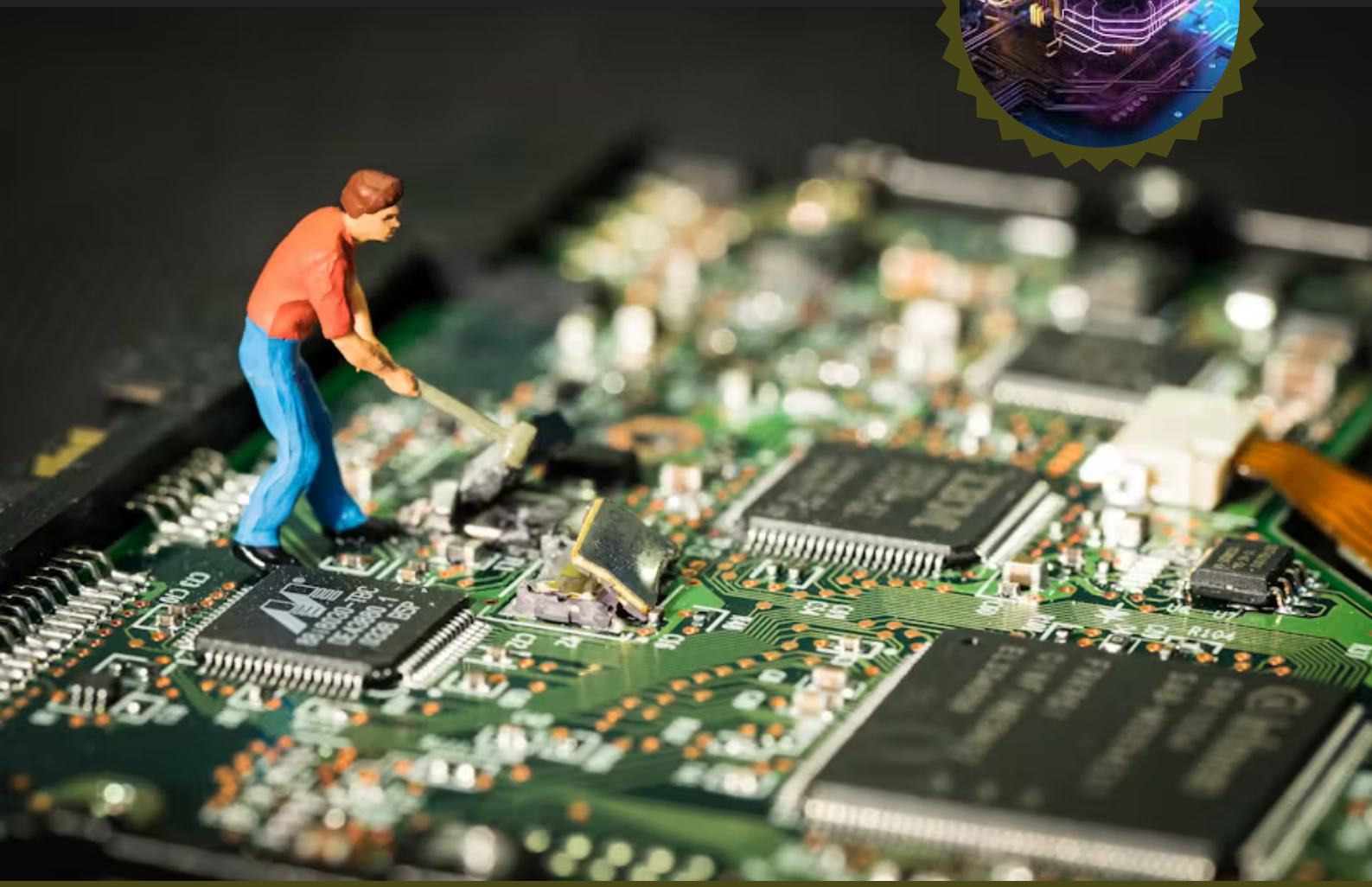
PROJET REVERSE ENGINEERING

ANALYSE DE CIRCUITS ÉLECTRONIQUES



Projet 9

Année 2024

Ramirez Aurélien

Confavreux Nathan

SOMMAIRE

01 - INTRODUCTION

Reverse engineering des circuits électroniques.
Au cours de ce projet, nous avons entrepris l'analyse de deux routeurs, le Huawei B315s-22 et le Zyxel ax1800, dans le but d'identifier leurs composants, d'analyser les signaux qu'ils émettent et de comprendre leur fonctionnement interne.
Initialement, notre projet a débuté avec le démontage du routeur 4G Huawei B315s-22. Nous avons désossé l'appareil, identifiant chaque composant et relevant les signaux émis. Cependant, notre progression a été interrompue lorsque la carte du routeur a subi un dysfonctionnement, la rendant inopérable. Cet incident a souligné les imprévus auxquels on peut faire fasse lors de ce genre de manipulation.
Nous avons donc opté pour l'analyse d'un deuxième routeur, le Zyxel. Nous avons donc réaliser les même opération que sur le Huawei puis après une identification des points de tests nous avons trouver un shell restreint nous empêchant d'accéder au firmware du routeur. Malgré cela, nous avons tenté de contourner ces restrictions pour pouvoir extraire et analyser le firmware, afin de mieux comprendre le fonctionnement interne du dispositif.

Ce rapport documente notre analyse à travers ces deux routeur:

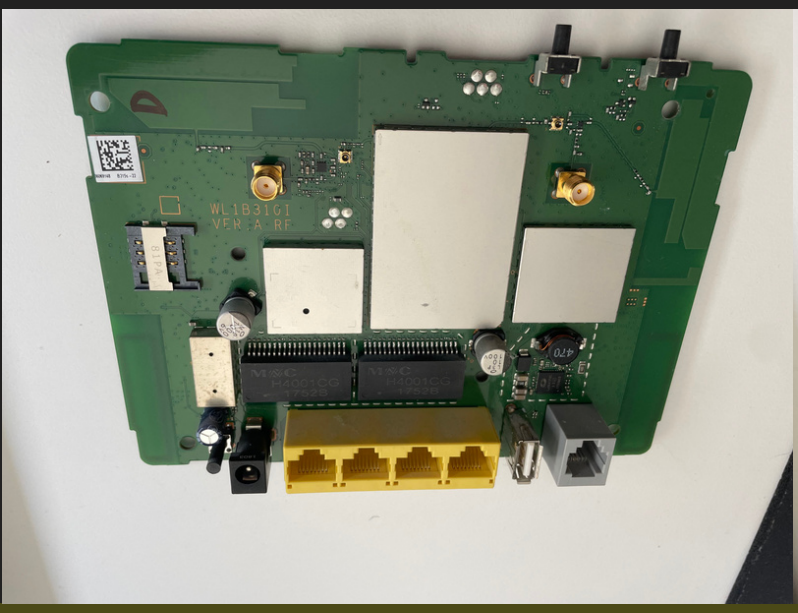
02 - IDENTIFICATION DES COMPOSANTS

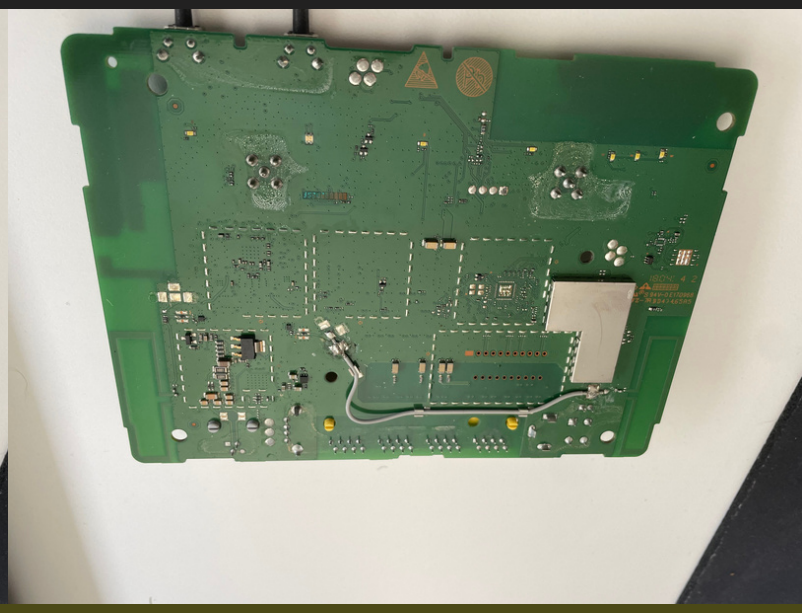
Huawei b315s-22 :

FCC ID: QISB315S-22

Page fccid.io : https://fccid.io/QISB315S-22/User-Manual/UserManual-2936290

Démontage du routeur



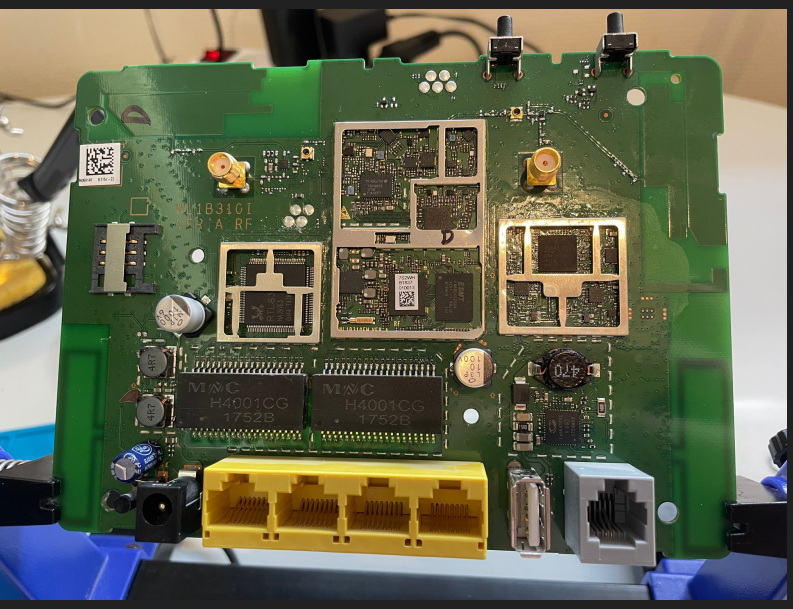


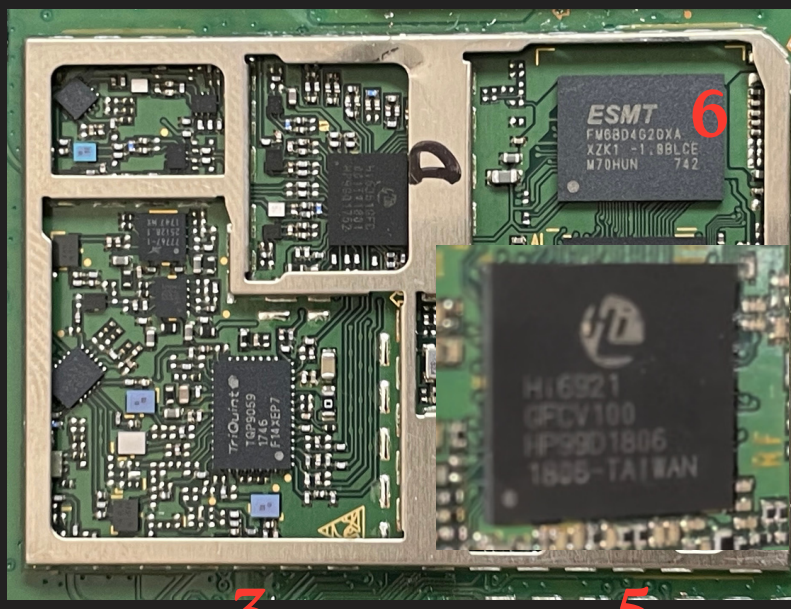
Projet 9

Année 2024

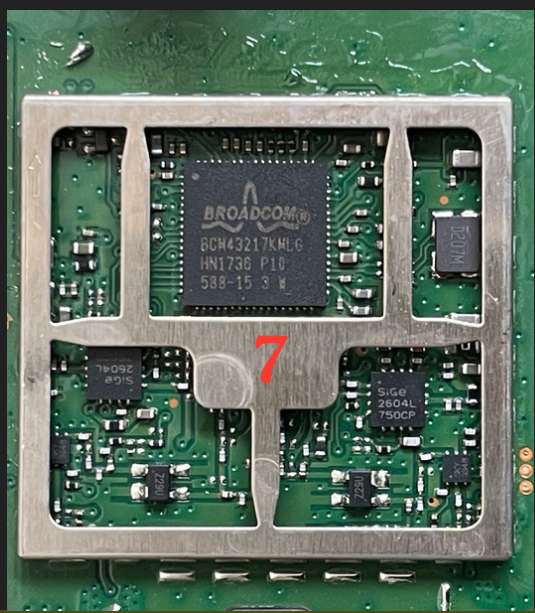
02 - IDENTIFICATION DES COMPOSANTS

Huawei b315s-22 :





Analyse des composants

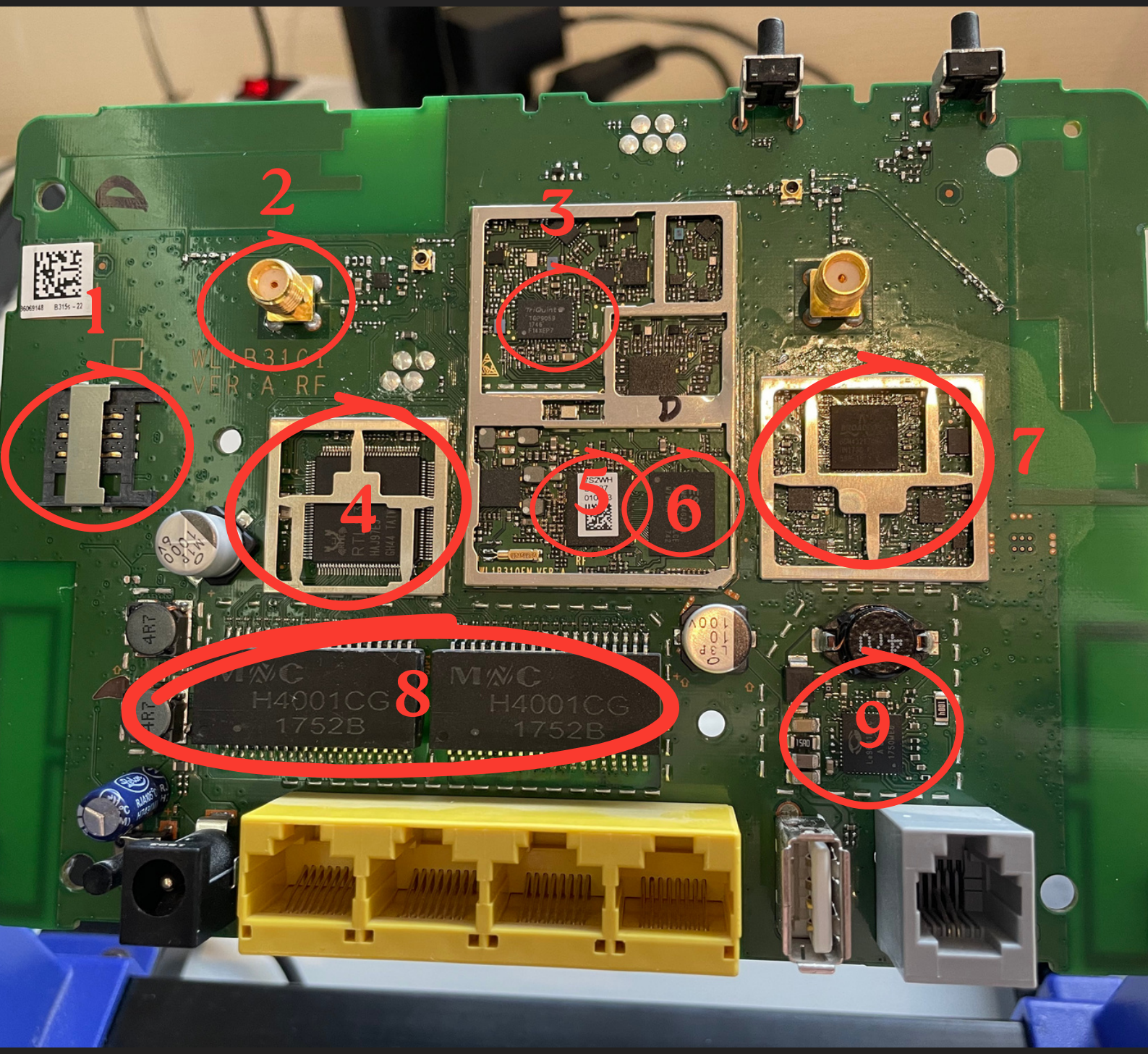


Projet 9

Année 2024

02 - IDENTIFICATION DES COMPOSANTS

Huawei b315s-22 :



02 - IDENTIFICATION DES COMPOSANTS

Huawei b315s-22 :

1- logement SIM

2- connecteur d'antenne

3-Le Triquint TQP9059 est un amplificateur de puissance RF (radiofréquence) utilisé dans les applications sans fil, telles que les réseaux de télécommunications, les dispositifs mobiles, les stations de base, etc., pour amplifier les signaux RF et améliorer la qualité et la portée des communications sans fil.

https://pdf1.alldatasheet.com/datasheet-pdf/download/691703/TRIQUINT/TQP9059.html

4- Le Realtek RTL8367SB-CG est un commutateur Ethernet géré qui est utilisé pour faciliter la communication au sein d'un réseau informatique.

https://www.alldatasheet.net/view.jsp?Searchword=RTL8367SB-CG

5-Le HI6921M est un amplificateur de ligne DSL hautement intégré conçu pour les passerelles résidentielles DSL, offrant une solution économique avec des performances élevées et une faible consommation d'énergie.

https://www.worldwayic.com/pro/hi/hi6921/4271667/hi6921.pdf

6-Le ESMT FM6BD4G2GXA-1.8BLC est une mémoire flash NAND utilisée pour le stockage de données dans divers appareils électroniques tels que les smartphones, les tablettes, les appareils photo numériques, etc.

https://www.alldatasheet.net/view.jsp?Searchword=FM6BD4G2GXA-1.8BLCGE2C

02 - IDENTIFICATION DES COMPOSANTS

Huawei b315s-22 :

7-Le Broadcom 8CH43217KMLG est un amplificateur de puissance RF (radiofréquence) utilisé dans les applications sans fil pour amplifier les signaux RF et améliorer la portée et la qualité des communications sans fil, notamment dans les routeurs

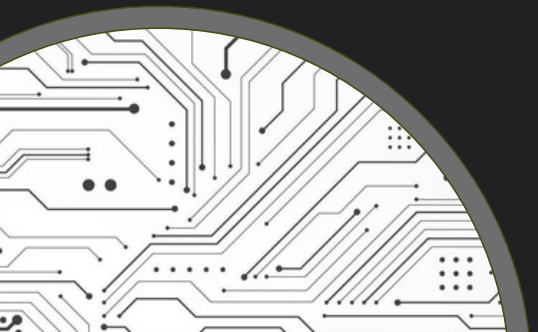
https://download.datasheets.com/pdfs/2011/9/18/6/24/57/689/avago_/manual/37_nods.pdf

8-Le H4001CG est un transformateur LAN 10/100 Base-T utilisé pour la transmission de données à des vitesses de 10/100 Mbps, avec des caractéristiques de montage en surface, une plage de température de fonctionnement de 0°C à 70°C et un rapport de tours primaire/secondaire de 1CT:1CT.

https://www.allelcoelec.fr/datasheets/d94/204742-H4001CG.pdf

9-Le LE9641PQC est un circuit d'interface de ligne abonné (SLIC) économique et économe en énergie, adapté aux applications vocales dérivées, offrant une fonctionnalité BORSCHT complète et des tests de ligne d'abonné complets.

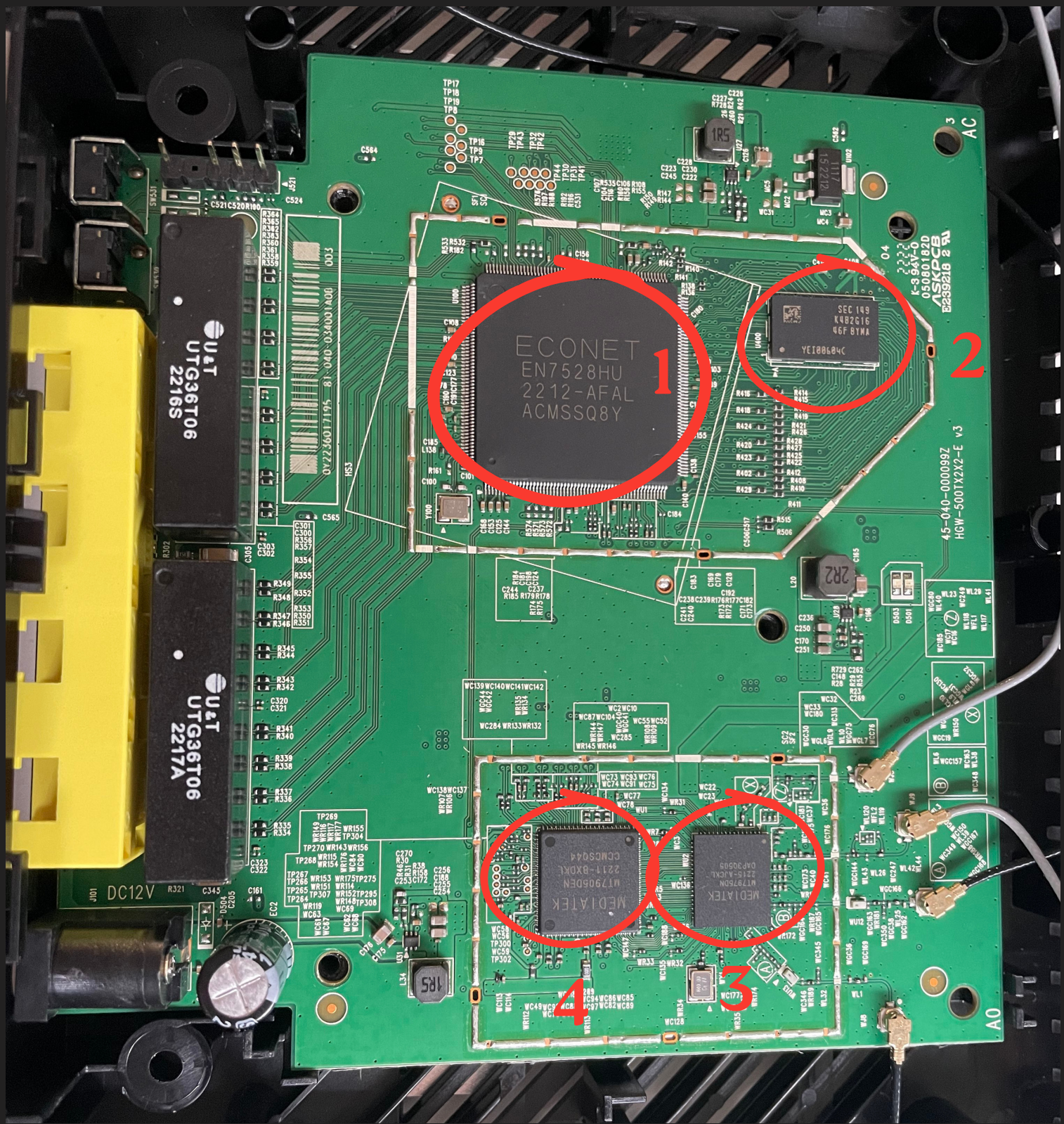
https://www.mouser.fr/datasheet/2/268/PB_Le9641_Sept_2014-1593958.pdf



02 - IDENTIFICATION DES COMPOSANTS

ZYXEL ax1800 :

FCC ID: I88WSM20



02 - IDENTIFICATION DES COMPOSANTS

ZYXEL ax1800 :

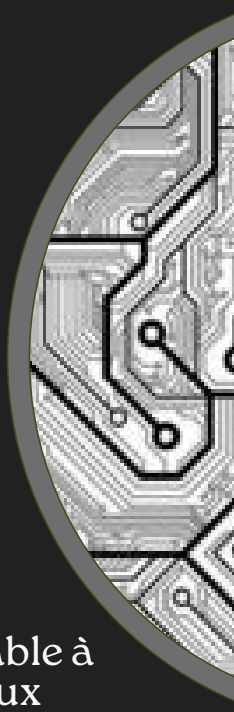
1

2

4

3

02 - IDENTIFICATION DES COMPOSANTS



ZYXEL ax1800 :

1- L'Econet EN7528HU est un commutateur Ethernet non administrable à huit ports, offrant une solution économique et simple pour les réseaux domestiques et les petites entreprises, avec des fonctionnalités de plug-and-play et une haute efficacité énergétique.

https://www.hkinventory.com/public/requestDataSheet.asp?partNum=EN7528HU&partNumInfo=Describe%3AIC+SMD+ROHS+LQFP216+216+PIN%2CBrand%3AEcoNet%2CProvided+Company+ID%3A37718&BrandName=EcoNetc

2- Le K4B2G16 est une puce de mémoire NAND Flash de 2 Gb fabriquée par Samsung, souvent utilisée dans les dispositifs de stockage de données tels que les SSD, les smartphones et les tablettes pour fournir une capacité de stockage élevée et des performances fiables.

https://www.alldatasheet.com/view.jsp?sField=0&Searchword=K4B2G16&list=133

3-
Le MEDIATEK MT7975DN est un processeur conçu par MediaTek, souvent utilisé dans les dispositifs mobiles et les appareils intelligents pour offrir des performances informatiques efficaces et des fonctionnalités avancées telles que la connectivité 5G, le traitement d'image et la gestion de l'énergie.

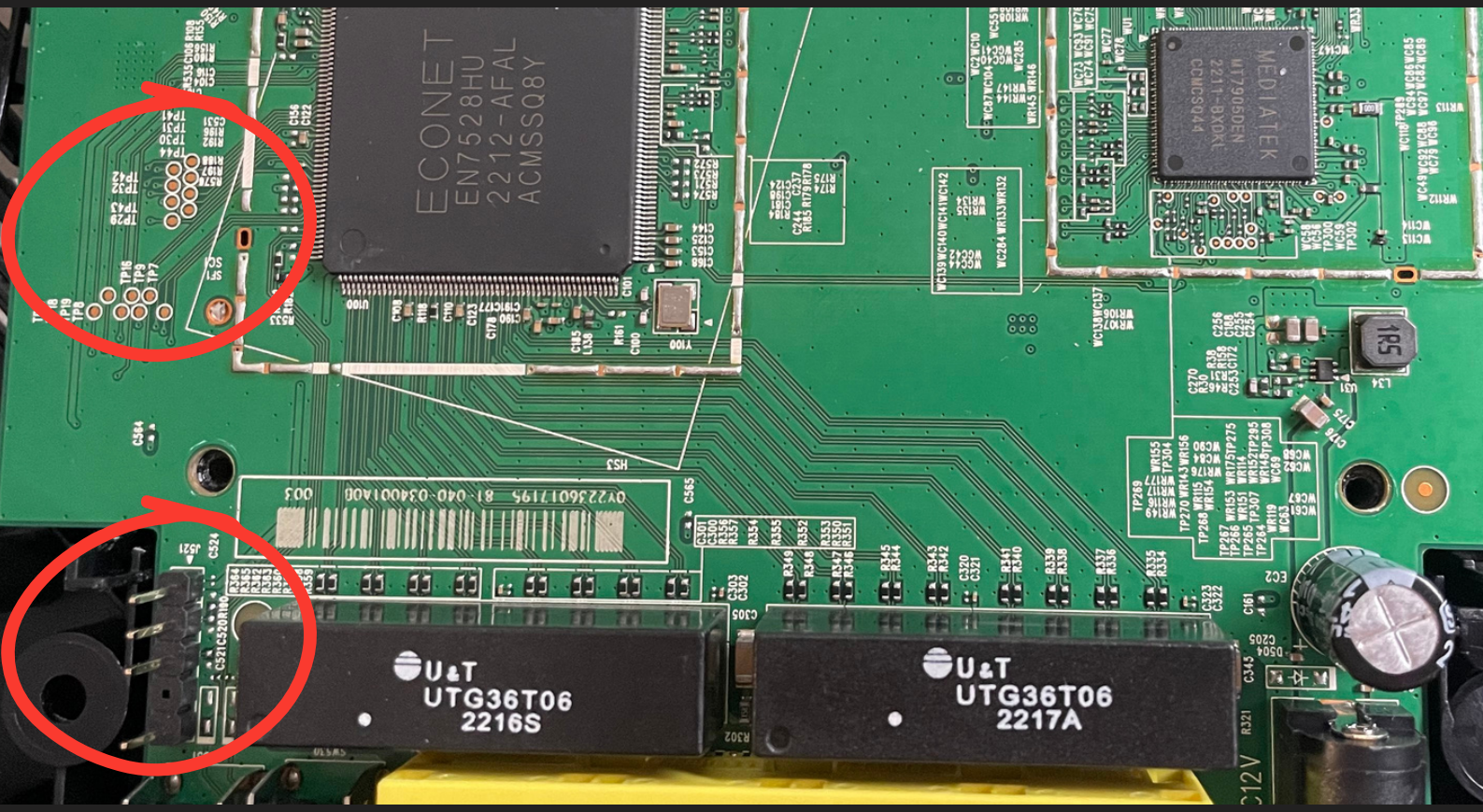
https://download.csdn.net/download/wgy5867709/19793752

4-Le MediaTek MT7905DEN est un processeur conçu par MediaTek, généralement utilisé dans les dispositifs mobiles et les appareils intelligents pour fournir des performances informatiques efficaces, une connectivité avancée et des fonctionnalités multimédias, telles que la prise en charge de la 5G, du traitement d'image et de l'intelligence artificielle.

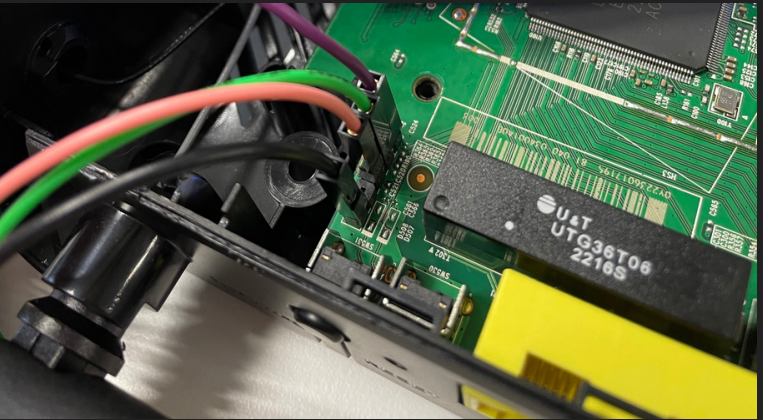
https://oss.komect.com/openhomeres/static/images/chipAndModel/%E7%BB%84%E7%BD%91%E8%8A%AF%E7%89%87/MT7905DAN.pdf

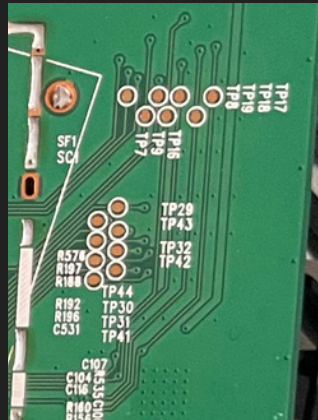
03 - IDENTIFICATION DES POINTS DE TESTS

ZYXEL ax1800 :



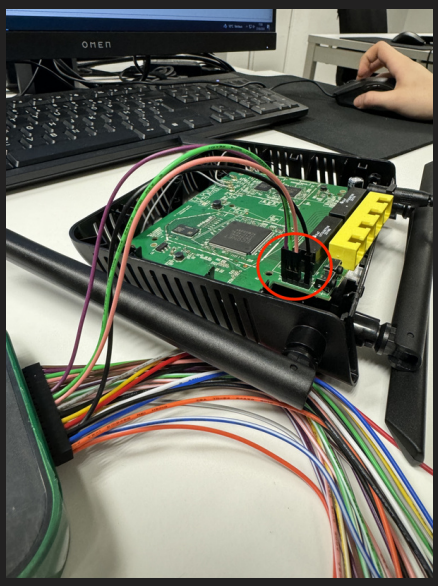
Les points de test sur un routeur sont des points stratégiques situés sur le circuit imprimé, permettant aux techniciens d'effectuer des mesures, des tests et même de capter des signaux à des points spécifiques du circuit pour évaluer son fonctionnement ou diagnostiquer des problèmes potentiels. Ces points sont accessibles via des connexions spécifiques et sont utilisés avec différents équipements de test pour valider les performances du routeur.

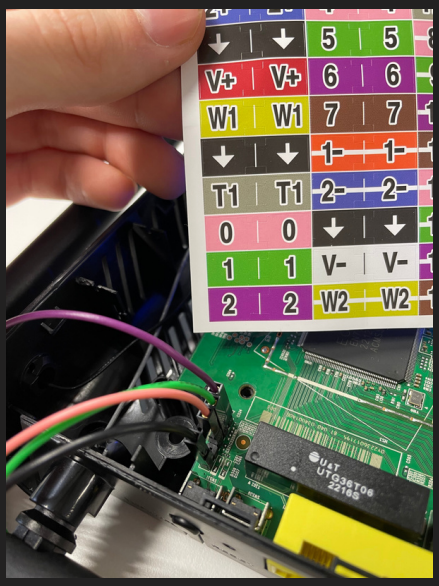


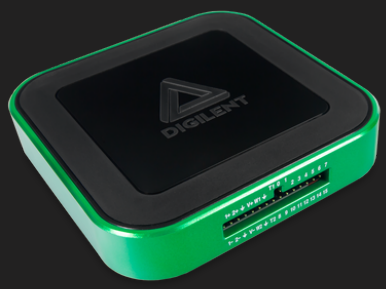


04 - TECHNIQUE ET SUIVI D'ANALYSE

Notre analyse s'est principalement porté sur le routeur Zyxel, en raison d'un problème technique sur le routeur Huawei, le rendant innopérable. Nous avons par contre, eu le temps de creuser certaines pistes intéressantes au niveau du Zyxel...



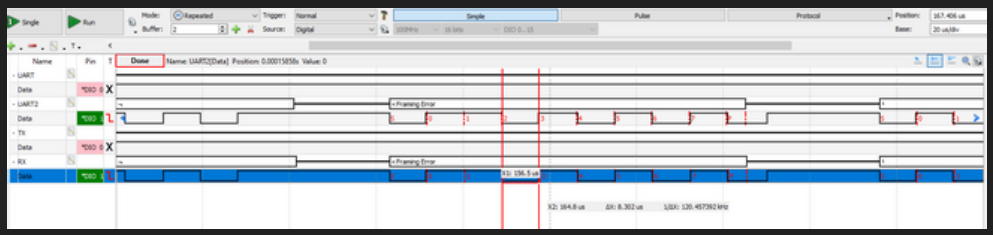




Premièrement, pour performer une analyse à l'oscilloscope, nous avons du trouver un point d'entrée/point de test, le plus intéressant est entouré en rouge ci-dessus

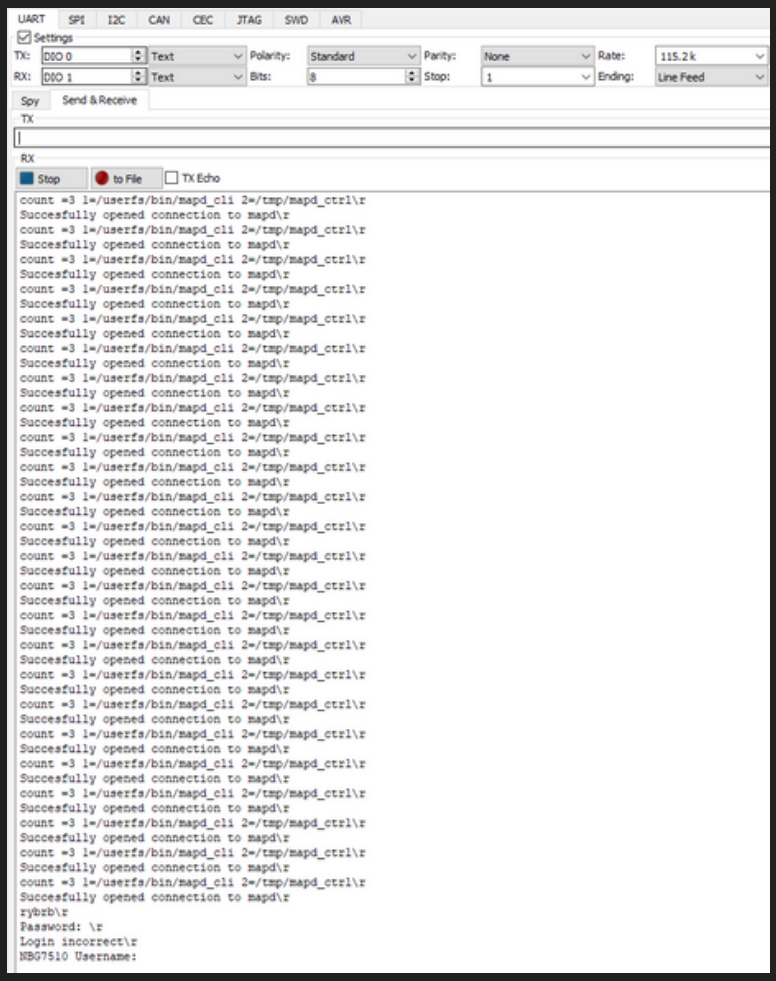
Nous avons utilisé un digilent analog discovery 3 pour réaliser une analyse complète du routeur Zyxel

De plus, nous avons pu identifier la taille d'un bit !



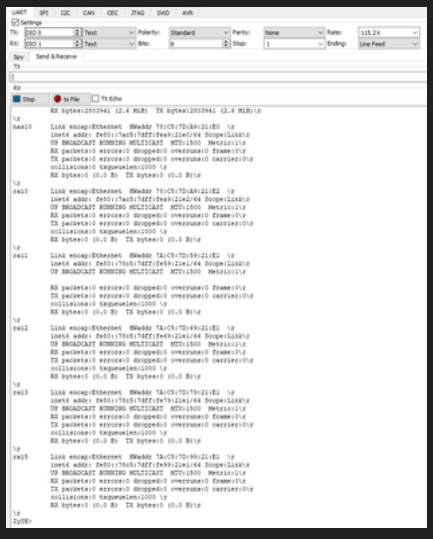
Nous avons donc utilisé une vitesse de transmission de 115.2k bauds pour le protocole UART

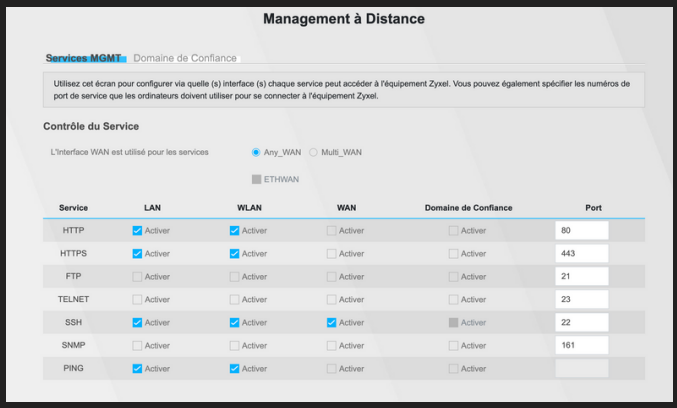
04 - TECHNIQUE ET SUIVI D'ANALYSE



Toujours en utilisant le logiciel associé au digilent nommé WaveForms, nous avons pu constater en utilisant DIO 0 en TX et DIO 1 en RX les logs de boot du routeur, puis via TX une interaction possible avec un pseudo-shell requérant un login/password

En utilisant le login/psswd par défaut du user admin (présent à l'arrière du routeur) nous sommes capable d'interagir réélement avec ce pseudo-shell, ici nous pouvons premièrement constater que c'est un shell extrêmement restreint en matière de commande utilisable





Activation du SSH pour une utilisation simplifié du terminal

04 - TECHNIQUE ET SUIVI D'ANALYSE

```
nate@MacBook-Pro-de-Nathan Desktop % ssh -oHostKeyAlgorithms=+ssh-rsa admin@192.168.123.1
The authenticity of host '192.168.123.1 (192.168.123.1)' can't be established.
RSA key fingerprint is SHA256:UeqTH7InmAr8da94qpRokvOfaifXR1h3K/tteRxovxY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.123.1' (RSA) to the list of known hosts.
admin@192.168.123.1's password:
No entry for terminal type "xterm-256color";
using dumb terminal settings.
ZySH> ls
```

À savoir : le paramètre -oHostKeyAlgorithms=+ssh-rsa est obligatoire pour établir une connexion SSH sur les anciennes version d'OpenSSH
(plus d'info : https://unix.stackexchange.com/questions/699192/ssh-authentication-issue-with-openssh-private-key)

Nous avons trouvé le moyen d'afficher les commandes dispo dans ce shell restreint avec la commande "?'

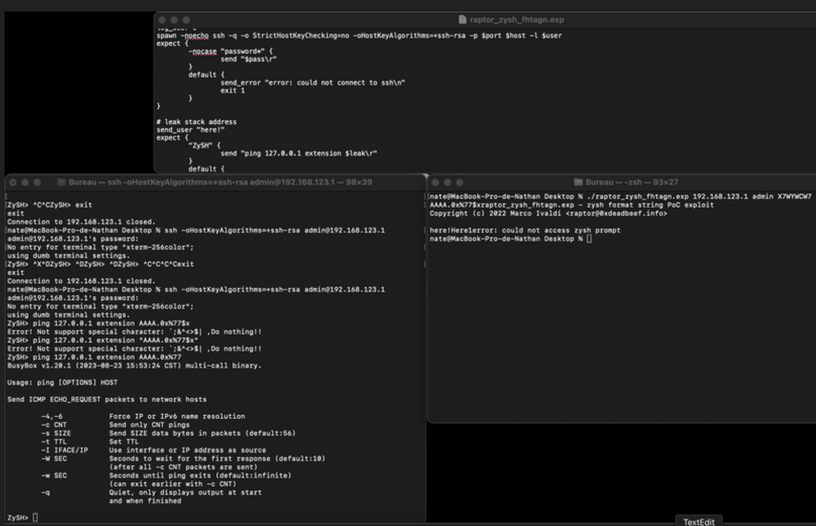
```
ZySH>
cfg                 - DAL command line interface
debug               - <N/A>
dns                 - ZYXEL command line
dsllinestatus       - Show Econet DSL line status
ethwanctl           - ZYXEL command line
exit                - Close an active terminal session
history             - Display or clear CLI history
ifconfig            - Show network interface configuration
ping                - Send ICMP ECHO_REQUEST to network hosts
pppoectl            - ZYXEL command line
sys                 - ZYXEL command line
tcpdump             - Text based packet capture utility
traceroute          - monitor each routed node during whole routing path to <host>
vcautohuntctl       - ZYXEL command line
voicedbgcli         - ZYXEL command line
wan                 - ZYXEL command line
wlan                - ZYXEL command line
zycli               - ZYXEL command line
```

Nous avons découvert la commande ping, mais aussi la commande traceroute, intéressantes pour faire pop un shell, malheureusement les caractères filtrés `;&^<>$| nous empechait de faire pop un shell par tous les moyen possible comme : traceroute "$(echo sh)". Tanpis, j'essaye aussi les commandes cfg pour dump des fichiers de config : access denied,

Nous sommes donc "admin", un utilisateur avec des privilèges très restreint. Après quelques recherches, notre première piste fut de tenter un exploit connu depuis 2022 présent sur les routeur Zyxel exploitant une faille de la commande "ping" permettant une privesc afin d'obtenir un shell root. Pour cela nous avons utilisé un tool nommé "RouterSploit".

```
nate@MacBook-Pro-de-Nathan routersploit % ./rsf.py

      Exploitation Framework for       by Threat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.4.1
 Homepage   : https://www.threat9.com - @threatnine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9.com

 Exploits: 132 Scanners: 4 Creds: 171 Generic: 4 Payloads: 32 Encoders: 6

rsf > use creds/routers/zyxel/ssh_default_creds
rsf (Zyxel Router Default SSH Creds) > set target 192.168.123.1
[+] target => 192.168.123.1
rsf (Zyxel Router Default SSH Creds) > run
[*] Running module creds/routers/zyxel/ssh_default_creds...
[-] 192.168.123.1:22 SSH Error while testing connection [Errno 51] Network is unreachable
[*] Target does not expose SSH
rsf (Zyxel Router Default SSH Creds) > use scanners/autopwn
rsf (AutoPwn) > set target 192.168.123.1
[+] target => 192.168.123.1
rsf (AutoPwn) > run
[*] Running module scanners/autopwn...
```

Après quelques tentatives de debug directement dans le code de l'exploit, rien à faire, l'exploit n'est pas réalisable sur cette version du firmware

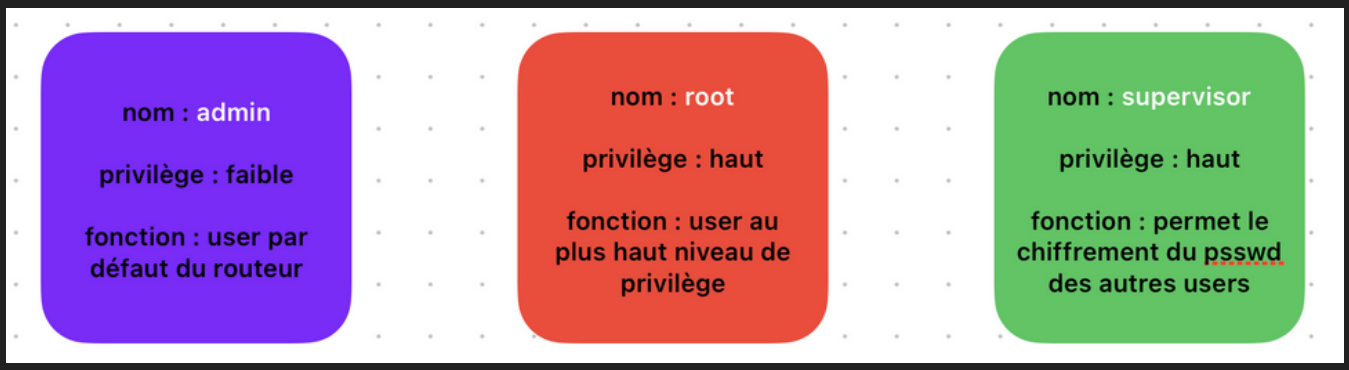


04 - TECHNIQUE ET SUIVI D'ANALYSE

De plus, grâce à l'outil RouterSploit, nous avons tenté quelques attaques bruteforce par dictionnaire sur le user "root", sans succès...

Après quelques recherches et en s'inspirant énormément du writeup de th0mas.nl (https://th0mas.nl/2020/03/26/getting-root-on-a-zyxel-vmg8825-t50-router/) ayant réalisé le reverse engineering complet d'un autre routeur de la gamme Zyxel

En résumé, il y a trois différents user :



Comme expliqué précédemment, l'objectif est d'avoir un shell sans restriction, celui-ci n'est accessible qu'en utilisant un utilisateur à haut privilèges

Dans son writeup, il utilise malheureusement, une solution inexploitable pour notre modèle de routeur, nous avons donc continué nos investigations en conservant le même objectif !

```
ZySH>
cfg                     - DAL command line interface
debug                   - <N/A>
dns                     - ZYXEL command line
dsllinestatus           - Show Econet DSL line status
ethwanctl               - ZYXEL command line
exit                    - Close an active terminal session
history                 - Display or clear CLI history
ifconfig                - Show network interface configuration
ping                    - Send ICMP ECHO_REQUEST to network hosts
pppoectl                - ZYXEL command line
sys                     - ZYXEL command line
tcpdump                 - Text based packet capture utility
traceroute              - monitor each routed node during whole routing path to <host>
vcautohuntctl           - ZYXEL command line
voicedbgcli             - ZYXEL command line
wan                     - ZYXEL command line
wlan                    - ZYXEL command line
zycli                   - ZYXEL command line
```

Tanpis, nous essayons aussi les commandes cfg pour dump des fichiers de config : access denied, je rappelle qu'admin à les privilèges les plus bas par defaut. Donc les commandes sont éxecutés en fonction de ces mêmes privilèges

Une autre commande à attirer notre attention...
La commande sys

04 - TECHNIQUE ET SUIVI D'ANALYSE

La commande sys me semble intéressante, nous décidons donc tester toutes ses possibilités, de toute façon aucun risque en apparence, nous n'avons aucun privilège... EN APPARENCE !!!

```
ZySH> sys
Usage: sys help
       sys show
       sys atsh
       sys atsn <SeriesNumber>
       sys atwz <MAC> <CountryCode> <EngDbgFlag> <FeatureBit> <MacNumber>
       sys atcd Erase ROM-D partition.
       sys atcr [reboot] Reset to default, erase Data partition.
          sys atvp set or get VendorName & ProvinceName from MRD partition.
       sys --autogenpwd <enable>
       sys --autogenpwd <enable> <prefix>
       sys --autogenpwd <disable> <password>
       sys --autogenpwd show
       sys --WPSbtn <enable>
       sys --WPSbtn <disable>
       sys --WPSbtn show
       sys seqnum [1|2]
       sys getbootpartition
       sys nonboot
```

sys --autogenpwd show renvoi "Admin pwd is by default", cela veux t'il dire que nous avons la possibilité de changer notre password ? Une action normalement réservé aux utilisateurs à privilège

```
ZySH> sys --autogenpwd show
Admin pwd is by default
```

Un autre argument est disponible "enable", nous décidons de nous le tester...

```
ZySH> sys --autogenpwd enable
Enable: AutoGen the admin pwd by SN..
```

Soudain, toujours sur WaveForms, nous observons les lignes suivantes :

```
Deleted user admin.\r
file size of source = 2\r
Changing password for admin\r
Password for admin changed by root\r
Added user admin.\r
Enabled user admin.\r
```

05 - RÉSULTAT

Toute à l'heure, je mentionnais sur le schéma des utilisateurs, le rôle de "supervisor", concrètement le mot de passe stocké en hash dans les fichier de conf tel que /etc/passwd et /etc/shadow de l'utilisateur supervisor, est la clé de chiffrement utilisé pour chiffrer le mdp de l'utilisateur root, afin d'éviter au maximum les potentiels hackers qui tenterait d'exploiter le matériel

La commande utilisée précédemment permet de changer le password de l'utilisateur actuellement connecté, action réalisable seulement avec des privilèges root. Nous pouvons donc en utilisant cette même commande exécuter des commandes précises permettant d'accéder potentiellement à un shell root.

```
Password for admin changed by root\r
```

Malheureusement, après ça, admin étant le seul utilisateur auquel nous avions accès, ni le dashboard web, ni le CLI, ni le SSH n'était désormais accessible... Ce qui à mis fin à nos recherches :(

```
nate@MacBook-Pro-de-Nathan Desktop % ssh -oHostKeyAlgorithms=+ssh-rsa admin@192.168.123.1
admin@192.168.123.1's password:
Permission denied, please try again.
```

06 - FUTURE POSSIBILITÉS

Mais, nous pouvons au moins vous mentionner ce qu'il aurait été possible de faire, si nous avions pu récupérer le shell du user admin...

Avec la commande sys nous aurions pu réaliser des bypass shell CLI en utilisant des commandes tel que sys sh + quelques stratégies de bypass (https://www.exploit-db.com/docs/english/44592-linux-restricted-shell-bypass-guide.pdf) pour accéder, enfin à un shell avec les privilèges root

```
VMG8825-T50 login: root
Password:
# id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
Linux VMG8825-T50 3.18.21 #6 SMP Tue Jul 30 10:35:51 CST 2019 mips GNU/Linux
```

Ouvrir les fichiers de config, apprendre de l'environnement, placer une backdoor, probablement dump le firmware, les possibilités sont infinies avec un shell root, toutes ces informations croustillantes pourront dès lors être accessible sans problème

```
$ xxd flashdump
00000000: 0010 8893 5a79 7865 6c20 436f 6d6d 756e  ....Zyxel Commun
00000010: 6963 6174 696f 6e73 2043 6f72 702e 0000  ications Corp...
00000020: 0000 0000 564d 4738 3832 352d 5435 3000  ....VMG8825-T50.
...
00000040:            [root password]
00000050:        [default admin password]
...
00000080: 0000 0000 0000 0000 0002 0003 0506 0708  ................
00000090: 0f00 0000 0000 0000 0000 0000 015a 5958  .............ZYX
000000a0: 4541 0123 4500 5041 4745 0000 0000 0053  EA.#E.PAGE.....S
000000b0:              [serial nr]
000000c0: 0004 0505 0400 0002 0000 0000 0000 0000  ................
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000e0:        [default WiFi password]
000000f0: 0104 0202 2620 1919 1256 0000 0000 0000  ....& ...V......
```

07 - CONCLUSION

En conclusion, ce projet de **reverse engineering** des circuits électroniques nous a apporté une grande expérience. À travers l'**analyse détaillée** des routeurs **Huawei** et **Zyxel**, nous avons pu explorer l'intérieur de ces dispositifs, en identifiant les **composants**, en analysant les **signaux émis** et en tentant de **comprendre** leur fonctionnement.

Malgré les **défis** et **problèmes** rencontrés, tel que le **dysfonctionnement** du premier routeur et les **restrictions** imposées par le shell sur le deuxième, nous avons pu mettre en **pratique** nos **connaissances** afin d'effectuer des recherches, en utilisant des outils de mesure tels que **l'oscilloscope** et **l'analyseur logique** pour décoder les signaux et analyser les circuits.

Ce projet nous a permis de **développer** non seulement nos **compétences techniques** en matière d'électronique, mais aussi notre **capacité à résoudre des problèmes !**

Merci pour ce projet !