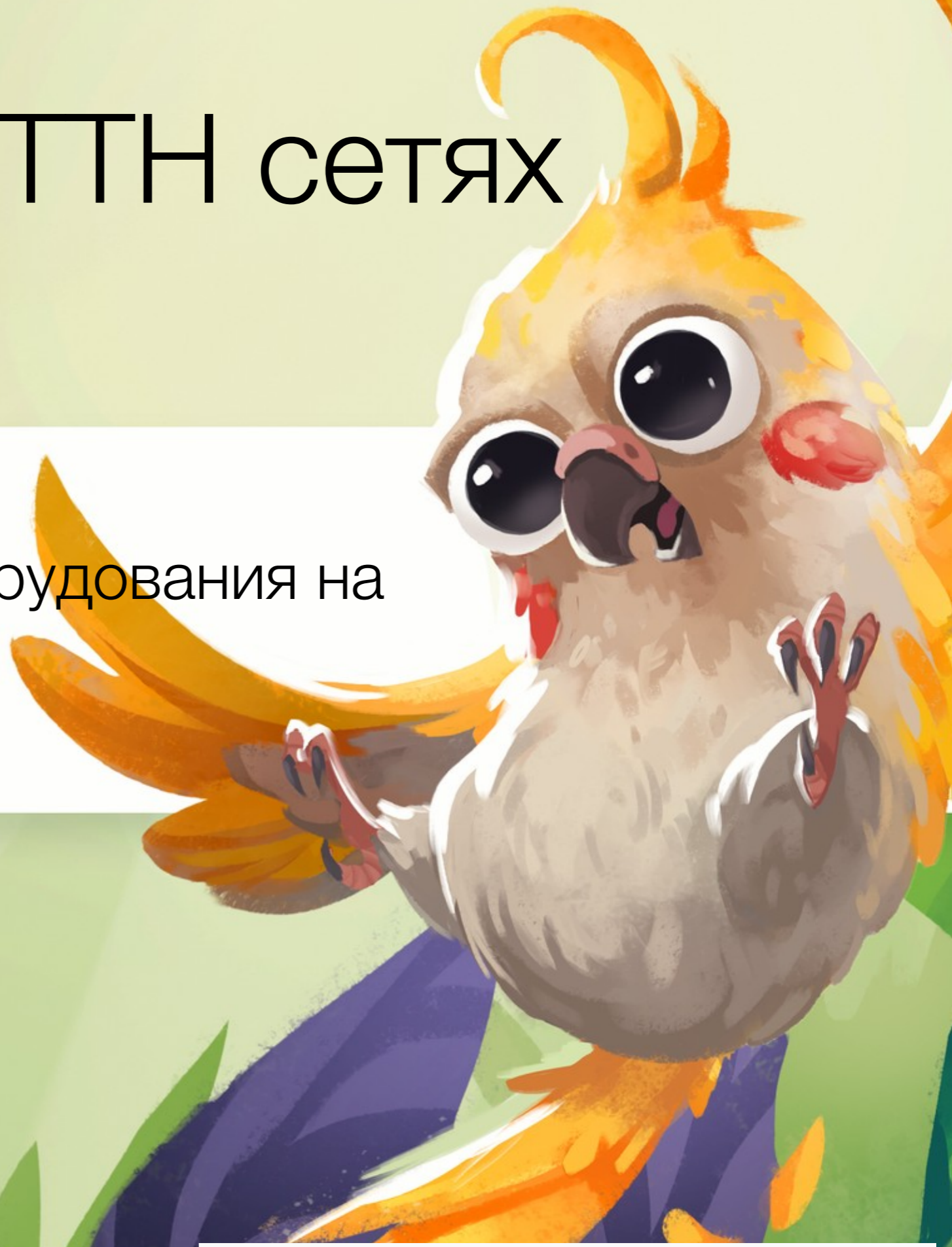


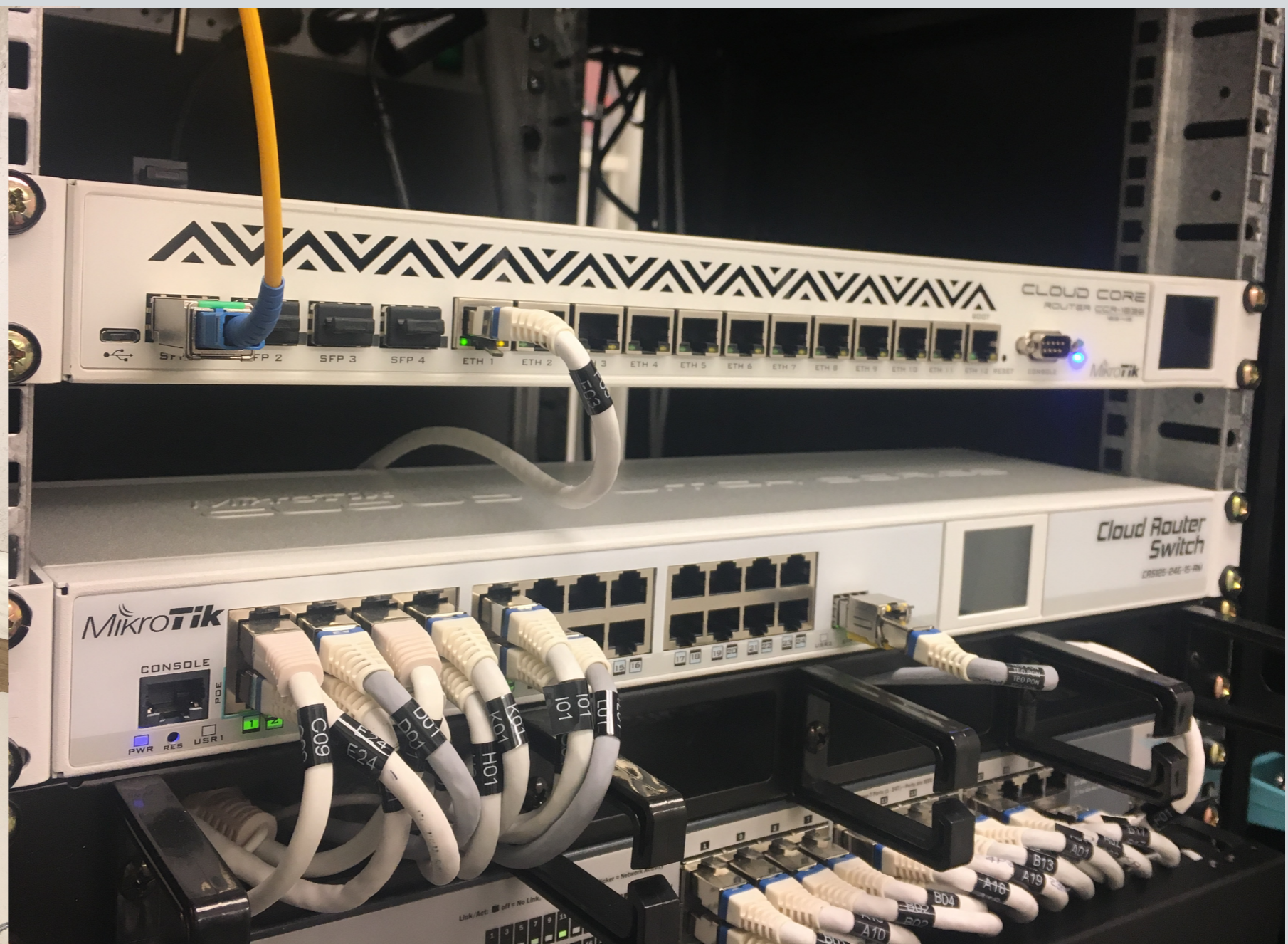
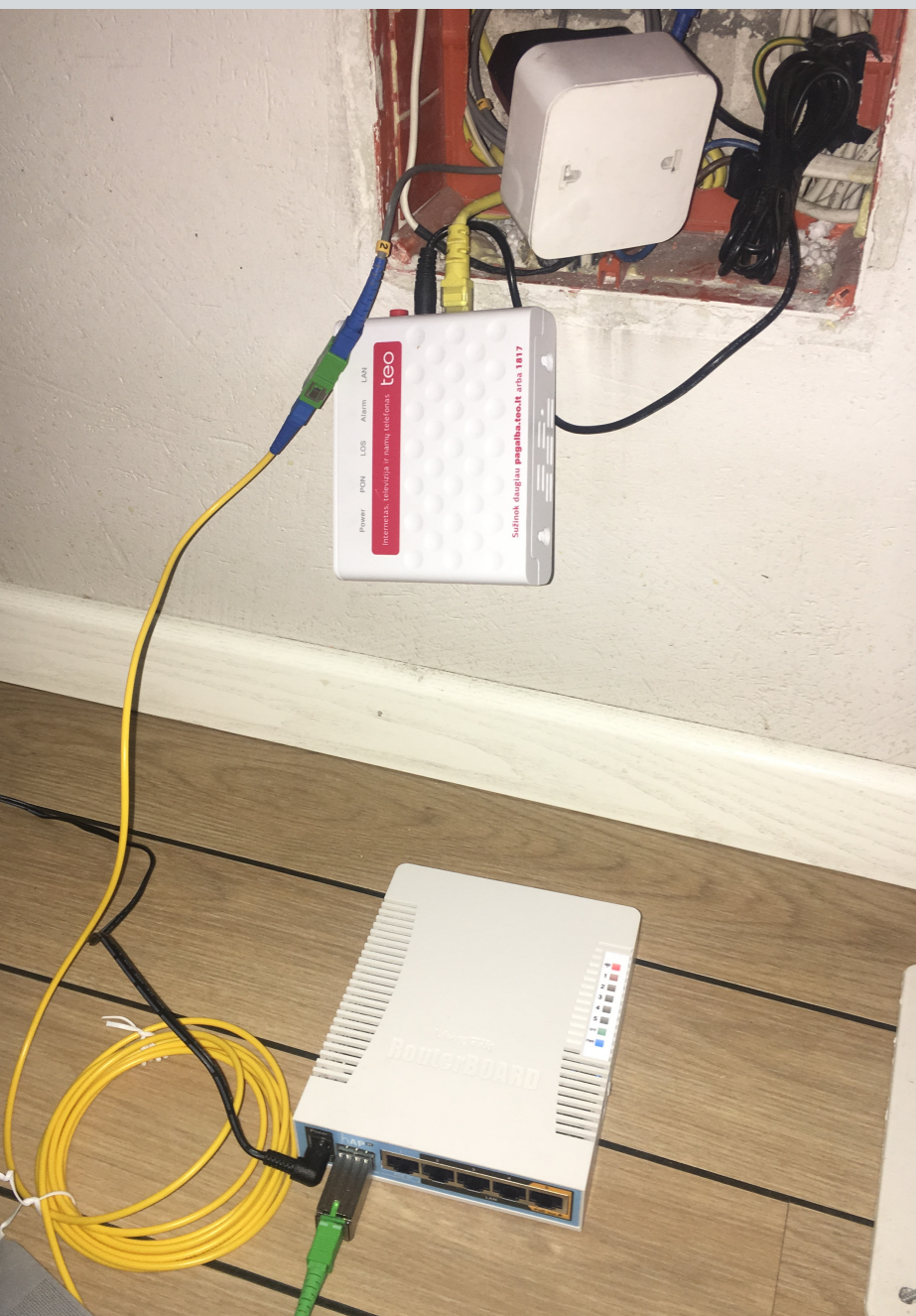
SFP в GPON FTTH сетях

замена абонентского оборудования на
SFP + *MikroTik*

Андрей Коваленко, Glera Games (Литва)

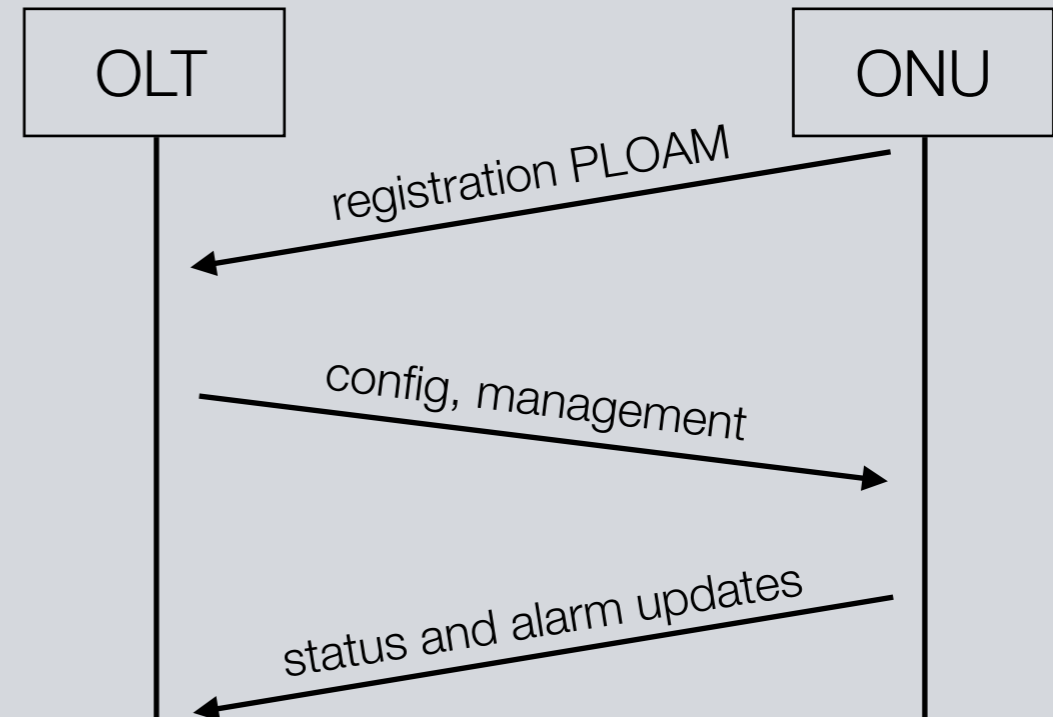


Задача



Какие бывают GPON SFP

- OLT
- ONT/ONU
 - поддержка OMCI

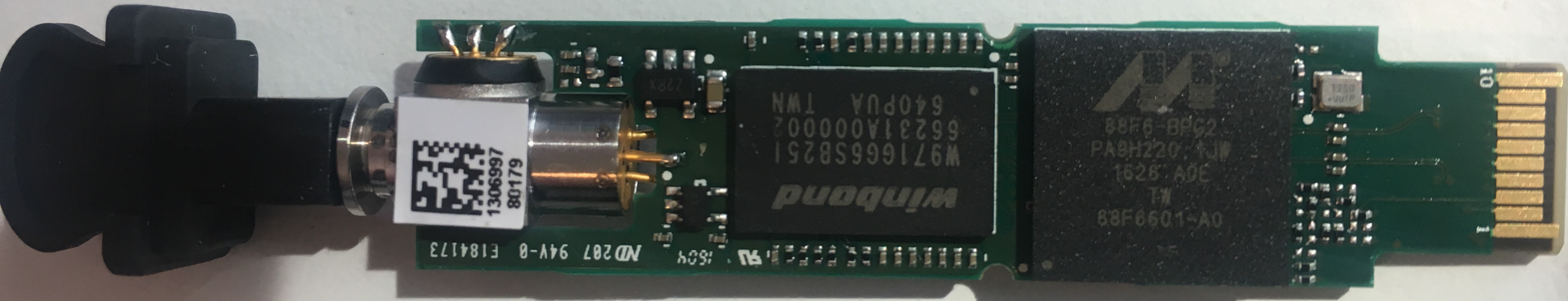


- если ваш провайдер готов прописать на OLT ваш модуль как абонентское устройство, то вам стоит попробовать MikroTik SFPONU. Это идеальный вариант и вы не получите минусов указанных далее

MikroTik SFPONU

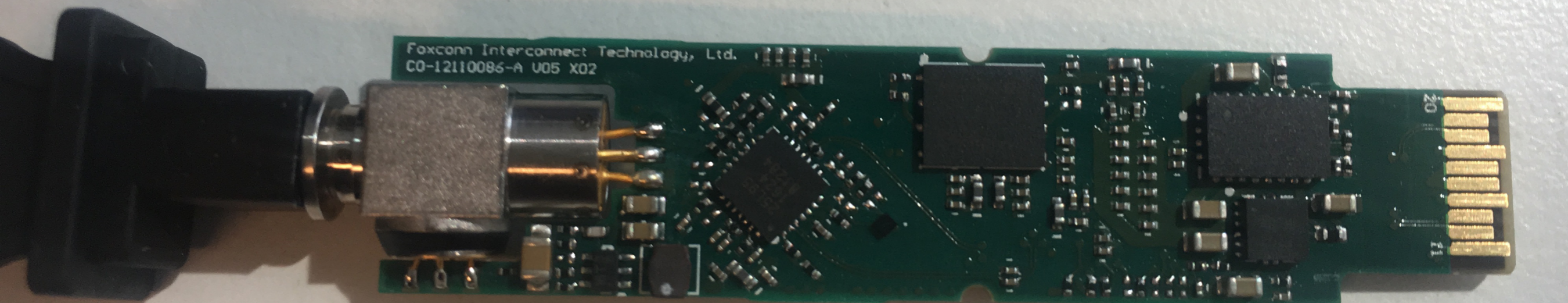
DDR2 128Mb

CPU ARMv5



Flash 16Mb

DC-DC



Laser driver

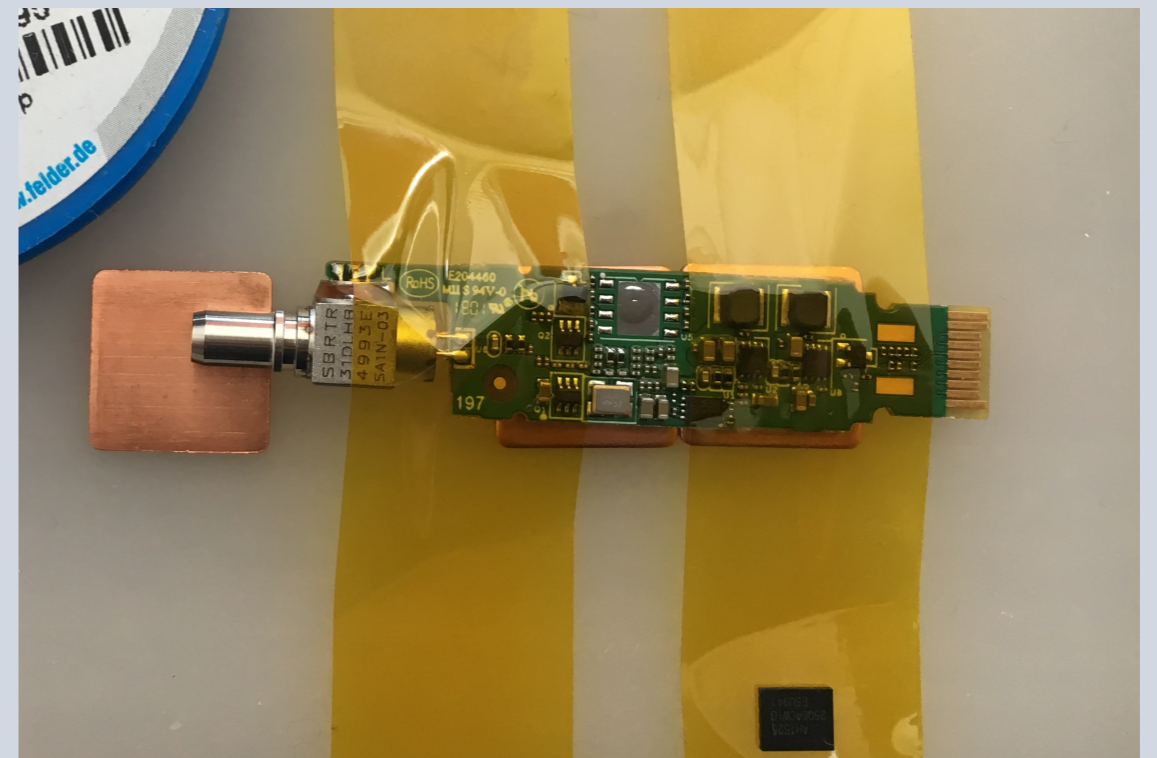
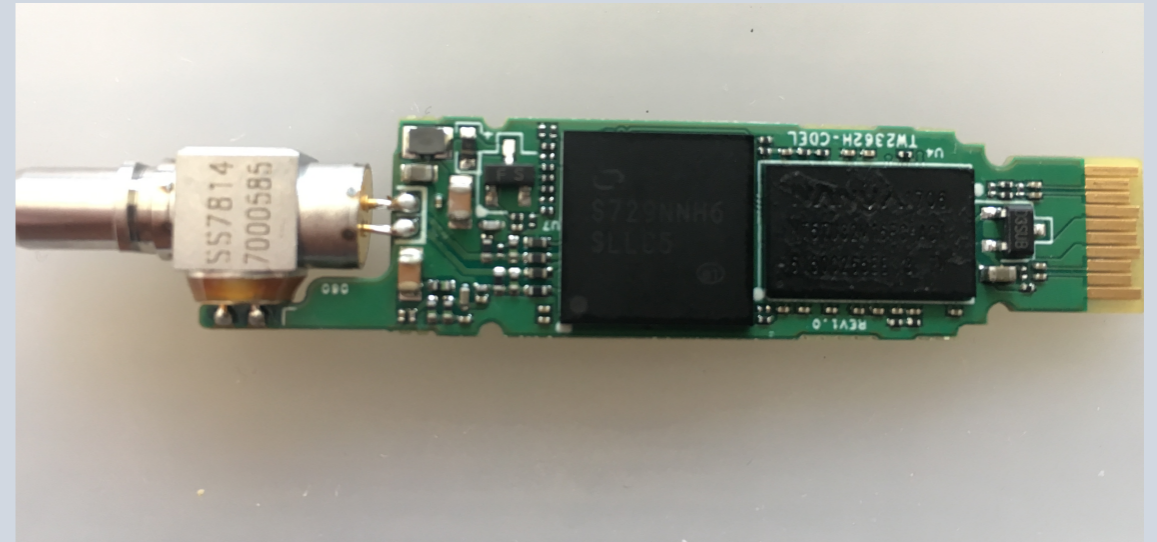
Временное решение

- webUI, CLI, telnet; webUI работает только если есть сигнал на оптическом входе
- OpenWRT / linux kernel
- PLOAM, OMCI, и тд
- full IPv4 and IPv6 support
- цена 60\$ + 28\$(доставка DHL в Литву)



Подходит, но не работает

- CPU - Lantiq Falcon, MIPS 34Kc V5.6
- NAND - 64Mb
- Flash - 8Mb



- имеем две прошивки от испанцев под их провайдера Movistar?, могу ошибаться, но мне кажется эти прошивки им делал производитель, так как там указан автор zhaohaiyang, в оригинальной luowenbin

- скачиваем родную прошивку всей flash, смотрим

```
# binwalk ./ziza_op151s_working.BIN
DECIMAL    HEXADECIMAL  DESCRIPTION
-----
164512     0x282A0      CRC32 polynomial table, little endian
186487     0x2D877      Unix path: /B/BOOT/ENV/CONFIG/EGIS
459264     0x70200      ulmage header, header size: 64 bytes, header CRC: 0x4839EC66, created: 2017-07-12 04:01:47, image size: 1184511 bytes, Data Address: 0x80002000, Entry Point:
0x80002000, data CRC: 0xD4AF7C71, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "OpenWrtLinux-3.10.12-svn"
459328     0x70240      LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 3481980 bytes
1769472    0x1B0000     Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2353577 bytes, 727 inodes, blocksize: 262144 bytes, created: 2018-04-02 20:55:52
4194816    0x400200     ulmage header, header size: 64 bytes, header CRC: 0x4839EC66, created: 2017-07-12 04:01:47, image size: 1184511 bytes, Data Address: 0x80002000, Entry Point:
0x80002000, data CRC: 0xD4AF7C71, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "OpenWrtLinux-3.10.12-svn"
4194880    0x400240     LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 3481980 bytes
5505024    0x540000     Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2352865 bytes, 727 inodes, blocksize: 262144 bytes, created: 2017-07-19 09:30:18
7929856    0x790000     JFFS2 filesystem, big endian
```

- замечаем два похожих блока, видим подтверждение и в telnet

```
root@SFP:~# cat /proc/mtd
dev: size erasesize name
mtd0: 00060000 00010000 "Boot"
mtd1: 00010000 00010000 "Env"
mtd2: 00390000 00010000 "ImageA"
mtd3: 00390000 00010000 "ImageB"
mtd4: 00060000 00010000 "Config"
mtd5: 00010000 00010000 "SECTION_EGIS"
mtd6: 00250000 00010000 "rootfs"
mtd7: 00010000 00010000 "rootfs_data"
```

- между ними можно переключаться из telnet
- если прошивка плохая, она становится inactive и запускается с другой

- извлекаем содержимое используя firmware-mod-kit, пришлось его немного модифицировать

```
./extract-firmware.sh ./3FE45464AOCK21.upf
```

- начинаем искать контрольные суммы для разных частей прошивки: header, u-boot, squashfs...

Handwritten notes: crc32 от Secure partition

```

00000000 43 6F 70 79 | 72 69 67 68 | 74 20 32 30 | 30 30 2D 32 | 30 31 30 20 | 54 26 57 2E | 20 41 6C 6C | 20 72 69 67 | 68 74 73 20
00000024 72 65 73 65 | 72 76 65 64 | 2E 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 57 65 64 20 | 4A 75 6C 20
00000048 31 39 20 30 | 39 3A 33 30 | 3A 31 39 20 | 32 30 31 37 | 00 00 00 00 | 00 00 00 00 | 02 01 00 00 | DC 4D 9F 6F | F1 5D D3 F4
0000006C 41 42 43 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 33 46 45 34 | 35 34 36 34 | 41 4F 43 4B | 32 31 00 00 | 00 00 00 00
00000090 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 0E 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000000B4 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000000D8 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000000FC 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
00000120 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
00000144 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
00000168 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
0000018C 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000001B0 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000001D4 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000001F8 00 00 00 00 | 00 00 00 00 | 00 00 38 00 | 01 00 00 00 | AB 26 6F 59 | 00 00 38 00 | 3F 13 12 00 | 00 00 24 00 | 00 00 14 00
0000021C BE F3 D8 10 | 6E F9 23 20 | 6E 9F AD DC | 73 71 75 61 | 73 68 66 73 | 00 00 00 00 | 00 00 00 00 | 47 54 4F 31 | 30 30 49 5F
00000240 55 46 50 20 | 56 31 2E 30 | 2E 31 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 47 54 4F 31 | 30 30 49 5F
00000264 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 33 46 45 34 | 35 34 36 34 | 41 4F 43 4B | 32 31 00 00
00000288 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 41 4C 43 4C | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000002AC 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
000002D0 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
000002F4 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
00000318 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
0000033C FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
00000360 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
00000384 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
000003A8 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
000003CC FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF
000003F0 FF FF FF FF | FF FF FF FF | FF FF FF FF | FF FF FF FF | 27 05 19 56 | 48 39 EC 66 | 59 65 9F 2B | 00 12 12 FF | 80 00 20 00
00000414 80 00 20 00 | 04 AF 7C 71 | 05 05 02 03 | 4F 70 65 6E | 57 72 74 4C | 69 6E 75 78 | 2D 33 2E 31 | 30 2E 31 32 | 2D 73 76 6E
00000438 00 00 00 00 | 00 00 00 00 | 5D 00 00 80 | 00 7C 21 35 | 00 00 00 00 | 00 00 00 6F | FD FF FF A3 | B7 7F 4C 34 | 87 87 DD 78
0000045C D1 0D C5 8D | 61 19 84 44 | EF 7C 60 19 | 75 20 C4 EC | 89 C3 5B A9 | FA 57 15 4F | 18 43 47 4C | 19 3D F5 E8 | 19 0B 54 B1
00000480 2B 03 2B 9B | 99 99 F2 7F | 4D 32 A6 7C | AA C0 C8 2A | 67 C9 3C AF | 5B 60 73 8F | 95 B0 48 24 | 70 D7 9C 84 | 6A 91 FE C9
000004A4 9D CC 68 96 | 5C B1 D9 56 | 4C 8C 70 B8 | 80 5E E5 EA | 7B DC 59 48 | 28 81 10 08 | 2B E6 70 8F | 20 40 AA 0B | F4 47 3E 2D
000004C8 B8 40 61 80 | BD 90 BC 73 | E9 75 86 14 | 84 E9 DA 8B | B5 55 8F 7A | F0 60 30 28 | 50 3E 79 13 | 90 2C 1C FE | 86 88 8D D9
000004E4 C4 5A CE 4F | 5B C4 31 10 | B8 80 29 0A | 7B 4B BA F7 | 3B C7 55 72 | 82 CA 8F 4C | A9 44 91 2B | 2A BA 96 3E | 2B C9 24 8F
00000500 73 4D 80 A7 | 36 90 BC 88 | CF 38 44 14 | E0 A3 05 46 | DD 37 28 29 | 5D 51 2F 63 | 47 4B 79 0F | 25 54 02 F3 | AB 2D 01 EE
00000524 FA 48 CD 82 | 5B D3 C1 F0 | 9F 11 58 F3 | 5C 38 DC CC | 95 E9 7B F2 | F9 7F F1 C4 | DF D9 43 BB | 64 68 9B 86 | A8 60 1D F7
00000548 76 E1 B1 D7 | 4C 15 81 90 | 97 B9 48 E8 | 8C 7E EA 36 | A5 68 E5 4F | 7F CB 3F 5A | 56 7C BD DB | 98 B3 AF 3A | 1F 62 06 C2
00000574 E8 01 00 10 | 39 1C D1 A7 | 6C 66 5A 32 | FF 97 46 72 | C1 D5 E5 84 | FB 14 CB BB | 54 71 D5 36 | E2 5C D8 2C | 9B 47 9A E8
000005A0 68 53 C5 02 | 95 83 6B 32 | 6A E6 F7 BE | 1F 2D 95 A3 | 1A 69 18 EA | 38 B2 0F 64 | 95 B5 98 B1 | A7 42 80 79 | 7F CA F8 A0
00000600 43 6F 70 79 | 72 69 67 68 | 74 20 32 30 | 30 30 2D 32 | 30 31 30 20 | 54 26 57 2E | 20 41 6C 6C | 20 72 69 67 | 68 74 73 20
00000624 72 65 73 65 | 72 76 65 64 | 2E 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 57 65 64 20 | 4A 75 6C 20
00000648 31 39 20 30 | 39 3A 33 32 | 3A 32 32 20 | 32 30 31 37 | 00 00 00 00 | 00 00 00 00 | 02 01 00 00 | DC 4D 9F 6F | 79 1D 53 98
00000674 41 42 43 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 33 46 45 34 | 35 34 36 34 | 41 4F 43 4B | 34 32 00 00 | 00 00 00 00
00000698 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 0E 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
000006C4 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00

```

Handwritten notes: crc32 header

Адрес в прошивке - описание КОНТРОЛЬНОЙ СУММЫ

- по адресу 0x68 лежит crc32 от всего файла, пишем туда 00 00 00 00, затем прописываем туда полученный crc32
- по адресу 0x200 и по 0x20C (le) длинна всей прошивки
- по адресу 0x208 (le) дата создания
- по адресу 0x210 длинна бутлоадера с адреса 0x400
- по адресу 0x214 длинна squashfs с адреса 0x140200 до конца
- по адресу 0x218 адрес начала squashfs (без копирайта -0x200)
- по адресу 0x21C (le) crc32 от бутлоадера до конца, 0x400 до конца
- по адресу 0x220 (le) crc32 от 0x200 до 0x400 при этом в сам адрес прописываем нули
- в прошивке на устройстве нет секции Copyright, заливается блок начиная с 0x200

- подсматриваем важные параметры на модеме/конверторе, который предоставляет провайдер, это производитель (ZTE, ALCL, T&W, HW), software version, hardware version, serial number, password, VLAN (internet) нужен будет позже
- заменяем в прошивке эти параметры на подсмотренные, кроме SN, он меняется в telnet как: `#manufactory set sn <ваш sn>`
- собираем прошивку, используя firmware-mod-kit
`# ./build-firmware.sh`
- обновляем контрольные суммы
- заливаем через web UI
- смотрим operation status, если O(5) init - радуемся

Настройка на стороне MikroTik

- сам модуль это bridge, то есть если нужен VLAN и/или PPPoE (Беларусь ByFly), то настраиваем это на MikroTik, если не нужны, то по DHCP вы уже должны получить IP (Литва Telia, бывший TEO)
- VLAN интерфейс создаем на SFP интерфейсе, если нужен
- на этом этапе мы не увидим ip на интерфейсе если нам нужен PPPoE так как он работает поверх L2. Поднимаем PPPoE тоннель на SFP интерфейсе, и должны получить IP на интерфейсе тоннеля

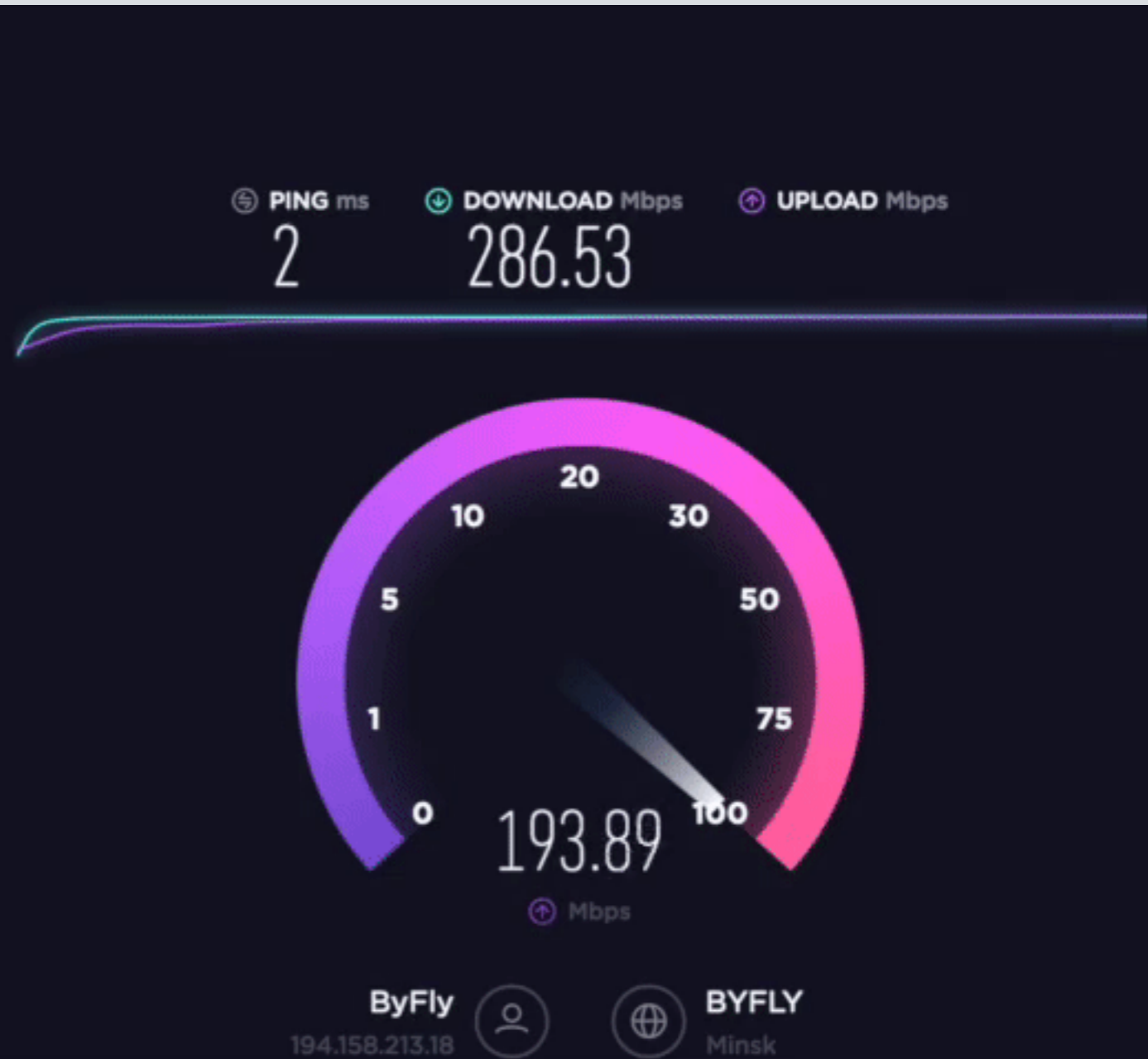
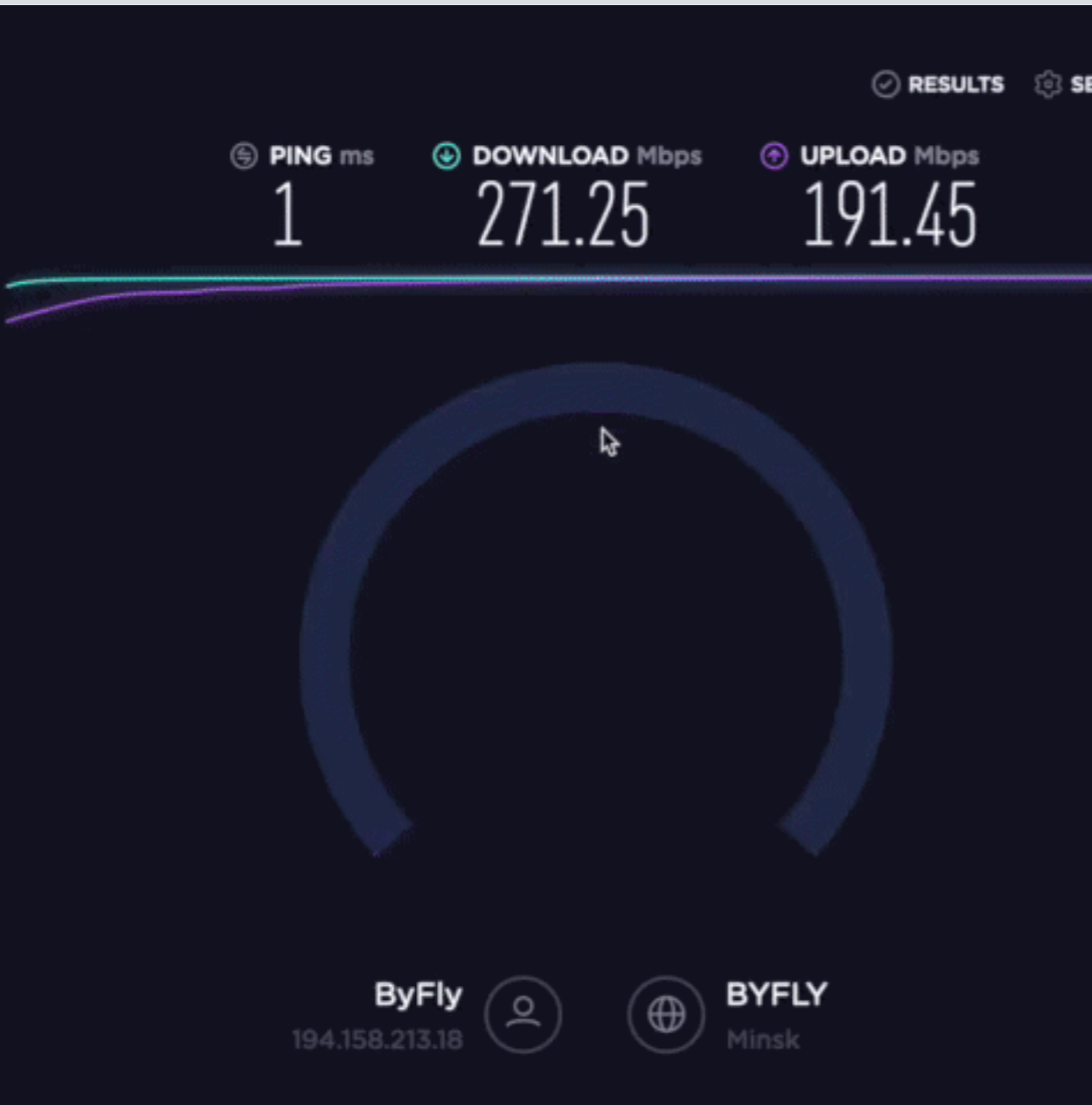
Есть ли выигрыш?

- предел скорости (DN/UP) определяется не на клиентской стороне, а на стороне провайдера, то есть получить мы можем все равно только то, что дают
- задача не получить меньше

Результат

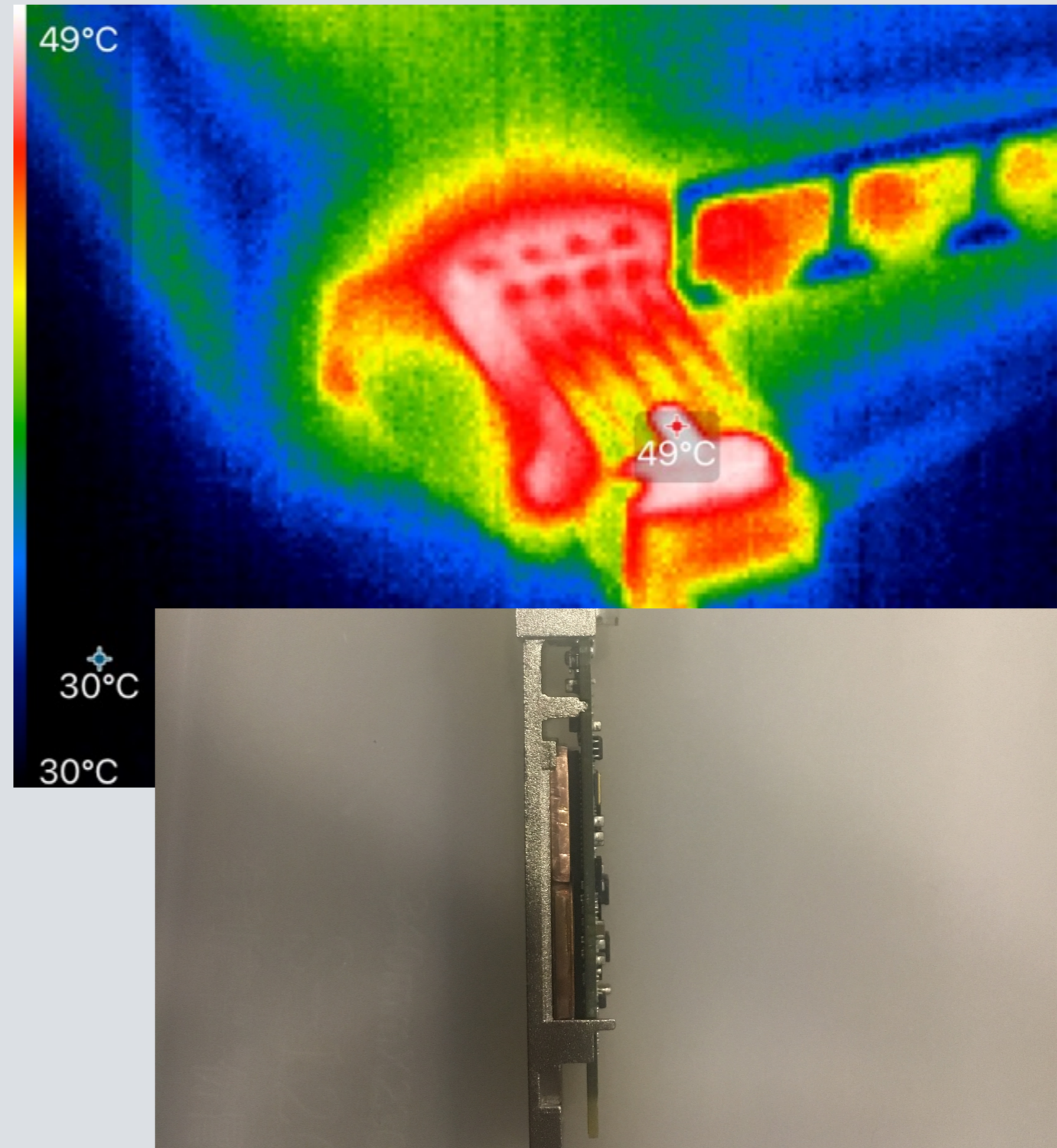
original

SFP



Минусы

- греется - пару градусов можно отвоевать заменив “резиновый” термоинтерфейс на медные пластины
- цена
- размер
- менять в пределах прошивки можно только SN и password
- если провайдер обновит версию SW можно остаться без интернета
- SIP, IPTV
- прикидывается абонентским устройством от провайдера



Как самому собрать прошивку

- <https://github.com/kovalenko/SFP-GPON.git>
- если не получается - пришлите мне: страну, провайдера, производителя OLT/ONU, версии Hw и Sw. Например: Беларусь, ByFly, ZTE, V3.0, V2.30.20P6T14S

Что дальше

- приоритет сейчас MikroTik SFPONU, она лучше по всем критериям (*моим)
- на сегодня: могу менять прошивку (занимает 5-8 минут), пока не нашел пути изменения прошивки без выпаивания flash. Так как нет документации на CPU, то пока в поисках выводов UART

Спасибо



- Андрей Коваленко, <mailto:kovalenko@glera.net>

Дальше немного оффтопа

```
[admin@MikroTik] > /interface ethernet monitor sfpl
    name: sfpl
    status: no-link
  auto-negotiation: done
    advertising:
link-partner-advertising:
  sfp-module-present: yes
    sfp-rx-loss: yes
  eeprom-checksum: bad
    eeprom: 0000: 03 04 01 00 00 00 00 00 00 00 00 00 03 0c 00 14 c8 .....
            0010: 00 00 00 00 4d 49 4b 52 4f 54 49 4b 20 20 20 20 ....MIKR OTIK
            0020: 20 20 20 20 00 00 00 00 53 2d 47 50 4f 4e 2d 4f      .... S-GPON-0
            0030: 4e 55 2d 72 32 20 20 20 52 32 20 20 05 1e 00 48 NU-r2  R2  ...H
            0040: 00 1a 00 00 4d 4b 54 4b 30 30 30 33 31 30 20 20 ....MKTK 000310
            0050: 20 20 20 20 31 36 31 32 31 39 20 20 68 f0 05 39      1612 19  h..9
            0060: 6c 3b 6b e1 1c 55 00 00 00 00 00 00 00 00 00 00 00 00 1;k..U..
            0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            00a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            00b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            00c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            00d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            00e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
            00f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Как менять EEPROM

*и потерять гарантию :)

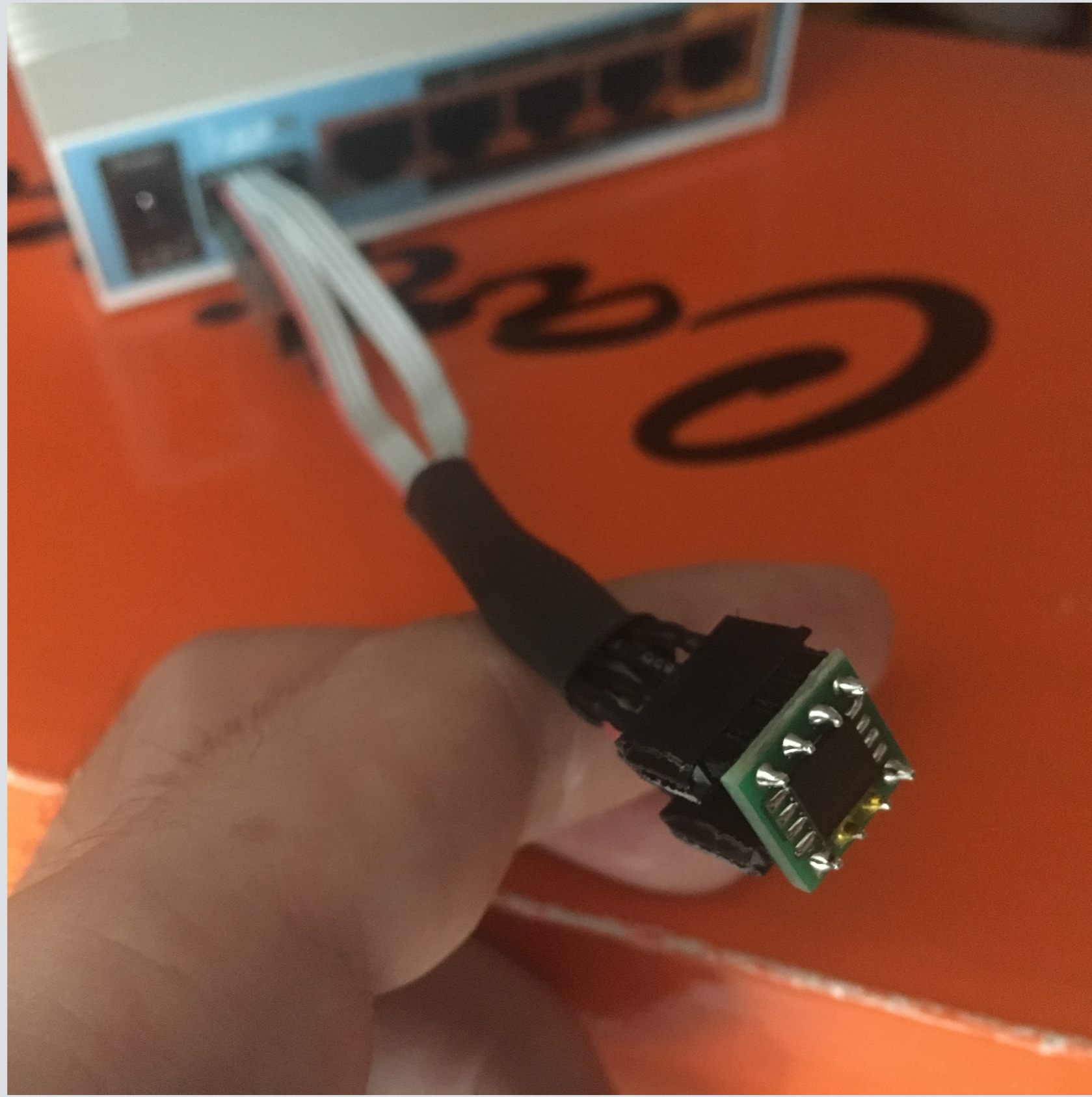
- on SFP-> 1:GND, 15,16:+3.3V, 4:SDA, 5:SCL
- on RPi-> 1:+3.3V, 6:GND, 3:SDA, 5:SCL
- install i2c-tools
- `i2cdetect -y 1`
- `i2cdump -y 1 0x50`
- `i2cset -y 1 0x50 0x1b 0x20`



Теперь виден “health”

```
[admin@MikroTik] > /interface ethernet monitor sfp1
      name: sfp1-gateway
      status: no-link
      auto-negotiation: done
      advertising:
link-partner-advertising:
      sfp-module-present: yes
      sfp-rx-loss: yes
      sfp-type: SFP-or-SFP+
      sfp-connector-type: SC
      sfp-link-length-9um: 20000m
      sfp-vendor-name: MIKROTIK
sfp-vendor-part-number: S-GPON-ONU-r2
      sfp-vendor-revision: R2
      sfp-vendor-serial: MKTK000310
sfp-manufacturing-date: 16-12-19
      sfp-wavelength: 1310nm
      sfp-temperature: 53C
      sfp-supply-voltage: 3.268V
sfp-tx-bias-current: 0mA
      eeprom-checksum: good
      eeprom: 0000: 03 04 01 00 00 00 00 00 00 00 00 00 03 0c 00 14 c8 .....
      0010: 00 00 00 00 4d 49 4b 52 4f 54 49 4b 20 20 20 20 ....MIKR OTIK
      0020: 20 20 20 20 00 00 00 00 53 2d 47 50 4f 4e 2d 4f      .... S-GPON-0
      0030: 4e 55 2d 72 32 20 20 20 52 32 20 20 05 1e 00 48 NU-r2  R2 ...H
      0040: 00 1a 00 00 4d 4b 54 4b 30 30 30 33 31 30 20 20 ....MKTK 000310
      0050: 20 20 20 20 31 36 31 32 31 39 20 20 68 f0 05 06      1612 19 h...
      0060: 6c 3b 6b e1 1c 55 00 00 00 00 00 00 00 00 00 00 00 1;k..U..
      0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
      0080: 64 00 ce 00 5f 00 d8 00 8c a0 75 30 88 b8 79 18 d..._... ..u0..y.
      0090: af c8 00 00 88 b8 00 00 7b 86 22 d0 6e 17 27 10 ..... (.".n.'.
      00a0: 07 cb 00 0f 06 30 00 14 00 50 43 00 02 02 00 00 .....0.. .PC.....
      00b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
      00c0: 00 00 00 00 3f 80 00 00 00 00 00 00 01 00 00 00 .....?...
      00d0: 01 00 00 00 01 00 00 00 01 00 00 00 00 00 00 f6 .....
      00e0: 35 59 7f aa 00 00 00 00 00 00 00 00 00 01 2a 00 5Y..... *.
      00f0: 05 40 00 00 05 40 00 00 00 00 00 00 00 00 00 00 .@...@..
```

Flash на разъеме



GRON сплиттер 1:2



Dual Windo

产品名称: FBT盒式

产品

工作

STK0163014332



STK0163014332

Made in China