H550 project defence

Exploitation of an old access point

Aguililla Klein Esteban

ULB

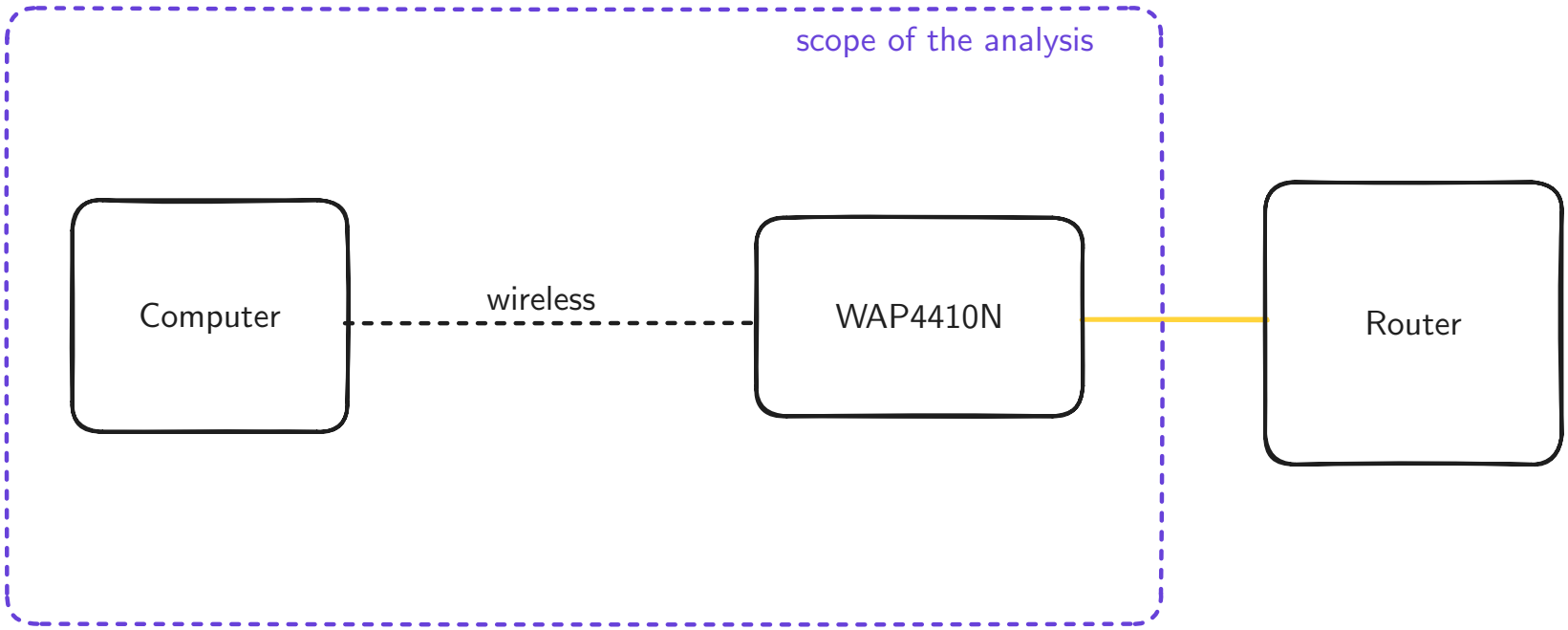
2024

Context

- released in october 2008
- end of sale in 2014
- end of support in 2019
- aimed at small businesses

Figure: WAP4410N Access Point

lab setup



- local network without access to the internet
- the router is out of scope

reconnaissance

split into four parts,

1. physical
2. bootloader
3. console
4. network traffic

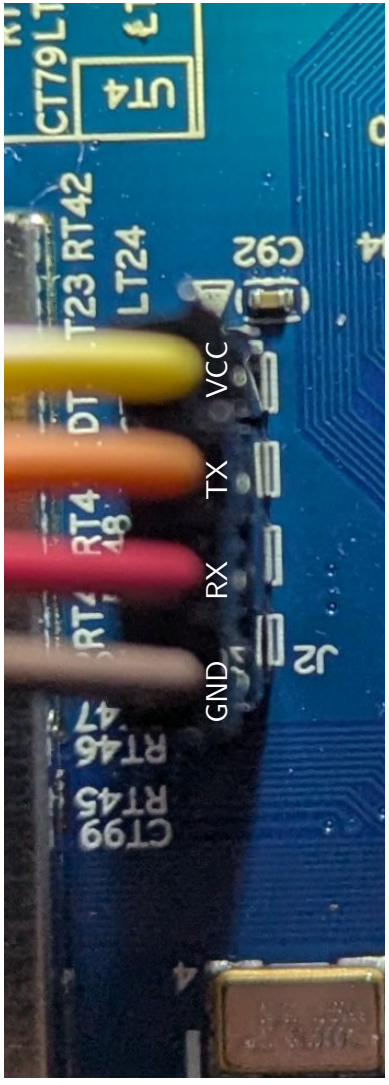
- architecture :
  - MIPS32
  - big endian
- memory :
  - 48 TSOP NAND flash
  - MXIC-29LV640DBTC
- I/O :
  - UART 3.3V

finding the uart

to find the UART, take measures with a multimeter

pin	R_{VSS}	V	info
1	$8.6k\Omega$	$\approx 3.3V$	VCC
2	$\infty k\Omega$	$\approx 0V$	TX
3	$\infty k\Omega$	$\approx 0V - VCC$	RX
4	$0k\Omega$	$0V$	GND

in some cases it might be disabled, broken, ...



bootloader

after connecting to the uart,

- boot log (a lot of useful information)
- can interrupt autoboot and get to U-boot console

in the U-boot console,

- unprotected
- reduced subset of U-boot (or is it due to the age ?)
- info about the hw, firmware, memory layout

```
ar7100> bdinfo
flashstart  = 0xBF000000
flashsize   = 0x00800000
flashoffset = 0x0002F690
```

console

- ash shell
- busybox
  - old version
  - reduced
- root user
- squashfs3
  - readonly
- utilities for handling the device internals

extracting the partition table,

```
[VAP0 @ wap86eb04]# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00040000 00010000 "u-boot"
mtd1: 00010000 00010000 "u-boot-env"
mtd2: 00650000 00010000 "rootfs"
mtd3: 00140000 00010000 "uImage"
mtd4: 00010000 00010000 "nvram"
mtd5: 00010000 00010000 "calibration"
```

firmaware version,

network

something todo