

Diseño e integración de un sistema de acceso condicional para TDT

AUTOR

Ignacio Cierco Lasbats

DIRECTOR DE PROYECTO

David Pujals

ABERTIS TELECOM

DIRECTOR PONENTE

Mercedes Magdalena Vall-Llossera Ferran
UPC – Teoria de Senyal i Comunicacions

Junio 2008

Índice general

<i>Índice general</i>	2
<i>Índice de figuras</i>	4
1.-Introducción	6
1.1.- Objetivos	7
1.2.- Fases del proyecto	7
1.3.- Arquitectura	7
1.4.- Estructura de la memoria	8
2.- Contexto	10
2.1.-Acceso Condicional	10
2.1.1.-Definición	10
2.1.2.-Encriptación.....	10
2.1.3.-Tipos de acceso condicional	12
2.2.- Marco legal	13
2.2.1.-Marco Europeo	13
2.2.2.-Legislación española.....	14
2.3.-TDT (Televisión Digital Terrestre)	16
2.3.1.-Marco regulador	16
2.3.2.-Evolución de la TDT en España	18
2.3.3.-Situación de la TDT.....	19
2.3.4.-Estado de la tecnología	21
2.3.5.-Capas del servicio TDT	21
2.3.6.-Características de la TDT	22
3.- Entorno	23
3.1.- MPEG-2	23
3.1.1.- Breve historia.....	24
3.1.2.- MPEG-2 Vídeo	24
3.1.3.- MPEG-2 Audio	25
3.1.4.- MPEG-2 Systems	25
3.2.- DVB	27
3.2.1.- Identificadores	27
3.2.2.- DVB en el mundo	28
3.3.- PSI/SI	29
3.3.1.- PSI (Program Specific Information)	29
3.3.2.- DVB-SI (Service Information)	30
3.4.- Transport Stream	31
3.4.1.- Generación del transport stream	31
3.4.2.- Componentes del transport stream.....	33
3.5.- Entorno de desarrollo	34
3.5.1.- Software.....	35
3.5.2.- Equipamiento.....	35

3.5.3.- Medidas	40
4.- Ejecución del proyecto	41
4.1.-Planificación.....	41
4.1.1.- Estudio.....	41
4.1.2.- Especificación de la solución.....	42
4.1.3.- Desarrollo de la aplicación	43
4.1.4.- Pruebas de funcionalidad.....	43
4.2.- Arquitectura	44
4.2.1.- Arquitectura 1: Emulación virtual	44
4.2.2.- Arquitectura 2: Emulación con cabecera local	45
4.2.3.- Arquitectura 3: Sistema semi-completo.....	46
4.2.4.- Arquitectura 4: Sistema completo.....	47
4.3.- Descripción de la aplicación	48
4.3.1.- Componentes	48
4.3.2.- Estructura de la programación	49
4.3.3.- ¿Cómo sincronizar el transport stream?.....	49
4.3.4.- ¿Cómo leer datos?	55
4.3.5.- ¿Cómo encriptar el stream correspondiente?.....	61
4.3.6.- Rutina	62
5.- Resultados.....	65
5.1.- Funcionamiento	65
5.1.2.- Uso global.....	65
5.1.2.- Características.....	71
5.2.- Limitaciones técnicas	72
6.- Conclusiones.....	73
7.- Anexos.....	75
7.1 Directiva 1998/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998.	75
7.2 MPEG.....	82
8.- Glosario de términos	84
9.- Referencias y bibliografía	86
9.1.- Referencias.....	86
9.2.- Bibliografía	87

Índice de figuras

Figura 1.- Arquitectura genérica	8
Figura 2.- Plataformas acceso condicional España	10
Figura 3.- Sistema de clave secreta o simétrico.....	11
Figura 4.- Sistema de clave pública o asimétrica.....	12
Figura 5.- Penetración TV Digital y fechas de apagado.....	20
Figura 6.- Venta de receptores TDT	20
Figura 7.- Capas del servicio TDT	22
Figura 8.- Esquema de elementos que conforman un Transport Stream	26
Figura 9.- DVB en el mundo	28
Figura 10.- Esquema de tablas PSI/SI	31
Figura 11.- Generación de un TS a partir de paquetes PES	32
Figura 12.- Campos de un Transport Stream	33
Figura 13. - DTA-140	36
Figura 14.- Diagrama de bloques DTA-140	37
Figura 15.- Esquema básico inicial	44
Figura 16.- Arquitectura 1	45
Figura 17.- Arquitectura 2. Subfase1.....	45
Figura 18.- Arquitectura 2. Subfase2.....	46
Figura 19.- Arquitectura 2. Subfase3.....	46
Figura 20.- Arquitectura 3	47
Figura 21.- Arquitectura 4	48
Figura 22.- Requerimientos, componentes y problemas	48
Figura 23.- Estructura de un transport stream	50
Figura 24.- Transport stream packet.....	50
Figura 25.- PID	52
Figura 26.- Transport_scrambling_control	52
Figura 27.- Valores del Adaptationfield	52
Figura 28.- Transport Stream adaptation field	55
Figura 29.- Program association table.....	56
Figura 30.- Program map tables	59
Figura 31.- Stream type assignments.....	60
Figura 32.- Ejemplo Stream_type	62
Figura 33. - Diagrama de flujo 1	63
Figura 34.- Diagrama de flujo 1	64
Figura 35.- Estructura de funcionamiento.....	65
Figura 36.- Estructura de funcionamiento	65
Figura 37.- Estructura de funcionamiento	66
Figura 38.- Ej TS con servicios encriptados.....	67
Figura 39.- Ej TS encriptado totalmente.....	68
Figura 40.- Análisis stream video	69

Figura 41.- Análisis stream video encriptado	69
Figura 42.- Packet explorer encriptado.....	70
Figura 43.- Packet explorer no encriptado.....	70

1.-Introducción

La Televisión Digital Terrestre (TDT) ya es una realidad a la que prácticamente toda la población tiene acceso. Las cadenas ya comienzan a emitir sus contenidos en digital y a acompañarlos de productos que ofrecen valor añadido a los propios radiodifusores, tales como el acceso condicional a diversos tipos de contenido.

Dentro de la cadena de distribución de televisión digital, el Sistema de Acceso Condicional (CAS) tiene como objetivo limitar la recepción de determinados servicios únicamente a los usuarios autorizados por el proveedor del servicio. El CAS permitirá que sólo los usuarios autorizados, provistos del adecuado receptor, puedan tener acceso a determinados servicios. El CAS permitirá seleccionar los servicios y los instantes de tiempo en que éstos pueden ser utilizados por los usuarios autorizados, así como permitir gestionar de forma sencilla las autorizaciones de cada usuario, bien de forma individual o colectiva.

Paralelamente a este modelo de negocio, un operador de infraestructuras necesita hacer la contribución a los diversos emplazamientos de las diferentes señales de televisión para su posterior difusión. Esta contribución no es trivial, ya que estas señales no pueden ser interceptadas de forma sencilla por un usuario doméstico.

En vista de este conjunto de factores, se pensó en la necesidad de una aplicación capaz de llegar a encriptar un “transport stream” (TS), ya sea solamente el video y el audio de un servicio determinado o todo el TS. Por un lado, se ofrece una manera de acceso condicional y por otra se ofrece la posibilidad de utilizar dicho software como un elemento más de la cabecera con el objetivo de difundir las diversas señales a los emplazamientos de una forma totalmente segura.

1.1.- Objetivos

El objeto principal del proyecto es el diseño de una aplicación que sea capaz de encriptar uno o varios servicios de un TS, con la finalidad de utilizar dicha aplicación como solución “low cost” a diversas necesidades en el ámbito de la Televisión Digital Terrestre.

Dentro de estas necesidades se pueden citar varias, como por ejemplo un acceso condicional a servicios de TDT local por el bajo coste de la solución, encriptación de las contribuciones vía satélite de las diversas señales de los radiodifusores para su posterior difusión terrestre (por normativa las contribuciones no pueden ser en abierto).

Esta solución viene determinada por las necesidades antes descritas que son las que tiene Abertis Telecom.

La aplicación se ha pensado con unos requerimientos estipulados por la propia empresa. Por poner un ejemplo, una de las principales premisas, es que la aplicación dejará pasar de forma transparente la MIP, que es la tabla que introduce el adaptador “Single Frequency Network” (SFN), para que los moduladores trabajen correctamente en esta modalidad.

1.2.- Fases del proyecto

El proyecto consta de 4 fases bien diferenciadas:

- **Fase de estudio:** Se ha buscado información general para definir la situación actual, así como información técnica relativa al manejo de equipamiento y diseño de la aplicación.
- **Fase de especificación:** Se han identificado el hardware y el software necesarios. Se han definido las arquitecturas, y la estructura de la aplicación.
- **Fase de desarrollo:** Se centra en el desarrollo de la aplicación y en su prueba en diferentes tipos de arquitecturas
- **Fase de pruebas:** Se han definido los paquetes de pruebas necesarios y se han realizado las pruebas sobre arquitecturas más completas y cercanas a la realidad.

1.3.- Arquitectura

Se han definido unas arquitecturas especiales que ayudarán a determinar el comportamiento de funcionalidad de la aplicación. En un primer momento las pruebas se realizaron sobre cabeceras generadas en su totalidad con equipos del laboratorio.

Posteriormente, surgió la necesidad de probar la aplicación en un entorno real. La arquitectura para este tipo de entorno, se complica y es necesario más equipos para poder realizar las pruebas. El gráfico siguiente muestra de una manera genérica esta estructura más completa.

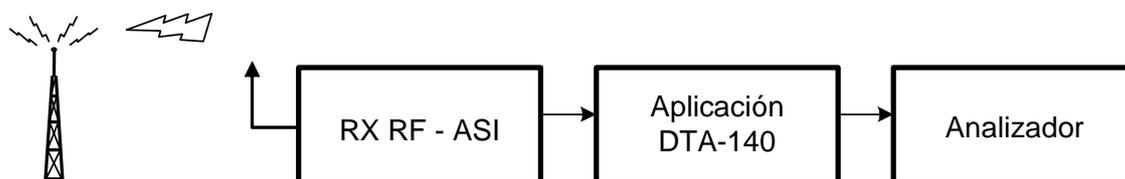


Figura 1.- Arquitectura genérica

Para la realización del proyecto se ha trabajado con cuatro arquitecturas diferentes. Las dos primeras, son arquitecturas sencillas, mientras que las dos últimas son arquitecturas más complejas, similares a las descritas en el gráfico anterior. En puntos posteriores se detallarán todas las arquitecturas de manera más completa.

1.4.- Estructura de la memoria

Esta memoria se estructura en diferentes partes. Se ha intentado ordenar los puntos de manera que a medida que se avanza en la lectura de la memoria, se va profundizando en las diferentes fases del proyecto realizado.

En el capítulo primero, se da una introducción breve al proyecto, explicando sus objetivos principales, sus fases, nociones sobre las arquitecturas montadas y una visión general de la estructura de la memoria.

En el segundo capítulo se aporta información relacionada con el proyecto. Éste se centra en temas como una pequeña introducción al acceso condicional, dado que el proyecto está centrado en el desarrollo de una aplicación orientada al acceso restringido a los servicios de la TDT. También se hace una breve introducción a los tipos de encriptado y los diferentes tipos de acceso condicional que contempla el “Digital Video Broadcasting” (DVB). Por último, en vista que los avances en materia de acceso condicional están restringidos por la situación legal vigente y por el desarrollo de la TDT, se han estudiado las leyes y planes de los últimos años, para tener una idea de las implicaciones del marco legal en este tema, así como el marco regulador de la TDT, su evolución y situación actual en España y Europa.

El tercer capítulo se centra en aportar información más técnica y cercana a la aplicación. En él, se presentan los conceptos de Información de Servicio (PSI/SI), pasando por el DVB y el estándar MPEG-2. También se aporta información detallada sobre un TS, su composición y la forma de trabajar con él. Finalmente se enumeran todos los elementos hardware y software, utilizados para el desarrollo del proyecto, dando una breve descripción de cada uno de ellos.

En el capítulo cuarto se amplían los puntos de planificación y arquitectura, dando información más detallada de las fases por las que se ha pasado para el desarrollo del proyecto, así como de las diferentes arquitecturas utilizadas. Por último se detallan los componentes de la aplicación, justificando la necesidad y la elección de cada uno de ellos.

Finalmente se presentan algunos anexos, glosario de términos, referencias y bibliografía.

2.- Contexto

2.1.-Acceso Condicional

2.1.1.-Definición

Dentro de la cadena de distribución de televisión digital, el Sistema de Acceso Condicional (CAS) tiene como objetivo limitar la recepción de determinados servicios únicamente a los usuarios autorizados por el proveedor del servicio. Dichos usuarios estarán provistos de un receptor apropiado para la recepción de estos servicios. El CAS permitirá seleccionar los servicios y los instantes de tiempo en que éstos pueden ser utilizados por los usuarios autorizados. Permite también gestionar de forma sencilla las autorizaciones de cada usuario, bien de forma individual o colectiva.

En la siguiente figura podemos ver las tres principales plataformas de TV Digital que hasta hace poco operaban en España: [1]

Acceso Condicional			
Fabricante			
Tipo	Simulcrypt	Multicrypt	Multicrypt

Figura 2.- Plataformas acceso condicional España

2.1.2.-Encriptación

La reserva de los derechos adquiridos sobre las producciones a retransmitir así como el cumplimiento de las obligaciones legales, hace imprescindible proceder a la encriptación de la señal transmitida.

Se han desarrollado varios sistemas de encriptación que han ido evolucionando a los largo de los años, principalmente, para mejorar su protección contra “hackers”.

En los siguientes apartados se describen dos.

2.1.2.1.-Criptografía de clave secreta o simétrica

La criptografía simétrica se basa en la utilización de la misma clave para el cifrado y para el descifrado, es decir, la robustez de un algoritmo de cifrado simétrico recae en el conocimiento de dicha clave. Sus ventajas son la sencillez de implementación, su rapidez y

la robustez que provee; sin embargo, la manera de distribuir las claves a los usuarios es difícil de resolver: la distribución de claves: como la clave debe ser secreta para garantizar plenamente la confidencialidad de los datos cifrados, ¿cómo y a quién se distribuyen las claves para permitir una comunicación bidireccional. [2]

La figura 2 esboza un criptosistema de clave secreta o simétrico:

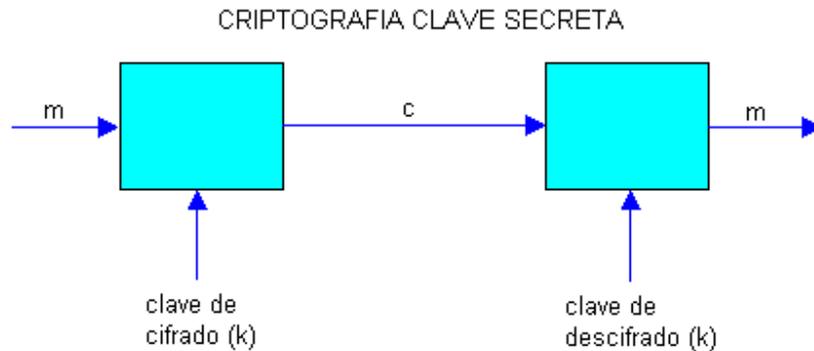


Figura 3.- Sistema de clave secreta o simétrico.

Un ejemplo matemático sería una operación con inversa como la raíz cuadrada. Dentro de la criptografía, los algoritmos de cifrado simétrico más comunes son DES, Triple-DES, IDEA, Rijndael.

2.1.2.2.-Criptografía de clave pública o asimétrica

Como solución al problema de la distribución de claves nació la criptografía de clave pública, que se basa en la utilización de dos claves, una para cifrar y otra para descifrar. A partir de un mensaje cifrado con su clave, se puede obtener el mensaje con la clave de descifrado; es decir, un usuario A cifra un mensaje con la clave pública del usuario B (destinatario), éste para descifrarlo utiliza su clave secreta únicamente conocida por él; por tanto cada usuario tendrá que mantener y gestionar dos claves, lo cual hace más complejo y lento el sistema. Dicho esquema se presentó en 1976 por Diffie y Hellman.

La siguiente figura muestra un criptosistema de clave pública:

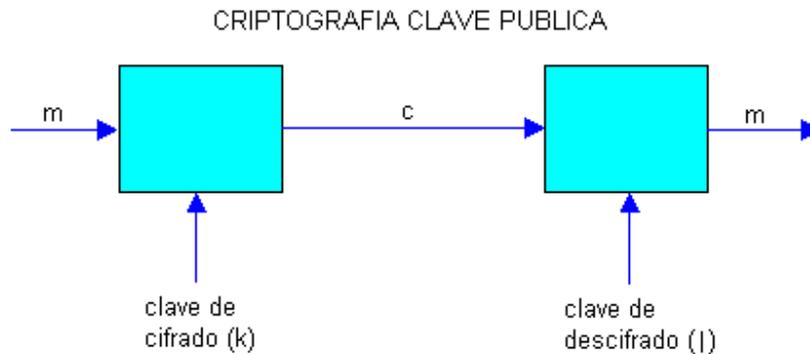


Figura 4.- Sistema de clave pública o asimétrica

Entre los ejemplos de criptosistemas de clave pública se encuentra el famoso RSA, El Gamal. [3]

2.1.3.-Tipos de acceso condicional

Para hacer decodificadores con un uso más universal, los dos procesos que se establecieron bajo la norma estándar del sistema DVB son “simulcrypt” y el “multicrypt”.

2.1.3.1.-Symulcrypt

Es el tipo de acceso condicional utilizado por Canal Satélite digital. Es un sistema que se caracteriza por permitirle a la plataforma poseer varios sistemas de acceso condicional diferentes. La ventaja es que puede utilizar diferentes fabricantes de decodificadores. [4]

2.1.3.2.-Multicrypt

Es el tipo de acceso condicional que había utilizado Vía Digital. La diferencia con el primero es que permite la utilización de dos sistemas de acceso condicional en el mismo decodificador mediante un módulo de ampliación (posiblemente una tarjeta PCMCIA). [5]

2.2.- Marco legal

En los últimos años, el panorama audiovisual en nuestro país, se ha visto afectado por grandes cambios debido a la implantación de la televisión digital. Términos como “accesibilidad universal” o “integración”, están tomando mucha importancia y se están convirtiendo en valores de peso en este nuevo despliegue. Actualmente, la rápida introducción de la TDT en los hogares, junto con el inminente apagado de las emisiones analógicas, hace que la integración total de la población tome un carácter prioritario. Sobre todo, si se tiene en cuenta que se están estableciendo las bases para una plataforma digital, donde tengan cabida todos los públicos. Es por ello, que tanto a nivel nacional como europeo, se está intentando crear un marco legal, donde se definan las pautas a seguir para poder conseguir uno de los principales objetivos de la televisión digital: “Televisión para todos”.

La accesibilidad debe representar un elemento importante de la calidad de vida de todos los ciudadanos, y debe ser exigible como un derecho. Basándose en esta idea, las iniciativas reguladoras y legislativas en dicha materia se han ido mejorando a lo largo del tiempo, y se pretende que, en un futuro, converjan en un marco adecuado donde no exista la discriminación.

Este apartado se centra en el marco legal que envuelve a la accesibilidad en TDT.

2.2.1.-Marco Europeo

2.2.1.1.-Protección jurídica de los servicios de acceso condicional o basados en dicho acceso

ACTO

Directiva 98/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso.

SÍNTESIS

Ámbito de aplicación

La propuesta cubre todos los servicios prestados sobre la base de un acceso condicional, como la televisión o la radio de pago, los servicios de vídeo y audio a la carta, la edición electrónica, o una extensa gama de servicios en línea que se ofrecen al público previo pago de un abono o mediante un pago por consumo.

Actividades infractoras

Todos los Estados miembros adoptarán las medidas necesarias para prohibir en su territorio las siguientes actividades:

- la fabricación, importación, distribución, venta, alquiler o posesión con fines comerciales de dispositivos ilícitos, es decir, cualquier equipo o programa informático diseñado o adaptado para hacer posible el acceso a un servicio protegido.
- la instalación, el mantenimiento o la sustitución --con fines comerciales-- de un dispositivo ilícito;
- el uso de comunicaciones comerciales para la promoción de dispositivos ilícitos.

Sanciones y recursos

Los Estados miembros adoptarán las medidas necesarias para:

- prever sanciones eficaces, disuasorias y proporcionadas al efecto potencial de la actividad infractora;
- velar por que los proveedores de servicios protegidos cuyos intereses se vean afectados por una actividad infractora llevada a cabo en su territorio puedan interponer una demanda por daños y perjuicios, y pedir una orden judicial o, en su caso, la incautación de los dispositivos ilícitos.

Principios relacionados con el mercado interior

Los Estados miembros no podrán:

- restringir la prestación de servicios protegidos, o de servicios vinculados, que tengan su origen en otro Estado miembro;
- restringir la libre circulación de los dispositivos de acceso condicional, con excepción de los dispositivos que la Directiva califica de ilícitos. [6]

2.2.2.-Legislación española

La incorporación de la Directiva 95/47/CE al Derecho español se llevó a cabo mediante el Real Decreto-Ley 1/1997, de 31 de enero, el cual vino a cubrir la laguna normativa existente en materia de sistemas de acceso condicional, en un momento en el que era inminente la puesta en servicio en España de una plataforma de televisión digital por satélite. Este Real Decreto-Ley fue convalidado por las Cortes Generales, después de su tramitación como proyecto de ley, lo que dio lugar a la aprobación en mayo de 1997 de la Ley 17/1997.

El Real Decreto-Ley 16/1997, de 13 de septiembre, de modificación de la Ley 17/1997, admite todos los tipos de decodificadores, siempre que éstos sean inmediata y

automáticamente abiertos y compatibles. El carácter de inmediata y automáticamente abiertos y compatibles puede resultar de dos maneras:

- las características técnicas de los decodificadores (multicrypt).
- de un acuerdo entre los operadores (simulcrypt).

Para el efectivo cumplimiento de lo anterior se atribuyen a la CMT una serie de facultades, entre las que se encuentra la de fijar las condiciones legales, técnicas y económicas del acuerdo entre los operadores cuando el descodificador no es directamente abierto desde un punto de vista técnico y los operadores no son capaces de llegar a un acuerdo.

El Real Decreto-Ley 16/1997, de 13 de septiembre, es la última norma aprobada en este ámbito, por lo que no se ha producido ningún cambio con respecto a la situación descrita en el informe de la Comisión Europea de noviembre de 1999.

Se considera que la Ley 17/97, con su modificación por el Real Decreto-Ley 16/97, incorpora por completo al Derecho español todas las disposiciones de la Directiva 95/47/CE, por lo que no existen disposiciones de esta Directiva que no se hayan incorporado a la legislación española.

La Ley 17/97, con su modificación por el Real Decreto-Ley 16/97, incorpora por completo al Derecho español todas las disposiciones de la Directiva 95/47/CE, e incluye además algunas disposiciones sobre:

- a) la definición de los sistemas y servicios de acceso condicional;
- b) el Registro de operadores de acceso condicional;
- c) la necesidad de que los decodificadores sean abiertos y compatibles, bien por sí mismos, o bien por acuerdos entre los operadores;
- d) las condiciones impuestas a los operadores de acceso condicional para TV digital para garantizar que éstos ofrezcan sus servicios técnicos en condiciones no discriminatorias a todas las entidades de difusión;
- e) la prohibición de que los operadores de acceso condicional condicionen la contratación de los servicios a la utilización de sus propios equipos de codificación y de control de facturación.

Por lo que respecta a la Autoridad Nacional de Regulación, en España, las autoridades encargadas de la aplicación de la Directiva 95/47/CE son el Ministerio de Ciencia y Tecnología, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y la Comisión del Mercado de las Telecomunicaciones.

Por otra parte, para asegurar la interoperabilidad entre los diferentes sistemas de acceso condicional utilizados por los operadores, la normativa española exige que los sistemas y decodificadores para el acceso condicional que se comercialicen sean inmediata y automáticamente compatibles, bien por las características técnicas de éstos o por un acuerdo entre operadores (art. 7.º de la Ley 17/1997, con la modificación introducida por el Real Decreto-Ley 16/1997)).

Cuando los decodificadores no son abiertos y compatibles por sus características técnicas, los operadores, al ser inscritos en el Registro de Operadores de Servicios de Acceso Condicional asumen el compromiso de que pueden ser abiertos y compatibles mediante

acuerdos entre los operadores. La CMT, a falta de acuerdo, puede establecer, a instancia de cualquier operador, las condiciones jurídicas, técnicas y económicas equitativas, razonables y no discriminatorias que garanticen el carácter inmediata y automáticamente abierto y compatible de los sistemas.

El resultado final es que se impone la interoperabilidad entre los sistemas y decodificadores para acceso condicional, sin ceñirse a una tecnología concreta ni a un componente concreto del decodificador. Todos y cada uno de los componentes que este equipo incorpore, sean propietarios o estandarizados, deberán permitir que en su conjunto y como resultado final perseguido, no impidan que el decodificador del usuario sea inmediata y automáticamente abierto y compatible, en otras palabras, que permita recibir toda la gama de servicios de televisión digital que se exploten en el mercado. Esta interpretación de la norma permitiría asimismo considerar que las nuevas tecnologías que se incorporan al decodificador (APIs, herramientas de navegación, etc.) no pueden actuar en contra de esa obligación de resultado marcada por la Ley.

2.3.-TDT (Televisión Digital Terrestre)

La Televisión digital es una nueva forma de ver y entender la televisión, que permite, además de visualizar contenidos, ofrecer diferentes tipos de servicios y funcionalidades que no se podían implementar con la televisión analógica.

La televisión digital ofrece muchas ventajas en comparación con otros medios de comunicación. Sus características principales están detalladas en el punto 6 de este apartado. Se hace necesario remarcar que la televisión es un medio de comunicación que cuenta con un gran número de seguidores, los cuales ya están familiarizados con ella. Es un sistema aceptado por toda la población y que no requiere la dificultad de uso de otras tecnologías.

Por otro lado, la TDT también presenta una serie de requerimientos mucho más fuertes como son la necesidad de herramientas de gestión de Información de Servicio (también conocida como SI y explicada en puntos posteriores), la necesidad de herramientas de descarga remota de software, y la posibilidad de encriptar eventos y/o programas que deben ser resueltos a través tecnología.

2.3.1.-Marco regulador

En España, los primeros pasos para el despliegue de la TDT vinieron condicionados por el Real Decreto 2169/1998, también llamado “Plan Técnico de la TDT”. En él, se recogían puntos generales importantes (plazos, asignaciones,...) para la implantación de esta nueva televisión. Entre ellos destacan:

- Asignación de las bandas de emisión del servicio de TDT.

- Modo de configuración de redes 8 K para permitir la generación de redes SFN de amplia cobertura.
- Establecimiento de una red isofrecuencia de cobertura nacional formada por cuatro canales múltiples (16 programas), cuyas licencias de explotación serían concedidas posteriormente a Quiero TV (14) (Diciembre 1999) + Net TV (1)+Vevo TV (1) (Junio 2002)
- Definición de una red a nivel nacional con posibilidad de desconexiones regionales, que fue concedido a los tres canales privados con licencia nacional en analógico (Antena 3, Tele5, Canal +) y dos canales a TVE; emitiendo el mismo contenido (Simulcast). (Abril 2002)
- Reserva de un canal radioeléctrico autonómico para redes SFN.
- Limitación del servicio de datos de un 20% de la capacidad del canal múltiple.
- Apagado analógico antes del 1 de Enero del 2012.

Con este Plan quedaba acotado el plazo máximo para realizar el corte analógico, además de definidos una serie de parámetros como asignaciones, configuraciones y limitaciones.

Algunos años más tarde, por otro lado, se definió el ámbito de las cadenas locales. Para ello, se creó el Real Decreto 439/2004, posteriormente modificado por el 2268/2004, donde se aprobó el Plan Técnico de la TDT Local:

- Se crean 281 (266+15) demarcaciones de televisión local digital en las distintas Comunidades Autónomas, asignándose frecuencias a las capitales de provincia y municipios con más de 100.000 habitantes.
- Cada demarcación tendrá al menos un canal múltiple. Si el espectro radioeléctrico lo permite se podrán asignar hasta dos canales múltiples.
- Cada canal múltiple tendrá como mínimo cuatro programas, pudiéndose establecer un número mayor en caso de que la tecnología lo permita salvaguardándose la calidad del servicio.
- Modo de configuración de redes 8 K para permitir la generación de redes SFN.
- Limitación del servicio de datos de un 20% de la capacidad del canal múltiple.

Como puede verse, el Plan Técnico de la TDT Local incluye nuevas especificaciones. También mantiene algunas características establecidas en el Plan anterior más general.

Por último, para agilizar el proceso de implantación se creó la Ley de Medidas Urgentes para el Impulso de la Televisión Digital Terrenal. Fue aprobada en Consejo de Ministros el día 30 de Diciembre del 2004. En ella, se recogen los siguientes puntos:

- Modificación del Plan Técnico de la TDT antes de verano del 2005.
- Pronta asignación de frecuencias de Quiero TV para que los nuevos programas puedan estar operativos en otoño del 2005.
- Coordinación de las fechas de lanzamiento de las televisiones de ámbito nacional con las autonómicas y locales digitales:
 - Estatales: Nuevos programas en otoño del 2005.
 - Autonómicas: A partir de Enero del 2005.
 - Locales: Desde Agosto 2005 a 1 de Enero 2008.

- Adelanto del apagado analógico al 1 de Enero del 2010.

Con estas medidas se pretendía que a finales del 2005, existieran 21 programas en TDT en abierto gratuitos. De esta forma se acelera el proceso de implantación de la TDT para poder adelantar el apagado analógico 2 años.

2.3.2.-Evolución de la TDT en España

Para entender la evolución que ha seguido la TDT en España, es necesario remontarse a 1998 cuando se creó el Plan Técnico Nacional de la TDT. A continuación se desglosan los hitos más importantes por cada año desde 1998 [7]:

1998

- Real Decreto 2169/1998: Plan Técnico Nacional de la TDT:
 - Plan de Cobertura.
 - Apagado Analógico el 01/01/2012.

2000

- Quiero TV comienza a emitir 14 programas.
- Utiliza la red de Retevisión: 147 Centros y 80% población.

2001

- Mux de la Comunidad de Madrid: (Telemadrid, La Otra, Quiero TV y Onda 6).
- Asignación Mux de La Rioja (2 + 2 privados).

2002

- Creación Foro TDT.
- Comienza la emisión de la RGN: TVE1, La 2, A3, C+ y Tele5.
- Cierre de Quiero TV.
- Comienzan a emitir Veo y Net TV.
- Cataluña asigna todo el Mux a la CCRTV.

2003

- Asignación Mux privado Cataluña (1 sólo privado).
- Asignación Mux Navarra (2 + 2 privados).

2004

- Plan técnico TDT local:
 - 266 Demarcaciones; 1064 programas TV local.
 - Apagado en 2006
 - Calendario TV Autonómicas Públicas en digital.
 - Reducción Cobertura Veo y Net al 25% de la población.
- SIMO: RTVE presenta contenidos interactivos.
- Modificación plan técnico:

- Incremento Demarcaciones: 281 Demarcaciones = 1124 programas TV locales.
- Apagado en 2008.
- Adjudicación 7 múltiplex locales en Baleares 28 programas.
- Plan del Consejo de Ministros:
 - Modificar varias leyes (Ley General Telecom., Ley TV Privada y Ley TV Local)
 - Anuncio de asignación frecuencias de Quiero TV.
 - Nueva fecha apagado analógico para 2010.

2005

- Remisión al Congreso del Proyecto de Ley de Medidas Urgentes para el Impulso de la TDT.
- Creación de la Comisión para la Transición a la TDT.
- Foro de la TV Digital
- Publicación en el BOE de la Ley 10/2005 (Medidas Urgentes...), de 14 de junio.
- Consejo de Ministros con el Plan de Reforma del Sector Audiovisual.
- Consejo Asesor de Telecomunicaciones
- Plan Técnico Nacional de la TDT.
- Aprobación Nuevo PTNTDT
- Corrección errores del PTNTDT modificando la fecha limite.
- Limite de presentación de las solicitudes de más canales digitales.
- Inicio emisiones nacionales digitales.

2.3.3.-Situación de la TDT

La evolución de la TDT ha seguido distintos caminos en cada país. Este apartado se divide en dos partes. Por un lado se aborda el ámbito europeo, donde se dan algunos datos de los países más avanzados y datos generales sobre índices de penetración, apagados y venta de receptores. Por otro lado, se analiza la situación particular española.

2.3.3.1.-En Europa

En este punto se detalla la situación de los países más evolucionados hasta el momento en cuanto a TDT [7]:

Reino Unido (Freeview):

- 35 Programas de TV gratuitos.
- 25 Emisiones de Radio.
- Servicios interactivos (MHEG-5).
- 11 Programas de TV de pago (Top Up).

Italia (Dgtv):

- 33 Programas nacionales de TV, gratuitos, con aplicaciones interactivas.

- 6 Emisiones de radio.
- 12 Servicios de Pago por evento (fútbol, cine).

Francia (TNT):

- 18 programas de TV gratuitos.
- 11 Programas de TV de pago.

Resulta interesante también, conocer las fechas de apagado, los porcentajes de penetración así como el número de receptores TDT vendidos hasta el momento. Estos datos nos dan una idea de cómo va evolucionando la expansión de la TDT a nivel europeo. En las 2 tablas siguientes se muestran estos datos:

Países	Penetración	Apagado
Reino Unido	70% (SAT+TDT+Cable)	2012
Suecia	12% (540.000 hogares)	2008
Finlandia	30%	2007
Alemania	25,7% (SAT+TDT+Cable)	2010
Francia	10%	2011
Italia	20% (4.000.000 hogares)	2008

Figura 5.- Penetración TV Digital y fechas de apagado

En el caso de Reino Unido y Alemania los datos que se disponen de TDT van unidos a satélite y cable. Es difícil de obtener una idea de la evolución en esto dos casos.

Países	1998	1999	2000	2001	2002	2003	2004	2005
Reino Unido	247	552	774	1240	1260	3900	6380	8700
Suecia		15	35	85	100	200	425	475
Finlandia				10	40	300	400	690
Alemania						170	1700	1900
Francia								1420
Italia						25	1000	3250
TOTAL	247	567	809	1335	1400	4595	9905	16435

Figura 6.- Venta de receptores TDT

2.3.3.2.-En España

Según los estudios realizados en mayo de 2006 [7], la implantación de la TDT en España continuaba mejorando:

- Se alcanzó la cifra de 3,8 millones de hogares con acceso a la TDT (20% del total).
- Se contabilizaron 1.650.000 receptores TDT vendidos. Se preveía que a final de 2006 se alcanzaría la cifra de 2.200.000 (el total de ventas se estima en 28.000.000).
- El índice de penetración de la TDT es de un 5,8% sobre el parque de televisores y de un 12% sobre el parque de hogares. (Este dato ha sido obtenido sobre 190.000 edificios con 20 viviendas/edificio).

La situación de los programas era la siguiente:

20 Programas nacionales gratuitos de TV:

- 4-8 programas autonómicos.
- 4-8 programas locales.
- Radio + servicios interactivos.

2.3.4.-Estado de la tecnología

La tecnología empleada para difundir la señal de TDT, se basa en el estándar DVB-T. Se trata de una tecnología madura, donde las soluciones en cuanto a modulación, transmisión y receptores están bien definidas y dan buenos resultados. Se espera, a corto plazo, el descenso de precios en los receptores MHP y con tarjeta “smartcard” . De esta manera, se incrementarán los índices de penetración de este tipo de receptores en el mercado, con lo cual se alcanzará un entorno digital completo extremo a extremo.

En un futuro cercano, se prevé una evolución tecnológica de la TDT para alcanzar mayor calidad y prestaciones. Estos avances se conseguirán gracias a sistemas de codificación avanzada, basados en el estándar MPEG-4. Gracias a ellos se permitirá:

- Aumentar el número de canales.
- Ofrecer servicios de Televisión de Alta definición.
- Modificar los modos de las redes y hacerlas más robustas.
- Mejora en las herramientas de gestión y almacenamiento de contenidos

2.3.5.-Capas del servicio TDT

El servicio de TDT está estructurado en 4 capas tal como se detalla en el esquema de la figura. Para llevar a cabo este proyecto, ha sido necesario trabajar con las cuatro capas, desde la multiplexación e inyección de SI (Capa2) a Aplicaciones interactivas (Capa 3). Además, se ha estudiado el sistema de Difusión implantado actualmente en España (Capa 1), y por supuesto se ha tenido que trabajar con la capa 4:

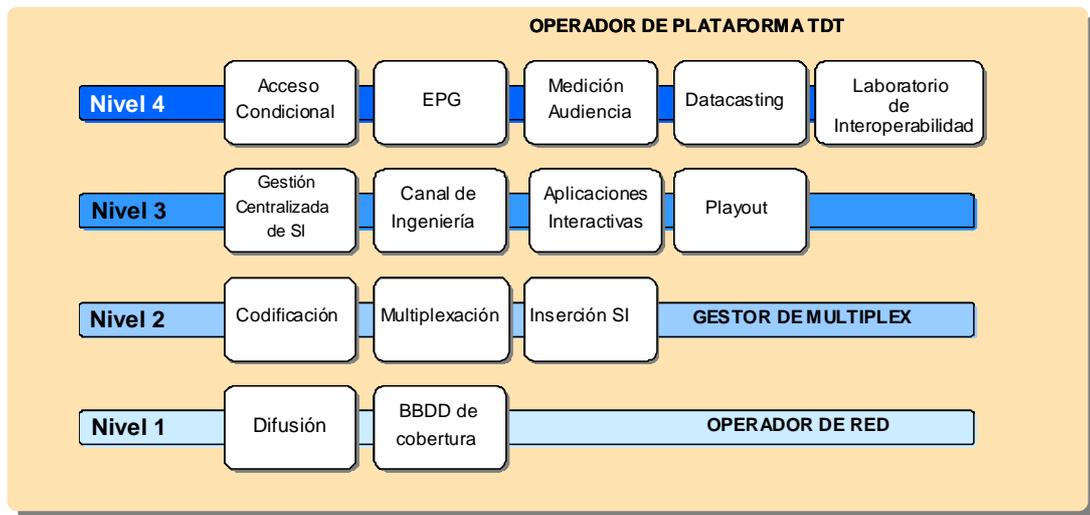


Figura 7.- Capas del servicio TDT

2.3.6.-Características de la TDT

Como ya se ha comentado el paso del mundo analógico al digital ofrece una serie de ventajas. Estas nuevas características dan un valor añadido a la TDT, respecto al sistema analógico anterior. Se podrán ver más canales, con más calidad y con interactividad. A continuación se detallan los aspectos más relevantes:

- Aumenta el número de canales ofrecidos: En el lugar donde antes se emitía un canal, ahora se pueden emitir 4. Se ofrecen canales generalistas, temáticos y algunos dirigidos específicamente a cierto público.
- Aumenta la calidad del vídeo y del audio: El vídeo tiene calidad DVD y se permite el formato 16:9. En cuanto al audio, se puede tener Dolby 5.1. Además, la calidad de vídeo y audio es fácilmente controlable.
- Se pueden transmitir otro tipo de datos además del audio y el vídeo. Así, pueden ofrecerse servicios como aplicaciones interactivas, que se ejecuten en el receptor del usuario. De esta manera se consigue que el espectador pase de comportarse pasivamente ante el receptor y comience a influir en los contenidos y servicios visualizados.

3.- Entorno

Para poder comprender el contexto completo en el que sitúa este proyecto, es necesario tener cierto conocimiento sobre MPEG-2 y DVB, así como de señalización PSI/SI.

Además, al trabajar con temas de acceso condicional, se hace necesario conocer las diferentes normativas relacionadas con la encriptación del transport stream. Es por todo ello que se ha organizado este apartado en los puntos siguientes:

- 3.1.- MPEG-2.
- 3.2.- DVB.
- 3.3.- PSI/SI.
- 3.4.- Transport Stream.(TS)
- 3.5.- Entorno de desarrollo.

Obsérvese como el último punto está orientado a la descripción más concreta del material utilizado. Finalmente en el apartado siete se hará una descripción técnica.

3.1.- MPEG-2

MPEG-2 es un estándar genérico definido por el comité MPEG (Motion Picture Expert Group). Sus especificaciones no están orientadas a ninguna aplicación concreta, pues incluye un conjunto de herramientas que permiten su uso en un gran nombre de aplicaciones. Esta flexibilidad provoca que sea un estándar muy complejo, pero muy útil para un gran número de aplicaciones digitales.

MPEG-2 especifica los formatos con que se deben representar los datos a la entrada del descodificador y el conjunto de reglas y procesos de descodificación. Sus principales aplicaciones son:

- TV: Radiodifusión terrestre, satélite y cable.
- HDTV: Radiodifusión terrestre, satélite y cable.
- Vídeo en sistemas de almacenamiento digital.
- Vídeo bajo demanda (VoD).
- Videocomunicación: vídeo multipunto y múltiples calidades.
- Vídeo sobre diferentes redes: ATM, Ethernet, LAN, ...
- Edición no lineal, post producción.

La aparición de MPEG-2 provocó que el mundo digital pasara de ser una industria donde todo el mundo iba por libre, a ser una industria dinámica y unificada, con estándares que fomentaban la interoperabilidad de los productos y la competitividad.

Inicialmente MPEG-2 se dividía en diez partes, pero la parte 8 (bit video), finalmente se canceló. Con lo cual actualmente hay 9 partes en el estándar MPEG-2 cada una de ellas dedicadas a un ámbito:

- Systems: Especifica como combinar o multiplexar diferentes tipos de información multimedia en un solo stream para que puede ser transmitido o almacenado.
- Vídeo: Especifica la codificación de la señal de vídeo.
- Audio: Especifica la codificación de la señal de audio.
- Conformance: Especifica como se tienen que diseñar los tests para la verificación del bit stream y de los descodificadores.
- Software: Especifica software de simulación correspondiente a las partes: Systems, Vídeo y Audio.
- Digital Storage Media – Command and Control (DSM-CC): Especifica protocolos para gobernar la interacción de los usuarios con bitstreams de MPEG-1 y MPEG-2 almacenados en DSM.
- Non Backward Compatible (NBC) Audio: Especifica la codificación de la señal de audio en un formato no compatible con el sistema MPEG-1.
- Real Time Interface (RTI): Especifica un interfaz en tiempo real entre el adaptador al canal de transmisión y el descodificador de transport stream de MPEG-2 Systems.
- DSM-CC Conformance: Especifica métodos para verificar si una implementación DSM-CC cumple la parte 6 de MPEG-2 DSM-CC.

Dado que el estándar DVB (descrito en el siguiente apartado) sólo usa tres partes: MPEG-2 Systems, MPEG-2 Audio y MPEG-2 Video, no se explicarán el resto de partes. Más información se puede encontrar en la referencia bibliográfica [].

3.1.1.- Breve historia

En los años 80, se desarrollaron las primeras normativas para la digitalización de las señales de vídeo y audio, basados todos los algoritmos en el comportamiento del ojo y el oído humano, más sensibles a determinadas señales.

En los años 90 el comité de la ISO denominado MPEG desarrolló el primer estándar de compresión digital común para el audio y el vídeo, el ISO 11172, el MPEG-1. De forma paralela, se trabajó en un estándar, compatible con el anterior, pero con el objetivo de especificar un sistema de codificación de audio y vídeo apropiado para la transmisión a través de diferentes redes, y para el almacenamiento en diferentes formatos digitales. El resultado fue el estándar ISO 13818, MPEG2. [Anexo 7.2]

3.1.2.- MPEG-2 Vídeo

El flujo necesario para poder transmitir determinados formatos de vídeo digital puede llegar a ser de 270 Mbps. Por tanto, se hace necesaria la existencia de un formato estándar de vídeo comprimido que reduzca estos “bit rates” tan elevados.

La especificación de MPEG-2 parte de una señal de vídeo 4:2:2 (270 Mbps) o 4:2:0 (162 Mbps) y reduce estas velocidades binarias tan elevadas gracias a la compresión de vídeo. Esta compresión está basada en la incapacidad del ojo humano para discernir variaciones de alta frecuencia en la señal de color. Para ello, se aplican tres tipos de compresión. El objetivo es reducir al mínimo la presencia de la señal de redundancia espacial, temporal y estadística:

- Redundancia espacial: En una imagen, un píxel y sus vecinos guardan mucha similitud entre ellos.
- Redundancia estadística: En una secuencia de bits, existen valores de bits que se repiten.
- Redundancia temporal: En una secuencia de imágenes, un mismo píxel tiene tendencia a repetirse temporalmente. Es la redundancia que más fácilmente se puede eliminar, provocando así un mayor factor de compresión.

3.1.3.- MPEG-2 Audio

Las técnicas de compresión permiten reducir el “bitrate” que requieren dos canales de audio de calidad CD de 1,4 Mbps hasta 200 Kbps.

La compresión de la señal de audio aprovecha las características psicoacústicas del oído humano, y el hecho de que los tonos de alta potencia tienden a enmascarar los tonos de potencia inferior adyacentes.

El proceso de compresión parte de la señal de audio de 0 Hz a 22 KHz. Esta señal está dividida en 32 sub-bandas frecuenciales. Cada sub-banda se filtra, se cuantifica y se codifica según las características del oído humano.

MPEG-2 audio no aporta mejoras a nivel de compresión respecto a MPEG-1 sino que abre posibilidades, como por ejemplo enviar 5 canales de audio para sonido envolvente y hasta 7 canales monofónicos para diferentes idiomas.

3.1.4.- MPEG-2 Systems

De los procesos de codificación de audio y vídeo se obtienen las tramas elementales (Elementary Streams - ES). Dichas tramas son un flujo continuo de datos que contienen información de una única fuente de audio o vídeo. Para construir programas, hace falta un sistema de asociaciones entre ellos, que aporte además sincronización de los diferentes flujos. MPEG-2 da solución a esto que multiplexar los diferentes ES, que provienen de las etapas anteriores de codificación, para obtener un Transport Stream (TS). El TS será el único flujo de información que se enviará por el canal y, por tanto, a parte de contener diferentes Elementary Streams multiplexados, también llevará información que permita

localizar estos ES y desmultiplexarlos de manera sincronizada. En la figura 8 podemos verlo de una forma gráfica.

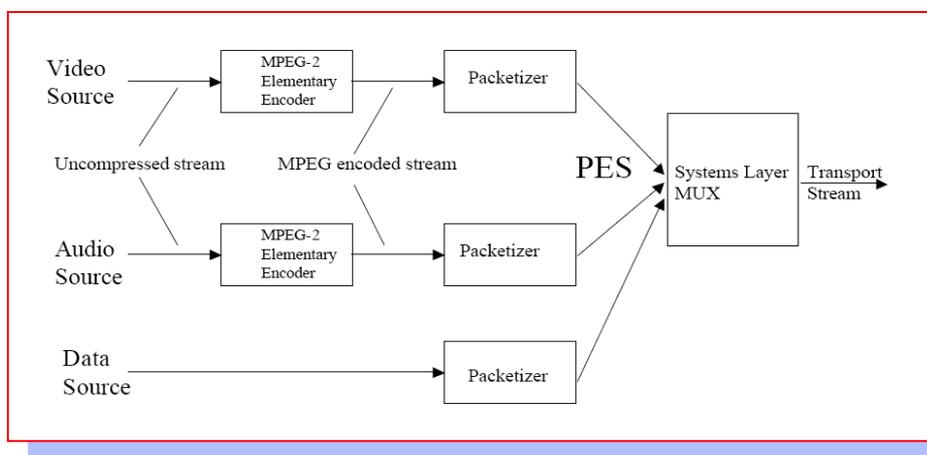


Figura 8.- Esquema de elementos que conforman un Transport Stream

El proceso para obtener un TS a partir de un ES, pasa por adaptar estos ES a paquetes del tipo Packetised Elementary Streams (PES). Para ello se divide cada ES en trozos. Cada trozo es llamado PES. Un PES consiste en una cabecera y un “payload”. El “payload” consiste en los datos cogidos secuencialmente del ES. Los paquetes PES pueden ser de longitud variable hasta un máximo de 64 KBytes. Dicha longitud dependerá del “bitrate” que tengan los ES en el momento de empaquetarlos en paquetes PES. Para que el multiplexor pueda trabajar con paquetes de longitud constante se convierten los paquetes PES en paquetes de 188 bytes llamados paquetes TS. Estos paquetes TS han de poder ser transmitidos a través de canales muy ruidosos y propensos a introducir errores como en las redes de cable o satélite. Es por ello que tienen una longitud tan reducida.

El último paso para tener un único TS, es multiplexar los paquetes TS en un único TS. La única restricción para multiplexar los diferentes paquetes es mantener el orden secuencial entre los paquetes de un mismo ES.

Al otro lado de la cadena, en el receptor, el primer paso es extraer la información de sistema para poder identificar los datos recibidos y regenerar los ES. Para que un TS pueda ser descodificado por el receptor es necesaria la transmisión de estructuras auxiliares. Estas estructuras auxiliares o datos de sistema son un conjunto de tablas. Las conocidas como PSI/SI. Su funcionamiento se explicará en el punto 3. Una vez regenerados los ES, son decodificados, y las unidades de presentación resultante de este proceso son almacenados en buffer para ser presentados en el momento indicado.

Para sincronizar el codificador y el decodificador se utilizan los timestamps y las referencias de reloj son muestras o valores que intervienen en el proceso de codificación y multiplexación de cada programa. Cada programa tiene asignado un reloj, System Time Clock (STC), que se toma como la base de tiempos.

3.2.- DVB

El proyecto DVB (Digital Video Broadcasting) aparece en 1993 como respuesta a las necesidades de proporcionar un formato común que permitiera la difusión de televisión Digital. El proyecto incluye representantes de más de 200 compañías de unos 25 países de todo el mundo. Su objetivo es el establecimiento de un marco de referencia para la introducción de servicios de televisión digital a través de diversos medios de transmisión, así como el desarrollo de normas y métodos de operación de sistemas de transmisión por satélite, cable, etc.

Una de las primeras decisiones del DVB fue utilizar el MPEG-2 como estándar de compresión de vídeo y audio. Por otra parte el DVB definió las técnicas de modulación y métodos de codificación para la corrección de errores, que permitan la transmisión vía satélite, cable y terrestre (DVB-S, DVB-C y DVB-T). También ha proporcionado un algoritmo común para los sistemas de acceso condicional, ha definido la transmisión de la información de servicio (DVB-SI) que permite al espectador un acceso fácil y rápido al programa y ha establecido formatos para la inserción de datos para aplicaciones.

El DVB no crea sus estándares sino que proporciona las especificaciones que son entregadas a organizaciones como ETSI, CENELEC, ITU-R, ITU-T i DAVIC.

España ha adoptado el estándar DVB-T para la emisión de la señal de TDT en todo el territorio.

3.2.1.- Identificadores

Dado que la televisión digital permite tener una gran cantidad de canales, comparado con el sistema analógico, surge la problemática de identificación de cada uno de ellos. Hasta ahora, cada canal estaba identificado con su canal de frecuencia, pero ahora en una misma frecuencia de canal puede haber hasta 4 canales de vídeo más algunos de radio.

Para poder definir de manera inequívoca cada uno de los servicios que existen, se hace necesario tener algún tipo de señalización especial. DVB ha definido una serie de identificadores para solventar este problema. Estos identificadores son obligatorios. Su asignación viene recogida en la normativa ETR 162 del ETSI, "Allocation of Service Information(SI) codes for DVB systems". [8] Su asignación es responsabilidad de la ETSI:

- Dos identificadores relativos a las redes. Dichos identificadores son:
 - El identificador de red originaria (**Original_Network_id**): Permite la identificación unívoca del servicio contenido en un determinado flujo de transporte, independientemente del tipo de red por el que ese flujo de transporte está siendo transportado. Hace referencia a la red originaria de entrega de dicho flujo.

- El identificador de red (**Network_id**): Por su parte, el identificador de red corresponde con la red de entrega que está transportando ese flujo de transporte.

- **Transport_Stream_ID**: El identificador de flujo de transporte es un parámetro que, en combinación con el Original_Network_ID, permite la referencia unívoca de un determinado flujo de transporte.

- **Service_ID**: permite la referencia unívoca de un flujo dentro de un flujo de transporte.

A través de estos identificadores, un servicio queda unívocamente identificado a través de la siguiente combinación de parámetros: Original_Network_ID + Transport_Stream_ID + Service_ID.

Por otro lado, dada la combinación Original_Network_ID + Service_ID, aunque no constituye una referencia unívoca a un servicio, debe apuntar a un único servicio. Ello implica que un servicio puede referenciarse sin ambigüedad por dicha combinación, aunque para un determinado servicio puedan existir varios Service_ID en un mismo Original_Network_ID.

3.2.2.- DVB en el mundo

En el gráfico de la figura 9 [8], además de otros sistemas como DMB, ISDB, DVB-H y ATSC, se muestran los países que han adoptado el sistema DVB-T en el mundo. El gráfico está actualizado con datos de Septiembre de 2006.

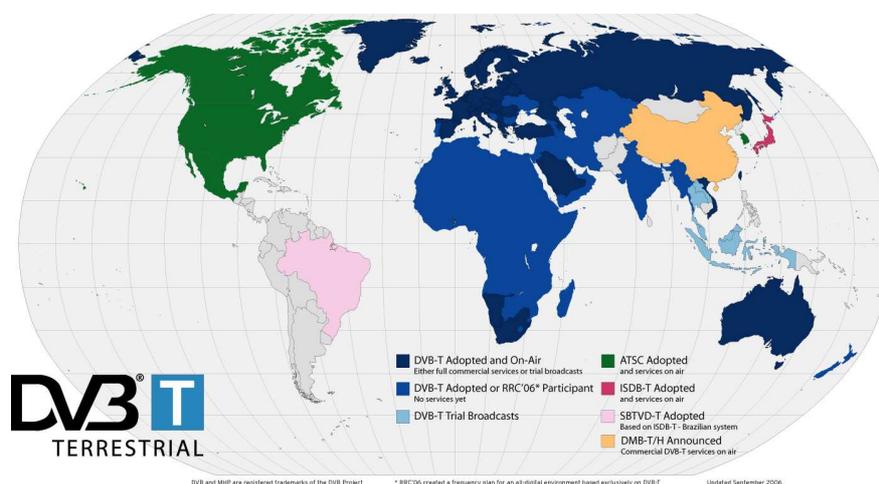


Figura 9.- DVB en el mundo

3.3.- PSI/SI

La Información de Servicio está formada por una serie de tablas de datos necesarias para que la trama digital cumpla las normativas vigentes. Esta información es necesaria para la correcta recepción de los transport streams por parte de los terminales.

Dichas tablas posibilitan la sintonización automática de los terminales, la localización de programas, la creación de la guía electrónica de programas, etc.

Existen dos tipos de tablas de Información de Servicio:

- **PSI (Program Specific Information)** definidas por MPEG-2 y relativas a un solo programa.
- **SI (Service Information)** definidas por DVB y que son relativas a un flujo de transporte.

3.3.1.- PSI (Program Specific Information)

Con la finalidad de facilitar el proceso de demultiplexación al decodificador, MPEG-2 Systems establece un método para la descripción de los contenidos de los Transport Streams. Dicho método se materializa en un conjunto de tablas conocido PSI (Program Specific Information). Las tablas PSI, suministran al decodificador información del sistema: parámetros de red, los programas que componen el TS, los ES que forman cada programa, la naturaleza de cada ES, mecanismos para identificar el contenido de cada paquete, parámetros de acceso condicional y otros.

Las tablas que componen la PSI son:

- **PAT (Program Association Table)** Correspondencia entre un programa y el PID de los PIDs de las PMT. Todos los TS deben incluir la tabla PAT.
- **PMT (Program Map Table)** Da un mapa de relaciones entre el programa y los componentes que lo forman. Es necesaria una identificación mínima de un programa: PID del PCR, tipo de streams y componentes de programa. Para añadir más información se utilizan descriptores.
- **CAT (Conditional Access Table)** Suministra la asociación entre uno o más sistemas de acceso condicional y los EMMs.

Además, existen una serie de elementos para incluir información adicional en la trama de datos:

- **Private sections.** Junto con las tablas PSI es posible transportar datos privados. El formato con que son transmitidos los datos dentro del transport stream no está definido para MPEG-2 System.
- **Descriptores.** Permiten introducir información adicional de forma estandarizada sobre el TS. Se envían en algunos bucles de las secciones PSI.

3.3.2.- DVB-SI (Service Information)

El DVB proporciona más información que la definida por las tablas MPEG-2. La DVB-SI informa sobre los servicios disponibles, los eventos de cada servicio, las descripciones textuales y técnicas de cualquier elemento, etc. Además, también puede incluir información sobre servicios y eventos de otros TS y otras redes. [9]

Las secciones DVB-SI, al igual que la Private Section, constan de campos fijos y diferentes bucles, donde se pueden incluir descriptores. Estos descriptores son estructuras sintácticas que permiten transmitir más información adicional. DVB define sus descriptores y en qué tablas pueden ser utilizados cada uno.

La sintaxis DVB-SI está muy relacionada a la PSI. Las tablas que componen la SI son:

- **NIT (Network Information Table)** Incluye identificadores de TS, frecuencias de canal, transpondedores, características de modulación, etc. Esta información quedará almacenada en la memoria no volátil de los receptores.
- **BAT (Bouquet Association Table)** Suministra información respecto a “bouquets” (selección de servicios), incluyendo una lista de los servicios que lo forman. Esta tabla es opcional.
- **SDT (Service Description Table)** Contiene datos que describen los servicios: nombres de servicios, el proveedor de servicios, etc. Los servicios pueden pertenecer a un mismo transport stream (actual) o ser una referencia a otros (other).
- **Event Information Table (EIT)** Contiene datos relativos a eventos o programas: nombre del evento, instante de inicio, la duración, etc. Los servicios pueden pertenecer a un mismo transport stream (actual) o ser una referencia a otros (other).
- **RST (Running Status Table)** Permite actualizar el estado de un evento cuando suceden cambios imprevistos en la programación.
- **TDT (Time and Date Table)** Suministra información de la hora y la fecha en la zona horaria de referencia .
- **TOT (Time Offset Table)** Suministra información relacionada con la hora y la fecha , y si es necesario, las diferencias horarias de algunas zonas respecto la zona de referencia.
- **ST (Stuffing Table)** Se utiliza para invalidar secciones existentes.
- **SIT (Selection Information Table)** Se utiliza únicamente en los bitstreams finitos (parciales) (por ejemplo almacenados o grabados). Transporta un sumario de la información SI necesaria para describir estas tramas.
- **DIT (Discontinuity Information Table)** Se utiliza únicamente en los bitstreams finitos. Se inserta cuando la SI de la trama puede ser discontinua.

Una trama de Transporte puede también llevar información de otras redes con las que comparta el área de cobertura. Esto posibilita que los receptores puedan cambiar de una red a otra sin necesidad de realizar una re-sintonización de canales. Las tablas propias se llaman “Actual” mientras que las de otras redes se denominan “Other”. A continuación se muestra un esquema que muestra las tablas obligatorias y optativas, actual y other, y quien las ha definido.

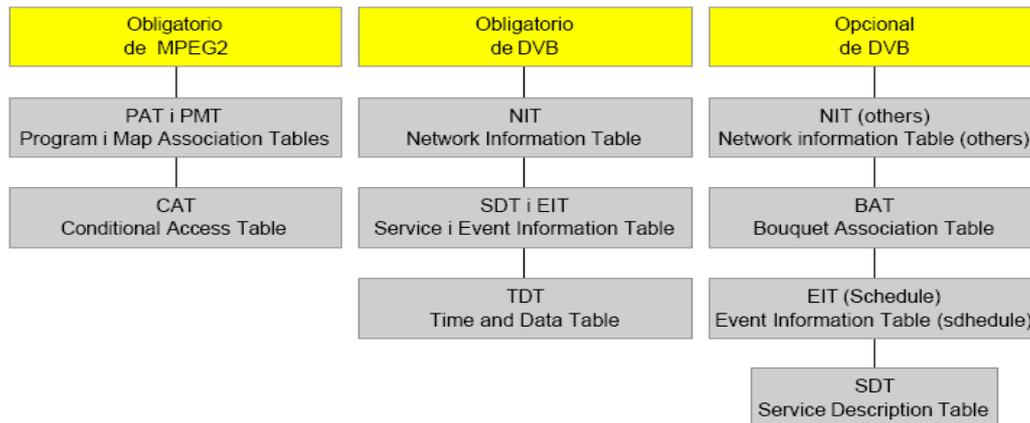


Figura 10.- Esquema de tablas PSI/SI

3.4.- Transport Stream

3.4.1.- Generación del transport stream

El Transport Stream (TS) soluciona los problemas críticos con respecto a la pérdida de un paquete, puesto que se limita la longitud de estos a 188 bytes, por lo cual está orientado a la radiodifusión de vídeo pese a que hace falta añadir todavía métodos de protección contra errores. Por otra lado, el Transport Stream multiplexa varios programas dentro de un mismo flujo binario de datos.

La multiplexación del transport stream consiste, como se ha dicho, en pequeños paquetes de longitud constante. Un paquete de transporte es siempre de 188 bytes, de los cuales 4 son de cabecera más un campo de adaptación opcional y 184 son de información (payload), tal y como se puede apreciar a la figura 11. Los paquetes PES se dividen entre los payloads de los paquetes de transportes.

El proceso de división de paquetes debe seguir dos premisas. Una es que el primer byte de cada paquete PES debe ser el primero del payload del paquete de transporte. La segunda premisa es que cada paquete de transporte sólo puede llevar información de un PES.

Es bastante probable que no haya un número entero de paquetes de transporte para

transportar todo el PES, con lo cual pueden quedar paquetes sin acabar de llenar. Para que se cumplan las premisas anteriores, existe un campo de adaptación que permite acabar de llenar el paquete. Son los denominados bits de relleno. Este uso se puede minimizar utilizando longitudes de paquetes PES grandes, puesto que así aseguramos una gran parte de los paquetes de transporte completamente llenos.

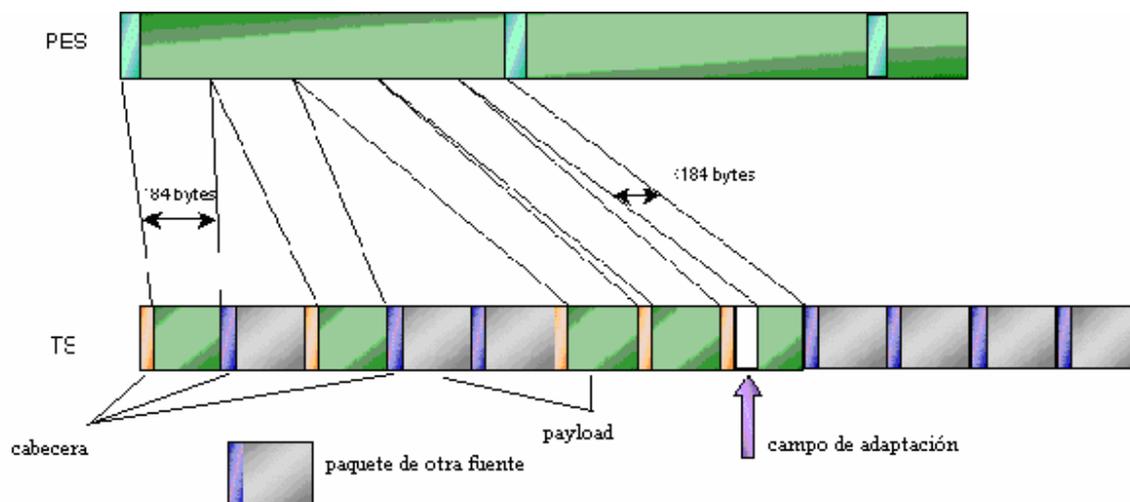


Figura 11.- Generación de un TS a partir de paquetes PES

Los paquetes que resultan de este proceso forman el Transport Stream. No se especifica el orden en que los paquetes de transporte llegan al multiplexor. Lo único que sí que se especifica es que los paquetes de un mismo PES han de enviarse secuencialmente.

3.4.2.- Componentes del transport stream

El esquema de la figura 12 muestra de qué campos se compone un paquete del transport stream e identifica la información que transportan los bits de cabecera:

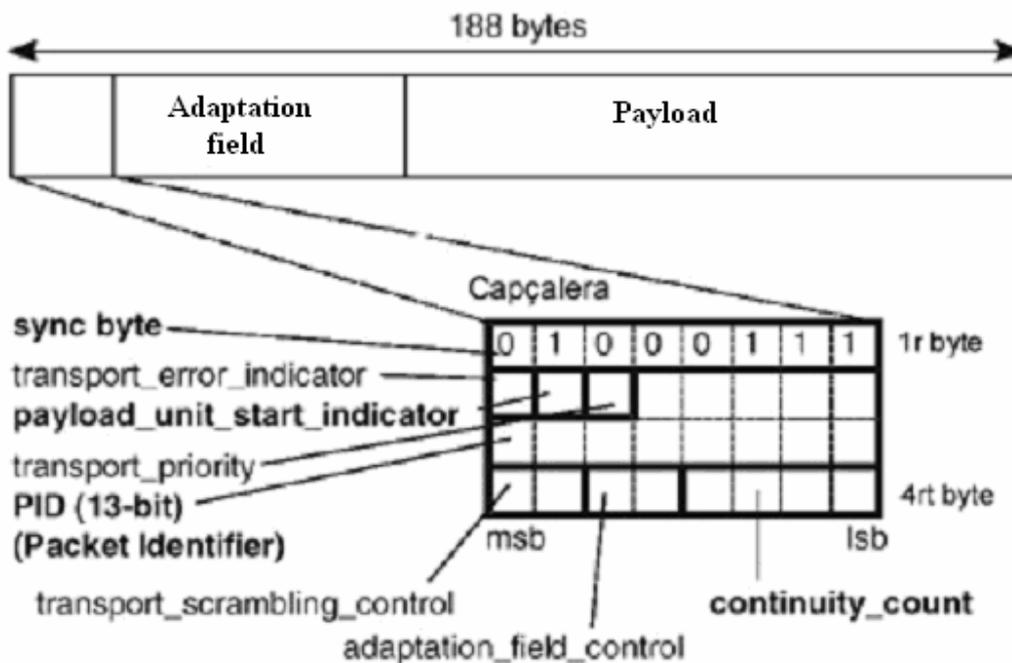


Figura 12.- Campos de un Transport Stream

El significado de los campos más importantes de los bits de cabecera es el siguiente:

- Byte de sincronismo.** Sirve para que el decodificador pueda sincronizarse correctamente con los datos entrantes. Tiene el valor 0x47 y delimita el inicio de un paquete TS. Además, al contrario de los paquetes PES, este valor de sincronización puede darse en cualquiera de los 187 bytes restantes. Esto se debe a que 188 bytes son pocos porque un decodificador pueda perderse a l' hora de regenerar los paquetes.
- Indicador de error de transmisión.** Este bit se pone activo cuando se detecta un error en la transmisión.
- Indicador de comienzo de payload.** Indica si en la cabecera del payload hay la de un PES.
- PID.** Como ya se ha mencionado, los paquetes de TS pueden transportar información de programas diferentes, además de datos para la reconstrucción de la información,

cada uno perteneciente a diferentes PES. Aparece un campo de 13 bits que se denomina PID (identificador de paquete) que permite distinguir paquetes de diferentes “elementary streams”. De los 2^{13} valores posibles, hay 17 reservados para funciones especiales. Esto permite 8175 valores que son asignables a todos los otros ES que forman el TS. El multiplexor debe garantizar que cada ES tenga un único PID. La normativa MPEG no especifica qué valores de PID se deben dar a los ES (a excepción de los 17 mencionados).

-Control de scrambling. Indica si hay o no datos encriptados en el payload.

-Control del campo d’adaptación. Indica si la cabecera tiene campo de adaptación.

-Contador de continuidad. El codificador lo incrementa en 1 cada vez que envía un paquete de la misma fuente. Esto permite que el decodificador sea capaz de deducir si ha habido una pérdida (o ganancia, incluso) de un paquete de transporte y evitar errores que no se podrían deducir de otra manera.

A continuación, se describen algunos de los campos existentes dentro de un campo de adaptación:

-Longitud del campo de adaptación. Indica la longitud de la cabecera extra.

-Indicador de discontinuidad. Se da en el PCR y en el contador de continuidad. Se usa por evitar pérdidas de información producidas por un salto en el codificador.

-PCR. Es la referencia del reloj del programa.

-Stuffing bytes. Son bytes de relleno para conseguir una trama de 188 bytes de información exactamente en el supuesto de que no hubiera información suficiente.

-Splice countdown. Indicador que permite una conmutación limpia entre un TS y otro TS.

3.5.- Entorno de desarrollo

Para la creación de la aplicación en este proyecto, así como para las pruebas realizadas posteriormente, ha sido necesario cierto equipamiento específico y un determinado software. En este apartado se describirá detalladamente cada uno de los elementos utilizados. Para ello, se han definido tres grandes subgrupos: software, equipamiento y medidas. Se ha intentado ordenar los componentes según el orden seguido para utilizarlos.

3.5.1.- Software

3.5.1.1.-Visual Studio

Después de valorar las diferentes tarjetas del mercado con entrada y salida ASI, finalmente se eligió una tarjeta ya conocida, Dektec DTU-140. Las APIS de dicha tarjeta estan hechas en C++. Por tanto la elección del software para el desarrollo de la aplicación vino determinado por esta característica. Visual Studio.net es una plataforma para la programación y compilación de componentes para aplicaciones, sitios webs o programas basados en C++.



Microsoft Visual Studio es un entorno de desarrollo integrado (IDE, por sus siglas en inglés) para sistemas Windows. Soporta varios lenguajes de programación tales como Visual C++, Visual C#, Visual J#, ASP.NET y Visual Basic .NET, aunque actualmente se han desarrollado las extensiones necesarias para muchos otros.

Visual Studio permite a los desarrolladores crear aplicaciones, sitios y aplicaciones web, así como servicios web en cualquier entorno que soporte la plataforma .NET (a partir de la versión 6). Así se pueden crear aplicaciones que se intercomunican entre estaciones de trabajo, páginas web y dispositivos móviles.

Otro de los criterios para la elección de dicho software es que permite desarrollar una interfaz gráfica de una forma sencilla gracias al módulo de c#.

Con la finalidad de poder trabajar con funcionalidades propias de la tarjeta Dektec, fue necesario incluir la librerías propias de la tarjeta DTA-140. También fue necesario instalar el paquete de librerías SDK para windows xp.

3.5.2.- Equipamiento

3.5.2.1.-Tarjeta Dektec DTA-140

Uno de los primeros pasos antes de comenzar a desarrollar la aplicación fue la elección de la tarjeta capturadora del transport stream. Esta elección se hizo entre los diferentes

proveedores de Abertis Telecom. Al final el proveedor seleccionado fue Dektec, y el modelo de tarjeta la DTA-140.

La decisión se tomo considerando varios aspectos. El principal fue que dicha tarjeta dispusiera tanto de entradas y salidas ASI. Otro punto importante fue la disponibilidad del hardware en el laboratorio de Abertis Telecom

En la figura 13 podemos ver físicamente dicha tarjeta:



Figura 13. - DTA-140

Features:

- High-speed DVB-ASI input and output, compliant to EN50083-9 and DVB document A010
- Parallel, independent operation of input and output channel at the full DVB-ASI bit-rate range from 0 to 214 Mbps.
- Adaptive cable equalisation
- Optional time stamp per packet arrival.
- 8-Mbytes input bbuffer for large jitter tolerance; independent 8 Mbytes output buffer
- Inverted DVB-ASI output for special tests
- Automatic recognition and adjustment of inverted DVB-ASI input signals

A continuación se muestra el diagrama de bloques de dicha tarjeta:

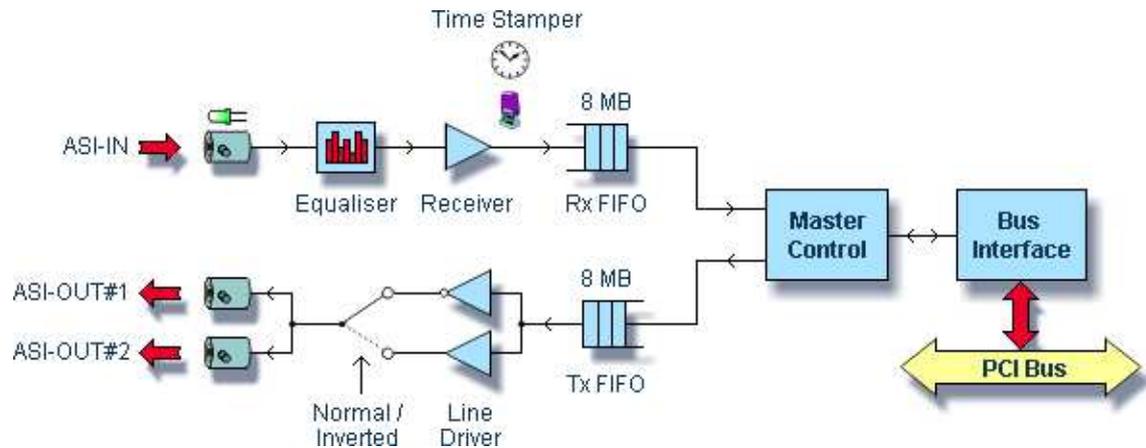


Figura 14.- Diagrama de bloques DTA-140

3.5.2.2.-Coders

Para poder realizar la codificación adecuada de los servicios se han utilizado los encoders Scientific Atlanta modelo 9032. La razón de su elección ha sido la experiencia con ellos y la disponibilidad en el laboratorio de varios de ellos.



Sus características principales son:

- Entrada SDI y PAL
- Salida ASI.
- Genera NIT y PAT
- Codificación MPEG2.
- Interfaz intuitiva web browser.

3.5.2.3.-Jade

Teóricamente, las pruebas de la aplicación no requerirían del uso de este equipamiento. Sin embargo, teniendo en cuenta que la aplicación podría tener un uso comercial, se ha querido simular un entorno real de difusión. Para ello, se ha introducido el equipo Jade, el cual se encarga de insertar la señalización de las tablas SI especificadas por DVB.

Al igual que Coral, Jade pertenecía inicialmente a la casa Thales, que ahora forma parte de Thomson-GrassValley.

Jade dispone de una tarjeta Passpro con entrada y salida ASI. La configuración para poder generar las tablas se obtiene a través de un fichero xml con un formato especial. El fichero puede recibirse por IP, o bien se puede generar a través de un editor que Jade incorpora. Dado que Jade, además de generar NIT y SDT, permite generar EIT present/following y Schedule, requiere de algún método de sincronización de tiempo. Es, por ello, que Jade permite crear las tablas en función de su reloj interno y generar la tabla TDT para que los eventos estén vinculados a esta.



En las pruebas llevadas a cabo en este proyecto, el papel de Jade ha sido generar las tablas NIT, SDT y EIT.

3.5.2.4.-Sodielec

Sodielec es un receptor profesional compatible con ETS 300 744.



Sus características principales son:

- Recepción y demodulación de señal DVB UHF y VHF .
- 2 Salidas ASI MPEG-2 TS.
- También permite analizar entrada externa ASI MPEG-2 TS.
- Configuración a través de web view.

Al igual que Jade, la utilización de este equipo no es necesaria obligatoriamente para el desarrollo de este proyecto, pero ante la posible integración de esta aplicación en un entorno real, se requiere este equipo para poder simular un entorno completo.

3.5.2.5.-Multiplexores

Para poder unir los diferentes transport streams generados por Coral, Jade y Sodielec, se hace necesario un multiplexor. Orientando los últimos tests a pruebas reales, se han chequeado 3 modelos de multiplexores diferentes, pues en etapas de la difusión de la TDT a nivel nacional se utiliza alguno de los tres modelos.

Todos ellos han sido utilizados para proporcionar un único transport stream al modulador. Sus funciones han sido:

- Generar la nueva PAT, con sus correspondientes PMT's.
- Ser transparente para las tablas NIT, SDT, EIT y TDT y para los parámetros de entrada ONID, TSID, y SID.

- Proporcionar una salida de 19.905.882 bps para poder ser adaptada a la entrada del modulador. Así se evita problemas de overflow.

3.5.2.6.1.-Amber



Amber es un multiplexor que inicialmente pertenecía a la casa Thales-BM. Ahora, al igual que Coral y Jade, forma parte de Thomson-GrassValley. Entre sus principales características destacamos:

- Remultiplexado de hasta 8 Transport Streams de entrada.
- Input/Output bitrates de hasta 50Mbps.
- Gestión de PSI/SI.
- Filtrado de PID's.
- Configuración a través de interfaz Ethernet.

3.5.2.6.2.-Scientific Atlanta D9600



Las principales características del multiplexor D9600 de Scientific Atlanta son:

- Remultiplexado de 4, 8, 12, 16 o 24 entradas en función del modelo.
- 2 Salidas.
- Bitrate de entrada desde 1 a 214 Mbps, bitrate salida desde 1 a 200Mbps.
- Gestión PSI/SI.
- Filtrados de PID's.
- Configuración a través de interfaz Ethernet.

3.5.2.6.3.-Thomson



Las principales características del multiplexor Thomson DBX 4300 son:

- Multiplexado de hasta 26 Transport Streams.
- Entradas: de 6 a 26.

- Salidas: hasta 4 con un bitrate máximo de 130 Mbps.
- Gestión PSI/SI.
- Filtrados de PID's.
- Configuración a través de software propietario.

3.5.3.- Medidas

Por último, para poder verificar la correcta configuración de cada uno de los equipos, se han realizado medidas a la entrada y salida de cada uno de ellos. En el mercado existen varios instrumentos de medidas. Por su facilidad de manejo y configuración se ha optado por un equipo de la casa Dektec: DTU-225.

El DTU-225 de Dektec tiene las siguientes características principales:

- Adaptador USB.
- Permite leer MPEG-2 Transport Streams.
- Permite también video SDI.
- Buffer local de 8 Megabytes.



Para poder usar el hardware, se requiere de un software específico también facilitado por Dektec: DTC-320 StreamXpert. También incorpora el software StreamSpres el cual permite la reproducción de transports stream pregrabados.

Mediante dicho software se permite:

- Análisis del transport Stream de entrada mostrando PID y bitrate de cada componente.
- Análisis de PSI/SI mostrando los descriptores de cada tabla.
- Gráfico del bitrate de entrada.
- Análisis de la ETR 290, generando ficheros logs si se configura de manera adecuada.
- Análisis detallado del PCR.
- Decodificación del servicio seleccionado para ver video en tiempo real.
- Grabación de Transport Streams con límite de capacidad o tiempo.

4.- Ejecución del proyecto

4.1.-Planificación

Este proyecto ha sido dividido en diferentes fases. La finalidad de esta división ha sido organizar la documentación obtenida y crear hitos suficientemente marcados, a lo largo de la evolución del mismo.

Las fases definidas son:

- Fase de estudio.
- Fase de especificación.
- Fase de desarrollo.
- Fase de pruebas.

A continuación se explicará con más detalle cada fase, así como los resultados obtenidos al final de cada una de ellas.

4.1.1.- Estudio

Antes de comenzar a trabajar en el proyecto, ha sido necesario adquirir conocimientos más profundos sobre la Televisión Digital Terrestre. Además se han tenido que aprender nuevos conceptos relacionados con el diseño de sistemas de acceso condicional, señalización y manejo de equipos.

A grandes rasgos, la fase de estudio, consta de una etapa de investigación en la que se ha tenido como principal objetivo el análisis de la situación actual y la adquisición de documentación técnica, tanto a nivel de estándares, hardware necesario, códigos y librerías, como de guías de usuario para poder trabajar con el equipamiento necesario.

La información técnica, proviene en su gran mayoría de documentación publicada por DVB y la ETSI. [9]. Además, para obtener un mayor conocimiento de la TDT a nivel de señalización y arquitectura, se han consultado estudios y documentos privados pertenecientes a Abertis Telecom. La documentación relacionada con la programación proviene, además de la red y de documentación interna, de un curso formativo realizado en La Salle. Por último, todas las guías de usuario para trabajar con los equipos han sido facilitadas directamente por sus fabricantes.

Al final de esta fase se pretendía tener un conocimiento amplio de la situación actual en diferentes ámbitos, del sistema de acceso condicional, del código c++ necesario para el diseño de la aplicación, de los elementos necesarios para montar un entorno de pruebas y de

su funcionamiento. Después de la búsqueda de información se establecieron unos objetivos concretos. La duración de esta fase ha sido de 3 meses.

En el apartado de bibliografía se detallan algunas de las referencias más útiles.

4.1.2.- Especificación de la solución

Este proyecto pretende diseñar una aplicación capaz de encriptar los streams de video y audio de un transport stream, para que pueda ser integrada en un entorno real, ya sea para dar un servicio de acceso condicional low cost o la distribución de la señal a los diferentes emplazamientos, para que desde allí pueda ser difundida. La aplicación debe de ser capaz tanto de encriptar la señal como desencriptarla. También tiene que ser una aplicación estable, es decir que no puede haber ningún tipo de fallo durante el funcionamiento la aplicación esta arrancada, ya que el servicio de televisión no puede fallar en ningún momento. Dichos requerimientos técnicos se traducen en dudas y éstas a su vez en componentes necesarios. Cada componente representa un pequeño problema de código que hay que resolver.

Esta fase se centra en la identificación de los componentes necesarios para la creación de la aplicación:

- Hardware.
- Software.
- Aplicación.

A nivel de hardware se ha utilizado la plataforma del laboratorio de pruebas de Abertis Telecom. En ella se encuentran los diferentes equipos que conforman una cabecera digital: coders, inyector de SI (Service information), multiplexor y modulador, analizadores y grabadores de TS (Transport streams), etc.

En cuanto al software, se han valorado diferentes entornos de desarrollo. Finalmente, debido a su popularidad y facilidad de uso, se ha optado por Visual Studio.

La elección de la tarjeta se baso en las especificaciones de la aplicación y se tuvo en cuenta la bolsa de proveedores de AbertisTelecom, así como su equipamiento dentro del laboratorio.

Para realizar las pruebas finales, se han tenido que definir diferentes arquitecturas de sistema. Cada una de ellas supone un avance respecto a su anterior. La idea de utilizar diferentes arquitecturas es probar la aplicación en los diferentes ámbitos, comenzando en el nivel más bajo. Las últimas pruebas requieren además de un conocimiento profundo sobre aplicaciones, conocimiento sobre cabeceras en TDT.

Esta fase pretende dar respuesta a la incógnitas de qué componentes usar en la aplicación, qué entorno de desarrollo es el más ideal o qué arquitectura usar para realizar las pruebas.

Para todas ellas, se ha requerido la información recopilada en la primera fase. Esta fase tenía una duración estimada de 2 meses.

4.1.3.- Desarrollo de la aplicación

Una vez superadas las fases 1 y 2, ya se disponía de todo lo necesario para comenzar con el desarrollo de la aplicación.

Durante el proceso de creación, se encontraron problemas añadidos que no se habían contemplado en las fases 1 y 2. Es por ello, que en algunos casos, se tuvo que profundizar más en la búsqueda de información, así como en el estudio de nuevas arquitecturas y componentes.

La aplicación consiguió adaptar perfectamente las necesidades establecidas en la fase 1. Para probar el funcionamiento de la aplicación a medida que se desarrollaba se utilizaron diversos métodos, la emulación virtual encriptando un archivo .ts fue la primera opción. De manera periódica se montaba una arquitectura de 2º nivel (véase apartado de arquitecturas), encriptando un transport stream generado localmente. El montaje de 3er nivel quedó para las pruebas de funcionalidad.

La finalidad de esta fase ha sido la creación de una aplicación partiendo desde cero. La duración de esta fase ha sido de 3 meses.

4.1.4.- Pruebas de funcionalidad

En vista que la aplicación diseñada puede tener un uso comercial, se ha creído conveniente realizar pruebas de funcionalidad sobre un entorno real de emisión. Para ello, ha sido necesaria una arquitectura de 3er nivel.

Previamente, se definieron diferentes paquetes de pruebas a realizar. Algunos están orientados meramente a la evaluación del rendimiento. Éstos verifican el desarrollo de la aplicación y contribuyen con la definición de posibles mejoras.

También existen paquetes de pruebas orientados a evaluar la calidad del servicio prestado. Estas pruebas toman medidas de tiempos de respuesta, optimización del pc, facilidad de manejo, etc.

Al finalizar todas las pruebas en laboratorio y estudiar los datos recogidos, se ha realizado una prueba piloto, con resultados satisfactorios, para demostrar el funcionamiento en un entorno real. La duración de esta fase ha sido de 2 meses.

4.2.- Arquitectura

A medida que se ha ido avanzando en el desarrollo, ha surgido la necesidad de trabajar con arquitecturas más complejas. En este punto se describen las cuatro arquitecturas usadas a lo largo del proyecto.

Inicialmente, el paso previo a cualquier arquitectura ha sido el diseño de la aplicación. Para ello ha sido necesario utilizar un PC, al que se le ha instalado el entorno de desarrollo Microsoft Visual Studio. Ha sido necesario, también la instalación de librerías especiales para poder programar con las APIS de la tarjeta. Como resultado de esta estructura se ha obtenido un código C++, que cumple con las especificaciones y requerimientos necesarios. A continuación se muestra un esquema de dicha estructura.

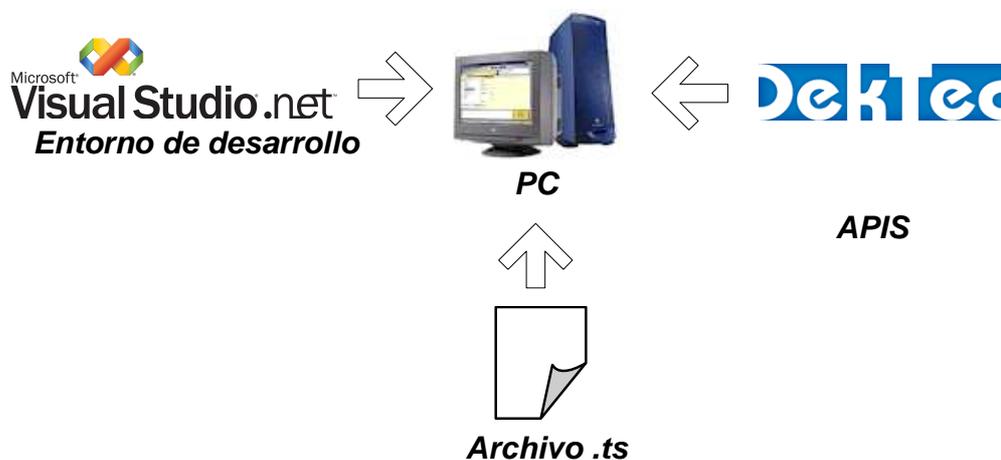


Figura 15.- Esquema básico inicial

Los siguientes pasos van enfocados a la prueba de la aplicación diseñada. De este modo se han verificado su correcto funcionamiento y se han determinado las prestaciones sobre un entorno real.

4.2.1.- Arquitectura 1: Emulación virtual

Para emular la aplicación en cualquier PC se ha grabado previamente un ts generado desde una cabecera local y obteniendo el resultado en consola. Así se ha podido comprobar que la lectura que realiza la aplicación de un transport stream es la correcta. En la figura 16 podemos observar de forma gráfica lo anteriormente explicado

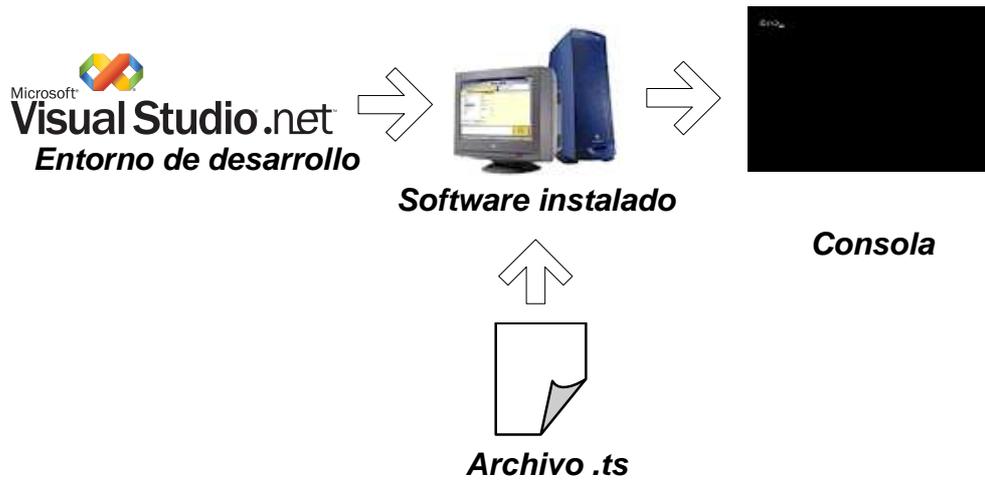


Figura 16.- Arquitectura 1

4.2.2.- Arquitectura 2: Emulación con cabecera local

El siguiente paso en la prueba de la aplicación, ha sido analizar la lectura de un transport stream en tiempo real, es decir utilizando la entrada ASI de la tarjeta Dektec. Esta fase se divide en tres subfases:

- 1) Lectura utilizando la entrada ASI y salida por consola
- 2) Lectura de un archivo .ts y resultado por la ASI de la tarjeta
- 3) Lectura y resultado por las entradas y salidas ASI de la tarjeta

Los esquemas de las figuras 17, 18, y 19 muestran las configuraciones para cada una de estas subfases.

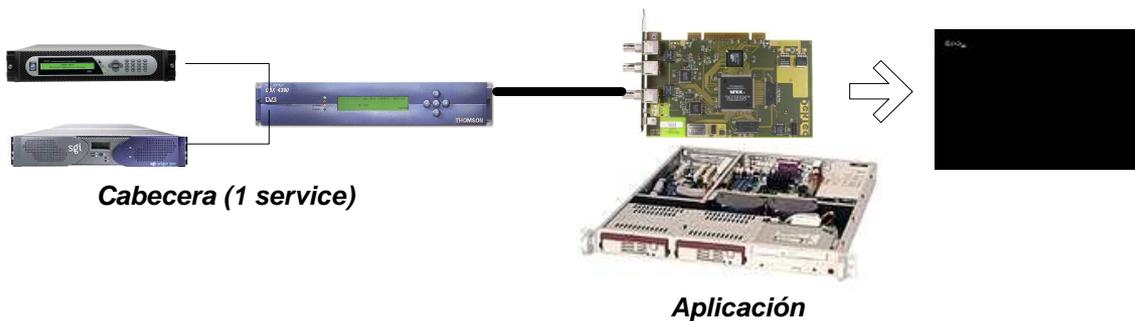


Figura 17.- Arquitectura 2. Subfase1

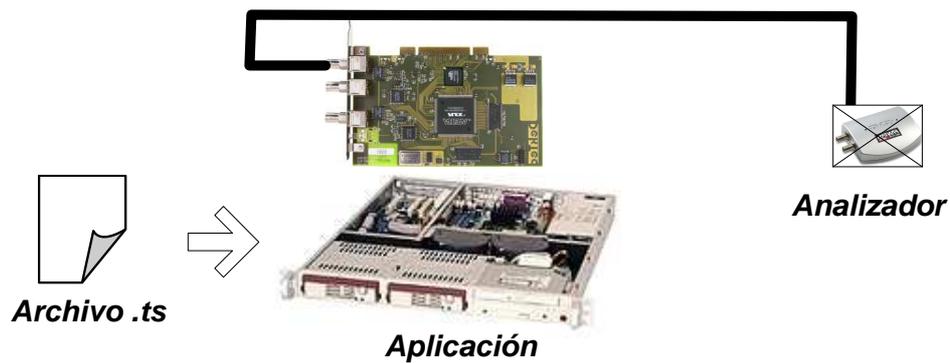


Figura 18.- Arquitectura 2. Subfase2

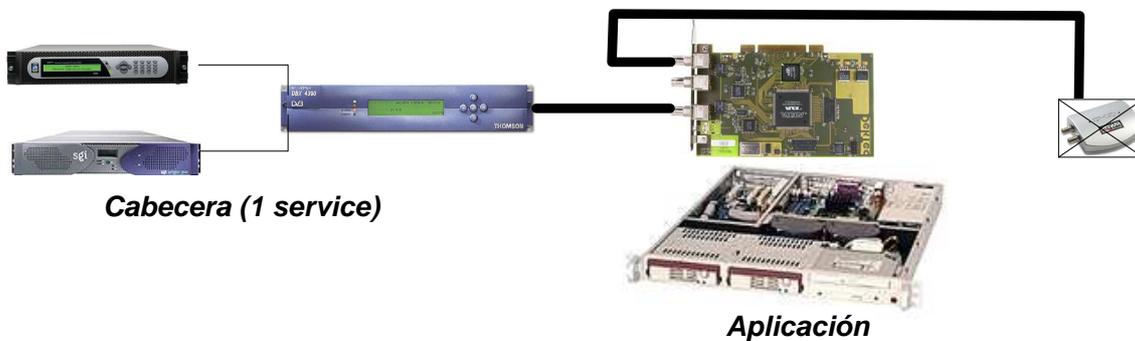


Figura 19.- Arquitectura 2. Subfase3

4.2.3.- Arquitectura 3: Sistema semi-completo

Ante la posibilidad de utilizar la aplicación en un entorno real, se planteó la opción de realizar las pruebas sobre un entorno más completo, incluyendo material utilizado en los despliegues de señal actuales. Para ello, se ha generado una cabecera localmente añadiendo 3 servicios más y también introduciendo en el transport stream canales de datos como pueden ser aplicaciones MHP, EIT's y un parámetro importante, la MIP. De esta manera se puede simular un canal de transmisión, tal como se muestra en la figura 20.



Figura 20.- Arquitectura 3

El insertador de MIP es un elemento muy importante a la hora de realizar las pruebas y validar la aplicación. La aplicación demultiplexa el transport stream y modifica los paquetes, por tanto produce un retardo. Este retardo estará dentro de los márgenes correctos sino no afecta a la MIP. De esta forma la aplicación se puede utilizar en redes SFN para contribución.

4.2.4.- Arquitectura 4: Sistema completo

Para completar las pruebas sobre un entorno real, se ha diseñado una arquitectura más completa donde el transport stream a encriptar es recogido del aire, es decir se ha utilizado un receptor de RF con salida ASI como se muestra en la figura 21. Esta última prueba es importante, ya que cada transport stream puede tener elementos diferenciales con otros transport stream. Por poner un ejemplo, en el mux 64 podemos ver que existe un canal denominado "canal de ingeniería" donde los fabricantes de receptores introducen firmwares nuevos para la actualización de sus receptores, en otros transports streams podemos ver un mismo servicio lleva diferentes audios. También existe un transport stream donde el vídeo está codificado en mpg4. Estos casos no suponen a priori, ningún inconveniente extra para la aplicación, sin embargo, dada la experiencia con varios equipos y softwares que interactúan con transports stream, se ha visto que suelen aparecer comportamientos poco esperados.

Por otra parte, también es importante destacar que a ciertas frecuencias los transports streams llevan una tabla denominada MIP. Esta tabla es la que introducen los insertadores de SFN, se utiliza para que los moduladores puedan trabajar en esta modalidad, de tal forma que si hay zonas de solape entre dos emplazamientos, el usuario final pueda visualizar los servicios de televisión y radio correctamente. Por tanto, es una tabla bastante delicada, y la aplicación de encriptación la tiene que dejar pasar de forma transparente, sin modificar ningún parámetro y sin ningún "delay" que pueda alterar el momento de transmisión de los moduladores.

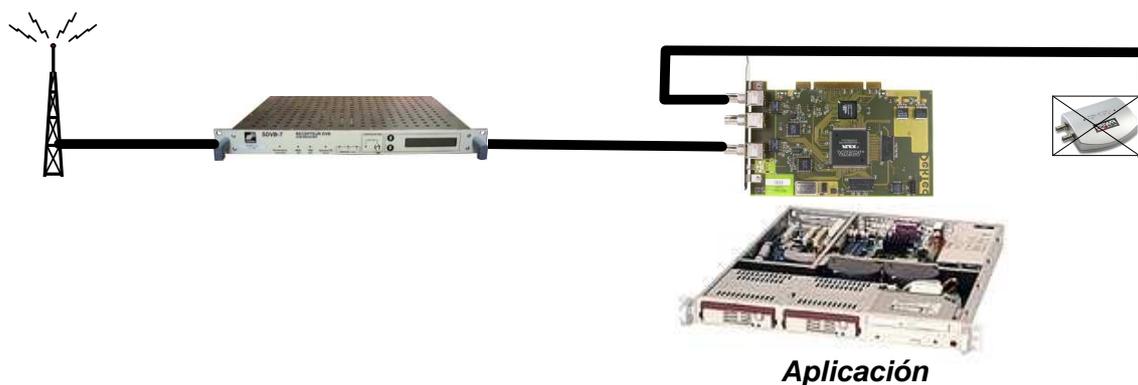


Figura 21.- Arquitectura 4

4.3.- Descripción de la aplicación

4.3.1.- Componentes

Antes de definir completamente el diseño de la aplicación, ha sido necesario analizar los componentes necesarios para obtener la funcionalidad deseada.

A continuación se detallan los requerimientos y los componentes y problemas que se derivan de cada uno de ellos:

Requerimiento	Componentes	Problemas
Diseñar aplicación	Código c++	
Recibir datos de manera sincronizada	Código para sincronizarse con la cabecera del transport stream	La tarjeta recoge 188 bytes cada vez
	Código para empezar a leer en el punto adecuado,	Método rápido y simple
Leer del transport stream	Código para leer el interior del transport stream	Hay que identificar cada componente del TS
Dejar pasar los SFN	Código óptimo, que no introduzca un retardo demasiado elevado	Al modificar los componentes del TS, la aplicación introduce un retardo

Figura 22.- Requerimientos, componentes y problemas

Obsérvese como en la columna de la derecha se muestran algunos de los problemas principales que se han encontrado en el diseño de cada componente.

En este apartado se detallan más ampliamente cada uno de los componentes y la solución adoptada. El título escogido para ofrecer la descripción de los problemas y soluciones, para

cada uno de los componentes, ha sido la pregunta lógica que uno se formula antes de introducirse en el código. De esta manera se ha intentado trazar una línea de pensamiento, para que cualquier persona ajena al estándar DVB pueda llegar a comprender el funcionamiento de la aplicación.

En el último apartado se ha incluido un gráfico global donde se unen todos los componentes y se muestra su flujo de funcionamiento.

4.3.2.- Estructura de la programación

Este apartado está enfocado a la metodología que se ha seguido para desarrollar la aplicación a nivel de código.

El código de la aplicación se ha basado en una estructura de clases. Una de las principales ventajas de trabajar con clases, aparte de la nitidez y claridad del código, es la reestructuración de la aplicación en cualquier momento del desarrollo sin que ello conlleve demasiado trabajo extra, es decir, añadir una nueva funcionalidad a la aplicación conlleva crear una nueva clase con esa función e introducirla en el código de una forma relativamente sencilla.

Otra de las ventajas de trabajar con clases es la facilidad para desarrollar la aplicación en sus diferentes fases, y por tanto avanzar de una forma segura sin arrastrar problemas anteriores.

4.3.3.- ¿Cómo sincronizar el transport stream?

Antes de empezar a programar la aplicación, una de las preguntas fue como sincronizar el transport stream, cómo saber dónde tiene su comienzo y su final. En apartados anteriores ya se ha comentado de qué constaba un transport stream, pero para poder trabajar con él hace falta una definición a nivel de byte. Para entender como realizar esta acción, fijémonos en la siguiente figura.

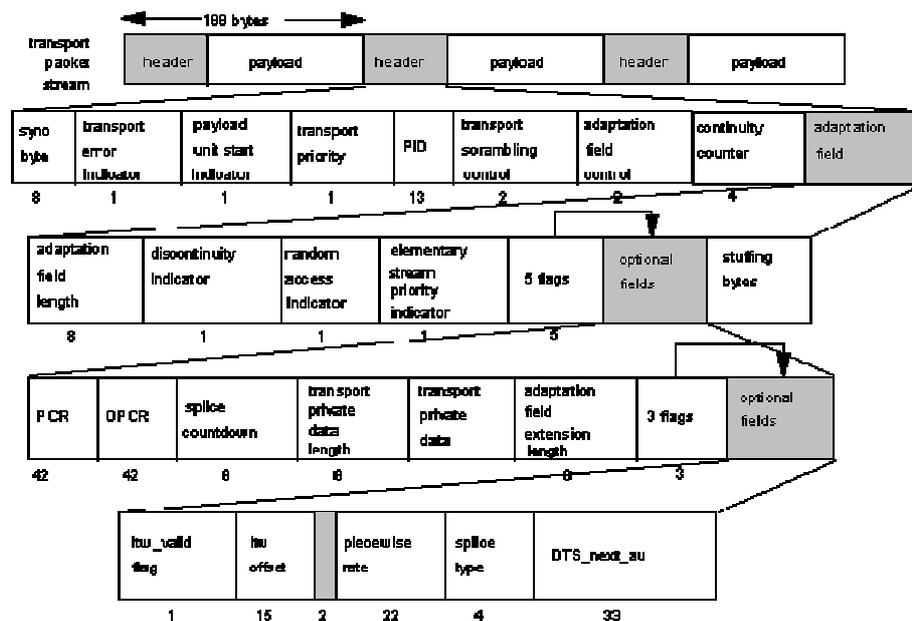


Figura 23.- Estructura de un transport stream

Vemos que el transport stream tiene 4 bytes de cabecera que siempre tienen el mismo valor, estos son los bytes que ayudarán a identificar el inicio del TS, a partir de aquí los bytes restantes pertenecen al payload, en total 188 bytes (ver figura 24). [11]

Sintaxis	Número de bits
transport_packet(){	
sync_byte	8
transport_error_indicator	1
payload_unit_start_indicator	1
transport_priority	1
PID	13
transport_scrambling_control	2
adaptation_field_control	2
continuity_counter	4
if(adaptation_field_control=='10' adaptation_field_control=='11'){	
Adaptation_field()	
}	
if(adaptation_field_control=='01' adaptation_field_control=='11'){	
For (i=0;i<N;i++){	
data_byte	8
}	
}	
}	

Figura 24.- Transport stream packet

4.3.3.1 Definición semántica de los campos de un Transport Stream packet

sync_byte Es el byte de sincronismo. Siempre tiene el mismo valor '01000111' (0x47). Este valor no se puede repetir en los otros campos del TS packet. El hecho de que cada 188 bytes se repita el sync_byte, facilita a los codificadores la identificación del inicio de los paquetes.

transport_error_indicator Es un flag de un bit. Cuando tiene un valor de '1', indica que como mínimo existe un bit erróneo incorregible en el TSp asociado. Este bit puede ser puesto a '1' por entidades externas a la capa de transporte. Cuando su valor es igual a '1', no puede ser puesto a '0' a menos que los bits erróneos hayan sido corregidos.

payload_unit_start_indicator Es un flag de un bit que solamente tiene el significado para los TSps que transporten PESps o datos PSI.

Cuando la carga útil del TSp contiene datos de un PESp, el indicador tiene el siguiente significado: un '1' indica que la carga útil de este TSp comenzará con el primer byte de un PESp, y un '0' indica que ningún PESp comenzará dentro de este TSp. Si el indicador vale '1', solamente un solo PESp puede comenzar en este TSp

Cuando la carga útil del TSp contiene datos PSI, el indicador tiene el siguiente significado: un '1' indica que el TSp transporta el primer byte de una sección PSI, y que el primer byte de la carga útil de este TSp es el pointer_field. Las secciones PSI no han de coincidir forzosamente con el inicio de la carga útil de los TSps, por eso el campo pointer_field se encargará de indicar donde se encuentra el inicio de la sección. Un '0' indica que el TSp no transporta el primer byte de una sección PSI y, por tanto, el campo pointer_field no está presente.

Para paquetes vacíos el indicador es '0'.

transport_priority Es un indicador de un bit. Cuando este vale '1' indica que el paquete asociado es prioritario contra el resto de paquetes que tienen el mismo PID pero que tienen el indicador a '0'. El mecanismo de transport puede usar este indicador para priorizar datos dentro de un ES. En función de la aplicación el campo transport_priority puede ser usado sin tener en cuenta el valor PID o solamente para un solo PID. Este campo puede ser modificado por codificadores específicos de canal.

PID (Packet Identifier) Es un campo de 13 bits. Se utiliza para distinguir los paquetes TS que transporten datos de un ES de aquellos que transportan datos de otros ESs. De los 2^{13} valores posibles, 17 están reservados. Esto significa que hay 8175 valores que pueden ser asignados a diferentes ES, y representan el máximo número de ESs que pueden estar en un solo Transport Stream. Es responsabilidad del distribuidor, asegurarse de que cada ES tiene

asignado un solo PID. MPEG no define qué valor ha de recibir cada ES, esto queda en manos del distribuidor.

Solamente los transport packets con PID de valores 0x0000, 0x0001, y 0x0010-0x1FFE pueden transportar el campo PCR.

Valor	Descripció
0x0000	Program Association Table
0x0001	Conditional Access Table
0x0002-0x000F	Reservat
0x00010 ... 0x1FFE	Pot ser assignat al network_PID, Program_map_PID, elementary_PID, o per altres propòsits.
0x1FFF	Paquets buits

Figura 25.- PID

Transport_scrambling_control: Este campo de 2 bits indica el modo de encriptación (scrambling mode) de la carga útil del TS_p. La cabecera del TS_p y el Adaptation field (cuando está presente) no se pueden encriptar ya que contienen parámetros que pueden ser leídos y modificados durante su transporte. En los paquetes sin carga útil, el transport_scrambling_control vale '00' (figura 26).

Valor	Descripció
00	No encriptat
01	Definit per l'usuari
10	Definit per l'usuari
11	Definit per l'usuari

Figura 26.- Transport_scrambling_control

adaptation_field_control: Este campo de 2 bits indica si la cabecera del TS_p va seguida del campo de adaptación y/o de la carga útil.

Valor	Descripció
00	Reservat per un ús futur, per la ISO/IEC
01	no adaptation_field, només payload
10	adaptation_field només, només payload
11	adaptation_field seguit per payload

Figura 27.- Valores del Adaptationfield

continuity_counter: Es un campo de 4 bits. Conceptualmente este campo toma el valor de un contador que está asociado al PID del TSp. Este contador se incrementa cada vez que se envía un TSp con este PID. Por tanto, cada TSp tiene un valor de continuity_counter incrementado en una unidad respecto el anterior TSp de igual PID.

El contador se resetea cada vez que llega a su máximo (15), y no se incrementa cuando el TSp no contiene carga útil (adaption_field_control vale '00' o '10')

Los paquetes duplicados tienen el mismo valor de continuity_counter que el paquete original.

En un Transport Stream, se definen los paquetes duplicados como aquellos en que cada byte es una copia del paquete original con la excepción del campo PCR, que si está presente, tiene el valor que le corresponde. Siempre han de contener carga útil, y tan solo pueden ser enviados consecutivamente dos TSps con el mismo PID.

El continuity_counter se considera continuo cuando este difiere en una unidad positiva respecto del contador del TSp anterior del mismo PID, o cuando se dan las condiciones de no incremento explicadas anteriormente (adaptation_field_control igual a '00' o '10', o paquetes duplicados).

El continuity_counter puede ser discontinuo cuando el valor del discontinuity_indicator vale '1'. En el caso de paquetes sin carga útil el valor del continuity_counter no esta definido.

data_byte: Los bytes de datos tienen que ser de datos continuos (en el mismo orden) pertenecientes a los PESps, en las secciones PSI, a bytes de relleno posteriores a las secciones PSI, o a datos privados dentro de ninguna de estas estructuras como se indica por su PID. En el caso de paquetes sin carga útil (PID igual a '0x!FFF'), los bytes de datos pueden ser cualquier. El número de bytes de datos se especifica por 184 menos el número de bytes del campo de adaptación. (ver sección 4.3.3.2)

4.3.3.2. Campo de adaptación (Adaptation field)

Sintaxi	Número de bits
Adaptation_field() {	
Adaptation_field_length	8
if(adaptation_field_length > 0) {	
Discontinuity_indicator	1
Random_access_indicator	1
Elementary_stream_priority_indicator	1

PCR_flag	1
OPCR_flag	1
Splicing_point_flag	1
Transport_private_data_flag	1
Adaptation_field_extension_flag	1
If(PCR_flag == '1') {	
program_clock_reference_base	33
Reserved	6
program_clock_reference_extension	9
}	
If(OPCR_flag == '1') {	
original_program_clock_reference_base	33
Reserved	6
original_program_clock_reference_extension	9
}	
If (splicing_point_flag == '1') {	
splice_countdown	8
}	
If(transport_private_data_flag == '1') {	
transport_private_data_length	8
for (i=0; i<transport_private_data_length;i++){	
private_data_byte	8
}	
}	
If (adaptation_field_extension_flag == '1') {	
adaptation_field_extension_length	8
ltw_flag	1
piecewise_rate_flag	1
seamless_splice_flag	1
reserved	5
if (ltw_flag == '1') {	
ltw_valid_flag	1
ltw_offset	15
}	
if (piecewise_rate_flag == '1') {	
reserved	2
piecewise_rate	22
}	
if (seamless_splice_flag == '1'){	
splice_type	4
DTS_next_AU[32..30]	3
marker_bit	1
DTS_next_AU[29..15]	15

marker_bit	1
DTS_next_AU[14..0]	15
marker_bit	1
}	
for (i=0;i<N;i++) {	
reserved	8
}	
}	
For (i=0;i<N;i++){	
stuffing_byte	8
}	
}	
}	

Figura 28.- Transport Stream adaptation field

4.3.4.- ¿Cómo leer datos?

Una vez ya se ha solucinado cómo sincronizarse con el transport stream, el siguiente paso es interpretar los diferentes datos y tablas que están en el TS. El primer paso de todos es leer la PAT (program asociation table). Esta es la tabla que asocia el service id de cada programa con el PID de la PMT.

4.3.4.1.- PAT

Como ya se ha explicado en el apartado de PSI/SI, la PAT es una tabla que introduce el estandar MPEG. Es única para cada transport stream. Una de las premisas de cualquier equipo que genere PAT, es que esta tiene que venir en el stream con PID 0. Este dato es muy importante si queremos demultiplexar el transport stream, ya que nos dirá la asociación entre el program number de cada servicio con el PID de su PMT. Esta última tabla será la encargada de asociarnos un servicio con todos sus componentes. Hablare más detalladamente de la PMT en el próximo apartado.

A continuación se muestra detalladamente todos los bits que componen la PAT.

Sintaxi	Número de bits
Program_association_section() {	
table_id	8
section_syntax_indicator	1
'0'	1
reserved	2
section_length	12
transport_stream_id	16
reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8
for (i=0; i<N;i++) {	
program_number	16
reserved	3
if(program_number == '0') {	
network_PID	13
}	
else {	
program_map_PID	13
}	
}	
CRC_32	32
}	

Figura 29.- Program association table

table_id: Es un campo de 8 bits, el valor del cual ha de ser '0x00'.

Section_syntax_indicator: Es un campo de 1 bit que ha de valer '1'.

Section_length: Es un campo de 12 bits. Los dos primeros bits han de valer '0'. Los 10 bits restantes especifican el número de bytes de la sección a partir de este campo, incluyendo el CRC. Este campo no puede exceder el valor 1021(0x3FD).

Transport_stream_id: Es un campo de 16 bits que sirven como etiqueta para identificar este TS de cualquier otro multiplexado dentro de una red. Su valor es definido por el usuario,

Version_number: Es un campo de 5 bits, el valor del cual es la versión de toda la PAT. El `version_number` ha de incrementarse en una unidad siempre que la información de la PAT cambie. Cuando el `current_next_indicator` vale '1', el `version_number` ha de ser aquel que pertenece a la versión de la PAT actualmente aplicable. Cuando el `current_nert_indicator` vale '0' el `version_number` ha de ser aquel que corresponda a la próxima versión de la PAT aplicable.

Current_next_indicator: Es un indicador de 1 bit. Si vale '1' indica que la PAT enviada es aplicable actualmente. Cuando vale '0', indica que la tabla enviada aún no es aplicable y ha de ser la próxima tabla en pasar válida.

Section_number: Es un campo de 8 bits, el valor del cual es el número de esta sección. El section_number de la primera sección de la PAT ha de ser '0x00'. Y ha de incrementarse en una unidad para cada sección adicional de la PAT.

Last_section_number: Es un campo de 8 bits, el valor el cual indica el número de la última sección de toda la PAT.

Program_number: Es un campo de 16 bits. Especifica el programa al cual es aplicable el program_map_PID. Permite la definición de hasta 65535 programas en un TS, ya que el valor '0x0000' esta reservado a la tabla NIT y por tanto el siguiente PID ha de ser el network_PID, en todos los otros casos el valor de este campo se define por el usuario. No puede adquirir el mismo valor más de una vez dentro de una misma versión de la PAT.

Nota: El program_number puede ser usado para designar un canal de difusión (broadcast), por ejemplo.

Network_PID: Es un campo de 13 bits que solamente es usado cuando el valor del program_number val '0x0000'. Especifica el PID de los TS que contienen la NIT. El valor del network_PID es definido por el usuario, pero solamente puede adquirir unos valores determinados.

Program_map_PID: (PMT_PID) Es un campo de 13 bits que especifica el PID de los TP que contienen la program_map_section aplicable al programa especificado por el program_number. Ningún program_number puede tener más de un program_map_PID asignado. El valor del program_map_PID se define por el usuario, pero solo puede adquirir unos valores determinados.

CRC_32: Es un campo de 32 bits que cuenta el valor de CRC que se aplica a la totalidad de la program_association_section.

Dependiendo de los servicios que haya en el transport stream, la PAT contendrá más o menos bits. A la hora de programar la lectura de la PAT será importante tener en cuenta este aspecto y ser prudentes con estos aspectos, ya que la aplicación tiene que servir para cualquier transport stream, es decir, puede contener uno o varios servicios.

A continuación se muestra una pequeña parte del código utilizado en la lectura de la PAT

```
class PAT : public TableSection
{
    int Nprog,rate;//nuevo atributo rate
    Pair pairs[1024];

public:
    void initiate();
    void toString();
    int getStuffingBytes();
    int getServId(int i){return pairs[i].getP();}
    int getTablePid(int i){return pairs[i].getPid();}
    int getNprog(){return Nprog;}
    void procRate(){rate++;}
```

```

PAT(void){};
~PAT(void);
PAT(char d[1024]):TableSectio(d){
    Nprog= (sl-2-1-1-1-4)/4;
    for(int i=0;i<Nprog;i++){
        int p,ppid;
        p= (section[i*4]<<8) / section[i*4+1]&0xff;
        ppid= (((section[i*4+2] & 0x1f) <<8) / (section[i*4+3]&0xff));
        pairs[i]=Pair(p,ppid);
    }
    rate=1;
}
};

void PAT::toString(){

    printf("--PAT Rx=%i----- \n",rate);
    printf("TableId: 0x%x\nTStreamId: 0x%x\nVersionNumber: %i\n",tid,tsid,vn);
    printf("Número de Programas: %i\n",Nprog);
    for(int i=0;i<Nprog;i++){
        printf("Programa=%i PID=0x%x\n", pairs[i].getP(), pairs[i].getPid());
    }
    printf("----- \n");
}

void PAT::initiate(){
}

int PAT::getStuffingBytes(){
    return 1;
}

PAT::~PAT(void)
{
}

```

Es importante recalcar el parámetro VersionNumber que es quien nos marca si la PAT sufre algún tipo de modificación y, por tanto, si se tendrá que realizar otra lectura de ésta. Se comprueba, tal como se ha indicado anteriormente, como la arquitectura de la aplicación es una arquitectura de clases como he explicado anteriormente. Una de las clases principales es la PAT.

4.3.4.2.- PMT

La tabla PMT la define también el estandar MPEG-2. El multiplexor regenera esta tabla para asociar los diversos componentes (audio, video, MHP, etc,) a cada servicio.

A continuación podemos ver los diferentes campos que encontramos en la PMT

Sintaxi	Número de bits
TS_program_map_section() {	
table_id	8
section_syntax_indicator	1
'0'	1
Reserved	2
section_length	12
program_number	16
Reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8
Reserved	3
PCR_PID	13
Reserved	4
program_info_length	12
for (i=0; i<N; i++) {	
descriptor()	
}	
for (i=0; i<N1; i++) {	
stream_type	8
Reserved	3
elementary_PID	13
Reserved	4
ES_info_length	12
for (i=0; i<N2; i++) {	
descriptor()	
}	
}	
CRC_32	32
}	

Figura 30.- Program map tables

Program_number: Es un campo de 16 bits. Especifica el programa al cual es aplicable el program_map_PID. Una descripción de programa ha de ser transportada dentro de una sola TS_program_map_section. Esto implica que una definición de programa nunca será de una longitud superior a 1016(0x3F8) bytes.

Section_number El valor de este campo de 8 bits ha de ser '0x00'

Last_section_number El valor de este campo de 8 bits ha de ser de '0x00'. Este campo de 8 bits ha de ser '0x00'.

PCR_PID Es un campo de 13 bits que indica el PID de los TS que contienen los campos PCR validos del programa especificado en el program_number.

Stream_type Es un campo de 8 bits que especifica el tipo de elemento de programa transportado por los paquetes con el mismo PID que especifica el elementary_PID. Los valores del stream_type son especificados en la siguiente tabla.

Valor	Descripción
0x00	ITU-T ISO/IEC Reserved
0x01	ISO/IEC 11172 Video
0x02	ITU-T Rec. H.262 ISO/IEC 13818-2 Video or ISO/IEC 11172-2 constrained parameter video stream
0x03	ISO/IEC 11172 Audio
0x04	ISO/IEC 13818-3 Audio
0x05	ITU-T Rec. H.222.0 ISO/IEC 13818-1 private_sections
0x06	ITU-T Rec. H.222.0 ISO/IEC 13818-1 PES packets containing private data
0x07	ISO/IEC 13522 MHEG
0x08	ITU-T Rec. H.222.0 ISO/IEC 13818-1 Annex A DSM CC
0x09	ITU-T Rec. H.222.1
0x0A	ISO/IEC 13818-6 type A
0x0B	ISO/IEC 13818-6 type B
0x0C	ISO/IEC 13818-6 type C
0x0D	ISO/IEC 13818-6 type D
0x0E	ISO/IEC 13818-1 auxiliary
0x0F-0x7F	ITU-T Rec. H.222.0 ISO/IEC 13818-1 Reserved
0x80-0xFF	User Private

Figura 31.- Stream type assignments

Elementary_PID Es un campo de 13 bits que especifica el PID de los TS que transportan el elemento de programa asociado.

ES_info_length Es un campo de 12 bits, los primeros 2 bits han de ser '00'. Los 10 bits restantes especifican el número de los descriptores, asociados al elemento de programa, que comienzan inmediatamente después del campo ES_info_length.

Una vez reconocida la PMT del programa correspondiente hay que analizar dicha tabla, el dato más significativo que se lee de dicha tabla es el PID del stream type 2 y 3, correspondientes.

A continuación podemos ver la parte del código que define la clase de PMT

```
class PMT : public TableSection
{
    int PCRpid,pil,Nstream,servId;
    PMTElement* elements[1024];
    Descriptor* piDesc[1024];
}
```

public:

```

    PMTElement* getElement(int j){return elements[j];}

    int getNstream(){return Nstream;}

    PMT(void);
    ~PMT(void);
    PMT(char s[1024]):TableSection(s){
        servId=tsid;
        PCRpid=((section[0]&0x1f)<<8)/(section[1]&0xff);
        pil=((section[2]&0xf)<<8)/(section[3]&0xff);
        int i=4;
        for(int j=0;i<pil+4;j++){
            piDesc[j]=new Descriptor(&section[i]);
            i=i+2+piDesc[j]->getLen();
        }
        int left=sl-i-4-3;
        for(Nstream=0;i<left;Nstream++){
            elements[Nstream]=new PMTElement(&section[i]);
            i=i+elements[Nstream]->getElemLen();
        }
    }
};

```

4.3.5.- ¿Cómo encriptar el stream correspondiente?

Una vez se han diseñado las dos clases para leer la PAT ya la PMT ya disponemos de suficiente información para poder aplicar la clase encriptación y realizar el tratamiento deseado sobre el TS.

Una vez apliquemos la clase PMT sobre el transport stream, se obtiene la información de cada servicio. Y a partir de aquí se puede aplicar la encriptación solamente sobre los paquetes deseados.

Dependiendo de qué encriptación se puede realizar sobre el transport stream, se elige un tipo de paquete u otro. Normalmente se realiza la aplicación sobre el vídeo y audio de cada servicio. El stream type correspondiente al video es el 2 y el del audio el 3. En la figura siguiente se muestra ver un ejemplo de un paquete del transport stream y donde se identifican el stream_type=2, por tanto el correspondiente al video.

reserved	2	0x3[3]	shall be set to 11
version_number	5	0x15[21]	
current_next_indicator	1	0x1[1]	The table sent is currently applicable
section_number	8	0x0[0]	
last_section_number	8	0x0[0]	
reserved	3	0x7[7]	
PCR_PID	13	0x5DD[1501]	
reserved	4	0xF[15]	
program_info_length	12	0x0[0]	
Elementary Stream			
ES [PID 0x05DD, TYPE 02]			
stream_type	8	0x2[2]	ITU-T Rec. H.262 ISO/IEC 13818-2 Video
reserved	3		
elementary_PID	13	0x5DD[1501]	
reserved	4		
ES_info_length	12	0x3[3]	
descriptor			
ES [PID 0x05DE, TYPE 06]			

Figura 32.- Ejemplo Stream_type

A continuación se presenta la clase que define la encriptación.

```
class ENCRIP : public TS
{
    int Nprog,rate;//nuevo atributo rate
    Pair pairs[1024];

public:
    void initiate();
    void toString();
    int getStuffingBytes();
    int getNprog(){return Nprog;}
    int getStreamType();
    void procRate(){rate++;}
    Encrip(void){};
    ~Encrip(void);
    Encrip(char d[1024]):TableSectio(d){
        if Nprog= d;
        {
            for(int i=0;i<188;i++){
                int p,ppid;
                p= (section[i*4]<<8) | section[i*4+1]&0xff;
                ppid= (((section[i*4+2] & 0x1f) <<8) | (section[i*4+3]&0xff));
                pairs[i]=Pair(p,ppid);
            }
        }
        rate=1;
    }
};
```

4.3.6.- Rutina

Con la finalidad de tener una visión más global y clara del funcionamiento de la aplicación, se han creado unos diagramas de flujo, donde se puede ver el funcionamiento de la aplicación y el papel desarrollado por cada una de las componentes explicadas.

En el gráfico siguiente se ve de forma resumida cómo funciona la aplicación internamente para realizar la función de encriptado correctamente, es decir, dejando pasar de forma totalmente transparente los ES no correspondientes al vídeo y al audio, y encriptando los que llevan la información de vídeo y audio.

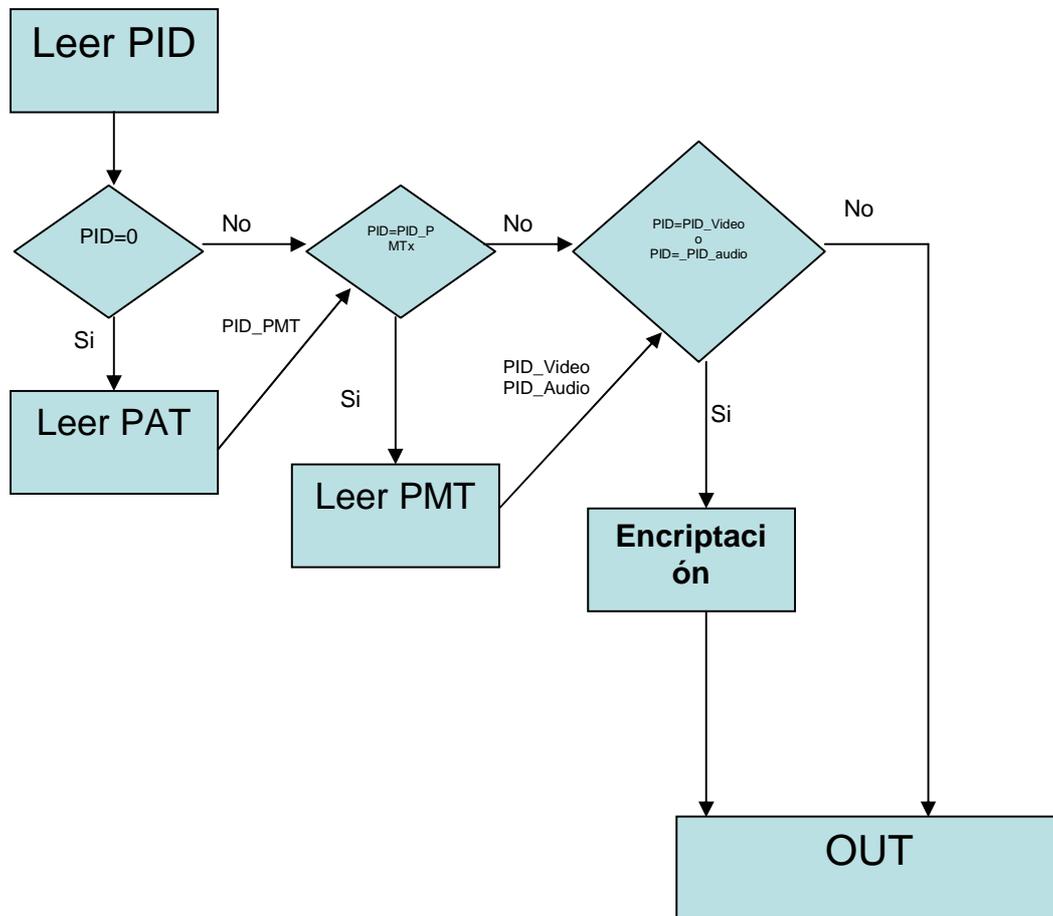


Figura 33. - Diagrama de flujo 1

Hay que tener en cuenta que la tarjeta DTA-140 funciona con filosofía FIFO, por tanto el paquete que entra primero es el primero que sale. Es decir de esta forma se mantiene el orden con que esta formado el transports stream y por tanto no varía el bitrate de entrada a la salida.

De todas formas, este es el diagrama de flujo para la aplicación funcionando con un transport stream el cual solamente lleva un servicio de TV. Posteriormente se han realizado modificaciones en la aplicación para poder realizar la misma función pero con transports streams los cuales llevan más de un servicio de TV. Esta sería la solución elegida para poder realizar un acceso condicional se uno o varios servicios en concreto. En la figura 34 podemos ver de una forma gráfica el diagrama de flujo.

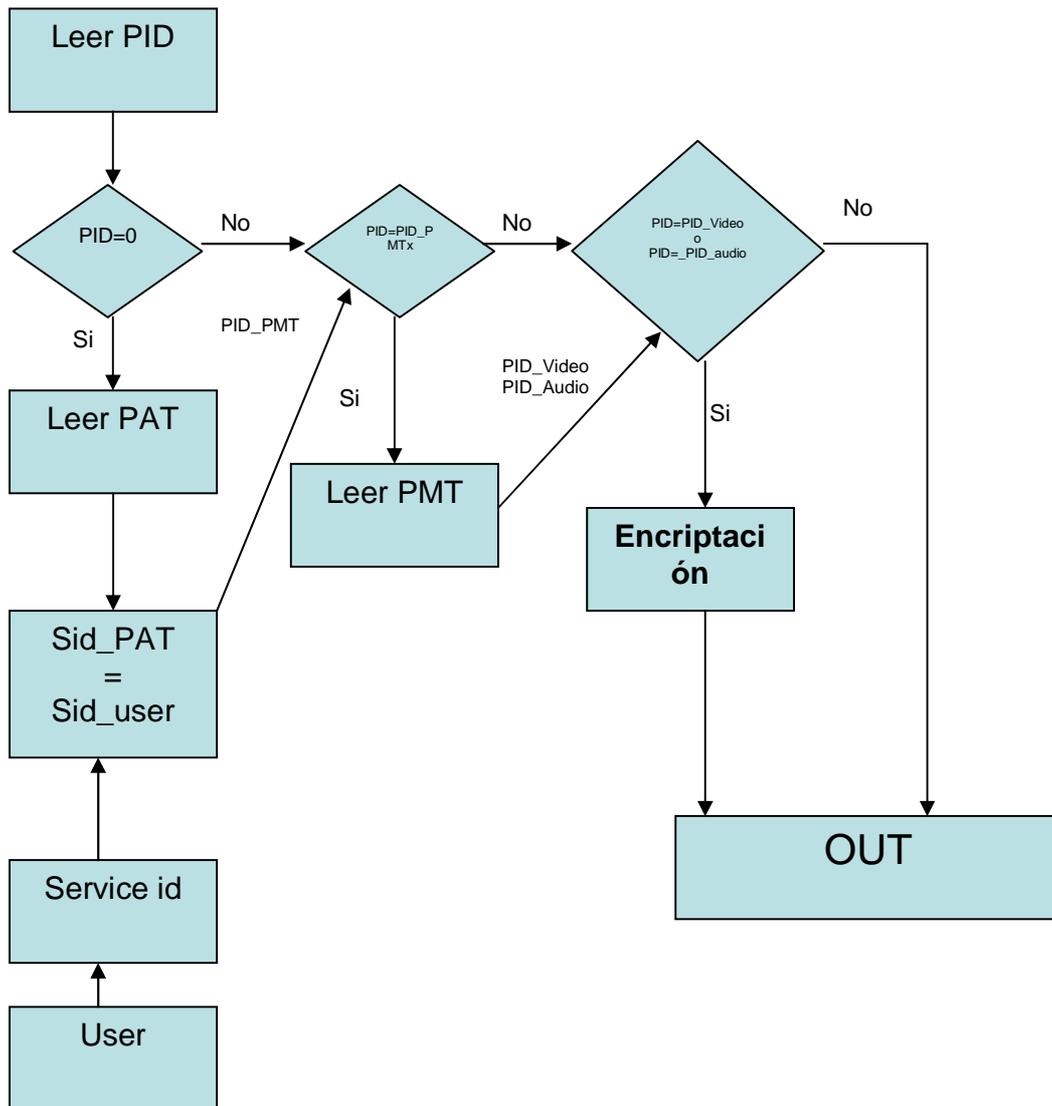


Figura 34.- Diagrama de flujo 1

5.- Resultados

El apartado de resultados se divide en dos partes:

- **Funcionamiento:** Se analiza el funcionamiento de la aplicación de forma global.
- **Limitaciones técnicas:** Se detallan las limitaciones técnicas que hay que tener en cuenta para un correcto funcionamiento de la aplicación.

5.1.- Funcionamiento

5.1.2.- Uso global

La aplicación es relativamente sencilla de manejar. Corre sobre un server, el cual está ubicado en la cabecera como podemos ver en la siguiente figura.

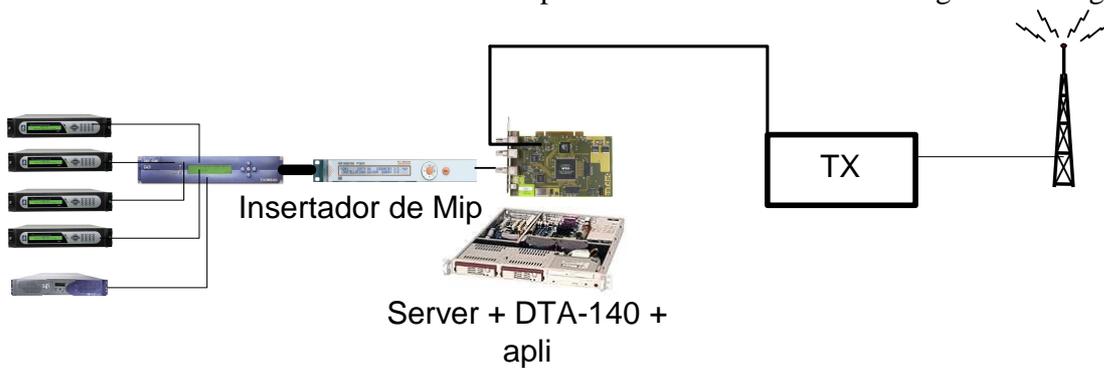


Figura 35.- Estructura de funcionamiento

En recepción el esquema sería parecido al que se indica en la figura 36 si utilizamos la aplicación para un entorno de contribución:

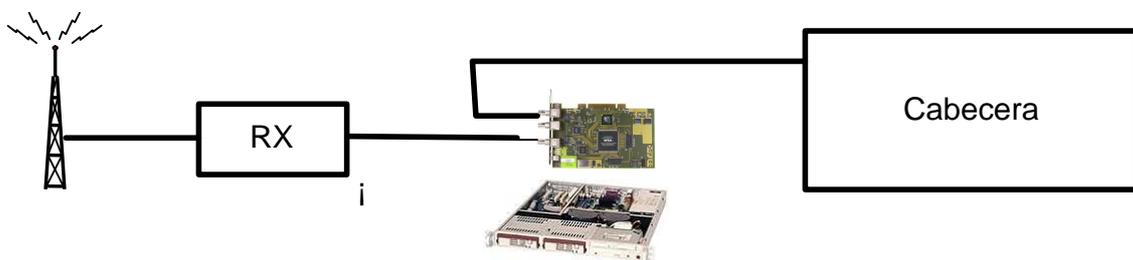


Figura 36.- Estructura de funcionamiento

Este server se puede controlar vía vnc (escritorio remoto). La aplicación se lanza desde una sencilla interfaz gráfica, donde desde allí aparecen cinco opciones a elegir. Por comodidad se ha integrado tanto el software de encriptación como el de desencriptación. Por tanto, la aplicación a instalar tanto en la parte transmisora como en recepción es la misma.

En la siguiente figura podemos ver las diferentes opciones a elegir cuando se lanza la aplicación:

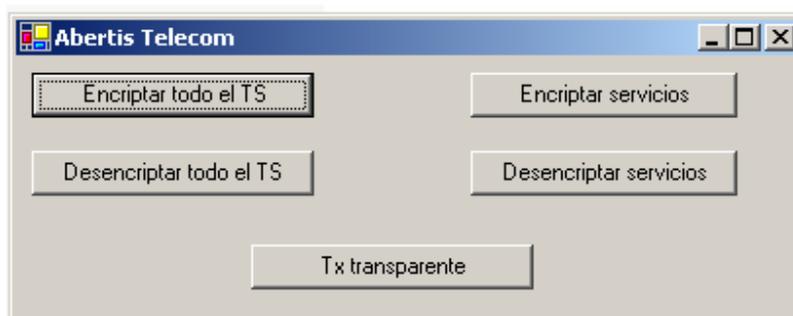


Figura 37.- Estructura de funcionamiento

Encriptar todo el TS: El transport stream saliente se encripta completamente (exceptuando los bits de cabecera) con el algoritmo definido. Esta sería la opción elegida cuando se utilice la aplicación para contribución de señales TDT.

Desencriptar todo el TS: Cuando en transmisión se utiliza la primera opción, se ejecuta esta opción para recuperar íntegramente el transport stream.

Encriptar servicios: Esta es la opción elegida cuando se quiere que solamente se haga una encriptación del video y del audio. El código está diseñado para la encriptación de estos dos stream en todos los servicios del transport stream.

Desencriptar servicios: Idem que la opción dos, pero con la particularidad de que solamente desencriptará el video y el audio de los servicios.

Tx Transparente: Cuando se elige esta opción, el transport stream saliente es el mismo que el entrante. Se ha desarrollado esta funcionalidad con el motivo principal de ayuda a la corrección de problemas si por alguna razón desconocida surgieran.

A continuación se hace un análisis de algunos ejemplos de transports stream salientes, dependiendo de si estamos en el primer caso o en el segundo.

En la figura 38 se puede observar la encriptación del vídeo y audio de dos servicios. La aplicación de análisis es capaz de detectar que son streams de vídeo y audio gracias a que la PMT le informa que PID del servicio en concreto son los pertenecientes al vídeo y al audio, pero si analizamos directamente los streams de vídeo y audio simplemente la aplicación no sería capaz de definir qué tipo de stream es, ya que al estar encriptado los bits de estos streams están aparentemente sin orden alguno.

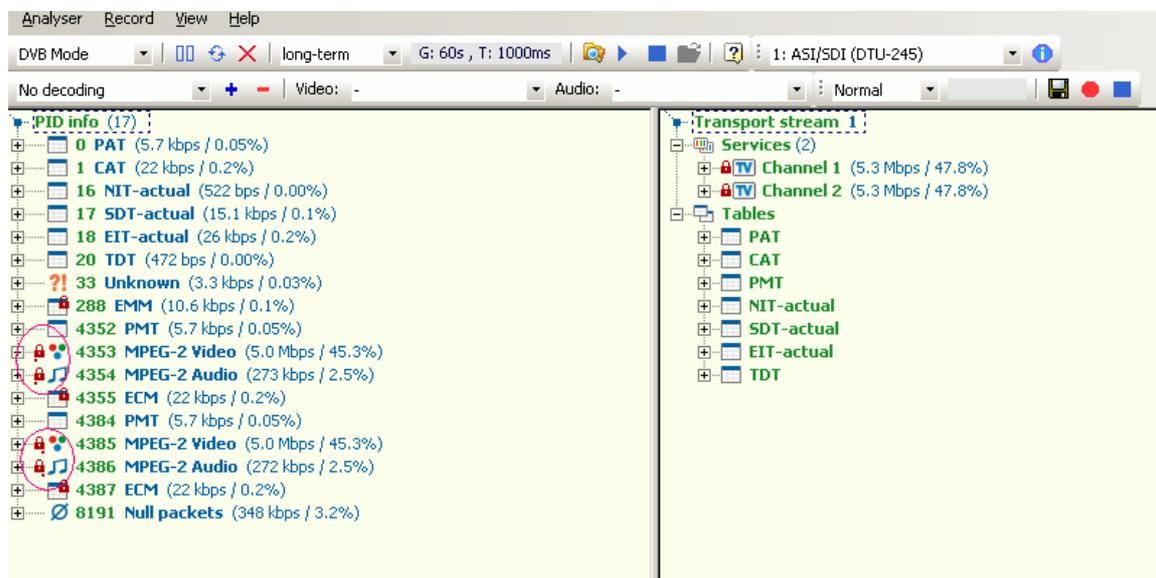


Figura 38.- Ej TS con servicios encriptados

En la figura 39 se observa, el análisis de un transport stream el cual está totalmente encriptado, exceptuando, evidentemente, los bits de la cabecera, ya que sino no se podría definir el sincronismo en la aplicación receptora, y ésta no sabría definir el principio y el final de los paquetes de 188 bytes. Se puede comprobar que aparentemente si sale definida la PAT, pero es puramente casualidad, ya que si coincide un valor de 0x00 en el lugar correspondiente donde se situaría el PID, las aplicaciones trabajando en modo DVB lo entienden como el PID correspondiente a la PAT y así lo señalizan.



+	Icon	PID	Service	Data Rate
+	Document	0	PAT	(0 bps / 0.0)
+	Document	1	CAT	(0 bps / 0.0)
+	Unknown	17	Unknown	(0 b)
+	Unknown	18	Unknown	(0 b)
+	Person	288	EMM	(0 bps /
+	Unknown	4352	Unknown	(
+	Lock	4353	Unknown	(
+	Lock	4354	Unknown	(
+	Unknown	4355	Unknown	(
+	Unknown	4384	Unknown	(
+	Lock	4385	Unknown	(
+	Lock	4386	Unknown	(
+	Unknown	4387	Unknown	(
+	Unknown	4608	Unknown	(
+	Lock	4609	Unknown	(
+	Lock	4610	Unknown	(
+	Unknown	4611	Unknown	(
+	Unknown	4640	Unknown	(
+	Lock	4641	Unknown	(
+	Lock	4642	Unknown	(
+	Unknown	4643	Unknown	(
+	Null	8191	Null packet	

Figura 39.- Ej TS encryptado totalmente

En la figura siguiente podemos ver el análisis de un stream de video no encryptado. Como se puede comprobar se puede realizar una extracción frame a frame de su contenido y obtener toda la información referente a este video, tal como la resolución, bit rate, aspect ratio, etc..

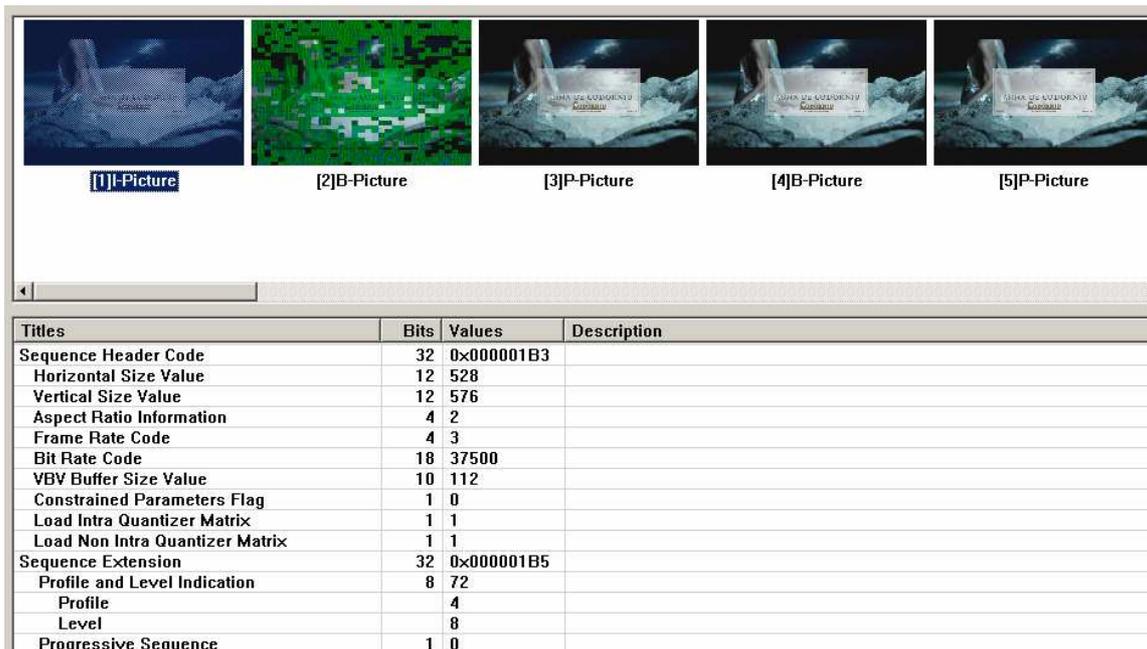


Figura 40.- Análisis stream video

A continuación realizamos el mismo análisis al mismo stream de video pero pasando previamente por la aplicación con la opción de “encriptación servicios”. Como se puede comprobar en la figura esta vez no podemos obtener ningún tipo de información de este vídeo a excepción del PID. (la información del PID del vídeo está contenida dentro de la PMT).

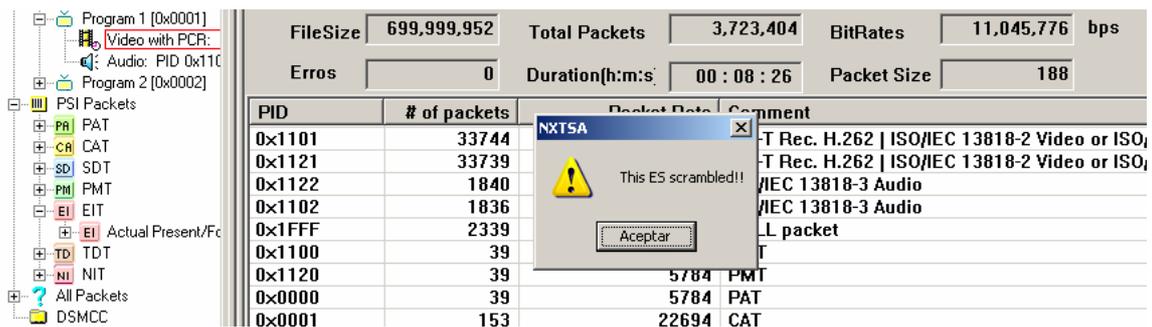


Figura 41.- Análisis stream video encriptado

La figura 42 muestra el análisis de un transport stream encriptado totalmente con la peculiaridad de la no encriptación de los bits de sincronismo. Aparentemente el programa de análisis parece recoger la información de este paquete de forma correcta. Pero como se ha comentado antes si se intenta la descodificación con un receptor cualquiera se muestra

que esta información no es correcta. Simplemente lo que hace es interpretar los bits que aparecen en la misma posición.

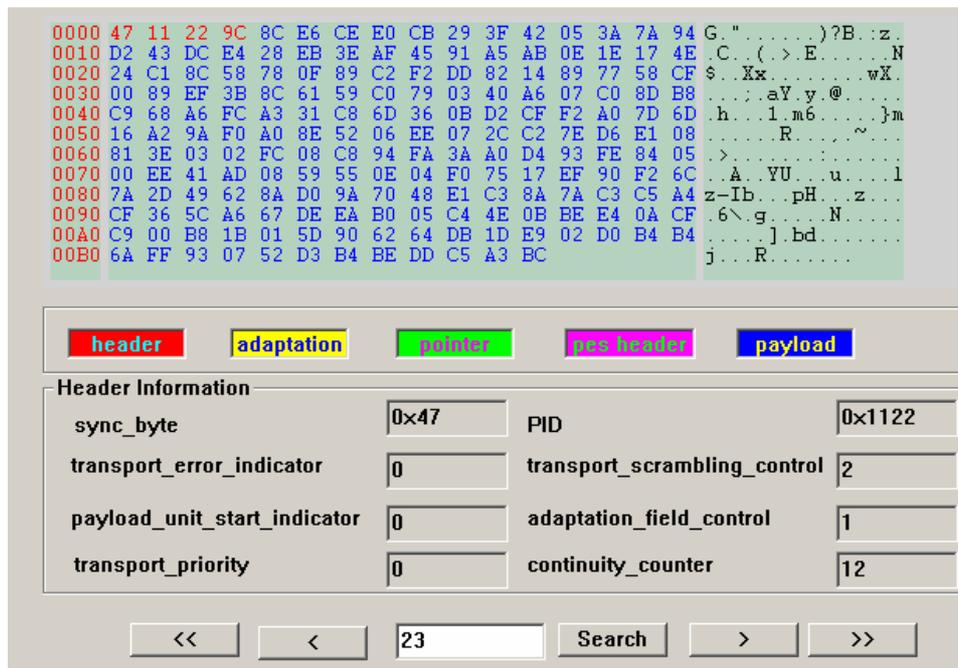


Figura 42.- Packet explorer encriptado

Para corroborar este hecho la próxima figura muestra el análisis del mismo paquete pero esta vez sin encriptar. Se comprueba que el único campo que se mantiene igual es el de los bits de sincronismo.

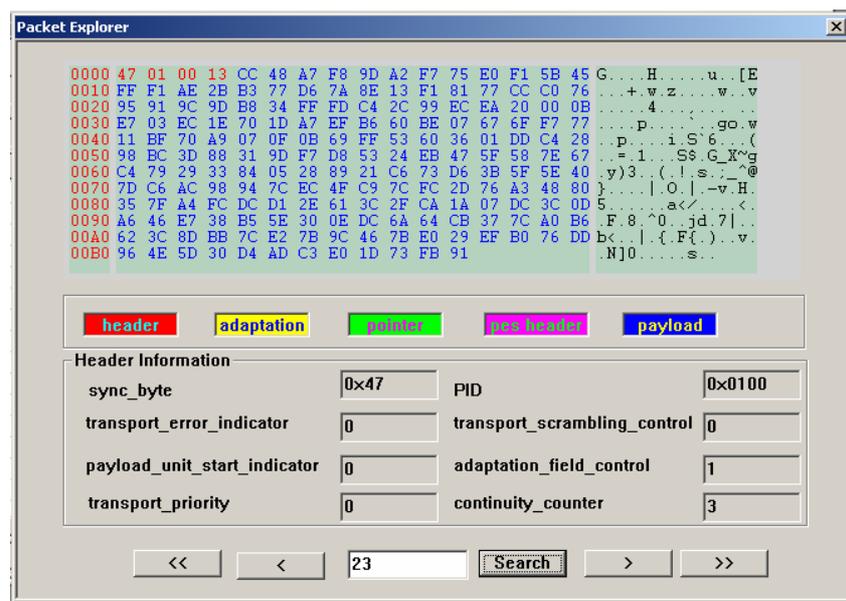


Figura 43.- Packet explorer no encriptado

5.1.2- Características

En este apartado se pretende realizar una explicación de las principales características de la aplicación. A continuación se listan algunas de ellas

Transparencia con la SFN: Un parámetro importante en la infraestructura de Abertis Telecom, es la tabla MIP. Esta tabla es muy importante cuando existen zonas de solape, entonces el modulador tiene que trabajar en modo SFN, y para poderlo hacer correctamente necesita que la aplicación deje pasar la MIP de forma transparente, sin introducir ningún retardo y sin alterar la información.

Sencillez de uso: La aplicación es muy sencilla de utilizar y de configurar. La tarjeta DTA-140 tiene definidas externamente las dos interfaces, tanto de entrada como de salida. La aplicación consta de dos ejecutables: Apli_abertis.exe y cript.exe y de los drivers correspondientes a la tarjeta. La instalación de los drivers es filosofía windows, basta con ejecutar el setup de estos en el server donde hemos instalado la tarjeta. Posteriormente hay que grabar los dos ejecutables en el mismo path. Basta con ejecutar el Apli_abertis.exe que es el que lanzará la interfaz gráfica, la cual llamará al otro ejecutable (con paso de variables) a otro ejecutable que es la aplicación en si.

Modificación algoritmo encriptación: El algoritmo de encriptación se ha implementado como una clase, por tanto la modificación de éste se puede realizar a nivel de código de una forma rápida. La ventajas de desarrollarlo así son que si la aplicación se utiliza para contribución, por tanto la encriptación y desencriptación recae siempre en las dependencias del operador de red, por temas de seguridad esta clave se puede ir cambiando cada cierto tiempo. De tal forma que si se llegara a descubrir la clave, solamente disfrutarían de la señal en un periodo de tiempo muy corto. Partimos de la base que normalmente estos sistemas funcionan 1+1, es decir, se dispone siempre de un equipo de "backup". Esto nos da la ventaja de que en el mantenimiento periódico de los equipos, en caso de querer modificar el código, habría que grabar el nuevo ejecutable tanto en la parte emisora como en la receptora, pero esto no supondría un corte de señal gracias al sistema de "backup".

5.2.- Limitaciones técnicas

La aplicación tiene una serie de limitaciones técnicas que hay que tener en cuenta. De hecho más que limitaciones técnicas serían una serie aspectos a mejorar en siguientes fases de desarrollo de la aplicación. Al ser una aplicación que se ha desarrollado en código c++ y con una filosofía de clases las posteriores mejoras y variaciones de la aplicación son relativamente sencillas de implantar. De hecho uno de los requisitos que se tomó la posible ampliación e integración de la aplicación en futuros proyectos.

Elección del servicio a encriptar a través de la interfaz gráfica: Actualmente en la aplicación no podemos elegir de una forma sencilla el servicio a encriptar. Ya que al ser una aplicación con el objetivo de realizar la contribución de los diferentes servicios, el servicio a encriptar se modifica a nivel de código c++.

Robustez en la encriptación: El algoritmo de encriptación es un algoritmo sencillo, no se han realizado pruebas de robustez, ya que hay que adquirir un cierto nivel de conocimiento en las diversas variantes que tienen los “hackers” en realizar este tipo de maniobras.

Limitación de coste: Si la aplicación se utiliza para un acceso condicional, donde la descryptación se realiza en las dependencias del usuario final, el coste de los receptores se vería incrementado ya que tendría que disponer de un módulo adicional capaz de descryptar el servicio elegido.

6.- Conclusiones

La TDT continúa extendiéndose en todo el territorio y ya es una realidad en la mayoría de hogares, de hecho hay alguna Comunidad Autónoma donde el apagón analógico se producirá en breve (2 años antes del apagón general). Los diferentes radiodifusores, ya sean a nivel nacional, autonómico o local están ya preparándose para el apagón. Los últimos canales en ofrecer su programación en TDT han sido los locales, pero la previsión a un año vista es que ya puedan ofrecer sus contenidos en TDT.

Por otro lado, ya existen varios modelos de televisión de pago. Los usuarios ya han aceptado el modelo “pay-per-view”. No es una novedad el pago por la visión de ciertos programas. Es un modelo ya consolidado en nuestro territorio.

El objetivo de este proyecto ha ido variando de forma que se ha ido adaptando a las necesidades que se han ido viendo por parte de la empresa. En un primer momento se pensó en hacer un modelo de acceso condicional clásico. Una vez valorado tanto las características comerciales como las características técnicas de dicho modelo, surgió la necesidad de realizar un acceso condicional de bajo coste, más enfocado hacia las televisiones autonómicas y locales. Por otro lado al tener experiencia en diversos ámbitos de la TDT, como el MHP (aplicaciones interactivas), y viendo el desarrollo de éstas (en los estándares se contempla ya el canal de retorno), surgió la idea de hacer un desarrollo conjunto entre el acceso condicional y el MHP. Este proyecto no pretende fusionar las dos tecnologías, sino dar el primer paso hacia esta interacción.

Desde el departamento también ha surgido la problemática de utilizar algún tipo de aplicación para las contribuciones de las señales de TDT. La necesidad viene dada al requerirse algún tipo de encriptación de dichas señales, ya que por normativa no se puede transportar las señales en abierto, si estas están destinadas a la contribución de los diversos emplazamientos.

En el desarrollo del proyecto, se ha trabajado en la mejora de cada componente que integra la aplicación. Se han realizado pruebas sobre cuatro arquitecturas diferentes, comenzando por una arquitectura sencilla, donde se realizan pruebas sobre un pc, hasta llegar a una arquitectura completa, donde se ha montado una cabecera y se ha integrado la aplicación en un transport stream real. En todas ellas se han obtenido resultados satisfactorios.

El principal problema, ha sido encontrar la optimización de la aplicación para no introducir un retardo demasiado elevado entre el TS de entrada y el TS de salida. Se han ido optimizando las clases de tal forma que el algoritmo del programa sea muy sencillo pero efectivo. Este requerimiento venía dado por la necesidad de dejar transparencia en la tabla MIP, ya que ésta lleva la información de la SFN.

La evaluación de los resultados finales se ha basado en la reconstrucción del transport stream de salida mediante el algoritmo inverso de encriptación, viendo que este se

reconstruía correctamente y se podía recomponer la señal de vídeo y audio sin ningún tipo de problema.

Otra resultado importante a tener en cuenta es, como he dicho antes, la transparencia de la tabla MIP. Para comprobar el comportamiento de la aplicación con esta tabla, se ha generado un “transport stream” en local, añadiendo un insertador de MIP, y volviendo a modular el “transport stream” y viendo en un modulador que este daba la MIP por buena.

Este proyecto, representa un modelo de negocio en futuras aplicaciones, y en diversos ámbitos de la TDT, pudiendo integrar dicha aplicación en otras estructuras como pueden ser utilizar el estándar MHP para realizar un acceso condicional de “low cost”.

7.- Anexos

7.1 Directiva 1998/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998.

Directiva 1998/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 2 de su artículo 57, y sus artículos 66 y 100 A,

Vista la propuesta de la Comisión (1),

Visto el dictamen del Comité Económico y Social (2),

De conformidad con el procedimiento establecido en el artículo 189 B del Tratado (3),

(1) Considerando que entre los objetivos de la Comunidad, de acuerdo con el Tratado, figura el de crear una unión cada vez más estrecha entre los pueblos de Europa y promover el progreso económico y social eliminando las barreras que los separan;

(2) Considerando que la prestación transfronteriza de servicios de radiodifusión y de servicios de la sociedad de la información puede contribuir, desde la perspectiva individual, a la plena efectividad de la libertad de expresión como derecho fundamental y, desde el punto de vista colectivo, a la consecución de los objetivos establecidos en el Tratado;

(3) Considerando que el Tratado prevé la libre circulación de todos los servicios que normalmente se prestan a cambio de una remuneración; que este derecho, aplicado a los servicios de radiodifusión y a los servicios de la sociedad de la información, constituye también una manifestación concreta en el Derecho comunitario de un principio más general, el de libertad de expresión consagrado en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que dicho artículo reconoce explícitamente el derecho de los ciudadanos de recibir o de comunicar informaciones sin consideración de fronteras, y que cualquier restricción de dicho derecho debe basarse en la debida consideración de otros legítimos intereses que merezcan protección jurídica;

(4) Considerando que la Comisión emprendió una consulta de amplio alcance basada en el Libro Verde «La protección jurídica de los servicios codificados en el mercado interior»; que los resultados de dicha consulta confirmaron la necesidad de un instrumento jurídico

comunitario que garantizase la protección jurídica de todos los servicios cuya remuneración depende del acceso condicional;

(5) Considerando que el Parlamento Europeo, en su Resolución de 13 de mayo de 1997 sobre el Libro Verde (4), pedía a la Comisión que presentase una propuesta de Directiva relativa a todos los servicios codificados en los que se utiliza la codificación para garantizar el pago de un canon, mostrándose de acuerdo en que se deben incluir los servicios de la sociedad de la información, prestados a distancia por medios electrónicos previa solicitud individual del receptor del servicio, así como los servicios de radiodifusión;

(6) Considerando que las oportunidades que ofrecen las tecnologías digitales permiten brindar al consumidor mayores posibilidades de elección y contribuyen al pluralismo cultural, mediante el desarrollo de un abanico cada vez más amplio de servicios a efectos de los artículos 59 y 60 del Tratado; que la viabilidad de estos servicios dependerá con frecuencia del uso del acceso condicional para garantizar la remuneración del proveedor del servicio; que, en consecuencia, parece necesaria la protección jurídica de los proveedores de servicios contra dispositivos ilícitos que permitan el acceso sin cargo a dichos servicios para garantizar la viabilidad económica de los servicios;

(7) Considerando que la importancia de esta cuestión quedó reconocida en la Comunicación de la Comisión sobre una «Iniciativa europea sobre comercio electrónico»;

(8) Considerando que, de conformidad con el artículo 7 A del Tratado, el mercado interior implica un espacio sin fronteras interiores en el que queda garantizada la libre circulación de mercancías y servicios; que el apartado 4 del artículo 128 del Tratado exige que la Comunidad tenga en cuenta los aspectos culturales en su actuación en virtud de otras disposiciones del Tratado; que en virtud del apartado 3 del artículo 130 del Tratado la Comunidad debe contribuir, mediante las políticas y actividades que lleve a cabo, a asegurar la existencia de las condiciones necesarias para la competitividad de la industria comunitaria;

(9) Considerando que la presente Directiva se entiende sin perjuicio de las posibles disposiciones nacionales o comunitarias futuras destinadas a garantizar que una serie de servicios de radiodifusión, reconocidos como de interés público, no se basen en el acceso condicional;

(10) Considerando que la presente Directiva se entiende sin perjuicio de los aspectos culturales de cualquier ulterior acción comunitaria relativa a nuevos servicios;

(11) Considerando que la disparidad entre las normativas nacionales relativas a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso puede crear obstáculos a la libre circulación de servicios y mercancías;

(12) Considerando que la aplicación del Tratado no es suficiente para suprimir estos obstáculos al mercado interior; que, por consiguiente, es necesario suprimirlos previendo un nivel de protección equivalente entre los Estados miembros; que esto implica la

aproximación de las normas nacionales relativas a las actividades comerciales en las que intervienen dispositivos ilícitos;

(13) Considerando que parece necesario procurar que los Estados miembros proporcionen una protección jurídica adecuada frente a la comercialización destinada a obtener un beneficio económico directo o indirecto de un dispositivo ilícito que posibilite o facilite el soslayar, sin autorización para ello, cualquier medida técnica adoptada para proteger la remuneración de un servicio suministrado con total legalidad;

(14) Considerando que estas actividades comerciales relacionadas con dispositivos ilícitos comprenden comunicaciones comerciales entre las que se incluyen todas las formas de publicidad, mercadotecnia directa, patrocinio, promoción de ventas y relaciones públicas para promocionar dichos productos y servicios;

(15) Considerando que estas actividades comerciales van en perjuicio de los consumidores a los que no se manifiesta el origen de los dispositivos ilícitos; que resulta necesario un nivel elevado de protección del consumidor para combatir este tipo de fraude; que el apartado 1 del artículo 129 A del Tratado dispone que la Comunidad debe contribuir a que se alcance un alto nivel de protección de los consumidores mediante las medidas que adopte en aplicación del artículo 100 A;

(16) Considerando que, por consiguiente, es necesario completar el marco jurídico relativo a la creación de un espacio audiovisual único establecido en la Directiva 89/552/CEE del Consejo, de 3 de octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva (5), en lo que se refiere a las técnicas de acceso condicional tal como se establece en la presente Directiva, para garantizar, en particular, la igualdad de trato a los prestadores de servicios de radiodifusión transfronteriza, con independencia del lugar en que se encuentren establecidos;

(17) Considerando que, de conformidad con la Resolución del Consejo, de 29 de junio de 1995, sobre la aplicación uniforme y eficaz del Derecho comunitario y sobre las sanciones aplicables por incumplimiento de sus disposiciones relativas al mercado interior (6), los Estados miembros deben adoptar medidas que conduzcan a una aplicación del Derecho comunitario con una eficacia y un rigor equivalentes a los empleados en aplicación de su Derecho nacional;

(18) Considerando que, con arreglo al artículo 5 del Tratado, los Estados miembros adoptarán todas las medidas apropiadas para asegurar el cumplimiento y efectividad del Derecho comunitario, en particular velando por que las sanciones escogidas sean eficaces, disuasorias y proporcionadas y las vías de recurso apropiadas;

(19) Considerando que la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros no debe exceder de lo necesario para alcanzar los objetivos del mercado interior, de conformidad con el principio de proporcionalidad previsto en el párrafo tercero del artículo 3 B del Tratado;

(20) Considerando que la distribución de dispositivos ilícitos incluye la transferencia por cualquier medio y la puesta en el mercado de los mismos para su circulación dentro y fuera de la Comunidad;

(21) Considerando que la presente Directiva se entiende sin perjuicio de la aplicación de cualesquiera disposiciones nacionales que puedan prohibir la posesión privada de dispositivos ilícitos, de la aplicación de las normas comunitarias sobre competencia y de la aplicación de las normas comunitarias relativas a los derechos de propiedad intelectual;

(22) Considerando que el Derecho nacional relativo a las sanciones y las vías de recurso previstas en contra de las actividades comerciales infractoras podrá establecer el requisito de que dichas actividades se hayan llevado a cabo con conocimiento, o teniendo razones suficientes para tener conocimiento, de que dichos dispositivos son ilícitos;

(23) Considerando que las sanciones y las vías de recurso a que se refiere la presente Directiva se entenderán sin perjuicio de las sanciones o vías de recurso de otro tipo que puedan establecerse en el Derecho nacional, tales como medidas preventivas en general o incautación de dispositivos ilícitos; que los Estados miembros no están obligados a establecer sanciones penales para las actividades infractoras cubiertas por la presente Directiva; que las disposiciones de los Estados miembros relativas a demandas de indemnización deberán ser conformes a sus sistemas legislativos y judiciales nacionales;

(24) Considerando que la presente Directiva se entiende sin perjuicio de la aplicación de las normas nacionales que no entren en el ámbito por ella coordinado, tales como las adoptadas para la protección de los menores, incluidas las adoptadas en cumplimiento de la Directiva 89/552/CEE, o las disposiciones nacionales en materia de orden público o de seguridad pública,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1 Ámbito de aplicación

El objetivo de la presente Directiva es la aproximación de las disposiciones de los Estados miembros relativas a las medidas en contra de dispositivos ilícitos que permiten el acceso no autorizado a servicios protegidos.

Artículo 2 Definiciones

A efectos de la presente Directiva se entenderá por:

a) «servicio protegido», cualquiera de los siguientes servicios, siempre que se presten a cambio de remuneración y sobre la base del acceso condicional:

radiodifusión televisiva, según se define en la letra a) del artículo 1 de la Directiva 89/552/CEE,

radiodifusión sonora, a saber cualquier transmisión por hilo o radioeléctrica, incluida la transmisión por satélite, de programas de radio destinados a su recepción por el público,

servicios de la sociedad de la información, en el sentido del punto 2 del artículo 1 de la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información (7), o el suministro de acceso condicional a los servicios antedichos considerado como servicio independiente;

b) «acceso condicional», cualquier medida o mecanismo técnico en virtud del cual se condicione el acceso al servicio protegido en forma inteligible a una autorización individual previa;

c) «dispositivo de acceso condicional», cualquier equipo o programa informático diseñado o adaptado para hacer posible el acceso a un servicio protegido en forma inteligible;

d) «servicio vinculado», la instalación, mantenimiento o sustitución de dispositivos de acceso condicional, así como la prestación de servicios de comunicación comercial relacionados con los mismos o con servicios protegidos;

e) «dispositivo ilícito», cualquier equipo o programa informático diseñado o adaptado para hacer posible el acceso a un servicio protegido en forma inteligible sin autorización del proveedor del servicio;

f) «ámbito coordinado por la presente Directiva», cualquier disposición relativa a las actividades infractoras que se especifican en el artículo 4.

Artículo 3 Principios del mercado interior

1. Cada Estado miembro adoptará las medidas necesarias para prohibir en su territorio las actividades enumeradas en el artículo 4, así como para establecer las sanciones y vías de recurso previstas en el artículo 5.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros no podrán, por motivos que entren en el ámbito coordinado por la presente Directiva:

a) restringir la prestación de servicios protegidos, o de servicios vinculados, que tengan su origen en otro Estado miembro;

b) restringir la libre circulación de los dispositivos de acceso condicional.

Artículo 4 Actividades infractoras

Los Estados miembros prohibirán en su territorio cada una de las siguientes actividades:

- a) la fabricación, importación, distribución, venta, alquiler o posesión con fines comerciales de dispositivos ilícitos;
- b) la instalación, mantenimiento o sustitución con fines comerciales de un dispositivo ilícito;
- c) el uso de comunicaciones comerciales para la promoción de dispositivos ilícitos.

Artículo 5 Sanciones y vías de recurso

1. Las sanciones deberán ser eficaces, disuasorias y proporcionadas al efecto potencial de la actividad infractora.
2. Los Estados miembros adoptarán las medidas necesarias para garantizar que los proveedores de servicios protegidos cuyos intereses se vean afectados por una actividad infractora de las mencionadas en el artículo 4, llevada a cabo en su territorio, tengan acceso a las vías de recurso apropiadas, incluidos la interposición de una demanda por daños y perjuicios y la obtención de una orden judicial u otras medidas cautelares y, cuando proceda, la solicitud de que se eliminen los dispositivos ilícitos de los circuitos comerciales.

Artículo 6 Aplicación

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para cumplir la presente Directiva a más tardar el 28 de mayo de 2000. Informarán inmediatamente de ello a la Comisión.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito coordinado por la presente Directiva.

Artículo 7 Informes

A más tardar tres años después de la entrada en vigor de la presente Directiva, y posteriormente cada dos años, la Comisión presentará un informe al Parlamento Europeo, al Consejo y al Comité Económico y Social relativo a la aplicación de la presente Directiva acompañándolo, cuando proceda, de propuestas, en particular en lo que se refiere a las definiciones del artículo 2, para su adaptación en función de la evolución técnica y económica, así como de las consultas llevadas a cabo por la Comisión.

Artículo 8 Entrada en vigor

La presente Directiva entrará en vigor el día de su publicación en el Diario Oficial de las Comunidades Europeas.

Artículo 9 Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el 20 de noviembre de 1998.

Por el Parlamento Europeo

El Presidente

J. M. GIL-ROBLES

Por el Consejo

El Presidente

E. HOSTASCH

(1) DO C 314 de 16. 10. 1997, p. 7 y DO C 203 de 30. 6. 1998, p. 12.

(2) DO C 129 de 27. 4. 1998, p. 16.

(3) Dictamen del Parlamento Europeo de 30 de abril de 1998 (DO C 152 de 18. 5. 1998, p. 59), Posición común del Consejo de 29 de junio de 1998 (DO C 262 de 19. 8. 1998, p. 34) y Decisión del Parlamento Europeo de 8 de octubre de 1998 (DO C 328 de 26. 10. 1998). Decisión del Consejo de 9 de noviembre de 1998.

(4) DO C 167 de 2. 6. 1997, p. 31.

(5) DO L 298 de 17. 10. 1989, p. 23. Directiva modificada por la Directiva 97/36/CE del Parlamento Europeo y del Consejo (DO L 202 de 30. 7. 1997, p. 60).

(6) DO C 188 de 22. 7. 1995, p. 1.

(7) DO L 204 de 21. 7. 1998, p. 37. Directiva modificada por la Directiva 98/48/CE (DO L 217 de 5. 8. 1998, p. 18).

7.2 MPEG

El algoritmo de compresión de vídeo de MPEG utiliza dos técnicas fundamentales: Compensación del movimiento basada en bloques para la reducción de la redundancia temporal, y Codificación (DCT–Discrete cosine Transform) para la reducción de la redundancia espacial. La técnica de compensación de movimiento se aplica en ambas direcciones: hacia adelante o causal (forward) y hacia atrás o no causal (backward). La señal restante es codificada utilizando las técnicas basadas en transformaciones. Los predictores de movimiento, denominados vectores de movimiento, son transmitidos junto con la información espacial.

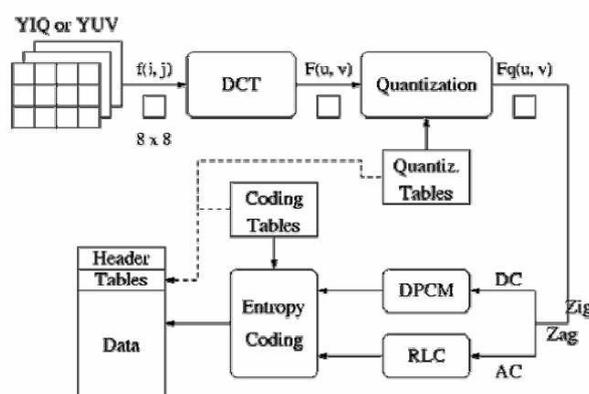
1. Reducción de la Redundancia Temporal.

Para soportar el acceso aleatorio al vídeo almacenado, se definen tres tipos fundamentales de imágenes o cuadros: codificados internamente (I), predictivos (P) e interpolados bidireccionalmente (B).

La predicción para la compensación del movimiento supone que la imagen actual puede ser modelada como una traslación de las imágenes precedentes. En el estándar MPEG, cada imagen es dividida en bloques de 16x16 píxeles denominados macrobloques. Cada macrobloque es predicho a partir del frame anterior o del siguiente estimando la cantidad de movimiento en el macrobloque durante el intervalo entre frames. La sintaxis de MPEG especifica cómo representar la información de movimiento para cada macrobloque, utilizando para ello vectores de movimiento. Sin embargo no especifica cómo van a ser calculados estos vectores.

2. Reducción de la Redundancia Espacial.

Para la reducción de la redundancia espacial en cada frame I o en la predicción de errores en frames P o B, el estándar MPEG utiliza técnicas de codificación basadas en DCT.



La DCT incluye la FFT y su operación básica es transformar una serie de puntos del dominio espacial a una representación idéntica en el dominio de la frecuencia. La DCT se aplica sobre una matriz generalmente de 8x8 cuya salida es otra matriz de iguales

8.- Glosario de términos

AIT: Application Information Table.
API: Application Programming Interface.
ARIB: Association of Radio Industries and Businesses (organización japonesa encargada de la estandarización)
ART: Artículo.
ATSC: Advanced Television Systems Committee.
AWT: Abstract Window Toolkit.
BAT: Bouquet Association Table.
BBS: Bulletin Board Systems.
CAT: Conditional Access Table.
CEIAF: Centro Especial de Integración Audiovisual y Formación.
CEN: Comité Europeo de Normalización.
CENAM: Centro Nacional de Metrología.
CENELEC: Comité Europeo de Normas de Telecomunicaciones.
CET: Central European Time.
CLUT: Color LookUp Table.
CMT: Comisión del Mercado de las Telecomunicaciones.
CRTC: Comisión de Radio-Televisión de Canadá.
CTN: Comité Técnico de Normalización.
DA: Disposición Adicional.
DAVIC: Digital Audio Video Council.
DF: Disposición final.
DIT: Discontinuity Information Table.
DVB: Digital Video Broadcasting.
EIT: Event Information Table.
EPG: Electronic Program Guide.
ES: Elementary Stream.
ETSI: Instituto Europeo de Normas de Telecomunicaciones.
FCC: Comisión Federal de las Comunicaciones.
GMT: Greenwich Mean Time.
GUI: Gráfico User Interface.
HAVi: Home Audio Video Interoperability.
HDTV: High Definition Television.
HW: Hardware.
IBV: Intervalo Blanco Vertical.
ID: Identificador.
IDE: Integrated Development Environment.
LGTel: Ley General de Telecomunicaciones.
LSSICE: Ley de Servicio de la Sociedad de la Información y Comercio Electrónico.
M: Mandato.
MHP: Multimedia Home Platform.
MPEG: Motion Picture Expert Group.
MUX: Multiplexor.
NIT: Network Information Table.

NPT: Normal Play Time.
NTP: Network Time Protocol.
ONID: Original_Network ID.
PAT: Program Association Table.
PES: Packetised Elementary Streams.
PMT: Program Map Table.
PPV: Pay per view
PTE: Plataforma Tecnológica Europea.
PSI: Program Specific Information.
PTNTDT: Plán Técnico Nacional de la TDT.
RGB: Red Green Blue.
RST: Running Status Table.
RTOS: Real-Time Operating Systems.
SC: Subcomité.
SDK: Software Development Kit.
SDT: Service Description Table.
SFN: Single Frequency Network.
SI: Service Information.
SID: Service ID.
SIT: Selection Information Table.
ST: Stuffing Table.
STB: Set Top Box.
SW: Software.
TDT: Televisión Digital Terrestre.
TDT: Time and Date Table.
TIC: Tecnologías de la Información y la Comunicación.
TOT: Time Offset Table.
TS: Transport Stream.
TSID: Transport_Stream ID.
UTC: Coordinated Universal Time.
VBI: Vertical Blanking Interval (Intervalo Vertical en Blanco).
VoD: Video on Demand.
WET: Western European Time.
XML: eXtensible Markup Language.

9.- Referencias y bibliografía

9.1.- Referencias

[1] "La compresión como elemento esencial de la televisión digital", Ciro A. Martínez García Moreno, Soluciones Avanzadas Diciembre de 1995, pp. 48-52.

[2] http://www.lsi.upc.es/~joseluis/lc-pub/pgp/intro_cripto.html

[3] http://www.lsi.upc.es/~joseluis/lc-pub/pgp/intro_cripto.html

[4] <http://www.sateliteinfos.com/>

[5] <http://www.sateliteinfos.com/>

[6] <http://derecho-internet.org/node/34>

[7] "España: Estado actual de la TDT"; Gutiérrez Eladio. Junio 2006.

[8] <http://www.dvb.org>: Web oficial del proyecto DVB, donde se puede encontrar información referente a los diferentes estándares que regulan la difusión de la señal de televisión digital.

[9] Tutorial TDT, LaSalle, marzo 2006

[10] <http://www.etsi.com/>

[11] <http://www.salle.url.edu/Eng/elsDTA/elsVideo/webts/index.htm/>

9.2.- Bibliografía

<http://www.mundoplus.tv/muchomas/zonatdt>: Web que proporciona información sobre el estado actual de la TDT, parámetros técnicos, ventajas de la TDT, frecuencias e información relacionada con MHP.

<http://www.tdtcat.net/tdtcat/AppPHP/cat/index.php>: Web con información sobre TDT en Cataluña.

<http://www.tvdi.net>: Web con información sobre TDT a nivel nacional.

<http://www.dgtvi.it>: Web con información relativa a la TDT en Italia.

<http://es.wikipedia.org>: Enciclopedia libre donde se puede encontrar información variada.

“Diseño para todos en las tecnologías de la información y las comunicaciones”; Rodríguez Cristina. Octubre 2004.

“An introduction to DTV receiver technology”; Morris Steve. 2005.

“Situación MHP en España”; Subgrupo 1 del Grupo de trabajo 7 del Foro Técnico de la Televisión Digital. Abril 2005.

“Guía de implementación de la TDT en España”; Subgrupo2 del Grupo de trabajo 7 del Foro Técnico de la Televisión Digital. Septiembre 2005.

“Estándares y legislación en España”; Mayoral Concha. Noviembre 2005.

“Normativa y legislación”; Fuertes José Luís, Martínez Loïc. Diciembre 2005.

“Análisis comparado de las normas autonómicas y estatales de accesibilidad”; Alegre Lluís, Casado Natividad, Vergés Jordi. Enero 2006.

Curso de TDT. La Salle. Marzo 2006.

“Estandarización y legislación internacional”; Martínez Loïc. Mayo 2006.

“Interactive Services based on DVB technologies”; Karimi Nima. Octubre 2006.

EN 301 192 v1.1.1; “Digital Video Broadcasting (DVB); DVB specification for data broadcasting”.

TR 101 202; “Digital Video Broadcasting (DVB); Implementation guidelines for data broadcasting”.

ETSI EN 300 468 v1.6.1; “Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems”.

Documentación interna. Abertis Telecom.