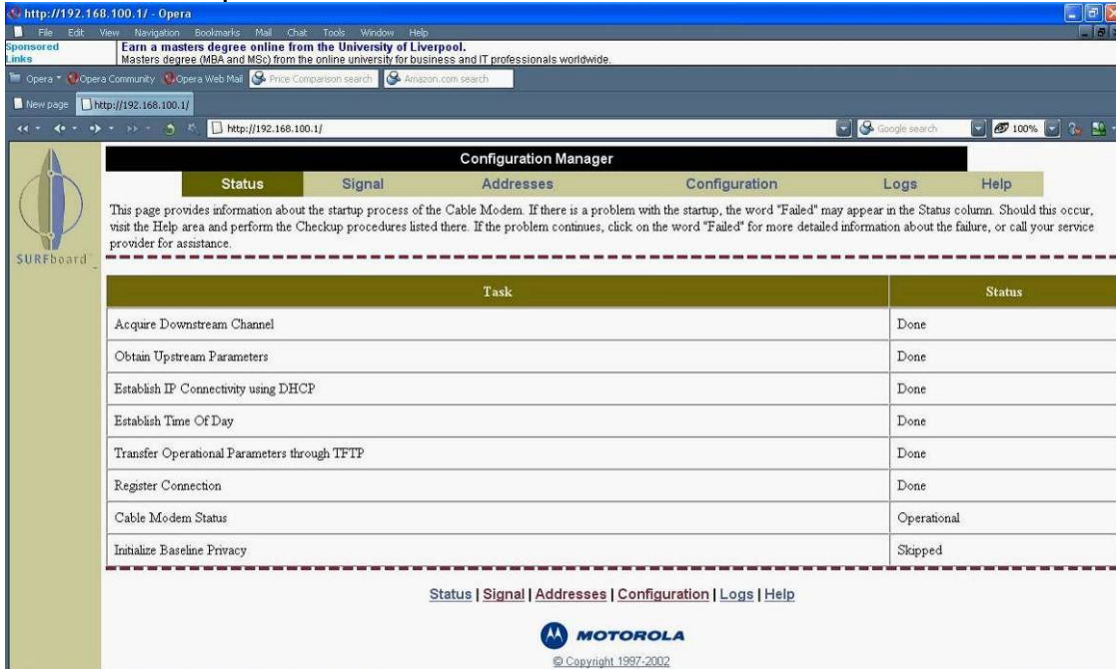
Once in the modems internal web page click on set search frequency parameters and you will now see this screen:

Frequency (Hz)	Status
331000000	Valid Channel
765000000	Valid Channel
807000000	Valid Channel
858000000	Valid Channel
147000000	Valid Channel
471000000	Valid Channel
763000000	Valid Channel
705000000	Valid Channel

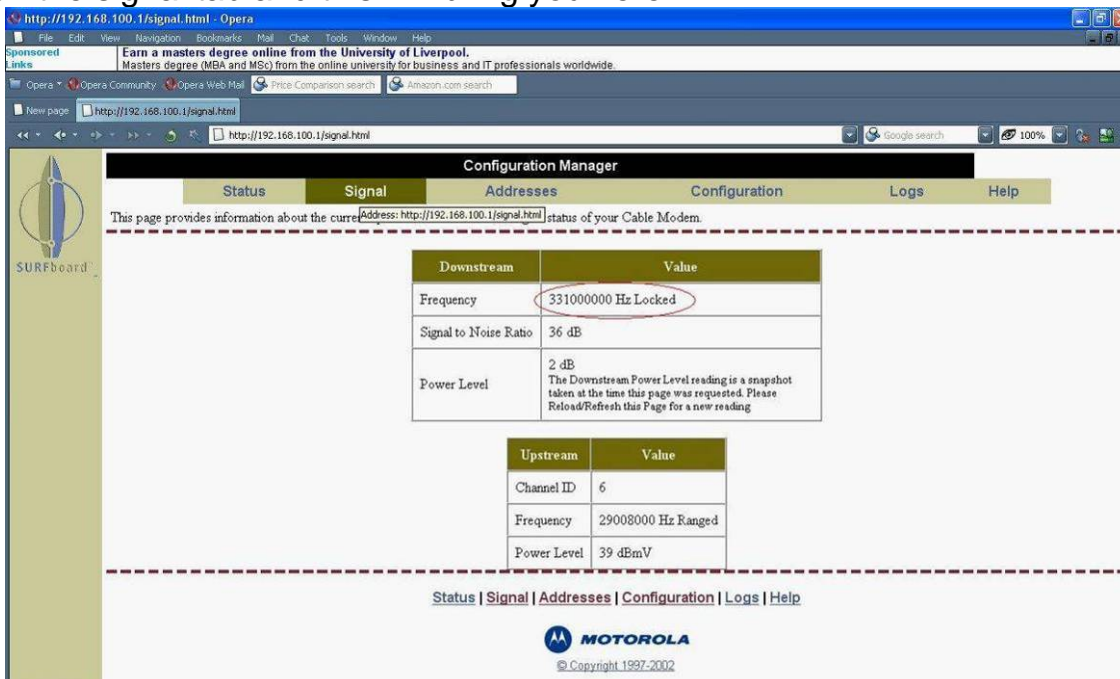
Now just delete one of the frequencies and in the box that says history frequency enter the correct downstream frequency for your area and click on “add” then click on “set all frequencies as valid” and that’s it all done.

PS these screen shots were taken from an ambit 200 with the 100/120 you will not need to delete any frequencies as there will only be one downstream frequency preset into the modem.

If you are unsure on how to find out your downstream frequency you can check your subbed modems internal web page in the same way although you will not need to enter a username or password here’s some screenshots from a surfboard modem:



Click on the signal tab and this will bring you here:



As you can see the downstream frequency has been changed to match TW's configuration.

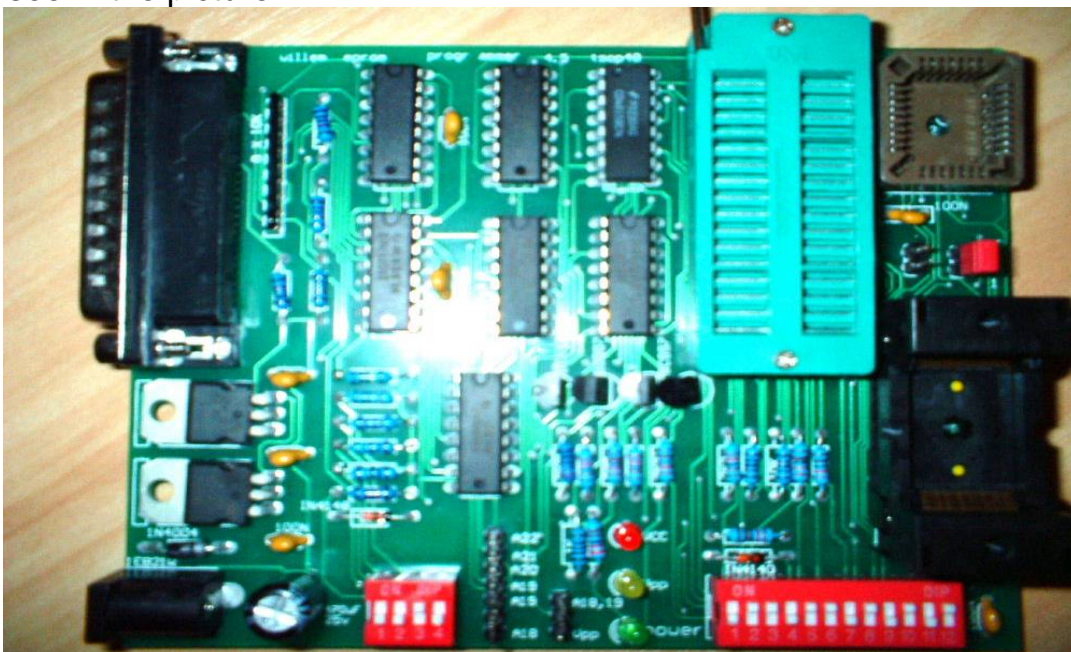
Please note the hacked Ambit modems are under attack From NTL and there are serious problems with these modems and a fix may never be found, but hopefully the resourcefulness of the people who are in the scene will find a solution to the current problems being experienced with NTL users. If some clever bugger finds a fix, for the NTL Updates then this tutorial will be updated accordingly. The way they initially kill your modem, is by upgrading the firmware on your modem (Firmware is what tells your modem how to operate). Once your Ambit has the update you will not be able to use Hyper / Terra terminal. If your modem has updated you will need to restore it to its original state, to do this there are two ways, an easy way and a hard way. I'll put in the tutorial for the hard way for educational purposes but you should be able to do it via the easy method. OK the hard way will require a certain amount of skill this requires you to remove the modems TSOP (Thin Small Outline Package), basically the 48 pin chip soldered to the modems circuit board. Secondly you will then need read, erase and then write to the chip. And thirdly, also the hardest part of the process, you'll need to re-solder the chip back to the board. Here's the tutorial on re-flashing the TSOP back to its pre updated state.

The following screen shots and text were put together by [Jim Rose](#)



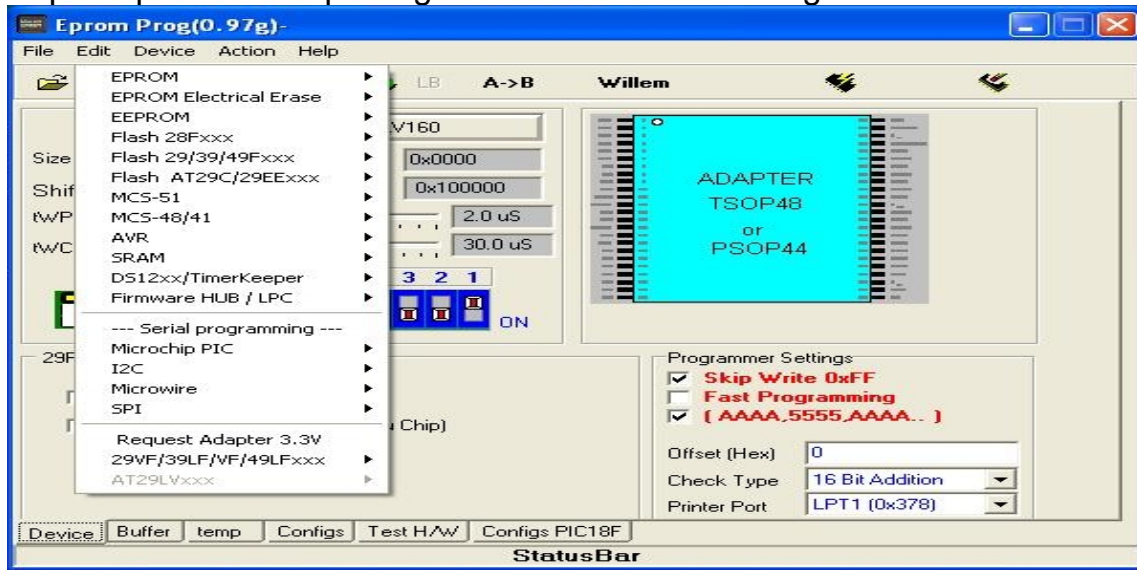
6d. Programming Ambit Chips, with Willem 4.5

1. Here is a picture, of how, I set the Willem up, the only jumper I had on is the 29f, as you can see in the picture:

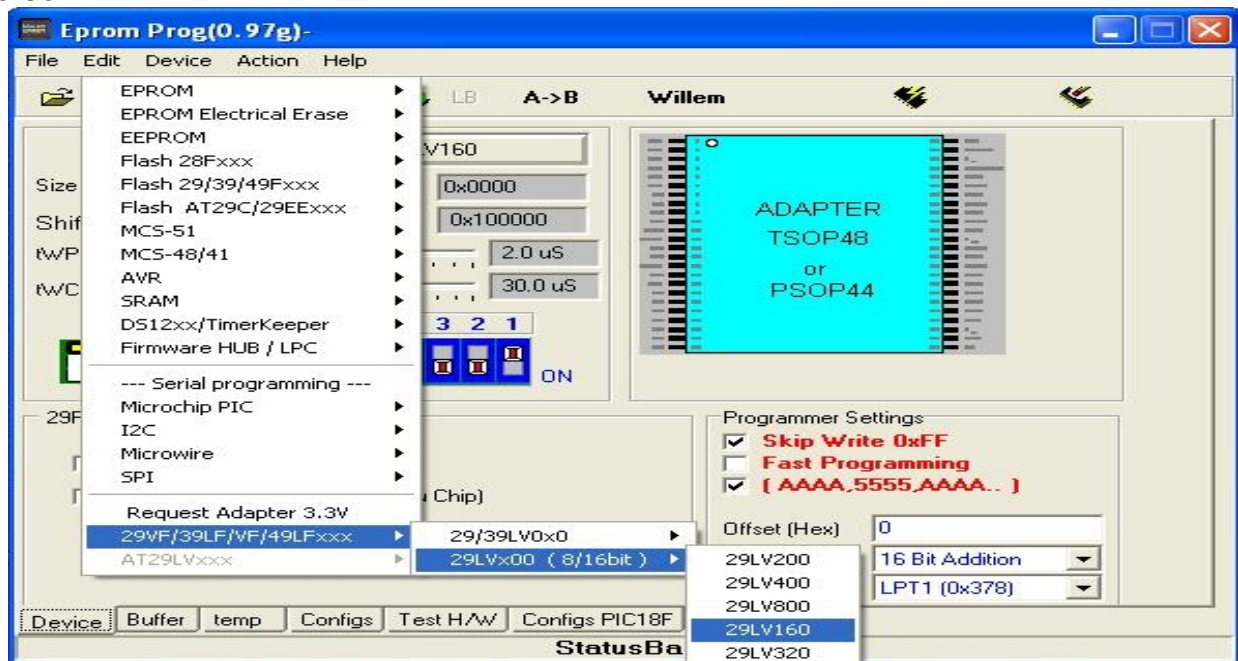


2. Ok once the Willem is set up put the chip in with the circle end at the top near the red jumper (29f). Put the serial lead in and the power lead in. I used a 12v, 1 amp power adapter.

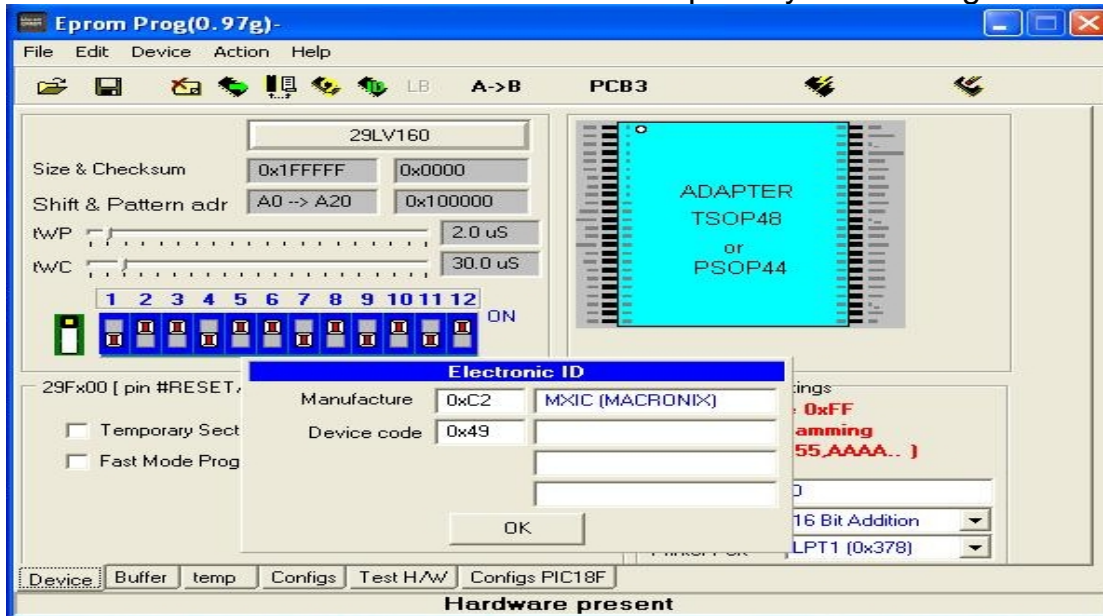
3. Now open up software epr097g which is included. Now go to device like below:



then go to 29VF/39LF/VF/49LFxxx, then 29LVx00 (8/16 bit), then down to 29LV160, like so

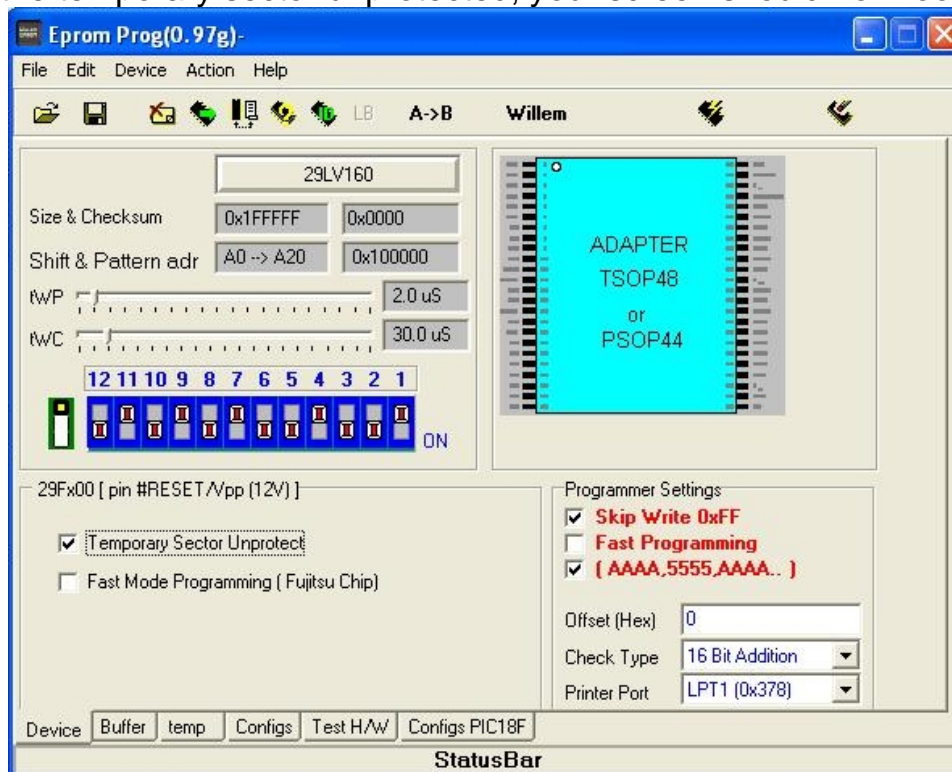


4. Once this is selected hit the id button to id the chip and you should get the following:



5. Once you hit ok, erase the chip the erase button is underneath the minimize button in the picture above. Don't panic if it goes to about 5% then cuts out, just repeat this process about 5 or 6 times to be sure. You can then do a blank chip test by clicking on the chip with the question mark.

6. OK moving onto the settings of the software to program chip
Firstly where its says PCB3 on the above picture click on it to change it to Willem , then check the temporary sector unprotected, your screen should now look like this:



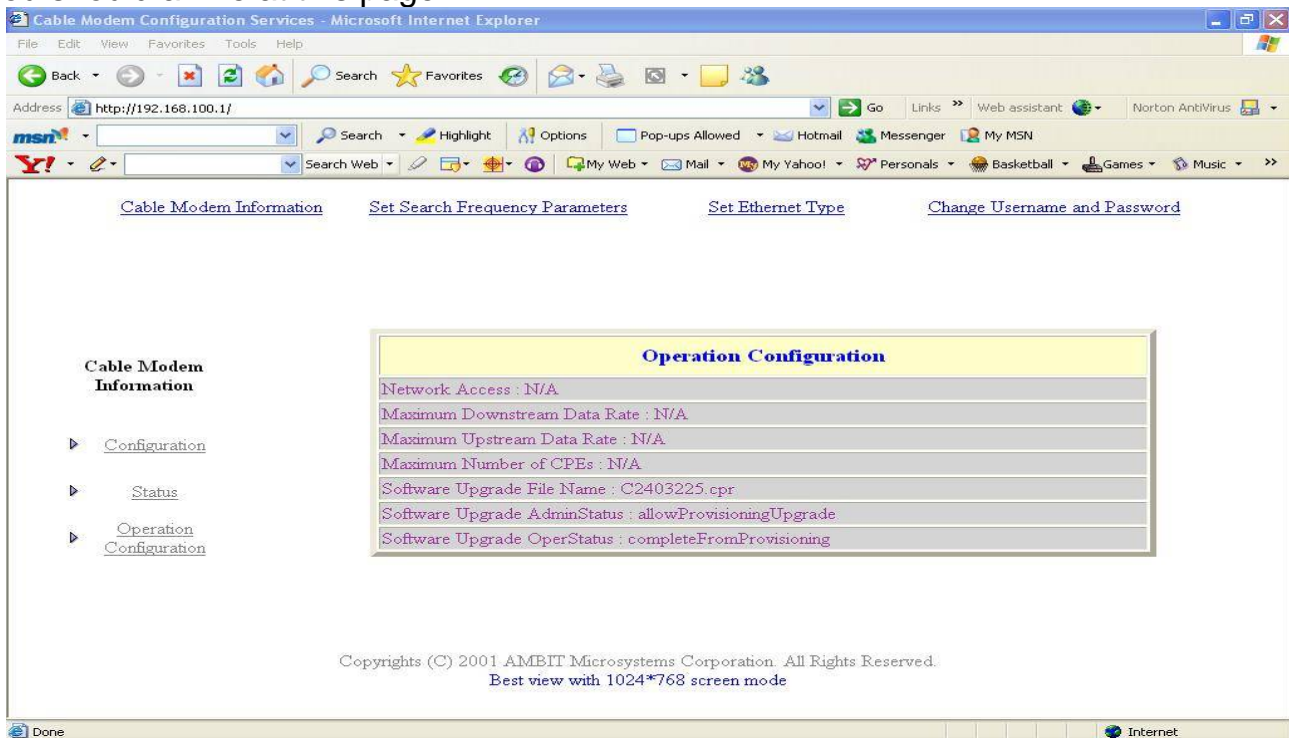
As you can see it gives you the dip switch settings but they are back to front as you can see they go from 12 to 1.

7. Now what you have to do is clear the buffer which you can do by clicking on the little yellow box with red X through it. Once you have done this load up your dump which should be in BIN form.

8. Once you have loaded up your pre-updated dump click on program chip which is the little picture of the chip with the lightening through it. It took about 10-15mins programming and verifying the chip.

9. Now put the chip down, there are various methods of doing this if you search around. Once the chip is down, plug in your Ethernet cable and your power lead (NOT CABLE FEED) into the modem and switch on. Then the Sync, Power and Rdy lights will come on solid for about 10 seconds then they will all flash in sequence if this does not happen and the Power, Rdy and Sync stay solid there is a problem either try re-laying the chip or reprogram it again.

10. Now open up internet explorer and type 192.168.100.1 into the address bar and you should arrive at this page:



As you can see it still has the old screen and where it says software upgrade file name it has the old software C2403225.cpr.

All you need to do now is put your new MAC on and do the no-update mod which you can find on **Unlocker-Forums** modem section.

I hope this helps you, please feel free to add to this tutorial, as some people might have different ways of doing this, but this the way I got it to work. AS FOR WORKING DUMPS I DON'T KNOW IF IM ALLOWED TO POST THEM WITH THIS, JUST PM ME AND I WILL SEND THEM TO YOU. Thanks to DannyMaxPower for his help, peace out JIM ROSE.

So, that's the hard way but luckily for you guys some genius came up with this method.

The following screen shots and text were put together by [JimboTheHo](#)



6e. Ambit 200 Firmware Downgrading via Ethernet

This guide will allow you to easily unlock terminal locked modems that stop at 3348 in HyperTerminal. Objective is to downgrade the firmware on the Flash to pre-updated non-terminal locked. Thus allowing us access to CM> prompt. After following this guide you need to follow the modem tutorial as usual. I advise not putting the modem on stream whilst you do this, it is not needed and will avoid it updating again.

Things you're going to need:

- Max232 cable and HyperTerminal Software
- Copy of image1.bin (included with this tutorial)
- Ethernet cable
- Solarwinds Tftp (included)

Installing Solarwinds

First step is to run the Solarwinds setup file [SolarWinds-TFTP-Server.exe](#). Just click Yes > Next > Yes when asked, Tftp server will install.

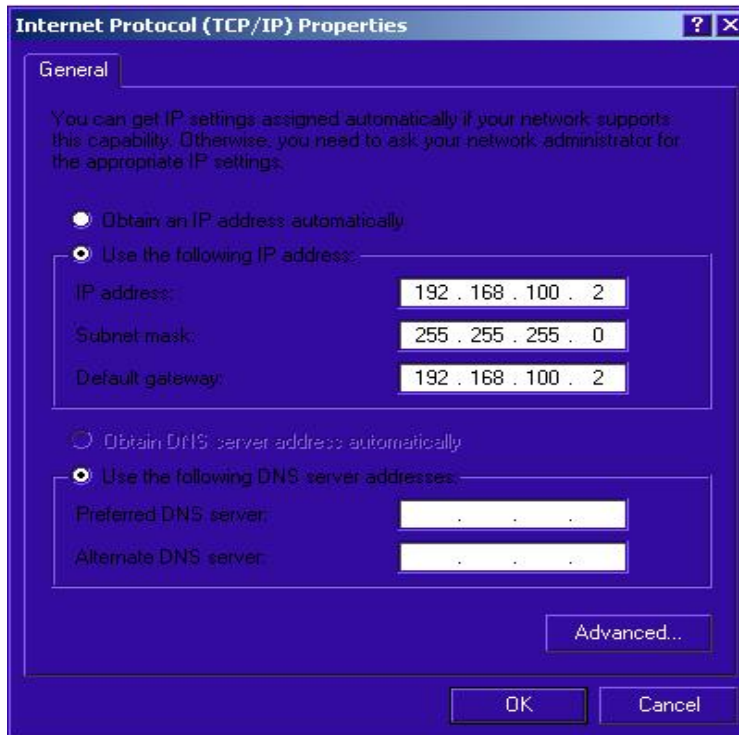
Next we need to configure our PC Ethernet card for connection with modem, goto:

Start > Settings > Control panel

Then Select **Network Connections**.

Right click on **local area connection** and click properties. In the white box you need to click on **Internet Protocol (TCP/IP)** then click **Properties**.

Information needs to be as below:



Setting up the locked modem

Now, it's time to connect your modem. You need to plug in Ethernet cable to you PC and MAX232 adapter to your pc serial card. Don't power the modem up just yet.

First you need to load HyperTerminal and open a connection to com port as usual. Now, plug your modem in but be ready to push P when prompted:

Enter '1', '2', or 'p' within 2 seconds or take default...

Shortly, after powering up.

If Successful you will see **Board IP Address [0.0.0.0]:**

Here you need to type **192.168.100.1** then press **enter**

IP mask **press enter**

IP gateway **press enter**

Mac address **press enter**

Internal/External **press I**

It will now say if successful

Init EMAC, DMA, and MII PHY...

Autonegotiation started, waiting for completion...Autonegotiation successful...

MAC setup for FullDuplex

Then, Display Main Menu.

Here **press D** to download the image and save to flash. It will ask for server and file details.

TFTP Get Selected

Board TFTP Server IP Address [0.0.0.0]:

Now we need to start the TFTP server.

First we need to copy the pre-updated image image1.bin to your c:\ root. This is included with the Tutorial. Just extract to c:\ with Winrar.

To load TFTP Server Click **Start>Programs>Solarwinds Free Tools>TFTPSEVER**

You need to make sure that any firewall applications you are running don't stop the TFTP server connecting. It's best to close them whilst running this tutorial to avoid problems.

Solarwinds Configuration



Click File > Configure you will be produced with the screen shown above. Make sure **C:** is selected as above and that **image1.bin** is listed. Click **OK** to save. There is no need to change any other settings. You should also note the IP address is correct in the status bar of TFTP Server.

Image Transfer

Back in HyperTerminal we can now enter our TFTP details as below.

Board TFTP Server IP Address [0.0.0.0]: **192.168.100.2**

Enter TFTP filename []: **image1.bin**

If all is good it will display:

Free store: a0300000
Starting TFTP of image1.bin from 192.168.100.2
Getting image1.bin using octet mode

.....
This is now copying to the modem. When complete it will say if successful:

CRC Verified
Destination image
0 = bootloader
1/2 = CM image
3 = specify flash sector
(0-3)[1]: Here **press 1** to save to Image 1 on the modem.

Stored 906916 bytes
Verified 906916 bytes

If asked **Store parameters to flash ? [n]** press **Y**

You will now be displayed with the main menu again. **Press B** to reboot the modem and load from flash.
If all goes well the modem will reboot. If all has gone well you should see the modem scanning for frequencies.

Congratulations you've done it.

Now be sure to do the MaxDloadTries = 0 fix before connecting to the cable stream.
Just follow the modem tutorial as normal.

You also need to be sure to change you PC's Ethernet IP configuration back to DHCP (Obtain IP address automatically) before connecting to the internet.

Respect to Bulla.

Please note that, both of these methods will only restore your modem back to, it's original state, this combined with the "no update" mod should keep your modem in a pre updated state.

6f. Latest release for the Ambit 200

The following screen shots and text were put together by

Boltar



SIGMA X2 Build 125 *CRACKED* Ambit 200 Tutorial

Introduction

There are 2 methods to flash this image onto your 200, the first is via a Blackcat cable (JTAG). If you are familiar with JTAG/Blackcat then you need no detailed instruction as you should already know what you are doing. Just write the included *sigmax2_125_cracked_dump.bin* file onto the flash using the '**Write All**' function in SchwarzeKatze. The other method is by using a serial connection and a max232/3 interface; this method will be explained below.

ALERT: *If you already have the older SigmaX on your 200 and have no JTAG interface then you cannot flash this image onto your modem. Even the Sigma bootloader that allows flashing is buggy, if you try to use this Sigma flash menu you will brick the modem. Look at the end of this tutorial for a way to restore a compatible bootloader so you may flash the new image correctly.*

Flashing the SIGMAX2 image onto the 200

Connect your modem to your PC using a MAX232/3 interface

Connect the modem to the PC via an Ethernet cable

In Windows Networking set the network adaptor connected to the modem to a manual configuration with these details:

IP Address: **192.168.100.10**

Subnet Mask: **255.255.255.0**

Gateway: **<don't enter anything>**

DNS: **<don't enter anything>**

Open up HyperTerminal or Tera Term using the following parameters:

Baud Rate: **115200**

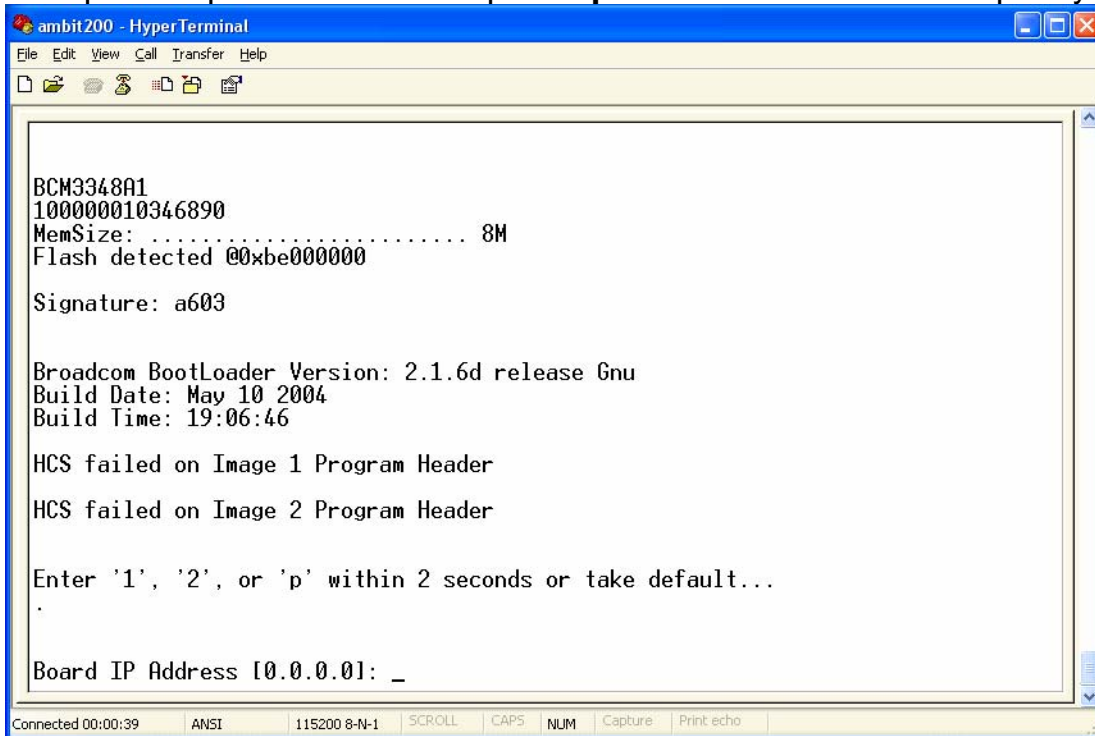
Data Bits: **8**

Parity: **None**

Stop Bits: **1**

Handshaking: **None**

Now power up the modem and press 'p' in the terminal window quickly.



```
ambit200 - HyperTerminal
File Edit View Call Transfer Help
[Icons]

BCM3348A1
100000010346890
MemSize: ..... 8M
Flash detected @0xbe000000

Signature: a603

Broadcom BootLoader Version: 2.1.6d release Gnu
Build Date: May 10 2004
Build Time: 19:06:46

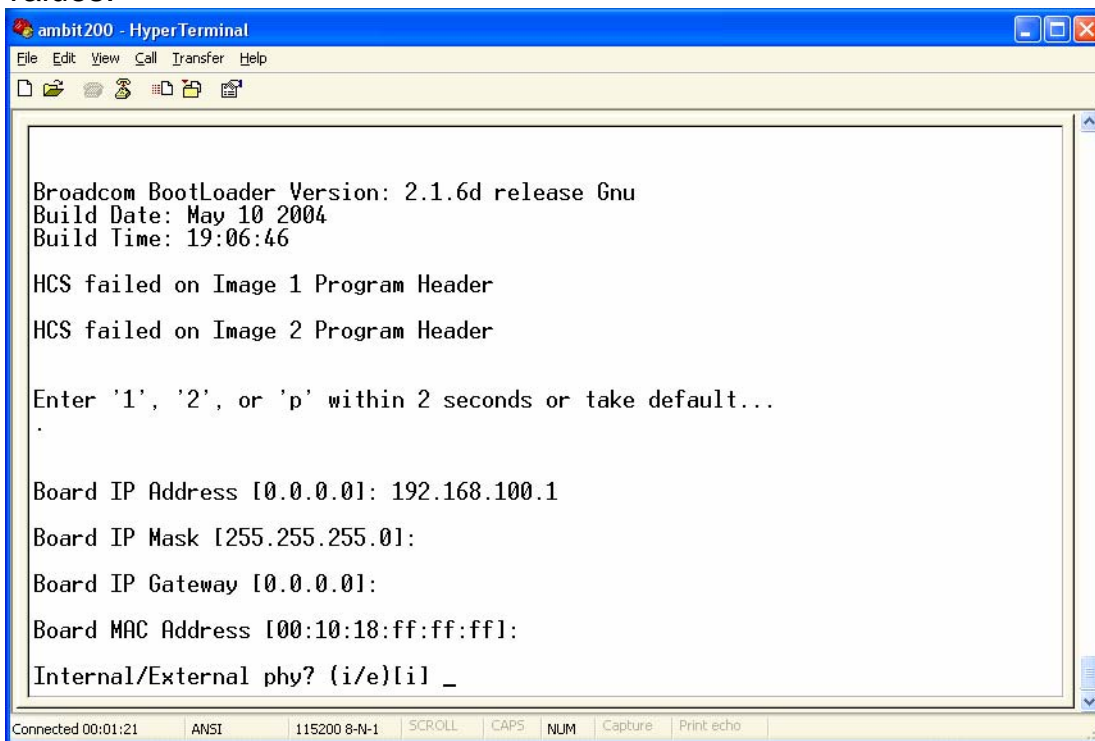
HCS failed on Image 1 Program Header
HCS failed on Image 2 Program Header

Enter '1', '2', or 'p' within 2 seconds or take default...
.

Board IP Address [0.0.0.0]: _
```

Connected 00:00:39 | ANSI | 115200 8-N-1 | SCROLL | CAPS | NUM | Capture | Print echo

Enter the **192.168.100.1** for the *Board IP Address*, just press return for the other values.



```
ambit200 - HyperTerminal
File Edit View Call Transfer Help
[Icons]

Broadcom BootLoader Version: 2.1.6d release Gnu
Build Date: May 10 2004
Build Time: 19:06:46

HCS failed on Image 1 Program Header
HCS failed on Image 2 Program Header

Enter '1', '2', or 'p' within 2 seconds or take default...
.

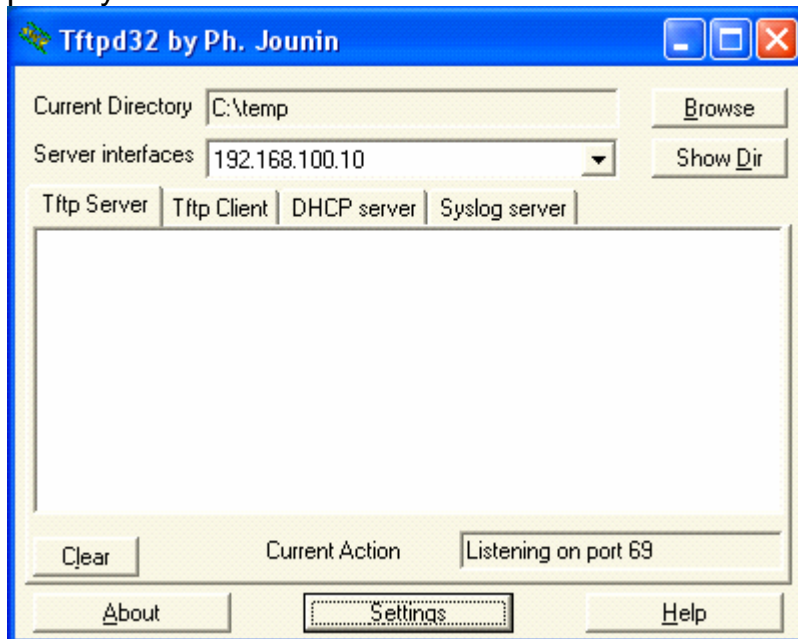
Board IP Address [0.0.0.0]: 192.168.100.1
Board IP Mask [255.255.255.0]:
Board IP Gateway [0.0.0.0]:
Board MAC Address [00:10:18:ff:ff:ff]:
Internal/External phy? (i/e)[i] _
```

Connected 00:01:21 | ANSI | 115200 8-N-1 | SCROLL | CAPS | NUM | Capture | Print echo

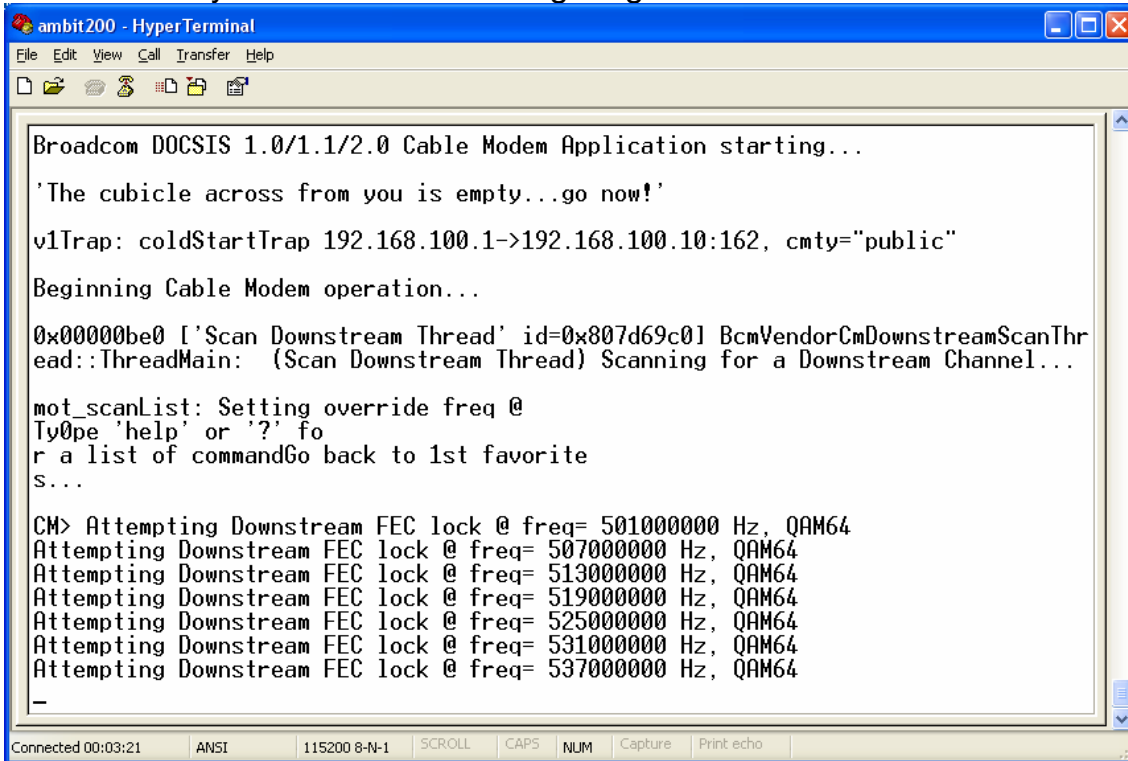
After entering this data you should be presented with the flash menu.

```
ambit200 - HyperTerminal
File Edit View Call Transfer Help
Board MAC Address [00:10:18:ff:ff:ff]:
Internal/External phy? (i/e)[i]
Init EMAC, DMA, and MII PHY...
Autonegotiation started, waiting for completion...Autonegotiation successful...
MAC setup for FullDuplex
Main Menu:
=====
d) Download and save to flash
g) Download and run from RAM
c) Store icePROM bootloader to flash
b) Boot from flash
e) Erase flash sector
m) Set mode
s) Store bootloader parameters to flash
i) Re-init ethernet
r) Read memory
w) Write memory
-
Connected 00:02:51 ANSI 115200 8-N-1 SCROLL CAPS NUM Capture Print echo
```

At this point, start the **tftpd32** program that came with this archive. Make sure that **192.168.100.10** is present in the **Server Interfaces** box. My example shows the **Current Directory** as **C:\temp** but of course this is only an example, don't take it literally. Make sure the **Current Directory** is set to the same place you extracted this archive. You have to click the **Settings** button to change this.



You will then be returned to the main menu. You may now reboot the modem. The new Sigma firmware should start to boot. Lots of data will flash past you on the terminal until you reach the scanning stage.



```
ambit200 - HyperTerminal
File Edit View Call Transfer Help
Broadcom DOCSIS 1.0/1.1/2.0 Cable Modem Application starting...
'The cubicle across from you is empty...go now!'
v1Trap: coldStartTrap 192.168.100.1->192.168.100.10:162, cmty="public"
Beginning Cable Modem operation...
0x00000be0 ['Scan Downstream Thread' id=0x807d69c0] BcmVendorCmDownstreamScanThre
ad::ThreadMain: (Scan Downstream Thread) Scanning for a Downstream Channel...
mot_scanList: Setting override freq @
Type 'help' or '?' fo
r a list of commandGo back to 1st favorite
s...
CM> Attempting Downstream FEC lock @ freq= 501000000 Hz, QAM64
Attempting Downstream FEC lock @ freq= 507000000 Hz, QAM64
Attempting Downstream FEC lock @ freq= 513000000 Hz, QAM64
Attempting Downstream FEC lock @ freq= 519000000 Hz, QAM64
Attempting Downstream FEC lock @ freq= 525000000 Hz, QAM64
Attempting Downstream FEC lock @ freq= 531000000 Hz, QAM64
Attempting Downstream FEC lock @ freq= 537000000 Hz, QAM64
-
```

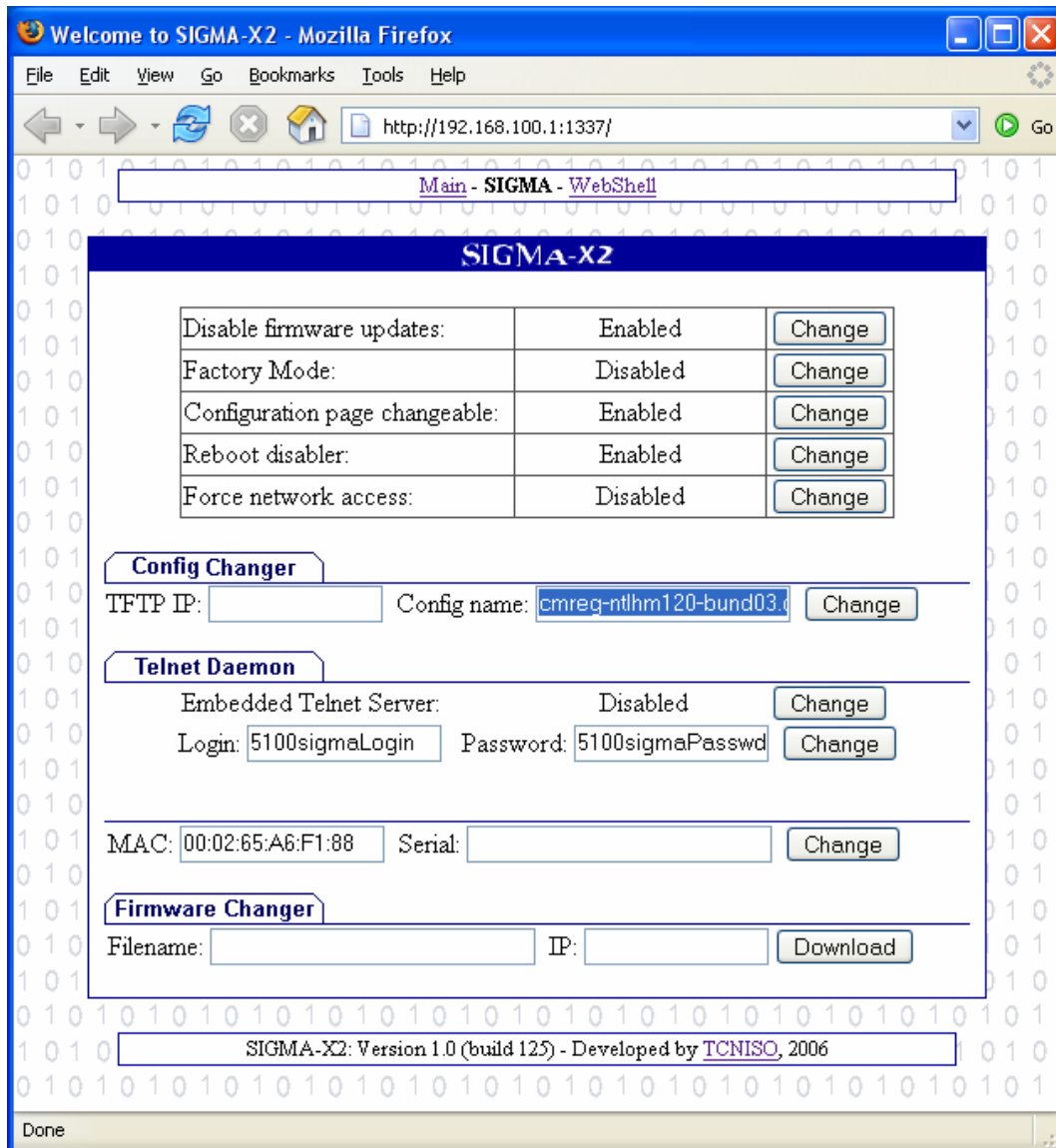
At this point you may now start to enter the settings for your area. Firstly however, you should stop the channel scan to make it easier to see what you are doing. To do this type in the following commands

```
cd /cm_hal  
scan_stop
```

The channel scan should then stop. Now, enter your settings.

```
cd /non-vol/halif  
mac_address 1 aa:bb:cc:dd:ee:ff (change this to a valid mac)  
cm_tuner 14  
annex_a  
cm_annex 3 (pure NTL areas ONLY should enter this)  
cd ../docsis  
ds_frequency 402750000 (change this your area's DS frequency)
```

If you want to force the 10Mbit configuration file (*which you probably do*) then enter the web configuration page (<http://192.168.100.1:1337/>) and enter **cmreg-ntlhm120-bund03.cm** into the *Config name:* box and click the change box next to it.



You can enable telnet using this interface too, as well as change the MAC address or change the firmware. If you enable telnet, make sure you change the username and password.

Now commit these changes to flash by entering the single command:

write

That's it! Reboot the modem and you should be all up and running.

Have fun,
Bolt...

PS. If the modem ever stops working, you can clear it by entering these commands.

```
cd /event  
flush  
cd /non  
write
```


6g. Restoring a Compatible Bootloader.

If you have Sigma on your Ambit200, you no longer have a working flash menu at bootup (Where you press 'p' when the modem starts up). This will allow you to restore a working bootloader so you can flash another image onto the modem.

You must have both these installed for everything to work:

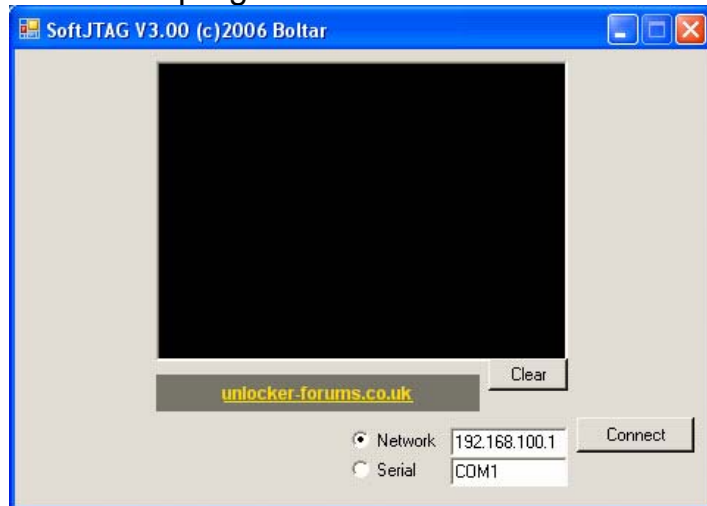
.NET Framework 2.0

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en>

Visual J# Redistributable Package

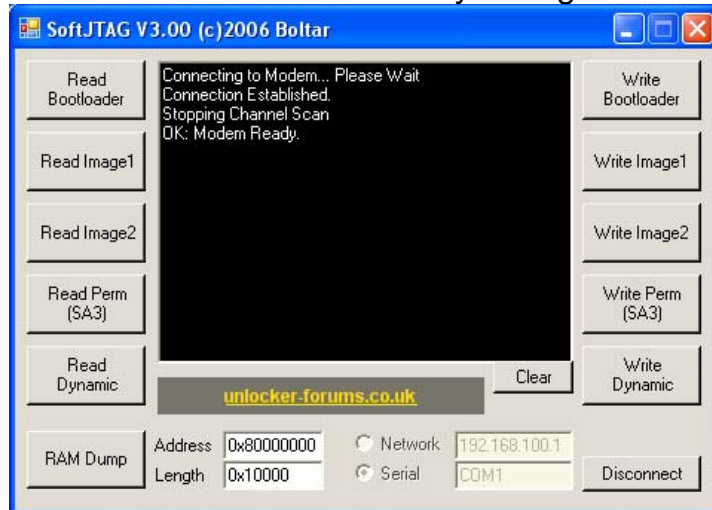
<http://www.microsoft.com/downloads/details.aspx?familyid=F72C74B3-ED0E-4AF8-AE63-2F0E42501BE1&displaylang=en>

Firstly, connect your modem to your PC with a MAX232/3 interface and boot up the modem without the cable feed attached. Wait about 10 seconds then start the **SoftJTAG** program in this archive. This window will appear.



Select **Serial** (*change the COM port value if you are not using COM1*)
Click **Connect**.

The window should eventually change to this:

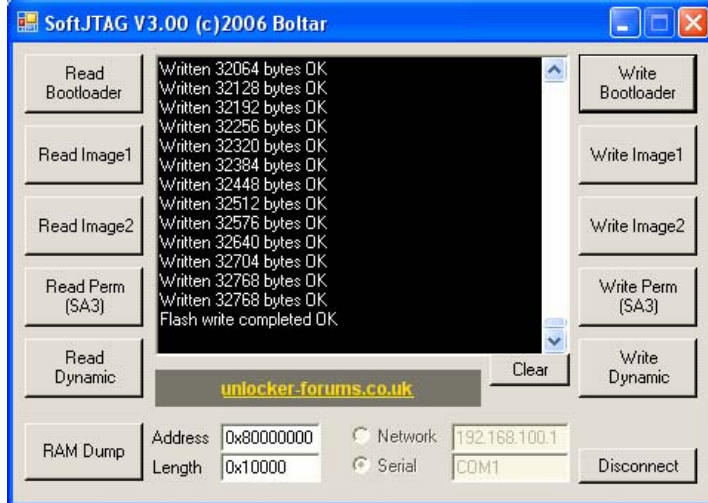


Now click on **Write Bootloader** and browse to the *bootloader.bin* file included with this archive.

It should then begin to write the file to the modem's flash memory.

It does take rather a long time, so go do something else for a while.

Eventually it will finish and should look like this.



That's it! Reboot the modem and you should now have the familiar flash menu equipped bootloader restored onto the modem.

6h. Ambit 120 Tutorial

All screenshots and text were compiled by Granty & Mark370 of Unlocker Forums



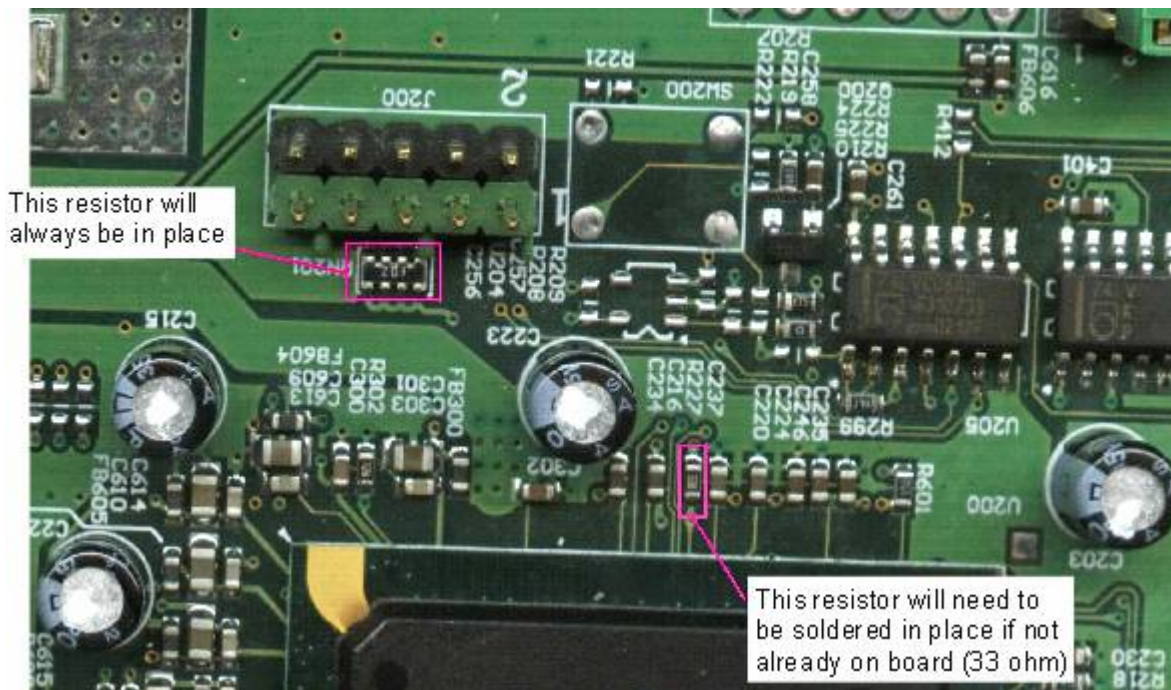
Files needed

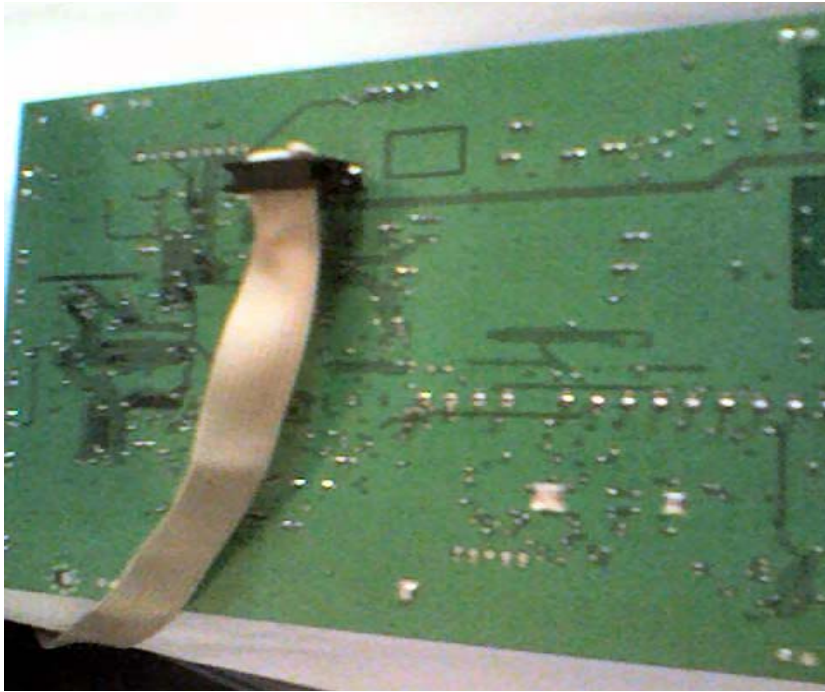
- 1) ntlhm120_ntl0001.cpr;
- 2) Infinite_Bootloader;
- 3) IMH-A120-2.40.3212-SHELLED.bin
- 4) Tftp.exe

Cables used

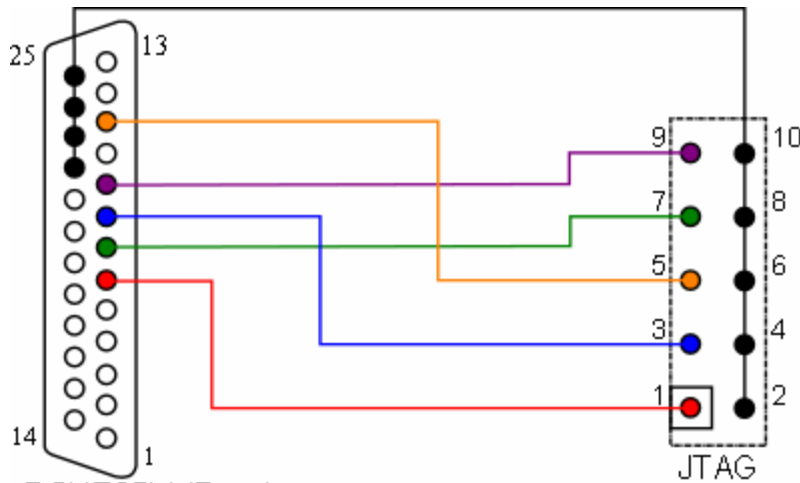
- 1) Non IC Blackcat cable;
- 2) Rs232 Cable;
- 3) Blackcat Software;

First off solder a 10pin header onto the **rear** of the 120ambit, also make sure that these resistors are attached onto the modem you are flashing R227.



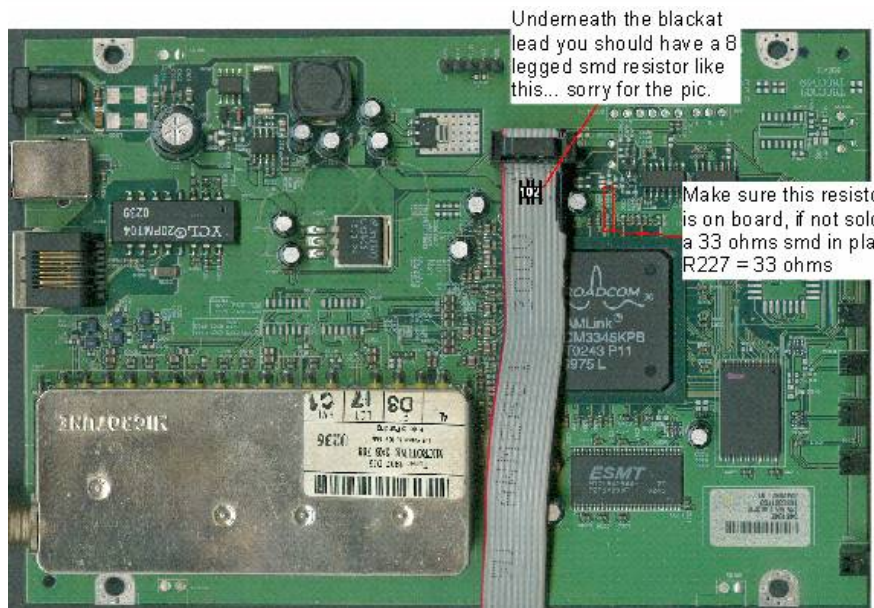


If the non IC Blackcat cable is set up for a Motorola modem, you'll need to install the pin header, to the underneath of the board like this. However, you'll need to desolder, the pin header to put the modem back in its casing.



DSUB25M (Rear)
Male Parallel Port Connector

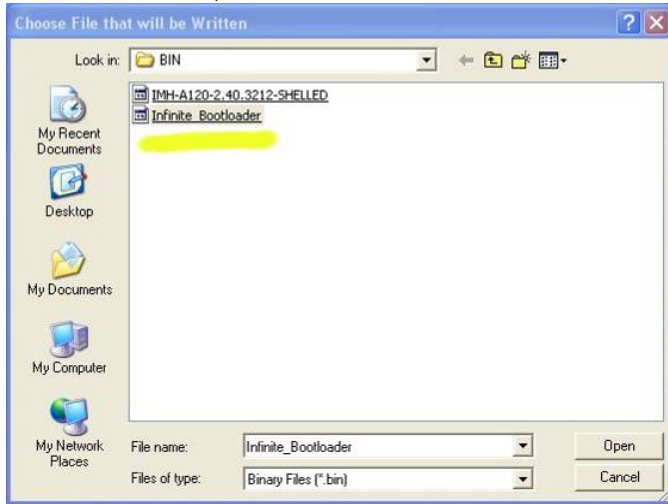
If you would prefer to have the pin header permanently soldered to the top of the Board you'll need to invert your Blackcat like so.



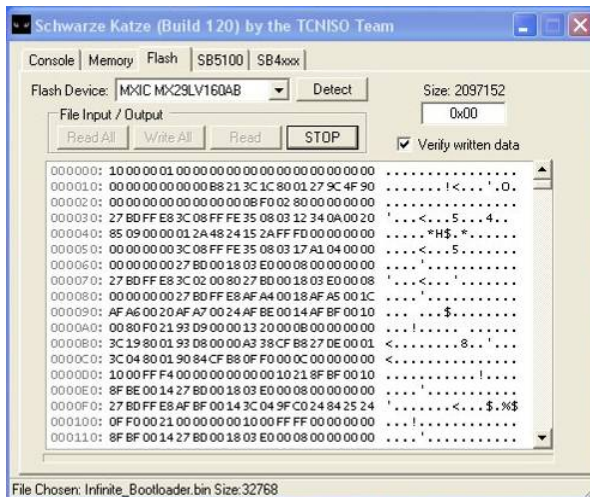
Connect your inverted Blackcat to the top of the board, like this.

Then connect Blackcat cable and run software.

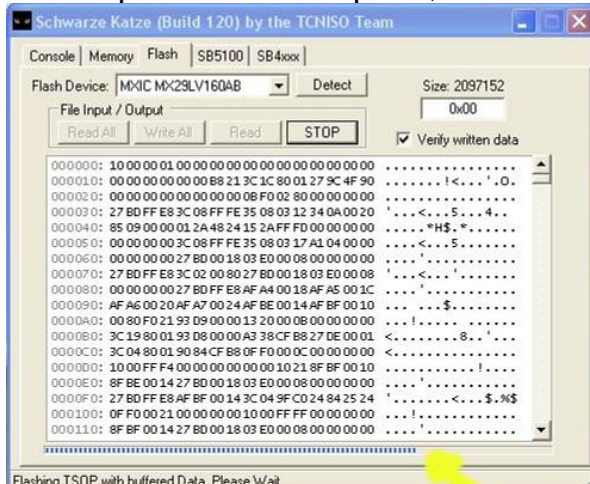
- 1) Go to the flash tab and click detect
- 2) Click on write, Search for the bin folder and select: Infinite_Bootloader



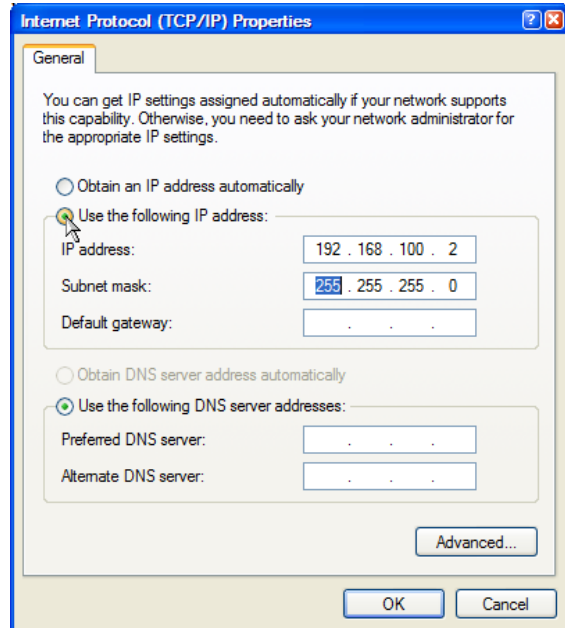
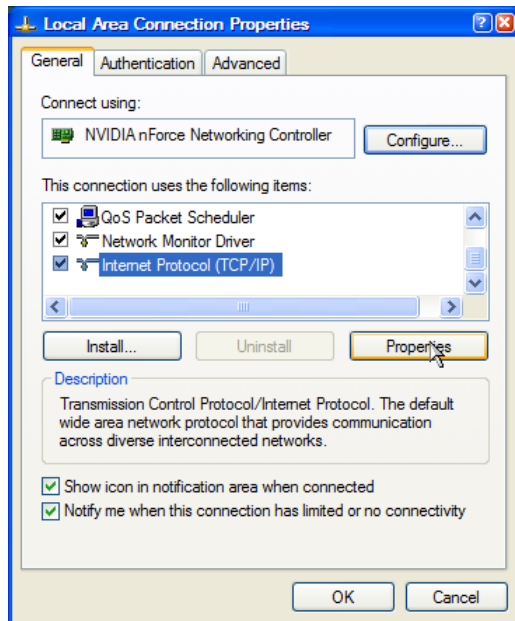
- 3) Click Ok and let this load



- 4) Once operation is complete, close the Blackcat software & disconnect the cable



- 5) Go to area network connections and click on “Internet Protocol (TCP/IP)”, and select properties.



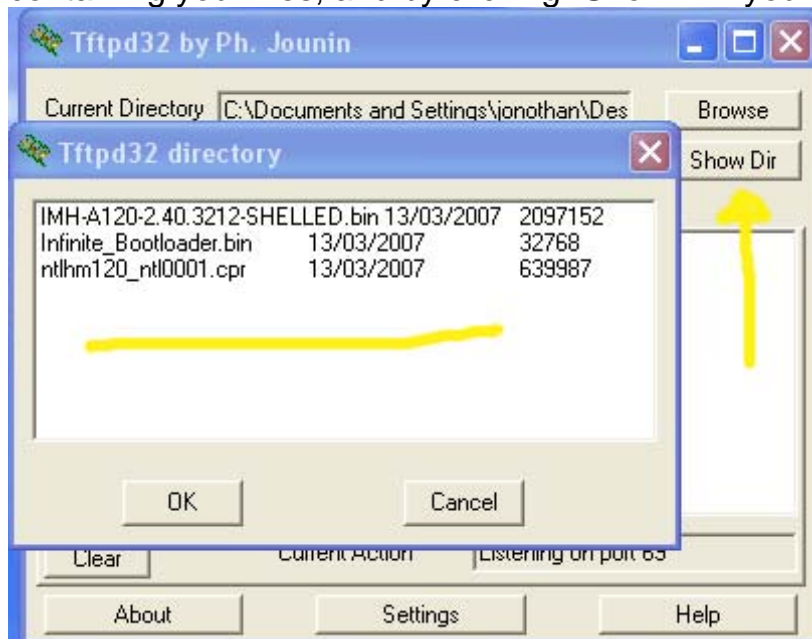
- 6) Select the “Use the following ip address:”
IP address: 192.168.100.2
Subnet mask: 255.255.255.0
Default gateway: Leave Blank

Leave the rest as it is and click ok

- 7) In the connection properties window, select the advanced tab and untick the box “Protect my computer internet connection firewall”, click ok then close this down. (**Note:** in the latest windows XP, this might not be possible, so you will need to disable the entire windows firewall temporarily – just enable it again later)

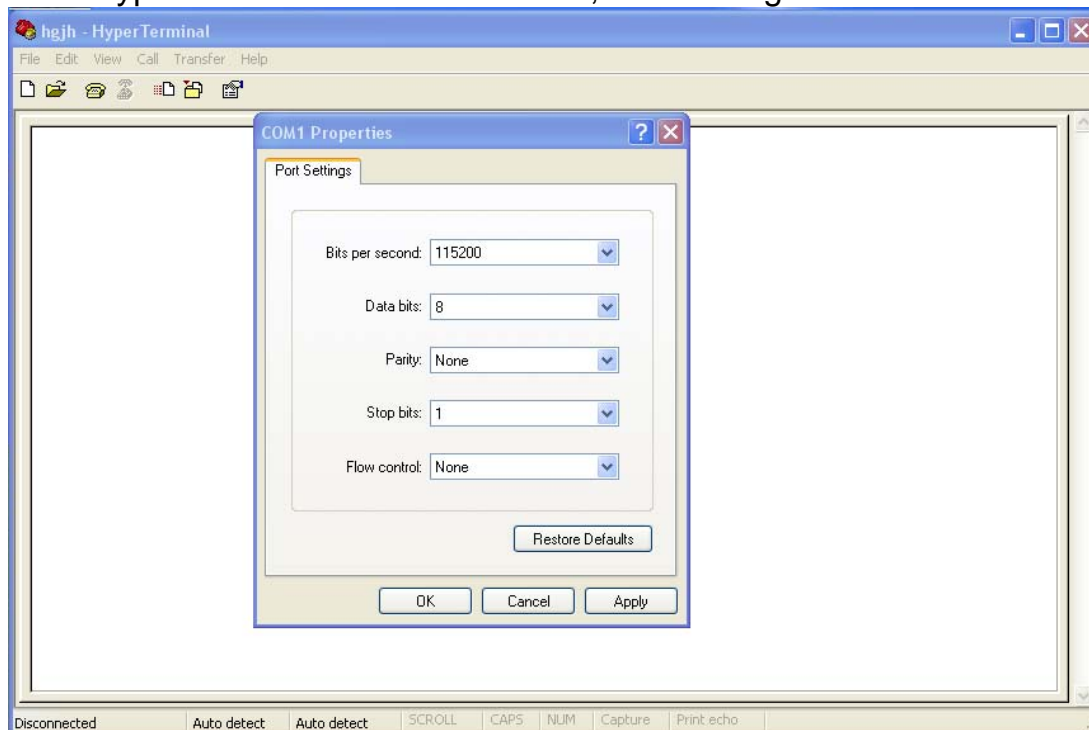


- 8) Start Tftpd32, and making sure that the current directory is showing the folder containing your files, and by clicking “Show Dir” you can make they are there.



The server should read: 192.168.100.2

- 9) Start HyperTerminal and select com 1, with settings as below:



- 10) Once connected press **1**, **2**, or **P** within 2 seconds

- 15) Once done, reboot modem and press any key within 2 seconds, then select choice 6.

```
x2 - HyperTerminal
File Edit View Call Transfer Help
To change any of this, press any key within 2 seconds
1) set Image1 Primary
2) set Image2 Primary
3) Download Image1
4) Download Image2
5) Download BootCode
6) Parameters Setup
99) Exit
Choice : 6
This board's LAN IP address? [192.168.100.1]:
Subnet mask for LAN? [255.255.255.0]:
Do you want to change the board's Ethernet address? [N] y
What should byte 0 be? [00]: 00
What should byte 1 be? [00]: 02
What should byte 2 be? [59]: 8A
What should byte 3 be? [F2]: 16
What should byte 4 be? [6C]: 3F
What should byte 5 be? [AC]: E6
Do you want to change the board's USB Interface address? [N] N
IP address of the TFTP Boot server to boot from? [0.0.0.0]: 62.254.64.23
What is the name of the file to be loaded and started? [ram.bin]: ntlhm120_ntl100
Connected 00:09:57 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print echo
```

- 16) Now respond as shown in the picture above and text below:

This board's LAN IP address? [192.168.100.1]: **Press Enter**
Subnet mask for LAN? [255.255.255.0]: **Press Enter**
Do you want to change the board's Ethernet address? [N] **y**

- 17) Next you need to enter your Mac address in stages. To do this you need to press **Enter** after each **2 digits**.

- 18) Now it will prompt you to if you want to change the USB interface address, if you want to do this, you can (in this case just type **y**, and enter the MACas you did the Ethernet one) but most people, you won't need to do this so just press **Enter**

- 19) You now need to enter your TFTP server address, type this and press **Enter**

- 20) Now enter the following as it asks you:

What is the name of the file to be loaded and started? **ntlhm120_ntl0001.cpr**
Type: **99** & press **Enter**
Type: **2** & press **Enter**

23) Once this is done unplug modem and connect feed cable, HyperTerminal will still be running on connection of modem. Go into a web browser and goto:

http://192.168.100.1/P_engineer.htm

Username: root

Password: root

24) In the boxes displayed you will see the TFTP you entered and the file name:

ntlhm120_ntl0001.cpr

Leave the modem 5 minutes then undo the changes made in steps 5, 6 and 7 by changing your "Internet Protocol TCP/IP" settings back to:

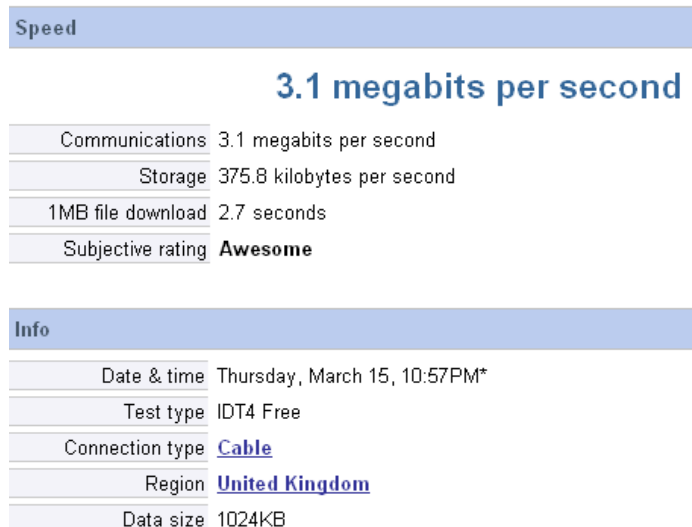
"Obtain an IP address automatically" and

"Obtain a DNS server address automatically"

25) Reboot the PC and modem together. Give the modem a further 10 minutes and you will have internet access.

The Mac I used was a 120 mid, below is a speed test taken from:

<http://www.bandwidthplace.com/speedtest/>



7. Ambit 250 - Guide to Hacking v2

The following text was put together by

[Astra](#)



NOTE: This was only tested on NTL ex-C&W. Other providers will need to amend the config file & frequency as required.

7a. Updating Ambit 250 to hacked firmware

To flash the firmware onto the Ambit250 you must use a MAX232/233 interface.

Connect this up as per-normal.

Connect up the cable feed to the modem, and the Ethernet cable to the PC LAN card.

Make a new folder on your PC.

Copy "**250hack_dump_telnet.bin**" into it.

Copy "**tftpd32.exe**" onto it (this was posted along with the ambit200-sigma hack)

In Windows Networking set the network adaptor connected to the modem to a manual configuration with these details:

IP address: **192.168.100.10**

Subnet Mask: **255.255.255.0**

Gateway: **192.168.100.1**

DNS: <**don't enter anything**>

Start **tftpd32.exe**

Now start HyperTerminal and connect to the COM port of the PC using these settings:

Bits per second: **115200**

Data bits: **8**

Parity: **None**

Stop bits: **1**

Flow control: **None**

Power the modem up.

Enter '1', '2', or 'p' within 2 seconds or take default...

Choose option P (press this quickly as if you miss it, it will continue booting)

Next enter: **192.168.100.1** as the "Board IP Address" and just press enter for the rest:

Board IP Address [0.0.0.0]: **192.168.100.1**

Board IP Mask [255.255.255.0]:

Board IP Gateway [0.0.0.0]:

Next when asked "Do you wish to store it?", type: **Y**, & "sector to start store": **0** (zero)

```
Image does not have standard header. Do you wish to store it? [n] Y
Programming 2097152 bytes
Enter sector to start store: 0

Store parameters to flash ? [n]
```

The modem will now write the new firmware to flash.
Now you should get the main menu again.

The modem is now flashed and you can close this copy of HyperTerminal and disconnect your MAX232/233.

Set the LAN card back to dynamic IP and Gateway and reboot the modem.

Give it a minute to power up.

Now start a new copy of HyperTerminal, this time we select:

Port: **TCP/IP (Winsock)**
Host address: **192.168.100.1**
Leave the port number as 23

```
Broadcom Corporation Embedded Telnet Server (c) 2000-2003
WARNING: Access allowed by authorized users only.
```

Press enter and enter the following login and password:

```
login: admin
password: infinite
```

```
WARNING: It is possible to crash the system, cause a deadlock,
or cause the connection to be shut down via Telnet.
```

```
Run commands with caution!
```

```
Console now switched to Telnet session...
```

```
Scanning DS Channel at 240000000 Hz...
```

```
Scanning DS Channel at 249000000 Hz...
```

```
...
```

We are now back in the console using telnet.

It should be scanning for a frequency to lock onto. We want to stop this so enter:

```
cd \cm_hal
scan_stop
cd \
```

Now open Internet Explorer and browse to the following page: <http://192.168.100.1>

Login: **Infinite**

Password: **SetValue**

NOTE: Case Sensitive!!! Capital I,S and V

NOTE: FireFox does not load the pages - you must use Internet Explorer

Click on SECURITY

Type in your DS frequency and click, apply.

Switch back to the HyperTerminal window.

```
cd \non
write
cd \
```

We now need to change the MAC address. We do this by writing the new Ethernet MAC into RAM first.

Assuming our MAC address is AA:BB:CC:DD:EE:FF, enter:

```
write_memory -s 4 0x807e8b98 0xAABBCCDD
write_memory -s 2 0x807e8b9c 0xEEFF
```

Next we must force the modem to commit this to flash, so enter:

```
cd \non
write
cd \
```

Now to configure the other settings required to get online.

Code:

```
cd \non
cd hal
cm_tuner 19
write
annex_a
write
usb_mac_address <your usb mac address here>
write
```

NOTE: for the USB MAC, include the ":" i.e.: 11:22:33:44:55:66

the USB MAC is determined by adding one to the last digit i.e.: 11:22:33:44:55:67

Power off the modem for a few seconds and then back on again.
Give it a minute to connect and obtain an IP address.
You should now be able to access the web.

7b. Force modem to use the 10mb config file

Reconnect to the modem via telnet using HyperTerminal (as you did before.)

Type in:

```
cd \non
cd doc
dhcp_settings
My IP Address: [192.168.100.1]
Subnet Mask: [255.255.255.0]
Router IP Address: [192.168.100.254]
```

Those are the only 3 that really need to be changed.

Do you want to change the other settings? [no] **Y**

TFTP Server IP Address: [10.10.10.254] **type in the IP of your TFTP server here**

Config file name: [cm.bin] **cmreg-ntlhm120-bund03.cm**

Time Server IP Address: [10.10.10.254]

SysLog Server IP Address: [10.10.10.254]

Now type in the following lines:

```
enable force_cfgfile true
write
```

Now reboot the modem.

You should still be able to connect to the web. You can check which config file you are running by accessing: <http://192.168.100.1> and look in the Connection page.

Now it is important to change the modems telnet username & password to prevent unauthorized access.

Reconnect to the modem via telnet using HyperTerminal (as you did before).

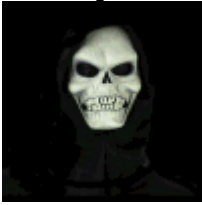
Type in:

```
cd \non
cd msg
user_name <your desired username here>
password <your desired password here>
write
```

The settings will not be changed until you reboot your modem.

7c. Finding your TFTP IP

All screenshots and text were compiled by
Granty



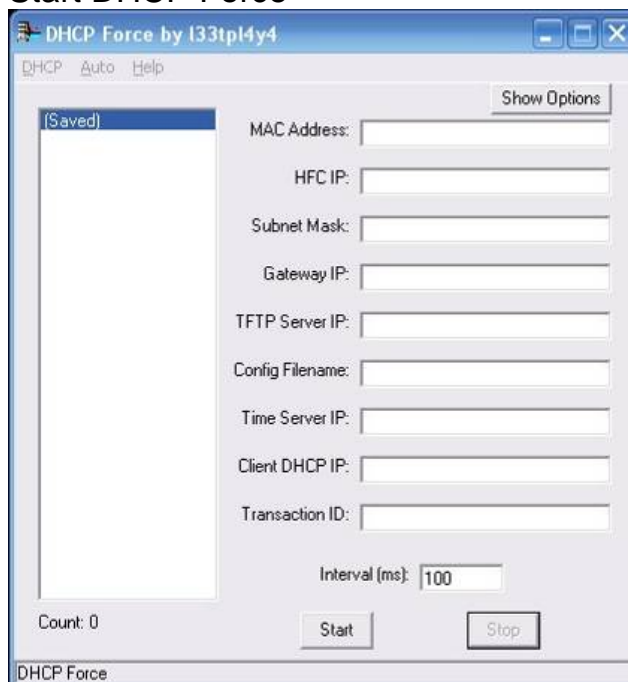
Here we have an example of the 250 asking for your TFTP address.

```
cd \non
cd doc
dhcp_settings
My IP Address: [192.168.100.1]
Subnet Mask: [255.255.255.0]
Router IP Address: [192.168.100.254]

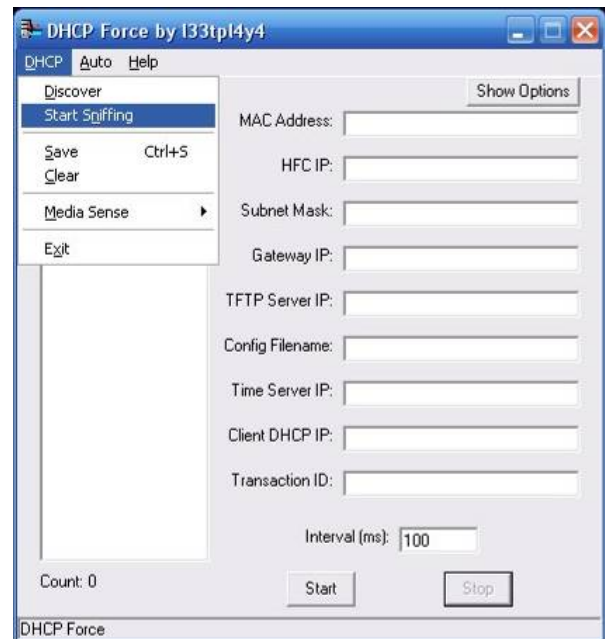
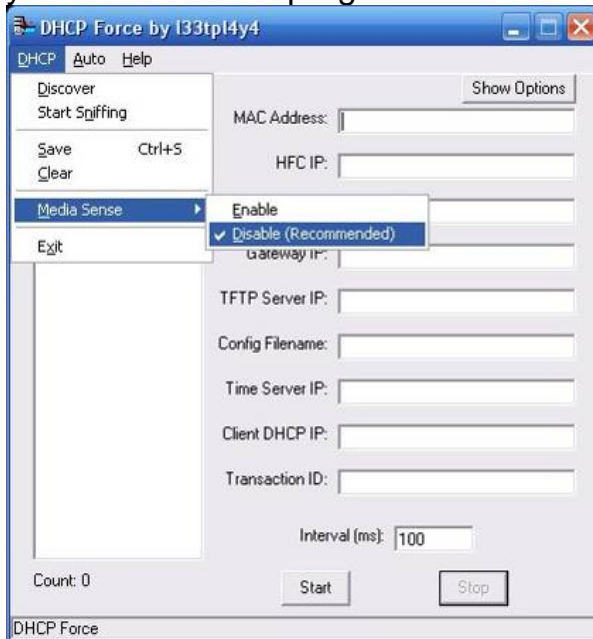
Those are the only 3 that really need to be changed.
Do you want to change the other settings? [no] Y
TFTP Server IP Address: [10.10.10.254] type in the IP of your TFTP
server here
Config file name: [cm.bin] cmreg-ntlhm120-bund03.cm
Time Server IP Address: [10.10.10.254]
SysLog Server IP Address: [10.10.10.254]
```

Now to get the TFTP address you need to do the following:

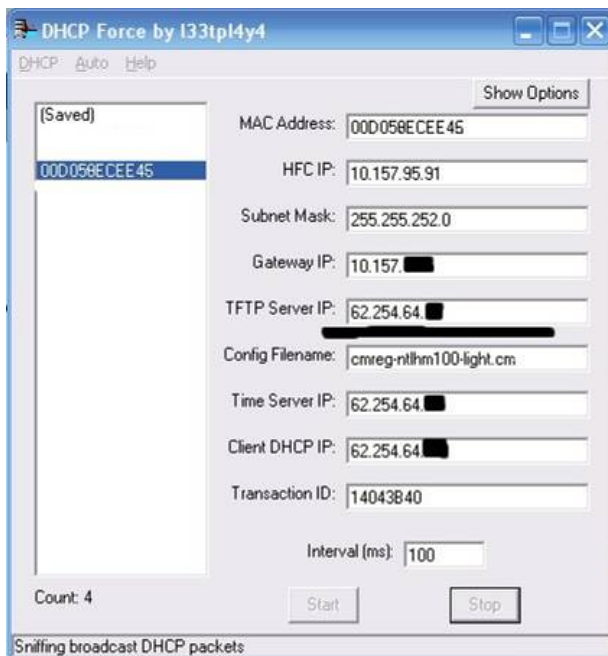
1) Start DHCP Force



- 2) Click on DHCP and scroll down to media sense, select disable, and it will ask you to re-start the program



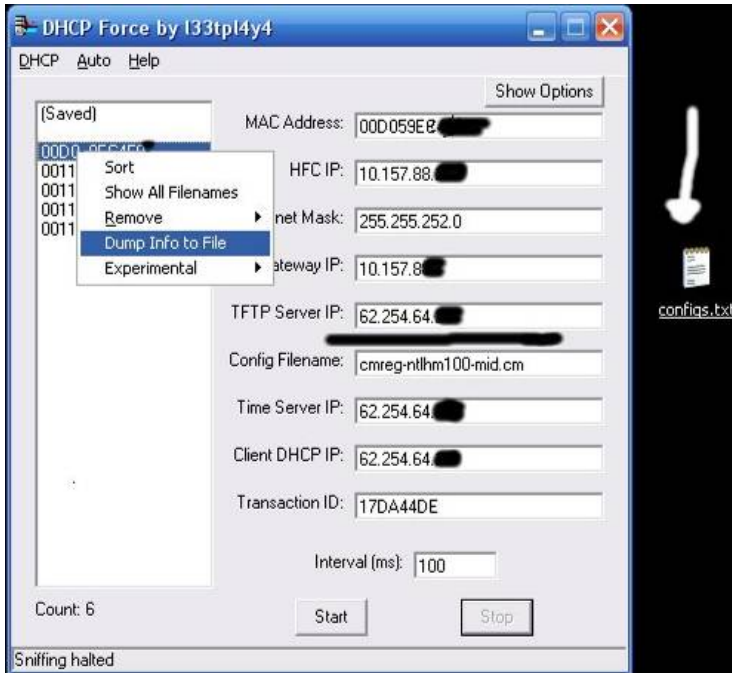
- 3) Go back and select start sniffing. DHCP will start sniffing for Macs, when you have a list of Macs available in the left column, click on each Mac address, until you see your TFTP server IP



This is all you need, copy and paste this into the HyperTerminal for the use in modification of the 250...as in first image.

NOTE: I have blacked out the areas for my safety but yours will show the full TFTP server IP, for the same reason this Mac has also been altered.

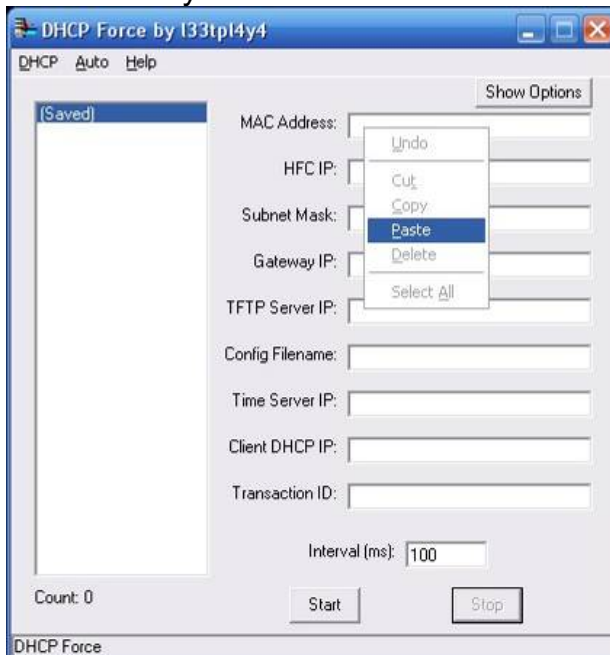
If you would like to share the Macs you have found you can save a list without the need of endless typing, just right click on a MAC, and select “Dump Info to File”. You will then end up with a file named config.txt
ALL the MAC’s will be saved to this file, not just the one you selected



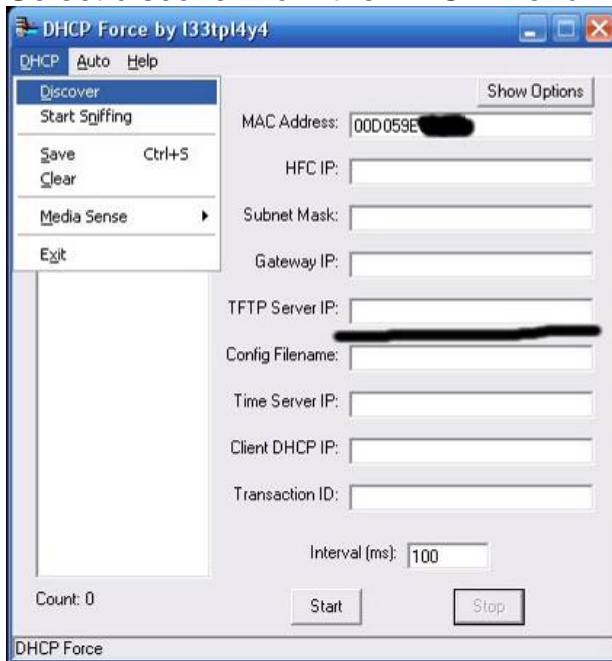
Method 2

There is a fast and simple way of obtain your TFTP IP:

- A) Start DHCP
- B) Where it says Mac address insert the Mac you are using at the moment:



C) Select discover from the DHCP Menu:



D) Now just wait, after a while you will obtain your TFTP Server IP

NOTE: I have tried this method but it has never worked for me, this is why I have listed 2 methods.

7d. 250 configurator guide

All screenshots and text were compiled by
Mark370 of Unlockers



Once your Ambit250 has had the firmware flashed successfully its time for you to input your area settings this is made easy with Boltars 250configurator App.

The 250 configurator requires the following 2 Microsoft application's to run correctly:

1. **Microsoft .NET Framework Version 2.0 Redistributable Package (x86)**
<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en>
2. **Microsoft Visual J# Version 2.0 Redistributable Package**
<http://www.microsoft.com/downloads/details.aspx?familyid=F72C74B3-ED0E-4AF8-AE63-2F0E42501BE1&displaylang=en>

Connection

You can either use a max232/233 cable through your COM Port or Ethernet cable through Telnet.

list of the details about your area that you will need:

1. A Valid Mac Address
2. Tuner Type
3. Annex Mode
4. Downstream Frequency
5. Config File
6. TFTP Server IP
7. Admin Status (always 3)
8. Max DL Tries (always 4)
9. Force Cfg (ticked)
10. Telnet (Enabled) - well that's up to you

Some area settings

NTL:

cm_tuner: 19
cm_annex_3: For pure sometimes only if annex_b don't work
ds_frequency: 402750000
Config file: cmreg-ntlhm120-bund03.cm [10/20megs]

CW:

annex_a
cm_tuner: 19
ds_frequency: 586750000

TW:

cm_tuner: 19
annex_b
ds_frequency: 331000000
Config file: cm-20480-768 [20megs]

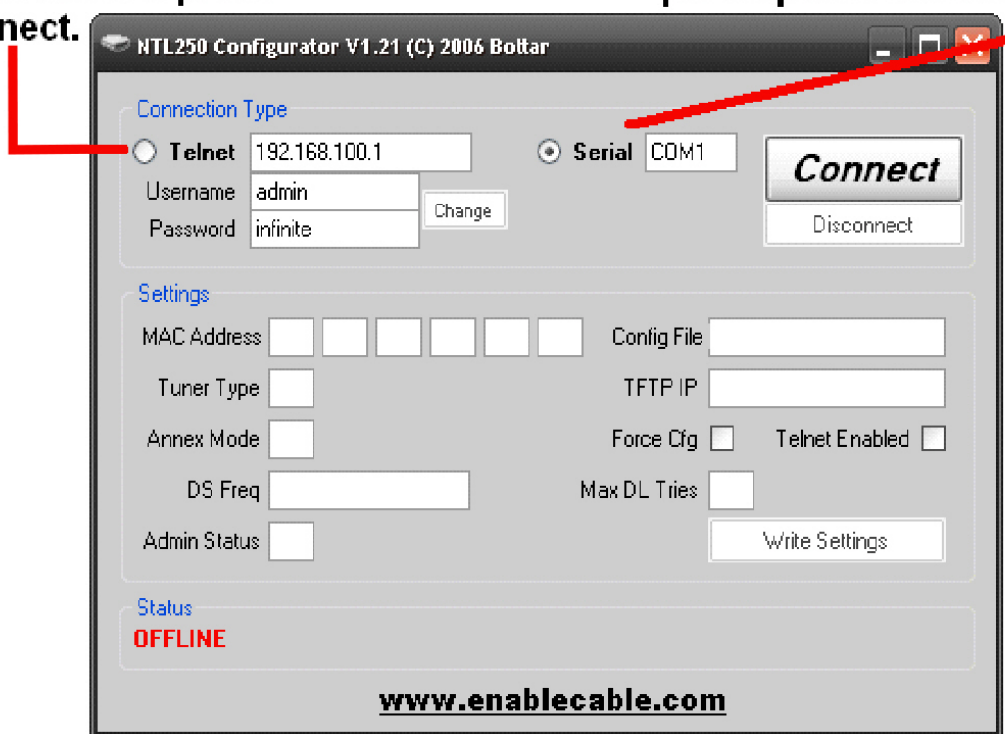
Getting Started

Now you have your area details, MAC and your TFTP Server IP lets get started.

1. Connect all cables up and power up modem
2. Click either Telnet or select serial & Comport

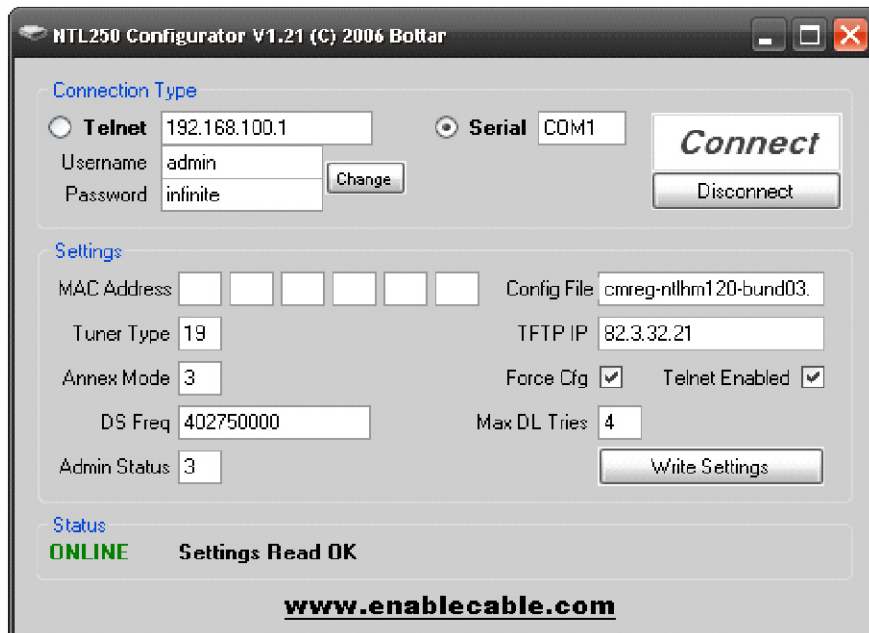
**If your using ethernet cable
select telnet & press
Connect.**

**If your using max232/233
cable select serial & com
port & press Connect.**



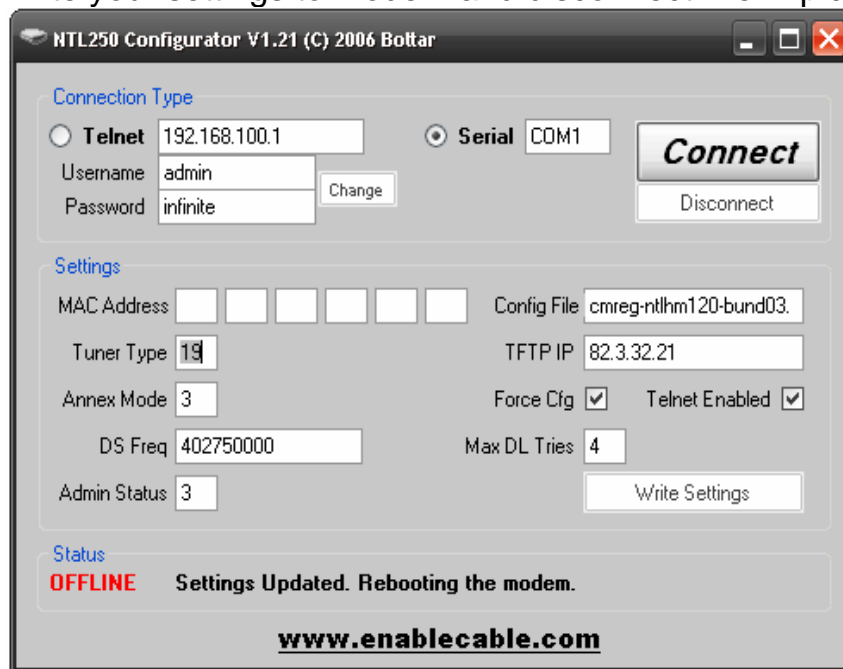
3. Now click Connect and once connected enter all of your area settings so it looks like this:

NOTE: These settings are for NTL-PURE, change as appropriate, and make sure to fill in all boxes with details for your area, i.e for NTL-Pure, ex-C&W / TW



NOTE: MAC address has been removed for security reasons

- Once all boxes are filled in and ticked, press: **Write Settings**, now the app will write your settings to modem and disconnect like in picture below:



- That's it, reboot modem

Troubleshooting

If you find your modem won't come online and your area has upgraded to 20megs don't for get you'll have to input the bpi CMDs in Telnet. To do this, follow the instructions below:

1. First stop channel scan with this command:

```
cd \cm_hal
scan_stop
cd \ (press enter)
```

2. Now enter the bpi cmd

```
cd non-vol
cd docsis
enable bpi false
write
```

3. Reboot modem

If all has gone well you'll get these results on your modems internal web page [http://192.168.100.1/]

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	402750000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	cmreg-ntlhm120-bund03.cm
Security	Disabled	Disabled

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	402750000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	cmreg-ntlhm120-bund03.cm
Security	Disabled	Disabled

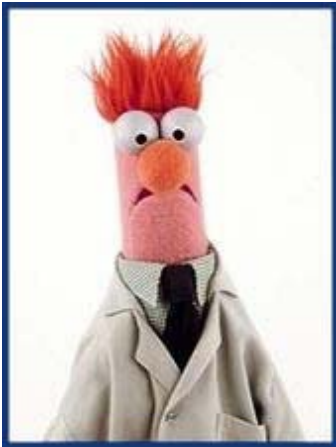
Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	402750000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	cmreg-ntlhm120-bund03.cm
Security	Disabled	Disabled

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	3349
Software Version	5.01.01.000_004(III)
Cable Modem MAC Address	
Cable Modem USB MAC Address	
Cable Modem Serial Number	
CM certificate	Installed

Status	
System Up Time	0 days 00h:02m:08s
Network Access	Allowed
Cable Modem IP Address	

8. Motorola SB3100

I've never done a SB3100 myself but I found this posted on www.world-of-digital.com
The following screen shots and text were put together by [Cashmere](#)



- 1) Manually assign a 192.168.100.10 ip to the network card you want to use:

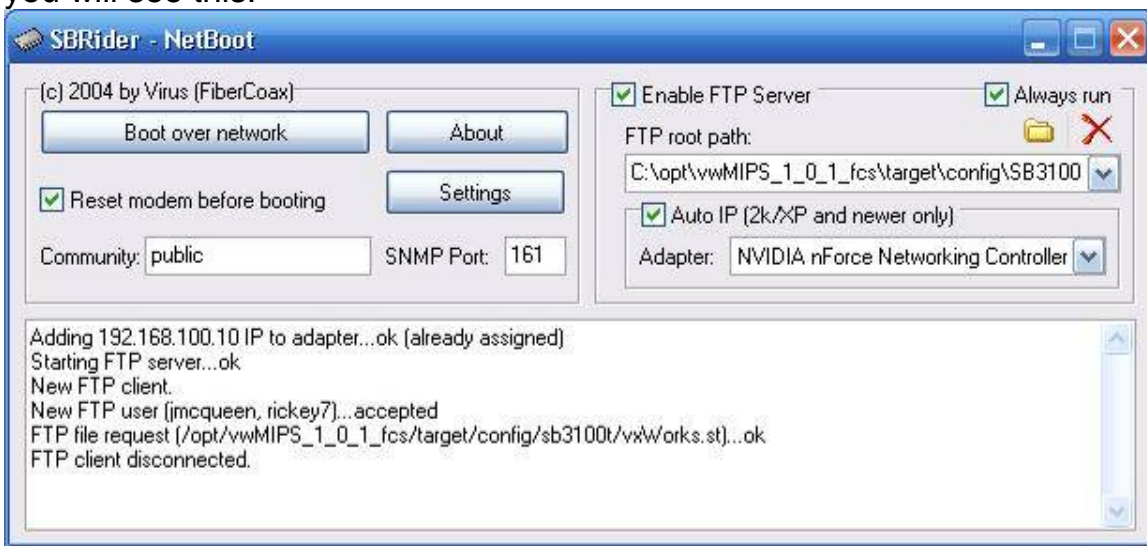


- 2) Connect your sb3100 using just the Ethernet cable and power.
- 3) Extract the files supplied in the kit to your desktop
- 4) Cut and paste the opt folder to your root drive which in my case was C:/
- 5) Run Netboot. This is now the important part so pay attention. Boot over Network will not work in our case (SB3100) so don't try.

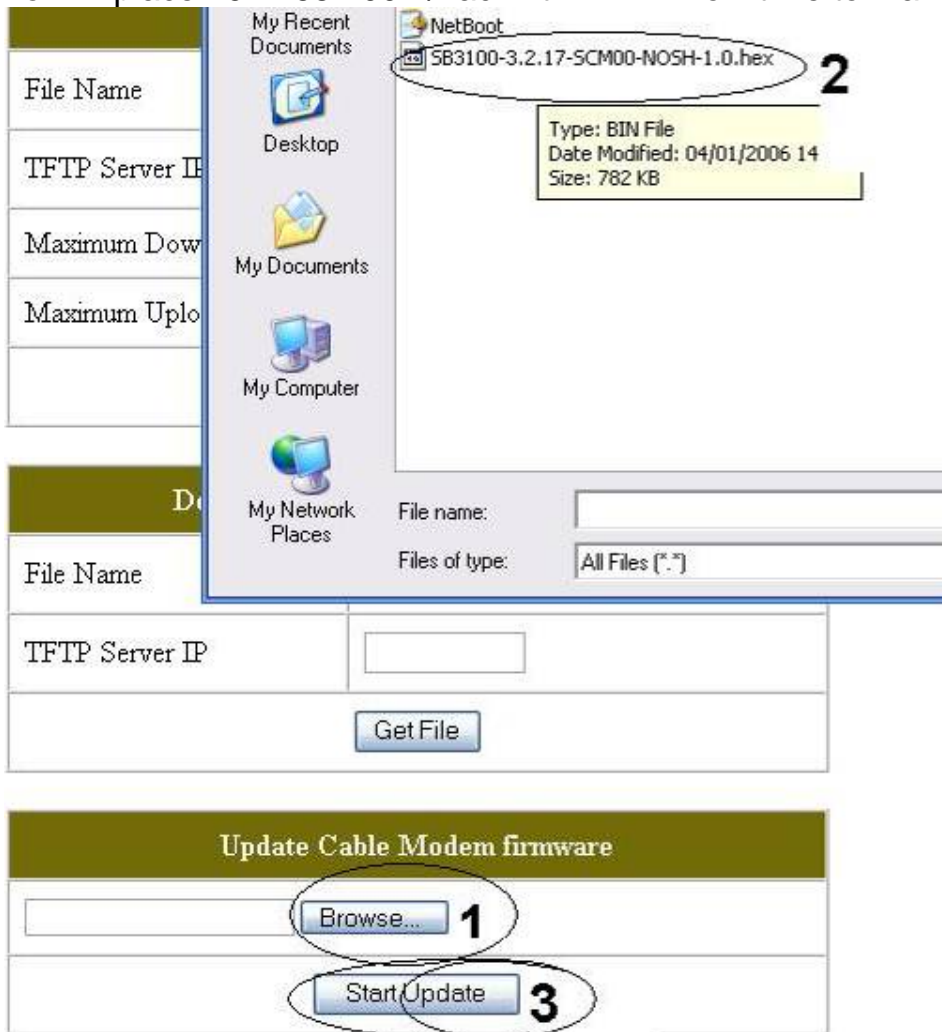
- 6) All we need checked r Enable ftp server...always run and auto IP also check our path to the vxworks is showing:



- 7) If all is well we should see this picture if you do then proceed to next step /if not get it sorted.
- 8) Now the magic bit. a pin or a cocktail stick will do...on the back of the SB3100 u will see a small hole(just below ethernet plug) this is a reset button....what we need to do here is trick the modem a little.
- 9) This parts all about timing and it may take a few trys. My method was to use the old 123 delay and it works for me.
- 10) So here we go. With your netboot running and SB3100 connected...press,123,press,press and then wait a sec, if you got the timing right you will see this:



11) You may now close netboot as we don't need it anymore/Temporary firmware is now in place 192.168.100.1/hack.html..... now time to make it permanent



12) Follow the 3 steps here and wait for at least 5 mins and let it do its thing, during this time the modem will reset and your new firmware will be permanent.

9. Motorola SB4100 & SB4200

I don't know who put this tutorial together but it was posted on www.world-of-digital.com by

666



9a. Change Firmware on Surfboard Modem - 1 PC Method

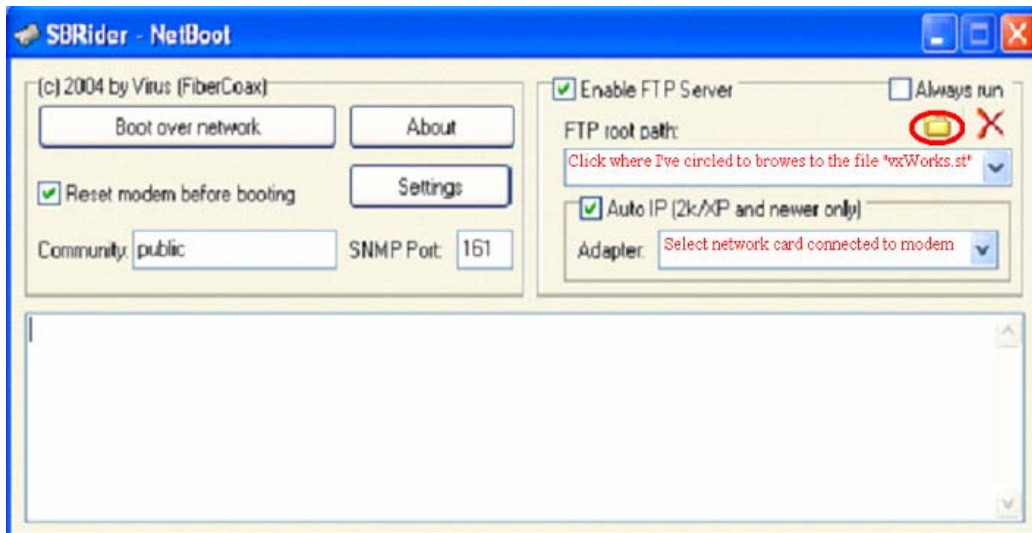
This guide is written in steps designed for printing. One step per page, (3 pages in all) – Also important reminders are in red, step headings are in blue. Good Luck.....

Required files:

- **NetBoot.exe**
- **NetBoot.ini**
- **vxWorks.st**
- **SB__00-0.4.4.5-SCM01-NOSH-___.hex.bin**
(the underscores represent different possible files, i.e. 4200, 4100, 2.03, etc. the one used here is: SB4200-0.4.4.5-SCM01-NOSH-2.03.hex.bin)



- 1) Load Netboot,
If you are using windows XP or windows 2000 tick the AUTO IP box as shown below.
- 2) If you are not using either version of windows then you **MUST** set the IP to 192.168.100.10 yourself. Usually this can be done by loading control panel, clicking on network and then open the network adaptor connected to the modem. Just scroll down the list until you find TCP/IP and click on properties and input a manual IP (subnet mask = 255.255.255.0)
- 3) Now set up like this:
Reset Modem before booting: **Ticked**
Community: **public**
SNMP Port: **161**
Enable FTP Server: **Ticked**
Always run: **NOT Ticked** (make sure you untick this)
Auto IP (2k/XP & newer only): **Ticked**
Adapter: **Select the network card connected to modem**
FTP root path: **Click on the yellow folder button circled in red below and select the "vxWorks.st" file**

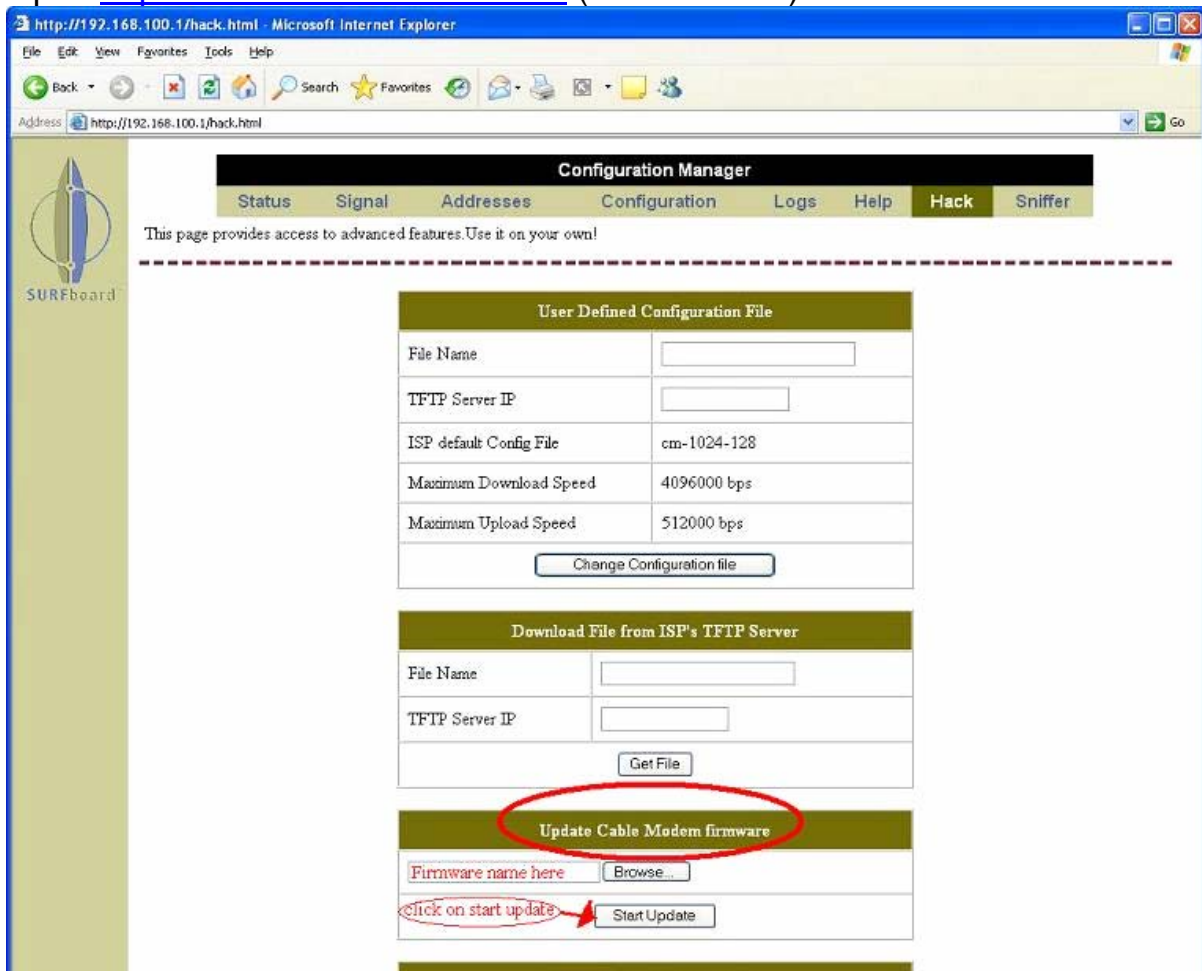


NOTE: Each model has own specific files so ensure you use the correct ones

NOTE: Remember to type the location to the file "vxWorks.st"

NOTE: Select the correct network interface if you have more than one, its the one that connects the computer to the modem.

- 4) When your ready click on boot over network, and wait for your modem to reboot.
- 5) Open <http://192.168.100.1/hack.html> (shown below)



- 6) Browse to your firmware and then click on start update.
- 7) Wait, it can take up to 5 minutes. Your modem will reboot if successful.

9b. Modems from America or Japan

For anybody who has a modem that comes from America or Japan, you will need to do the following:

- 1) Firstly flash your modem with Fibercoax V9F4
- 2) Reset to defaults and reboot your modem
- 3) Go to the internal web pages <http://192.168.100.1> & click on the configuration tab.
- 4) Click on the dropdown menu and select “European PAL I/B/G” & click save changes.

Your modem will permanently have this feature available no matter what firmware you decide to flash your modem with.

- 5) If you now decide you want to change the firmware you’ve got installed you’ll need to first enter <http://192.168.100.1/00-> into your web browser
This will allow your modem to take updates, (as Fibercoax disables updates by default).
- 6) Now just follow the tutorial again but in Netboot change your SNMP port to **225** and flash your new choice of firmware to the modem.

10. Hacked Firmware

Ok hacked firmware comes in three flavors Fibercoax, Hackware and Sigma. Personally I stay away from Sigma as I just don't like the developers TCNISO but there firmware is as good as the other two so basically it's up to you. I'm going to leave out Sigma for the SB4100 & SB4200 as we'll cover it later on with the SB5100. You'll be able to get any of the firmware you need from the following link

<http://members.ispwest.com/madcow007/cable/>

10a. Fibercoax

Fibercoax is relatively easy to use. You change the settings of the modem by using "flags", these are entered into your web browser on the modems html page. The following is taken from the read me file that comes with the Fibercoax firmware.

How To Use It

To be able to use this features, simply do this:

`http://192.168.100.1/ + flag`, whereas the flags are :

Flags

Flag /00-

Allows firmware Updates (by default all updates are disabled)

ex.:

- `http://192.168.100.1/00-`
- To restore defaults: reboot the cablemodem

Flag /01-

(Stealth mode)

ex.:

- `http://192.168.100.1/01-`
- To restore defaults: reboot the cablemodem

/04- set config name to NVRam

ex.:

- `blah.cm`
- To go back to ISP defaults: `http://192.168.100.1/04-`
(Check the config name that was set, on the fibercoax tab)

/05- boot from Stand alone kernel

ex.:

- `http://192.168.100.1/05-`

We left this feature for advanced users that wants to change Firmware's temporarily (an example would be going to DOCSIS 1.1 FW and back to 1.0) and also to prove that a serial cable isn't needed to do this. Rebooting will restore your FW from flash

/06- Sets SNMP port to defaults

/07- followed by UPPER case 6-byte hex will change HFC MAC address
(<http://192.168.100.1/07-0123456789AB> - stands for 01:23:45:67:89:AB)

/08- followed by 24 digits will change serial number
(<http://192.168.100.1/08-123456789012345678901234>)

/24- Set memory location to dump (uppercase alpha)
ex.:

- <http://192.168.100.1/24-80589680>
(Check the dump results on the Fibercoax tab)

FAQ

Q) When using the flag do I need to put the ' - ', ex.: /00- ?

A) Yes

Q) What is the stealth mode after all for?

A) It disables the HFC interface and releases the HFC IP, which is used by ISPs so to access your cable modem, via SNMP and others.

Q) Using flag /01- , will I loose network access (internet)?

A) No, you won't. It will make your cable modem stealthy against intrusions, from the HFC side.

Q) Where can I see the config name that I'm using at the mo?

A) Go to the fibercoax tab, and it will be on the top of the page

Q) Will I have to enter the config file name, each time I reboot?

A) No. the config file name that you have set previously, will be retained after booting.

Q) How do I boot from network?

A.) Setup a FTP server with IP 192.168.100.10, put a kernel in
"/opt/vwMIPS_1_0_1_fcs/target/config/sb4200/vxWorks.st" of FTP server, and
create a user with the following settings: username: jmcqueen ; password :
rickey7

Status Page

Originally MADE possible by FIBERCOAX TEAM

Here's a screenshot from the status page so you've got an idea of what it looks like:



The screenshot shows a Microsoft Internet Explorer browser window displaying the Configuration Manager Status page for FiberCoaxNet. The browser's address bar shows the URL <http://192.168.100.1/>. The page features a navigation menu with tabs for Status, Signal, Addresses, FCoax, Configuration, Logs, and Help. A paragraph of text explains that the page provides information about the startup process of the Cable Modem and that the word "Failed" may appear in the Status column if there is a problem. Below this text is a table with two columns: Task and Status. The table lists eight tasks, all of which are marked as "Done" or "Operational". At the bottom of the page, there is a copyright notice: © Copyright 1997-2000.

Task	Status
Acquire Downstream Channel	Done
Obtain Upstream Parameters	Done
Establish IP Connectivity using DHCP	Done
Establish Time Of Day	Done
Transfer Operational Parameters through TFTP	Done
Register Connection	Done
Initialize Baseline Privacy	Done
Cable Modem Status	Operational

10b. Hackware

Hackware is a lot more, straight forward, with its easy user interface via the “Hack tab” below is a screen shot which is pretty self explanatory.

Configuration Manager

Status | Signal | Addresses | Configuration | Logs | Help | **Hack** | Sniffer

This page provides access to advanced features. Use it on your own!

User Defined Configuration File

File Name	<input type="text"/>
TFTP Server IP	<input type="text"/>
ISP default Config File	cm-1024-128
Maximum Download Speed	4096000 bps
Maximum Upload Speed	512000 bps

Download File from ISP's TFTP Server

File Name	<input type="text"/>
TFTP Server IP	<input type="text"/>

Update Cable Modem firmware

Cable Modem Identification

HFC MAC Address	00.11.22.AA.BB.CC
USB CPE MAC Address	00.11.22.AA.BB.CD

Developer's Tools

Status | Signal | Addresses | Configuration | Logs | Help | Hack | Sniffer

MOTOROLA
© Copyright 1997-2000

Internet

Enter your config here TW cm.10240-384 & NTL cmreg-sb4100 -bund03.cm

Enter your Mac Addresses here notice the slight difference in the HFC & USB Mac Address

Please note once you've installed your firmware you will need to put in your favorite frequency, this is your downstream frequency. The frequencies for the various areas are as follows:

TW: **33100000**
NTL: **402750000**
Ex-C&W: **586750000**

11. SB4100/SB4200 using a MAX232/MAX233 serial cable

The following screen shots and text were put together by me,

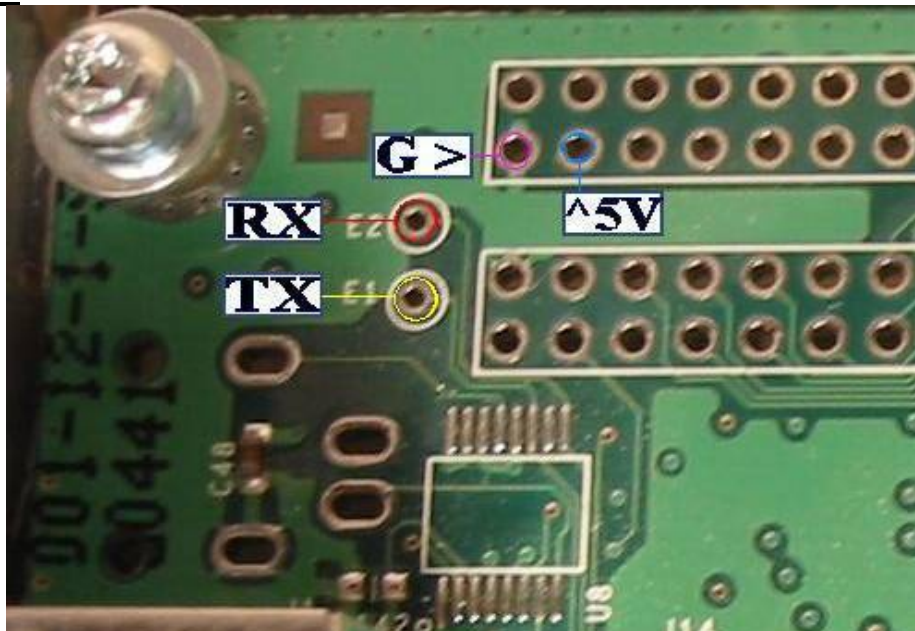
[Cableguy69](#)



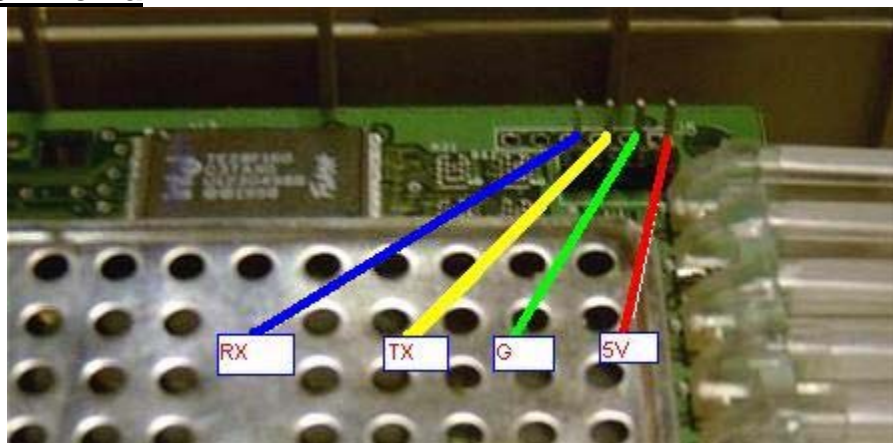
These are the solder points for the SB4100 & SB4200 where you'll need to connect your serial cable. Also if you're using a Max 232 from Tailor Made Circuits you'll need to connect to the modem as follows,

- 1 = Tx = Red
- 2 = Rx = Yellow
- 3 = Vcc = Blue
- 4 = GND = Black

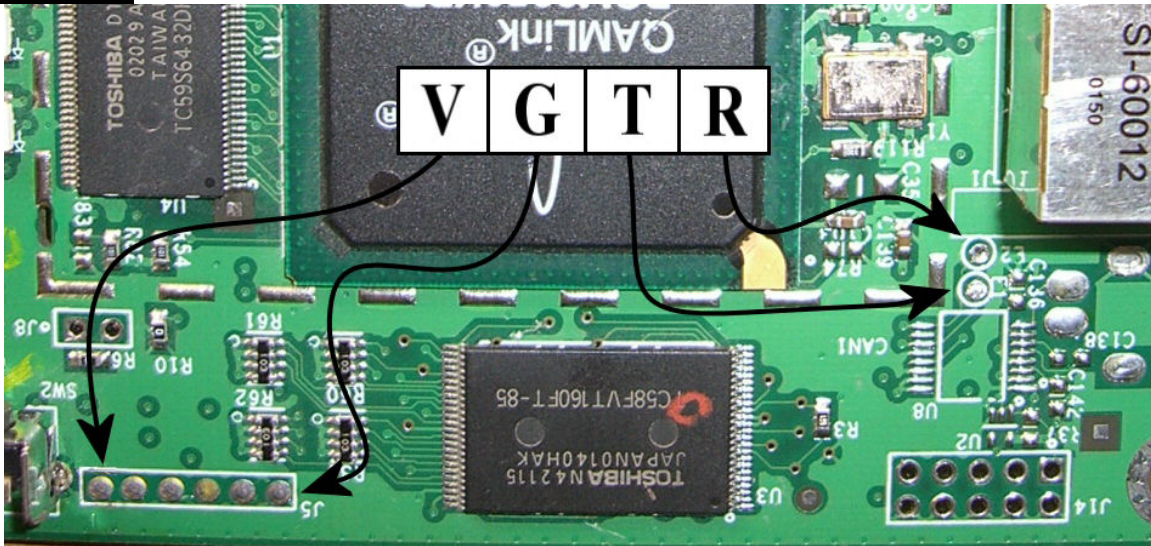
11a. SB4100



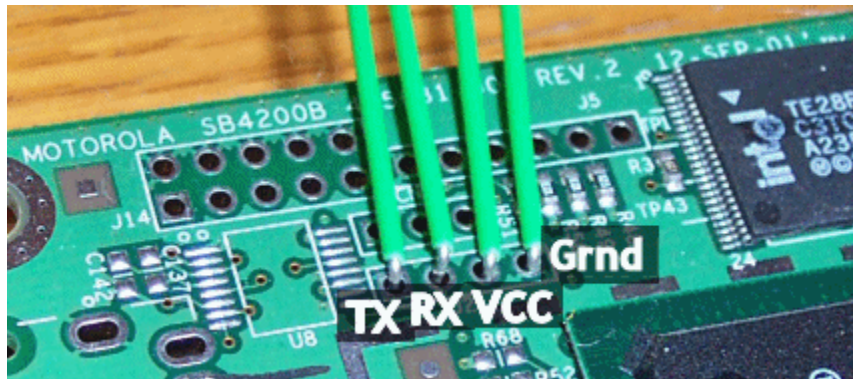
11b. SB4100 - Rev a



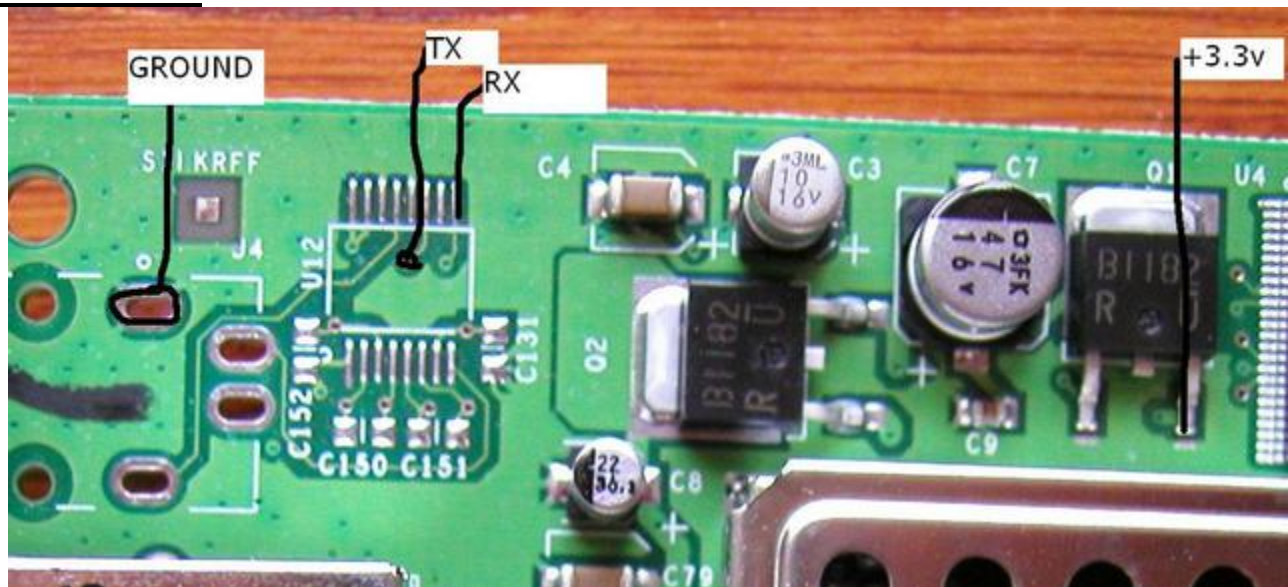
11c. SB4101



11d. SB4200



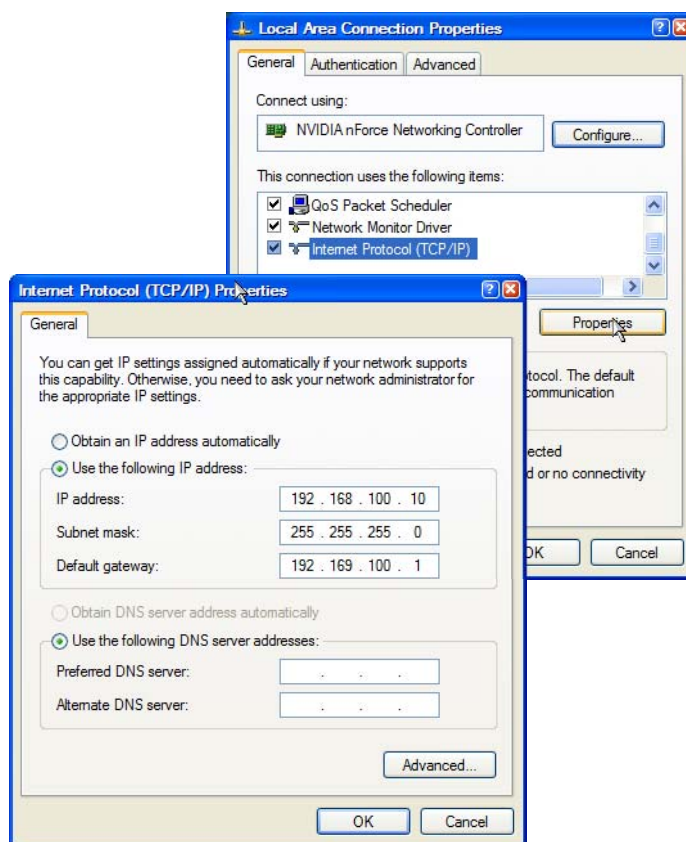
11e. SB5100



Now once you've connected your interface cable:

- 1) Start by going to:
Start → Control Panel → Network Connections
- 2) Right click **local area connection** and click properties.
(If you have more than one, make sure that you select the one your modem is connected to)
- 3) Click on "Internet protocol (TCP/IP)" once (do not uncheck it), & click properties, now set it up like this:

NOTE: You will need to have your Ethernet cable attached.



- 4) Now open the program called Boot.exe
- 5) Open HyperTerminal or Terraterm and set your baud settings to: **38400**
- 6) Connect your serial cable to your modem interface and power up your modem
- 7) Type: **2** & press **Enter**, this will allow you to boot over Ethernet.
You should now see something like this:

```
File Edit View Call Transfer Help
CPU: BCM3350
FLASH: Intel 28F160C3T
Version: 5.3.1
BSP version: 1.1/0
Creation date: Jan 13 2001, 16:38:48

Press any key to stop auto-boot...
21
[SB4100 Boot]: 2
Booting over the network...
Attaching network interface enetBcm0...
enetBcmAttach: mac address 00: [REDACTED] 75
done.
Attaching network interface lo0... done.
Loading... 2992872
Starting at 0x80010000...

Connected 00:03:29 Auto detect 38400 8-N-1 SCROLL CAPS NUM Capture Print-echo
```

```
FIREBALL Boot Server 2.0
File Server
[05/08/2005 21:45:01] Client 1 sent: USER jmcqueen
[05/08/2005 21:45:01] Client 1 sent: PASS rickey7
[05/08/2005 21:45:01] Client 1 Status: Idle
[05/08/2005 21:45:01] Client 1 sent: TYPE I
[05/08/2005 21:45:01] Client 1 sent: PORT 192.168.100.1 4,1
[05/08/2005 21:45:01] Client 1 sent: RETR /opt/vwMIPS_1_0
[05/08/2005 21:45:01] Client 1 Status: Downloading
[05/08/2005 21:45:05] Client 1 Status: Idle
[05/08/2005 21:45:05] Client 1 sent: QUIT
[05/08/2005 21:45:05] Client 1 logged out!

Exit IP Address: 82.42.109.47
```

- 8) Once Boot.exe has finished running reboot your modem and go to 192.168.100.1 and you should now see this page:

Configuration Manager

Status Signal Addresses Configuration Logs Help Hack Sniffer

This page provides information about the startup process of the Cable Modem. If there is a problem with the startup, the word "Failed" may appear in the Status column. Should this occur, visit the Help area and perform the Checkup procedures listed there. If the problem continues, click on the word "Failed" for more detailed information about the failure, or contact your service provider for assistance.

Task	Status
Acquire Downstream Channel	Done
Obtain Upstream Parameters	Done
Establish IP Connectivity using DHCP	Done
Establish Time Of Day	Done
Transfer Operational Parameters through TFTP	Done
Register Connection	Done
Initialize Baseline Privacy	Skipped

Status | Signal | Addresses | Configuration | Logs | Help | Hack | Sniffer

11e. "bootp referenced but not included" Error (SB3100/SB4100/SB4200)

Some modems may get the following error. "bootp referenced but not included":

```
FLASH: Intel 28F160C3T
Version: 5.3.1
BSP version: 1.1/0
Creation date:

Press any key to stop auto-boot...
21
[SB4200 Boot]: 2
Bootrom version: SB4200-0.4.4.0-SCM06-NOSH
Booting over the network...
Attaching network interface enetBcm0...
enetBcmAttach: mac address [redacted]
done.
bootp referenced but not included

SB4200
```

[31/01/2007 16:46:53] Boot Server Started

Exit IP Address: 192.168.100.10

If you get the following error, use the following command as posted by [Witchy2K1](#)

SBxx00 TELNET COMMAND LINE

Use the following commands in your [Telnet](#) Client if you get error "**bootp referenced but not included**" when running option 2

SB3100

```
cs(0,0)admin:/opt/vwMIPS_1_0_1_fcs/target/config/sb3100t/vxWorks.st  
e=192.168.100.1 h=192.168.100.10 u=jmcqueen pw=rickey7 f=0x8 tn=SB3100 o=bs1
```

SB4100

```
2 enetBcm(0,0)admin:/opt/vwMIPS_1_0_1_fcs/target/config/sb4100/vxWorks.st  
h=192.168.100.10 e=192.168.100.1 u=jmcqueen pw=rickey7 f=0x8 tn=SB4100 o=bs1
```

SB4200

```
2 enetBcm(0,0)admin:/opt/vwMIPS_1_0_1_fcs/target/config/sb4200/vxWorks.st  
h=192.168.100.10 e=192.168.100.1 u=jmcqueen pw=rickey7 f=0x8 tn=SB4200 o=bs1
```

To get into Telnet:

- 1) Goto the **start** menu and select **Run**
- 2) Type: **telnet** & press **Enter** (A telnet window should now pop up)

And that's it your done.

NOTE: If for any reason this does not work, you can also do it this way:

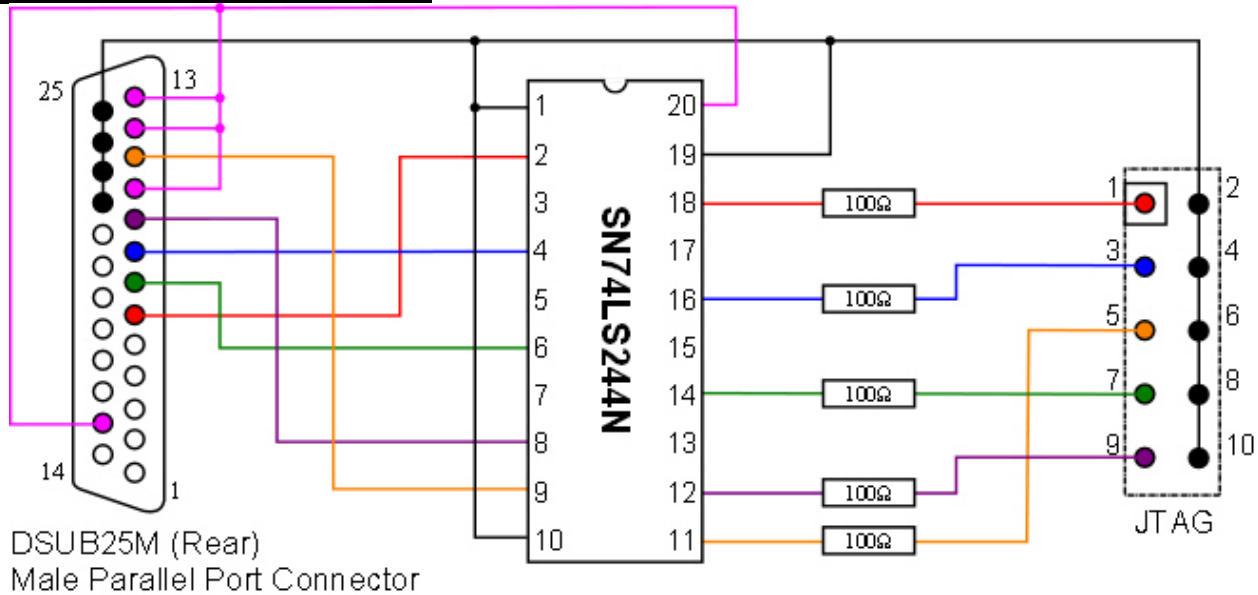
- 1) Goto the **start** menu and select **Run**
- 2) Type: **cmd** & press **Enter** (A new dos window should pop up)
- 3) In the dos window, type: **telnet** & press **Enter**

12. Blackcat

A Blackcat cable is the interface you'll need if you plan on modifying a Motorola SB5100 below are the schematics for making a Blackcat.

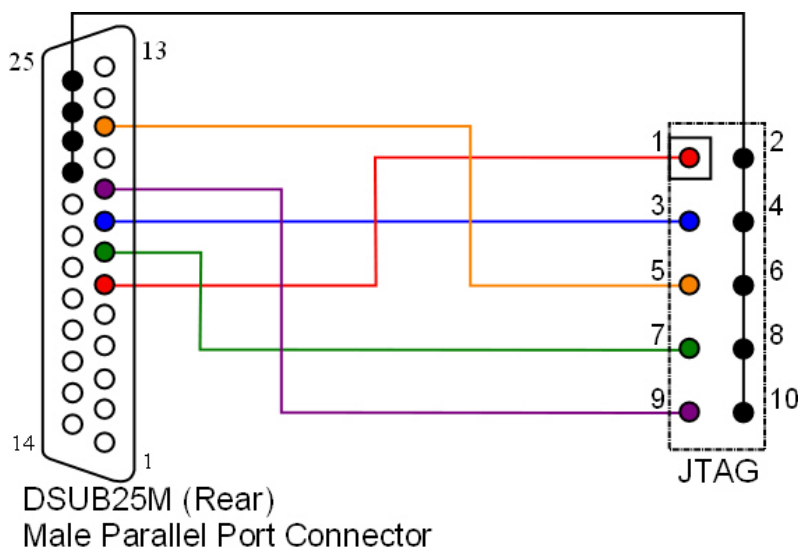
The following images were re-made by [LLAADD](#)

12a. SN74LS244N Version



12b. Chipless version

And here's an alternative that doesn't require a chip or resistors. There has been some talk of frying your modem using this method but I've tried this myself on a SB4100 and a SB5100 and it worked fine on both modems.



12c. Making a Chipless Blackcat

Ok so now you've got your Blackcat made up it might be wise to install a ten pin header onto your modems JTAG points to easily attach and remove your Blackcat. And here's a little more info on making a Blackcat without a chip.

The following photos and text were put together by [Granty](#)



This is a simple method of making a non i.c **BLACKCAT CABLE**

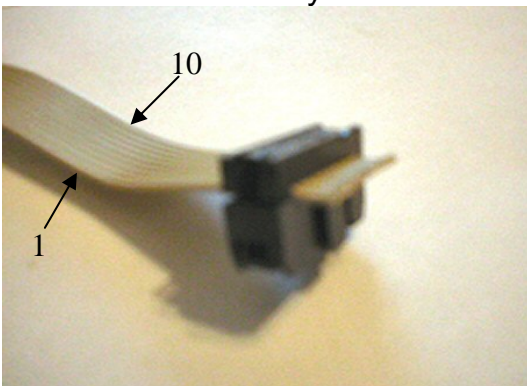
Below is a list of the items you will need from www.maplins.co.uk

- 1 x JB59P [2X5 DIL IDC SOCKET]
- 1 x JB85G [2X5 IDC PCB HEADER]
- 1 x XR74R [FLAT IDC CABLE 20 WAY (SEPARATE INTO 2x 10 WAY)]
- 1 x YQ48C [D-SUB 25 WAY plug]
- 1 x JW91Y [25W D TYPE HOOD]

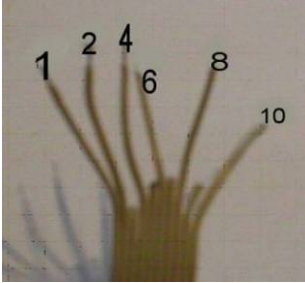


Open the DIL idc socket and slide the idc cable through and squeeze tightly to close the socket.

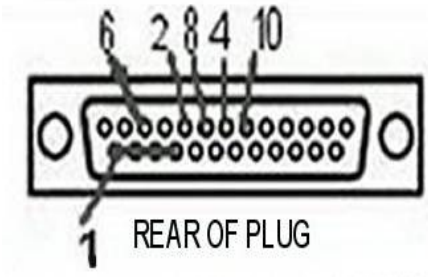
Take note of the way the socket is facing below.



At the other end of the idc cable cut the wires like in the pic below.
You will not be using 3,5,7,9 so cut and remove these wires



Solder wires to the rear of the 25-way plug, make sure to follow the pic below & above.
The number 1 wire should bridge 4 pins on the bottom row as in picture



Solder the PCB header onto your surfboard 5100 series

With the cut out facing as in the picture below

Failure to do this will render the header useless and you will have to remove and re solder.



Once finished your cable should connect like the picture below the next step is to load software and connect the cable to your pc.



Ok so now you've got your Blackcat made up it might be wise to install a ten pin header onto your modems JTAG points to easily attach and remove your Blackcat.

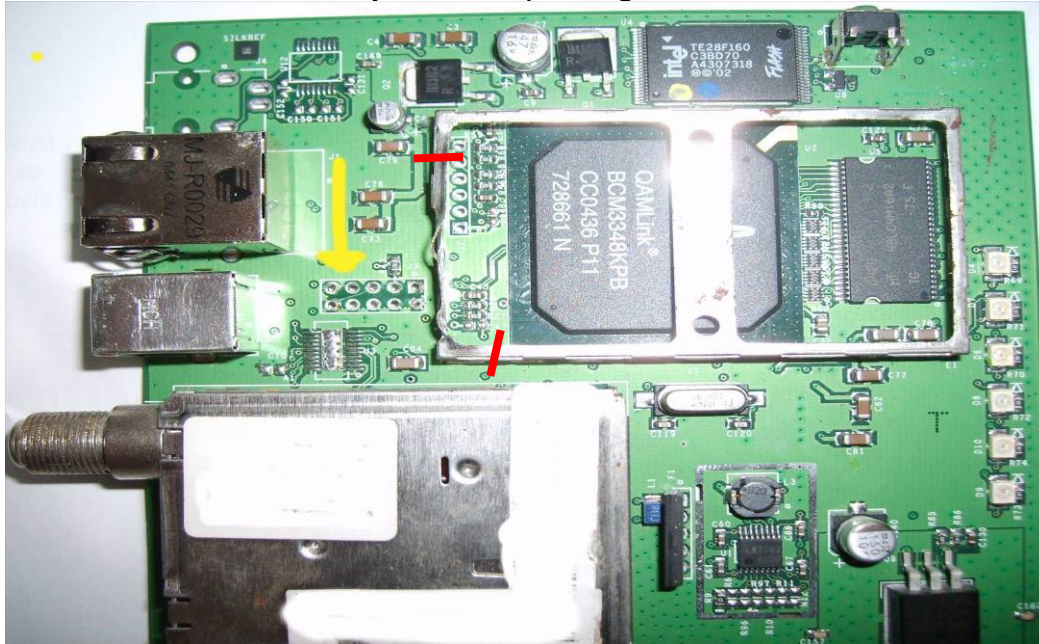
12d. Soldering a pin header

All screenshots and text were compiled by
Granty



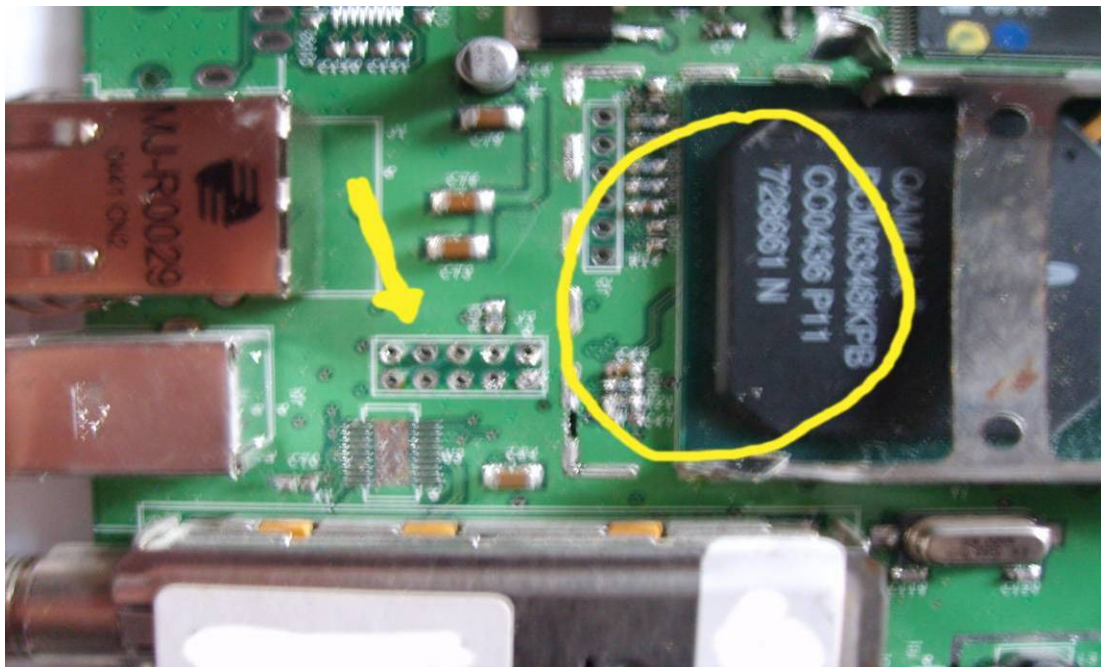
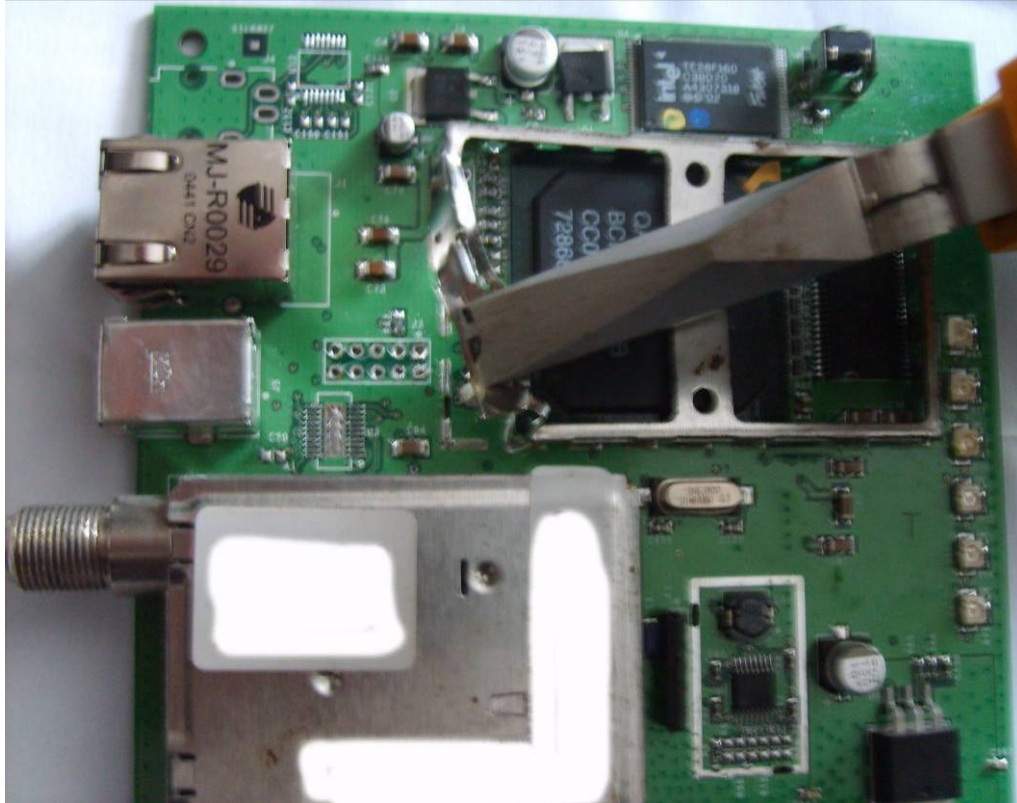
This is a guide to enable you to solder the 10 pin Header onto the Motorola Surfboard Series Modems

- 1) Remove the case and you can see in this first picture of the surfboard where your 10 pin header goes, whether it is a solder less type or not. For the header to sit correctly you must remove the lid off the chip and some of the surrounding metal. There's no need to worry about replacing the lid there's no use for it.

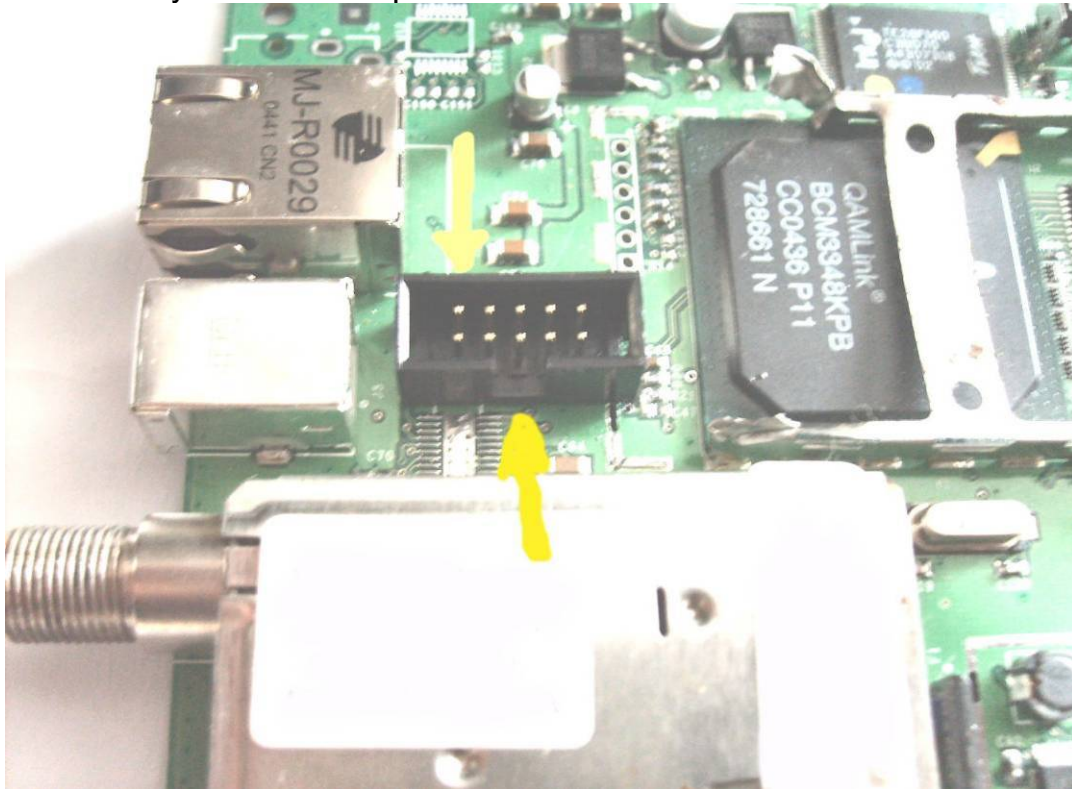


NOTE: Be very careful when doing this, as if you just try pulling it off, it may damage the circuit board. The best way to do this is to use a heavy duty wire cutter and cut through the metal in the 2 places marked in red above. Again be careful not to damage any components around the area.

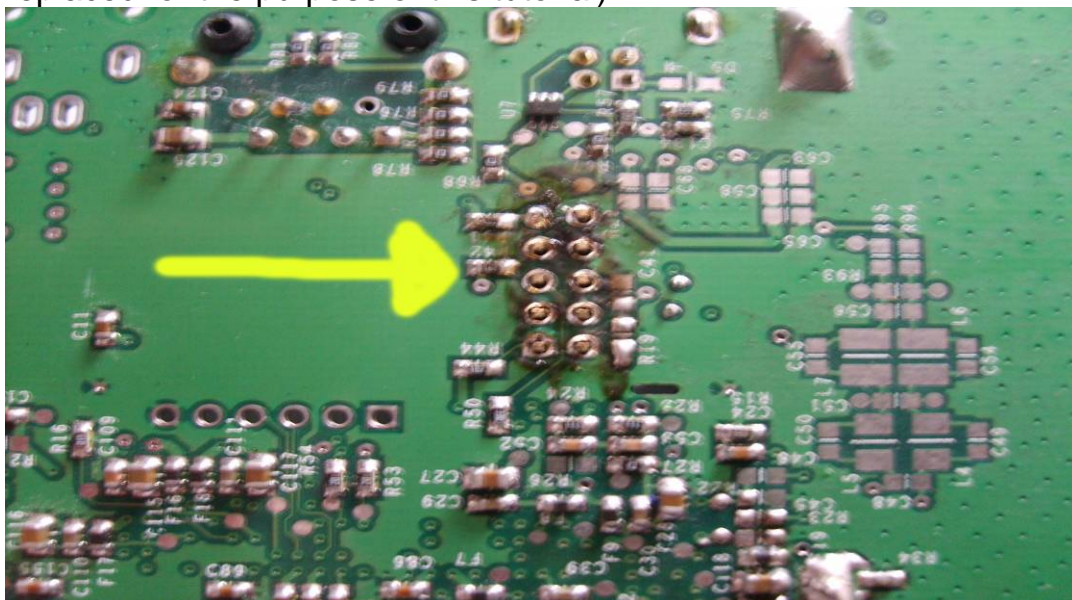
- 2) Now with a pair of pliers carefully twist the metal between the 2 cut points back and forth until it becomes loose then it should easily come off.



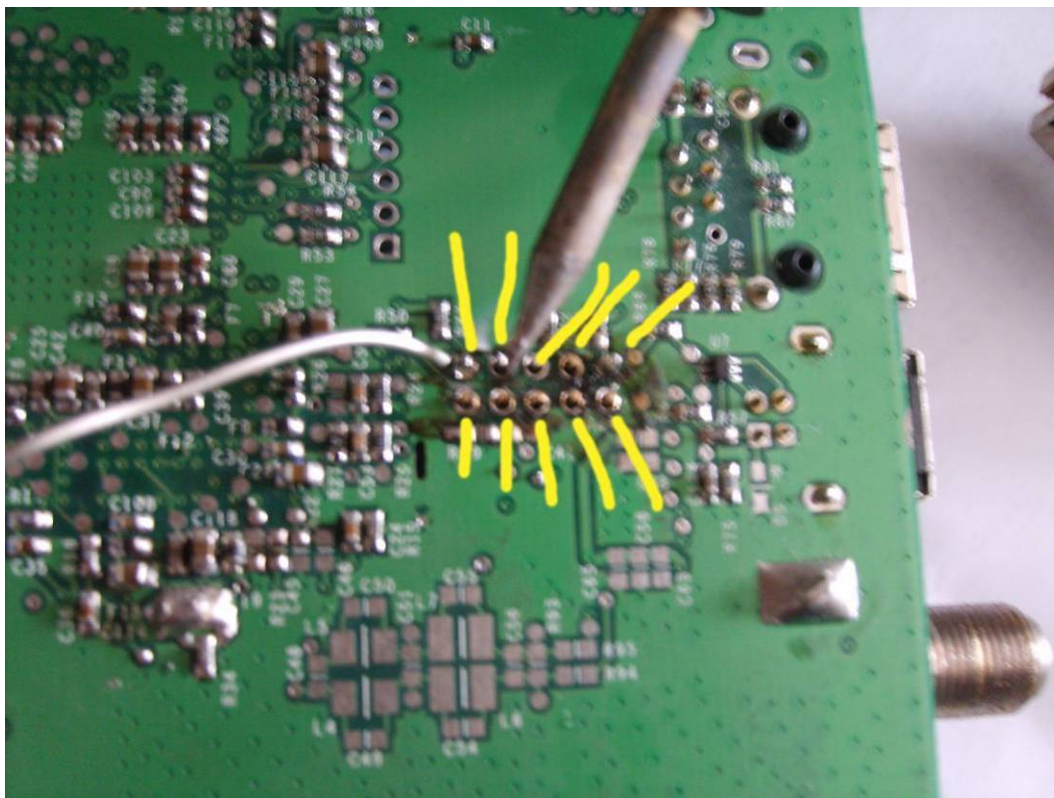
- 3) Once this has been done, and all sharp edges tucked away you can place your header onto the surfboard, but it must be placed in the correct way, as shown, if you are going to flash the modem with the non IC version of the Blackcat lead. This must be followed correctly otherwise you will not get the flash to take and can screw your modem up.



- 4) Once in place you can turn the modem over so we can start to solder the header onto the surfboard (As you can see in the picture there's a lot of Glaze on the board, this is just because the modem has had the header removed and replaced for the purpose of this tutorial)



- 5) The next thing is to plug your soldering iron in and when hot enough, tin the end with some solder. This will increase the flow when you come round to solder the header onto the board. There's no need to pile a load of solder onto the header and use braid to clean off you can do this quite easily by soldering each pin one by one to the board if you have a steady hand.



The best thing to do first off is to have a play around with some copper wire just to get the feel of how much solder you need to put onto your iron and then crack on, you don't need to be a master (I am no master, believe me)

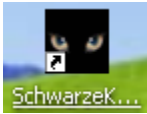
- 6) That's it, you're done! Just make sure that there are no short circuits. It's always a good idea to clean off any flux with an anti-static brush & a special electrical spray (DO NOT use normal cleaners as they may damage the board)

13. SB5100 Tutorial with Broadcom Commands

All screenshots and text were compiled by
Granty



- 1) Connect cable to surfboard
- 2) Start Blackcat software



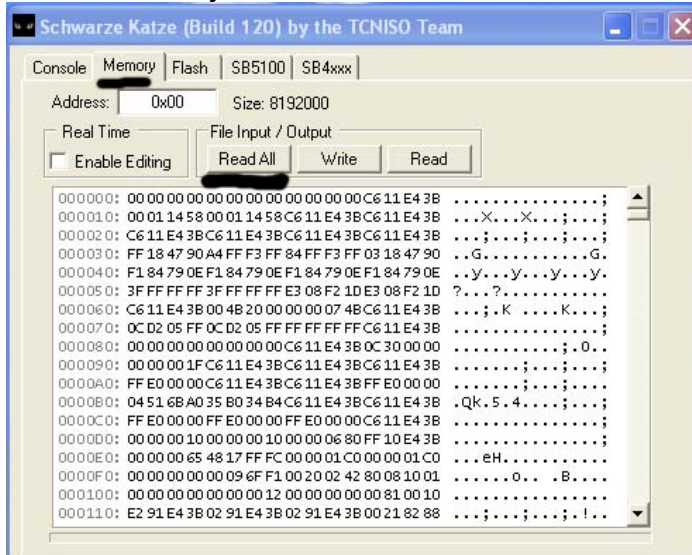
- 3) Once you have started this process do not attempt to open any other programs

NOTE: If for any reason after you have read the memory it says cannot detect flash, unplug the power from the modem and re plug .This should solve the problem as long as you have read and saved the memory you can carry on to the next step

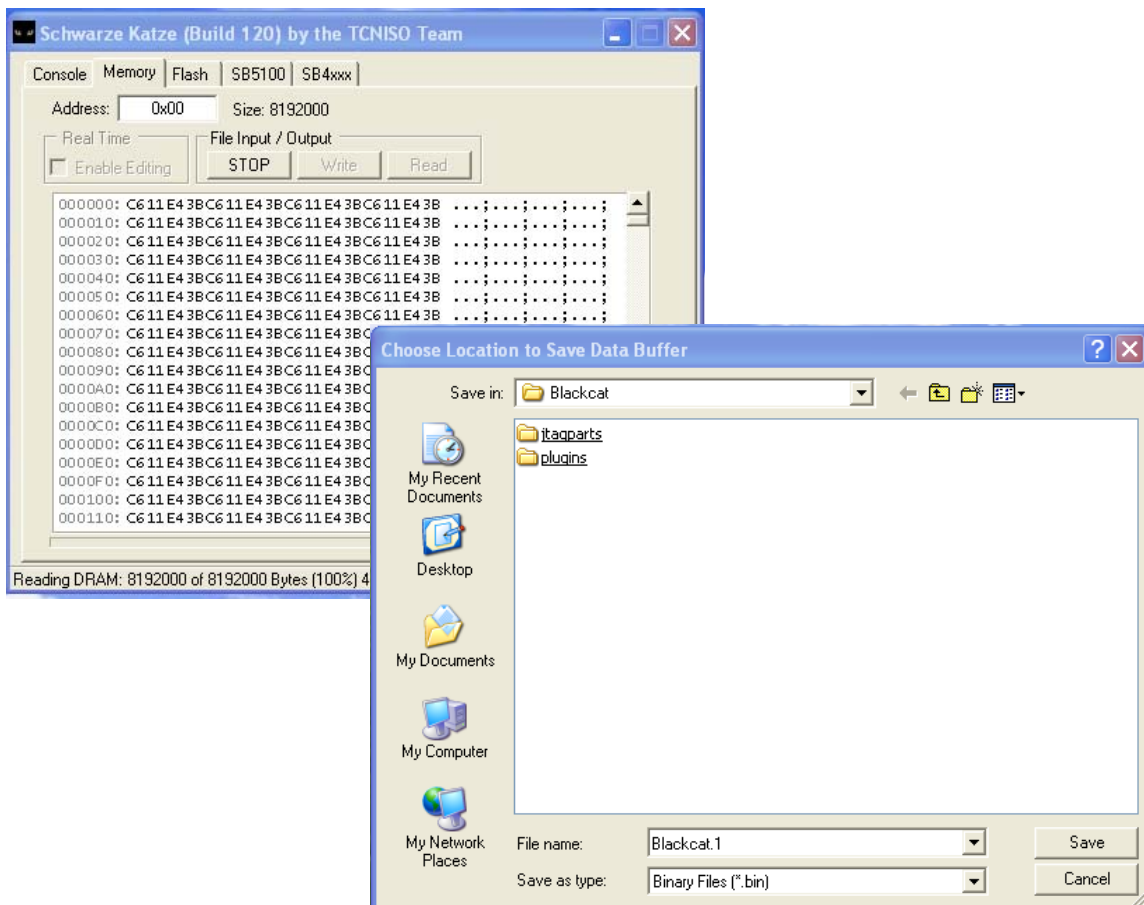
- 4) Go to Console tab and should detect Manufacturer:

```
Schwarze Katze (Build 120) by the TCNISO Team
Console | Memory | Flash | SB5100 | SB4xxx
Black Cat Console
Jtag Engine initiated successfully
BlackCat plugin services started.....
0: NULL plugin created
loading plugins from C:\Program
Files\TCNISO\BlackCat\plugins\
2:8192: [EJTAG] loaded from C:\Program
Files\TCNISO\BlackCat\plugins\ejtag.dll
3:655360: [FlashPlugin] loaded from C:\Program
Files\TCNISO\BlackCat\plugins\flashpi.dll
4:16384: [PCPARPORT] loaded from C:\Program
Files\TCNISO\BlackCat\plugins\pcparport_win32.dll
5:4096: [JTAG] loaded from C:\Program
Files\TCNISO\BlackCat\plugins\pptap1.dll
Link Success /BlackCat/EJTAG:1<->/BlackCat/JTAG
Link Success /BlackCat/JTAG:1<->/BlackCat/PCPARPORT
Link Success /BlackCat/FlashPlugin:1<->/BlackCat/MEMORY
6 plugins loaded
0x00000000 = 0
Manufacturer: broadcom
Part: bcm3348
```

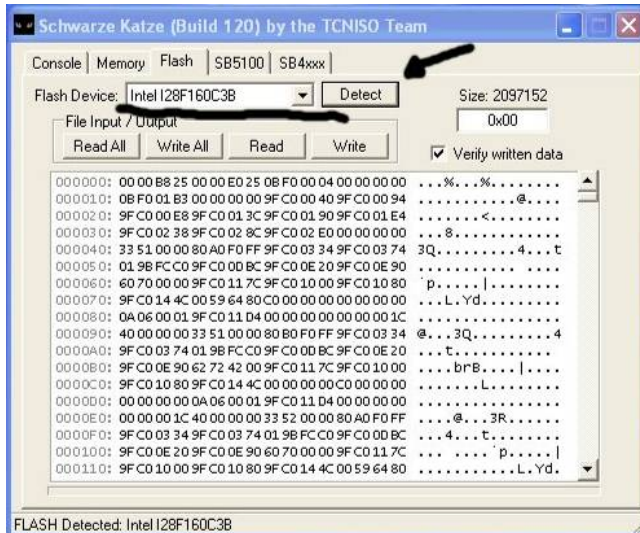

5) Go to Memory tab and select read all:



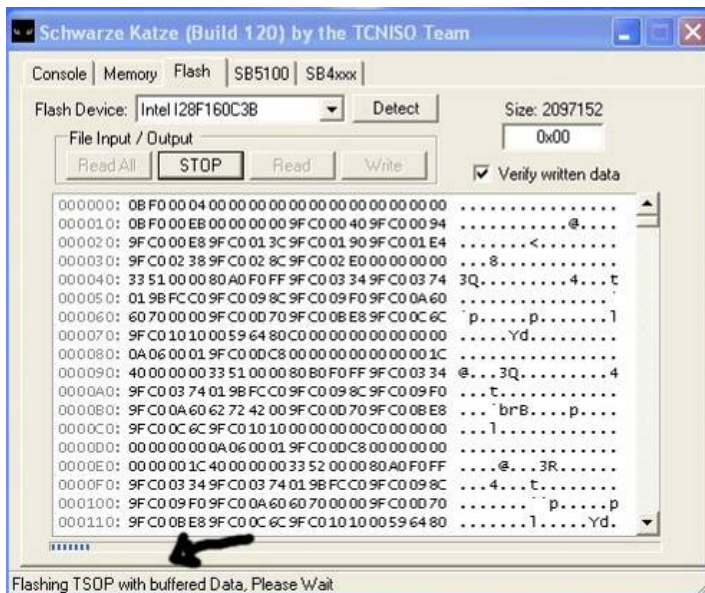
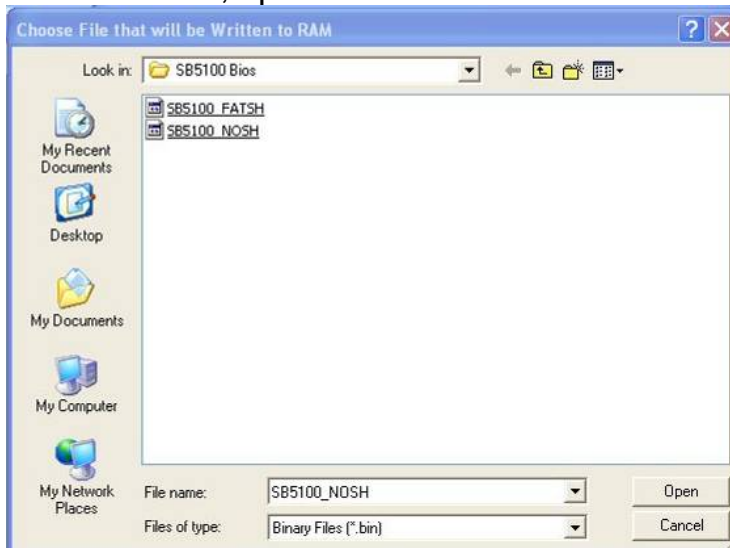
This will take a while, when finished save file as blackcat.1,



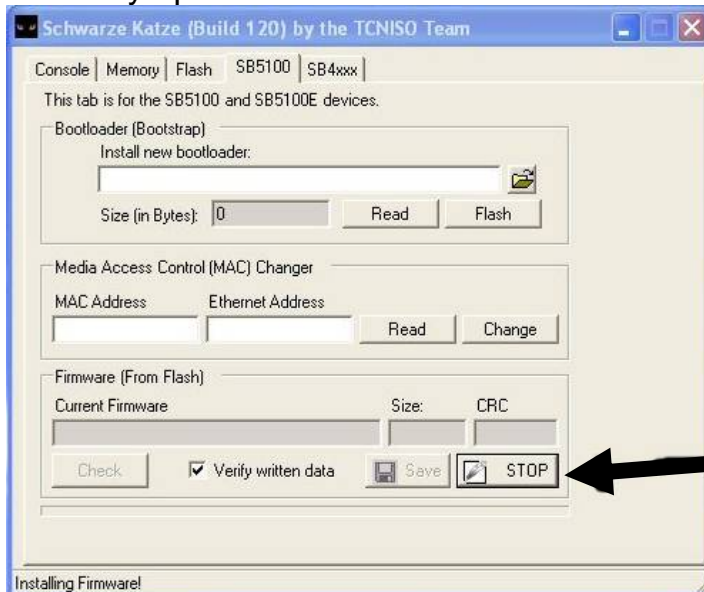
6) Go to the flash tab and click Detect



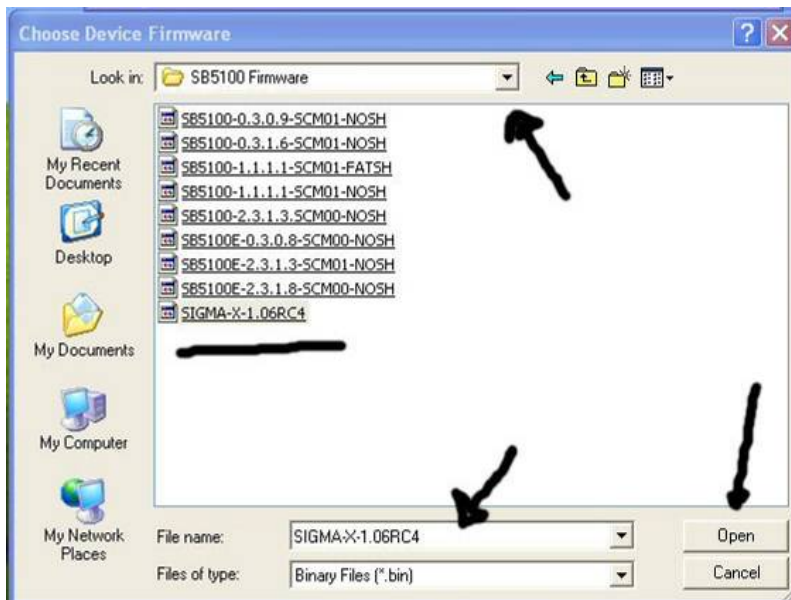
7) Click **write all**, open the SB5100 bios folder and select the nosh file and open



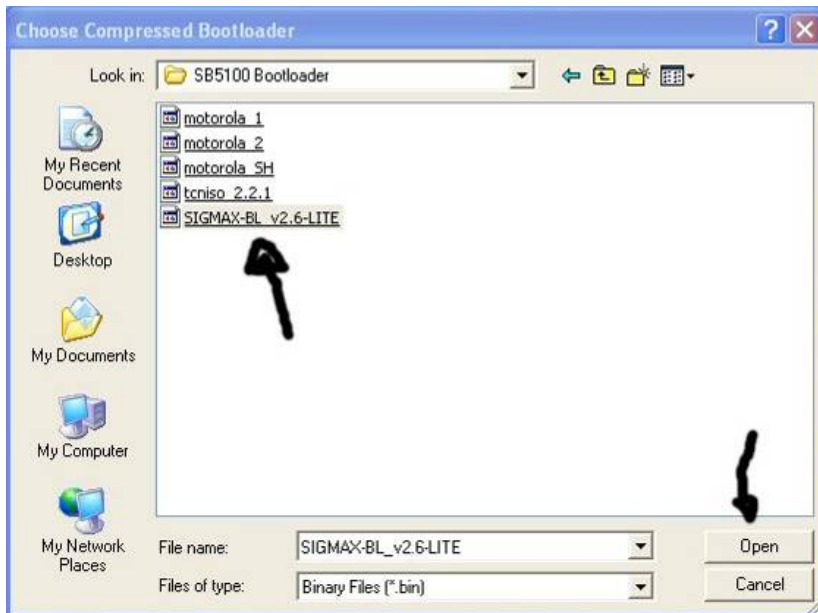
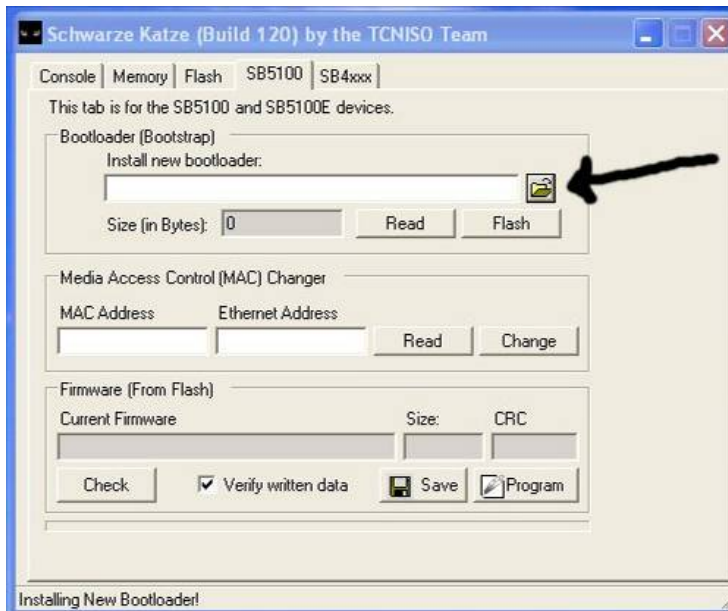
- 8) This is the page you will have on display next; don't panic because this is where you will have to wait at least 40mins for it to finish what its doing. When finished it will say operation done.



Click here, this will say "Program", but once clicked and the firmware is selected, it will change to "STOP"



- 9) Click on the 'SB5100' tab, click 'Program' and choose the 'SIGMA-X-1.06.bin' firmware. Got to be this one I had to search the folders on the CD for it. This will take a while to load. When it's done, it will confirm new firmware installed.
- 10) Next on the Boot loader (bootstrap), click on the yellow folder above the flash tab and find the 'SIGMAX-BL_v2.6-LITE.bin' file. Then click 'Flash', when finished it will say new bootloader installed.



11) When done, unplug the power cable from modem and re-connect

12) Open up an internet browser and goto: <http://192.168.100.1/>

- 13) Go across to the sigma tab & put a known working Mac in: "HFC MAC Addr:" and then click Change next to that box.

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

. Basic :.

Original Config:

Config File: Change

Config TFTP IP: Change

. Media Access Controller :.

HFC MAC Addr: 00:D0:59:F5:22:50 Change

Serial: 128103332400868102010000 Change

. Advanced :.

- 14) Unplug power cable again, and reconnect, then go back to: <http://192.168.100.1/>
- 15) If not done change this setting to factory mode enabled, then unplug power and reconnect.

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

. Basic :.

Factory mode: Enabled Change

View: Change

docsDevSwOperStatus: Change

docsDevSwAdminStatus: Change

. SpooF :.

- 16) In the sigma window go to the webshell tab and in the broadcom shell command box;
- Type: **cd non-vol** & click **Execute**
- Type: **cd halif** & click **Execute**
- Type: **cmanex_3** & click **Execute**
- Type: **UpdateSettings** & click **Execute**

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

Instance: Console Thread (0x80747a34)

Active Command Table: Non-Volatile Settings Commands (non-vol)

CH-App -> non-vol

Instance: Console Thread (0x80747a34)

vxWorks Shell

Command

Broadcom Shell Command

cd non-vol 

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

Instance: Console Thread (0x80747a34)

Active Command Table: HalIf NonVol Commands (halif)


CH-App -> non-vol -> halif

Instance: Console Thread (0x80747a34)

vxWorks Shell

Command

Broadcom Shell Command

cd halif 

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

Instance: HAL Interface NonVol Settings (0x8074cd58)

CM DOCSIS Annex Mode: 3


NOTE: You must write the settings and reboot for the change to take eff

Instance: Console Thread (0x80747a34)

vxWorks Shell

Command

Broadcom Shell Command

cm_annex 3 

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

Instance: CableModem EventLog NonVol Settings (0x8074c034)

Dynamic Non-Vol Settings successfully written to the device.
Permanent Non-Vol Settings successfully written to the device.

Instance: Console Thread (0x80747a34)

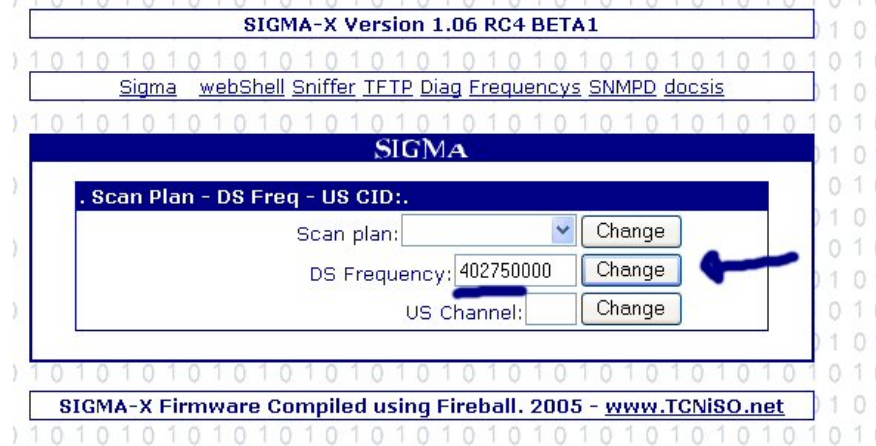
vxWorks Shell

Command

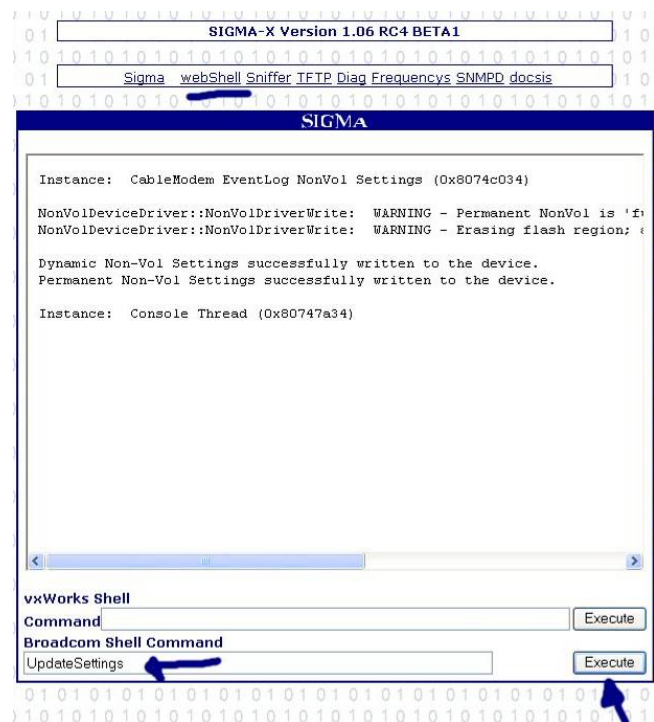
Broadcom Shell Command

UpdateSettings 

- 17) Go to the frequency tab and type in your downstream frequency & click Change, (mine is NTL area, enter yours as appropriate)



- 18) Go back to webShell, and in the broadcom shell command box; Type: **UpdateSettings** & click **Execute**



19) Unplug power cable & reconnect. Go to <http://192.168.100.1/> then Sigma page

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

. Basic :.

Original Config:

Config File:

Config TFTP IP:

. Media Access Controller :.

HFC MAC Addr:

Serial:

. Advanced :.

Here type in a valid and working MAC address and press Change.

NOTE: The MAC address shown above is not a real one, it's just made up

20) Unplug modem and connect coax cable (NTL feed cable) & power up. Go back again to: <http://192.168.100.1>, this time write in the config box the config file for 20meg (mine again is Ntl, enter yours as appropriate)

SIGMA-X Version 1.06 RC4 BETA1

Sigma webShell Sniffer TFTP Diag Frequencys SNMPD docsis

SIGMA

. Basic :.

Original Config:

Config File:

Config TFTP IP:

. Media Access Controller :.

21) Unplug modem power and re-connect, start up modem & you should be online.

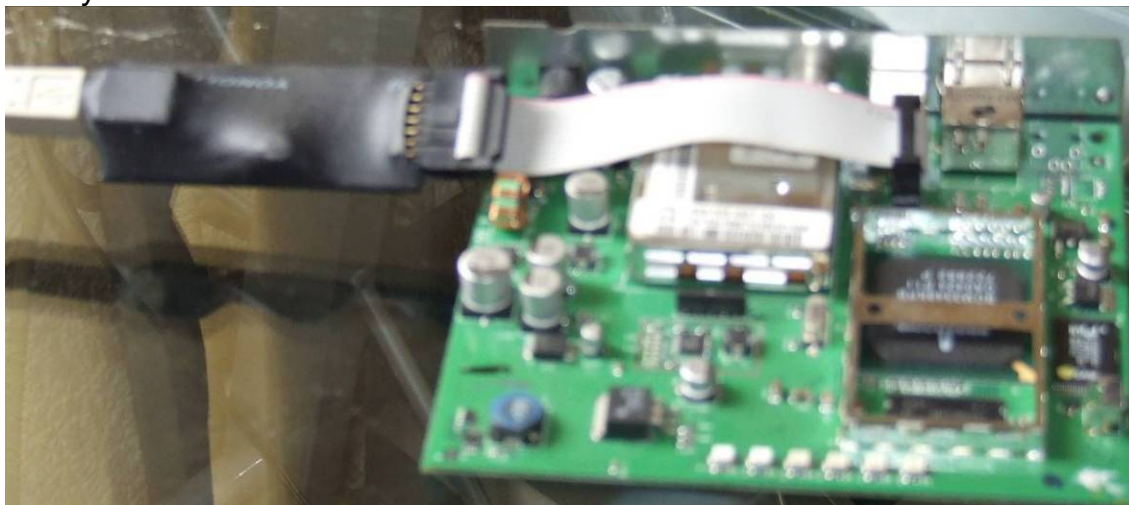
13a. USB JTAG ON A SB5100 USING FERCSA`S X2 STEALTH13.5

All screenshots and text were compiled by

Koevoet



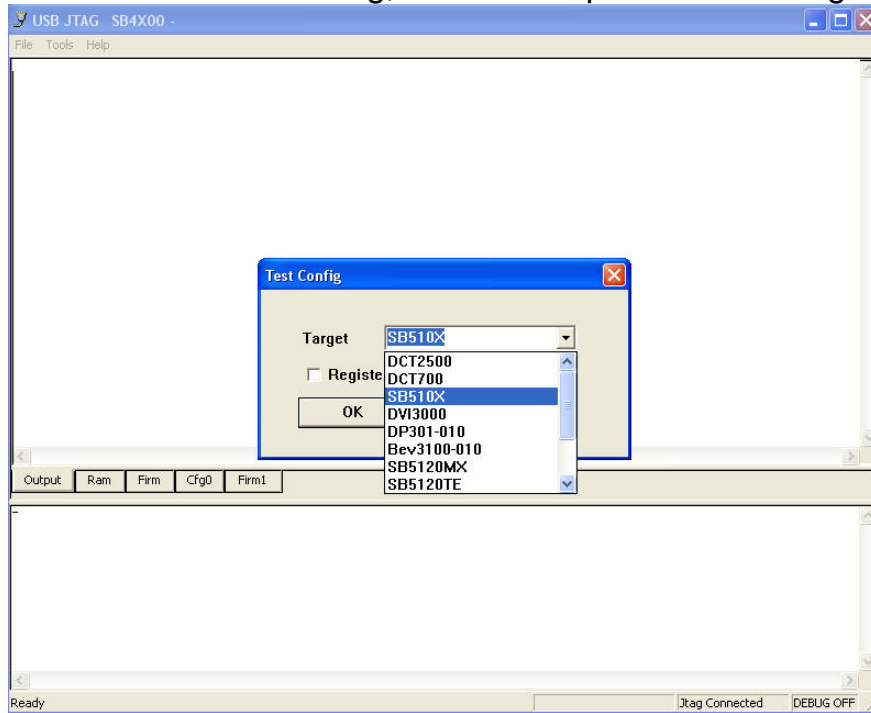
1. Firstly the JTAG will connect to the modem as follows:



2. You will then have to initialize the software, by clicking on the USB JTAG software icon.

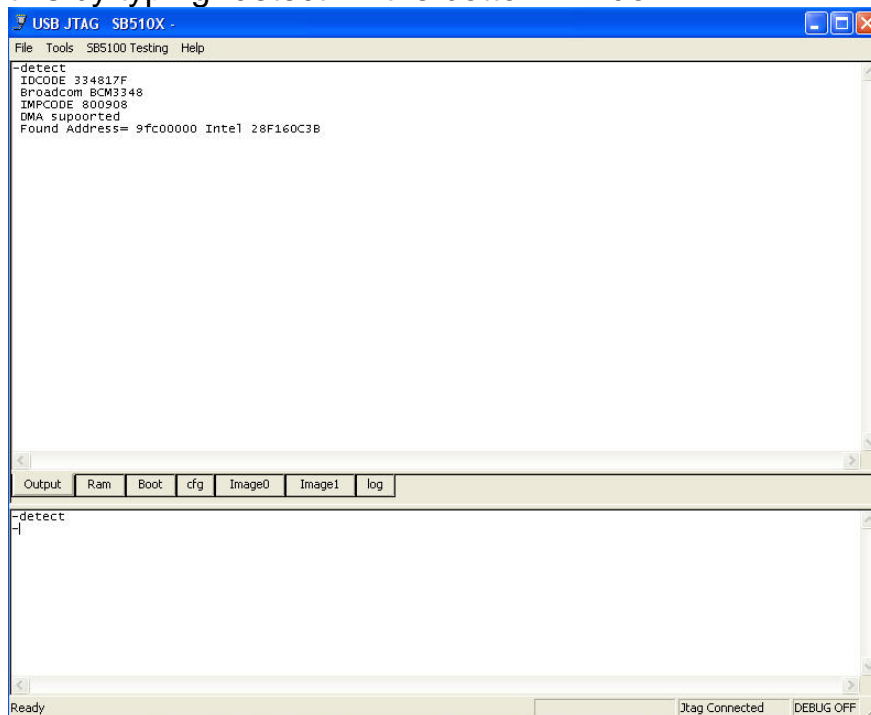


- Now you need to select the type of modem you are going to flash, to do this click on tools then config, it will then open the following menu:



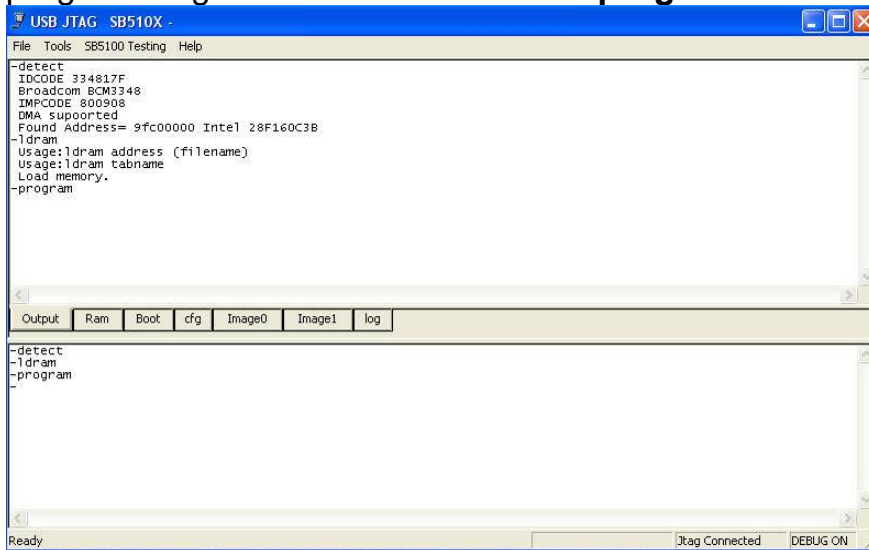
In this case we will be selecting SB510X, as it's a SB5100 modem we are going to be programming.

- Next we need to detect the modem, to see if the USBJTAG recognizes it, we do this by typing "detect" in the bottom window:



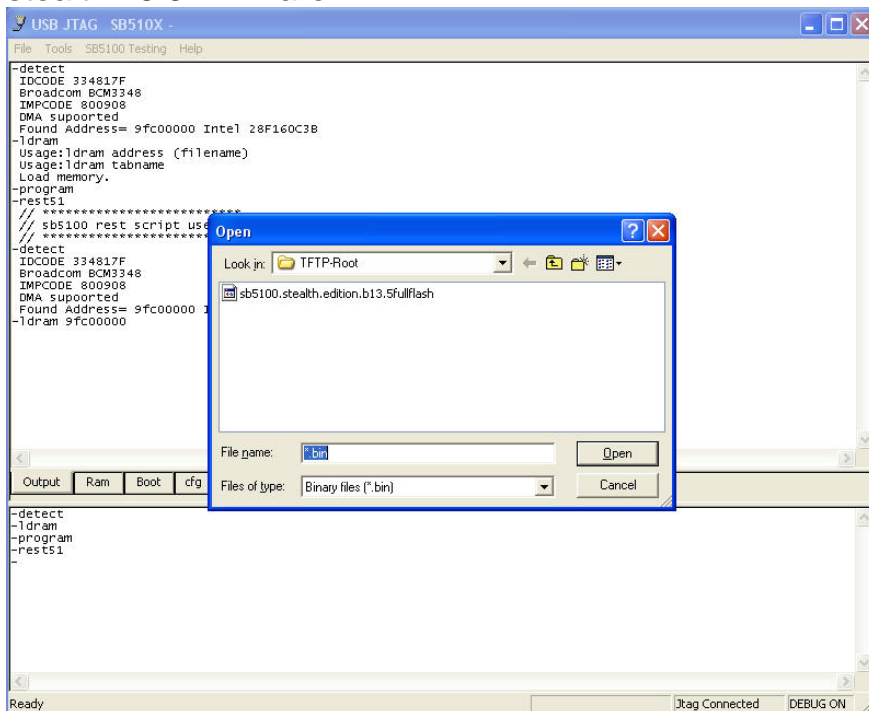
As you can see from above, it sees the modem has an Intel flash

5. Now we need to issue 2 more commands to get the modem ready for programming these are: **ldram** & then **program**

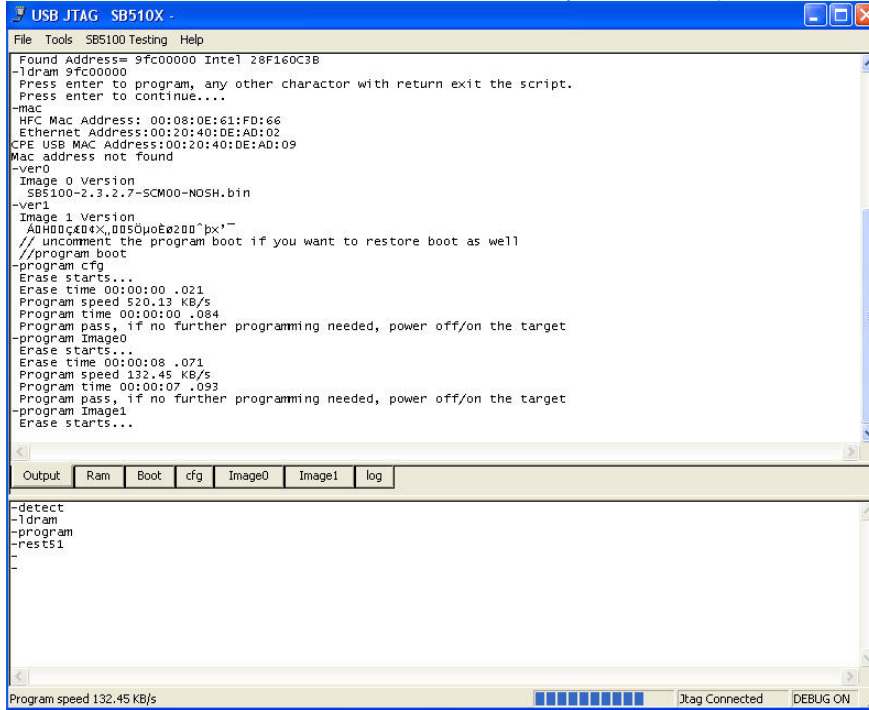


As you can now see in the bottom right hand corner it says “Debug on” this tells us the modem can now be flashed without fear of it crashing, it is best to leave this for 30 seconds to verify that it does not go back to “off” as some Chips contain a watchdog.

6. We will now use a command for restoring a flash, this command is useful for flashing new full flash dumps as well as backups of the modem the command is “**rest51**”. In your software folder you should have the rest51.usp file with the relevant commands for this to work. When this command is inserted you will then have to locate your full flash dump, in this case I am using Fercsa’s latest stealth 13.5 firmware.



7. The firmware should now flash after you have pressed enter



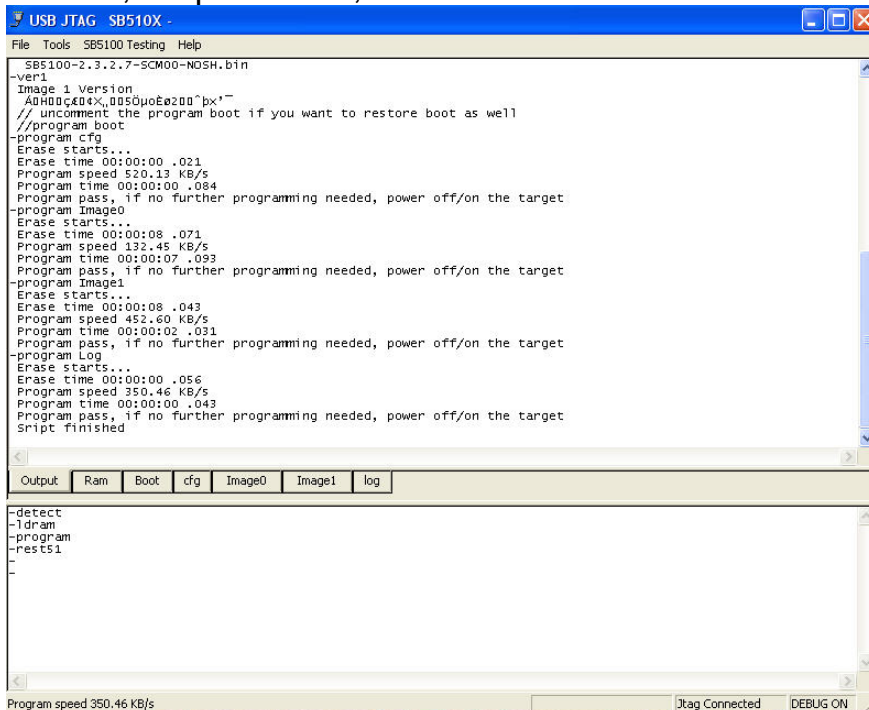
```
USB JTAG SB510X -
File Tools SB5100 Testing Help
Found Address= 9fc00000 Intel 28F160C3B
-l dram 9fc00000
Press enter to program, any other character with return exit the script.
Press enter to continue...
-mac
HFC Mac Address: 00:08:0E:61:FD:66
Ethernet Address:00:20:40:DE:AD:02
CPE USB MAC Address:00:20:40:DE:AD:09
Mac address not found
-ver0
Image 0 Version
SB5100-2.3.2.7-SCM00-NOSH.bin
-ver1
Image 1 Version
ADH00c40eX,0050uoE0200`bx'~
// uncomment the program boot if you want to restore boot as well
//program boot
-program cfg
Erase starts...
Erase time 00:00:00 .021
Program speed 520.13 KB/s
Program time 00:00:00 .084
Program pass, if no further programming needed, power off/on the target
-program Image0
Erase starts...
Erase time 00:00:08 .071
Program speed 132.45 KB/s
Program time 00:00:07 .093
Program pass, if no further programming needed, power off/on the target
-program Image1
Erase starts...
```

Output Ram Boot cfg Image0 Image1 log

```
-detect
-l dram
-program
-rests1
-
```

Program speed 132.45 KB/s [Progress Bar] Jtag Connected DEBUG ON

8. On completion it will say if no further programming is needed turn off the modem, script finished, in other words reboot it.



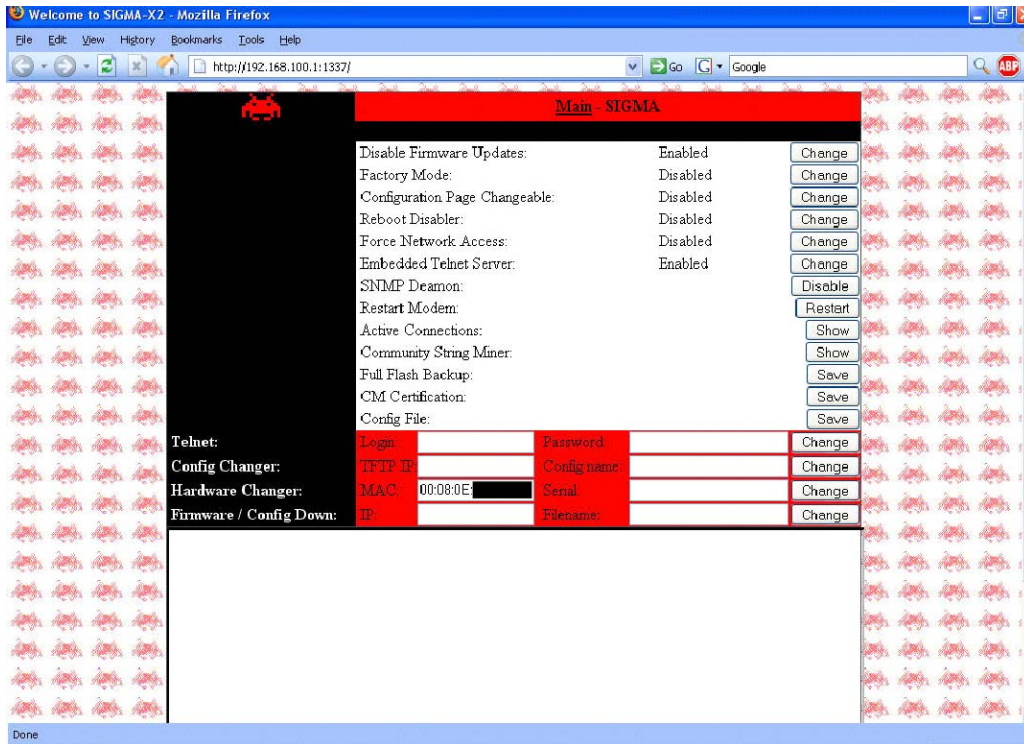
```
USB JTAG SB510X -
File Tools SB5100 Testing Help
SB5100-2.3.2.7-SCM00-NOSH.bin
-ver1
Image 1 Version
ADH00c40eX,0050uoE0200`bx'~
// uncomment the program boot if you want to restore boot as well
//program boot
-program cfg
Erase starts...
Erase time 00:00:00 .021
Program speed 520.13 KB/s
Program time 00:00:00 .084
Program pass, if no further programming needed, power off/on the target
-program Image0
Erase starts...
Erase time 00:00:08 .071
Program speed 132.45 KB/s
Program time 00:00:07 .093
Program pass, if no further programming needed, power off/on the target
-program Image1
Erase starts...
Erase time 00:00:08 .043
Program speed 452.60 KB/s
Program time 00:00:02 .031
Program pass, if no further programming needed, power off/on the target
-program Log
Erase starts...
Erase time 00:00:00 .056
Program speed 350.46 KB/s
Program time 00:00:00 .043
Program pass, if no further programming needed, power off/on the target
Script finished
```

Output Ram Boot cfg Image0 Image1 log

```
-detect
-l dram
-program
-rests1
-
```

Program speed 350.46 KB/s [Progress Bar] Jtag Connected DEBUG ON

9. Now to check if it has all gone well, on reboot connect the Ethernet cable and browse to <http://192.168.100.1:1337>, and you should be confronted with the following:



If so then congratulations, you have just flashed a SB5100 modem with Fercsa`s X2 stealth 13.5 firmware.

To get hold of a USBTAG or software you can go here <http://www.usbjtag.com/>

14. Motorola SB5101

14a. Method 1

Unfortunately there's no hacked firmware available yet for the SB5101 but have a read of the following that was posted on Modshack by:

R3V3NG3R



In the blackcat program folder, go to the broadcom folder and add this line to the broadcom.bc file `jtagpart 0x3349 "bcm3349" "bcm3349_docsis"` and create a new .bc file containing this line `script "./jtagparts/common/ejtag.bcs"` and save the file as `bcm3349.bcs`

Build 126+ is the only version that has support for 5101 devices. Unfortunately for all you pirates, these builds have online protection integrated so you must be a member and have purchased a firmware.

Well now you can sort your 5101 modem out without being a TCNIO member and having the latest Shwarzekatze.

Do the above in build 120.

14b. Method 2

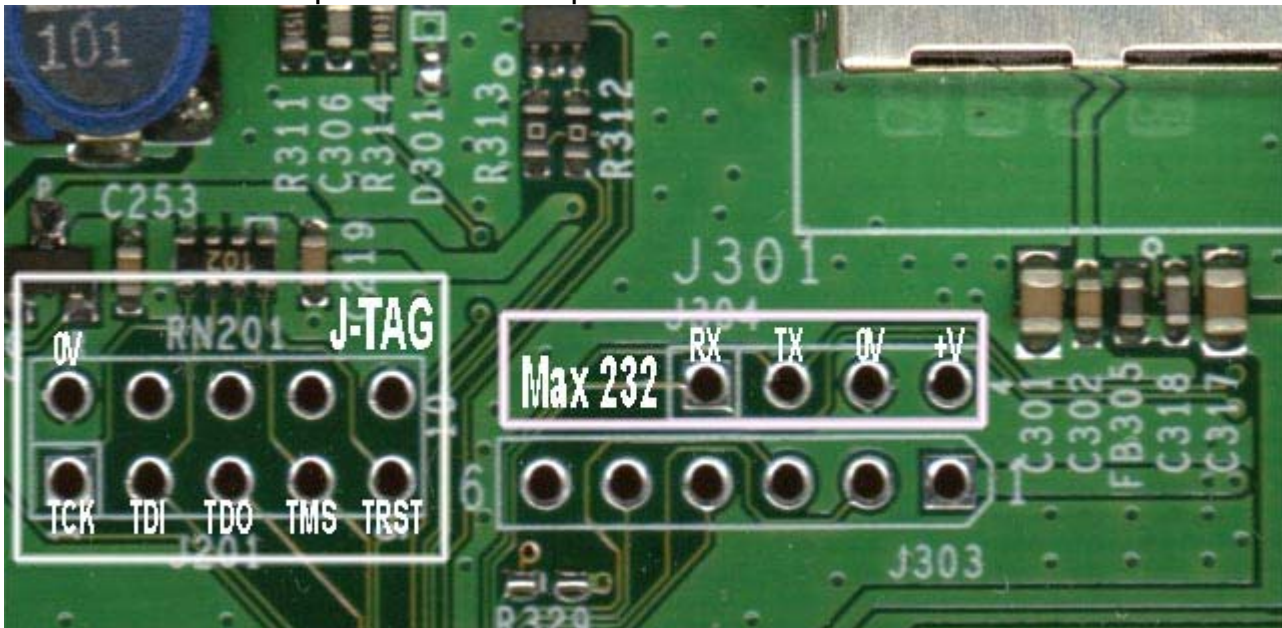
Here's another way to mod the SB5101 without using modified firmware.

The following screen shots and text were put together by [Boltar](#)



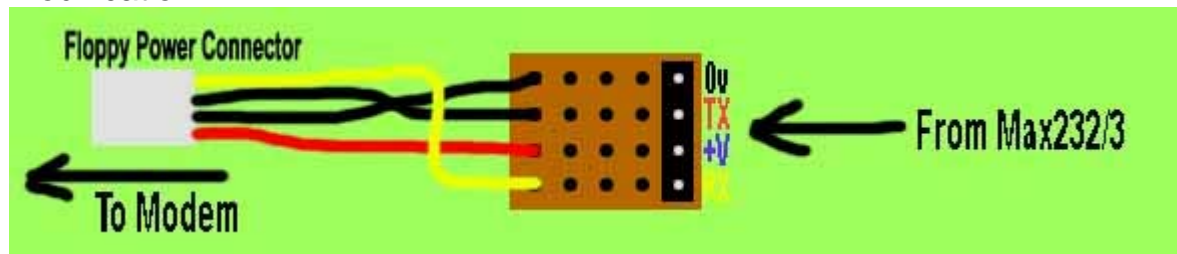
The JTAG and serial ports make it cable modem modding perfection. There is however a distinct lack of firmware that will work on it. You can of course use the Ambit 250 hacked firmware on which works fine (*as the Ambit 250 is pretty much the same modem as a SB5101E*). However, this tutorial is for those of you that would rather use the more up to date original firmware that came with the modem. On mine, that firmware is SB5101E-0.4.1.4-SCM02-NOSH. Of course, this firmware has no console, so, you would think you are stuck with simply changing the MAC address via blackcat and putting up with the subscribed config of the MAC you are using, which means scratching around looking for the few bund03 configs in your sniffers. Well you don't have to do that. Here's a simple guide to using the original SB5101E firmware with all the config override options. I am assuming you are familiar with the basic concepts of blackcat programming and serial flashing; this tutorial will not go into huge detail about these processes as you are expected to know. I recommend you use build 128 of SchwarzeKatze too.

The 5101 will need to be soldered up with the JTAG and SERIAL port headers. This is an illustration of the pin-outs of each port.



Note that the serial port pin outs are arranged differently to the standard pin outs most of us are used to, and you may need to create a small adapter. I used a small piece of strip board, a 4 pin header and a floppy power cable I cut from an old power supply

(see image). This adapter changes the pin outs to the same order as the ambit modems, allowing the standard pre-built Max232/3 cables to work without modification.



The JTAG points are however standard.

Taking a full backup.

Connect the cable feed and boot the modem and allow it to obtain a lock. You will know it's locked when you see all the 4 green LED's lit on the front. Now power down the modem and disconnect the cable feed. Connect the blackcat cable and power the modem up again, this time take a full backup of the modem firmware using SchwarzeKatze. Go to the 'Flash' tab and click 'Read All' to do this.

Flashing a new bootloader.

After the full backup is done you need to flash a new bootloader. As standard, the 5101E has a quiet bootloader, this needs to be replaced with another to allow us access to the main flash menu. Just use SchwarzeKatze to flash the included **bootloader.bin** file onto the modem using the 'Bootloader (Bootstrap)' function in the 'SB5100' tab. Wait until this is finished.

Netbooting a shelled firmware.

Power down the modem and connect your Max232/3 cable. Load up your terminal emulator and power up the modem. You should now see the familiar "Press '1', '2' or 'p'" prompt appear. Press 'p'. Enter **192.168.100.1** as the main board IP as usual, and again, as usual set your windows tcp/ip settings to IP:192.168.100.10 NetMask:255.255.255.0 , all standard stuff so far.

Start up your tftp server (*there's one included*) and make sure that its root folder is set to the same folder that you extracted the attached rar file into. In the flash menu, select option 'g'. Enter **192.168.100.10** as the TFTP IP and enter **SB5100E-2.3.2.0-SCM03-FATSH.bin** as the filename. It will download it and scroll a few things on the terminal screen, and then it will ask if you want to save parameters to flash, enter **no**. The shelled firmware will then run, although this firmware is meant for a 5100E, it will still run on a 5101E, it just doesn't support the tuner used in the 5101E so it cannot lock onto the DS frequency, but that doesn't mean we can't use the firmware to change the modem's settings, getting the idea now? He he!

When all booted it will start to scan for channels, but will be complaining because the tuner is not supported, stop this by entering these commands.

Code:

```
cd /cm_hal
scan_stop
```

Now enter the following commands to setup your modem. *Note some of these commands need alteration.*

Code:

```
cd /non
cd halif
mac_address 1 aa:bb:cc:dd:ee:ff (change to a valid MAC)
cd ../docsis
enable bpi true
enable force_cfgfile true
dhcp_settings
```

```
My IP Address: [10.10.10.10] <press return>
Subnet Mask: [255.255.255.0] <press return>
Router IP Address: [10.10.10.254] <press return>
```

Those are the only 3 that really need to be changed. Do you want to change the other settings? [no] Y

```
TFTP Server IP Address: [10.10.10.254] <type in the IP of your area's TFTP server here>
```

```
Config file name: [cm.bin] cmreg-ntlhm120-bund03.cm
Time Server IP Address: [10.10.10.254] <press return>
SysLog Server IP Address: [10.10.10.254] <press return>
```

```
cd ../snmp
max_dload_tries 0
docsDevSwAdminStatus 3
write
```

Note that you can find your TFTP IP from using DHCP Force or most other MAC sniffers.

That should be it, reboot the modem and reconnect the cable feed and all should be well. You can change the MAC address again using Blackcat or by repeating the steps from **Net booting a shelled firmware**.

All the best,
Boltar.

15. Webstar DPC2100, EPC2100

All screenshots and text were compiled by
Watsy1612 (of Digitalworldz)



This guide will teach u how to clone a Webstar modem I have done much research into this. Most of the guide I made myself and other bits I found on and around the internet. But this will work 100% and it's real easy.

1) Identifying your modem:

The Webstar epc2100 & dpc2100 is practically the same as the sb5100. You could have a DPC version or an EPC version they are both exactly the same, but the way you open them is different and the boards are slightly different!

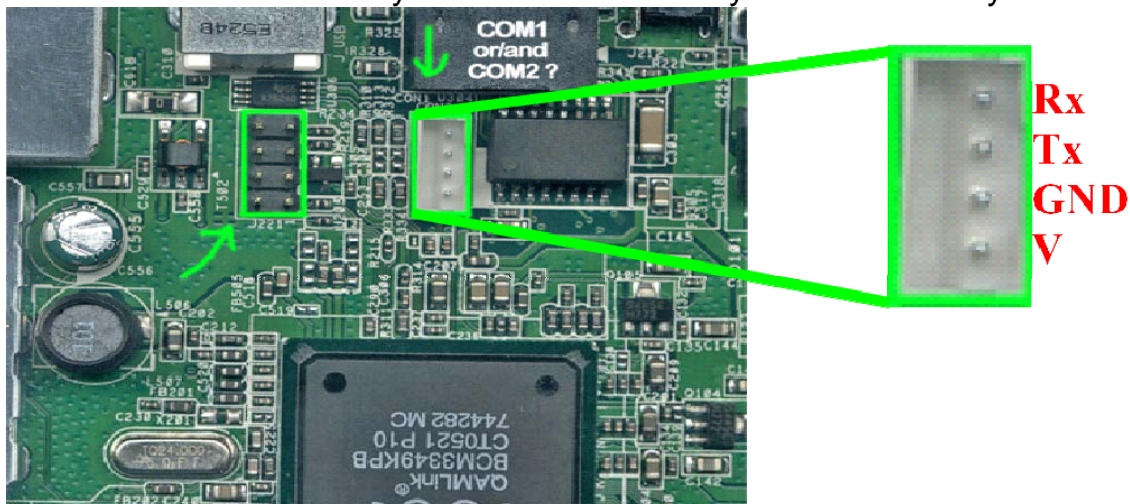


On the left EPC, on the right DPC

2) Opening the Modem:

- a. Using a sharp knife to remove the foot pads
- b. This will reveal two, t-10 screws which need removing
- c. Examine the outline of the case to see two small notches on the underneath, where you can insert a small flat headed screwdriver to pop the case off.

You should now have something that looks like below, this is still the same for both modems and it's only the white connector you need to worry about.



Lye the modem down flat so the Broadcom writing on the big Broadcom chip is upside down, then start at the top of the white connector.

Pin 1 = Rx

Pin 2 = Tx

Pin 3 = GND

Pin 4 = V

NOTE: You can also just buy a console cable and connect it straight in to the white connector on the board. The easiest way is to get an rs232 board and a 4 pin console cable, but if you cannot get a console cable simply attach a sound cable from the back of a CD/DVD drive to your max232 board to the four pins at the end, it's that easy.

- 3) Connect the console cable to the white connector and make sure the power to your modem is off. Then start hyper terminal which can be done by going to:

Start → All Programs → Accessories → Communications → Hyper Terminal.

When it loads, do the following:

- a. Enter **any number** in the area code box
- b. Click **OK** to the accept default modem settings
- c. Click **OK** on the next screen again
- d. It'll popup with a box saying new connection, call it **Webstar** & click **OK**
- e. Select your com port and click **OK**
- f. Enter the port settings as shown and click **OK**:

Bits per Second = **115200**
Data bits = **8**
Parity = **NONE**
Stop Bits = **1**
Flow Control = **Hardware**

- 4) Once your console cable is connected and your hyper terminal is communicating to the modem, as long as you have done all of the above, then you should start to see messages in your console window.

You will be asked to press 1, 2, or p before the request disappears,

Type: **p**

This will halt the boot process and will display the modems console menu like below:

Note: If it does not, disconnect power to the modem, and connect again, making sure you press p in time (you only have a second or so to do this!)

Main menu

D) Download and save to flash

G) Download and run from ram

- C) Store iceProm Bootloader to flash
- B) Boot from flash
- E) Erase Flash Sector
- M) Set mode
- S) Store Bootloader Parameters to flash
- I) RE-init Ethernet
- R) Read Memory
- W) Write Memory

5) Before doing anything else in Hyper Terminal, we need to set up TFTP. Start TFTP, click on settings, and change the output directory to the directory for the firmware image.

6) Not go back to Hyper Terminal and hit the magic D button on your keyboard.

NOTE: Some of them I have done, have flashed the modem straight away, others ask you to put the TFTP server IP in but it's real easy and the instructions are on screen.

7) Wait about **20-25 minutes** depending on your setup.

8) Hurray, you have a Webstar modem running on ambit 250 firmware. Just go to: <http://192.168.100.1> in your internet browser and change the MAC, then restart and away you go.

16. Baseline Privacy (BPI) Hack

This text was compiled by

Koevoet



In some areas, NTL are initializing baseline privacy (BPI), this is the first steps for the CC`s to attempt to stop the cloning business, if your modem locks on a d/s freq, but will not come online, have a look on the main page (of <http://192.168.100.1>) to see if it says baseline privacy skipped or enabled.

If BPI is enabled, then you will have to telnet to the modem and apply these commands to disable it, this will allow you to come online, bear in mind this may not be the cause as some clones do still come online even with bpi enabled!

You'll need to Telnet to your modem and enter the following commands:

```
cd /non-vol/docsis
enable bpi false
write
cd /
reset
```

To get into Telnet:

- 1) Goto the **start** menu and select **Run**
- 2) Type: **telnet** & press **Enter** (A telnet window should now pop up)

And that's it your done.

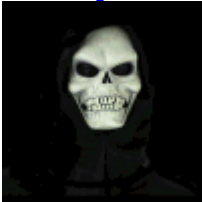
NOTE: If for any reason this does not work, you can also do it this way:

- 1) Goto the **start** menu and select **Run**
- 2) Type: **cmd** & press **Enter** (A new dos window should pop up)
- 3) In the dos window, type: **telnet** & press **Enter**

17. Directly install SB5000 Series modems to PC and run off PC PSU

Here's how you can directly install the SB5000 series modems to your PC and run it off the PC's PSU.

The following screen shots and text were put together by [Granty](#)



First thing is to open the case and find space to fix the surfboard.

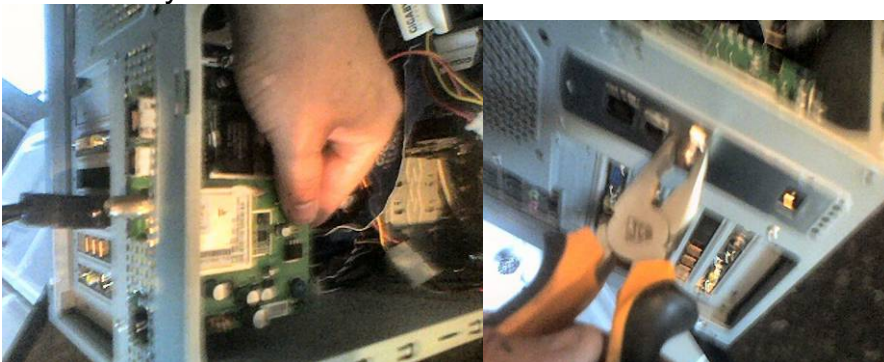
Open the SB and remove from its case.

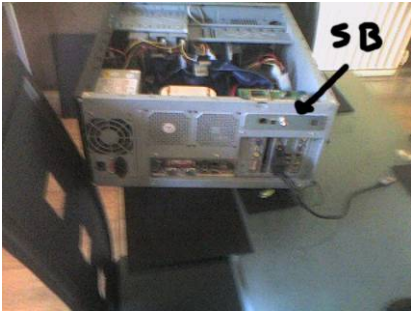
Remove the nut that's attached to the coax feed and remove the metal plate.

Now line up the SB from inside, making sure that plenty of air can circulate around it, and that it will not touch any of the electrical parts of the PC, and mark out where you need to remove the metal (I used a small pair of snips)...



Once this has been done, be very careful that NONE of the metal falls into the PC. Now just fix the backing plate over the hold you make with the modem in place, fastened by the nut:





Once this is done, it should look like this, or as near as. You can just use the power adapter that came with the surfboard, and if you want to do this, you are now done!

BUT!

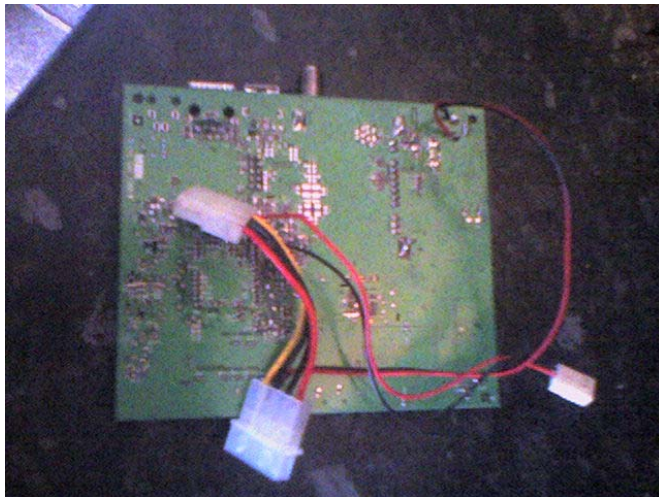
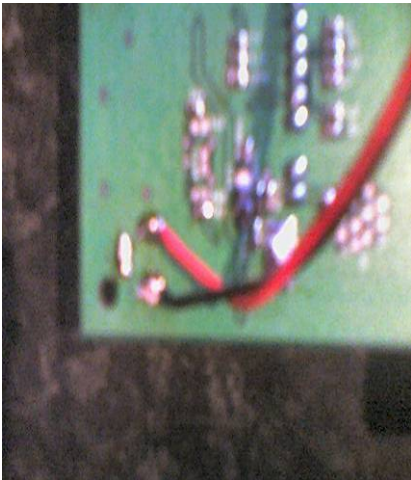
What I did was to solder a spare adapter I had to the power supply of the Surfboard, and connect it to my power supply from the PC:

Yellow = 12V

Black = 0V (Negative)

Note: red wire from picture on the left, leads to the yellow wire on the Molex connector in the picture on the right.

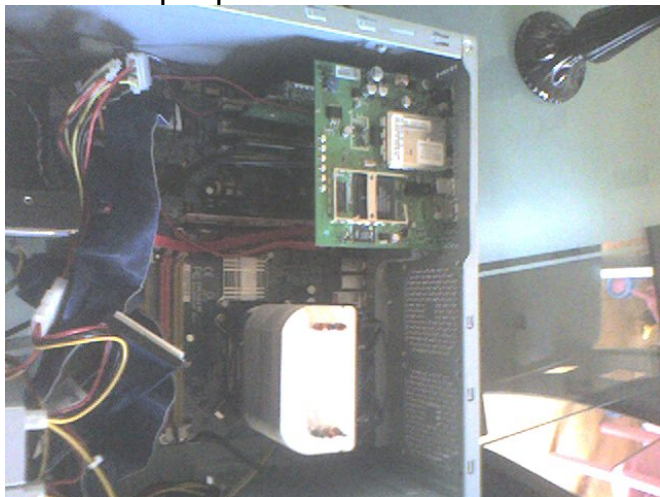
This would free up a valuable socket space, and do away with the SB transformer



Picture showing internal power (Green Lights)



More sample pictures below:



Regards, Granty.

18. Secret MIB's & Secret way to upgrade cable modem via BITFILE

The following text was compiled by
Dshocker (of TCNISO)



Look down at the bottom you will see secret MIB's for the modems.
Like getting and setting your modem cert... Dshocker

Well here it is everything you will need for you're modem
You can upgrade modem firmware do what ever, Read the Read me.
Under this text because if you don't I will not help you.
Hope you have fun
Dshocker

PS: for each modem if you wanna use it on Sb5100.
You name the bitfile SB5100.bit SB4100, SB4100.bit, SBG900,
SBG900.bit etc...

Officially Released by Dshocker

18a. Factory Mode

Before I talk about bit files I should explain what factory mode is:

Factory mode, when enabled, gives you access via SNMP to the factory MIB.
The factory MIB is a list of OID's, each OID having a unique function.
Here is a very small list of things you can do remote via SNMP when in, factory mode,

- get/set the HFC, Ethernet and USB MAC addresses.
- get/set the modem serial number.
- get/set the modem cert.'s (cm, vendor, and secure code).
- ping IP address'.
- execute shell commands
- execute injected code (see cmFactoryBCMGroup 'CommandType, AddressOrOpcode, ByteCount and Data')

18b. Bit Files

The bit file method works on firmware 0.4.5.0 and up on SB3100, SB4100, SB4101
And, SB4200.

And on any SB5100, SB5101 and SBG900.

The bitfile method works like this.

1) Using SNMP you set the OID 1.3.6.1.4.1.1166.1.19.3.1.18.0 to the interger.

The value of your HFC MAC address. (Calc.exe)

- 2) The modem then TFTP gets a 'bitfile' from 192.168.100.10
4100 modem will TFTP get SB4100.bit, and 4200 modem will TFTP get SB4200.bit
- 3) If the bit file is the correct size and contains the exact sequence of, bytes, then factory mode is enabled and the modem reboots!
- 4) When the modem reboots you have full access to all the factory MIB and OID's, within it.

NOTE: Factory mode will stay enabled until you turn it off by setting 1.3.6.1.4.1.1166.1.19.4.29.0 to integer 1 and reboot the modem!

Sorry no source code for you :P - a compiled bitfile is in the rar.

18c. Enable Factory MIB

This tutorial will show you how to enable the factory MIB on a modem and change the MAC and serial, via SNMP

- 1) Put the .bit file into your TFTP server's directory.
- 2) Use SNMP to set the OID 1.3.6.1.4.1.1166.1.19.3.1.18.0 to the decimal of your HFC MAC address
Example: `snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.3.1.18.0 i 12345678`
The modem will now get the bit file and if it's correct it will enable factory mode and reboot!
Once the modem is rebooted....
- 3) You can now set the OID 1.3.6.1.4.1.1166.1.19.4.3.0 to your NEW ETHERNET MAC address
Example: `snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.3.0 s "12:34:56:78:9a:00"`
- 4) You can now set the OID 1.3.6.1.4.1.1166.1.19.4.4.0 to your NEW HFC MAC address.
Example: `snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.4.0 s "12:34:56:78:9a:0a"`
- 5) You can now set the OID 1.3.6.1.4.1.1166.1.19.4.6.0 to your NEW SERIAL NUMBER.
Example: `snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.6.0 s "12345678901234567890"`

- 6) To finish up disable the factory MIB by setting the OID
1.3.6.1.4.1.1166.1.19.4.29.0 to int 1
Example: snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.29.0 i

Now reboot your modem and all is done.

18d. Factory mode OID list for Motorola cable modems

AKA FACTORY MIB's for Factory mode

This list is generic among Motorola cable modems

SB3100, SB4100, SB4101, SB4200, SB4220, SB5100, SB5101, SBG900 and probably more, HOWEVER some OID's will not exist on some modems, E.g.

(cmFactoryBCMGroup oid's)

To execute code, only exist in SB5100, SB5101 and SBG900)

cmPrivateArpFilterGroup

1.3.6.1.4.1.1166.1.19.2

1.3.6.1.4.1.1166.1.19.2.1.0 cmArpFilterEnabled

1.3.6.1.4.1.1166.1.19.2.2.0 cmArpFilterInterval

1.3.6.1.4.1.1166.1.19.2.3.0 cmArpFilterLimit

1.3.6.1.4.1.1166.1.19.2.4.0 cmArpFilterInArps

1.3.6.1.4.1.1166.1.19.2.5.0 cmArpFilterOutArps

1.3.6.1.4.1.1166.1.19.2.6.0 cmArpFilterInArpsThisFilter

cmConfigPrivateBaseGroup

1.3.6.1.4.1.1166.1.19.3

cmConfigFreqObjectsGroup

1.3.6.1.4.1.1166.1.19.3.1

1.3.6.1.4.1.1166.1.19.3.1.1.0 cmConfigFreq1

1.3.6.1.4.1.1166.1.19.3.1.2.0 cmConfigFreq2

1.3.6.1.4.1.1166.1.19.3.1.3.0 cmConfigFreq3

1.3.6.1.4.1.1166.1.19.3.1.8.0 cmFreqPlanType

1.3.6.1.4.1.1166.1.19.3.1.11.0 cmUpstreamChannelId1

1.3.6.1.4.1.1166.1.19.3.1.12.0 cmCarrierFrequencyOffset

1.3.6.1.4.1.1166.1.19.3.1.14.0 cmSnmpHFCTPort

1.3.6.1.4.1.1166.1.19.3.1.15.0 cmSnmpHFCTrapPort

1.3.6.1.4.1.1166.1.19.3.1.17.0 cmSnmpDisplayHtml

1.3.6.1.4.1.1166.1.19.3.1.18.0 cmResetToDefaults

1.3.6.1.4.1.1166.1.19.3.1.19.0 cmStandbyMode

1.3.6.1.4.1.1166.1.19.3.1.20.0 cmHybridMode

1.3.6.1.4.1.1166.1.19.3.1.21.0 cmUpstreamChannelId3

1.3.6.1.4.1.1166.1.19.3.1.22.0 cmUpstreamPower1

1.3.6.1.4.1.1166.1.19.3.1.23.0 cmUpstreamPower2

1.3.6.1.4.1.1166.1.19.3.1.24.0 cmUpstreamPower3

1.3.6.1.4.1.1166.1.19.3.1.25.0 cmDocsis20Capable

1.3.6.1.4.1.1166.1.19.3.1.26.0 cmUpstreamChannelId2

cmPrivateFactoryGroup	
1.3.6.1.4.1.1166.1.19.4	
1.3.6.1.4.1.1166.1.19.4.1.0	cmFactoryVersion
1.3.6.1.4.1.1166.1.19.4.2.0	cmFactoryDbgBootEnable
1.3.6.1.4.1.1166.1.19.4.3.0	cmFactoryEnetMacAddr
1.3.6.1.4.1.1166.1.19.4.4.0	cmFactoryHfcMacAddr
1.3.6.1.4.1.1166.1.19.4.6.0	cmFactorySerialNumber
1.3.6.1.4.1.1166.1.19.4.9.0	cmFactoryClearFreq1
1.3.6.1.4.1.1166.1.19.4.10.0	cmFactoryClearFreq2
1.3.6.1.4.1.1166.1.19.4.11.0	cmFactoryClearFreq3
1.3.6.1.4.1.1166.1.19.4.12.0	cmFactorySetReset
1.3.6.1.4.1.1166.1.19.4.13.0	cmFactoryClrConfigAndLog
1.3.6.1.4.1.1166.1.19.4.14.0	cmFactoryPingIpAddr
1.3.6.1.4.1.1166.1.19.4.15.0	cmFactoryPingNumPkts
1.3.6.1.4.1.1166.1.19.4.16.0	cmFactoryPingNow
1.3.6.1.4.1.1166.1.19.4.17.0	cmFactoryPingCount
1.3.6.1.4.1.1166.1.19.4.28.0	cmFactoryCliFlag
1.3.6.1.4.1.1166.1.19.4.29.0	cmFactoryDisableMib
1.3.6.1.4.1.1166.1.19.4.30.0	cmFactoryUpstreamPowerCalibration1
1.3.6.1.4.1.1166.1.19.4.50.0	cmFactoryBigRSAPublicKey
1.3.6.1.4.1.1166.1.19.4.51.0	cmFactoryBigRSAPrivateKey
1.3.6.1.4.1.1166.1.19.4.52.0	cmFactoryCMCertificate
1.3.6.1.4.1.1166.1.19.4.53.0	cmFactoryManCertificate
1.3.6.1.4.1.1166.1.19.4.54.0	cmFactoryRootPublicKey
1.3.6.1.4.1.1166.1.19.4.55.0	cmFactoryCodeSigningTime
1.3.6.1.4.1.1166.1.19.4.56.0	cmFactoryCVCCValidityStartTime
1.3.6.1.4.1.1166.1.19.4.58.0	cmFactoryCMManufacturerName
1.3.6.1.4.1.1166.1.19.4.59.0	cmFactoryHtmlReadOnly
1.3.6.1.4.1.1166.1.19.4.60.0	cmFactoryCmUsbMacAddr
1.3.6.1.4.1.1166.1.19.4.61.0	cmFactoryCpeUsbMacAddr
1.3.6.1.4.1.1166.1.19.4.62.0	cmFactoryCmAuxMacAddr
1.3.6.1.4.1.1166.1.19.4.63.0	cmFactoryTunerId
1.3.6.1.4.1.1166.1.19.4.64.0	cmFactoryHwRevision
1.3.6.1.4.1.1166.1.19.4.65.0	cmFactoryUsAmpld
1.3.6.1.4.1.1166.1.19.4.66.0	cmFactory80211RegDomain
1.3.6.1.4.1.1166.1.19.4.67.0	cmFactoryResidentialGatewayEnable
1.3.6.1.4.1.1166.1.19.4.70.0	cmFactoryFWFeatureID
1.3.6.1.4.1.1166.1.19.4.90.0	cmFactorySwServer
1.3.6.1.4.1.1166.1.19.4.91.0	cmFactorySwFilename
1.3.6.1.4.1.1166.1.19.4.92.0	cmFactorySwDownloadNow
1.3.6.1.4.1.1166.1.19.4.93.0	cmFactoryGwAppPublicKey
1.3.6.1.4.1.1166.1.19.4.94.0	cmFactoryGwAppPrivateKey
1.3.6.1.4.1.1166.1.19.4.95.0	cmFactoryGwAppRootPublicKey
1.3.6.1.4.1.1166.1.19.4.31	cmFactoryDownstreamCalibrationGroup

1.3.6.1.4.1.1166.1.19.4.31.1.0 cmFactorySuspendStartup
1.3.6.1.4.1.1166.1.19.4.31.2.0 cmFactoryDownstreamFrequency
1.3.6.1.4.1.1166.1.19.4.31.3.0 cmFactoryDownstreamAcquire
1.3.6.1.4.1.1166.1.19.4.31.4.0 cmFactoryTunerAGC
1.3.6.1.4.1.1166.1.19.4.31.5.0 cmFactoryIfAGC
1.3.6.1.4.1.1166.1.19.4.31.6.0 cmFactoryQamLock
1.3.6.1.4.1.1166.1.19.4.31.7.0 cmFactoryDownstreamCalibrationTableMaxSum
1.3.6.1.4.1.1166.1.19.4.31.8.0 cmFactoryDownstreamCalibrationTableMinSum
1.3.6.1.4.1.1166.1.19.4.31.9.0 cmFactoryTop
1.3.6.1.4.1.1166.1.19.4.31.10.0 cmFactoryDownstreamCalibrationOffset
1.3.6.1.4.1.1166.1.19.4.31.100 cmFactoryCalibrationEntry
1.3.6.1.4.1.1166.1.19.4.31.100.1.1 cmFrequencyCalibrationIndex
1.3.6.1.4.1.1166.1.19.4.31.100.1.2 cmFactoryCalibrationFrequencyData

cmFactoryBCMGroup

1.3.6.1.4.1.1166.1.19.4.32
1.3.6.1.4.1.1166.1.19.4.32.1.0 cmFactoryBCMCommandType
1.3.6.1.4.1.1166.1.19.4.32.2.0 cmFactoryBCMAddressOrOpcode
1.3.6.1.4.1.1166.1.19.4.32.3.0 cmFactoryBCMByteCount
1.3.6.1.4.1.1166.1.19.4.32.4.0 cmFactoryBCMData

cmRegPrivateGroup

1.3.6.1.4.1.1166.1.19.5

cmStatsGroup

1.3.6.1.4.1.1166.1.19.9

cmStatsObjectsGroup

1.3.6.1.4.1.1166.1.19.9.1
1.3.6.1.4.1.1166.1.19.9.1.5.0 cmResetIfCmStatusCounters
1.3.6.1.4.1.1166.1.19.9.1.6.0 cmResetCMSignalQualityCounters
1.3.6.1.4.1.1166.1.19.9.1.7.0 cmQam256PowerFactorTableVersion

cmTftpConfigPrivateGroup

1.3.6.1.4.1.1166.1.19.6
1.3.6.1.4.1.1166.1.19.6.1
1.3.6.1.4.1.1166.1.19.6.1.1.1 cmCfgClassId
1.3.6.1.4.1.1166.1.19.6.1.1.2 cmCfgMaxDsRate
1.3.6.1.4.1.1166.1.19.6.1.1.3 cmCfgMaxUsRate
1.3.6.1.4.1.1166.1.19.6.1.1.4 cmCfgUsChannelPriority
1.3.6.1.4.1.1166.1.19.6.1.1.5 cmCfgMinUsDataRate
1.3.6.1.4.1.1166.1.19.6.1.1.6 cmCfgMaxUsChannelXmitBurst
1.3.6.1.4.1.1166.1.19.6.1.1.7 cmCfgCovPrivacyEnable

cmCfgBpiTimeOutGroup

1.3.6.1.4.1.1166.1.19.6.2

1.3.6.1.4.1.1166.1.19.6.2.1.0 cmCfgAuthorWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.2.0 cmCfgReauthorWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.3.0 cmCfgAuthorGraceTime
1.3.6.1.4.1.1166.1.19.6.2.4.0 cmCfgOperWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.5.0 cmCfgRekeyWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.6.0 cmCfgTekGraceTime
1.3.6.1.4.1.1166.1.19.6.2.7.0 cmCfgAuthorRejectWaitTimeOut

cmOtherConfigGroup

1.3.6.1.4.1.1166.1.19.6.3
1.3.6.1.4.1.1166.1.19.6.3.1.0 cmCfgDsFreq
1.3.6.1.4.1.1166.1.19.6.3.2.0 cmCfgUsChannelId
1.3.6.1.4.1.1166.1.19.6.3.3.0 cmCfgNetAccessCtrl
1.3.6.1.4.1.1166.1.19.6.3.4.0 cmCfgSoftUpgradeFile
1.3.6.1.4.1.1166.1.19.6.3.5.0 cmCfgTotalSnmpWriteAccessCtrl
1.3.6.1.4.1.1166.1.19.6.3.6.0 cmCfgTotalSnmpMibObj
1.3.6.1.4.1.1166.1.19.6.3.7.0 cmCfgVendorId
1.3.6.1.4.1.1166.1.19.6.3.8.0 cmCfgVendorSpecific
1.3.6.1.4.1.1166.1.19.6.3.9.0 cmCfgModemCapabilities
1.3.6.1.4.1.1166.1.19.6.3.10.0 cmCfgModemIp
1.3.6.1.4.1.1166.1.19.6.3.11.0 cmCfgTotalEthernetMacAdrs
1.3.6.1.4.1.1166.1.19.6.3.12.0 cmCfgEthernetMacAdrs
1.3.6.1.4.1.1166.1.19.6.3.13.0 cmCfgTelcoSetting
1.3.6.1.4.1.1166.1.19.6.3.14.0 cmCfgSnmplpAddr
1.3.6.1.4.1.1166.1.19.6.3.15.0 cmCfgMaxCpe
1.3.6.1.4.1.1166.1.19.6.3.16.0 cmCfgTftpServerTimeStamp
1.3.6.1.4.1.1166.1.19.6.3.17.0 cmCfgTftpServerProvModAddr
1.3.6.1.4.1.1166.1.19.6.3.18.0 cmCfgUuFlashParms
1.3.6.1.4.1.1166.1.19.6.3.19.0 cmCfgMulticastPromiscuous
1.3.6.1.4.1.1166.1.19.6.3.20.0

cmDhcpGroup

1.3.6.1.4.1.1166.1.19.10

cmDhcpObjectsGroup

1.3.6.1.4.1.1166.1.19.10.1

1.3.6.1.4.1.1166.1.21.1 cmTrapObjectValueChange
1.3.6.1.4.1.1166.1.21.62.1 ?
1.3.6.1.4.1.1166.1.21.62.2 ?
1.3.6.1.4.1.1166.1.21.62.3 ?
1.3.6.1.4.1.1166.1.21.62.4 ?
1.3.6.1.4.1.1166.1.21.2 cmTrapLog
1.3.6.1.4.1.1166.1.21.62.5 ?
1.3.6.1.4.1.1166.1.21.62.6

Links

Well it looks like were at the end, I hope some of the above has helped you on your way to cloning, whatever modem it is you've got. Hopefully everybody that needs to be mentioned has been if theirs anybody I've left out, apologies. I'll try to keep the tutorial updated whenever anything new happens on the scene.

If you have a problem with the any of the above tutorials you will find any of the following web sites a great resource of information.

www.unlocker-forums.co.uk

www.digi-city.co.uk

www.digidudez-forums.co.uk

www.hackable.co.uk

www.digitalworldz.co.uk

www.wizardmods.co.uk

www.datacave.co.uk

www.all-forums.co.uk/forum

www.surfboardhacker.net

www.fibercoax.net

www.tcniso.net

Cheers

Cableguy69

