International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series G

Supplement 49

(09/2020)

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 the applicable existing passive optical network (PON) systems specified in the respective ITU-T Recommendations, and other PONs. It addresses the issue of rogue optical network units (ONUs), their prevention, detection, isolation and mitigation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G Suppl. 49	2011-02-25	15	11.1002/1000/11322
2.0	ITU-T G Suppl. 49	2020-09-18	15	11.1002/1000/14545

Keywords

GPON, higher speed PON, isolation, mitigation, NG-PON2, ONU, PON, rogue, rogue behavior, rogue ONU, XGS-PON.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

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 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 optical distribution network (ODN) combines all ONU outputs towards the optical line terminal (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 passive optical network (PON), causing interference and disrupting communications of other ONUs on the PON. An ONU that has been designed, produced and deployed with an intent to be compliant with the standards, but as a result of a design flaw, a manufacturing error, hardware or software failure, environmental or other external impact, transmits optical power up the PON to the OLT in violation of the parameters of the standard is called a "rogue ONU".

This kind of rogue behaviour is not unique to PON systems, but may exist in any communication system that uses the same shared channel scheme, leading to the situations where a single rogue device may impact other devices or disrupt the operation of the entire system. Diagnosing and isolating the offending device can be difficult since the affected devices are not always the ones causing the disruption. In the context of PON systems, this Supplement raises 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 do not follow 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, the techniques considered in this Supplement may facilitate their detection.

The remainder of this Supplement is structured as follows.

Clause 2 lists the acronyms and abbreviations used herein.

Clause 3 discusses potential causes of the rogue ONU behaviour and describes general rogue behaviour prevention techniques.

Clause 4 presents possible techniques for rogue ONU detection.

Clause 5 presents possible techniques for rogue ONU isolation and mitigation.

Clause 6 discusses the best operational practices and strategies in dealing with rogue ONUs and actual PON deployments.

In comparison with the original release of this Supplement (02/2011), the present release addresses:

– Spectral aspects of rogue ONU behaviour;
– Leveraging multi-wavelength capabilities of TWDM PON system for rogue ONU isolation and mitigation;
– Advances in rogue interference detection;
– Advances in rogue ONU isolation;
– Best operational practices in application of rogue ONU detection, isolation and mitigation techniques.

2 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AC	Alternating Current
ASIC	Application-Specific Integrated Circuit
BER	Bit-Error Rate
BIP	Bit Interleaved Parity
BWmap	Bandwidth map
CT	Channel Termination
CW	Continuous Wave
EMS	Element Management System
eSTOP	Emergency Stop (state)
FEC	Forward Error Correction
FPGA	Field Programmable Gate Array
HEC	Hybrid Error Correction
ICTP	Inter-Channel-Termination Protocol
MAC	Media Access Control
ODN	Optical Distribution Network
OLT	Optical Line Terminal
ONU	Optical Network Unit
PMD	Physical Medium-Dependent (sub-layer)
PLOAM	Physical Layer Operations, Administrations and Maintenance
PON	Passive Optical Network
TWDM	Time and Wavelength Division Multiplexing
Rx	Receiver
Tx	Transmitter

3 Rogue condition causes and prevention

In a single-channel PON system, 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 physical medium-dependent (PMD) specification.) An ONU that emits power above the "off power" level outside of its allocated timeslot is a rogue ONU. 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.

The following clauses describe several conditions that can cause a rogue ONU, and the measures that can be employed to stop them.

3.1 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 contain errors.

The 13-bit hybrid error correction (HEC) in each 64-bit 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 6×10^{-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 5×10^{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 7×10^{17} years (in other words, a very long time). Thus, HECeffectively eliminates the transmission errors within the protected field.

If each allocation record stood on its own, then that would be the end of the consideration. However, since in a burst allocation series only the first allocation carries the StartTime, an interpretation of each subsequent allocation is contingent upon correct interpretation of preceding 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.

3.2 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 which is responsible for configuring the ONU's media access control (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 in 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 difficult by design, 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 described 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.

3.3 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 as 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 an error. It is desirable that a simple burst duration monitor (anti-babbling) be incorporated into the transceiver.

3.4 Transmitter hardware 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 transmitter (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.

4 Rogue ONU detection

The ONU transmits to the OLT in a timeslot provided by the OLT in the bandwidth map (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 text highlights basic methods that may be employed to detect, isolate, and mitigate rogue ONUs. These methods supplement the prevention techniques discussed in the preceding clause and are enabled by the standard-based capabilities of the existing PON systems specified in the respective ITU-T Recommendations.

4.1 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 element management system (EMS) to the extent possible. In some cases, upstream communications problems may prevent the ONU from transmitting the alarms.

4.2 Specific detection techniques

The following methods will assist in detecting rogue ONU behaviour.

A. ONU autonomous monitoring:

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

b) The 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.

c) 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.

Whenever autonomous ONU monitoring leads to recognition 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.

B. OLT-based monitoring for rogue conditions:

a) Monitoring for upstream transmission drift and drift compensation failures.

b) Monitoring for unexpected well-formed upstream bursts within optical silence intervals.

c) Monitoring for presence of optical power within optical silence intervals.

d) Monitoring for abnormal level and patterns of forward error correction (FEC) errors within upstream transmission.

e) Monitoring for abnormal level and patterns of BER errors with upstream transmission.

f) Monitoring for upstream burst delineation failures.

Each OLT monitored condition has to have a corresponding separate alarm which should be subject to configuration on per OLT channel termination basis. If a detection mechanism has some threshold to cross before declaring an alarm, then the threshold should be configurable as well.

5 Rogue ONU isolation, identification, and mitigation

5.1 Isolation and identification

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, bit interleaved parity (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.

c) The upstream Tx modulation and Tx-enable operation are largely independent. When in "off burst" mode, the modulation signal for the transmitter is unspecified in the standards. A common practice is to modulate the disabled Tx with an alternating 1/0 pattern to keep the AC coupling circuit charged. An alternative option is to modulate the disabled Tx with a well-formed burst containing preamble, delimiter, and a standard-compliant framing sublayer header, which includes the ONU-ID, thus providing an identification of the transmission source. The advantage of the latter option is that if the ONU becomes rogue through an undetected failure to disable the Tx, a transmission landing at a silence interval would provide the OLT with a straight-forward identification of the offending ONU.

d) A modification to item (c) above has been proposed that would extend the "off-burst" modulating signal to include a physical layer operations, administrations and maintenance (PLOAM) message of a specified type. Two PLOAM message types were considered for that

purpose: Serial_Number_ONU and Registration PLOAM. Three observations have to be made:

i) If a rogue burst is well formed and contains a valid ONU-ID, no additional identification is needed.

ii) Normally, an OLT CT attempts to parse the 48 bytes following the burst header as a PLOAM message, only if the burst has been correlated with the allocation structure that has the PLOAMu flag set. In case of a rogue burst, there is, by definition, no allocation structure to correlate it with, and no PLOAMu flag value is known.

iii) If an OLT CT receives a burst with an un-assigned ONU-ID, which normally is the case if and only if there is serial number grant to correlate the burst with, the OLT CT parses the remainder of the burst as a Serial_Number_ONU message.

5.2 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 (1)), or above the high power threshold (see paragraph (2)), 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 transmitter by default (e.g., at installation) should be in the "off" state and require explicit enabling to become active. This is a safety precaution to prevent, for example, a potential failure to shut off, resulting in rogue behaviour.

5.3 Systematic approach to Rogue ONU isolation, identification, and mitigation

The specific rogue ONU isolation, identification, and mitigation operations can be elementary or composite.

Elementary operations involve issuing a single PLOAM message, or performing bandwidth map modification. In multi-wavelength PON systems, an additional type of elementary operations is available, namely, issuing a single Inter-Channel-Termination protocol (ICTP) message.

The elementary operations may include:

– Disabling an ONU by its discovered serial number; that is, placing a specific ONU in the Emergency Stop (O7) with the targeted Disable_Serial_Number PLOAM message.

– Disabling all ONUs subtending to the given OLT CT with the Disable_Serial_Number PLOAM message addressed to all tuned-in ONUs.

– Disabling the ONUs, that attempt activation and whose serial numbers have not yet been discovered, with the Disable_Serial_Number PLOAM message using the Disable_Discovery operation code.

– Deactivating an ONU with a specific ONU-ID using the Deactivate_ONU-ID PLOAM message.

– Adjusting the equalization delay of a specific ONU with a Ranging_Time PLOAM message.

– Temporary withdrawal of all bandwidth allocations to a given ONU without disabling the ONU.

– Temporary suppression of quiet windows on the PON.

– Temporary Bandwidth map modification with increased inter-burst guard times.

– Temporary Bandwidth map modification with rearranged ONU transmission order.

– Issuing an ICTP message of rogueAlert() or rogueClear() type.

– Issuing an ICTP message of rogueActionTaken() type.

Composite operations contain multiple elementary operations, condition checks and decision steps, and may include:

– Systematic withdrawal of all bandwidth allocations to the active ONUs.

– Systematic disabling and re-enabling of the active ONUs.

– Controlled handover of a given ONU to a specified wavelength channel.

– Systematic transfer of active ONUs to a different wavelength channel(s).

5.4 ONU Emergency Stop management

An ONU with a specific SN can be disabled (placed in the Emergency Stop, or eSTOP state) intermittently, in the course of executing a rogue ONU isolation and identification procedure, or permanently, as a primary rogue ONU mitigation technique. An ONU that have been positively identified as rogue is prohibited from operating on the PON, it is placed in the eSTOP state

permanently and should remain disabled. Placing an ONU into and removing an ONU from eSTOP state is achieved with the Disable_Serial_Number PLOAM message using appropriate parameters.

1) Placing an ONU into Emergency Stop state.

In single-channel PON systems, the OLT CT should take into account the possibility of an accidental loss of the PLOAM message due to intermittent reasons. To that end, the OLT CT periodically reissues the targeted Disable_Serial_Number PLOAM message using the Disable operation code while time-to-time providing allocations to the disabled ONU's ONU-ID to confirm that no upstream transmission occurs in response. The provisions should be made for restoration of the log of the ONUs in the eSTOP state upon line card reboot, power cycle or replacement.

In a multi-wavelength PON system, the OLT should in addition take into account the possibility of uncontrolled wavelength channel change by the ONU. Placing of the ONUs into eSTOP state should be coordinated across the OLT CTs of the multi-wavelength system using ICTP with the distinction being made between in the intermittent and permanent disabling of the ONUs. Thus, each OLT CT in a multi-wavelength system should maintain an eSTOP log of the ONUs across the entire system, and be able to restore the log upon line card reboot, power cycle or replacement.

2) Removing an ONU from Emergency Stop state.

In a multi-wavelength PON system, once a decision to remove an ONU from the eSTOP state is made, this decision should be communicated over ICTP to all OLT CTs of the system which mark the ONU in their respective Emergency Stop logs as cleared. Once this is done, each OLT CT periodically issues the targeted Disable_Serial_Number PLOAM message using the Enable operation code while providing serial number grant allocations on the PON, as is the case with a single-channel PON system. Once an OLT CT detects a successful activation attempt in the local TWDM channel by the ONU which has been marked as cleared in its Emergency Stop log, it notifies the peer OLT CTs that the ONU has been discovered. The OLT CTs then remove the ONU from their Emergency Stop logs.

6 Best operational practices

The rogue interference detection techniques should be non-invasive, should be applied by the OLT in a fully automated fashion and amount to continuous monitoring of a well-defined set of conditions.

Each monitored condition has to have a corresponding separate alarm which should be subject to configuration on a per OLT Channel termination basis. If a detection mechanism has some threshold to cross before declaring an alarm, then the threshold should be configurable as well.

The rogue isolation, identification and mitigation techniques, which are necessarily service-affecting, should allow both automatic and manual invocation. At the early stages of a PON system deployment, only manual invocation of such techniques should be supported.

For each monitored rogue interference condition (as indicated by the corresponding alarm), it should be possible to specify a procedure involving a combination of elementary and composite operations with necessary additional condition checks and decision steps, to be autonomously executed by the given OLT CT upon raising the corresponding rogue interference alarm.

Automatic execution of thus specified procedures should remain at operator discretion and should be subject to an explicit enable operation, which the operator can enact at a later stage of a PON system deployment, when sufficient operational experience is accumulated.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020