Zyxel LTE3202-M437

Ce modem 4G LTE fourni par Free dans le cadre de son offre Free-pro de modèle Zyxel LTE3202-M437 avec une SIM permettant de faire du failover de l'accès Fibre contient un configuration custom.

Son interface Web à un accès restreint avec des identifiants custom dont seul Free a connaissance. Free dans ses procédures, peut avoir accès directement à cette interface Web lorsque cette dernière est branchée en RJ45 sur le routeur Fibre. ::smiley_qui_sourit_bêtement::

Mon cas

Le réseau Free ne passant pas du tout dans ma zone, le service failover est donc quasiment inéxistant.

De plus ça ne donne que accès à internet en sortant sur une IP partagée, donc tchao les service hébergé derrière la fibre.

J'ai donc essayé ce routeur avec une autre SIM d'un autre provider.

Il faut penser à enlever le code PIN de la carte SIM, et à reset le boîtier, ça fini par fonctionner avec un peu de bol.

Cependant on accède toujours pas à l'interface Web, et le code Wifi par défaut ne peux être changé.

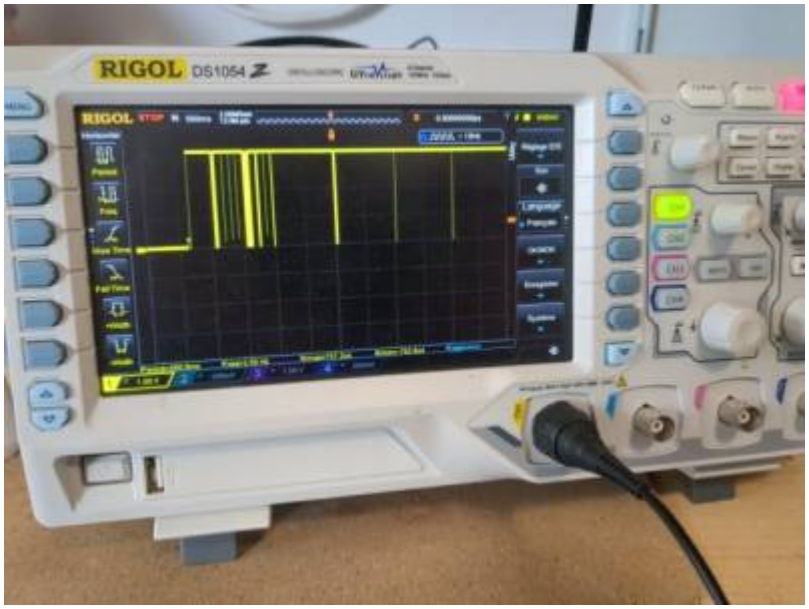
On va donc chercher à avoir la main un minimum sur cet équipement.

Seek the serial port

On va chercher le port Série sur le PCB de l'équipement.

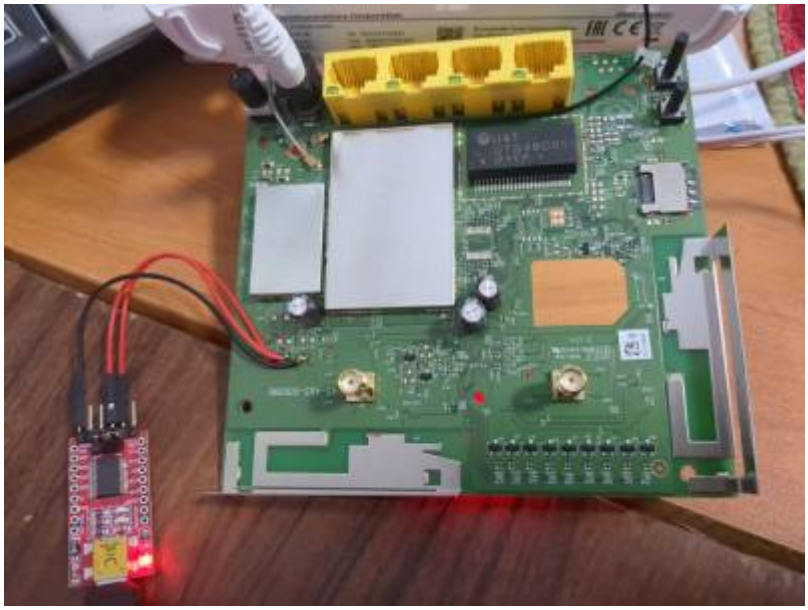
En testant avec un oscillo pour être sûr d'avoir le bon signal sur des points-test, on arrive à voir des choses qui bougent lors de l'allumage de l'appareil. On cherche une masse commune, et on test... et zou.

A l'aide de l'échelle et des bases de temps on peut déterminer le baudrate, ou demander gentillement à la fonction analyseur logique de l'oscillo.



Ici on est sur un mode classique soit : **8N1 à 115200**.

On soude et on test avec un terminal



Un patte pour le RX, une pour le TX, et une pour la masse.
Inverser les pattes RX et TX si jamais ça marche pas ;) et zou

```
U-Boot 1.1.3 (May 29 2020 - 10:46:18)

Board: Ralink APSoC DRAM:  128 MB
relocate_code Pointer at: 87fa0000
enable ephy clock...done. rf reg 29 = 5
SSC disabled.
!!! nand page size = 2048, addr len=4
....============================================
Ralink UBoot Version: 5.0.0.0
--------------------------------------------
ASIC 7620_MP (Port5<->None)
DRAM_CONF_FROM: Auto-detection
DRAM_TYPE: DDR2
DRAM component: 1024 Mbits
DRAM bus: 16 bit
Total memory: 128 MBytes
Flash component: NAND Flash
Date:May 29 2020  Time:10:46:18
============================================
icache: sets:512, ways:4, linesz:32 ,total:65536
dcache: sets:256, ways:4, linesz:32 ,total:32768

 ##### The CPU freq = 580 MHZ ####
 estimate memory size =128 Mbytes
.## Starting application at 0x81E00000 ...


Z-LOADER V2.05 | 05/29/2020 10:46:20


..Hit ESC key to stop autoboot: 1
```

Ensuite... on fait quoi avec le bootloader?

On peut laisser tourner le boot et voir ce qu'il en ressort... mais rien que du debug, beaucoup d'info mais pas de prompt... enfin si.

```
Please press Enter to activate this console.
LTE3202-M437 login: admin
Password:
Login incorrect
```

Mais je suis pas fan de bruteforce over serial, et puis lors du boot on a la ligne suivante qui semble intéressante :

```
..Hit ESC key to stop autoboot: 1
```

On reboot donc et on tente le coup du **echap** puis la commande **help**:

```
..Hit ESC key to stop autoboot: 1
ZLB> help
ATGO              boot up the whole system
ATGU              go back to U-Boot command line
ATNR    x,y       upgrade image by TFTP (x=type[1:ras, 2:bootloader,
3:config, 4:romd 6:factory], y=filename)
ATBT    x         block0 write enable (1=enable, 0=disable)
ATEN    x,(y)     set BootExtension Debug Flag (y=password)
ATSE    x         show the seed of password generator
ATWZ    a,(b,c,d) write MAC , Country code, EngDbgFlag, MAC Quantity to
FLASH
ATSH              dump manufacturer related data in FLASH
ATBU              dump manufacturer related data in working buffer
ATCB              copy FLASH MRD to working buffer
ATSN    x         set serial number to flash
ATSB              save working buffer to FLASH
ATQY    x         set MAC Quantity to working buffer
ATFL    x         set EngDebugFlag to working buffer
ATCO    x         set country code to working buffer
ATSR              reset
ATRT    (x,y,z,u) RAM read/write test (x=level, y=start addr, z=end addr,
u=interations)
ATRM              restore default MRD
ATBR              reset to default Romfile
ATER              erase ROM-D data
ATHV    x         set hardware version to flash
ATGP    x,y       led control
ATBS    x         set board serial number to flash
ZLB>
```

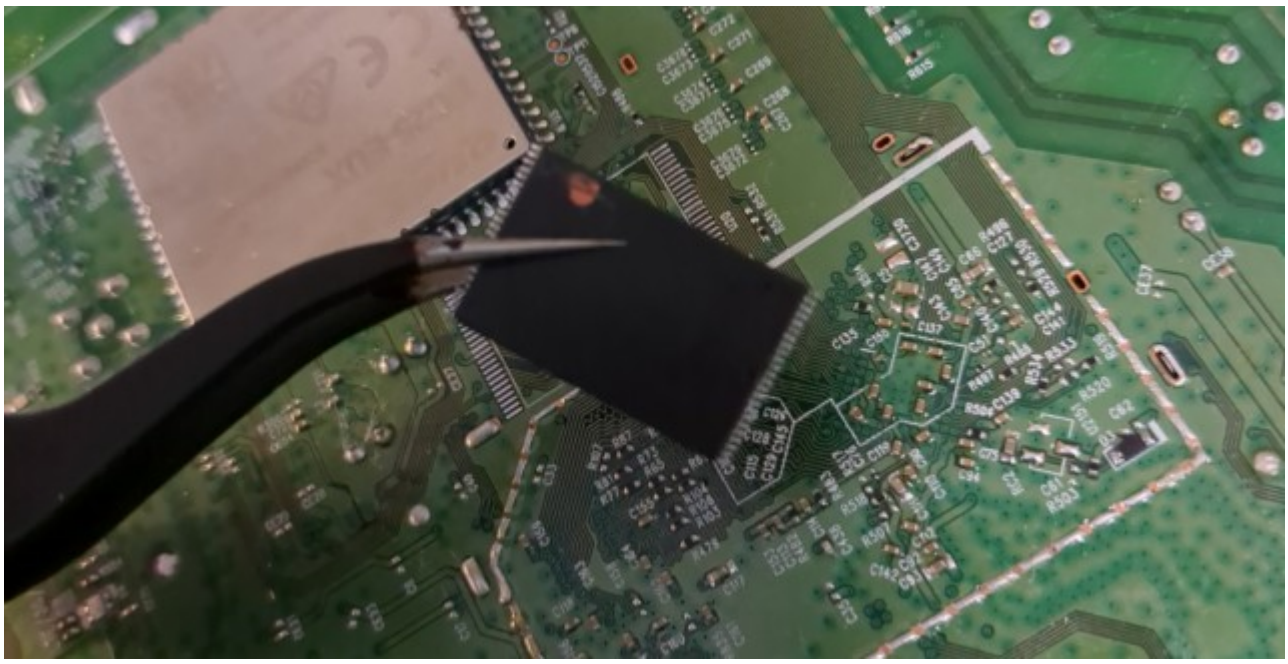
Et bien sûr nous avons des **Permission Denied** si on tente de un **ATGU** ou autre...
Bref c'est relou, je tente de voir si y'a pas une config de Jumpers pour désactiver le fameux Denid,

mais ça semble pas possible de manière phyisique.

On va jouer un peu

N'arrivant pas a trouver d'interfaçage JTAG ou SPI, je décide tout de même de voir ce qu'il y'a dans cette petite mémoire.
Je tente donc de déssouder cette puce au boîtier TSOP48, c'est tout petit et ça fait mal aux yeux.

On se retrouve face à une flash de type **TC58BVG0S3HTA00**



Saitsfait de mon déssoudage, on passe à la lecture de celle-ci.

Très mignon...

Annexe

https://spdl.zyxel.com/LTE3202-M430/user_guide/LTE3202-M430_V1.0.pdf
https://w.electrodragon.com/w/images/3/34/MT7620_Datasheet.pdf
https://www.manualslib.com/manual/1639995/Mediatek-Ralink-Mt7620.html

https://openwrt.org/docs/techref/hardware/soc/soc.mediatek

- Flash TC58BVG0S3HTA00 :
  https://pdf1.alldatasheet.com/datasheet-pdf/view/1312276/KIOXIA/TC58BVG0S3HTAI0.html