2006-2007
Optical networks

RESILIENCE IN ACCESS NETWORKS

Eduardo Garín
Alex Juanicotena
Andrés Navarro

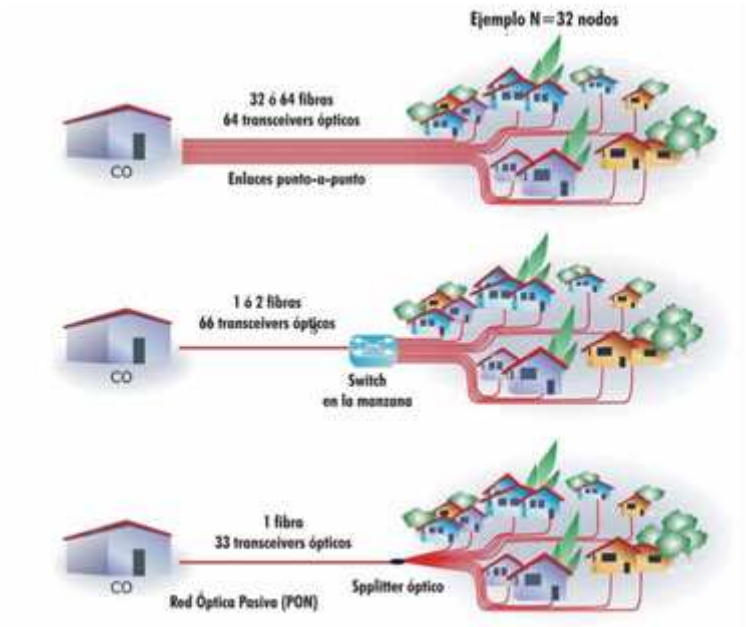
RESILIENCE IN ACCESS NETWORKS

1 INTRODUCTION

The earliest example of resilience in optical networks was in the choice of beacon sites so that news of an invasion could be rapidly spread across the country even if one site was unable to **transmit** the message. Current telecommunication networks now make extensive use of optical transmission media for data transport. Network security generally uses reconfigurable electrical components, with fully duplicated optical **links.** For this project, we are going to focus on the access networks and the possible protection schemes so they are resilient in case of failures.

Nowadays, access networks are mostly based on Cable and DSL systems. The increasing demand of bandwidth for all the new services available, it is just a matter of time that the companies change their networks to Fibre to the Home. From this point of view, optical fibre technology is a strong solution due to its potential unlimited bandwidth, and the decreasing prices of the lasers. It is just not enough with either DSL or even Cable in order to keep up with the needs of the clients. Things are changing already, and some companies are using fibre for the access networks too, and since they worried about their resilience for the transport part before, they need to worry about this issue for the access part too. What is more, if we think about all the new buildings which must include the pre-wiring then it becomes easier and easier to bring the fibre right to our doors.

Talking about the future architectures, Passive Optical Networks (PON) are a reliable bet: their cost included in the electro-optic equipment and the efficiency for the tree-branch topologies are an appealing choice compared to the traditional point-to-point based topologies..



Arquitectura punto-a-punto vs punto-multipunto con switch en la manzana vs PON

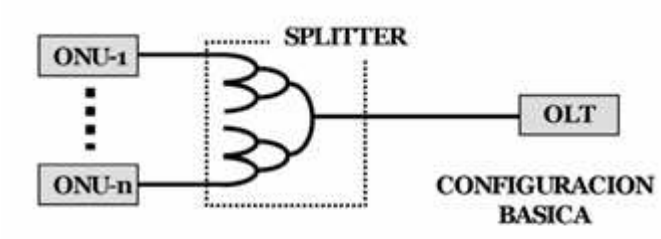
PON architectures are focusing on the telecommunications market as the way to attack the Last-Mile-Problem. The main advantages are:

- PON networks allow us to reach customers up to 20 Km away from the central optical node. This distance is much greater that the DSL maximum distance (about 5 km).
- PON networks minimize the amount of optical fibre needed to reach the customers since it uses tree-like topologies, not like the point-to-point ones used for other Technologies. Besides, this kina of architectures simplify the density of equipment needed in the central node, decreasing therefore the cost.
- PON networks offer a greater bandwidth density per user, due to the higher capacity of the optical fibre.
- The equipment is compatible with the one used for Cable systems, so the costs of installing fibre will not increase this way.
- PON networks make the QoS better, and simplify the maintenance of the network since they are immune to electromagnetic noise, they do not propagate electrical signal coming from thunder storms…
- PON allow us to use higher data rates by using WDM techniques.

Even though PON networks have existed as a concept since the 90's, it has been only in the last few years when they have become a hot topic because of the improvement of the technology required. Now several operators have started to work with this new technology, and it is obviously the next step to build the new networks, once the DSL becomes obsolete.

2 BASIC CONCEPTS

The Basic PON topology consists 3 components: An OLT (Optical Line Termination) which is located at the central optical node (company), the splitter, and the ONU (optical Network Unit). Usually, it is the OLT that interconnects with a transport network which gets the traffic flow coming from several OLT and routes them to the header end. The ONU is located at the customer house, and therefore implementing a FTTH (Fibre To The Home) scheme.



There are several topologies out in the market to implement access networks, including ring topologies (very rare), tree and tree-branch topologies and optical linear bus topologies. The splitting is done by using several 1x2 optical splitters or by using 1xN splitters directly. For this project, the goal is to obtain all the possible protection schemes that can be implemented between the ONU and the OLT so in case a fibre gets cut, the information can keep flowing between both ends.

Another important aspect of PON networks is the fact that all of them use single mode fibre. The downstream channel consists in a point-multipoint network; the OLT manages the whole bandwidth that is shared between the customers dividing it in time slots. The upstream channel, on the other hand, is a point to point network where several ONUs send traffic to a single ONT. Working with single mode fibre, we can use WDM techniques so the wavelengths used for the downstream and upstream direction do not interfere. Most of implementations include two wavelengths, one for each stream. The wavelengths used are normally 1290 nm for the downstream channel and 1310 for the upstream. The evolution in the technology has allowed to minimize the size of the optical filters used for this separation of wavelengths, so they can be integrated within the transceivers located at the user equipment. The wavelengths are from the second window and not the third to reduce cost.

At the same time that PON architectures use TDMA multiplexing techniques to manage the times in which the ONU can send their information (the ONT manages this), the ONT also uses TDMA for the downstream channel.

It is also very important the fact that the power launched from the OLT needs to be different depending of the distances to the different ONU. It will obviously need more power to transmit to a customer 20 km away than to another customer 5 km away. This is solved by the optical transceivers and the electronics needed for this have become simpler, smaller and easier to control the transceiver externally.

DEDICATED PROTECTION

Dedicated protection transmits by both the working and the protection paths. The signal is duplicated in the transmitter node and it is sent to the receiver by both paths.
The optical signal is usually duplicated by passive 50:50 splitters. In the receiver, one of the paths is selected and directed to the node. The receiver may select one path by default and this path is called the working path. When the working path fails the receiver switches to the other path, which is called the protection path. There is another option in which the receiver selects the path with the best quality, in which case the signal quality is measured using the Bit-Error-Rate (BER) or the Signal-to-Noise Ratio (SNR).

Dedicated protection restores service faster than shared protection. The reason is that shared protection needs to communicate both nodes in order to initiate protection switching, and this communication needs additional time. However, the protection resources are always busy and these resources are at least 100% of the protected resources.

Dedicated protection in point to point connections is called as 1+1.

SHARED PROTECTION

Shared protection transmits by only one path: the working path or the protection path. The transmitter and the receiver use the working path by default. When the receiver detects a failure in the working path (by any criterion) it asks the transmitter to switch to the protection path. An automatic Protection Switching (APS) protocol communicates between the transmitter and receiver nodes and its role is to manage the protection switching.

Owing to the need to communicate between the two nodes to perform the protection switching, shared protection is slower then dedicated protection. The communications are managed by the APS protocol. On the other hand, the protection resources are free when the working path carries the transmitted data. The protection path(1) may therefore protect various working paths (N) at the same time. Shared protection is therefore also called “1:N protection”. When one working path is protected by one protection path, N is equal to 1. In that case, the shared protection is called “1:1 protection”.

3 A LITTLE BIT OF HISTORY

APON, BPON y GPON

In 1995 seven telecommunications operators saw the possibility of PON networks and created the Full Service Access Network (FSAN) in order to unify the specifications for broadband in the homes. FSAN includes more than 30 equipment manufacturers.

Members of FSAN Developer a specification called APON for the access networks using optical fibre, and sent this to the ITU. The name was changed to BPON (standing for Broadband PON), meaning the possibility of supporting other standards related to broadband such as Ethernet, VPL, etc…

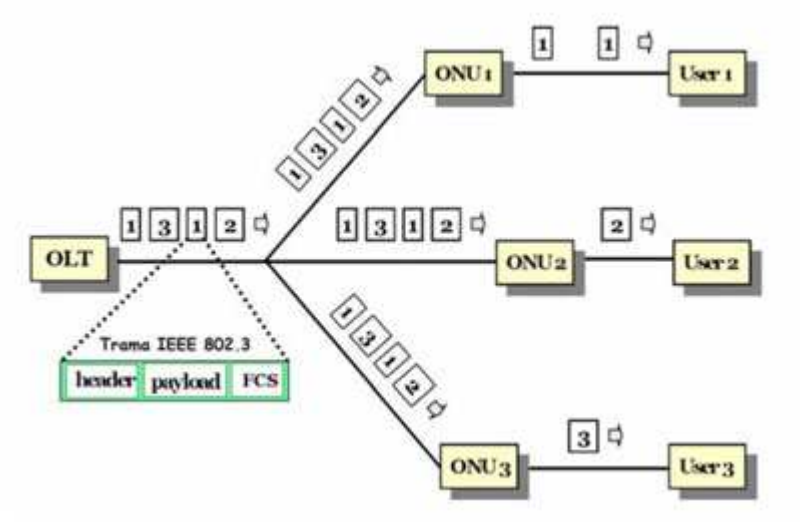
In 1997, FSAN sent the specifications to the ITU, and after seven years, the ITU approved the following standards related to PON networks for broadband.

G.983.1 (general description), G983.2 (management and maintenance layer), G983.3 (QoS for BPON), G983.4 (dynamic bandwidth assignation), G983.5 (protection), G983.6 ONT protection layer), G983.7 (management layer of the dynamic bandwidth)

But BPON is not the last contribution of FSAN to passive optical networks. The increasing demand of bandwidth has forced them to created new standards, such as the G-PON (Gibabit-capable PON) (2003-2004). Three recommendations have been released since then: G.984.1, G984.2 and G.984.3. For our project, these specifications do not include anything new about protection, so we will not use it for our objectives. However, it is important to note that GPON increases even more the interoperability between different manufacturers, allowing to use ONUs and OLTs from different ones.

Ethernet PON, EPON

In January 2001, the IEEE created the new Standard EPON (Ethernet PON). This architecture is different from the last ones because it does not use ATM cells, but Ethernet traffic directly, optimizing the efficiency of IP traffic, and therefore becomes much easier to interconnect different nodes because it does not need SDH architectures for the transport in WANs. But again, this standard does not add anything about the protection schemes.



Costs in the equipment are approximately 10% less than G-PON equivalent equipment.

Finally, the next step seems to be GEPON, a review of the last standard that will include the necessary specifications to use 10 GbE, multiplying by 10 the bandwidth.

4 PROTECTION

When talking about protection, it is relatively easy to find a lot of information for transport networks. Lots of research papers have been published about ring networks, and even bus networks. But when we talk about access networks, things are different. The most important work for this kind of networks and the main disadvantage about this is COST.

Transport networks obviously need to have a lot of protection, basically because if a fibre is cut and there is no other path available for the transmission, then lots of people and business lose the connection and probably a lot of money. Then, it is justified to spend a lot of time and effort to design and implement really efficient and “intelligent” networks that can stand against possible failures, and redirect the traffic to those “extra” paths. It is also justified to spend a lot of money and invest in this kind of topologies. Ring networks are an easy example of how a failure can be managed.

But, the question is: Can we forget about protection in PON networks? The question arises since it seems ridiculous to use so much fibre for only one client. The answer is NO, we cannot forget about protection. Customers are not only neighbourhoods and individual customers. Banks, administration buildings and even hospitals are using FTTH nowadays, and lots of money and even lives are in danger if a fibre gets cut and there is not protection. So these kinds of clients are going to be willing to pay for this kind of service, because they need it! But the fact is that today, costs have decreased a lot, and for new buildings the cost of installing FTTH is not much more expensive than DSL or Cable prices.

There are several ways in which a fibre can get cut. With all the construction work in every city in these days, it is more than likely to have failures in the access networks. What is more, depending on the continent of the world that the network is going to be placed, chances of earthquakes, tornados, and other natural disasters can cause damage and eventually cut the fibres.

Then, now that we know how important is to have protection, we will explain the different schemes available for Passive Optical Networks. We will show the schemes, explain how they work and compare them, looking for the best one depending on the situation. Finally, we will propose two new schemes and then we will give a very brief and basic review of how the logical part of the networks is implemented.

5 PROTECTION IN PON SECTION

From the viewpoint of administration of the access network, the protection architecture of PON is considered to enhance the reliability of the access networks. However, protection shall be considered as an optional mechanism because its implementation increases the cost.

Possible switching types
There are two types of protection switching:
i) automatic switching; and
ii) forced switching.

The first one is triggered by fault detection, such as:

- loss of signal
- loss of frame
- signal degrade (BER becomes worse than the predetermined threshold)

The second one is activated by administrative events, such as fibre rerouting, fibre replacement, etc.

Depending on protection requirements, both switching types should be possible in the PON system. OAM function realizes the switching mechanism, so an information field should be reserved in the OAM frame for the switching mechanism.

Possible duplex GPON configurations and characteristics

There can be several types of duplex PON systems. Each configuration should need diferent specifical control protocol. For example, no switching protocol is required for the OLT/ONU in Figure 4a, since the switching is only applied for the optical fibres. Also, in Figure 4b, no switching protocol is required since the switching is carried out only in the OLT.

Configuration examples

Type A: The first configuration doubles only the optical fibres. In this case, the ONUs and OLT are singular.

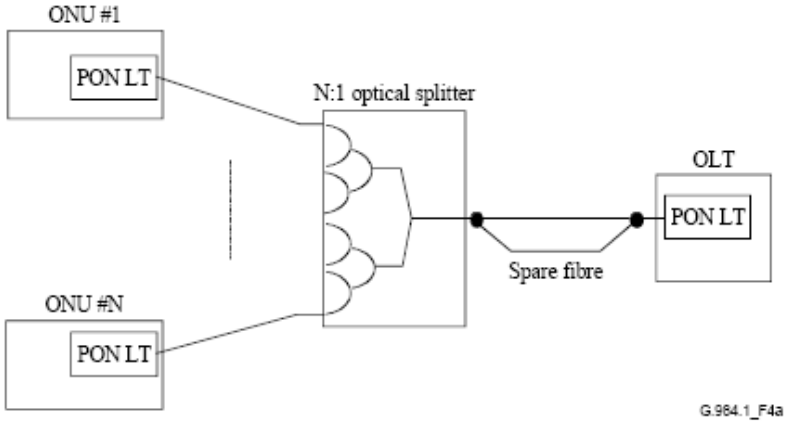


Figure 4a/G.984.1 – Duplex GPON system: Fibre duplex system

Type B: The second configuration doubles the OLTs and the optical fibres between the OLTs and the optical splitter, and the splitter has two input/output ports on the OLT side. This configuration reduces the cost of duplexing the ONUs, although only the OLT side can be recovered.

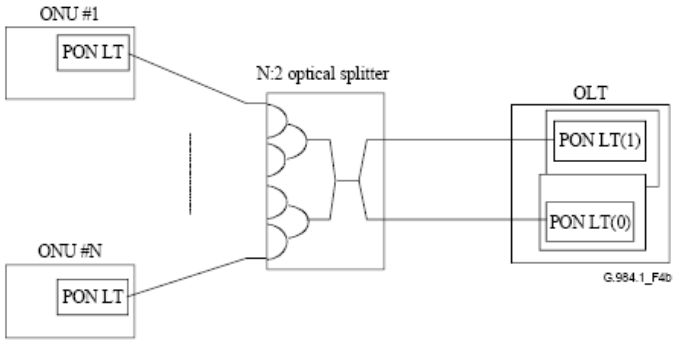


Figure 4b/G.984.1 – Duplex GPON system: OLT-only duplex system

Type C: The third configuration 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 standby facilities. Therefore, the full duplex cost enables a high reliability.

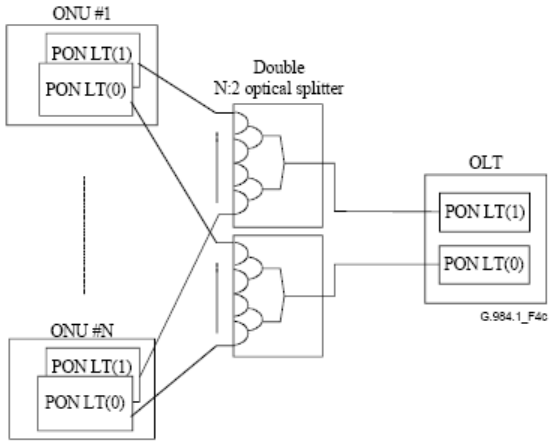


Figure 4c/G.984.1 – Duplex GPON system: Full duplex system

Type D: If the ONUs are installed in the customer buildings, the in-house wiring may or may not be duplexed. Additionally, if each ONU is owned by a different user, the reliability requirement depends on each user and only a limited number of ONUs may have the duplex configuration. Based on this consideration, the last configuration (Figure 4d) permits a partial duplexing on the ONU side. This Figure shows an example where there are duplex (ONU#1) and single (ONU#N) ONUs. Its key principles are:

1) using double N:2 optical splitters to connect PON LT(0) in ONU#1 to splitter N(0) and PON LT(1) in ONU#1 to splitter N(1);

2) connecting PON LT in ONU#N to either optical splitter (because it is single);

3) using double 2:1 optical splitters to connect PON LT(0) in the OLT to splitter(0) and PONLT(1) in the OLT to splitter(1);

4) connecting double N:2 optical splitters and double 2:1 optical splitters, where one port of splitter(1) is connected to splitter N(0), and one port of splitter(0) to splitter N(1);

5) using the cold standby method in both OLT and ONUs to avoid optical signal collision from PON LT(0) and PON LT(1) in the OLT, or PON LT(0) and PON LT(1) in ONU #1.

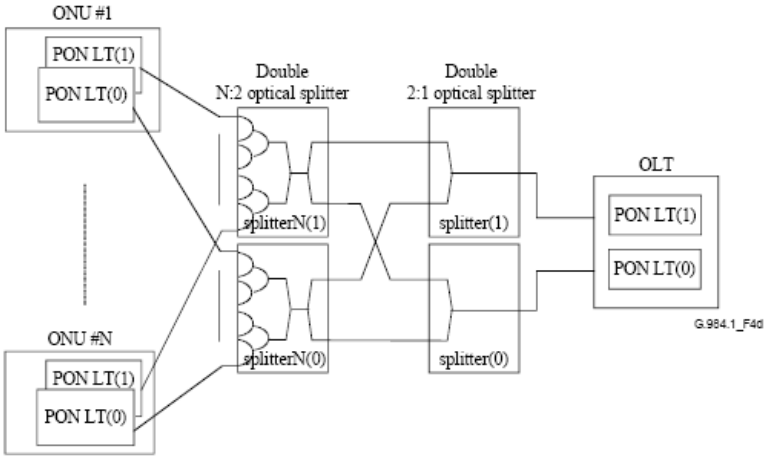


Figure 4d/G.984.1 – Duplex GPON system: Partial duplex configuration

Characteristics

Type A: In this case, signal loss or even frame loss is inevitable in the switching period. However, all the connections between the service node and the terminal equipment should be held after this fibre switching.

Type B: This configuration requires cold standby of the spare circuit in the OLT side. In this case, signal loss or even frame loss is, in general, inevitable in the switching period. However, all the connections supported between the service node and the terminal equipment should be held after this switching.

Type C: In this case, the hot standby of the spare receiver circuits is possible in both ONU and OLT sides. In addition, hitless switching (without frame loss) is also possible in this configuration.

Type D: The characteristics of this type are the same as Type B.

Requirements

i) The protection switching function should be optional.

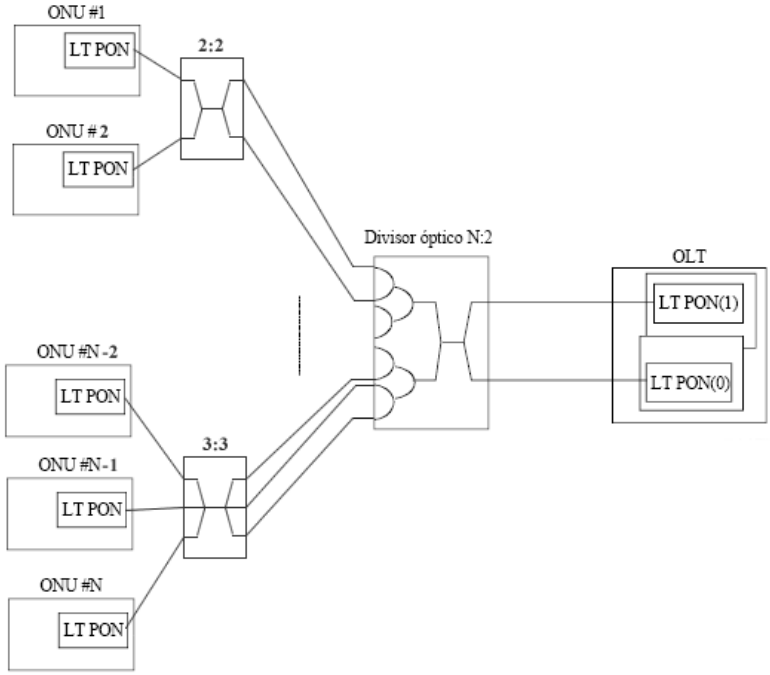
ii) Both automatic protection switching and forced switching are possible in the PON system, if required, even though they are optional functions.

iii) All the configuration examples will be possible, even though they are optional functions.

iv) The switching mechanism is generally realized by the OAM function, therefore, the required OAM information field must be reserved in the OAM frame.

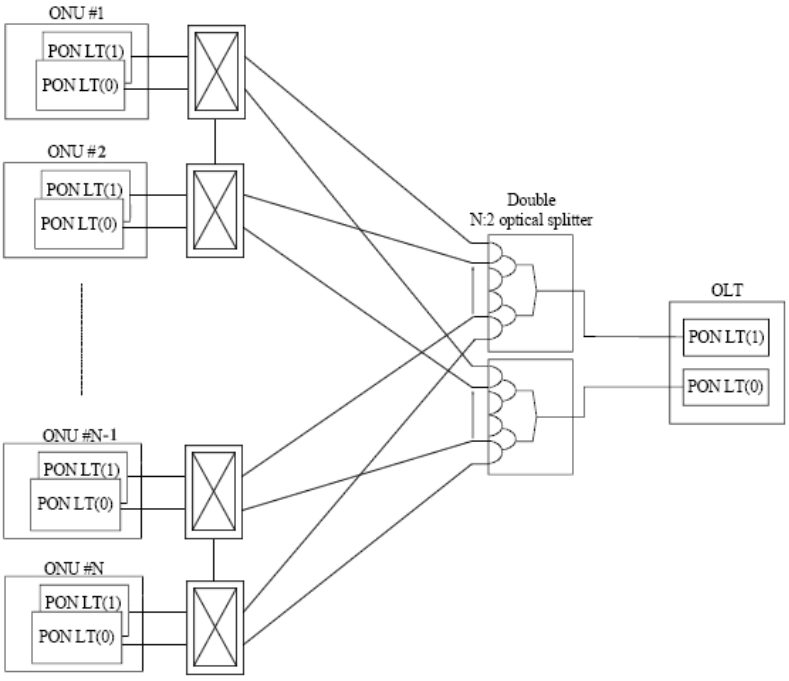
6 NEW CONFIGURATIONS

CONFIGURATION 1 (From Type B)



This configuration is a variant of the TYPE B configuration above. There is going to be an M:M coupler installed next to the each group of M ONUs. The technique is based on sharing M fibres from the splitter to the coupler. This way we will get as many redundant paths as inputs the coupler has, an the protection capacity will be increased by this factor. It is a matter of individual study for each neighborhood the amount of ONUs that will be grouped.
By using this scheme we are using two segments of dedicated protection, and therefore the signal is going to be atenuated twice; once by the splitter and again by the coupler. There will be required a separate study of the power budget depending on the neighborhood size, the distances between the different buildings…

CONFIGURATION 2 (From Type C)



This new configuration is a variant of the TYPE C configuration above. It consists in placing an optical switch right before the ONU and creating a new optical link between the different switches. This way we can make several groups of ONU depending on the needs of the clients, the size of the neighbourhood… This means that we are using a "segment" of shared protection before connecting to the ONU.
The mechanism starts in case there are failures in two separate fibres that reach one of those switches. If this happens, then one of the switches connected to this switch will redirect his traffic to this switch that is no longer receiving traffic from the regular fibres that should be coming from the splitter. The redirection is made by the extra link between the switches, as we can see in figure XX.
Again, it is subject of study the amount of ONUs that will be connected by those switches, and obviously it is more expensive using all these switches. However, it is more safe.
Apart from that, it is necessary to create a new protocol to operate with the switches, and we will not get into that in this report.

7 PROTECTION SWITCHING: PON PROTECTION FUNCTION

Type B switching architecture

No specific requirements for type B configuration ONUs are foreseen.
For the OLT, two new functions are required: a select function to choose the PON-IF and a
shut-down function for the stand-by PON-IF.

Type C switching architecture

For type C configuration, the B-PON section protection is required. One B-PON section corresponds to one connection between an OLT and an ONU, and may contain several TCONTs and VPI paths. B-PON section protection is executed independently by each branch line failure.
This permits mixed connection of protected and unprotected ONUs and leads to higher reliability and flexibility in the ODN switching network.

1:1 (Shared) and 1+1 (Dedicated) architecture

i) *1:1 architecture*
In the source direction, the working entity conveys the traffic in the normal case. If the working entity fails or a forced/manual switch is executed, the protection entity conveys the traffic.

ii) *1+1 architecture*
In the source direction, the signal is bridged to both the working and protection entities. In the sink direction, one source signal (which must have good transmission quality) is selected.

NOTE: Only the 1:1 architecture can support extra traffic.

Figures 9 and 10 show the 1:1 and 1+1 switching architecture, respectively.

X:N architecture

In this scheme, X protection PONs are provided for N working PONs (with X between 1 and N). The N working PONs can have a mixture of protected and unprotected ONUs. The protected ONUs can be connected to any of the X protection PONs, so that protected ONUs belonging to the same working PON can be connected to different protection PONs and protected ONUs belonging to different working PONs can be connected to the same protection PON.
This scheme is compatible with both the 1:1 and 1+1 switching implementations and is independent of protocol. It provides protection against multiple failures in different working PONs with less than N protection PONs.

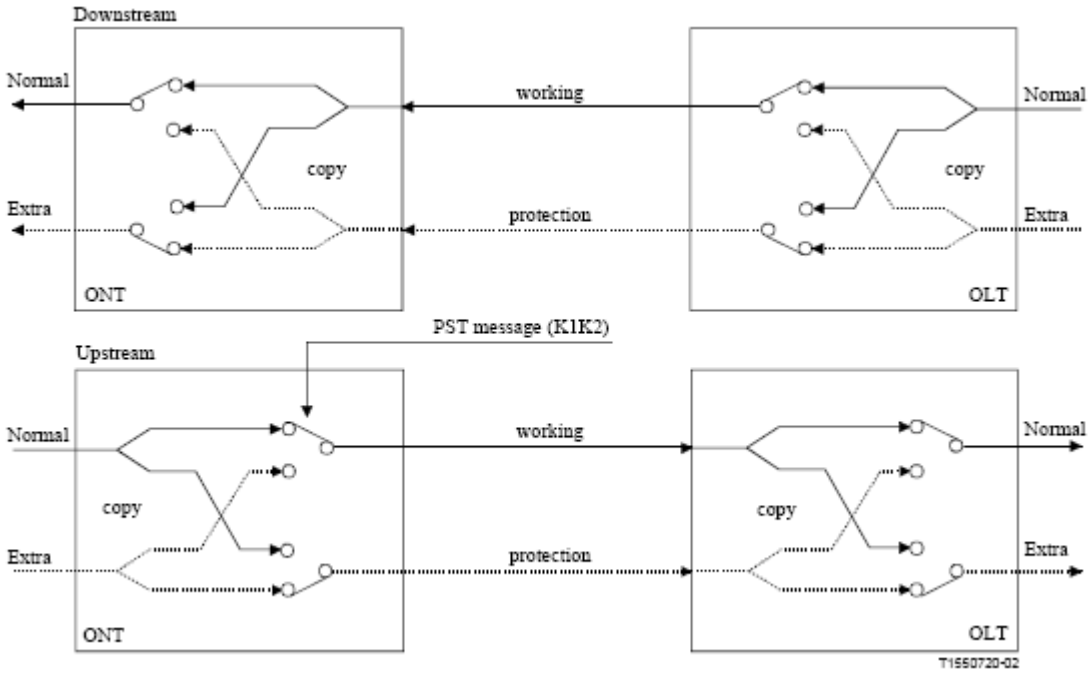


Figure 9/G.983.5 – 1:1 switching architecture

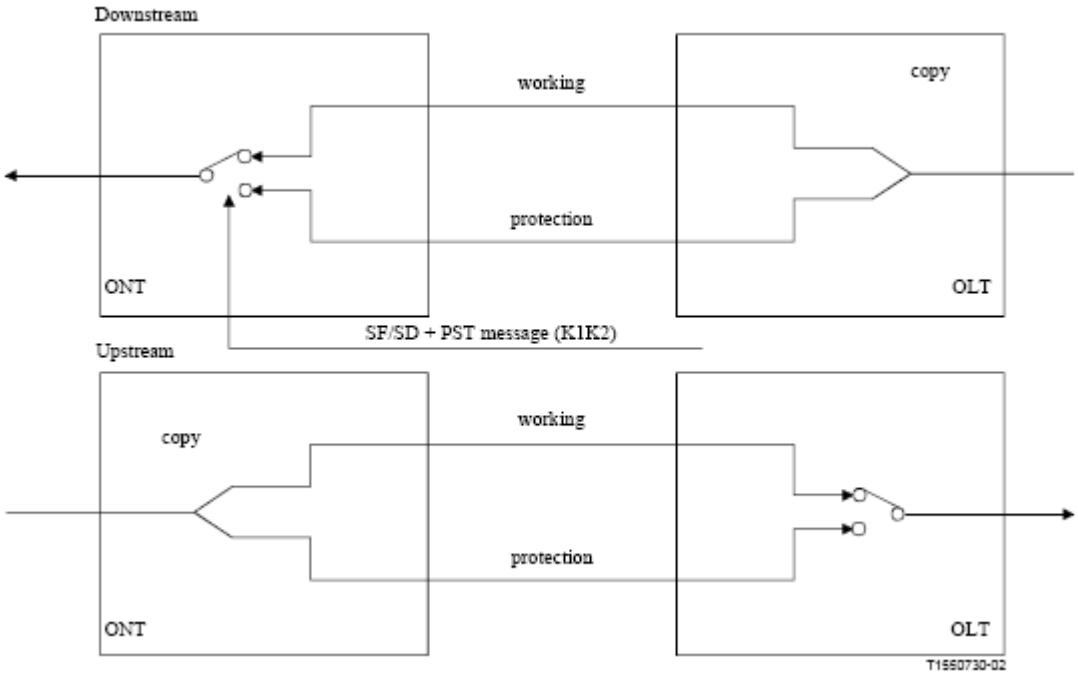


Figure 10/G.983.5 – 1+1 switching architecture

Duplex PON system

In case of a duplex system (Type C switching architecture) where a redundant PON protects the active PON, protection switching will be activated using specified messages in PLOAM cells. This sequence will require that the line numbers of the OLT must be totally the same as those of the ONU. This line identifier is assigned to a transmitter based on the interconnection scheme of OLTs with ONUs. The line identifier is sent at both OLT and ONU to check whether the received line identifier is the same as its own identifier.
This is defined as the PON Section Trace (PST) message. Then each equipment can verify its continued connection to the intended transmitter. If the received line number differs from the own line number, the equipment generates an alarm, MIS (Link Mismatching) to notify an operator or a user.
The PST messages include the K1, K2 bytes as they are specified in ITU-T Rec. G.783 for performing Automatic Protection Switching. The complete description of this is given in ITU-T Rec. G.983.5.
In case of a singular system (Type B switching architecture), link mismatching is optional.

Automatic Protection Switching

Automatic Protection Switching (APS) at the PON TC layer may be provided as an optional function. APS use depends on the number of users and service reliability. Redundant configurations of dual ODNs or dual ONUs should be considered for business applications. Some control bits for the protection protocol are reserved in the PST message field.
A complete description of APS function is given in ITU-T Rec. G.983.5. See Annex D for further details.
Time required for APS including ranging time for 32 ONUs shall be considered to support POTS and/or ISDN services; on-going connections should not be disconnected when APS is carried out.

Background and requirements

Network configuration is basically satisfied with the type B and type C configurations described in ITU-T Rec. G.983.1. The following items are required for the B-PON survivability architecture:

– Type B protection configuration. In this configuration type (shown in Figure 1), no equipment redundancy is provided in the ONUs. The protection-capable OLT performs switching if its working PON interface fails or its directly connected fibre breaks. G.983.1 compliant ONUs satisfy type B protection configuration without modification.

– Type C protection configuration. In this configuration type (shown in Figures 2 and 3), equipment redundancy is provided in both the OLT and ONUs. The protection-capable OLT performs switching if any PON interface in the OLT or ONUs fails or if any fibre in the ODN breaks. This Recommendation addresses the modifications to ITU-T Rec. G.983.1 necessary to support the type C protection configuration.

– Mixture of protected and unprotected ONUs in type C configuration. The protection functions shall allow a mixture of protected and unprotected ONUs. In certain fault scenarios, the unprotected ONUs may suffer service disruption while the protected ONUs are recovered.

– X:N variant of type C protection configuration. In this variant of configuration type C (shown in Figure 3), equipment redundancy is provided in the OLT (some or all of the Line Terminals (LTs)) and some or all ONUs. This variant allows protected ONUs to be connected to any of the protection LTs, independent of which working LT they belong to.This variant is optional.

– Extra traffic for type C configuration. Extra traffic should be able to be carried over the protection entities while the working entity is active. The extra traffic will not be protected. This option provides effective usage of bandwidth in the protection entities. It must be possible for an operator not to activate this extra traffic option.

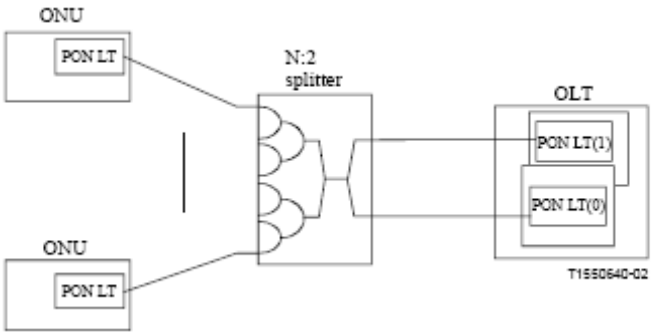


Figure 1/G.983.5 – Type B: OLT-only protected system

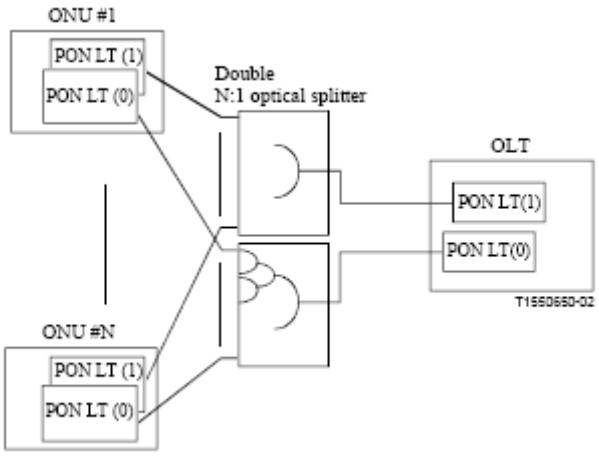


Figure 2/G.983.5 – Type C: Fully protected system, 1:1 and 1+1

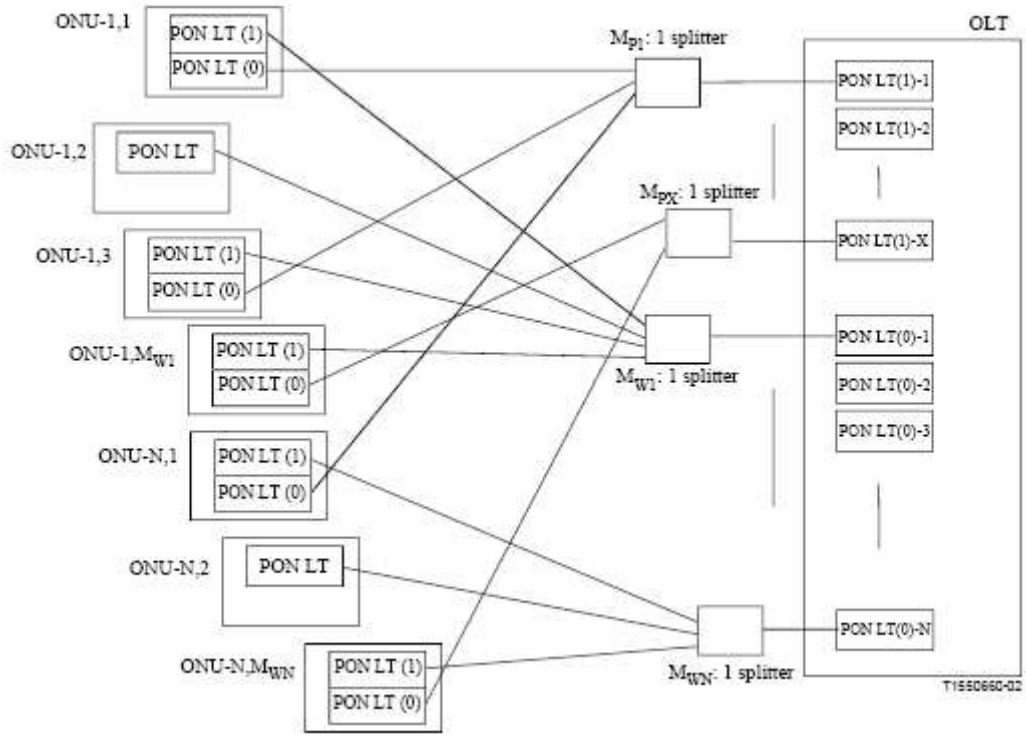


Figure 3/G.983.5 – Type C: X:N protection system

A redundant B-PON system shall satisfy the following requirements:

– It should be possible to have both the type B and type C protection configurations on the same OLT:

• It should be possible to duplicate the OLT-PON-Interface and the fibres between the OLT and splitter and to duplicate the entire fibre path between the OLT and ONU for a set of ONUs.

• The two configurations should be available on the same OLT, but not on the same ODN interface.

– It should be possible to have multi-vendor interoperability between OLT and ONU.

– In the type C configuration, it should be possible to have a mixture of protected and unprotected ONUs on one B-PON interface.

– The addition or removal of a protected ONU on a PON should not affect other ONUs on the same PON.

– It should be possible to have automatic switching, which would be triggered by a fault detection such as loss of signal, loss of cell delineation, signal degrade (e.g. BER becomes worse than the pre-determined threshold), etc.

– It should be possible to have forced switching, which would be activated by administrative events such as fiber rerouting, fiber replacement, etc.

– It is necessary to avoid unnecessary switching. Because unstable switching affects service quality, unnecessary protection switching and unnecessary revertive protection switching should not occur.

– It should be possible to realise switching without connection loss of the ATM connections.

– It should be possible for the operator to choose between a revertive and a non-revertive switching mode.

– The service halt time should be less than 50 ms if the extra traffic option is not used.

– The events or conditions that trigger automatic switching should be chosen among the G.983.1 OAM parameters.

– The chosen protocols and mechanisms must apply to the B-PON section layer.

– The type C configuration should be able to support extra traffic:

• Extra traffic should be carried over the protection entities while the working entity is active and would not be protected. This capability will provide effective usage of bandwidth on the protection entities.
• This requirement is applicable only for the type C configuration.
• It must be possible for an operator not to activate the extra traffic option (e.g. to achieve a lower service interruption time).

Optical network survivability requirements

Layer structure of the B-PON survivability optical network
The layer structure of the optical network and the physical medium dependent layer requirements are the same as in 8.1 and 8.2/G.983.1.

Layer architecture of type C switching

In this clause, the layer architecture of B-PON protection is described. In order to protect each branch line and accommodate mixed protected and unprotected ONUs, survivability for the B-PON system is executed by switching each ONU's traffic. Figure 7 shows the layer architecture of B-PON protection, which is based on the ITU-T Rec. G.805 description. Figure 8 shows the multiplexing structure of the section/path layers between the OLT and ONU with the protection function.
A B-PON section is defined as the VP group between the OLT and an ONU. If "n" ONUs are connected to an OLT, then there are "n" B-PON sections. These sections are supervised using PLOAM cells as the TC layer function.
The B-PON section layer protection function is not on the ATM layer, but it is established in the TC layer between one ONU and OLT section including all VPI paths in the ONU, and is executed independently for each branch line failure. To do this, the B-PON section can be checked using the TC layer OAM function. This B-PON section-layer protection leads to higher reliability and flexibility in the ODN protection switching network.

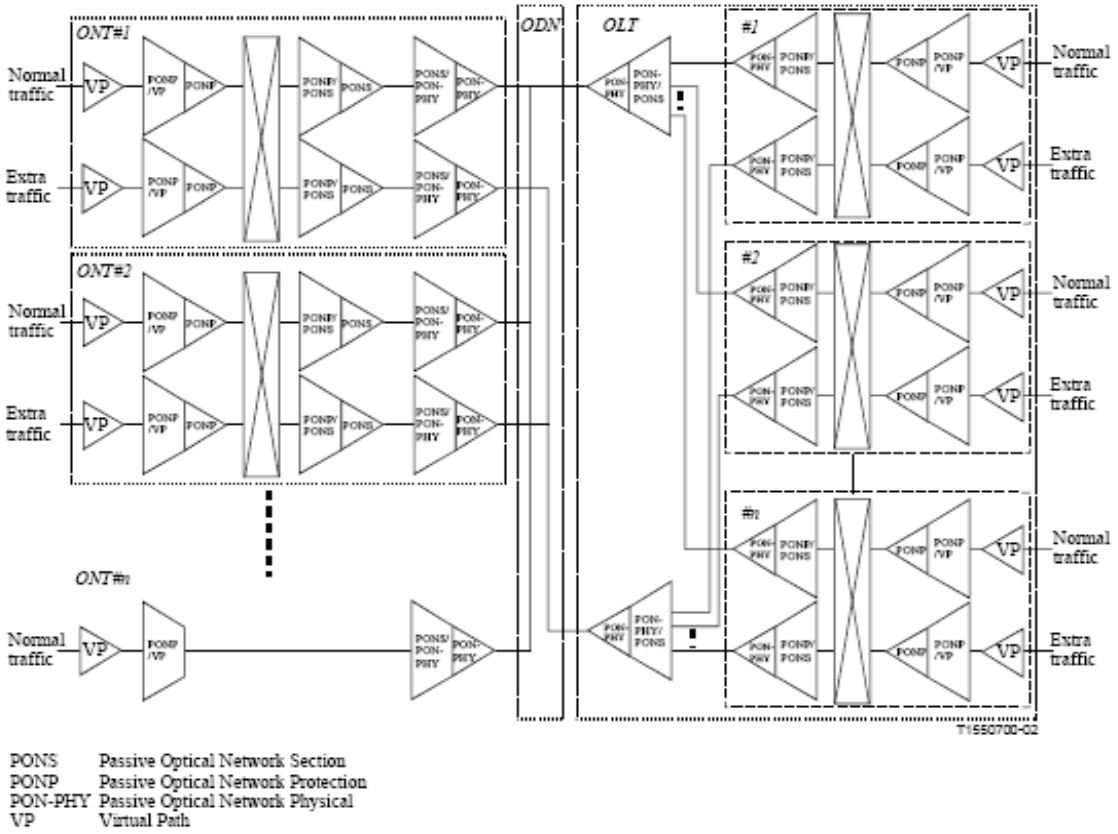


Figure 7/G.983.5 – The layer architecture example in B-PON

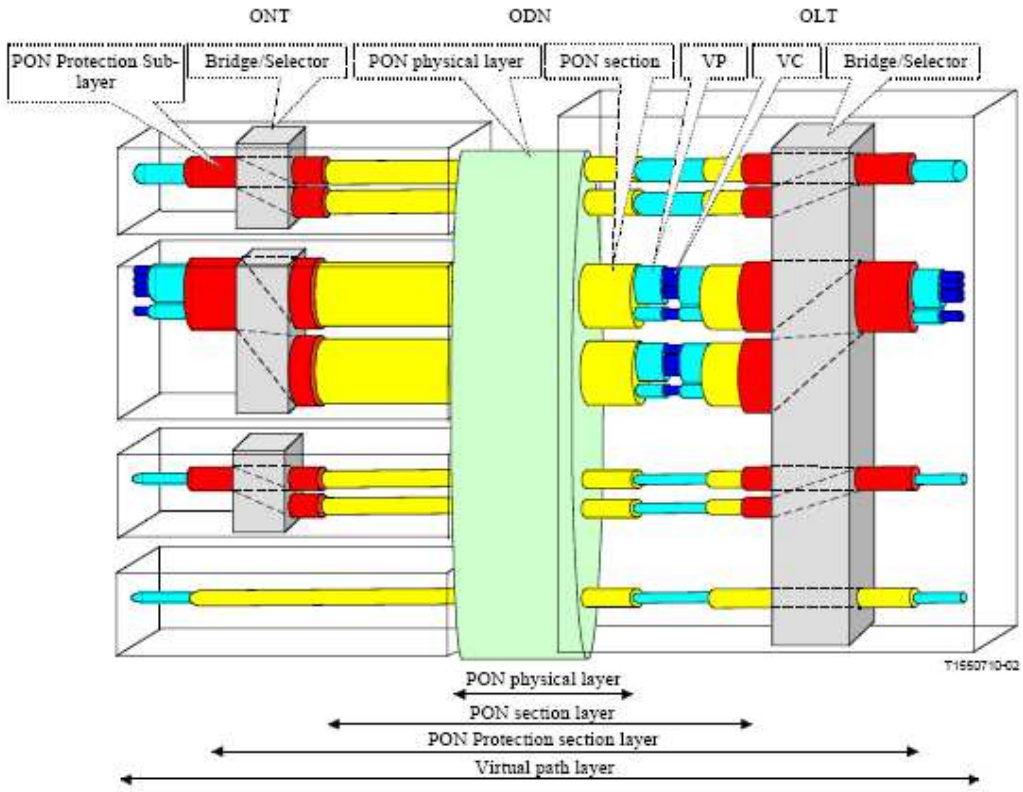


Figure 8/G.983.5 – The layer image in B-PON

Switching criteria

Basically, type B switching does not require any communication between the OLT and ONUs, and forced and automatic switching are executed only at the OLT side. The trigger for automatic switching should be the same as for type C.

Type C switching commands are described as follows.

1) *Externally initiated commands*
Externally initiated commands (e.g. forced switch/manual switch operation) are always issued by the OLT side.

2) *Automatically initiated commands*
Automatic protection switching is based on the failure conditions of the working and protection B-PON sections. Signal Fail (SF) and Signal Degrade (SD) commands are provided by the OLT and ONU.

8 CONCLUSIONS

After showing all the different configurations, we should be able to propose the best of all. However, there is not a best topology; some will be good enough for one situation, but not for other ones. Then we can say that we will use the proper configuration depending on the situation, and the money available. Obviously we can exponentially increase the protection by increasing the cost.

9 DIFFICULTIES READING THE SPANISH ITU-Ts

We can now say that we experienced some difficulties when reading the Spanish ITU-Ts. Some paragraphs were quite difficult to understand. Let the next paragraph serve as an example:

“”Una sección B-PON se define como el grupo de VP entre la OLT y una ONU. Si hay "n" ONU conectadas a una OLT, habrá "n" secciones B-PON. Estas secciones se supervisan utilizando células PLOAM para la función de capa TC.
La función protección de la capa de sección B-PON no está en la capa ATM, sino que se crea en la capa TC entre una ONU y una sección OLT que incluye todos los trayectos VPI en la ONU, y se realiza de manera independiente para cada fallo de línea de rama. Para ello, la sección B-PON se puede comprobar utilizando la función OAM de capa TC. Con esta protección de la capa de sección B-PON se consigue mayor fiabilidad y flexibilidad en la red de conmutación de protección ODN.””

This paragraph can be found in page 14 **Rec. UIT-T G.983.5 (01/2002)**