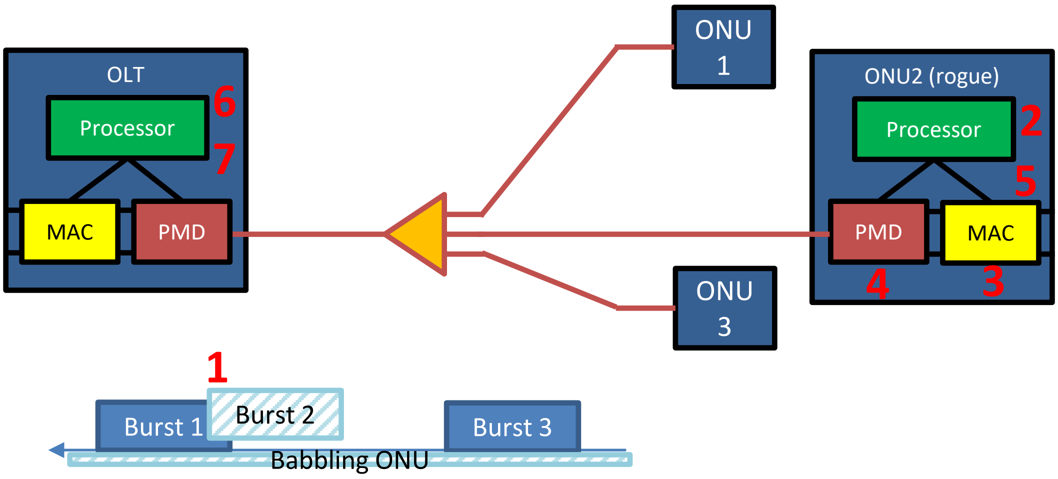
ITU-T Study Group 15

G Suppl. 49 Rogue optical network unit (ONU) considerations

- G.984 family of Gigabit Passive Optical Networks:
  - G-PON, G.984.x series
  - XG-PON (NG-PON1), G.987.x series
  - XGS-PON, G.9807.x series
  - 50G-PON, G.9804.x series
  - NG-PON2, G.989.x series

- Rogue optical network unit:
  - A rogue ONU emits power above the "off power" level outside of its allocated timeslot.
  - In a multi-wavelength PON system, the ONU, in addition, should only transmit in the wavelength channel that it has been assigned to by the OLT.



Rogue ONU causes and prevention

1. ONUs can emit light inappropriately in several ways. A rogue ONU might transmit a normally formed burst at the incorrect time, causing a collision with a valid transmission. Alternatively, the rogue ONU could just transmit continuously, causing increased noise on all the other bursts on the PON.

The following major categories of failures have been know to occur.

2. Software errors: The control software is typically very complex and developed incrementally. Inadvertent errors are likely to happen, and these could result in rogue ONU operation. It is good design practice to make sure that software errors are contained, and the hardware has failsafe mechanisms.

3. Media access control errors: The MAC device is primarily in charge of safeguarding the PON channel. ASICs are quite reliable; however, FPGA-base designs offer several avenues to rogue behaviour. Proper designs should have additional safety mechanisms so that an errant FPGA can’t transmit by mistake.

4. Transmitter hardware error: The transmitter PMD may have a hardware failure that results in the laser being stuck in the ‘on’ position (the so-called “babbling ONU”). Low level hardware monitoring can detect these error conditions and take corrective action.

Rogue ONU detection

5. ONU autonomous monitoring: A properly designed ONU should have sufficient self-checking to ensure that it is operating in the correct way, and if error conditions are found it should shut itself down.

6. OLT-based monitoring: The OLT monitors all the PON transmissions, and keeps track of errored bursts on an ONU by ONU basis. Patterns of these errors can be used to detect possible rogue ONUs.

Rogue ONU isolation, identification, and mitigation

7. A rogue ONU can be isolated / identified in various ways depending on the nature of the ONU fault. For example, if the ONU is found to be transmitting but has failed to respond to PLOAM commands, then that is a strong indicator. The rogue transmissions might be successfully received, and the ONU-ID read that way.

A variety of more invasive tests are possible; for instance, disabling all the ONUs, and then bringing them back online one at a time. This is certainly service affecting, but it may be the only way to track down the problematic ONU. Such tests are best manually triggered.

Once the offending ONU is identified, it should be remediated, by first attempting a reboot, a re-imaging, and then finally a remote disable. Then the ONU can be replaced as soon as possible.

For more information, please visit the ITU-T Study Group 15 website at: www.itu.int/go/tsg15

© International Telecommunication Union 2022