Universidade de Aveiro
2020

Departamento de Eletrónica,
Telecomunicações e Informática

Patrícia Isabel Almeida Campino Martins do Vale

Evolutionary Optical Framework - NG-PON2: Controlo e sincronização de ONUs via ICTP (Inter-Channel-Termination Protocol)

Evolutionary Optical Framework - NG-PON2: Control and synchronization of ONUs via ICTP (Inter-Channel-Termination Protocol)

Universidade de Aveiro
2020

Departamento de Eletrónica,
Telecomunicações e Informática

Patrícia Isabel Almeida Campino Martins do Vale

Evolutionary Optical Framework - NG-PON2: Controlo e sincronização de ONUs via ICTP (Inter-Channel-Termination Protocol)

Evolutionary Optical Framework - NG-PON2: Control and synchronization of ONUs via ICTP (Inter-Channel-Termination Protocol)

Universidade de Aveiro Departamento de Eletrónica,
2020 Telecomunicações e Informática

Patrícia Isabel Almeida Campino Martins do Vale

Evolutionary Optical Framework - NG-PON2: Controlo e sincronização de ONUs via ICTP (Inter-Channel-Termination Protocol)

Evolutionary Optical Framework - NG-PON2: Control and synchronization of ONUs via ICTP (Inter-Channel-Termination Protocol)

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Computadores e Telemática, realizada sob a orientação científica do Professor Doutor Valter Filipe Miranda Castelão da Silva, Professor Adjunto da Escola Superior de Tecnologia e Gestão de Águeda da Universidade de Aveiro, e Professor Doutor Paulo Jorge de Campos Bartolomeu, Investigador Doutorado do Departamento de Eletrónica, Telecomunicações e Informática

o júri / the jury

presidente / president	Professor Doutor Arnaldo Silva Rodrigues de Oliveira, Professor Auxiliar, Universidade de Aveiro
vogais / examiners committee	Professor Doutor Frederico Miguel do Céu Marques dos Santos, Professor Adjunto, Instituto Superior de Engenharia de Coimbra
	Professor Doutor Valter Filipe Miranda Castelão da Silva, Professor Adjunto, Universidade de Aveiro

agradecimentos / acknowledgements

Gostaria de agradecer à Fundação para a Ciência e a Tecnologia e à InovaRia, que me deram a oportunidade de realizar esta dissertação com contexto empresarial. Gostaria também de agradecer à Altice Labs, que me recebeu e forneceu todas as condições e equipamentos necessários à exploração do trabalho. Um agradecimento aos meus orientadores Professor Valter, Professor Paulo e Licínio, que estiveram sempre disponíveis para me ajudar e mostraram interesse, e ainda à equipa da Altice Labs que me integrou e esclareceu dúvidas. Por último, um grande agradecimento aos meus pais, irmãs, amigos e ao meu namorado por todo o apoio.

palavras-chave

PON, Redes Óticas Passivas, GPON, Gigabit PON, NG-PON2, PON de Próxima Geração, Protocolo Inter-Channel-Termination, ICTP.

resumo

O estudo de novas tecnologias com potencial para suportar taxas de transferência elevadas é importante para dar resposta à constante evolução do consumo de informação da Internet. As Redes Óticas Passivas de Próxima Geração (NG-PON) vêm tentar ultrapassar este obstáculo. A mais recente, NG-PON2, utiliza vários canais na mesma fibra para transmitir e receber dados, aumentando consideravelmente a largura de banda de uma única fibra. Esta nova forma de comunicação veio a introduzir um novo problema: a troca de informação entre estes canais com o mínimo de distúrbios na rede. O Protocolo Inter-Channel-Termination (ICTP) foi apresentado para certificar que esta comunicação é feita corretamente num ambiente de vários operadores.
Baseado num ambiente pré-construído com o uso simultâneo das tecnologias Gigabit PON (GPON) e NG-PON2, foi desenvolvido um sistema com características semelhantes às de um cenário real. Neste sistema, foram implementados dois casos de uso do ICTP e, para cada um, testaram-se dois eventos. Os resultados obtidos mostraram a possibilidade de serem usados num cenário real, sem falhas e com atrasos reduzidos.

keywords

PON, Passive Optical Networks, GPON, Gigabit PON, NG-PON2, Next Generation PON, Inter-Channel-Termination Protocol, ICTP.

abstract

The study of new technologies with the potential to support high transfer rates is important to respond to the constant evolution of Internet information consumption. The Next-Generation Passive Optical Networks (NG-PON) tries to overcome this obstacle. The most recent one, NG-PON2, uses several channels in the same fiber to transmit and receive data, considerably increasing the bandwidth of a single fiber. This new form of communication has introduced a new problem, the exchange of information between these channels with a minimum of disturbances on the network. The Inter-Channel-Termination Protocol (ICTP) was presented to certify that this communication is done correctly in a multi-operator environment.

Based on a pre-built environment with the cooperative use of Gigabit PON (GPON) and NG-PON2 technologies, a system with similar characteristics to those of a real scenario was developed. In this system, two ICTP use cases were implemented and, for each one, two events were tested. The results obtained showed the possibility of being used in a real scenario, without failures and with small delays.

Contents

List of Figures

List of Tables

Acronyms

10G-EPON	10-Gigabit Ethernet Passive Optical Network
APON	Asynchronous Transfer Mode Passive Optical Network
ATM	Asynchronous Transfer Mode
AWG	Arrayed Waveguide Granting
BPON	Broadband Passive Optical Network
BWmap	Bandwidth Map
CO	Central Office
CRC	Cyclic Redundancy Check
CT	Channel Termination
DBA	Dynamic Bandwidth Allocation
DSL	Digital Subscriber Line
EPON	Ethernet Passive Optical Network
EqD	Equalization Delay

FSAN	Full Service Access Network
FTTB	Fiber-to-the-Building
FTTC	Fiber-to-the-Curb
FTTH	Fiber-to-the-Home
FTTx	Fiber-to-the-x, in reference to FTTH, FTTC, FTTB, …
Gb/s	Gigabit per second
GEM	GPON Encapsulating Method
G-EPON	Gigabit Ethernet Passive Optical Network
GPON	Gigabit Passive Optical Network
ICTP	Inter-Channel-Termination Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
ILODS	Intermittent Loss of Downstream Synchronization
IP	Internet Protocol
IPFIX	IP Flow Information Export
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
LOB	Loss of Burst

Mb/s	Megabit per second
Ms	Milliseconds
MUX	Multiplexer
NE	Network Element
NG-PON	Next-Generation Passive Optical Network
ODN	Optical Distribution Network
OLT	Optical Line Terminal
ONT	Optical Network Terminal
ONU	Optical Network Unit
PB	Petabyte (10^{15} bytes)
PHY	Physical Layer
PLOAM	Physical Layer Operation Administration and Maintenance
PON	Passive Optical Network
PtP WDM	Point-to-Point Wavelength Division Multiplexing
QoS	Quality of Service
SN	Serial Number

TC Layer	Transmission Convergence Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TLV	Type Length Value
TWDM	Time and Wavelength Division Multiplexing
VPN	Virtual Private Network
VSSN	Vendor-Specific Serial Number
WDM	Wavelength Division Multiplexing
WL	Wavelength
WM	Wavelength Multiplexer
WMM	Wavelength Mobility Manager
XG-PON	10-Gigabit Passive Optical Network
XGS-PON	10-Gigabit Symmetrical Passive Optical Network

1 Introduction

1.1 Context and Motivation

Internet use has been exponentially growing since the release of the World Wide Web to the public in 1993 [1], having reached the first billion users by 2005 [2]. Currently, it has already achieved the 4.5 billion mark [2], which is almost 60% of the current world population [3]. Not only the number of users is constantly increasing, but also the amount of time spent on the Web [4], as well as the data size exchanged in each month [5].

Year	Number of users ($x10^9$)	Time spent (hours/day)	Data size (PB/month)
1995	0.045	-	0.180
2000	0.415	-	84
2005	1.030	-	2 426
2010	2.023	3.2	20 151
2015	3.186	5.4	72 521

Table 1.1: Internet users, time spent, and data size exchanged by year

Due to this consistent growth in traffic, a greater, faster, and more reliable Internet access has become a must. This is attainable by Passive Optical Networks (PON), which have been quickly progressing throughout the years.

Nevertheless, current technologies will eventually stop satisfying the current bandwidth needs, so the study of Next-Generation PON will be essential for the future. The Next--Generation Passive Optical Network 2 (NG-PON2) standard is an attempt to fulfill the need of higher data rates in a long-term perspective, due to its ability to expand and to support higher bandwidth per customer, more customers per feeder fiber, extended passive reach, low economical investment (since all the previously installed infrastructure can be reused), low energy consumption, and co-existence with previous Gigabit Passive Optical Network (GPON) standards [6].

An important aspect of NG-PON2 that differs from previous standards is the ability to have multiple bi-directional channels to transmit and receive data, that can be configured with various data rates to suit any need. This is an important aspect of the expandability of NG-PON2 since there can be an incrementing number of channels and data rates. Since this concept of different channels is fairly recent, there are new requirements to comply with how these work overall.

This work focuses on one important part of these new requirements: the communication between the NG-PON2 channels. This communication has been studied before, in 2017, by The Broadband Forum, which developed a guideline for a protocol that could do just that. This protocol is the Inter-Channel-Termination Protocol (ICTP) and is specified in their technical report - TR-352.

1.2 Objectives

Based on a pre-built system that supports previous PON standards and NG-PON2, the Optical Network Units (ONU) must be capable of registering in any channel and, if required, change channels, while staying in service and ensuring that there is a minimal break of that service during the process. All of the Optical Line Terminal (OLT) Channel Terminations (CT) may or may not be on the same card of the system, or even the same system, and need to be coordinated while sharing information between each other, using ICTP.

This dissertation serves the purpose of:

- Studying the different PON standards up to this date;
- Studying the ICTP protocol in an NG-PON2 scenario;
- Studying the current hardware and software developed in the pre-built system;
- Exploring a solution to integrate into the current OLT architecture;
- Developing and deploying the solution into the existing software;
- Developing and running tests to validate the implemented use cases.

1.3 Structure

The work of this dissertation is organized into five different chapters.

This first chapter introduces the context, objectives, and overall structure of the dissertation, as well as some related work. In the second chapter, a brief introduction to PON architectures and the evolution of its standards is made, highlighting their main differences and progress. Later, in the same chapter, the technology NG-PON2 is thoroughly described, along with its protocol, ICTP.

The third chapter describes the development of the implementation of the use cases, presenting each proceeding and choice made throughout this stage. The fourth chapter extensively describes the deployed test bed, along with the tests performed on the use cases and their results.

Finally, the last chapter addresses the conclusions and results from the case study, which answers the problems set in the first chapter and meets the goals set. Lastly, it is made a brief reflection on the completed work and possible future development.

2 State of the Art

This chapter briefly introduces the main elements necessary for the understanding of the succeeding topics. Initially, a first look of the overall evolution of Passive Optical Networks (PON) will be presented, highlighting some of the main characteristics of each standard, followed by the thorough description of the last PON standard available to date and its Inter-Channel-Termination Protocol (ICTP), which will be the main focus of this work.

2.1 The evolution of Passive Optical Networks

A PON is a fiber optic communication that passively delivers broadband networks, meaning that no module requires a power supply from the Central Office (CO) to the user [7].

Since the introduction of PONs in the late 1980s [8], they are now the solution to the increase in customer bandwidth demands, at a reduced operational cost [9]. Given that this need is continuously expanding, the evolution of PONs is indispensable.

Over the years, several PON technologies have been developed that offer different characteristics and architectures, which are going to be explored in the following sections.

2.1.1 Passive Optical Networks

PON features a *point-to-multipoint* topology, allowing only one Central Office to distribute the signal to multiple end-users [7, 10], unlike other renowned network technologies, like the Digital Subscriber Line (DSL), which follows a *point-to-point* architecture [11]. The next subsections will describe the different types of architectures a PON standard might have.

General architecture

The three main components in PON architectures are the Optical Line Terminal (OLT), the Optical Distribution Network (ODN), and the Optical Network Unit (ONU). These elements can be seen below in Figure 2.1. An OLT, which is located in a Central Office (CO), is connected through an optical fiber to one or more 1:N optical splitters. The OLT is used to control the data flow across the ODN, upstream and downstream, and provide services to the subscribed users. Each distributed fiber forwards these services towards an ONU, where the signal is further dispersed to all subscribers attached to this ONU. Initially, the downstream services were mostly videos, so the upstream channels were usually of lower data rates. Lately, with the surge of cloud services, gaming, and streaming, the upstream bandwidth is more requested, and newer technologies have a symmetric relationship between download and upload. An ONU can also be called an Optical Network Terminal (ONT), if it is located inside the client's premises [7, 9, 12, 13, 14].

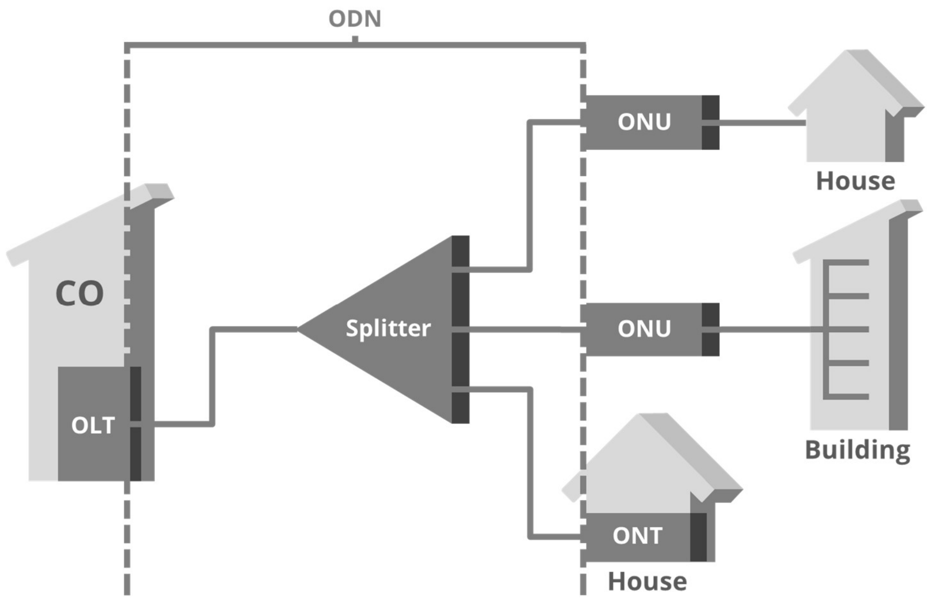


Figure 2.1: Basic Passive Optical Network architecture with each component

Fiber-to-the-x architectures

PON allows broadband connectivity to be made directly to or just outside of houses, buildings, or offices, which is called Fiber-to-the-x (FTTx), where the *x* can be replaced depending on how close the fiber is distributed to the user [9, 15]. The most common varieties, which are depicted in Figure 2.2, are:

- Fiber-to-the-Curb (FTTC): the fiber cable is installed up to a switch located within 300 meters of the property, from which a coper cable is used to connect to one or more customers. In Figure 2.2, this is the top case, where the line that has a darker color represents the fiber that attaches the CO to the switch, while the lighter colored line symbolizes the copper cable used to connect the switch to the client's structure.
- Fiber-to-the-Home (FTTH): deployment of the fiber directly to the home of a client. In this case, an ONT is commonly used. In Figure 2.2, FTTH is the middle case, where the fiber connects directly to the client's structure.
- Fiber-to-the-Building (FTTB): the fiber reaches the boundary of a building, where the connection to the individual customers within the same building is made similar to FTTC. What differs this from FTTC is that, in this case, a switch is not used, and the end-users are within the same building. This is shown at the bottom of Figure 2.2, where the fiber is connecting the CO to the boundary of a building, as seen by the darker colored line, which is then dispersed throughout the building usually with a copper cable, depicted in Figure 2.2 with a lighter colored line.

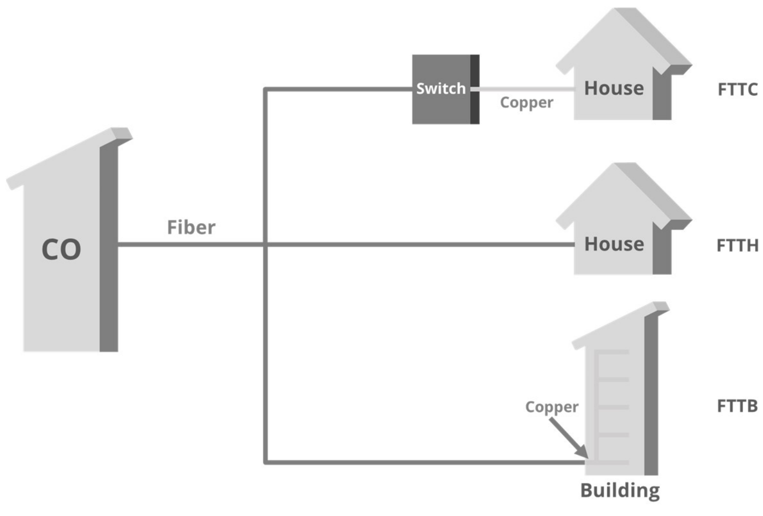


Figure 2.2: Most common FTTx scenarios

Multiplexing architecture

There are two main multiplexing architectures used by PON standards: Time Division Multiplexed PON (TDM-PON) and Wavelength Division Multiplexed PON (WDM-PON).

In a TDM-PON implementation, where a single channel is shared between users [16], an OLT is connected to different ONUs through one or more optical splitter. This is exemplified in Figure 2.3. In the downstream direction (left to right according to the figure), all the packets that originate from the OLT are broadcasted by the splitter and sent to every ONU, which recognizes their packets through address labels contained in the headers. In the upstream direction (right to left according to the figure), the signals from each ONU are multiplexed according to the time sent and forwarded to the OLT [17].

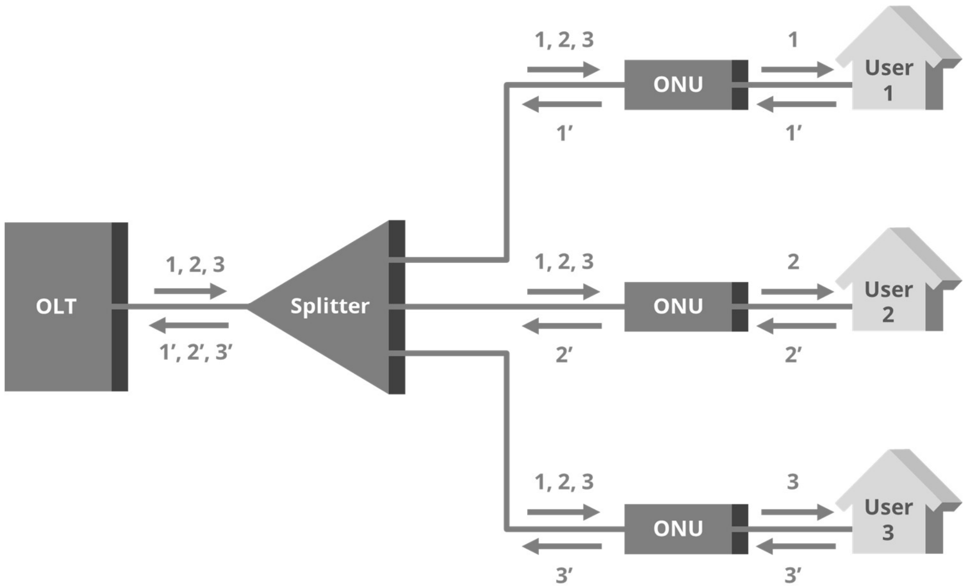


Figure 2.3: Typical TDM-PON architecture

Figure 2.4 portrays a WDM-PON architecture, which splits channels into wavelengths using a passive wavelength multiplexer/demultiplexer and a wavelength router that replaces the optical splitter in a traditional architecture. This router, usually implemented using an Arrayed Waveguide Grating (AWG), allows each OLT-ONU pair to be assigned with a dedicated wavelength, bringing more privacy and security than the TDM-PON architecture [17, 18]. This architecture has multiple challenges like the elevated cost of the initial set-up and of its components. On account of this, this implementation is not usually used by itself among Internet Service Providers (ISP) or vendors.

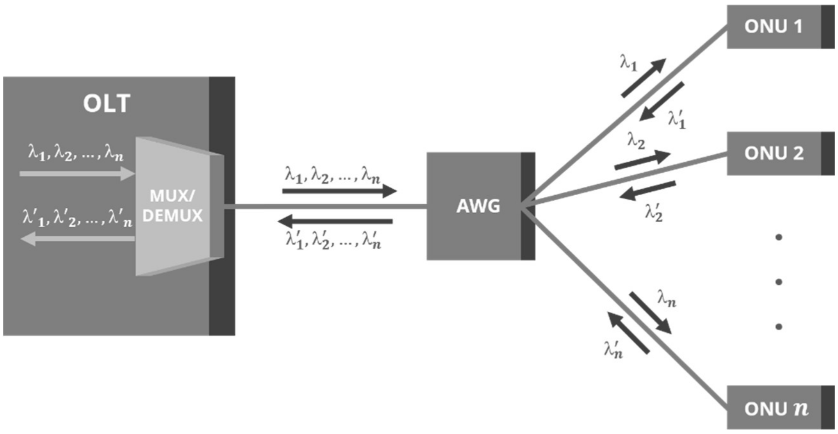


Figure 2.4: Typical WDM-PON architecture

More recent PON standards use a hybrid form of these two architectures, which is the Time and Wavelength Division Multiplexed PON (TWDM-PON), show below in Figure 2.5. The Wavelength Division Multiplexing is used to aggregate multiple flows through four pairs of wavelengths, and the AWG is replaced by a splitter that distributes the signal. This replacement increases how passive the network is and reduces the cost of deployment. The ONUs are equipped with tunable transmitters and receivers, which are tunable to any of the four upstream or downstream wavelengths, respectively. Optionally, more pairs of wavelengths and different rates can be added [19].

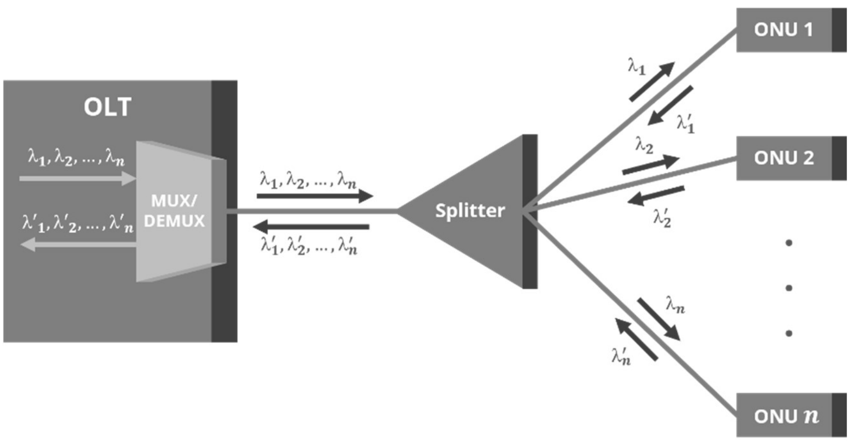


Figure 2.5: Typical TWDM-PON architecture

Protection architecture

Despite optional, the protection architecture assures the reliability of the access network. A protection switching can be triggered automatically, which occurs by fault detection (*i.e.* losing signals, frames, and other errors), or by force, which is activated by administrative events, such as fiber rerouting or replacement.

The following Figure 2.6 shows the duplex system model for the access network, where the protection of the ODN between the OLT and the ONU is depicted [20].

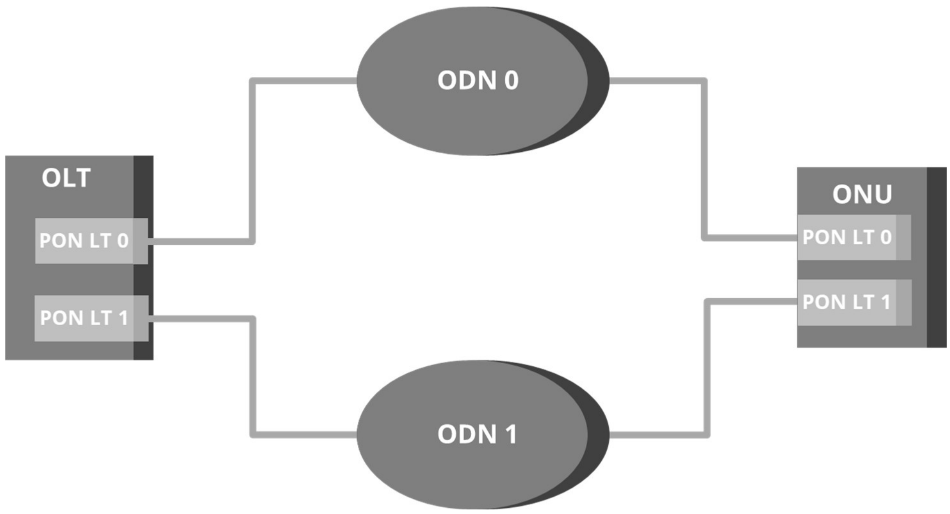


Figure 2.6: Duplex system model

As of a more recent standard, Gigabit PON (GPON), there is a second system model for a dual-parented access network, as seen in Figure 2.7. The only difference between this model and the one shown previously in Figure 2.6 is that there are two OLTs (parents) instead of one, being relevant the protection between the ODN interface in the ONU and each OLT [21].

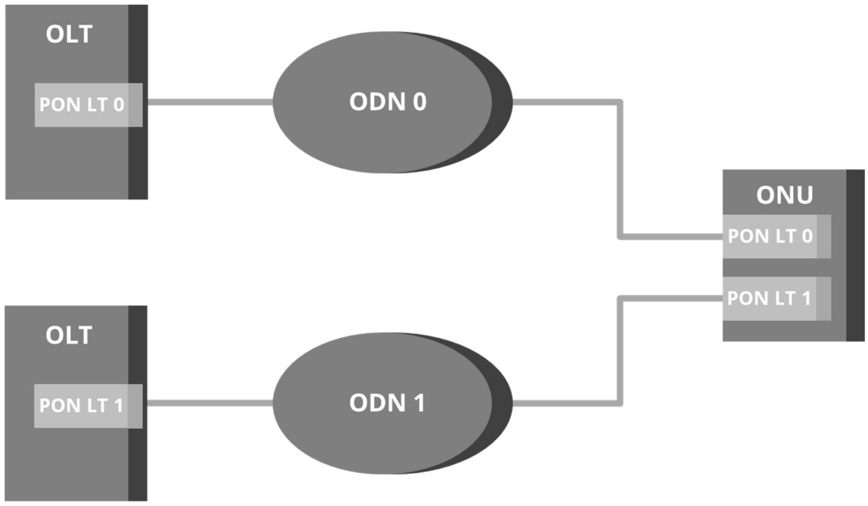


Figure 2.7: Dual-parented duplex system model

Depending on the changes made to the architecture, there are in total four types of protections, designated:

- Type A – only duplicates the optical fibers. This configuration is deprecated since GPON;
- Type B – doubles the OLTs and the optical fibers between them and the optical splitter, which has two input/output ports on the OLT side. This reduces the cost of duplexing the ONUs and only the OLT side can be recovered in case of failure. This system is portrayed below in Figure 2.8;

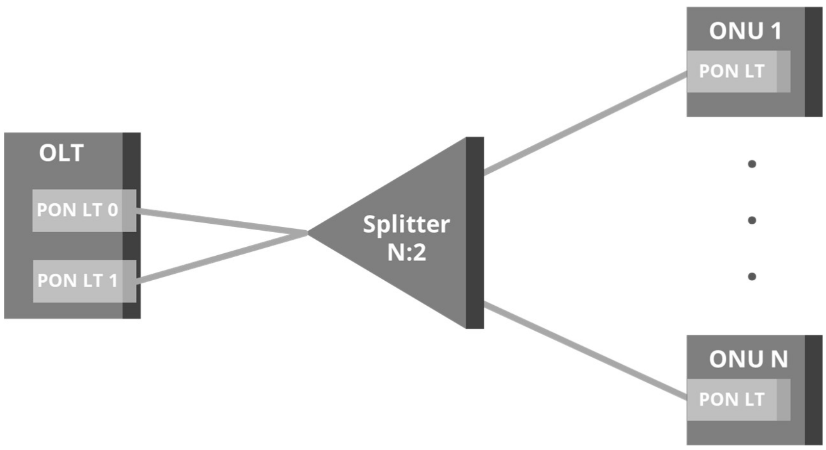


Figure 2.8: Duplex system: OLT-only duplex system

- Type C – doubles not only the OLT side facilities but also the ONU side. In this configuration, recovery from failure at any point is possible by switching to the other elements. Therefore, the full-duplex enables high reliability, but is more expensive;

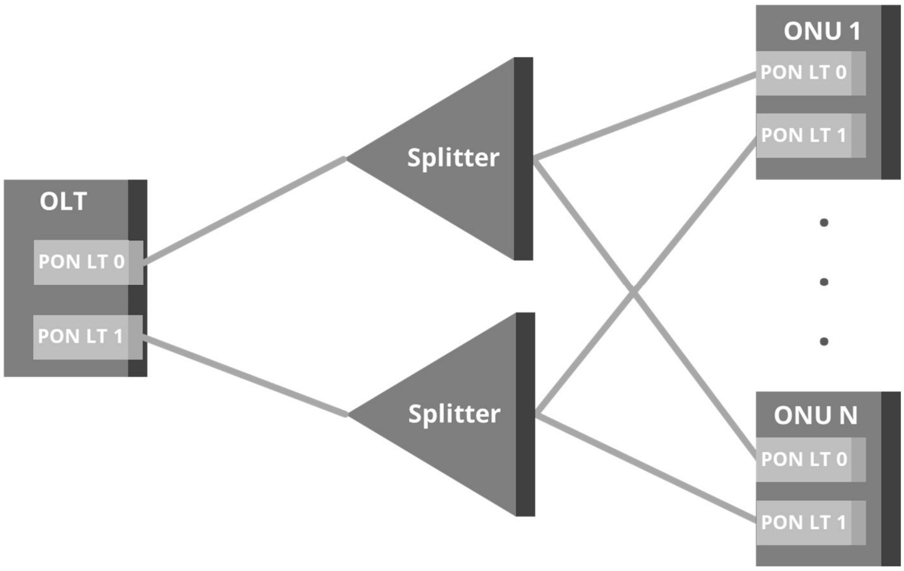


Figure 2.9: Duplex system: Full duplex system

- Type D - deprecated configuration since GPON that allows the mixing of duplicated ONUs with non-duplicated ones, essentially providing a combination of types B and C protection.

In these duplex systems, the PON line terminations do not need to reside in a single OLT equipment. They may even be located in physically diverse locations, resembling the dual-parented duplex system [21].

The protection model requires [21]:

- Optional protection switching;
- Possibility to implement both automatic and forced switching;
- Possibility to configure any type of protection;
- Persistence in all connections supported between the service node and the terminal equipment after switching.

All these types of architectures have been applied in different standards of PON developed so far. These PON standards will be explored in the following sections, along with some of their characteristics.

2.1.2 Asynchronous Transfer Mode PON/Broadband PON

Featuring a TDM-PON architecture, the first PON standard, Asynchronous Transfer Mode (ATM) PON (APON), is based on ATM, due to its traffic management capabilities and robust Quality of Service (QoS) support [12]. Initially used for telephone networks, it had a 54 megabit per second (Mb/s) transmission rate. However, with the rise of the Internet, this rate was then improved to 155 Mb/s, which was later upgraded to 622.08 Mb/s, because of the bandwidth demand increase. With this development, the name was also changed to Broadband PON (BPON) [10, 22].

BPON brought several improvements to APON, for instance, cost-effective deployment, enhanced security, Dynamic Bandwidth Allocation (DBA), and numerous broadband services like ATM, Ethernet access, and video distribution, thus adding additional wavelengths [23]. Furthermore, it supports more bandwidth than APON, up to 1244.16 Mb/s downstream and 622.08 Mb/s upstream [20].

BPON started implementing Wavelength Division Multiplexing (WDM) techniques, which allowed operators to offer additional services without disturbing the basic APON system. These techniques consisted of bidirectional multiplexing that used different wavelengths for upstream and downstream signals [22].

2.1.3 Ethernet PON

Despite ATM's ease in implementing QoS in the OLT and ONUs at the user and network sides, the data is transmitted in packets, which are broken down into ATM cells, and then rebuilt when received. This significantly increases costs and complexity [24].

Ethernet PON (EPON) introduces the transmission of packets of different sizes, by exchanging Ethernet packets instead of ATM cells. Thus, splitting packets into cells is no longer necessary, and the challenges associated with it cease to exist. Hardware is also cheaper, and the transmission rates are scalable [10, 24].

This technology allows bidirectional transmission of up to 1 Gigabit per second (Gb/s) and is usually split across 32 ONUs [11].

2.1.4 Gigabit PON

Gigabit PON (GPON) consists of a 2.4 Gb/s downstream transmission rate and the upstream can either be 1.2 Gb/s or 2.4 Gb/s. Even though, with the given technology, it was only necessary to support a split of up to 64 ONUs, GPON supports a 1:128 split ratio instead, accounting for the continuous evolution of optical modules. GPON can transport Ethernet, ATM, and TDM traffic, by using the GPON Encapsulating Method (GEM) [21].

In 2011, the Full Service Access Network (FSAN), Institute of Electrical and Electronics Engineers (IEEE) and International Telecommunication Union (ITU) groups proposed the next generation of PON, that had to meet the demands by increasing data rate, support more ONUs, extend passive reach, lower costs, and co-exist with GPON [6]. Two solutions were proposed: Mid-Term Next-Generation PON (*i.e.* NG-PON1) and Long-Term Next-Generation PON (*i.e.* NG-PON2). NG-PON1 aims to overcome the insufficient capacity of EPON with Gigabit EPON (G-EPON)/10-Gigabit EPON (10G-EPON) and GPON with 10-Gigabit PON (XG-PON). It can offer up to 10 Gb/s symmetrical data rates, but it is not enough to satisfy the constant increase in demand. NG-PON2 makes use of TWDM-PON to provide higher data rates than previous standards of up to 40 Gb/s downstream and upstream [6].

2.1.5 10-Gigabit PON

10-Gigabit PON (XG-PON) introduced a new downstream speed of 10Gb/s. Two standards were established regarding XG-PON's upstream transmission rate: XG-PON1, featuring 2.5

Gb/s, and XG-PON2, with 10 Gb/s. Since the latter is symmetrical, it can also be referred to as 10-Gigabit Symmetrical PON (XGS-PON) [25].

Co-existence is achievable between both XG-PON standards and additional services such as GPON or video distribution via a WDM multiplexer, given that its wavelengths do not overlap. Since network operators implemented split rates of 1:32 to 1:64, and to keep this co-existence, a 1:64 split is the minimum requirement for XG-PON [25].

Table 2.1 shows the transmission speed comparison among the different PON technologies mentioned.

PON standard	Downstream transmission (Mb/s)	Upstream transmission (Mb/s)
APON	622.08	155.52
BPON	1244.16	622.08
EPON	1244.16	1244.16
GPON	2488	2488
XG-PON	10000	10000

Table 2.1: PON standards' maximum transmission rates comparison

2.2 Next-Generation Passive Optical Network 2

Unlike previous NG-PON1 standards that were thought only as mid-term solutions to overcome the insufficient capacity of the time, NG-PON2 was rethought to be a long-term solution for higher data rate [6].

NG-PON2 requires the support of higher bandwidth per customer, more customers per feeder fiber, extended passive reach, low economical investment, low energy consumption, and co-existence with the previous GPON standard [6].

2.2.1 Requirements

In order to achieve these requirements, some technologies were considered: TDM-PON, WDM-PON, TWDM-PON, and a few others. After some benchmarking, the best approach was the TWDM-PON, which supports high capacity and is less disruptive and more cost-effective than other solutions [26].

Following this choice, NG-PON2 implements a multiple wavelength channels TWDM architecture, with four to eight channel pairs, each comprising one downstream and one upstream wavelength channel. These can be incrementally configurable, with the possibility of starting from only one pair deployed. This means that not all channel pairs need to be active. There are three combinations for the data rates in each channel:

- 10 Gb/s downstream and 10 Gb/s upstream;
- 10 Gb/s downstream and 2.5 Gb/s upstream;
- 2.5 Gb/s downstream and 2.5 Gb/s upstream.

The typical TWDM-PON uses four bi-directional channels, each with 10 Gb/s downstream and 10 Gb/s upstream, resulting in a combined 40 Gb/s downstream and 40 Gb/s upstream capacities. It also supports a split ratio of at least 1:256 and can coexist with the legacy PONs GPON, XG-PON1, G-EPON, and 10G-EPON [26, 27].

This standard also supports a Point-to-Point Wavelength Division Multiplexing (PtP WDM) architecture, which provides a dedicated wavelength per Optical Network Unit (ONU) in both downstream and upstream directions. The defining characteristic of PtP WDM is that each ONU is served by one or more dedicated wavelengths.

2.2.2 Architecture

Following a TWDM architecture, as depicted in Figure 2.10, NG-PON2 is composed by an Optical Line Terminal (OLT), containing multiple Channel Terminations (CT) for each channel available and a Wavelength Multiplexer (WM) that connects them, a splitter, and several ONUs. An ONU is assigned to a CT wavelength when it is registered in the system.

This means that more than one ONU can use the same wavelength of a CT. For example, in Figure 2.10, the ONUs 1 and 2 are using CT 1's wavelength. However, additional ONUs may use whichever wavelength is available and assigned to them when they are registered. Each CT and ONU communicate through a transmitter and receiver. A WM is a passive wavelength multiplexer that combines NG-PON2 wavelengths (usually four) into a single fiber. The termination of a CT can be called a Channel Pair (CP) and the termination of the WM can be called a Channel Group (CG). This nomenclature is especially useful in a protection scenario, as seen in the following section.

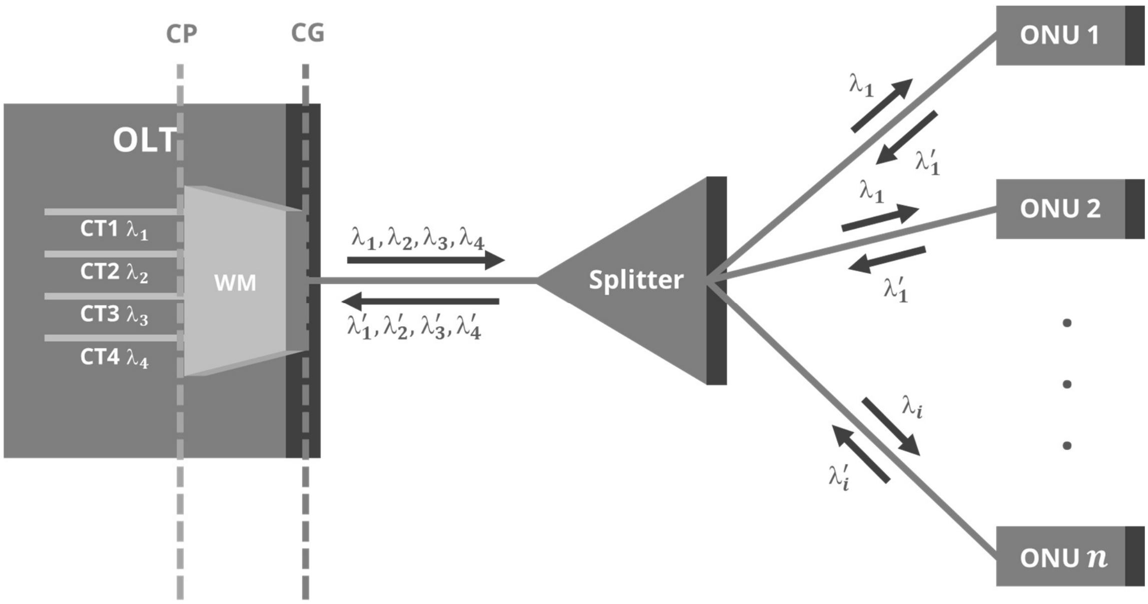


Figure 2.10: Typical NG-PON2 architecture

2.2.3 Protection architecture

NG-PON2 supports a Type B configuration, where a specific Channel Group (CG) has two OLT terminations, essentially meaning a duplicate OLT. An example of this can be seen in Figure 2.11. The two CTs that terminate the same Channel Pair (CP) are known as Type B peers [28].

This kind of protection allows mitigation if a failure were to occur in the fiber between the Channel Terminations and the Wavelength MUX or the fiber from the Wavelength MUX to the splitter, or even in case of failure of the Wavelength MUX or, in case of dual-parenting, an entire OLT. In case of one of these failures, all Channel Pairs within the Channel Group are switched simultaneously. If a single Channel Termination or an attached fiber fails, only that Channel Pair is switched, while the other pairs of the Channel Group stay the same, meaning that each Channel Pair is protected individually [28].

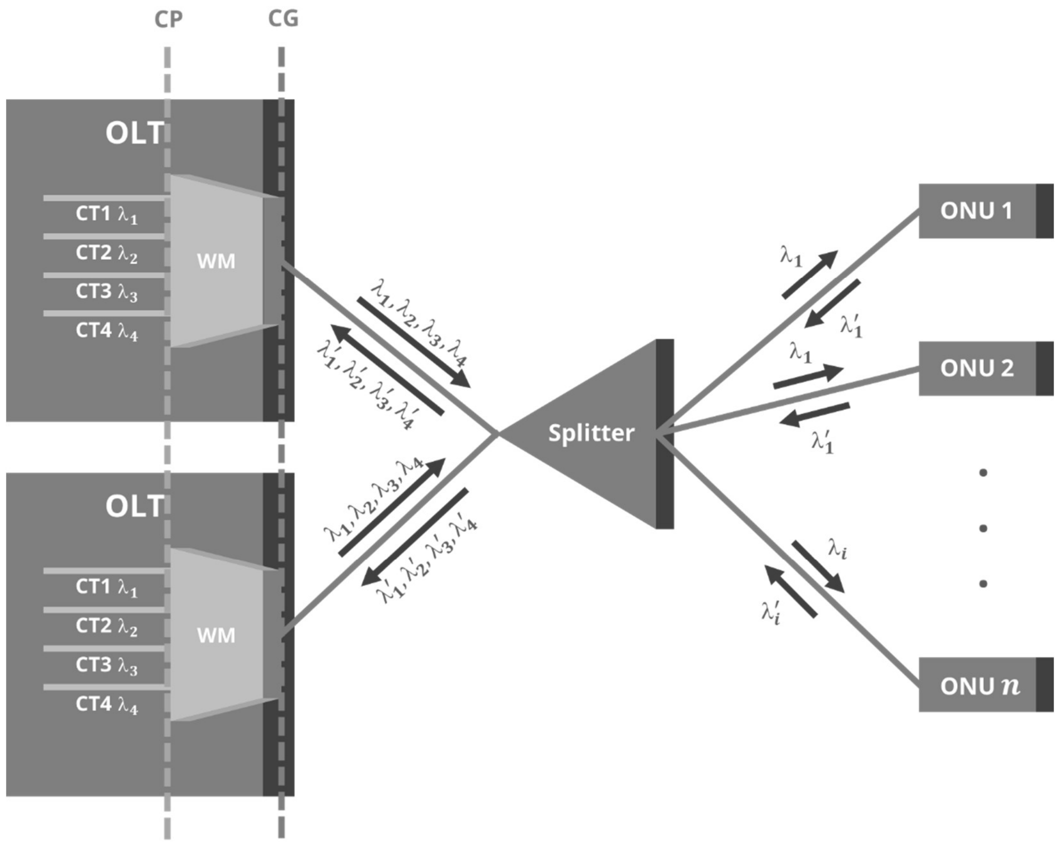


Figure 2.11: Type B dual-parenting protection in NG-PON2

Type B protection ensures that only one CT stays active providing service to the ONUs, while the other, if available, adopts a standby role, which monitors the upstream and is ready to overtake the other CT in case of a failure that prevents its peer from continuing as the active CT [28].

2.3 Inter-Channel-Termination Protocol

Previously, it was discussed how NG-PON2 is a multi-wavelength PON with different Optical Line Terminals (OLT) Channel Terminations (CT). These CTs must exchange information between each other related to channel configurations, status, and ONU management and, in case of a failure, the ONU should switch wavelengths with a minimal loss of service. This is made possible with the use of the Inter-Channel-Termination Protocol (ICTP). ICTP can be used not only in NG-PON2, but also in some single wavelength PON standards like GPON. It also supports multi-operator environments, where different operators share the same Optical Distribution Network (ODN) [29].

In the following sections, some of the most important characteristics of ICTP will be discussed.

2.3.1 Architecture

ICTP follows the same architecture of NG-PON2, where it stands as a back-office transport infrastructure, as depicted in Figure 2.12. This infrastructure is used by the OLT CTs from the NG-PON2 system for their interaction with each other.

Figure 2.12 shows a set of NG-PON2 Optical Network Units (ONU) attached to the point-to-multipoint passive ODN, that aggregates a set of OLT CTs via a Wavelength Multiplexer (WM) in an OLT. Each of these CTs ends a TWDM channel or a PtP WDM channel, which is a pair of one downstream and one upstream wavelength channel providing logical point-to-multipoint or point-to-point connectivity, respectively. An ONU is equipped with a tunable transceiver, which allows it to tune to a subset of available TWDM and PtP WDM channels [29].

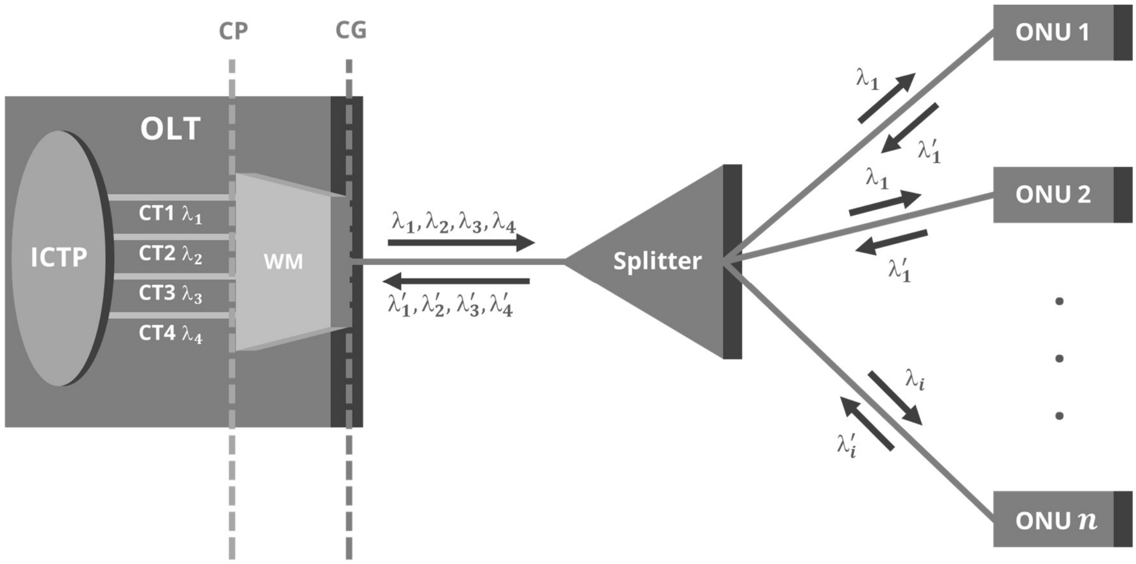


Figure 2.12: NG-PON2 architecture with ICTP infrastructure

To deal with communication between CTs so that an ONU can switch wavelengths channels without disrupting the system, ICTP considers that the information to be used by the ONU on the channel is either available to all CTs or at least one of them, and can be shared by that one CT with the others in the system. This assumption applies to both a single and multi-operator scenario [29].

ICTP also supports different kinds of protection architectures which will be detailed in the section below.

2.3.2 Protection architecture

It is possible to use Type B Protection alongside ICTP, where a single Channel Group has a Channel Pair with two OLT Channel Terminations. Figure 2.13 shows a dual-parented type B protection configuration, where each CT is housed in different OLTs [29].

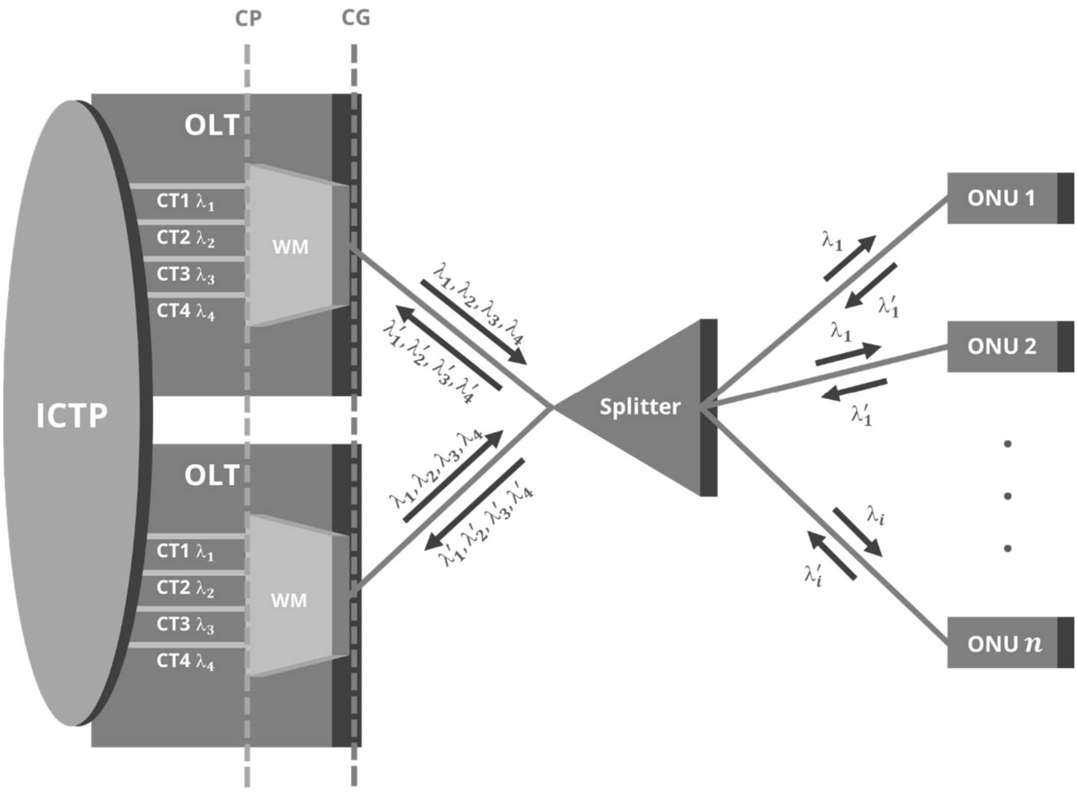


Figure 2.13: Type B dual-parenting protection with ICTP

This protocol also supports a Type Wavelength Protection, which is exclusive to multi-wavelength PON systems and depends on the availability of at least two CTs operating on different downstream and upstream wavelength channels while being connected to the same ODN. This allows the protection of the CTs against the failure of the CT and/or the fiber connected to it, switching the affected ONUs to the wavelength channels associated with another CT [29]. This is usually used for PON standards such as NG-PON2, while the type B protection mentioned previously refers to other standards like GPON or XGSPON, which do not have multiple wavelengths.

For the communication between the OLT CTs, it is important to define some guidelines, especially in the case of a multi-operator environment. The next section specifies the various transportation options for ICTP.

2.3.3 Transportation

Since ICTP is possible to be used alongside a variety of system configuration scenarios, there is, likewise, a variety of ICTP transportation options:

- CTs within the same NG-PON2 card, communicating over an internal shared memory or a message-passing channel;
- CTs on distinct line cards installed within the same OLT Network Element (NE) or chassis, communicating over a secure backplane communication channel;
- CTs on distinct line cards installed within different OLT NEs of the same central office, communicating over a secure Local Area Network (LAN) infrastructure;
- CTs on distinct line cards installed within different OLT NEs at geographically distinct locations, communicating over a Virtual Private Network (VPN);
- CTs on distinct line cards installed within different OLT NEs at geographically distinct locations, communicating over an open public infrastructure, where IPsec VPN (Internet Protocol Security VPN) is used to secure ICTP communications.

When the CTs are in distinct line cards installed within different OLT NEs, whether in the same Central Office or geographically in different locations, these OLTs can be owned by the same or different operators (multi-operator environment). In an NG-PON2 system involving multiple OLT CTs, the communication between CTs may have different transportation options [29].

It is essential to specify how the messages between CTs are exchanged. This is described in the next section.

2.3.4 Message Transport

The ICTP Message Transport includes two major components: the Protocol Stack, shown in Figure 2.14, and the Proxy.

The Protocol Stack shows the Transport Layer, which is divided into four different layers. As the Network Layer Protocol, the OLT NE must support IPv4 and, optionally, IPv6. It must also support TCP, as it also is the Transport Layer Protocol. The IP Layer only supports point-to-point transmissions for ICTP message delivery. Lastly, the Data Link and Physical Link Layers are link-specific and are not specified [29].

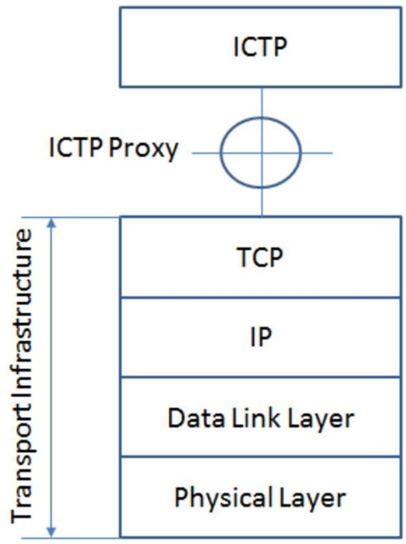


Figure 2.14: ICTP protocol stack

The ICTP Proxy is the interface between the ICTP layer and the ICTP Transport Infrastructure. A single proxy can host one or more CTs, which may belong to the same NG-PON2 system or a different system. One OLT NE may have one or more proxy instances, each with a unique IP address [29].

The Proxy functions are:

- Maintain the identity of the NG-PON2 system to which each hosted CT belongs, as well as a configuration table with:
  - The IDs of the CTs in the system, including any Type B Protection CTs;
  - The channel partition association for each CT;
  - The characterization of each CT as TWDM or PtP WDM;
  - The indication of whether each CT is locally hosted by the same proxy or a peer proxy elsewhere;
  - The forwarding information to reach remote CTs managed by other proxies.

- Maintain a point-to-point TCP connection with each peer hosting a CT included in any configuration tables maintained by the proxy. The TCP socket associated with each connection is the forwarding information of the peer proxy in a configuration table;
- Analyze the ICTP Message header upon receiving it from a locally hosted CT, and look up the NG-PON2 system configuration, forwarding it to one or more recipient CTs which can be hosted locally or remotely;
- Analyze the ICTP Message header upon receiving it over a TCP connection from a remotely hosted CT, and look up the NG-PON2 system configuration, forwarding it to the locally hosted recipient CTs.

The communication between the ICTP proxy and the locally hosted CTs and the representation form of the local forwarding information is left to the implementation and is not specified [29].

To complement the transportation options and methods of exchanging the messages, it is crucial to understand how each of these messages are structured, which is briefly described in the following section.

2.3.5 Messages

An ICTP message is divided in ten different fields, as seen in the Figure 2.15 below.

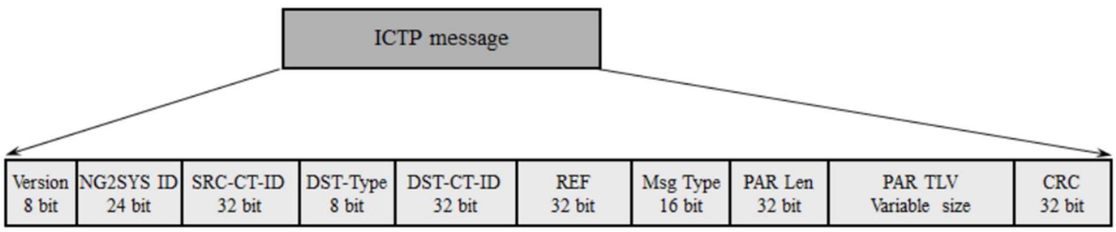


Figure 2.15: ICTP message format

Since these fields are too elaborated and most were unnecessary for the development of this work, they will be briefly described below. These ten fields are:

- **Version (8 bits)**: ICTP protocol version number;
- **NG2SYS ID (24 bits):** NG-PON2 system identifier of the sender;
- **SRC-CT-ID (32 bits)**: The identifier of the individual CT issuing the ICTP message;
- **DST-Type (8 bits)**: The qualifier for the DST-CT-ID field below. This qualifier is complex and can be thoroughly examined in page 29 of the TR-352[1];
- **DST-CT-ID (32 bits)**: The identifier of the ICTP message destination. The format depends on the DST-Type and can be analyzed in page 30 of the TR-352[1];
- **REF (32 bits)**: Message reference number. More information in Section 6.2 of the TR-352[1];
- **MSG Type (16 bits)**: ICTP message type. More information in Section 6.3 of the TR-352[1];
- **PAR Length (32 bits)**: The length of the Parameter Type Length Value (TLV) list below;
- **PAR TLV (variable size)**: A concatenated list of message parameters, each described with a {Type, Length, Value} triplet. More details in page 30 of the TR-352[1];
- **CRC (32 bits)**: The error detection code computed using the Cyclic Redundancy Check (CRC32) algorithm.

These messages are exchanged in various situations that occur in the system according to the management of the ONUs by the CTs. These situations are known as use cases. With the purpose of generalizing the ICTP for multi-operator scenarios, the data elements used in these use cases are previously defined and can be analysed in the next section.

2.3.6 Data Elements

In order to ensure secure and reliable mechanisms that enable remote administration, maintenance, and management in a system that may contain more than one service provider

[1] The Broadband Forum TR-352, Issue 1 (2017)

domain, it is essential to define ICTP accurately. In this and the following subchapter 2.3.7, the key use cases for ICTP are defined, which include NG-PON2 system creation and consistency verification, ONU activation, authentication and service provisioning, and ONU wavelength channel mobility management [29].

The Table 2.2 below lists the data elements used in the use cases of the next subchapter. The data elements in bold are the most relevant to the development of this work.

Data Element	Description
NG2SYS ID	NG-PON2 System Identifier, a 20-bit number that identifies an NG-PON2 system within an administrative domain.
PON-ID	A 32-bit unique structured number that identifies a TWDM or PtP WDM Channel Termination entity within an administrative domain.
DWLCH ID	TWDM Downstream Wavelength Channel ID, a 4-bit number that identifies a downstream wavelength channel. It is equal to the ordinal number of the channel in Table 6-3 in Recommendation G.989.3[2].
UWLCH ID	TWDM Upstream Wavelength Channel ID, a 4-bit number that identifies an upstream wavelength channel.
ONU-ID	A 10-bit unique number assigned by OLT CT that identifies an activated ONU in an NG-PON2 system.
Alloc-ID	Allocation Identifier, a 14-bit unique number assigned by OLT CT that identifies an ONU traffic-bearing entity as a recipient of upstream bandwidth allocations.
XGEM Port-ID	A 16-bit unique number assigned by the OLT CT that identifies an individual upstream or downstream logical connection.
PON-TAG	An 8-byte value that is chosen by the operator and is a static identity of the OLT CT for security context binding.
SN	Serial Number, an 8-byte value composed of a 4-character vendor ID and a 4-byte integer Vendor-Specific Serial Number (VSSN) that provides a globally unique static identifier of an ONU.
REG-ID	Registration ID, a 36-byte string that serves as a dynamic identifier of an ONU for basic authentication.

[2] Rec. ITU-T G.989.3 (2015) – Clause 6.1.5.4

Teqd	Upstream Physical Layer (PHY) frame offset, or zero-distance equalization delay, is the elapsed time between the start of the downstream PHY frame carrying a specific Bandwidth Map (BWmap) and the upstream PHY frame implementing that BWmap.
MSK	Master Session Key, a 128-bit value that is shared between the OLT CT and the given ONU as a result of an authentication procedure and which serves as a starting point for the derivation of all of the other secret keys used in subsequent secure communications.
Data Encryption Keys	A set of four (two pairs for unicast and two pairs for broadcast) 128-bit numbers shared between the OLT CT and the ONU and used to encrypt the data traffic between them.

Table 2.2: Data elements used in use cases and their descriptions [29]

In the following section, the use cases that make use of these data elements will be described thoroughly.

2.3.7 Use Cases

Some use cases defined in this subchapter are also applicable to PtP WDM, which is subject to further study. Another subset of those use cases, specifically those related to Type B protection, apply to single-channel PON systems, such as XGSPON and GPON. ICTP must support the use cases listed below in Table 2.3. In this table, the use cases in bold will be the most relevant for the development of this work.

G.989.3[3] Table VI.1 Number	Use Case	Description
1	CT Profile Sharing	A CT periodically sends a broadcast ICTP message containing its channel profile to other CTs.

[3] Rec. ITU-T G.989.3 (2015)

2	Silent Start and CT Initialization	When a new CT is initialized, it employs ICTP to verify its configuration consistency with the system configuration and to avoid accidental interference.
3	Initial Zero-Distance Equalization Delay	A CT transmits an ICTP message containing its selected local Zero-distance Equalization Delay (EqD) to the next CT in the pre-defined total order ring. Upon receipt of an ICTP message containing Zero-distance EqD, the CT adjusts its local Zero-distance EqD to the larger of the two values and transmits a message containing its new local Zero-distance EqD to the next CT in the pre-defined total order ring.
4	Initial ONU Validation upon Activation	When a CT receives Serial Number (SN) ONU PLOAM (Physical Layer Operation Administration and Maintenance) message from an activating ONU, the CT verifies the reported PON-ID and validates whether the SN is allowed on the NG-PON2 system. If the reported PON-ID is different from the CT's own, the CT uses ICTP to query the owner of the reported PON-ID providing the SN of the stray ONU, the UWLCH ID where it has been detected, and an indication whether the SN is valid.
5	**SN and Assigned ONU-ID Consistency Verification**	For the ONU which passes the initial validation, the OLT CT sends a broadcast ICTP message to confirm the SN uniqueness (that SN hasn't been assigned an ONU-ID) and the consistency of the proposed ONU-ID assignment (that ONU-ID hasn't been assigned an SN).
6	**ONU Discovery Resolution**	If the OLT CT receives the SN which is valid on the NG-PON2 system, but cannot associate the reported Reg-ID with a valid service profile, it sends a broadcast ICTP message to ask the peer CTs if anyone recognizes the ONU, before handing the ONU over to the interested bidder.
7	Alloc-ID Assignment Consistency Verification	Whenever an OLT CT assigns a non-default Alloc-ID to an ONU, it verifies with an ICTP interaction that the proposed Alloc-ID has not been assigned to any other ONU-ID in the NG-PON2 system.

8 & 9	ONU Handover	In case of a planned ONU handover from one (DWLCH ID, UWLCH ID) pair, or source, to another (DWLCH ID, UWLCH ID) pair, or target, an ICTP transaction guaranteeing state consistency of the involved CTs is executed. If the source and target CTs share a security association, the transaction may include the exchange of the MSK and active data encryption keys. Upon completion of planned ONU handover or recovery from an Intermittent Loss of Downstream Synchronization (ILODS) which involves a change of the operating (DWLCH ID, UWLCH ID) pair, an ICTP transaction guaranteeing state consistency of the involved CTs is executed.
10	ONU LOB Mitigation	When an OLT CT fails to receive an expected transmission from a particular ONU, it uses a broadcast ICTP alert to notify the peer CTs of the NG-PON2 PON system of the loss of communication with the ONU.
11	-	This use case has been obsoleted.
12	Rogue ONU Mitigation	This use case covers various techniques of rogue ONU isolation (such as attendance report) and mitigation including broadcast or directed request to peer CTs in an NG-PON2 system to stop a particular ONU from transmitting upstream.
13	Wavelength Protection CT Initialization	The peer CTs on an NG-PON2 system use ICTP to communicate Transmission Convergence (TC) layer configuration and service while configuring the ONU, and to exchange the notifications between OLT CTs when protection is triggered.
14	-	This use case has been obsoleted.
15	Synchronization of ONU Dynamic TC Data	The peer CTs on an NG-PON2 system use ICTP to communicate dynamic TC (Transmission Convergence) layer data.
16	Synchronization of ONU Dynamic Service Data	The peer CTs on an NG-PON2 system use ICTP and IPFIX (IP Flow Information Export) to communicate dynamic service layer data.

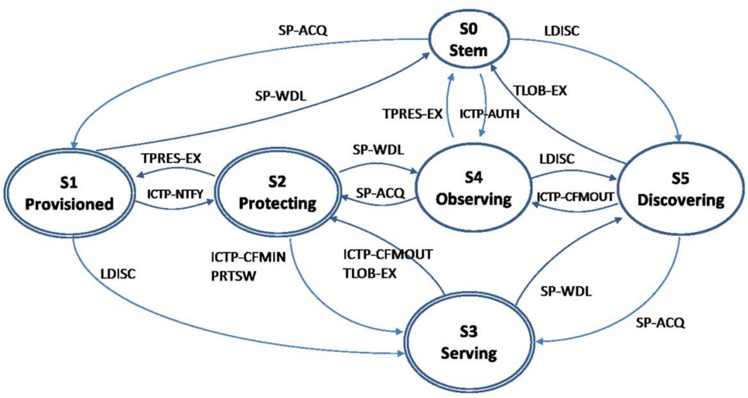
Table 2.3: ICTP use cases and descriptions [29]

The interaction between CTs and ONUs in ICTP is extremely elaborate and needs to be carefully stipulated. State Machines are a fitting method of studying these interactions and will be explored in the next section.

2.3.8 State Machines

This protocol makes use of two state machines that are specific to ONUs. Every time an OLT CT becomes aware of an ONU, it instantiates a Serving State Machine for that ONU. The state of each instance of this machine is generally independent of the state of other instances maintained by the OLT CT. There is also a Tuning State Machine, which is used as a part of the OLT's ONU-specific state once the OLT transitions out of the Stem state of the Serving State Machine, but this State Machine is too technical and far out the scope of this work. For more information on the Tuning State Machine, the Section 7.2.2.2 of the TR-352[4] can be analyzed.

The OLT CT Serving State Machine is composed by six states, two timers and eleven inputs. The diagram and its events can be seen below in Figure 2.16.



Acronym Legend

Local events:	
LDISC	Local ONU discovery
PRTSW	Protection switching
SP-ACQ	Service profile - acquisition
SP-WDL	Service profile - withdrawal
TLOBI-EX	Expiration of the LOBi condition timer, Tlobi
TPRES-EX	Expiration of the ONU presence timer, Tpres.
ICTP primitives:	
ICTP-NTFY	ONU service notification, onuNotify()
ICTP-AUTH	ONU authentication request, onuAuthen()
ICTP-CFMOUT	Handover confirmation indication, ConfirmIn()
ICTP-CFMIN	Handover confirmation acknowledgment, ConfirmOut()

Figure 2.16: Serving State Machine state and transition diagram [29]

[4] The Broadband Forum TR-352, Issue 1 (2017)

Since this State Machine is extensive, only its relevant aspects for this work will be explored. The full description can be found in Section 7.2.1.2 of the TR-352[5].

Only five of the six states are applicable, listed below in Table 2.4. The timers are irrelevant in this case, and three of the machine's inputs can be seen in Table 2.5.

State	Description
Stem	The default state for all ONU-IDs that are disassociated with the given OLT CT. The data structures pertaining to the ONU-ID are invalidated and may be de-allocated. These ONU-specific data structures are instantiated upon one of the following events: • Local ONU discovery • Request to authenticate an ONU from a peer OLT CT • Acquisition of a Service profile for an ONU
Provisioned	The OLT CT has a service profile for the ONU identified by the Serial Number and/or Registration ID. ONU-ID has not been assigned.
Serving	The OLT CT has a service profile for the ONU, hosts, and provides service to the ONU. The OLT CT periodically broadcasts onuNotify().
Observing	The OLT CT has no service profile for the ONU but is aware that the ONU is being hosted by a peer OLT CT in the NG-PON2 system.
Discovering	The OLT CT is hosting the ONU but has no service profile for it. The OLT CT is seeking an adopter for the ONU by periodically broadcasting onuAuthent().

Table 2.4: Serving State Machine states and descriptions [29]

Input	Applicable states	Semantics
ICTP Primitives		
onuAuthent()	Stem, Provisioned, Protecting, Observing	Request from an OLT CT in an NG-PON2 system to the peer OLT CT in an NG-PON2 system to authenticate the ONU for which the sender OLT CT lacks the service profile.
onuClaim()	Serving, Discovery	Declaration by an OLT CT of availability of the service profile for the ONU.
onuNotify()	Provisioned, Protecting, Observing	Notification by the OLT CT which has a service profile for the ONU that the ONU is being hosted and served.

Table 2.5: Serving State Machine inputs, applicable states and semantics [29]

[5]The Broadband Forum TR-352, Issue 1 (2017)

Even though the Serving State Machine is important to understand the functional part of ICTP, it was not rigorously followed in the development of this work and it will not be further discussed.

3 Management of ONUs via ICTP

This chapter introduces the experimental work, where the hardware and software are described, and the implementations of the use cases are described.

The experimental part of this work was made with the cooperation of Altice Labs, which had the major part of the system already built, including the hardware/software of the OLT, multiplexer, splitter, and ONU/ONT, as well as the architecture, communication, and behavior of PONs like GPON and NG-PON2.

To add to those previously implemented features, this work intends to develop the means to control and synchronize ONUs, employing ICTP for NG-PON2 and GPON, in C++.

Even though the ICTP standards were tried to be followed as closely as possible, some implementations had to be changed or withdrawn altogether, such as the communication protocol between the ICTP Managers from TCP to UDP for simplicity reasons, since the system already used UDP communications; the reuse of indications from the OLT because creating new ones specific to each case would be time consuming and complex with a great learning curve; and the message format was extremely simplified since there were multiple components unnecessary for the implemented use cases.

To develop all fourteen of the ICTP's use cases would be unrealistic for this dissertation, considering the amount of time it takes to develop one use case alone. Since this was known from the beginning of this work, it was decided to sort the use cases by relevance. Their importance was evaluated according to different criteria, such as already developed features (*e.g.,* the synchronization of ONUs in the system), or the lack of time (use cases that were too complex). Additionally, it was important to choose use cases that would be representative of the overall behavior of ICTP. Further information about this choices can be consulted in the following sections.

3.1 Hardware

In order to start the development and tests of the communication between OLT CTs, a scenario had to be assembled, whose architecture should resemble the Figure 3.1 below. This architecture is extremely similar to the one on Figure 2.13. It is a Type B protection with an ICTP infrastructure, dual-parented OLTs, one splitter, and several ONUs.

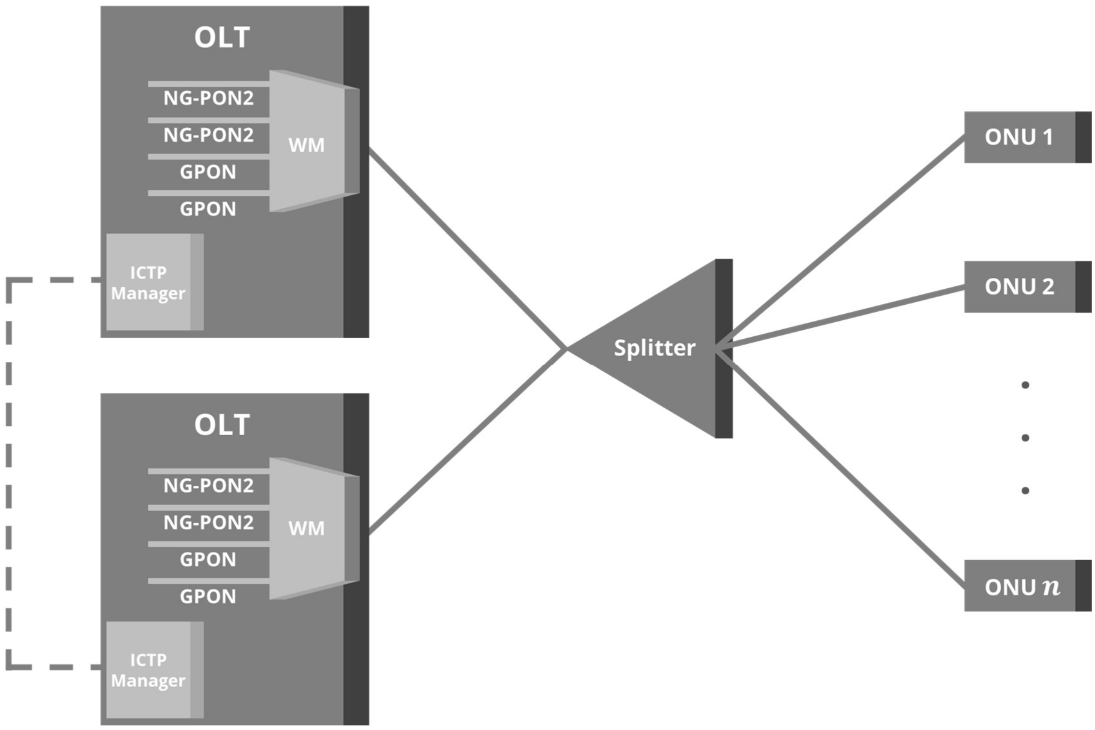


Figure 3.1: General ICTP scenario architecture

Both GPON and NG-PON2 standards were chosen in a coexistence scenario, supporting Type B protection each. Thereby, the connected ONUs/ONTs in the system are either GPON or NG-PON2.

The ICTPManager module is present in every OLT in the system, to carry out communications related with ICTP between every OLT, via UDP. In the next section, the development of this module, as well as the underlying decisions, will be discussed.

3.2 Software

The main objective of this work is to implement and test the use cases described in chapter 2.3.7. However, from these fourteen use cases, only a number of them made sense in the given scenario for previously explained reasons. Since the GPON standard is more matured and stable than NG-PON2 in the used pre-built system, it is important for the first use cases to be compatible with GPON, preventing any problems that can still exist in NG-PON2 and that are out of the scope of this work to fix. These use cases are numbers 2, 3, 4, 5, 6, 7, 8 and 9. Among these, there were some use cases that were more complex than others, so it was decided to start implementing the less time consuming ones. By ascending order of complexity, these were 6, 5, 7, 4, 2, 3, 8 and 9.

The inherent overhead created by the required studying of essential information related to and preceding ICTP, specifically all the components and mechanisms in NG-PON2 and GPON, made it necessary to prioritize the use cases being addressed. As a result, and considering the topmost important use cases mentioned above, use case 6 was chosen initially for covering a large part of the essential elements of the system. Afterward, use case 5 was also implemented.

Even though the majority of the software was already done for the OLT part, the ICTPManager had to be created from scratch, as well as a few other components, like the indications, message structure and allocation, and message handlers for each new indication.

As mentioned in the previous section, the ICTPManager is a module that handles the ICTP part in every OLT. This unit communicates with the remaining of the OLT and the other Managers via UDP, with a specific socket for the OLT and one just for the Managers. When it initializes, it opens both sockets and listens to both port. Since there is no way of knowing where the other OLTs/Managers are located and their specifications, this has to be given to each Manager by an administrator. There are a number of ways of doing this, and considering a test scenario like this one, it was best to pass the specifications of the Manager initiated and fellow peers as a parameter, also giving the option of managing the pairs in the ICTPManager program itself. The first three parameters would be the ID, IP address, and slot ID related to the ICTPManager initiated. Further sets of three optional parameters would be the information of peer Managers. This made it convenient to initialize the Managers for testing purposes. An ICTPManager also has the choice of displaying, adding, and removing pairs while running.

The components of the system communicate through the use of indications that send out messages, identified with a code. Some of this indications have been previously developed, like the OLT communications. The indication sent from the OLT to the Manager had to be slightly changed, so it would fulfill the requirements to send exactly what was needed. For this end, a new indication similar to the already implemented was created. This indication receives the message's code, a buffer pointer with the information to deliver to the Manager plus its length, the IP address of the Manager receiving the message, and the port of the UDP socket.

The message codes are used to identify what type of message is being sent in an indication and is unique for a certain use case. Since the previously existing codes in the system were used for events irrelevant to ICTP, it was necessary to create a new range of addresses allocated specifically for the ICTP messages, dividing this range in two for both OLT-Manager messages and Manager-Manager messages.

The buffer referred was organized in a structure. This meant the creation of new structures that contained information to be transmitted over an indication for all use cases. Two structures were created: *ICTPIndication* and *ICTPReplyInd*.

ICTPIndication is the structure used by the OLT and the Managers. To simplify, this structure is generalized to be used in any use case in either OLT-Manager and Manager-Manager communications. The details of this new structure can be seen in Table 3.1 below. Since this structure was generalized, some of these variables are not always used.

Name	Type	Description
slotId	8-bit unsigned integer	The slot identification of where the ONU was detected or of the Manager sending the indication.
linkId	8-bit unsigned integer	The link identification of where the ONU was detected or of the Manager sending the indication.
managerId	8-bit unsigned integer	The Manager identification that sent the indication.
onuId	8-bit unsigned integer	The detected ONU identification.
serial	8-byte character array	The Serial Number of the detected ONU.

Table 3.1: Information of structure *ICTPIndication*

The second structure, *ICTPReplyInd*, is used for replies between Managers. They indicate the success or failure of an action of, for example, recognizing an ONU. This was also generalized for both use cases, hence some variables may not always be used. More information on this structure can be consulted in Table 3.2 below.

Name	Type	Description
slotId	8-bit unsigned integer	The slot identification of where the ONU was detected or of the Manager sending the indication.
managerId	8-bit unsigned integer	The Manager identification that sent the indication.
matchedSn	8-bit unsigned integer	If an equal SN was found. Values are '1' if there was a match and '0' if there was not match
matchedOnuId	8-bit unsigned integer	If an equal ONU-ID was found. Values are '1' if there was a match and '0' if there was not match

Table 3.2: Information of structure *ICTPReplyInd*

Whenever an indication is sent to a Manager, a handler is needed to manage the message. This handler was created for each message code and behaves differently depending on the received message. Except for the reply, messages differ depending on the use cases. The message with code *ICTPReply* is reused throughout the use cases because the ICTP standard does not specify what to do after a use case is handled and doing so is not in the scope of this work. Currently, the role of the handler of this message is logging what was received from a Manager. Additional information about further handlers can be found in their respective use case implementation in the following subsections.

3.3 Use case 6 implementation

The use case 6 describes a communication between the OLT Channel Terminations when one receives a SN from a ONU which is valid, but cannot be associated with a valid service profile, hence sending a broadcast message to peer CTs to check if any of them recognizes the ONU. This can be broken down into five main steps:

- A new ONU is detected by the OLT;
- The OLT sends an indication with the ONU information to the ICTPManager;
- The ICTPManager sends a broadcast indication with the received ONU information to the other ICTPManagers;
- Having received that indication, the ICTPManagers check if the ONU is recognized;
- The ICTPManagers reply whether the ONU is recognized by them or not.

The sequence diagram seen in Figure 3.2 depicts these steps and the interactions between the different components in the system.

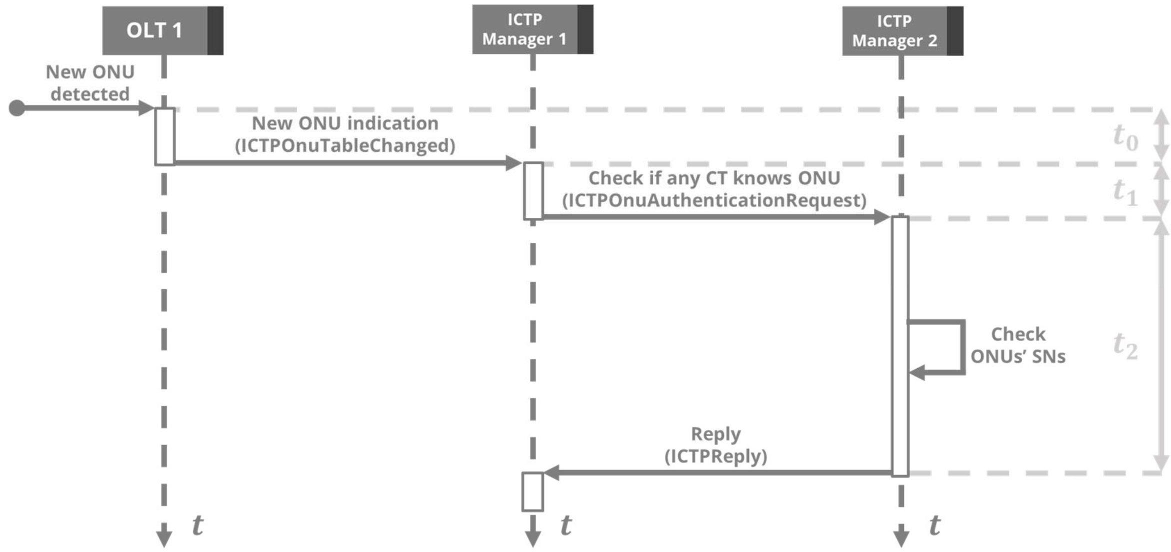


Figure 3.2: Sequence diagram of the developed use case 6

The first step of development was the detection of a new ONU. This detection was already present in the system, but a new indication had to be added for the Manager. The method used to send this indication was developed specifically for ICTP, with a particular message code that lets the Manager know about a new ONU from the OLT, named *ICTPOnuTableChanged*. Another message type was needed for the broadcast message from one Manager looking for a Channel Termination that knows the received ONU, named *ICTPOnuAuthenticationRequest*. The use of these messages is shown in Figure 3.2.

When the OLT sends an indication to the Manager with the message code *ICTPOnuTableChanged*, the matching handler forwards the received ONU information *slotId*, *linkId*, *onuId* and *serial*, with the addition of its *managerId*, to all known Manager pairs, in search of one that recognizes the ONU.

This Manager-Manager communication is also done in the form of an indication, with the same parameters as the previous OLT-Manager indication. For this effect, there was no use on duplicating the previous indication logic, so the same one was used. The employed message code is *ICTPOnuAuthenticationRequest*. Its corresponding handler starts by setting the variable *matchedSn* from the structure *ICTPIndication* to '0'. Then, with the received information of the ONU, the Manager checks if that ONU is known to it. The initial Manager awaits the response of all the contacted Managers.

To check if the Manager knows the ONU, another tool that was previously implemented was used. This tool is a table that registers all the ONUs known to the system and keeps all their information and states updated. Since there is no way of searching an ONU through its Serial Number (SN), all the known ONUs have to be cycled through and compare its SN with the received one.

Finally, if the Manager got a match in a SN, the loop that is iterating over the ONUs is broken ahead of time, and the variable *matchedSn* is set to '1'. Independent of recognizing the ONU or not, the Manager always sends an indication with the message code *ICTPReply* and structure *ICTPReplyInd*, that contains its *managerId* and the *matchedSn* variable.

The delays from one machine sending an indication to another receiving it must be around 2 ms, depending on the distance of both machines. However, when performing an operation from the moment of reception of an indication to the moment of sending out the following indication, a machine should take no more than 50 ms. This is discussed in Cisco's article 'Putting 50-ms In Perspective', by Lionel Florit [30]. As seen in Figure 3.2, the delays t_0, t_1 and t_2 should take no more than 50 ms each. However, since both delays t_0 and t_1 do not perform an exhaustive operation and only create another indication to send out, this should not take over 1 or 2 ms. The most intensive operation in this implementation is the search of the ONU's SN, performed in t_2, which should not be over 50 ms.

3.4 Use case 5 implementation

This use case is activated whenever a known ONU by the Chanel Termination (CT) is registered and online. The CT then checks the ONU's information uniqueness and consistency by sending a broadcast message to all peer CTs. This check consists in validating the ONU's Serial Number (SN) uniqueness (no ONU-ID in the system has that SN assigned to it), and the ONU-ID consistency (no SN has been assigned to that ONU-ID). This logic can be broken down into five main steps:

- A registered ONU is detected online by the OLT;
- The OLT sends an indication with the ONU information to the ICTPManager;
- The ICTPManager sends a broadcast indication with the received ONU information to the other ICTPManagers;
- Having received that indication, the ICTPManagers verify the information's uniqueness and consistency;
- The ICTPManagers reply whether the ONU's information is unique and consistent or not.

The sequence diagram seen in Figure 3.3 depicts these steps and the interactions between the different components in the system.

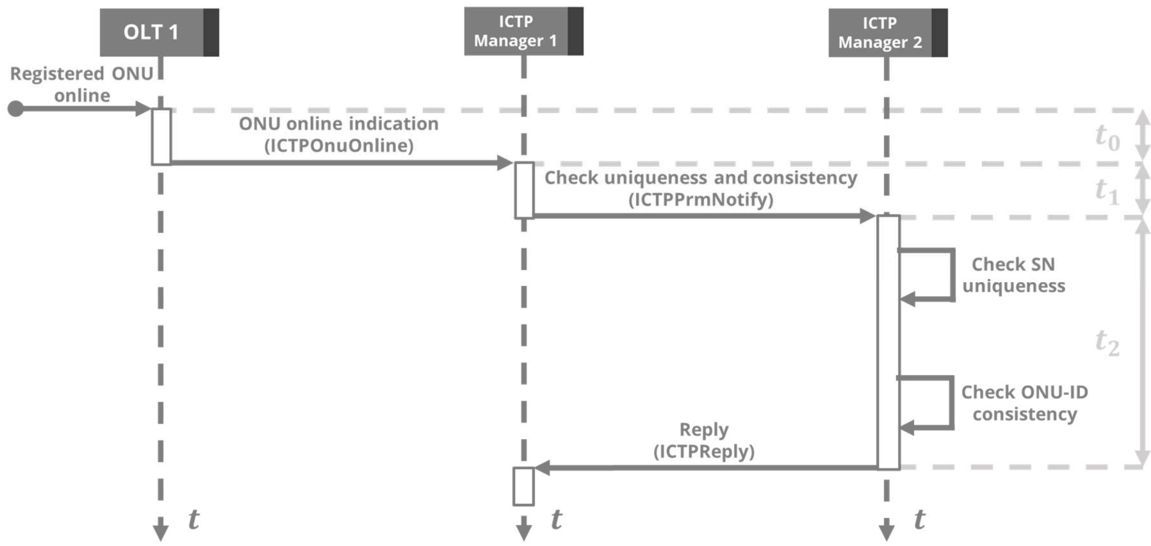


Figure 3.3: Sequence diagram of the developed use case 5

Just like the previous use case, the first step to start the development was to add an indication to the OLT that alerted the Manager whenever a recognized ONU would go online. The message type created specifically for this situation was named *ICTPOnuOnline*. While there is no difference in the composition of *ICTPOnuOnline* and *ICTPOnuTableChanged*, the distinction was made between these messages because the context is different, and for logging reasons. After receiving this message, the Manager broadcasts a message to all peer Managers using a new message type as well, named *ICTPPrmNotify*. Both uses of these messages are exemplified in Figure 3.3.

When the Manager receives the indication of the OLT with code *ICTPOnuOnline*, the message's handler forwards the received information of the ONU to the other Managers, with the addition of it *managerId*.

Once more, this broadcast is done as an indication with a new message type named *ICTPPrmNotify*. Whenever this message is received, the corresponding Manager starts by setting the values of *matchedSn* and *matchedOnuId* from the *ICTPReplyInd* to '0'. After this, the Managers checks the SN's uniqueness by searching every position of the known ONUs table to check if that SN is already used for another ONU. Finally, the ONU-ID's consistency is verified by checking the ONU-ID's SN and confirming that it has no other attribution different to the received SN.

If the Manager finds that the SN is not unique, it sets the variable *matchedSn* to '1', and if the ONU-ID is not consistent, it sets the variable *matchedOnuId* to '1' as well. In the end, the Manager sends an indication with message code *ICTPReply* and structure *ICTPReplyInd* containing both *matchedSn* and *matchedOnuId* variables, as well as its *managerId*.

Just like in the previous use case 6, the delays from one machine sending an indication to another receiving it must be around 2 ms, and from the moment of reception of an indication to the moment of sending out the following indication, it should take no more than 50 ms. As seen in Figure 3.3, the 50 ms rule should be applied to the delays t_0, t_1 and t_2. The most exhaustive operation is done in t_2 when the search of the ONU's SN and checking of the ONU's ID is performed. Since both times t_0 and t_1 do not perform such an intensive operation like t_2 and only create another indication to send out, these delays should not take over 1 or 2 ms.

4 Use case validation and results

4.1 Testbed

A test scenario containing the interactions and communications between each module, and subsequent elapsed time measurements between important operations was established, to evaluate if the developed use cases (numbers 5 and 6) were viable in a real scenario.

This test scenario, which is depicted in Figure 4.1, includes two OLTs with an ICTPManager module each, one accessible at IP address 10.112.42.83, and another at IP address 10.112.42.134, henceforth referred to as OLT/Manager 1 and OLT/Manager 2, respectively. These ICTPManagers communicate between each other through a unique port via UDP. There is a difference to the typical architectures, which is the multiplexer. In the used system, to simplify and lower the costs, both OLTs share a common multiplexer. It is important to note that the two systems are physically placed side by side, which may not reflect the actual configuration in a real-case scenario.

Even though this use case is viable in an NG-PON2 scenario, it is entirely testable in a GPON environment because of the chosen use cases to be implemented. This technology was preferentially used given its stability compared to NG-PON2, which is not yet a commercial feature of the OLTs in question.

The OLT 1 contains one NG-PON2 slot with two Channel Terminations in slot 3 and a GPON slot in slot 17, and OLT 2 also includes one NG-PON2 slot with two CTs in slot 7, and 3 GPON slots in slots 2, 3 and 5. The wavelengths, represented by λ_n in Figure 4.1, are shared among the GPON slots, but distinguished for each NG-PON2 CT. In this case, since the ONUs are being used through GPON only, they only use the λ_5 wavelength for downstream and λ'_5 for upstream, and the wavelengths $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ and $\lambda'_1, \lambda'_2, \lambda'_3, \lambda'_4$ are not in use.

In order to easily test both outcomes of whether the second ICTPManager finds a Serial Number match or not for use case 6, and whether the SN is unique and the ONU-ID is consistent for use case 5, two ONUs were added to the system. The OLT 2 recognizes ONU 1, but not ONU 2. The OLT 1 has both ONU 1 and ONU 2 as registered ONUs. The ONUs are being captured in the GPON slot ID 17 for Manager 1, and slot ID 3 for Manager 2. The other slots are not used in the chosen use cases.

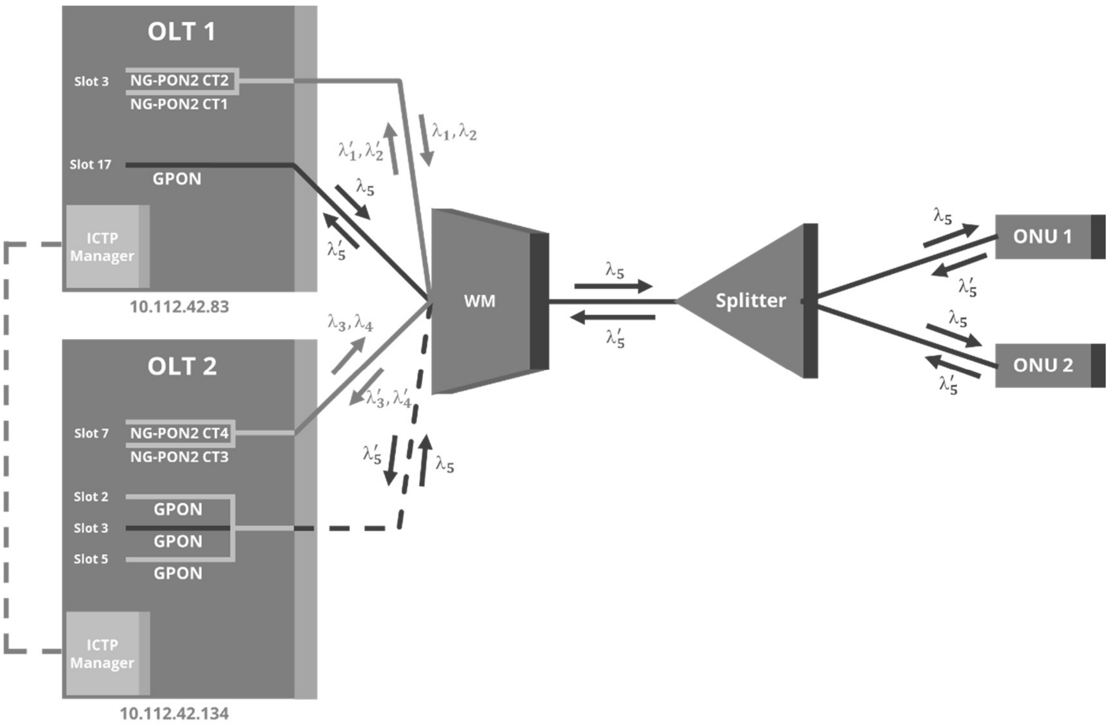


Figure 4.1: Test scenario architecture

To begin the tests, both ICTPManagers are run in their corresponding OLTs. To initialize the Managers, some parameters have to be specified, depending on the Manager that is being initialized. The first set of three parameters refers to the specific Manager's ID, IP address, and slot ID, while the next parameters in sets of three are concerning its pairs. In the case of

Manager 1, its pair will be Manager 2, and vice versa. The Manager's ID is a static identifier chosen randomly, unique among all Managers. Figure 4.2 demonstrates the initialization of both Managers, being the Manager 1 above, and Manager 2 below. For example, to initialize the Manager 1, the first parameter is its ID (1), secondly its IP address (10.112.42.83), and lastly is its slot ID (17). After this set of parameters is the information about its pairs, in this case, Manager 2, with Manager ID (2), IP address (10.112.42.134), and lastly its slot ID (3).

```
[root@OLT-UNICOM-1~]# ./ICTPManager 1 10.112.42.83 17 2 10.112.42.134 3

[root@OLT-UNICOM-2~]# ./ICTPManager 2 10.112.42.134 3 1 10.112.42.83 17
```

Figure 4.2: The initialization of both Managers with the corresponding parameters. Manager 1 is above, and Manager 2 is below

When initialized, the Manager shows an exit option, along with three more options that allow the management of the Manager's pairs. It is possible to add a pair, remove one if the list of pairs is not empty, and display the list of pairs. The pairs that were passed as arguments in the Manager's initialization are automatically saved on this list. Figure 4.3 below shows the displayed options after a Manager is initialized.

```
-Options-------------
|  0: Exit          |
|  1: Add pair      |
|  2: Remove pair   |
|  3: Display pairs |
---------------------
Enter option:
```

Figure 4.3: Pair options in a Manager

Figure 4.4 shows the sequence of adding a random pair with ID (3), IP address (10.112.42.10), and slot ID (10), removing it, and finally displaying all pairs of the Manager after the operations, thus demonstrating all three options of pair management of the ICTPManager. The Manager used for this example was Manager 1, which was initialized previously with Manager 2 as a pair.

```
Enter option: 1
Input pair details
Manager ID: 3
IP address: 10.112.42.10
Slot: 10
Manager pair added!

Enter option: 2
-Pairs-------------------------------------
| PairID | ManID |      IPadd      | Slot |
|    0   |    2  |  10.112.42.134  |   3  |
|    1   |    3  |   10.112.42.10  |  10  |
-------------------------------------------
Input pair ID to remove: 1

Enter option: 3
-Pairs-------------------------------------
| PairID | ManID |      IPadd      | Slot |
|    0   |    2  |  10.112.42.134  |   3  |
-------------------------------------------
```

Figure 4.4: All 3 options for managing pairs in ICTPManager with Manager 1 as an example, initialized in advance with Manager 2 as a pair

Even when the pairs are being managed, the Manager never stops listening to possible incoming messages and acts accordingly to the received message.

After this initialization, the use cases are ready to be tested. The system itself does not have any suitable way of testing the time elapsed between two operations, especially in an environment with two distinct machines. The time measurements have to be from the time stamp in the logger. This originates an obstacle when it comes to measuring the delay of indications from one machine to the other, since the clock synchronization between the machines were not precise enough and always had a difference of one or two milliseconds. Due to this challenge, the tests made to messages going from one machine to the other were discarded. This does not affect the results much because the only delays between two machines were the dispatch and reception of an indication, which is almost always considerably low. Furthermore, since every step was a manual process where one test alone took around three minutes to complete, the system was only tested one hundred times. A script that turned off and on the ONUs at the right time and another script that received the logger data and calculated the difference of the times were also developed. Since these scripts were only for support and convenience, they will not be discussed any further.

Commonly, it is believed that an operation should not take over 50 ms to complete. This is highly debated in Cisco's article 'Putting 50-ms In Perspective', by Lionel Florit [30]. As rule of thumb, 50 ms is a measure that is more than enough to guide some operation delays. However, as the article specifies, this is not always valid, especially in case of a failure and recovery situations.

A total of two hundred tests were performed. Initially, one hundred for both use cases where Manager 2 recognized the ONU, then one hundred more for both use cases where Manager 2 did not recognize the ONU. All the completed tests can be explored in the following sections.

4.2 ONU Discovery Resolution use case

4.2.1 Validation

The test follows the same steps as described previously in the sequence diagram in Figure 3.2. When Manager 1 has the indication that a new ONU has been found, it queries Manager 2 with the information from that ONU. In this case, regarding the ONU 1, Manager 2 will recognize and reply positively to Manager 1. However, Manager 2 will not be able to identify ONU 2, and it will give a negative response.

While the ICTPManagers are running, whenever a change in the OLT's ONU table occurs, the Managers get notified by the corresponding OLT, via an *ICTPOnuTableChanged* message. For testing purposes, two ONUs known to OLT 1 were unregistered one at a time: one that would be recognized by OLT 2 because it was previously registered in it, and another that would not.

First, it was tested the ONU that is recognized by Manager 2. When it is detected, Manager 1 sends an *ICTPOnuAuthenticationRequest* message to Manager 2, that subsequently tries to match the received ONU's Serial Number with an ONU known by it. This is done by searching all the 128 positions in a table of known ONUs in the corresponding slot. When a SN matches, it replies positively to Manager 1. The received messages' information can be seen below in Figure 4.5.

```
[Handler] ICTPOnuTableChanged Received:
slotId = 17
linkId = 0
onuId = 126
serial = 5054494e:91163473
```

```
[Handler] ICTPOnuAuthenticationRequest Received:
slotId = 17
linkId = 0
onuId = 126
serial = 5054494e:91163473
 An ONU with the same SN has been found!
```

Figure 4.5: New ONU detected that is recognized by the other Manager. Manager 1 is on the left, Manager 2 is on the right

When Manager 2 does not recognize the ONU, the process is the same, but the last reply of Manager 2 is negative. This case is shown in Figure 4.6 below, only differing from Figure 4.5 on the print of Manager 2 when it recognizes the ONU.

```
 [Handler] ICTPOnuTableChanged Received:
slotId = 17
linkId = 0
onuId = 127
serial = 5054494e:91163471
```

```
[Handler] ICTPOnuAuthenticationRequest Received:
slotId = 17
linkId = 0
onuId = 127
serial = 5054494e:91163471
```

Figure 4.6: New ONU detected that is not recognized by the other Manager. Manager 1 is on the left, Manager 2 is on the right

Even though the use case is logically correct and does what it is expected of it, there is still no guarantee that it would work in a real scenario. For example, the time it takes to perform an operation can be quite time consuming. As a result, it is crucial to perform some tests on the time it takes to complete, at least, the most important processes. This is analysed in the next section.

4.2.2 Results

The results can be extremely different depending on whether Manager 2 recognizes or not the ONU. For this reason, this results section will first present the tests for the case where Manager 2 knows the ONU, and then for when it does not.

For the first case where Manager 2 always recognizes the ONU from Manager 1, the relevant tests that could be performed were:

1. Time between Manager 1 receiving the indication *ICTPOnuTableChanged* from the OLT and sending the indication *ICTPOnuAuthenticationRequest* to Manager 2;

2. Time between the arrival of the indication *ICTPOnuAuthenticationRequest* in Manager 2, checking the SN from the ONU and matching that SN, and replying to Manager 1 with the indication *ICTPReply*;

3. Overall time since Manager 1's reception of the indication *ICTPOnuTableChanged* from the OLT, to the received reply *ICTPReply* from Manager 2.

For the second case where Manager 2 does not recognize the ONU from Manager 1, the tests were practically the same, with the difference of the test number two, where Manager 2 never matches the received SN.

From one hundred tests, most of the data was consistent, with a few outliers. The tests can be analyzed in Figure 4.7.

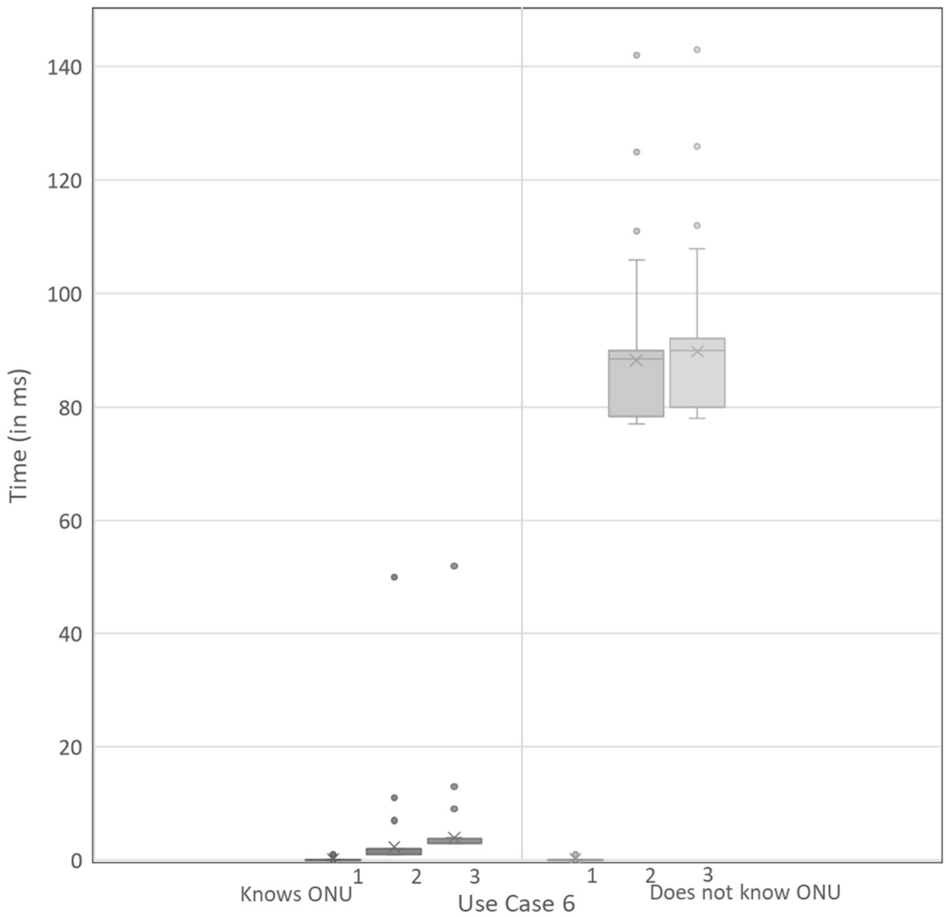


Figure 4.7: Chart of results from tests of use case 6

The table Table 4.1 below specifies the averages of the graph above, in ms.

Knows ONU – Average (ms)			Does not know ONU - Average (ms)		
1	2	3	1	2	3
0.14	2.34	3.97	0.19	88.20	89.77

Table 4.1: Averages of results from tests of use case 6

In Test 1, the time measured was between the receipt of the information of the ONU and the delivery of that new indication. The only operation in between the two was the copy of the information and the creation of a new indication. It was expected to take almost no time to go through this process, hence, with the average of 0.14 ms for the first case and 0.19 ms for the second, the delays are in line with the expectations.

Test 2 measures the time from the arrival of the indication from the other Manager to the reply. The operation done in between was the sweep of the known ONUs table to the Manager and comparison of their Serial Numbers. Test 2 was performed with a ONU whose SN was in that table for the first case. In the second case, an unknown ONU was used. It was anticipated that the time measurements from the second case would be far greater than the other case since the Manager has to conduct 128 failed comparisons. Furthermore, in case one, the registered ONU was always in the same position of the table, the second position.

The second Test shows a higher variability, with some recorded delays much higher than the average of 2.34 ms for the first case and 88.20 ms for the second one. The highest value in case one was 50 ms, while the highest for case two was 142 ms. With a quick look through the list of values and considering that each test was around three minutes apart, it could be that these peaks occurred in a moment of lag from either the system or the network connection used to access the system and deploy the tests. However, the average was still too high considering the 50 ms mentioned before.

Test 3 was a combination of the two previous tests with the addition of the time from sending an indication to receiving it between machines. Since the averages were 3.97 ms in case one and 89.77 ms in case two and, subtracting the values of the previous test with these, it is safe to say that all the indications performed from one machine to the other took around 1.50 ms.

In the second case of the Test 3 where Manager 2 does not know the ONU, the results seem slightly high, even for the worst case. Compared to the previously mentioned value of 50 ms per operation, the second case greatly surpasses it. This is something that can and should be improved. Even for the first case, if the known ONU were in one of the last positions, the delay should be substantially close to the second case, and this is worrisome. Since the search implemented is linear, this could be a point of improvement, and a binary search, or a quicker search algorithm, could be used instead. However, this could mean that the data must be sorted, and a ONU's SN is slightly more intensive to sort than, for example, the ONU's ID. These times could absolutely be improved with a better ONU information storing system or a faster and more efficient search algorithm.

4.3 SN and Assigned ONU-ID Consistency Verification use case

4.3.1 Validation

The test follows the same steps as the use case's sequence diagram in Figure 3.3. When Manager 1 receives the indication of a known ONU going online, it queries Manager 2 with the ONU's information. In this case, Manager 2 will find that ONU 1's SN is not unique because it will recognize it, and ONU 2 will be unique and consistent.

While the ICTPManagers are running, when a recognized ONU becomes online, the Managers get notified by the corresponding OLT, via an *ICTPOnuOnline* message. For testing purposes, two ONUs known to OLT 1 were unregistered one at a time: one that would be recognized by OLT 2 because it was previously registered in it, and another that would not.

First, ONU 1 was tested. When it is detected, Manager 1 sends an *ICTPPrmNotify* message to Manager 2 that first checks for the ONU's SN uniqueness by searching all 128 positions in the table of known ONUs in the corresponding slot. Then, Manager 2 searches the ONU-ID consistency by checking if the ONU-ID has an associated SN. If it discovers any inconsistency, it replies negatively to Manager 1. The received message's information can be seen below in Figure 4.8.

```
 [Handler] ICTPOnuOnline Received:
slotId = 17
linkId = 0
onuId = 20
serial = 5054494e:91163473
```

```
[Handler] ICTPPrmNotify Received:
slotId = 17
linkId = 0
onuId = 20
serial = 5054494e:91163473
 An ONU with the same SN has been found in position 1!
```

Figure 4.8: ONU online which SN is recognized by the other Manager. Manager 1 is on the left, Manager 2 is on the right

When Manager 2 does not recognize the SN nor the ONU-ID is associated with other SN, the process is the same, but the last reply of Manager 2 is positive, since this proves that the

SN is unique and the ONU-ID is consistent. This case is shown in Figure 4.9 below, only differing from Figure 4.8 on the print of Manager 2 when it recognizes the SN.

```
[Handler] ICTPOnuOnline Received:
slotId = 17
linkId = 0
onuId = 10
serial = 5054494e:91163471
```

```
[Handler] ICTPPrmNotify Received:
slotId = 17
linkId = 0
onuId = 10
serial = 5054494e:91163471
```

Figure 4.9: ONU online which SN is not recognized by the other Manager nor the ONU-ID is associated. Manager 1 is on the left, Manager 2 is on the right

The use case works as expected, but, since there is no guarantee that it would work in a real scenario, it is essential to perform some tests on the delays that would take to complete, at least, the most important processes. This is analysed in the next section.

4.3.2 Results

The results can be different depending on whether the SN uniqueness or ONU-ID consistency tests fail. Only two scenarios were tested: when the SN was not unique, and when the SN was unique. The ONU-ID consistency was chosen not to be tested because it involved learning additional parts of the system and there was lack of time for that. Due to this, the ONU-ID consistency did not change during the tests, but it was checked, nonetheless. For this reason, this section will first present the tests for the case where Manager 2 recognizes the SN, and then for when it does not.

For the first case, where Manager 2 always recognizes the SN from Manager 1's ONU, the relevant tests that could be performed were:

1. Time between Manager 1 receiving the indication *ICTPOnuOnline* from the OLT and sending the indication *ICTPPrmNotify* to Manager 2;
2. Time between the arrival of the indication *ICTPPrmNotify* in Manager 2, checking the SN from the ONU and matching that SN, checking the ONU-ID consistency, and replying to Manager 1 with the indication *ICTPReply*;

3. Overall time since Manager 1's reception of the indication *ICTPOnuOnline* from the OLT, to the received reply *ICTPReply* from Manager 2.

For the second case where Manager 2 does not recognize the SN from Manager 1's ONU, the tests were practically the same, with the difference of the test number two, where Manager 2 never matches the received SN.

From one hundred tests, most of the data was consistent, with a few outliers. The tests can be analyzed below in Figure 4.10.

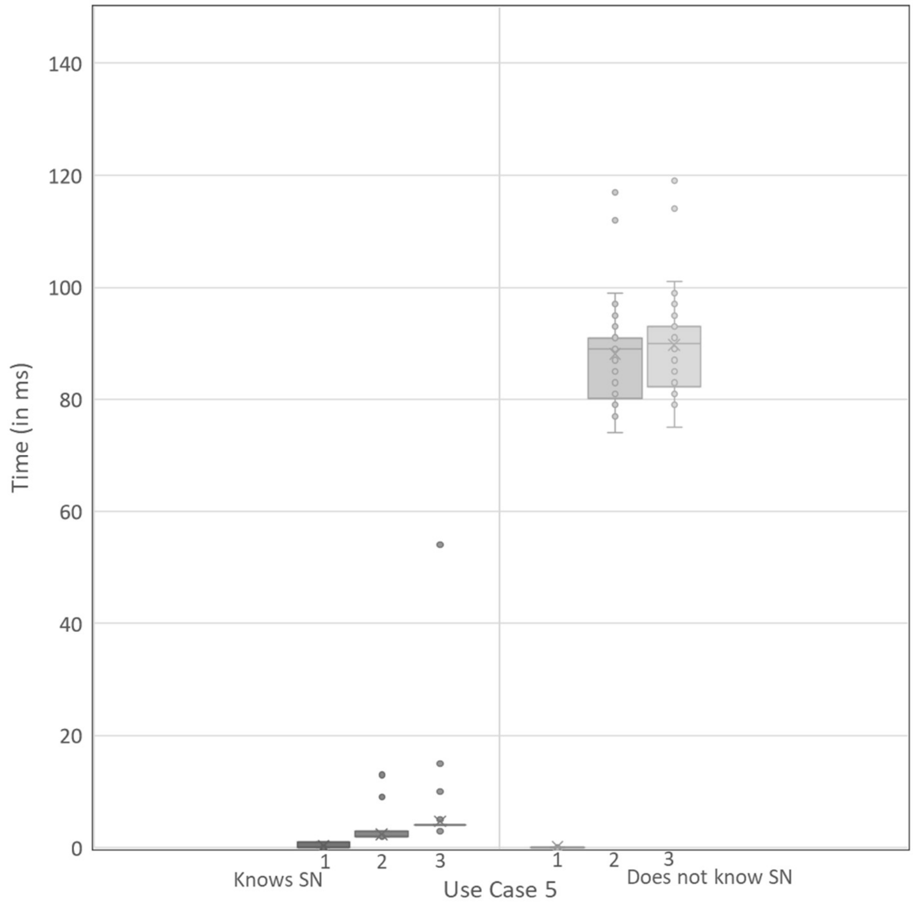


Figure 4.10: Chart of results from tests of use case 5

The table Table 4.2 below specifies the averages of the graph above, in ms.

Knows SN – Average (ms)			Does not know SN - Average (ms)		
1	2	3	1	2	3
0.30	2.43	4.73	0.22	88.11	89.73

Table 4.2: Averages of results from tests of use case 5

These results are very similar to the ones of the use case 6. This is almost certainly because the computational effort resembles the one of the previous use case.

In Test 1, the time measured was between the receipt of the information of the ONU and the delivery of that new indication. The only operation in between the two was the copy of the information and the creation of a new indication. It was expected to take almost no time to go through this process, so, with the average of 0.3 ms for the first case and 0.22 ms for the second, the times were very appropriate, precise, and expected.

Test 2 measures the time between the arrival of the indication from the other Manager and the reply. During this period, a sweep of the ONUs table to the Manager is performed to compare their Serial Numbers and check the ONU-ID's assigned Serial Number. Test 2 was performed with a ONU SN that was in that table for the first case, but not for the second case. Again, it was anticipated that the time measurements from the second case would be far greater since the Manager has to make 128 failed comparisons. Furthermore, in case one, the registered ONU was once more always in the same position of the table, the second position. By contrast, in the second use case the best outcome (SN uniqueness and ONU-ID consistency) is actually the most exhaustive, since the SN should not be found in any of the 128 positions.

The second Test shows variable latency measurements in both cases, with values much greater than the average of 2.43 ms for the first case and 88.11 ms for the second one. These average delays resemble the last use case 6. The highest value in case one was 13 ms, while the highest for case two was 117 ms. These outliers were smaller in these results, but it is probably for the same reason as the ones from the previous use case: they occurred in a moment of lag from either the system or the network connection used to access the system and deploy the tests.

Test 3 was a combination of the two previous tests with the addition of the delay from sending an indication to receiving it between machines. Since the averages were 4.73 ms in case one and 89.73 ms in case two, and subtracting the values of the previous test with these, it is safe to say that all the indications performed from one machine to the other took around 1.75 ms, which seems acceptable. This test had a big spike for case one where the Manager 2 recognizes the SN. Since there was only one of 54 ms, it is easily excused as another of the lag spikes from before.

In the second case of the Test 3 where Manager 2 does not know the SN, the results seem, again, unsurprisingly high. In the second case, which is the case of success for this use case since it shows that the SN is unique and the ONU-ID is consistent, the delays are too high, especially compared to the norm of 50 ms. Again, the search implemented could be improved to a quicker search algorithm. However, for this case, it seems like a simple option to search by SN would greatly and effortlessly enhance the results times.

5 Conclusions and future work

5.1 Conclusions

This dissertation aimed to implement the Inter-Channel-Termination Protocol (ICTP) in a pre-built system that supported previous PON standards. Two use cases from ICTP were implemented and validated in a realistic scenario. Based on the obtained results, we conclude that it is possible to reliably implement these use cases in a real scenario. However, these contain some delays that need to be reviewed, since they passed the 50 ms mark by a few milliseconds [30].

Some of the norms made by The Broadband Forum were not fulfilled in the development of the use case, such as the communication between Managers (the use of TCP was changed to UDP) and the message structure, mainly to simplify and hasten the process of the development.

Although the use cases worked as expected and, in the performed tests, did not fail, the results could have been better. The results from use case six were adequate for the first case where the second Manager knew the ONU, but only because its position in the table of the known ONUs was in the beginning. For the second case where the Manager did not recognize the ONU, the results were not acceptable, even for the worst case scenario. This can and should be revised, so that the delays are more suitable for this kind of operation.

The results from use case five were very similar to the one that was previously done. In this use case, the delays were even more worrisome, since the greatest delay belonged to the scenario that would be considered positive, meaning that the ONU's Serial Number was unique, and that its ONU-ID was consistent. These values were too far from the standard of 50 ms and should be considered one priority for improvement.

5.2 Future Work

The completion of the use cases is fundamental to progress with the study of ICTP. Since the situation of multi-operators is important in the perspective of ICTP, all use cases should be supported. Furthermore, since some of the standards like the message structure and communication protocol were modified, this ought to be changed to fit the specification accurately, or else the multi-operator environment would be impossible.

Further tests should be done, at least a thousand. These were very time consuming, and that is the reason no more were done at the time. This is important to check if the use case implementations were in fact correct, and that no fault would occur. Also, it could confirm that the high values were indeed due to lag in the network or system.

Depending on the use case, other types of tests could have been done, like the time of loss of signal, or the down time of an ONU changing channels. However, the use cases needed to involve that sort of operation, which the numbers 5 and 6 did not.

Finally, it would be extremely vital to significantly lower the delays that were greater than 50 ms.

References

[1] CERN, “The birth of the Web,” [Online]. Available: https://www.home.cern/science/computing/birth-web. [Accessed 27 9 2019].

[2] Internet Live Stats, “Internet Users,” [Online]. Available: https://www.internetlivestats.com/internet-users. [Accessed 27 9 2019].

[3] Worldometers, “Current World Population,” [Online]. Available: https://www.worldometers.info/world-population/. [Accessed 27 9 2019].

[4] M. Meeker, “Internet Trends 2018,” 2018. [Online]. Available: https://relayto.com/cdn/media/files/JzrE69rBRKm9NhkUM2Fk_internettrendsreport2018.pdf.

[5] Cisco, “Cisco Visual Networking Index: Forecast and Trends, 2017-2022,” 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf.

[6] S. Bindhaiq, A. S. M. Supa'at, N. Zulkifli, A. B. Mohammad, R. Q. Shaddad, M. A. Elmagzoub and A. Faisal, “Recent development on time and wavelength-division multiplexed passive optical network (TWDM-PON) for next-generation passive optical network stage 2 (NG-PON2),” *Optical Switching and Networking,* vol. 15, pp. 53-66, 2015.

[7] A. O. Edevbie and O. F. Opeyemi, “Comparative Analysis of GPON and DSL Access Technologies for Enhancing Broadband Internet Penetration in Nigeria,” *International Journal of Applied Information Systems (IJAIS),* vol. 10, no. 8, pp. 16-21, 2016.

[8] J. R. Stern, J. W. Ballance, D. W. Faulkner, S. Hornung, D. B. Payne and K. Oakley, “Passive Optical Local Network for Telephony Applications and Beyond,” *Electronics Letters,* vol. 23, no. 24, pp. 1255-1256, 1987.

[9] G. Keiser, FTTX Concepts and Applications, New Jersey: John Wiley & Sons Ltd., 2006.

[10] C. H. Lee, W. V. Sorin and B. Y. Kim, "Fiber to the Home Using a PON Infrastructure," *Journal of lightwave technology,* vol. 24, no. 12, pp. 4568-4583, 2006.

[11] F. Effenberger, D. Clearly, O. Haran, G. Kramer, R. Li, M. Oron and T. Pfeiffer, "An introduction to PON technologies [Topics in Optical Communications]," *IEEE Communications Magazine,* vol. 45, no. 3, pp. S17-S25, 2007.

[12] L. G. Kazovsky, N. Cheng, W. T. Shaw, D. Gutierrez and S. W. Wong, Broadband Optical Access Networks, England: Wiley, 2011.

[13] M. Kumari, R. Sharma and A. Sheetal, "Passive Optical Network Evolution to Next Generation Passive Optical Network: A Review," *2018 6th Edition of International Conference on Wireless Networks & Embedded Systems (WECON),* pp. 102-107, 16 Nov. 2018.

[14] C. F. Lam, Passive Optical Networks: Principles and Practice, Elsevier, 2007.

[15] Epik Networks, "FTTX Explained - FTTN vs FTTC vs FTTB," 24 August 2019. [Online]. Available: https://www.epiknetworks.com/blog/fttn-fttb-fttc-fttx-explained/. [Accessed 10 October 2019].

[16] D. P. Shea and J. E. Mitchell, "Long-Reach Optical Access Technologies," *IEEE Network,* vol. 21, no. 5, pp. 5-11, 2007.

[17] M. Cen, "Study on Supervision of Wavelength Division Multiplexing Passive Optical Network Systems," 2011.

[18] Fiber Optic Telecom Co., Ltd, "Wavelength Division Multiplexing (WDM) Optical Fiber Technology," 7 May 2018. [Online]. Available: https://www.fiberoptictel.com/wavelength-division-multiplexing-wdm-optical-fiber-technology/. [Accessed 18 October 2019].

[19] Y. Luo, X. Zhou, F. Effenberger, X. Yan, G. Peng, Y. Qian and Y. Ma, "Time- and Wavelength-Division Multiplexed Passive Optical Network (TWDM-PON) for Next-Generation PON Stage 2 (NG-PON2)," *Journal of Lightwave Technology,* vol. 31, no. 4, pp. 587-593, 2013.

[20] ITU-T, "Recommendation G.983.1, Broadband optical access systems based on Passive Optical Networks (PON)," 2005.

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

[22] ITU-T, “Recommendation G.983.3, A broadband optical access system with increased service capability by wavelength allocation,” 2001.

[23] H. Alobaidan, “Current and Future FTTH Technologies,” *Journal of Wireless Networking and Communications,* vol. 7, no. 2, pp. 35-40, 2017.

[24] G. Kramer and G. P. Biswanath Mukherjeee, “Ethernet PON (ePON): Design and Analysis of an Optical Access Network,” *Photonic Network Communications,* vol. 3, no. 3, pp. 307-319, 2001.

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

[26] D. Nesset, “NG-PON2 Technology and Standards,” *Journal of Lightwave Technology,* vol. 33, no. 5, pp. 1136-1143, 2015.

[27] ITU-T, “Recommendation G.989.1, 40-Gigabit-capable passive optical networks (NG-PON2): General requirements,” 2013.

[28] ITU-T, “Recommendation G.989.3, 40-Gigabit-capable passive optical networks (NG-PON2): Transmission convergence layer specification, Amendment 2,” 2018.

[29] The Broadband Forum, “TR-352, Multi-wavelength PON Inter-Channel-Termination Protocol (ICTP) Specification,” 2017.

[30] L. Florit, “Putting 50-ms In Perspective,” Cisco, 2010.