International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series G
Supplement 49
(02/2011)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Rogue optical network unit (ONU) considerations

ITU-T G-series Recommendations – Supplement 49

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 49 to ITU-T G-series Recommendations

Rogue optical network unit (ONU) considerations

Summary

Supplement 49 to ITU-T G-series Recommendations provides additional guidelines relative to ITU-T G.984.x-series and ITU-T G.987.x-series Recommendations, and other passive optical networks (PONs). It addresses the issue of rogue optical network units (ONUs), their prevention, detection, isolation and mitigation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G Suppl. 49	2011-02-25	15

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 49 to ITU-T G-series Recommendations

Rogue optical network unit (ONU) considerations

1 Scope

A passive optical network has a shared medium in the upstream direction, and the passive ODN combines all ONU outputs towards the OLT. Therefore, an ONU that is not transmitting in a manner consistent with parameters specified in the standard can threaten all upstream transmissions on the PON causing interference and disrupting communications of all ONUs on the PON. An ONU that transmits optical power up the PON in violation of the parameters of the standard is called a "rogue ONU".

This kind of situation is not unique to PONs, as many wireless and RF-based systems use the same shared channel scheme. However, under certain hardware and software conditions (attributed to circumstances including design, manufacturing, device failure, environmental, external, or other influences), an ONU may exhibit behaviour that disrupts the operation of other ONUs on the same PON. Such rogue ONU behaviour can cause performance issues or outages for one or more ONUs on the PON. Also, diagnosing and isolating the offending ONU can be difficult since the affected ONUs are not always the ONUs causing the disruption. This Supplement raises the awareness of rogue ONU behaviour and provides system designers and implementers with techniques and tools to facilitate the prevention, detection, isolation, and removal of the offending ONU to avert or minimize service interruptions to other ONUs on the PON.

This treatment distinguishes a rogue ONU from a unit that intentionally or maliciously transmits optical signals that are not in accordance with the standard. In the strictest sense, these devices or intentional jammers are not ONUs, since they are not following the ITU-T Recommendations that describe ONUs. They are essentially illegal devices that intend to deny or steal service from the network. However, these devices may exhibit behaviour and use processes that are similar to rogue ONUs and, therefore, considerations contained in this Supplement may assist in mitigating their potential impact. Security measures are specified in the standard to further assist in reducing threats from malicious sources.

The following clauses consider several rogue conditions that can occur and the design measures that can be employed to address them. Rogue ONU prevention, detection, isolation, and mitigation techniques are intended to avert or minimize service interruptions on a PON when a rogue condition occurs, and are not intended to be a substitute for solid engineering practice and adherence to the standards. Clause 4 provides the expansion of abbreviations and acronyms.

2 Rogue condition causes and prevention

The key requirements in the standard that can be used to determine rogue behaviour are as follows: the ONU should only transmit at its specified "on power" in timeslots that are allocated to it by the OLT, and the ONU should emit less than the "off power" at all other times. (The exact values of the power levels are given in the PMD specification.) An ONU that emits power outside of its allocated timeslot is a rogue ONU. The following clauses describe several conditions that can cause a rogue ONU, and the measures that can be employed to stop them.

2.1 Unauthorized transmission errors

One possible cause of rogue behaviour to consider is the reception by the ONU of errored transmissions from the OLT. It is possible that the bandwidth map allocations can contain errors. The hybrid error correction (HEC) in each entry can correct up to two errors, and detect three positively. Therefore, in most cases, when errors occur, they will be corrected or at least detected.

It is exceedingly unlikely to get a four bit error combination. At the specified post-FEC BER of 10^{-12}, the chances of this happening are 6E-43. If the transmission averages 125 bandwidth map entries per frame, the PON will transmit one million entries per second. The mean time before seeing an undetected error is then 5E+28 years. In addition, such a fault would be transient; therefore, errors of this type are not practically significant.

In the cases where the ONU cannot repair the allocation, then that allocation must be discarded (as required). Using the same assumptions as above, the mean time to an uncorrectable error in an allocation is 7E+17 years (in other words, a very long time). Thus, HEC-13 essentially eliminates the transmission errors.

If each allocation record stood on its own, then that would be the end of the consideration. However, XG-PON specifies an option for concatenated allocations. In cases where an allocation is lost, the ONU should treat the remaining allocations in that burst as lost also, since the content of the lost allocation is not known. Many types of algorithms can be hypothesized that the ONU might use to confirm ownership of the lost allocation. However, the analysis above shows that such errors are so rare that these algorithms may not provide appreciable benefit.

2.2 Software errors

A much more likely source of incorrect transmission can be classified as "software error". Nearly every ONU implementation has a microprocessor that operates under stored program control and that is responsible for configuring the ONU's MAC device. By its very nature, software is very likely to have hidden failure cases that may only emerge years after release. So, it can be envisioned (although hard to quantify) that the software on an ONU might become unstable at some point in its lifetime.

In most cases, a failed software instance will just "hang up". In these cases, the ONU will likely stop responding to commands, and possibly stop passing data, but it is unlikely to exhibit rogue behaviour. The common design solution for this is for the MAC (or processor chip itself) to have a watchdog timer. If the software does not reset this timer periodically, then the timer circuit can assume the software has hung-up, and the circuit will reset the processor and cause a reboot of the ONU's program.

In other cases, the failed software might misconfigure the MAC device. In cases where the MAC device is an application-specific integrated circuit (ASIC), it would be unlikely for the software to accidentally configure parameters that would cause the MAC to enter rogue behaviour. The ASIC will have most of its basic transmission control circuits hard-wired, and the software cannot change them. It is desirable to design the MAC ASIC in such a way that accidental misconfiguration that would result in rogue behaviour is minimized. A cautionary example: many MACs have debugging modes that turn the laser on continuous wave (CW) to make power measurements easier. Activating such a mode should be intentionally difficult, with several unrelated register settings required. This will make a malfunction, including the possibility of intentionally or unintentionally setting the laser into continuous mode, less likely.

However, if the MAC device is a field programmable gate array (FPGA), then it is easy for failed software to overwrite the FPGA's programming with damaging consequences. Essentially, this would mean that the software error condition would have spread to the MAC. This case could be solved using the methods in the next clause.

In the case where the software has failed and induced the ONU to rogue behaviour, the protocol has a disable serial number message that may assist in recovery. It is desirable that the disable message be processed in the MAC itself, outside of the software's area of control. In that way, if an ONU's software has failed and the ONU has entered a rogue state, the OLT can positively force the rogue ONU to shut down by issuing the disable message to it.

2.3 Media access control errors

The media access control (MAC) device is the hardware that controls the optical transceiver. If the MAC has become defective for some reason, it can easily make the ONU rogue. As mentioned above, ASIC-based MACs are very reliable, since they are hard-wired to obey the recommended transmission protocols, and they are tested to a degree that design errors are quite rare. So, the source of an ASIC error is most likely a hardware-layer fault (a faulty transistor, for example).

FPGA-based MAC failures are much more likely, in that their programming could be loaded incorrectly, and then the behaviour is undefined. A cautionary example: when an FPGA-based ONU reboots, reloading the firmware into the FPGA is typically part of the boot sequence. While this is happening, the MAC is essentially broken. Care should be taken to ensure the laser remains off during this time.

Therefore, it is possible for MAC errors to occur that result in rogue behaviour. In some cases, the faulty MAC may still be responsive to the disable message, and the problem could be resolved in this way. In other cases, the disable feature will be unresponsive. To recover from this type of failure, another part of the ONU must shut down the laser. There are two possibilities: the software, and the transceiver itself.

It is desirable for the processor to have a negative control (forcing off) on the transmitter, for this purpose. If this is true, then when the software detects (through an algorithm) that the ONU is improperly transmitting a signal, it can shut down the transmitter by overriding the MAC. This negative control may also have applications in power saving as well.

It is desirable for the transceiver to be able to ignore the MAC's faulty instructions. If this is true, the transmitter can become a "conscientious objector", and it will ignore the illegal orders from its MAC. The range of invalid commands is large, and the transceiver circuitry is very simple; therefore, it is impossible to detect all invalid errors. But, simple errors are easy to detect. For example, if the Tx-enable signal goes on for a very long time (e.g., more than 1 ms), that is most likely a mistake. It is desirable that a simple burst duration monitor (anti-babbling) be incorporated into the transceiver.

2.4 Transceiver error

The last link in the transmitter control chain is the transmitter itself. The transceiver is typically very simple, with only a handful of transistors between the Tx-enable pin and the laser. However, one can have a failed transistor, and the transmitter would nevertheless remain on. It is desirable that the transmitter be designed so that there is no single component failure that will allow the laser to emit. The ordinary burst-mode Tx-enable path would be the primary control of the laser, but there should be at least one additional path or means of control to disable the laser or indeed the entire transmitter. For example, this could involve turning the modulation or bias current sources off, or powering down the whole transmitter module. Such controls do not need to be fast (millisecond-scale speeds are sufficient). Additionally, such controls can also be useful for power saving features.

Control of the emergency shutdown circuit can come from multiple sources: the software, the MAC, and even the transceiver itself can detect the failure. It is desirable for each of these oversight functions to have an independent path to the Tx shutdown feature. In this way, if any entity believes rogue behaviour is happening, the Tx will be pulled down.

One final means of control is through the internal ONU signal path. It is desirable to cease transmitting a modulated signal if the Tx is stuck in the "on" position. A transmitter emitting CW light may disrupt the PON by degrading the receiver sensitivity. The degree of disruption and service impact to other ONUs on the PON may vary.

3 Rogue detection, isolation, and mitigation

The ONU transmits to the OLT in a timeslot provided by the OLT in the BWmap allocation. Drifts in the ONU transmission timing can occur over time, and may be compensated in the OLT by the use of equalization delay changes. However, to avoid potential rogue behaviour, the OLT needs to monitor for transmissions from an ONU outside of the allocation assignment and the ONU needs to be aware of whether it is transmitting in the assigned timeslot or not.

Faults can also occur which cause an ONU to transmit data outside of its timeslot, such as when a laser is stuck "on" or an ONU transmits continuously. This type of unauthorized traffic can impair communications to all ONUs on the PON. In some cases, the condition may clear itself, or the condition may cause intermittent or low-level impairment on the PON which does not trigger an alarm. Therefore, it is necessary to have transmission monitoring to both the OLT and the ONU to detect upstream transmissions from an ONU that is experiencing a fault condition. Monitoring and analysis of the ONU upstream transmission would prevent the condition where an ONU transmitting unauthorized data traffic would go undetected.

The following highlights basic methods that may be employed to detect, isolate, and mitigate rogue ONUs. These methods supplement processes contained in the preceding clauses and are enabled by capabilities contained in ITU-T G.984.x-series and ITU-T G.987.x-series Recommendations.

3.1 General

To mitigate the possibility of a rogue ONU disrupting communications on a PON, both the OLT and the ONU should individually monitor their activities, be able to detect behaviour that could result in a rogue condition, and take action to remove the offending ONU from the PON.

a) The capability to shut off the ONU laser should be available in the ONU as rogue behaviour can result in impaired communications from the OLT.

b) All alarms generated by the OLT and ONU as a result of a rogue condition should be made available in the EMS to the extent possible. In some cases, upstream communications problems may prevent the ONU from transmitting the alarms.

3.2 Detection

The following methods will assist in detecting rogue ONU behaviour.

a) The ONU watchdog timer will be used to monitor upstream data and recognize transmissions that occur outside of the transmission window.

b) If the ONU watchdog timer recognizes that the ONU is improperly transmitting, the ONU should attempt to signal an alarm (e.g., ONU problem, laser shutting down), and then turn the laser off.

c) Autonomous OLT and ONU monitoring could be used to identify a potential rogue condition. The OLT should monitor the upstream channel continuously to judge if the PON is well ordered or if there are potential problems, e.g., out-of-sequence alarms. Problem conditions should be alarmed and the offending ONU identified if possible.

d) The OLT should monitor all PON activity and ONUs monitor their own activity to identify rogue behaviour, including:

  - power in incorrect timeslots
  - failed drift compensation when ONU drifts out of the assigned timeslot and it is not automatically corrected

e) The ONU should have the capability for its output transmitter signal/power level to be monitored and included in a feedback loop to:

- ensure that the transmitter is only transmitting in the timeslot that the laser has permission to transmit in
- have the ability to monitor if any power is being transmitted outside the allotted timeslot
- have the capability to measure the modulation/bias current of the transmitter to ensure it is within specifications
- have the ability to take appropriate action to ensure it is not operating outside of specifications.

3.3 Isolation

The following methods are intended to assist in isolating rogue ONU behaviour.

a) User-initiated tools should be available for the isolation of a rogue ONU. These tools should have negligible impact on services. Feature possibilities include:

- directed assignment of ONUs to specific timeslots as a means of isolating the rogue ONU
- correlation of individual PON performance metrics to the relative positions of the ONU timeslots
- systematically disabling/enabling ONUs on PON to identify ONUs functioning properly and isolate the rogue ONU.

b) User-initiated query tool should be available to identify a potential rogue ONU and have the ability to analyse the entire PON, or individual ONUs on a PON. These tools should not be service affecting and data should not be lost during the discovery event. The query results may include, but are not limited to, BIP errors (upstream/downstream) and timeslot violations per ONU. BIP errors may be detectable even if jammed transmissions are not decipherable. The tool would provide statistics that might not be alarmed and may indicate a PON/ONU in trouble but not completely impaired.

3.4 Mitigation

The following methods will assist in mitigating rogue ONU behaviour.

a) When an ONU initially ranges on a PON, the number of failed ranging attempts should be configurable by the operator. If the configurable number of consecutive failed ranging attempts is reached, the OLT should attempt to shut down the ONU transmitter so that it no longer participates in future ranging attempts.

1) If the configurable number of failed consecutive ranged attempts is exceeded, then this condition should be alarmed using an EVENT indication, and an attempt made to place the ONU into the Emergency Stop (eSTOP) state.

2) The ONU should remain Disabled and not transmit data on the PON until directed to by the OLT. This action is intended to assist in preventing an ONU that may have problems as indicated by excessive ranging attempts from entering the PON.

b) If the OLT maintains the database of known ONUs and at a subsequent discovery attempt a persistent rogue behaviour is detected by an ONU whose serial number cannot be determined, the rogue ONU can be assumed to be in the database. In such a case all the serial numbers in the database that are not currently active can be disabled. The condition should be alarmed and an attempt made to signal those ONUs into the Emergency Stop (eSTOP) state using the stored serial number. Those ONUs should remain Disabled and not transmit data on the PON until directed to by the OLT. The OLT may further attempt to enable the suspected ONUs one-by-one in order to identify the rogue ONU.

c) There are two cases of rogue optical behaviour as seen by the OLT. In one case, the optical power of the rogue ONU is so low that in its designated time slot, the OLT would receive a low optic receive level. In the other case, the rogue is constantly on at full power, resulting in normal average power readings for the rogue ONU's time slot, but higher average power readings in other ONU time slots.

   1) The OLT should be able to determine if the ONU upstream receive power level for a particular ONU time slot falls below the minimum required value. If it does, it may contribute to or be an indicator of, rogue behaviour, for example, a rogue ONU that is partially on. The minimum upstream receive power level should be based on the receiver sensitivity of the appropriate optical class and should be configurable.

   2) The OLT should be able to determine if the ONU upstream receive power levels for ONUs on the PON in general are higher than their normal value. This may be an indicator of a rogue that is stuck on at full power. The upstream receive power level for each ONU should be compared to historical receive power levels. A power increase of 3 dB or more may indicate rogue behaviour of another ONU. The power level threshold should be configurable.

   3) If the ONU upstream receive power level falls below the minimum required value (see paragraph 3.4c1), or above the high power threshold (see paragraph 3.4c2), then this condition should be alarmed and the ONU placed into the Emergency Stop (eSTOP) state. The ONU should remain Disabled and not transmit data on the PON until directed to by the OLT.

d) The ONU should have the capability to monitor its own behaviour and autonomously turn off the laser if a fault condition is detected. This capability would serve as a secondary measure in the event that the primary method to turn off the laser via the OLT is not possible.

   1) The ONU should turn its laser off if it detects rogue behaviour in order to prevent possible harm to the PON.

   2) The ONU should attempt to send a message to the OLT to indicate why the ONU is going out of service.

e) The ONU transmitter default state (e.g., at installation) should be in the "off" position. This is a precaution to prevent, for example, cases where there is a failure to prevent the transmitter from being shut off, resulting in potential rogue behaviour.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ASIC	Application-Specific Integrated Circuit
BIP	Bit Interleaved Parity
EMS	Element Management System
FPGA	Field Programmable Gate Array
HEC	Hybrid Error Correction
MAC	Media Access Control
ODN	Optical Distribution Network
OLT	Optical Line Terminal

ONU	Optical Network Unit
PMD	Physical Medium-Dependent (sub-layer)
PON	Passive Optical Network

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011