Universidad Zaragoza
1542

Proyecto Fin de Carrera

ESTUDIO, DESARROLLO E IMPLEMENTACIÓN DE UNA RED IP DE SEGURIDAD MEDIANTE EL USO DE REDES ÓPTICAS PASIVAS Y TECNOLOGÍAS GPON.

Autor

Iván Lardiés Sánchez

Director y ponente

Octavio Benedí Sánchez

José Ruiz Mas

Ingeniería de Telecomunicación / E.I.N.A.

Febrero 2014

ESTUDIO, DESARROLLO E IMPLEMENTACIÓN DE UNA RED IP DE SEGURIDAD MEDIANTE EL USO DE REDES ÓPTICAS PASIVAS Y TECNOLOGÍAS GPON.

RESUMEN

En los últimos años, el considerable aumento en el ancho de banda requerido por diferentes aplicaciones, en especial el vídeo de alta calidad, ha hecho necesario el despliegue de redes FTTH (*Fiber to the home*) basadas en fibra óptica hasta el hogar del usuario. Esto es extensible a los sistemas de seguridad, ya que desde la aparición de las cámaras de alta definición, el ancho de banda consumido por las redes de videovigilancia ha aumentado considerablemente, lo que hace conveniente pensar en la implementación de una red basada en fibra óptica con capacidad de gigabit.

Este proyecto fin de carrera trata de desarrollar e implementar una red IP de seguridad basada en tecnología FTTH-GPON (*Gigabit-capable Passive Optical Network*), aprovechando todas las ventajas que proporciona la transmisión por fibra óptica hasta el terminal de abonado, tanto en términos de ancho de banda como en la seguridad de los datos.

FTTH proporciona una red punto a multipunto sin componentes activos entre la central y el abonado, permitiendo que múltiples abonados compartan una misma conexión formando una red óptica pasiva P2MP (*Point-to-MultiPoint*). El estándar GPON permite velocidades de hasta 2.48 Gbps en descendente y 1.24 Gbps en ascendente, y una relación de división teórica de 1:128. Además dispone de un modelo de gestión y control, denominado OMCI (*ONT Management and Control Interface*), encargado de la configuración de los equipos de usuario.

En el desarrollo de un sistema de seguridad resulta especialmente importante capturar de manera continuada alarmas y otro tipo de información proveniente de los equipos para facilitar la detección de posibles averías o incidentes, pensando en la seguridad física y lógica de la red. Para ello contamos con una arquitectura de gestión centralizada llamada *TELNET GPON Management System* o TGMS, en la que se desarrollarán nuevos módulos específicos destinados a la gestión de alarmas que permitan detectar variaciones en los parámetros físicos y lógicos de la red. Con estos módulos adicionales se pretende dotar al sistema de una mayor seguridad frente a sabotajes o intrusiones en la red.

Índice general

Índice de figuras

Índice de tablas

Acrónimos

AES Advanced Encryption Standard.

AJAX Asynchronous JavaScript And XML.

APC Angled Physical Contact.

ATM Asynchronous Transfer Mode.

BER Bit Error Rate.

BIP Bit Interleaved Parity.

BPON Broadband Passive Optical Network.

BWmap Mapa de ancho de banda.

CAPEX Capital Expenditures.

CCTV Circuito cerrado de televisión.

CPD Centro de procesamiento de datos.

CRC Cyclic redundancy check.

CSS Cascading Style Sheets.

DBA Dynamic Bandwidth Assignment.

DBRu Dynamic Bandwidth Report upstream.

DFB Distributed Feedback Laser.

DL Downlink.

DSL Digital Subscriber Line.

EMI Interferencia electromagnética.

EPON Ethernet Passive Optical Network.

EqD Equalization Delay.

FEC Forward Error Correction.

FTTH Fiber To The Home.

FTTx Fiber To The x.

GEM GPON Encapsulation Method.

GPON Gigabit-capable Passive Optical Network.

GTC GPON Transmission Convergence.

HTML HyperText Markup Language.

HTTP Hypertext Transfer Protocol.

IGMP Internet Group Management Protocol.

ITU International Telecommunication Union.

IP Internet Protocol.

JSON JavaScript Object Notation.

MAC Medium Access Control.

MIB Management Information Base.

OAM Operation Administration and Maintenance.

ODN Optical Distribution Network.

OLT Optical Line Terminal.

OMCC ONT Management and Control Channel.

OMCI ONT Management and Control Interface.

ONT Optical Network Terminal.

ONU Optical Network Unit.

OPEX Operating Expense.

OTDR Optical Time Domain Reflectometer.

P2MP Point-to-Multipoint.

P2P Point-to-Point.

PCBd Physical Control Block downstream.

PDU Protocol Data Unit.

PLOAM Physical Layer Operation Administration and Maintenance.

PLOu Physical Layer Overhead upstream.

PMD Physical Medium Dependent.

PON Passive Optical Network.

POTS Plain Old Telephone Service.

QoS Quality of Service.

RF Radiofrecuencia.

RIC Rango intercuartílico.

RPC Remote Procedure Call.

RTP Real-Time Transport Protocol.

RTSP Real-Time Streaming Protocol.

SDU Service Data Unit.

T-CONT Transmission Container.

TCP Transmission Control Protocol.

TDMA Time Division Multiple Access.

TGMS TELNET GPON Management System.

UDP User Datagram Protocol.

UL Uplink.

UNI User Network Interface.

VLAN Virtual Local Area Network.

WAMP Windows-Apache-MySQL-PHP.

WDM Wavelength Division Multiplexing.

XGPON Extended GPON.

XML Extensible Markup Language.

1. Introducción

1.1. Contexto y ubicación del proyecto

El proyecto fin de carrera se ha realizado en la empresa Telnet Redes Inteligentes S.A. y está centrado en el desarrollo de una red de seguridad basada en tecnología GPON (*Gigabit-capable Passive Optical Network*). GPON es un estándar definido en 2004 por parte del ITU-T (*International Telecommunication Union*) en el conjunto de recomendaciones G.984.x., en el cual se incluyen velocidades de línea hasta 2.488 Gbps para el enlace descendente y 1.244 Gbps para el ascendente.

La red GPON consta de un equipo de cabecera, denominado OLT (*Optical Line Terminal*) y ubicado en las dependencias del operador, y el equipo terminal, ONT (*Optical Network Terminal*), en las dependencias de los usuarios, conformando una red punto-multipunto (P2MP). El estándar permite hasta 128 equipos de usuario en cada red, pero la tecnología actual sólo contempla 64.

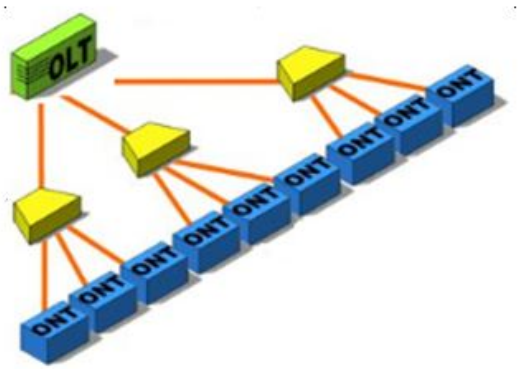


Figura 1.1: Topología P2MP de red GPON

Para conectar la OLT con la ONT, se emplea un cable de fibra óptica monomodo que transporta tráfico en distintas longitudes de onda WDM (*Wavelength Division Multiplexing*). El tráfico ascendente se transmite en 1310 nm y el descendente en 1490 nm, aprovechando así respectivamente la segunda y tercera ventana de transmisión sobre fibra óptica. Además, es posible transmitir en descendente vídeo RF (Radiofrecuencia) *broadcast* en 1550 nm.

El tráfico originado en la OLT es distribuido hasta las ONTs mediante un divisor óptico pasivo, denominado *splitter*, en una o varias etapas, en una topología de árbol. En sentido descendente, el *splitter* comparte su entrada con todas las salidas, repartiendo la potencia, y en ascendente combina las señales procedentes de las ONTs en una única fibra, compartiendo ancho de banda. En el anexo A se explica más detalladamente la arquitectura FTTH y en el anexo B, el estándar GPON.

Por otra parte, en las redes destinadas a seguridad, el mayor ancho de banda es consumido por las cámaras IP de videovigilancia. Este ancho de banda requerido ha aumentado notablemente estos últimos años debido a la aparición de las cámaras digitales de alta definición, las cuales ofrecen mayor resolución pero también generan más tráfico en la red. La bajada de precios de estas cámaras debida a su popularización unida a la reducción en el coste de almacenamiento ha provocado un considerable aumento en el tráfico que deben soportar las redes destinadas a seguridad. Por esta razón se convierte en necesaria la implementación de redes de acceso basadas en fibra óptica con capacidad de gigabit hasta las dependencias del usuario, siendo GPON una opción a considerar. Para una mayor información sobre las redes de videovigilancia, consultar el anexo D.

1.2. Objetivos

El objetivo principal del proyecto es el desarrollo y la implementación de una red IP destinada a un sistema de seguridad mediante el uso de redes GPON. El primer paso es analizar las ventajas que aportan las redes GPON, tanto en términos de seguridad física y lógica, como en ancho de banda disponible, respecto a las redes basadas en cobre y a redes de fibra óptica basadas en equipos activos y de topología punto a punto.

Respecto a la gestión de la red, se pretende realizar una mejora en la monitorización de alarmas o eventos, para facilitar la detección de posibles averías o incidentes, pensando en la seguridad de la red. Para ello contamos con una arquitectura de gestión centralizada llamada *TELNET GPON Management System* o TGMS (ver anexo C), que facilita la posibilidad de detectar nuevas ONTs, comprobar el estado de las conectadas y de la red en su totalidad. Se desarrollarán nuevos módulos en esta herramienta que nos permitan dotar al sistema de una mayor seguridad frente a sabotajes o intrusiones en la red.

La realización de este proyecto tiene los siguientos objetivos:

- Entender los modelos de redes destinadas a seguridad que se proponen en la actualidad y justificar la propuesta de desarrollo de una red GPON.
- Aumentar el ancho de banda disponible que ofrecen las actuales redes de seguridad hasta las dependencias del usuario.
- Minimizar los costes, tanto CAPEX (*Capital Expenditures*) como OPEX (*Operating Expense*), en el despliegue de una red de seguridad, mediante el uso de elementos pasivos y con una topología adecuada.

- Adoptar una solución de despliegue eficiente en términos de consumo energético.
- Aumentar el grado de seguridad en nuestra red, tanto física como lógica, aprovechando las características de GPON y con nuevos módulos del TGMS que permitan detectar modificaciones de los parámetros de la red y evitar así posibles sabotajes o intrusiones.
- Proporcionar al usuario un sistema de seguridad con un servicio de datos como valor añadido, usando la misma infraestructura de fibra óptica.

1.3. Trabajo previo, metodología y herramientas

En primer lugar, **el trabajo previo** a este proyecto ha consistido en el estudio de la tecnología FTTH y en particular el estándar GPON, definido en el conjunto de recomendaciones ITU-T G.984.x [1][2][3] y G.988 [4].

Además, ha sido conveniente conocer las características de los equipos comercializados por Telnet, tanto la SmartOLT como la ONT, y el TGMS, su herramienta web usada para la configuración, monitorización y administración de la red GPON. También ha resultado oportuno el estudio de los sistemas de seguridad actuales, en especial el campo de la videovigilancia, ya que las cámaras IP son los dispositivos más importantes en cuanto a ancho de banda requerido.

Una parte significativa del proyecto consta del desarrollo de nuevas funcionalidades en el sistema de gestión de redes GPON, fundamentalmente en el apartado de detección de alarmas. Para ello, es necesaria la implementación de un sistema de adquisición y análisis de datos, mediante el cual se capturen los datos de interés de los equipos que componen la red GPON y los almacenen en bases de datos MySQL para su posterior análisis.

En este sentido, se optará por una **metodología** basada en la arquitectura de software *Model-View-Controller*, independizando las partes del programa correspondientes al controlador de funciones, a la aplicación del modelo elegido y a la presentación de los datos.

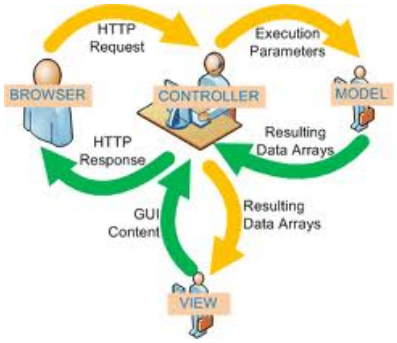


Figura 1.2: Esquema Model-View-Controller

Además, se facilitará la escalabilidad en la gestión de las bases de datos optando por la técnica de *sharding*. Esta técnica se basa en el crecimiento horizontal de las bases de datos, agrupando conjuntos de datos de modo que tenga cierto sentido y permitiendo de esta manera un direccionamiento más rápido, mejorando el rendimiento. En este caso cada día crearemos una base de datos nueva y así controlaremos el crecimiento y facilitaremos la búsqueda de los datos de interés.

En lo referente a **las herramientas utilizadas**, para el desarrollo del sistema de gestión de alarmas se hará uso de la plataforma de desarrollo web WAMP, basada en Windows como sistema operativo, un servidor HTTP Apache, MySQL como gestor de bases de datos y PHP como lenguaje de programación. Aunque el desarrollo se realizará en un equipo con Windows, el sistema se ejecutará en un servidor Linux.

También se utilizará la técnica de desarrollo web AJAX (*Asynchronous JavaScript And XML*) para realizar cambios sobre las páginas sin necesidad de recargarlas, mejorando de esta manera la interactividad, velocidad y usabilidad de la aplicación. Para gestionar eventos y agregar interacción a la web, se ha utilizado la biblioteca de JavaScript JQuery. Además, será necesario el uso de librerías para representar mediante gráficas los parámetros de interés de la red. Por otra parte, debido a que PHP limita el tiempo máximo de ejecución de sus programas, se recurrirá a la programación en C para la ejecución continua de programas en un segundo plano. En el anexo G se explica este apartado de una manera más detallada.

1.4. Planificación de tareas a realizar

El trabajo a realizar para la correcta consecución de este proyecto se divide en cuatro partes:

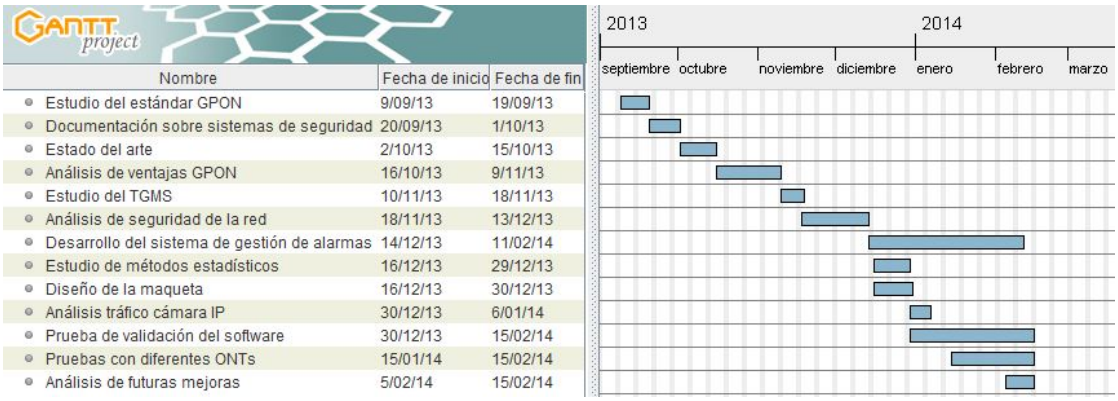
1. **Estado del arte:** El primer paso es conocer el tipo de soluciones y servicios que ofrecen en la actualidad las empresas del sector, y de esta manera analizar los beneficios que puede aportar el desarrollo del sistema propuesto.

2. **Ventajas de GPON frente a las soluciones existentes:** En esta parte del proyecto se justifica el uso de los equipos que componen la red GPON, analizando sus ventajas respecto a las redes actuales basadas en cobre.

3. **Análisis de la seguridad de la red:** En un primer lugar se estudiarán las posibles situaciones de riesgo que pueden afectar a la seguridad de nuestra red, para posteriormente analizar de qué manera podemos detectarlas mediante un sistema que capture y almacene parámetros de interés de los equipos que componen la red.

4. **Pruebas de validación del sistema:** Se diseñará la maqueta de red GPON y la interfaz web para posteriormente verificar el correcto funcionamiento del sistema de detección de alarmas ante posibles situaciones de riesgo.

Es recomendable representar de forma gráfica mediante un **diagrama de Gantt** el tiempo dedicado a cada una de las tareas necesarias para la realización del proyecto.



Nombre	Fecha de inicio	Fecha de fin
Estudio del estándar GPON	9/09/13	19/09/13
Documentación sobre sistemas de seguridad	20/09/13	1/10/13
Estado del arte	2/10/13	15/10/13
Análisis de ventajas GPON	16/10/13	9/11/13
Estudio del TGMS	10/11/13	18/11/13
Análisis de seguridad de la red	18/11/13	13/12/13
Desarrollo del sistema de gestión de alarmas	14/12/13	11/02/14
Estudio de métodos estadísticos	16/12/13	29/12/13
Diseño de la maqueta	16/12/13	30/12/13
Análisis tráfico cámara IP	30/12/13	6/01/14
Prueba de validación del software	30/12/13	15/02/14
Pruebas con diferentes ONTs	15/01/14	15/02/14
Análisis de futuras mejoras	5/02/14	15/02/14

Figura 1.3: Diagrama de Gantt

1.5. Organización de la memoria

La memoria de este proyecto se divide en dos partes. La primera parte principal donde se recogen los aspectos fundamentales del desarrollo del proyecto y la segunda parte formada por los diferentes anexos que completan el trabajo.

La memoria empieza con esta introducción, la cual pone en situación al lector sobre la tecnología que se va a utilizar, los objetivos que se persiguen con el desarrollo del proyecto y las herramientas y los métodos que se van a utilizar para su elaboración. En el segundo apartado se realiza un estudio sobre los despliegues actuales en materia de seguridad, analizando los puntos donde se podrían introducir mejoras con la arquitectura y los componentes de la solución propuesta.

En el siguiente punto se analizan los posibles riesgos que puede sufrir una red GPON y se estudia la manera de evitarlos o detectarlos mediante el desarrollo de un sistema de detección de alarmas. Para terminar se realizan una serie de pruebas sobre una maqueta funcional para verificar que el software funciona de la manera deseada. En los últimos puntos se recogen las conclusiones deducidas en la realización del proyecto y un conjunto de posibles mejoras para continuar con el trabajo.

Los anexos se elaboran con la finalidad de complementar la información de los puntos principales de la memoria, desarrollando en profundidad los apartados de más interés o aclarando algún apartado que requiera mayor extensión.

Tabla 1.1: Anexos

Anexo	**Contenido**
A	Arquitectura FTTH-GPON
B	GPON
C	TGMS
D	Redes IP de videovigilancia
E	Dispositivos de seguridad
G	RPC
H	Programación Web
I	Proceso de Ranging

2. Entorno tecnológico: antecedentes

2.1. Soluciones existentes

Un aspecto importante es la realización de un estudio competitivo para conocer los servicios que ofrecen las empresas del sector, así como estudiar sus puntos fuertes y débiles en beneficio del sistema que se quiere ofrecer.

En este caso, hemos analizado las soluciones que proponen distintas empresas con despliegue de redes de videovigilancia. Estas son algunas de ellas:

- ACTi Corporation.
- Adilec.
- AXIS.
- Cisco.
- LevelOne.
- Milestone.
- Veracity.

En la Figura 2.1 podemos ver la topología de red que utiliza la empresa Cisco en sus despliegues para sistemas de seguridad.

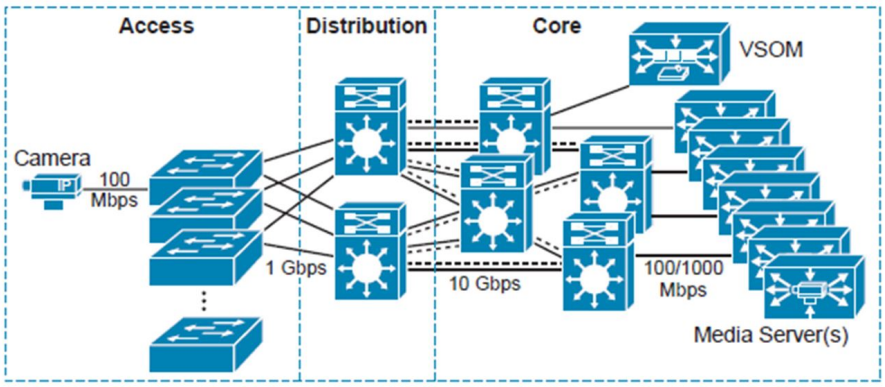


Figura 2.1: Despliegue de red de la empresa Cisco

Hemos comprobado que las soluciones que nos proponen estas empresas son redes punto a punto (P2P) Ethernet compuestas en su mayoría por tres capas de equipos activos formando un modelo de red jerárquico [9] como el mostrado en la Figura 2.1, compuesto de: una capa de acceso, una capa de distribución y una capa base o núcleo.

Si queremos proponer otra solución para el despliegue de red es importante tratar de cumplir tres requisitos fundamentales:

- Hacer uso de tecnologías avanzadas en términos de tasa de transmisión, funcionalidad y seguridad.
- Controlar tanto el coste inicial de instalación como el de mantenimiento.
- Adoptar la solución más eficiente en términos de consumo energético.

Este proyecto tiene como objetivo verificar que las redes ópticas pasivas, más concretamente las basadas en tecnología GPON, satisfacen estas condiciones y presentan una serie de ventajas adicionales respecto a las redes activas P2P actuales.

Como podemos ver en la Figura 2.2, una empresa fabricante de equipamiento de redes y equipos de telecomunicación como Huawei [10] muestra las redes ópticas pasivas como una posible solución en redes destinadas a videovigilancia de escenarios de gran longitud como autopistas o gaseoductos, aprovechando la baja atenuación de la fibra óptica.

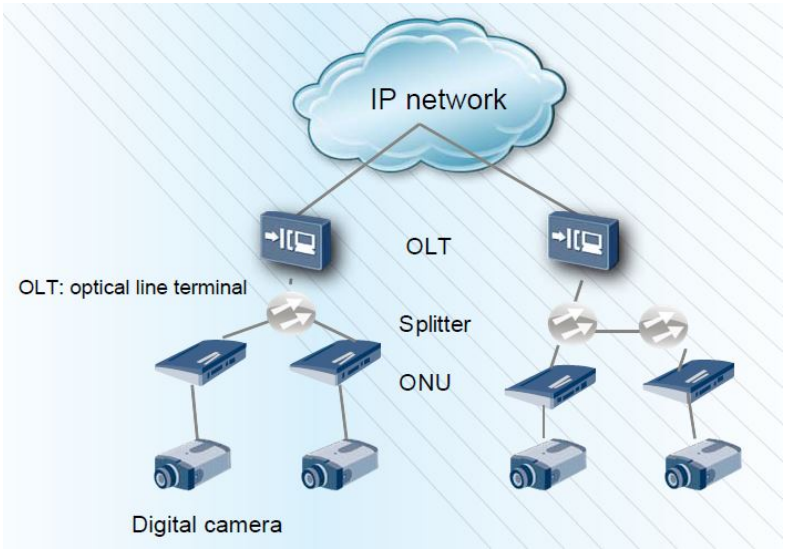


Figura 2.2: Solución de red PON propuesta por Huawei

2.2. Tecnología GPON

En 2004, se terminaba de definir GPON [5] por parte del ITU-T en el conjunto de recomendaciones G.984.x. El estándar incluye varias velocidades de línea hasta 2.488 Gbps en el enlace descendente y 1.244 Gbps en el ascendente, compartido por los equipos de usuario que componen la red, hasta un límite de 64. La red GPON se compone principalmente de un equipo de cabecera propiedad del operador, la OLT, y los equipos terminales de usuarios, ONTs, siguiendo una topología en árbol en una arquitectura punto-multipunto. Para distribuir el tráfico originado en la OLT se utilizan divisores pasivos, *splitters*, en una o varias etapas, hasta llegar a cada ONT.

El método de encapsulación GPON es GEM (*GPON Encapsulation Method*) que permite soportar cualquier tipo de servicio: Ethernet, TDM (Multiplexación por división de tiempo), o ATM (*Asynchronous Transfer Mode*) en un protocolo de transporte síncrono basado en tramas periódicas de 125 microsegundos. GPON no sólo ofrece mayor ancho de banda que sus tecnologías predecesoras, es además mucho más eficiente y permite a los operadores continuar ofreciendo sus servicios tradicionales sin tener que cambiar los equipos instalados en las dependencias de sus clientes.

GPON también implementa capacidades de OAM (*Operation, Administration and Maintenance*) avanzadas, ofreciendo una potente gestión del servicio extremo a extremo. Entre otras funcionalidades incorporadas destacan: monitorización de la tasa de error, alarmas y eventos, descubrimiento y *ranging* automático, etc. GPON permite al operador hacer uso de un modelo de gestión denominado OMCI (*ONT Management and Control Interface*) (ver anexo B.5), que facilita la administración remota de los equipos de usuario, reduciendo así los costes de operación y mantenimiento.

Una de las características clave de las redes GPON es ofrecer a los usuarios más tráfico cuando lo necesitan, si algún usuario de la misma red no está empleando todo su ancho de banda disponible. Esta funcionalidad es denominada asignación dinámica del ancho de banda o DBA (*Dynamic Bandwidth Allocation*).

Para el tráfico descendente (1490 nm.) se realiza un *broadcast* óptico, aunque cada ONT sólo es capaz de procesar el tráfico que le corresponde o para el que tiene acceso, gracias a las técnicas de seguridad AES (*Advanced Encryption Standard*).

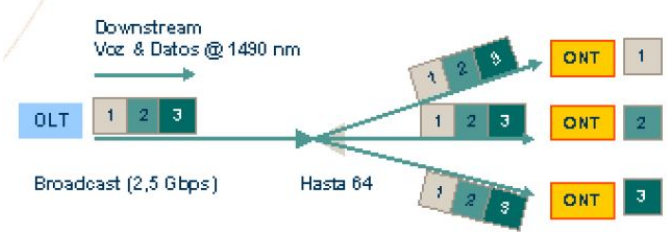


Figura 2.3: Transmisión descendente broadcast

En ascendente (1310 nm.) se usan protocolos basados en TDMA (Acceso múltiple por división de tiempo), que aseguran la transmisión sin colisiones desde las ONT hasta la OLT.

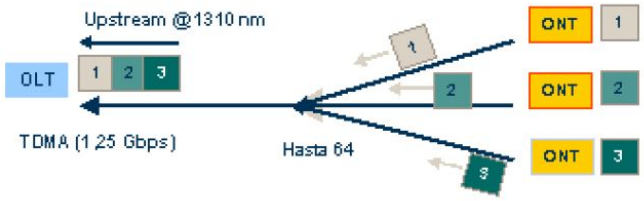


Figura 2.4: Transmisión ascendente TDMA

2.2.1. Ventajas frente a redes P2P Ethernet

Las ventajas que aporta GPON respecto a P2P Ethernet se basan en el uso de componentes pasivos, los cuales disminuyen los costes de consumo de potencia y reducen el número de dispositivos requeridos en la red. En GPON tenemos la ventaja añadida de poder desplegar la red de fibra óptica hasta los equipos finales, sin la necesidad de un último tramo de cobre que disminuya nuestras prestaciones.

Como podemos ver en la Figura 2.5, el equipo de cabecera, la OLT, y los distribuidores ópticos pasivos sustituyen a los equipos de las capas de acceso y distribución correspondientes en las redes P2P Ethernet, simplificando bastante el despliegue con una reducción de costes significativa. Serían necesarios uno o varios switches de agregación, dependiendo de la capacidad de la red, para agregar el tráfico de diferentes OLTs.

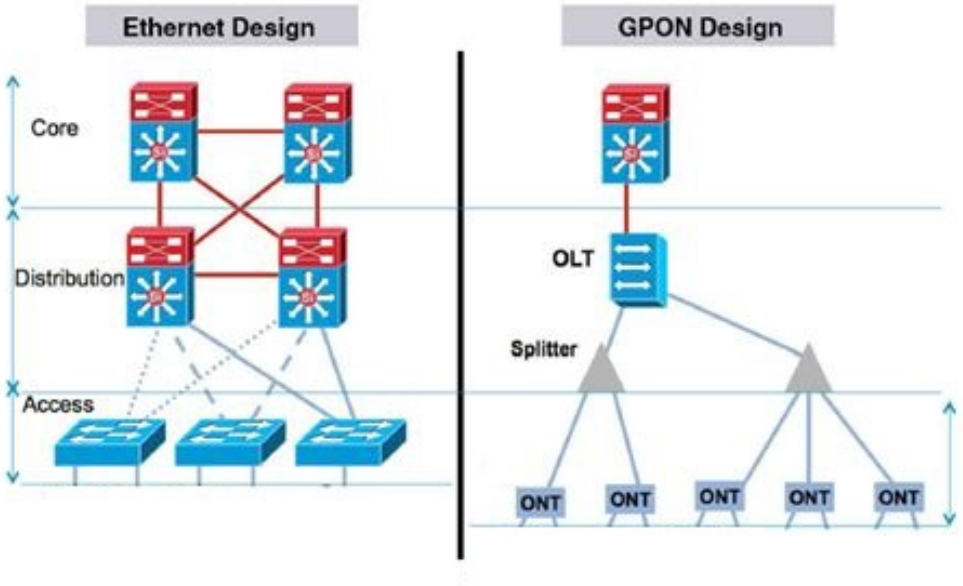


Figura 2.5: Comparativa de topologías P2P-GPON

Las **ventajas** que aporta GPON respecto a las redes basadas en cobre son las siguientes:

1. **Ancho de banda y distancia.** El medio óptico permite superar los límites de ancho de banda y distancia existentes en las tecnologías xDSL (*Digital Subscriber Line*). Se dispone de 2.5 Gbps en el enlace descendente y 1.25 Gbps en el ascendente, con una distancia máxima entre OLT y ONT de 20 km. sin necesidad de dispositivos que regeneren o repitan la señal. Además, debido a su carácter compartido se mejora la eficiencia en transmisión de tráfico multicast.

2. **Economía.** Debido a su topología punto a multipunto, GPON reduce el CAPEX en fibra óptica y en interfaces ópticos, ya que la OLT dispone de 4 puertos PON (*Passive Optical Network*), con los que puede dar servicio hasta 64 usuarios cada uno. Por otra parte, la red está formada por componentes pasivos, principalmente *splitters*, lo cual produce un considerable ahorro de consumo y de equipamiento. Además, en los últimos años el precio de la fibra está disminuyendo debido al masivo despliegue producido.

3. **Calidad de servicio.** De manera nativa, GPON dispone de un modelo de QoS (*Quality of Service*) que garantiza el ancho de banda necesario para cada servicio y usuario (*Triple Play real*: Voz, banda ancha y televisión) mediante la asignación dinámica de ancho de banda.

4. **Seguridad.** La fibra óptica no produce radiación electromagnética (EMI) ni se ve afectada por ella, lo que la hace resistente a las acciones intrusivas de escucha. Para acceder a la señal es necesario manipular la fibra, con lo que la atenuación aumenta y por tanto puede llegar a detectarse. Además, la información en descendente se cifra en AES256 (*Advanced Encryption Standard*).

5. **Operación y mantenimiento.** De manera nativa, GPON cuenta con un modelo de gestión que facilita al operador la administración remota de los equipos de usuario, lo que se traduce en una reducción en el OPEX.

6. **Escalabilidad.** Gracias a la multiplexación en longitud de onda WDM, para aumentar la capacidad de la red no es necesario cambiar la infraestructura de fibra desplegada. Si implementamos GPON (2,5 Gbps para 64 usuarios), en el futuro podremos evolucionar a XGPON (*Extended GPON*: tasas de 10Gbps compartidos), WDM PON (1Gpbs simétrico para cada usuario) o 10G-PON (10Gpbs simétrico por usuario) y seguir utilizando la misma infraestructura de fibra. Esto representa una ventaja respecto a las redes de cobre, ya que para aumentar la capacidad de la red necesitan cambiar a un cable de categoría superior que soporte la capacidad deseada (Cat 5, Cat 5e, Cat 6, etc.).

2.2.2. Mejoras en el despliegue

La topología de las redes GPON implica una reducción de coste tanto en el número de fibras como en interfaces ópticos, así como también en el número de equipos necesarios. De cada uno de los puertos de la OLT sale una única fibra óptica que puede dar servicio a 64 equipos de usuario. Desde los *splitters* sale una fibra óptica para cada usuario, pero si esta distribución se realiza cerca de las ONTs y en varias etapas, el número de fibras ópticas necesario para el despliegue de la red disminuye considerablemente.

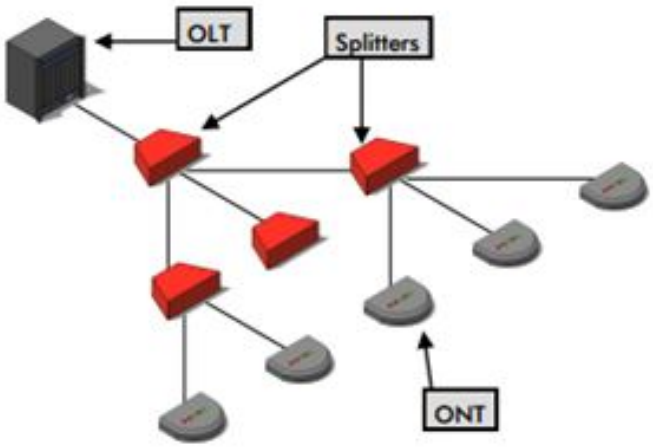


Figura 2.6: Topología de red PON

Una de las mayores ventajas que aportan las redes ópticas pasivas es el uso de *splitters* para distribuir la señal. Son dispositivos pasivos, lo que significa que no necesitan alimentación para trabajar, con todos los beneficios que eso conlleva. Implica una reducción en los gastos por el consumo eléctrico, además de que no hay sobrecalentamientos y por tanto no se necesitan dispositivos de ventilación ni existen peligros de descargas eléctricas, ni cortocircuitos ni incendios. Todos estos problemas han de tenerse en cuenta en despliegues de redes basadas en Ethernet, compuestas por un conjunto de equipos activos, switches, de mayores dimensiones y conectados mediante enlaces punto a punto.

Figura 2.7: *Splitter* óptico

2.2.3. Características del medio físico

En cuanto al medio físico utilizado, es una gran ventaja el empleo de fibra óptica hasta los equipos de usuario frente al uso del par trenzado de cobre, principalmente en términos de ancho de banda y alcance. El estándar GPON sobre fibra monomodo admite tasas de 2.5 Gbps en el enlace descendente y 1.25 Gbps en ascendente, con un alcance de 20 km sin necesidad de regenerar la señal. Estos datos distan mucho en el caso de emplear par trenzado de cobre, ya que si alcanzamos tasas de 1 Gbps, tendremos un alcance máximo de 100 metros. Esto es debido a que la fibra óptica presenta ventanas de transmisión en longitudes de onda con muy bajas atenuaciones. En la Tabla 2.1 se muestran los valores máximos de atenuación según la longitud de onda de trabajo.

Tabla 2.1: Atenuación en la fibra óptica

Longitud de onda	Atenuación
1310 nm.	$\leq$ 0.35 db/km.
1490 nm.	$\leq$ 0.25 db/km.
1550 nm.	$\leq$ 0.2 db/km.

Un beneficio añadido es la escalabilidad que tienen las redes de fibra óptica gracias al empleo de multiplexación por división de longitud de onda (WDM), tecnología que permite aumentar el ancho de banda disponible multiplexando varias señales con diferentes longitudes de onda sobre una única fibra óptica.

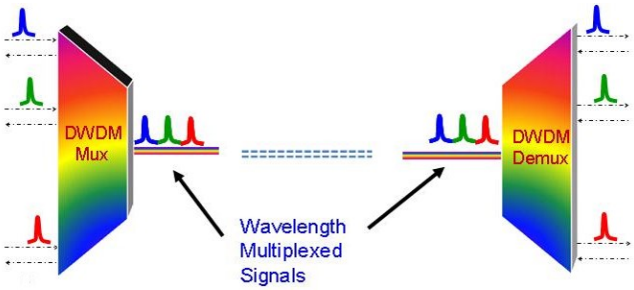


Figura 2.8: Multiplexación WDM

Esto implica que, una vez realizado el despliegue de fibra, no es necesario hacer cambios sobre él para aumentar la capacidad de la red. Si tenemos desarrollada una red GPON, podremos evolucionar a XGPON (tasas de 10Gbps compartidos), WDM PON (1 Gbps simétrico para cada usuario) y 10G-PON (10 Gbps simétricos para cada usuario) sin que la modificación de la infraestructura de fibra suponga un gasto añadido. Esto presenta una ventaja respecto a las redes basadas en cobre, ya que los cables Ethernet se clasifican en categorías según la tasa de transmisión soportada y por tanto, si queremos aumentar la capacidad de la red debemos cambiar el cableado a una categoría superior.

La fibra también tiene ventajas respecto al par trenzado en cuanto a dimensión y peso. Además, en un tubo de fibra óptica se pueden transportar hasta 512 fibras, simplificando aún más el diseño, y permitiendo la posibilidad de sobredimensionar el despliegue para una futura expansión de la red. Por otra parte, aunque se tienda a pensar que el precio de la fibra es muy superior al del cable Ethernet, ha disminuido en los últimos años y seguirá en decrecimiento a consecuencia del aumento en su producción. Esto también implica que no supone un gran coste aplicar redundancia en una fibra teniendo dos para una misma red, a diferencia del coste de aplicar redundancia en una red punto a punto, duplicando todos los enlaces de la red. En caso de caída del enlace, una ventaja adicional que presenta la fibra óptica es que se puede precisar la localización del fallo en la fibra mediante el uso de instrumentos de medida óptica como el OTDR (*Optical Time Domain Reflectometer*).

Por último, la fibra óptica presenta adicionalmente una serie de ventajas en la seguridad de la red, ya que, a diferencia del par de cobre, ni emite ni se ve afectada por radiación electromagnética, evitando de esta manera interferencias y acciones intrusivas de escucha. El hecho de que no conduzca la corriente eléctrica implica la ausencia de problemas por descargas eléctricas, cortocircuitos, incendios, etc.

2.3. Estudio de capacidad de la red GPON

El estándar GPON soporta tasas de 2.5 Gbps en el enlace descendente y 1.25 Gbps en ascendente, compartidos por los 64 usuarios que pueden llegar a componer la red. Gracias a la asignación dinámica del ancho de banda que proporciona GPON, la red puede asignar un mayor ancho de banda a un usuario al que teóricamente le correspondería si la asignación fuese estática.

El equipo de cabecera de redes GPON fabricado en Telnet, se denomina SmartOLT y dispone de cuatro puertos GPON, cuatro puertos Gigabit Ethernet y un puerto 10 Gigabit Ethernet, proporcionando tres modos de funcionamiento en cuanto a la conmutación de tráfico según el grado de ocupación de las redes GPON.

Figura 2.9: SmartOLT de Telnet Redes Inteligentes

En el primer modo de funcionamiento cada uno de los puertos Gigabit Ethernet estaría vinculado de manera dedicada a cada uno de los puertos GPON disponibles. Este modo se utilizaría en redes pequeñas de pocos usuarios que no excedan el Gigabit proporcionado por la cada uno de los puertos.

Los puertos Gigabit Ethernet también pueden actuar de manera compartida para las redes GPON conectadas, aumentando el ancho de banda ofrecido cuando el número de redes y de usuarios se incrementa. Este sería el segundo modo de empleo y debido a su carácter compartido se mejoraría la eficiencia en transmisión de tráfico multicast.

Por último, cuando la ocupación de las redes GPON es muy alta, la OLT también tiene la posibilidad de utilizar un puerto 10 Gigabit de transporte compartido para los cuatro puertos, soportando el total de tráfico demandado por ellos, tanto ascendente como descendente.

Este mecanismo de funcionamiento permite asimilar el crecimiento de abonados mediante la progresiva agregación de las PON según su número de usuarios, facilitando un crecimiento escalable. Para facilitar la comprensión de este método de funcionamiento, la Tabla 2.2 muestra la eficiencia respecto al tráfico demandado por las diferentes redes y el tráfico que la SmartOLT puede proporcionar:

Tabla 2.2: Eficiencia de los tres modos de conmutación de tráfico de la SmartOLT

Tráfico demandado	4x1G Dedicado	4G Compartido	10G Compartido
1 PON (2.5G/1.25G)	DL[1]:40 % (1/2.5)[2] UL:80 % (1/1.25)	DL:100 % UL:100 %	DL:100 % UL:100 %
2 PON (5G/2.5G)	DL:40 % (1/2.5) UL:80 % (1/1.25)	DL:80 % (4/5) UL:100 %	DL:100 % UL:100 %
3 PON (7.5G/3.75G)	DL:40 % (1/2.5) UL:80 % (1/1.25)	DL:53 % (4/7.5) UL:100 %	DL:100 % UL:100 %
4 PON (10G/5G)	DL:40 % (1/2.5) UL:80 % (1/1.25)	DL:40 % (4/10) UL:80 % (4/5)	DL:100 % UL:100 %

[1]DL: *Downlink*. UL: *Uplink*.
[2]Ratio: Tráfico soportado/Tráfico demandado

Además de la SmartOLT, se va a hacer uso de un switch de agregación, denominado SmartXGS, el cual dispone de 24 puertos 1Gb/10 Gb Ethernet para conectar las diferentes OLTs y conmutar su tráfico hacia el correspondiente CPD (Centro de procesamiento de datos) o *Data Center*. Resulta conveniente realizar un breve análisis del número de SmartOLTs que se pueden llegar a conectar a este switch, dependiendo del tipo de tráfico predominante en la red.

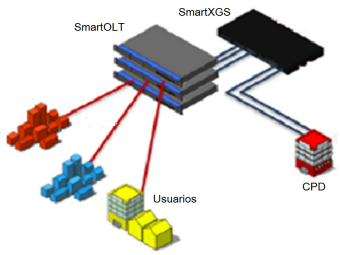


Figura 2.10: Despliegue de red GPON

En un escenario con mayor cantidad de tráfico descendente, tendremos que proporcionar a cada red GPON 2.5 Gbps, lo que implica 10 Gbps en cada OLT para sus 4 puertos. Si el switch SmartXGS tiene 24 puertos 10 Gigabit, podremos conectar hasta 12 OLTs. Este número podría ser superior si tenemos en cuenta la tasa de concurrencia del servicio, es decir, todos los usuarios no estarán demandando el total del tráfico todo el tiempo.

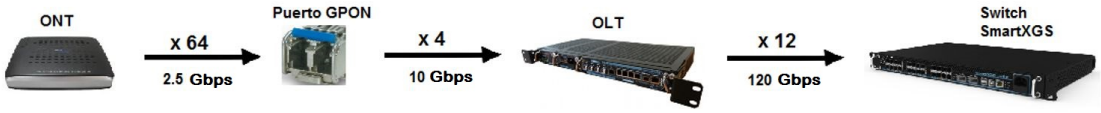


Figura 2.11: Capacidad en escenario con tráfico predominante descendente

En un escenario con tráfico predominante de tipo ascendente, como sería el caso de una red de videovigilancia donde el mayor ancho de banda es consumido por las transmisiones de las cámaras de vídeo hacia la OLT, necesitaríamos proporcionar a cada red GPON 1.25 Gbps, lo que significa 5 Gbps en cada OLT. En este caso, podríamos conectar un mayor número de OLTs al switch SmartXGS, concretamente 16, que generarían 80 Gbps en 16 puertos del switch, los cuales se conmutarían por 8 puertos 10 Gigabit hacia el CPD. Igual que en el caso anterior, este número podría aumentar si tenemos en cuenta la tasa de concurrencia del servicio.

Figura 2.12: Capacidad en escenario con tráfico predominante ascendente

En cuanto al número de equipos, cada OLT puede dar servicio a 64 ONTs en cada puerto GPON, haciendo un total de 256 en los cuatro. En un despliegue con 12 OLTs podríamos tener hasta 3072 equipos de usuario, y con 16 OLTs en escenarios donde predomina el tráfico ascendente podríamos dar conexión a 4096 ONTs.

Por último, a cada ONT se pueden conectar varios dispositivos, ya sea mediante los 4 puertos 10/100/1000Base-TX Ethernet o mediante conexión WIFI. El número de dispositivos dependerá del ancho de banda disponible y el consumo de cada uno de ellos. Para mayor información sobre los dispositivos de seguridad consultar anexo E.

Para comparar en términos de capacidad una red GPON con una red Ethernet P2P como la que se muestra en la Figura 2.13, tendríamos que realizar el cálculo del número de equipos necesarios en una red P2P para dar conexión a tres mil equipos terminales.

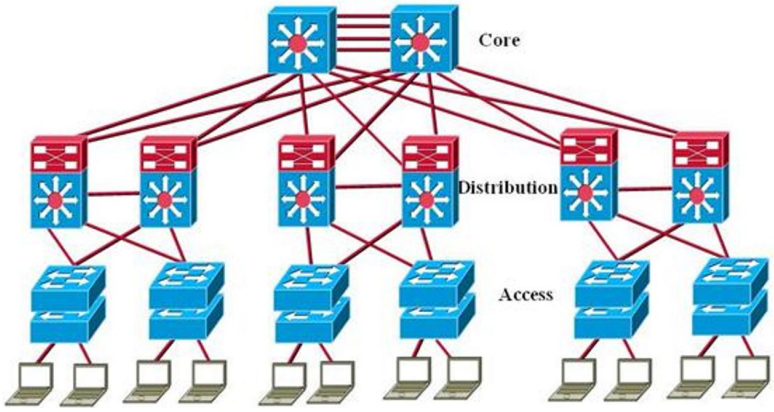


Figura 2.13: Estructura red P2P Ethernet

Con un switch de acceso que disponga de 24 puertos 100 Mbps, necesitaríamos 128 de ellos para dar conexión a 3072 equipos, lo que supone 3072 enlaces punto a punto. Estos 128 switches de acceso necesitarían conmutar esos 2.4 Gbps al menos a cuatro switches de distribución mediante enlaces Gigabit Ethernet aplicando algún tipo de redundancia, y por último dos switches del núcleo, con enlaces 10 Gigabit Ethernet. Se necesitan más de 130 equipos de conmutación, mientras que en la red GPON sólo se requieren 13 (12 OLTs y el switch de agregación) para dar servicio a un mismo número de equipos finales. Esto supone un ahorro aproximado del 90 % en términos de espacio requerido y de energía consumida.

El precio de todos estos equipos activos, su consumo de energía, sus dimensiones, así como la necesidad de un gran espacio para su colocación con su correspondiente ventilación y mantenimiento, hacen que esta red tenga un coste muy superior al de la red GPON. Si nos basamos en estudios realizados [13][14][15] el CAPEX en redes P2P Ethernet es un 20 % superior al de redes GPON y el beneficio aumenta de manera proporcional al número de usuarios.

3. Estudio de la seguridad en redes GPON

Resulta fundamental en la realización de este proyecto dedicar un apartado al estudio de la seguridad en la arquitectura de red que se propone. El estudio debe comenzar con un análisis de los posibles riesgos existentes en este tipo de redes, para posteriormente concretar los riesgos que son evitados por la naturaleza de la red y desarrollar un sistema de detección de alarmas que evite los restantes.

3.1. Análisis de riesgos en la seguridad de una red de fibra óptica

En primer lugar es importante conocer los posibles peligros que pueden afectar a la seguridad de una red basada en fibra óptica.

1. Conectar un equipo intruso a la red mediante un *splitter* desconectando una ONT de nuestra red.
2. Intentar manipular la fibra para extraer señal de ella mediante curvatura.
3. Dañar o romper la fibra para inhabilitar la red.
4. Inyectar luz proveniente de una fuente externa para interferir en nuestra señal.
5. Desconectar la ONT o la OLT para dejar inoperativos los componentes de seguridad conectados a ella.
6. Cambiar la localización de la ONT para su posterior manipulado.
7. Desconectar los dispositivos de seguridad conectados a cada ONT.

Si tenemos en cuenta estos riesgos también estaremos detectando situaciones fortuitas no deseadas como pueden ser fallos en el enlace de fibra, desconexiones de equipos debidas a fallos en la alimentación u otras incidencias que pueden dejar sin conectividad a componentes de nuestra red de seguridad.

Algunos de estos riesgos se evitan debido a las características que presentan las redes GPON en cuanto a su topología, el protocolo de transmisión utilizado y el medio físico empleado. Sin embargo, una buena parte de ellos deben ser tenidos en cuenta a la hora de desarrollar nuestro sistema de detección y control de alarmas para aumentar la seguridad de la red.

3.2. Estudio de las prestaciones en seguridad que aporta GPON

Un buen punto de partida es analizar las ventajas que aporta una red GPON de manera nativa en términos de seguridad, con el objetivo de examinar sus puntos débiles y reforzarlos mediante la implementación de un sistema de detección de alarmas.

Debido a su topología de árbol punto-multipunto (P2MP), la información que transmite una ONT en sentido ascendente sólo es recibida por la OLT, por tanto no llega a las demás ONTs que componen la red, lo que aumenta la seguridad de los datos ante posibles conexiones a la red de ONTs intrusas. Esto es especialmente útil para los sistemas de videovigilancia, ya que la información de interés es la transmitida en el enlace ascendente, las transmisiones de vídeo de las cámaras a la OLT. Para detectar estas posibles ONTs ajenas a nuestro sistema, cada ONT posee un número de serie único que podemos conocer en todo momento, permitiendo sólo la conexión a ONTs con número de serie conocido.

Si la OLT no reconoce el número de serie de una ONT que se ha conectado a su red, le envía un mensaje PLOAM (*Physical Layer Operations, Administration and Maintenance*) (ver anexo B.4) de *'Disable_Serial_Number'* y la ONT pasa a un estado de parada de emergencia en el cual no puede realizar transmisiones en ascendente. En el TGMS esta ONT nos aparece como *'Disabled'* y hasta que el operador no apruebe su admisión en la red no podrá transmitir datos a la OLT. De esta manera se tiene constancia de la existencia de una ONT no registrada intentando conectarse a la red y recibiendo tráfico descendente.

Para evitar que el tráfico descendente pueda ser descifrado, la información transmitida desde la OLT se cifra mediante AES256, esquema avanzado de cifrado por bloques, lo que significa que en caso que se acceda a la señal, no es inmediato conocer la información transmitida. La clave de cifrado es transmitida por la ONT para que no exista posibilidad de ser recibida por las demás ONTs.

Otro de los mensajes de importancia que transmiten las ONTs es el *'Dying_Gasp'*. Se trata de un aviso que lanza la ONT cuando se ha quedado sin alimentación y por tanto, se va a apagar. Se consigue gracias a un condensador implantado en la ONT y de esta manera la OLT está informada al instante del evento.

También el medio físico aporta un nivel de seguridad, ya que la fibra óptica no emite radiación electromagnética, lo que la hace resistente a acciones intrusivas de escucha, a diferencia del par trenzado de cobre utilizado en las redes actuales.

3.3. Diseño y desarrollo del sistema de seguridad

Uno de los objetivos fundamentales de este proyecto es aumentar y fortalecer la seguridad de nuestra red de acceso para asegurar que nuestros datos se transmiten en todo momento de manera fiable y segura. Con esta finalidad se ha desarrollado un sistema de detección y gestión de alarmas capaz de detectar variaciones en parámetros de interés de nuestra red.

El sistema de detección y gestión de alarmas deberá ser capaz de realizar las siguientes tareas:

1. **Adquisición de las potencias que reciben los equipos de la red,** para conocer en todo momento la atenuación que introduce la red en la señal y alertar de posibles variaciones en ella.
2. **Monitorización del tráfico transmitido en ascendente por cada ONT,** para comprobar en tiempo real que el tráfico entre ONT y OLT es el esperado según los dispositivos conectados a cada ONT y advertir en caso de pérdida considerable de tráfico.
3. **Control del estado de conexión de los equipos,** de manera que el sistema nos avise si un equipo de la red se ha quedado sin conexión poniendo en peligro la seguridad de nuestra red.
4. **Cálculo de la distancia entre la OLT y la ONT,** para controlar posibles alteraciones no deseadas en la localización de nuestros equipos.

La adquisición de los parámetros de interés se ha realizado mediante procesos RPC(*Remote Procedure Call*), entre el equipo de desarrollo y la OLT, explicado con un mayor detenimiento en el anexo F.

3.3.1. Potencia recibida por los equipos de la red GPON

La fibra óptica no emite radiación electromagnética ni se ve afectada por ella, lo que evita interferencias y la hace resistente a acciones intrusivas de escucha. Por tanto, si alquien quiere extraer la señal debe manipular directamente la fibra, produciendo una atenuación que puede ser detectada.

Principalmente se puede hablar de dos métodos de extracción de señal en la fibra óptica:

- **Extracción mediante *splitters* y conectores:** Desconectar una ONT de la red y conectar un *splitter* en su lugar para distribuir la señal hasta un equipo intruso.
- **Extracción mediante curvatura de la fibra:** Al curvar la fibra, el ángulo de incidencia sobre la pared del núcleo va a variar, provocando que un pequeño porcentaje de la señal se refracte. Con un equipo especializado se podría llegar a recuperar la información. El esquema sería similar al que aparece en la Figura 3.1.

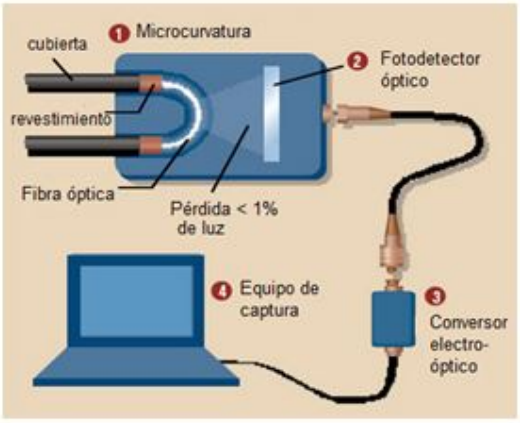


Figura 3.1: Extracción de señal por curvatura de la fibra

Ambos casos producirán una reducción en la potencia recibida que deberá ser detectada por nuestro sistema de seguridad. De esta manera se evitarían ataques del tipo *Man in The Middle* o *sniffing*[1], problemas comunes de privacidad en redes Ethernet y difícilmente detectables. También se producirá una variación en la potencia recibida en los equipos en caso de jamming, un intento de saturar la red mediante la inyección de luz continua, causando interferencias dentro del sistema, lo que inhabilitaría nuestra red de seguridad.

Por esta razón, un parámetro importante a vigilar en nuestro sistema de seguridad será la potencia que reciben los equipos que componen la red, tanto la OLT como las diferentes ONTs. Para ello se ha desarrollado un sistema de adquisición y almacenamiento de datos para su posterior análisis.

Cuando capturamos la potencia recibida por la OLT y por la ONT debemos tener en cuenta lo siguiente. La OLT está transmitiendo continuamente tráfico a las diferentes ONTs de su red, por tanto puede considerarse como una fuente de luz continua. Esto significa que la potencia recibida en las ONTs tendrá menos variaciones y su medida será más constante.

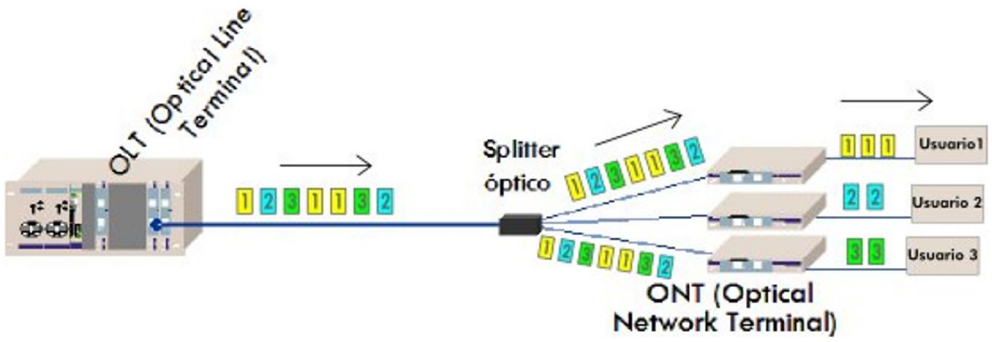


Figura 3.2: Transmisión en el enlace descendente

[1]Capturar la información de la red con un equipo intruso.

Por el contrario, la ONT transmite a ráfagas en los periodos que le asigna la OLT, lo que provoca unas variaciones significativas en la medida de la potencia recibida en la OLT dependiendo del instante de adquisición de dicha medida. También afectará la longitud de las tramas recibidas, ya que variará el tiempo que tiene el conversor analógico para calcular la potencia de la señal.

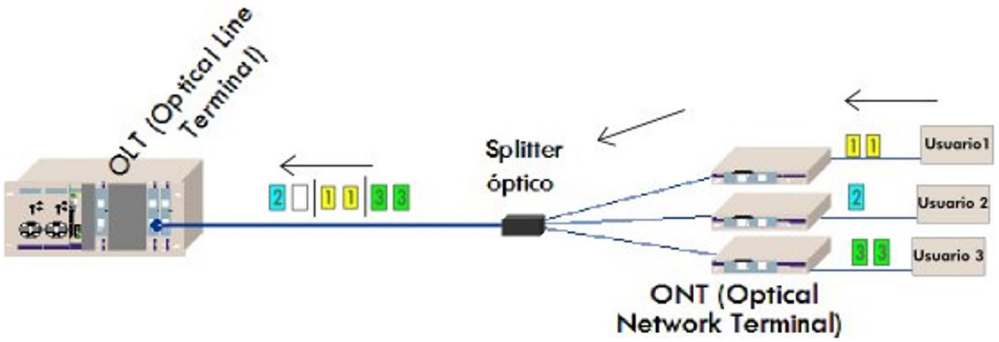


Figura 3.3: Transmisión en el enlace ascendente

Por esta razón, vamos a tener una componente aleatoria en los valores de potencia recibida en la OLT provocando variaciones en la medida. Además, los componentes electrónicos también aportan cierta aleatoriedad, así como las reflexiones causadas en el medio óptico.

Para desarrollar un sistema que detecte atenuaciones reales de manera eficiente tenemos que proporcionar un análisis de datos robusto que sea capaz de detectar todos los posibles datos anómalos con mínima tasa de falsas alarmas. Para detectar estos datos anómalos disponemos de una serie de herramientas estadísticas [16] basadas en diferentes parámetros que nos permiten establecer un umbral para distinguir valores atípicos de valores normales. Estos valores atípicos se denominan *outliers* y tienen un efecto negativo en el análisis de datos, produciendo una posible distorsión en algunos parámetros estadísticos.

Análisis estadístico

El primer criterio de detección de *outliers* que se puede utilizar está basado en la media y la desviación típica. Este criterio sólo es válido si los datos siguen una distribución normal. Aplicando la desigualdad de Chebyschev, sea X variable aleatoria de media μ y varianza finita σ^2, entonces, para todo número real $a > 0$,

$$P(|X - \mu| > a\sigma) \leq \frac{1}{a^2} \tag{3.1}$$

Por tanto en el intervalo $(\mu - a\sigma, \mu + a\sigma)$ se encuentran el $[(1 - \frac{1}{a^2})100]\,\%$ de las muestras. Particularizando con a=3, en el intervalo $(\mu - 3\sigma, \mu + 3\sigma)$ se situarán el 89 % de los datos. Por tanto, tomaremos un dato como *outlier* si está separado de la media más de tres desviaciones típicas.

El inconveniente de trabajar con la media es que es una medida muy afectada por la dispersión, por tanto cuanto menos homogéneos sean los datos, menos información proporciona. Además, tanto la media como la desviación estándar también se ven muy afectadas por la presencia de valores extremos ya que no son medidas robustas. En el caso del análisis de los valores de potencia recibidos, podemos capturar valores que disten mucho de la realidad debido a un fallo en el sensor de captura o por reflexiones en el medio óptico, lo cual modificaría los parámetros estadísticos de una manera no deseada.

Por este motivo se propone un segundo criterio de detección de *outliers*, el método de Tukey, basado en parámetros de estadística robusta como son la mediana y el rango intercuartílico. Este método es menos sensible a oscilaciones de los valores de la variable, y es más representativo que el análisis con la media aritmética cuando la población es bastante heterogénea. Además, este método no hace ninguna suposición sobre la distribución de los datos, por tanto no tienen por qué seguir una distribución normal, al contrario de lo que sucedía con la media y la desviación típica. La mediana y los cuartiles no son representativos cuando la cantidad de datos es pequeña, por tanto al principio necesitaremos un tiempo determinado de recogida de datos hasta que los valores de los cuartiles sean lo suficientemente representativos.

La mediana representa el valor de la variable en la posición central de un conjunto de datos ordenados. Es un caso particular de los cuartiles. Los cuartiles son los tres valores que dividen al conjunto de datos ordenados en cuatro partes porcentualmente iguales. El primer cuartil (Q1) es el valor que deja por debajo al 25 % de los valores. El segundo cuartil se corresponde con la mediana (Q2) ya que deja por debajo al 50 % de los valores, igual que por arriba. El tercer cuartil (Q3) es superior al 75 % de los valores.

Los cuartiles son fácilmente representables en el gráfico conocido como *box-plot* o diagrama de caja, desarrollado por el estadístico norteamericano John W. Tukey en 1977, tal y como se muestra en la Figura 3.4.

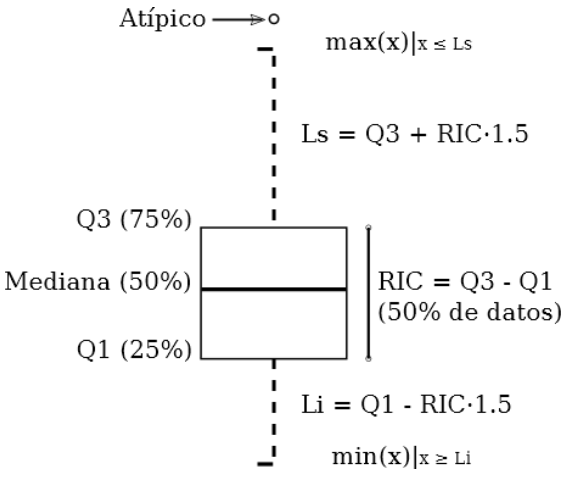


Figura 3.4: Box-plot o diagrama de caja

La diferencia entre el tercer cuartil y el primero (Q3-Q1) se conoce como rango intercuartílico (RIC):

$$RIC = Q_3 - Q_1 \tag{3.2}$$

El límite superior de la caja corresponde al cuartil Q3 y el límite inferior al cuartil Q1, por tanto la altura de la caja vendrá determinada por el rango intercuartílico. De la caja salen unas líneas que delimitan el rango de valores que se consideran normales. Este rango tiene su límite superior en Q3+1.5xRIC y su límite inferior en Q1-1.5xRIC. Los valores fuera de este rango serán considerados *outliers*. Además, si el valor está fuera del rango (Q1-3xRIC, Q3+3xRIC) es considerado outlier extremo.

$$x \notin (Q1 - 1{,}5RIC, Q3 + 1{,}5RIC) \Rightarrow Outlier\ leve \tag{3.3}$$
$$x \notin (Q1 - 3RIC, Q3 + 3RIC) \Rightarrow Outlier\ extremo \tag{3.4}$$

El siguiente paso es aplicar estos métodos estadísticos al conjunto de muestras recogido. Se han capturado más de 700 muestras para realizar el análisis, y se ha representado su distribución en un histograma, mostrado en la Figura 3.5:

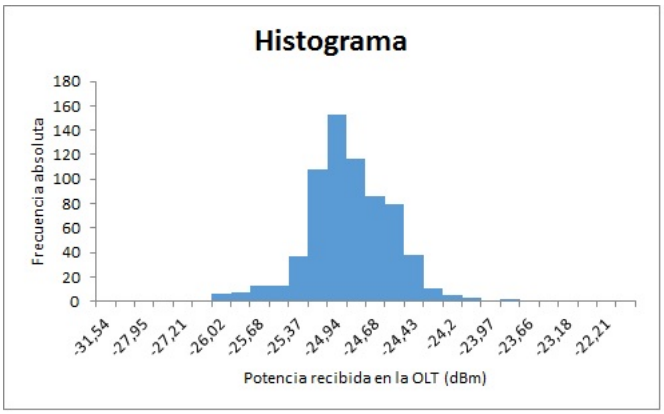


Figura 3.5: Histograma de la potencia recibida en la OLT

En el histograma se puede observar que la variable no sigue una distribución normal, por tanto la media y la desviación típica no serían parámetros estadísticos representativos. Para esta distribución de la variable, se han calculado los parámetros estadísticos de interés, cuartiles y mediana, y los resultados se recogen en la Tabla 3.1 (en dBm):

Tabla 3.1: Parámetros estadísticos

Primer cuartil (Q1)	-25.08
Mediana (Q2)	-24.94
Tercer cuartil (Q3)	-24.68

Con estos datos podremos calcular el rango intercuartílico, y con ello determinar el rango de valores que nuestro sistema va a considerar como normales.

$$RIC = Q_3 - Q_1 = 0{,}4 \tag{3.5}$$

$$Outlier\ leve \Rightarrow x \notin (Q1 - 1{,}5RIC, Q3 + 1{,}5RIC) = (-25{,}68, -24{,}08) \tag{3.6}$$
$$Outlier\ extremo \Rightarrow x \notin (Q1 - 3RIC, Q3 + 3RIC) = (-26{,}28, -23{,}48) \tag{3.7}$$

En la implementación del sistema se ha considerado el primer rango (Q1-1.5RIC, Q3+1.5RIC) en la determinación de valores anómalos, ya que el segundo intervalo (Q1-3RIC,Q3+3RIC) es poco restrictivo.

Un gráfico adecuado para la representación gráfica de estos parámetros es el *box-plot* o diagrama de caja como el de la Figura 3.6. Como hemos mencionado antes, los límites de la caja son el primer y tercer cuartil, y está dividida por la mediana. Las líneas perpendiculares comprenden el rango (Q1-1.5RIC,Q3+1.5RIC).

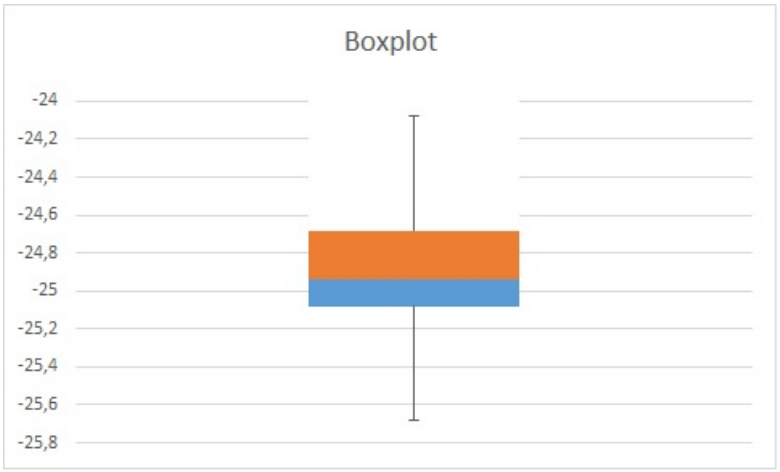


Figura 3.6: Boxplot de la potencia recibida en la OLT

El sistema deberá generar una alarma si detecta variaciones en la atenuación introducida por la red. Una única detección de un valor atípico en la potencia recibida generará una alarma de menor importancia, ya que puede ser a causa de un error puntual que no represente correctamente el estado de la red. Sin embargo, la detección de una alarma de manera repetitiva podría significar un cambio real en la atenuación de la red, por tanto se ejecutaría una alarma de mayor grado con el fin de alertar al usuario de una posible situación crítica. De este modo evitamos las falsas alarmas y mejoramos la eficiencia del sistema. El ratio para considerar una alarma como activa será predeterminado por el operador y serán desactivadas cuando se recupere la situación de normalidad.

También es conveniente conceder al sistema de análisis un periodo inicial de calibración para establecer unos parámetros estadísticos representativos de la red, y de este modo evitar falsas alarmas cuando se conecte una ONT por primera vez.

3.3.2. Tráfico transmitido en el enlace ascendente por cada ONT

La OLT dispone de una serie de contadores de bytes tanto de las tramas que recibe en el enlace ascendente como de las tramas que transmite en descendente. Para este caso en concreto, es interesante monitorizar y controlar el tráfico ascendente que recibe la OLT procedente de cada una de las ONTs que componen la red, y de esta manera comprobar en todo momento que el tráfico generado por los dispositivos de seguridad conectados a las ONTs se corresponde con las tasas de transmisión esperadas. Este control del tráfico será mas eficiente en el caso de cámaras de videovigilancia, ya que generan un flujo constante del orden de Mbps, por lo tanto será más fácil detectar si una cámara ha dejado de enviar señal a la ONT.

El sistema debe alertar cuando detecte una variación significativa en el tráfico transmitido por una ONT. De esta manera se informará de posibles fallos en la transmisión de la señal generada por las cámaras hasta la ONT. Estos fallos pueden ser debidos a desconexiones en la alimentación de la cámara o en el enlace entre la ONT y la cámara. Pueden estar causados por una manipulación de los equipos o de manera fortuita. En ambos casos se deberá informar al usuario de la falta de señal de vídeo.

Si se utilizan cámaras que sólo graban y transmiten en caso de detectar movimiento o alarma, se podrá hacer uso de este contador de tráfico ascendente para avisarnos del momento en el que la cámara empieza a generar datos de vídeo y por tanto, de la aparición de una situación de alerta. Como el tráfico es diferenciado por ONT, podremos conocer el equipo que presenta problemas y localizar así más fácilmente el dispositivo de seguridad inoperativo. Dependiendo de la tasa recibida también se podrá saber si el fallo se ha producido en uno o varios dispositivos.

Por último, también se puede usar este contador para tener un control general del tráfico soportado por la red y de esta manera saber si es necesario ampliarla añadiendo equipos, tanto ONTs como OLTs.

3.3.3. Estado de conexión de los equipos

La OLT puede detectar a través de la interfaz OMCI el cambio de estado de una determinada ONT e informar al sistema para que tenga constancia de ello. El TGMS desarrollado en la actualidad no otorga tanta importancia a los estados de desconexión porque el usuario puede apagar la ONT cuando no la necesite, sin embargo en una red de seguridad deben permanecer operativas en todo momento.

Si alguna de nuestras ONTs se desconecta sin nuestro conocimiento, ya sea debido a la manipulación de una persona o a un fallo en la alimentación, será motivo de alarma, ya que nos quedaremos sin conexión en los equipos de vigilancia asociados a esa ONT, dejando zonas de interés vulnerables.

3.3.4. Distancia entre OLT y ONT

Resulta importante para nuestro sistema conocer en todo momento la distancia en la que se encuentran las ONTs respecto a la OLT, ya que si este parámetro cambia a lo largo del tiempo significa que alguien ha cambiado la localización de la ONT, añadiendo o quitando cable de fibra óptica, con la posibilidad de haber introducido nuevos elementos no deseados en nuestra red. Debido a la baja atenuación que introduce la fibra óptica, es posible que la variación en la potencia no fuese significativa y por tanto no se detectase una alarma monitorizando los valores de potencia recibidos.

Para determinar ese valor de distancia, capturaremos el valor del tiempo de ecualización que la OLT asigna a cada una de las ONTs para situarlas a la misma distancia virtual mediante el proceso de *ranging*. De esta manera se evitan las colisiones entre las transmisiones de cada una de ellas en el enlace ascendente. Este tiempo de ecualización depende de la velocidad de la luz y de la distancia, de manera que el tiempo asignado es mayor cuanto más cerca está la ONT de la OLT. Para mayor información acerca del proceso de *ranging*, consultar anexo H.

En el cálculo de la distancia a partir del tiempo de ecualización, se debe realizar un proceso de calibración, mediante el cual conectemos una longitud de fibra conocida y guardemos el valor del tiempo de ecualización proporcionado por la OLT. Con estos datos determinados podemos calcular la distancia hasta la ONT. Este valor del tiempo de ecualización es asignado en el inicio de la comunicación, por tanto es siempre el mismo durante una sesión, desde la conexión de la ONT hasta su desconexión. Sin embargo, cuando una ONT se desconecte y se vuelva a conectar, este valor puede cambiar debido a la falta de precisión en la medida, aunque no de manera significativa.

Las variaciones en esta medida son causadas por el tiempo de procesado del mensaje de *ranging* en la ONT. La OLT cuenta el tiempo que transcurre desde que manda el mensaje hasta que lo recibe, y por tanto el tiempo total se verá afectado por lo que tarde la ONT en procesar y contestar el mensaje. Por esa razón existirán variaciones en el cálculo de la distancia para diferentes ONTs que se encuentren a una misma distancia de la OLT. Para el sistema de seguridad, será importante saber distinguir entre valores de distancia normales y valores que puedan considerar un cambio real en la localización de la ONT. Con este fin, sería conveniente caracterizar cada ONT en un tiempo de calibración inicial para conocer el rango de valores que podemos asumir como normales en la medida de la distancia. De esta manera evitaríamos falsas alarmas en situaciones de normalidad.

Para ello se han realizado una serie de pruebas de medición con distintas ONTs comerciales. Las pruebas han consistido en registrar el valor de distancia que almacenaba el sistema en cada inicio de sesión de una determinada ONT a una distancia conocida y fija de la OLT.

Las pruebas se han realizado con las tres ONTs que han compuesto nuestra maqueta:

- GPON Tester, equipo de certificación de redes GPON, dedicado a realizar medidas y por tanto con una mayor precisión.
- ONT con 4 puertos Gigabit Ethernet, 2 puertos POTS (*Plain Old Telephone Service*) y un puerto RF, semejante a las que nos podemos encontrar en el mercado actual.
- ONT monopuerto Gigabit Ethernet.

Las tres ONTs se han conectado a la OLT mediante una fibra óptica de aproximadamente ocho metros y medio de longitud. Para el estudio se han recogido 100 muestras, representando gráficamente la distribución de la variable mediante un histograma en la Figura 3.7. (en la Tabla 3.2 se muestran las 10 primeras muestras):

Tabla 3.2: Mediciones de distancia (en metros)

Nº muestra	GPON Tester	ONT 4GE+2POTS+RF	ONT 1GE
1	7.7	101.3	103.7
2	8.8	102.0	105.0
3	9.2	100.1	104.2
4	7.3	101.5	102.4
5	8.6	101.1	104.4
6	8.7	101.7	103.8
7	7.5	101.6	102.9
8	9.2	102.0	102.9
9	9.0	100.7	104.8
10	8.7	102.2	105.0

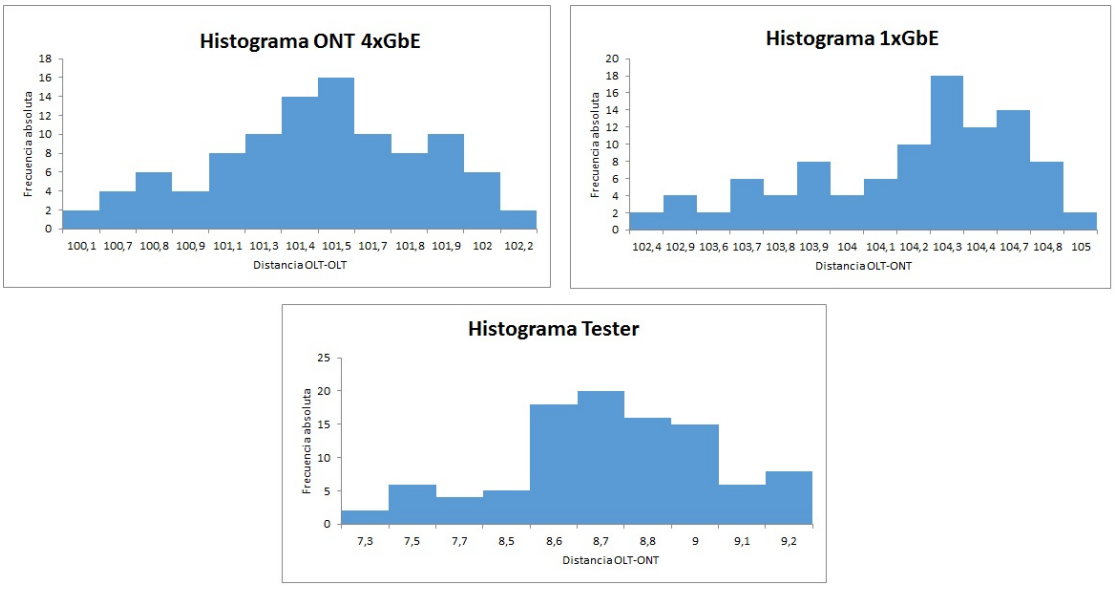


Figura 3.7: Histograma de la distancia registrada en las diferentes ONTs.

Como se puede observar, el GPON Tester fabricado para realizar este tipo de medidas tiene una mayor exactitud que las ONTs comerciales, ya que el tiempo de procesado del mensaje de *ranging* es mucho menor al de las otras ONTs.

Los histogramas demuestran que la variable no sigue una distribución normal, por tanto deberemos analizar parámetros estadísticos tales como la mediana y los cuartiles para determinar el rango de valores considerados como normales y evitar así falsas alarmas. En la Tabla 3.3 se muestran los resultados de las distintas medidas.

Tabla 3.3: Parámetros estadísticos (en metros)

	GPON Tester	ONT 4GE	ONT 1GE
Mediana	8.70	101.55	104.15
Primer cuartil Q1	8.60	101.10	103.80
Tercer cuartil Q3	9.00	101.80	104.40
RIC (Q3-Q1)	0.4	0.7	0.6
(Q1-1.5RIC,Q3+1.5RIC)	(8 , 9.6)	(100.05 , 102.85)	(102.9 , 105.3)
(Q1-3RIC,Q3+3RIC)	(7.4 , 10.2)	(99 , 103.9)	(102 , 106.2)

En este caso y debido fundamentalmente a la asimetría de los datos, el intervalo más restrictivo (Q1-1.5RIC,Q3+1.5RIC) daría lugar a falsas alarmas en situaciones de normalidad, por tanto el sistema adoptará el segundo intervalo (Q1-3RIC,Q3+3RIC) para determinar si el valor capturado es anómalo y debe alertar al usuario de un cambio real de la localización de la ONT.

4. Implementación del sistema

Una vez realizado el análisis de la seguridad en redes GPON y el desarrollo del sistema de detección y gestión de alarmas, el siguiente paso es construir una maqueta de una red GPON y diseñar la herramienta web que actúe de interfaz entre el usuario y el sistema de control de alarmas . Por último, se deben realizar las pruebas que verifiquen el correcto funcionamiento de nuestro sistema de seguridad.

4.1. Diseño de una maqueta funcional

El primer paso para realizar estas pruebas es el diseño y montaje de una maqueta funcional de una red GPON con todos sus componentes. Para el montaje de la maqueta se ha usado una OLT, utilizando uno de sus puertos para conectar una red GPON compuesta de tres ONTs y un *splitter* con división 1:6. Además se ha utilizado una bobina de fibra óptica monomodo de 2 kilómetros y medio de longitud para simular un despliegue más realista.

En cuanto a la atenuación introducida en la red, el *splitter* 1:6 en el enlace descendente divide la potencia de entrada desde la OLT entre sus 6 salidas hacia las ONTs, por tanto introduce una atenuación en la señal a la salida de 1/6. La fibra óptica introduce una atenuación de 0.2 - 0.35 dB[1] por kilómetro, por tanto en 2 kilómetros y medio tendremos una atenuación máxima aproximada de 0.9 dB.

Para simular el caso más desfavorable que contempla el estándar GPON, con un nivel de *splitter* de 1:64 y una distancia entre OLT y ONT de 20 kilómetros, se ha optado por colocar un atenuador de 15 dB en el puerto de la OLT. En esta situación el *splitter* introduciría una atenuación de 1/64 y la fibra óptica 7 dB como máximo. También se deberían tener en cuenta las atenuaciones en empalmes y conectores en caso que hubiera.

$$Atenuación\ teórica = 10log(64)dB + 0{,}35dB/km\ x\ 20km = 25dB \tag{4.1}$$

$$Atenuación\ en\ maqueta = 10log(6)dB + 0{,}35dB/km\ x\ 2{,}5km + 15dB = 23{,}65dB \tag{4.2}$$

[1]La atenuación depende de la longitud de onda de trabajo

Además de los componentes de la red GPON, hemos conectado una cámara IP de videovigilancia a uno de los puertos Gigabit Ethernet de una ONT para analizar el tráfico que introduce en la red. La maqueta completa sería la mostrada en la Figura 4.1:

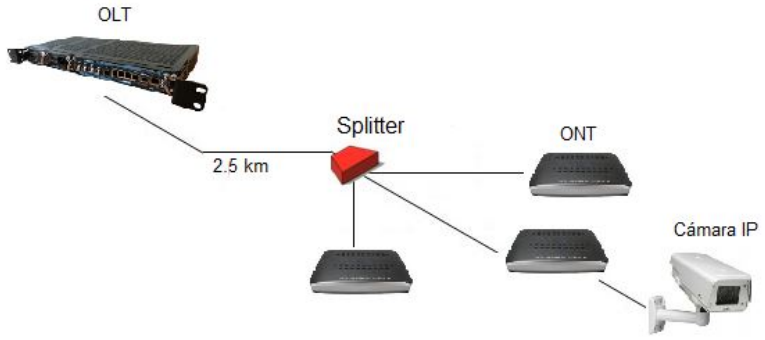


Figura 4.1: Diseño de la maqueta

4.2. Diseño de la interfaz Web

Con la maqueta montada y funcionando correctamente, el siguiente paso es el desarrollo de una página web que facilite al usuario la visualización en tiempo real de los parámetros de interés que captura el sistema de adquisición. Para una mayor información sobre el desarrollo de la interfaz web, consultar anexo G.

La interfaz web se descompone en seis apartados de monitorización y control en tiempo real de los siguientes parámetros:

1. Potencia recibida tanto en OLT como en las ONTs de la red.
2. Tráfico en ascendente que recibe la OLT de cada ONT.
3. Distancia entre la OLT y cada ONT.
4. Estado de conexión de los equipos de la red GPON.
5. Eventos y alarmas OMCI comunicadas por la OLT. Este punto ya estaba implementando en el TGMS, con una mejor explicación en el anexo C.
6. Registro de alarmas activadas en todas las secciones.

En el primer apartado se visualizan los datos de **potencias recibidas** tanto en la OLT como en las diferentes ONTs de la red. La página web da la posibilidad de monitorizar la potencia recibida en tiempo real tanto en formato de tabla como en forma de gráfica para cada una de las ONTs conectadas a la red. Es importante verificar que no se producen falsas alarmas en situaciones de normalidad.

SerialNumber OLT	SerialNumber ONT	Potencia recibida en OLT (dBm)	Potencia recibida en ONT (dBm)	Tiempo
00:09:58:DD:00:1E	0x544c524900000051	-26.38	-29	2014-01-21 15:14:07
00:09:58:DD:00:1E	0x544c5249000000c9	-24.68	-25.37	2014-01-21 15:14:06
00:09:58:DD:00:1E	0x544c5249000000d0	-19.95	-20.45	2014-01-21 15:14:04
00:09:58:DD:00:1E	0x544c524900000051	-26.38	-29	2014-01-21 15:13:57
00:09:58:DD:00:1E	0x544c5249000000d0	-20.08	-20.45	2014-01-21 15:13:44
00:09:58:DD:00:1E	0x544c5249000000d0	-19.91	-20.45	2014-01-21 15:13:24
00:09:58:DD:00:1E	0x544c5249000000c9	-24.81	-25.37	2014-01-21 15:13:04
00:09:58:DD:00:1E	0x544c5249000000d0	-20.04	-20.45	2014-01-21 15:13:03
00:09:58:DD:00:1E	0x544c524900000051	-26.57	-28	2014-01-21 15:12:55
00:09:58:DD:00:1E	0x544c5249000000d0	-19.58	-20.45	2014-01-21 15:12:43

Figura 4.2: Listado de la potencia recibida

Como se puede ver en la Figura 4.2, cada ONT se muestra debidamente identificada con su número de serie, el cual es único, y el número de serie de la OLT a la cual está conectada.

En la gráfica de la Figura 4.3 se representa la potencia recibida en la OLT procedente de una determinada ONT a lo largo del tiempo. Además, se muestra una línea de color amarillo representando el valor de la mediana del conjunto de datos recogidos hasta ese momento, y dos líneas verdes adicionales que limitan el rango de valores considerados por el análisis estadístico como normales. Cualquier valor que supere esos límites será considerado como anómalo y se alertará al usuario.

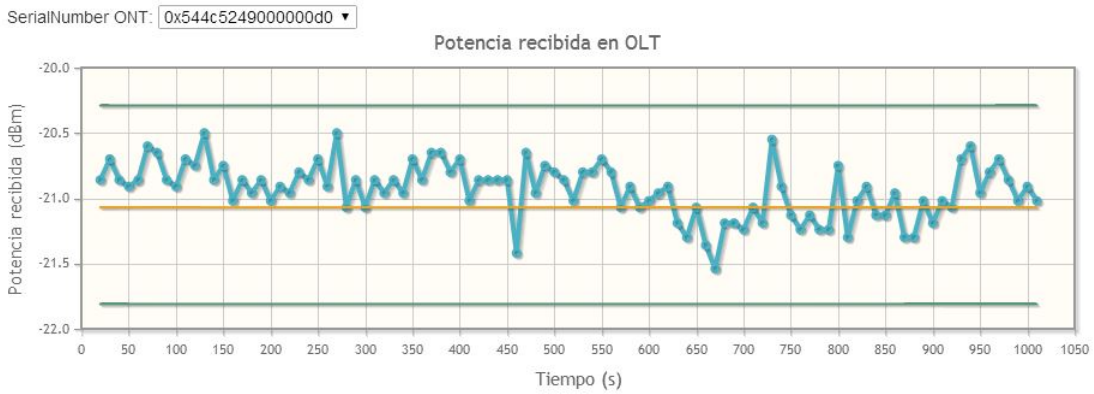


Figura 4.3: Gráfica de la potencia recibida en la OLT

En la gráfica de la Figura 4.4 que representa la potencia recibida en cada ONT se puede comprobar que es un valor mucho más estable que el recibido en la OLT por el motivo mencionado con anterioridad, la OLT se comporta como una fuente de luz continua. Por esta razón no tiene sentido aplicar el método de análisis empleado con la OLT, y solamente se mostrará una línea de color amarillo que indique la mediana de los valores adquiridos.

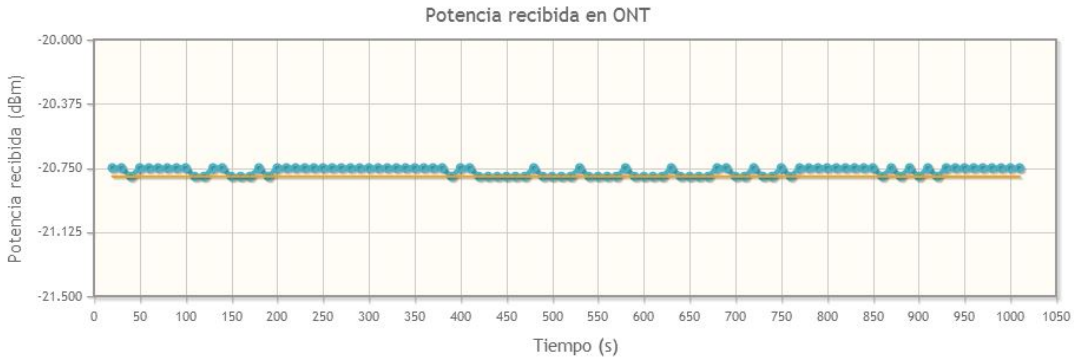


Figura 4.4: Gráfica de la potencia recibida en la ONT

El segundo apartado se centra en el control del **tráfico recibido** por la OLT en todo momento procedente de cada una de sus ONTs, con la finalidad de detectar variaciones que indiquen la pérdida de la transmisión de alguno de los componentes de seguridad conectados. El sistema monitorizará la tasa de transmisión en situaciones de correcto funcionamiento y avisará en el momento que haya un cambio significativo en ella durante un periodo de tiempo predeterminado por el operador para evitar falsas alarmas.

Al igual que en el apartado de la potencia recibida, la herramienta web facilita la monitorización de la tasa en ascendente tanto en formato lista como en una gráfica, como la mostrada en la Figura 4.5 (tasa mostrada en kbps).

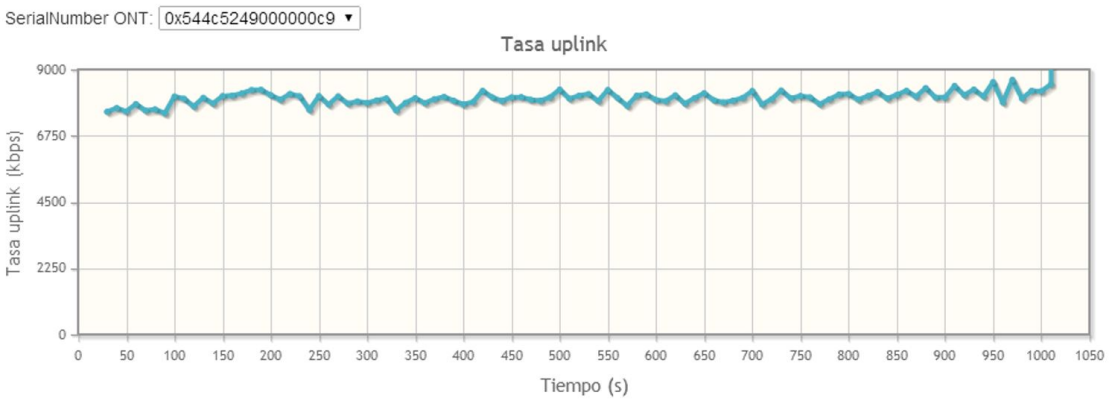


Figura 4.5: Monitorización de la tasa en ascendente por ONT

El siguiente apartado se corresponde con la monitorización de **la distancia** entre la OLT y las distintas ONTs de la red GPON. El sistema implementado puede llegar a gestionar un gran número de redes y equipos. Por esta razón, es necesario una serie de identificadores además del número de serie de la OLT y la ONT. Estos identificadores son:

- **Device** (0-3): Identifica el número de tarjeta de red de la OLT, en caso de que tenga varias, hasta un límite de cuatro.
- **Channel** (0-3): Determina el número de puerto PON al que está conectada la red.
- **ONT-ID** (0-63): Identifica al equipo de usuario dentro de la red GPON.

De esta manera cualquier equipo es fácilmente localizable dentro del sistema. El listado de ONTs con su correspondiente distancia a la OLT se muestra en la Figura 4.6.

ID	SerialNumber OLT	Device	Channel	ONT ID	SerialNumber ONT	Distancia OLT-ONT
1	00:09:58:DD:00:1E	0	0	0	0x544c5249000000d0	2560.5
2	00:09:58:DD:00:1E	0	0	2	0x544c524900000051	2464.4
3	00:09:58:DD:00:1E	0	0	1	0x544c5249000000c9	2556.6

Figura 4.6: Registro de distancias OLT-ONT

Otro apartado importante es controlar durante todo momento **el estado de conexión** de los equipos. En la página web nos aparecerá un listado (ver Figura 4.7.) con todas las ONTs que han estado conectadas a una OLT de nuestra red con sus correspondientes identificadores y su estado actual en tiempo real, además del momento exacto en el que se produjo el cambio de estado.

ID	SerialNumber OLT	Device	Channel	SerialNumber ONT	Estado ONT	Tiempo inicio
0	00:09:58:DD:00:1E	0	0	0x544c4e5412345678	Never connected	2013-12-13 11:45:07
1	00:09:58:DD:00:1E	0	0	0x544c524958d1000d	Never connected	2014-01-15 08:10:34
2	00:09:58:DD:00:1E	0	0	0x544c5249000000d0	Online	2014-02-17 10:21:38
3	00:09:58:DD:00:1E	0	0	0x544c5249000000c9	Online	2014-02-17 10:24:55
4	00:09:58:DD:00:1E	0	0	0x544c524900000051	Online	2014-02-17 10:21:20

Figura 4.7: Estado de conexión de las ONTs

La sección dedicada a mostrar **alarmas OMCI y cambios de estado de las ONTs** estaba ya implementada en el TGMS y simplemente ha sido llevada a nuestro sistema para facilitar al usuario este tipo de información. Las alarmas están numeradas en el anexo C.3 y explicadas con más detalle en la recomendación ITU-T G.984.3 [3]. Los cambios de estado también se detallan en el anexo C.4. En la Figura 4.8 se muestra un ejemplo de la monitorización de este apartado.

OLT Time	Server Time	SerialNumber OLT	Device	Channel	SerialNumber ONT	Event Type	Event ID
2010/01/01-12:08:08	2014-02-10 08:22:27	00:09:58:DD:00:1E	0	0	0x544c524900000051	Evento	Online
2010/01/01-12:07:45	2014-02-10 08:22:04	00:09:58:DD:00:1E	0	0	0x544c524900000051	Evento	Detected
2010/01/01-12:07:45	2014-02-10 08:22:04	00:09:58:DD:00:1E	0	0	0x544c524900000051	Evento	OMCI Error
2010/01/01-12:07:44	2014-02-10 08:22:04	00:09:58:DD:00:1E	0	0	0x544c524900000051	Evento	Detected
2010/01/01-12:07:27	2014-02-10 08:21:47	00:09:58:DD:00:1E	0	0	0x544c5249000000c9	Alarma	Loss of GEM channel delineation ONUi
2010/01/01-12:07:27	2014-02-10 08:21:47	00:09:58:DD:00:1E	0	0	0x544c5249000000c9	Alarma	Loss of GEM channel delineation ONUi
2010/01/01-12:05:47	2014-02-10 08:20:07	00:09:58:DD:00:1E	0	0	0x544c5249000000d0	Evento	Online
2010/01/01-12:05:35	2014-02-10 08:19:55	00:09:58:DD:00:1E	0	0	0x544c5249000000c9	Evento	Online
2010/01/01-12:05:19	2014-02-10 08:19:38	00:09:58:DD:00:1E	0	0	0x544c5249000000d0	Evento	Detected
2010/01/01-12:05:19	2014-02-10 08:19:38	00:09:58:DD:00:1E	0	0	0x544c5249000000c9	Evento	Detected

Figura 4.8: Alarmas OMCI y cambios de estado de las ONTs

Para terminar, en el último apartado se mostrarán al usuario las **alarmas que han sido activadas** en las secciones comentadas anteriormente. De esta manera se facilita su labor y se mejora la rapidez en la visualización. También se dispone de un historial de alarmas para que el usuario tenga a su disposición en todo momento el registro de alarmas de días anteriores. La interfaz web (ver Figura 4.9) permite realizar un filtrado por tipo y grado de alarma, para diferenciar las más importantes, así como mostrar sólo las activas en ese momento.

Figura 4.9: Interfaz web: apartado de alarmas

Los tipos de alarma que pueden aparecer en esta sección se pueden ver en el siguiente apartado dedicado a las pruebas realizadas con el objetivo de simular posibles situaciones reales de peligro.

4.3. Pruebas de simulación

Una parte fundamental en el desarrollo de cualquier sistema de *software* es la realización de pruebas con el fin de verificar su correcto funcionamiento. Para ello se llevarán a cabo una serie de simulaciones que traten de reproducir posibles situaciones reales.

La primera prueba tiene como objetivo comprobar la respuesta del sistema frente a **cambios en la atenuación** que introduce la red. Se debe alertar de las siguientes situaciones:

- Curvatura de la fibra.
- Introducción en la red de un *splitter* con equipo intruso.
- Manipulado con daño o rotura de la fibra.
- Inyección de luz en la fibra por una fuente externa.

También es posible que se produzca una atenuación apreciable en el caso de añadir cable de fibra en el enlace entre OLT y ONT, aunque debido a la baja atenuación que presenta la fibra óptica será más difícil de detectar.

Para simular estas situaciones, realizamos una curvatura en la fibra de nuestra maqueta. En la Figura 4.10 se muestra la gráfica correspondiente a la representación de la potencia recibida en caso de una variación significativa en los valores de potencia registrados durante un periodo de tiempo representativo:

Figura 4.10: Variación en la potencia recibida

Como podemos ver en la gráfica anterior, una variación de 1-2 dBs es fácilmente apreciable. Para facilitar el trabajo al usuario, en el apartado de la página web de alarmas activadas aparecerán varias alarmas correspondientes a los diferentes valores de potencia recibida fuera del rango aceptado. Las primeras serán de menor grado hasta que el sistema detecte que el ratio de valores atípicos supera el umbral determinado para considerar una posible incidencia en la red.

De este modo se alerta al usuario de la aparición de una atenuación extra en el enlace, lo que puede significar una posible situación de peligro para la seguridad de la red o un fallo en su estructura. La alarma se desactivará cuando se reciban valores de potencia correctos durante un periodo de tiempo determinado. En la Figura 4.11 se muestra el apartado de alarmas activadas.

SerialNumber ONT	Motivo de alarma	Valor de alarma	Tiempo activacion	Tiempo desactivacion
0x544c5249000000d0	Potencia recibida en la OLT inferior: Alarma roja	-21.54	2014-01-28 14:45:46	
0x544c5249000000d0	Potencia recibida en la OLT inferior: Alarma amarilla	-22.44	2014-01-28 14:45:26	
0x544c5249000000d0	Potencia recibida en la OLT inferior: Alarma amarilla	-22.29	2014-01-28 14:45:04	

Figura 4.11: Registro de alarmas activadas

También será importante diferenciar este caso anterior, con un cambio en la potencia recibida durante un periodo de tiempo significativo, de la adquisición de datos anómalos en instantes puntuales que no reflejan el estado real de la red (ver Figura 4.12). Pueden ser debidos a un fallo en el sensor de captura, un error en el conversor analógico-digital o reflexiones en el medio óptico.

Figura 4.12: Dato de potencia anómalo puntual

Otra situación en la que debemos comprobar la respuesta del sistema es en la **desconexión de los equipos de la red**, tanto las ONTs como las OLTs. De esta manera podemos alertar de las siguientes incidencias:

- Desconexión de una ONT de nuestra red para conectar un equipo intruso.
- Desconexión de una ONT para añadir mayor longitud de fibra y cambiar su localización.
- Desconexión de una ONT para inhabilitar los dispositivos de seguridad asociados a ella.
- Desconexión de la OLT para inhabilitar la red.
- Desconexión de una ONT a causa de cambios en la potencia que recibe (saturación o falta de señal).

Cuando se detecta la desconexión se muestra una alarma de menor grado durante un minuto (o el tiempo estipulado por el operador) ya que puede ser debida a una reconfiguración o un reinicio del equipo. Sin embargo, cuando el tiempo supera este valor se alerta con una alarma roja de que el equipo no está operativo, y en consecuencia los dispositivos conectados a él.

En la sección de alarmas activadas podremos observar el proceso completo asociado a la desconexión-conexión de una ONT tal y como se muestra en la Figura 4.13. En la desactivación se registra el instante de recuperación de la conexión con la ONT.

Figura 4.13: Activación de alarma por desconexión de ONT

Con los equipos de cabecera, las OLTs, las alarmas se ejecutan de la misma manera. Estos equipos suelen estar en las dependencias del operador, por tanto su manipulación por parte de una persona ajena será más díficil, pero de esta manera controlamos posibles fallos en la conexión o en la alimentación.

Cuando se produce la desconexión de la OLT perdemos también como consecuencia la conexión con todas las ONTs de la red:

ID	SerialNumber OLT	SerialNumber ONT	Motivo de alarma	Valor de alarma	Tiempo activacion	Tiempo desactivacion
1	00:09:58:DD:00:1E	0x544c524900000051	ONT no operativa	Activa	2014-02-11 14:55:50	
2	00:09:58:DD:00:1E	0x544c5249000000c9	ONT no operativa	Activa	2014-02-11 14:55:49	
3	00:09:58:DD:00:1E	0x544c5249000000d0	ONT no operativa	Activa	2014-02-11 14:55:48	
4	00:09:58:DD:00:1E		OLT desconectada	Activa	2014-02-11 14:55:46	

Figura 4.14: Activación de alarma por desconexión de OLT

Respecto al **control de la distancia**, la prueba consiste en añadir un cable de fibra óptica de unos cinco metros entre la OLT y una ONT. Para ello, debemos desconectar el cable de fibra que llega a la ONT, lo que producirá una alarma por desconexión del equipo además de la alarma por el cambio en la distancia entre la OLT y la ONT. En la Figura 4.15 se muestran las alarmas ejecutadas en un cambio de localización de la ONT.

ID	SerialNumber OLT	SerialNumber ONT	Motivo de alarma	Valor de alarma	Tiempo activacion	Tiempo desactivacion
1	00:09:58:DD:00:1E	0x544c5249000000d0	Cambio de distancia	2565.1	2014-02-17 13:05:23	
2	00:09:58:DD:00:1E	0x544c5249000000d0	ONT no operativa	No Activa	2014-02-17 13:04:19	2014-02-17 13:05:23

Figura 4.15: Alarmas por cambio en la distancia OLT-ONT

La siguiente prueba que debemos realizar para verificar que el sistema responde correctamente es la **desconexión de la cámara conectada a la ONT** de la red. El sistema debería detectar un descenso significativo en el tráfico transmitido por esa ONT y mostrar una alarma que alerte al usuario de la incidencia.

SerialNumber OLT	SerialNumber ONT	Motivo de alarma	Valor de alarma	Tiempo activacion
00:09:58:DD:00:1E	0x544c5249000000c9	Descenso de trafico	18.32	2014-02-10 11:10:44

Figura 4.16: Alarma por descenso del tráfico recibido

En la representación gráfica (ver Figura 4.17) también se observa con claridad el descenso en la tasa transmitida por la ONT. En el caso de las cámaras de videovigilancia, el tráfico que van a generar es del orden de Mbps, por tanto la ausencia de flujo va a ser muy apreciable. La cámara utilizada en la maqueta transmite con tasas en torno a 8 Mbps.

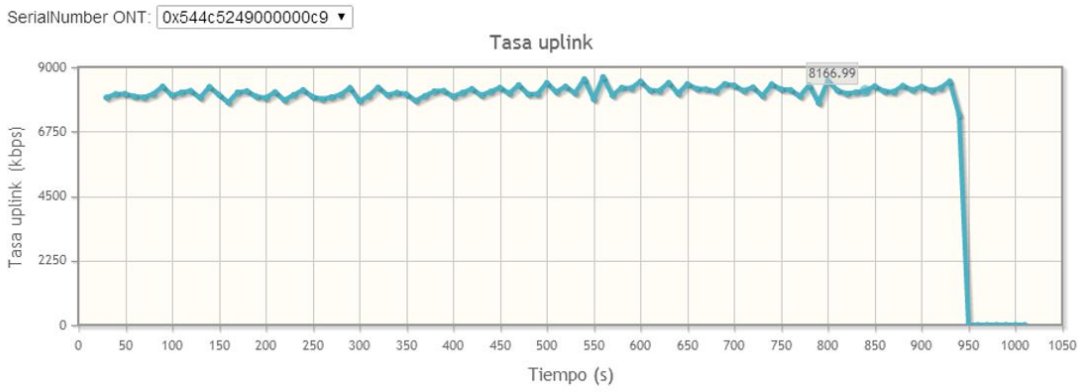


Figura 4.17: Gráfica del tráfico recibido

Por último, cabe destacar que esta serie de alarmas son totalmente complementarias y la ejecución de varias de ellas refuerza la alerta ante una posible situación de peligro para la seguridad de la red. Por ejemplo si se desconecta una ONT y cuando se vuelve a conectar el sistema alerta de un cambio en la localización y un cambio en la potencia recibida, serán indicios de la introducción de un *splitter* en la red con un posible equipo intruso, y el usuario deberá actuar en consecuencia.

En la Tabla 4.1 se sintetizan las pruebas realizadas y se muestran las alarmas que se han ejecutado en cada caso particular.

Tabla 4.1: Pruebas de simulación

	Potencia		Tráfico	Distancia	Desconexión	
	OLT	ONT	en ascendente	OLT-ONT	ONT	OLT
Curvatura en la fibra	✓	✓				
Cambiar ONT de la red por un equipo intruso			✓		✓	
Conectar equipo mediante splitter	✓	✓		✓	✓	
Dañar o romper la fibra	✓	✓	✓[1]		✓[1]	
Introducir luz en la fibra con un láser	✓	✓	✓[2]		✓[2]	
Cambiar localización ONT añadiendo más fibra	✓[3]	✓[3]		✓	✓	
Desconectar cámara			✓			
Desconectar ONT			✓		✓	
Desconectar OLT					✓	✓

El tiempo de detección de estas alarmas dependerá fundamentalmente de la frecuencia de adquisición de datos del sistema. Una mayor rapidez en la detección supondrá capturar más datos en un menor tiempo, aumentando la carga de trabajo y la capacidad de almacenamiento requerida.

En los casos de variación en la potencia y en el tráfico de la red, el tiempo de detección será mayor ya que se necesita registrar una cantidad continuada de muestras para poder determinar si realmente es una situación de riesgo real para la seguridad de nuestra red.

[1] En caso de rotura.

[2] La potencia introducida puede saturar los interfaces ópticos de los equipos, provocando su desconexión.

[3] Dependiendo de la longitud de fibra añadida.

5. Conclusiones y líneas futuras de trabajo

La bajada en el precio de las cámaras de alta definición y la reducción en el coste de almacenamiento hacen necesario considerar el despliegue de redes destinadas a sistemas de seguridad con mayor capacidad de transmisión, pensando inevitablemente en redes de fibra óptica. El análisis realizado en este proyecto verifica los beneficios que aportan las redes ópticas pasivas basadas en el estándar GPON en términos de ancho de banda, costes, eficiencia energética y seguridad. Con el estudio de capacidad de las redes GPON se ha demostrado que pueden dar servicio a un gran número de equipos finales con unas velocidades de transmisión elevadas, y además con una reducción de costes, de consumo energético y de espacio físico requerido en comparación con las redes desplegadas en la actualidad.

Si nos basamos en las pruebas realizadas, la implementación del sistema de detección y gestión de alarmas desarrollado en este proyecto cumple con el objetivo de aportar un mayor grado de seguridad a nuestra red. El sistema da la posibilidad de vigilar en todo momento los valores de potencia, tráfico, distancias y estados de conexión de los equipos, y avisar al usuario de cualquier incidencia que pudiera poner en peligro la seguridad de la red.

En este caso concreto de una red de videovigilancia, va a predominar el ancho de banda ascendente, debido a las transmisiones generadas por las cámaras hacia la OLT. Se puede aprovechar ese ancho de banda disponible en el enlace descendente para proporcionar un servicio complementario. Esto podría ser de gran utilidad en grandes superficies como estaciones, aeropuertos o centros deportivos, donde se proporcione un sistema de seguridad y un servicio adicional como valor añadido, como podría ser información en pantallas, publicidad, distribución de señal de vídeo a nivel interno, conectividad WiFi, etc.

Una opción futura muy interesante sería aprovechar los datos de potencias recibidas almacenados procedentes de todos los equipos de la red y realizar un análisis de consumo eléctrico para estudiar una posible mejora en este aspecto del equipo, evitando además posibles sobrecalentamientos. También se pueden aprovechar estos valores de potencia recogidos para efectuar un estudio sobre la degradación de los láseres de los equipos a lo largo del tiempo.

Por otro lado, también se pueden realizar mejoras en la infraestructura de la red. Sería muy recomendable que la fibra procedente de la OLT se conectara directamente a las cámaras y al resto de componentes. De esta manera, nos ahorraríamos el último tramo de cable Ethernet o de conectividad por WiFi que reducen las prestaciones de la fibra óptica, fundamentalmente en términos de seguridad. Una solución sería utilizar transceptores SFP que permiten la conexión con fibras monomodo, pero en el mercado actual hay muy pocas cámaras que lo incorporen. Una opción más avanzada sería el desarrollo de una tarjeta de red GPON que se pudiera acoplar a cualquier dispositivo y establecer conectividad con la OLT.

A nivel personal, el resultado ha sido completamente satisfactorio. He afianzado los conocimientos adquiridos en la universidad y además los he ampliado en el estudio de nuevas tecnologías como son las redes ópticas pasivas. También me ha resultado muy interesante el aprendizaje en el campo de la programación web y la gestión de bases de datos. El trabajo en la empresa como primer contacto con el mundo laboral ha sido muy gratificante.

Bibliografía

[1] Recomendación ITU-T G.984.1.

[2] Recomendación ITU-T G.984.2.

[3] Recomendación ITU-T G.984.3.

[4] Recomendación ITU-T G.988.

[5] GPON International Training. Telnet Redes Inteligentes S.A.

[6] Diseño, análisis e implementación de un sistema inteligente y distribuido de aprovisionamiento de un sistema FTTH ITU-T G.984 GPON para un operador de telecomunicaciones de ámbito local. PFC. Daniel Calatayud Ferrández. Septiembre 2012.

[7] FTTx PON Technology and Testing. Andre Girard, Senior Member of Technical Staff EXFO Electro-Optical Engineering. 2005.

[8] The problem of upstream traffic synchronization in Passive Optical Networks. Glen Kramer, Department of Computer Science University of California.

[9] Cisco Systems IP Network-Centric Video Surveillance. (white paper)

[10] Huawei Video Surveillance Network Solution. 2012.

[11] Cisco IP Video Surveillance Design Guide. Joel W. King, Technical Leader Cisco Systems. Agosto 2009.

[12] Towards networks of the future: SDN paradigm introduction to PON networking for business applications. Pawel Parol, Michal Pawlowski. Warsaw University of Technology. Septiembre 2013.

[13] Case Study for a GPON deployment in the Enterprise environment. Stanislav Milanovic. Highest Institute of Education, Science and Technology, Athens, Greece. Enero 2014.

[14] Flexible GPON Architectures for Mass Market FTTH. Danny Goderis, Director, Access Product Marketing Alcatel-Lucent. Febrero 2007.

[15] FTTH Network Economics: Key Parameters Impacting Technology Decisions.Samrat Kulkarni, Beth Polonsky and Mohamed El-Sayed. Alcatel-Lucent. 2008.

[16] A Review and Comparison of Methods for Detecting Outliers in Univariate Data Sets. Songwon Seo, BS, Kyung Hee University. 2006.