Exploring the Huawei HG8010H GPON ONT

Optical networking, ugly firmwares and more...

Marco d'Itri
<md@linux.it>
@rfc1036

Italian Hacker Camp 2018 - 3 August 2018

GPON basics

GPON: Gigabit Passive Optical Network

- In the CO: Optical Line Terminal (OLT).
- Street cabinet: 1:4 passive optical splitter.
- Building distribution frame: 1:16 passive optical splitter.
- In the customer premises: Optical Network Terminal (ONT).

One single fiber from the CO serves a tree of about 50 customers with the 1:64 splitting factor ($4 \times 16 = 64$, for Telecom Italia).

GPON basics (2)

Wave division multiplexing

- Downstream (1490 nm): 2.5 Gbps broadcast (but AES-encrypted).
- Upstream (1310 nm): 1.25 Gbps time division multiplexing.

The fiber is used bidirectionally, hence a single fiber strand enters the customer premises.

The Huawei HG8010H GPON ONT

The Huawei HG8010H GPON ONT

- CPE provided in Italy by Telecom Italia and Vodafone.
- Costs about 15$ on Alibaba.
- One optical GPON port.
- One copper Ethernet port.
- (Not so) dumb bridge: it needs a PPPoE router.

```
Linux version 2.6.34.10_sd5115v100_wr4.3
(root@vL10t193037) (gcc version 4.4.6 (GCC) )
#1 SMP Wed Jul 2 19:38:31 CST 2014
```

Digital Optical Monitoring data

`http://192.168.100.1/html/status/opticinfo.asp`
returns:

```
var opticInfos = new Array(new stOpticInfo
  ("InternetGatewayDevice.X_HW_DEBUG.AMP.Optic",
   " 2.08","-17.01","3306","38","13"),null);

function stOpticInfo(domain,transOpticPower,
  revOpticPower,voltage,temperature,bias)
```

So we get:

- Transmitted optical power (dBm)
- Received optical power (dBm)
- Voltage (mV)
- Temperature (℃)
- Bias current (mA)

Web GUI authentication

```
// nonce (not actually a constant)
function GetRandCnt() {return 'cbe1603a6d364f7d31acad86d8227dca'}

function SubmitForm() {
  var Username = document.getElementById('txt_Username');
  var Password = document.getElementById('txt_Password');

  // ...

  var Language = 'english';
  var cnt = GetRandCnt();
  var cookie2 = "Cookie=" + "rid=" + RndSecurityFormat("" + cnt)
    + RndSecurityFormat(Username.value + cnt) +
    RndSecurityFormat(RndSecurityFormat(hex_md5(Password.value))
    + cnt) + ":" + "Language:" + Language + ":" + "id=-1;path=/";
  document.cookie = cookie2;

  window.location.replace('/login.cgi');
  return true;
}
```

`RndSecurityFormat()` is SHA-256...

Accessing the shell

- Default username and password: `admin / admin`.
- But the privileged username and password `telecomadmin / admintelecom` (cannot be modified!) allows to download the configuration.
- The configuration is AES-encrypted, but the key is common to many Huawei CPEs...
- To access the shell, just set `TelnetLanEnable=1` (no SSH...), encrypt again the configuration and upload it.
- Then the `display optic` command will show what we need.
- Add Perl as needed...

Measuring optical power

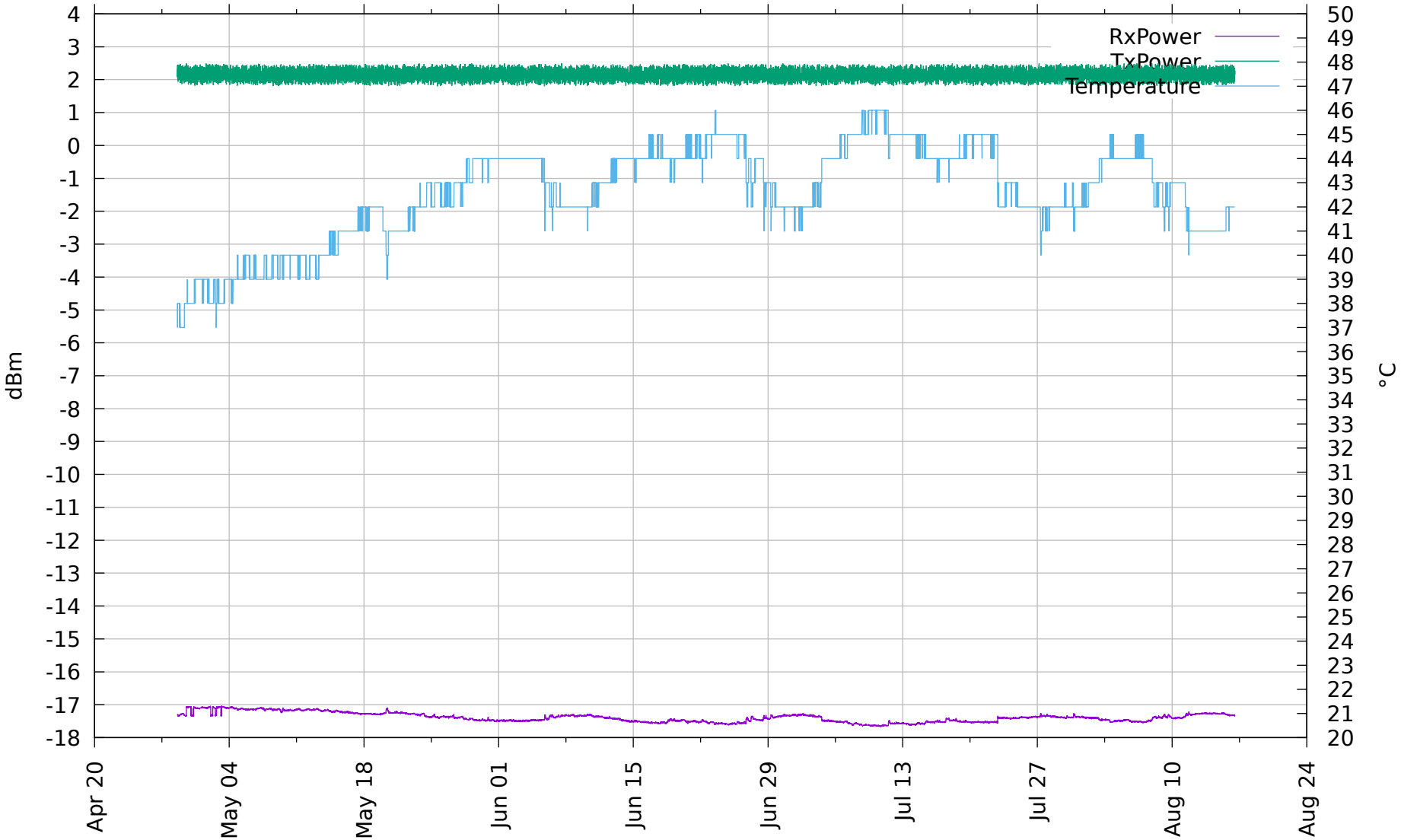
dB: the decibel is the ratio of two values of a physical quantity. Dimentionless.

$$\mathrm{dB} = 10 \cdot \log_{10}\left(\frac{Power_{in}}{Power_{out}}\right)$$

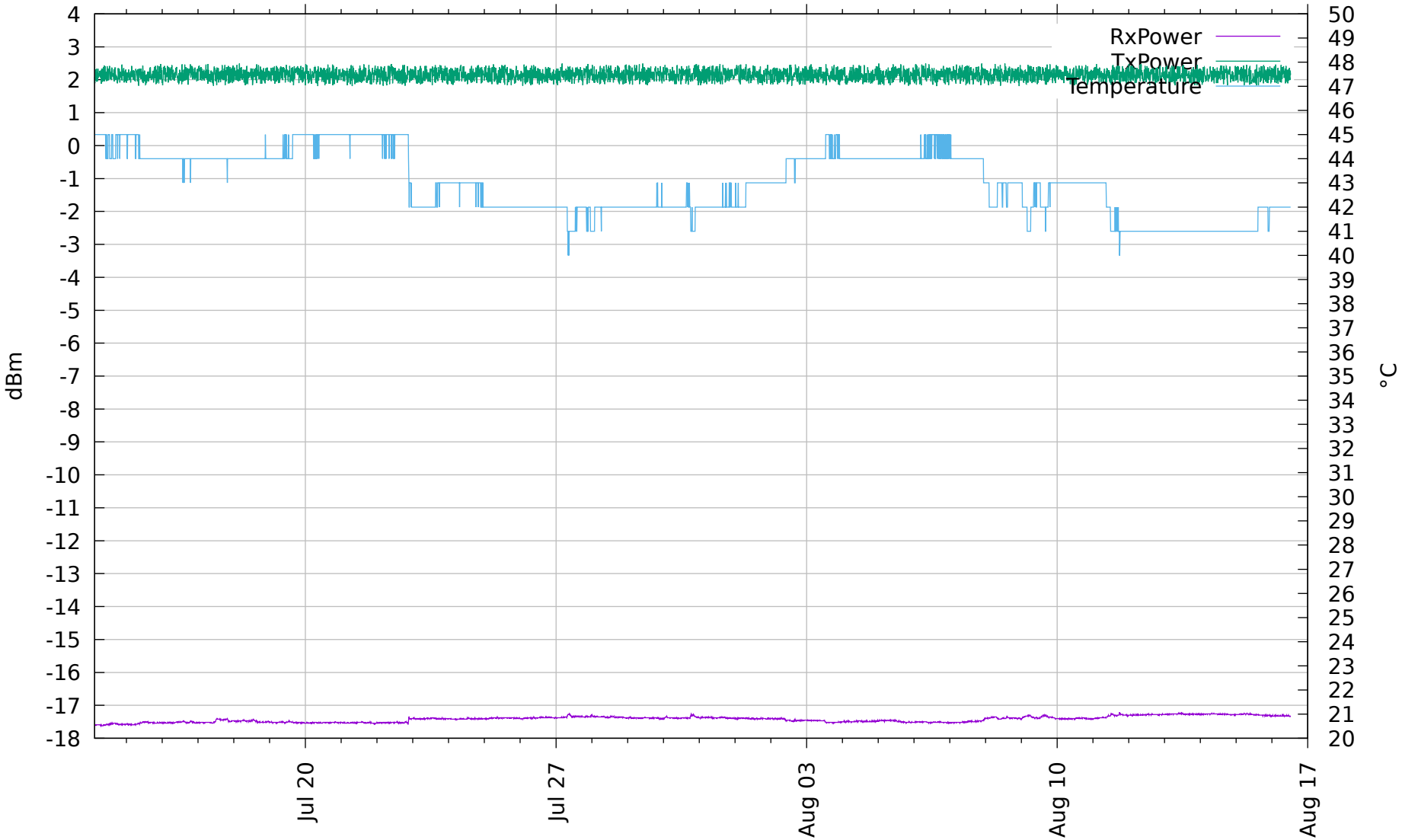
- $3\mathrm{dB} \approx 2$
- $-3\mathrm{dB} \approx \frac{1}{2}$
- $-10\mathrm{dB} = \frac{1}{10}$
- $-20\mathrm{dB} = \frac{1}{100}$

dBm: decibel-milliwatts represents power referenced to 1mW.

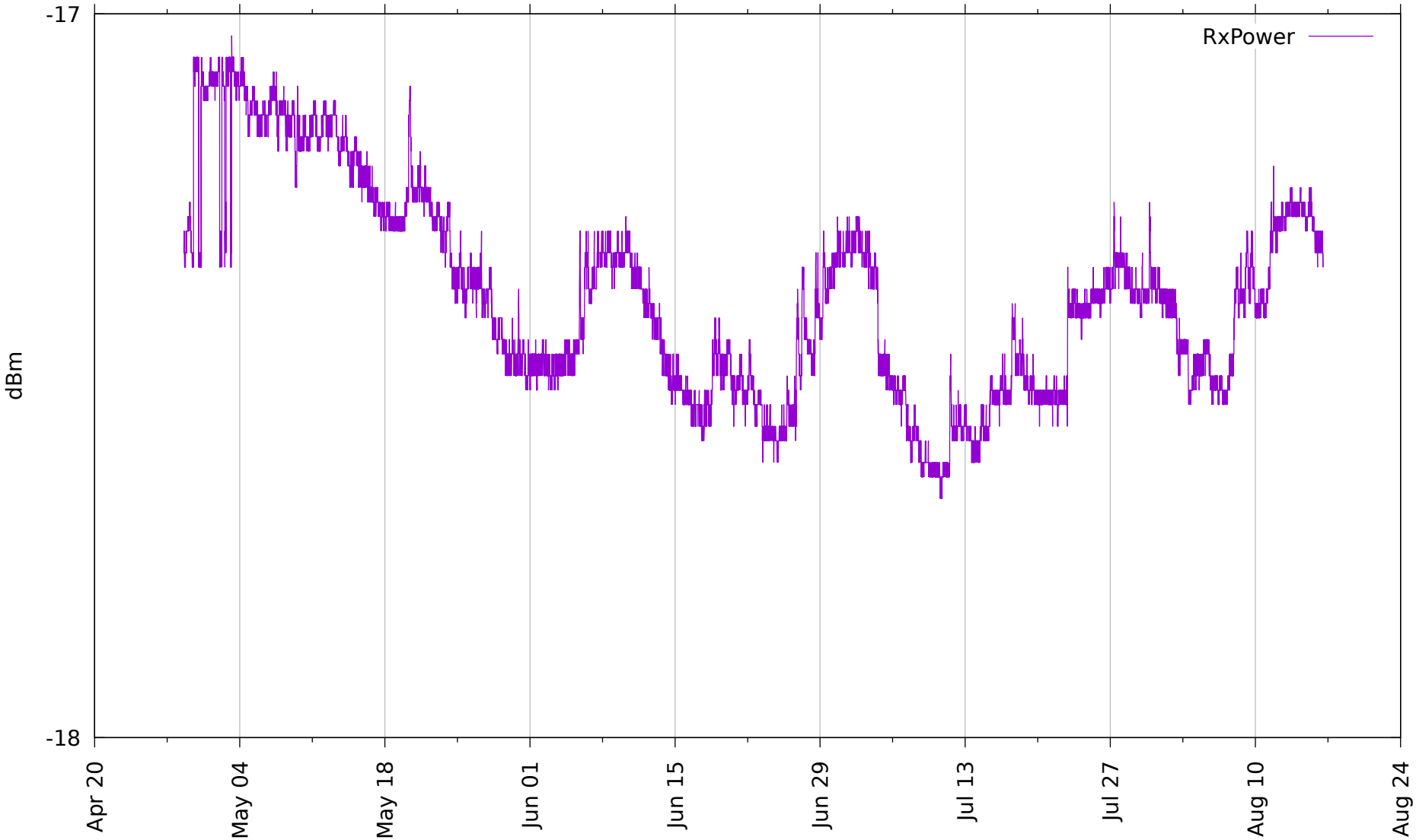
DOM paramters



DOM paramters



DOM paramters



Questions

Why is the RX power fluctuating?

- Is it really correlated to the environment temperature?
- Is it directly influenced by the environment temperature? Why?

Linux-based routing: PPPoE interface

Create a dedicated interface for PPPoE:

```
auto eth9
iface eth9 inet static
        address 192.168.100.2/30
        pre-up  ip link add link eth0 $IFACE type macvlan
        post-down ip link del $IFACE
```

And add some NAT to reach the router from your internal network:

```
iptables -t nat -A POSTROUTING -d 192.168.100.1 -j SNAT
  --to-source 192.168.100.2
```

Linux-based routing: `pppd@.service`

```
[Unit]
Description=PPP connection for %I
Documentation=man:pppd(8)
DefaultDependencies=no
IgnoreOnIsolate=yes
After=local-fs.target network.target apparmor.service ↩
  systemd-sysctl.service systemd-modules-load.service
Before=shutdown.target network-online.target
Conflicts=shutdown.target

[Service]
Type=forking
ExecStart=/usr/sbin/pppd call %I linkname %I updetach
ExecStop=/bin/kill $MAINPID
ExecReload=/bin/kill -HUP $MAINPID
StandardOutput=null
Restart=on-failure
PrivateTmp=yes

[Install]
WantedBy=multi-user.target
WantedBy=network-online.target
```

Linux-based routing: `pppd@.service`

A modern approach to starting `pppd`:

```
systemctl enable pppd@myisp
systemctl start pppd@myisp
systemctl status pppd@myisp

journalctl --unit=pppd@myisp.service ↩
  --since='30 days ago'
```

(Work in progress... Will appear in Debian later.)

Any questions?

`https://www.linux.it/~md/text/gpon-ihc2018.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)