CPON
Wired

February 2023

CableLabs®

Overview of Coherent PON Protection

Prepared by
Haipeng Zhang, Lead Architect, Wired R&D | h.zhang@cablelabs.com
Steve Jia, Distinguished Technologist, Wired R&D | s.jia@cablelabs.com
Alberto Campos, Fellow, Next-Gen Systems | a.campos@cablelabs.com
Matthew Schmitt, Principal Architect, Wired R&D | m.schmitt@cablelabs.com
Curtis Knittle, Vice President, Wired R&D | c.knittle@cablelabs.com

Executive Summary

Over the past decade, insatiable appetite for higher capacities in access network continues to exceed the capacity of the currently installed system. This trend has been driven by the continuous growth of data-intensive applications such as 5G xhaul, HD video streaming, cloud services, and the Internet of Things (IoT). Today, passive optical network (PON) technology based on power splitting is considered a cost-effective solution and has become one of the dominant architectures for meeting the everlasting growth in capacity demand. As the PON data rate evolves towards 100 Gbps or higher, technologies based on intensity modulation–direct detection (IM-DD) have been pushed to their limit because of limited receiver sensitivity and dispersion constraint. On the other hand, coherent optical technology is considered to be a future-proof solution for next-generation 100 Gbps single-wavelength PON because of its superior performance and vast potentials in terms of scalability, high sensitivity, and powerful digital equalization capabilities.

As more and more traffic and bandwidth will be carried by high-performance PONs, especially next-generation coherent PON (CPON), ensuring reliable and robust connectivity will become even more critical for network operators. New applications in remote health monitoring, telerobotic surgery, autonomous cars, home security, and other fields require uninterrupted access service for the end user. Although there are many existing optical protection and recovery architectures in the backbone and in metro networks, current cable optical access networks generally lack these approaches.

In this paper, we will discuss PON protection and redundancy designs and propose protection schemes for both traditional PON and emerging CPON.

1. PON Availability Evaluation

Reliability is the probability of a system or service lasting a defined period “t” without failures. Lasting without failures means to operate, perform, or function within acceptable levels. Even though they are both related in PON, it is worth distinguishing between service reliability and network reliability. In today’s world, PON encompasses a plethora of services and applications. Service reliability is used to measure how well services or applications are delivered. Each of these services or applications has its own criteria of what is acceptable and what is defined as a failure. For example, the acceptability criteria for web-browsing services are very different from the criteria for gaming, video streaming, or cellular backhaul. Because PON may carry all these services concurrently, we need to simultaneously meet the performance demands for all these services.

Although the term “reliability” is used extensively, the metric usually referred to by the industry is availability. Reliability and availability are related, but there is a subtle difference—availability is defined as the fraction of time that a system or service behaves as intended, meaning the percent of time it is available. The reliability of a PON is usually evaluated by its availability. Availability of a PON system depends on two parameters: mean time between failures (MTBF), which indicates how frequently failures occur, and mean time to restore or repair (MTTR), which indicates how soon service is restored. Failure in time (FIT), the failure frequency in 10^9 hours, is inversely proportional to MTBF: FIT = 10^9/MTBF. For a given system, availability is calculated by $\boldsymbol{A = 1 - \sum_i^N MTTR_i/(MTBF_i + MTTR_i)}$. A goal of the industry is to achieve 99.999% availability for businesses and services that require high availability, which is equivalent to a system being unavailable for less than 5 minutes and 15 seconds in a year.

Table 1 shows statistical failure rates and mean repair time for PON components based on the literature.[1] Based on these parameters, an unprotected PON with an 80-km fiber link can only have an availability of 99.958%, far from the industry goal of 99.999%.

[1] “Passive Optical Network Protection Considerations,” June 2017, ITU-T, Series G, Supplement 51

Table 1. Failure Rates and Repair Time for PON Components

Component	FIT	MTTR
OLT	2,500	4 hr
ONU	256	24 hr
Feeder fiber	80 km: 200/km	14 hr
Drop fiber	2 km: 200/km	14 hr
Splitter	200	12 hr

By adding redundancy to the critical components of a PON, such as the feeder fiber and OLT (optical line terminal), the MTTR of these components can be significantly reduced from several hours down to minutes. For example, with OLT and feeder fiber protection, assuming an MTTR of both components be around 1 minute, the network can reach 99.9987% availability. Furthermore, if ONU (optical network unit) and drop fiber redundancy is added to the system along with the OLT and feeder fiber protection, and with a 1-minute MTTR for the ONU and drop fiber, the system availability can reach 99.9999%.

2. Network Protection Design Examples

As PON data rates evolve toward 100 Gbps per wavelength, more and more traffic and bandwidth will be carried by the network, giving unprecedented importance to the protection of key components. In a PON system, failure of any key network components—including fiber cuts or failure in the OLT, ONU, power splitter, or optical amplifier (if employed)—will interrupt the service significantly. In a next-generation PON system with large link budgets, a very large number of subscribers or business/mobile backhaul services could be affected. This makes PON protection highly desirable.

Two network protection schemes based on 1:N OLT configuration are shown in Figure 1. In this design, there are N OLTs in the same central office, or in proximity, with each OLT supporting a PON network. An extra OLT device designated as the protection OLT provides redundancy and protection to all of the N OLTs. The protection OLT is connected to all the PON networks via a 1×N optical switch and N optical splitters (2×1 configuration). The protection OLT is also connected to the other OLT devices via separate OLT interconnects. This design mainly provides redundancy and protection to the OLTs. Initially, the protection OLT is configured for all the PON networks it potentially supports. Under normal operation, when the 1×N optical switch is closed, each OLT device is only supporting the corresponding PON network. When one of the OLTs detects a malfunction, this OLT stops transmitting downstream traffic and sends a protection switching message to the protection OLT. The protection OLT is then configured to support the corresponding PON network and sends a switching message to the 1×N switch. The 1×N switch opens the corresponding port, after which the protection OLT transmits downstream traffic to the PON network. The settings of the ONUs can also be stored in a controller working with the protection OLT. In this case, the protection OLT does not have to learn the settings of the new set of ONUs that it is serving through a lengthy initialization and ranging process. If a link fails, the specific settings can be passed along to the protection OLT. In a highly integrated system where multiple OLTs are integrated together, the OLT transmitter functionality could be decoupled from the OLT processing functionality, making the redundancy scheme presented here more seamless.

Figure 1A shows the addition of 1+1 redundancy links in each of the PON networks to protect the feeder fiber links. The protection OLT is connected to each PON network via a 1×N optical switch and a corresponding 2×1 passive optical splitter. Switching between the primary and the backup links is done by the 2×1 optical switches. The operating process is similar to the 1:N configuration but has the additional protection of sending a switching message to the 2×1 optical switch. Similarly, Figure 1B shows a 1:1 feeder fiber protection design combined with the 1:N OLT protection. In addition to the 1:N design that protects the OLT devices, 1:1 redundancy links in each of the PON networks are added to protect the feeder fiber links. The protection OLT is connected to each PON network via a 1×N optical switch and a corresponding 2×2 optical switch. The operating process is similar to the 1:N configuration but has the additional protection of sending a switching message to the 2×2 optical switch.

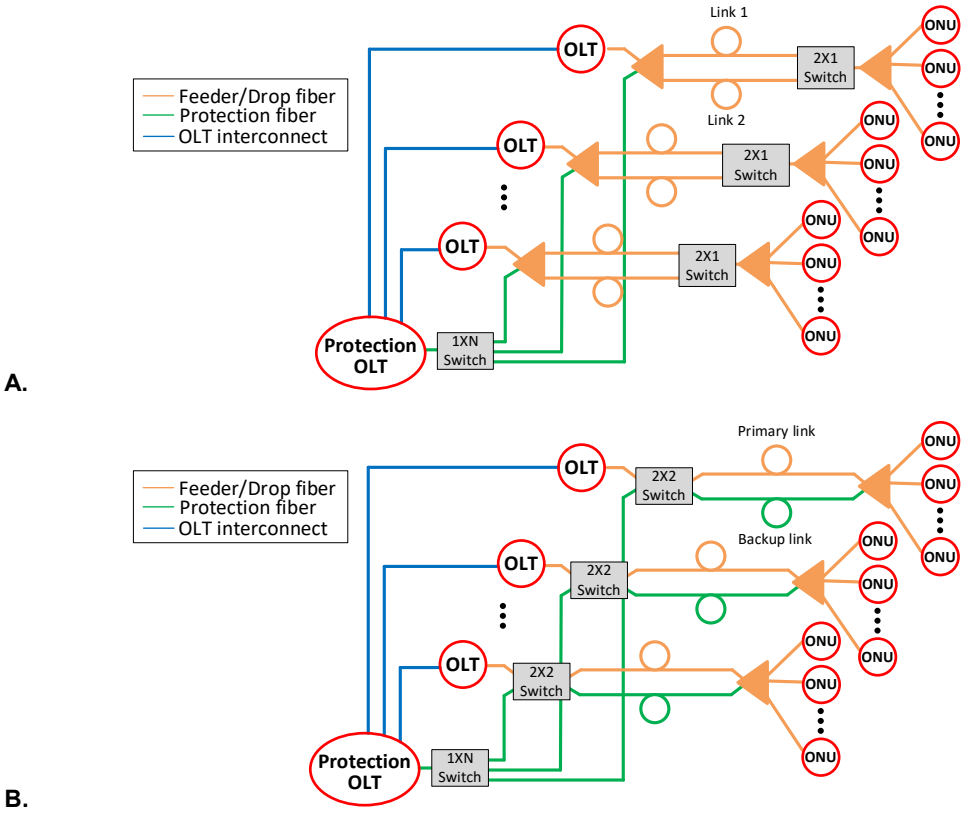

Figure 1. Example of PON Protection Architecture: 1:N OLT Protection: A, Combined with 1+1 Feeder Fiber Protection; B, Combined with 1:1 Feeder Fiber Protection

Figure 2 shows a PON protection scheme where two adjacent OLTs can be connected through a 1×2 passive splitter and an M×N optical switch to provide redundancy to each other. When one of the OLTs detects a malfunction, this OLT stops transmitting downstream traffic and sends a protection switching message to the M×N switch and its neighboring OLT. The switch and the neighboring OLT are then configured to support operation of both PON networks. A 1:1 configuration in the feeder fiber link provides redundancy, where both primary and backup feeder fiber links are connected to the output of the M×N optical switch. Switching between the primary and backup feeder fiber links can be realized by controlling the M×N optical switch.

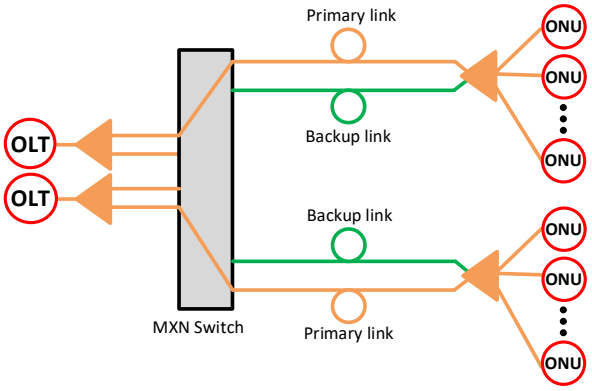

Figure 2. Example of PON Protection Architecture: Mutual Protection Between Two Adjacent OLTs Combined with 1:1 Feeder Fiber Protection

Overview of Coherent PON Protection

Leveraging the wavelength tunability of coherent optics, adjacent PON networks can provide mutual protection to each other by connecting the passive splitter node, as shown in Figure 3. Although only two OLT devices are shown, the design principle can be applied to use cases with multiple OLT devices. Under normal operation, the two coherent PON networks work at different wavelengths, i.e., λ1/λ2 for PON network 1 and λ3/λ4 for PON network 2. After the fiber links, on the other side of the ODN (optical distribution network), two optical splitters with 2×(N+1) configuration are adopted; here, N represents the number of ONUs in each optical link. Normal PON fiber links are shown in orange, and protection fiber links are shown in green. Compared with standard optical splitters in a PON network, which usually have 1×N configurations, the extra input and output ports on the optical splitters allow extra network protection by connecting two adjacent splitter nodes. It is also noted that the extra output can be regular output of one of the ONUs. Under normal operation, the downstream signal from OLT1 at wavelength λ1 is sent to coherent ONUs whose local oscillators are tuned to λ1 to receive the downstream signal and also to transmit the upstream signal at λ2 to OLT1. Similarly, the downstream signal from OLT2 at wavelength λ3 is received by ONUs with local oscillators (LOs) tuned to λ3, and the upstream signal at λ4 is received by OLT2. The redundant downstream signal at wavelength λ1 is split by the first 2X(N+1) splitter and sent to the second 2X(N+1) splitter. However, under normal operation, the ONUs tuned to λ3 do not receive signals at wavelength λ1. Similarly, the redundancy upstream signal at wavelength λ2 is also sent to OLT2 through the second splitter but is not detected because OLT2 is only receiving wavelength λ4. In addition, the redundancy upstream and downstream signals at wavelength λ3 and λ4 are also sent to OLT1 and ONUs that are tuned to λ1 and λ2, respectively. Depending on the power level of the redundancy signal and the link power budget, optical amplifiers are optional and can be added to the redundancy link if needed. It is also important that three phases—parameter learning, serial number acquisition, and ranging in the activation process—are implemented in the initial learning parameter phase for both PON systems. Each OLT should store the information of both normal link ONUs and protection link ONUs with the wavelength as the identifier, and all the ONUs in this protection domain should acquire the necessary operational parameters for upstream transmission in this phase as well. For more details on PON protection, refer to ITU-T G Supplement 51[1] and IEEE Std 1904.1, Clause 9.[2]

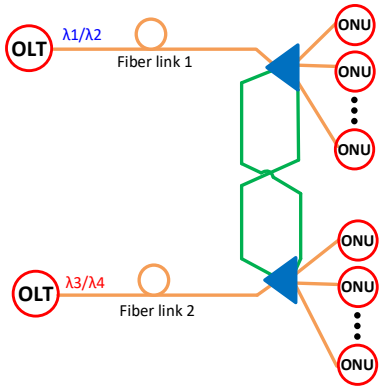

Figure 3. Example of PON Protection Architecture: Mutual Protection Between Two Adjacent Coherent PON Networks by Connecting the Passive Splitter Node

The advantage of coherent transceivers is that the wavelengths of both transmitters and LOs can be adjusted. When ODN or OLT device breakage occurs, i.e., fiber link 1 is down, a backup downstream signal is sent by the other OLT and the upstream transmission wavelength is changed accordingly. When fiber link 1 is down, downstream and upstream signals at wavelengths λ1/λ2 are no longer available, so the network is operating at wavelengths λ3/λ4. All the ONUs previously operating at λ1/λ2 are now switched to λ3/λ4. OLT2, which is running at λ3/λ4, now provides downstream signals and receives upstream signals from all the ONUs. The number of ONUs that can be protected is dependent on the optical power budget for each OLT link. The asymmetric optical splitter or combiner can be used to provide different splitting power levels for protecting ports. The optical amplifier can be also inserted to enhance the power budget of the protection link in certain cases.

[2] "IEEE Standard for Service Interoperability in Ethernet Passive Optical Networks (SIEPON)," IEEE, Standard 1904.1-2017

APPENDIX A Acknowledgements

CableLabs would like to thank the participants of the CPON Working Group, representing the following companies.

ADVA
Antronix
Broadcom
Calix
Charter Communications
Ciena
CIG Tech
Cisco
Cogeco
Comcast
CommScope
Cox Communications
GCI
Hisense
Huber+Suhner
Infinera
Izzi Telecom
Liberty Global
Macom
Marvell
Mediacom
Midco
NEL-America
Rogers
SCTE
Shaw Communications
Sparklight
TiBiT Communications
Vecima Networks
Group Videotron
Vodafone Group