Optical Fiber Technology 26 (2015) 82–93

Contents lists available at ScienceDirect

Optical Fiber Technology

www.elsevier.com/locate/yofte

Invited Papers

Assessment methodology of protection schemes for next generation optical access networks

Carmen Mas Machuca [a], Lena Wosinska [b,*], Jiajia Chen [b]

[a] Technische Universität München (TUM), Chair of Communication Networks, 80333 Munich, Germany
[b] KTH Royal Institute of Technology, School of ICT, 16440 Kista, Sweden

ARTICLE INFO

Article history:
Available online 12 August 2015

Keywords:
Protection
Optical access networks
Reliability
Cost
Power consumption

ABSTRACT

Optical access networks are evolving towards next generation solutions offering much higher bandwidth per end point. Moreover, the uninterrupted access to the network services is becoming crucial and therefore operators are now considering protecting their access networks. However, the cost factor is still very important due to the relatively low cost sharing in access segment. For this purpose, this paper proposes an assessment methodology that can be used to compare different protection schemes and help to identify the suitable solution for a given scenario. The assessment criteria includes some reliability measures such as Failure Impact Factor (FIF) and connection availability, as well as cost parameters such as the investment required in greenfield and brownfield scenarios and the increase in power consumption compared to the unprotected network. The proposed criteria have been used to compare 7 representative protection schemes shown in literature, which differ mainly in the number of protected network elements and the technology used for protection (fiber, wireless, etc.). The considered protection schemes have been applied to a hybrid wavelength division multiplexing/time division multiplexing Passive Optical Network (Hybrid PON) architecture in an urban area. It has been shown that it is difficult to identify the absolute best scheme with respect to all the considered criteria. However, depending on the requirements from the operator regarding the targeted reliability performance in the network, an appropriate protection scheme can be recommended for either a greenfield or a brownfield scenario.

1. Introduction

The continuous increase of bandwidth required by users is challenging access network operators to provide a sustained bitrate of 300 Mbps per user in 2020 [1]. In order to cope with this problem operators having copper based access networks can increase the capacity of the existing copper infrastructure with new technologies (e.g., G. FAST) To the best of our knowledge, no protection schemes have been implemented in the copper based access networks due to the low capacity, short distances and, consequently, low impact of failures, which do not motivate additional investments to provide protection. However, upgrading the existing copper infrastructure can only be a short term solution. The future proof alternative for operators is to migrate the legacy networks to optical access networks. In some dense urban areas, operators have already deployed optical access networks, mainly Ethernet Passive Optical Networks (EPONs) or Gigabit Passive Optical Networks (GPONs), where 1 or 2.5 Gbps is shared by several tens of users utilizing Time Division Multiplex (TDM). To further increase the access network capacity per user, operators can either decrease the sharing factor or migrate to a new technology, e.g., Next Generation PON2 (NGPON2).

Fig. 1 illustrates the basic PON architecture that consists of an Optical Line Terminal (OLT) located at the Central Office (CO), which is interconnected to several Optical Network Units (ONUs) at the end point of the access network through a splitting point, denoted as Remote Node (RN).

One CO may accommodate several OLTs and one OLT may include multiple PON Line Terminal (PON LT) cards, (i.e. optical interfaces for sending/receiving optical signals. OLTs can also host some other components (e.g., Optical Switch (OS) for protection purpose, which is described in the later sections). Similarly, ONU includes at least one PON Network Termination (NT) to receive/-transmit optical signals and possibly some other components for resiliency purpose. The optical fiber interconnecting the OLT and RN is referred as Feeder Fiber (FF), whereas the one connecting the RN with each ONU is referred as Distribution Fiber (DF). In general, PON architectures can include several splitting stages (see

* Corresponding author.
E-mail addresses: cmas@tum.de (C. Mas Machuca), wosinska@kth.se (L. Wosinska), jiajiac@kth.se (J. Chen).

http://dx.doi.org/10.1016/j.yofte.2015.07.014
1068-5200/

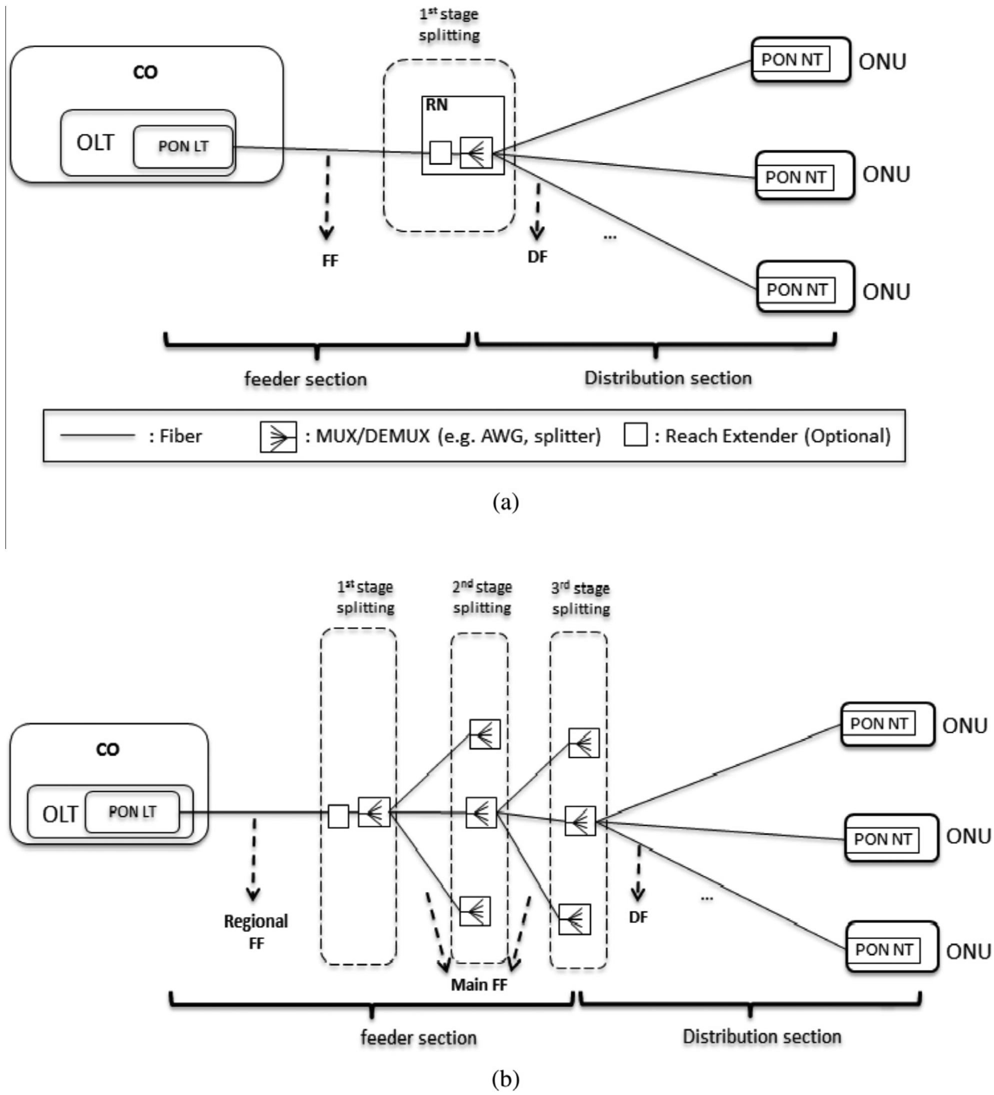

Fig. 1. Basic PON architecture without any protection (a) with single stage of splitting and (b) with multiple stages of splitting (PON LT/NT: Passive Optical Network Line Terminal/Network Termination; OLT: Optical Line Terminal; ONU: Optical Network Unit; CO: Central Office; RN: Remote Node).

Fig. 1(b)), which can increase the flexibility in the fiber plant design to aggregate ONUs (i.e. different splitting stages at the optical distribution network as, e.g., in a GPON 1:32 with two splitting stages of 1:8 and 1:4 respectively). However, these splitting stages can also be related to node consolidation, where several central offices are aggregated into one (so-called main CO), so that the equipment at the remaining central offices can be replaced by a splitting device. In this case, FF can be divided as Main FF (MFF) between different stages of the RNs and Regional FF (RFF) between the OLT at the main CO and the 1st splitting stage.

Thanks to the recent advances in optical technology, a single PON (e.g. NGPON2) can be used to interconnect different types of end points (ONUs), e.g., residential users, base stations, microcells, business users, etc. Consequently, the reliability performance of future access networks needs to be sufficiently high in order to avoid service interruption for a big number of users. Moreover, the required connection availability may vary among the different types of end users. So far, operators were not interested to invest in protection of access networks due to the high investment and low sharing factor. However, resilience in access network is becoming a critical issue because of the increase of number of users served in a single access network area as well as growing importance of uninterrupted access to the network services.

It is shown that fiber access networks without any protection are characterized by poor reliability performance [2]. This fact has been realized already in late 90's and the standard PON protection architectures have been defined by ITU-T [3] around two decades ago. These standard PON protection schemes are referred to as Type A, B, C and D. In Type A only the FF is redundant. Type B protection duplicates the shared part of the PON, i.e., FF and optical interfaces (i.e., PON LT) at the OLT. In Type B the primary optical interface at OLT is normally working while the second one is used as a cold standby. Type C represents 1+1 dedicated end-to-end path protection with full duplication of the PON resources. In Type C both the primary and secondary interfaces are normally working (hot standby), which allows very fast recovery time. Type D protection specifies the independent duplication of FF and DFs and thus, it enables network provider to offer differentiated reliability level for the users. It is obvious that adding redundant components and systems can improve network reliability performance, but it may not be a practical solution for the cost sensitive access networks. Therefore, both system deployment cost (related to CAPital