D4.13

Resilience in heterogeneous long reach access networks

Dissemination Level:

- **Dissemination level:**

  PU = Public,
  RE = Restricted to a group specified by the consortium (including the Commission Services),
  PP = Restricted to other programme participants (including the Commission Services),
  CO = Confidential, only for members of the consortium (including the Commission Services)

Abstract:

The report provides guidelines how to establish resilience, monitoring and protection strategies in a heterogeneously utilized long reach optical access network. New optical monitoring and infrastructure management techniques and their connection to the network control plane are also described. The most suitable and cost-efficient technologies and approaches for resiliency, monitoring, and protection are also identified and discussed.

COPYRIGHT

© Copyright by the DISCUS Consortium.

The DISCUS Consortium consists of:

Participant Number	Participant organization name	Participant org. short name	Country
Coordinator			
1	Trinity College Dublin	TCD	Ireland
Other Beneficiaries			
2	Alcatel-Lucent Deutschland AG	ALUD	Germany
3	Coriant R&D GMBH	COR	Germany
4	Telefonica Investigacion Y Desarrollo SA	TID	Spain
5	Telecom Italia S.p.A	TI	Italy
6	Aston Universtity	ASTON	United Kingdom
7	Interuniversitair Micro-Electronica Centrum VZW	IMEC	Belgium
8	III V Lab GIE	III-V	France
9	University College Cork, National University of Ireland, Cork	Tyndall & UCC	Ireland
10	Polatis Ltd	POLATIS	United Kingdom
11	atesio GMBH	ATESIO	Germany
12	Kungliga Tekniska Hoegskolan	KTH	Sweden

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the DISCUS Consortium. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

All rights reserved.

Authors:

Name	Affiliation
Marco Ruffini	TCD
Joerg Hehmann	ALUD
Jiajia Chen	KTH
Julio Montalvo	TID

Internal reviewers:

Name	Affiliation
Andrea Di Giglio	TI
Roland Wessäly	Atesio
Christian Raack	Atesio

Due date: 30 June 2015

TABLE OF CONTENTS

1 INTRODUCTION 7

2 PROTECTION AND HIGH RESILIENCY TECHNIQUES IN LR-PONS 7

2.1 HYBRID FIBRE/MICROWAVE PROTECTION TO SUPPORT MOBILE SERVICES 8

2.1.1 Architecture 10

2.1.2 Performance evaluation 13

2.2 MICROWAVE PROTECTION AND RESILIENCY FOR FIXED ACCESS 16

2.3 SDN-ENABLED PON PROTECTION EXPERIMENTS 19

2.3.1 1:1 protection experiments 19

2.3.2 N:1 protection experiments 23

2.3.3 Further discussions 26

3 ADVANCED FIBRE INFRASTRUCTURE MANAGEMENT WITH INTELLIGENT SPLITTER MONITORING (ISM) 27

4 NEW PROPOSALS FOR OPTICAL LAYER SUPERVISION IN LR-PONS 29

4.1 TRANSMISSION AND REFLECTION ANALYSIS BASED DARK FIBRE SUPERVISION 29

4.1.1 TRA Based monitoring technique 31

4.1.2 Operation principle 32

4.1.3 Validation and discussion 33

4.2 EMBEDDED OTDR (EOTDR) FOR LR-PONS 35

4.2.1 eOTDR in OLT 35

4.2.2 eOTDR in ONU 36

4.3 PREVENTIVE COLOURLESS FIBRE SUPERVISION IN WDM-PONS 37

5 RELIABILITY, OPTICAL SUPERVISION AND MANAGEMENT IN LR-PONS: CONCLUSIONS 38

6 REFERENCES 42

ABBREVIATIONS 45

1 Introduction

DISCUS Long Reach Passive Optical Networks (LR-PONs) are designed to be heterogeneously utilized, this is, to support both mobile and fixed services, as well as to support the simultaneous operation of several service and network providers. Having this in mind, in this deliverable we analyse in detail several aspects related to operational issues of the LR-PONs: first, resiliency and protection; second, fibre management; and finally, optical layer supervision.

Resiliency in the access segment is a cornerstone due to the long reach target of up to 120 km. Therefore, the DISCUS LR-PON architecture has dual-parental protection, which provides feeder section protection inherently. In previous deliverables, e.g., D2.2, D2.6 and D4.4, the resiliency issue is widely discussed. Several important reliability performance parameters have been presented. In this deliverable, high reliability schemes are proposed in Section 2 using wireless protection, both for mobile services and fixed access. Protection experiments based on Software Defined Network (SDN) control plane are also reported.

While network resiliency guarantees specific service reliability requirements, it is also very important to properly manage fibre infrastructures during LR-PON operation (network construction, network reconfiguration after a fault reparation, etc…), as well as properly detect and, if possible, locate optical layer faults that may take place in the LR-PON fibre infrastructure.

In Section 3, we show an advanced fibre infrastructure management system based on intelligent splitters, as a remote tool for reliable fibre connection management and optical splitter monitoring.

Section 4 shows new proposals for optical layer supervision in PONs. First, a cost effective alternative to OTDRs based on Transmission-Reflection analysis in dark fibres is presented in section 4.1. Embedded OTDR technology is examined both from OLT side and ONU sides in section 4.2. A low cost preventive monitoring system for quick detection of fibre faults in WDM-PONs is also described in 4.3.

Final conclusions on reliability, optical supervision and management are reported in section 5, with further discussions on fast protection strategies and the role of the control plane in protection and monitoring.

2 Protection and high resiliency techniques in LR-PONs

In this section, we focus on the cases with high reliability targets, e.g., mobile *xhauling*, etc., where end-to-end protection should be offered in flexible way, as well as fixed services with special reliability requirements. Therefore, a novel protection scheme, i.e., hybrid fibre/microwave protection for mobile *xhauling* is firstly presented in Section 2.2. Resiliency of fixed access with a wireless protection is studied in Section 2.3. PON protection experiments are also reported and analyzed in Section 2.3 in order to well support protection in DISCUS LR-PONs.

2.1 Hybrid fibre/microwave protection to support mobile services

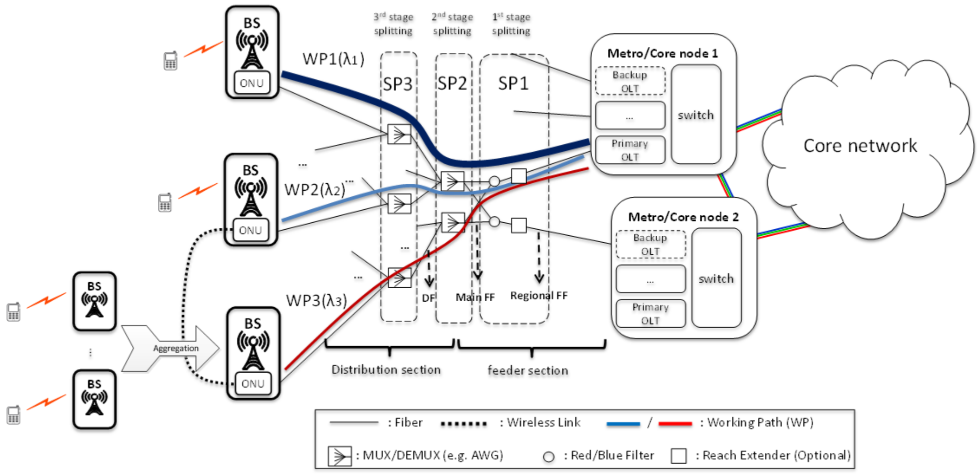
The bandwidth demand required by 3G/4G and the future 5G mobile services is expected to reach an astounding increase, i.e. in the magnitude of 1000-fold in the coming decade [1], which in turn will bring a number of challenges on *xhauling* networks (including backhaul, fronthaul, etc.). In the DISCUS architecture, convergence of optical and wireless access networks is considered, where the related reliability issue is investigated in this sub-section. Here we take backhaul as an example, similar approaches can be applied to fronthaul as well, which may have different requirements on capacity, delay and other network performance.

Several backhauling alternatives for cellular networks are available, such as based on copper, fibre or microwave. Microwave approach is able to provide capacity up to several Gbps with a maximum reach of a few kilometers. A recent report [2] estimates that microwave represents approximately 50% of global backhaul deployments. Copper networks, which make up for approximately 20% of all backhaul deployments, are likely to decrease their penetration, due to their limited capacity and poor ability to scale in a cost efficient manner. Looking forward, fibre is expected to replace copper based wire-line connections, and increase its overall share. In contrast to the other two technologies, the fibre connection can easily provide very high bandwidth (e.g. over 100Gbps) and long reach (i.e. in the magnitude of several tens of kilometers) while consuming less energy [3]. Therefore, fibre based approaches are promising for backhauling the future ultra-high capacity mobile networks. It has been found that passive optical network (PON) outperforms other fibre based network architectures in terms of cost and power efficiency [4]. Furthermore, network operators are advocating node consolidation, where several central offices can be merged and located in a single central access node, in order to reduce operational complexity and cost [5]. In this regard, long-reach PON (LR-PON) is considered as one of the best alternatives, which is in line with the DISCUS architecture. In LR-PON the maximum reach can exceed 100 km [4], which makes it possible to combine the access and metro networks into one segment, and in this way simplify network operation and reduce the cost. Moreover, advances in wavelength division multiplexing (WDM) technology, make WDM based PONs to promising candidates, offering high data rate and large splitting ratio [4]. Therefore, we focus on WDM based LR-PON for mobile backhaul, where an optical line terminal (OLT) is located at the central office (also referred to as the metro/core node which is at the edge of the core network) while each optical network unit (ONU) is backhauling the traffic from one cell and is co-located with the associated base station (BS).

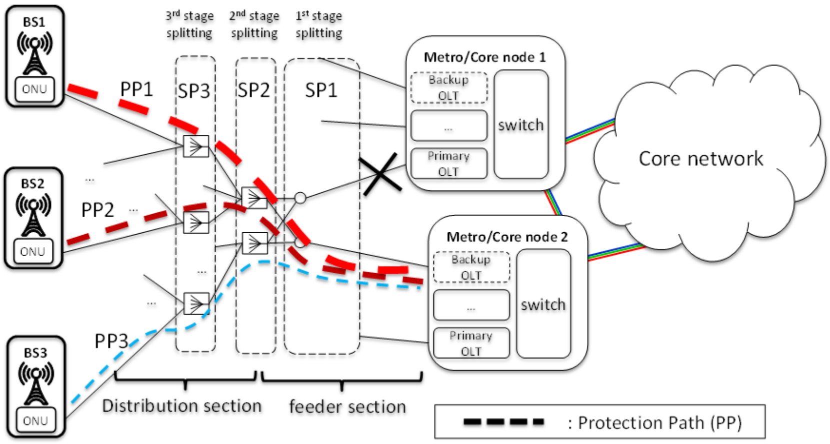
Meanwhile, the rapidly growing traffic demand increases importance of reliability performance of mobile backhauling [4], where the availability requirement of 4 or 5 nines (99.99% or 99.999%) needs to be satisfied. It has been demonstrated in [6] that without any protection in PON, connection availability of 4 nines cannot be achieved, in particular in long reach deployment scenarios. There are many resiliency schemes proposed for PON based fixed access network, most of which could be also applied for mobile backhauling applications. [7] and [8] both present restorable architectures for WDM-PONs, but the protection function of these two schemes covers only part of the fibres, i.e., either feeder fibre (FF) shared among all the ONUs [8] or distribution fibre (DF) which is dedicated to a specific ONU [7]. Full protection schemes based on duplicated fibres have also been investigated. For instance, two types of resilience schemes that can offer full protection capability have been standardized by ITU-T [9]. Obviously, they can offer very high reliability performance by duplicating all fibre segments and optical equipment. In [10], a reliable PON architecture utilizing multiple stages of wavelength MUX/DEMUXs (e.g., arrayed waveguide gratings (AWGs)) is proposed. In this case an ultra-high number of ONUs can be supported by a single PON. [11] introduces a scalable mechanism which combines star and bus topologies. However, all of these schemes come at the expense of high investment cost, in particular for the civil work to deploy a geographically disjoint DFs dedicated to each ONU, which substantially increases the cost on a per-user/cell basis. In contrast, utilizing wireless technology for protection of mobile backhaul network allows for reusing the existing infrastructure of the cells (e.g., BS tower) to accommodate extra antennas needed for the protection purposes, so that no big extra cost is needed apart from the wireless equipment. Meanwhile, establishing wireless connections for protection is obviously less cost- and time-consuming compared to the wired technology. Moreover, the wireless equipment used for protection could be switched off or put in low-power mode to save energy during the normal operation. Most of the schemes mentioned above, e.g., [10], [11], consider protection of the fibre infrastructure while optical components are still unprotected. Recent studies [12], [13] point out that a single component failure (e.g., failure of OLT) may have a high impact and affect all connections served by this component. In [14] and [15] survivable PON based wireless-optical access networks are proposed, where the protection is based on routing the signals through backup ONUs and wireless routers. However, these solutions still suffer from some disadvantages, i.e., 1) the backup segment requires extremely high spare capacity, particular for a potential failure occurring in feeder section, and 2) the transmission via wireless routers may cause severe delay if multiple hops are involved. It has been shown in [14] that even with the optimized algorithm (that can minimize the latency by selecting proper path for routing) the delay via the wireless routers could be more than 5ms when the traffic load is high. Furthermore, using such a scheme could cause approximately 30% packet loss in case of failure occurred at the OLT. It might be acceptable for residential users, but for mobile backhauling it may become a serious issue, particularly for future 5G mobile services.

Considering the aforementioned aspects, we present a hybrid fibre and microwave based protection scheme that offers resilience for mobile backhaul network [16]. In addition, our approach can flexibly support different reliability requirements and provide either full protection, including fibres and optical devices, or only feeder section, i.e., feeder fibres (FFs) and OLT, which are shared by all ONUs. We evaluate our scheme in terms of reliability performance, complexity and flexibility in providing resiliency, and compare with some existing approaches. The results show that our architecture outperforms all the other considered schemes by offering higher connection availability and flexibility at potentially lower cost. Furthermore, we investigate the Failure Impact Factor (FIF) [12] of the unprotected part in all the considered architectures and verify the necessity to protect some high impact components.

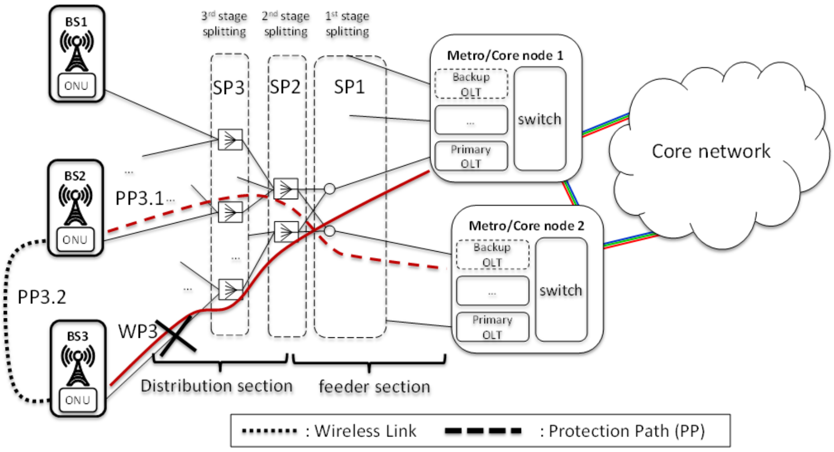
2.1.1 Architecture



(a) Working path



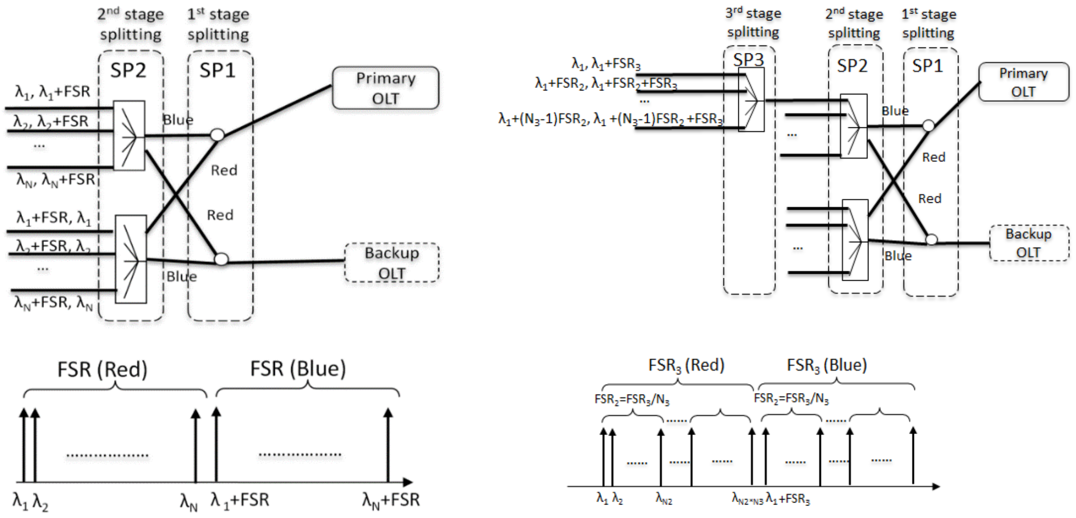
(b) Protection path for the feeder section



(c) End-to-end prtoection

Fig. 1. Proposed protection scheme (λ1 for WP1 and λ2 for WP2 belong to blue band, while λ3 for WP3 belongs to red band.). SP: Splitting Point.[19]

This subsection describes the proposed architecture, namely hybrid fibre and microwave self-protected PON which is illustrated in Fig. 1 [19]. The working paths (WPs), e.g., WP1, WP2, and WP3 shown in Fig. 1, indicate the connection between the central node and base station under the normal operation where there is no fibre cut or any equipment failure. All the paths we considered here are for bidirectional communication. Either the same waveband or two separate ones are used for the upstream and downstream traffic. The proposed scheme is in line with DISCUS architecture with long-reach PON having several stages of splitting points (SPs). Two key features of our approach are: 1) dual-homed FFs for the protection in the feeder section shared by all the cells; and 2) an optional microwave connection in the distribution section (e.g., for a macro-cell that aggregates the traffic from multiple small BSs shown in Fig. 1), which is established between two neighboring ONUs having disjoint distribution fibres. In this way, a full protection, where all the components along the working path are protected, can be provided for some selected cells. In addition, the optional microwave connection offers high flexibility for implementing backup in the distribution part of the network, i.e., only where it is required.



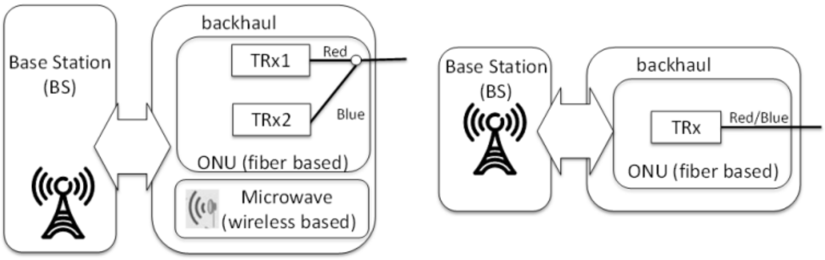
(a) (b)

Fig. 1. Configuration of splitting stages: (a) 2-stage and (b) 3-stage

Figure 2a shows the configuration of the case with two stages of splitting points (SPs) (i.e., k=2). In the first stage, two waveband filters, e.g., red/blue filters, are placed to split all the wavelengths into two wavebands, while in the second stage two wavelength MUX/DEMUXs or power splitters are required. The ONUs connected to the first SP2 utilize blue waveband for working and red waveband for backup. On the other hand, the ONUs associated to the second SP2 (on the bottom) have red waveband for working and blue waveband for protection. In this way, the spectrum is fully utilized. Furthermore, by deploying splitting components, e.g., AWGs or power splitters in the second and/or further stages, the structure can support both pure WDM PON and TWDM PON. In case of pure WDM PON, a dedicated wavelength is assigned to each cell. For TWDM PON, at least one stage of SPs has to be splitters in order to enable several cells share the same wavelength. The consecutive SPs can be co-located at the same geographical place. For instance, all the SP1s and SP2s can be co-located, if the length of main FFs (MFFs) is very short (almost = 0). Reach extender (RE) can be used to improve the optical power budget of the connections if needed. This PON architecture is exactly in line with DISCUS long-reach access.

In case where AWGs are employed in our scheme, several free spectral ranges (FSRs) are utilized. As illustrated in Fig. 2a, N denotes the splitting ratio of the AWGs at the 2nd stage, where their FSR is equal to the red (R) or blue (B) band of the filters at SP1. The maximum number of connected BSs in this case is $2N$ and the channel spacing of AWGs is FSR/N. It can be further extended to be a more general case with more stages of splitting points (e.g., three-stage case shown in Fig. 2b). We use N_i ($1 \leq i \leq k$) to denote the maximum fan-out (i.e. the number of output ports) of the *SPi* and FSR_i ($1 \leq i \leq k$) to represent the *FSR* of the AWGs in the *SPi*. Then, the maximum number of BSs supported by the PON is $N_1 * N_2 \ldots * N_k$ and the wavelength channel spacing of the AWGs in the i-th stage of SPs ($i>1$) is FSR_i/N_i. It should be noted that $N_1=2$, which means the number of output ports for the band filters at the first stage of SPs is fixed and equal to two. FSR_k corresponds to the size of the whole R or B band. The channel spacing of the AWGs in the *SPi* should be the same as the FSR_{i-1}, i.e. $FSR_i/N_i=FSR_{i-1}$ ($1 \leq i \leq k$). For the cases where power splitters are deployed in some SPs or replace all the AWGs in the aforementioned scenarios, e.g., if broadcast-and-select WDM PON or TWDM PON are considered, the configuration of the first stage of SPs (SP1) should not be changed. At the ONU side, a tunable filter may be required to select the assigned wavelength from the signals broadcasted by the splitters. Meanwhile, in all the cases the wavelength plan for each cell (or the cells in the same embedded TDM PON for TWDM PON case) can be exactly the same.

Figure 3 shows the configuration of the ONU. In Fig. 3(a), two optical and one microwave transceivers (TRXs) are installed in the ONU offering end-to-end resiliency for its neighbor. For microwave technology, we consider a point-to-point link, which can be millimeter wave or licensed sharing access/authorized sharing access bands. One optical TRX sends its own primary signal while the other two (i.e. one optical and one microwave TRXs) are for distribution section protection of its neighbor. Thanks to a proper configuration of SPs in our scheme, it is guaranteed that the optical TRXs for working and protection always use different wavebands (i.e., one for R band and one for B band). When the distribution section protection of its neighbor is not required, one optical TRX at the ONU is sufficient (see Fig. 3(b)).



(a) (b)

Fig. 3. Configuration of ONU (a) with and (b) without protection for its neighbor

2.1.2 Performance evaluation

In this section, we assess the performance of the proposed hybrid fibre/microwave protection scheme with respect to complexity and flexibility in provisioning protection, connection availability, and failure impact. For simplicity, we consider our proposed architecture utilizing a pure WDM PON with two stages of SPs (i.e., k=2). For the comparative study we select three existing schemes where the similar number of ONUs per working FF is considered. The key findings from the comparison can be applied to a general case with more stages of SPs or to a TWDM PON. Hereafter, we refer to our approach as Scheme 1 and to the ones presented in [10], [11] and [15] as Schemes 2-4, respectively.

Complexity

The complexity considered here is a measure for the additional equipment, fiber links and resource (e.g., spectrum) needed in the protection schemes, implying extra cost required to provide resilience. In our scheme, we put one backup optical TRX and one wireless TRX at ONU side in order to provide end-to-end protection. In contrast, in Scheme 2 and 3, either optical switches (OSs) or more DFs are required, particularly for DF protection. Wireless connection proposed in our scheme makes the deployment for DF protection more flexible and less costly compared to Scheme 2 and 3, because much less civil work is needed to set up the wireless connection between ONUs than to put protection fibre in the ground. The average cost of deploying one kilometer fibre duct is $60000 [12] while establishing a wireless connection is obviously much cheaper (around $150 and its yearly spectrum leasing fee is approximately $200 [17]). This huge difference in expense enables hybrid fibre and microwave scheme for protection in mobile backhauling to be significantly less costly than the pure fibre based schemes. Compared with Scheme 4 in [15] which is also a hybrid fibre and wireless protection, our scheme requires neither dedicated backup ONUs (i.e., the extra ONU which is needed only for protection but not connected with any BS) nor interconnection fibres between two PONs. The wireless connections in Scheme 4 may suffer from multi-hop communication through wireless routers that may cause potential high delay. Besides, half of capacity in one PON should be reserved in order to guarantee FF protection of its neighboring PON. Meanwhile, when a potential failure occurs in the feeder section of PON, via wireless routers all the traffic first needs to congest in the ONU dedicated for backup purpose. We assume C is the bandwidth required for the connection between the OLT and one ONU, and then the wireless segment in Scheme 4 should be able to handle the capacity up to $(M-1)xC$. Considering C=100Mbps and M=32, it might be still feasible to have wireless routers to handle the capacity up to around 3Gbps. However, for future 5G mobile service with the magnitude of 1000-fold capacity increase in the coming decade, using Scheme 4 for protection may cause a severe scalability problem.

At the OLT side, our scheme utilizes two separate OLTs with dual-homed FFs which protect each other by utilizing waveband efficiently. Scheme 3 [11] exploits shared TRX protection and puts m extra backup TRXs for M working ones (m≤M) in the OLT which can only provide m:M shared TRX protection. However, OLT failures may be caused not only by a TRX fault but also by malfunctioning of other components (e.g. chassis including power supply, card board, etc.)[17][18]. Therefore, only TRX protection may not be sufficient. In summary, our scheme has relatively low complexity in offering protection and high efficiency of bandwidth utilization compared with the other considered approaches.

Connection availability

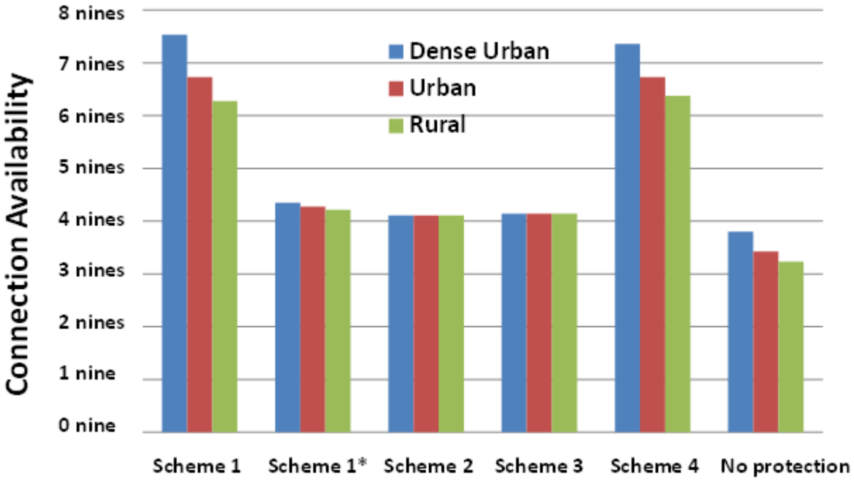


Fig. 4. Connection availability performance for all the considered schemes

The methodology and input data for reliability calculation can refer to [19], which have been also included in the previous deliverable (D2.1). The results shown in Fig. 4 prove that our scheme with full protection offers the highest connection availability, over 7 nines (99.99999%) in the urban area. Even with only feeder section protected (i.e., Scheme 1*), our approach still outperforms Scheme 2 and 3 which have protection for both FF and DF. The high availability results in our scheme are due to the protection of the entire OLT. Furthermore, the OLT failure can have an impact on the network reliability performance, which is assessed in the next section.

Moreover, it should be noted that we do not differentiate the fibre link availability in rural/urban areas while in practice the fibre link availability might be different. However, this difference would not change the general trend of reliability performance for different schemes as shown in Fig. 4.

Failure Impact Factor

Failure impact factor (FIF) [12] is a measure, which can reflect a risk that a large number of customers are affected by a single failure. For instance, all the connections in the PON would be down due to an OLT failure, while fault in an ONU would only affect one cell. Thus, by evaluating FIF of different components in PON we can identify the critical parts of the network that should be protected in the first place. The calculation of FIF takes two parameters into account, i.e., number of customers affected by a failure occurring in a certain component or a link (referred to as failure penetration ratio *FPR*) and its unavailability *U,* which equals to the probability that it is failed [19].

According to this definition, FIF of a connection in our scheme with full protection (i.e. in Scheme 1) and in Scheme 4 would be zero because there the entire paths are protected. For this reason, we only discuss FIF of a connection in Scheme1*, Scheme 2 and 3.

TABLE I

COMPARISON OF FAILURE IMPACT FACTOR

Scheme 1*	FIF	Scheme 2	FIF	Scheme 3	FIF
ONU	2,55E-05	ONU	2,55E-05	ONU	2,55E-05
DF	2,8E-05	OS	6E-06	AWG	0,00144
AWG	0,00048	AWG (M×M)	0,11520	OS	0,00096
		Splitters	0,02560	OLT	0,00496
		OLT	0,44799		
SUM	0,00053	SUM	0,58882	SUM	0,00739

Table I shows the results obtained for rural scenario, i.e., where the FIF is highest among all the considered scenarios. According to [12][13], FIF < 0.1 (which implies that less than 1000 users would be affected by any failure given that the connection availability is higher than 99.99%) would be an acceptable level from a network operator perspective. Our scheme with only FF protection has obviously lower FIF of connection than the other two considered schemes because the unprotected part is only belonging to one connection. In Scheme 2, FIFs of the OLT and AWG are extremely high because many connections are affected by failures of these components. In this case, a protection for OLT and AWG is recommended since the failure impact is high.

Flexibility of protection deployment

According to the FIF results, the impact of failures of ONU and DF is much lower than OLT and FF. Nevertheless, the protection of all ONUs and DFs requires deploying large amount of TRXs (wireless/optical) and fibres. Thus, the operators may prefer to offer ONU and DF protection only optionally to some important connections requiring very high reliability performance (e.g., Macro BSs covering large areas) in order to avoid big investments, which may not pay off.

The comparison of flexibility to offer protection capability is shown in Table II. All the schemes can provide protection for FF and DF but protection of OLT or some components in SPs is not always available. Schemes 3 and 4 have to provide full protection (i.e., both DF and FF protection) to all the users. It means that either all the supported cells have full protection or no protection at all. Scheme 2 can be upgraded from only FF protection to FF+DF protection for some selected cells by adding extra OSs and fibres interconnecting two neighboring ONUs, which requires expensive civil work. However, in our scheme, we can flexibly offer protection either to the SP1s or all the way down to the cell, according to the reliability requirement of a certain connection. Besides, the operator may install the TRXs wherever and whenever ONU and DF protection is needed. As the BSs are already deployed, the extra cost for upgrading protection includes only the optical TRXs and wireless connection setup. It can be considered as an important advantage for our scheme since it enables operators to have a flexible solution to meet the diverse reliability requirements without need of paying high cost for the protection upgrade.

TABLE II
COMPARISON OF PROTECTION CAPABILITY

	Scheme 1	Scheme 2	Scheme 3	Scheme 4
Protection of FF	Yes	Yes	Yes	Yes
Protection of DF	Optional	Optional	Mandatory	Mandatory
Protection of OLT	Yes	No	Only *m:M* TRX protection	Yes (for feeder protection, half of total capacity should be reserved.)
Protection of SPs	SP1s are always protected, the others are protected if DF protection is offered)	M (1×M/2) AWGs are protected	No	Yes
Protection of ONU	Optional	No	No	Yes

2.2 Microwave protection and resiliency for fixed access

In previous section a technique supporting increased reliability and protection for mobile services was described. Nevertheless, in some cases, some customers using LR-PON for fixed access services may also have high requirements in terms of resiliency and protection.

Hybrid access services, such as described in Broadband Forum WT-348 [20], offer the possibility to increase bandwidth of low speed copper lines by bonding fixed broadband and mobile access networks. Hybrid access services open other interesting use cases, such as faster service activation for new customers or an increased reliability Wide Area Network (WAN) connection. Here we analyze this latter use case in the DISCUS fibre access network for ONUs which require an increased reliability connection, see the following figure.

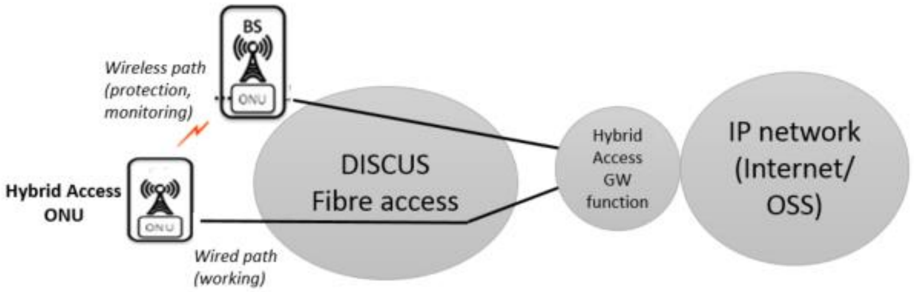


Fig. 5. Hybrid fixed-mobile access generic architecture in DISCUS. GW: Gateway. OSS: Operations and Support Systems.

The hybrid access (HA) ONU may operate as follows:

- HA-ONU has a primary working path in the fixed access network (DISCUS LR-PON).
- HA-ONU has a secondary path through a BS of the wireless network which can be used by network operators for two main purposes. First, it can be used as a backup protection channel (typically with a lower speed) when a connection fault takes place in the fixed access. Secondly, this secondary path can also be used for monitoring purposes of the ONU itself and the fibre access network, communicating the customer premises with the operator's OSS in case it is required.
- A Hybrid Access GW may be required in case that traffic aggregation is desired between both access paths, performing traffic classification, distribution and re-combination.

TABLE III
UNAVAILABILITY VALUES FOR HYBRID ACCESS ONU

Parameter	Unavailability	Failure Penetration Rate
ONT TRX (tunable)	1,1E-5	1
ONT chassis	2,5E-5	1
Wireless path	3,3E-5	1
PON	1,33E-4	10,4*
Backhaul fibre	1,2E-5 (per km)	512
OLT TRX	1,1 E-5	512
OLT chassis	2,2E-5	512
OLT wavelength multiplexer (AWG)	9,0E-6	512

***Averaging the FPR of last fibre drops, distribution fibres and 4 feeder fibres in a cascaded configuration 1x8 plus 1x16 splitters (1:512 total split ratio) with fault probability of 75%, 20% and 5%, respectively.**

For monitoring purposes, the wireless path can be used for reporting ONU status and monitoring parameters as well as physical layer measurements from ONU embedded OTDR if available. Embedded OTDR technology from ONU side is analyzed further in this Deliverable, see Section 4.2.2.

Here we examine the impact of this wireless path in the access network reliability.

For reliability purposes, the ODN of the ONU used for wireless protection should be different that the HA-ONU's.

First, we can see how the Failure Impact Factor (FIF) is reduced almost two orders of magnitude using the feeder fibre and OLT protection in DISCUS LR-PON, see the following figure.

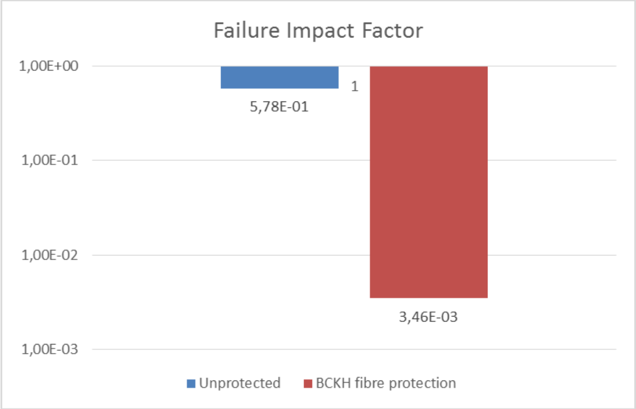


Fig. 6. Failure impact factor of an unprotected LR-PON and a LR-PON with backhaul fibre protection (DISCUS).

Next, we analyse the availability increase due to the wireless backup channel, see the following figure.

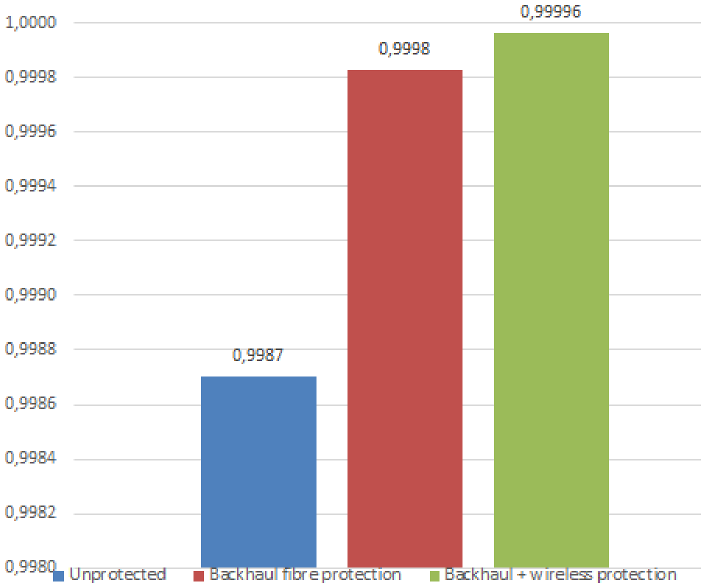


Fig. 7. Connection availability in hybrid access within DISCUS LR-PON.

With the assumed reliability parameters, the total connection availability reaches four 9's in the case of hybrid access from three 9's in the standard DISCUS LR-PON connection. The reliability in the unprotected scenario would be only two 9's.

Apart from the advantage of the availability improvement, this backup channel opens also the possibility of employing eOTDR fibre supervision from ONU side. The eOTDR technology is able to provide fibre measurements from ONU side when a fibre fault takes place (see section 4.2) and report the measurement results to a remote system using the wireless backup channel. Thus, the hybrid fibre/wireless access is not only beneficial from protection and network reliability side, but also from the point of view of operational and maintenance cost-efficiency.

2.3 SDN-enabled PON protection experiments

In our work on LR-PON protection we have investigated end-to-end service restoration times for networks using next generation LR-PON and Software Defined Network (SDN) controlled core networks. Our PON protocol is implemented on FPGA and is networked to an SDN controller running OpenFlow. In this section we present and evaluate the DISCUS dual-home LR-PON protection mechanism.

During the course of the project we have investigated different types of protection mechanisms, namely 1+1 [21], 1:1 [22] and N:1 [23]. While the ultimate goal in DISCUS is to demonstrate N:1 protection, which allows sharing standby OLTs among different PONs, we discuss also the results of the 1:1 case as such scenarios present a build up towards the N:1 case have many features in common. The protection mechanism 1+1 was already presented in D4.4.

All protection cases are based on dual homing, e.g., the feeder fibre section of the PON is protected by connecting the first stage splitter to two MC nodes.

In a previous deliverable D4.4, Section 5, we have already discussed the main ideas behind control-plane based link restoration for 1+1 and N:1 protection, and showed testbed results for the 1+1 protection case. In addition, the abstract control-plane view of the third scenario, that handling PON protection, was presented in section 3.4 of deliverable D6.3 “Report on the design of the interfaces of the control plane”, while the primitive APIs used for protection were presented in section 5 of the same deliverable. While further implementations details will be presented in the deliverable D6.5 “Final report on the specification of the metro/core node architecture, including reports for D6.4 and D6.6”, in this section we report the protection results we have obtained for the 1:1 and N:1 protection cases. Both cases reuse the results on PON activation already presented in D4.4 (and thus not reported in here).

2.3.1 1:1 protection experiments

While the 1+1 feeder fibre protection schemes, described in D4.4, duplicates the core traffic, so that only access restoration is required, the 1:1 protection requires interaction with the core control plane which needs to activate pre-calculated backup paths (i.e., Label Swicthed Paths –LSP).

The 1:1 scenario assumes, like the 1+1, that a standby OLT is dedicated to a specific PON (and thus the operations for PON activation presented in D4.4 still apply). However the traffic in the core is not duplicated, and needs to be re-directed from the primary MC node to the secondary MC node when a failure occurs. While it is possible that a direct connection between primary and secondary MC nodes is available with enough capacity, in our tests we assumed the worst-case scenario, requiring re-routing of flows throughout the core network.

In order to calculate realistic protection times for an OpenFlow-based core network we have interconnected our access network lab in Trinity College Dublin with the Pan-European GEANT network. The experiment for the combined access and core networks spans the optical architecture test bed in Trinity College Dublin and the GEANT pan-European research and education network. In this experiment connectivity between the two portions is achieved over the Internet, while for the experiment described in the next section we were able to obtain two dedicated 1GE links to the GEANT nodes in UK and the Netherlands.

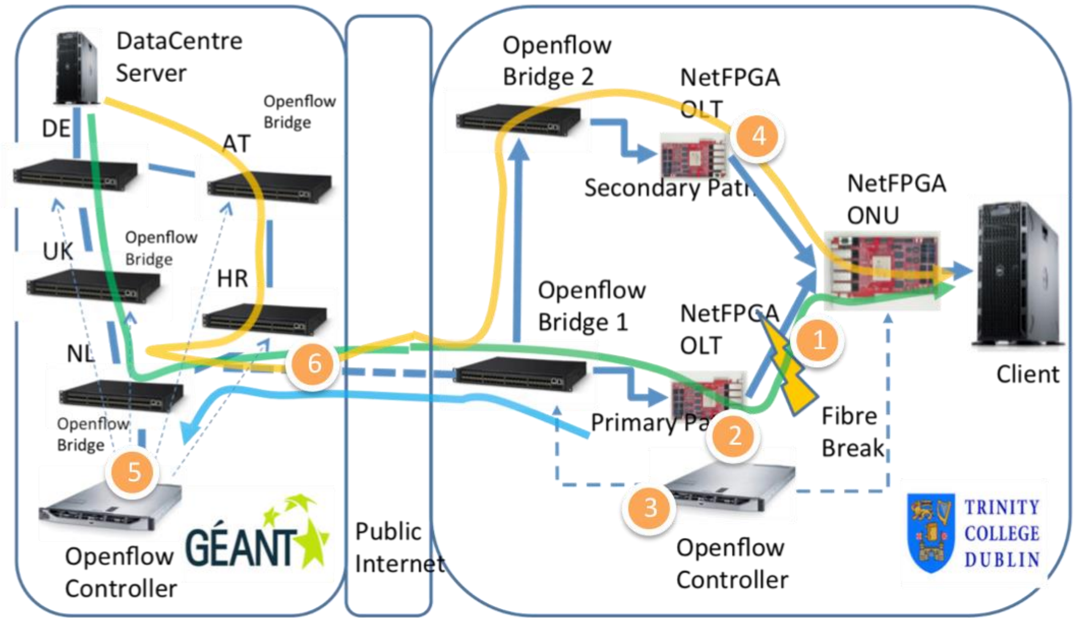


Fig. 8. Logical view of combined LR-PON access and SDN Core network for 1:1 protection

The GEANT OpenFlow facility is a test-bed environment deployed on top of the GEANT production network. The facility is built on network resources such as software-based OVSwitch OpenFlow switches and interconnecting network links. It is collocated with five of the GEANT Points-of-Presence in Vienna(AT), Frankfurt(DE), London(UK), Amsterdam(NL) and Budapest(HR).

The OFELIA Control Framework (OCF) is used by the GÉANT OpenFlow facility to manage requests for slice submission, instantiation, and decommissioning. OCF is a set of software tools for testbed management, which controls the experimentation life cycle such as resource reservation, instantiation, configuration, monitoring.

In GEANT we have created a five-node network topology, with nodes in Amsterdam (NL), Frankfurt (DE), Hungary (HR), Austria (AT) and London (UK). Collocated with Node DE is a server which acts as a Data Centre. The primary path in the core is through nodes DE, UK and NL, with the diverse fallback path from nodes DE through AT and HR to NL. Since node NL is the only gateway to our access network, both primary and protection paths pass through this node, while in a more realistic scenarios the node hosting the backup OLT would be connected directly to a node on the secondary path. However this serves the purpose of carrying out core network redirection. NL also hosts the OpenFlow core network controller.

For our access network, the configuration is comprised of a Pronto 3780 switch with 48 10G interfaces, running release 2.2 (OpenFlow v1.3 compatible firmware), and a Hitech Global 10G NetFPGA board acting as twin OLTs and ONU. The Pronto switch is configured with multiple virtual bridges. A VPN tunnel extends between the access and the core network gateways. A Dell R320 acts as the OpenFlow access controllers running RYU9. In our 1:1 scheme, data travels through the primary OLT and the primary bridge. The standby path, through the secondary OLT and secondary bridge does not carry any traffic until it is invoked, at which stage all primary traffic is redirected. Link availability is determined by the transmission of a UDP packet every 1ms between the DataCentre (DE node) and the Client (terminated on the ONU in the TCD testbed).

The failure detection mechanism was extended with respect to the 1+1 testbed in that it needs the OLT to be able to communicate with the MC node controller to pass information about the failure and trigger the OpenFlow route modification in the core. In our experiment described in Fig. 8, the feeder fibre between the primary OLT and first stage splitter on the PON is cut (1). This stops all data from being transmitted upstream or downstream on the Primary link. A hardware unit in the primary OLT FPGA monitors the upstream data. The hardware detection unit alerts the OLT controller which sends an in-band upstream alarm (2). An upstream alarm is required, because the OpenFlow bridge does not physically terminate the connection between the ONU and the OLT, which means that it is not possible for OpenFlow path switching rules (such as Group based port protection) to be invoked due to the fibre cut.

Failure detection is achieved by listening to the upstream transmission: once any ONU has been registered on a particular PON, the upstream fibre should be quiescent for no longer than a single quiet window. For a LR-PON of 125 Km, as proposed by the DISCUS project, this would be equivalent to no more than 1.3 ms. Taking round trip time into account, the hardware failure detection unit would detect a break in the fibre in approximately 2.5 ms, in order to avoid false alarms based on a particular occurrence of the quiet window.

Then, the data plane of the OpenFlow-based primary bridge intercepts the upstream alarm, which it then forwards to the access node controller (3). The OpenFlow controller instructs the OpenFlow switches to route traffic through the secondary bridge and the backup-OLT (4). The upstream alarm is also sent to the OpenFlow based controller for the core network (5). The core network controller builds the backup path in the core from the nodes DE through AT and HR to NL (6). While it is not possible for OpenFlow path switching rules to be invoked directly by interception of this alarm (that is, solely within the data plane), we have devised an OpenFlow relay (OF-Relay), located on-board the Pronto switch, that performs fast updating of the access fast recovery rules on the switch, as well as forwarding the alarm to the higher layer control infrastructure. The fast recovery paths are invoked and revoked by an application of a single *goto_table* statement injected into the primary switch.

The results for the test, measured over 50 failure/restoration cycles, are shown in Figure 9 for the access part and in Figure 10 for the core part. The average values we have calculated for protection is about 7 ms for the access and 117 ms for the core. The plot on the right hand side represents the measured data points, while those on the right hand side show the probability distribution obtained from the results. It can be seen that while we can obtain more deterministic protection times in the access, the core present more variable results. This is due both to the larger size and distances that occur and the lower degree of control we have on the GEANT network (both in terms of usage of the GEANT OpenFlow network and of the non-deterministic behavior of our links to GEANT which were achieved through the public Internet).

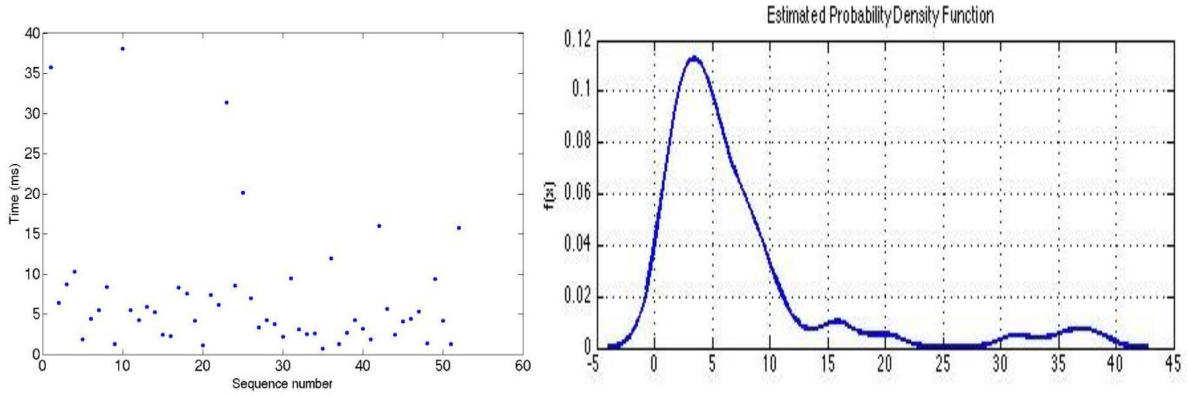


Fig. 9. Measured points (left hand side) and calculate distribution (right hand side) for connection restoration in the access.

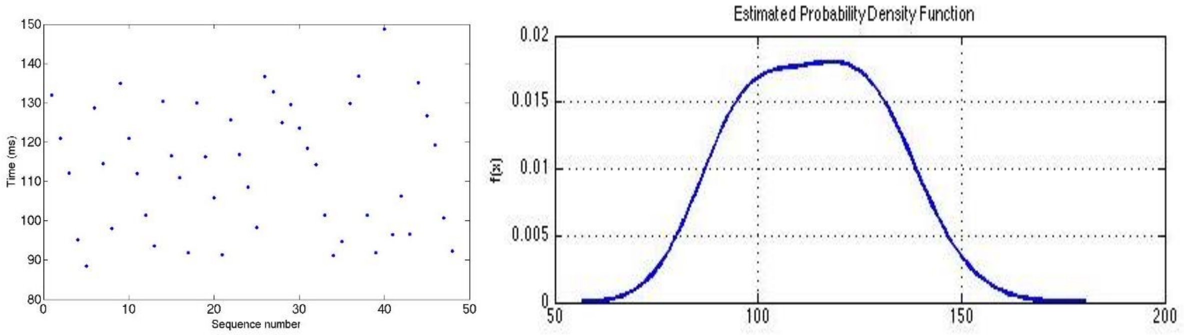


Fig. 10. Measured points (left hand side) and calculate distribution (right hand side) for core traffic reroute.

A breakdown of the latency time can be seen in Figure 11: full recovery takes place over an elapsed time period of 124 ms. Failure is detected in parallel by both primary and standby OLTs in this case, which occurs in about 3 ms. While the standby OLT proceeds with reactivation, which is completed in average within 7 ms, the primary OLT also notifies the control plane, triggering the traffic reroute in the core. It takes in average 117 ms in order to complete the core reroute, of which 67 ms are spent in the configuration (which occurs in series) of the OpenFlow controllers at the different nodes. The bulk of the 117ms is caused by two factors: link latency and the synchronous sequential update of the OpenFlow rules in the four OpenFlow switches along the backup path in the core. The time lag between the access control plane sensing the failure and the controller in the core receiving the trigger over the Internet connection takes about 50ms. For each of the four nodes, it takes between 16ms and 18ms for the core controller to execute the OpenFlow OFPFC_ADD instruction.

Much of the elapsed time is taken up by the time to transmit the instruction between the controller and node, and an acknowledgment to be received. POX executes these instructions synchronously and sequentially over a time period lasting 67 ms. This value, as shown in the next section, can be reduced significantly if the instructions could be issued asynchronously or in parallel by multi-threaded dispatcher. This becomes a function of the longest node update time between the controller and a node (in this instance, 18ms).

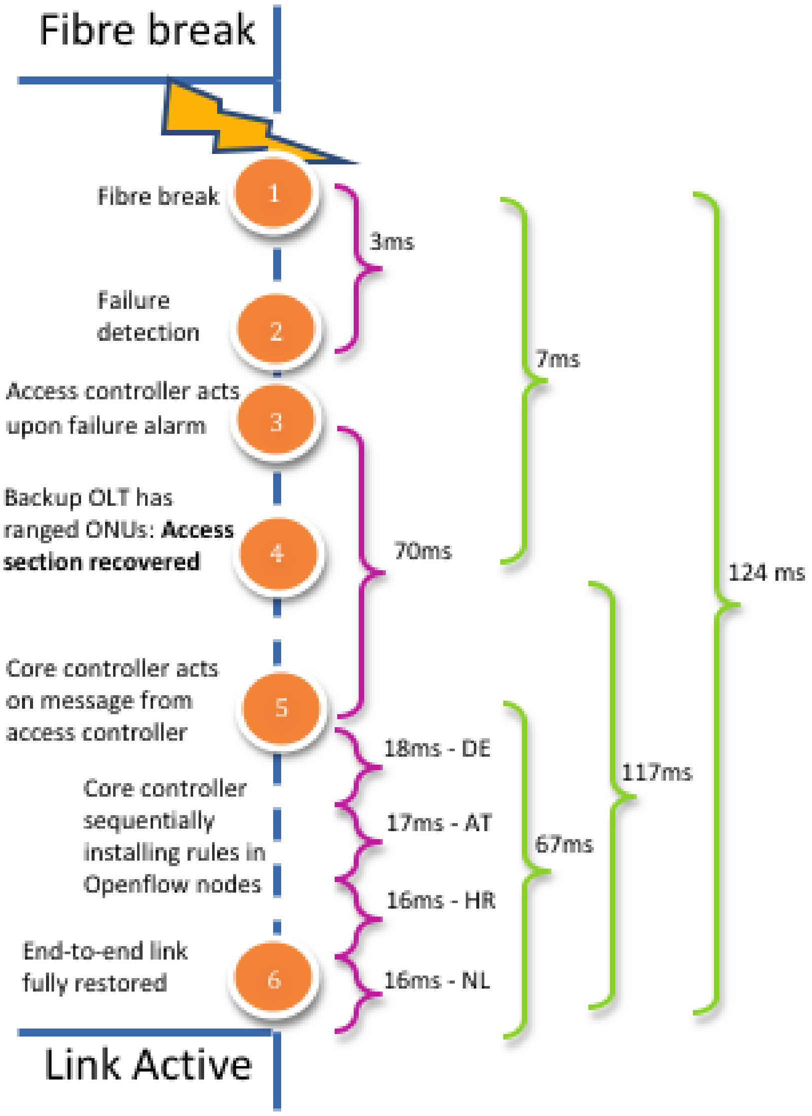


Fig. 11. Timing graph of control plane messaging and operations for feeder fibre protection using N:1 sharing of backup OLTs

In addition, the GEANT network is much larger than any national network in Europe, thus it represents a worst-case scenario. For typical sized countries using dedicated links between the access and the core, the total elapsed time for recovery could be reduced to 41ms. This would be composed of 7ms recovery in the access, 16 ms latency between access and core controllers, 18ms asynchronous parallel updates from core controller to switches.

2.3.2 N:1 protection experiments

The main difference between 1:1 and N:1 protection is that in N:1 standby OLTs are shared among a number of PONs in a N:1 ratio. While the core reroute remains similar to the 1:1 case, the access part requires some modifications. Firstly we need to include an optical fibre switch between the OLT and the PON. Secondly, and as a result of the presence of the optical switch, the standby OLT cannot sense anymore the loss of light from a PON. While there could be option to use the power meter of the optical switch to assess the loss of light, as previously discussed, the timing needs to be accurate in order to avoid false positive alarms due to quiet windows. In addition, if the upstream traffic is low a simple power meter would detect very low power, while the OLT is still able to recognize that there is a transmission as it can detects any incoming burst. For this reasons it is more reliable to use the primary OLT for detecting the failure: this event is then used to activate the access protection mechanism at the MC node controllers.

We tested our N:1 end-to-end protection service with dual-homed, backup OLT sharing by combining the Optical Network Architecture (ONA) lab in Trinity College Dublin and the GEANT Pan-European research network, as shown in Figure 12. While the setup is similar to that in **Error! Reference source not found.**, the figure shows the addition of he optical switch, and the use of private lines between our lab and the GEANT OpenFlow testbed. In addition at this stage of the FPGA development we had migrated our implementation into a more powerful Virtex 7 evaluation board. The testbeds are connected through two dedicated GE links. Although this link is well below the 10Gb capacity of the LR-PON, having dedicated data links allows us to reliably evaluate latency effects between diverse network elements and the higher-level control layers. The experiment replicates both the metro-access and core networks of a high-speed fixed line telecommunications network. Lie for the 1:1 case, the end-points replicate a data centre generating traffic (located in Frankfurt) and a reception or termination point located on a PON ONU in Dublin.

The primary and backup core routes are similar to those in the 1:1 case, with the difference that in this test we access the UK and NL nodes individually through two dedicated private GE connections. In this way we were able to reduce the variance associated with the use of public Internet links.

From an access perspective the only difference in the architecture is the presence of the optical switch, which connects the backup-OLT and the ONU, allowing the backup OLT to switch between a number of different PONs.

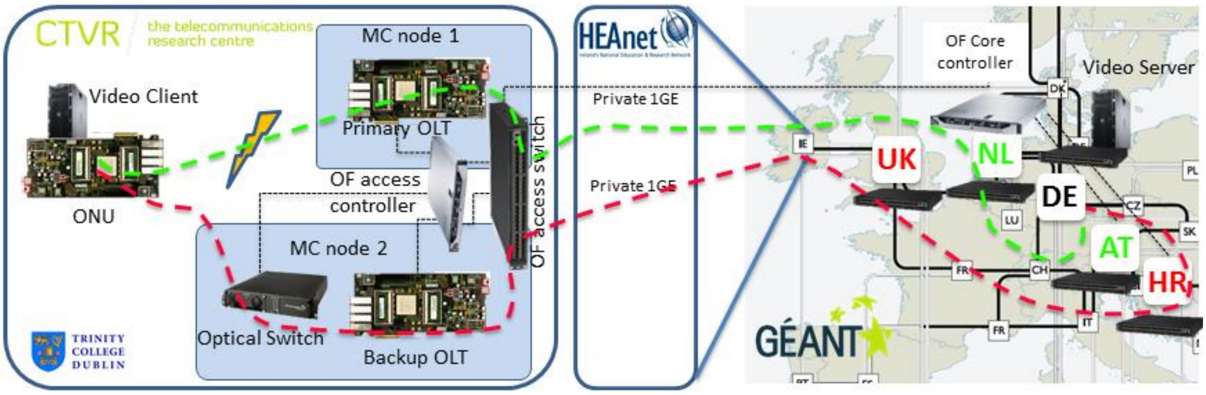


Fig. 12. Logical view of combined LR-PON access and SDN Core network for N:1 protection.

Figure 13 shows the end to end N:1 dual homed protection time of the LR-PON and SDN core over 50 experimental iterations, using the initial break in the fibre as a reference point.

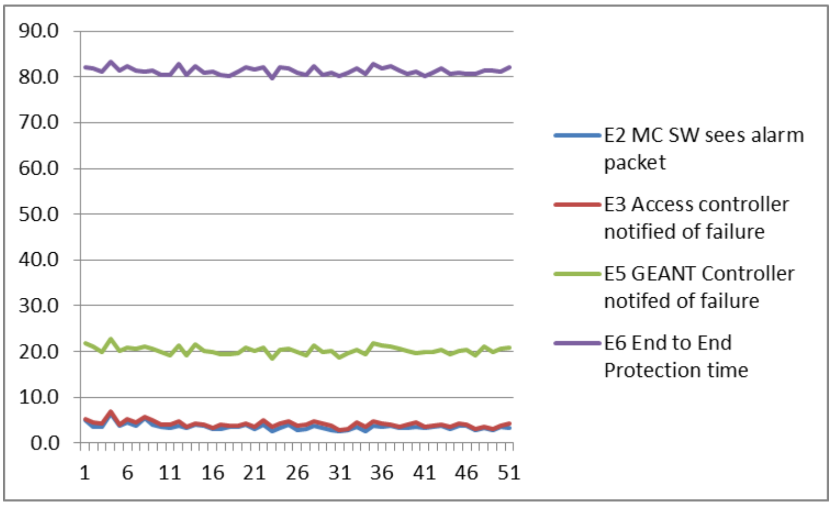


Fig. 13. Switchover time (milliseconds) for 50 iterations of N:1 protection experiment

Since the trigger failure event was issued to the FPGA board over a UART it was not possible to read an absolute time value from the FPGA boards for when the break in the primary fibre occurred. However, we were able to work back from the restoration point of traffic by subtracting the outage duration within each cycle. On average, the alert that identifies loss of the primary PON (E2) occurs 3.5ms after the break. The OpenFlow controller within the TCD ONA testbed sees the alert 0.59ms (E3) after this and publishes a NetEvent failure alert as well as a GlimEvent event. The NetEvent alerts the GEANT controller to invoke the alternate path through the core. The GlimEvent event invokes the secondary path in the optical switch. Within this experiment, the GEANT controller sees the NetEvent event 20.3 ms after the initial failure (E5). Separately, we have measured the asynchronous switchover of the optical switch as 23ms. Overall, Restoration time of the data traffic is measured as 81.29ms.

The restoration time of the network can be split into three distinct phases. These are the time it takes to detect a failure on the network, the access network recovery time and the core network recovery time. In Fig. 14 we show how these times stack up to give the 81ms protection figure. As discussed previously the hardware monitoring at the OLT can detect a failure in the network in about 2.5 ms. We can see from the results in Figure 14 that a further 1ms is taken for the alarm packet to be created and sent to the Metro core node switch. The access recovery time was measured by a counter at the ONU. The counter is started when the ONU enters the temporary loss of downstream synchronization state and stops when the ONU returns to the operational state.

We found the access recovery time to be approximately 25 ms, which can be further broken down into time required to tune the optical switch (23 ms) and time needed by protocol to re-establish downstream synchronization (2-3 ms). From our previous work we know that some time may be needed to re-range the ONUs in addition to the synchronization time (between 2 and 4 ms), however in this work we assume that ranging to the backup OLT can be done during normal operation of the PON. The remaining time is needed by the local OpenFlow controller to communicate with the optical switch to connect the backup OLT.

The core network recovery time happens in parallel to the access network recovery time. The core controller sees the failure event approximately 20 ms after it happens. It then begins to reconfigure the network to reroute data to the backup path. Since we know the latency of this path is approximately 50 ms we can calculate that core network switch over takes approximately 10 ms.

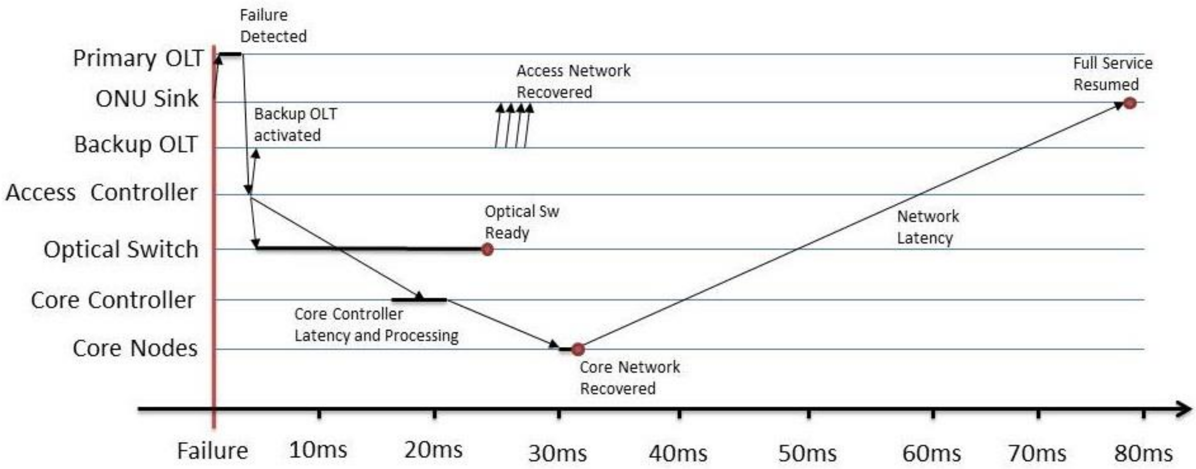


Fig. 14. Breakdown of protection time

2.3.3 Further discussions

In this section we discuss two main points. The first is the importance of having low protection times in the access, while the second relates on how could failure detection and monitoring mechanisms be handled by the DISCUS control plane.

2.3.3.1 Importance of fast access protection

While todays SLAs for residential broadband customers are quire slack, where in some cases agreement on restoration times could be of the order of weeks, a next-generation architecture like DISCUS requires better protection performance. Firstly the DISCUS access replaces the metro transmission network, which is normally protected in today's networks. Secondly, due to the longer feeder fibre and larger customer aggregation, fibre cuts become more frequent, and any cable cut could affect tens of thousand of customers.

Thirdly, it is expected that the DISCUS network will multiplex different type of users and services into the same physical infrastructure. If different broadband contracts with different SLAs are multiplexed into the same transmission network, the protection needs to be able to satisfy the strictest of all the SLAs requirements.

Finally, fast protection times can allow a much better utilization of protection resources. In [39][40][41] [39]we presented a method that by redirecting primary OLTs and IP network resources to protect for failed equipment, make it possible to reduce the overall amount of protection equipment by 50 to 80%. Since however these mechanisms requires redirecting active connections across large part of the network, such operations might only be viable if service restoration time, following any one failure or connection redirection, can be achieved in times below 100 to 200 ms.

2.3.3.2 Failure detection and monitoring in a control plane context

As evident from the previous sections, fault detection needs to occur within few ms if we want to keep the protection time low enough to operate without noticeable disruption. The method used for our experiments, based on Loss of Signal (LOS) detection by the OLT, allows to operate the decision mechanism based on time measurements, giving the ability to make a decision based on the protocol (e.g., as previously explained, to allow for the fact that no signal is generated by the ONUs during the quiet window).

A second option is to use the power monitors of the optical switch to detect Loss of Light (LOL). While the advantage is that this can operate directly at the MC node where the backup OLT is located (and thus potentially speed up the protection process), we find this solution inferior to the OLT—based one as the switch monitors operate in the analog domain and provide an average value of the incoming power (typical sampling times are few KHz). The main issue is that, due to the bursty nature of upstream transmission, the power averaging operated by the switch power monitor could generate false alarms during network quiet times, when there is little transmission from the ONUs towards the OLT.

The OLT-based fault detection is our preferred option, as it can quickly determine whether there is a disconnection in the ODN. It should be noticed that the protection technique examined in this section is only able to protect against a cut in the feeder fibre. The OLT can determine whether there has been a fault in the common part of the ODN (i.e., the feeder fibre or one of the EDFA in the remote node) as no information is received at the OLT in this case. It can also determine whether there has been a partial failure (e.g., fibre cut in a branch of the ODN), in which case it will loose signal only from a selected number of users and will not activate the feeder protection mechanism.

In both cases the OLT-based fault detection can be used to trigger an alarm towards the PON optical supervision system (such as one of the OTDR-based systems described below). It is envisaged that in this case the OLT could trigger a failure message towards the node controller also when there is a partial failure (i.e., one or more ONUs are not transmitting upstream). The controller can then forward this information to the Network Management System, which can operate intelligent algorithms based on the history of that specific ONU or using knowledge on the location of the ONUs with respect to the PON branches to infer the type of failure that occurred. This information can then be used to prompt an alarm to the network administrator which can complement this information with embedded OTDR testing, verify the failure location and ship a team to fix the fault, thus reducing sensibly the failure restoration time and its associated OPEX.

3 Advanced fibre infrastructure management with Intelligent Splitter Monitoring (ISM)

In the optical access domain deployment and maintenance of the passive infrastructure are still associated with very high operational expenditures (OPEX). Processes to manage the infrastructure are not so deeply developed and introduced compared to the copper world. Today available fibre infrastructure management systems are mainly based on the documentation during the rollout of the network. Problems occurred when the documentation went from bad to worse during lifetime and could end up in a nightmare, if net modifications to adapt the network for new requirements are not described exact in the documentation. A new approach is driven from the Chinese market to tag [24] the fibre connectors in the distribution frame. An automated readout system of the fibre tags can ensure the right fibre connections in the field. These tag information can support the work order management and the network documentation after rollout and network modification. A fibre infrastructure management system [25] is setup do manage this tag information. This system is strong during the installation and documentation of the fibre network infrastructure. Drawback of the system is that it does not support a remote operation. The system relies on a service craft that connects a handheld device to the mainframe of the node equipment. The information from the data collector within the node equipment is transmitted via the field operation tool to the management system as shown in Figure 15. The field operation tool could be a device like a Personal Digital Assistant (PDA), which also could provide electrical power to the node equipment.

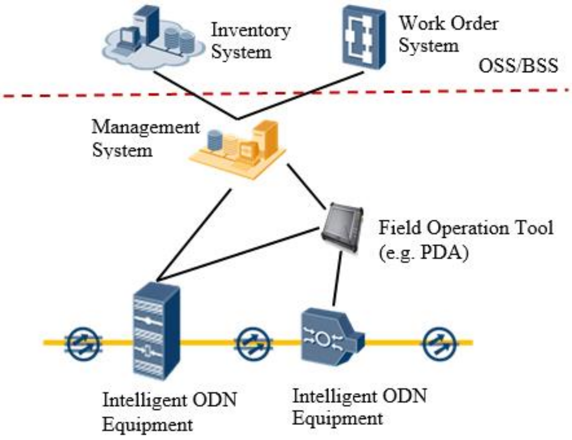


Fig. 15. Schematic of the architecture for a fibre infrastructure management system.

Advanced solutions for fibre management infrastructure system are of interest by the operators to implement remote measurement and configuration elements into their network. The intelligent splitter monitor (ISM) is a concept developed to determine the connectivity of the optical network units ONUs with regard to the corresponding splitter ports within the optical distribution network (ODN). The solution is based on a remote optical powered ISM module which detects the tapped upstream signal of the ONUs at each branch of the splitter. The measurement results are reported back to the central office where they will be bridged to a management system. Within the management system a correlation between the ONU status and the measurement results will be done to identify the connection of the ONUs to the splitter ports. This information is very important for the operator before he starts maintenance work in the field. The risk of mishandling on site will be drastically reduced.

A schematic drawing of the component is shown in Figure 16. Based on the hardware platform of the ISM an additional latching blocker function would allow further control capabilities in the remote nodes. The protection of the ODN from rogue ONUs will be addressed by a port blocker. In addition, depending on the energy balance, other sophisticated control functions might be possible.

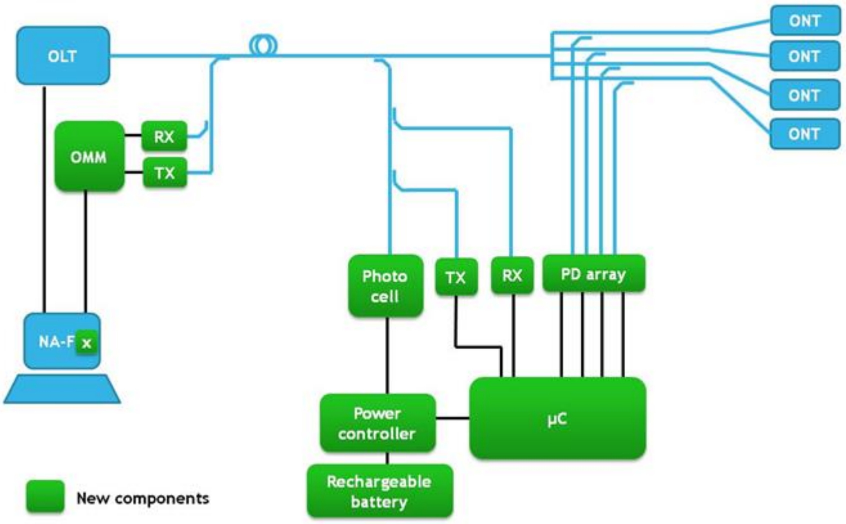


Fig. 16. Sub components of the splitter monitor. At the central office, an ODN management module (OMM) is added to provide the energy for the splitter monitor via a high power laser. The laser (TX) and the receiver (RX) are used for the communication between OMM and splitter monitor on the right hand side. The micro controller (μC) is used to process the upstream detection at the photodiode array (PD array).

Static connections and the lack of real-time updates on the health and status of the network inhibit flexibility and dynamic services on demand. It is the long term goal to build remote performance measurement and configuration functions into the outside fibre plant and to automate the manual main distribution frame (MDF).

The desire for flexible, automated solutions in the access plant is not new. For more than 15 years, operators have sought cost-effective automated switching and monitoring systems for the local loop. The fact that both well established operators (e.g. AT&T, Verizon, Comcast) and newer entrants (e.g. Google) have enthusiastically embraced and committed to the virtues of software-defined networking (SDN), strengthens the case for automating the entire network from core to access and including the optical distribution network. And yet, the price points and scale for automated technologies (particularly large-scale optical cross connect switches) still pose a huge challenge for the access network.

All of these facts indicate that SDN, automated provisioning, automated fault monitoring, protection switching, etc. will not be limited to the core network for long. The automation of OAMP functionality in the access network is coming and will likely be a big business.

4 New proposals for optical layer supervision in LR-PONs

4.1 Transmission and reflection analysis based dark fibre supervision

Nowadays, long reach passive optical networks are receiving more attention thanks to its large coverage (reach ≥ 60km) and high bandwidth [26][27]. DISCUS architecture is composed of LR-PON as access segment and flat core for backbone network. Among different topologies proposed for LR-PONs, the “ring and spur” approach (where a ring is employed for the feeder section and followed by several sub-trees forming the distribution segments as shown in Fig. 17) is currently receiving an extensive investigation because of its low infrastructure cost and high reliability [28]. However, due to high capacity provisioning and large coverage, a single failure occurs in the LR-PON can result into a huge loss of data. For DISCUS, dual parental protection is considered to avoid high impact on end users if any failure on feeder section occurs. Meanwhile, in order to minimize the interruption time and to improve the network reliability, pro-active fault monitoring of the LR-PON becomes extremely important.

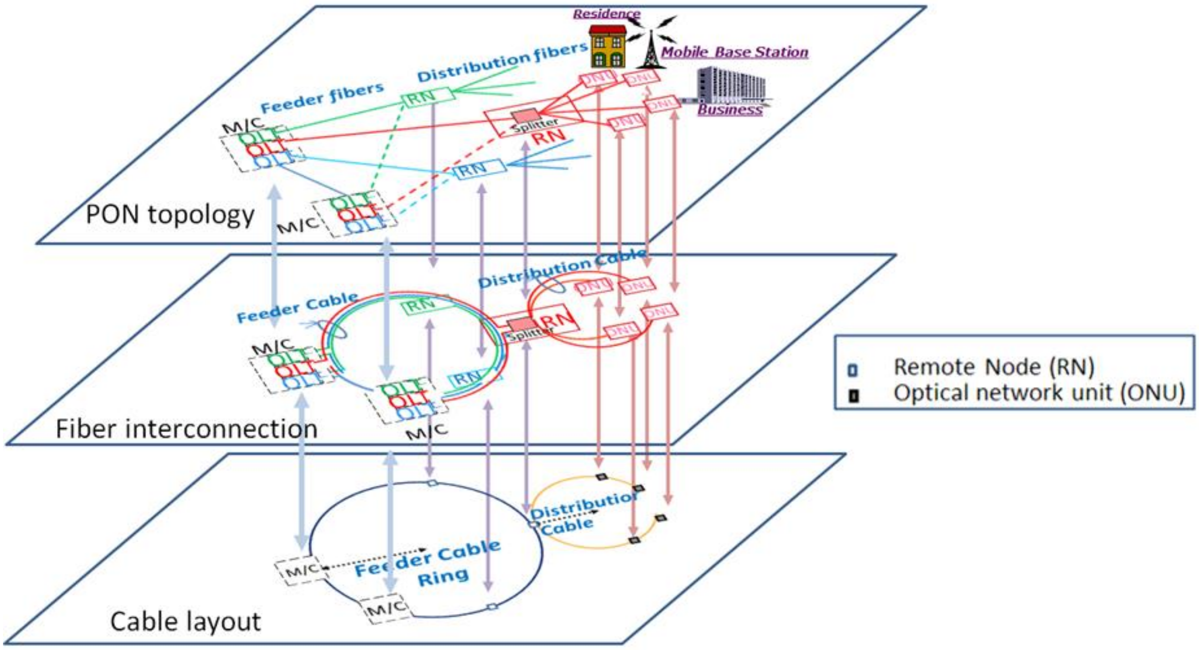


Fig. 17. Fibre interconnection of “ring-and-spur” LR-PON

Among various techniques, optical time domain reflectometry (OTDR) is currently the most widely used one for PON monitoring. However, for LR-PON, OTDR monitoring approach might have some issues, e.g., the measurement time is very long and the working wavelength of OTDR is not compatible with the installed active optical devices. Besides OTDR-based solutions, other methods can be found in the literature, the authors proposed in [29] to use optical reflectors to monitor the whole network (metro and access), while the authors in [30] suggested to use optical encoders to monitor the metro ring of Long Reach-PON (LR-PON). For both aforementioned techniques, the localization functionality, which is a key for LR- PON fault monitoring, unfortunately cannot be supported.

In this section, we report a monitoring system using *dark fibre* and multi-wavelength Transmission Reflection Analysis (nλ-TRA), which is capable of detecting, identifying and localizing major faults (breaks, bendings…) in the feeder ring [31]. A “dark fibre” refers to a fibre that is deployed in the same cable as the working fibre but does not carry any data yet. To monitor the dark fiber instead of working fiber, the failure that is shared by the fibers in the cable (i.e., shared risk link group) can be detected. Therefore, dark fibre monitoring can cover the major faults, such as cable cuts and bending/seepage [32]. Also, by using a dark fibre, one can choose any set of monitoring wavelengths without affecting the data signals. Given that, the dark fibre based monitoring scheme enables an effective and flexible LR-PON monitoring.

4.1.1 TRA Based monitoring technique

Among different monitoring techniques, Transmission Reflection Analysis (TRA) approach, which only requires to measure the power of transmitted and backscattered monitoring signals, outperforms the other solutions (e.g. OTDR) with respect to measurement time, system complexity and dynamic range. TRA is a simple, efficient and inexpensive monitoring technique, which has been proposed for sensing applications [32] using a single-mode fibre in point-to-point configuration. The definition of the TRA technique can be found in [32]. A brief introduction is provided hereafter to depict its basic concept. As shown in Fig. 18, when a Continuous Wave (CW) signal with a launched power P_0 is injected into one end of the optical fibre, a transmitted power P_T can be measured at the other end of the fibre. At the same time, a reflected/backscattered power P_B, which is mainly due to Rayleigh backscattering distributed all along the fibre, can be observed at the same end of the fibre as the signal is launched. The schematic diagram of TRA technique is depicted in Fig. 19. A continuous-wave light emitted by a Super Luminescent Diode (SLD) is launched into a single mode fibre through an optical circulator. An optical isolator is used to minimize the reflection from the fibre end. P_T is measured by a powermeter located after the isolator while P_B is measured by another powermeter connected to the circulator. Since for a given fibre with a single lossy event, the relationship between P_T and P_B only depends on the event location, by measuring P_B and P_T the event can be localized. However, this TRA approach is only suitable for non-reflective events (e.g., bending, seepage). Moreover, in the long reach (e.g. fibre length >> 20 km) case, the TRA technique presents quite low fault localization accuracy when the events occur close to the remote end.

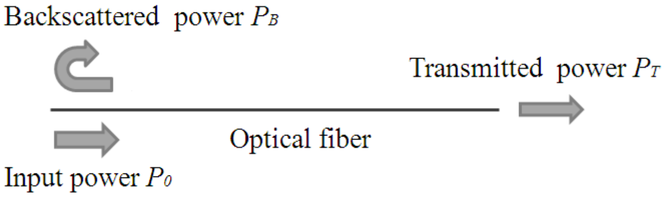


Fig. 18. Definition of transmitted (PT) and backscattered (PB) powers

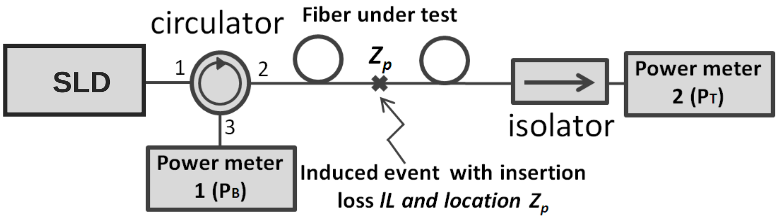


Fig. 19. Schematic diagram of TRA approach.

In order to make the TRA approach compatible with reflective events (e.g., fibre break, connector mismatch) that may occur in the LR-PON, in [33] we have proposed a novel multi-wavelength TRA (nλ-TRA) technique. The schematic diagram of the proposed nλ-

TRA is shown in Fig. 20, where a 2λ-TRA (i.e., using two wavelengths) is taken as an example. Each time, one of the two light sources (SLD_1 at λ_1 and SLD_2 at λ_2) is launched into the test fibre. The transmitted power (PT_1 at λ_1 and PT_2 at λ_2) and the integrated reflected/Rayleigh backscattered power (P_{B1} at λ_1 and P_{B2} at λ_2) are measured by the two power meters similar as the previous case with single-wavelength TRA. The localization process of a reflective event can be based on the unique relationship between the backscattered (P_{B1} and P_{B2}) and transmitted (P_{T1} and P_{T2}) powers for a given event location z_p and return loss (RL). In other words, two different equations (since the related parameters are wavelength dependent) can be formed to calculate P_{B1} and P_{B2}, the problem of localizing an event finally can be addressed by solving these two equations with only two unknown variables (i.e. z_p and RL).

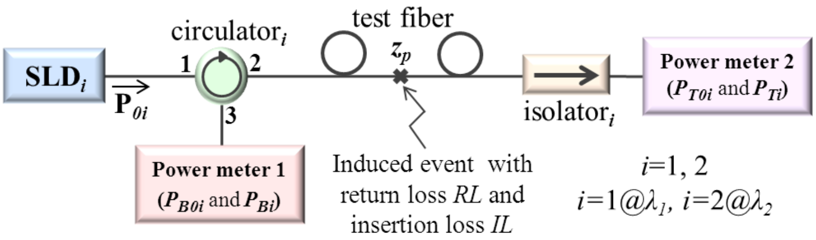


Fig. 20. Schematic diagram of 2λ -TRA technique [34].

Furthermore, considering of improving the low accuracy at the remote end so as to measure the long-reach case, a bi-directional scenario has been proposed by us in [34]. As shown in Fig. 20, by launching the signal in both fibre ends with two opposite directions, the remote end in Fig. 21(a) becomes the front end in Fig. 21(b). Both theoretical analysis and experimental validation demonstrate that this bi-directional scheme can reach high localization accuracy for localizing a fault near the remote fibre end.

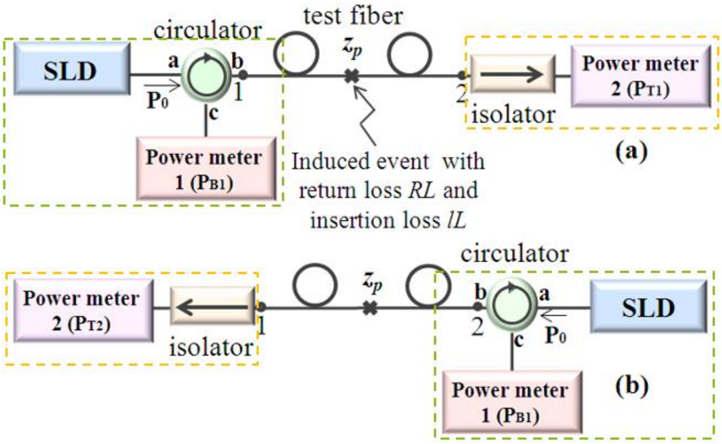


Fig. 21. Schematic diagram of bi-directional TRA technique.

4.1.2 Operation principle

The proposed LR-PON monitoring system is depicted in Fig. 22, which combines the aforementioned nλ-TRA and the BD-TRA. In which, the 2×2 optical switch (OS) is used to realize a bi-directional measurement configuration especially tailored for the ring structure. The OS state in parallel lines means that the measurement is performed in the clockwise direction, whereas it is performed in the counter-clockwise direction when the OS state is in the state of crossing lines. Both PTs and PBs are measured by the dual-channel powermeter.

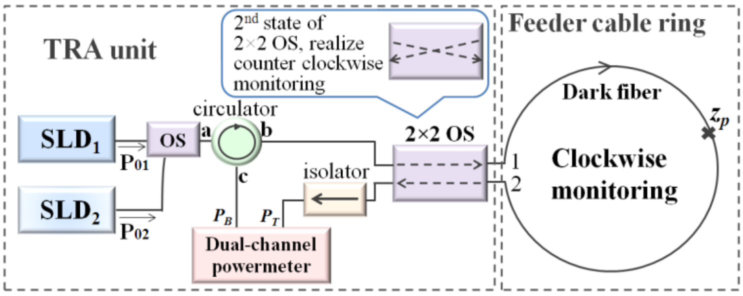


Fig. 22. Schematic diagram of the proposed "dark fibre"and nλ-BD-TRA based monitoring scheme.

Let us note that the events occurring in a fibre can be divided into non-reflective and reflective. Bending and seepage are included in the first type while fibre break is counted in the second type. For achieving high accuracy of localization, 1λ- and 2λ-TRA should be applied in the first and second case, respectively. The corresponding calculation models are described in [36] and [37] for monitoring bending and fibre break.

The overall monitoring procedure is described hereafter. If a fault occurring in the feeder cable ring is detected by the logical/network layer, one of the two light sources in the monitoring system will be first triggered. The next step consists in measuring the transmitted monitoring power (P_T) detected by the power meter at the central office (CO). If the power meter shows a null output of P_T, it indicates the occurrence of a fibre break. In such a case, the other light source will also be triggered to realize a 2λ-BD TRA solution and localize the break. If the power meter only shows a decrease of P_T, it indicates that the fibre is still connected but an event with a big loss introduced, which implies either a fibre bending or seepage. The 1λ-BD TRA measurement will then be activated to localize the bending or seepage.

4.1.3 Validation and discussion

The experimental set up is shown in Fig. 22. In the experiment, a fibre break and a bending are introduced at five different locations along a 56.03 km-long standard single-mode fibre. The SLDs used in our experiment are operated at 1307.5nm (SLD_1) and 1564.6 nm (SLD_2) with 80.4 nm and 57.9 nm spectral width, respectively. The input power (P_0) is 10.73 mW for SLD_1 and 12.79 mW for SLD_2. For comparison purposes, the event localization has also been measured by a commercial OTDR, which has a localization accuracy of 30 m (a pulse duration of 300 ns has been selected in order to get a necessary dynamic range). The experimental results for fibre break are presented in Table IV. Good agreements between the OTDR measurements and the 2λ-BD-TRA scheme have been achieved.

TABLE IV

COMPARISON OF THE BREAK LOCALIZATIONS (z_p) MEASURED BY OTDR AND THE PROPOSED TRA BASED APPROACH

	z_{p1} [km]	z_{p2} [km]	z_{p3} [km]	z_{p4} [km]	z_{p5} [km]
OTDR	0	1.726	26.44	51.12	56.03
2λ-BD-TRA	0.003	1.727	26.42	51.13	56.02

Difference	3m	1m	20m	10m	10m

Besides fibre breaks, experimental verifications of bending have also been carried out. In bending measurement, 1λ-TRA is applied as the monitoring technique and SLD_1 is used as the light source. Similar with fibre break, a bending with an 11.2dB bending loss (measured by OTDR) is introduced at five different locations of the fibre ring. Experimental results for TRA based solution are presented in Table V. A maximum localization difference (δz_p) of 18 m has been observed at the location of 26.44km, demonstrating the capability for the localizing of bendings in a fibre ring with good accuracy. It should also be noted that all the localization differences in both Table IV and Table V are within the spatial resolution of OTDR (30m).

TABLE V

COMPARISON OF THE BENDING LOCALIZATIONS (ZP) MEASURED BY OTDR AND THE PROPOSED TRA BASED APPROACH

	z_{p1} [km]	z_{p2} [km]	z_{p3} [km]	z_{p4} [km]	z_{p5} [km]
OTDR	0	1.726	26.44	51.12	56.03
1λ-BD-TRA	0.0016	1.736	26.422	51.123	56.017
Difference	1.6m	10m	18m	3m	13m

The summary of comparison on LR-PON localization functionality between OTDR and the TRA based technique is presented in Table VI. Apart from short measurement time, simple light source and low system complexity, the proposed solution could offer a large dynamic range and a high resolution simultaneously by using a high monitoring power, which are extremely difficult to be achieved in OTDR solution. It should be noted that the TRA based scheme has difficulty to handle multiple events occurring at the same time. However, the probability of such a situation is very low.

TABLE VI

COMPARISON BETWEEN OTDR AND THE PROPOSED TRA BASED MONITORING

	OTDR	The proposed TRA based monitoring solution
Measure time	2 minutes	3 seconds
Spatial resolution [m]	~30	break: 1(best)/60 (worst) [36] bending: 1(best)/20(worst)[35]
Light source	Modulated in time domain	Unmodulated CW
Dynamic range	<45dB	>60dB

4.2 Embedded OTDR (eOTDR) for LR-PONs

4.2.1 eOTDR in OLT

The embedded OTDR solution at the OLT side operates by on top modulation of the downstream signal by a dedicated OTDR pattern. The pattern could be a PRBS sequence or an orthogonal bit code. Previous deliverable D4.4 describes the e-OTDR solution in detail [37]. The applicability of the embedded OTDR for LR-PONs within an amplified feeder section was also shown. In the second half of the DISCUS project the method was stabilized. Other orthogonal bit codes were investigated and analyzed. The most promising approach was to apply Golay codes instead of a PRBS pattern. The Golay codes length had to be adjusted to the fibre link length. The algorithm for the code generation is very simple. In each iteration step the new Golay A sequence will be generated by concatenating the former A and B sequences. The Goly B sequence will be generated by concatenating the former A and $\underline{B}$ (inverse) sequences. The optical signal will be performed by laser on/laser off.

A=1, B=1

A=11, B=10

A=1110, B=1101

A=11101101, B= 11100010

…

For a 20km feeder link suitable Golay codes are 2048 bit long. The preferred duration for each bit is 100ns. The bit pattern for the feeder measurement from the OLT side is transmitted in a loop for up to 1million cycles. The high number of measurements is needed to average the OTDR signal and to suppress the noise. The measurement process was defined in a way that the first Golay code A was transmitted for 1 million averages and then the second Golay code B was transmitted afterwards. This was done for practical reason. Otherwise measurement time had to be wasted for loading the sequences alternately into the memory of the embedded OTDR transceiver. It is supposed that the block wise measurement routine has no negative impact to the result.

The following figures show the measurement results of a PRBS and a Golay code measurement. The measurement parameters were selected in that way that both methods can be compared by each other. After a detailed analysis of both methods we can conclude that the performance is the same for both bit patterns. It is recommended to stay with the PRBS pattern due to easier data processing.

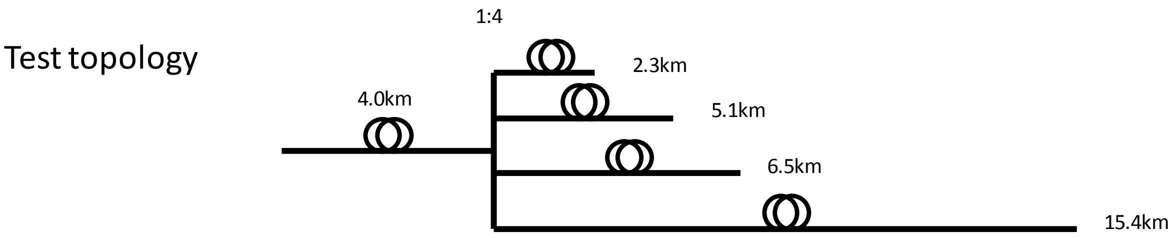


Fig. 23. Fibre topology for comparison measurement. The simple structure consists of a 4km long feeder section followed by a 1:4 splitter and 4 fibre branches with different length.

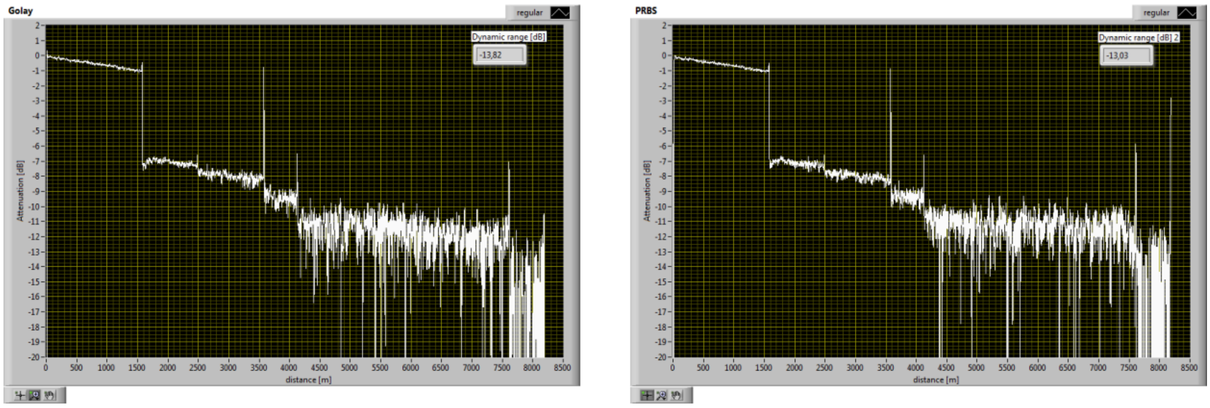


Fig. 24. OTDR measurement with different bit pattern. The left figure is based on Golay sequences and the right figure is based on a 2^11-1 PRBS signal.

The figure above and the former investigations demonstrate the strength of the embedded OTDR for monitoring the feeder section of the LR-PON. Feeder up to 80km can be measured very accurate in a timely manner. The measurement behind the splitter or within the drop section of the PON is often not possible due to the splitter attenuation. To overcome that problem it is proposed to measure from the ONU side, too. The main challenge for the measurement from the ONU side is the burst mode scheme in the upstream direction of PON networks. Because the length of the upstream burst varies during the operation it is not possible to modulate on top of the date. We cannot assume that the burst is long enough to carry the complete PRBS sequence. Therefore it is proposed to define dedicated measurement windows to perform the monitoring measurement. Within the measurement window a so called dummy burst has to be generated which fits to the length of the OTDR measurement sequence. The dedicated measurement window allows a 100% modulation of the dummy burst. No real data content will be disturbed by the 100% modulation. The number of averages can be reduced by a factor of 10 to get the same result compared to the feeder measurement from the OLT side. The operation of the proposed method could be demonstrated but the effort of this method has to be discussed. The main drawback of this solution is the high number of needed measurement windows for all branches of the network, because the measurement window can only be used for one ONU.

4.2.2 eOTDR in ONU

If the drop link is of interest only, all ONUs can perform the measurement at the same time. The measurement signals are only useable up to the splitter. The reflected OTDR signal after the splitter will interfere with the other OTDR signals from the other ONUs. A solution for a synchronized measurement is not known up to know. The second drawback of the upstream solution of the embedded OTDR is the cost. The cost at the ONU is related to one user only, whereas the downstream solution is shared over all users. The drop section is much shorter than the feeder section. Therefore the probability of a fibre issue is much higher in the feeder section than in a single drop section. The relevance of the availability of a monitoring tool is higher for the feeder section than for the drop section where only one user is affected. A further technical problem rises if the fibre is broken and the measurement signal has to be transferred back to the central office. An alternative reporting path has to be established. A radio link might be an option if the affected user can report some very simple information which allows the operator to indicate the problem. The following table summarizes the usability of the embedded OTDR solution for the two applications, the measurement from the OLT in downstream direction and from the ONU in upstream direction.

It is recommended to apply the embedded OTDR measurement from the OLT side and to check the applicability from the ONU side under economic aspects.

TABLE VII
Comparison between eOTDR Technique in OLT and ONU

Embedded OTDR solution		
location of embedded OTDR transceiver	**OLT**	**ONU**
measurement direction	downstream	upstream
network section	feeder	drop
use per fiber length	high	low
typical measurement time (10dB dynamic)	4min	10 min per ONU
spatial resolution	10m	10m
traffic impact	no (low)	yes (extra measurement windows)
benefit per user	high	low
cost per user	low	high
reporting path in case of fiber break	given	not given

4.3 Preventive colourless fibre supervision in WDM-PONs

T-OTDRs are a powerful tool for fault location in WDM-PONs with filtered ODNs. Nevertheless, the time required for measuring each fibre up to the customer end is around tenths of seconds, thus the monitoring of a complete WDM-PON may delay several minutes. As an example, it would take 16 minutes to characterize 32 fibres of a WDM-PON if each fibre measurement takes 30 seconds. As OTDRs are typically shared by a high number of PONs for cost efficiency reasons, the total preventive monitoring time is multiplied by the number of PONs. As a consequence, the detection of a fibre fault in a central office may delay several hours, too much in order to guarantee Service Level Agreements and avoid customer complaints, also increasing the time to repair of the fibre fault.

In this section, we analyse a preventive monitoring module to be used as a low cost support tool for periodically checking in a quick way the physical layer connectivity of WDM-PONs.

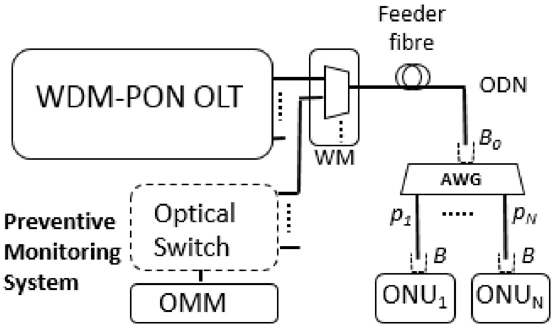


Fig. 25. Generic architecture of the proposed technique.

The preventive monitoring system consists of a centralized optical monitoring module (OMM), an optional optical switch to select the desired ODN to be tested, and an array of wavelength multiplexers (WM) that combines the data signals from each optical port of the WDM-PON OLT with the test signal of the OMM [38]. In the ODN, the technique adds a single reflector B_0 in the input of a cyclic Arrayed Waveguide Grating (AWG) mux/demux with N ports (p1…pN). Finally, at the end of each branch of the mux/demux (or optionally inside the remote devices/ONUs), a single colourless optical reflector B is used.

The monitoring technique can operate at the same time than data transmission within the same ODN. In the OMM, a reference optical signal (λ0) and a monitoring broadband light source (BLS) are delivered to the WR-ODN through the corresponding WM. Both reference and monitoring signals are comprised within free wavebands in the ODN not used for data transmission. The reference optical signal is reflected by reflector B0 at the input of the AWG and received back in the OMM. On the other hand, the monitoring broadband light source is filtered by the AWG, delivering a different monitoring signal (λm1-λmN) to the end of the corresponding AWG output port (p1…pN), where the monitoring signal is reflected by reflector B and received back in the OMM. At the same time, for each port of the AWG data signals are transmitted upstream and downstream using other cycles of the AWG in the C and L optical bands, thus each AWG port is simultaneously used for data transmission and monitoring.

For each remote device, the reflections of the reference signal (λ0) and the monitoring signal (λmi, i=1…N) are digitally processed in the OMM, and self-referenced measurement values are obtained. The measurement values obtained depend on the optical losses at the AWG for each port and the fibre attenuation between each AWG port and each colourless reflector (B) of the corresponding remote device.

This system can measure the attenuation of all the ouput fibres of the AWG in a few seconds, thus it can be used as a low cost support system for quick detection of physical layer faults in WDM-PONs.

In case of a physical layer fault detected by the preventive monitoring system, the T-OTDR measurement can be used in the specific wavelength in order to precisely locate the fibre fault, thus reducing the service interruption time, the time to repair and saving network operational costs by helping guarantee the Service Level Agreement.

5 Reliability, Optical Supervision and Management in LR-PONs: Conclusions

The inherent DISCUS approach for reliability and supervision includes backhaul fibre protection, OLT protection and eONUs in the amplified RNs. Embedded ONUs establish the communication channel for RN monitoring and management, and they can be used by the ODN management module for the intelligent splitter monitor as well as for the monitoring of the RN optical amplifiers.

The technologies and approaches analysed in the DISCUS project for advanced fibre access network reliability, supervision and management with a comparison between the main advantages and disadvantages are shown in the following table.

TABLE VIII
RELIABILITY, OPTICAL SUPERVISION AND MANAGEMENT TECHNOLOGIES

Technology	Pros	Cons
OLT eOTDR	• In-service supervision • Compact • Integrated data and supervision	• TRX cost increase • Low OTDR dynamic range
Transmission-Reflection Analysis	• Cost effective	• Not applicable for in-service monitoring • Requires fibre ring layout
Bidirectional Time of Flight Analysis*	• Allows E2E PON fibre supervision through amplifiers without ODN modification	• Precise ONU synchronization required • Complex trace analysis • Hybrid access required
Tunable OTDR* (WDM-PON)	• Allows E2E PON fibre supervision in WDM-PONs	
Colorless Preventive Monitoring (WDM-PON)	• Allows quick failure detection, complementing T-OTDR in WDM-PONs • Low cost	• Requires T-OTDR for fault location.
ONU eOTDR	• Allows PON fibres monitoring (incl. last drop fibres).	• TRX cost increase • Hybrid access required • Not applicable to backhaul fibres monitoring
Hybrid Access ONU	• Allows increase access reliability • Allows enhanced monitoring by ONU eOTDR	• Connection cost increase
Hybrid Fibre-Wireless Protection in Mobile Backhaul	• Allows increase mobile backhaul reliability • Cost effective	• Requires distribution fibre protection
Intelligent Splitter Monitor	• Allows automatic and reliable fibre management in the PONs • Allows new possibilities for PON operations (customer identification/detection, optical port monitoring…)	• Splitter cost increase • Requires ODN Management Module in the RN

	• Does not depend on local powering	

*** See Deliverable D4.4.**

A general picture showing the preferred solutions for DISCUS is shown in Fig. 26. The devices related to resiliency, management and monitoring are filled in grey color. It is assumed that the measurements from TRA, T-OTDR (plus preventive monitoring), and OLT eOTDR are communicated also with NMS/OSS through AN controllers. In-line communications to NMS/OSS are also assumed in OMM (through eONU) and HA-ONU wireless path.

TRA analysis, as described in D4.1, is the preferred solution for dark fibre monitoring, as a cost-effective alternative to traditional OTDRs. Intelligent splitters (shown in PONz) offer also the possibility of managing fibre connections in PON ODNs in a reliable way and help keeping clean the inventory database, but an ODN management module (OMM) is required in the LE site in order to remotely power up the intelligent splitter using light power. The OMM can communicate with AN controller via the embedded ONU. An embedded ONU is also used in any RN in order to manage and monitor the status of the optical amplifiers.

A hybrid access ONU (HA-ONU) is also shown in PONy, which has a protection wireless connection to a Base Station in PONx. The high reliability hybrid fibre/wireless protection proposal for mobile backhaul can be performed if the HA-ONU is used for mobile backhaul, see Fig. 1 in section 2.1.1. Embedded OTDR can be used by HA-ONU because the OTDR measurements can be communicated to NMS/OSS using the protection wireless connection in case of a fault in the fibre access.

Embedded OTDRs in OLTs can be a cost effective alternative to traditional external OTDRs located in the MC nodes, offering the advantage of integrating data and monitoring planes in a single element.

Finally, for WDM-PONs with wavelength filters in the ODN, Tunable OTDRs are considered as the most powerful monitoring approach, capable of identifying and locating a fibre fault from MC node up to customer premises in a simple way. An optional preventive monitoring system can be used by adding a preventive monitoring module in the MC node and colorless reflectors at ONU side for quick physical layer fault detection.

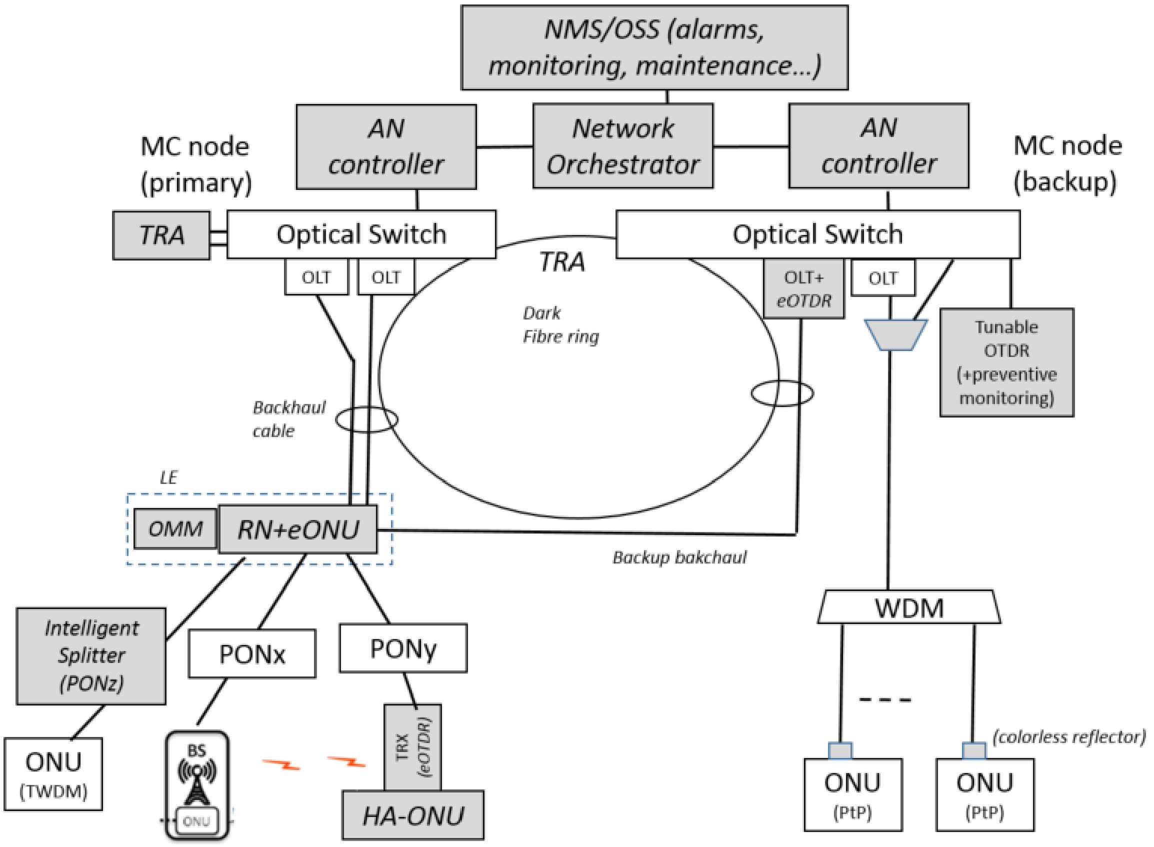


Fig. 26. Global scenario of optical supervision, management and reliability in DISCUS LR-PONs. TRA: Transmission-Reflection Analysis. LE: Local Exchange. RN: Remote Node. OMM: ODN Management Module. AN: Access Network. HA-ONU: Hybrid Access ONU. eONU: Embedded ONU. eOTDR: Embedded OTDR. WDM: Wavelength Division Mux/Demux.

6 References

[1] Qualcomm Incorporated (2013, June), “The 1000x data challenge,” available on http://www.qualcomm.com/1000x/.

[2] T. Naveh, “Mobile backhaul: fibre vs. microwave: Case study analyzing various backhaul technology strategies,” white paper, Ceragon Network Ltd., Oct. 2009.

[3] P. Monti, S. Tombaz, L. Wosinska, and J. Zander, “Mobile backhaul in heterogeneous network deployments: Technology options and power consumption,” in 14th International Conference on Transparent Optical Networks (ICTON), July 2012.

[4] D. Breuer, F. Geilhardt, R. Hülsermann, M. Kind, C. Lange, T. Monath, E. Weis, "Opportunities for next-generation optical access," IEEE Commun. Mag., vol.49, pp.s16-s24, Feb. 2011.

[5] D. P. Shea, and J. E. Mitchell, “Long-reach optical access technologies,” IEEE Network, vol. 21, no. 5, pp. 5-11, Sept. 2007.

[6] J. Chen, C. M. Machuca, L. Wosinska, and M. Jaeger, “Cost vs. Reliability Performance Study of Fibre Access Network Architectures”, IEEE Commun. Mag., vol. 48, No. 2, pp.56-65, Feb. 2010.

[7] Z. X. Wang, X. F. Sun, C. L. Lin, C. K. Chan, and L. K. Chen, “A novel centrally controlled protection scheme for traffic restoration in WDM passive optical networks,” IEEE Photon. Technol. Lett., vol. 17, no. 3, pp. 717–719, Mar. 2005.

[8] K. Lee, S. B. Lee, J. H. Lee, Y. G. Han, S. G. Mun, S. M. Lee, and C. H. Lee, “A self-restorable architecture for bidirectional wavelength-division-multiplexed passive optical network with colorless ONUs” Opt. Express vol. 15, no. 8, pp. 4863-4868, Apr. 2007.

[9] “Broadband optical access systems based on Passive Optical Networks (PON),” ITU-T Recommendation G983.1, 2005.

[10] J. Chen, L. Wosinska, M. N. Chughtai, and M. Forzati, “Scalable passive optical network architecture for reliable service delivery,” J. Opt. Commun. Netw., vol. 3, no. 9, pp. 667–673, Aug. 2011.

[11] H. Fan, J. Li, and X. Sun, “Cost-effective scalable and robust star-cross-bus PON architecture using a centrally controlled hybrid restoration mechanism,” J. Opt. Commun. Netw., vol. 5, no. 7, pp. 730–740, July 2013.

[12] M. Mahloo, A. Dixit, J. Chen, C. Carmen, M. Machuca, B. Lannoo, and L. Wosinska, “Towards reliable hybrid WDM/TDM passive optical networks,” IEEE Commun. Mag., vol. 52, no. 2, pp. S14-S23, Feb. 2014.

[13] A. Dixit, B. Lannoo, D. Colle, M. Pickavet, J. Chen and M. Mahloo, “Efficient protection schemes for hybrid WDM/TDM passive optical networks,” IEEE International Conference on Communications (ICC), Workshop on New Trends in Optical Networks Survivability, June 2012.

[14] S. Sarkar, H.-H. Yen, S. Dixit, and B. Mukherjee, “RADAR: risk-and-delay aware routing algorithm in a hybrid wireless-optical broadband access network (WOBAN),” in Optical Fibre Communication Conf. and the Nat. Fibre Optc Engineers Conf. (OFC/NFOEC), 2007, OThM4.

[15] T. Feng, and L. Ruan, “Design of a survivable hybrid wireless-optical broadband access network,” J. Opt. Commun. Netw., vol. 3, no. 5, pp. 458–464, May 2011.

[16] K. Iwatsuki, and J.-i. Kani, "Applications and Technical Issues of Wavelength-Division Multiplexing Passive Optical Networks With Colorless Optical Network Units," J. Opt. Commun. Netw, vol.1, no.4, pp.C17-C24, Sep. 2009.

[17] M. Mahloo, P. Monti, J. Chen, L. Wosinska, "Cost Modeling of Backhaul for Mobile Networks," in Proc. of IEEE International Conference on Communications (ICC), Jun., 2014.

[18] J. Chen, "Efficient Resiliency Mechanisms for Next Generation Passive Optical Networks", in the 9th International Conference on Information, Communications and Signal Processing (ICICS), Dec. 2013.

[19] Y, Yang, K. W. Sung, L. Wosinska and J. Chen, "Hybrid Fibre and Microwave Protection for Mobile Backhauling", IEEE/OSA Journal of Optical Communications and Networking, vol. 6, no. 10, pp.869-878, Oct. 2014 .

[20] Hybrid Access for Broadband Networks, WT 348, Broadband Forum, work in progress, 2015.

[21] S. McGettrick, L. Guan, A. Hill, D.B. Payne, M. Ruffini, Ultra-fast 1+1 Protection in 10 Gb/s Symmetric Long Reach PON. ECOC 2013.

[22] F. Slyne, N. Kituswan, S. McGettrick, D.B. Payne and Marco Ruffini. Design and experimental test of 1:1 End-to-End Protection for LR-PON using an SDN multi-tier Control Plane. Paper Mo.3.2.4, ECOC 2014.

[23] S. McGettrick, F. Slyne, N. Kitsuwan, D.B. Payne, M. Ruffini. Experimental End-to-End Demonstration of Shared N:1 Dual Homed Protection in Long Reach PON and SDN-Controlled Core. To appear in OFC 2015.

[24] ITU-T L.64: ID tag requirements for infrastructure and network elements management, Oct. 2012.

[25] BBF TR-311: Fibre infrastructure management system: Architecture and Requirements. Feb 2015

[26] H. Song, et al.: Long-Reach Optical Access Networks: A Survey of Research Challenges, Demonstrations, and Bandwidth Assignment Mechanisms, IEEE Commun. Surv. Tutor., vol. 12, pp. 112-123, 2010.

[27] J. Chen, et al.: cost-effective fault supervision schemes for next generation optical access networks, in Proc. ACP 2014, Shanghai, China, November 2014, paper ATh1H.4.

[28] E. Wong: Next-Generation Broadband Access Networks and Technologies, J. Lightwave Technol. Vol. 30, pp. 597-608, 2012.

[29] K. Fouli, et al.: Time-, wavelength-, and code-domain optical reflection monitoring for next-generation access-metro networks, Comput. Commun., vol. 8, pp. 1011-1021, June 2011.

[30] M. A. Esmail and H. Fathallah: Long-reach PON management and protection system based on optical coding," in Proc. SIECPC 2011, Riyadh, Saudi Arabia, April 2011, pp. 1-4.

[31] M. Cen, et al: Advanced Transmission-Reflection-Analysis (TRA) System for Long-Reach Passive Optical Network Monitoring, ICTON, July 2015.

[32] V V. Spirin, et al: Localization of a Loss-Inducing Perturbation With Variable Accuracy Along a Test Fibre Using Transmission-Reflection Analysis, IEEE PHOTONIC TECH. L., Vol. 16, pp.569-571, 2004.

[33] M. Cen, et al.: Multi-wavelength transmission-reflection analysis for fibre monitoring, Opt. Express, vol. 22, pp. 31248-31262, 2014.

[34] M. Cen, et al.: Localization and quantification of reflective events along an optical fibre using a bi-directional TRA technique, Opt. Express, vol. 22, pp. 9839-9853, 2014.

[35] M. Cen, et al. : Fast and Simple Fault Monitoring for Long-reach Passive Optical Networks, in Proc. ECOC 2014, Cannes, France, September 2014, paper P.7.15

[36] M. Cen, et al.: Efficient Monitoring for Ring-based Long-Reach Passive Optical Networks, in Proc. OFC 2015, Los Angeles, USA, March 2015, paper Th4H.4

[37] DISCUS deliverable 4.4 Optical layer supervision tools and processes for long reach optical access, May 2015

[38] C. Vázquez et al., ”Método y sistema para la monitorización de redes de fibras ópticas”, ES, Patent application nº P201530018, (2015).

[39] M. Ruffini, D. Mehta, B. O’Sullivan, L. Quesada, L. Doyle, D. B. Payne. Deployment Strategies for Protected Long-Reach PON. IEEE/OSA Journal of Optical Communications and Networking, vol. 4, Issue 2, p118 – 129, Jan 2012.

[40] A. Nag, D. B. Payne, M. Ruffini, N:1 Protection Design for Minimising OLTs in Resilient Dual-Homed Long-Reach Passive Optical Network. Paper Tu2F.7, OFC 2014.

[41] M. Ruffini, D. Payne, L. Doyle. Protection Strategies for Long-Reach PON. ECOC 2010.

Abbreviations

AWG	Arrayed Waveguide Grating
BS	Base Station
DF	Distribution Fibre
eOTDR	Embedded OTDR
FF	Feeder Fibre
FIF	Failure Impact Factor
FPGA	
FPR	Failure Penetration Ratio
FSR	Free Spectral Range
HA	Hybrid Access
ISM	Intelligent Splitter Monitor
LR-PON	Long Reach Passive Optical Network
NMS	Network Management System
OAMP	Operation Administration Maintenance and Provisioning
OCF	OFELIA Control Framework
ODN	Optical Distribution Network
OLT	Optical Line Termination
OMM	ODN Management Module
ONA	Optical Network Architecture
ONU	Optical Network Unit
OTDR	Optical Time Domain Reflectometer
OSS	Operations and Support Systems
PDA	Personal Digital Assistant
PON	Passive Optical Network
PRBS	Pseudo Random Bit Sequence
RE	Reach Extender
SDN	Software Defined Networking
SLA	Service Level Agreement
SLD	SuperLuminiscent Diode
SP	Splitting Point
TRA	Transmission Reflection Analysis

TWDM	Time and Wavelength Division Multiplexing
VPN	Virtual Private Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WM	Wavelength Multiplexer
WP	Working Path

Version	Date submitted	Comments
V1.0	30/06/2015	First version sent to the EU.
V1.1	01/07/2015	Slightly edited second version sent to the EU