ANEXOS

A. Arquitectura FTTH-PON

A.1. Introducción

La tecnología FTTH [7] propone la utilización de fibra óptica hasta el hogar del usuario proporcionando una serie de servicios avanzados, como el Triple Play: Voz, datos y televisión. Las principales ventajas de tener un bucle de abonado de fibra óptica son muchas: mayores anchos de banda, mayores distancias desde la central hasta el abonado, mayor resistencia a la interferencia electromagnética, mayor seguridad, menor degradación de las señales, etc. El decremento de la atenuación supone la reducción en el número de repetidores, lo que conlleva un menor consumo eléctrico, menores inversiones iniciales, menor espacio y menos puntos de fallo. Aunque tender la fibra hasta el hogar pueda suponer una fuerte inversión inicial (CAPEX), se amortizará con la reducción de los gastos de mantenimiento (OPEX) respecto a la infraestructura actual y a los nuevos servicios que se pueden ofrecer.

Una topología punto a punto P2P basada en Ethernet, requiere una gran cantidad de componentes y de cable de fibra óptica, aumentando el coste de instalación y de mantenimiento. Por esta razón, FTTH también proporciona una red punto a multipunto sin dispositivos electrónicos u optoelectrónicos activos para la conexión entre el abonado y el operador, permitiendo además múltiples abonados compartiendo una misma conexión, formando una red denominada PON P2MP. Esta topología P2MP reduce drásticamente los costes de instalación, de gestión y mantenimiento. Además, P2P Ethernet no permite la difusión de vídeo mediante *broadcast* sin un aumento considerable de los costes.

Por estas razones, PON comenzó a ser considerado a finales de los años noventa, tanto por las operadoras como por los suministradores, como una interesante solución para ofrecer acceso de fibra óptica hasta los usuarios residenciales.

A.2. Esquema de transmisión en P2MP PON.

En P2MP PON se utiliza una única fibra para transmitir y recibir, haciendo uso de la multiplexación por longitud de onda WDM. Los datos del enlace ascendente son distribuidos en una longitud de onda distinta (1310 nm.) para evitar colisiones con la trasmisión descendente (1490 nm.), y son agregados por la misma unidad divisora pasiva. A través del uso de WDM se asigna una tercera longitud de onda (1550nm.) dedicada para el *broadcast* de vídeo RF. En la Figura A.1 se muestra este esquema.

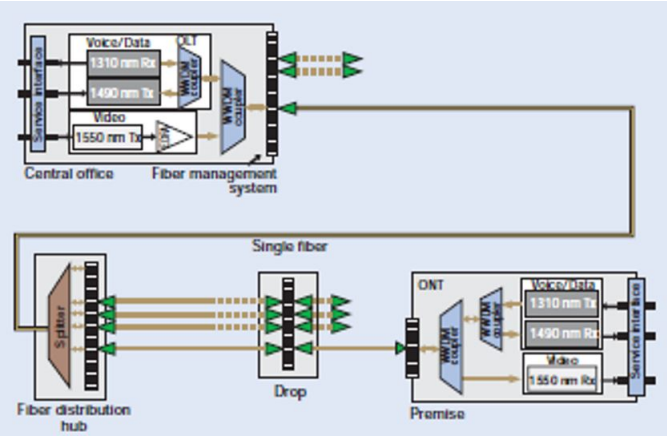

Figura A.1: Conexión P2MP-PON

A.3. Componentes de la PON

La red PON consta de una OLT ubicada en las dependencias del operador, y varias ONTs en las dependencias de los abonados para FTTH. La OLT consta de varios puertos de línea PON, cada uno soportando hasta 64 ONTs. Para conectar la OLT con la ONT, se emplea un cable de fibra óptica monomodo. El tráfico originado en la OLT puede ser distribuido mediante un divisor pasivo (*splitter*) a las 64 ONTs, en una o varias etapas, en una topología de árbol. La red de distribución óptica ODN (*Optical Distribution Network*) está formada por los cables *feeder*, de distribución y de acometida, y los *splitters*.

Un *splitter* es un dispositivo pasivo bidireccional con un puerto de entrada y múltiples de salida. En la dirección descendente 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. Introduce la misma pérdida en el sentido ascendente y en el descendente: 3 dB en cada salida por cada múltiplo de 2 del número de salidas. La OLT usa un láser DFB (*Distributed feedback laser*) de espectro estrecho para la transmisión de voz y datos, mientras que la ONT utiliza un láser Fabry-Perot, de espectro ancho, para su transmisión.

Debido a que la potencia en el enlace descendente se divide hacia todas las ONTs, las redes P2MP PONs tienen considerables pérdidas ópticas. Para asegurar que se opera correctamente en toda la red, se ha de establecer un balance de pérdidas (*loss budget*), el cual especifica las mínimas y máximas pérdidas tolerables entre la OLT y una ONT. La atenuación de la red óptica es la potencia que se pierde a lo largo de toda la red. Es la suma de la atenuación introducida por la red más las pérdidas de inserción que introduce cada componente (*splitters*, conectores y empalmes).

La fibra monomodo tiene diferentes atenuaciones dependiendo de su categoría (A, B, C y D) con valores de 0.3 a 0.5 dB/km. Se pueden producir atenuaciones adicionales en la fibra debido a: macrocuvaturas, microcurvaturas, desalineamientos, desuniones, suciedades o roturas.

Se usan conectores APC (*Angled Physical Contact*) debido a la alta potencia de la señal de vídeo analógico que transporta la PON. Estos conectores APC tienen un ángulo de 8 grados entre fibras que proporcionan muy pequeñas reflexiones y unas pérdidas de 0.2 dB. Los empalmes mecánicos introduce unas pérdidas de 0.5 dB y los de fusión alrededor de 0.1 dB, pero son de mayor coste.

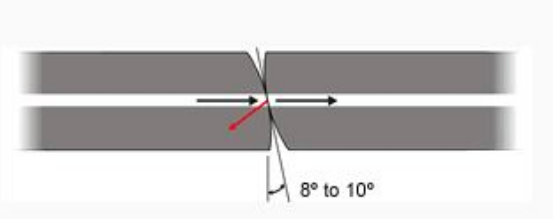

Figura A.2: Conector APC

A.4. Protocolos de redes PON

Existen diferentes tipos de redes PON, basados en distintos protocolos o estándares: *Broadband PON* (BPON), *Ethernet PON* (EPON) y *Gigabit-capable PON* (GPON).

Broadband PON (BPON), definido en la serie de recomendaciones ITU-T G.983, usa ATM (*Asynchronous Transfer Mode*) como el protocolo de transporte con velocidades simétricas y asimétricas de 155.52 y 622.08 Mbps, y asimétrica de 1244.16 Mbps. Permite hasta 32 usuarios en cada PON y un alcance lógico máximo de 20 km.

Ethernet PON (EPON), definido por IEEE 802.3ah, permite velocidades simétricas de 1.25 Gbps (velocidad efectiva de 1 Gbps) con FEC (*Forward Error Correction*) opcional. Tiene un alcance máximo lógico de 20 km y soporta hasta 32 usuarios.

Gigabit-capable PON (GPON), definido en la serie de recomendaciones ITU-T G.984, permite velocidades simétricas y asimétricas de hasta 2.488 Mbps. Todos los fabricantes de equipos deben cumplirla para garantizar la interoperabilidad. Proporciona una gran flexibilidad, ya que puede transportar cualquier tipo de datos basándose en ATM y GEM (*GPON Encapsulation Method*). Tiene un alcance lógico máximo de 60 km. y soporta hasta 64 usuarios en cada red. Información extendida de GPON en el anexo B.

GPON es más eficiente en el uso de ancho de banda que EPON, tiene mayor ancho de banda que BPON y EPON. Además, es un mejor sistema para el servicio de vídeo y por lo tanto, es más rentable. GPON es considerado más flexible y potente que EPON, pero EPON es más simple y más adaptable a en aplicaciones de corto alcance.

B. GPON

B.1. Arquitectura TDM

En la dirección descendente, la OLT multiplexa las tramas GEM en el medio de transmisión usando GEM Port-ID como identificador para diferenciar a que conexión lógica pertenece cada trama GEM. Cada ONT se queda con la trama GEM que le corresponde basándose en ese identificador.

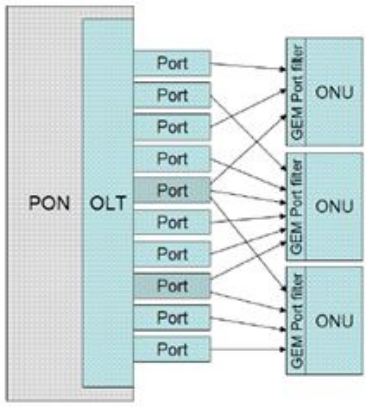

Figura B.1: Multiplexado en sentido descendente

En la dirección ascendente, la OLT organiza y reparte el ancho de banda entre las diferentes ONTs transmitiéndoles un mapa de ancho de banda en la dirección descendente, identificando estas tramas de tráfico por su Alloc-ID. Cada ONT debe transmitir en sus slots temporales asignados. Las tramas en ascendente se multiplexan en tiempo siguiendo el esquema mostrado en la Figura B.2.

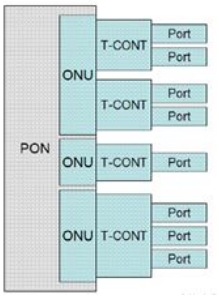

Figura B.2: Multiplexado en sentido ascendente

El ONU-ID es un identificador de 8 bits que la OLT asigna a una ONT durante el proceso de activación de dicha ONT, usando el canal de mensajes PLOAM. Es un identificador único en la PON y permanece válido hasta que la ONT es apagada, desactivada por la OLT, o puesta en un estado de inactividad. El GEM Port-ID es un identificador de 12 bits que es asignado por la OLT a cada conexión lógica individual. El Alloc-ID es un identificador de 12 bits que la OLT asigna a una ONT para identificarla en la asignación de ancho de banda que realiza la OLT. Por defecto, el Alloc-ID es igual al ONU-ID, se asigna implícitamente.

Un T-CONT (*Transmission Container*) es un objeto de la ONT que representa un grupo de conexiones lógicas que aparecen como una única entidad para la asignación del ancho de banda ascendente de la red. Cada ONT tiene un número fijo de T-CONTs. Durante la activación de la ONT se crean automáticamente todas las instancias T-CONT soportadas. Para activar un T-CONT que lleve tráfico de subida del usuario, la OLT establece un mapeo mediante OMCC (*ONT Management and Control Channel*) entre el T-CONT y el Alloc-ID.

B.2. Pila de protocolos GPON

La capa del protocolo de convergencia de transmisión GPON (GTC: *GPON Transmission Convergence*) está situada entre la capa del medio físico (PMD: *Physical Media Dependent*) y los clientes GPON, y se compone de dos subcapas: de entramado y de adaptación (ver Figura B.3). Las unidades de datos de servicio (SDU: *Service Data Unit*) en secciones GEM son convertidas en unidades de datos de protocolo GEM (PDU: *Protocol Data Unit*) en la subcapa GTC de adaptación.

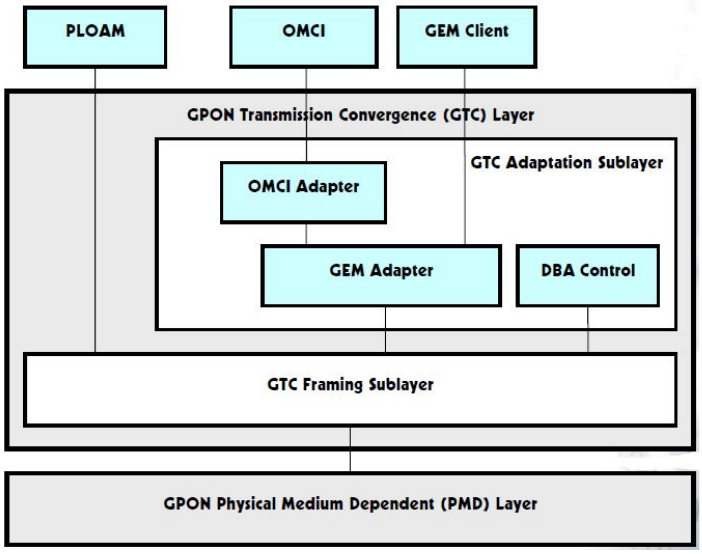

Figura B.3: Pila de protocolos GPON

La capa GTC se compone de un plano de control y gestión y un plano de datos de usuario. La gestión referente a PLOAM y OMCI está dentro del plano de control y gestión, mientras que SDUs, excepto OMCI, están dentro del plano de usuario.

La trama GTC en dirección descendente consiste en una cabecera o PCBd (*Physical Control Block downstream*) y el campo de datos GTC. Cada trama tiene una duración fija de 125 microsegundos (38880 bytes a una velocidad de 2.5 Gbps). Dentro del campo de datos GTC hay varias tramas GEM, cada una de tamaño variable, tal y como refleja la Figura B.4. Cada trama GEM tiene su cabecera GEM con su Port-ID, por tanto cada ONT se queda con las tramas GEM destinadas a ella. Dentro del PCBd se transporta mensajes PLOAM y el mapa de ancho de banda (BWmap), que indica a las ONTs los slots en los cuales puede transmitir.

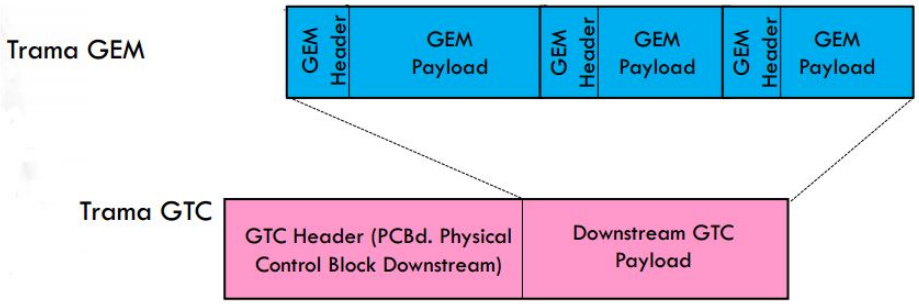

Figura B.4: Estructura de tramas GEM y GTC en sentido descendente

La trama GTC ascendente se compone de ráfagas procedentes de las distintas ONTs. En conjunto las tramas duran 125 microsegundos. Cada ráfaga está compuesta por una cabecera o PLOu (*Physical Layer Overhead upstream*) y uno o más intervalos de asignación de ancho de banda asociados con un Alloc-ID específico. Antes de la ráfaga debemos mantener un tiempo de guarda. El PLOu se compone de un preámbulo, un delimitador y 3 bytes de cabecera de ráfaga (BIP: *Bit Interleaved Parity* , ONU-ID y Ind). El intervalo de asignación de ancho de banda asociado a un Alloc-ID por defecto lleva una cabecera PLOAM seguido de una DBRu (*Dynamic Bandwidth Report upstream*). Para el resto de Alloc-ID, sólo lleva la cabecera DBRu.

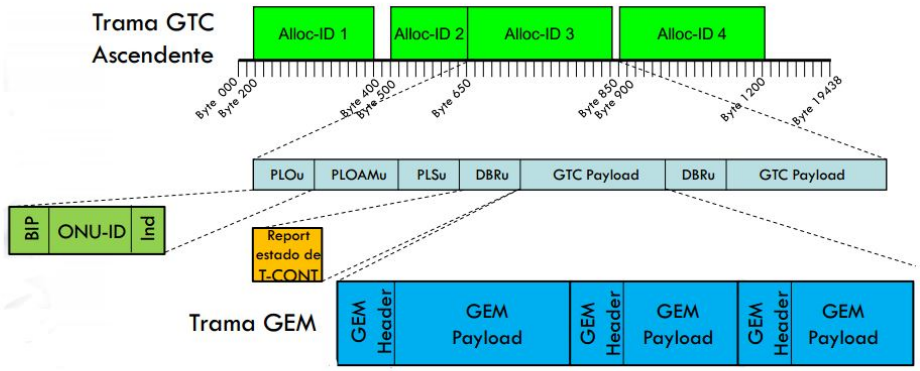

Figura B.5: Estructura de tramas GEM y GTC en sentido ascendente

La capa GTC tiene dos funciones principales. Una de ellas es encargarse del control de acceso al medio para el tráfico ascendente. Las tramas de tráfico descendente indican a las ONTs, mediante un mapa de ancho de banda (BWmap), cuándo deben transmitir su tráfico para que no existan colisiones, indicando el tiempo de comienzo y de final, además del Alloc-ID correspondiente. Este BWmap se incluye en la cabecera GTC, en el campo PCBd.

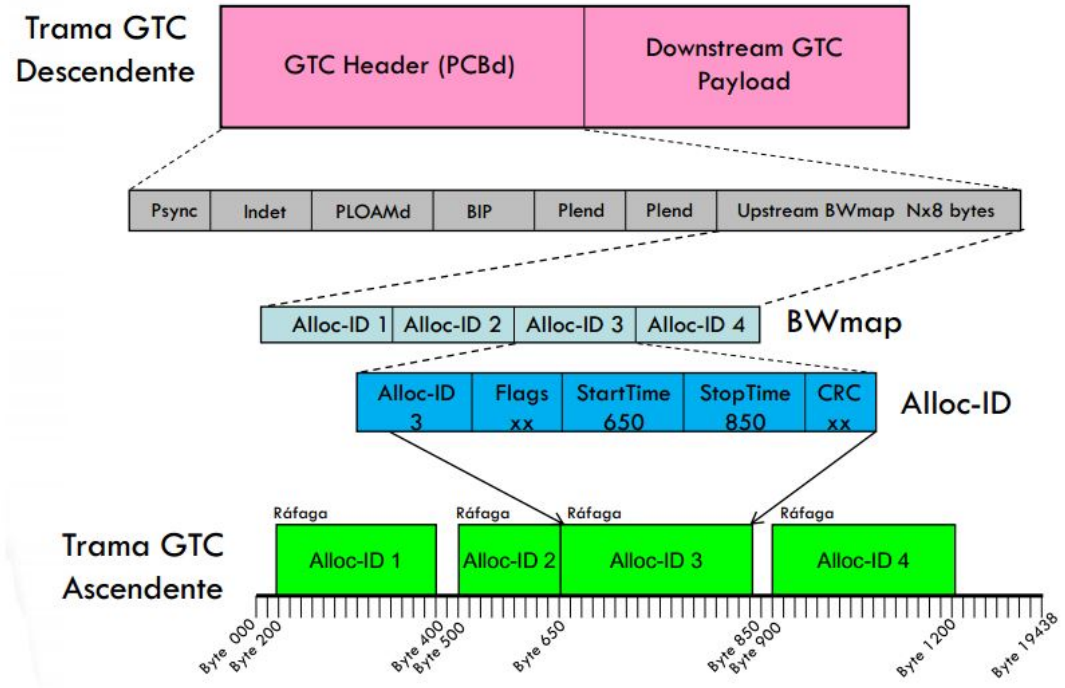

Figura B.6: Control de acceso al medio TDMA

La OLT asigna dinámicamente permisos de transmisión a las ONTs basándose en su estado de actividad y su configuración de tráfico. La asignación dinámica supone una mejora en el aprovechamiento del ancho de banda al ser un tráfico a ráfagas. Esto implica que se puedan añadir más usuarios a la red y dar un servicio más rápido. El ancho de banda se asigna a nivel de Alloc-ID, es decir, una ONT puede tener varios Alloc-ID cada uno con una tasa de tráfico distinta, por tanto a cada uno se le asigna un ancho de banda distinto dentro de la misma ONT.

Existen dos posibles métodos de implementación para la asignación dinámica de ancho de banda DBA:

- *Status reporting:* La OLT solicita un informe de ocupación del buffer de la ONT.
- *Traffic monitoring:* La OLT recibe tramas GEM *idle* de la ONT que tiene que transmitir, está desocupada.

La segunda función principal de la capa GTC es el registro de las ONTs, el cual se realiza dentro del proceso de activación, cuando una ONT inactiva quiere unirse

a la estructura y las transmisiones de una red GPON. Este proceso de activación se realiza mediante mensajes PLOAM. Tiene tres fases: aprendizaje de parámetros, adquisición del número de serie y *ranging*. Durante el aprendizaje de parámetros, la ONT adquiere los parámetros de operación que debe usar en la transmisión ascendente. En la adquisición del número de serie, la OLT descubre una nueva ONT por su número de serie y le asigna su ONU-ID.

Para el proceso de *ranging*, las ONTs deben compensar sus diferentes distancias a la OLT añadiendo un tiempo extra de referencia denominado retardo de ecualización EqD (*Equalization Delay*). De este modo se podrán sincronizar sus ráfagas ascendentes y evitar colisiones. Para evitar las colisiones con otras ONTs durante el proceso de activación, el resto de las ONTs suspenden su actividad por un periodo de tiempo denominado *quiet window*. El proceso de ranging se encuentra explicado con más detalle en el anexo H.

B.3. Seguridad de la red GPON

En GPON los datos en dirección descendente son enviados en *broadcast* a todas las ONTs unidas a la PON, por tanto, un usuario podría reprogramar su ONT para escuchar todos los datos en descendente de todos los usuarios. Por el contrario, ninguna ONT puede escuchar el tráfico en ascendente del resto de las ONTs de la PON. Para escuchar este tráfico ascendente tendría que interceptarlo directamente en la fibra, lo cual tendría que hacerlo en espacios públicos y seguramente dañaría esa fibra.

El algoritmo de encriptación que se usa es AES, que consiste en un bloque cifrado que opera con bloques de datos pseudoaleatorios de 16 bytes (128 bits). Aplica al bloque de datos una OR exclusiva con el bloque de cifrado para generar los datos cifrados de 128 bits. Para recuperarlos se vuelve a aplicar la OR exclusiva con el bloque de cifrado. Para esto es necesaria una clave de cifrado, la cual es generada y transmitida por la ONT para evitar ser escuchada por el resto de las ONTs.

Sólo el campo de datos de la trama GEM es encriptado, la cabecera GEM no. El proceso de encriptación en descendente es aplicado antes que FEC, y posteriormente se aplica un proceso de mezclado.

Forward error correction (FEC) se usa en la capa de transporte en sistemas de comunicaciones y se basa en transmitir los datos en un formato codificado, introduciendo redundancia para detectar y corregir los errores de transmisión, y como consecuencia, mejorar el BER (*Bit Error Rate*). Evita las retransmisiones y mejora el enlace 3-4 dB. Nos permite aumentar la tasa de bit y la distancia entre OLT y ONT, así como un número mayor de divisiones en la PON.

B.4. Canal de mensajes PLOAM

PLOAM (*Physical Layer OAM*) es un canal habilitado en la trama GTC para el envío de mensajes entre OLT y ONT. Proporciona funciones de gestión de la capa GTC de la red GPON. Estas funciones incluyen: la activación de las ONTs, el establecimiento del canal OMCC, configurar el cifrado, gestión de las claves y señalización de alarmas.

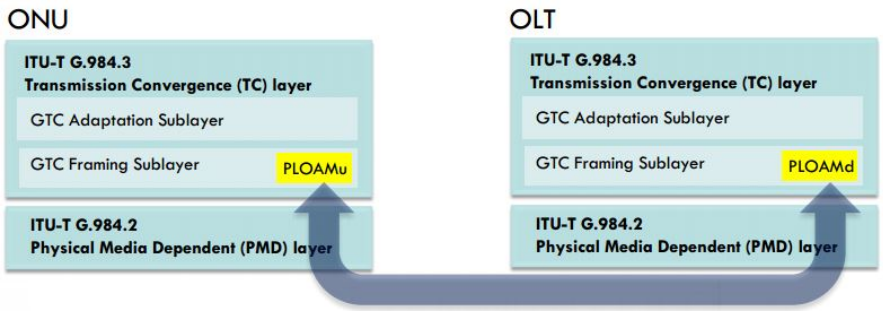

Figura B.7: Canal de mensajes PLOAM

Los datos PLOAM son transportados en un campo de 13 bytes dentro de la cabecera de la trama GTC. Además del campo de datos de 10 bytes, incluye un byte para el ONU-ID, otro byte para indicar el tipo de mensaje y un byte de CRC (*Cyclic redundancy check*) encargado de comprobar que la trama es correcta. En la Figura B.8 se muestra esta estructura genérica de los mensajes PLOAM.

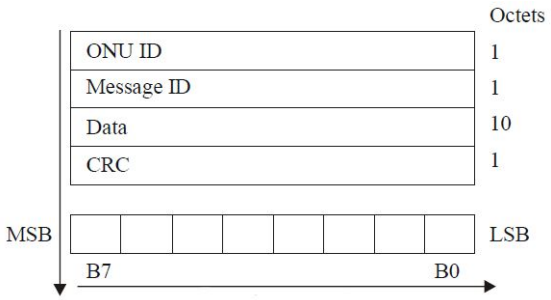

Figura B.8: Estructura genérica de un mensaje PLOAM

B.5. OMCI

El mecanismo de transporte OMCI (*ONT management and control interface*) es un servicio OAM cuyo fin es descubrir, controlar y gestionar las funciones de la ONT. OMCI opera en una conexión virtual bidireccional dedicada entre la ONT y la estación de gestión, la cual puede estar en la misma OLT o en un elemento más lejano de la red. El protocolo OMCI se define en las recomendaciones ITU-T G.984.3, G.984.4 y G.988, y facilita la interoperabilidad entre ONTs y OLTs de distintos fabricantes. Es un protocolo asimétrico, en el que la OLT manda sobre la ONT.

OMCI permite a la OLT establecer y liberar conexiones con la ONT, gestionar los puertos físicos de la ONT y solicitar información de la configuración y estadísticas sobre el rendimiento. También permite a la ONT informar automáticamente a la OLT sobre alarmas, cruce de umbrales de rendimiento y cambios de valor en muchos atributos de gestión.

En GPON, el protocolo OMCI se basa en una conexión GEM entre OLT y ONT, establecida en la inicialización de la ONT. Para el intercambio de mensajes OMCI se habilita un canal T-CONT y un puerto GEM específicos. Ambos constituyen el canal OMCC (*ONT Management Control Channel*).

Gracias a OMCI, la ONT detecta e informa de fallos en los equipos, en el *software* y en interfaces y ejecuta sus alarmas correspondientes. Para evitar grandes cantidades de mensajes de alarma, conviene filtrar aquellos que carezcan de importancia antes de declararlos como alarma.

El protocolo independiente MIB (*Management Information Base*) describe el intercambio de información a través de OMCI y se define en términos de entidades de gestión (*Managed entities*). Estas entidades de gestión son representaciones abstractas de recursos y servicios de una ONT. En la recomendación G.984.4 se describen más de 300 entidades. Algunas de estas entidades son obligatorias y otras dependen de la arquitectura de la ONT. En la Figura B.9 se detallan los diferentes campos de una trama OMCI.

GEM header (5 bytes)	Transaction correlation identifier (2 bytes)	Message type (1 byte)	Device identifier (1 byte)	Message identifier (4 bytes)	Message contents (32 bytes)	OMCI trailer (8 bytes)

Figura B.9: Estructura de trama OMCI

C. TGMS

C.1. Introducción

La empresa Telnet Redes Inteligentes S.A. cuenta con una arquitectura de gestión centralizada denominada *TELNET GPON Management System* o TGMS [6]. Es una herramienta web que actúa de interfaz intermedia entre el operario y las OLTs. Se encarga de la configuración, control, monitorización y administración de un conjunto de OLTs y sus ONTs asociadas.

Esta herramienta facilita la posibilidad de detectar nuevas ONTs, comprobar el estado de las conectadas y de la red, y monitorizar distintos parámetros que reflejen alarmas o eventos que permitan la detección de problemas en la red.

Una de sus principales características es la sencillez que aporta al protocolo OMCI con un lenguaje más comprensible y cercano y una interfaz más intuitiva. Además, es un sistema escalable, se pueden añadir equipos a la red de manera fácil sin que suponga una gran inversión. Esto es gracias a la reusabilidad de las configuraciones, es decir, sólo es necesario definir una vez los servicios o configuraciones disponibles para después asignarlas a tantos usuarios como sea necesario. Esto hace posible la puesta en marcha de una red GPON en pocos minutos.

El TGMS también se encargará de que se cumplan una serie de restricciones en cuanto a colisiones de mapas VLAN (*Virtual Local Area Network*) a nivel de puerto físico de la ONT y evitar excesos en el ancho de banda disponible en la PON. De esta manera el operador no tiene que preocuparse de estos posibles incidentes.

Otra ventaja que ofrece el TGMS es la posibilidad de sustituir una OLT minimizando el tiempo de desconexión con las ONTs conectadas. Sólo sería necesario cambiar en el TGMS la configuración de la OLT con la nueva IP y el número de serie de la nueva OLT. De este modo la nueva OLT heredaría la configuración de la anterior y continuaría con el servicio prestado.

C.2. Funciones del TGMS

- Aprovisionamiento de OLTs y ONTs.
- Actualización de Firmware de las OLTs, envío y recepción de aprovisionamientos y chequeo de versión.
- Monitorización de alarmas.
- Monitorización de estados y parámetros de las ONTs en tiempo real.

C.3. Monitorización de alarmas

El TGMS dispone de un mecanismo de comunicación con la OLT, de manera que todas las alarmas producidas son monitorizadas en el sistema y almacenadas en una base de datos MySQL, a la cual tendrán acceso los usuarios mediante el interfaz del TGMS. En la tabla C.1. se muestran todas estas alarmas:

Cuadro C.1: Alarmas OMCI

Software Error
Loss of signal
Loss of signal ONUi
Drift of window ONUi
Loss of frame ONUi
Remote defect indication ONUi
Loss of PLOAM ONUi
Loss of GEM Channel Delineation ONUi
Loss of acknowledgement ONUi
Signal degraded ONUi
Signal fail ONUi
Physical equipment error ONUi
Dying gasp ONUi
Loss of key ONUi
Transmission interference warning
Transmission interference alarm
Virtual Scope ONU laser always on
Virtual Scope ONU laser degradation
Virtual Scope ONU EOL
Virtual Scope ONU EOL database is full
Auth. failed in registration IP mode
Downstream received optical power below threshold
Downstream received optical power above threshold
Bit error based signal fail
Bit error based signal degraded
Transmitted optical power below lower threshold
Transmitted optical power above upper threshold
Laser bias current above threshold
ANI-G alarm released

Todas estas alarmas están explicadas con más detalle en la recomendación ITU-T G.984.3 [3].

C.4. Estados de conexión de una ONT

El TGMS muestra en tiempo real el estado de conexión de las diferentes ONTs que componen la red GPON. Hay once posibles estados, determinados en la Tabla C.2, con su correspondiente descripción:

Cuadro C.2: Posibles estados de una ONT en la red

Never Connected	Nunca ha sido vista
Not Connected	Ya no está conectada
Active	Recién detectada
Configured	Funciona correctamente
Disabled	Desactivada
Ranging Error	Error en el proceso de ranging
Unexpected Error	Error inesperado
Configuration Incomplete	Configuración incompleta
Provisioning Error	Error durante el aprovisionamiento
Configuration Mismatch	Configuración incorrecta
OMCI Communication Error	Error en comunicación OMCI

Requiere especial atención el estado *'Disabled'* ya que si la OLT no reconoce el número de serie de una ONT que se ha conectado a su red, le envía un mensaje PLOAM 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 pasará a estado *' Online'* .

D. Redes IP de videovigilancia

D.1. Introducción

La videovigilancia consiste en monitorizar remotamente lugares públicos o privados, mediante el uso de cámaras que transmiten las imágenes tomadas a equipos de monitorización que reproducen o graban las imágenes en una pantalla. Capturan imágenes de gente y objetos en movimiento con el fin de reconocer comportamientos sospechosos, detectar intrusiones, monitorizar carreteras o concentraciones masivas de gente, y evitar incidencias como posibles incendios.

Aunque sus primeros usos comenzaron en 1950, no fue hasta 1970 cuando realmente se implementaron los primeros circuitos cerrados de televisión (CCTV). Un circuito cerrado de televisión es un sistema de vídeo que transmite imágenes en un bucle cerrado.

D.2. Desarrollo de redes basadas en IP

Los sistemas de monitorización mediante circuitos cerrados de televisión han experimentado un gran proceso tecnológico en los últimos años. La aparición en los 90s de las primeras grabaciones digitales dio lugar a una pequeña revolución en el campo de la videovigilancia. Desde entonces, se han desarrollado los componentes digitales necesarios para implementar la transmisión de vídeo mediante protocolo IP, aunque todavía hay redes híbridas con cámaras analógicas que usan codificadores para enviar los datos por la red IP.

Un sistema IP de videovigilancia [11] consiste en múltiples cámaras conectadas a servidores de vídeo grabando y procesando transmisiones de vídeo, y un centro de operaciones donde el vídeo es visualizado y monitorizado a tiempo real. Las cámaras de seguridad IP pueden ser controladas remotamente desde el centro de operaciones. Para soportar la red de vídeo IP y permitir el control remoto de las cámaras, se requiere una red IP/Ethernet de alta velocidad.

La Figura D.1 sintetiza la transición desde las redes de videovigilancia analógicas a las redes IP actuales.

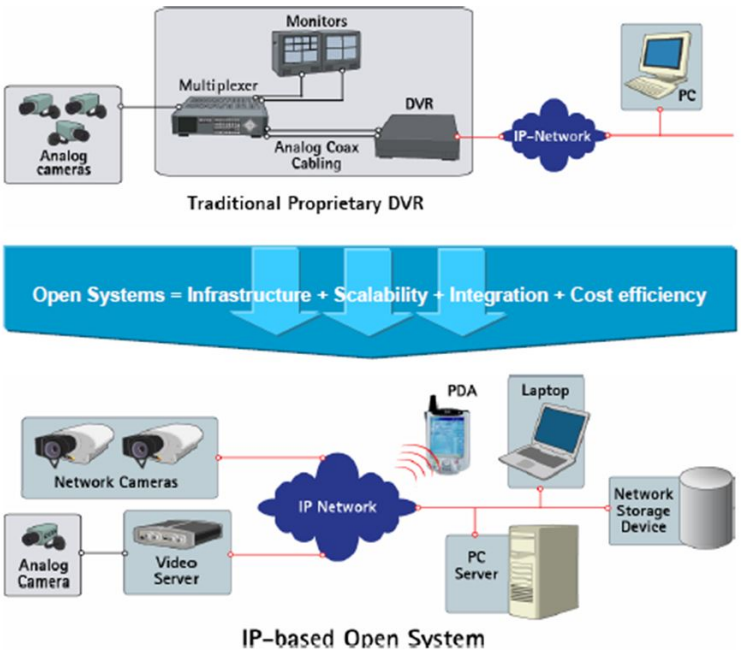

Figura D.1: Transición de redes analógicas a redes IP

Las ventajas del sistema de videovigilancia IP frente a los sistemas anteriores analógicos son las siguientes:

1. Acceso remoto a un vídeo en directo o grabado en cualquier momento y desde cualquier parte de la red.

2. Aumenta la disponibilidad ofreciendo un alto nivel de redundancia.

3. Mayor escalabilidad y flexibilidad, el sistema puede expandirse según las necesidades del usuario sin cambios significativos en la estructura de la red.

4. Las imágenes digitalizadas pueden transportarse sin una reducción de calidad ya que se eliminan las pérdidas producidas en las conversiones analógico-digitales.

5. Las imágenes digitalizadas son almacenadas con mayor eficiencia.

6. La arquitectura IP hace fácil integrar diferentes servicios de seguridad (control de accesos, alarma de incendios,etc.).

7. Posibilidad de mandar órdenes a la cámara desde el *software* de gestión, por ejemplo, activar el zoom para una mayor precisión en situaciones de interés.

8. Gestión inteligente de eventos mediante *software*. Puede identificar comportamientos o detectar movimiento automáticamente, con la posibilidad de activar una alarma o gestionar la cámara con movimientos o zoom en tiempo real.

9. Los costes de gestión y de equipamiento son menores que en un sistema analógico. La tecnología Power over Ethernet también disminuye los costes de instalación de cableado de suministro.

Además de estas ventajas, el uso de cámaras digitales también aporta una serie de novedades como una mejor resolución y nitidez o mayor capacidad de zoom. Proporcionan un escaneado progresivo, el cual es mejor que el escaneado entrelazado en las analógicas, que conlleva un retardo de 17 ms entre el escaneo de las líneas pares e impares de la imagen completa, lo que produce que los objetos o personas en movimiento aparezcan difuminados. Además, las cámaras IP pueden ser alimentadas mediante PoE, usando el mismo cable en el que son transmitidos los datos, minimizando costes de cableado y facilitando la instalación. Y por último, pueden estar equipadas con un buffer que guarde y envíe imágenes antes y después de una alarma, ahorrando en ancho de banda y en capacidad de almacenamiento requerida.

El problema que surge con las cámaras de alta resolución es que aumentan el ancho de banda requerido, hasta 16 Mbps, y se necesita una mayor capacidad de almacenamiento del, ya que generan hasta 2GB por cada hora de grabación, lo que significa 48 GB al día. Una solución es acortar los periodos de retención. Otra posibilidad es iniciar el guardado de datos sólo cuando sucedan eventos particulares.

Los factores clave para el éxito de la videovigilancia IP han sido: la caída de los costes, la calidad de las cámaras usando técnicas de compresión muy efectivas y la mejora en el procesado en las cámaras IP. Si necesitamos implementar un gran sistema de más de cien cámaras, la cantidad de vídeo a transmitir, ver y archivar hace imposible a una persona analizar y detectar movimientos o comportamientos sospechosos. Por esta razón, la videovigilancia ha sido históricamente una herramienta usada en investigaciones a posteriori.

La videovigilancia inteligente es una tecnología que usa *software* para identificar automáticamente objetos, comportamientos o actitudes en las imágenes grabadas. Esto conlleva una serie de ventajas: puede activar una alarma que avise al personal de seguridad o gestionar la cámara con movimientos o zoom para una mayor precisión. También reduce el ancho de banda y ahorra almacenamiento transmitiendo sólo datos de eventos relevantes. Permite que el personal de seguridad no tenga que hacer videovigilancia continua. Permite una búsqueda rápida de eventos relevantes en el archivo grabado. Hace posible identificar objetos en la escena y seguir su actividad.

Esta nueva tecnología también presenta inconvenientes. Por ejemplo, es complicado para el sistema diferenciar entre un comportamiento normal y uno sospechoso. En los sistemas inteligentes siempre hay un compromiso entre la frecuencia de reconocimiento y el número de falsas alarmas. Si el umbral de detección es muy permisivo, tendremos muchas posibilidades de detectar un evento peligroso real, pero será mayor el número de falsas alarmas. Esto produce una pérdida de tiempo y productividad en el personal y un uso innecesario de ancho de banda y de la capacidad de almacenamiento de la red. Por el contrario, si el umbral es muy restrictivo, tenemos más posibilidades de pasar por alto algún incidente, pero las falsas alarmas serán escasas y el uso de ancho de banda será más eficiente.

D.3. Técnicas de compresión de los datos de vídeo

Debido a la resolución y calidad de las cámaras IP, se generan grandes cantidades de datos que ocupan un gran ancho de banda. Por esta razón, estos datos deben ser comprimidos antes de ser enviados por la red mediante el uso de códecs. Las tecnologías de compresión de vídeo digital más utilizadas en videovigilancia IP son: MJPEG, MPEG-4 y H.264.

Un códec es un dispositivo o programa que realiza la codificación y decodificación de datos de vídeo digitales. Un códec MJPEG transmite vídeo como una secuencia de imágenes JPEG codificadas, mientras que MPEG-4 usa algoritmos de predicción para lograr mayores niveles de compresión que MJPEG y conservando la calidad de la imagen. MJPEG tiene menos complejidad, por tanto puede ser implementado en hardware menos costoso, pero requiere un mayor ancho de banda que MPEG-4. La compresión H.264 permite comprimir los datos en un 80 % en relación con MJPEG, y un 50 % en relación con MPEG-4. H.264 y MPEG-4 proporcionan audio sincronizado a diferencia de MJPEG.

MJPEG se transporta sobre TCP (*Transmission Control Protocol*), el cual garantiza la llegada de los paquetes mediante reconocimientos del receptor. Paquetes no reconocidos son retransmitidos. Por lo tanto, es bueno usarlo en redes ligeramente congestionadas o con una inherente pérdida de paquetes como sería el transporte inalámbrico. TCP es más útil para vídeos que no van a ser visionados en directo, ya que introduce un retardo debido al reconocimiento de paquetes. Se utiliza en vídeos que son grabados para un posterior visionado.

MPEG-4/H.264 es comúnmente transmitido sobre UDP (*User Datagram Protocol*), RTP (*Real-Time Transport Protocol*) o RTSP (*Real-Time Streaming Protocol*). UDP no garantiza la entrega de paquetes y no proporciona la retransmisión de paquetes perdidos. Por esta razón, UDP/RTP es más indicado para redes con pequeña tasa de paquetes perdidos y ancho de banda garantizado por mecanismos de calidad de servicio QoS. Si se producen pérdidas, existirá una degradación de la calidad de la imagen. UDP permite la opción de envío multicast IP. Algunas cámaras y codificadores también proporcionan MPEG-4 sobre TCP.

Los datos de vídeo que usan compresión MPEG-4/H.264 son más sensibles a la pérdida de paquetes y a la latencia porque usa imágenes predictivas, por lo tanto el ancho de banda de la red deberá estar preparado para prevenir tanto la pérdida de paquetes como la latencia.

D.4. Ancho de banda y capacidad de almacenamiento requeridos

Comparado a VoIP, los datos de vídeo consumen considerablemente más ancho de banda de la red. La función de visionado requiere un ancho de banda similar a la función de transporte, ya que el cliente recibe la señal de vídeo desde los servidores. La gestión del sistema también influye en los requisitos de ancho de banda de la red. El ancho de banda usado para el control carece de importancia respecto al consumido por los datos de vídeo, pero se debe tener muy en cuenta desde la perspectiva de la calidad de servicio QoS.

La tasa de salida desde una cámara IP depende de su configuración respecto a: resolución del códec (MJPEG, MPEG-4, H.264), tasa de frames o tasa de bits y cualquier factor de calidad aplicado. El ancho de banda será mayor con resoluciones y tasas mayores. Para MPEG-4 con resolución D1 (720x480) tenemos una tasa de bit de 1-2 Mbps. Para H.264 con resolución HD (1920x1080) tenemos 4-6 Mbps.

Para calcular la capacidad de almacenamiento necesaria intervienen muchos factores: el número de cámaras, el número de horas que graba cada cámara, el tiempo que necesitas los datos almacenados, si las cámaras graban continuamente o se activan por alarmas y el valor de parámetros como la tasa de frames, el tipo y el ratio de compresión, la resolución de la imagen y la complejidad de la escena que grabas.

D.5. Calidad de servicio QoS

El tráfico de vídeo es sensible a la latencia, a la pérdida de paquetes y al jitter (variación del retardo). Una transmisión de vídeo con compresión MPEG4 o H.264, es más sensible a la pérdida de paquetes porque usa imágenes predictivas. El ancho de banda y la calidad de servicio son dos factores críticos para reducir la pérdida de paquetes, el retardo y el jitter. El ancho de banda debe ser cuidadosamente planeado para evitar la congestión de la red. En algunas ocasiones, es inevitable que aparezca congestión de la red, entonces el QoS da prioridad al tráfico más importante para evitar que sea descartado o retrasado. QoS se basa en el marcado de paquetes.

QoS en IP se basa en el uso de las VLANs, permitiendo al usuario fijar prioridades y clasificaciones de los servicios. De esta manera, si hay más de un servicio en la red (por ejemplo, vídeo IP de una cámara y una señal de control de tráfico), una VLAN puede ser asignada a cada servicio, cada una con su propia clasificación y prioridad, para que el rendimiento de una no afecte a la otra.

D.6. Unicast y Multicast IP

Las transmisiones unicast envían una copia de cada paquete entre una dirección de fuente y una dirección de equipo destino. Unicast es simple de implementar pero no es eficiente si el número de sesiones es muy grande. Si se tiene que transmitir la misma información en muchas ocasiones a distintos equipos, el impacto en el ancho de banda será significativo. Para una mayor eficiencia en el uso del ancho de banda se implementa multicast IP.

En transmisiones IP multicast, un equipo envía una copia de cada paquete a una dirección especial que es usada por varios equipos interesados en recibir esos paquetes. Esos usuarios son miembros de un grupo multicast y pueden estar localizados en cualquier lugar de la red. Con el multicast IP se reduce la carga de tráfico de la red minimizando replicaciones innecesarias de transmisiones de vídeo. Por el contrario, hace la red más insegura, ya que cualquier equipo puede acceder a los datos enviados. A cada cámara se le asigna un único grupo multicast con su correspondiente dirección IP de grupo. El usuario que quiera recibir la transmisión de vídeo de esa cámara deberá suscribirse a ese grupo multicast. Los equipos del grupo multicast pueden unirse y dejar el grupo dinámicamente y pueden ser miembros de varios grupos.

El tráfico de multicast IP se transporta sobre UDP, el cual no tiene mecanismos de fiabilidad como control de flujo o mecanismos de recuperación de errores, pero dispone de herramientas como la calidad de servicio QoS que mejoran la fiabilidad. Los servidores de vídeo propagan los datos de vídeo a los usuarios usando transmisión IP unicast, pero los switches y routers que soportan multicast replican la transmisión a los equipos asignados en el grupo multicast.

El multicast IP está basado en IGMP (*Internet Group Management Protocol*), el cual está diseñado para permitir a una fuente de vídeo enviar sus datos de vídeo a múltiples hosts como una única instancia, conservando ancho de banda. IGMP opera con grupos de direcciones IP, usando un rango de direcciones específicamente usado para vídeo multicast. Como una dirección multicast no tiene una dirección MAC conocida, un switch manda los paquetes multicast por todos los puertos, de manera que todos los equipos están recibiendo los paquetes aunque no pertenezcan al grupo destinatario. Esto consume muchos recursos de red. Para mejorar esto, se hace uso del protocolo IGMP *snooping*, que permite al switch escuchar la conversación IGMP entre equipos y routers para conocer los equipos que están unidos al grupo multicast destinatario, mejorando la eficiencia del ancho de banda de la red.

E. Dispositivos de seguridad

En una red de seguridad, los componentes principales en términos de ancho de banda requerido van a ser las cámaras de videovigilancia, sin embargo existen diferentes componentes que pueden estar presentes en una red de seguridad:

- Detectores de presencia y movimiento.
- Sistema de control de acceso o fichaje.
- Detectores de humo, gas, inundación, etc.
- Sistema de megafonía e interfonía.

Una de las ventajas que aporta el equipo de usuario en las redes GPON, la ONT, es que proporciona interfaces Gigabit Ethernet para conectar cualquiera de estos dispositivos mediante cable RJ-45 de manera habitual, lo que significa que no es necesario un coste añadido en adaptar la señal óptica a los dispositivos deseados.

La ONT proporciona segmentación mediante la asignación de diferentes VLANs en sus interfaces, lo que permite asignar anchos de banda de manera independiente a cada dispositivo, posibilitando al usuario fijar prioridades y clasificaciones de los servicios.

La ONT también proporciona conectividad WIFI, por tanto también sería una opción a considerar si se desea colocar elementos de seguridad lejos de nuestra ONT.

Figura E.1: ONT de Telnet Redes Inteligentes

F. RPC

Para la comunicación entre nuestro equipo y la OLT se hace uso de un proceso de comunicación denominado RPC (*Remote Procedure Call*), el cual nos permite ejecutar una subrutina o proceso en un equipo diferente situado en una red compartida. De este modo, el programador no tiene que estar pendiente de esta comunicación ni conocer sus detalles.

Por ello, las RPC son muy utilizadas dentro del paradigma cliente-servidor, siendo el cliente el que inicia el proceso solicitando al servidor que ejecute cierta función y envíe un resultado de vuelta al cliente. En el esquema mostrado en la Figura F.1 se refleja el funcionamiento de estas llamadas.

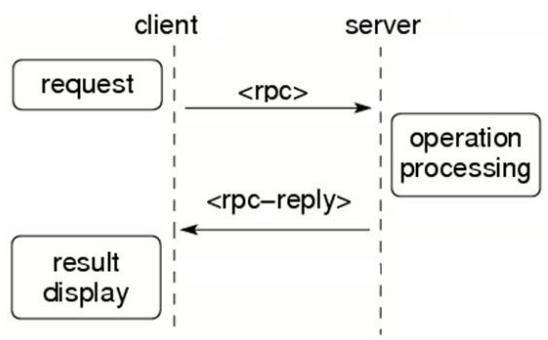

Figura F.1: Proceso RPC

En este caso, cada OLT está configurada de tal manera que acepta RPCs a las que responde con resultados a los parámetros implícitos en la llamada remota. De esta manera, podremos obtener valores en tiempo real referentes a las ONTs de nuestro sistema, facilitando el desarrollo del proceso.

G. Programación Web

El sistema de gestión de alarmas implementado en este proyecto es una herramienta web que sigue la arquitectura cliente-servidor.

El código ejecutado en el servidor está programado en PHP mientras que en el lado del usuario se encuentra todo lo relativo a HTML, CSS y JavaScript. Además, el servidor se comunica con las bases de datos MySQL mediante sentencias desde PHP.

Sin embargo, para el desarrollo de programas que requieren una ejecución continua, como en este caso la adquisición de ciertos parámetros cada X tiempo, se ha optado por la programación en C, debido al límite en el tiempo máximo de ejecución que presenta la programación PHP. Se podía haber optado por otros lenguajes como Python o Java, pero se decidió el uso de C aprovechando los conocimientos previos en este lenguaje.

Figura G.1: Arquitectura cliente-servidor

Por otra parte, se ha hecho uso de AJAX con la finalidad de crear una aplicación interactiva que sea capaz de realizar cambios en la página web sin necesidad de recargarla por completo, reduciendo de esta manera la carga de tráfico entre cliente y servidor, y mejorando la interactividad, velocidad y funcionalidad de la herramienta. Esto se consigue gracias a que AJAX mantiene en segundo plano una comunicación asíncrona con el servidor, permitiendo al usuario continuar con la interacción sin alteraciones. JavaScript es el lenguaje interpretado utilizado en el que se efectúan las funciones de llamada de AJAX.

JQuery, la biblioteca de JavaScript más utilizada, se usa con el fin de simplificar la manera de interactuar con elementos HTML, gestionar eventos y agregar interacción con la técnica de AJAX a la web. Con las funciones propias de esta biblioteca se consigue una reducción en el tiempo y en el espacio.

Debido a la necesidad de representar los datos recogidos por el sistema, se ha utilizado un complemento de JQuery para el desarrollo de gráficas, llamado jqPlot, con una amplia gama de posibilidades.

La información transmitida por el servidor al navegador se hace en formato JSON (*JavaScript Object Notation*), como alternativa a XML (*eXtensible Markup Language*), ya que resulta más sencillo escribir un analizador sintáctico que convierta el texto de entrada en otras estructuras, comúnmente árboles, más útiles para un posterior análisis.

H. Proceso de Ranging

En GPON se realiza un *broadcast* óptico en el enlace descendente, la información que transmite la OLT llega a todas las ONTs de la red, sin posibilidad de colisiones. Sin embargo, la transmisión en ascendente está basada en TDMA (*Time Division Multiple Access*), lo que requiere que todos los elementos de la red GPON se mantengan sincronizados a una referencia temporal común.

El acceso a un medio compartido común, en este caso la fibra óptica, requiere de un mecanismo determinista que evite colisiones entre las transmisiones de las diferentes ONTs en el enlace ascendente [8]. En este caso, la OLT es la encargada de asignar los periodos de transmisión a cada una de las ONTs de la red.

Además de esto, hay que tener en cuenta que cada ONT está a una distancia distinta de la OLT, es decir, las transmisiones van a tener distintos tiempos de propagación, lo que va a provocar colisiones en la recepción de tramas tanto en la OLT como en los *splitters* que combinan las señales en el enlace ascendente.

En la Figura H.1 se muestra el problema comentado, con una colisión de tramas en recepción debido a los diferentes tiempos de propagación de ONTs situadas a distancias diferentes.

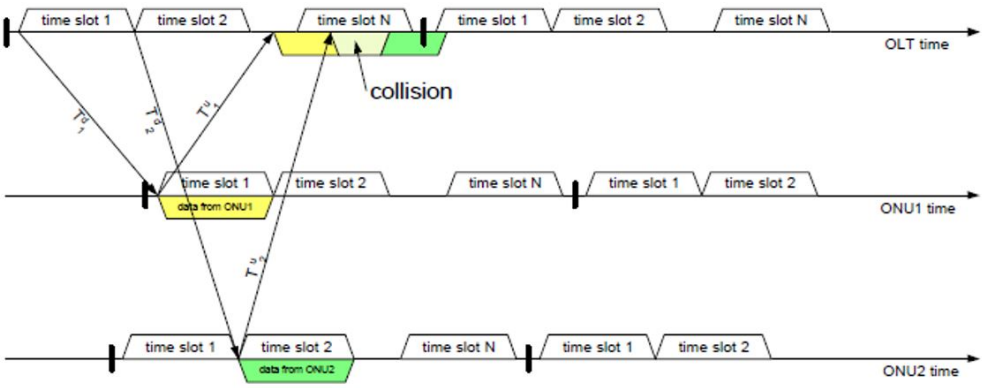

Figura H.1: Colisión de tramas transmitidas por diferentes ONTs

Para dar solución a este problema, la OLT asigna un tiempo de ecualización a una ONT cuando ésta se quiere unir a la red, mediante un proceso de *ranging*, de manera que sitúa todas las ONTs que componen la red a una misma distancia virtual. Este tiempo de ecualización es mayor cuanto más cerca está la ONT de la OLT.

El proceso de *ranging* consiste en el envío de un mensaje de control por parte de la OLT seguido de una respuesta de la ONT en cuestión. La OLT conoce el tiempo de emisión y recepción del mensaje, por tanto puede calcular el tiempo de propagación y asignarle el tiempo de ecualización que corresponda. Para evitar las colisiones con otras ONTs durante el proceso de *ranging*, la OLT manda un mensaje de control al resto de las ONTs para que suspendan sus transmisiones ascendentes por un periodo de tiempo denominado *quiet window*.

De este modo se podrán sincronizar las ráfagas ascendentes procedentes de las distintas ONTs y evitar colisiones, tal y como muestra la Figura H.2.

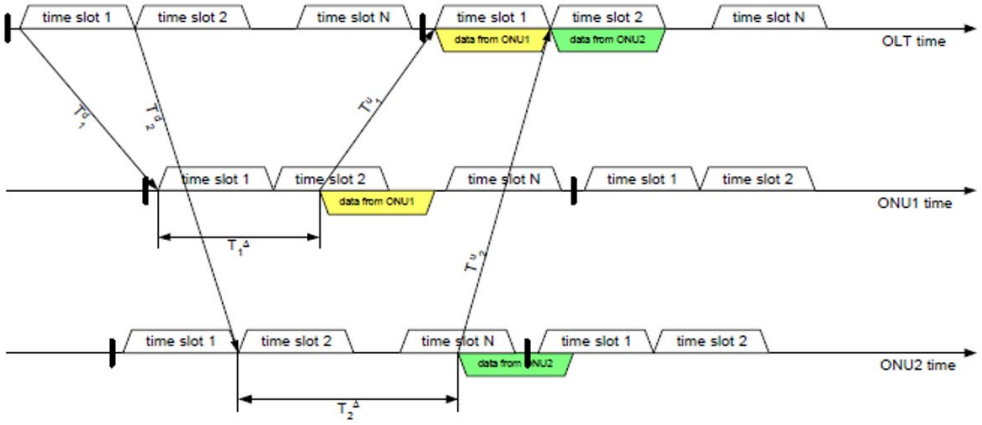

Figura H.2: Después del ranging, las tramas llegan correctamente

Con esto no se consiguen evitar todas las colisiones, ya que los componentes electrónicos introducen un factor aleatorio que provoca la aparición de jitter, es decir, variación en el retardo de la señal, lo que puede llegar a ocasionar solapamientos entre ráfagas. Para evitar este problema se introduce una banda de guarda al comienzo de cada paquete, con una longitud de 16 a 64 bits. A continuación también se introduce un preámbulo con el objetivo de fijar la fase de la señal de entrada y leer los datos de manera correcta.

En cualquier caso, si la OLT recibe la transmisión de una ONT en un slot temporal que no corresponde con el determinado, puede enviar una alarma mediante OMCI a la ONT de tipo *'Drift of Window'* con un nuevo valor del tiempo de ecualización que corrija la situación.