International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series G

Supplement 51

(06/2017)

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

Passive optical network protection considerations

ITU-T G-series Recommendations – Supplement 51

International Telecommunication Union

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 51 to ITU-T G-series Recommendations

Passive optical network protection considerations

Summary

Passive optical networks (PONs) can generally be considered point-to-multipoint networks, much like wireless networks such as wireless fidelity (Wi-Fi), 2G–4G or the hybrid fibre coax (HFC) networks used by multiple system operators. Redundancy is generally not fundamental in these networks as contrasted with ring-based topologies.

Nonetheless, there are services such as business services, mobile backhaul and high-density residential services, which may justify the addition of PON redundancy and protection switching.

Recommendation ITU-T G.984.1 outlines several topologies for achieving redundancy; these have been named type A, type B, type C and type D. Since the publication of ITU-T G.984.1, many other studies of various aspects of PON availability, redundancy and switching have been made available.

The ITU-T G.987 series, ITU-T G.989 series and ITU-T G.9807.1 describe the 10-Gigabit-capable passive optical network (XG-PON), the 40-Gigabit-capable passive optical network (NG-PON2) and the 10-Gigabit-capable symmetric passive optical network (XGS-PON) systems. Each of these further describe protection aspects of those systems. In particular, the details of automatic protection switching in type B has been more fully worked out.

This Supplement collects this information and, guided by input from operators, distils it into use cases and methods that are recommended for adding redundancy and increasing the reliability of PON networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G Suppl. 51	2012-05-11	15	11.1002/1000/11652
2.0	ITU-T G Suppl. 51	2016-02-26	15	11.1002/1000/12841
3.0	ITU-T G Suppl. 51	2017-06-30	15	11.1002/1000/13342

* 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

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

		Page
1	Scope	1
2	Abbreviations and acronyms	1
3	Background – Fibre protection	3
3.1	PON system components – Failure rates	3
3.2	Failures in time and mean time between failures	3
4	PON protection use cases	4
4.1	Large numbers of subscribers per PON line card	4
4.2	Business and mobile backhaul services	5
4.3	PON reach extenders	5
4.4	Emergency services	5
4.5	PON maintenance	5
5	Protection architectures	6
5.1	Type A	6
5.2	Type B	7
5.3	Dual-parented type B protection	7
5.4	Type C protection	8
5.5	Extra traffic for type C protection	9
5.6	Type C protection using link aggregation	9
5.7	Type D – Deprecated	9
5.8	Type B with N:1	9
6	Availability and switching speed goals	10
6.1	Availability in an unprotected PON	10
6.2	Assumptions for availability calculations	11
6.3	Availability of an unprotected PON	12
6.4	Protection path monitoring	12
6.5	Switching speed and impact on availability	12
7	Fast failure detection	14
8	Fast protection switchover mechanisms	15
8.1	Ranging before switchover (pre-ranging)	16
8.2	Ranging after switchover (limited re-ranging)	18
8.3	No pre-configuration of standby OLT EqD values per ONU (fast ranging)	19
8.4	Equalization-delay-agnostic protection switch	20
8.5	Typical practice of fast protection switchover mechanisms and viability analysis	20
9	Recommended architectures versus use cases	25
10	Ethernet linear protection switching to support type B PON protection	25
10.1	Protection switching service characteristics	26
10.2	OLT PON port type B Protection State Machine	27

Page
10.3 Initial connection configuration 33
10.4 Description of end to end protection switching..... 34
Bibliography..... 36

Supplement 51 to ITU-T G-series Recommendations

Passive optical network protection considerations

1 Scope

Passive optical networks (PONs) are point-to-multipoint networks, much like wireless networks such as wireless fidelity (Wi-Fi), 2G–4G or the hybrid fibre coax (HFC) networks used by multiple system operators. Redundancy is generally not fundamental in these networks when compared to ring-based topologies.

Nonetheless, there are services such as business services, mobile backhaul and high-density residential services that may justify the addition of PON redundancy and protection switching.

[b-ITU-T G.984.1] outlines several topologies for achieving redundancy; these have been named type A, type B, type C and type D. Since the publication of [b-ITU-T G.984.1], many other studies of various aspects of PON availability, redundancy and switching have been made available.

This Supplement collects this information and, guided by input from operators, distils it into use cases and methods that are recommended for adding redundancy and increasing the reliability of PON networks.

2 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

2G–4G second Generation to fourth Generation

10G-EPON 10-Gigabit Ethernet Passive Optical Network

BA Bandwidth Allocation

BNG Broadband Network Gateway

BW Bandwidth

CCM Continuity Check Message

EMS Element Management System

E-PON Ethernet Passive Optical Network

EqD Equalization Delay

FIT Failure in Time

FTTH Fibre to the Home

FWI Forced Wakeup Indicator

G-PON Gigabit-capable Passive Optical Network

HFC Hybrid Fibre Coax

IGMP Internet Group Management Protocol

ISDN Integrated Services Digital Network

LAG Link Aggregation

LOF Loss of Frame

LOS Loss of Signal

LSB Least Significant Bit

MAC	Media Access Control
MEG	Maintenance Entity Group
MEP	Maintenance entity group Endpoint
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NG-PON2	40-Gigabit-capable Passive Optical Network
NMS	Network Management System
OAM	Operations, Administration and Maintenance
OAN	Optical Access Network
ODN	Optical Distribution Network
OLT	Optical Line Terminal
ONU	Optical Network Unit
PLOAM	Physical Layer Operations, Administration and Maintenance
PON	Passive Optical Network
POTS	Plain Old Telephone Service
QoS	Quality of Service
RE	Reach Extender
RTD	Round-Trip Delay
RTT	Round-Trip Time
SDi	Signal Degrade
SFi	Signal Fail
SLA	Service Level Agreement
SME	Small to Medium-sized Enterprises
SNI	Server Node Interface
S-VID	Service VLAN Identifier
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
UNI	User Network Interface
VID	VLAN Identifier
VLAN	Virtual Local Area Network
WDM	Wavelength Division Multiplexing
Wi-Fi	Wireless Fidelity
XG-PON	10-Gigabit-capable Passive Optical Network
XGS-PON	10-Gigabit-capable Symmetric Passive Optical Network

3 Background – Fibre protection

Optical access networks (OANs) are now delivering multimedia services including data, voice and video. OANs also serve as mobile backhaul connecting wireless towers to metro or core networks. Although the physical media in the last (or first) mile could be different from fibre, OANs are an integral part of any broadband access network. Most OANs use passive optical network (PON) architectures.

As society moves towards 'everything in cloud', 'everything on a click', 'remote working', 'global collaboration', 'e-business' and 'social networking', a single network failure can disrupt services of hundreds of users and have a cascading effect. Users will find it unacceptable because their survival and well-being are now highly dependent on the health of the access networks. The access network will be considered an essential service. Thus, to meet service level agreements (SLAs) and guarantee the appropriate level of connection availability, fault management within any type of PON becomes more significant for reliable service delivery and business continuance. Failure of any network component will interrupt the service resulting in a significant loss of revenues. Service subscribers expect the quality of service (QoS) to be at least at the same level as that provided by the copper-based plant. Currently, PONs are mostly poorly protected or not protected at all. Fibre cuts are not the only issue. Failure may occur in the optical line terminal (OLT), optical network unit (ONU) power splitter or optical amplifier, if employed.

3.1 PON system components – Failure rates

There have been several reports on failure rates and time to repair for PON system components. Failure rates differ widely and depend on geography, environment, assumptions and component design, at a minimum. Table 1 is a compilation of the component failure rates taken from these references and has references to the various sources used for failure rates and times to repair for the different elements of the network.

3.2 Failures in time and mean time between failures

The failure of some network elements has more impact on services than others. For example, ONU failure or distribution fibre cuts affects only one user. But a failure of OLT, feeder fibre or a remote node can shut down the entire PON. Mean time to repair (MTTR) will also be different for different network elements. Table 1 summarizes some statistical data relating to unavailability of the network due to failure of network components. Here, the FIT column lists the failure frequency over 10^9 h and MTTR applies to each failure.

Unavailability is defined as the probability that the equipment, service or fibre is unavailable at any time and can be defined mathematically as:

Network unavailability due to a component failure = FIT × MTTR × 10^{-9}

Another measure of failure rates is the mean time between failures (MTBF). This is the average time between failures for an MTBF (h) = 10^9/FIT.

FIT versus MTBF will be used for the rest of this Supplement.

Table 1 – Survey of failure rates and repair times for PON components in published literature

Equipment	Reference	FIT	MTTR (h)	Unavailability
OLT	[b-Alcoa]	NA	NA	NA
	[b-Chen, 2008]	2 500	4	1×10^{-5}
	[b-Hajduczenia]	7 000	5	3.5×10^{-5}
	[b-Chen, 2010], [b-Tsubokawa]	NA	NA	NA
ONU	[b-Alcoa]	NA	NA	NA
	[b-Chen, 2008]	256	24	6.1×10^{-6}
	[b-Hajduczenia]	2 500	12	3×10^{-5}
	[b-Chen, 2010], [b-Tsubokawa]	NA	NA	NA
Deployed optical fibre cable (Note 1)	[b-Alcoa]	10/km–250/km (Note 2)	NA	NA
	[b-Chen, 2008]	NA	NA	NA
	[b-Hajduczenia]	200/km	14	2.8×10^{-6}
	[b-Chen, 2010], [b-Tsubokawa]	18/km	6	6×10^{-11}
Splitter	[b-Alcoa]	NA	NA	NA
	[b-Chen, 2008]	50–120	24	1.2×10^{-7} to 2.9×10^{-6}
	[b-Hajduczenia]	200	12	2.4×10^{-6}/km
	[b-Chen, 2010], [b-Tsubokawa]	50–100	6	3×10^{-7} to 6×10^{-7}
Optical switch	[b-Alcoa]	NA	NA	NA
	[b-Chen, 2008]	200	14	4.8×10^{-6}
	[b-Hajduczenia]	NA	NA	NA
	[b-Chen, 2010], [b-Tsubokawa]	NA	NA	NA

NOTE 1 – [b-GR-418] requires no more than 400 FIT/mile, equal to 250 FIT/km. Also, the MTTR for [b-GR-418] is 6 h not 24 h.

NOTE 2 – [b-Alcoa] distinguished between aerial and buried fibre. Aerial = 10 FIT/km, buried 250 FIT/km. The 250 FIT/km may be a result of poor control of utility digging policies; it should be seen as an upper bound (as evidenced by the fact that [b-GR-418] has a requirement of less than 250 FIT/km).

NOTE 3 – Some data shown are based on Table 5.1 of [b-Chen, 2008], and [b-Alcoa].

4 PON protection use cases

There are many applications where PON protection will be desired or necessary. Some use cases are described here.

4.1 Large numbers of subscribers per PON line card

Larger numbers of subscribers are enabled with higher speed PONs, high density PON line cards and large split ratios due to larger link budgets (e.g., C+ optics and XG-PON extended link budgets).

There are already several large-scale PON deployments around the world based on the Ethernet passive optical network (E-PON) or Gigabit-capable passive optical network (G-PON). Efforts are under way to mature XG-PON or 10-Gigabit Ethernet passive optical network (10G-EPON) technologies cost-effectively. With their deployment, the subscriber count per PON can increase several fold. In addition, higher density PON line cards service larger subscriber counts even without increased split ratios. Since cost of protection will be shared by a large number of subscribers, PON protection will become more cost effective even as it becomes more necessary. Given these are generally residential services, "five 9s" (availability 99.999% of the time) may or may not be necessary.

4.2 Business and mobile backhaul services

Business and mobile backhaul services have higher availability requirements, normally five 9s or higher, based on SLAs. They cannot afford network outages even for a very short period, as this could have very serious negative consequences to their business. For these customers, additional costs of protection will be less important than keeping the communication working.

4.3 PON reach extenders

To bring about the cost and energy savings required for next-generation PONs to remain economically viable, there are emerging requirements from operators for node consolidation and reduction of real estate with the associated benefits of operational cost reduction. With the centralization of equipment comes a vulnerability of the network to large-scale outages in the event that a node is rendered out of service due to some catastrophic event such as fire, earthquake or flood. Such networks are likely to also have an active remote node that will employ optical amplifiers increasing the probability of failure. The very long distances allowed by reach extenders (REs) will also increase the probability that there may be a trunk fibre cut. In such networks, MTTR will also be longer.

In addition, PON REs allow higher split ratios since the split ratios will not be limited due to the link budget used for long reach. A use case with REs is shown in Figure 1.

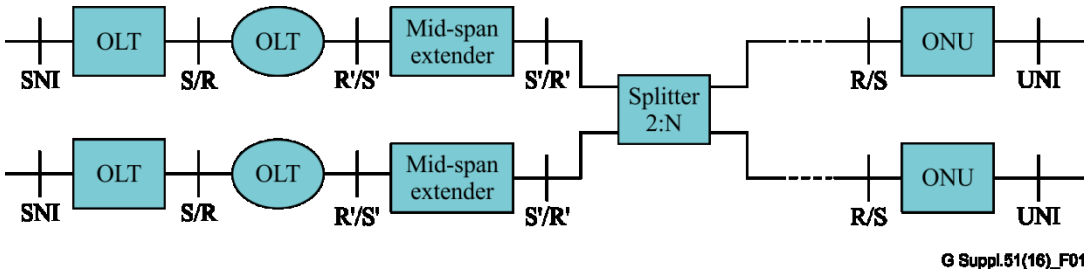

Figure 1 – Use case with reach extenders

4.4 Emergency services

Emergency services like hospitals, police, fire as well as other safety- and security-related departments require continuous communications regardless of the cost. PON protection will be very important for such subscribers.

4.5 PON maintenance

PON protection may be useful in avoiding planned maintenance outages. Often when software or hardware upgrades of an OLT (or ONT or PON) are scheduled, there is an unavoidable PON outage of seconds or minutes as a result. The operator may schedule the upgrade to take place during a so-called 'maintenance window', typically a time in the early morning where there is limited use of the PON by subscribers. This is clearly less than ideal, as there is still a service outage. Subscribers

may often be using the service even in the maintenance window. Moreover, the operator's technicians are required to perform these maintenance activities during unpopular work schedules.

PON protection has been utilized to allow near "hitless" software and hardware upgrades. The process involves initiating a manual PON protection switchover from one OLT or PON to another. In this use case, fast switchover is required as the purpose is to reduce the typical outage of seconds or minutes to fractions of a second, thereby avoiding disruption of service and allowing maintenance to proceed during normal business hours.

5 Protection architectures

There are quite a few PON protection architectures already defined in PON standards both by ITU-T and IEEE, such as type B, type B dual homing, type C, extra traffic for type C and type D to ensure network reliability and resiliency. The difference between these protection schemes depends on what is being protected: feeder fibre; feeder and drop fibres; OLT equipment; OLT and ONU equipment; or a mix and match between them. These all have different impacts on availability and cost depending on probability of fibre cuts (due to "backhoe fade" and non-human intervention, such as falling trees from snow or storm and hungry rats and monkeys), equipment MTTF, temperature swings and fibre-rich versus fibre-poor optical distribution networks (ODNs). As operators are deploying more and more subscribers on an access node, high availability and redundancy are becoming requirements.

Compared with transport networks, access networks are very cost sensitive because only a few subscribers need to share all the costs associated with the protection. Currently there is a lack of deployment of PON protection systems, largely because of cost considerations. Building redundancy into PON will make it more expensive. Any protection architecture should minimize additional cost of protection and at the same time improve network resiliency to an acceptable level. Furthermore, deployment of protection will become more cost effective and attractive if protection assets can also be used to carry over extra traffic during normal use, thus increasing the network capacity.

The ODN constitutes the most significant cost and failure of a PON system and thus any architecture deployed should minimize the cost of the ODN while providing resiliency. Some more cost-effective solutions include:

a) use of N:1 protection where 1 OLT provides protection to N PONs (where N > 1) through an optical switch;

b) use of a protection PON for extra traffic during peak times;

c) use of protection on demand and as per the need of customers, such as software upgrades.

Which methods are most feasible depends on cost and availability. A subscriber may have an SLA requirement of five 9s (which means not more than 5.25 min failure in 1 year), but going beyond this will increase costs significantly. Operators may offer a suite of services with different levels of QoS or availability.

5.1 Type A

This protects only feeder fibre (as in Figure 2) and its usefulness depends on the ODN architecture. Two events in 2011 in New Jersey, USA: hurricane Irene and an untimely snow fall in October (when trees still had their leaves) caused serious damage to trees. Many trees fell on power and communication cables hanging on poles causing disruption of electric power and communication for several days in several thousand homes and businesses.

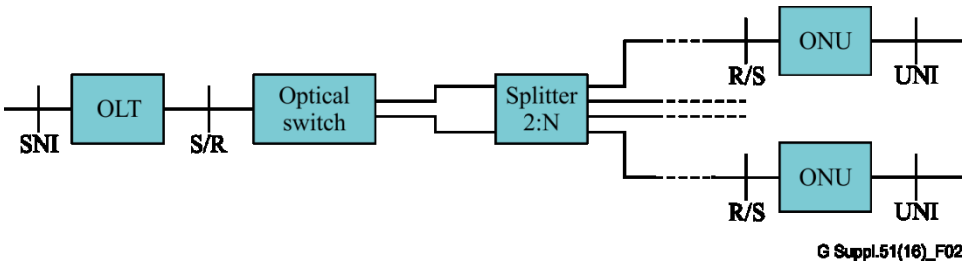

Figure 2 – Type A PON protection

If the ODN fibre is deployed underground, fibre cut or fibre damage from rats or other animals (via gnawing) are serious concerns. If fibre cables are hanging on poles, any weather storm or earthquake could inflict serious damage to the ODN. In these cases, feeder fibre protection (type A) is very useful. Type A PON protection requires either manual intervention of the operator or a voltage-controlled optical switch to physically connect the spare fibre between the splitter and the OLT and to bypass the defect on the primary link. In addition, type A typically does not require an additional OLT PON port to be consumed for protection proposes as in the case of type B and type C.

5.2 Type B

In this configuration, protection is provided over the major areas of concern, which include feeder fibre and OLT equipment with separate OLT blades (or separate chassis in the case of dual-parented) for working and protection OLTs, as shown in Figure 3. No equipment redundancy is provided in the ONUs or feeder fibres. Thus, it does not provide ONU or full ODN protection. Type B provides the automated switching capability, but with an additional PON port on the OLT. The protection-capable OLT performs switching if the working PON fails without modification to the ONUs attached. Issues regarding monitoring of equipment and fibre on the protection link need to be addressed and as such are left up to the implementer of the OLT system.

If the OLT or feeder fibre is unavailable, all subscribers on that PON lose service. If an ONU or drop fibre is unavailable, only subscribers connected to that ONU lose service. Since the protection resources in type B are shared by all subscribers on that PON, the protection cost per subscriber is significantly lower than type C. Type B protection uses a 2 × N optical power splitter which costs about the same as a 1 × N splitter and introduces no additional optical loss. Link monitoring and switching may be automatic. As a result, this architecture is relatively simple, inexpensive and is of primary interest for most operators, especially for residential and small to medium-sized enterprises (SMEs).

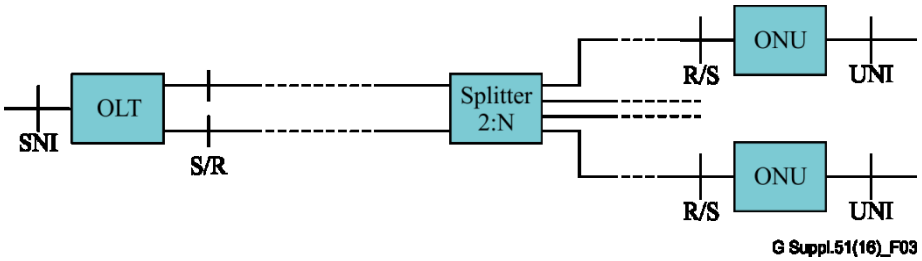

Figure 3 – Type B protection

5.3 Dual-parented type B protection

The standby OLT can reside together with the primary working OLT at the same central office location, but it is undesirable when protecting against catastrophic failures. To address this, one option is the use of dual-parented PONs as shown in Figure 4. In this example, any one subscriber is connected to two OLTs (working and protection) at different geographic locations via a 2 × N optical splitter. During normal operation, the ONUs are ranged and communicate with the working OLT.

In the event of a fibre break, or an OLT equipment or node fault, the protection OLT can take over control of the PON. With dual parenting the OLTs can even be from different manufacturers. It should be noted that with dual parenting the process of duplicating the working OLT database to the protection OLT may need to be defined for interoperability reasons. If not, dual parenting may remain a proprietary method of PON protection.

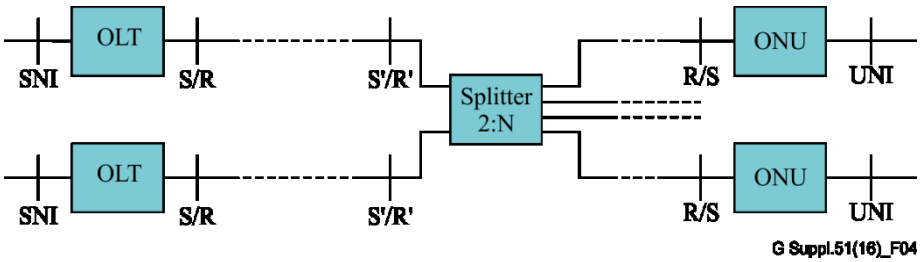

Figure 4 – Dual-parented type B protection

5.4 Type C protection

In this configuration, equipment redundancy is provided in the OLT, ODN and ONUs as shown in Figure 5. It provides two fully redundant links all the way into the subscriber's premises. It is the most costly, but provides the maximum availability. It is ideal for businesses and mobile back hauls. There are two options: linear 1 + 1 and linear 1:1 protection. In 1 + 1 protection, the protection PON is dedicated to each working PON. The normal traffic signal is copied and fed to both working and protection PONs with a permanent bridge between the two OLTs. Traffic of both is transmitted simultaneously to an ONU, which makes a selection between the two signals based on some predetermined criteria, such as server defect indication. In 1:1 protection, the normal traffic signal is transported either on the working PON or on the protection PON with automatic protection switching between OLTs.

The subscriber could have two separate ONUs, but this is not required. An ONU with two optical interfaces could be used.

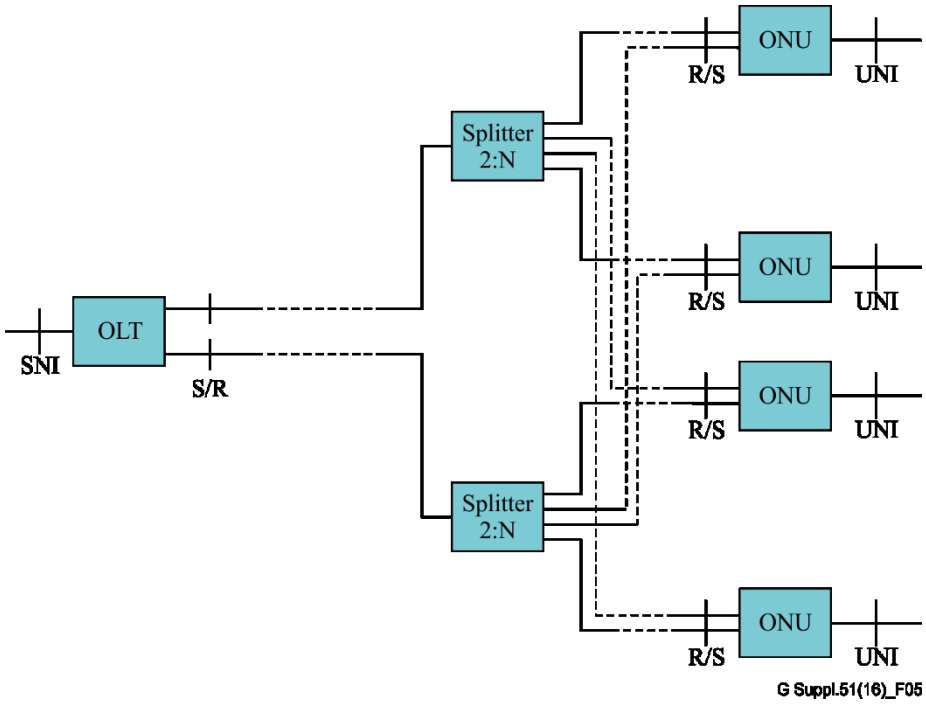

Figure 5 – Type C protection

5.5 Extra traffic for type C protection

Type C protection is ideal for delivering extra traffic which can be carried over the protection path while the primary working PON is active. This option provides effective usage of bandwidth (BW) in the protection resources. The extra traffic will not be protected. The operator must have an option not to activate this extra traffic.

5.6 Type C protection using link aggregation

Strictly speaking, this should not be considered "PON protection" as it makes no demands upon the PON equipment to switch. Topologically this approach looks identical to Figure 5, however, unlike true type C protection, the ONU does not have redundant optical transceivers but rather the ONUs are duplicated, one ONU to each PON. Similarly, the OLTs are completely duplicated as was done with dual homing. All of the service protection is done with the use of link aggregation (LAG) and the user network interface (UNI) and server node interface (SNI) interfaces from the ONU and OLT, respectively. In this approach the PONs may be considered simple Ethernet links. Similar to the "extra traffic" approach, under normal operation the aggregate traffic can be double that of a single PON, via this use of LAG. As in clause 5.5, the extra traffic will not be protected.

5.7 Type D – Deprecated

Type D protection, while originally in [b-ITU-T G.984.1], has since been deprecated.

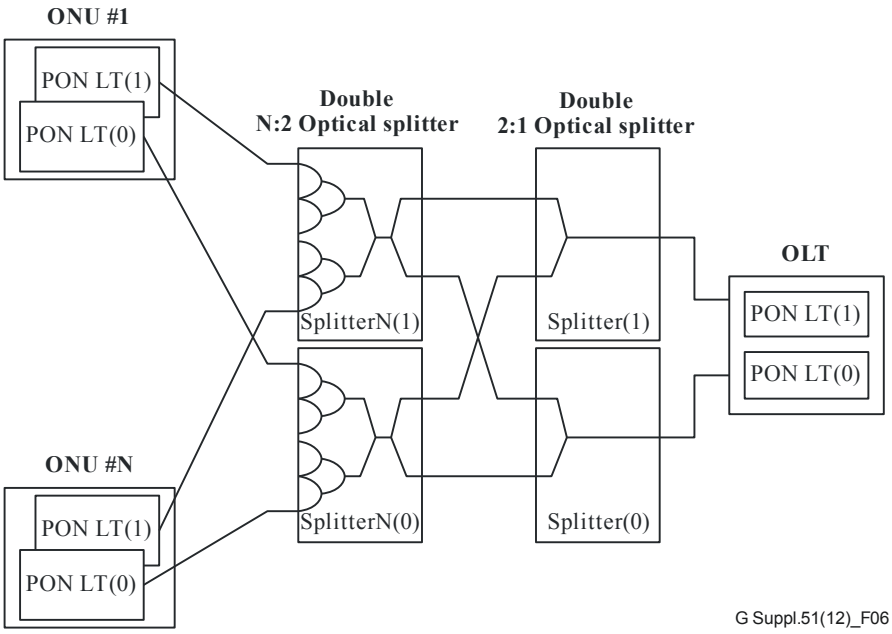

Figure 6 – Type D – Deprecated

5.8 Type B with N:1

In this architecture, one OLT protects multiple PONs (number, N) through an optical switch as shown in Figure 7 or as shall be seen by manual pre-configuration for the use case of PON maintenance. The N × 1 optical switch can be a simple mechanical motorized device that can connect the backup OLT to any working PON. It reduces the total cost, but there is an added cost of an optical switch, which is also an active element. Furthermore, if several working fibres share the same ODN duct and there is damage to more than one working fibre, this protection is insufficient. In the use case of PON maintenance, a virtual N:1 type B can be done by manual pre-configuration. In this case, a spare OLT line card is initially in the OLT chassis or prior to system upgrade a spare card is installed. The spare feeder fibre(s) of the PON(s) to be upgraded is(are) connected to the spare OLT port(s). Prior to switching, the spare OLT must obtain the database of the working OLT to maintain normal operation

after a switch. Once the spare OLT is ready to act as a backup, the operator initiates a forced PON protection switch. As stated before, for this method to be useful, the switching must occur much faster than the length of time in which a PON might recover if no fast recovery method (as detailed in clause 6) is used. Switching times of the order of milliseconds are desirable.

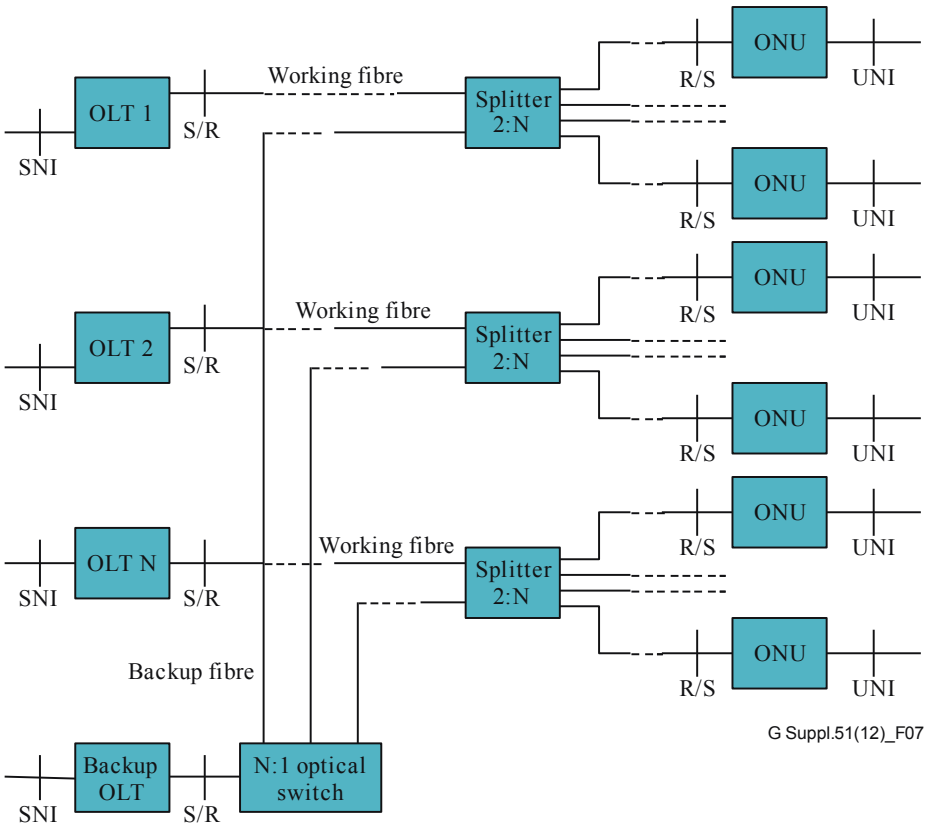

Figure 7 – Type B with N:1 using optical switch

6 Availability and switching speed goals

There is often a correlation between availability requirements and PON switching speed goals. However, this is not always the case. In the case of planned PON maintenance, it may be possible to achieve availability requirements without fast switching speeds. However, it is highly undesirable to induce the loss of service for minutes (or even seconds) on a planned basis. The allowed unavailability times are generally intended to be reserved for outages of an unplanned nature.

6.1 Availability in an unprotected PON

An unprotected PON system consists of an OLT, a feeder fibre, an optical splitter, dropping fibres and ONUs (in the case of concentrated splitting). Unavailable probability attributed to each component, U_i and the system availability, A, are expressed as:

$$U_i = \frac{MTTR_i}{MTBF_i + MTTR_i}$$

and

$$A = 1 - \sum_{i}^{N} U_i$$

respectively, where i indicates an identifier of each component. Examples of MTBF and MTTR of each component are shown in Table 1.

The values in Table 1 are examples, as MTBF depends on the component design, manufacturing process and practice. The MTBF of the OLT depends on its implementation and configuration such as the type of SNI and the number of PON ports per card. The MTBF of the ONU depends on its implementation and configuration such as the type of UNI and the number of UNI ports.

The fibre and splitter are passive components, so the MTBF is very large compared to the OLT/ONU as a device. However, human/animal/natural-induced breaks can occur in these devices depending on the deployment and operational situation of the PON. The deployment and operational situation is very different operator by operator or area by area: the probability of fibre cuts is very different between underground and aerial, for example, and the situation of the underground space is also very different case by case.

MTTR also depends on the operational situation. However, it is likely that it could take several hours for equipment in the central office to replace the failed card from inventory, while it could take 8 h to 24 h or more to replace outside plant and customer equipment, considering the necessary field work and delivery time.

In conclusion, the system availability is limited by the OLT/ONU in some cases and by fibre and splitter in addition in others.

In addition, it is important to consider not only the availability, but also the outage scale in telecommunication operators. For example, the outage scale of OLT failure (or feeder-fibre break) is large, e.g., 32 to 64, while that of ONU failure is only 1. Therefore, the OLT failure is considered more important in terms of inducing a simultaneous outage. While not directly related to availability, the impact of a large-scale outage can have other consequences such as customer loss and public relations problems.

6.2 Assumptions for availability calculations

Using the values in Table 1 and the formula for availability, the availability of a PON without protection can be determined.

To calculate availability, assumptions must be made about the FIT/MTBF and MTTR of the various network components. Table 2 lists the assumptions to be used in the examples in clauses 6.3 to 6.5, which are based loosely on the FIT and MTTR numbers of Table 1. Other numbers may be used, although it will be seen that availability is often dominated by one or two components.

Table 2 – Assumptions for availability calculations

Component	Assumption
Feeder fibre length	18 km
Feeder fibre FIT	18 km × 200/km = 3 600
Drop fibre length	2 km
Drop fibre FIT	2 km × 200/km = 400
Fibre MTTR	24 hours
OLT FIT	2500
OLT MTTR	4 hours
ONU FIT	256
ONU MTTR	24 hours
Splitter FIT	100

The fibre FIT chosen is a value between the aerial 10 FIT and the buried 250 FIT, simply as an example.

6.3 Availability of an unprotected PON

The relationship between the MTBF and FIT is as follows:

$$\mathrm{MTBF_{OLT}} = \frac{1\,000\,000\,000}{\mathrm{FIT_{OLT}}}$$

Therefore:

– OLT MTBF: 400 000 hours

– Using the same formula:

– ONU MTBF: 3 900 000 hours

– Feeder fibre MTBF: 278 000 hours

– Drop fibre MTBF: 2 500 000 hours

Based on the availability formula, the overall access network availability will be:

$$\mathrm{A} = 1 - \left(\frac{\mathrm{MTTR_{OLT}}}{\mathrm{MTBF_{OLT}+MTTR_{OLT}}} + \frac{\mathrm{MTTR_{ONU}}}{\mathrm{MTBF_{ONU}+MTTR_{ONU}}} + \frac{\mathrm{MTTR_{FF}}}{\mathrm{MTBF_{FF}+MTTR_{FF}}} + \frac{\mathrm{MTTR_{DF}}}{\mathrm{MTBF_{DF}+MTTR_{DF}}}\right)$$

The MTTR in the denominators is negligible compared to the MTBF, therefore, for an unprotected PON:

$$\mathrm{A} = 1 - \left(\frac{4}{400\,000} + \frac{24}{3\,900\,000} + \frac{24}{278\,000} + \frac{24}{2\,500\,000}\right) = 99.988\%$$

This is only one example; the fibre reliability in many cases is better than that used here and availability would improve accordingly. However, achieving five 9s is very unlikely in an unprotected configuration.

6.4 Protection path monitoring

It is an equally likely occurrence that backup components have failed when switching from active systems to backup systems, if not monitored. High levels of availability cannot be achieved without protection path monitoring. In the case of 1:1 protection, a method must be used to determine that the protection fibre is intact, as well as the protection OLT optics and electronics. The OLT receive path can be used to monitor upstream transmissions to ensure the protection fibre is functioning. With type B protection, the OLT transmitter cannot be used without impacting the functioning of the PON. If the OLT is not exercising the transmitter, it is unlikely to fail, however. One approach is to test the protection system periodically in a maintenance window. In this case, protection speed is of critical importance for high availability services.

In another example, in type B with N:1, it is important to check the condition of the optical switch and backup OLT in the normal state. One monitoring method is to compare the received upstream frame between the active OLT and the backup OLT. If they differ from each other in terms of the received frame count or upstream bit error rate, the backup OLT may be intentionally failed.

Thus, by periodically monitoring the protection path, the protected section can maintain a standby state without failure.

6.5 Switching speed and impact on availability

The impact of switching speed on availability depends on the protection architecture used, as well as the FIT and MTTR for the various components. Examples are shown in 6.5.1 that provide some insight into switching speed requirements. While overall service availability will depend on additional network factors beyond the access network, these examples will be limited only to the access network. An additional margin must be built into the system to achieve overall service availability.

6.5.1 Calculating availability for type B and type C scenarios

For examples 1 to 5, the probability that a backup component will fail at the same time as the primary component will be considered negligible. This failure probability can be included in the formula for each example by squaring the unavailability of any component that is protected.

Example 1: Type B protection availability – 60 s recovery speed

Using the same assumptions as with the unprotected PON but changing the MTTR from 4 h for the OLT and 24 h for the feeder fibre to 60 s (0.017 h) gives:

$$A = 1 - \left(\frac{0.017}{400\,000} + \frac{24}{3\,900\,000} + \frac{0.017}{278\,000} + \frac{24}{2\,500\,000}\right) = 99.998414\%$$

Example 2: Type B protection availability – 50 ms recovery speed

Using the same assumptions as above but changing the type B switching speed from 1 min to 50 ms gives:

$$A = 1 - \left(\frac{1.4x10^{-8}}{400\,000} + \frac{24}{3\,900\,000} + \frac{1.4x10^{-8}}{278\,000} + \frac{24}{2\,500\,000}\right) = 99.998424\%$$

As seen, there is almost no impact on availability by protection switching detection and recovery speed in a type B scheme. Even a 5 min recovery time would not significantly impact the availability, in this case. Note that higher availability of the drop fibre and feeder fibre would increase the overall availability and longer recovery times would then become a limiting factor.

It should be noted that type B can almost meet five 9s of availability. The dominant sources of unavailability are on the unprotected parts of the network, the drop fibre and the ONU. If the MTTR of these were improved, five 9s could be met, but only barely. Given other sources of availability outside of the access network, to reliably achieve five 9s, type C architecture should be examined.

It must be emphasized that this discussion does not preclude the need for switching speeds of much less than 60 s because: 1) the FIT/MTTR in the calculations for Examples 1 and 2 are just examples and switching can be much faster depending on the manufacturing scheme of the OLT/ONU, as well as operational situation of fibres/splitters as described in clause 6.1; 2) a shorter switching speed leads to shortening the duration of simultaneous service failures for subscribers under the same OLT, which can be up to 256, as per [b-ITU-T G.987.1], in type B protection. If the network operator wants to avoid any simultaneous breaks of T1/E1 or plain old telephone service/integrated services digital network (POTS/ISDN) connections (typically provided via emulation) under the same OLT, it is valid to implement a 50 ms to 120 ms switching time as described in clause 14.3 of [b-ITU-T G.984.1]. Also, 1 s should be a good target as a simultaneous outage of a broadcast service via fibre to the home (FTTH). As previously discussed, the use case of planned PON upgrades requires subsecond and even 50 ms to 120 ms switching times.

Example 3: Type C protection availability – 60 s recovery speed

With type C protection, very high levels of availability can be expected. In this case, recovery times will become a more significant factor. Again, start the process with the formula:

$$A = 1 - \left(\frac{MTTR_{OLT}}{MTBF_{OLT}+MTTR_{OLT}} + \frac{MTTR_{ONU}}{MTBF_{ONU}+MTTR_{ONU}} + \frac{MTTR_{FF}}{MTBF_{FF}+MTTR_{FF}} + \frac{MTTR_{DF}}{MTBF_{DF}+MTTR_{DF}}\right)$$

The difference now will be that the MTTR of all of the components will be relatively fast.

$$A = 1 - \left(\frac{0.083}{400\,000} + \frac{0.083}{3\,900\,000} + \frac{0.083}{278\,000} + \frac{0.083}{2\,500\,000}\right) = 99.99975\%$$

Example 4: Type C protection availability – 5 s recovery speed

Likewise, for a 5 s recovery:

$$A = 1 - \left(\frac{0.017}{400\,000} + \frac{0.017}{3\,900\,000} + \frac{0.017}{278\,000} + \frac{0.017}{2\,500\,000}\right) = 99.99998\%$$

Example 5: Type C protection availability – 50 ms recovery speed

For a 50 ms recovery:

$$A = 1 - \left(\frac{1.4x10^{-8}}{400\,000} + \frac{1.4x10^{-8}}{3\,900\,000} + \frac{1.4x10^{-8}}{278\,000} + \frac{1.4x10^{-8}}{2\,500\,000}\right) = 99.99999999999\%$$

Even if type C protection allows for five 9s of availability with a slow switching speed of 1 min, it is again emphasized that the preceding discussion does not preclude the use of switching speeds of less than 60 s, as explained previously.

7 Fast failure detection

In the case of a break in the fibre ODN, there will be multiple ONUs that enter the POPUP state in G-PON or LODS state in the XG-PON. Accordingly, a loss of signal (LOS) alarm will be reported for the whole PON interface in the working OLT as a complete PON failure, to indicate that the working OLT did not receive any expected transmissions in the upstream.

If protection switching has been implemented, the OLT may switch all ONUs upon failure to the protection fibres with schemes illustrated in the figures of clause 5. There is a relationship between the detection time, the frequency of the allocations and how well the OLT can recover the upstream bursts. A fibre cut or fibre pull is not an instantaneous event and can present itself as a reduction in the received power level at the OLT, as shown in Figure 8. Therefore, depending on the location of the ONU relative to the OLT and the nature of the fibre cut, the detection time may vary. An ONU that is relatively far away from the OLT may be impacted by a fibre cut faster than one that is closer.

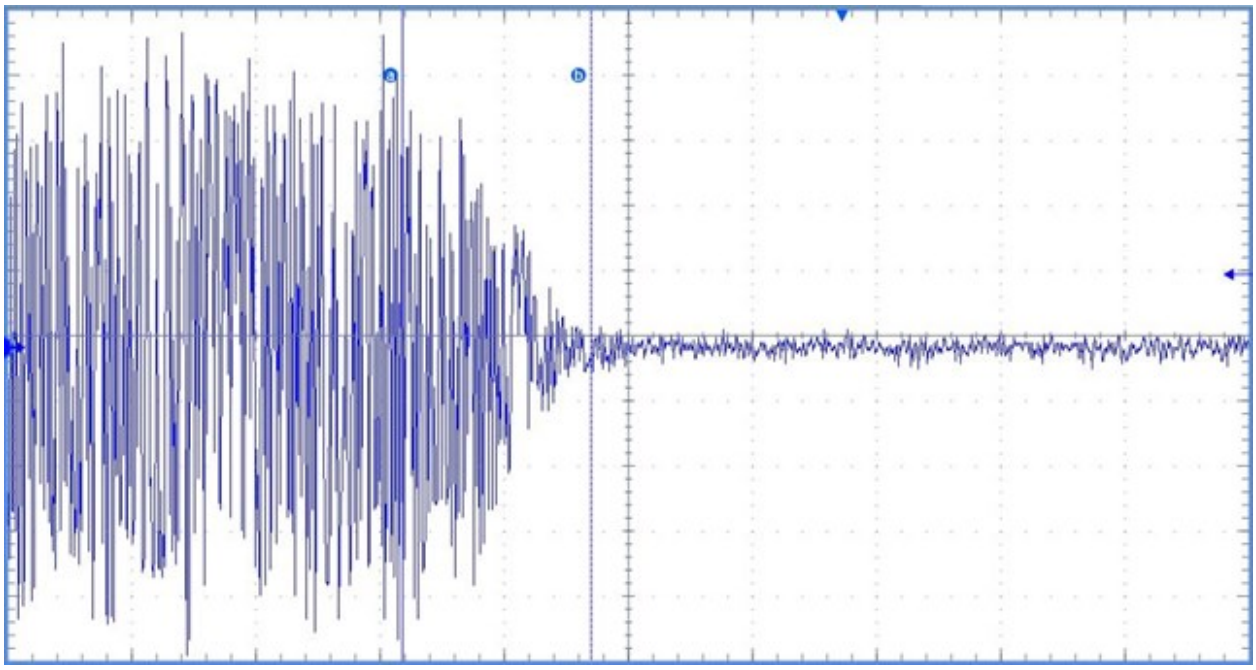

Figure 8 – Example trace of gradual LOS upon fibre cut

Other alarms generated by the OLT may be treated as a condition for fast failure detection. For example, when signal degrade (SDi) or signal fail (SFi) alarms appear in the OLT for all activated ONUs as an indication of link quality degradation, protection switchover may be triggered to enable the ONU to work in the backup path, while field engineers can detect possible issues in the fibre of the working path without affecting services.

Service providers may select other conditions to monitor the system performance and enable protection switchover accordingly; however, this is beyond the scope of this Supplement.

Note the duality of the requirements. If the fast failure detection and switchover is the priority, then it is reasonable to assume that the backup OLT remains powered up during the primary OLT operation, thus introducing an additional power consuming element of the access system. If ONU power saving is the priority, so that ONUs may be intermittently placed in the lower power mode with limited communication capabilities, then it is natural to expect the failure detection and service restoration time upon a switchover event to be negatively affected.

To take control over the ONUs in a protection-switching event, the backup OLT must obtain the necessary configuration and status information on the subtending ONUs.

There are three ways for the backup OLT to collect the ONU's configuration and status information.

1) The primary and backup OLT each communicate with the management system and the management system relays the necessary primary information to the backup OLT. This is a slow channel that is more suited to conveying the configuration information rather than dynamic status.
2) The backup OLT may snoop the upstream transmissions while remaining passive in the downstream. This channel requires the backup OLT to be permanently powered up and is functionally limited in a sense of unidirectionality and the lack of acknowledgement.
3) The primary and backup OLT may communicate via a direct channel similar to that conventionally employed in systems with high service availability requirements. Such a channel is not currently specified in the PON system context.

In an XG-PON system with deployed ONU power management functionality, the backup OLT can snoop the power-saving mode status of the ONUs by observing the upstream sleep-request physical layer operations, administration and maintenance (PLOAM) messages. Upon a protection switching event, the backup OLT can be expected to forcibly wake up the ONUs by setting the forced wakeup indicator (FWI) bit in bandwidth allocation (BA) or sending PLOAM messages indicating SA (OFF) in the downstream. Then, those ONUs may activate the power-saving mechanism later by negotiating with the backup OLT again.

8 Fast protection switchover mechanisms

Type B protection is the most popular protection architecture described in clause 14.2.1 of [b-ITU-T G.984.1], as shown in Figure 3, which has been deployed widely in the world. ONUs under a protection scheme are protected by an OLT group which is composed of two OLTs, where one OLT is in the operational state (referred to as the working primary OLT) and the other is a backup unit (referred to as the backup OLT). The data path connected to the working primary OLT is referred to as the primary (main) path and the data path connected to the backup OLT is referred to as the backup path.

If REs are deployed in the signal paths between the OLT and the ONUs, then the type B protection architecture could be extended as shown in Figure 9 (reproduced from Figure III.1 of [b-ITU-T G.984.6]). Due to extended link length, the risk of damage to the fibre increases and therefore, [b-ITU-T G.984.6] stipulates the need for OTL protection.

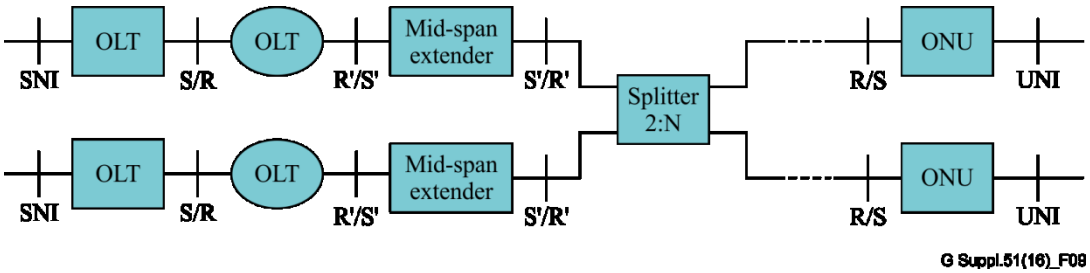

Figure 9 – Extended type B protection architecture with two independent reach extender units

Since the same wavelength is used in the downstream channel in both the primary and backup paths, the backup OLT cannot range any of the ONUs connected to the primary OLT via the regular ranging mechanism. In order to achieve a fast switchover, it is desirable to shorten the re-ranging processing as much as possible. There are four ways to meet this objective:

1) ranging before switchover (pre-ranging);
2) ranging after switchover (limited re-ranging);
3) no pre-configuration of standby OLT equalization delay (EqD) values per ONU (fast ranging);
4) equalization-delay-agnostic.

Under approach 1), all ONUs are provided with the EqDs for the primary and backup paths, effectively minimizing the time it takes to transition between operating states for the primary and backup paths. When the line failure is detected and the path switchover takes place, the ONUs are already prepared for operation on the backup path.

Under approach 2), the need to save time leads to a requirement to limit the ranging process taking place after switchover. Such limited re-ranging can be achieved if just a small subset of ONUs is ranged, while the EqDs for the others are derived through indirect means.

Under approach 3), all ONUs will be able to be sequentially ranged by the re-scheduled upstream arrangement, to accomplish the restoration.

Under approach 4), the ONUs retain the primary EqDs after the protection-switching event, with drift being mitigated by the backup OLT (see clause 8.4).

8.1 Ranging before switchover (pre-ranging)

This mechanism allows for the backup OLT to measure the round-trip delay (RTD) for the backup path without affecting the working OLT.

Mechanisms for ranging before switchover (pre-ranging):

The working OLT sends out a Ranging_Request BA to a target ONU and the target ONU responds with the Serial_Number_ONU PLOAMu message, which is received by both the working OLT and backup OLT. Based on the transmission time of the Ranging_Request BA and the reception times of the Serial_Number_ONU PLOAMu message in the two OLTs, the RTD between the backup OLT and target ONU can be measured and calculated.

The relationship between individual time parameters and references used during the ranging procedure is shown in Figures 10 and 11.

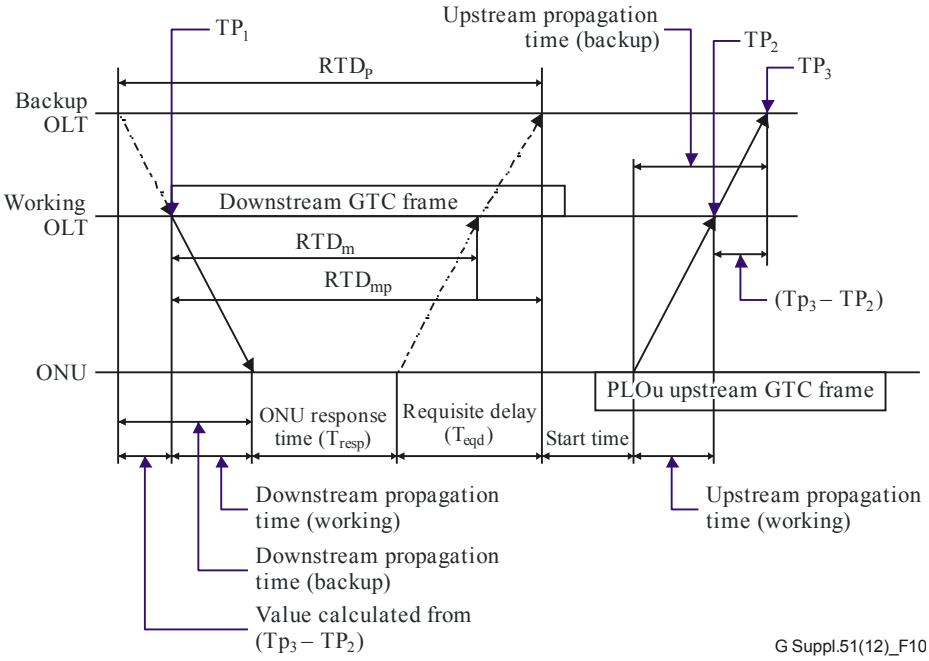

Figure 10 – Relationship between time references when the backup path is longer than the working path

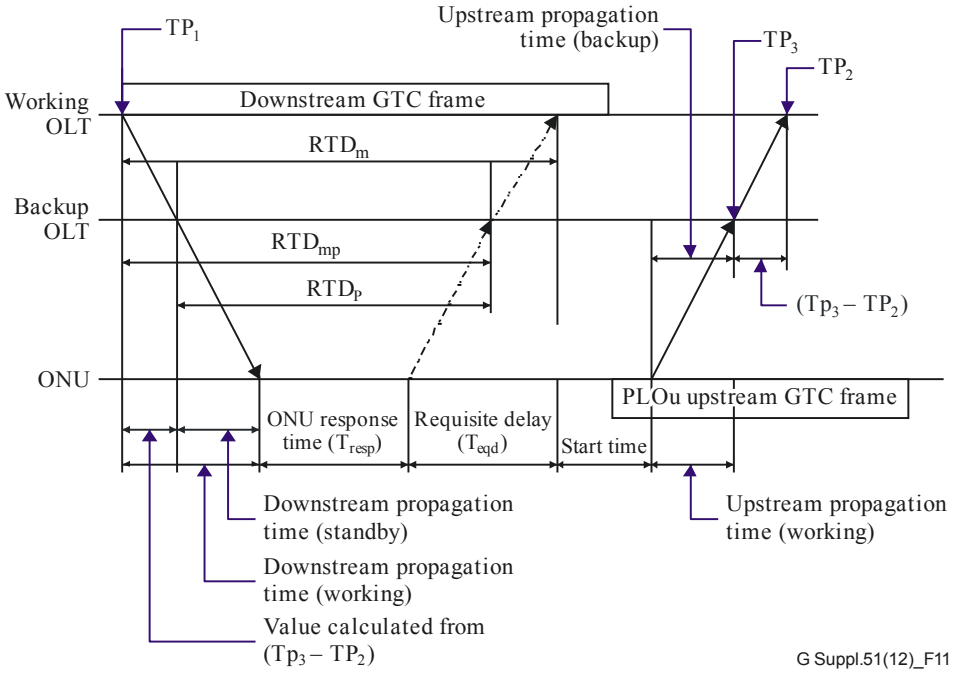

Figure 11 – Relationship between time references when the backup path is shorter than the working path

This mechanism comprises the following steps.

1) The working OLT sends a Ranging_Request BA (as specified in clause 10.2.5.2 of [b-ITU-T G.984.3]) to the given ONU and records the time (TP_1) when the Ranging_Request BA is transmitted.

2) The target ONU responds with a Serial_Number_ONU PLOAMu message at the StartTime assigned in Ranging_Request BA, after a fixed ONU response time (T_{resp}) and requisite delay (T_{RD}). The PLOAMu message can be received by both the working and backup OLTs.

3) The working OLT records the time (TP_2) when the Serial_Number_ONU PLOAMu message is received by the working OLT.

4) The working OLT calculates RTD_m and EqD_m for the working path.

5) The backup OLT records the time (TP_3) when the Serial_Number_ONU PLOAMu message is received by the backup OLT.

6) The RTD_p and EqD_p for the backup path can be calculated based on Equations (1) – (2), where RTD_{mp} denotes the round trip propagation delay for signal transmission from the working OLT to the target ONU and back from the target ONU to the backup OLT.

$$RTD_p = RTD_{mp} + (TP_3 - TP_2) = RTD_m + 2 \times (TP_3 - TP_2) \quad (1)$$

$$EqD_p = EqD_m - (RTD_p - RTD_m) = EqD_m - 2 \times (TP_3 - TP_2) \quad (2)$$

EqD_p can be sent by the working OLT to the target ONU via the Ranging_Time PLOAMd message {least significant bit (LSB) of byte 3 in the Ranging_Time PLOAMd message can be used to indicate whether the EqD_p is applied to the working or backup path, see clause 9.2.3.4 of [b-ITU-T G.984.3]} and used immediately after switching is completed without re-ranging.

8.2 Ranging after switchover (limited re-ranging)

For the case of limited re-ranging, the fewer ONUs that require it, the more switchover time is saved. The key is to keep the number of re-ranged ONUs as small as possible. Fortunately, type B protection has its own features for facilitating the minimum number: only the feeder fibre section is protected. As a result in timing relationships, the only difference between the working path and backup path is the possibly different RTDs caused by the possibly different lengths of the two trunk fibres. Therefore, it can easily be observed that the differences between the pre-switchover transmission time and the post-switchover transmission time are the same for all ONUs in the same system. It makes sense that the OLT obtains this "common transmission time difference" by just re-ranging any one of the connected ONUs, instead of completing a ranging process for every ONU. Then all the other EqDs can be updated by a simple calculation based on this information.

So in the case of type B, the best way of doing a limited re-ranging is to range only one ONU after switchover. Clauses 8.2.1 to 8.2.3 describe the recommended procedure.

8.2.1 Assumptions

Doing a limited ranging implies that all working path EqDs must be known by the backup OLT. Several basic ways are suggested of implementing this.

1) The pre-switchover EqDs receive timely updates between the working and the backup OLTs once they are updated in the working section.

2) The pre-switchover EqDs are periodically updated between the working and the backup OLTs.

3) The pre-switchover EqDs are issued from the working OLT to the backup OLT during switchover.

Though it is determined by the OLT's specific implementations, it is recommended that the EqD updating procedure be completed as quickly as possible.

8.2.2 Notations

RTD – Time interval at the OLT between transmission of a downstream frame and reception of a corresponding upstream burst from the given ONU. This time is composed of the round-trip propagation delay and the ONU response time. See clause 10.1.1 of [b-ITU-T G.984.3].

Δ_{RTD} – The time difference between the $RTD_{working}$ and RTD_{backup}. In the case of common feeder fibre, $\Delta_{RTD,N} = \Delta_{RTD,chosen\ ONU}$. Here, the chosen ONU refers to the ONU that is chosen from the working ONUs online.

T_{EqD} – The "zero distance" EqD, equal to the offset between the downstream and upstream frames at the OLT location. The OLT adjusts the EqD of each ONU such that, for all ONUs, the start of the upstream frame at the OLT occurs T_{EqD} s after the start of the downstream frame. See clause 10.4.3.3 of [b-ITU-T G.984.3].

EqD – The requisite delay assigned by the OLT to an individual ONU as a result of ranging. By adjusting their local transmission times with this value, all the ONUs are viewed as at the same distance from the OLT. See clause 10.1.1 of [b-ITU-T G.984.3].

8.2.3 Fast switchover procedure

The following process is provided for a type B protection fast switching while fatal corruption happens to the working section.

1) All ONUs detect LOS/loss of frame (LOF) alarm and transit from the operation state (O5) to POPUP state (O6).
2) The backup OLT is activated while the original working OLT becomes silent.
3) The backup OLT issues a broadcast POPUP message.
4) On receiving this broadcast message, all the connected ONUs transit from O6 to O4 (ranging state).
5) One of the ONUs is randomly chosen to be re-ranged.

$$EqD_{backup,n} = T_{EqD,n} - [RTD_{working,n} - (RTD_{working,chosen\ ONT} - RTD_{backup,chosen\ ONT})]$$

6) The backup OLT sends a ranging time PLOAM message with the updated EqD to every ONU.
7) On receiving this message, all the ONUs go to the operation state (O5).

The whole system works normally again.

8.3 No pre-configuration of standby OLT EqD values per ONU (fast ranging)

1) OLT configured to use all resources to recover ONUs upon failure detection:

   Upon the detection of a loss of PON or OLT failure, the backup OLT will change the upstream map to schedule all upstream resources to allow ONUs to sequentially range, as opposed to data grants.

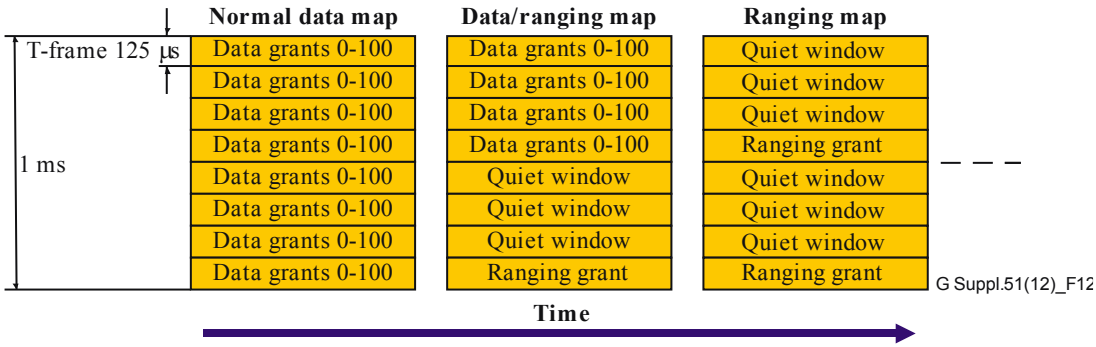

Figure 12 – Schedule of all upstream resources to allow ONUs to sequentially range

ONUs are configured to go to the O6 state upon LOS and return directly to the O5 state upon recovery of the downstream sync in the XG-PON system, or to the O4 state upon receiving a broadcast POPUP message in the G-PON system.

8.4 Equalization-delay-agnostic protection switch

In a practical network, if the ONUs retain the primary EqDs after a protection-switching event, the adjusted round-trip times (RTTs) observed by the backup OLT are no longer identical. ONUs transmit on generally different wavelengths with different refractive indices and the response times may change due to the serializer/deserializer phase randomization. The aggregate relative drift caused by these effects, however, can be bounded and will not exceed a few 10s of bit times. The backup OLT can mitigate the drift by providing additional guard time between the upstream bursts in the BW maps. Furthermore, depending on the mechanisms offered by the TC layer of a particular PON system, the backup OLT may re-acquire the ranging information without the service interruptions associated with the opening of quiet windows.

Prior to switchover, the backup OLT obtains the ODN design parameters and the value of the primary upstream PHY offset, T_{max}, via an offline management channel.

Upon the switchover, the backup OLT proceeds as follows:

1) The backup OLT ensures that the subtending ONUs are in operation state O5. In XG-PON, this is achieved by virtue of a well-formed downstream transmission. In G-PON, an individual directed POPUP message may be required, unless a new broadcast Swift_POPUP message (see Amendment 3 of [b-ITU-T G.984.3]) can be used to bring the ONUs in the POPUP state directly into the O5 state.
2) The backup OLT schedules the upstream transmissions by forming a BW map with extended guard times between the individual bursts and relating them to a yet unknown upstream PHY frame reference.
3) The backup OLT detects the individual upstream transmissions and observes the adjusted RTTs of the subtending ONUs. The adjusted RTTs form a distribution with bounded support.
4) The backup OLT selects an interim upstream PHY frame offset to be not less than the largest observed RTT.
5) The backup OLT issues individual relative EqD adjustments to align the ONUs at the selected interim upstream PHY frame offset. This is done with an available Ranging_Time message in XG-PON and with a new Ranging_Adjustment message in G-PON (see Amendment 3 of [b-ITU-T G.984.3]).
6) The backup OLT may adjust the upstream PHY frame offset at the desired value by issuing a broadcast relative EqD adjustment. This is done with an available Ranging_Time message in XG-PON or with a new Ranging_Adjustment message in G-PON (see Amendment 3 of [b-ITU-T G.984.3]).
7) The backup OLT restores the normal guard times in the BW maps.

In the subsequent operation, the backup OLT, which has become the serving OLT, conducts service as usual, including discovery and admission of the newly activated ONUs for which it opens a quiet window and performs ranging with EqD calculation.

8.5 Typical practice of fast protection switchover mechanisms and viability analysis

8.5.1 Pre-ranging

8.5.1.1 Transceivers in the working and backup OLTs

The transceiver in the working OLT is configured to be able to transmit and receive data and the transceiver in the backup OLT is configured to operate in the receive-mode only, i.e., its receive path is fully enabled while the transmit path is disabled either completely or partially, leaving only the laser in the disabled state to prevent generation of any spontaneous noise.

8.5.1.2 Pre-ranging time points

Pre-ranging can be processed during ONU activation and when the ONU is in the O5 state. Thus, the requisite delay (T_{RD}) referred to above could be PrD pre-assigned by the working OLT during the ONU activation procedure or EqD assigned by the working OLT after the ranging process is completed.

8.5.1.3 Calculation of the backup path EqD

Assuming that Equation (2) is used for the calculation of EqD_p, there are a few possible approaches to calculate EqD_p.

1) The backup OLT transmits TP_3 to the working OLT and the working OLT calculates the backup path EqD_p, which is delivered to the backup OLT and the target ONU.

2) The working OLT transmits TP_2 and EqD_m to the backup OLT and the backup OLT calculates EqD_p, which is transmitted to the working OLT and further transmitted to the target ONU by the working OLT.

3) The working OLT transmits TP_2 and EqD_m to the element management system/network management system (EMS/NMS), the backup OLT transmits TP_3 to the EMS/NMS and the EMS/NMS calculates EqD_p, which is transmitted to the backup and working OLTs and further transmitted to the target ONU by the working OLT.

Option 1) is recommended as the typical practice. TP_3, the reception time of *Serial_Number_ONU* PLOAMu message in the backup OLT, is sent to the working OLT via a pre-defined communication channel (or alternatively via the NMS/EMS) for calculation of EqD_p. Note that there is already a dedicated bit in the *Ranging_Time* PLOAMd message structure that indicates whether the delivered EqD is for working or backup paths. In this way, no changes to the existing PLOAM messages are needed to accomplish this functionality. Therefore, the target ONU can store EqD values for both working and backup paths separately.

When TP_3 is received, the working OLT calculates EqD_p for the backup path using Equation (2). It is assumed that the propagation delays in downstream and upstream channels are approximately equal and they do not change between subsequent ranging events. The EqD value is not sensitive to the difference in propagation delay between upstream and downstream wavelength and the guard time is tolerant of such a difference.

Note that due to different refractive indices for the downstream and upstream wavelengths, there might be a minor difference between the downstream and upstream propagation delays. The factor ($TP_3 – TP_2$) used in Equations (1) and (2) denotes the difference between upstream propagation delays for the main (primary) and protection paths.

In order to properly reflect the difference in propagation delay due to different refractive indices for the downstream and upstream wavelengths, it is necessary to introduce a correction coefficient C, thus making Equation (2) take the following form [see Equation (3)]. The value of this correction coefficient can be calculated as defined in Equation (4), where n_D and n_U represent the downstream and upstream channel refractive indices for the deployed SMF, respectively. The resulting Equation (5) provides the final relationship between the protection and main (primary) path EqD.

$$EqD_p = EqD_m – (1 + C) \times (TP_3 – TP_2) \quad (3)$$

$$C = n_D/n_U \quad (4)$$

$$EqD_p = EqD_m – (n_D + n_U)/n_U \times (TP_3 – TP_2) \quad (5)$$

In Equations (1) to (5), RTD_{max}, which denotes the maximum RTD value between the OLT and the farthest ONU, could be considered the same for both the working and backup OLTs. However, it is also possible for the working and backup OLTs to use different values of RTD_{max}. In Equations (3) and (5), EqD_p is calculated based on RTD_{max} of the working OLT and should be recalculated based

on RTD_{max} of the backup OLT, as shown in Equations (6) and (7), in which $RTD_{max(m)}$ denotes the RTD_{max} for the working primary OLT and $RTD_{max(p)}$ denotes the RTD_{max} for the backup OLT.

$$EqD_p = EqD_m - 2 \times (TP_3 - TP_2) - (RTD_{max(m)} - RTD_{max(p)}) \quad (6)$$

$$EqD_p = EqD_m - (n_D + n_U)/n_U \times (TP_3 - TP_2) - (RTD_{max(m)} - RTD_{max(p)}) \quad (7)$$

8.5.1.4 Time clock in the backup OLTs

The clock in the backup OLT should be synchronized with the clock in the working OLT. If the two OLTs are in the same rack, time synchronization could be achieved by existing and well-known mechanisms, e.g., a hardware time division multiplex (TDM) connection between two OLTs. If they are geographically distributed, time synchronization could be achieved by the methods shown in Table 3.

Table 3 – Inaccuracy of clock transfer between primary and backup OLT in different scenarios

	Time synchronization		
	Scenario 1: There is a dedicated communication path between OLTs	**Scenario 2: OLTs are both connected to a convergence device (Note 2) (e.g., BNG)**	**Scenario 3: OLTs are managed by the same EMS/NMS**
Geographically distributed	OLTs are time-synchronized with each other via [b-IEEE 1588]	OLTs are time-synchronized with the BNG via [b-IEEE 1588]	OLTs are time-synchronized with the EMS/NMS via [b-IEEE 1588]
Inaccuracy between two synchronized OLT clocks	Δ (Note 1)	$2 \times \Delta$	$2 \times \Delta$
Inaccuracy of the calculation of backup EqD with Equation (5)	$2 \times \Delta$	$4 \times \Delta$	$4 \times \Delta$
NOTE 1 – Δ means inaccuracy of time synchronization via [b-IEEE 1588], the range of which could be of the order of submicroseconds and is the same for all the EqDs of the ONUs. NOTE 2 – A "convergence device" is a device connected to the north interface of the OLTs. For reference, see Figure 1 in [b-TR-156]. A convergence device is also referred to as a broadband network gateway (BNG).			

Based on Table 3, in scenario 1, time synchronization is performed between the working and backup OLTs, so the inaccuracy between the time clocks in the two OLTs is Δ and the inaccuracy of EqD_p in Equation (2) is doubled to $2 \times \Delta$ since $2 \times (TP_3–TP_2)$ is used. In scenario 2, the time clocks in the working and backup OLTs are both synchronized to a time clock operating in the BNG, the inaccuracies of which are both equal to Δ and the inaccuracy between the time clocks in the working and backup OLTs are $2 \times \Delta$. The inaccuracy of EqD_p in Equation (2) is then doubled to $4 \times \Delta$ since $2 \times (TP_3–TP_2)$ is used. The inaccuracy calculation in scenario 3 is just like that in scenario 2. Therefore, the maximum inaccuracy of the calculation of backup EqD by Equation (2) is about 4 ms (if $\Delta \approx 1$ μs), which can be tolerated in the EqDs.

8.5.1.5 Lifecycle of the ranged backup path EqD

The measured EqD on the standby link may not be valid after some time, since temperature changes may result in adjustments of the EqD of the ONUs according to the drift control process. Typically the change in the EqD is due to the accumulated effect of temperature changes in the feeder fibre and the drop fibre. However, from observation of real PON networks, EqD adjustment will not be triggered very often if the ODN is stable. For pre-ranging, the backup path EqD can also be measured or updated with a specified interval during the operational state of an ONU to observe the RTT continuously and to mitigate the drift accumulation on the path.

There are a few mechanisms to update backup path EqDs:

1) when the working path EqDs need to be updated;
2) at a specified interval (e.g., every hour);
3) on command from the EMS/NMS (again, with the frequency defined by the management system, administrator or some external watchdogs).

Given that the update mechanism can be autonomous, the problem with the backup path EqD drift is considered as resolved, provided that at least three mechanisms exist to ensure that the backup path EqD is updated periodically.

8.5.1.6 Effectiveness

The pre-ranging method can be executed during the normal ONU working state. The EqD for the backup path can be set or updated before protection has taken place. Hence the backup OLT can bring the ONU back to service without a re-ranging procedure, saving time during protection switchover.

8.5.1.7 Standardization compliance

There is no new requirement to standardize compliance of the ONU and working OLT, but there is an enhanced requirement to support the pre-ranging mechanism for backup OLT implementation beyond G-PON or XG-PON standardization.

8.5.2 Limited ranging

8.5.2.1 Activities on the OLT side

Figure 13 illustrates the sequence of activities as the OLT operates during the fast switchover period.

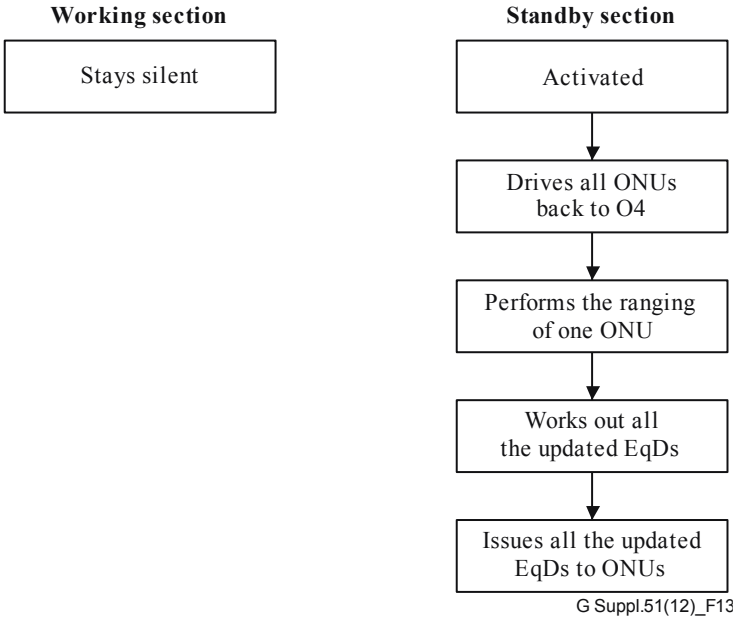

Figure 13 – Activities on the OLT side

8.5.2.2 Activities at the ONU side

Figure 14 illustrates the sequence of activities as the ONU operates during the switchover period.

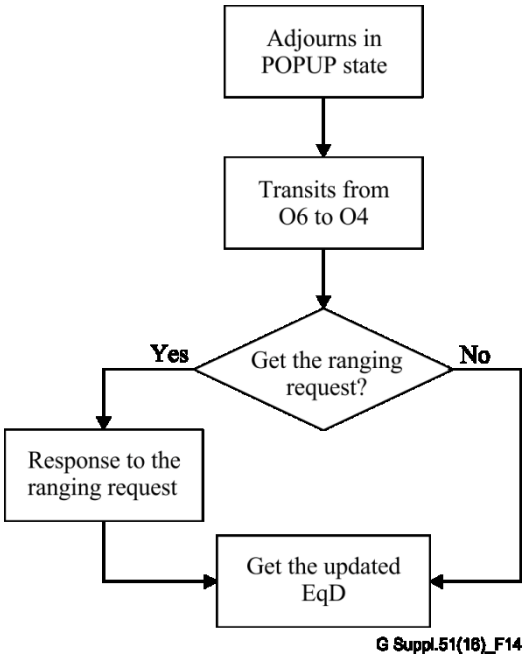

Figure 14 – Activities on the ONU side

8.5.2.3 EqD accuracy

In most cases, the accuracy of this method is sufficient to ensure that the ONUs can operate again successfully. In the worst case, its inaccuracy could be three times the original G-PON ranging inherited inaccuracy, which might present a problem. However, for all existing systems, the performance depends on the OLTs and most of the OLT implementations can deal with this level of inaccuracy quite well.

8.5.2.4 Fibre propagation delay

For a typical G-PON upstream waveband, the biggest refraction index difference is 0.000 045 7 among this 100 nm window. In the worst case, the length difference between the feeder fibre in the working section and that in the standby section could be up to 20 km. This will lead to a 4 bit propagation delay at most. However, this error can be tolerated by the OLT according to [b-ITU-T G.984.3].

8.5.2.5 Effectiveness

The limited ranging method is performed immediately after the protection switch has taken place. The "common transmission time difference", by re-ranging any one of the connected ONUs instead of completing a ranging process for every ONU, can save most of the time spent in the O4 state after protection switchover.

8.5.2.6 Standardization compliance

For the limited ranging method, all activities that are executed between the OLT and ONUs strictly follow the rules defined in the current G-PON Recommendation.

For the XG-PON system, standardization compliance is for further study.

8.5.3 Fast ranging

8.5.3.1 Effectiveness

With the fast ranging method, the maximum possible rate that ONUs could be ranged would be two per millisecond. A more conservative rate would be one ONU per millisecond. With 32 ONUs, it is theoretically possible to recover the PON within 50 ms. With 64 ONUs or more, this would be difficult or impossible. While simple, this method would be more likely used with type B PON protection, where service availability does not depend strongly on PON switching time.

8.5.3.2 Standardization compliance

For the fast ranging method, all activities that are executed between OLT and ONUs strictly follow the rules defined in the current G-PON and XG-PON Recommendations.

8.5.4 Equalization-delay-agnostic protection switch

8.5.4.1 Effectiveness

With the equalization-delay-agnostic protection switch mechanism in the type B protection switch, the ONUs can continue to use their old EqDs. The ONU transmissions will still be aligned for the most part (a small variance may occur), but there will be a significant common-mode delay shift. This is equivalent to the protection PON having a different zero distance EqD (T_{EqD}) value. If the protecting OLT can adapt to this new T_{EqD} value, it can resume ONU communications without reconfiguration. As result, the ONU can save time for the original re-ranging process when the protection switch occurs and maintain service availability.

8.5.4.2 Standardization compliance

For the re-using EqD values method, all activities that are executed between the OLT and ONUs strictly follow the rules defined in the current G-PON and XG-PON Recommendations.

9 Recommended architectures versus use cases

In clause 4 on use cases, some services, such as high density PON residential services, were considered as recommended for protection based on the large number of subscribers experiencing outages if a failure occurred. These residential services were not considered to generally have SLAs requiring five 9s of availability and above. These services would also include the use case of REs if the services are residential. For this level of availability the type B architecture may be ideal.

For business services five'9s is considered essential, while better availability may be desired. These depend on the SLAs negotiated between the operator and subscriber. For the highest level of availability, only type C may be capable of achieving the levels required.

Ultimately the operator must make an estimate of the overall service availability, including other network components (servers, back office equipment) in addition to the access equipment, and match this to the SLAs the operator will be expected to meet.

10 Ethernet linear protection switching to support type B PON protection

The Ethernet linear protection over a type B PON is described in [b-ITU-T G.Sup.54]. This clause provides additional information on the protection switching mechanism over TDM/time division multiple access (TDMA) PON systems configured as type B PON, which can be single or dual parented.

Figure 15 shows an Ethernet connection between a customer premises equipment (CPE) and the BNG over a PON system and an aggregation backhaul/metro network. A PON system consists of a PON card sitting in a slot of a head-end chassis (OLT), a feeder fibre connecting to an optical power splitter and a number of distribution fibres (up to N) connecting the 1:N optical splitter to an ONU, which

normally sits at or near the customer premises. Each ONU has one or more UNIs (Ethernet or other interfaces) to connect to different CPEs. While the multiplexing technique employed in the downstream (from OLT to ONU) is TDM (the ONU will parse the PON frames only if addressed to one of its UNIs), it is TDMA in the upstream direction, with the coordination and synchronization between ONUs transmissions being handled by the media access control (MAC) device sitting in the PON line card of the OLT. The upstream transmissions are enabled by using burst mode transmitters in the ONUs and burst mode receivers in the PON line cards of the OLT. The downstream and upstream transmissions are multiplexed in the fibre using wavelength division multiplexing (WDM).

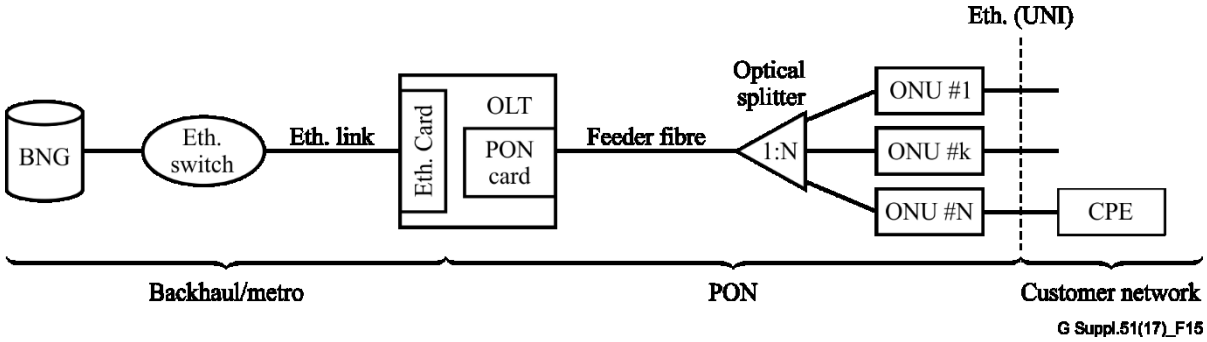

Figure 15 – Elements of a connection between a CPE and BNG over a PON and backhaul

In a type B PON protection configuration a 2:N optical splitter is used (instead of the more conventional 1:N), which has two input/output ports on the OLT side, from which two feeder fibres connect the splitter to two different OLT ports. A single parented configuration has both ports in the same chassis (ideally in separate line cards). A dual parented solution, as shown in Figure 16, has both ports in different chassis (ideally in geographically remote locations). This protection configuration can restore service traffic in case of failure of the PON feeder fibre, and the OLT PON port or card (if ports in different line cards). In the dual parented configuration, service traffic can also be restored in case of failure of the OLT chassis or the entire building where the OLT is located (if chassis in different buildings). This protection is activated only when a fault affects a large number of customers, i.e., all customers in a PON as a minimum.

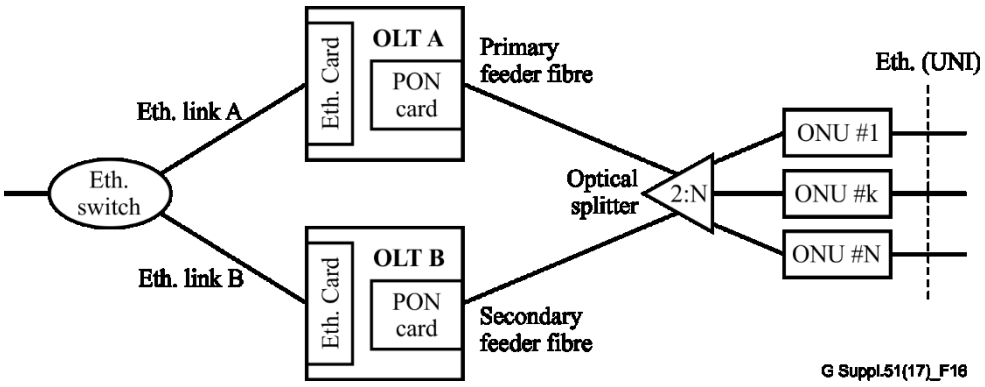

Figure 16 – General physical configuration of a dual-parented type B PON protection

The type B PON protection topology is described in [b-ITU-T G.984.1] and [b-ITU-T G.987.1]. This clause describes a fully automated mechanism where the Ethernet connections between all ONUs in the PON and a remote Ethernet network node, are rerouted through the redundant OLT port.

10.1 Protection switching service characteristics

As the solution targets residential and small business applications, the protection switching time is relaxed compared to a typical protection mechanism in a transport network and times of the order of

seconds are considered as appropriate. However, the mechanism does not involve the management system and is non-revertive. Also, the solution is based on virtual local area network (VLAN) switching and does not involve MAC learning. The solution is suitable for both unicast and multicast services.

Unicast Ethernet services are point-to-point Ethernet connections (EC) using single or double VLAN tagging. For multicast services, a dedicated VLAN is allocated to carry the traffic from a specific source (e.g., a communication provider). The multicast traffic is bridged to all connection terminations associated with the specific multicast VLAN. Protocols such as Internet group management protocol (IGMP) are used to control the Ethernet connection terminations joining the multicast VLAN channel.

10.2 OLT PON port type B Protection State Machine

The two associated OLT ports need to coordinate their status in order to avoid transmitting simultaneously at any time. To that goal, each OLT port needs to run a state machine (which also supports the silent start behaviour).

There are two sets of states, one set belonging to the "Standby" role, where the OLT port has its transmitter turned off ("Initialization", "Protecting", and "LOS-P" states), and another set belonging to the "Active" role ("Pre-Working", "Working", and "LOS-W" states), where the OLT port has its transmitter on and is in control of the ONUs. In order to avoid flapping between roles, after moving to the "Pre-Working" state, the OLT port locks down its active role for a pre-defined period of time, T_{hold}.

The type B protection mechanism ensures that as long as at least one OLT port is available, exactly one OLT port assumes the "Active" role, transmitting optical signals in the downstream direction and providing service to the ONUs. Meanwhile, the other OLT port, if available, assumes the "Standby" role, monitoring the upstream transmissions and being ready to take over if a failure prevents the peer OLT port from continuing in the "Active" role. Table 4 describes each state in more detail.

Table 4 – OLT port states for coordinating in a type B PON protection configuration

State	Semantics
Initialization (1) [Tx: OFF; Rx: ON]	The OLT port is provisioned as part of a type B protection configuration. It starts T_{sstart} timer. The optical transmitter is turned off.
Pre-Protecting (2)	*Not used. This state is only used when ICTP is active in a Multi-Wavelength PON [cf [b-ITU-T. G.989.3]]*
Protecting (3) [Tx: OFF; Rx: ON]	The OLT port has assumed the Standby role, while the peer OLT port controls the ONUs in the PON. The OLT port is not expected to support execution of the per-ONU state machines. The OLT port may obtain service information from the Active OLT port.
LOS-P (4) [Tx: OFF; Rx: ON]	The OLT port in the Standby role has detected a LOS condition. The OLT port starts T_{pfail} timer. The optical transmitter is turned off. The OLT port is not expected to support execution of the per-ONU state machines.

Table 4 – OLT port states for coordinating in a type B PON protection configuration

State	Semantics
Pre-Working (5) [Tx and Rx: ON]	The OLT port has assumed the Active role, turned its transmitter on and commenced downstream transmission, looking to confirm that its signal is received by the ONUs. The T_{hold} timer is started to guarantee a minimum time in the Active role covering states (5) through to (7). The T_{ract} timer is started to limit the time the OLT port awaits for its Active role to be confirmed by a proper upstream transmission.
Working (6) [Tx and Rx: ON]	The OLT port in the Active role has received a confirmation through a proper upstream transmission that its signal is received and processed. The OLT port controls the PON.
LOS-W (7) [Tx and Rx: ON]	The OLT port in the Working state (5) has detected a LOS condition, starts T_{wfail} timer, while continuing to transmit downstream. Unless the LOS condition is cleared, the OLT port remains in the LOS-W state until expiration of both T_{wfail} and T_{hold} timers.
Helpme (8)	*Not used. This state is only used when ICTP is active in a Multi-Wavelength PON (cf. [b-ITU-T G.989.3])*
COMM-FAIL (9) [Tx: OFF; Rx: ON]	The OLT port was not able to (re-)activate any ONU in the PON for a period of at least T_{ract}. The most likely reason being the loss of communication with all ONUs due to a fibre cut or failure of the OLT port receiver. The OLT port has thus moved to this State, where it will raise an alarm to the EMS.
EQPT-FAIL (10) [Tx and Rx: OFF]	The OLT port is not transmitting or receiving, so it is not participating in the protected PON.

There are two sets of states, one set belonging to the "Standby" role, where the OLT port has its transmitter turned off ("Initialization", "Protecting", and "LOS-P" states), and another set belonging to the "Active" role ("Pre-Working", "Working", and "LOS-W" states), where the OLT port has its transmitter on and is in control of the ONUs. In order to avoid flapping between roles, after moving to the "Pre-Working" state, the OLT port locks down its active role for a pre-defined period of time, T_{hold}. Figure 17 illustrates the complete state machine that each OLT port needs to run in order to define its behaviour in a type B protected PON.

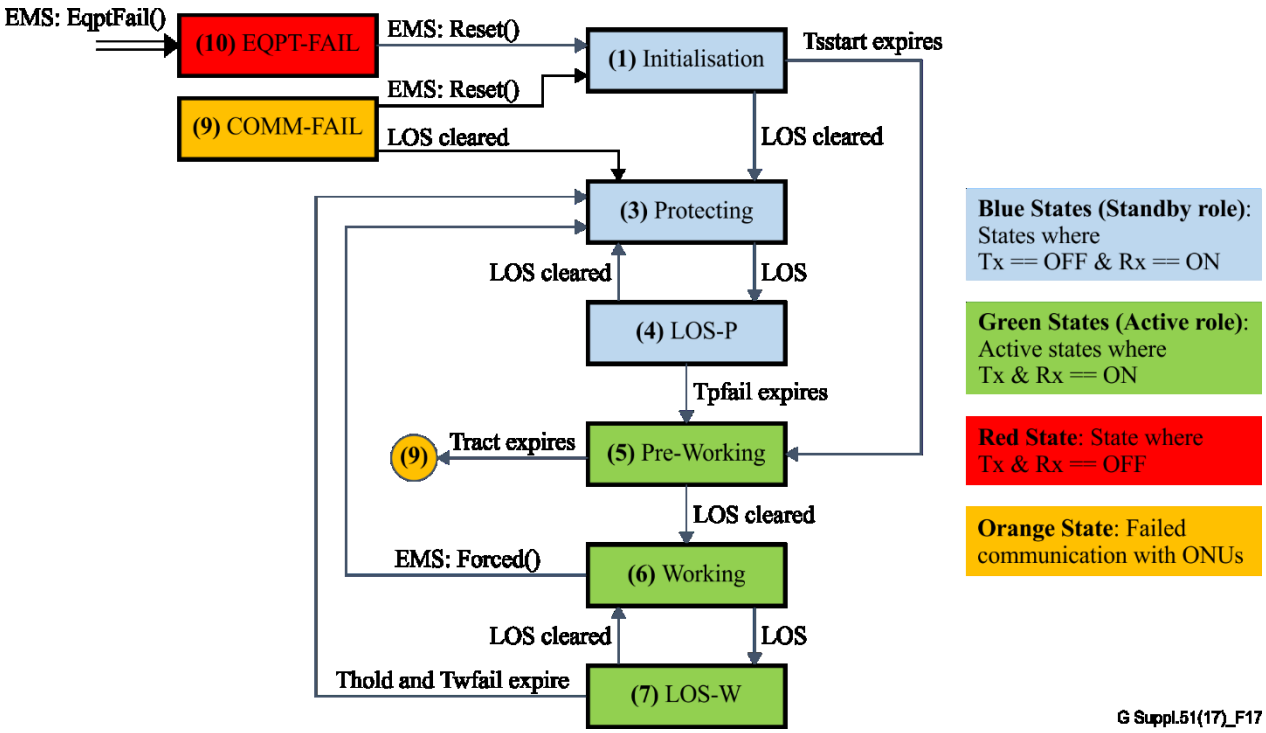

Figure 17 – OLT port state machine diagram

Table 5 describes the timers used in the State Machine. All the timers used in each state are only meaningful while the OLT port stays in that state. Once the port transits to a different state, all timers are cleared.

Table 5 – Timers used in each OLT port state machine for a type B PON protection

Timer	Full Name	State	Semantics
T_{sstart}	Silent start timer	Initialization (1)	The duration of time a re-initialized OLT port waits before assuming the Active role by default. The timer is started upon transition into the Initialization state. If an upstream transmission is detected, the timer is stopped. The expiration of the timer drives its transition into the Pre-Working state (5).
T_{pfail}	Protecting state failure timer	LOS-P (4)	The elapsed time between LOS declaration in the Protecting state and the decision to execute protection switching. The timer is started upon entry into the LOS-P state (4) after the LOS declaration in the Protecting state (3). The expiration of the timer drives a transition into the Pre-Working state (5).

Table 5 – Timers used in each OLT port state machine for a type B PON protection

Timer	Full Name	State	Semantics
T_{ract}	Receiver active confirmation timer	Pre-Working (5)	The maximum time an OLT port attempts to attain control over the ONUs. The timer is started upon entry into the Pre-Working state (5) and is stopped once any upstream transmission consistent with the bandwidth map is received. The expiration of the timer indicates a possible fibre cut or a silent transceiver failure. An Alarm must be issued, and the transceiver moves to COMM-FAIL state (9)
T_{hold}	Active states holding timer	Pre-Working (5), Working (6), LOS-W (7)	The duration of the time interval for which a lock is imposed on an OLT port that has just entered the Active states (5), (6), and (7), through the Pre-Working state (5). The timer is started upon entry into the Pre-Working state (5) and is run until expiration while in the active states. Transition out of the active states is not allowed until the timer has expired or an instruction is received such as EMS:Reset(), EMS:Forced(), or EMS:EqptFail().
T_{wfail}	Working state failure timer	LOS-W (7)	The timer T_{wfail} is started upon entry into the LOS-W state (7) and it is the elapsed time before the OLT port transits to the Protecting state (3), provided the timer T_{hold} has also expired.

Although the timers must be configurable by the system, it is necessary that the values of the timers T_{pfail}, T_{hold}, and T_{wfail}, obey the following relation:

$$T_{pfail} > T_{hold} > T_{wfail}$$

Table 6 describes the state transitions.

Table 6 – OLT port state transitions

Events	States							
	(1) Initialization	**(3) Protecting**	**(4) LOS-P**	**(5) Pre-Working**	**(6) Working**	**(7) LOS-W**	**(9) COMM-FAIL**	**(10) EQPT-FAIL**
LOS		(4) Start T_{pfail}			(7) Start T_{wfail}			
LOS Cleared	Stop T_{sstart} →(3)		Stop T_{pfail} → (3)	Stop T_{ract} → (6)		Stop T_{wfail} → (6)	→ (3)	
T_{sstart} expired	(5) Start T_{hold} Start T_{ract}							
T_{pfail} expired			(5) Start T_{hold} Start T_{ract}					
T_{hold} and T_{wfail} expired						→ (3)		
T_{ract} expired				Stop T_{hold} Stop T_{ract} → (9)				
EMS:Reset()	Reset T_{sstart}	(1) Start T_{sstart}	Stop T_{pfail} → (1) Start T_{sstart}	Stop T_{hold} Stop T_{ract} → (1) Start T_{sstart}	Stop T_{hold} → (1) Start T_{sstart}	Stop T_{hold} Stop T_{wfail} → (1) Start T_{sstart}	(1) Start T_{sstart}	(1) Start T_{sstart}

Table 6 – OLT port state transitions

Events	States							
	(1) Initialization	**(3) Protecting**	**(4) LOS-P**	**(5) Pre-Working**	**(6) Working**	**(7) LOS-W**	**(9) COMM-FAIL**	**(10) EQPT-FAIL**
EMS:Forced()					Stop T_{hold} → (3)			
EMS:EqptFail()	Stop T_{sstart} → (10)	→ (10)	Stop T_{pfail} → (10)	Stop T_{hold} Stop T_{ract} → (10)	Stop T_{hold} → (10)	Stop T_{hold} Stop T_{wfail} → (10)	→ (10)	

10.3 Initial connection configuration

Figure 18 illustrates the initial connection configuration between ONUs and the aggregation Ethernet switch on the network side.

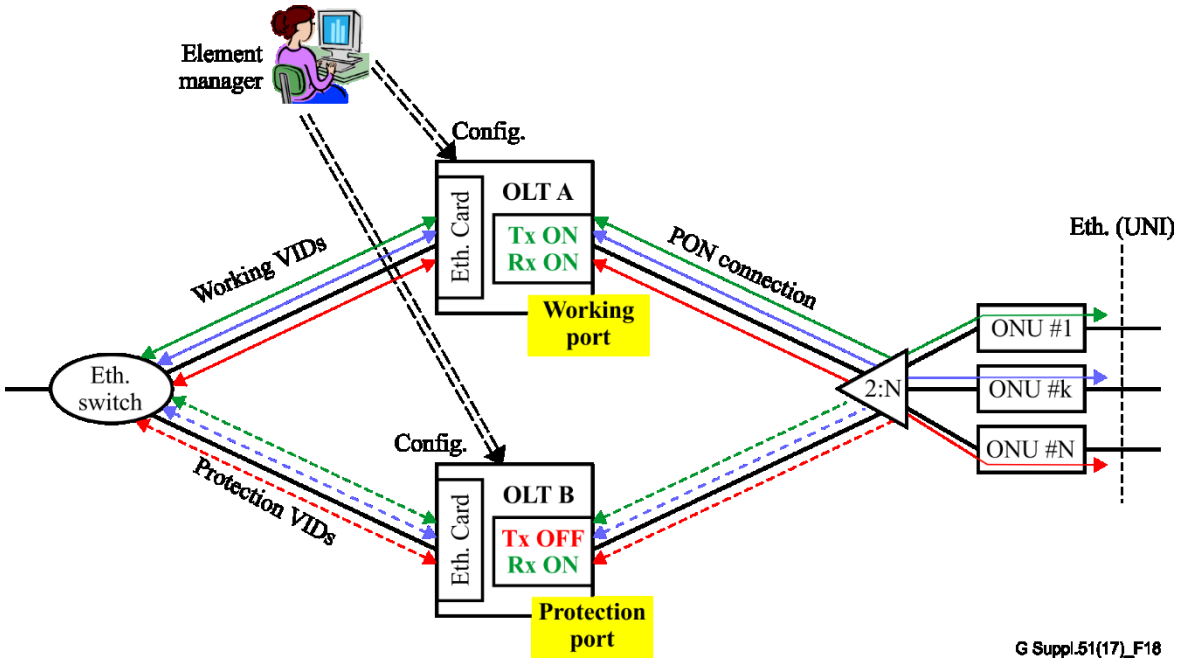

Figure 18 – Initial PON system connection configuration and protected Ethernet connections with two associated VLAN identifiers

All ONUs of a type B protected PON are pre-registered and configured, i.e., serial number, service profiles, etc., in both OLT ports (A and B in Figure 18), e.g., by using the element manager. First, the PON port in OLT A is initialized and configured in the "Working" state and, second, the PON port in OLT B is initialized and configured in the "Protecting" state. This means that while the working PON port will have its transmitter and receiver ON and will become active in taking control of the connected ONUs, the protecting PON port in OLT B will have its receiver ON, but its transmitter will be turned OFF and therefore will go into the standby role. Therefore, the ONUs are activated on the "Working" port (OLT A) only and the service traffic will flow between ONUs and the Ethernet switch through OLT A. The "Protecting" port in OLT B will be in Standby, not transmitting (in order to avoid interfering with downstream transmissions from OLT A), but listening to upstream optical power from all ONUs. Therefore, the OLT B port in the "Protecting" state behaves like an open switch for the service traffic, which is therefore blocked and not passed through. Note that in normal operating conditions, the OLT B port is unable to recover the received burst transmissions from the ONUs, because their transmission preambles are not long enough to enable a “blind” reception (i.e., detect the messages without prior knowledge of the transmission location within the virtual upstream PON frame).

It is important to stress that at any given time either none or at most one OLT PON port will be active passing service traffic through the OLT.

On the backhauling/metro links, a protected Ethernet connection will have two associated VLAN identifiers (VIDs), one over the working backhaul link (e.g., VID x) configured between the OLT A and the Ethernet switch and a second one over the protection backhaul link (e.g., VID p) between OLT B and the Ethernet switch. In the same way, each protected Ethernet connection between the ONU and the Ethernet switch will have two associated VIDs.

Ethernet operations, administration and maintenance (OAM) messaging must also be configured on all Ethernet connections using [b-ITU-T G.8013]. Maintenance entity group endpoints (MEPs) must

be configured at each active UNI of each ONU and a maintenance entity group (MEG) formed with its opposite peer in the Ethernet switch.

As shown in Figure 19, the two ports connecting the Ethernet switch to the two OLTs will be associated in a 1:1 SNCP switching using [b-ITU-T G.8031]. Continuity check messages (CCMs) will flow between the two MEPs over the Ethernet connections. To detect the signal fail condition, the Ethernet switch has two Ethernet MEP sink functions which are non-intrusively monitoring the working and protection input ports. Note that the path through OLT B is interrupted (open connection) as the PON transmitter is turned OFF and the service traffic is not passed over.

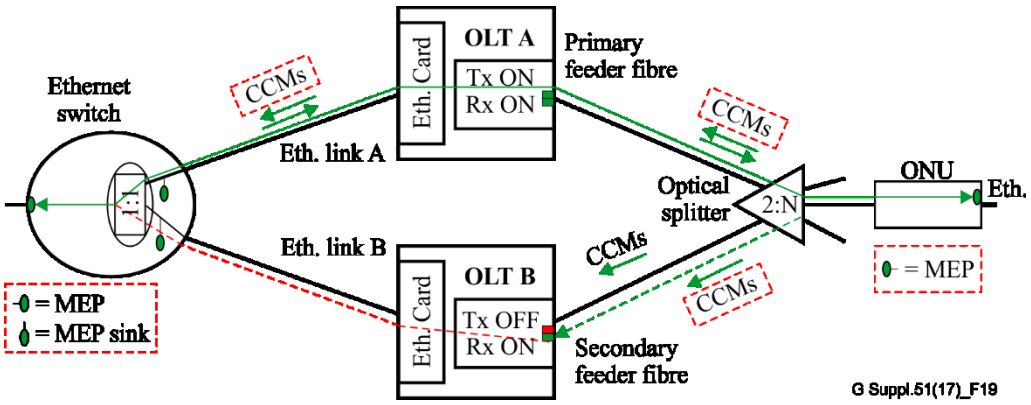

Figure 19 – Ethernet OAM and MEP association

Note that the Ethernet connections between UNI and the port at the Ethernet switch are identified by a service VLAN identifier (S-VID). Such service Ethernet connections (S-EC) may carry a user signal, or an aggregate of customer Ethernet connection signals (C-EC), each one identified by a customer VLAN identifier. The S-ECs are protected.

10.4 Description of end to end protection switching

The Ethernet switch uses ITU-T G.Sup.54 (Ethernet linear protection switching) to assert fault conditions for those S-ECs where CCMs have stopped being received and switches both directions of affected S-ECs traffic together over to the protection route. Note that this protection mechanism protects against failures within the PON portion of the end to end connection (except the ONUs, distribution fibres and optical splitter) and does not protect against failures of the Ethernet link between OLTs and the Ethernet switch.

The LOS at the OLT port is considered an adequate switching event trigger for residential and SME applications. The LOS condition is asserted after the OLT PON receiver does not detect any optical power for the duration of four consecutive PON frames, i.e., 0.5 ms.

The Ethernet linear protection switching is illustrated in Figure 20. Upon failure, LOS (from all active ONUs) is asserted at the "Working" (active) OLT port, it transits to a "LOS-W" state ready to move to the "Protecting" state after waiting a pre-defined time (T_{wfail}). When finally the OLT port transits to the "Protecting" (standby) state, it turns its transmitter OFF. As a consequence of the failure, all CCMs associated with the affected S-ECs have stopped flowing on the initial "Working" route. Since the "Working" OLT port cannot communicate with the ONUs, these will not receive transmission grants and therefore will remain quiet. As a consequence, the "Protecting" OLT port also detects LOS from all ONUs and moves to the "LOS-P" state. After the timer T_{pfail} expires, it transits to the "Pre-Working" state where it will turn its transmitter on and will become active by taking over control of all ONUs in the PON. Once the ONUs are re-activated, the OLT port finally moves to the "Working" state and the ONUs are now connected to OLT B, and the traffic flow on the protection route is restored. The CCM flows resume over the protecting route back to the Ethernet switch.

If the OLT port, having transited to the "Pre-Working" state, does not succeed in taking control of the ONUs for a period of time, T_{ract}, it will transit to the "COMM-FAIL" state and will issue an alarm.

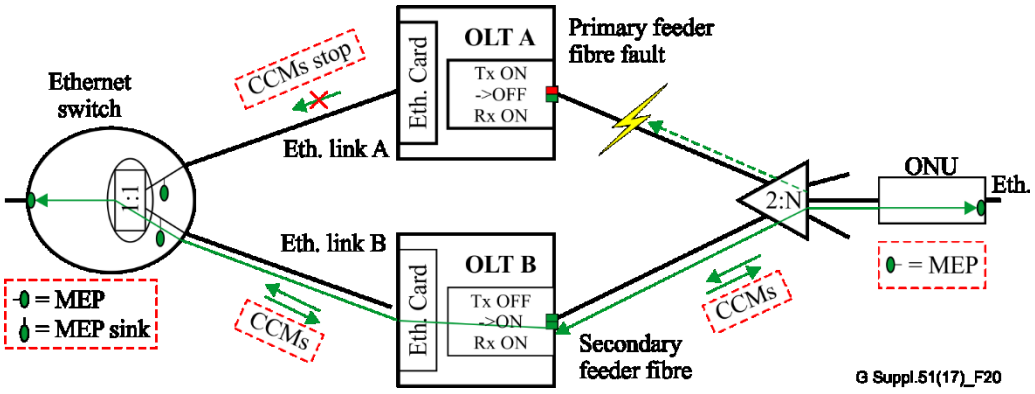

Figure 20 – Ethernet linear protection at a glance

Bibliography

[b-ITU-T G.984.1] Recommendation ITU-T G.984.1 (2008), *Gigabit-capable passive optical networks (GPON): General characteristics*.

[b-ITU-T G.984.3] Recommendation ITU-T G.984.3 (2014), *Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification.*

[b-ITU-T G.984.6] Recommendation ITU-T G.984.6 (2008), *Gigabit-capable passive optical networks (GPON): Reach extension*.

[b-ITU-T G.987.1] Recommendation ITU-T G.987.1 (2016), *10-Gigabit-capable passive optical networks (XG-PON): General requirements*.

[b-ITU-T G.987.3] Recommendation ITU-T G.987.3 (2014), *10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification*.

[b-ITU-T G.989.3] Recommendation ITU-T G.989.3 (2015), *40-Gigabit-capable passive optical networks (NG-PON2): Transmission convergence layer specification*.

[b-ITU-T G.8013] Recommendation ITU-T G.8013/Y.1731 (2015), *Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*.

[b-ITU-T G.8031] Recommendation ITU-T G.8031/Y.1342 (2015), *Ethernet linear protection switching*.

[b-ITU-T G.9807.1] Recommendation ITU-T G.9807.1 (2016). *10-Gigabit-capable symmetric passive optical network (XGS-PON)*.

[b-ITU-T G.Sup.54] ITU-T G-series Recommendations – Supplement 54 (2015), *Ethernet linear protection switching*.

[b-GR-418] Telcordia GR-418 (1999), *Generic reliability assurance requirements for fiber optic transport systems*.

[b-IEEE 1588] IEEE 1588-2008, *IEEE Standard for a precision clock synchronization protocol for networked measurement and control systems*.

[b-TR-156] Broadband Forum TR-156 (2008), *Using GPON Access in the context of TR-101*.

[b-Alcoa] Alcoa Fujikura Ltd. (2001). *Reliability of Fiber Optic Cable Systems: Buried Fiber Optic Cable, Optical Groundwire Cable, All-Dielectric, Self Supporting Cable*, Alcoa Fujikura Ltd. 16 pp.

[b-Chen, 2008] Chen J., Kantor M., Wajda K., Wosinska L. (2008). Network protection. In: Prat, J., Ed, *Next-generation FTTH passive optical networks: Research towards unlimited bandwidth access*, pp. 111–124. Dordrecht: Springer.

[b-Chen, 2010] Chen J. Wosinska L., Mas Machuca C., Jaeger M. (2010). Cost vs. reliability performance study of fiber access network architectures. *IEEE Communications Magazine* **48**(2), pp. 56–65.

[b-Hajduczenia] Hajduczenia M., Chengbin S., Zhen Z., El Bakoury H., Kozaki S., Matsuoka M. (2012). Resilience and service protection for Ethernet passive optical networks in SIEPON. *IEEE Communications Magazine* **50**(9), pp. 118–126.

[b-Tsubokawa] Tsubokawa M., Honda N., Azuma Y. (2012). Reliability and scalability of access networks with ladder structure. In: *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2012 and the National Fiber Optic Engineers Conference*, paper NM2K.5.

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, 2017