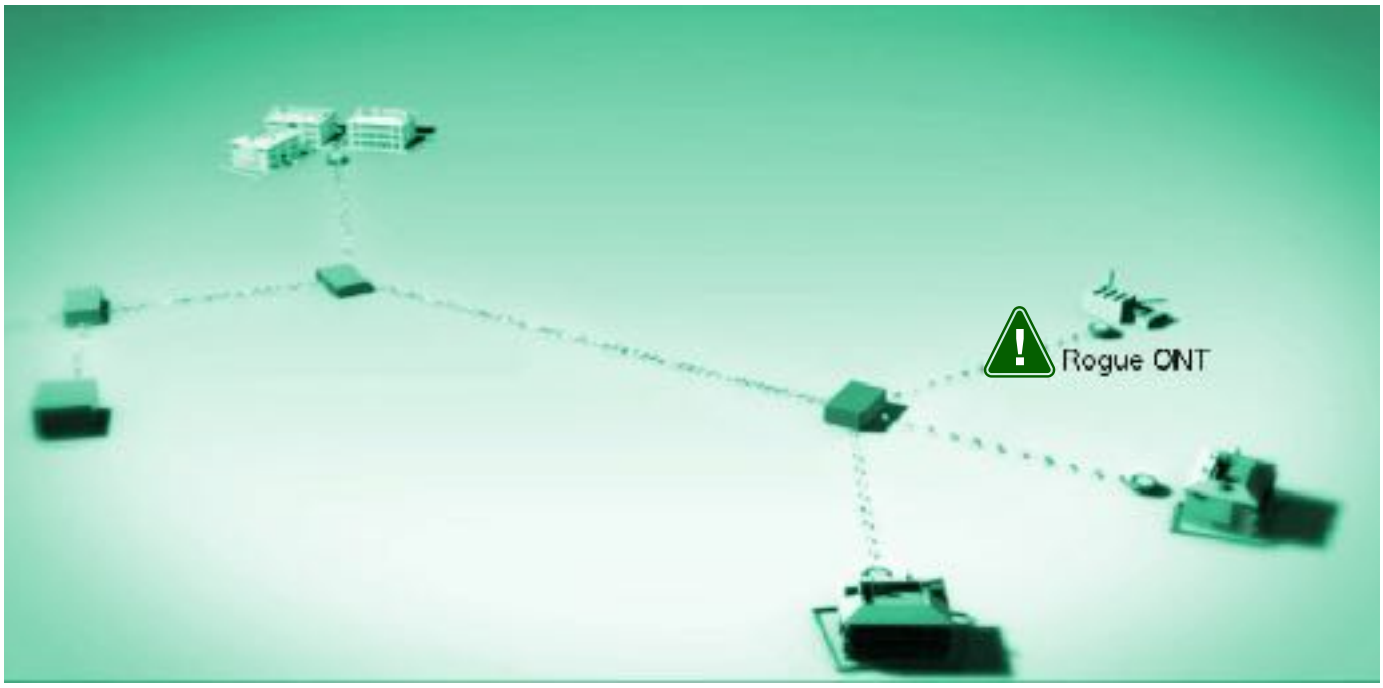


GPONDOCTOR

Roberto Trueba- CTO

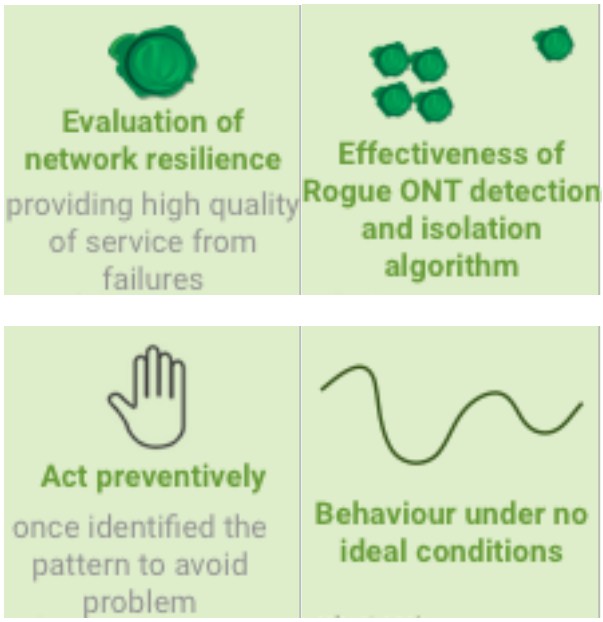
Another GPON channel goes down and you '**do not know why**'?, Is your OLTs' rogue ONT detection and isolation algorithm trustworthy?

Suddenly, a network operation engineer faces again the unexpected but common situation where another PON channel goes down after a long operational state. At the same time, customers that belong to same PON, call the Customer support office to complain about the poor quality of experience and service degradation they are now experiencing. The situation is getting worse, now it's not only service degradation, there are also some connectivity failures. Wow, does this sound familiar? if so, continue reading this white paper.

Let's start by introducing the most usual way to proceed. B/OSS (Business/Operations Support System) gathers all information and identifies the causes of deviation of the network's normal operation. Through the EMS (Element Management System), they get access access to that OLT command line, or even the optical power levels at the CPE, but the

"GPONDoctor Analyzer helps you to evaluate the resilience of your GPON network"

- More than just a GPON Protocol analyzer



events, notifications or alarms data are not enough to understand what is going on. Even more, upstream communication problems may prevent the ONT from transmitting alarms to the OLT or the EMS. And to make things worse, the ONTs are being randomly deactivated by the OLT, which increases the problem's complexity. Therefore, how can this be fixed?

Under these circumstances, You may be facing the problem of a **Rogue** or **Killer ONT**. At this point you may be wondering: what does a rogue ONT mean? How could it be that a previously tested ONT architecture, which was behaving normally for a long time, is now degrading all communications within the FTTH network? How frequent does this happen on FTTH networks? Are there any mechanisms to detect and isolate the rogue ONT?

What does a rogue ONT mean?

Briefly, "a rogue ONT" is an ONT or HGU (Home Gateway Unit) that doesn't transmit within a time-slot defined by the OLT (through BWMaps, time-slot allocations for upstream). According to ITU-T, a Rogue ONT is an ONT that emits power outside of its allocated time-slot (*Supplement 49 to ITU-T G-series Recommendations*).

One possible reason is when the ONT's optical laser becomes defective and drifts out of the assigned time-slot. If this time deviation be larger than the guard time, between two consecutive time-slots, it will cause collisions and impact on subscriber service performance. That ONT becomes "ROGUE" and the OLT will not be able to communicate with it.

How could it be that a previously tested ONT model, behaving normally for a long time, is now degrading the communications within the GPON network?

An example list of conditions that could increase risk, expose or cause a ROGUE behavior:

A) HEC errors in BWMaps (ONT transmission grants issued by the OLT): The ONT cannot repair the allocation, and therefore that allocation is discarded and no traffic is transmitted in the Upstream direction.

B) A failed software instance suddenly "hangs up" which makes the ONT not responding to OLT request or to lose it's State machine synchronization with the OLT.

C) Optical laser becomes defective and impacts on other ONTs communications to the OLTs..

D) CW (Continous Wave) turn laser fails with a condition of "always on" mode, impacting on the entire GPON upstream communication flow.

E) FTTH network growth - more ONTs increasing the MTTF (mean time to failure)

F) ONTs from different vendors - interoperability must be tested and this is tricky. If just the OLT has a software update, was it thoroughly lab tested with every different vendor ONT (even though they may not have a software update). No lab can mimic 100% what you have in the field.

G) Any software upgrade of OLTs, and/or ONUs

H) Any changes to the network that may affect the passive nature, power budget, delay (latency) of services software stacks, or infrastructure.

Are there any mechanisms to detect and isolate a rogue ONT?

Most relevant OLT vendors already incorporate proprietary algorithms for "Rogue ONT" detection and isolation. There are even some ONT manufacturers that also include their own mechanisms. However, the problem is still far from been solved as it is inferred from the continuously increasing large list of patents and reports published in that subject. Telecom operators running GPON networks for recent years are very aware of this situation that failing to detect a rogue ONT leads to Internet or other services interruption. Finding a solution still requires experts with high-tech skills.

Easing the pain with GPONDoctor

GPONDoctor analyzers, plugged in the middle of the PON through an optical splitter, are able to capture all the information exchanged between the OLT and the ONTs. By using a powerful analysis engine they manage to identify, in real time, any deviation from the standard as well as many other useful indicators. But for ROGUE ONT identification, it is of prime importance to understand the events quickly. GPONDoctor, with its advanced, intelligent, test architecture allows modification of the downstream GTC frames, will provide the telecom operator with the perfect tool to identify Rogue ONUs under any circumstance. This must be base-line lab tested upon pre-deployment, with the ability to monitor and identify the failure conditions on your live network using the same tool.

Applications of the "Rogue detection" feature:

- *Test of OLT's "Rogue ONT detection and isolation" algorithm*: By changing the BWMaps addressed to a certain ONT, it is possible to make an ONT behave as "Rogue" as it will transmit in a different time-slot from the specifically assigned slot by the OLT. Thereby, operation engineers will understand how OLTs behave under non-normal ONT behavior, which alarms are generated by the OLT and EMS, what do they mean, and if the OLT deactivate only the rogue unit or all the ONTs in the PON.

- *Check ONT behavior under non ideal conditions*: What an ONT will do when it receives uncorrectable FEC errors or a wrong CRC in BWMAP, What happens if the allocID of the BWMap is changed. These features will help to be prepared when errors are present in the PON (unintentionally or on purpose).

- *Identification and detection of patterns and causes of future network instability:* Severe instabilities on GPON networks are a sequence of small problems, which individually may not have any specific meaning. Therefore, by forcing conditions to generate alarms, events, notifications, and errors, we provide valuable, built-in, intelligent information to determine the full effects of specific patterns. The ability to quickly identify these patterns will allow you to react in real time and restore the normal functionality of the PON in a record time.

In summary, the presence of a "Rogue ONT" within a PON is common place, especially as your network grows, or with typical network changes/upgrades. Thanks to tools like GPONDoctor with its capability of downstream GPON frames editing, it is now possible to minimize the impact on your entire network performance, and vastly reducing your OPEX.