ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

MÁSTER EN INGENIERÍA DE TELECOMUNICACIÓN

Análisis comparativo de las principales tecnologías para transmisión de datos en PLC de banda estrecha

Autor: Margarita Sanz del Río

Director: Javier Matanza Domingo

Madrid

Julio 2018

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Análisis comparativo de las principales tecnologías para transmisión de datos en PLC de banda estrecha

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2017/18 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Margarita Sanz del Río Fecha: ……/ ……/ ……

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Javier Matanza Domingo Fecha: ……/ ……/ ……

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. ª Margarita Sanz del Río DECLARA ser el titular de los derechos de propiedad intelectual de la obra: Análisis comparativo de las principales tecnologías para transmisión de datos en PLC de banda estrecha, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente).*

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.
d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción

de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a …….. de ……... de …….

ACEPTA

Fdo……

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

MÁSTER EN INGENIERÍA DE TELECOMUNICACIÓN

Análisis comparativo de las principales tecnologías para transmisión de datos en PLC de banda estrecha

Autor: Margarita Sanz del Río

Director: Javier Matanza Domingo

Madrid

Junio 2018

"No basta con querer: debes preguntarte a ti mismo
qué vas a hacer para conseguir lo que quieres."

-Franklin D. Roosevelt

ANÁLISIS COMPARATIVO DE LAS PRINCIPALES TECNOLOGÍAS PARA TRANSMISIÓN DE DATOS EN PLC DE BANDA ESTRECHA

Autor: Sanz del Río, Margarita.
Director: Matanza Domingo, Javier.
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas.

RESUMEN DEL PROYECTO

En este proyecto se analizan y comparan las principales tecnologías para transmisión de datos en PLC de banda estrecha a dos niveles, técnico y comercial. En él se identifican sus principales ventajas y desventajas a fin de comprender mejor las implicaciones de cada uno. Debido a la falta de documentación de uno de ellos, también se incluyen los resultados obtenidos de su simulación en un entorno software.

Palabras clave: PLC, Smart Grids, PRIME, G3-PLC, Meters&More

1. Introducción

La tecnología de comunicación mediante líneas de potencia, también conocida por su nombre en inglés (*Power Line Communications*), se considera una tecnología muy adecuada para aplicaciones de medición inteligente. Incluso, la UE tiene como objetivo reemplazar al menos el 80% de los contadores de electricidad con contadores inteligentes para 2020.

A pesar de que en los últimos años se han desarrollado numerosos protocolos, se desconoce cuáles son las verdaderas implicaciones de cada uno, llegando al punto en el que no se ha acordado un único protocolo común que se implante de manera generalizada en distintos países.

2. Definición del proyecto

El proyecto que se documenta consiste en dos partes fundamentales. En primer lugar, y dada la falta de documentación disponible para el usuario, se ha desarrollado toda una investigación y análisis del estado del arte de los protocolos de *Smart Grids* que están, bien comercializándose, bien en estado de prueba, principalmente en Europa.

Las conclusiones obtenidas de esta investigación han dado pie al desarrollo de la segunda parte. En ésta se ha definido, programado e implementado en un entorno de pruebas uno de los protocolos de comunicaciones menos extendido y con mayor carencia de documentación, *Meters & More*.

3. Descripción del modelo

La simulación desarrollada presenta una arquitectura que sigue el esquema de elementos que se definen en la especificación técnica y qué está compuesta por un maestro y una serie de esclavos. En esta arquitectura el maestro es el único capaz de comenzar una comunicación y los esclavos sólo son capaces de enviar información si antes ha recibido una petición por parte del maestro.

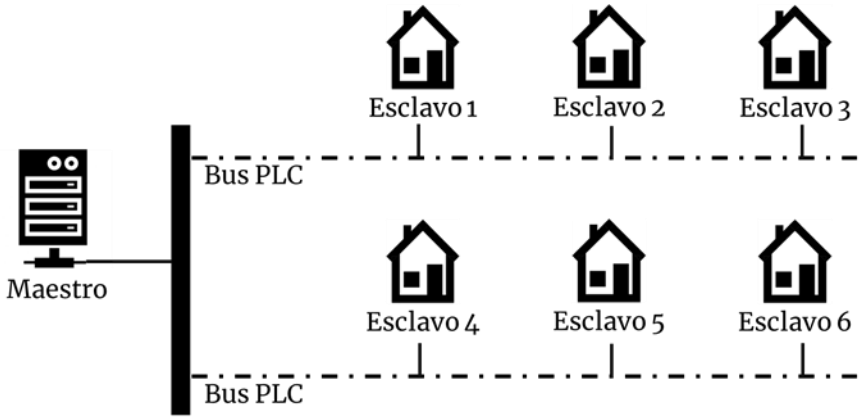


Figura 1. Arquitectura implementada en el entorno de pruebas

La comunicación dentro de la red se hace con un esquema tipo bus, donde todos los dispositivos reciben la información, pero solamente la procesan aquellos a los que va dirigido el mensaje. La comunicación consta de tres mensajes principales, siendo estos:

- Request: petición inicial que manda el maestro a un esclavo a fin de recopilar información de campo o enviar alguna orden.
- Indication: es la respuesta que genera el esclavo a la *request*, en ella el mensaje que se envía es el mismo y con ellos se confirma que la petición se ha recibido y que se está procesando.
- Confirm: responde al *indication*. De nuevo, se trata de un mensaje que copia la información del mensaje anterior y que envía el maestro una vez ha recibido respuesta por parte del esclavo. En el momento en el que el esclavo recibe este mensaje la comunicación termina.

Este protocolo implementa un sistema de *ACKs* donde cada mensaje confirma la recepción del mensaje anterior, exceptuando en el caso del *confirm*. En este último caso la ausencia de mensaje indica que no ha habido problemas de comunicación. Para poder implementar en este comportamiento se han incluido temporizadores que se han ajustado siguiendo los parámetros de la especificación técnica.

4. Resultados

Para garantizar que los resultados obtenidos no han sufrido sesgo de ningún tipo, se han llevado a cabo simulaciones donde parámetros cómo la probabilidad de error en la comunicación y el número de dispositivos dentro de la red se han hecho variables. De esta manera se garantiza que la información obtenida es veraz y cubre un rango de escenarios lo suficientemente amplio.

Los parámetros que se han estudiado se centran en comprender el rendimiento y aportar información que permita comprender mejor cuáles sus capacidades. En las figuras a continuación se observan, tanto la latencia entre dos nodos, medida como el tiempo que transcurre desde que se manda el *Request*, hasta que llega el *Indication*, como la latencia

total del sistema. Esta última medida permitirá comprender cómo varía el rendimiento en función del tamaño de la red.

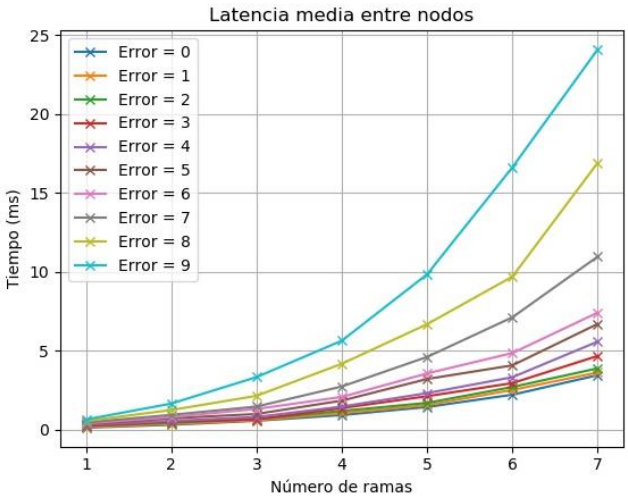


Figura 2. Latencia entre nodos

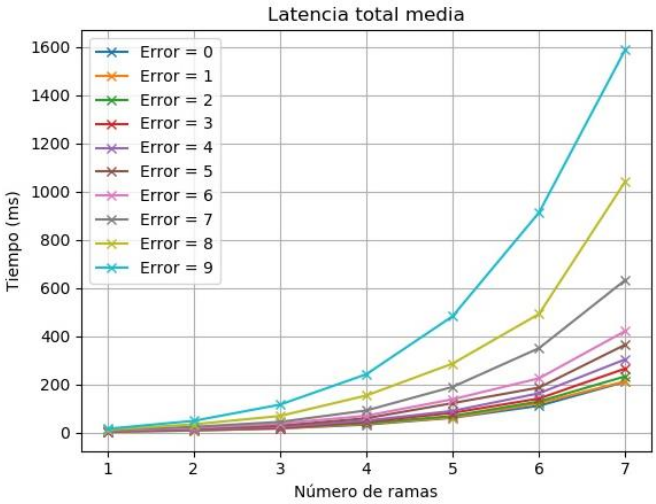


Figura 3. Latencia total

En la primera gráfica podemos ver que, a medida que el error aumenta, la latencia media entre nodos aumenta, siendo este factor determinante para garantizar la consistencia de las simulaciones. También que, a medida que exponemos el sistema a situaciones más duras, este se comporta peor que en el caso anterior. Esta es una característica que nos permite entender y justificar los casos de uso de este protocolo en escenarios reales, donde sólo tiene sentido cuando sabemos que las condiciones del medio son muy buenas.

La segunda figura muestra la latencia total media que se ha medida aplicando las mismas condiciones que se aplicaron para la obtención de la latencia entre nodos. Este parámetro resulta muy útil en términos de rendimiento puesto que, de cara a su aplicación, no es lo mismo disponer de una red con 10 nodos que de una red con 100.

5. Conclusiones

El proyecto presentado proporciona un punto de información completo y único que garantiza que un lector puede comprender las características de los protocolos descritos sin necesidad de poseer conocimientos técnicos profundos sobre el tema. De esta manera se fomenta la divulgación de esta nueva tecnología que cada vez se expande más por Europa y el mundo.

Además de todo lo anterior, este proyecto contribuye a la comunidad gracias a la aportación de medidas técnicas de uno de los protocolos estudiados, obtenidas a partir de una simulación desarrollada en un entorno software. De esta manera se garantiza la disponibilidad de información técnica que permite realizar comparaciones de manera precisa y fiable. Todo ello fomenta la investigación y desarrollo del sector de las redes, un sector ya en alza y crecimiento.

COMPARATIVE ANALYSIS OF THE MAIN TECHNOLOGIES FOR DATA TRANSMISSION IN NARROW BAND PLC

Author: Sanz del Río, Margarita.
Supervisor: Matanza Domingo, Javier.
Collaborating Entity: ICAI – Universidad Pontificia Comillas.

ABSTRACT

This project analyzes and compares the main technologies for data transmission in narrow-band PLC at two levels, technical and commercial. It identifies their main advantages and disadvantages in order to better understand the implications of each one. Due to the lack of documentation of one of them, a simulation has been developed and the results obtained from it are also included.

Keywords: PLC, Smart Grids, PRIME, G3-PLC, Meters&More

1. Introduction

Communication technology using power lines, also known as Power Line Communications (PLC), is considered a very suitable technology for intelligent measurement applications. Even the EU aims to replace at least 80% of electricity meters with smart meters by 2020.

Although many protocols have been developed in recent years, the true implications of each are unknown. There is not even an agreement where a single protocol has been chosen that is installed in a generalized manner in several countries.

2. Project definition

The project that is documented consists of two fundamental parts. In the first place and given the lack of documentation available to the user, a whole investigation and analysis of the state of the art of the Smart Grids protocols has been developed, which are either being commercialized or being tested, mainly in Europe.

The conclusions obtained from this investigation have given rise to the development of the second part. This has consisted in the definition, programming and implementation in a testing environment of one of the least widespread communication protocols and with the greatest lack of documentation, Meters & More.

3. System description

The developed simulation presents an architecture that follows the scheme of elements that are defined in the technical specification and that is composed of a master and a series of slaves. In this architecture, the master is the only one capable of starting a communication and the slaves are only able to send information if they have previously received a request from the master.

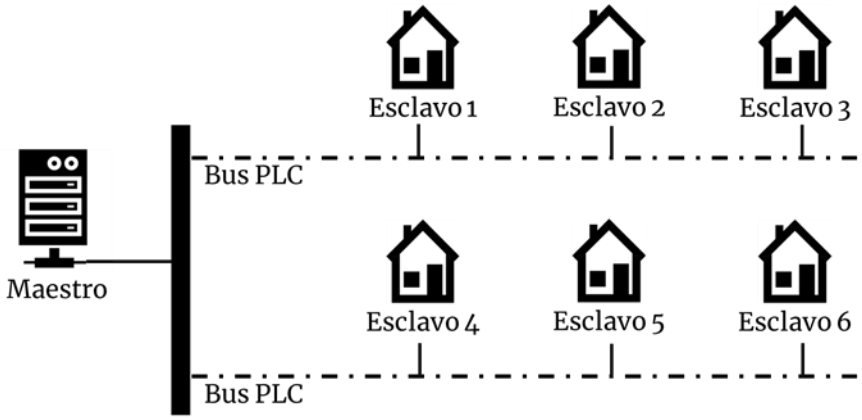


Figure 1. Implemented architecture

Communication within the network is done with a bus-type scheme, where all devices receive the information, but only processed by those to which the message is addressed. The communication consists of three main messages, being these:

- Request: Initial petition that the master sends to a slave to collect field information or send some order.
- Indication: It is the answer that generates the slave to the request, in it the message that is sent has the same SDU as the request and confirms that the request has been received and that it is being processed.
- Confirm: Responds to the indication. Again, this is a message that copies the SDU from the previous message and sends the teacher once it has received response from the slave. The moment the slave receives this message the communication ends.

This protocol implements a system of ACKs where each message confirms the reception of the previous message, except in the case of Confirm. In the latter case, the absence of a message indicates that there have been no communication problems. In order to implement this behavior, timers that have been adjusted following the parameters of the technical specification have been included.

4. Results

To ensure that the results obtained have not suffered bias of any kind, simulations have been carried out where parameters such as the probability of error in communication and the number of devices within the network have become variable. In this way, it is guaranteed that the information obtained is true and covers a wide enough range of scenarios.

The parameters that have been studied focus on understanding the performance and providing information. In the figures below, we can observe both the latency between two nodes, measured as the time that elapses between the order being sent, until the

indication arrives, and the total latency of the system. This last measure can be compared with the performance depending on the size of the network.

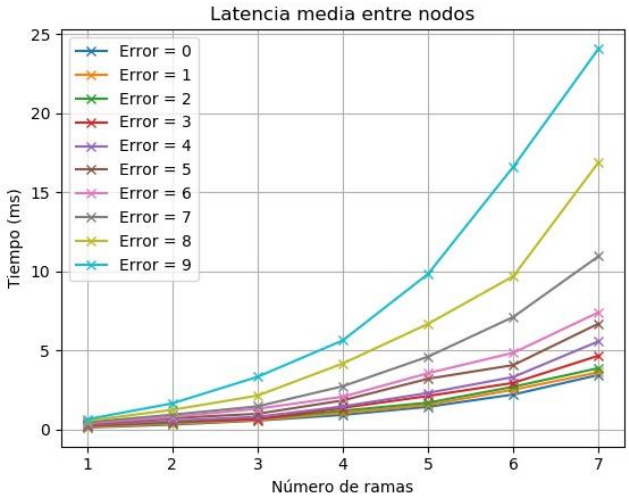


Figure 2. Latency between nodes

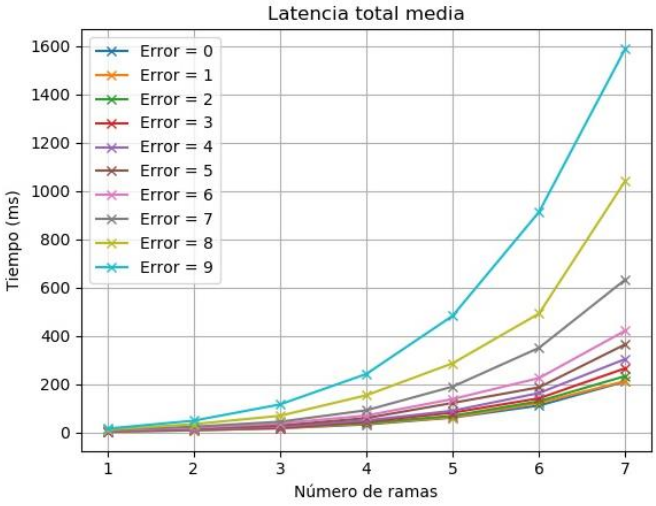


Figure 3. Total latency

In the first graph we can see that, as the error increases, the average latency between nodes increases, this being a determining factor to guarantee the consistency of the simulations. Also, as we expose the system to harsher situations, it behaves worse than in the previous case. This is a characteristic that allows us to understand and justify the cases of use of this protocol in real scenarios, where it only makes sense to use it when we know that the conditions of the environment are very good.

The second figure shows the average total latency that has been measured by applying the same conditions that were applied to obtain the latency between nodes. This parameter is very useful in terms of performance since, in terms of its application, it is not the same to have a network with 10 nodes than a network with 100.

5. Conclusions

The presented project provides a complete and unique information point that guarantees that a reader can understand the characteristics of the described protocols without needing to possess deep technical knowledge on the subject. Thus, the dissemination of this new technology that is increasingly expanding throughout Europe and the world is encouraged.

In addition to all the above, this project contributes to the community thanks to the share of technical measures of one of the protocols studied, obtained from a simulation developed in a software environment. In this way, the availability of technical information that allows accurate and reliable comparisons is guaranteed. All this promotes the research and development of the smart grids sector, a sector already on the rise and growth.

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

De una manera muy general, podemos definir la red eléctrica como una serie de líneas, transformadores y estaciones que permite transportar la energía eléctrica desde los mismos centros de producción hasta el hogar de cualquier consumidor. Este tipo de redes se encargan de transportar la energía que primero se crea en las centrales hasta el consumidor. Sin embargo, el despliegue de este tipo de redes comenzó a mitad del siglo pasado y, desde entonces, no se han hecho modificaciones. Es por esta razón que su modernización se convierte en un aspecto muy importante puesto que, la industria, debe adaptarse a las nuevas circunstancias para poder conseguir cubrir las nuevas necesidades tanto del consumidor final como de los productores.

En todas las redes hay una parte de la energía que se pierde en dos aspectos muy importantes, el transporte y la distribución. Durante el transporte nos encontramos con que la energía viaja de distinta manera atendiendo a cómo de cerca se encuentre del usuario final, viajando primero a tensiones muy altas (para minimizar las pérdidas) y reduciéndose esta tensión paulatinamente hasta llegar a una tensión que no supere los 1000V. Todo este proceso se realiza gracias a la instalación de centros de transformación y de una red de enlace que incluye elementos como transformadores, protecciones, elementos de control, etc. Todos estos dispositivos, a su vez, también necesitan poder soportar las necesidades futuras y por tanto una modernización [1].

En España, las tres actividades principales de generación, transporte y distribución, se encuentran separadas, siendo distintas entidades las responsables de su gestión. Estas empresas se enfrentan a varios problemas. Por un lado, tienen que ser capaz de transportar la energía entre las distintas estaciones y, por otro lado, dado que la energía no se puede almacenar, tienen que nivelar su producción haciendo estimaciones de la demanda. Es necesario prever el consumo y supervisar la generación. Para todo ello, Red Eléctrica elabora diariamente una estimación de la curva de demanda y gestiona la producción de tal manera que se ajuste lo máximo posible a la curva estimada.

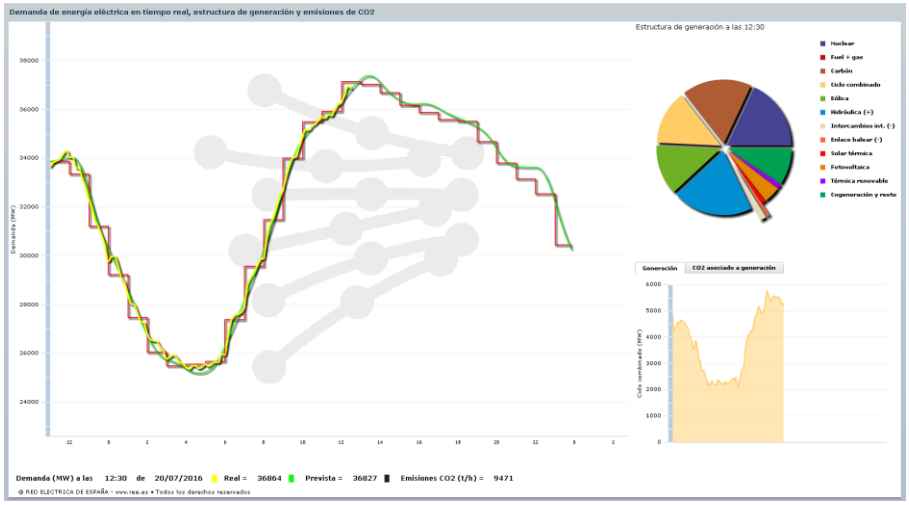


Figura 4. Curva de generación generada por Red Eléctrica

La ley 54/1997 implica que se ha liberalizado la actividad de generación y que por tanto existe la posibilidad de que los productores realicen ofertas. Los productores ofertan cantidades de electricidad a distintos precios que dependen de la hora del día, y los consumidores y comercializadores realizan ofertas de compra. Es decir, que la necesidad de controlar y monitorizar la red ha ido creciendo a lo largo de los últimos años [2].

Desde el punto de vista técnica, para la operación del sistema existen centros de control cuyo propósito es monitorizar la red y sus parámetros gracias a una red de telecomunicaciones que gestiona la principal red de transporte y los distintos centros de control.

En la actualidad existen más de 800 agentes que en su mayoría corresponde a productores en régimen especial. Los que se encuentran dentro de las energías renovables tienen algunas peculiaridades en cuanto a la disponibilidad y la planificación. Por otro lado, la demanda de energía es cada vez mayor y muchas de las redes trabajan en el límite de sus condiciones.

Además, también hay que tener en cuenta que en un futuro la participación en el mercado del consumidor final será mayor gracias a la implementación de placas solares, micro-generación, etc.

La realidad es que, hoy en día, la infraestructura eléctrica sí que cumple parte de las expectativas, pero es un hecho que tienen mejorar. Estas mejoras incluyen características para el usuario final y las funcionalidades que se esperan de la red. Las previsiones indican que surgirá un crecimiento moderado de la demanda, un crecimiento alto de las energías renovables y una necesidad de potencia firme y flexible. Las redes inteligentes surgen entonces y pueden ser definidas como "Redes eléctricas que pueden integrar de manera inteligente el comportamiento y las acciones de todos los actores conectados a ellas (quienes generan electricidad, quienes la consumen y quienes realizan ambas acciones) para proporcionar un suministro de electricidad seguro, económico y sostenible".

Las redes inteligentes permiten, del lado de producción, optimizar la generación de energía pudiendo prever con mayor exactitud y en tiempo real el consumo de energía, identificando picos y disminuyendo costes. Los contadores inteligentes permitirían dar solución a este problema, así como mejorar la integración de las energías renovables.

Las redes inteligentes integran las tecnologías de la información con las infraestructuras eléctricas actuales haciendo algo denominado "Internet de la energía".

El nuevo modelo energético pretende transformar el sistema actual en un sistema distribuido, donde cualquier agente que tenga conexión a la red tenga la posibilidad de aportar energía. Esto fomentaría la creación de micro-generadores, de tal manera que no existiría una dependencia tan grande con la generación de energía actual.

A nivel internacional ya se han empezado a desarrollar movimiento, protocolos, pilotos y despliegues que pongan en marcha este nuevo proyecto. En concreto, en la Unión Europea, la política del cambio se ha basado de el Plan 20-20-20, donde se pretende que para el 2020 se haya reducido en un 20% la emisión de gases de efecto invernadero, aportado un 20% a la generación de energía renovables y se haya mejorado la eficiencia energética en un 20%. De la misma forma, otros países como Australia, Canadá, Japón o Estados Unidos también están desarrollando políticas de reducción de emisiones cuyos planes incluyen la introducción de Redes Inteligentes.

1.1 MOTIVACIÓN DEL PROYECTO

Parece claro que las tecnologías de la información deben jugar un papel importante en la construcción de la red inteligente. Varios estudios abordaron la problemática de decidir qué tecnología sería la óptima para esta solución al comparar las principales ventajas y desventajas de diferentes medios de comunicación. La tecnología de comunicación mediante líneas de potencia, también conocida por su nombre en inglés (*Power Line Communications*), se considera una tecnología muy adecuada para aplicaciones de medición inteligente. Incluso, la UE tiene como objetivo reemplazar al menos el 80% de los contadores de electricidad con contadores inteligentes para 2020, siempre que sea rentable hacerlo.

Sin embargo, a pesar de que en los últimos años se han desarrollo numerosos protocolos que buscan sacar el mayor provecho a esta tecnología, no se ha llegado a acordar un único protocolo común que se implante de manera generalizada en distintos países.

Los sistemas de medición avanzada (AMI por sus siglas en inglés), están compuestos por hardware y software de última generación que combinan intervalos de toma de medidas con la constante disponibilidad de comunicaciones remotas. Estos sistemas permiten tomar medidas detalladas, organizarlas y transmitirlas a distintos dispositivos. AMI hace referencia a todo el sistema de medida que incluye, no sólo los dispositivos de medición en el lado del cliente, sino también las líneas de comunicación y los dispositivos de recepción y procesamiento de información disponibles en el lado del proveedor (típicamente proveedores de luz, agua, gas…). En la imagen que se muestra a continuación se pueden distinguir todos los elementos que conforman la arquitectura [3].

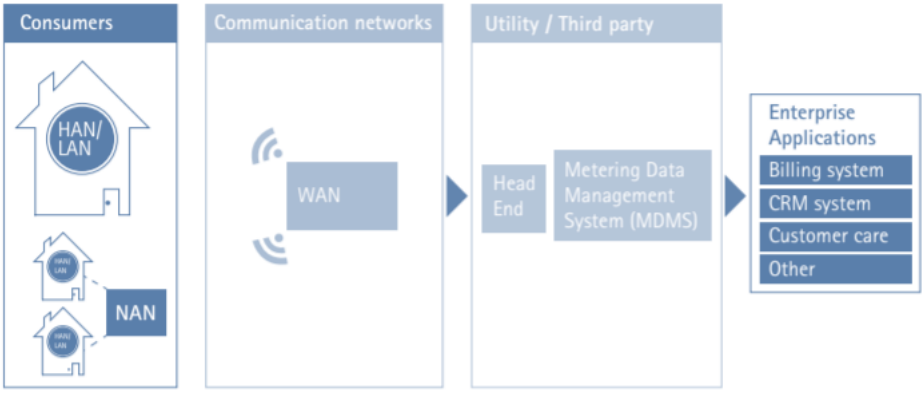


Figura 5. Principales bloques de la arquitectura AMI [4]

En la actualidad existen distintas variantes de PLC desplegadas que atienden a distintas especificaciones, incluyendo bandas de frecuencia, tasa de transmisión, modulación entre otras. En la tabla que se muestra a continuación se incluyen algunas de las principales características que representan cada una de esas variantes.

Tabla 1. Variaciones de PLC desplegadas en Europa [4]

PLC VARIANT	MAIN CHARACTERISTIC
G1	Open specifications for PLC communication S-FSK-based Max. bit rate 2.4 kbps IEC 61334
G3	Open specifications OFDM for the CENELEC A Band Frequency Band : 36-90.6kHz Bit rate (kbps): 5.6-45 36 channel-based OFDM system 6LoWPAN adaptation layer to transmit IPv6 over PLC Signal crossing the MV/LV transformers
PRIME	Open specifications 97 channel-based OFDM system

	Frequency Band : 42-89kHz Bit rates up to 128kbps
METERS AND MORE	Open technology Founded by Enel and Endesa Selected for standardization in OPEN meter project BPSK modulation Bit rate up to 4.8 kbps
ECHELON	BPSK-based Proprietary Narrowband PLC Solution CENELEC A Band (In utility applications)

Para entender mejor cuál es el alcance del despliegue de estas tecnologías en Europa en la figura que se muestra a continuación se puede ver, representado en un diagrama de colores, qué países han implantado qué tecnologías.

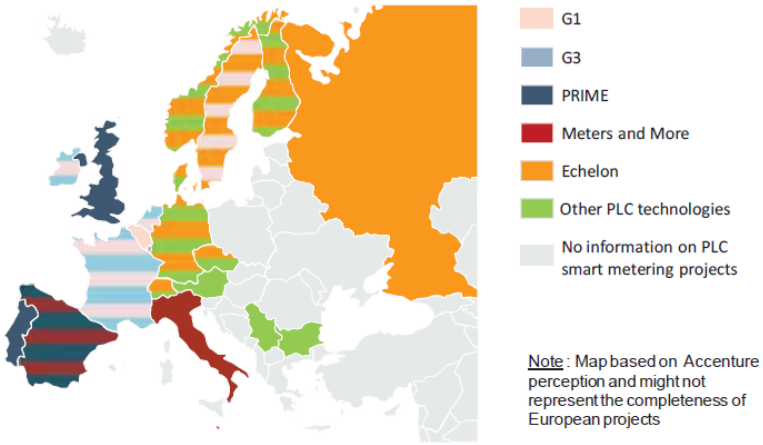


Figura 6. Distribución de las tecnologías de PLC en Europa [4]

Como ya se ha comentado anteriormente, en la actualidad no existe un protocolo establecido para el uso de esta tecnología en España. La elección de uno u otro a la hora de implantar sistemas AMI ha venido determinada en su totalidad por la propia entidad, sin la disposición de documentación suficiente que permita conocer en mayor medida cuáles son las consecuencias e impacto de una elección u otra. Sin embargo, en los últimos años las

empresas energéticas han mostrado un interés cada vez mayor por esta evolución, y es por ello que los protocolos desarrollados han ido adaptándose y mejorando.

Hasta el momento se han elaborado varios informes y *papers* que documentan alguna de las características más representativas de estas soluciones, sin embargo, no hay documentos que analicen en profundidad el impacto de estas soluciones, su alcance, y su comparación con otras soluciones disponibles en el mercado.

Además de todo lo anterior, en términos de documentación también existe una carencia grande de estudios que analicen la solución basada en *Meters&More*, ya que la inmensa mayoría de estudios se centran en PRIME y en G3-PLC. Esto es debido a que PRIME es una solución bastante extendida en España al Iberdrola fomentar su implantación entre sus consumidores; y G3-PLC es la solución promovida por G3-PLC Alliance, un grupo de empresas punteras en los ámbitos de la tecnología y la energía. Es por ello que no existen suficientes comparativas que incluyan *Meters&More*, proporcionando una visión más completa sobre las posibilidades de cada protocolo.

Todo ello lleva a la necesidad de establecer una comparativa entre los principales protocolos implantados en España, en este caso PRIME, G3-PLC y *Meters&More*.

1.2 SOLUCIÓN PROPUESTA

El proyecto que se documenta consiste de dos partes fundamentales. En primer lugar, y dada la falta de documentación disponible para el usuario, se ha desarrollado toda una investigación y análisis del estado del arte de los protocolos de *Smart Grids* que se están, bien comercializando, bien en estado de prueba, principalmente en Europa. Las conclusiones obtenidas de esta investigación han dado pie al desarrollo de la segunda parte. En ésta se ha definido, programado e implementado en un entorno de pruebas uno de los protocolos de comunicaciones menos extendido y con mayor carencia de documentación, *Meters & More*.

Hasta el momento los principales protocolos de comunicaciones que se planteaban eran *Prime* y *G3 PLC*. Sin embargo, y como se presentará en la sección de resultados y

conclusiones, estos protocolos no son los primeros protocolos que se desarrollaron ni los primeros que empezaron a comercializarse. El primer protocolo que empezó a abrirse paso por Europa fue *Meters&More*. Dado que se trata de una tecnología que está en proceso de iteración y mejora y que no está firmemente implantada en ningún país, resulta importante conocer cuáles son las opciones disponibles en el mercado y cuáles son las diferencias entre unas y otras. Esta información permitirá indagar más en cuáles son las necesidades que aún no están cubiertas y cómo mejorar la tecnología existente.

La información que se ha recabado respecto a los distintos protocolos ha sido tanto de ámbito técnico como de ámbito comercial, intentando aportar algo de luz a la expansión que cada una de las tecnologías ha ido consiguiendo a lo largo del tiempo.

Respecto a la implementación práctica de *Meters&More*, está decisión se tomo en base a la falta de documentación técnica referente a las características de este protocolo, lo que hace muy complicado establecer ningún tipo de comparativa a nivel de capacidad y comportamiento en campo. Es por ello que, empleando el *framework* OMNet++ se ha diseñado un entorno de pruebas a fin de conocer en más detalle qué resultados caben esperar de su implementación.

1.3 ESTRUCTURA DEL DOCUMENTO

Este documento se puede dividir en tres partes principales. La primera parte (comprendida por los 4.4.1a Capítulo 7.) describe en detalle las características técnicas de los tres protocolos analizados (*PRIME*, *G3PLC* y *Meters&More*). Cada uno de estos protocolos se describe de manera consecutiva en los consiguientes capítulos de tal manera que se proporciona una visión técnica de las tecnologías a utilizar además de una contextualización en cuanto a qué parámetros son los que cobran mayor relevancia y cuáles son los principales problemas que se han intentado solventar en el entorno de las *smart grids*. Un resumen general se proporciona en el Capítulo 8. , discutiendo y presentando los protocolos que mejor encajan a la hora de realizar una implantación en según qué tipo de escenarios técnicos.

Por otro lado, tenemos una segunda parte comprendida por el Capítulo 9. donde se deja de lado la parte técnica de las tecnologías para detallar la parte comercial. De la misma forma que en los apartados anteriores que analiza cuál es el alcance comercial que ha conseguido cada uno de estos protocolos para entender cuáles son más populares en según qué lugares y, sobre todo, cuáles son las proyecciones de futuro de cada tecnología. Con ello lo que se persigue es proporcionar al lector una visión global que incorpore una pequeña previsión a futuro de lo que el día de mañana podría implicar cada una de ellas. De nuevo, todo este análisis queda resumido en el último punto de este capítulo.

Por último, y con el fin de proporcionar a este estudio una visión más práctica, además de aportar mayor documentación a este ámbito, la tercera parte queda comprendida por los Capítulo 10. y Capítulo 12. . En ellos se presenta la simulación desarrollada y los resultados obtenidos, siempre a vista de realizar una comparación con los parámetros de los otros dos protocolos.

Este documento está estructurado en 12 capítulos. Los siguientes párrafos describen de manera resumida el contenido que se trata en cada uno de ellos.

El Capítulo 2. revisa las tecnologías empleadas a lo largo del proyecto. Se centra en demostrar cuáles son las principales ventajas de éstas y justificar su uso y beneficios.

El Capítulo 3. describe el estado del arte de las *smart grids* indagando en cuáles son los protocolos que se han desarrollado, y cuáles son los avances que se han conseguido y los que tienen mayor proyección de futuro.

El Capítulo 4. define la metodología empleada a lo largo de todo el proyecto, así como las estimaciones de tiempo y tareas principales en las que se han dividido cada una de las distintas etapas.

El 4.4.1describe los aspectos técnicos principales de las capas física, MAC y de convergencia de *PRIME*, identificando cuáles son los principales bloques que lo componen y las distintas funcionalidades que proporciona.

El Capítulo 6. describe los aspectos técnicos principales de las capas física, MAC y de convergencia de *G3PLC*, identificando cuáles son los principales bloques que lo componen y las distintas funcionalidades que proporciona.

El Capítulo 7. describe los aspectos técnicos principales de las capas física, MAC y de convergencia de *Meters&More*, identificando cuáles son los principales bloques que lo componen y las distintas funcionalidades que proporciona.

El Capítulo 8. resume las principales características técnicas de los tres protocolos y establece una comparativa entre ellas.

El Capítulo 9. resume las principales características comerciales de los tres protocolos, estudiando cuál es su historia, su proyección de futuro y su alcance comercial. También establece una comparativa entre ellas.

Por último, el Capítulo 10. y Capítulo 11. presentan el modelo que se ha desarrollado y simulado en un entorno software junto con los resultados obtenidos respectivamente. En estas secciones se especifican las principales características del modelo, los detalles de su implementación y las conclusiones y luz que han podido arrojar sus resultados sobre el proyecto en su conjunto.

Para terminar, el Capítulo 12. cierra el documento con una pequeña sección de conclusiones y trabajos futuros que se recomiendan en base a lo realizado. En esta sección se identifican los puntos fuertes y flojos de todo el trabajo así como se evalúa el nivel de cumplimiento de los objetivos proyectos en los primeros capítulos.

Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS

En relación a las tecnologías empleadas es necesario diferenciar las dos áreas en las que se ha dividido el proyecto. En una primera sección encontramos todo el trabajo relacionado con la investigación de los principales protocolos a partir de sus especificaciones técnicas y publicaciones de interés. Al final de esta sección se encuentra una comparativa a nivel comercial y técnico de estas tecnologías a fin de proporcionar un mayor entendimiento de su alcance. Durante toda esta primera parte la tecnología empleada ha sido, por su puesto, el motor de búsqueda de Google, tanto navegador como Google Académico, con el fin de encontrar el mayor número de publicaciones y descripciones que enriquecieran al máximo este proyecto.

En una segunda parte encontramos el diseño e implementación de una de estas tecnologías a fin de conseguir reducir el vacío informativo que hay a su respecto dentro del mundo de las redes inteligentes. Es en esta segunda parte donde se han empleado tecnologías propiamente dichas.

2.1 OMNET ++

OMNet++ es un simulador, basado en módulos, de redes. Está orientado a objetos y se emplea para el modelado de tráfico de redes de telecomunicaciones, protocolos, arquitecturas, etc.

Este sistema de modulación proporciona un núcleo de simulación que contiene todas las rutinas que se encargan de controlar tanto las simulaciones como las bibliotecas de simulación e interfaces de usuario. Se trata de la descripción de la topología del modelo en lenguaje tipo NED, la definición de mensajes y el código de los módulos simples.

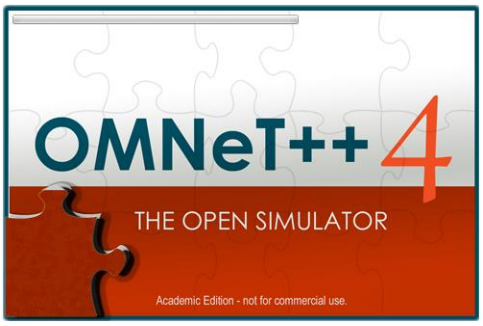


Figura 7. Logo del producto OMNet++ v4 [5]

El tipo de construcción que se utiliza cuando se emplea OMNet++ es una construcción modular. Esto significa que OMNet ++ proporciona una serie de módulos básicas con funcionalidades básicas sobre las cuales se estructuran comportamientos más complejos para poder generar así redes más complejas y realistas con una estructura jerárquica anidada [6].

La construcción de un modelo de simulación con OMNet++ se resumen en:

- Descripción de la estructura, en concreto los módulos y la relaciones utilizando lenguaje NED.
- Implementación de módulo simples utilizando C++ como lenguaje.
- Generación del modelo, donde se compilan los módulos y se en establecen las relaciones con la biblioteca de simulación.
- Configuración de los parámetros de simulación.

Otra de las ventajas de OMNet++ es que permite almacenar resultados estadísticos para poder elaborar gráficos que ilustren parámetros como el rendimiento, tiempo de propagación, tiempo de procesamiento, etc. Este tipo de parámetros resultan de vital importancia cuando se implementa un protocolo de comunicaciones, a fin de poder establecer comparativas con protocolos anteriores.

2.2 C++

Como lenguaje de programación se ha empleado C++. Éste se trata de una extensión del lenguaje C que posee características de los lenguajes de programación orientada a objetos. En este sentido se trata de un lenguaje híbrido.

Figura 8. Logo del lenguaje C++ [6]

Entre las ventajas de este lenguaje se encuentran las siguientes:

- Existen compiladores para diferentes sistemas operativos, esto representa uan ventaja en el ámbito de la portabilidad ya que significa que un mismo código puede ser compilado en distintas plataformas si se aísla el core del back-end de la interfaz gráfica.
- Se trata de una lenguaje muy robusto y versátil, actualmente utilizado para la creación de software, sistemas operativos, utilidades, compiladores, depuradores e IDEs.
- Una de sus principales características es la eficiencia de su código.
- Permite una mejor gestión y control de la memoria y una buena administración de recursos de computación.

De entre las desventajas de este lenguaje encontramos:

- Emplea librerías dinámicas. Este concepto es muy complejo ya que obliga al desarrollador a encargarse de la gestión de memoria de las librerías. En otros

lenguajes orientados a objetos como Java y .Net esta tarea se simplifica para el usuario.

- La mala gestión o el desconocimiento del programador puede llevar a error de gestión de memoria conocidos como *memory leaks*.

Capítulo 3. ESTADO DE LA CUESTIÓN

Se podría decir que la tecnología *Smart Grid* viene de la necesidad de medir, desde el mismo punto en que la red eléctrica, el consumo de energía a fin de ayudar a las empresas que se encargan de prestar el servicio a monitorizar la red y poder aplicar una tarificación mucho más acertada. Con este objetivo en mente, Samuel Gardiner patentó el primer medidor eléctrico que consistía en un reloj y un electromagneto que iniciaba y finalizaba la medida para poder determinar cuánto tiempo se utilizaba la electricidad. El único problema es que no medía la cantidad de corriente.

Más adelante, en 1879, J.B. Fuller inventó otro medidor similar pero esta vez basado en la corriente alterna [7]. El invento estaba basado en la idea de que, al fluir como electricidad, ésta haría vibrar una armadura entre dos bobinas, de nuevo midiendo únicamente el tiempo de consumo.

Thomas Edison desarrolló en 1882 el primer medidor propiamente dicho. Su invento consistió en dos electrodos conectados cuyo peso variaba en función de la cantidad de energía consumida. Midiendo este peso una vez al mes se podía establecer el costo del servicio.

En 1886, Edwin Weston inventó un amperímetro de precisión portátil que, desafortunadamente, no permitió medir el consumo de electricidad de manera directa [8]. Al menos, no hasta que Elihu Thompson desarrolló el vatímetro, mejorado más adelante y basado en un medidor de potencia cuyo sistema es en el que están basados muchos de los medidores de la actualidad.

El mercado ha ido modificando el tipo de contador, pasando de contadores electromecánicos a otra versión en los 90 que incluía circuitos integrados y tecnologías de comunicación, los medidores electrónicos. Éstos últimos son los precursores de AMR (*Automated Meter Reading)*.

El EEM (*Electronic Energy Meter*) digitaliza el voltaje y corriente mediante un conversor AD y calcula la potencia instantánea consumida. El EEM se encarga después de combinar esta información con el tiempo, de tal manera que lo que obtenemos al final es la energía consumida en kilovatios-hora.

Por otro lado, los AMR son una tecnología de medición electrónica pero unidireccional que permite recoger información del lado del usuario hacia el de la empresa a fin de poder procesarla y utilizarla para la facturación, elaboración de estadísticos, históricos, etc. Sin embargo, hoy en día ya no se conoce la tecnología AMR sino que se conoce la tecnología AMI, medidores inteligentes considerados los sensores por excelencia de las *Smart Grids* [8].

Smart Grid utilizada las TI para modernizar todo lo relacionado con las redes eléctricas, tanto el concepto como la funcionalidad. El primer proyecto que se conoció fue Telegestore. Un proyecto desarrollado en Italia en los años 2000 que instaló y puso en operación medidores inteligentes en unos 27 millones de residencias. Sin embargo, la primera vez que se utilizó este término no fue hasta el año 2005.

A continuación, se presentan el modelo conceptual y topología de una red inteligente. Se puede observar que integra todos los componentes de la red eléctrica ayudándose para ello de sistemas de telecomunicaciones. Además, también incluye elementos transversales como los que se relacionan con el mercado del sector.

Un aspecto importante de este tipo de redes es que, frente a las redes tradicionales, estas emplean un sistema descentralizado, incorporando nuevas fuentes de generación, la participación directa del consumidor final, y un acceso universal. Es decir, a día de hoy las redes inteligentes cumplen los siguientes puntos [9]:

- Observabilidad: permiten que se pueda monitorizar el estado de la red en tiempo real de una manera precisa gracias a la implementación de sensores y tecnologías avanzadas de medición.

- Controlabilidad: gracias a la característica anterior se puede llevar a cabo un control exhaustivo de la potencia del sistema.
- Análisis y actuación: proporciona mayor visibilidad y transparencia lo cual permiten llevar a cabo análisis basados en mejores datos y, por tanto, tomar decisiones de una manera más legítima y mejor estructurada.
- Auto aprendizaje: este tipo de redes implementan la inteligencia artificial que permite que se realicen auto diagnósticos para la localización de fallas y que el propio sistema lo suficientemente inteligente como para prevenir cualquier error y tomar nota de los mecanismos de prevención y mala praxis que se deben abandonar.
- Integración con otro tipo de energía: principalmente energías renovables. Este tipo de redes son compatibles con todo tipo de energía, desde la solar y eólica hasta la de micro generación e incluyendo sistemas para vehículos eléctricos, casas inteligentes, etc.

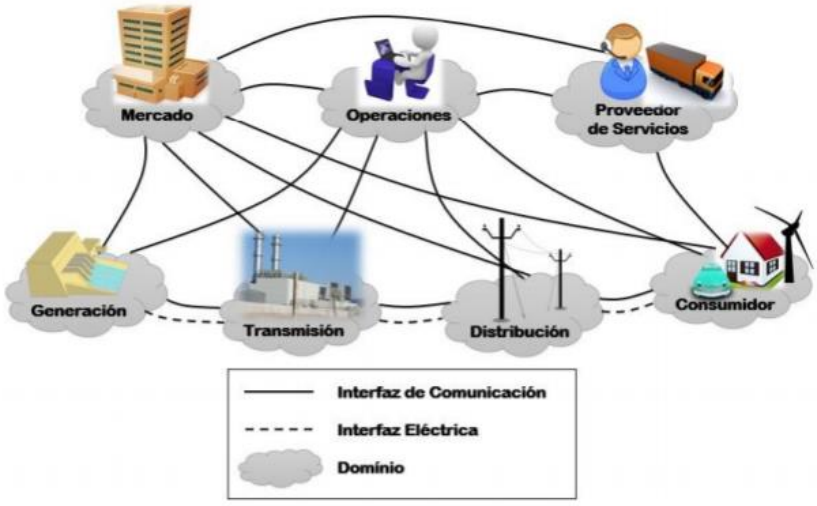


Figura 9. Modelo conceptual de una red inteligente [9]

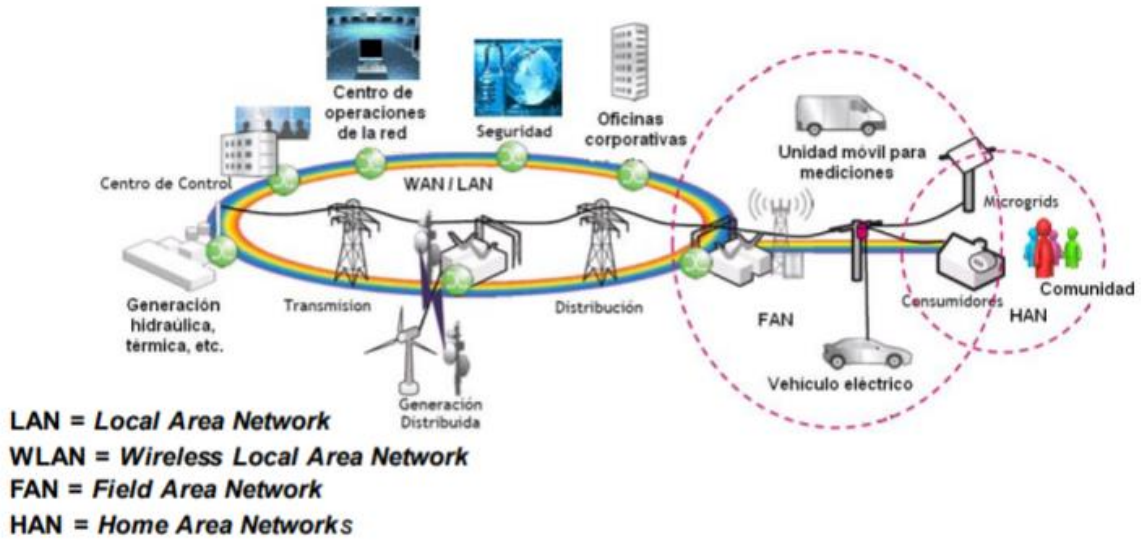


Figura 10. Topología [9]

En la tabla a continuación se presentan las principales características que poseen las redes inteligentes que ya han sido desplegadas o que están en proceso de despliegue.

Tabla 2. Características de las Smart Grids [7]

Características	**Descripción**
Automatización, inteligencia y control	A todos los niveles: - Sensores y actuadores. - Tecnologías de medición - Automatización distribuida
Posibilidad de inclusión de todo tipo de energía y métodos de almacenamiento	- Fuentes de energía en el local del usuario - Energías renovables - Almacenamiento - *Plug and Play*
Optimización	- De la capacidad de la red - Mantenimiento eficiente gracias a la monitorización - Ajuste de los dispositivos para minimizar cualquier tipo de pérdidas

El usuario como elemento clave en la gestión	- Información útil de cara al usuario con posibilidad de toma de decisiones en algunos puntos de la gestión - Si el usuario pose algún tipo de generación, posibilidad para introducir su energía dentro de la red
Nuevos productos, servicios y mercados	- Mayor variedad de opciones a elegir para el usuario dependiendo de la calidad de la energía, tiempo de respuesta, etc. - Mayor flexibilidad para todos los involucrados para modificar las características del negocio

El subsistema AMI, el más extendido dentro de las redes inteligentes, posee las siguientes funcionalidades:

- Medición cuantitativa de precisión.
- Control y calibración compensando variaciones de tensión.
- Envío de datos y recepción de comandos gracias a la comunicación.
- Visualización para el usuario final.
- Sincronización con el centro de control u otros sistemas.

En base a estas funcionalidades nos encontramos con que las características claves de los medidores, y los protocolos que los conforman son las siguientes:

- Fijación de precios en función del tiempo.
- Abastecimiento de datos relaciones con el consumo.
- Notificación de errores.
- Permisión de comandos de operación tipo encendido y apagado de manera remota.
- Establecimiento de límites de carga en función de la tarifa contratada.
- Detección de irregularidades.
- Comunicación con otros dispositivos.

- Contribución a la mejora ambiental y eficiencia energética.

En el ámbito que más nos afecta dentro de este trabajo, el de las comunicaciones en las redes inteligentes, los sistemas de telecomunicaciones desempeñan uno de los papeles más importantes en todos estos entornos. Existen numerosos sistemas de telecomunicaciones y para poder identificar cuál es el que mejor se ajusta a las necesidades de cada escenario es necesario identificar los siguientes factores:

- Velocidad de transmisión.
- Restricciones de acceso.
- Confidencialidad, autenticidad y accesibilidad.
- Representación de datos y tipo de visualización de la red.
- Rentabilidad.
- Potencial de expansión.

En términos de transmisión de información es importante prestar especial atención a la latencia, y confiabilidad. Las dimensiones de estos requerimientos son diferentes en función de cómo de inteligente es la red eléctrica en donde se va a llevar la implantación. En concreto estas son las clasificaciones que se consideran.

- Alta velocidad de transmisión (56 kbps a 128 kbps) si se desean mediciones avanzadas como, por ejemplo, la vibración de la línea e transmisión o la temperatura del transformadores de una subestación.
- Baja latencia para mejorar la estimación de la situación en tiempo real.
- Alta confiabilidad (99 a 99.99%) para garantizar que los datos son correctos y tomar decisiones acordes a éstos.

Para poder cumplir con estos requisitos tan exigentes se han desarrollado dos sistemas denominados WAMS (*Wide Area Measuremente System*) y WACS (*Wide Area Control Systems*).

WAMS, introduce capacidades de monitorización de red avanzadas gracias al uso de fasores como unidades de medición para recoger datos de la potencia dinámica de forma

sincronizada mediante GPS con una velocidad de muestreo muy alta. Este sistema permite mejorar la seguridad, estabilidad y confiabilidad del sistema de potencia.

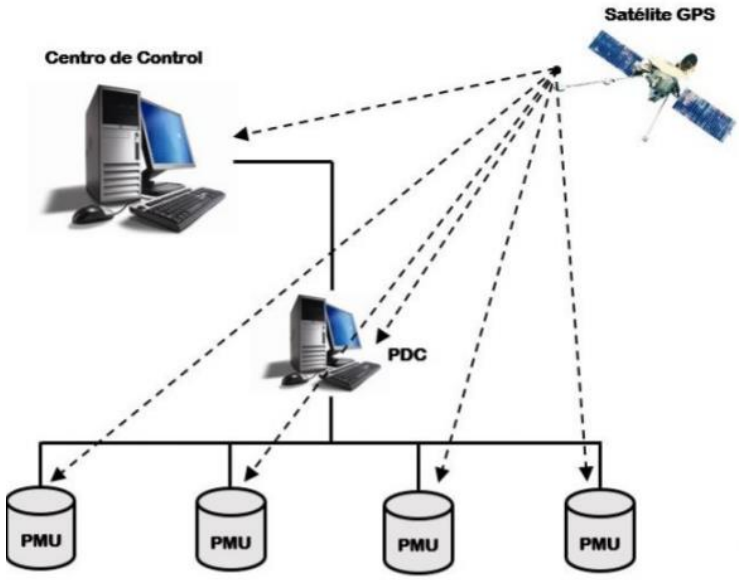


Figura 11 . Arquitectura del sistema WAMS [10]

Por otro lado, el sistema WACS es un sistema de control que utiliza información recogida por WAMS y ejecuta distintas acciones orientadas a la estabilidad en tiempo real y el control de los niveles de tensión.

Tras conocer cuál son los principales problemas a los que está poniendo solución las redes inteligentes, y cuales son sus principales características, también es importante conocer qué está pasando a nivel comercial en este mercado.

A continuación, se muestran una serie de imágenes obtenidas de la Comisión Europea que reflejan el estado de estas redes teniendo en cuenta factores como el estado de los proyectos y las inversiones que están haciendo en las tecnologías.

Es importante remarcar que, aunque la información que se muestra proviene solamente de datos europeos, no es sólo Europa donde se están desplegando este tipo de redes. Existen numerosos proyectos en Latinoamérica, Japón, Australia, EEUU, entre otros.

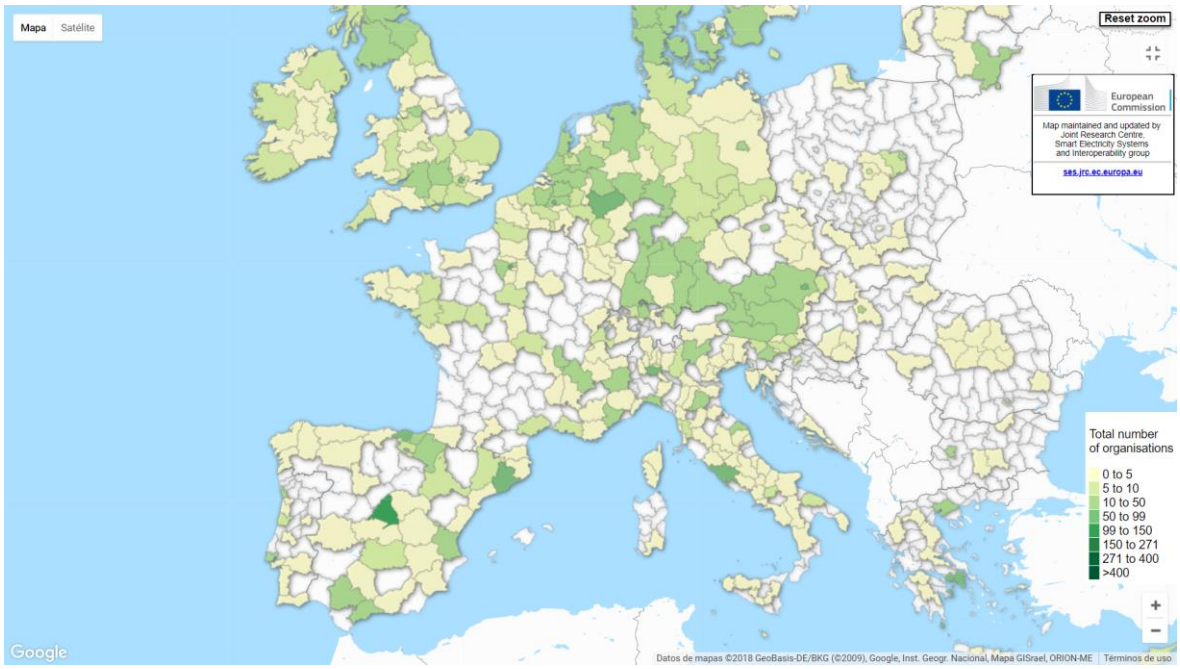


Figura 12. Organizaciones desarrollando proyectos de redes inteligentes [18]

Figura 13. Densidad de proyectos en investigación y desarrollo [18]

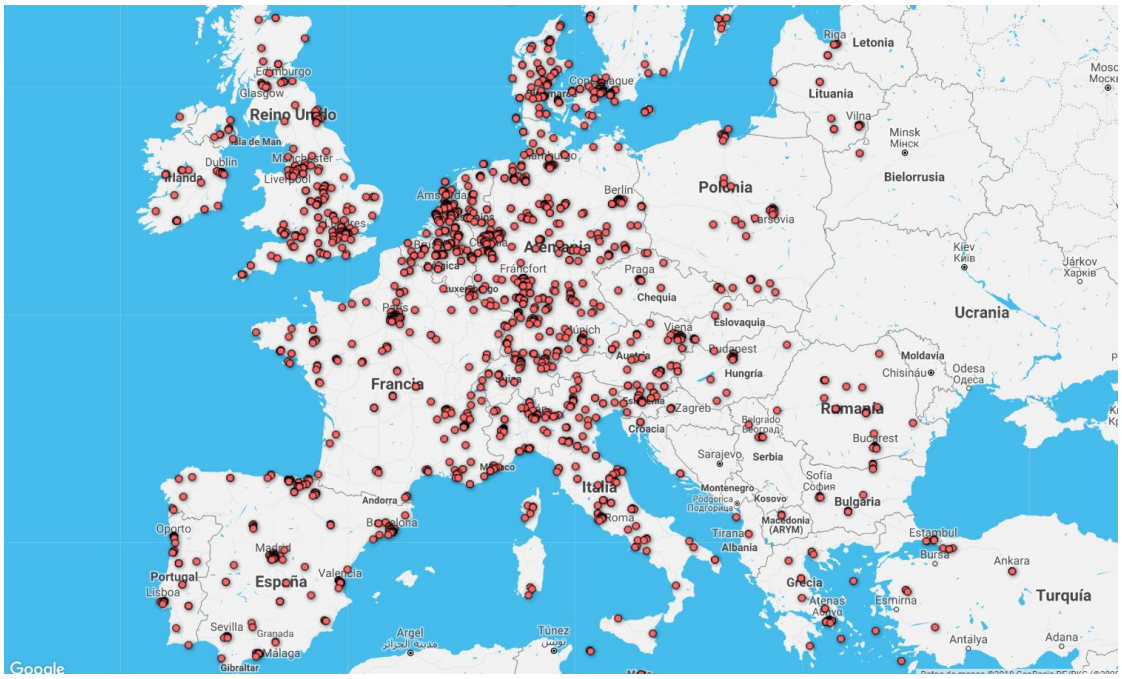


Figura 15. Densidad de proyectos en pruebas y demostraciones [18]

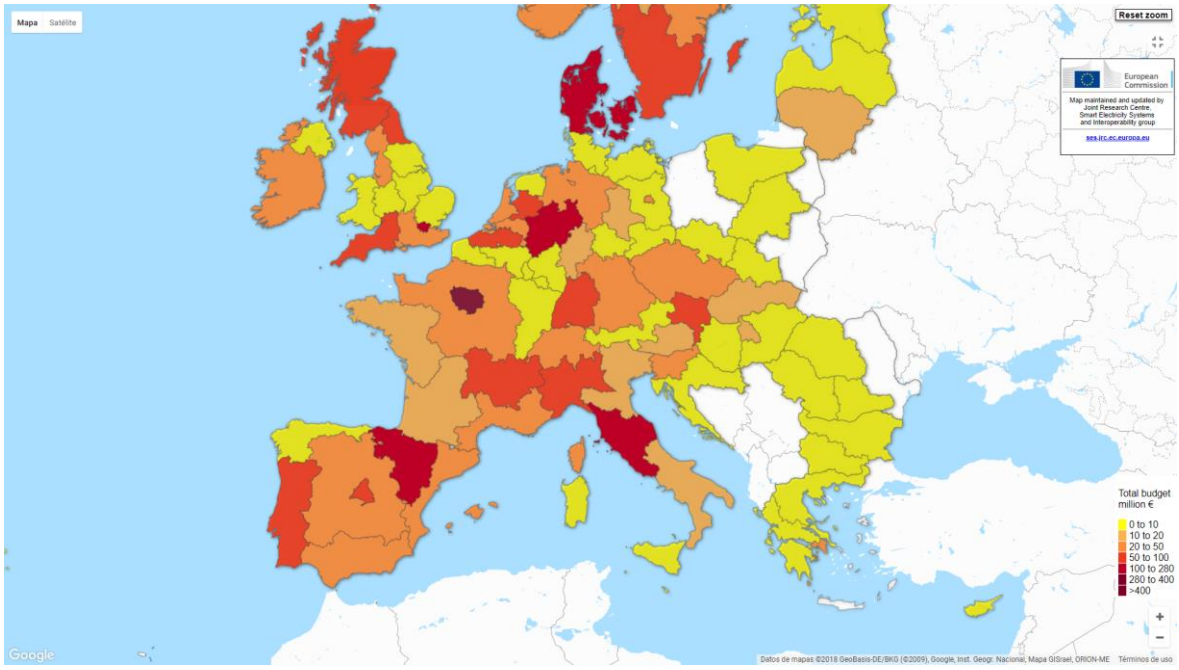


Figura 14. Presupuesto por región destinado a la investigación e implantación de redes inteligentes [18]

Capítulo 4. DEFINICIÓN DEL TRABAJO

4.1 JUSTIFICACIÓN

En la actualidad, el coste de la electricidad es un tema que está a la orden del día. Las empresas del sector se preguntan cómo mejorar el sistema energético español, tanto desde el punto de vista de la ventaja competitiva, como desde el punto de vista del mayor control de precios. Es por ello que, llegados a esta situación, las empresas se preguntan cómo pueden emplear las tecnologías a su alcance para mejorar y optimizar todo un sistema que necesita una clara renovación. Es este el punto en el nace el concepto de la red inteligente y son muchas las razones por las que es necesario seguir invirtiendo en su desarrollo y expansión.

La flexibilidad es una característica fundamental que proporciona esta nueva generación. La tecnología ayuda a mejorar los flujos de energía de tal manera de la gestión de picos en la demanda se gestionan de una forma más inteligente y eficiente. Las *smart grids* permiten que todo el sistema se adapte a las necesidades tan volátiles y cambiantes de lo usuarios gracias a que disponen de información en tiempo real de todos los puntos que forman parte de la cadena.

Pero no solamente suponen un avance en la gestión de la energía. Un punto muy doloroso en todo un sistema tan antiguo como es el de la red eléctrica es el mantenimiento. Hasta el momento la mayor parte del mantenimiento se hacía de manera reactiva. Es decir, una vez que surgía una avería o había un fallo en el sistema se empleaban medidas que aliviaran al máximo los daños colaterales surgidos de este error. Este nuevo mundo de redes inteligentes permite que las empresas lleven a cabo un mantenimiento preventivo, uno mucho más eficaz que no reacciona ante un error, sino que evita que se suceda ese error poniendo soluciones antes de que aparezca. Todo ello se consigue gracias a esta monitorización de la que se hablaba.

Pero las *smart grids* no sólo buscan dotar de soluciones a las empresas, sino también a los usuarios finales. Éstas les proporcionarán instrumentos para que puedan gestionar de una manera óptima su consumo, posibilitándoles información sobre la cantidad que se consume, cuándo y cuánto cuesta. Incluso, otra de las funcionalidades que más éxito está suponiendo, es la emplear estos sistemas en combinación con sistemas de autoproducción, de tal manera que se puedan combinar de forma sencilla el autoconsumo con el consumo de la red eléctrica. Todo esto viene bajo el nombre de generación distribuida.

La generación distribuida consiste en la micro generación de electricidad gracias a pequeñas fuentes distribuidas por la ciudad. Se trata de un sistema de cooperación con las grandes centrales de tal manera que se dota a las ciudades de mayor autosuficiencia. Dentro de este planteamiento también se incluye la generación a partir de energías renovables. Esta estrategia busca reducir las pérdidas en la distribución al situar más cerca del consumidor final las fuentes de energía.

Es por todo lo anterior que se entiende que es necesario promover una cultura basada en esta tecnología, donde el usuario final conozca, y tenga a su disposición la información necesaria para conocer, todos los aspectos de las principales tecnologías y protocolos que se han desarrollado y que están disponibles para su comercialización.

A pesar de que en España ya se han llevado a cabo implantaciones, sigue sin ser un tema claro y fácil de entender para el consumidor medio. Esta es la carencia que este trabajo pretende suplir gracias a la aportación de una documentación, aunque sí técnica, más liviana que las propias especificaciones técnicas que los proveedores ponen a disposición del cliente en su página web. De esta manera el usuario tendrá a su disposición información más clara que le permita establecer mejores juicios y comprender mejor cuáles son las ventajas que le proporciona un protocolo frente a otro y cuáles son las tecnologías que mejor se ajustan a sus circunstancias.

Además, también existe una carencia clara de documentación comparativa que establezca las tres tecnologías más comunes y defina cuáles son los pros y contras de cada una de ellas en todos sus aspectos.

4.2 OBJETIVOS

Los objetivos generales de este proyecto buscan contribuir a la documentación acerca de las tecnologías actualmente disponibles para la implementación de redes inteligentes basadas en PLC. Hay dos líneas principales dentro de las cuales se pueden categorizar los objetivos. La primera hace referencia al ámbito técnico y las especificaciones técnicas propias de cada solución. La segunda hace referencia al aspecto comercial en términos de implantación según qué solución, en función de los parámetros que posea el escenario. Los objetivos concretos se pueden resumir en los siguientes puntos:

- **Comprensión, análisis y síntesis de los principales parámetros técnicos de los tres protocolos más extendidos en el ámbito de las redes inteligentes.** Este objetivo pretende contribuir a la comunidad técnica gracias a la aportación de una documentación de lectura sencilla y clara que identifique cuáles son los aspectos más relevantes en el plano técnico de cada uno de los protocolos. La información tiene que ser tal que, sin necesidad de utilizar la especificación técnica, el lector sea capaz de implementar cualquiera de las tres capas estudiadas, física, mac y de convergencia, utilizando únicamente la información que se presenta en este documento. Para ello, se tiene que garantizar que los principales componentes y sus características se incluyen sin perder ningún tipo de precisión, pero al mismo tiempo de tal manera que se eliminen parte de las barreras que impiden que personas que no sean especialistas o dominen el sector comprendan cuáles son los principales funcionamientos de cada uno de los bloques. Además de los bloques fundamentales también será importante incluir las primitivas y bloques lógicos que intercambian cada uno de los niveles, así como información de las premisas sobre las que se basan las comunicaciones, por ejemplo, el tipo de conexión entre los dispositivos, el tipo de acceso al medio o el tipo de medio físico utilizado para las comunicaciones. Todo ello permitiría simular un entorno de pruebas completamente funcional y realista cuyos resultados podrían utilizarse para establecer comparativas y análisis sobre el rendimiento, latencia, colisiones, etc.

- **Realizar una comparación a nivel teórico de las características técnicas de las tres soluciones, proporcionando una visión más completa sobre el estado actual del sector y sus posibilidades**. Este estudio no se limita a dar información generalista sobre cada uno de los protocolos, sino que también incluye una comparación a nivel técnico de los principales indicadores de rendimiento de los protocolos basándose en estudios previos y publicaciones que se encuentren disponible. De nuevo, el fin es conseguir incorporar y recabar toda la información posible y reunirla en un único documento al que además se incluirán conclusiones propias y análisis propios que se hayan ido haciendo durante la síntesis de la documentación.
- **Estudiar, a nivel comercial, cuál es el nivel de implementación y aceptación de cada una de las soluciones y cuáles son sus expectativas de crecimiento de cara a los próximos años.** De acara a incluir un aspecto más comercial dentro del documento, también se ha realizado un análisis que indaga sobre cómo de extendidos están los distintos protocolos y cuáles son los planes de futuro que cada una de las compañías o grupos de compañías promotoras tienen planteados para los próximos años. El objetivo último es siempre proporcionar una visión global del estado de los protocolos de tal manera que, en caso de que se piense en realizar una nuevo despliegue o una compañía desee conocer cuáles son los principales jugadores dentro del mercado de las redes inteligentes, disponga de una documentación completa que identifique las razones por las que cada protocolo ha conseguido según qué alcance y cuáles podrían ser los principales problemas o retos a nivel de comercial de iniciar un nuevo despliegue en algunos países y regiones.
- **Comparar las ventajas y desventajas de la implantación de las tres soluciones estableciendo distintos escenarios y definiendo las condiciones óptimas bajo las que cada solución puede proporcionar un mayor rendimiento.** De la misma forma que con el aspecto técnico, resulta interesante conocer cuáles son las circunstancias que favorecen la implementación de cada uno de los protocolos a nivel comercial y a nivel técnico, consiguiendo identificar los puntos fuertes y débiles de

cada una de las tecnologías y entendiendo mejor cuáles son las razones que han generado el mapa de despliegue y desarrollo que existe actualmente.

Sin embargo, los objetivos de esta documentación no se limitan únicamente a los presentados anteriormente puesto que, como se ha ido explicando en apartados anteriores, este proyecto ha constado de dos partes donde la segunda a contribuido al análisis de la primera. Debido a la falta de documentación existente respecto a uno de los tres protocolos se ha decidido estudiar a nivel práctico este protocolo gracias a su implementación en un simulador. De esta segunda parte del proyecto el objetivo principal que se perseguía era conseguir establecer un entorno de simulación lo más preciso posible que, implementado en base a la documentación recopilada en este documento, permitiese obtener medidas de rendimiento, latencia, tiempo de procesamiento, etc. Con esta información se completa el estudio realizado a lo largo del documento proporcionando así un visión completa y detallada sobre todos los protocolos estudiados.

4.3 METODOLOGÍA

La metodología que se ha seguido comienza con una etapa larga de búsqueda de información, lectura de manuales técnicos y especificaciones sobre cada uno de los tres protocolos que se estudian. En esta primera etapa se pretende entender en profundidad cuáles son las ventajas de cada uno de los protocolos, así como las diferencias que hacen que cada uno sea idóneo en un escenario u otro.

Una vez se haya conseguido una visión global y suficientemente precisa de la parte técnica, se pasará a documentar cuál es el alcance comercial de los mismos. Con ello se busca comprender qué tecnologías han sido más exitosas y por qué, así como en qué países priman para entender cuáles son los factores que afectan a su implantación.

Por último, y con la intención de proporcionar mayor claridad sobre el ámbito técnico, se pasa a realizar una simulación de uno de los protocolos utilizando para ello la

información recopilada en apartados anteriores a fin de conseguir un escenario lo más fiable y preciso posible.

Para poder desarrollar todas las tareas anteriores siguiente una organización clara y estableciendo distintos hitos se va a utilizar un método de desarrollo conocido como Scrum.

4.3.1 SCRUM

Scrum es un proceso donde se aplican una serie de buenas prácticas que permiten trabajar de manera colaborativa y obtener el mejor resultado posible de un proyecto. De entre estas buenas prácticas encontramos:

- Desarrollo incremental de los requisitos en bloque de tiempo cortos y fijos, con iteraciones de hasta dos semanas si así fuera necesario.
- Priorización de los requisitos por valor para el cliente y coste de desarrollo.
- Control empírico del proyecto de tal manera que el cliente revisa periódicamente los resultados que se consiguen. Esto aumenta la participación del cliente en el desarrollo del proyecto, fundamental para garantizar el avance y cumplimiento de las necesidades del usuario del proyecto.

En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales. Planificación y Estimación Económica

Scrum se caracteriza por su ejecución en bloques de tiempo cortos y fijos donde se debe proporcionar un resultado completo, una funcionalidad completa, que se irá desarrollando y mejorando a medida que se vayan realizando más iteraciones.

Debido a todo lo explicado anteriormente este método de trabajo se vuelve idóneo para un proyecto cuya tecnología se innova constantemente y en el que resulta relativamente sencillo poder conseguir cierta funcionalidad lo más simplificada posible para posteriormente ir completándola.

En este caso el equipo estaba formado únicamente por el director de proyecto y el programador que realizaban reuniones semanales en las que se comprobaban la medida en que se habían cumplido los trabajos previos y establecían las nuevas líneas de trabajo para la siguiente reunión.

4.4 PLANIFICACIÓN Y ESTIMACIÓN ECONÓMICA

En términos de estimación es necesario resaltar que, gracias a la amplia penetración en equipo corrientes de plataformas como OMNet++ no se necesita disponer de un equipamiento específico para el desarrollo del proyecto. Es decir, el único coste que se tendrá en cuenta durante la evaluación es el tiempo dedicado por cada uno de los miembros del equipo.

Tabla 3. Actividades y duración realizadas durante el proyecto

Tarea	***Días***	***Horas***
Defición del proyecto	3	9
Introducción al tema	8	24
Análisis de la especificación PRIME	10	30
Síntesis y documentación de PRIME	5	15
Análisis de la especificación G3-PLC	13	39
Síntesis y documentación de G3-PLC	7	21
Análisis de la especificación M&M	5	15

Síntesis y documentación de M&M	2	6
Comparativa técnica de los tres estándares	15	45
Análisis del alcance comercial de PRIME	2	6
Análisis del alcance comercial de G3-PLC	1	3
Análisis del alcance comercial de M&M	1	3
Comparativa comercial de los tres estándares	1	3
Familiarización con OMNet++	10	30
Definición de las capas MAC y LLC de M&M	15	45
Modelado	25	75
Tests	7	21
Elaboración de la memoria del modelado	20	60
Revisión de la memoria	5	15
Elaboración de la presentación	5	15
Total		***480***

Para hacer la estimación se han contabilizado los días empleados para cada una de las actividades y se ha identificado una aproximación de 3h por día como tiempo dedicado en exclusiva al proyecto. Todo ello da lugar a una estimación de 480 horas de proyecto. Este tiempo se entiende como el tiempo empleado por el desarrollador principal. Sin embargo, dentro del equipo existen otro miembro que es el director de proyecto. El tiempo de trabajo estimado de este se ha contabilizado como un 20% del trabajo del desarrollador. Todo ello da lugar al siguiente desglose de costes.

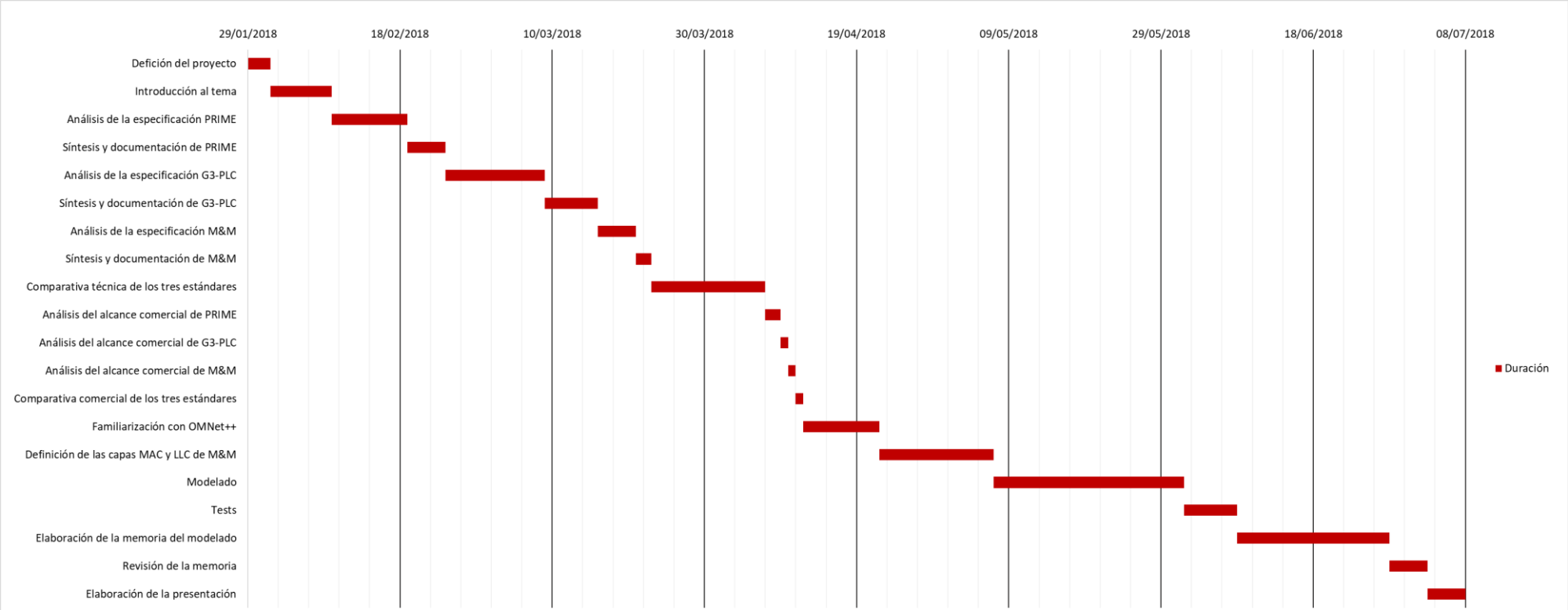
Tabla 4. Desglose de costes

Miembro	***Horas***	***Coste/hora***	***Coste total***
Desarrollador	480	30	14400
Jefe de proyecto	96	55	5280
Total			***19680***

Por último, y dado que se trata de un proyecto de investigación, no se incluye un estudio de viabilidad puesto que no es un producto ni servicio lo que presenta el proyecto. Es por tanto muy complejo identificar cuáles pueden ser los posibles impactos qué tenga y mucho más medirlo en términos de ganancias o pérdidas.

En lo referente a la planificación, se ha desarrollado un cronograma con las principales tareas en las que se ha desglosado el proyecto y el tiempo empleado en la realización de cada una de ellas. A modo de resumen, debajo del diagrama, se puede encontrar una tabla que establece, en días, el tiempo final utilizado.

4.4.1 CRONOGRAM



	Elaboración de la presentación	Revisión de la memoria	Elaboración de la memoria del modelado	Tests	Modelado	Definición de las capas MAC y LLC de M&M	Familiarización con OMNet++	Comparativa comercial de los tres estándares	Análisis del alcance comercial de M&M	Análisis del alcance comercial de G3-PLC	Análisis del alcance comercial de PRIME	Comparativa técnica de los tres estándares	Síntesis y documentación de M&M	Análisis de la especificación M&M	Síntesis y documentación de G3-PLC	Análisis de la especificación G3-PLC	Síntesis y documentación de PRIME	Análisis de la especificación PRIME	Introducción al tema	Defición del proyecto
Fecha de Inicio	3-jul.	28-jun.	8-jun.	1-jun.	7-may.	22-abr.	12-abr.	11-abr.	10-abr.	9-abr.	7-abr.	23-mar.	21-mar.	16-mar.	9-mar.	24-feb.	19-feb.	9-feb.	1-feb.	29-ene.
Duración	5	5	20	7	25	15	10	1	1	1	2	15	2	5	7	13	5	10	8	3

Figura 16. Cronograma

Capítulo 5. PRIME

5.1 DESCRIPCIÓN GENERAL

PRIME es una solución para sistemas basados en la tecnología PLC que se desarrollan en la banda CENELEC-A y que utiliza OFDM como esquema de modulación. En la *Figura 17* se presentan las distintas capas que se van a tratar a lo largo de este documento y que pueden verse resumidas en tres, La capa física (PHY), la capa de control de acceso al medio (MAC) y la capa de convergencia (CL).

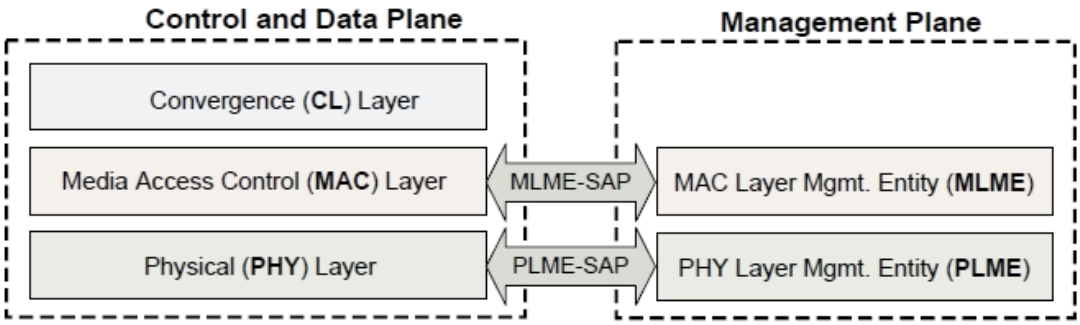


Figura 17. Capas que comprende la especificación PRIME [11]

La capa CL se encarga de llevar cabo funcionalidades de mapeo, de forma que cualquier tipo de tráfico pueda traducirse en su correspondientes MPDU. La capa MAC proporciona funcionalidades de acceso al medio, gestión del ancho de banda, gestión del establecimiento y mantenimiento de la topología a fin de poder resolver las direcciones que se vayan tratando. Por último, la capa física se encarga de recibir y transmitir MPDUs entre nodos utilizando la modulación OFDM. Se ha decidido utilizar esta modulación por las siguientes razones:

- Se adapta de manera natural a canales con frecuencias selectivas, un escenario muy común en este tipo de sistemas.
- Proporciona mucha robustez frente al ruido impulsivo. De nuevo una característica común de este tipo de sistemas debido a la variación en amplitud que sufren las señales.
- Es capaz de conseguir una eficiencia muy grande utilizando especificaciones muy sencillas en el transmisor y en el receptor.
- La especificación técnica define distintos esquemas para la codificación de paquetes de tal forma que la tasa de bit puede adaptarse a las características del medio gracias a una serie de instrucciones que se dan desde la capa MAC.
- Capa Física (PHY)

La capa física utiliza frecuencias que se mueven en la banda que va desde los 3kHz hasta los 500 kHz, de esta forma se conseguir tener una especificación que se puede adaptar fácilmente a distintas regulaciones en función del país. Sin embargo, las frecuencias que se encuentran por debajo de los 40 kHz traen consigo numerosos problemas dentro de los cuales se destacan:

- La impedancia que los transmisores ven queda por debajo de 1Ω.
- El ruido de fondo coloreado afecta con mayor intensidad a las frecuencias más bajas.
- Las salas de medida se ven afectas por el comportamiento, en términos de consumo, del cliente dando lugar a escenarios con características muy difíciles de predecir en términos de variación en tiempo de la función de transferencia y ruido.

Es por ello que la capa PHY de PRIME se desenvuelve principalmente entre los 41.992 kHz y los 471.6796875 kHz. Este rango se divide en ocho canales y en cada canal se aplica modulación OFDM, donde las señales viajan en símbolos de 2240 de duración, transmitidos a través de 97 sub-portadoras equiespaciadas entre sí. De estos 2240 µs, 192 se comprimen en forman de prefijo cíclico.

Además de todo ello, PRIME utiliza modulación diferencial y da la posibilidad de utilizar tres tipos de constelaciones, DBPSK, DQPSK O D8PSK.

Tras esta modulación, la especificación define un *scrambler* que se emplea para evitar que existan grandes secuencias de bits idénticos.

Finalmente, se aplica un *convolutional encoder* con una tasa de ½ junto con un bit *interleaving*. Esta sección se utiliza a fin de evitar errores en ráfaga durante la transmisión, pero dado que sólo son necesarios en ciertos escenarios, su uso es opcional y en caso de que el canal sea lo suficientemente bueno, se pueden obviar.

El funcionamiento en términos generales de esta capa es el siguiente. La capa PHY recibe un MPDU de la campa MAC y genera un paquete PHY. Sólo a la cabecera se le aplica el CRC (ya se le ha aplicado al *payload* en la capa MAC), y tras él se llevan a cabo el CC siempre y cuando el FEC se haya activado con anterioridad. Tras ellos llega el *scrambler*, que se aplica tanto a la cabecera con al *payload*, repeticiones adicionales en caso de que se el FEC esté activado (a fin de dar mayor robustez al paquete) y después el *interleaver*. Una vez que es estamos en este punto sólo nos queda modular el paquete utilizando algunas de las tres modulaciones disponibles y aplicar OFDM. Lo último que se añade es el prefijo cíclico. En la *Figura 18* se pueden ver todos estos bloques de una manera más clara.

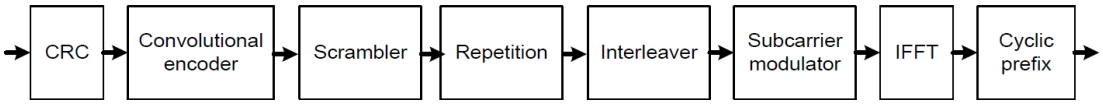


Figura 18. Diagrama de bloques de PRIME [11]

Existen distintos tipos de paquetes en términos de formato, que se pueden utilizar en PRIME, tipo a y tipo B. La principal diferencia entre ellos viene marcada por la duración se sus partes principales, así como el número de símbolos que se incluyen. En la *Figura 19* y en la *Figura 20* se puede ver esta información resumida. En el caso del paquete tipo A el valor de M se identifica en la cabecera y es como máximo 63. Para los paquetes tipo B cómo máximo puede valer 252.

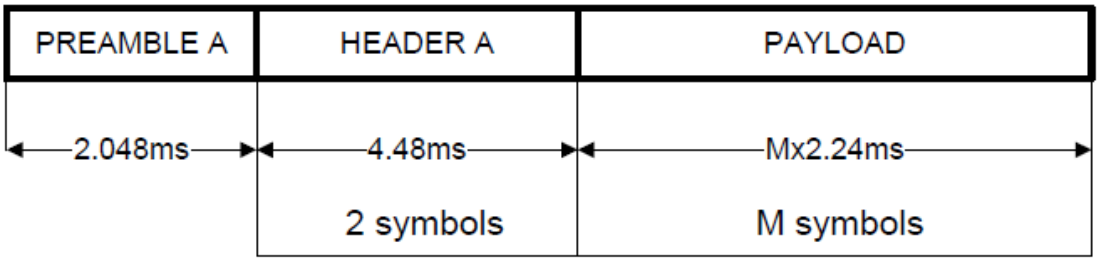


Figura 19. Configuración de un paquete tipo A

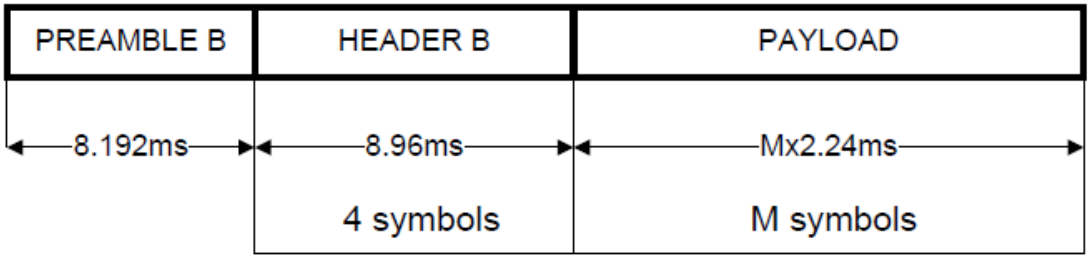


Figura 20. Configuración de un paquete tipo B [11]

En cuanto a los parámetros, existen una serie de parámetros comunes a todos los tipos de constelaciones/codificaciones y se muestran en la *Tabla 5*. El término NCH hace referencia al número de canales que se utilizan para la transmisión.

Tabla 5. Parámetros comunes en todas las implementaciones PRIME

Parámetros	**Valores**	
Reloj de la Banda Base	1000000	
Espacio entre sub-portadoras	488.28125	
Número de sub-portadores transportando información	N_{CH} x84 (cabecera)	N_{CH} x96 (*payload*)
Número de sub-portadoras transportando secuencias piloto	N_{CH} x13 (cabecera)	N_{CH} x1 (*payload*)

Intervalos FFT (muestras)	2048
Intervalos FFT (µs)	2048
Prefijo cíclico (muestras)	192
Prefijo cíclico (µs)	192
Intervalo de símbolo (muestras)	2240
Intervalo de símbolo (µs)	2240
Período del preámbulo (µs)	2048 (Tipo A) 8192 (Tipo B)

La *Tabla 6* muestra la tasa de transmisión de la capa PHY con distintas modulaciones y codificaciones. Lo modos robustos, aquellos que incluyen CC y *repetition coding*, sólo permiten emplear las constelaciones DBPSK y DQPSK.

Tabla 6. Tasas de transmisión para cada codificación

	DBPSK			**DQPSK**			**D8PSK**	
Convolutional Code ½	Sí	Sí	No	Sí	Sí	No	Sí	No
Repetition Code	Sí	No	No	No	Sí	No	No	No
Bits con información por sub-portadora	0.5	0.5	1	1	1	2	1.5	3
Bits con información por Símbolo OFDM	NCH x48	NCH x48	NCH x96	NCH x96	NCH x96	NCH x192	NCH x144	NCH x1288

Tasa de información sin codificar (kbps)	NCH x5.4	NCH x21.4	NCH x42.9	NCH x10.7	NCH x42.9	NCH x85.7	NCH x64.3	NCH x128.6
Número máximo de símbolos en el *payload*	252	63	63	252	63	63	63	63
Máxima longitud del MPDU2 con el número máximo de símbolos en el *payload* (bits)	NCH x3016	NCH x3016	NCH x6048	NCH x6040	NCH x6040	NCH x12096	NCH x9064	NCH x18144
Máxima longitud del MPDU2 con el número máximo de símbolos en el *payload* (bytes)	NCH x377	NCH x377	NCH x756	NCH x755	NCH x755	NCH x1512	NCH x1133	NCH x2268

5.2 CAPA PHY

5.2.1 PREÁMBULO

El preámbulo se utiliza con fines de sincronización. Se localiza al principio de cada PDU y, para maximizar la energía a transmitir, no se utilizan símbolos OFDM, sino una señal envolvente constante. El preámbulo resulta de crítica importancia puesto que nos desenvolvemos en escenarios de frecuencia selectiva donde las atenuaciones varían. Para poder combatirlo se emplea una secuencia chirp que proporciona propiedades de autocorrelaciones muy buenas en escenarios aperiódicos.

Preámbulo en paquetes tipo A

El preámbulo *S(t)* es la concatenación de los sub-símbolos $S^{C}_{SS}(t)$ con las cabeceras y colas solapadas. Su expresión matemática es la siguiente:

$$\mathrm{S(t)} = \sum_{i=0}^{N_{CH}} S_{SS}^{w_i}\left(t - i \cdot (T' - ro)\right), \qquad 0 < t < (T - ro) \cdot N_{CH} + ro$$

El sub-símbolo viene definido por la siguiente expresión. En ella, el parámetro A determina la potencia media del preámbulo. T' define la duración del sub-símbolo y su valor depende del número de canales activos.

$$S^{c}_{ss}(t) = A \cdot 10^{\frac{4}{20}} \cdot window\left(\frac{t}{T'}\right) \cdot \cos[2pi(f_0^c t + 1/2\mu_c t^2)], \qquad 0 < t < T'$$

Para una aclaración mayor, en la *Figura 21* muestra la estructura del preámbulo S(t) cuando hay tres canales activos. En este caso entonces, N_{CH}=3, ro=62 y T'=724µs.

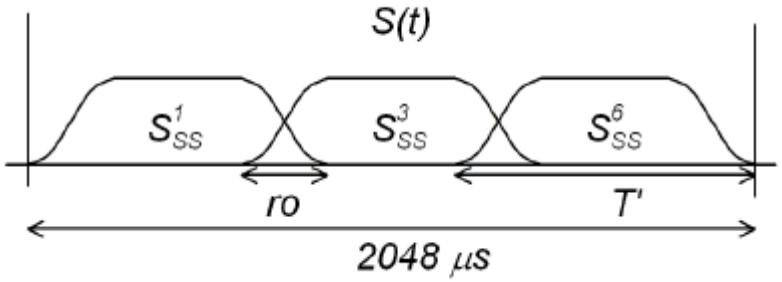


Figura 21. Estructura del preámbulo de un paquete tipo A [11]

Preámbulo en paquetes tipo B

El preámbulo en un paquete tipo B se forma a partir de la concatenación de tres símbolos $S_{PS}(t)$ y un símbolo de signo invertido. Cada $S_{PS}(t)$ está compuesto por N_{CH} sub-símbolos, donde N_{CH} es el número de canales activos. En lo referente a la obtención de cada uno de los parámetros, la metodología es la misma que la explicada en el apartado anterior, tal y como se observa en la *Figura 22.*

$$S(t) = \boxed{S_{PS}(t)}\boxed{S_{PS}(t)}\boxed{S_{PS}(t)}\boxed{-S_{PS}(t)}$$

Figura 22. Estructura del preámbulo de un paquete tipo B [11]

5.2.2 PILOTOS

El preámbulo siempre va seguido de una serie de símbolos OFDM que comprenden la cabecera. Cada símbolo de la cabecera contiene $13xN_{CH}$ sub-portadoras piloto, empezando por la primera sub-portadora de cada uno de los canales activos y separadas 7 sub-portadoras.

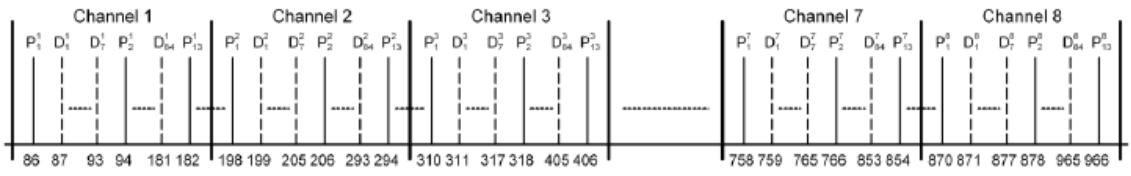


Figura 23. Distribución de los pilotos [11]

Las sub-portadoras que transportan los pilotas utilizan modulación BPSK y una secuencia binaria pseudo aleatoria. La fase de las sub-portadoras se controla mediante una secuencia conocida como *pn*, una extensión cíclica de la siguiente secuencia de 127-bits. Un 0 significa 0º de desfase y un 1 significa 180º de desfase. Cada bit se utilizará en una sub-portadora. El mismo proceso se utiliza en toda la cabecera OFDM donde las sub-portadoras piloto consecutivas tendrán asignado un bit, utilizándose tantos como canales activos haya.

$Pref_{0.126}$={0,0,0,0,1,1,1,0,1,1,1,1,0,0,1,0,1,1,0,0,1,0,0,1,0,0,0,0,0,0,1,0,0,0,1,0,0,1,1,0,0,0,1,
0,1,1,1,0,1,0,1,1,0,1,1,0,0,0,0,0,1,1,0,0,1,1,0,1,0,1,0,0,1,1,1,0,0,1,1,1,1,0,1,1,0,1,0,0,0,0,1,
0,1,0,1,0,1,1,1,1,1,0,1,0,0,1,0,1,0,0,0,1,1,0,1,1,1,0,0,0,1,1,1,1,1,1,1}

La secuencia anterior se genera a partir de un *scrambler* definido en la *Figura 24,* donde el estado inicial es con todo unos.

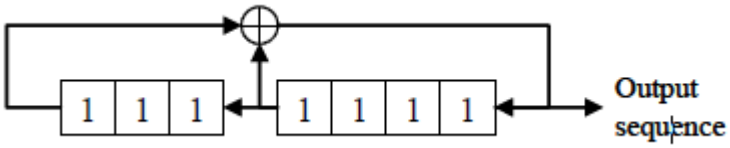


Figura 24. Algoritmo de generación de pilotos [11]

La principal diferencia existente en el ámbito de los pilotos entre los paquetes tipo A y tipo B reside en el número de símbolos OFDM que componen la cabecera. En el caso de los paquetes tipo A sólo hay dos símbolos, mientras que en los paquetes tipo B hay 4 símbolos dedicados.

5.2.3 CABECERA Y *PAYLOAD*

Paquetes tipo A

En los paquetes tipo A, los dos primeros símbolos OFDM en el PPDU se componen de $84xN_{CH}$ sub-portadoras de datos y $13xN_{CH}$ sub-portadoras piloto. Tras la cabecera cada símbolo OFDM *payload* contiene $96xN_{CH}$ sub-portadoras de datos y una sub-portadora piloto.

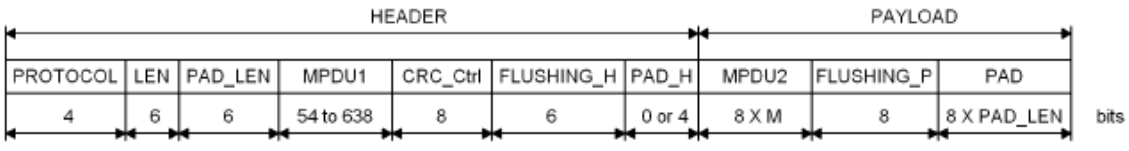


Figura 25. Estructura de la cabecera y *payload* de un paquete tipo A [11]

- HEADER: la cabecera comprende dos símbolos OFDM que contienen información tanto de la capa física como de la capa MAC. Los campos que abarca son los siguientes:

- PROTOCOL: hace referencia al esquema de transmisión del *payload*
- LEN: define la longitud del *payload* una vez que se ha codificado en símbolo OFDM. En caso de que sea 0 implica que no hay *payload*. En este aspecto PAD_LEN hace referencia al número de bits que han añadido para rellenar el MPDU.
- PAD_LEN: define la longitud del campo PAD en bytes antes de ser codificado.
- MPDU1: refiere a la primera parte del MPDU. La longitud en bits de este campo depende del número de canales activos siguiendo la siguiente regla:
  - $MPDU\ 1Len = \left[\frac{(N_{CH}\cdot 84-30)+2}{8}\right]\cdot 8-2$
- CRC_Ctrl: contiene el *checksum* del campo PROTOCOL, LEN, PAD_LEN y MPDU1.
- FLUSHING_H: refiere a los bits de *flushing* que se necesitan para la decodificación convolucional.
- PAD_H: incluye los bits codificados añadidos para conseguir un número entero de MPDUs. En la *Tabla 7* se muestran los bits que se deben añadir a la cabecera de paquetes tipo A en función del número de canales activos.

Tabla 7. Tamaño del campo PAD_H

N_{CH}	MPDU1	PAD_H
1	54	0
2	134	4
3	222	0
4	302	4
5	390	0

6	470	4
7	558	0
8	638	4

- PAYLOAD
  - MPDU2: corresponde a la segunda parte del MPDU
  - FLUSHING_P: incluye los bits necesarios para la codificación convolucional. Para resetear el *convolutional encoder* se ponen todos a cero.
  - PAD: asegura que el número de bits codificados genera un *payload* tal que el número de símbolos OFDM generados es un número entero.

Paquetes tipo B

En los paquetes tipo B, los cuatro primeros símbolos OFDM son siempre enviados utilizando DBPSK, cc "*on*" y repetición "*on*". Se componen de $84xN_{CH}$ sub-portadoras de datos y $13xN_{CH}$ sub-portadoras piloto. Tras la cabecera cada símbolo OFDM *payload* contiene $96xN_{CH}$ sub-portadoras de datos y una sub-portadora piloto.

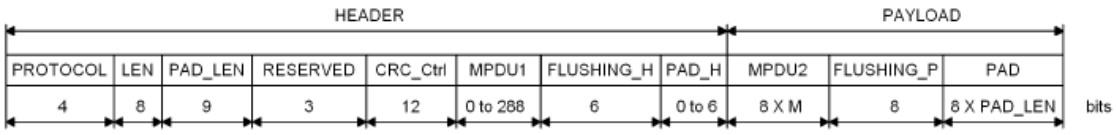


Figura 26. Estructura de la cabecera y *payload* de un paquete tipo B [11]

- HEADER: la cabecera comprende dos símbolos OFDM que contienen información tanto de la capa física como de la capa MAC. Los campos que abarca son los siguientes:

- PROTOCOL: hace referencia al esquema de transmisión del *payload*
- LEN: define la longitud del *payload* una vez que se ha codificado en símbolo OFDM. En caso de que sea 0 implica que no hay *payload*. En este aspecto PAD_LEN hace referencia al número de bits que han añadido para rellenar el MPDU.
- PAD_LEN: define la longitud del campo PAD en bytes antes de ser codificado.
- RESERVED: campo reservado para uso futuro
- CRC_Ctrl: contiene el *checksum* del campo PROTOCOL, LEN, PAD_LEN y RESERVED.
- MPDU1: refiere a la primera parte del MPDU. La longitud en bits de este campo es siempre múltiplo de 8 y depende del número de canales activos siguiendo la siguiente regla:
  - $MPDU\ 1Len = \left[\frac{(N_{CH}-1)\cdot 84\cdot\frac{1}{2}}{8}\right]\cdot 8$
- FLUSHING_H: refiere a los bits de *flushing* que se necesitan para la decodificación convolucional.
- PAD_H: incluye los bits codificados añadidos para conseguir un número entero de MPDUs. En la *Tabla 8* se muestran los bits que se deben añadir a la cabecera de paquetes tipo A en función del número de canales activos.

Tabla 8. Tamaño del campo PAD_H

N_{CH}	MPDU1	PAD_H
1	0	0
2	40	2
3	80	4

4	120	6
5	168	0
6	208	2
7	248	4
8	288	6

- PAYLOAD
  - MPDU2: corresponde a la segunda parte del MPDU
  - FLUSHING_P: incluye los bits necesarios para la codificación convolucional. Para resetear el *convolutional encoder* se ponen todos a cero.
  - PAD: asegura que el número de bits codificados genera un *payload* tal que el número de símbolos OFDM generados es un número entero.

5.2.4 CONVOLUTIONAL ENCODER

El flujo de bit sin codificar pasa por el *convolutional encoder* para poder ser codificador. Se trata de un *convolutional encoder* de tasa ½ con una longitud de 7. Como polinomios utiliza 1111001 y 1011011. En un primer instante se inicia a cero. Tras pasar la cabecera, se vuelve a inicializar a cero y entonces se pasa el *payload*. En la *Figura 27* se muestra el esquema de este bloque.

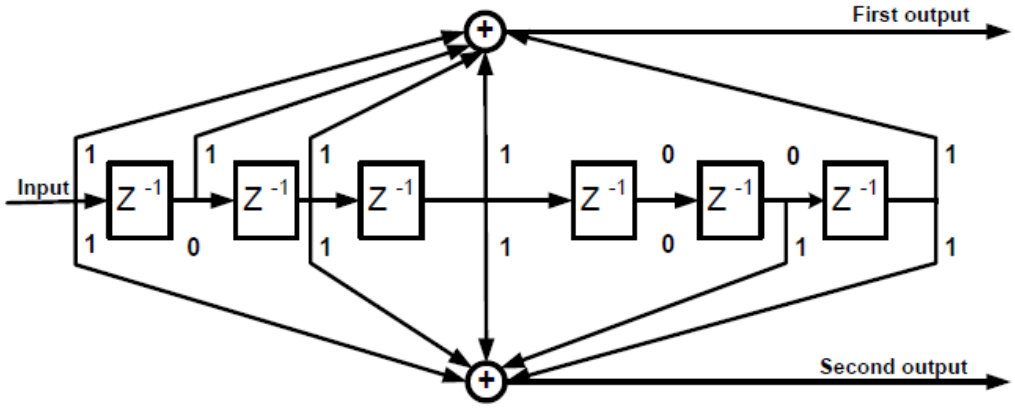


Figura 27. Convolutional Encoder [11]

5.2.5 SCRAMBLER

Este bloque se encarga de aleatorizar el flujo de bits de tal forma se reduce el factor de cresta producido en la IFFT cuando un flujo largo de ceros o unos aparece en cualquiera de ellos, cabecera o *payload*, después de su codificación. Este bloque siempre se lleva a cabo, no depende del tipo de paquete o escenario en el que nos hallemos.

Se trata de un simple xor entre el flujo de bits y una secuencia de pseudo ruido. Esta secuencia es la misma utilizada para los pilotos.

5.2.6 REPETIDOR

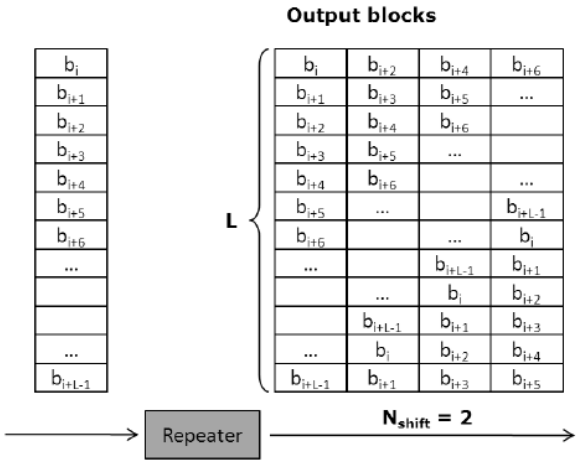


Figura 28. Repetidor [11]

Este bloque se encarga de introducir diversidad en las dos dimensiones, tiempo y frecuencia. Para ello repite una secuencia de bits cuatro veces con el fin de aumentar la robustez del sistema. El flujo a transmitir se divide en bloques de longitud L donde L es igual a $84xN_{CH}$ para la cabecera y $96xN_{CH}$ para el *payload* utilizando el modo robusto DBPSK y $192xN_{CH}$ cuando se utiliza el modo robusto DQPSK. Los bits de cada bloque replicado se obtienen al introducir y desplazamiento cíclico de N_{shift} a los bits del bloque anterior. El valor de esta variable depende del modo de transmisión y sus posibilidades se muestra en la *Tabla 9.*

Tabla 9. Desplazamiento para los modos robustos

Modo de transmisión	**N_{shift}**
DBPSK (cabecera)	2
DBPSK (*payload*)	2
DQPSK (*payload*)	4

5.2.7 INTERLEAVER

Por el desvanecimiento que existe en las líneas de potencia, los símbolos OFDM de distintas sub-portadoras sufren variaciones y llegan con distinta amplitud al receptor, dando lugar a errores. Para evitar que estos errores afecten a un símbolo entero y por tanto se pierda toda esa información, se introduce este bloque que disminuye el efecto de los errores en ráfaga. Esto asegura que los bits codificados adyacentes se transmiten en sub-portadoras no adyacentes.

5.2.8 MODULACIÓN

El PPDU *payload* se modula utilizando desplazamiento en fase diferencial. De este bloque sólo resulta interesante destacar que existen distintos tipos de modulación que PRIME tiene disponible, DBPSK, DQPSK Y D8PSK. Su utilización no difiere de la de otros sistemas y por tanto no se entrará en mayor detalle sobre este aspecto.

5.3 CAPA MAC

5.3.1 INTRODUCCIÓN

Una subred se puede entender, desde el punto de vista lógico, como una estructura con forma de árbol donde existen dos tipos de nodos: el nodo base y el nodo de servicio.

- **Nodo Base:** es aquel que inicia la de subred y cualquier otro nodo que quiera participar de la red deberá participar de un proceso de registro dirigido por este nodo.
- **Nodo de Servicio:** se entienden como hojas o ramas. Pueden estar en uno de los siguientes estados:

- **Desconectado:** es el estado inicial. No es capaz de enviar sus propios datos ni redirigir los que le llegan de otros nodos. Su principal consiste en buscar al nodo base y comenzar un proceso de registro.
- **Terminal:** es capaz de establecer conexiones y comunicarse con otro nodo pero no es capaz de redirigir los datos que le llegan de otros nodos. No tiene funcionalidades de *switch*.
- **Switch:** es capaz de proporcionar todas las funciones del estado terminal y además de reenviar datos de un nodo a otro dentro de la misma subred.

Los eventos que permiten que un nodo pase de un estado a otro son los siguientes:

- **Registro:** a través del cual el nodo de servicio se incluye en la lista de nodos registrados que almacena el nodo base. De esta forma pasa a formar parte de la subred.
- **De-registro:** el nodo servicio utiliza este evento para salirse de la red y por tanto de la lista de nodos disponible que almacena el nodo base. Este evento puede realizarlo tanto el nodo de servicio como el nodo base como resultado de un error.
- **Promoción:** es el evento gracias al cual un nodo de servicio pasa del estado terminal al estado *switch*. De esta forma se le asignan todas las capacidades disponibles.
- **Degradación:** a través de esto evento se degrada el estado del nodo de *switch* a terminal, disminuyendo así las funciones que puede llevar a cabo.

5.3.2 DIRECCIONAMIENTO

Cada nodo cuenta con una dirección universal de 48 bits conocida como dirección MAC y definida EUI-48. Esta dirección del nodo base identifica unívocamente la subred y se conoce como dirección de la sub-red (SNA por sus siglas en inglés).

Además, existen otras direcciones importantes, como la dirección de identificación de *switch* conocida como (LSID), una dirección única de 8 bits que identifica a cada nodo-

switch dentro de una subred. Es el nodo base el encargado de asignar estas direcciones cuando se suceden los eventos de promoción.

Durante el proceso de registro, cada nodo de servicio recibe e identificador de nodo local (LNID) de 14 bits . Este identifica un nodo de servicio entre todos los nodos de servicio que dependen de un mismo nodo-switch La combinación del LNID y SID forma un código de 22 bits (NID) que identifica al nodo de servicio dentro de toda la subred.

Durante establecimiento de la conexión, cada una de las conexiones se identifican gracias a un código de 9 bits conocido como LCID. La combinación del NID y LCID forma un código de 31 bits (CID) que identifica una conexión dentro de toda la subred.

Para una mayor aclaración, en la *Figura 29* se puede ver cuáles son estos códigos y su composición.

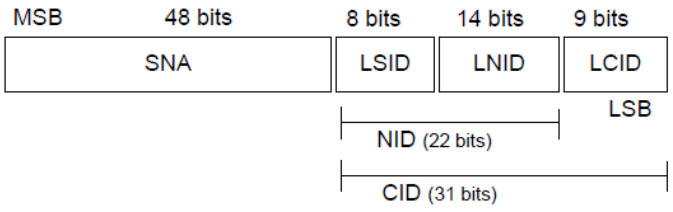


Figura 29. Estructura de direccionamiento

En lo referente al direccionamiento *multicast* y *broadcast* se utilizan distintos tipos de direcciones dependiendo del contexto en el que se esté desarrollando el tráfico. Algunos ejemplos de estos valores se muestran en la *Tabla 10*:

Tabla 10. Direcciones LNID en función del tipo de transmisión

Transmisión	**LNID**	**Descripción**
Broadcast	0x3FFF	Esta es la dirección de destino

Multicast	0X3FFE	Este tipo de direcciones hacen referencia a grupos
Unicast	Todos menos 0x3FFF y 0X3FFE	Para hacer referencia a un único nodo dentro de la subred

5.3.3 DESCRIPCIÓN FUNCIONAL

Cada nodo de servicio comienza en el estado desconectado. Estos deben mantener actualizada una tabla donde almacenen los mensajes *beacon* que reciban de cualquier de los nuevos nodos-switch, de esta manera conocen cuáles son los nodos-switch a los cuales pueden asociarse. Una vez han seleccionado uno de ellos comienza con el proceso de registro.

Antes de empezar, el nodo de servicio debe operar en una de las bandas dentro de su configuración, y por tanto escanear la banda durante un tiempo mínimo establecido en la especificación. Durante este tiempo pueden suceder dos cosas, o que no reciba ningún mensaje *beacon*, en cuyo caso el nodo de servicio debería enviar un paquete PNPDU en modo *broadcast* a fin de encontrar otros posibles mensajes en otras bandas. Dado que estos mensajes se envían en bandas distintas es posible existan colisiones. Es por ello que, si un nodo recibe otros PNPDU de otras fuentes, debe reducir la tasa de transmisión a fin de reducir las posibilidades de colisión. En el caso de que se encuentren mensajes *beacon* dentro de la misma banda simplemente debería elegir un nodo-switch y registrarse.

Los nodos base son los principales responsables de configurar y mantener la subred. De entre sus funciones destacan:

- Transmisión de mensajes *beacon*: mensajes de tipo *broadcast* enviados cada cierto tiempo.

- Promoción y degradación de nodos en estado terminal y *switch*. Para ello el nodo base posee una tabla donde almacena el código único SID con las nuevas peticiones.
- Gestión del registro: aceptando o rechazando los mensajes en función de distintos parámetros, por ejemplo, lo saturada que esté la red. También puede ser el nodo base el que inicie el proceso de registro de un nodo de servicio.
- Control del acceso al medio. El nodo base es el encargado de decidir qué mecanismo se utiliza para acceder al medio y durante cuánto tiempo se puede acceder. Además, durante los periodos de contención, el nodo base es el responsable de asignar canales a dispositivos específicos.
- Distribución de secuencias aleatorias para que los dispositivos puedan derivar claves de encriptado. De esta parte se hablará más en detalle en apartados posteriores.
- Gestión del tráfico multicas: gracias al mantenimiento de estos grupos a través de la gestión de todas las peticiones *join* y *leave.*

Acceso al medio

Un paquete comprende dos partes principales:

- *Contention Free Period* (CFP) donde solo los dispositivos a los que se les ha proporcionado permisos explícitamente pueden transmitir.
- *Shared Contention Period* (SCP) donde todos los dispositivos son libres de transmitir siempre y cuando cumplan con el algoritmo CSMA CA y posean los correspondientes tiempos de guarda y límites de SCP.

En este aspecto entra en juego un nuevo concepto que es el del super paquete que comprende un número determinado de paquetes. De esta forma se facilitan los cambios de SCP a CFP en redes muy grandes donde los paquetes *beacon* tal vez no se transmiten en cada paquete. Todos los tiempos mencionados anteriormente vienen definidos en el nodo base y depende de distintos factores como las condiciones del medio.

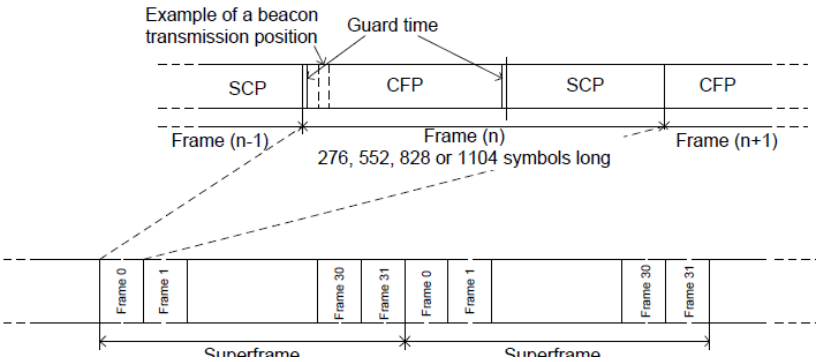


Figura 30. Estructura de un paquete MAC [11]

Respecto a los *beacons* se deben transmitir al menos una vez por super paquete. Estos contienen información administrativa y de operaciones de su respectiva subred. Estos se modulan en DBPSK_CC si se transmiten en paquetes PHY tipo A. Si se envían en paquetes PHY tipo B entonces se puede utilizar tanto la modulación DBPSK_R como la DQPSK_R. Dependiendo de cuál sea la modulación utilizada el slot asignado a estos mensajes varía.

Los mensajes de control de la capa MAC de cumplir las siguientes reglas:

- Siempre se deben transmitir en SCP
- Deben utilizar un nivel de prioridad concreto definido por la especificación
- La modulación que utilicen debe ser lo suficientemente robusta como para alcanzar al nodo receptor, pero menos robusta que DBPSK_CC

Switching

Los nodos-switch se encargan de encaminar tráfico de un nodo base a otro dentro de la subred de forma que la comunicación sea efectiva. Para poder levar a cabo esta función el paquete debe cumplir alguno de los siguientes requisitos que se categorizan en función de si es destinatario o fuente del paquete:

- Destinatario (HDR.DO=1):
  - Debe estar conectado a la subred a través de este nodo-switch.
  - O bien, se encuentra dentro de la dirección de *broadcast* de destino.
  - O bien, pertenece a la dirección *mutlicast* de destino.

- Fuente(HDR.DO=0):
    - El dispositivo origen está conectado a la subred a través de este nodo-switch.
    - El paquete tiene dirección *broadcast* o *multicast*.

En caso de que el paquete sea broadcast y lleve la etiqueta HDRO.DO=0 el nodo-switch debe tratarlo como un paquete *unicast* y enviárselo al nodo base. En caso de que el campo HDR.DO tenga valor 1 deberá enviarlo al siguiente nivel en forma de paquete broadcast. Cuando el nodo base recibe un paquete con dirección de *broadcast* y con la etiqueta HDR.DO=0 debe pasar este paquete hacia su MAC SAP para que llegue a las aplicaciones suscritas a este servicio.

Para los paquetes *multicast* el protocolo a seguir es el mismo, la principal diferencia es que para ofrecer este servicio el nodo base tiene que almacenar una tabla con todos los grupos existentes actualizados. Además, el nodo base puede pertenecer a un grupo *multicast*. En este caso, si recibe un paquete con una dirección *muticast* a la que está suscrito le enviará el paquete al MAC SAP correspondiente.

Conexiones directas

Existen dos escenarios distintos en lo referente al establecimiento conexiones directas en la subred. El primero corresponde a cuando el nodo fuente desconoce cuál es la dirección del nodo de servicio al que quiere enviar el paquete En este caso uno de los nodos de servicio iniciará la petición y será el propio nodo base el que la redirija hacia el nodo de servicio correspondiente.

El segundo escenario en el que se utilizan este tipo de conexiones es cuando nodo de servicio que inicia la petición ya conoce la dirección del nodo de servicio al que quiere enviar el paquete. En este caso no hace falta que el paquete pase por el nodo base, sino que se enruta directamente.

Agregación de paquetes

Una GDPU puede englobar uno o varios paquetes. Para asegurar que se mantiene la compatibilidad entre dispositivos que tanto permiten esta funcionalidad como no, existe una regla que indica que no se puede utilizar esta funcionalidad si existe al menos un dispositivo intermedio que va a procesar este paquete y que no soporta la agregación de paquetes.

Seguridad

Las funcionalidades de seguridad proporcionan a la capa MAC confidencialidad, autenticación e integridad gracias a la implementación de métodos de conexión segura y políticas de gestión de cables. Existen distintos perfiles que hacen referencia a distintos niveles de seguridad:

- Perfil 0: Este perfil hace referencia a una comunicación sin encriptación, es decir, sin seguridad. Sólo se aplicará este perfil en aquellos escenarios en los que las características existentes sean lo suficientemente buenas o cuando no sea necesario aplicar políticas más estrictas.

- Perfiles 1 y 2:
    - Están basados en primitivas criptográficas muy sólidas que utilizan el algoritmo AES-128 para la derivación de claves. A través de estos mecanismos se garantiza la confidencialidad, autenticidad e integridad de los paquetes que viajen por la subred.
    - La autenticación se garantiza gracias a que cada nodo posee una clave única que sólo él y el nodo base conocen.
    - Ataques de tipo "*Man in the Middle*" se evitan gracias a que se utiliza un contador de cuatro bytes en cada mensaje, de esta forma no se puede reenviar paquetes por segunda vez.

En lo referente al máximo tiempo que puede pasar desde que se crea una llave hasta que se cambia depende del número de canales disponibles. Estos valores se especifican en la *Tabla 11*.

Tabla 11. Tiempo máximo para el cambio de llaves

Canales disponibles	**Duración**
1x64Kb/s canal	49 días
2x64Kb/s canal	24 días
3x64Kb/s canal	16 días
4x64Kb/s canal	12 días
5x64Kb/s canal	10 días
6x64Kb/s canal	8 días
7x64Kb/s canal	7 días
8x64Kb/s canal	6 días

El algoritmo utilizado tiene un *hand-shake* donde los dispositivos se intercambian un *nonce.* Éste es un valor único creado para cada autenticación y utilizado para verificar que la llave utilizada para su encriptación es la correcta y por lo tanto el dispositivo pertenece a la subred. Cada nodo de servicio debe tener un contador de mensajes de 32 bits que empiece en cero y que incremente en uno con cada mensaje encriptado. Cada *nonce* se compone de la concatenación de los siguientes parámetros:

- 48 bits refiriendo a la dirección de la subred
- 8 bits refiriendo al SID
- 2 bits puestos a cero

- 14 bits refiriendo a la dirección LNID
- 32 bits de contador de mensajes

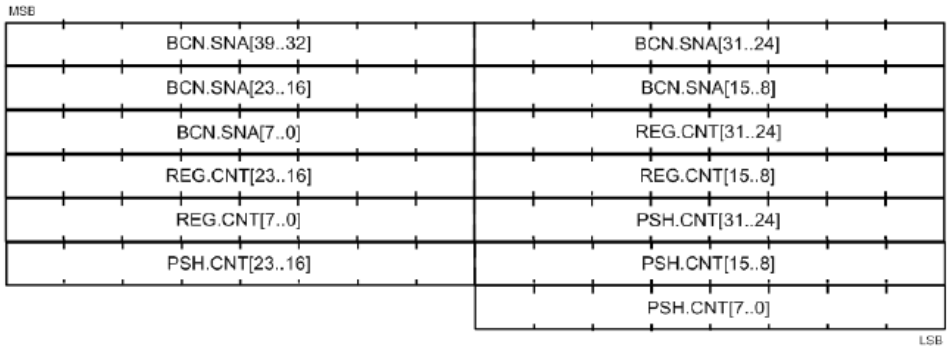


Figura 31. Estructura del *nonce* [11]

Todos los datos generados por la capa MAC, incluyendo las PDUs de señalización, utilizan el mismo perfil de seguridad. Este perfil se negocia durante el re proceso de registro. En él el terminal indica el perfil de seguridad que es capaz de soportar dentro del campo REG.SPC. El nodo base puede aceptarlo, y por tanto aceptar el registro, o puede aceptar el registro, pero no el perfil de seguridad. En este caso, en lugar de enviar el mismo valor en el campo REG.SPC en el mensaje de respuesta, pondrá el valor referente al perfil de seguridad que pide aplicar. También podría negar el registro en caso de que el dispositivo no sea capaz de aplicar el perfil requerido.

Dentro de las llaves existen distintos tipos de llaves:

- *Device Unique Key* (DUK): sólo para el proceso de derivación de claves
- *Key Wrapping Key* (KWK): derivada de la DUK utilizando la concatenación de la dirección de subred (SNA) y el *string* "KWK" como contexto. Sirve para las llaves recibidas por el nodo base.
- REG Key (REGK): se utiliza para proteger algunos de los mensajes gracias al algoritmo AES-128-CCM.

- *Working Key* (WK): se utiliza para encriptar los mensajes *unicast* que se transmiten del nodo base a los nodos de servicio y viceversa.
- *Subnetwork Working Key* (SWK): esta es una llave compartida por toda la subred. Se genera de manera aleatoria por el nodo base y se codifica utilizando el algoritmo AES-128-KW y se transmite en el mensaje REG_RSP y SEC.

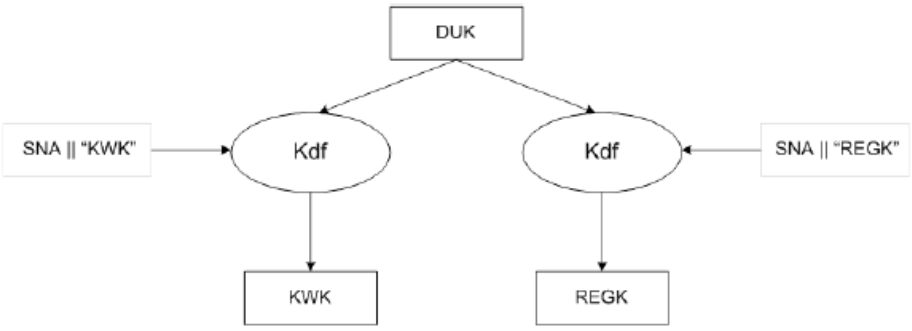


Figura 32. Jerarquía de llaves [11]

Para la encriptación y autenticación de los perfiles 1 y 2 se aplica el algoritmo AES-CCM. En la imagen que se muestra a continuación se puede ver cómo se aplica el algoritmo y cuál es la información que procesa y genera.

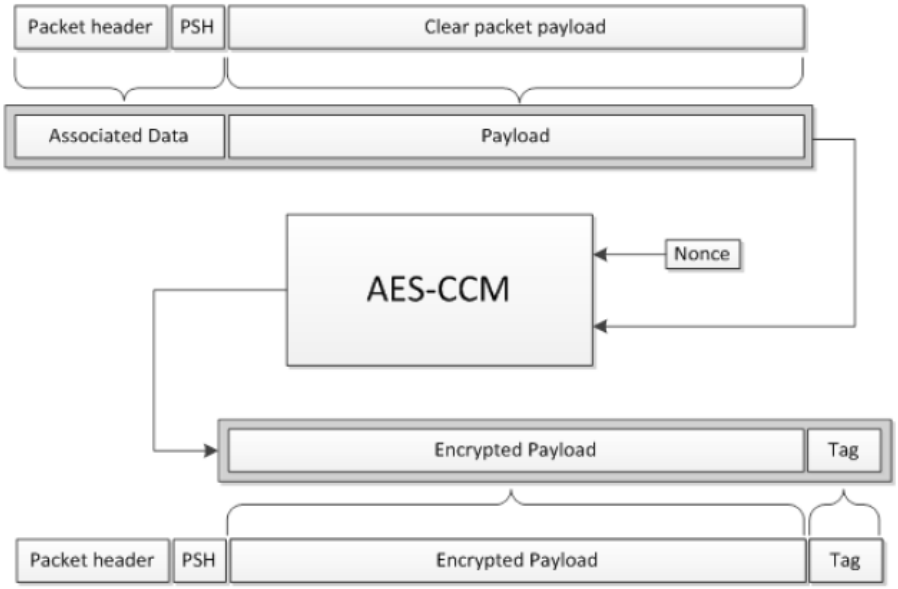


Figura 33. Algoritmo AES-CCM [11]

5.3.4 FORMATO DE TRAMAS MAC PDU

El formato de una cabecera MAC genérica es el de la cabecera seguida de uno o más paquetes y por último 32 bits de CRC. El tamaño es de 3 bytes y consta de los siguientes campos:

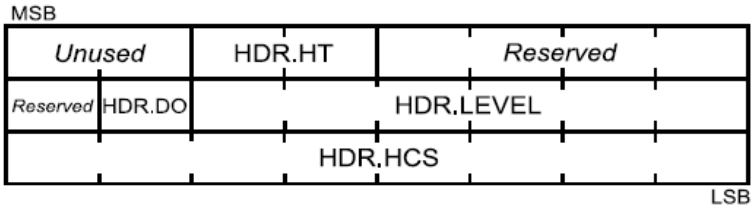


Figura 34. Cabecera de una trama MAC genérica [11]

Tabla 12. Campos de la cabecera de una trama MAC genérica

Nombre	Longitud	Descripción
Unused	2 bits	Bits sin uso, siempre a cero.
HDR.HT	2 bits	Tipo de Cabecera HDR.HT = 0 par GPDU
Reserved	5 bits	Siempre a 0 para esta especificación.
HDR.DO	1 bit	Downlink/Uplink. HDR.DO=1 downlink HDR.DO=0 uplink.
HDR.LEVEL	6 bits	Nivel de la PDU dentro de la jerarquía. Los paquetes entre el nodo base y el primer nivel tendrán valor HDR.LEVEL=0. Los paquetes entre los niveles k y k-1 tiene valor HDR.LEVEL=k. Si HDR.DO=0, HDR.LEVEL representa el nivel de la fuente Si HDR.DO=1, HDR.LEVEL representa el nivel del destinatario
HDR.HCS	8 bits	Secuencia de confirmación de la cabecera

Los paquetes no genéricos tendrán la siguiente estructura:

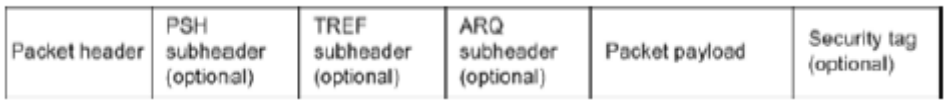


Figura 35. Estructura de un paquete de la capa MAC [11]

La cabecera ocupa 7 bytes y está compuesta por distintos campos que se muestran en la Figura 36 y se especifican en la *Tabla 13*.

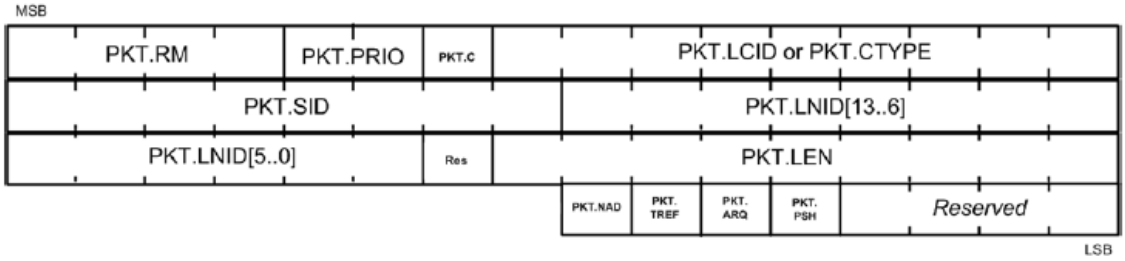


Figura 36. Cabecera de un paquete MAC [11]

Tabla 13. Parámetros de la cabecera de un paquete MAC

Nombre	Longitud	Descripción
PKT.RM	4 bits	Mínima modulación que soporta. 0 – DBPSK 1 – DQPSK 2 – D8PSK 3 – En desuso 4 – DBPSK + Convolutional Code 5 – DQPSK + Convolutional Code 6 – D8PSK + Convolutional Code 7-11 – En desuso 12 – Robust DBPSK 13 – Robust DQPSK 14 – En desuso 15 – Información desactualizada
PKT.PRIO	2 bits	Indica la prioridad. Va de 0 a 3.

PKT.C	1 bits	Control PKT.C=0 viajan datos PKT.C=1 viaja información de control
PKT.LCID / PKT.CTIPO	9 bits	LCID
PKT.SID	8 bits	Identificador del *switch.*
PKT.LNID	14 bits	Identificador de nodo local.
Reserved	1bit	Siempre a 0.
PKT.LEN	9 bits	Longitud del paquete sin considerar la cabecera
PKT.NAD	1 bit	Sin agregación en el destino. PKT.NAD=0 indica que el paquete puede sufrir agregación en el destino. PKT.NAD=1 el paquete no sufrirá agregación en el destino.
PKT.TREF	1 bit	Existencia de cabecera TREF PKT.TR=0 no existe PKT.TR=1 existe
PKT.ARQ	1 bit	Existencia de cabecera ARQ PKT.ARQ=0 no existe PKT.ARQ=1 existe.
PKT.PSH	1 bit	Existencia de cabecera de seguridad PKT.PSH=0 no existe. PKT.PSH=1 existe
Reserved	4 bits	Siempre a 0

CRC

Es el último campo del GDPU. Se utiliza para detectar errores durante la transmisión. Está formado por un polinomio cuyos coeficientes son los bits de datos que se están comprobando. El polinomio generador del CRC es el siguiente:

$$\boldsymbol{CRC = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^{8} + X^{7} + X^{5} + X^{4} + X^{2} + X + 1}$$

Cabecera de Seguridad PSH

Esta cabecera sólo se utiliza cuando se aplican los perfiles 1 o 2. A continuación se muestran, tanto una imagen con los campos que engloba y su longitud, como la *Tabla 14* describiendo estos campos.

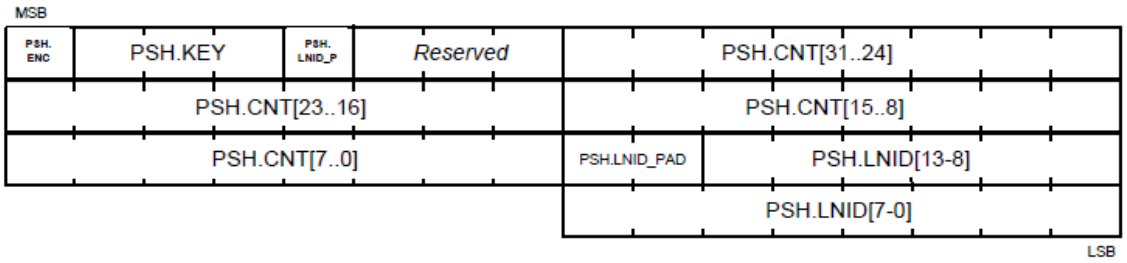


Figura 37. Campos de la cabecera de seguridad PSH [11]

Tabla 14. Descripción de los campos de la cabecera de seguridad PSH

Nombre	Longitud	Descripción
PSH.ENC	1 bit	*Flag* para indicar si el paquete va encriptado. 0 – El paquete solo ha sido autenticado 1 – El paquete ha sido autenticado y encriptado
PSH.KEY	3 bits	Llave utilizada para codificar el paquete 0 – WK 1 – SWK 2 – REG 3-8 – Reservados para uso futuro
PSH.LNID_P	1 bit	*Flag* que determina si el PSH.LNID está incluido. 0 – No se incluye

		1 – Sí se incluye
Reserved	3 bits	Always 0 en this version of the specification. Reserved en future use.
PSH.CNT	32 bits	Contador utilizado para la elaboración del *nonce*.
PSH.LNID_PAD	2 bits	Siempre a 0 para esta versión.
PSH.LNID	14 bits	Parámetro LNID del transmisor para crear el *nonce* cuando no puede derivarse directamente del paquete.

Paquetes de control

Existen distintos tipos de paquetes de control. Estos permiten que el nodo de servicio comunique información de control con su nodo-switch y al revés. Estos se transmiten como un GDPU y en la cabecera, el campo PKT.C se pone a 1. Para identificar el tipo de paquete de control se utiliza el campo PKT.CTIPO. En la *Tabla 15* se muestran todos los paquetes de control, con su descripción y valor.

Tabla 15. Tipos de paquetes de control

PKT.CTIPO	Nombre	Descripción
1	REG	Gestión de registro
2	CON	Gestión de conexión
3	PRO	Gestión de promoción
5	FRA	Cambio en la estructura del paquete
6	CFP	Petición de CFP
7	ALV	Keep-Alive
8	MUL	Gestión multicast
10	SEC	Información de seguridad

Para poder recuperar mensajes de control que han sido transmitidos, pero se han extraviado, de camino al receptor, se definen una serie de políticas de retransmisión. Para ello los dispositivos deben mantener un temporizador de retransmisión y un temporizador

de mensaje fallido. Estas políticas sólo se aplican a los siguientes tipos de paquetes cuando requieren una respuesta:

- CON_REQ_S, CON_REQ_B; 1915
- CON_CLS_S, CON_CLS_B; 1916
- REG_RSP; 1917
- PRO_REQ_B; 1918
- MUL_JOIN_S, MUL_JOIN_B; 1919
- MUL_LEAVE_S, MUL_LEAVE_B; 1920
- MUL_SW_LEAVE_B 1921
- SEC

Para entender mejor cómo funciona este mecanismo de retransmisión, a continuación se adjuntan la Figura 38 y la Figura 39 donde se muestran los mensajes intercambiados entre tres nodos de una sub red cuando no hay y cuando sí hay retransmisión.

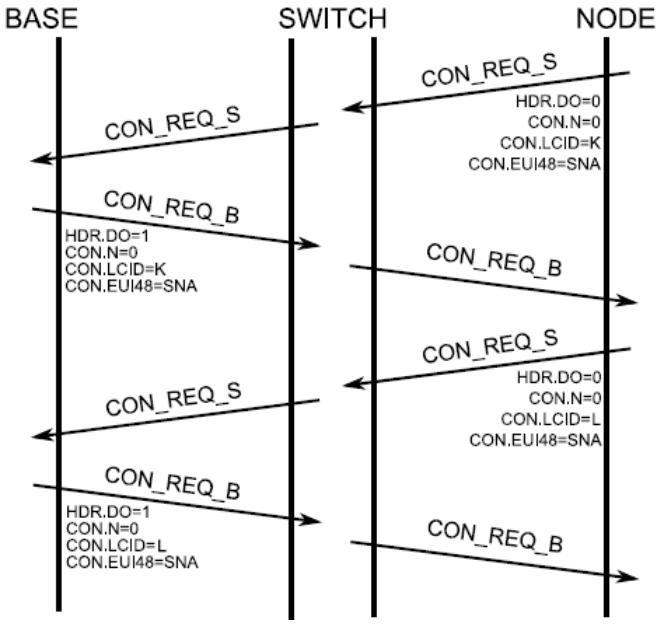


Figura 38. Intercambio de mensajes sin retransmisión [11]

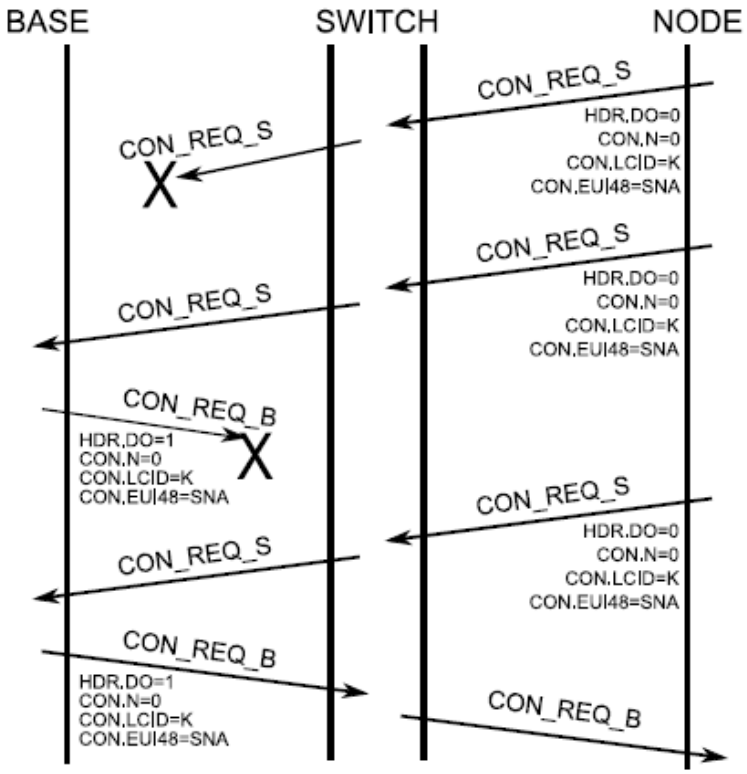


Figura 39. Intercambio de mensajes con retransmisión [11]

Paquetes de control de tipo REG (PKT.CTIPO=1)

Dentro del paquete de control tipo REG, los campos que se incluyen no poseen ninguna característica particular. Estos hacen referencia al perfil de seguridad a aplicar. Identificación de capacidades de nodo transmisor (agregación de paquetes, funciones de *switch*,…), identificación de mecanismos de *Keep Alive*, etc.

Sin embargo, sí que resulta interesante explicar que existen distintos tipos de paquetes tipo REG que se intercambian los nodos durante el proceso de registro. A continuación se muestra la Tabla 16 identificando estos tipos.

Tabla 16. Tipo de paquetes de control REG

Nombre	HDR.DO	PKT.LNID	REG.N	REG.R	Descripción
REG_REQ	0	0x3FFF	0	R	Petición de registro R=0 para eliminar todas las conexiones previas de este nodo. R=1 para mantener las conexiones previas del nodo.
REG_RSP	1	< 0x3FFF	0	R	Respuesta al registro. Este paquete asigna el LNID al nodo de servicio.
REG_ACK	0	< 0x3FFF	0	R	Confirmación del estado de registro.
REG_REJ	1	0x3FFF	1	0	Registro rechazado por el nodo base.
REG_UNR_S	0	< 0x3FFF	1	0	Tras un REG_UNR_B: confirmación de de-registro. Sin paquetes precedentes: petición de de-registro
REG_UNR_B	1	< 0x3FFF	1	0	Tras REG_UNR_S: de-registro confirmado Sin paquetes precedentes: petición de de-registro iniciada por el nodo base.

Paquetes de control de tipo CON (PKT.CTIPO=2)

Este tipo de paquetes se utilizan para negociar la conexión. El significado de este tipo de paquetes difiere en función de cuál sea la dirección que lleve. Los campos que se incluyen en este tipo de paquetes hacen referencia al estado de la conexión, el tipo de conexión (directa o no), mecanismos que se deben aplicar (como ARQ), parámetros de seguridad, parámetros específicos de la conexión, etc. En la Tabla 17 se incluyen todos los tipos de paquetes de control que existen.

Tabla 17. Tipos de paquetes de control CON

Nombre	HDR.DO	CON.N	Descripción
CON_REQ_S	0	0	Establecimiento de conexión iniciado por el nodo de servicio
CON_REQ_B	1	0	El nodo base debe considerar que la conexión se ha establecido con el identificador CON.LCID. Tras CON_REQ_S: Conexión aceptada. Sin paquetes precedentes: petición del establecimiento de conexión.
CON_CLS_S	0	1	El nodo de servicio considera esta conexión cerrada: Tras CON_REQ_B: conexión rechazada por el nodo Tras CON_CLS_B: confirmación de conexión cerrada Sin paquetes precedentes: Petición de cierre de conexión.
CON_CLS_B	1	1	El nodo base considera que la conexión no se necesita más Tras CON_REQ_S: establecimiento de conexión rechazada por el nodo base. Tras CON_CLS_S: confirmación de cierre de conexión. Sin paquetes precedentes: petición de cierre de conexión.

Paquetes de control de tipo PRO (PKT.CTIPO=3)

Este tipo de paquetes se utilizan para promocionar nodos de servicio de sus funcionalidades de terminal a funcionalidades de *switch*. De los campos que engloban destacan el tipo de promoción (negativa o positiva), identificadores asignados (NSID), parámetros de calidad en la recepción, frecuencias de transmisión asignadas para los paquetes *Beacon*, tipo de modulación de los paquetes *Beacon*, y otros parámetros de funcionalidades asociadas y ACK. De nuevo, existen distintos tipos de paquetes dentro de los paquetes tipo PRO, pero en este caso no resultan de tanto interés y no se especificarán.

Paquetes de control de tipo FRA (PKT.CTIPO=5)

Este tipo de paquetes se envían desde el nodo base en modo *broadcast* hacia todos los nodos-switch y éstos lo envían hacia todos sus nodos de servicio de forma que llegan a toda la subred. Se utilizan para notificar cambios en la estructura de los paquetes en un momento específico del futuro.

Paquetes de control de tipo CFP (PKT.CTIPO=6)

Se utilizan para proporcionar acceso a canales de tipo CF a un nodo terminal o nodo-switch específico. De entre sus campos no destaca nada en especial. Existen también distintos tipos de mensajes que principalmente hacen referencia a peticiones y respuestas.

Paquetes de control de tipo ALV (PKT.CTIPO=7)

Estos son paquetes de señalización tipo *Keep-Alive* intercambiados entre el nodo de servicio, el nodo de servicio por encima de este y el nodo base. También se utilizan para comprobar el rendimiento de un nodo en particular y su gestión de robustez. De entre los campos que se incluyen están el identificador de petición o respuesta, el tiempo a esperar entre distintos mensajes de *keep-alive*, número de repeticiones, campos de validación, campos de control de calidad de la transmisión, etc. De nuevo, entre los tipos mensaje que se incluyen sólo existen peticiones y respuestas y es por ello que no se especifican en este documento.

Paquetes de control de tipo MUL (PKT.CTIPO=8)

Este tipo de paquetes se utilizan con motivos de control de pertenencia a los distintos grupos *multicast*. Los únicos tipos de mensajes que existen en lo referente a este tipo de paquetes son de peticiones y respuestas relacionadas con la unión y salida de dispositivos a grupos.

Paquetes de control de tipo SEC (PKT.CTIPO=10)

Este paquete es un mensaje *unicast* transmitido, autenticado y encriptado (WK) por el nodo base y todos los nodos-switch del resto de la subred con el fin de circular la secuencia aleatoria utilizada para generar la *Working Key*. Esta secuencia es dinámica y cambia con el tiempo para asegurar que se mantienen los niveles de seguridad. Los campos que se incluyen en este tipo de mensajes son los siguientes:

Tabla 18. Campos de los paquetes tipo SEC

Nombre	Longitud	Descripción
SEC.KEY	2 bits	Indica que clave se está actualizando 0 - reservado 1 – SEC.WK 2 – SEC.SWK 3 – SEC.WK y SEC.SWK
Reserved	6 bits	Siempre a 0 en esta versión
SEC.WK	192 bits	(opcional) Working Key encriptada por KWK.
SEC.SWK	192 bits	(opcional) SWK encriptada por KWK.

5.3.5 FORMATO DE TRAMAS BEACON PDU

Estas tramas las transmite cada nodo-switch dentro de la subred incluido el nodo base. El objetivo es que circule información de la estructura de los paquetes mac y por tanto de acceso al canal hacia todos los dispositivos que son parte de la subred. Las BPDU se transmite cada cierto intervalo de tiempo definido y son utilizadas también con findes de

sincronización. De entre sus campos destacan: el establecimiento de calidad a partir de parámetro rtdp (*Round Trip Drop Probability*), es decir, la probabilidad de que un paquete cambie de sentido durante su transmisión; el indicador de la frecuencia de transmisión de BPDU; y el coste de transmitir desde el nodo-switch al nodo base calculado en base a la modulación utilizada.

5.3.6 FORMATO DE TRAMAS DE PROMOCIÓN

Si un nodo se desconecta y no tiene conectividad con ningún otro nodo-switch, éste debería enviar notificaciones a sus vecinos para indicar que necesita ser promocionado por cualquier de los nodos terminales existentes.

5.3.7 PUNTO DE ACCESO AL SERVICIO MAC

El punto de acceso al servicio de la capa MAC proporciona una serie de primitivas que permiten a la capa de convergencia interaccionar con la capa MAC. El uso de estas primitivas no es obligatorio, sino que queda opcional y dependiente del tipo de implementación que se realice, pudo emplear éstas, o sólo algunas o incluso una interfaz completamente distinta. En la Figura 40, la Figura 41, la Figura 42y la Figura 43se muestran los ejemplos de uso de algunas de estas primitivas.

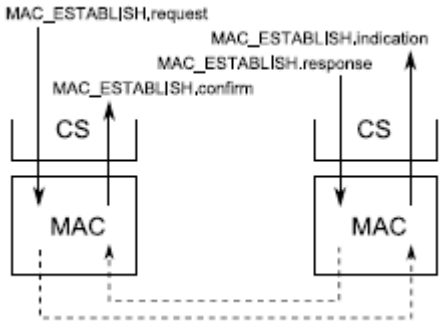


Figura 40. Establecimiento de conexión [11]

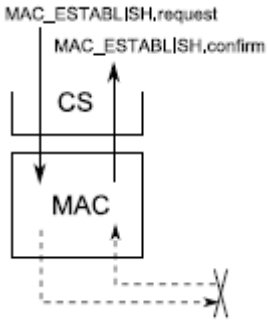


Figura 41. Fallo en el establecimiento de conexión [11]

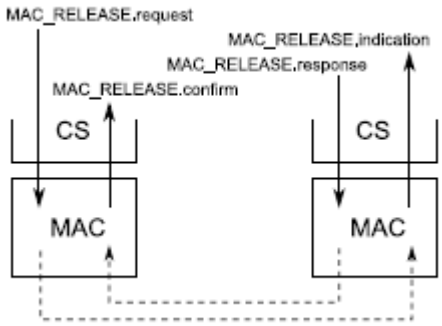


Figura 42. Cancelación de la conexión [11]

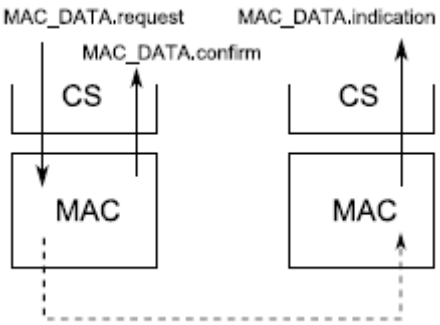


Figura 43. Transferencia de datos [11]

Dado que el uso de estas primitivas no es algo crítico, en este documento sólo se van a citar. Información más detallada se puede encontrar en la especificación técnica para posibles implementaciones.

Tabla 19. Primitivas de la capa MAC

Primitivas del nodo de servicio	**Primitivas del nodo base**
MAC_ESTABLISH.request	MAC_ESTABLISH.request

MAC_ESTABLISH.indication	MAC_ESTABLISH.indication
MAC_ESTABLISH.response	MAC_ESTABLISH.response
MAC_ESTABLISH.confirm	MAC_ESTABLISH.confirm
MAC_RELEASE.request	MAC_RELEASE.request
MAC_RELEASE.indication	MAC_RELEASE.indication
MAC_RELEASE.response	MAC_RELEASE.response
MAC_RELEASE.confirm	MAC_RELEASE.confirm
MAC_JOIN.request	MAC_JOIN.request
MAC_JOIN.Response	MAC_JOIN.response
MAC_JOIN.indication	MAC_JOIN.indication
MAC_JOIN.confirm	MAC_JOIN.confirm
MAC_LEAVE.request	MAC_LEAVE.request
MAC_LEAVE.indication	MAC_LEAVE.indication
MAC_LEAVE.confirm	MAC_LEAVE.confirm
MAC_DATA.request	MAC_REDIRECT.response
MAC_DATA.confirm	MAC_DATA.request
MAC_DATA.indication	MAC_DATA.confirm
	MAC_DATA.indication

También existen otra serie de primitivas orientadas a la gestión de entidades cuyo objetivo es permitir que entidades externas pueda gestionar los procesos de registro, promoción y deregistro de un nodo de servicio. Este tipo de primitivas quedan aún más fuera

del alcance de este documento y no se tratarán puesto que no se consideran relevantes para la comparación de los tres estándares.

5.3.8 PROCESO DE REGISTRO

El proceso de registro es un proceso en tres sentidos. El nodo base responde a la petición de registro (REG_REQ) enviada por el nodo de servicio y el nodo de servicio envía un mensaje confirmando la respuesta. El nodo de servicio informa sobre las capacidades que puede soportar en términos de robustez, el máximo valor de SAR (*segmentation and reassembly)*, etc.

El paquete de control REG siempre se envía sin encriptar. Sin embargo, algunos parámetros como REG.SWK y REG.WK se encriptan con llaves especificas del contexto tal y como se ha explicado en secciones anteriores. En los tres mensajes intercambiados, estos campos se encriptan y desencriptan utilizando llaves distintas, lo que confirma, que ambos dispositivos pertenecen a la subred.

En términos de seguridad, los pasos de registro son los siguiente:

1. El nodo terminal genera un *challenge.*
2. El *challenge* se incluye en el paquete REG_REQ y se autentica utilizando REGK.
3. El nodo base valida que el REG_REQ se ha autenticado correctamente.
4. El SWK y WK se encapsulan utilizando KWK. El REG_RSP se autentica utilizando REGK y el *challenge* creado por el nodo terminal se concatena.
5. El nodo terminal valida el paquete REG_RSP.
6. Actualiza las claves WK y SWK.
7. El paquete REG_ACK se autentica utilizando WK.
8. El nodo base valida el REG_ACK.

5.3.9 PROCESO DE RE-REGISTRO

Este proceso puede iniciarlo tanto el nodo de servicio como el nodo base. A continuación se incluyen la Figura 44 y la Figura 45, reflejando ambos escenarios.

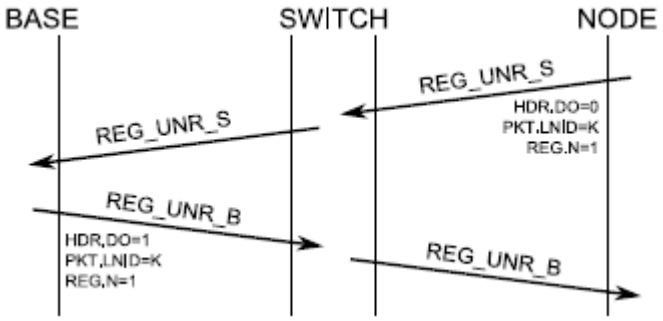


Figura 44. Deregistro inciado por el nodo terminal [11]

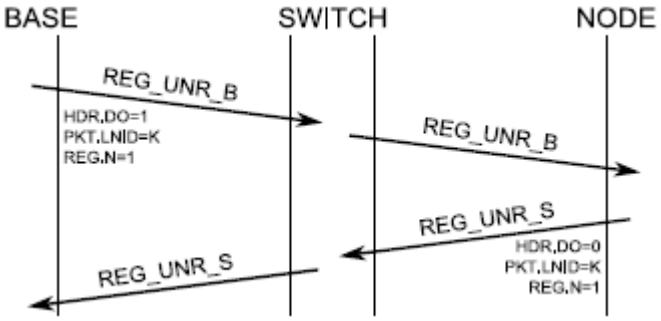


Figura 45. Deregistro iniciado por el nodo base [11]

5.3.10 PROCESO DE PROMOCIÓN

Cualquier nodo terminal que reciba PNPDUs puede generar peticiones de promoción hacia el nodo base y, en última instancia, generar peticiones de promoción a *switch* y por tanto escalar dentro de la subred.

El nodo base es el único que puede decidir si el nodo debe promocionar o no, siempre y cuando haya peticiones. Éste sólo enviará respuesta a aquellos nodos que decida promocionar, el resto no recibirán respuesta. Sólo se enviará una respuesta negativa en el caso de que algo extraño suceda.

En la Figura 46 se muestra un ejemplo del intercambio de paquetes en un escenario de promoción iniciado por el nodo de servicio.

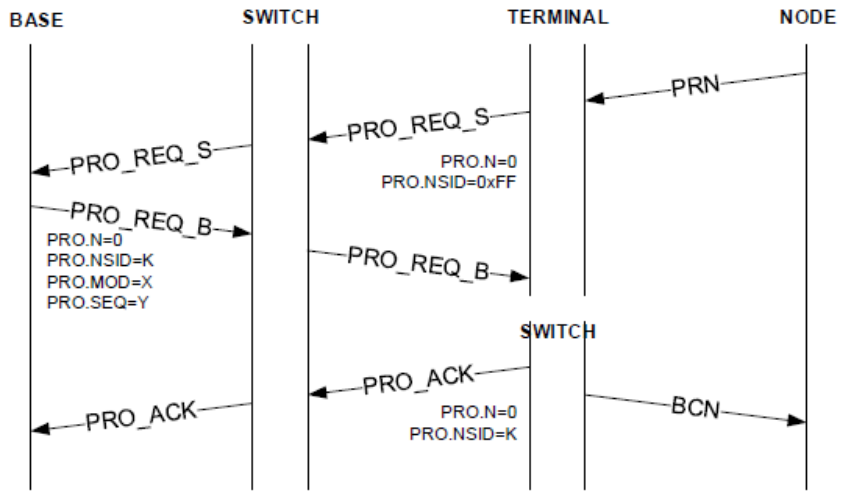


Figura 46. Proceso de promoción iniciado por el nodo de servicio [11]

5.3.11 PROCESO DE DEGRADACIÓN

El nodo base o un nodo-switch pueden decidir degradar la función de *switch* en cualquier momento. Este proceso cubre esta necesidad. El paquete tipo PRO se utiliza también para la degradación de servicio. En el momento en el que se lleva a cabo, el nodo-switch deja de enviar paquetes *beacon* y pierde la capacidad de encaminar paquetes de otros nodos.

5.3.12 PROCESO DE KEEP ALIVE

Se utiliza, bien para detectar si un nodo de servicio ha abandonado la subred por cambios en la configuración de la misma, bien para llevar a cabo proceso de gestión de la robustez en cada uno de los nodos intermedios que existen en el camino a un nodo de servicio. Este proceso viene caracterizado por el uso de un *timer* que se pone a cero cada vez que se recibe alguno de estos paquetes con parámetros validos en el campo TIME:

- REG_RSP
- ALV_REQ_B
- PRO_REQ

La gestión de los *keep alive* se hace *hop-by-hop* lo que significa que cada *switch* es responsable de el mensaje que encamina. En la Figura 47 se muestra un ejemplo de esta característica.

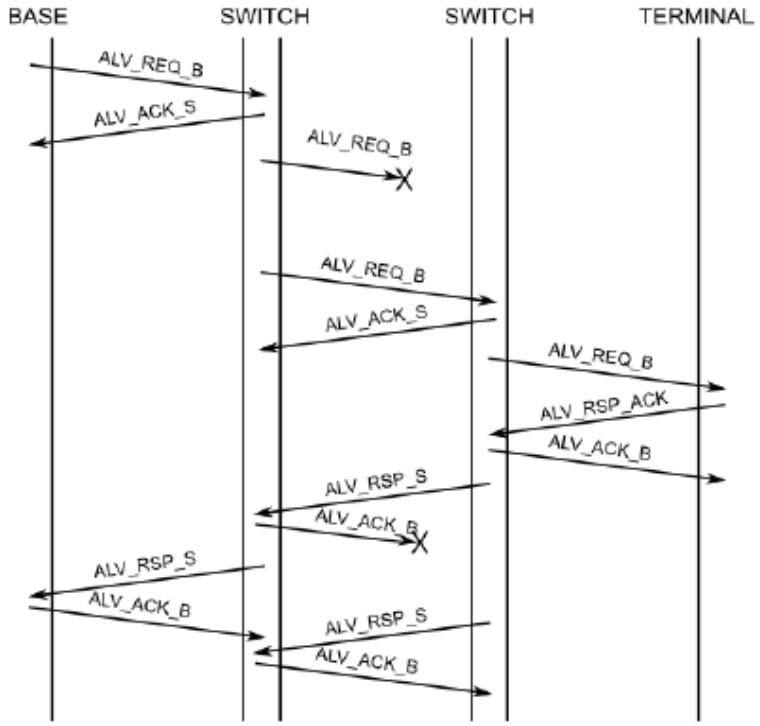


Figura 47. Ejemplo de transmisión de mensajes tipo ALV [11]

5.3.13 GESTIÓN DEL NIVEL DE ROBUSTEZ

Este mecanismo proporciona las capacidades necesarias para seleccionar la modulación que mejor cubre las necesidades del escenario en el que nos movemos. La principal dependencia viene marcada por las características del medio. En función de cómo de bueno sea el canal por el que se va a transmitir se tomará la decisión de, bien reducir el nivel de robustez asignado, y con ello utilizar un esquema de modulación menos restrictivo, bien incrementarlo para asegurar que el número de errores durante la transmisión se reduce lo máximo posible. Los distintos esquemas de modulación son los siguientes: *Robust* DBPSK, *Robust* DQPSK, DBPSK_CC, DBPSK, DQPSK_CC, DQPSK, D8PSK_CC and D8PSK

5.3.14 GESTIÓN DEL ARQ (AUTOMATIC REPEAT REQUEST)

ARQ es una propiedad que se negocia durante el registro durante el cual, se indica la preferencia por su uso o no en el campo CON.ARQ. Este mecanismo trabaja con dispositivos directamente conectados siempre y cuando ambos lo soporten. Existen distintos tipos de paquetes que se envían referidos al ARQ. Entre ellos destaca el general, el ACK, el WIN y el NACK. Para identificar dentro de un paquete general qué tipo de paquete viaja, existe un campo ARQ.INFO cuyos bytes indican cuál de los tres es. Si lo que hay es un paquete NACK, lo que significa es que se han perdido varios paquetes y por tanto se mandan tantos NACK como paquetes perdidos se hayan registrado. Un paquete NACK indica la confirmación de todos los paquetes anteriores al paquete que éste hace referencia.

El paquete ARQ.WIN hace referencia a la necesidad de adaptar la ventana del transmisor a un valor especificado en el parámetro ARQ.WINSIZE de tal manera que el buffer se adapte a las necesidades del receptor para que los paquetes no se pierdan por falta de memoria.

5.3.15 COMPATIBILIDAD CON LA VERSIÓN PRIME 1.3.6

Toda subred que permita que dispositivos que trabajan con la versión PRIME V1.3.6 o superior se registren tienen que proporcionar mecanismos que garanticen la compatibilidad de ambas versiones. Las principales restricciones son:

- El nodo base siempre debe trabajar en la versión 1.4 puesto que en la versión 1.3.6 no se proporcionan funcionalidades que permitan gestionar temas de compatibilidad.
- Todas las PDU transmitidas en modo robusto deben utilizar el paquete PHY BC.
- El tamaño máximo de segmentación SAR debe ser limitado por el nodo base a 64 bytes o menos.
- El tamaño de la trama debe ser fijo e igual a 276 símbolos OFDM.

- El nodo base debe fijar la duración del CFP a un valor que garantice que los *beacons* transmitidos en modo robusto pueden viajar dentro del CBCN.CFP.
- No se puede actualizar el contador de slots de *beacons* puesto que estos se transmiten dentro del CFP.

Los paquetes a transmitir tendrán el mismo formato que el descrito anteriormente. La única diferencia es que se incluirá una cabecera que cumpla las especificaciones de la versión 1.3.6. de tal forma que los dispositivos que trabajen en esta versión sean capaces de procesar el paquete y descartarlo al detectar el *payload* del mismo no coincide con sus restricciones.

5.4 CAPA DE CONVERGENCIA

La capa de convergencia se divide en dos sub capas distintas. Existe una parte denominada *Common Part Convergence Sublayer (CPCS)* que proporciona un conjunto de funcionalidades genéricas y comunes a todos los servicios de comunicaciones que se quieran implantar. Éstos se encuentran en la segunda sub capa conocida como *Service Specific Convergence Sublayer (SSCS)*. Puede haber tantas SSCS como se desee, pero una única CPCS.

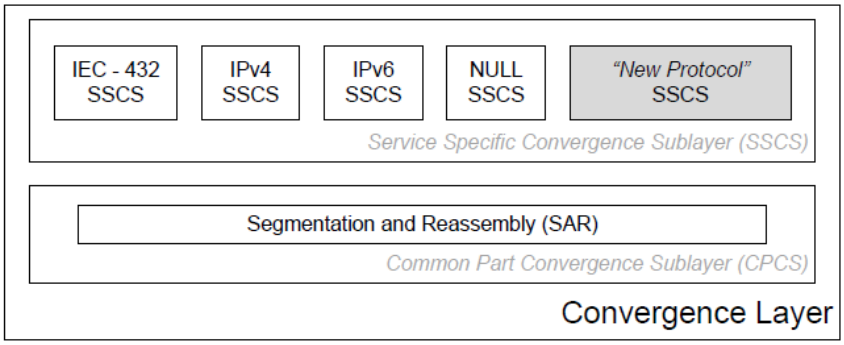


Figura 48. Arquitectura de la capa de convergencia [11]

5.4.1 COMMON PART CONVERGENCE SUBLAYER (CPCS)

En términos de procesamiento de PDU, el tamaño máximo de PDU que pueden procesar los servicios de la capa superior no pueden superar un tamaño concreto especificado por PRIME. En caso de que el tamaño sea recibido será fragmentado en esta capa. En tal caso se aplicarán funcionalidades de SAR y se incluirá una cabecera a cada uno de los segmentos de tal manera que las capas superiores sepan que la información se ha fragmentado.

Existe la posibilidad de que se reciban *NULL Service-Specific Convergence Sublayer PDUs.* En este caso la capa MAC tiene total visibilidad y transparencia hacia las capas superiores. En caso de que esto suceda, las funcionalidades que se permiten aplicar consistirán en un mapeo directo hacia las primitivas que tiene disponible la capa MAC y que ya se explicaron en apartados anteriores.

5.4.2 IPV4 SERVICE-SPECIFIC CONVERGENCE SUBLAYER (IPV4 SSCS)

Este servicio proporciona mecanismos que permiten transferir paquetes IPv4 de manera eficiente a lo largo de la subred. De entre las principales características destacan:

- Un nodo de servicio puede enviar paquetes IPv4 bien al nodo base bien a otro nodo de servicio.
- El nodo base debe actuar como un router entre la subred a la que pertenece y otras subredes.
- No se permite establecer más de un camino durante el envío de paquetes IPv4.
- Para poder configurar una dirección se debe usar DHCP.
- El elemento dentro del dispositivo encargado de determinar si un paquete se debe enviar directamente a otro nodo de servicio o hacia el *Gateway* es la capa IPv4 SSCS, la cual hace funciones de ruteo.
- La funcionalidad SAR de la capa CPCS siempre debe aplicarse.

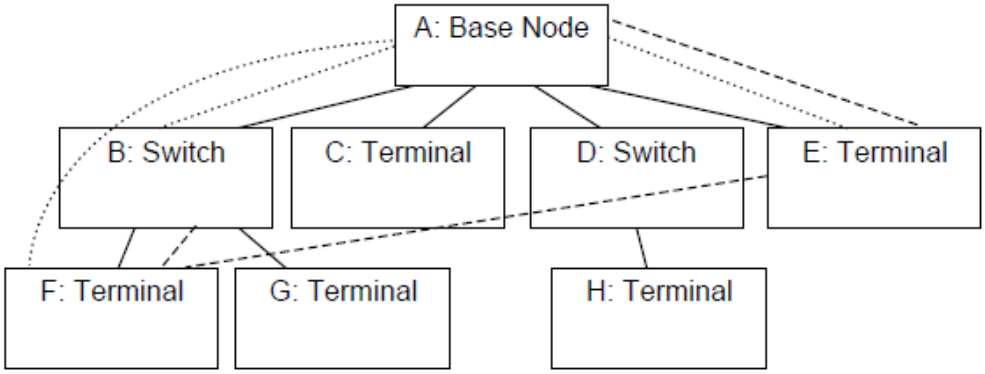


Figura 49. Ejemplo de conexiones usando IPv4 SSCS [11]

Resolución de direcciones

La capa IPV4 SSCS es la responsable de determinar a qué nodo de servicio se debe enviar el paquete utilizando la dirección IPv4 que aparece en la cabecera de este.

Cuando se trata de un paquete *unicast* se debe traducir la dirección IPv4 a una dirección EUI-48. El nodo de servicio debe establecer una conexión con el servicio de resolución de direcciones del nodo base estableciendo en el campo TIPO el calor TIPO_CL_IPv4_AR.

Para el registro y el deregistro el nodo de servicio utiliza el mensaje AR_REGISTER_S para registrar la dirección IPv4 junto con la correspondiente dirección EUI-48. Esta información queda almacenada en las tablas que se sitúan en el nodo base. Pueden existir múltiples direcciones IPv4 asociadas a una misma dirección EUI-48. De la misma forma, si se desea deregistrar enviará un mensaje tipo AR_DEREGISTER_S y el nodo base eliminará esa entrada de su tabla.

Para direcciones *broadcast* el nodo base establece un mapeo entre la dirección 255.255.255.255 y una conexión con LCID de valor LCI_CL_IPv4_BROADCAST. Todas las direcciones IPv4 tipo *broadcast* enviarán el paquete a todos los dispositivos dentro de la

subred. El receptor de este paquete deberá revisar que la dirección IPv4 pertenece a la subred, sólo en ese caso aceptará el paquete.

De la misma forma las direcciones *multicast* las direcciones IPV4 *multicast* se mapean a una conexión MAC *multicast* a través del nodo base utilizando el protocolo de resolución de direcciones. En este caso lo importante para enviar un paquete es establecer un LCID apropiado. El mapeo no se hará con direcciones como en el caso del *broadcast* o *unicast*, el mapeo se establece con direcciones LCID y para ello el dispositivo debe haberse unido al grupo previamente.

Es importante tener en cuenta que el protocolo IP es un protocolo no orientado a conexión y que por tanto no proporciona mecanismos para el control del estado de los paquetes/calidad de la comunicación. Es necesario implementar otras funcionalidades como ARQ en caso de que se quiera establecer una comunicación confiable.

Transmisión de paquetes

Para poder transmitir paquetes se debe establecer una conexión entre la fuente y el destino. La capa IPV4 SCSS examinará cada paquete IPV4 para determinar la dirección a la que debe ir dirigido. Además, es capaz de reutilizar conexiones ya establecidas sin necesidades de cerrarlas y volverlas a abrir. Para ello incorpora una tabla donde almacena la siguiente información:

Tabla 20. Entradas de la tabla IPV4

Parámetro	Descripción
CL_IPv4_Con.Remote_IP	Dirección IPv4 remota
CL_IPv4_Con.ConHandle	MAC Connection handle
CL_IPv4_Con.LastUsed	Instante de tiempo registrado del último paquete recibido/enviado
CL_IPv4_Con.HC	Esquema de compresión de cabeceras utilizado
CL_IPv4_CON.RxSeq	Secuencia esperada para el siguiente paquete recibido

CL_IPv4_CON.TxSeq	Numero de secuencia del próximo paquete a enviar

Calidad de servicio

El protocolo MAC de PRIME especifica que el mecanismo de acceso usando tiempos de contención puede soportar cuatro niveles de prioridad. El nivel 1 es el utilizado para mensajes de control MAC pero no sólo para ello. Los paquetes IPv4 incluyen un parámetro, conocido como TOS, en la cabecera para indicar la QoS del paquete. A continuación se presenta la Tabla 21donde se muestra cuál es el mapeo entre los niveles de QoS de IPv4 y PRIME.

Tabla 21. Mapeo de QoS entre IPV4 y la capa MAC de PRIME

IPV4	**MAC**
000 – Routine	3
001 – Priority	3
010 – Immediate	2
011 – Flash	2
100 – Flash Override	1
101 – Critical	1
110 – Internetwork Control	0
111 – Network Control	0

Tipos de paquetes

El formato de las PDUs de la capa IPV4 SSCS sigue siempre un mismo patrón con pequeñas excepciones en alguno de los paquetes. A continuación se presenta la Tabla 22 donde se definen los tipos de paquetes y los campos que engloban.

Tabla 22. Tipos de paquetes IPV4

Mensaje	Campo	Longitud (bits)	Descripción
AR_REGISTER_S	AR.MSG	8	Tipo de mensajes. En este caso 0.
	AR.IPV4	32	Dirección a regitrar
	AR.EUI-48	48	Dirección a registrar
AR_REGISTER_B	AR.MSG	8	Tipo de mensajes. En este caso 1.
	AR.IPV4	32	Dirección registrada
	AR.EUI-48	48	Dirección registrada
AR_UNREGISTER_S	AR.MSG	8	Tipo de mensajes. En este caso 2.
	AR.IPV4	32	Dirección a deregistrar
	AR.EUI-48	48	Dirección a deregistrar
AR_UNREGISTER_B	AR.MSG	8	Tipo de mensajes. En este caso 3.
	AR.IPV4	32	Dirección deregistrada
	AR.EUI-48	48	Dirección deregistrada
AR_LOOKUP_S	AR.MSG	8	Tipo de mensajes. En este caso 4.
	AR.IPV4	32	Dirección a buscar
AR_LOOKUP_B	AR.MSG	8	Tipo de mensajes. En este caso 5.
	AR.IPV4	32	Dirección a buscar
	AR.EUI-48	48	Dirección a buscar

	AR.Status	8	Indica si se en control (0) o no (1)
AR_MCAST_REG_S	AR.MSG	8	Tipo de mensajes. En este caso 8.
	AR.IPV4	32	Dirección multicast a registrar
AR_MCAST_REG_B	AR.MSG	8	Tipo de mensajes. En este caso 9.
	AR.IPV4	32	Dirección multicast registrada
	Reserved	2	Reservado
	AR.LCID	6	LCID asignado
AR_MCAST_UNREG_S	AR.MSG	8	Tipo de mensajes. En este caso 10.
	AR.IPV4	32	Dirección multicast a deregistrar
AR_MCAST_UNREG_B	AR.MSG	8	Tipo de mensajes. En este caso 11.
	AR.IPV4	32	Dirección multicast deregistrada

5.4.3 IPV6 SERVICE-SPECIFIC CONVERGENCE SUBLAYER (IPV6 SSCS)

En lo referente a la especificación PRIME, las diferencias entre el servicio de IPV4 e IPV6 es mínimo, adaptándose únicamente a las peculiaridades de IPV6. El tipo de paquetes a utilizar coinciden, así como las primitivas y la lógica tras ellas. Es por ello que en este apartado no es explicará más detallado sobre este servicio.

Capítulo 6. G3 PLC

6.1 DESCRIPCIÓN GENERAL

El protocolo G3-PLC tiene como uno de sus principios proporcionar mecanismos que garanticen su coexistencia con otras tecnologías PLC. Para ello establece tres mecanismos principales:

- Coexistencia con división de frecuencia: permite eliminar la interferencia con otros dispositivos que implementan el mismo protocolo gracias al uso de planos de bandas ITU-T G.9903.
- *Frecuency notching*: es un mecanismo que permite eliminar las interferencias con otros dispositivos de tipo ITU-T G.9903 dentro de un rango particular al hacer "muescas" a un o varias subportadoras.
- Mecanismo de preámbulo: permiten garantizar que el acceso al medio es justo y que se puede convivir con otras tecnologías PLC que operen sobre la misma banda de frecuencias.

6.2 CAPA PHY

La línea de potencia es un canal muy hostil. Sus características y parámetros pueden variar con la frecuencia, la localización, el tiempo y el tipo de dispositivo que esté conectado. OFDM puede hacer un uso efectivo de canales con anchos de banda limitados permitiendo el empleo de técnicas de codificación más sofisticadas. Esta combinación permite que se establezcan líneas de comunicación muy robustas a través de las líneas de potencia.

El ancho de banda disponible se divide en un número de sub portadoras concreto. Sobre éstas, se aplica la codificación convolucional y Reed-Solomon para proporcionar redundancia de bits que hagan al sistema más robusto frente a la perdida de información causada por el ruido de fondo o impulsivo. También se aplica *interleaving* a fin de reducir

la correlación entre el ruido y una secuencia de bits recibida (reduciendo así los errores de ráfaga).

La señal OFDM se genera a través de la transformada inversa de Fourier (IFFT por sus siglas en inglés), sobre los bits ya codificados utilizando esquemas diferenciales. El símbolo OFDM se construye gracias a la adición de un prefijo cíclico al principio de cada bloque generado por la IFFT. La longitud de este prefijo se escoge de tal manera que no exista excesiva interferencia entre símbolos OFDM sucesivos.

En la *Figura 50* se puede ver el diagrama de bloques que conforma el protocolo G3.

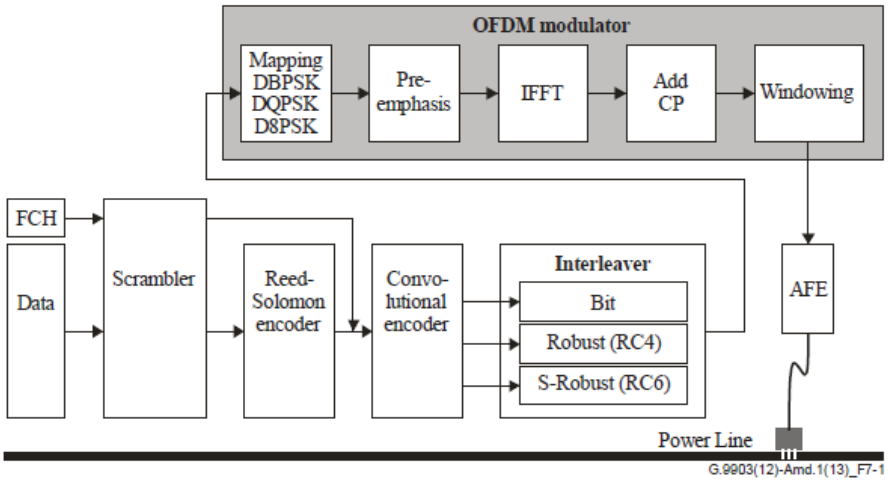


Figura 50. Diagrama de bloques del protocolo G3-PLC [12]

6.2.1 PARÁMETROS DEL SISTEMA

Al tratar con modulaciones diferenciales, el diseño del receptor se vuelve mucho más sencillo en comparación con otro tipo de modulaciones. Las fases de las subportadoras consecutivas se utilizan como referencia para obtener la fase de la portadora actual. El número máximo de subportadoras es 128, resultando en un tamaño de IFFT de 256 como máximo. Esto implica una separación de 1.5625 kHz (Fs/N) entre subportadoras en el plano CENELEC y 4.6875 kHz (Fs/N) para el plano FCC, donde Fs es la frecuencia de muestreo y N es el tamaño de la IFFT.

El sistema trabaja en dos modos distintos, conocido como modo normal y modo robusto. En el modo normal el FEC se compone de un codificador Red-Solomon y codificador convolucional. En el modo Robusto, el FEC está compuesto por un Red-Solomon, codificador convolucional y código de repetición (RC) que repite cada bit cuatro veces de tal forma que el sistema se vuelve más Robusto.

La tasa de datos se calcula en base al número de símbolos transmitidos por cada paquete PHY (N_S), el número de sub portadoras (N_{CAR}) y el número de bits de paridad añadidos en el bloque FEC.

Banda CENELEC-A

La banda CENELEC-A engloba desde 3kHz a 95kHz El número de símbolos transmitidos en cada paquete PHY se selecciona en base a dos parámetros, la tasa de datos requerida y el nivel de Robustez mínimo requerido. En la *Tabla 23 Tabla 24 Tabla 25* se pueden ver los valores.

Tabla 23. Tamaño del bloque Red-Solomon según la modulación

CENELEC-A Número de símbolos	**Reed-Solomon bloques (bytes) D8PSK**	**Reed-Solomon bloques (bytes) DQPSK**	**Reed-Solomon bloques (bytes) DBPSK**	**Reed-Solomon bloques (bytes) Robusto**
12	(80/64)	(53/37)	(26/10)	-
20	(134/118)	(89/73)	(44/28)	-
32	(215/199)	(143/127)	(71/55)	-
40	-	(179/163)	(89/73)	(21/13)
52	-	(233/217)	(116/100)	(28/20)
56	-	(251/235)	(125/109)	(30/22)
112	-	-	(251/235)	(62/54)

252	-	-	-	(141/133)

Tabla 24. Tabla 20. Tasa de datos en función de la modulación (sin incluir FCH)

CENELEC-A	**Tasa de datos en función de la modulación, bit/s**			
Número de símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	21 829	12 619	3 410	-
20	32 534	20 127	7 720	-
32	42 619	27 198	11 778	-
40	-	30 385	13 608	2 423
52	-	33 869	15 608	3 121
56	-	34 792	16 137	3 257
112	-	-	20 224	4 647
252	-	-	-	5 592

Tabla 25. Tasa de datos según la modulación (incluyendo FCH)

CENELEC-A	**Tasa de datos en función de la modulación, bit/s**			
Símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	23 235	14 026	4 817	-
20	33 672	21 264	8 857	-
32	43 501	28 081	12 662	-
40	-	31 154	14 377	3 192

52	-	34 513	16 252	3 765
56	-	35 402	16 748	3 867
112	-	-	20 579	5 002
252	-	-	-	5 765

Banda CENELEC-B

La banda CENELEC-B va de los 95kHz a 125 kHz. El número de símbolos, el tamaño de bloque del codificador Red-Solomon y las tasas de datos asociadas con 16 tonos se presentan en la Tabla 26, la Tabla 27 y la Tabla 28.

Tabla 26. Tamaño del bloque Red-Solomon en función de la modulación

CENELEC B	**Bloque Reed-Solomon (bytes)**			
Símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	35/19	23/7	-	-
20	59/43	39/23	19/3	-
32	95/79	63/47	31/15	-
40	119/103	79/63	39/23	9/1
52	155/139	103/87	51/35	12/4
56	167/151	111/95	55/39	13/5
112	-	223/207	111/95	27/19
252	-	-	251/235	62/54

Tabla 27. Tasa de datos en función de la modulación (sin FCH)

CENELEC B	**Tasa de datos en función de la modulación, bps**			
Símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	4309	1587	-	-
20	8425	4506	587	-
32	12853	7646	2440	-
40	15055	9208	3361	146
52	17631	11035	4439	507
56	18344	11541	4738	607
112	-	15806	7253	1450
252	-	-	9303	2137

Tabla 28. Tasa de datos en función de la modulación (incluyendo FCH)

CENELEC B	**Tasa de datos en función de la modulación, bps**			
Símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	5245	2523	-	-
20	9233	5314	1396	-
32	13524	8318	3111	-
40	15658	9811	3964	749
52	18154	11558	4962	1030
56	18845	12042	5239	1108
112	-	16121	7568	1765

252	-	-	9467	2301

Banda FCC

La banda FCC va desde los 10 a los 490 kHz. La separación entre las subportadoras es de 4.6875 kHz y el número de subportadoras útiles es 72. DBPSK, DQPSK y D8PSK, son los esquemas de modulación que soporta esta banda, lo que da lugar a una tasa de bits de hasta 300 bits/s operando en el modo normal. El número de símbolos en cada paquete PHY depende de la tasa de datos requerida y del nivel de Robustez especificado.

Tabla 29. Bloque RS en función de la modulación

FCC	**Bloque Reed-Solomon (bytes)**			
Símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	(161/145)	(107/91)	(53/37)	(12/4)
20	-	(179/163)	(89/73)	(21/13)
28	-	(251/235)	(125/109)	(30/22)

Tabla 30. Tasa de datos en función de la modulación (excluyendo FCH)

FCC	**Tasa de Datos (bit/s)**			
Símbolos	**D8PSK**	**DQPSK**	**DBPSK**	**Robusto**
12	152,899	95,957	39,015	4,217
20	-	138,135	61,864	11,016
28	-	166,469	77,213	15,584

Máxima Longitud de PSDU

La longitud máxima de PSDU en bytes que se puede obtener utilizando el protocolo G3 es una función que depende de la configuración PHY establecida en base al número de sub-portadoras disponibles por cada símbolo OFDM (N_{CAR}), el tipo de modulación (MOD) y otros parámetros.

$$N_S = FL_{Band} x \min[FL_{max}, ceil(\frac{(MaxRSBlockSize\ x\ 8 + CC_{ZeroTail}) x\ Rep\_Code}{FL_{Band}\ x\ N_{CAR}\ x\ mod_{size} x\ CC_{Rate}})]$$

Donde:

- MaxRSBloquesize = 255 bytes
- Ns es el número de símbolos por paquete PHY
- CC_{Rate}=0.5
- $CC_{ZeroTail}$=6
- FL_{Band}=4 para los planes CENELEC y 1 para FCC
- FL_{max} = es la longitud máxima de paquete posible.
- Rep_Code hace referencia al tamaño del bloque repetidor (4 para el modo robusto y 1 para el resto)
- Mod_size el número de bits por constelación
    - 1 para DBPSK o BPSK en modo robusto
    - 2 para DQPSK u QPSK
    - 3 para D8PSK u 8PSK
    - 4 para 16QAM

Estructura de los paquetes

Los paquetes PHY soportan dos tipos de tramas. La trama típica para OFDM se presenta en la ***Error! Reference source not found.***. Cada paquete comienza con un preámbulo que se utilizado con fines de sincronización y detección. SYNCP hace referencia a los símbolos que se multiplican por +1 en la función *sign* y SYNCM hace referencia a los que se multiplican por -1. El preámbulo consiste en ocho SYNCP seguidos de un símbolo y

medio SYNCM sin prefijo cíclico entre símbolos adyacentes. Este es seguido por 13 símbolos de información situados en el FCH (*Frame Control Header*). Ahí se almacena toda la información necesaria para proceder a la demodulación. Tras ello vienen los símbolos que transportan datos.

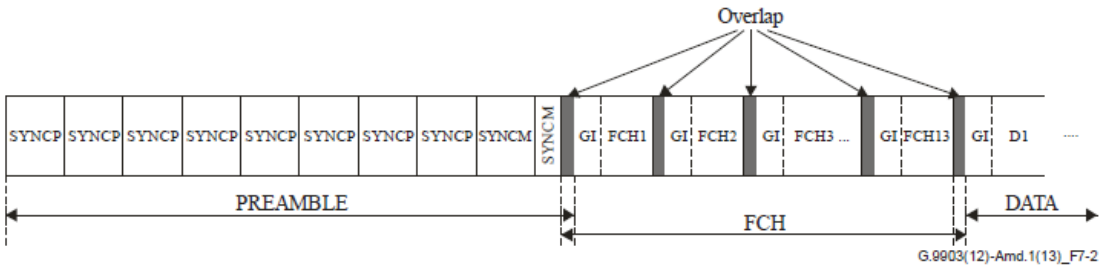


Figura 51. Estructura de un paquete de datos [12]

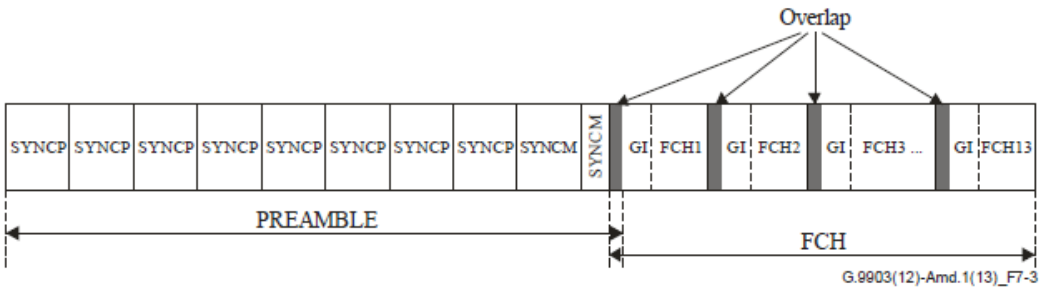


Figura 52. Estructura de un paquete ACK/NACK [12]

Preámbulo

Es preámbulo está compuesto por ocho símbolos SYNCP idénticos y 1 ½ símbolo SYNCM idénticos. Cada uno de ellos tiene 256 muestras y se almacena previamente en el transmisor. Se transmiten justo antes de transmitir la información. Los símbolos SYNCM son idénticos a los SYNCP con la diferencia de que la fase está desplazada π. En el receptor, la distancia entre los símbolos SYNCP y SYNCM se utiliza para la sincronización.

Todos los símbolos en el preámbulo deben tener el mismo factor de ganancia en comparación con los símbolos de datos. La ganancia se establece a 3dB.

Cabecera de control (FCH)

El FCH es una estructura de datos transmitida al principio de cada paquete PHY de datos que contiene información referente al correspondiente paquete. Incluye información sobre el tipo de paquete, el tono al que mapea, el índice del paquete, la longitud, etc. Los datos del FCH están protegidos con CRC5 para CENELEC y CRC8 para FCC.

Los trece símbolos transmitidos inmediatamente después del preámbulo se utilizan para la cabecera de control (FCH). Se transmiten en el modo super robusto. Los planos se dividen en sub-bandas (grupos de tonos) para poder adaptarse de forma selectiva a la calidad del canal. Cada sub-banda contiene seis tonos. Cada bit del tono se asocia a una sub-banda, indicando si lleva información o no.

Tabla 31. Campos de FCH para CENELEC

Campo	Byte	Bit número	Bits	Descripción
PDC	0	7-0	8	Contador de detección de fase
MOD	1	7-6	2	Tipo de modulación: 0: Robusto 1: DBPSK o BPSK 2: DQPSK o QPSK 3: D8PSK o 8-PSK
FL	1	5-0	6	Longitud en símbolos PHY
Reservado por ITU-T	2	7-6	2	Debe ser 0

TM[5:0]	2	5-0	6	TM[5:0] – Mapa de tono En CENELEC-B reservados.
Esquema de modulación del *payload*	3	7	1	0: Diferencial 1: Coherente
DT	3	6-4	3	Tipo de delimitador: 0: Inicio de un paquete sin respuesta esperada. 1: Inicio de un paquete con respuesta esperada 2-7: Reservado por ITU-T
FCCS	3	3-0	4	Secuencia de control de paquete (CRC5)
	4	7	1	
ConvZeros	4	6-1	6	6 ceros para el codificador convolucional

Tabla 32. Mapa de tonos para CENELEC

Mapa de tono Campo	**CENELEC-A**	**CENELEC-B**
TM[0]	35.9375 to 43.75 kHz	98.4375 to 106.25 kHz
TM[1]	45.3125 to 53.125 kHz	107.8125 to 115.625 kHz
TM[2]	54.6875 to 62.5 kHz	117.1875 to 121.875 kHz
TM[3]	64.0625 to 71.875 kHz	Sin uso en la banda Cenelec-B
TM[4]	73.4375 to 81.25 kHz	Sin uso en la banda Cenelec-B
TM[5]	82.8125 to 90.625 kHz	Sin uso en la banda Cenelec-B

Tabla 33. Campos de FCH para paquetes ACK/NACK en CENELEC

Campo	Byte	Bit número	Bits	Descripción
FCS-1	0	7-0	8	MAC FCS[7:0]
SSCA	1	7	1	Para evitar la collision con otros segmentos 0: No hay más segmentos 1: Hay más segmentos
Reservado por ITU-T	1	6-0	7	Debe ponerse a 0
FCS-2	2	7-0	8	MAC FCS[15:8]
Reservado por ITU-T	3	7	1	Debe ponerse a 0
DT	3	6-4	3	Tipo de delimitador: 0-1: Reservado por ITU-T 2: ACK 3: NACK 4-7: Reservado por ITU-T
FCCS	3	3-0	4	Secuencia de control de paquete (CRC5)
	4	7	1	
ConvZeros	4	6-1	6	6 ceros para el codificador convolucional

El código de redundancia CRC5 se utiliza para la detección de errores en el FCH. Se calcula utilizando la siguiente fórmula por donde pasan los bits empezando por el primer byte más significativo. El CRC5 es el resto obtenido de la división entre el polinomio inicial (0b11111) y el polinomio FCH.

$$G(x) = x^5 + x^2 + 1$$

En el caso de la banda FCC se transmiten doce símbolos después de preámbulo y estos constituyen la cabecera FCH. Se transmiten en modo super Robusto y utilizando BPSK con modulación "*Coherente"*, es decir, necesita que la señal de reloj del receptor esté sincronizada en fase con la del transmisor.

Tabla 34. Campos FCH para paquetes en la banda FCC

Campo	Byte	Bit Número	Bits	Descripción
PDC	0	7-0	8	Contador para la detección de fase
MOD	1	7-5	3	Tipo de modulación 0:Robusto (diferencial o Coherente) 1: DBPSK o BPSK 2: DQPSK o QPSK 3: D8PSK o 8-PSK 4: 16-QAM 5-7: Reservado por ITU-T
Esquema de modulación del *payload*	1	4	1	Esquema de modulación: 0: Diferencial 1: Coherente
DT	1	3-1	3	Tipo de delimitador: 0: Inicio de un paquete sin respuesta 1: Inicio de un paquete con respuesta esperada

FL	2	0 7-0	1 8	Longitud del paquete en símbolos PHY
TM[7:0]	3	7-0	8	TM[7:0]: Mapa de tono
TM[15:8]	4	7-0	8	TM[15:8]: Mapa de tono
TM[23:16]	5	7-0	8	TM[23:16]: Mapa de tono
Reservado por ITU-T	6	7-5	3	Debe ponerse a 0
Two RS Bloques	6	4	1	0: El transmisor está transmitiendo dos bloques RS. 1: El transmisor está transmitiendo uno.
Reservado por ITU-T	6	3-0	4	Debe ponerse a 0
Reservado por ITU-T	7	7-6	2	Debe ponerse a 0
FCCS	7 8	5-0 7-6	6 2	Secuencia de control de paquete (CRC8)
ConvZeros	8	5-0	6	Ceros para el codificador convolucional

Tabla 35. Campos FCH para paquetes ACK/NACK en FCC

Campo	Byte	Bit Número	Bits	Descripción
FCS-1	0	7-0	8	MAC FCS[7:0]
SSCA	1	7	1	Para evitar la collision con los siguientes segmentos 0: No se esperan más segmentos

				1: Se esperan más segmentos
Reservado por ITU-T	1	6 – 4	3	Debe ponerse a 0
DT	1	3 - 1	3	Tipo de delimitador: 0-1 : Reservado por ITU-T 2: ACK 3: NACK 4-7: Reservado por ITU-T
Reservado por ITU-T	1	0	1	Debe ponerse a 0
Reservado por ITU-T	2	7-0	8	Debe ponerse a 0
FCS-2	3	7-0	8	MAC FCS[15:8]
Reservado por ITU-T	4	7-0	8	Debe ponerse a 0
Reservado por ITU-T	5	7-0	8	Debe ponerse a 0
Reservado por ITU-T	6	7-0	8	Debe ponerse a 0
Reservado por ITU-T	7	7-6	2	Debe ponerse a 0
FCCS	7	5-0	6	Secuencia de control de paquete (CRC8)
	8	7-6	2	
ConvZeros	8	5-0	6	Ceros para el codificador convolucional

El código de redundancia CRC8 se utiliza para la detección de errores en la cabecera FCH. El polinomio empleado para la obtención de esta secuencia es el siguiente. El polinomio inicial es 0xFF u el código CRC8 es el resto obtenido de la división entre el polinomio FCH y el polinomio inicial.

$$G(x) = x^8 + x^2 + x + 1$$

Scrambler

Este bloque ayuda a aleatorizar la distribución gracias a aplicación de un XOR. La fórmula a la que corresponde este bloque se presenta a continuación, junto con la **Error! Reference source not found.**.

$$S(x) = x^7 \oplus x^4 \oplus 1$$

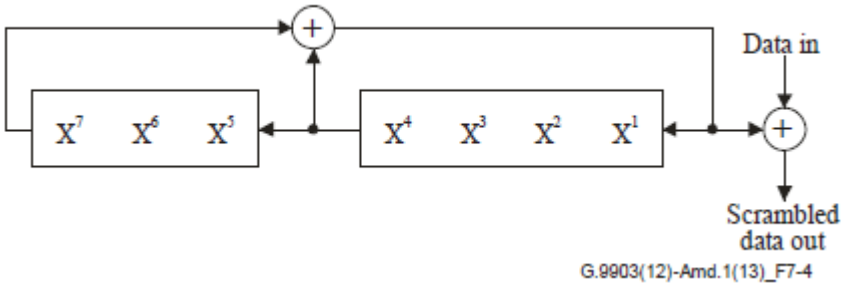


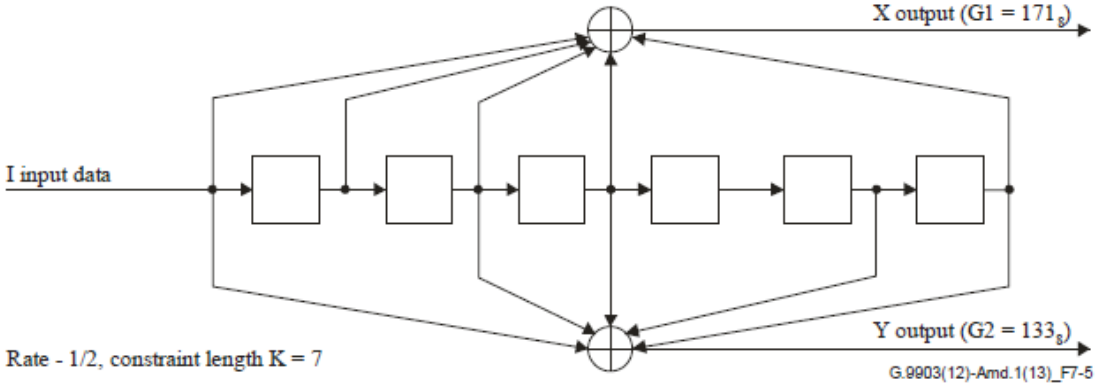
Figura 53. Scrambler [12]

Codificación FEC

El codificador FEC está compuesto por un codificador Reed-Solomon seguido de un codificador convolucional. En el modo robusto se añade un bloque de repetición, conocido como RC4, que rebite cuatro veces cada bit obtenido en la etapa anterior. En el modo súper robusto se utiliza RC6.

Codificador convolucional

Este bloque tiene una tasa de 1/2, k=7 y utiliza como conexiones x=0b1111001 y y=0b1011011. Si se desea resetear se introduce una tanda de bits a cero. La estructura de



este bloque se muestra en la **Error! Reference source not found.**.

Interleaver

Proporciona protección frente a dos tipos de errores:

- Errores en ráfaga que corrompen varios símbolos OFDM consecutivos.
- El desvanecimiento de frecuencia que corrompe varias frecuencias adyacentes y por tanto a un gran número de símbolos OFDM.

Figura 54. Estructura del codificador convolucional [12]

Para poder luchar contra ambos problemas al mismo tiempo, el *interleaver* se aplica en dos pasos. En el primero cada columna se desplaza de manera circular un número de veces dado. De esta forma un símbolo OFDM corrupto se dispersa sobre diferentes símbolos. En el segundo paso, cada fila se desplaza de manera circular un número dado de veces, lo que previene del error por desvanecimiento de frecuencia.

Para la modulación DBPSK o BPSK, la matriz permutadora corresponde a la matriz base mientras que con otras modulaciones se utiliza ésta misma un número determinado de veces hasta que consigue el tamaño necesario.

Tras este paso, los módulos encargados de hacer el mapeo para la modulación leen la matriz fila a fila.

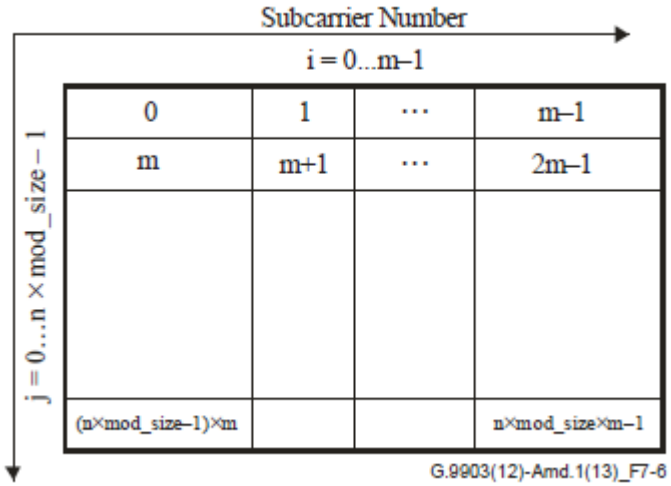


Figura 55. Organización de los bits en la matriz de permutación [12]

Windowing

Con el fin de reducir la emisión fuera de banda y lóbulo espectral, el coseno alzado se aplica a los símbolos que transmiten datos. La cola y cabeza de los símbolos consecutivos se superponen y se suman.

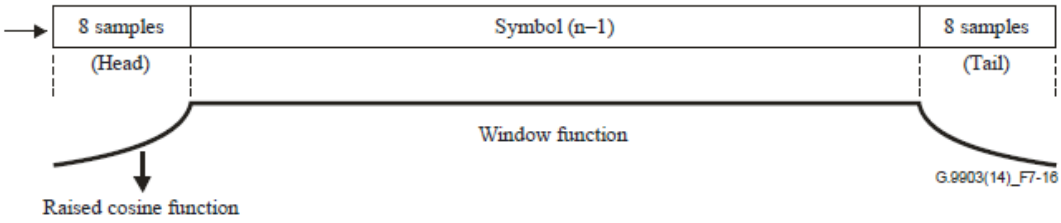


Figura 56. Ejemplo de windowing [12]

Mapeo de tonos

El mapeo de tonos es un parámetro adaptativo que, en función de la estimación del canal, contiene una lista de las sub-portadoras que pueden utilizarse para la comunicación. Los dispositivos ITU-T G.9903 deben estimar el nivel SNR de la señal recibida y adaptarse, seleccionando los tonos que pueden emplearse, la modulación óptima y la tasa de datos que pueden garantizar una comunicación confiable. También debe especificar que nivel de potencia debe usar el transmisor y que valores de ganancia.

El objetivo principal de este mapeo es conseguir que el receptor reciba una señal lo mejor posible dadas unas condiciones en el canal. Para ello, el receptor debe informar al transmisor sobre cuáles son los tonos que debe utilizar para la transmisión y cuáles deben ser *dummy*. El transmisor debe informar sobre cuánta amplificación o atenuación debe aplicar el receptor a cada uno de estos tonos.

Para los tonos que no llevan información, la función que realiza el mapeo debe emplear un código binario que obtiene de una secuencia de pseudo ruido. El elemento generador de esta secuencia se presenta en la *Figura 57*.

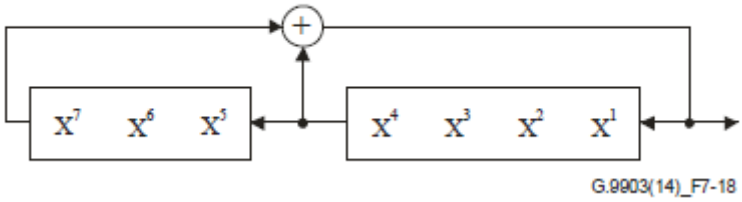


Figura 57. Generador del código de pseudo ruido [12]

Esquema de modulación Coherente

Para la banda CENELEC, los dispositivos operan utilizando la modulación diferencia para FCH y *payload*. Sin embargo, el dispositivo tal vez soporte la modulación coherente para el *payload*. En tal caso podría ser requerido que aplicase este sistema de modulación.

En la banda FCC, el FCH se codifica utilizando el modo super robusto con modulación BPSK.

De manera similar al modo diferencia, el modo coherente debe soportar dos tipos de paquetes: de datos y ACK/NACK. En el caso de los paquetes de datos, la porción de datos del paquete PHY debe ir precedida de un símbolo y seguida de otro donde ambos símbolos deben insertarse entre el último símbolo FCH y el primer símbolo con datos. El símbolo que va al final debe tener la misma fase de referencia que se utilizaría en el modo diferencial para un símbolo SYNCP. Los tonos piloto deben ir en los símbolos de datos. La estructura de un paquete ACK/NACK debe ser la misma que la utilizada para el esquema diferencial.

En un esquema Coherente el preámbulo está compuesto por 8 símbolos SYNCP idénticos seguidos de un símbolo SYNCM y medio.

Los tonos piloto se pueden utilizar en el modo Coherente para ayudar con la recuperación del reloj y la estimación del canal. En particular son útiles con el medio es hostil y hay fuertes ruidos y variaciones de frecuencia. Estos pilotos sólo se deben insertar en los símbolos de datos, no en los de FCH.

6.2.2 PRIMITIVAS

Datos

La recepción de una primitiva PD-DATA.request por una entidad PHY da lugar a la transmisión de un PSDU. Primero se construye el PPDU conteniendo la PSDU y después se transmite. Una vez transmitida la respuesta, es necesario preparar la primitiva PD-DATA.confirm para garantizar que se ha recibido la respuesta. De la misma forma, la recepción de una primitiva PD-ACK.request da lugar a la transmisión de un ACK/NACK.

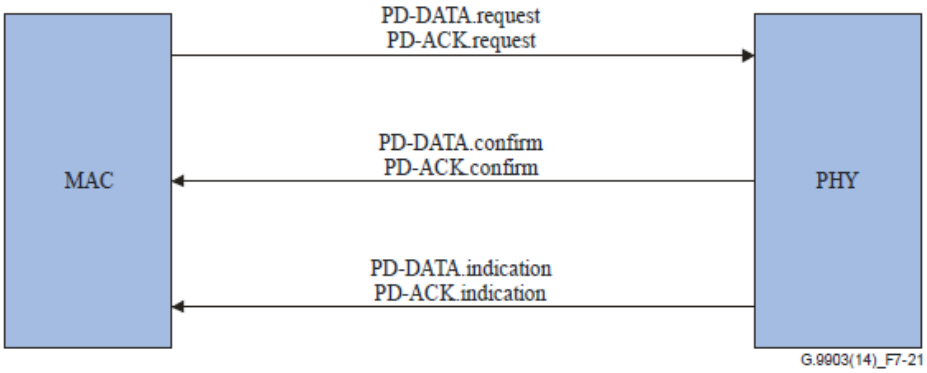


Figura 58. Flujo de primitivas de datos o ACK [12]

Tabla 36. Parámetros de PD-DATA.request

Nombre	Tipo	Rango	Descripción
psduLength	Integer	0x00-0xEF en CENELEC 0x00-0x1EE en FCC	Número de bytes que hay en el PSDU listos para ser transmitidos por la entidad PHY
Psdu	Integer Array	Ninguno	Conjunto de bytes que conforman la PSDU listos para ser transmitidos en la petición de la entidad PHY

Tabla 37. Parámetros de PD-DATA.confirm

Nombre	Tipo	Rango	Descripción
Status	Enumeración	SUCCESS, BUSY_RX, BUSY_TX, FAILED	Resultado de la petición para transmitir un paquete

Tabla 38. Parámetros de PD-DATA.indication

Nombre	Tipo	Rango	Descripción
psduLength	Integer	0x00-0xEF en CENELEC 0x00-0x1EE en FCC	Número de bytes que hay en el PSDU recibidos por la entidad PHY
Psdu	Integer	–	Conjunto de bytes que conforman la PSDU recibida
ppduLinkQuality	Integer	0x00-0xFF	Calidad del enlace medida en la recepción

Tabla 39. Parámetros de PD-ACK.request

Nombre	Tipo	Rango	Descripción
FCH	Structure	Clause 7.6 PHY	La capa MAC proporciona todos los parámetros necesarios para contruir la cabecera de control FCH en el paquete ACK

Tabla 40. Parámetros de PD-ACK.confirm

Nombre	Tipo	Rango	Descripción
Status	Enumeration	SUCCESS, BUSY_RX, BUSY_TX, FAILED	Confirmación de la transmission de un paquete ACK

Tabla 41. Parámetros de PD-ACK.indication

Nombre	Tipo	Rango	Descripción
FCH	Structure	Clause 7.6 PHY	La capa MAC recibe el paquete

Primitivas de gestión

Hay dos tipos de primitivas de gestión: *Get* y *Set*. Se utilizan para iniciar comandos o recoger información de la capa PHY.

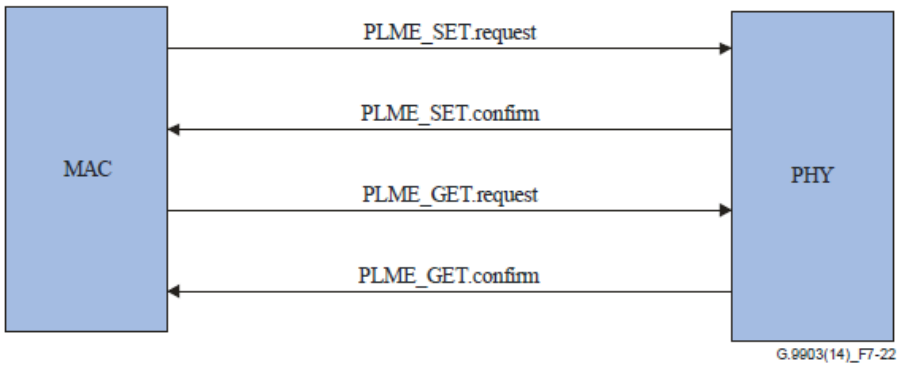


Figura 59. Primitivas de gestión [12]

Tabla 42. Parámetros de PLME_SET.request

Nombre	Tipo	Rango	Descripción
TXPower	Integer	0x00-0x20	La capa MAC notifica a la entidad PHY sobre la ganancia/potencia que debe usar al transmitir el siguiente paquete
PayloadModulationTipo	Integer	0x0-0x4	Configura la modulación del paquete 0 : Modo robusto 1 : DBPSK o BPSK 2 : DQPSK o QPSK 3 : D8PSK o 8-PSK
PayloadModulationScheme	Integer	0x0–0x1	Define si el esquema de modulación debe ser diferencial o Coherente 0 : Diferencial 1 : Coherente

ToneMap	Array	0x0-0x1	Utilizado para hacer el mapeo de tonos. Un valor 0 indica que en esta sub-portadora no se debe transmitir información. El valor 1 indica que sí se debe transmitir información.
PreEmphasis	Array	0x00-0x1F	Identifica la ganancia de cada sub-portadora
ToneMask	Array	0x0-0x1	Identifica si el tono es inservible o si es válido.
DT	Integer	0x00-0x07	Tipo de delimitador.

Tabla 43. Parámetros de PLME_SET.confirm

Nombre	Tipo	Rango	Descripción
TXPower	Integer	0x00-0x20	Devuelve el valor almacenado a la capa MAC
PayloadModulationTipo	Integer	0x0-0x04	Devuelve el valor almacenado a la capa MAC. Identifica la modulación
			0 : Modo Robusto
			1 : DBPSK o BPSK
			2 : DQPSK o QPSK
			3 : D8PSK o 8-PSK
			4 : 16-QAM
PayloadModulationScheme	Integer	0x0-0x1	Define el dipo de esquema a emplear, diferencial o Coherente
			0 : Diferencial
			1 : Coherente

ToneMap	Array	0x0-0x1	Devuelve el valor almacenado a la capa MAC
PreEmphasis	Array	0x00-0x1F	Devuelve el valor almacenado a la capa MAC
ToneMask	Array	0x0-0x1	Devuelve el valor almacenado a la capa MAC
DT	Integer	0x00-0x07	Tipo de delimitador.

6.2.3 ESPECIFICACIONES TÉCNICAS DEL TRANSMISOR

Los dispositivos ITU-T G.9903 operan en líneas de voltaje bajo y en líneas de voltaje medio. Cuando operan en líneas de voltaje medio, pueden comunicarse con otros dispositivos que operen en líneas de voltaje bajo. Esto significa que el receptor en baja potencia puede detectar la señal después de haber sido atenuada como resultado del efecto de un transformador de media potencia a baja potencia. Al pasar la señal por el transformador, se espera que ésta sufre atenuación en sus niveles de potencia y también atenuación dependiente de la frecuencia. Para ello tanto el transmisor como el receptor emplean mecanismos que solventan estos problemas.

Un nodo ITU-T G.9903 también puede operar como repetidor, puede decodificar los paquetes que recibe, analizarlos y enviarlos a una señal de potencia mayor de forma que se compensa, parcialmente, la atenuación introducida por el transformador.

Los dispositivos trabajan con una interfaz de cara a medio voltaje que consta básicamente de un filtro cuya finalidad es permitir que la señal del PLC pase y al mismo tiempo proteger los equipos de comunicación de altos voltajes y otros posibles problemas que puedan venir causados por operaciones intermedias.

En la *Figura 60* se muestra el diagrama del circuito básico de un dispositivo ITU-T G.9903. Éste incluye un mecanismo que protege al PLC de cortocircuitar. Además incluye un filtro de paso de alto de acoplo que intermediará en el PLC y la línea de voltaje medio.

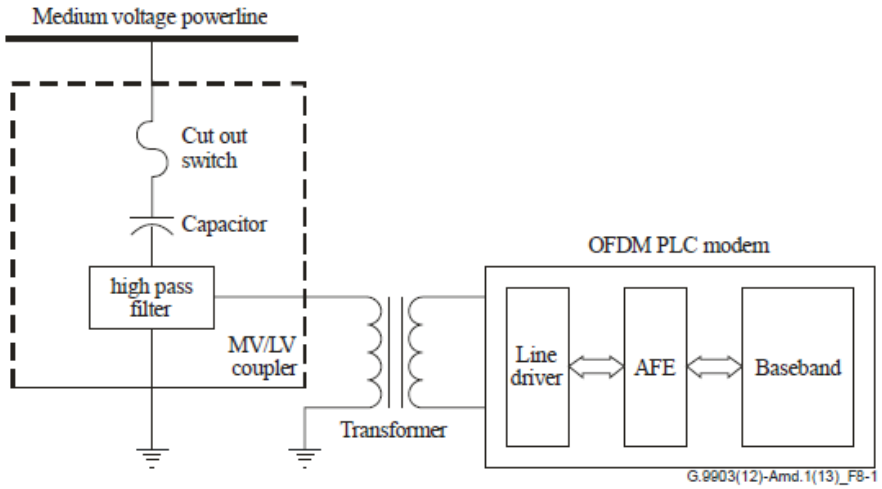


Figura 60. Circuito básico de un dispositivo ITU-T G.9903 [12]

Es necesario conocer en qué fase trabaja cada medidor. Esta información en principalmente útil a nivel de sistema para comprobar si ha habido perdidas inesperadas en la distribución de la línea. Además, esta información proporciona un indicador sobre la presencia de fases neutrales incorrectas que pueden dar lugar a mediciones erróneas.

El receptor proporciona su propia marca de tiempo sobre el paquete recibido y calcula el retardo y la diferencia de fase entre el marcado por el transmisor. Para poder tomar estas mediciones es necesario:

- La capa MAC y PHY deben recibir una señal de detección de cruce por cero montada sobre una sinusoide.
- Todos los dispositivos, incluido el medidor, deben tener un temporizador interno que se sincronice con la señal de detección de cruce por cero.
- Todos los dispositivos deben tener un detector de cruce por cero que genere un pulso de tal forma que el pulso tenga un ancho del 5% del periodo total.

- El pulso generado debe alcanzar el 90% de su valor final con una derivación de tiempo de no más de +5% del ciclo de la línea de potencia.
- La localización del paquete de referencia utilizado para el cálculo de la fase en ambos, transmisor y receptor, debe ir en la primera muestra del campo PHY FCH.

6.3 CAPA MAC

El acceso al canal se implementa gracias al uso de CSMA/CA con tiempo de espera aleatorio. Este tiempo de espera reparte el tiempo entre las estaciones que intenta transmitir de tal forma que se reduce la probabilidad de que dos transmitan al mismo tiempo y los paquetes colisionen.

Una colisión puede ocurrir en cualquiera de las siguientes circunstancias:

- La estación transmisora recibe algo distinto a un paquete ACK/NACK cuando está esperando una respuesta.
- La estación transmisora no recibe nada después de cierto y por tanto llega a la conclusión de que la ausencia de respuesta implica colisión.

6.3.1 ESPACIO ENTRE PAQUETES

Los intervalos de tiempo entre paquetes constituyen el espacio entre paquetes y son necesarios debido a los tiempos de propagación y procesamiento. Los tiempos de contienda en el espacio entre paquetes (CIFS) ocurren después de que haya terminado la transmisión anterior. Además, existe otro intervalo, definido como el intervalo inter-paquete de respuesta (RIFS). Éste es el tiempo entre el final de una transmisión y el inicio de su correspondiente respuesta. Por último también se define un tiempo inter-paquete extendido (EIFS) para las condiciones en las que la estación no conoce completamente cuál es el estado del medio. En la *Figura 61* se muestran estos tres tiempos.

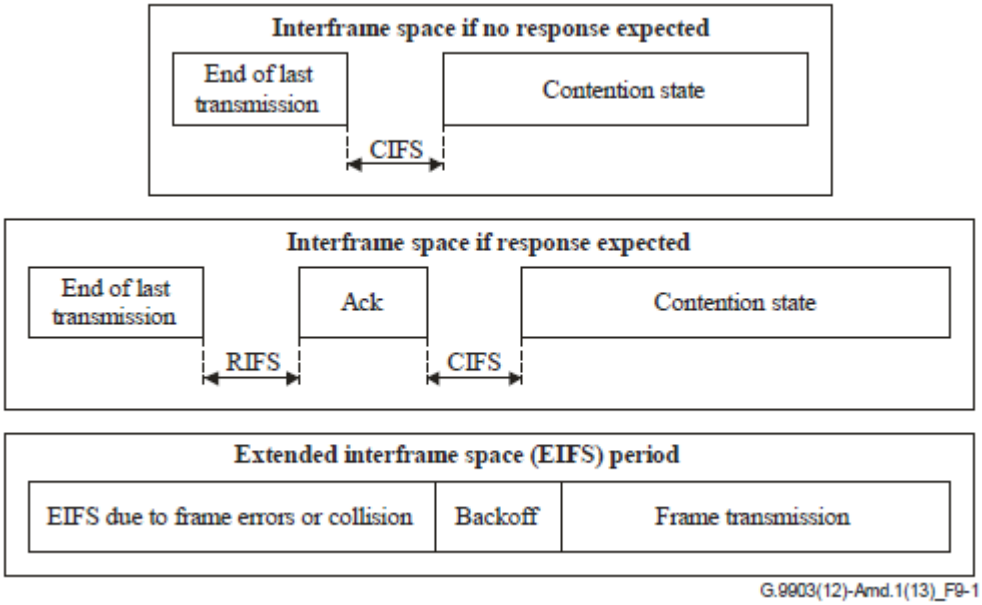


Figura 61. Tiempos inter-paquetes [12]

6.3.2 CSMA/CA

El acceso al canal se hace mediante el mecanismo CSMA/CA. Cuando el canal está ocupado, los dispositivos pueden saberlo gracias al uso de unas portadoras especiales (PCS) que son proporcionadas por la capa PHY. En este caso, una portadora virtual (VCS) se pone en estado *BUSY* y lo comunica a la capa MAC, la que define al medio como *BUSY* también.

Cada dispositivo debe mantener cuatro variables para cada intento de transmisión: NB, NBF, minCWCount y CW. NB es el número de veces que el algoritmo CSMA/CA ha sido requerido cuando se intentaba transmitir un paquete. NBF es el contador que identifica cuantos intentos de tipo *back-off* se han llevado a cabo. minCWCount es el número de veces que la ventana de contención ha llegado al mínimo valor. Por último, CW es la ventana de contención de cada dispositivo.

6.3.3 ESTABLECIMIENTO DE PRIORIDADES

Este protocolo permite definir distintas prioridades de tal manera que el acceso al canal tenga en cuenta estas prioridades. Esta aplicación es muy útil cuando se trata de aplicaciones de tiempo real o de control y se procesa un mensaje urgente. Existen sólo dos niveles de prioridad (alta y normal) de tal manera que se reduce al máximo la complejidad del protocolo. La implementación de estas prioridades se realiza gracias al uso de dos ventanas distintas,

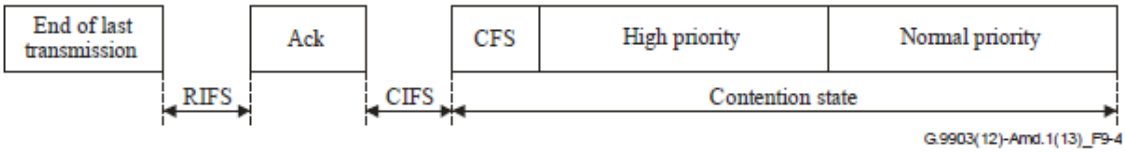


Figura 62. Ventanas de prioridades [12]

El periodo CFS (*Contention Free Slot*) debe utilizarse para transmitir los segmentos de un paquete MAC sin el procedimiento de *back-off* de CSMA/CA. Las estaciones de prioridad alta y normal competirán por el acceso al medio en sus correspondientes ventanas.

6.3.4 ARQ

El mecanismo de respuesta automatizada (ARQ) se implementa basado en el conocimiento y desconocimiento de la retransmisión. La capa MAC utiliza el mecanismo ARQ como tipo de respuesta. ACK es una respuesta positiva tradicionalmente que, al ser recibida, le permite al transmisor asumir que el paquete se ha enviado correctamente. Para el caso contrario está NACK. Las Figura 63 y Figura 64 muestran el diagrama de flujo que explica la transmisión y recepción de ACK y NACK.

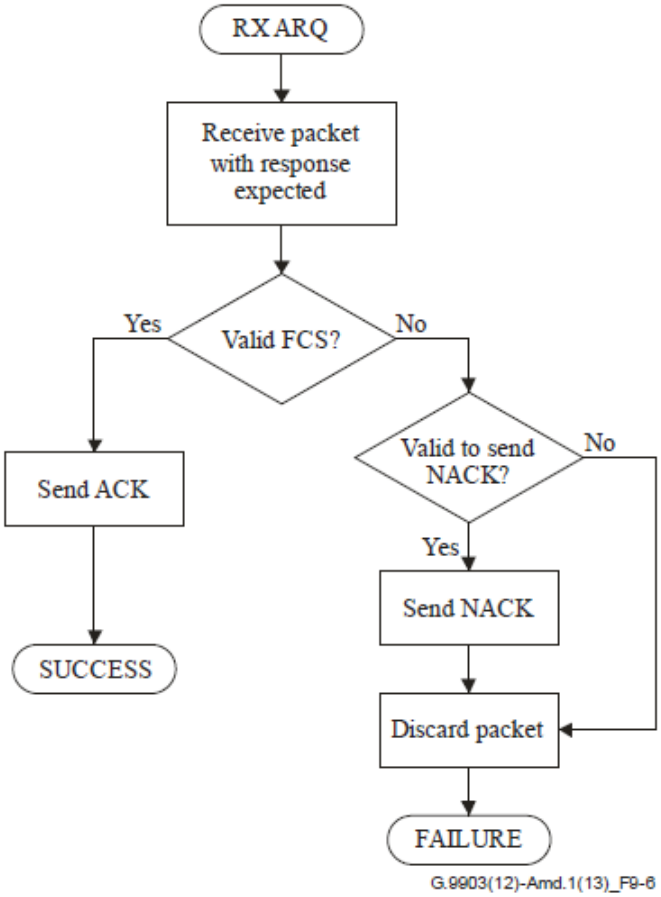


Figura 63. Diagrama sobre la recepción de ARQ [12]

Si el originador no recibe un mensaje de confirmación puede asumir la transmisión no ha ido bien e intentar transmitir de nuevo en el periodo de contienda correcto. Si de nuevo no se recibe ninguna confirmación, el transmisor puede decidir si volver a intentarlo o terminar la comunicación.

En el lado del receptor, el ARQ genera un mensaje de confirmación para el paquete PLC con el FCS correcto si el paquete corresponde con la dirección de lleva el ARQ. En este caso puede generar el paquete NACK sólo cuando el FCS falla, pero la dirección sigue siendo buena. Todos los nodos detectarán el ACK, pero sólo aquel que tenga la dirección adecuada lo procesará como confirmación.

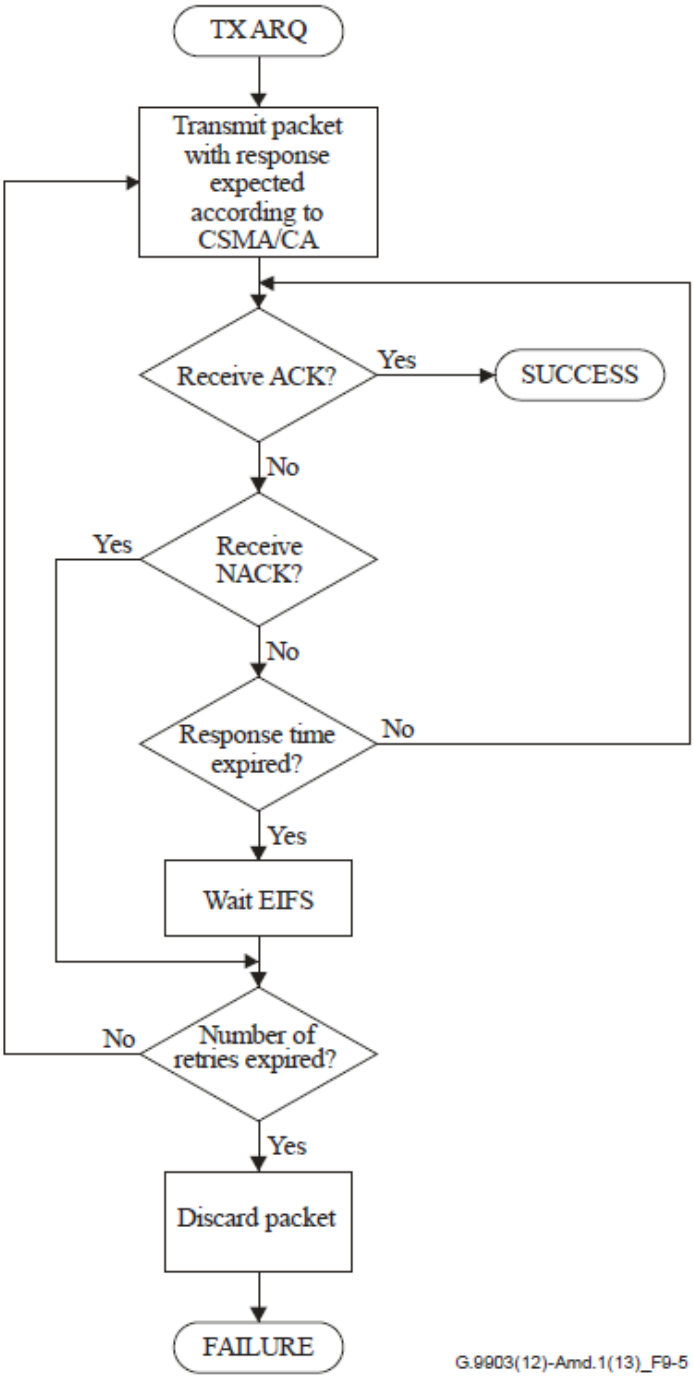


Figura 64. Diagrama de flujo sobre la transmisión de ARQ [12]

6.3.5 SEGMENTACIÓN Y REENSAMBLADO

La capa PHY de ITU-T G.9903 soporta distintos tipos de modulación y mapas de tonos. El número de bytes de datos en el *payload* de un paquete PHY cambia de manera dinámica en base a las condiciones del canal. Esto significa que el *payload* MAC debe poder soportar la fragmentación y el reensamblado. Si el tamaño del *payload* MAC es demasiado grande para entrar en un PSDU *(PHY Service Data Unit),* debe ser partido en segmentos más pequeños que puedan ser transmitidos en un PSDU. La segmentación tal vez requiera la adición de bytes de *padding*. Todo tipo de direccionamiento debe soportar esta característica.

Cuando la segmentación ocurre cada segmento resultante debe cumplir las siguientes características:

- La cabecera MAC y FCS deben estar presentes en todos los segmentos.
- Todos los segmentos deben tener el mismo valor en el campo que indica el número de secuencia
- El contador de segmentos (SC) debe estar a 0 para el primer segmento y de ahí incrementar
- Si se necesita que los datos estén encriptados, la encriptación se debe hacer antes de la segmentación.
- Todos los segmentos exceptuando el último deben tener el campo de control de contención (CC) para informar al receptor de que el siguiente paquete PHY se enviará en el slot de libre contienda siguiente.
- El último segmento debe tener a uno el campo que indica que es último segmento (LSF) para que el receptor pueda proceder al reensamblado.
- La longitud de segmento especifica la longitud del *payload* MAC en bytes para el segmento, sin importar si es un fragmento o no.

6.3.6 OTRAS ESPECIFICACIONES

Muchas de las primitivas y servicios incluidos en la especificación de este protocolo se basan en el estándar IEEE 802.15.4. Es por ello que, para las especificaciones que restan, sólo se hará mención de aquellas características que no queden resumidas en el IEEE 802.15.4. De esta forma se asume que, todo lo que no se ha incluido a continuación, se rige por las normas definidas en dicho estándar.

Extensiones incluidas en el segmento de control de la cabecera MAC

Tabla 44. Formato de un paquete MAC general

Octets: 3	**2**	**1**	**0/2**	**0/2/8**	**0/2**	**0/2/8**	**0/6**	**Variable**	**2**
Segmento de control	Paquete de control	Número de secuencia	PAN de destino	Dirección de destino	PAN fuente	Dirección fuente	Seguridad auxiliar	*payload*	FCS
MHR								*payload*	MFR

Tabla 45. Campos del segmento de control

Campo	**Byte**	**Número de bit**	**Bits**	**Descripción**
RES	0	7-4	4	Reservado por ITU-T

TMR	0	3	1	Petición de mapa de tonos 1: Se pide 0: No se pide
CC	0	2	1	Control de contienda: 0: El siguiente paquete se debe transmitir en el periodo de contienda 1: El siguiente paquete se debe transmitir en el periodo de clibre ontienda
CAP	0	1	1	Cambio de prioridad: 0: Normal 1: High
LSF	0	0	1	Ultimo segmento 0: No 1: Sí
SC	1	7-2	6	Contador de segmentos
SL[9-8]	1	1-0	2	Longitud del segmento
SL[7-0]	2	7-0	8	Longitud del segmento

Respuesta al mapeo de tonos

La capa MAC genera un mapa de tonos en modo de respuesta si el bit que hace referencia al mapa de tonos se ha puesto a uno durante la petición. Esto significa que un dispositivo ha hecho una petición reclamando un mapa de tonos a fin de garantizar la mejor calidad en la comunicación. El dispositivo de destino tiene que estimar cuál es la calidad de enlace y generar los parámetros de la capa PHY en consecuencia.

Tabla 46. Formato de la respuesta

Bytes	**1**	**7 (en CENELEC) 12 (en FCC)**	**2**
Campos	Command frame	*payload*	MFR

Tabla 47. Mapa de tonos para una banda CENELEC

Campo	**Byte**	**Bit number**	**Bits**	**Descripción**
TXRES	0	7	1	Resolución de ganancia definida por tramos. 0: 6 dB 1: 3 dB
TXGAIN	0	6-3	4	Ganancia deseada en formato tramos..
MOD	0	2-1	2	Tipo de modulación: 0 – Modo robusto 1 – DBPSK o BPSK 2 – DQPSK o QPSK 3 – D8PSK o 8-PSK
Modulación	0	0	1	0: Diferencial 1: Coherente
Reservado por ITU-T	1	7-6	2	Debe ponerse a cero
TM[5:0]	1	5-0	6	Mapa de tono [5:0]
LQI	2	7-0	8	Indicador de calidad

TXCOEF[3:0]	3	7-4	4	Especifica la ganancia en forma de tramos solicitada para los tonos representados en el mapa TM[0] (opcional)
TXCOEF[7:4]	3	3-0	4	Especifica la ganancia en forma de tramos solicitada para los tonos representados en el mapa TM[1] (opcional)
TXCOEF[11:8]	4	7-4	4	Especifica la ganancia en forma de tramos solicitada para los tonos representados en el mapa TM[2] (opcional)
TXCOEF[15:12]	4	3-0	4	Especifica la ganancia en forma de tramos solicitada para los tonos representados en el mapa TM[3] (opcional)
TXCOEF[19:16]	5	7-4	4	Especifica la ganancia en forma de tramos solicitada para los tonos representados en el mapa TM[4] (opcional)
TXCOEF[23:20]	5	3-0	4	Especifica la ganancia en forma de tramos solicitada para los tonos representados en el mapa TM[5] (opcional)
Reservado por ITU-T	6	7-0	8	Debe ponerse a cero

Tabla 48. Mapa de tonos para una banda FCC

Campo	**Byte**	**Bit number**	**Bits**	**Definition**
TXRES	0	7	1	Resolución de ganancia definida por tramos. 0: 6 dB 1: 3 dB
TXGAIN	0	6-3	4	Ganancia deseada en formato tramos.

MOD	0	2-0	3	Tipo de modulación: 0 – Modo robusto 1 – DBPSK o BPSK 2 – DQPSK o QPSK 3 – D8PSK o 8-PSK 4 – 16-QAM
TM[0:7]	1	7-0	8	Mapa de tono [0:7]
TM[8:15]	2	7-0	8	Mapa de tono [8:15]
TM[16:23]	3	7-0	8	Mapa de tono [16:23]
LQI	4	7-0	8	Indicador de calidad
TXCOEFF				Especifica el número de tramos de ganancia solicitados
Modulación squeme	11	7	1	0: Diferencial 1: Coherente

6.3.7 SEGURIDAD

Un dispositivo final no puede acceder a la red sin una identificación preliminar. La identificación y autenticación se basan en dos parámetros personalizados para cada dispositivo:

- Una dirección MAC EUI-48.
- Un secreto de 128 bits, conocido como el secreto pre-compartido (PSK), utilizado como credencial durante el proceso de autenticación. Se comparte entre el mismo dispositivo y un servidor de autenticación. La autenticación mutua está basada en la prueba de que el otro conoce este clave PSK.

Los procesos de identificación y autenticación se activan cuando el dispositivo final se inicializa y pueden empezar de nuevo en cualquier momento en función de cuál sea la política de seguridad que se aplique en esa red. Ambos procesos se realizan a través del protocolo LBP que embebe al protocolo de autenticación EAP.

En términos de autenticación se consideran dos tipos de arquitecturas:

- La función de autenticación del servidor es soportada por LBS *(LoWPAN Bootstrapping Server)* y toda la información de autenticación se carga directamente en el LBS.
- La función de autenticación no la realiza el servidor, sino que la realiza un dispositivo remoto, normalmente un servidor AAA *(Authentication, Authorization and Accounting),* y el LBS sólo se encarga de enviar toda la información a este servidor, pero no realiza funciones de autenticación per se.

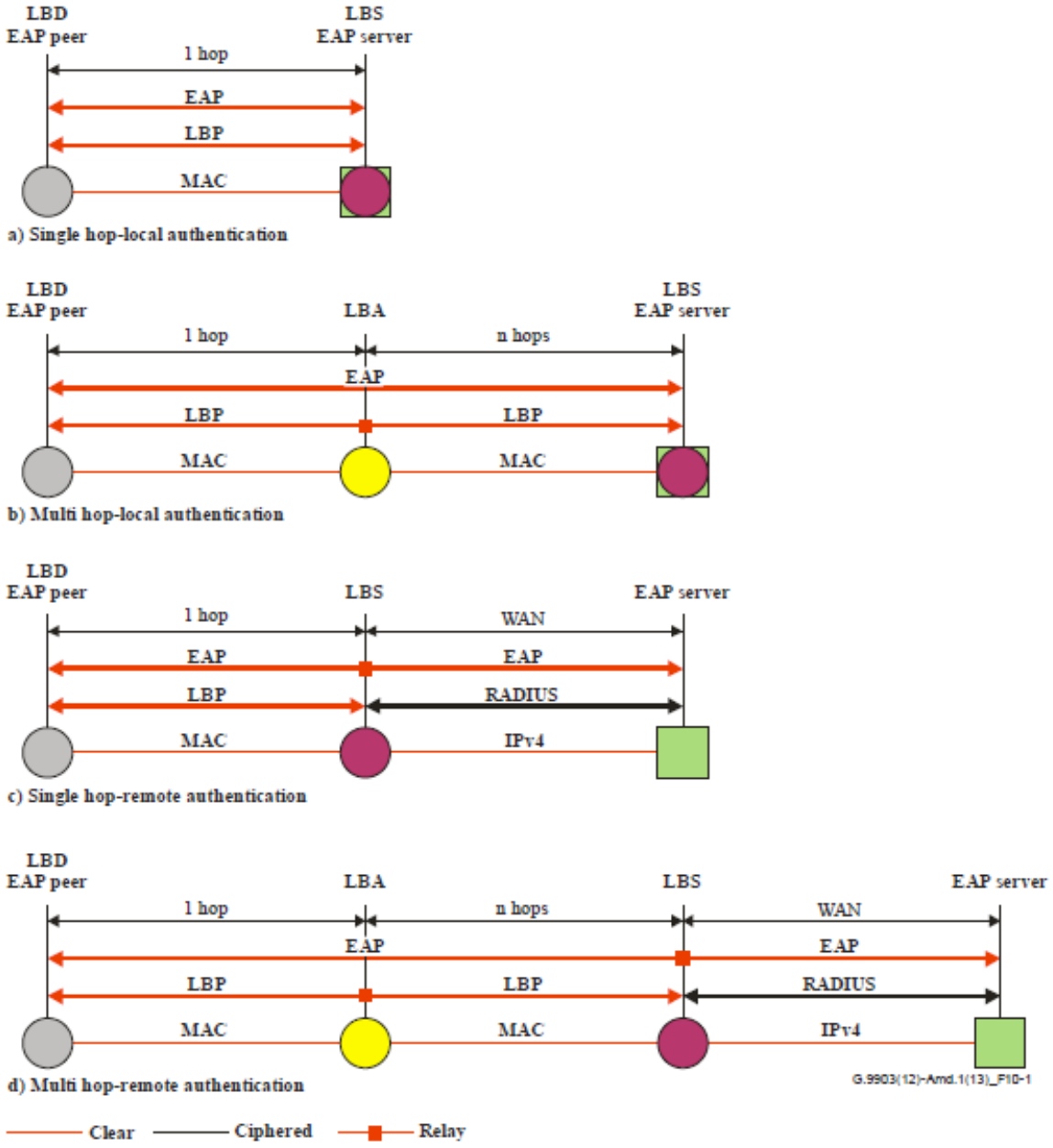


Figura 65. Funcionamiento de LBP y EAP [12]

En concreto, este protocolo implementa EAP-PSK que se caracteriza por lo siguiente:

- Simplicidad: está todo basado en una única contraseña (PSK).
- Seguridad: utiliza unos esquemas criptográficos sofisticados y robustos.

- Extensibilidad: se puede extender fácilmente a una distribución de contraseñas para grupos.

En términos de confidencialidad e integridad, ambas características se garantizan a distintos niveles.

- A nivel MAC: se utiliza un esquema de cifrado CCM para cada uno de los paquetes transmitidos entre los nodos de la red. Los paquetes MAC se encriptan y desencriptan en cada salto del enlace. Sólo se hace excepciones para algunos tipos de paquetes.
- A nivel EAP-PSK: este esquema proporciona confidencialidad e integridad en lo conocido como Canal Protegido (PAHANNEL), a los mensajes intercambiados sobre EAP entre el servidor y el dispositivo.

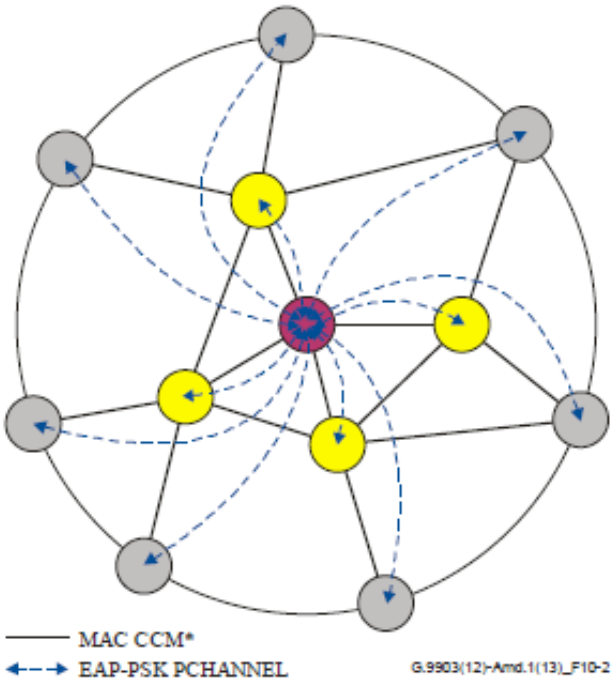


Figura 66. Confidencialidad e integridad [12]

6.4 CAPA DE CONVERGENCIA

La capa de convergencia de este protocolo simplemente especifica una serie de parámetros que se pueden utilizar cuando se quiere implantar en una red que utiliza IPv6 en lugar de IPv4. Para ello proporciona una serie de atributos definidos como *Information Base* que son genéricos y que, en algunos casos, no sólo aplican a las redes tipo IPv6, sino también a otro tipo de extensiones que se quieran añadir.

Como esta información se puede encontrar fácilmente resumida en formato tabla en la propia especificación del protocolo, en este documento no se ahondará en mayor detalle puesto que no hay mayor valor que se pueda añadir a esta sección. En caso de que se desee implantar este protocolo con nuevas extensiones, simplemente se deberá acudir a [12] y definir los valores deseados.

Capítulo 7. METERS AND MORE

7.1 DESCRIPCIÓN GENERAL

Meters and More es uno de los primeros protocolos para la comunicación a través de líneas de bajo voltaje que surge en el mercado. Este protocolo surge debido a que se ha considerado que las redes de bajo voltaje no se pueden tratar como un medio de difusión normal por el efecto que causan sobre las ondas y la atenuación que se genera, lo que puede dar lugar a que sea imposible establecer la conexión con algunos nodos en la red.

Además de este inconveniente, la configuración de la capa física en redes de bajo voltaje se considera la conexión de múltiples puntos operando en modo *half-duplex*. De esta forma, es necesario establecer una serie de normas de acceso de tal manera que se eviten las colisiones.

Para poder conseguir una línea de comunicación virtualmente directa entre dos nodos, Meters and More define una serie de funcionalidades que permiten el uso de técnicas de repetición. De esta forma, Meters and More se basa en una estructura compuesta por un concentrador y un conjunto de ramas interconectadas que dan lugar a distintas secciones. Este modelo seguramente nos suene conocido puesto que, como se ha explicado en otros apartados, PRIME ha entendido que esta es la mejor arquitectura para la comunicación en este tipo de redes y ha basado su protocolo en este modelo también.

Sin embargo, a diferencia de PRIME, Meters & More define dos tipos de sub-redes haciendo que esta arquitectura sea algo distinta. Por un lado define la arquitectura tipo A, donde encontramos tres tipos de dispositivos, el concentrador el repetidor y el destinatario. El repetidor lo que nos permite es añadir muchas funcionalidades de seguimiento y

simplificar también las tablas de direccionamiento que tengan que tener los dispositivos de la red, no siendo necesario que conozcan el camino directo al nodo destino.

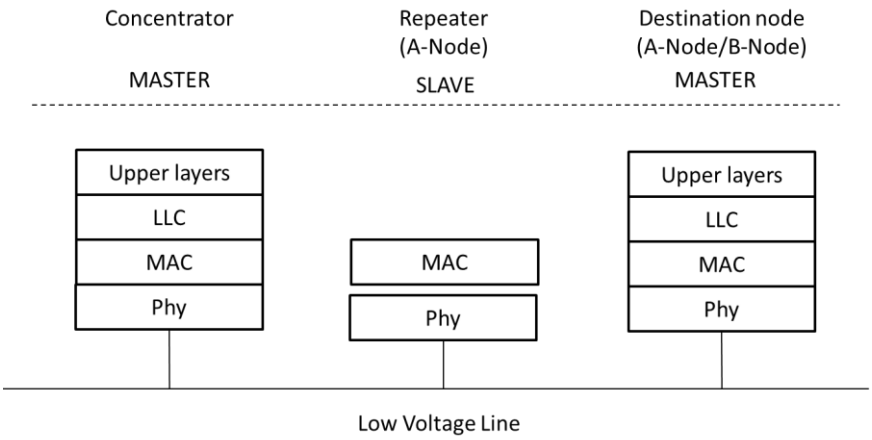


Figura 67. Arquitectura de la subred tipo A [13]

Por otro lado nos encontramos con las redes tipo B. Un tipo de redes mucho más sencillas donde sólo hay un dispositivo inteligente, el maestro tipo A, y después nodos mucho más sencillos que serían los esclavos. Nodos tipo B.

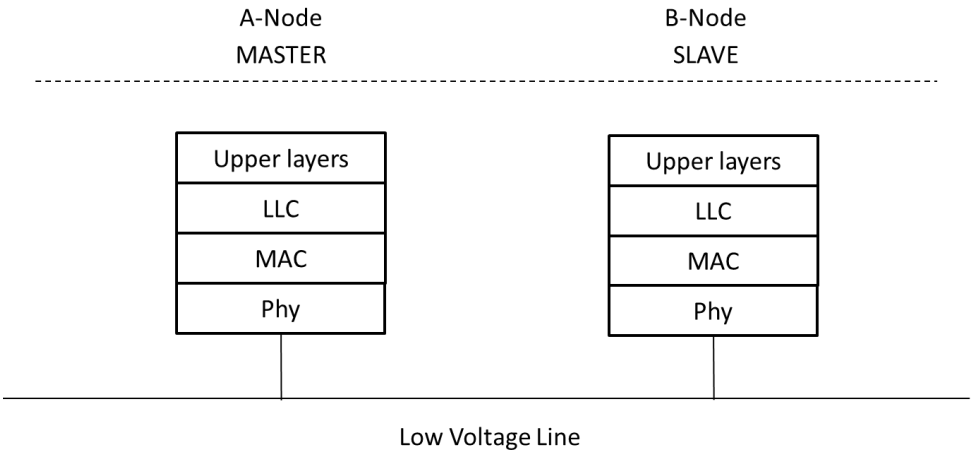


Figura 68. Arquitectura de la subred tipo B [13]

Con estos dos esquemas lo que nos encontramos es con una red principal, que está compuesto por dispositivos tipo A que pueden variar entre los tres tipos ya mencionados, y de la cual cuelgan redes secundarias tipo B que son redes mucho más sencillas donde sólo encontramos dispositivos finales que no tienen ningún control sobre la red.

Respecto a los tipos de comunicación que se pueden establecer, se definen cuatro distintos en esta especificación:

- Clase S: Se envían paquetes, pero no hace falta respuesta (Sxx).
- Clase RA: Toda petición necesita una respuesta, pero de un nodo tipo A.
- Clase RB: Toda petición necesita una respuesta, pero de un nodo tipo B.
- Clase RC: Una petición puede aceptar más de una respuesta (RCx).

En la *Figura 69*, la *Figura 70*, la *Figura 71* y la *Figura 72* se muestran ejemplos de mensajes que se intercambiarían en cada una de las disciplinas especificadas.

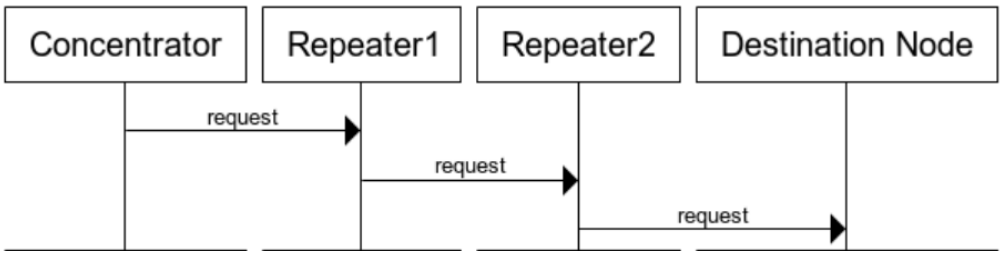


Figura 69. Ejemplo de clase S [13]

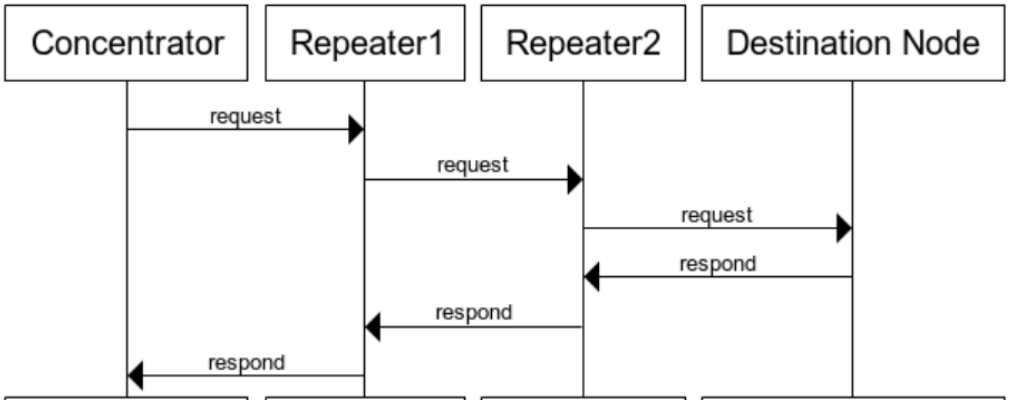


Figura 70. Ejemplo de clase RA [13]

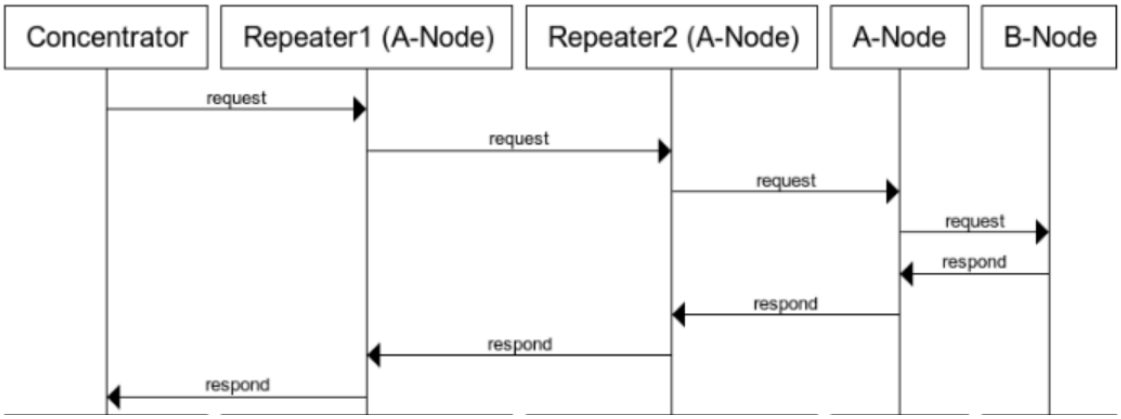


Figura 71. Ejemplo de clase RB [13]

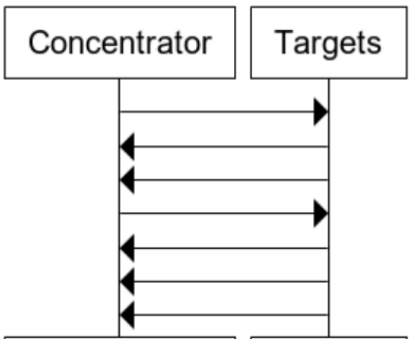


Figura 72. Ejemplo de clase RC [13]

7.2 CAPA PHY

La capa PHY define el método utilizado para transmitir datos sobre el medio físico. Durante la transmisión se encarga de, codificar y encapsular la información que llega de la capa MAC y convertirla en un paquete tipo PHY, la modulación de ese paquete utilizando BPSK. Por otro lado, durante la recepción, se encarga de la sincronización, la demodulación y la decodificación, pudiendo así extraer la información que la capa MAC tiene que procesar.

7.2.1 ESTRUCTURA

La Figura 73 muestra un diagrama que refleja cuáles son los campos que conforman una trama física en el protocolo Meters and More y cómo se genera dicha trama.

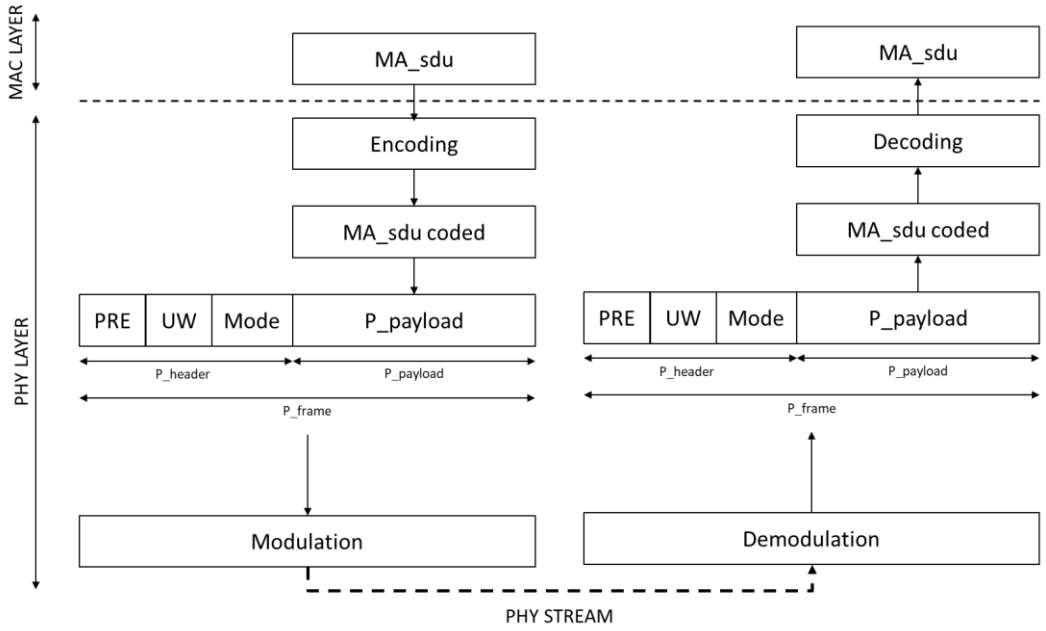


Figura 73. Estructura de la capa PHY [13]

Preámbulo (PRE)

Se trata de una secuencia de 1s y 0s alternados que se necesita para que el receptor pueda emplear el muestreo más exacto. Su longitud debe ser programable utilizando uno de

los siguientes valores, 16, 24, 32 y 40 bits. El patrón a utilizar es 0xAAAA, 0xAAAAAA, … dependiendo de la longitud.

Palabra única (Unique Word UW)

Se trata de un patrón de 32 bits que se utiliza para la sincronización a nivel de paquete y para la sincronización a nivel de byte. Su valor es 0x014AE326.

Modo

Es un patrón de 8 bits que delimita el inicio del código convolucional utilizado en el *payload* del paquete PHY.

P_payload

Se trata de la información codificada.

Modulación

La modulación utilizada es BPSK, una modulación binaria con desplazamiento de fase, con una tasa de símbolo de 9600 símbolos por segundo. El esquema utilizado se basa en, un esquema no diferencial para la cabecera (donde los 1 y 0 se codifican con fases separadas por 180º) y fase diferencial en el *payload*, donde un 1 binario se transmite añadiendo 180ª a la fase del símbolo anterior y 0ª cuando se quiere enviar un 0.

7.2.2 CODIFICADOR

El codificador consta de dos bloques, un codificador convolucional y un *interleaver*. A continuación, se muestra un esquema de ello. También se incluyen dos esquemas donde se describen al codificador convolucional y al *interleaver*.

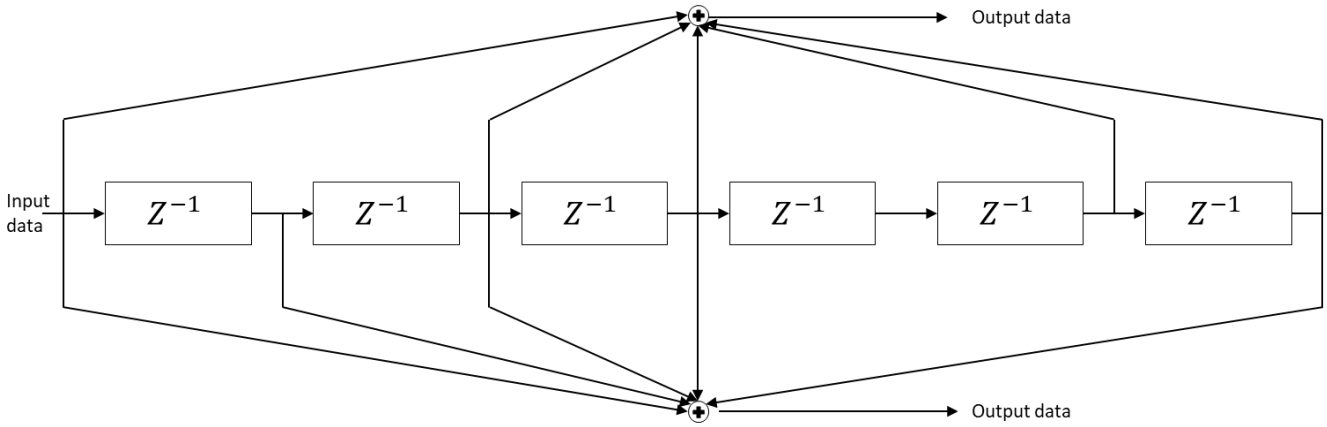


Figura 74. Esquema del codificador covolucional [13]

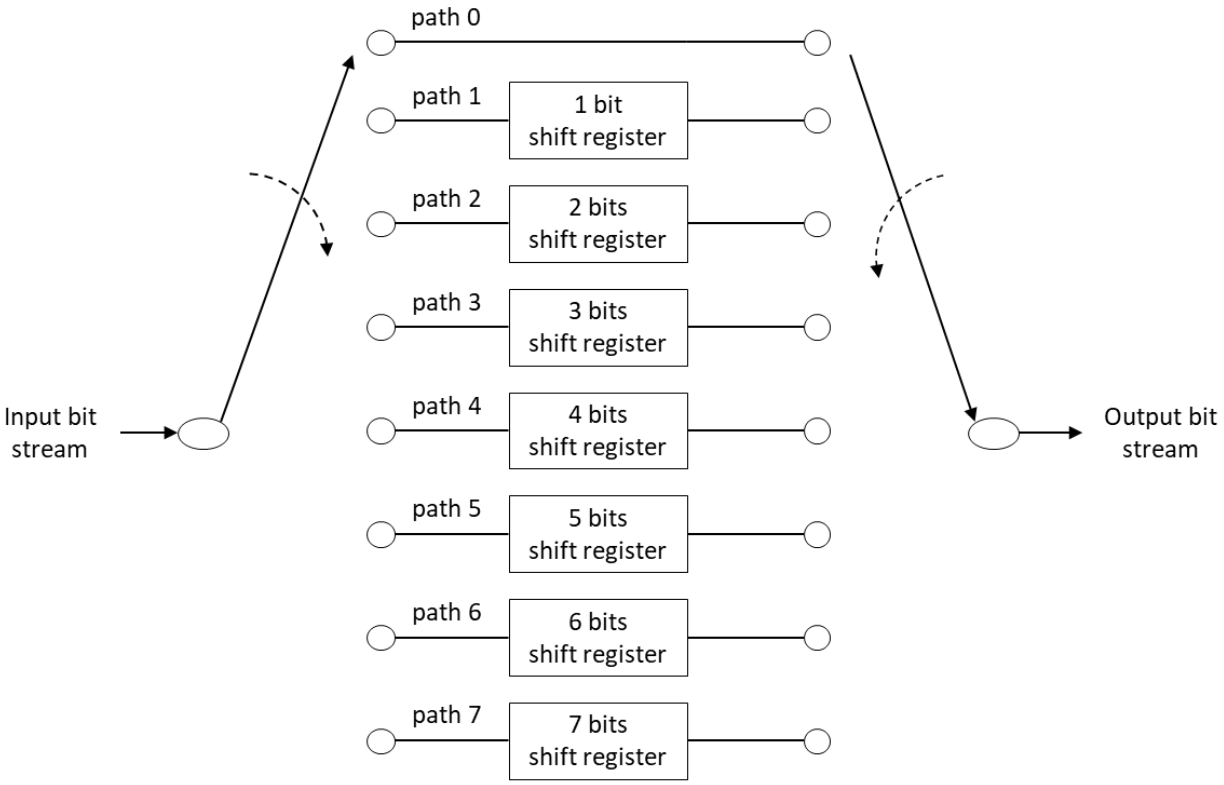


Figura 75. Esquema del interleaver [13]

Para entender mejor este esquema de *interleaver* se va a poner un ejemplo, que se muestra en Tabla 50 donde se va a suponer que el estado inicial del *interleaver* es el que se muestra en Tabla 49 y se tiene un flujo de 24 bits de entrada.

Tabla 49. Estado inicial del interleaver

PATH1	I0						
PATH2	I1	I2					
PATH3	I3	I4	I5				
PATH4	I8	I7	I8	I9			
PATH5	I10	I11	I12	I13	I14		
PATH6	I15	I16	I17	I18	I19	I20	
PATH7	I21	I22	I23	24	I25	I26	I27

Tabla 50. Ejemplo de interleaving

INPUT STREAM	SHIFT REGISTERS CONTENT								OUPUT STREAM
b0	**b0**								**b0**
b1	b1	**i0**							**i0**
b2	b2	i1	**i2**						**i2**
b3	b3	i3	i4	**i5**					**i5**
b4	b4	i6	i7	i8	**i9**				**i9**
b5	b5	i10	i11	i12	i13	**i14**			**i14**
b6	b6	i15	i16	i17	i18	i19	**i20**		**i20**
b7	b7	i21	i22	i23	i24	i25	i26	**i27**	**i27**
b8	**b8**	b0							**b8**
b9	b9	**b1**	i0						**b1**
b10	b10	b2	**i1**	i2					**i14**
b11	b11	b3	i3	**i4**	i5				**i4**
b12	b12	b4	i6	i7	**i8**	i9			**i8**
b13	b13	b5	i10	i11	i12	**i13**	i14		**i13**
b14	b14	b6	i15	i16	i17	i18	**i19**	i20	**i19**
b15	b15	b7	i21	i22	i23	i24	i25	**i26**	**i26**
b16	**b16**	b8	b0						**b16**
b17	b17	**b9**	b1	i0					**b9**
b18	b18	b10	**b2**	i1	i2				**b2**
b19	b19	b11	b3	**i3**	i4	i5			**i3**
b20	b20	b12	b4	i6	**i7**	i8	i9		**i7**
b21	b21	b13	b5	i10	i11	**i12**	i13	i14	**i12**
b22	b22	b14	b6	i15	i16	i17	**i18**	i19	**i18**
b23	b23	b15	b7	i21	i22	i23	i24	**i25**	**i25**

7.2.3 SERVICIOS

Las primitivas disponibles en la capa PHY son las siguientes:

- P_Data.Request: solicita la transmisión de una unidad MAC a través del medio físico.
- P_Data.confirm: es la confirmación a nivel local de la petición (Ok para 00h y NOK para 01h).
- P_Data.indication: solicita una notificación de la llegada del paquete.

7.3 CAPA MAC

7.3.1 PRIMITIVAS

La siguientes primitivas son las utilizadas entre la capa MAC y LLC:

- MA_DATA.request: se pasa a la capa MAC e invocada por la capa LLC para pedir la transmisión de un SDU al nodo final.
- MA_DATA.indication: se pasa de la capa MAC a la capa LLC para transferir un SDU que se ha recibido.
- MA_DATA.confirm: esta primitiva pasa de la capa LLC a la capa MAC para confirmar si el SDU que se ha enviado anteriormente ha llegado o no sin problemas. Siempre termina un MA_DATA.request y notifica a la capa LLC que la capa MAC está disponible para transmitir otra petición.

Por otro lado, la primitiva MA_EVENT.indication se transmite entre las capas MAC y la de gestión de red (NM). Notifica eventos que son importante para la gestión de la comunicación.

7.3.2 CLASES DE SERVICIO

Las clases de servicio son los tipos de comunicación que se pueden proporcionar utilizando este protocolo, en lo que a la gestión de petición/respuesta se refiere. Esto quiere decir, la manera en que se realiza la petición y, sobretodo, se envía la respuesta, pueden variar en función de cuál sea el tipo de servicio que se necesite. Las principales clases de servicio que proporciona la capa MAC son:

- Sxx: en este escenario el mensaje de confirmación a una petición sólo se envía cuando el canal se libera de repeticiones de la sub red tipo A. Es decir, se da prioridad

a la comunicación que se está llevando a cabo en la subred A, y sólo cuando esta esté vacía se envía la confirmación a la petición. Se utiliza cuando la capa LLC ha pedido un servicio de tipo envío/no respuesta. Esta clase de servicio tiene mucho sentido en este tipo de servicios puesto que ya el transmisor ha dejado claro que la respuesta a su petición no es una prioridad.

- Rxx: la confirmación se da durante el tiempo que utilizan tanto el paquete en *downstream* como en *upstream*. Se define como la confirmación de ida y vuelta. Se utiliza cuando a la capa LLC se le ha pedido un servicio de petición/respuesta. En este caso pasa todo lo contrario, el transmisor ha decidido que necesita una respuesta lo antes posible porque esta respuesta sí es crítica y por ello no se espera a que el canal esté libre. Se transmite independientemente de si hay paquetes de subida o de bajada en la red.

7.3.3 ESTRUCTURA DEL PAQUETE

La Figura 76 muestra la estructura de un paquete de capa MAC continuación se pasan a detallar con mayor detalle en qué consisten cada uno de ellos. Nótese en que esta explicación no se incluye el campo NB porque es un campo de longitud un byte que no se utiliza.

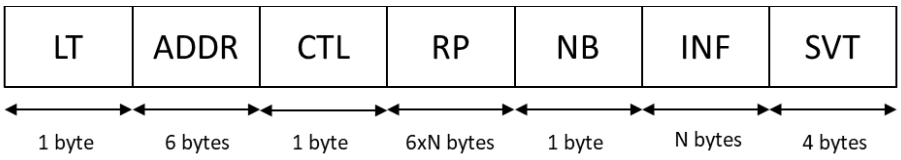


Figura 76. Estructura de un paquete MAC [13]

Longitud (LT)

Está compuesto por un byte e indica el número de bytes que contiene el paquete, excluyéndose a sí mismo.

Dirección (ADDR)

Está compuesto por 6 bytes y contiene tanto la dirección de destino como la dirección de origen.

Control (CTL)

Está compuesto por un byte y contiene la configuración relacionada con la función de ese paquete. En relación con dicha función existen cuatro tipos de funciones distintas.

- RIP hace referencia a repetición y se encarga de gestionar la repetición de ese paquete hasta el último repetidor involucrado.
- NOR1 gestiona la conexión entre el último repetidor y el nodo final.
- NOR2 gestiona la repetición hacia atrás entre el nodo final y el último repetidor.
- Por último, CRP hace referencia a un tipo de paquetes que genera un repetidor cuando el tipo de respuesta ha expirado.

Parámetros de repetición (RP)

Este campo está presente tanto en los paquetes tipo RIP como CRP e indica la configuración de repetición que hay que seguir en términos de conexiones. Su longitud varía ya que está compuesto por tantos subcampos como repetidores haya, todos ellos de una longitud fija de 6 bytes.

En los paquetes tipo RIP, si el repetidor está direccionando a otros nodos utilizando sus códigos ACA, este campo contendrá, bien este tipo de direcciones de los repetidores intermedios (sin incluir la del destino final), bien directamente la del destino final.

Si el tipo de direccionamiento que está utilizando es SCA, entonces incluirá las correspondientes direcciones, pero en formato SCA. La principal diferencia entre estos dos tipos de direcciones es que una es la dirección MAC clásica (ACA) mientras que la otra es un identificador que considera la subred en la que se encuentra también (SCA).

Por otro lado, en los paquetes tipo CRP, este campo sólo contiene la dirección (sea bien ACA o SCA) del nodo repetidor cuyo temporizador expiró y ha empezado la repetición.

Información (INF)

Tiene una longitud variable de bytes (siempre un número entero de bytes) y contiene información que ha sido intercambiada *end-to-end* entre los nodos maestro y esclavo.

Secuencia de control (SVT)

Contiene el resto (con longitud de 32 bits) hecho el complemento a uno de la división entre los campos LT e INF.

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + \mathrm{x} + 1$$

7.3.4 PROCEDIMIENTOS

Filtrado

Permite comprobar si los paquetes que se han intercambiado son correctos o contienen algún error. Durando la recepción se comprueba que haya congruencia entre el número de bytes que realmente contiene el paquete y lo que aparece en el campo LT (longitud). También la congruencia del campo SVT y, por último, la congruencia del número de bytes del campo INF dentro de los parámetros establecidos.

Detección de fase

El proceso de detección de fase requiere que el concentrado y cualquier posible nodo repetidor sincronicen la transmisión del paquete, haciéndola coincidir con el paso por cero del voltaje en la línea de baja potencia.

Repetición

El nodo que se encargan de realizar la repetición, la capa MAC utiliza los campos de control y repetición del paquete para establecer la información de transmisión del nodo maestro e indicarla a otro nodo o viceversa.

Entre el nodo final y el repetidor solamente pueden viajar paquetes de tipo NOR1. Entre nodos tipo A y nodos tipo B sólo pueden viajar paquetes de tipo NOR1 y NOR2.

Los repetidores realizan el control de repetición utilizando el campo CRP para informar al nodo maestro de cualquier posible error que haya ocurrido durante la comunicación con los nodos contiguos. Los paquetes CRP son enviados por los nodos repetidores sólo en casa de que se necesite servicios de tipo petición/respuesta. Este tipo de paquetes llevan siempre sentido de descarga y sólo generan si el temporizador a expirado.

7.4 CAPA DE CONVERGENCIA

7.4.1 PRIMITIVAS

La siguientes primitivas se utilizando para permitir el flujo de información entre las capas superiores y la capa MAC.

En primer lugar, tenemos DL_Data.request. Esta primitiva viaja desde la capa de convergencia (LLC) cuando se necesita realizar una petición a una capa LLC de un nodo remoto.

La primitiva DL_Data.confirm genera una confirmación local ante la recepción de un L_PDU. Sólo tiene sentido a nivel local, no genera ningún tipo de primitiva más allá.

DL_Data.indication viaja desde la capa LLC para indicar la llegada de un L_PDU. Se genera cuando la capa MAC pasa una primitiva tipo MA_Data.indication explicada en apartados anteriores.

7.4.2 ESTRUCTURA

Las PDUs generadas por esta capa tienen los siguientes campos:

- Campo de control: consiste en un byte utilizado para definir el tipo de PDU que se ha recibido.
- Dirección: siguiendo los formatos ya explicados.
- Datos.

7.4.3 PROCEDIMIENTOS

Existen tres procedimientos principales que se desarrollan en esta capa. Están el direccionamiento, la transmisión de información y la recepción de información.

Respecto al direccionamiento, el emparejamiento entre el transmisor y el receptor es gestionado gracias a la dirección MAC o SCA que se envía utilizando las primitivas DL_Data.

La transmisión de información de una estación maestro a una esclava se consigue a través del envío de un SDU propiamente mapeado, donde el valor del campo de control depende de la disciplina y de la dirección especificada en la primitiva DL_Data.request.

Durante la recepción de información si se recibe un L_PDU válido, la capa de convergencia genera la indicación apropiada hacia la capa superior correspondiente.

Capítulo 8. DISCUSIÓN Y COMPARATIVA

Una vez que se ha dado una definición de los tres principales protocolos que se encuentran desplegados a día de hoy, en este apartado se va a desarrollar una comparativa entre ellos de tal manera que se pueda comprender mejor, a nivel técnico, qué es lo que hace que algunos se implanten en ciertas circunstancias y que otros no.

En esta comparativa no se busca definir exactamente cuál es la raíz de estas diferencias, dándose por hecho que existe un conocimiento básico sobre las técnicas empleadas en cada una de las principales capas de los tres protocolos.

8.1 CAPA PHY

En general, en cuanto a la comparativa de la capa física, lo que nos encontramos es que tanto PRIME como G3 PLC son protocolos muy completos y similares con ciertas diferencias, pero en general pequeñas. Mientras que, en el caso de Meters & More, el esquema de esta capa es un esquema muy simplificado con muchos menos elementos.

PRIME es capaz de transportar un máximo de 2268 bytes por paquete con una tasa de 128.8 kbps utilizando D8PSK, siendo este su modo menos robusto. Si utilizásemos el modo más robusto, es decir, DBPSK, podría transportar 277 bytes por paquete en una tasa de 21.4kbps. En el caso de G3, cada uno de sus tres modos (Robusto, DBPSK y DQPSK), transmiten 133, 235 y 235 bytes de datos a una tasa de 33.4 kbps como máximo en el caso del modo menos robusto (DQPSK) [14].

Por otro lado, en términos de comunicación, también resulta interesante conocer cuántas portadoras se tienen a disposición a la hora de transmitir, porque esto también indicará que podemos transmitir más información o menos al mismo tiempo. En el caso de PRIME, éste

utiliza 97 sub-portadoras espaciadas con uso intervalos muy estrechos, mientras que PLC G3 emplea sólo 36 sub-portadoras, pero mucho más espaciadas.

En términos de modulación, hay una diferencia muy importante entre PRIME y G3. DPSK necesita de un símbolo de referencia enviado en la primera sub-portadora de cada símbolo OFDM par cada una de las frecuencias en el caso de PRIME, o al principio de cada paquete, es decir, en el dominio del tiempo, en el caso de G3. Para intentar reducir al máximo el impacto de esta adición, en el caso del dominio en frecuencia se debería utilizar muchas sub-portadoras, pero transmitir pocos símbolos en cada una de ellas, mientras en el dominio del tiempo, se deberían utilizar menos sub-portadoras y enviar muchos símbolos en cada una de ellas. Es decir, las reglas son opuestas entre estos dos protocolos. En el caso de G3, lo que se puede hacer es utilizar los símbolos de referencia de tal manera que formen un único símbolo OFDM, reduciendo así su impacto. Pero al mismo tiempo, si el medio tiene distorsiones de corta duración, estos símbolos de referencia se ven afectados por dos problemas. El primero es que ya de por sí los símbolos se pueden corromper, pero no sólo eso, un símbolo de referencia corrupto implica que la detección del siguiente símbolo va a tener errores puesto que hay una dependencia en términos de fase entre ellos. Para eliminar este posible efecto, el *interleaver* de G3 PLC permuta la información dentro del paquete de tal manera que siempre hay que calcularlo en función del tamaño de datos que se transmiten [14].

Pasando a la siguiente fase, el código convolucional de ambos protocolos es el mismo. PRIME permite que esta fase sea seleccionable en función de las condiciones del medio, mientras que G3 PLC siempre emplea un codificador y es el Reed Solomon, que puede ser adicional en caso de que también se desee utilizar el convolucional. Esto hace que por definición G3 PLC sea más robusto mientras que PRIME tiene algunos modos menos seguros.

También hay una parte muy importante durante la transmisión y este es el preámbulo, que se utiliza para la sincronización. En el caso de PRIME, éste aplica una secuencia de *chirp* sobre el rango de frecuencias correspondiente cuya duración es igual a la de un símbolo

OFDM si intervalo de guardia. En el caso de G3 el preámbulo consiste en un símbolo OFDM que se repite nueve veces y media y donde el último símbolo y medio se envían con signos distintos [14].

Basándonos en toda esta información debe haber dos características que necesitemos conocer para entender qué diferencia a estos dos protocolos. Por un lado está la densidad de potencia espectral que empelan en función de la frecuencia en la que se hayan. Es decir, cuánto trabajo nos cuesta conseguir que la información se transmita sin errores en función de la frecuencia en la que decidamos trasmitir. En cuanto a este tema se han desarrollado numerosos estudios que demuestran que, en términos generales, ambos protocolos tienen las mismas características y, para los rangos de frecuencias más utilizados, ésta no es una característica que los defina demasiado. A continuación podemos ver la *Figura 77* y la *Figura 78* que muestran esta comparativa.

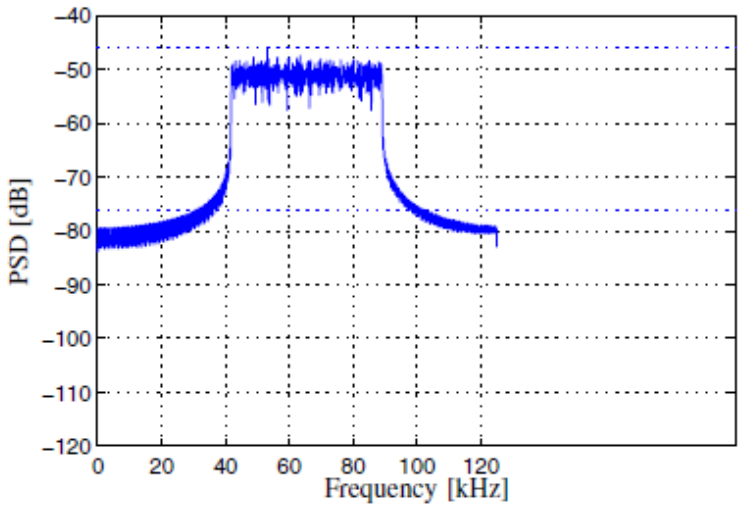


Figura 77. Densidad de potencia espectral utilizando PRIME [15].

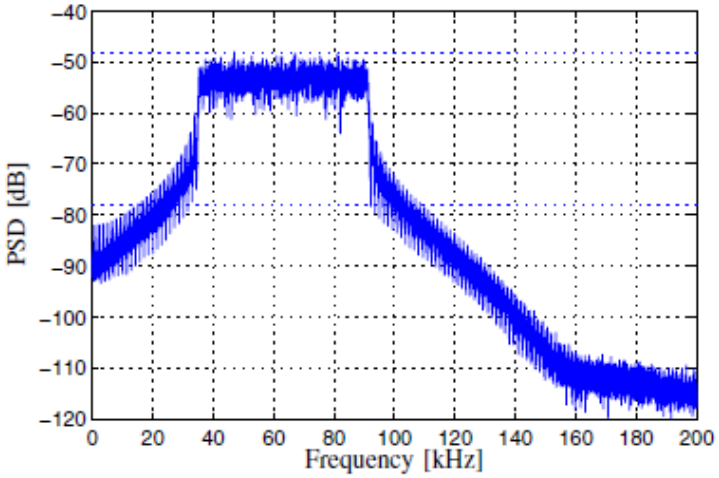


Figura 78. Densidad de potencia espectral empleando G3 PLC [15]

Otro tema muy importante es el comportamiento de ambos protocolos en escenarios donde haya bastante ruido. Ya se ha contado en apartados anteriores, que el ruido es un elemento muy peligroso y que afecta mucho en este tipo de comunicaciones. Conseguir un protocolo robusto que garantice que, a pesar de haber mucho ruido, la comunicación se va a realizar sin errores es una prioridad muy alta. A continuación se muestran la *Figura 79* y la *Figura 80* que se han publicado en estudios donde se ha puesto ambos sistemas a prueba en distintos escenarios de ruido. El parámetro principal que se ha medido ha sido el FER y, dado que para el protocolo PRIME existen numerosas combinaciones, mientras que para G3 PLC sólo tres, se han utilizado sólo los modos que se han considerado "comparable". Es decir, en el caso de PRIME se han utilizado los modos DBPSK, DQPSK, D

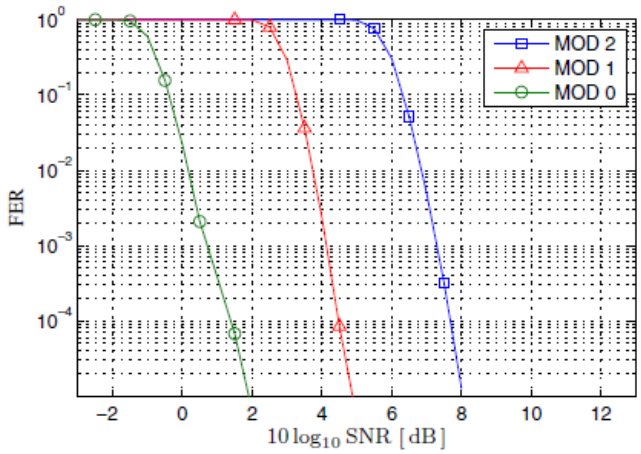


Figura 79. Rendimiento de G3 PLC [16]

8PSK pero todos con código cíclico, es decir, modo seguro, y se han identificado como PROT4, PROT5 Y PROT6 respectivamente. Por otro lado para G3 PLC se han empleado los tres modos que tiene, el modo Robusto (DBPSK con repetición), DBPSK y DQPSK y se ha hecho referencia a ellos como MOD0, MOD1 y MOD2 respectivamente.

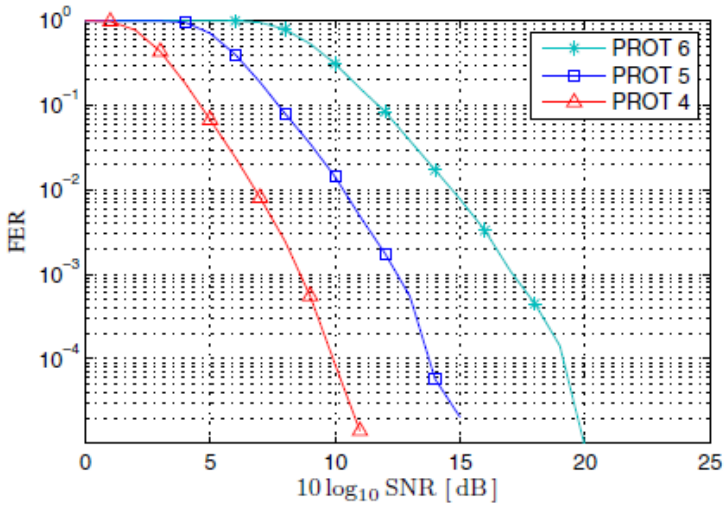


Figura 80. Rendimiento de PRIME [16]

De toda esta información lo que podemos sacar en claro es que PRIME se comporta peor que G3 en términos generales. La especificación PRIME proporciona unas tasas de transmisión más altas, pero para conseguirlo sacrifica robustez y en este tipo de escenarios no siempre es recomendable. Por su parte G3 proporciona una confianza muy alta, es un protocolo muy robusto que resiste situaciones pésimas y siempre garantiza una confiabilidad muy alta. Pero para conseguirlo, sacrifica en la tasa de transmisión. De esta forma, debido a que gran parte de la información que viaja en un paquete es información redundante, se necesitan más paquetes para transmitir la misma información y eso hace que el sistema sea menos eficiente.

Todo esto básicamente nos quiere decir que, si las condiciones del medio son favorables, entonces podemos disfrutar de las ventajas de PRIME con una confiabilidad alta y una tasa de transmisión muy alta también. Por su parte, en este tipo de escenarios nos encontraríamos conque G3 PLC sería demasiado ineficiente empleando demasiados métodos para dar robustez a un sistema que de por sí no se expone a condiciones tan

adversas. Por otro lado, en caso de que nos encontremos en un escenario donde sí las condiciones son muy desfavorables, G3 PLC nos garantiza que la comunicación no va a tener errores incluso aunque no se emplee le modo robusto. Por su parte PRIME es incapaz de proporcionar estas tasas de confiabilidad en este tipo de escenarios porque no dispone de las características adecuadas para hacerlos frente.

En lo referente a Meters & More, este protocolo lleva menos tiempo en el mercado y no se ha puesto a prueba tanto como PRIME y G3 PLC con lo que establecer una comparativa tan detallada a nivel de rendimiento se hace mucho más complejo. En términos de tasa de transmisión, la especificación define una tasa de transmisión constante de 4.8 kbps. Este protocolo sólo proporciona un tipo de modulación con lo que cabe esperar que sólo se pueda conseguir una tasa de transmisión de bit. La tasa de transmisión de símbolo es de 9600 símbolos por segundo. Estas medidas no son muy buenas si las comparamos con PRIME o G3PLC. Tanto los símbolos transmitidos como la tasa de transmisión es muy inferior [17].

Si comparamos la arquitectura, algo que llama mucho la atención es que la arquitectura de M&M es una arquitectura muy simple que únicamente cuenta con un convolucionador y un *interleaver*, siendo ambos de características similares a los descritos en G3 PLC y PRIME. Esto implica que la robustez que este protocolo proporciona a escenarios adversos, con mucho ruido o con desvanecimiento de la potencia en algunas frecuencias, sea muy baja, de tal manera que la confiabilidad que proporciona pudiera no llegar a ser la suficiente [18].

Por otro lado, una de las características muy positivas que tiene este protocolo es que su implementación es muy sencilla. Los transmisores y receptores no necesitan ser muy complejos y su arquitectura puede ser muy básica de tal manera que su instalación y mantenimiento se simplifican enormemente, algo que en general no pasa ni con G3 PLC ni con PRIME. Es cierto que G3 PLC ya prevé esta situación y define características que sean fáciles de implementar en los dispositivos, pero en ningún caso son comparables a M&M [18].

Debido a la falta de información disponibles, en lo referente a gráficas y resultados experimentales, más adelante en este documento se implementará la capa física de esta especificación a fin de poder conseguir resultados que puedan comparar el rendimiento de este protocolo con el de PRIME y G3PLC.

En general lo que sí podemos concluir es que se trata de un protocolo mucho más sencillo, menos robusto, con unas tasas inferiores a las proporcionadas por PRIME o G3 PLC y un rendimiento muy posiblemente inferior también en lo referente a densidad espectral de potencia y comportamiento frente a escenarios de ruido.

8.2 CAPA MAC

Cuando comparamos los tres protocolos según las funcionalidades que ofrece la capa MAC nos volvemos a encontrar con una situación similar a la que ya vimos en el caso de la capa PHY. Los dos protocolos principales, PRIME y G3 PLC, tienen unas características muy similares, mientras que M&M se queda algo atrás en cuanto a funcionalidades disponibles.

Empecemos por resumir cuáles son los principios en los que se basa el protocolo PRIME. El acceso al medio se hace a través del uso del mecanismo CSMA/CA. Es decir, implementa una funcionalidad que reduce la probabilidad de que se produzcan colisiones debido a que varios dispositivos intentan transmitir al mismo tiempo. Esta funcionalidad es muy importa y afecta directamente a la confiabilidad que se puede tener de este protocolo.

En segundo lugar, nos encontramos con que PRIME ofrece la funcionalidad de segmentación y reensamblado de paquetes. Es decir, a pesar de que hay un tamaño de trama máximo para transmitir, en caso de que el tamaño del mensaje sea más grande que el que soportan algunos dispositivos intermedios, se puede partir este paquete en distintos segmentos de tal manera que todos los dispositivos son capaces de interpretar que todos los segmentos pertenecen a un mismo paquete y que en la recepción en el destino final, a fin de que el dispositivo procese la información correctamente, deben ser analizados en conjunto.

De nuevo esta funcionalidad es muy importante puesto que nos permite adaptarnos a muchos escenarios donde las configuraciones de los dispositivos no están limitadas a unas características concretas. Esto hace del protocolo uno más interoperable y mucho más funcional.

Para mejorar la funcionalidad y garantizar una comunicación fluida, PRIME incluye el uso del protocolo ARQ, un protocolo que fuerza al receptor a responder una vez que recibe el paquete con dos tipos de mensajes ACK y NACK. Esto se utiliza para el control de errores en la transmisión de datos, garantizando la integridad de los mismos. A pesar de que este tipo de protocolos se suelen utilizar en sistemas que no actúan en tiempo real, por el tiempo que se pierde en el reenvío de paquetes, en los escenarios de las *Smart Grid* el tiempo real no es una limitación y se prioriza la recepción de datos correctas para evitar facturaciones que no correspondan, por ejemplo. En caso de que el mensaje se haya recibo correctamente se enviará un mensaje ACK de respuesta y en caso de que no un NACK. En este último caso el transmisor tendrá que reenviar el mensaje de nuevo [9].

En relación a otras versiones, PRIME tiene versiones anteriores y esta versión del protocolo garantiza su compatibilidad con versiones anteriores gracias al esquema de la arquitectura de las cabeceras de los paquetes, que las hace comprensibles tanto para dispositivos que utilicen la versión anterior como dispositivos que implementen la nueva. De nuevo, todo esto refleja su interoperabilidad.

Por último, en términos de seguridad, un aspecto muy importante y a uno de los mayores retos que se enfrentan este tipo de redes, el protocolo PRIME ofrece tres perfiles de seguridad definidos como 0, 1 y 2. El perfil 0 hace referencia a la no seguridad, es decir, no implementa ningún mecanismo y sólo se utilizaría en escenarios donde verdaderamente las características sean lo suficientemente seguras como para no tener que proteger los datos. El perfil 1 y 2 implementan. los dos, seguridad y se diferencian en el número de veces que realizan las repeticiones de datos haciendo las estructuras más seguras. En ambos emplea el protocolo *Hand Shake* con un *nonce* único para dispositivo. Para la generación de llaves

utilizan el protocolo AES-128 y para la encriptación y el autenticado de dispositivos en la red emplea AES-CCM [16].

Es decir, como podemos ver PRIME es un protocolo bastante completo a nivel MAC con muchas características a ofrecer que garantizan que la comunicación es lo más segura y de la mayor calidad posible.

Por su lado G3 PLC no se queda corto. De nuevo nos encontramos con que emplea CSMA/CA como método de acceso al medio, con lo que también controla la colisión de errores y define una serie de tiempo en la transmisión donde, en función del tipo de información a transmitir o el tipo de dispositivo que va a transmitir la información, se reserva ese periodo o se permite la libre contienda entre los dispositivos.

Como no podía ser de otra forma, siendo un protocolo tan extendido como más adelante se mostrará en otros apartados, G3 PLC también incluye la funcionalidad de segmentación y reensamblado de tal manera que no limita su arquitectura a la red en la que se mueva, sino que los dispositivos son lo suficientemente inteligentes como para diferenciar segmentos de paquetes completos [12].

En relación al control de errores G3 PLC también implementa el protocolo ARQ de tal manera que se garantiza que la información que llega es una información que no ha sido manipulada durante la transmisión y por tanto ha habido ataques de tipo "*Man in the middle"*.

En el caso de G3 PLC no ha habido versiones anteriores con lo cual no es necesario que presente funcionalidades de compatibilidad para este fin. Sin embargo, algo que es importante remarcar, es que G3 PLC está pensado para funcionar en dos bandas distintas, la banda CELENEC y la banda FCC. Esta característica hace que es protocolo sea muy versátil y que se pueda adaptar a un rango mayor de escenarios que PRIME, por ejemplo.

Por último, volviendo al tema de la seguridad, G3 PLC también ha pensado en la seguridad como un punto muy importante a tener en cuenta y ha incluido el uso de llaves creadas a partir del protocolo EAP-PSK y, de nuevo, el protocolo AES-CCM para la

encriptación y autenticación. Si bien es cierto que no define varios perfiles como hemos visto en el caso de PRIME, sí que define uno como mínimo que es capaz de cubrir las necesidades de seguridad de muchos de los escenarios [18] [11].

Por último, nos encontramos con el protocolo M&M. Este protocolo, como ya se vio en el análisis de la capa PHY, se trata de un protocolo mucho menos desarrollado en comparación con PRIME y G3 PLC. En cuanto a la capa MAC la situación no ha cambiado demasiado. Las principales funcionalidades que presenta son las siguientes.

Por un lado, de cara a poder implantarse en un rango mayor de redes, este protocolo sí incluye capacidades de Segmentación y reensamblado. Si bien es cierto que en la especificación original no hace referencia en ningún punto a esta característica, existen mejoras que sean ido añadiendo donde si se incluyen y por tanto es importante tenerlas en cuenta.

Otra característica que ha incluido es el direccionamiento SAP. Esta característica no es otra que la funcionalidad de identificar y comprobar los paquetes de datos entrantes. Antes de autorizar el procesamiento de estos paquetes verifica su ruta. El beneficio de este tipo de direccionamiento es que no se necesitan conexiones *end-to-end*, algo que simplifica mucho la arquitectura lógica que tiene que tener la red. Además, en caso de que no haya conexión IP entre los dispositivos, el direccionamiento SAP permite que un router SAP pueda establecer la conexión [17].

Sin embargo, algo que echamos mucho en falta en esta especificación es la referencia, por un lado, de un protocolo de gestión del acceso al medio de tal manera que la eficiencia de la red se vea maximizada. Esto sobre todo teniendo en cuenta que los datos que se envían son datos sensibles y críticos y por tanto es importante garantizar que no se pierden. Por otro lado, y siguiente con esta filosofía, un protocolo de control de errores que garantice que, en el caso de que los datos se hayan visto manipulados estos se descartarán.

Si bien es cierto que en términos de seguridad tampoco hace referencia a ninguna metodología, podría darse el caso de que este protocolo sólo se pretendiera utilizar en

entornos muy seguros o que ya implementan otro tipo de seguridad, por ejemplo, física. En tal caso no haría falta implantar protocolos de seguridad a mayores.

En función de toda esta información, lo que podemos concluir en esta comparación es que, de nuevo, PRIME y G3 PLC son protocolos mucho más completos, con unos esquemas mucho mejor construidos y que presentan un amplio rango que características que principalmente buscan que sean muy usables e interoperables en entornos que utilicen dispositivos que no tengan por qué estar diseñados para ellos en concreto. Por su parte, M&M se presenta como un protocolo mucho más joven, con menor experiencia y menos amplio de miras, con funcionalidades mucho más reducidas que, en principio, le permiten competir en el mercado pero que seguramente, en la mayoría de las circunstancias no le permitirían ganar la batalla frente a los demás.

8.3 CAPA DE CONVERGENCIA

Las capas de convergencia de los tres protocolos se basan principalmente en la disposición de primitivas muy básicas que permitan comunicarse con cualquier tipo de aplicación que se sitúe por encima de la capa PHY y la capa MAC.

En el caso de PRIME, la capa de convergencia consta de dos niveles, un nivel común a todas las aplicaciones, que es el que se pone en contacto con la capa MAC y un nivel específico por cada aplicación que se implemente en el dispositivo. Este esquema es un esquemas muy sencillo y útil que garantiza unos niveles de compatibilidad muy altos y que sea muy conveniente en muchos tipos de redes. Entre sus principales aplicaciones se encuentran tanto IPv4 como IPv6, para las cuales define una serie de primitivas especiales que garantiza que ambos tipos de protocolos son fácilmente compatibles con las capas MAC y PHY que define PRIME [16].

En el caso de G3 PLC, la capa de convergencia no es una capa tan bien construida. Este protocolo simplemente define una serie de primitivas, no tan específicas como PRIME, pero

tampoco tan genéricas como M&M que principalmente se inspiran en las primitivas que ya vienen definidas en el estándar 802.15.4.

Por último, tenemos M&M que sustituye los protocolos TCP e IP por su capa DLL. Esta capa sólo presenta primitivas genéricas que garantizan la compatibilidad con cualquiera de los protocolos de niveles superiores que vienen definidos por la misma casa que M&M. Es decir, los niveles de compatibilidad que presentan esta capa no son muy altos a pesar de que la arquitectura sea muy sencilla y fácil de implementar. Se muestra esta arquitectura en la *Figura 81*.

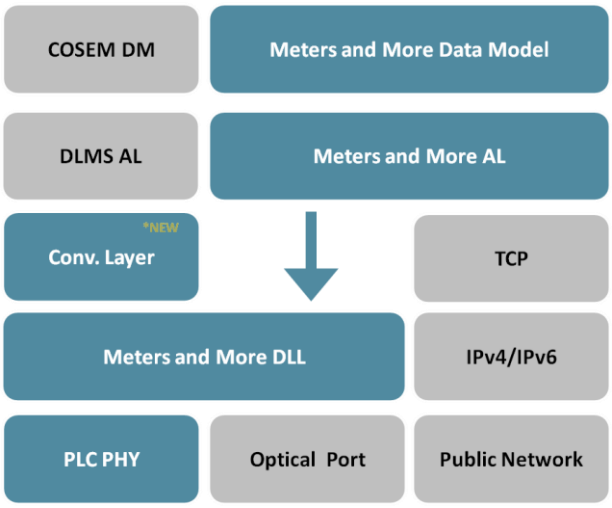


Figura 81. Arquitectura de M&M [19]

Es decir, en términos generales nos encontramos con que la capa de convergencia que está más lograda de los tres protocolos es la de PRIME, mientras que G3 PLC garantiza mucha compatibilidad basándose en el cumplimiento del estándar 802.15.4, algo bastante genérico, y por último M&M a grandes rasgos sólo garantiza la compatibilidad con su propia tecnología en lo referente a niveles superiores.

Capítulo 9. ALCANCE COMERCIAL

En la actualidad existen distintas variantes de PLC desplegadas que atienden a distintas especificaciones, incluyendo bandas de frecuencia, tasa de transmisión, modulación entre otras.

Para entender mejor cuál es el alcance del despliegue de estas tecnologías en Europa en la figura que se muestra a continuación se puede ver, representado en un diagrama de colores, qué países han implantado qué tecnologías.

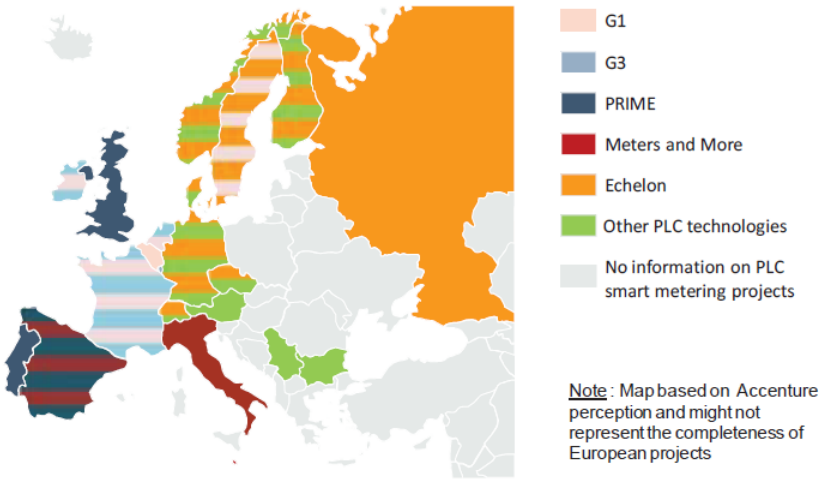


Figura 82. Principales protocolos expandidos en Europa [10]

Los primeros países interesados en la implantación de sistemas AMI basados en PLC han escogido Echelon, Meters and More o G1-PLC, mientras que los desarrollos que están liderando este sector en la actualidad se centran en Prime y G3-PLC.

9.1 PRIME

PRIME es una solución bastante extendida en España al Iberdrola fomentar su implantación entre sus consumidores. Esta tecnología surgió en el año 2007, aunque no fue hasta el 2008 que empezaron a surgir publicaciones sobre ella, para finalmente, en el 2009, demostrar su interoperabilidad y comenzar su despliegue. En términos generales, los números que se pueden dar sobre el alcance de su expansión es de más de 15 millones de medidores instalados en más de 9 países alrededor del mundo

Si acudimos a la página oficial de PRIME [12], lo que nos encontramos es en mayor detalle estos números. Para poder entenderlos mejor se dividirán las zonas en EMEA, Asia/Pacífico y América.

En la zona EMEA, una de las zonas donde mayor peso tiene Iberdrola, la expansión de PRIME ha sido revolucionaria. Encontramos que los países donde actualmente hay medidores instalados son Djibuti (una zona al este de África), el Líbano, Polonia, Portugal, Rumanía, Reino Unido, España y Suiza. A día de hoy, el despliegue de Iberdrola cuenta con unos 4 millones de medidores en nueves países distintos cooperando con distintos vendedores, que utilizan distintas versiones de PRIME y DLMS COSEM como protocolo del nivel de aplicación. En 2016 llegaron consiguieron alcanzar el 70% de instalaciones [21].

Por su parte, Unión Fenosa, empresa subsidiaría en distribución de electricidad de GAS NATURAL FENOSA, cerró el año 2014 con más de 1.26 millones de medidores inteligentes domésticos instalados e integrados en sistemas remotos. Este número representa el 35.2% del mercado de la compañía. Además, dado que esta empresa tiene una cuota de mercado muy alta en toda España, todo el proceso de instalación y despliegue se agilizará a medida que los consumidores reclamen este producto puesto que es algo con lo que ya se han integrado.

Figura 83. Logo de la compañía PRIME Alliance [20]

De la misma manera, PRIME Alliance trabaja con Energa operator, EDP, SCOTTISH POWER para conseguir abarcar mayor territorio y aumentar así su implantación en Europa.

Pasando a la zona de América, nos encontramos con que Iberdrola trabaja en el despliegue de la tecnología a través de su filial NEOENERGIA. Actualmente se encuentra en actividades de evaluación que demuestren que PRIME es una solución que puede cubrir la demanda en redes locales. En la siguiente fase se utilizará un área piloto mayor donde se desplegarán y podrán a prueba estos medidores en términos de escalabilidad y acondicionamiento. Actualmente, los países donde han aterrizado han sido Argentina y Brasil [21].

Por último, llegamos a la zona del Asia/Pacífico. En esta zona nos encontramos que la empresa encargada de la expansión es Energex, una de las empresas de distribución de electricidad más grandes y con mayor crecimiento de Australia. En la actualidad dan servicio a unos 2.8 millones de personas en la zona del sureste de Queensland. Por el momento Energex está evaluando PRIME para determinar su sostenibilidad dentro de la red australiana. En esta área, los países en los cuales, bien se han desplegado ya algunos medidores, bien se están llevando a cabo estudios, son Australia, Rusia, India y Corea del Sur.

Como podemos ver, PRIME es un estándar muy sólido, con una base técnica muy bien desarrollada que le ha permitido introducirse en el mercado de una manera rompedora y conquistar zonas del mundo dentro de las cuáles está creciendo, adaptándose y evolucionando. A pesar de no haber sido el primer protocolo en desarrollarse, ha conseguido ganar cuota de mercado y ha presentado un modelo lo suficientemente robusto como para crear, y tomar beneficio de, la necesidad de instalación de medidores inteligentes en los hogares. Por otro lado, otro factor que ha ayudado mucho durante su expansión ha sido el respaldo y solidez que una empresa tan asentada como Iberdrola proporciona a cualquier proyecto.

9.2 G3 PLC

La alianza G3-PLC surge bajo el sponsor de Enedis, y fue formada con el fin de dar soporte y promover la implementación y desarrollo de la tecnología g3-plc. Entre sus miembros destaca la presencia de todo tipo de compañía que intervienen en este mercado como, por ejemplo, compañía de electricidad, fabricantes de equipos y semiconductores, vendedores de tecnologías IT o incluso compañías de automóviles [12].

Figura 84. Logo de la compañía G3-PLC Alliance [12]

Los objetivos principales de esta compañía son:

- Dar soporte al estándar G3-PLC a nivel internacional, favoreciendo así su rápida implementación y aceptación a nivel mundial.

- El desarrollo de un marco común para la realización de pruebas a equipos que facilite la interoperabilidad de este protocolo con todos aquellos que deseen implantarlo en sus sistemas.
- Educar el mercado y promover el valor y beneficios de las aplicaciones de G3-PLC.
- Establecer un foro donde se puedan llevar a cabo discusiones y debates sobre posibles revisiones, proposición de ideas para nuevas implementaciones, etc. De esta forma se convertiría en un punto donde tanto compradores como desarrolladores podrían poner en común sus necesidades.

La presencia que tiene este protocolo a nivel internacional es muy grande, habiendo conseguido implantar esta tecnología, en distintos escenarios en casi todos los continentes del mundo. Ahora mismo, los proyectos que se están desarrollando se pueden categorizar en tres escenarios distintos.

Por un lado, tendríamos el estado piloto, donde se está estudiando la viabilidad de este estándar y poniendo en común con las empresas de servicios públicos nacionales. Un ejemplo de países donde se encuentran este tipo de proyectos serían México, China, Turquía o Rusia.

En un segundo tipo encontraríamos los proyectos en desarrollo, donde este protocolo ya está en uso. Principalmente este tipo de proyectos se encuentran en Europa, en países como Francia y Alemania, aunque fuera de Europa tendríamos también a una gran potencia como Japón. Además, para estos países G3-PLC Alliance cuenta con la ayuda y apoyo de los principales proveedores de servicios de los países donde se desarrollan como ERDF en Francia, EDP en Portugal, WIN Enegery and St Louis Coop en USA y TEPCO y Chugoku en Japón [12].

Por último, tendríamos los proyectos en proceso de pruebas de campo. Es decir, se encuentran en el último estado antes de pasar a su implantación definitiva. Estos proyectos se han extendido por muchos más países como Sudáfrica, India, Filipinas, etc. En general se trata de países del sureste asiático que se encuentran en desarrollo.

En la documentación oficial de la página web de la compañía podemos encontrar la Figura 85 donde se ve en mayor detalle cuáles son los países en los que actualmente G3-PLC tiene algún tipo de presencia.

Figura 85. Presencial actual de G3-PLC a nivel mundial [22]

Si pasamos a analizar los números no encontraríamos con que G3-PLC Alliance trabaja en un proyecto cuyo objetivo es conseguir 35 millones de medidores inteligentes instalados y 600.000 concentradores de datos listos para ser utilizados en el período de seis años que va desde el 2015 al 2021. Sólo en 2016 consiguieron instalar 37000 medidores en Francia con resultados muy satisfactorios en términos de tasa de éxito, tasa de colección de datos y tasa de mejoras a nivel SW. Todo ello sirviendo de propulsor para este estándar en los próximos años.

Por último, es importante destacar que de entre los miembros que forman parte de esta alianza se encuentran empresas muy reconocidas en el campo de las telecomunicaciones a nivel internacional como son: Texas Instruments, Ericsson, Panasonic, Toshiba y Siemens.

9.3 METERS & MORE

Esta tecnología surge de la mano de Enel Distribuzione SpA y Endesa Distribución SA, quienes constituyeron y asociación no gubernamental internacional conocida como METERS AND MORE y cuya base se instaló en Bruselas.

Figura 86. Logo de la compañía Meters & More [13]

La asociación opera y promueve nuevas generaciones de protocolos de comunicación METERS AND MORE y está abierta a terceros partidos. Desde su constitución, alrededor de 45 nuevas compañías se han unido a esta asociación. Esta asociación se beneficia de la experiencia de Enel's Telegestore, que es la única solución AMI que opera a nivel mundial con más de 40 millones de consumidores.

El protocolo M&M se implementa en medidores electrónicos que Endesa empezó a instalar entre sus 13 millones de consumidores en España, cifra que ya se ha cubierto este año.

En la actualidad, M&M ha desplegado más de 50 millones de medidores y sigue aumentando. Entre los países donde ha llevado a cabo el despliegue se encuentran los siguientes:

- Italia: con más de 38 millones de medidores operando gracias a la empresa Enel y otras empresas nacionales.
- España: donde cuenta con alrededor de 10 millones de medidores operando y un proyecto de instalación de más de dos millones. Todo ello gracias a la ayuda de la

compañía Endesa. Además, de la mano de Viesgo, M&M cuenta con otros 800k medidores operando.

- Rumanía: donde ya hay 420k medidores en despliegue y progreso, cifra que se ha logrado gracias a ENEL y E.ON.
- Montenegro: aquí M&M cuenta con 150k medidores operando más un proyecto de instalación 95k medidores más. Para ello se ha ayudado de EPCG.
- Latam: M&M tiene un proyecto de 100k medidores en instalación gracias a Edelnor y otras empresas nacionales.

Como podemos ver, el alcance de este protocolo incluso supera el de PRIME y G3 PLC dado que se trata de un protocolo con mayor recorrido y al mismo tiempo más sencillo y fácil de interoperar con las redes existentes. M&M utiliza una pasarela basado en una extensión del protocolo de comunicaciones existente entre los medidores inteligentes y los dispositivos del hogar que permite ambos, la medida de niveles de consumo y la inclusión de nuevos servicios. Además, se puede comunicar con otras tecnologías como Wi-Fi, ZigBee, Bluetooth, etc. Esto hace que M&M haya tenido tanto éxito y le sigue permitiendo crecer a los niveles que está haciéndolo.

9.4 COMPARATIVA

Si bien es cierto a que a nivel de datos concretos lo que podríamos decir sin temor a confundirnos es que Meters and More es el estándar más extendido a nivel internacional a día doy, no por ello se trata del estándar que mayor proyección de futuro tiene de los tres. Meters and More se trata de un estándar con mayor recorrido y mayor simpleza a nivel técnica que hace que, en muchos de los escenarios sea la opción perfecta. Sin embargo, muchas veces los escenarios no son tan idílicos como nos gustaría y necesitamos algo que nos dé mejor rendimiento, aunque sea más complejo.

En cuanto al despliegue comercial actual, en la segunda posición encontraríamos PRIME. Un protocolo muy robusto, muy orientado al detalle, que engloba y da soporte en

situaciones adversas pero que mantiene de alguna forma la simpleza a la que tiende Meters and More. Se trata de una solución ya probada en muchos escenarios con resultados a nivel de rendimiento muy buenos y al que además dan soporte pesos muy pesados en el campo de los servicios esenciales. Es por ello que cuenta con la aprobación del consumidor puesto que le respalda la "empresa de toda la vida".

Por último, en tercera posición en el pódium encontraríamos G3-PLC en lo que a comercialización se refiere. Se trata de un estándar muy potente, que cubre absolutamente todas las necesidades, que ha pensado en todos los posibles escenarios y ha desarrollado una solución para todos ellos. Sin embargo, tal vez sea demasiado complejo como para implantarse tan rápido como sus competidores. Es por ello por lo que, a nivel de instalaciones llevadas a cabo y proyectos en desarrollo, se trata de un estándar que va por detrás de los anteriores. A pesar de ello, como ya se ha visto en apartados anteriores, ha conseguido un gran peso a nivel internacional y está consiguiendo crearse un nombre dentro del sector que muy posiblemente en el futuro lo mueva a la posición número uno, convirtiéndose en el estándar de comunicaciones PLC por excelencia.

Capítulo 10. MODELO IMPLEMENTADO

En el siguiente apartado se presenta toda la información relacionada con los casos de uso, análisis, desarrollo e implementación del protocolo de comunicaciones *Meters & More*.

10.1 ANÁLISIS DEL SISTEMA

Antes de comenzar con la codificación del protocolo es necesario establecer los requisitos fundamentales que se deben satisfacer de cara a poder obtener los datos más fiables de las pruebas que se desarrollen.

Dentro de las principales características que debe presentar la implementación del protocolo se encuentran:

- **Realismo**. Dado que el objetivo último de este código es conseguir implementar un escenario del cual se puedan obtener medidas que complementen la información técnica que se encuentra ya disponible, es necesario garantizar que el entorno que se desarrolla para las pruebas es lo más fiable posible. De esta manera se garantiza que las comparaciones que hagan con otros protocolos se encuentran bajo las mismas premisas. En cualquier otra situación los resultados no serían válidos. Para esto se han modelado las líneas de comunicación estableciendo los retardos y tiempos de propagación propios de una línea real.
- **Escalabilidad.** De nuevo, nos encontramos ante un sistema que es completamente escalable en el mundo real. Esto significa que las simulaciones e implementaciones del código no pueden ser estáticas, deben ser escalables y no pueden estar hechas para un número fijo de dispositivos.
- **Consistencia**. Es necesario garantizar que se cumplen con todas las características del protocolo, interpretar correctamente la especificación técnica

y documentación disponible y garantizar que todo queda reflejado en la configuración de los dispositivos.

Todas estas características quedan reflejadas en los distintos casos de uso o escenarios que se han desarrollado con este modelo. En concreto, y dadas las características que se han descrito ya en apartados anteriores respecto a las funcionales del protocolo, el comportamiento que se ha simulado se muestra casi en su totalidad en la siguiente figura.

A modo explicativo, en ella se presenta como los dispositivos (maestro y esclavos) se inicializan, configuran con los parámetros básicos de comunicaciones y el maestro genera el primer REQUEST que va dirigido a un esclavo. Todos los esclavos reciben el mensaje, pero sólo lo procesa aquel dispositivo para el cual vaya dirigido, es decir cuya dirección coincida con la del mensaje. Una vez procesado, el mensaje se almacena en un buffer de repeticiones de tal forma que, si después de que el temporizador termine no se ha recibido ningún mensaje del maestro, se establece que ha habido un fallo en la comunicación y por tanto se procede a una retransmisión. Tras esta operación se genera un mensaje de respuesta conocido como INDICATION que confirma la recepción del REQUEST.

Cuando el maestro recibe el mensaje, primero simula el tiempo de procesamiento, para después eliminar el mensaje REQUEST de su buffer, parar el temporizador y almacenar el nuevo mensaje, INDICATION en el buffer de repeticiones. Para confirmar este mensaje se envía un CONFIRM que de nuevo viaja por la red alcanzando a todos los dispositivos que estén conectados a ellas. Cuando envía este mensaje arranca el temporizador.

El esclavo receptor del CONFIRM, lo procesa, elimina el INDICATION del buffer y paraliza el temporizador no enviando ningún otro mensaje. A pesar de que cada mensaje es un ACK del anterior, el caso del CONFIRM es un caso especial puesto que sino la comunicación jamás terminaría. En este caso, para el maestro, la ausencia de mensajes una vez el temporizador ha terminado es una confirmación de que no ha habido problemas y por tanto establece el fin de la comunicación al eliminar el CONFIRM de su buffer.

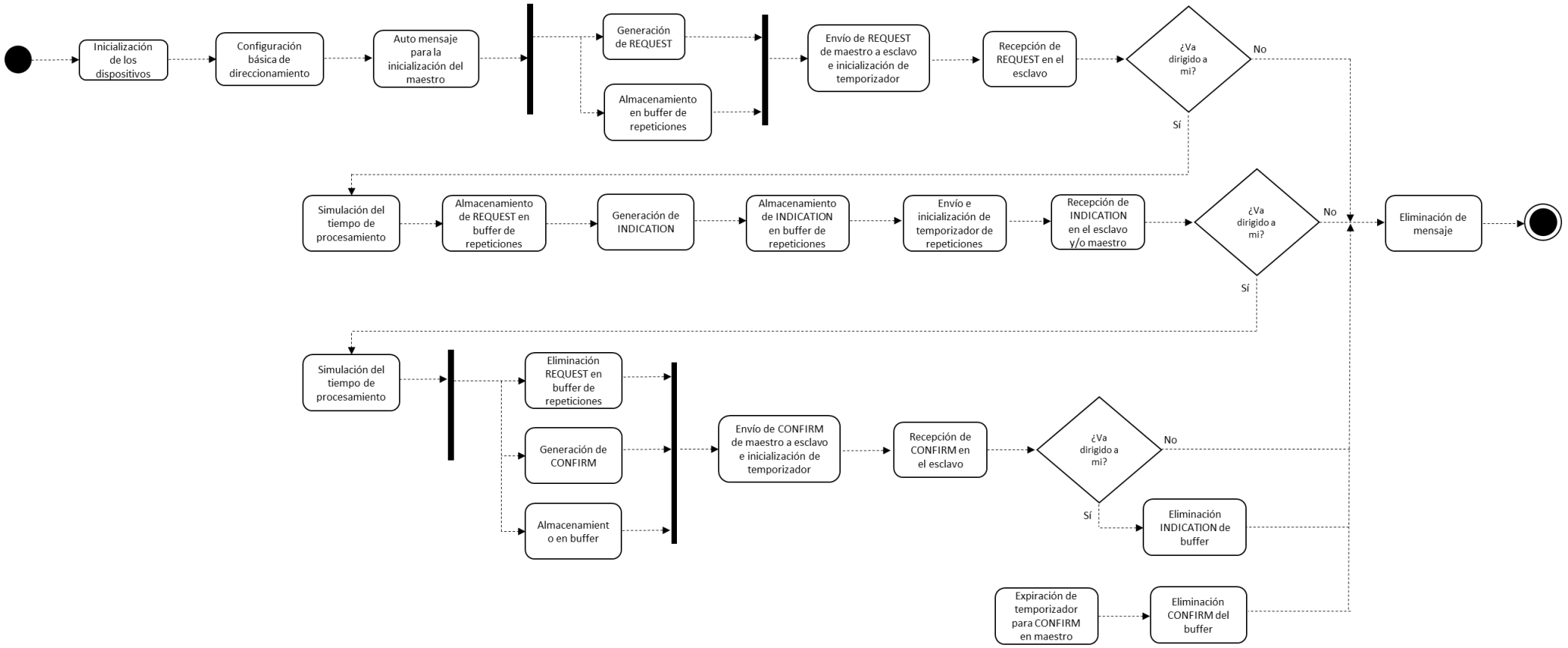


Figura 87. Diagrama de flujo del sistema implementado

10.1.1 ANÁLISIS DE RIESGOS

Como se ha mencionado anteriormente, la metodología utilizada para el desarrollo del proyecto es Scrum. Para poder afrontar cualquier tipo de problema y riesgo en el desarrollo de cada uno de los *sprints* se desarrolla una etapa de Análisis de Riesgos con fines evaluativos del proceso en cuestión y su evolución con cara al proyecto.

Se entiende como riesgo a la posible materialización de alguna amenaza, siendo las consecuencias un agente dañino para el sistema. A medida que se aumenta la complejidad de un proyecto también aumentan los riesgos. Las posibles decisiones a tomar necesitan de un análisis y previsión de posibles problemas que puedan surgir categorizándolos e intentando exponer soluciones. De la misma forma sucede cuando se realizan mejoras en los proyectos.

A continuación, se presenta una tabla donde se muestran las categorías de riesgos que han surgido durante el desarrollo del proyecto, así como qué objetivo se debe cumplir y cuál es la posible solución a aplicar:

Tabla 51. Análisis de riesgos

Riesgos	Riesgo 1	Riesgo 2	Riesgo 3
Definición	Modificación de requerimientos	Falta de documentación técnica	Dificultados con el entorno de desarrollo
Objetivo	Reducir el riesgo	Reducir el riesgo	Aceptar el riesgo si es el entorno óptimo
Solución	Se debe desarrollar un modelo parametrizable de tal manera que sea lo menos estático posible	Investigación a fondo de toda la documentación disponible para hacer un modelo lo más completo	Familiarización mediante tutoriales del nuevo entorno

10.2 DISEÑO

Una vez que se ha establecido qué es lo que tiene que hacer el sistema, es necesario estudiar cómo funcional los principales componentes y cómo se relacionan entre ellos. Esto nos ayudará a entender cómo se tienen que establecer las comunicaciones de cara a la arquitectura.

10.2.1 ARQUITECTURA EXTERNA

La arquitectura externa, se basa en los componentes, elementos y sistemas que intervienen en el proyecto, reflejando así su alcance. La arquitectura externa es también la arquitectura referente a los elementos hardware que componen el proyecto y que soportan el correcto funcionamiento del sistema en cuanto a calidad de servicio.

La arquitectura externa de todo el sistema se representa de forma sencilla en el siguiente esquema.

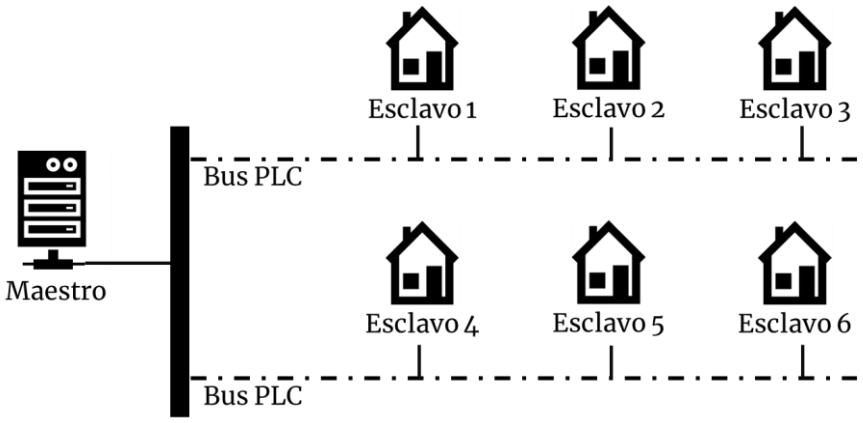


Figura 88. Arquitectura externa del sistema

El primer elemento hardware que tendríamos sería el maestro que se comunicaría con los esclavos a través de dos líneas tipo bus donde habrá dispuestos tres esclavos en cada una de ellas. Este esquema es un esquema muy realista donde el maestro se encontraría situado en la estación de transformación más cercana y cada uno de los esclavos representarían los medidores

inteligentes que estarían instalados en los hogares. Sin embargo, y a pesar de que con esta arquitectura es suficiente, es importante no olvidar que el escenario completo incluiría otro maestro en la sede de la compañía distribuidora desde donde se harían todas las peticiones y gestionarían las comunicaciones.

10.2.2 ARQUITECTURA INTERNA

La arquitectura interna es la encargada de la descripción de las unidades funcionalidades del proyecto. En este caso no se especifica una arquitectura interna porque ya se ha explicado cuál es el funcionamiento del protocolo y es ésta mismo comportamiento el que constituye la arquitectura interna del modelo.

10.3 IMPLEMENTACIÓN

Durante el siguiente apartado se detallarán las etapas del proceso de implantación del sistema siguiendo el diseño y la arquitectura que se ha ido explicando y desarrollando durante todo este capítulo.

Para poder exponer de forma clara la implementación se irán detallando los distintos módulos basados en la arquitectura externa, interna y propia del proyecto. Junto con toda esta información también se especifica qué técnicas se han utilizado en el proyecto para la consecución de su funcionamiento.

10.3.1 CARACTERÍSTICAS DEL MODELO

Para lograr una mayor comprensión del proyecto y poder especificar su desarrollo es necesario primero comenzar con una descripción de las características que componen el sistema. El objetivo principal del proyecto es conseguir simular un entorno lo suficientemente realista que permita obtener datos de rendimiento, retardos, tasas de error,

etc. Que permitan establecer comparaciones más precisas con otros protocolos que se encuentran actualmente en el mercado.

10.3.2 MÓDULOS

Ya en apartados anteriores se han introducido los principales módulos que comprenden el sistema, siendo estos el maestro y el esclavo, además de la propia red PLC que se utiliza como medio de comunicación. Sin embargo, desde el punto de vista de la implementación, lo más interesante resulta el comportamiento del maestro y esclavos puesto que es en estos donde se encuentra toda la lógica que proporciona las características a este modelo.

En ambos casos las funcionalidades principales en alas que se dividen son las siguientes:

- Gestión de envío y recepción de mensajes, así como procesamiento en caso de que éste sea el destinatario.
- Gestión del temporizador de repeticiones que garantice que la comunicación se lleva a cabo y que la información no se pierde.
- Gestión del buffer de mensajes de repetición que evite que la comunicación se quede a medias.

Además, y debido a las limitaciones del software utilizado, un reto importante a la hora de gestionar todo el procesamiento de información fue el de simulación del tiempo de procesamiento en los nodos origen y destino. Para ello se hizo uso de una característica propia del software que es la capacidad de un nodo de enviarse auto-mensajes con un cierto retardo que simule el tiempo de procesamiento y que mantenga al dispositivo en estado ocupado para evitar que otra comunicación pueda interferir. A continuación, se presenta parte del código desarrollado para estas funcionalidades, junto con un diagrama de secuencia que identifica cada uno de los escenarios que se describen en el código con el fin de proporcionar una mayor claridad sobre el funcionamiento del modelo.

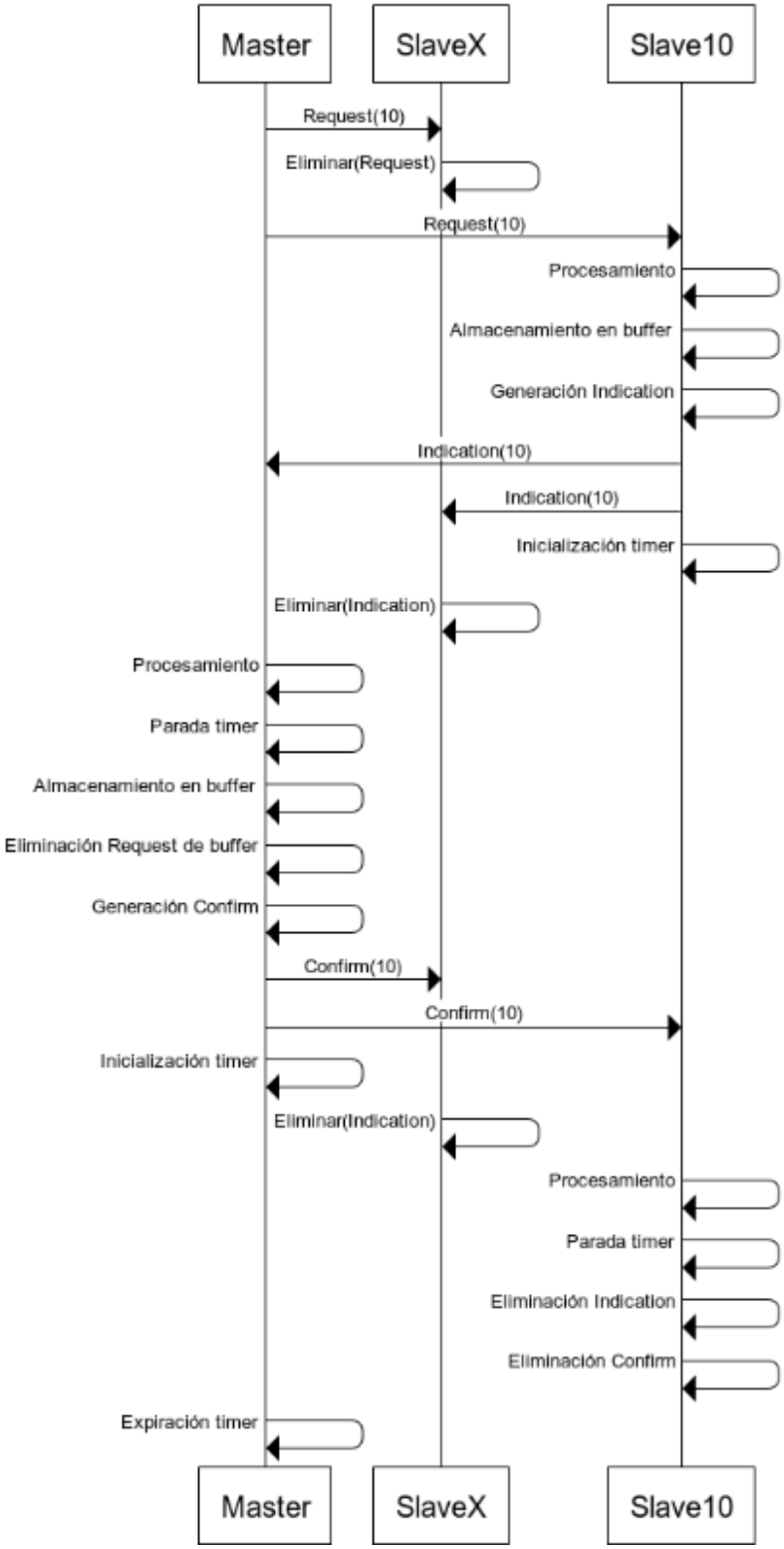


Figura 89. Gestión de mensajes en escenario sin errores

```
void CommonMAC::handleDataMsg(MacMessage *macmsg){

…
                case REQUEST:{

                    llcmsg->setSdu(INDICATION);
                    macmsg->setId(macmsg->getId()+1);
                    send(macmsg, 1);

                    EV << "SIMULATING TRANSMISSION\n";
                    simtime_t propagationTime = (macmsg-
>getByteLength()/1200)*1000;
                          …
                    cMessage *txMsg = endTxMsg->dup();
                    txMsg->setKind((short)macmsg->getId());
                    scheduleAt(simTime()+propagationTime, txMsg);
                    saveMessage(macmsg, txMsg);
                          …
                    break;
                }

                case INDICATION:{

                    latencyBetween2Nodes = simTime() - latencyBetween2Nodes;
                    pairLatencyVector.record(latencyBetween2Nodes);
                    lista.delete_element(listaRepeticiones, macmsg->getId()-1);
                    llcmsg->setSdu(CONFIRM);
                    macmsg->setId(macmsg->getId()+1);
                    send(macmsg, 1);

                          …

                    cMessage *txMsg = endTxMsg->dup();
                    txMsg->setKind((short)macmsg->getId());
                    scheduleAt(simTime()+propagationTime, txMsg);
                    saveMessage(macmsg, txMsg);
                    break;
                }

                case CONFIRM:{

                    lista.delete_element(listaRepeticiones, macmsg->getId()-1);
                    delete(macmsg);
                    status=IDLE;
                          …

                    break;
                }
}
```

En concreto, en el código anterior es una versión simplificada de la función que gestiona el tratamiento de mensajes en función del tipo de mensaje que sea. Como se puede apreciar en el código, se distinguen tres tipos de mensajes distintos, los que ya se presentaron en la parte teórica de descripción del protocolo, y el almacenamiento en buffer y gestión de temporizadores en función de si es necesario o no activarlos debido al mensaje que se transmite.

De nuevo, y como ya se ha explicado antes, la gestión de los temporizadores y tiempos de espera (procesamiento y propagación) son los más críticos a lo largo de todo el código y es por hecho que la manera en que se ha decidido tratarlos ha sido con mensajes que se envían desde el dispositivo a sí mismo y que permiten simular un estado ocupado de cara al resto de la red.

En el diagrama a continuación se presenta un pequeño fragmento de lo que sucedería si uno de los temporizadores expira a mitad de la comunicación y cómo se gestionaría entre los dispositivos que están involucrados.

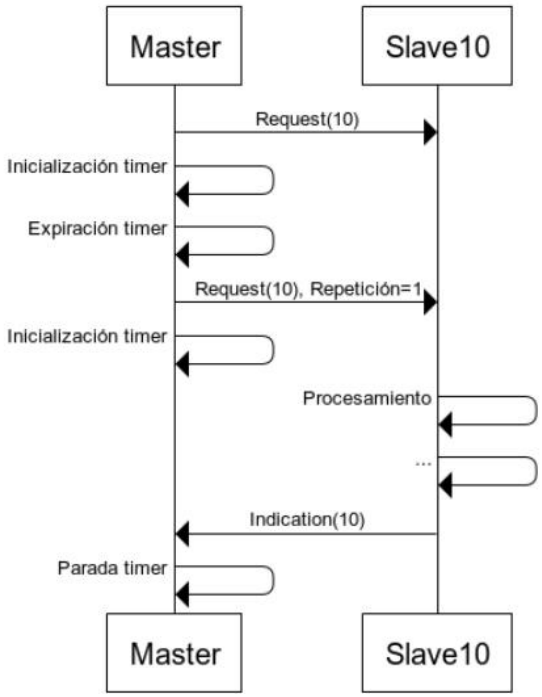


Figura 90. Gestión de temporizadores

```
if(!Waitting){

    EV << "SIMULATING TIME BEFORE SENDING AGAIN";
    cMessage *self = new cMessage("self");
    simtime_t waittingTime = TIME_BEFORE_SENDING_AGAIN;
    self->setKind(nodo.mensajeId);
    scheduleAt(simTime()+waittingTime, self);

    nodo.timer = self->dup();
    lista.edit_element(listaRepeticiones, nodo.mensajeId, nodo);

    Waitting = true;

}else{

    cPacket *packet = nodo.mensajeRetransmision->getEncapsulatedPacket();
    LlcMessage *llcmsg = check_and_cast<LlcMessage *>(packet);

    if(llcmsg->getSdu()!=CONFIRM){

        if(nodo.retransmisiones<MAX_REPETITIONS){

            nodo.retransmisiones++;
            MacMessage *macmsg = nodo.mensajeRetransmision->dup();
            send(macmsg,1);

            …

            lista.edit_element(listaRepeticiones, nodo.mensajeId, nodo);

            …

        }else{

            …
            lista.delete_element(listaRepeticiones, nodo.mensajeId);
            delete(msg);
            …
        }

    }else{

        lista.delete_element(listaRepeticiones, nodo.mensajeId-1);
        lista.delete_element(listaRepeticiones, nodo.mensajeId);
        Waitting = false;
        …

    }
```

De nuevo, de manera simplificada, el código refleja cómo se gestionan estos temporizadores y cómo se decide si es necesario realizar una retransmisión o no. Este papel es importante porque, como se ha explicado, existe un mensaje que no funciona como los demás y este es el CONFIRM. Este mensaje es ACK del INDICATION, pero no tiene un ACK propio, sino que la falta de retransmisiones por parte del esclavo indica que todo ha ido bien y por tanto que no es necesario volver a enviar el CONFIRM.

Por último, y dado que se trata de un aspecto fundamento dentro del diseño de la arquitectura y de la gestión de información transmitida y recibida en cada nodo, se presenta el elemento empleado como buffer de retransmisiones que gestione toda la lógica de almacenamiento de mensajes de tal manera que se permitan conversaciones simultáneas sin que la integridad y confidencialidad de la información quede en entredicho.

Este aspecto es muy importante puesto que, a pesar de que por el momento el protocolo está diseñado de tal forma que sólo el maestro puede hacer peticiones y comenzar las comunicaciones y nunca el esclavo, en una conversación uno a uno hasta el final., sí que podría darse la situación en la que el protocolo se adaptase a nuevas necesidades.

En este escenario se permitirían varias comunicaciones simultáneas, o incluso se les daría a los esclavos la posibilidad de reclamar información del maestro, proporcionándoles así mayor autonomía.

Es decir, de cara a futuros estudios y futuros avances, este proyecto está pensado para adaptarse a cualquier cambio y permitir establecer nuevas y mejoradas medidas. La arquitectura de la estructura se define en el siguiente diagrama de clases. En este diagrama solamente se explican más en detalle las clases en concreto que se han desarrollado para conseguir la estructura deseada. Clases como *CMessage* son clases propias del software y cuya explicación se encuentra fuera del alcance de este proyecto.

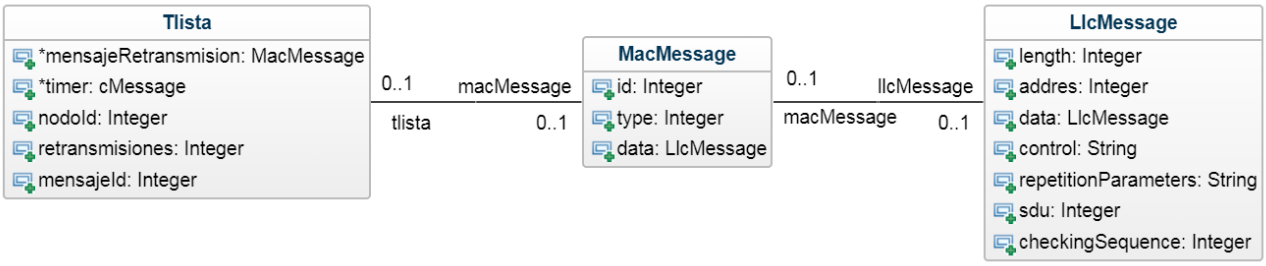


Figura 91. Diagrama de clases de la estructura del buffer

Capítulo 11. ANÁLISIS DE RESULTADOS

En este capítulo se presentan los resultados obtenidos a partir de la implementación que se ha explicado en el capítulo anterior. A pesar de que en este proyecto existen otro tipo de resultados estudiados en la parte teórica, en este apartado no se incluyen puesto que ya se han explicado.

Antes de comenzar a exponer los resultados obtenidos, es importante remarcar que el estudio que se ha hecho del protocolo *Meters and Mores* ha sido sólo a nivel de capa MAC. Tanto la capa PHY como la capa LLC se presentan como algo breve y resumido de tal manera que se aporte la consistencia a la simulación necesaria, pero sin ahondar en sus componentes o estructuras. Esta decisión se tomó a lo largo del proyecto por dos razones principales.

La primera razón es que, en la capa PHY, la estructura del protocolo es una estructura muy básica cómo ya se ha explicado a lo largo de su análisis. Es por ello que, sin necesidad de realizar implementaciones, se puede simular de una manera muy sencilla su comportamiento con un nivel de certeza relativamente alto. Esto no sucedería con PRIME ni con G3-PLC puesto que se tratan de protocolos mucho más robustos con muchos más sistemas para la proporción de características más sofisticadas, que dificultan su simulación en un entorno como OMNet++.

La segunda razón justifica la decisión de no implementar la capa de convergencia, o capa LLC. Esta se basa en la falta de información existente acerca de su estructura. Así como la falta de funcionalidades añadidas que merecen la pena estudiarse. De nuevo algo muy parecido a lo que sucede con la capa PHY.

Todo ello ha dado lugar al establecimiento de un entorno de pruebas que generase de manera lo más certera posible el comportamiento del sistema a fin de comprender cómo se comporta, qué cabe esperar de él y cuáles son los valores que se pueden obtener.

A pesar de que la capa MAC sí que dispone de más información dentro del estándar, aún no es suficiente como para entender perfectamente cómo funciona. Es por ello que, en base a lo que se ha extraído de la especificación técnica y de diversos *papers*, se han seguido las distintas premisas que se presentan a continuación.

CSMA/CA

Es necesario implementar un entorno que simule la existencia de CSMA/CA. Es decir, es necesario garantizar que en el entorno de pruebas existe un mecanismo que garantiza que los paquetes de dos comunicaciones distintas no pueden chocar entre ellos, dando lugar a la pérdida de ambos. Para garantizar que esta regla de oro se cumple, se ha implementado el comportamiento de los dispositivos de tal manera que sólo el maestro puede generar una nueva comunicación y que los esclavos no pueden pedir información al maestro bajo ninguna circunstancia. De esta manera se garantiza que, dado que el maestro decide con quién comunicarse y cuando, éste podrá gestionar qué paquetes se encuentran dentro del bus, impidiendo que haya colisiones. Es cierto que existen mecanismos para evitar colusiones mucho más sofisticados que implementan periodos de contienda a través de mensajes pilotos. Sin embargo, dada la estructura de *Meters and More*, nada hace que pensar que se hayan introducido mecanismos más complejos que el que se ha decido implementar.

Número de repeticiones

Otra premisa importante sobre la cual se han tenido que tomar decisiones ha sido la gestión del número de repeticiones que se pueden hacer antes de dar por perdida la comunicación. En la especificación técnica se explica la existencia de un mecanismo de repeticiones que garantiza que, en caso de que el medio problemático, con ruido, existe un mecanismo que garantiza que no toda la información se pierde cuando se envía el paquete, sino que existe la posibilidad de reenviar el paquete en caso de que pase un cierto tiempo de espera que también ha tenido que ser definido, al no encontrarse explícito en la especificación. Para la identificación del número de repeticiones se ha decidido utilizar la siguiente fórmula:

$$N = \frac{1}{1 - Pe}$$

En esta fórmula N es el número de retransmisiones y Pe la probabilidad de error de paquete, también conocida como PER. Para poder identificar qué valores hay contemplar como razonables para esta variable, es necesario entender cuáles son las características que presentan las redes típicas PLC. En el documento [22] se muestra la gráfica a continuación. Esta gráfica refleja los valores de error de bit (BER) en función de distintos valores de SNR para dos comunicaciones distintas, entre X e Y y entre X y Z. En este mismo documento se identifica que el escenario más realista es el escenario X,Y donde una curva refleja las condiciones sin ruido impulsivo y la otra con ruido impulsivo.

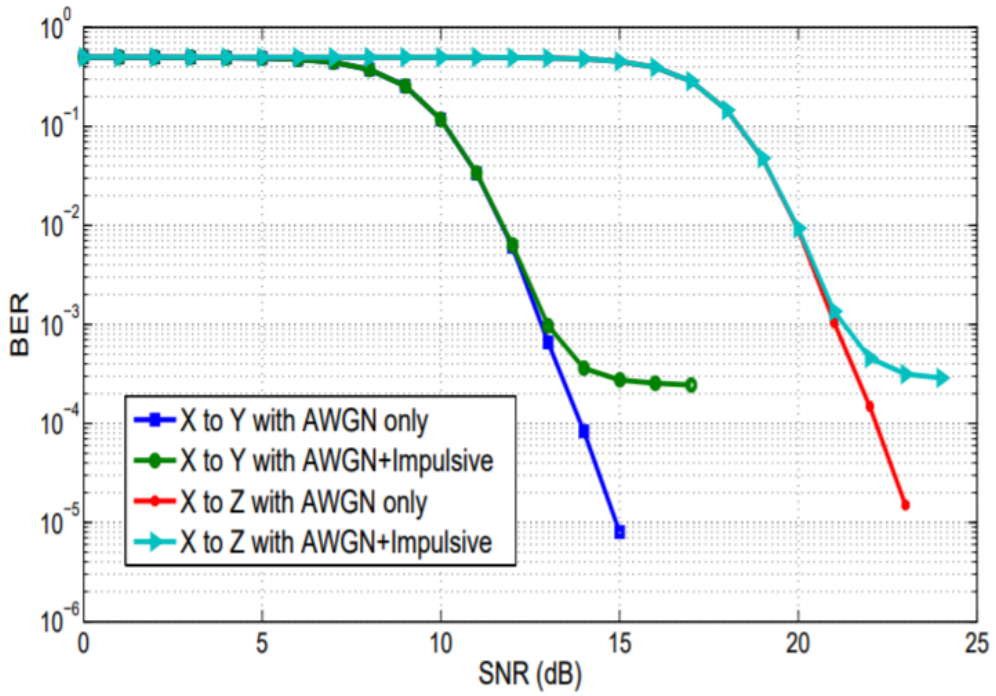
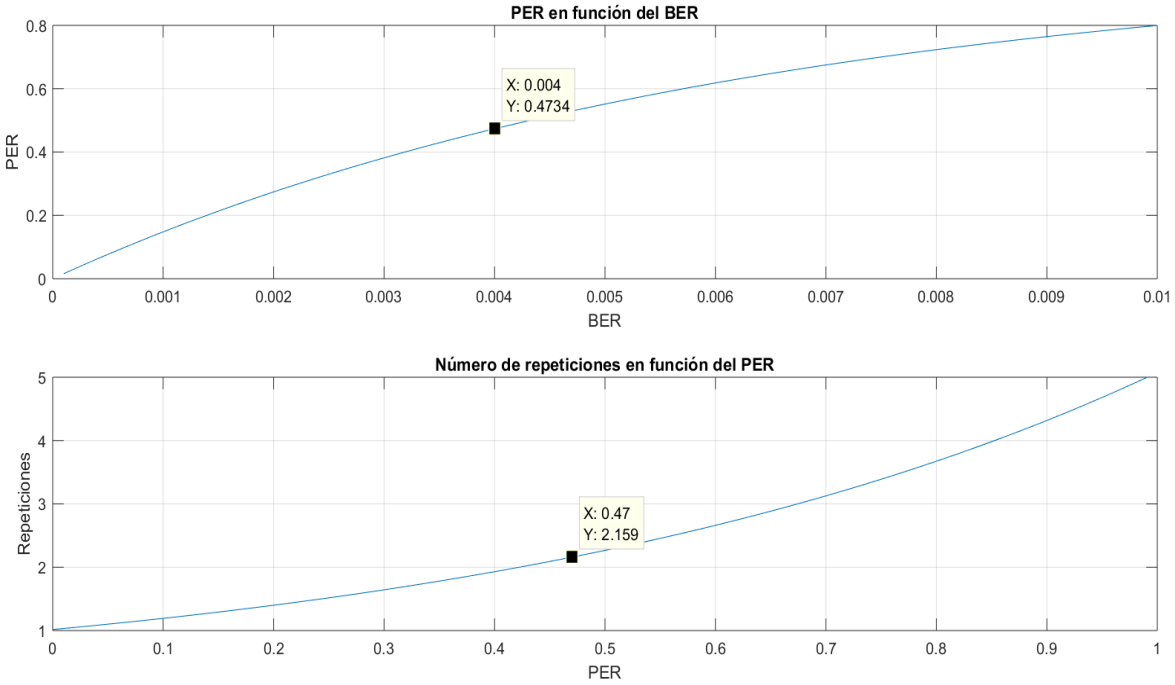


Figura 92. BER vs. SNR en sistemas PLC de bajo voltaje.

Como se puede ver, el rango de valores oscila entre 1e-4 y 1e1 en condiciones de error razonables. Basándonos en estos valores y en la siguiente fórmula, se han calculado los distintos valores de PER.

$$PER = (1 - (1 - BER)^{bit\_length})$$

En esta fórmula la longitud de bit del paquete se ha fijado a 160 bits al tener cada



paquete una longitud mínima de 12 bytes.

Figura 93. PER y número de repeticiones en función del BER

Con la intención de seleccionar un valor intermedio que refleja un escenario real, se ha decidido fijar el valor del BER a 0.004, es decir, un SNR de unos 13dB, obteniendo así unos valores de PER y número de repeticiones del 47% y 3 respectivamente. Es importante notar que, a pesar de que el número de repeticiones ha salido de 2.159, el hecho se superar el valor 2 indica que es necesario una unidad más ya que no se pueden realizar un número decimal de repeticiones.

Tiempo de espera

Por último, a la hora de justificar la elección del tiempo de espera para la retransmisión de paquetes, se va a seguir un método empírico y ajustado a las necesidades de este proyecto. Para ello se va a partir de un entorno ideal donde no hay errores y el canal está disponible y

se va a calcular la latencia media entre dos nodos. Para este tipo de protocolos un aspecto importante sería tener un tiempo de espera variable, que se realimente y adapte a las necesidades del medio, pero como se ha visto, *Meters and More* no está preparado para este tipo de aplicaciones. Este valor ha sido de 1.5 ms.

El estudio se ha orientado a la búsqueda de información acerca del rendimiento del sistema medido a través de dos variables. La primera de las variables ha sido la latencia entre dos nodos. Esta latencia se ha medido como el tiempo que pasa desde que el maestro envía la petición REQUEST hasta que le llega la respuesta RESPONSE. Por otro lado, la segunda variable ha sido la latencia total del sistema, que se me ha medido como el tiempo que pasa desde que el servidor manda la primera REQUEST hasta que finaliza la última comunicación, ya sea porque el paquete se ha perdido y ha alcanzado el número máximo de repeticiones, o porque ha recibido el último CONFIRM del último servidor. Los datos obtenidos de la primera variable se muestran en las gráficas que se presentan a continuación.

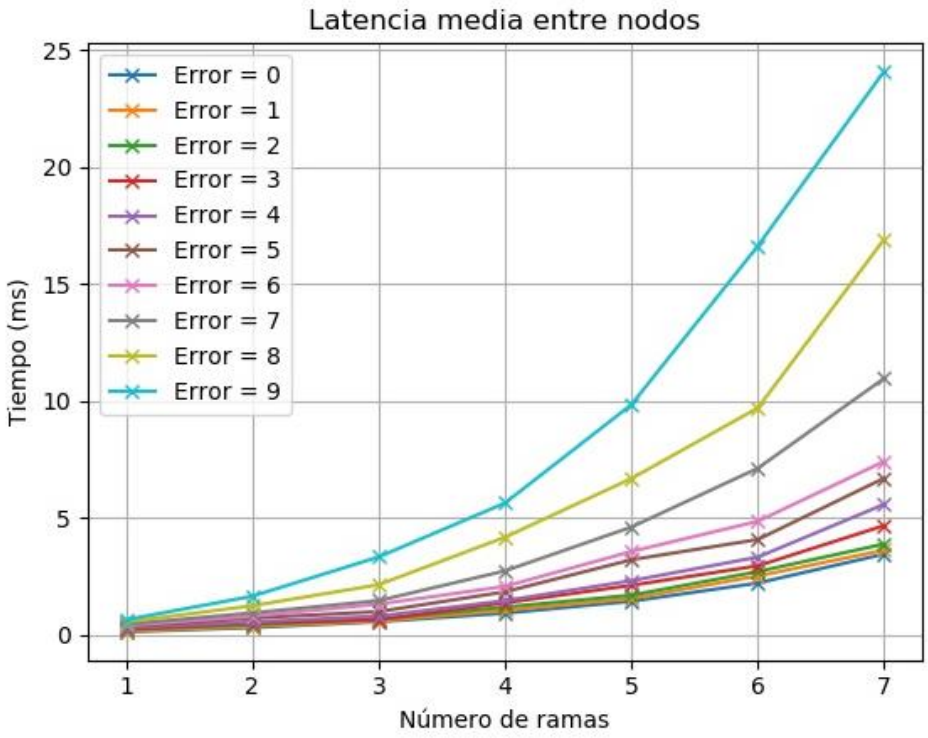


Figura 94. Latencia entre nodos

Para garantizar que la simulación incluía el mayor número de escenarios posibles, se han hecho variable el número de ramas del escenario, variando desde una rama hasta siete, y se han hecho diez repeticiones por ramas. Al mismo tiempo se han ido variando las probabilidades de error desde 0% hasta 90% de tal manera que los mismos escenarios de error se someten a las mismas circunstancias.

Esta primera gráfica podemos ver que, a medida que el error aumenta la latencia media entre nodos, siendo este factor determinante para garantizar la consistencia de las simulaciones, y también podemos ver que, a medida que exponemos el sistema a situaciones más duras, este se comporta mucho peor que en el caso anterior. De nuevo, esta es una característica que nos permite entender y justificar los casos de uso de este protocolo en escenarios reales, donde solamente tiene sentido cuando sabemos que las condiciones del medio son muy buenas y lo que buscamos es un protocolo sencillo, fácil de implementar y, sobre todo, fácil de combinar con protocolos de capas superiores que implementen las lógicas más complejas de las que carece *Meters and More*.

A partir de un error de más del 20% de paquetes perdidos, la latencia media empieza a superar valores límites que solamente podrán ser juzgados y analizados por aquellas entidades que vayan a aplicar el protocolo en sus instalaciones, entendiendo si estos valores son o no lo suficientemente buenos como para que pueda proporcionar un servicio adecuado.

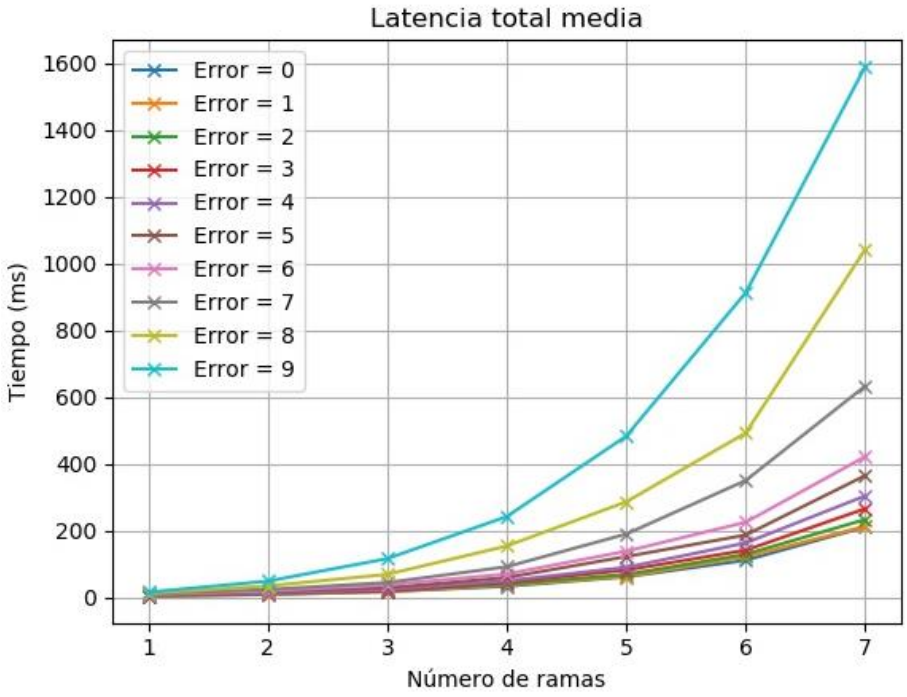


Figura 95. Latencia total media

La figura anterior muestra la latencia total media que se ha medida aplicando las mismas condiciones que se aplicaron para la obtención de la latencia entre nodos. Este parámetro resulta muy útil en términos de rendimiento puesto que, de cara a su aplicación, no es lo mismo disponer de una red con 10 nodos que de una red con 100. Es por ello que entender hacía qué tiene el sistema en función de cómo de grande sea el ámbito en el que se aplica y las condiciones del medio es fundamental a la hora de comparar entre los distintos protocolos a utilizar.

De nuevo nos encontramos con un comportamiento muy similar donde, al aumentar el número de ramas y la probabilidad de error, mayor es el tiempo que tarda el maestro en hacer una ronda con todos sus esclavos. Estos valores guardan consistencia con los obtenidos en las mediciones anteriores y simplemente justifican con números lo que el protocolo ya dejaba intuir en su especificación técnica. Se les han aportado datos empíricos a sus estimaciones.

Estos resultados, de manera aislada, no proporciona información suficiente. El mayor valor del que disponen es la contextualización que proporcionar al usuario de cara a comprender qué implicaciones tiene la instalación de cada de los protocolos medidos, sin la necesidad de ponerlos a prueba en pequeños entornos anteriormente. Con ello se pretende simplificar el estudio y análisis de este tipo de redes favoreciendo el desarrollo de nuevas funcionalidades que den solución a los problemas que estas comparaciones hayan podido arrojar sobre lo que ya se conocía.

Capítulo 12. CONCLUSIONES Y TRABAJOS FUTUROS

12.1 CONCLUSIONES

Este proyecto se presenta como una documentación más accesible y completa que proporciona al lector una visión general de las características más importantes de los tres protocolos de transmisión en PLC más extendidos en Europa. Se beneficia del uso de un lenguaje menos técnico que facilita la lectura a aquel lector que no necesariamente es un experto en el tema, aunque sí que debe presentar ciertos conocimientos básicos del sector y los algoritmos descritos.

El desarrollo del proyecto ha permitido identificar cuáles son las carencias más representativas en términos de información disponible, dando así una razón para desarrollar la simulación de uno de los protocolos estudiados. De esta forma se contribuye a la documentación disponible gracias a la aportación de parámetros técnicos como el rendimiento, la tasa de errores, el tiempo de procesamiento, etc.

A continuación se detallan las principales ventajas que ofrece este proyecto desde los dos principales puntos de análisis que se han presentado.

- **Elaboración de una síntesis divulgativa de los principales aspectos técnicos de los tres protocolos más extendidos en Europa.** Esta fue la razón principal por la que se definió este proyecto. A pesar de tratarse un tema muy en boca de todos, aún existe una falta muy importante de documentación técnica que verdaderamente explica qué son esos términos y esas tecnologías que se utilizan en las redes inteligentes. Este proyecto evita que este tipo de tecnologías queden únicamente reducidas a los ámbitos industriales, donde equipos técnicos sean lo

únicos capaces de comprender de qué se está hablando y cómo hay que tratarlo. Este documento se presenta como una síntesis de tipo divulgativo que, en su primera parte, no establece juicios de opinión, limitándose a recuperar los aspectos más importantes de las características técnicas de cada uno de los protocolos y recogiendo toda esta información en una misma fuente que hace más accesible este conocimiento al usuario medio.

- **Documentación y comparativa a nivel técnico de los tres protocolos.** Este estudio no sólo incluye una síntesis técnica simplificada de las características de estos tres protocolos, sino que también proporciona una comparación a nivel técnico de los principales indicadores de rendimiento. Para ellos se han empleado las medidas principales que garantizan que, sin necesidad de un conocimiento profundo del sector, cualquier lector pueda conocer cómo se miden las distintas tecnologías y de qué manera sus prestaciones afectan en mayor o menor medida al comportamiento último de la red. A la hora de identificar las necesidades que este proyecto cubría, quedo clara constancia de la existencia de una carencia grande de documentación con este tipo de características que no se limitasen únicamente a descripciones técnicas.
- **Documentación y comparativa del alcance comercial de los tres protocolos.** Como ya se ha definido en otras secciones del documento, se buscaba proporcionar una visión global del estado de los protocolos de tal manera que, si el lector desea conocer cuáles son lo beneficios o desventajas a nivel comercial de una tecnología u otra, dispusiese de esta información en un único documento. Tras el análisis llevado este proyecto garantiza que el usuario dispone de todos los parámetros fundamentales a nivel comercial para entender cuál es el alcance de cada una de las tecnologías y que características son las que las hacen más idóneas para un tipo entorno u otro.
- **Presentación de escenarios donde se identifiquen las fortalezas de cada tecnología a nivel comercial.** Al final de la comparativa comercial se incluyen parámetros que, de manera clara identifican situaciones cotidianas con las que el lector puede sentirse identificado. De esta manera se garantiza que la

comprensión es total y que no es necesaria la ayuda de otras documentaciones adicionales.

Por otro lado, este proyecto no se limita a una mera documentación, sino que además incluye un desarrollo práctico a modo de implantación y simulación de uno de los protocolos estudiados. Esta es una parte fundamental del proyecto donde, no sólo se reduce le estudio a una mera síntesis y documentación de información que ya se encuentra disponible en la red, sino que además se aportan datos técnicos que suponen una carencia importante dentro del sector.

Esta segunda parte supuso un reto dada la falta de información disponible en cuanto a las características técnicas del protocolo. Es justamente por ello que el objetivo fundamental era conseguir desarrollar un modelo lo más parametrizable posible, que incluyese el máximo posible de escenarios dentro de las simulaciones de tal manera que se garantizase que lo resultados obtenidos no tenían sesgo alguno y podían utilizarse cómo medidas estándar de comportamiento del sistema. Para ello se utilizó una herramienta software de simulación de redes que permitió elaborar una arquitectura clara y sencilla, fácilmente comprensible y escalable, que pudiese ser perfeccionada y expandida a medida que nuevas características fuesen desarrollándose dentro del protocolo.

Este proyecto constituye una fuente de documentación muy importante que, a pesar de estar al día con el estado del arte de las tecnologías, es fundamental que se mantenga y se vaya completando a medida que nueva documentación vaya surgiendo o nuevas mejoras e implantaciones vayan añadiéndose.

12.2 TRABAJOS FUTUROS

Este trabajo es un trabajo de investigación de un sector que se encuentra en pleno auge y desarrollo. Es difícil identificar trabajos futuros concretos, con características concretas, puesto que este sector aún se encuentra en desarrollo y en estados iniciales en muchos de los casos. Es por ello que, el principal trabajo futuro del que se puede hablar es

en la continuación de documentación de los avances que se vayan desarrollando, así como el mantenimiento de documentos como este, donde se hable no sólo de las consecuencias comerciales de las nuevas mejoras, sino también a nivel técnico, identificando posibles puntos de mejora o nuevos mercados donde implementar estas tecnologías.

Además, también resulta crucial, no sólo elaborar trabajos estáticos, sino también incluir todo tipo de simulaciones y estudios que complementen los parámetros definidos en las especificaciones técnicas. Sólo de esta forma se podrán identificar puntos de mejora que permitan que estas tecnologías siguen creciendo y expandiéndose.

Capítulo 13. BIBLIOGRAFÍA

[1] Y. A. M. Mendoza, E. J. Ramirez, T. P. P. Di Santis, L. M. R. Molina y N. A. P. García, «ESTADO DEL ARTE DE SMART GRID: PARTE I,» Universidad del Sinú, Mérida, 2015.

[2] E. Comission, «European Comission,» European Comission, 2017. [En línea]. Available: https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters. [Último acceso: Abril 2018].

[3] E. M. I. Ortega, «Redes de Comunicación en Smart Grid,» Ingenius, 2015.

[4] A. T. A. &. M. J. Haidine, «Deployment of power line communication by European utilities in advanced metering infrastructure,» IEEE International Symposium , 2013, March.

[5] OMNet++, «OMNet++ Discrete Event SImulator,» OMNet++, Enero 2018. [En línea]. Available: https://www.omnetpp.org/. [Último acceso: Febrero 2018].

[6] Wikipedia, «Wikipedia,» Wikipedia, 31 Mayo 2018. [En línea]. Available: https://es.wikipedia.org/wiki/C%2B%2B. [Último acceso: 12 Junio 2018].

[7] Anónimo, «Smart Grids y la evolución de la red eléctrica,» Observatorio Industrial del Sector de la Electrónica, Tecnologías de la Información y Telecomunicaciones, 2015.

[8] Matsumoto, «The HIstory of Electric Measuring Instruments and Active Components,» 2015. [En línea]. Available: http://ieeeghn.org/wiki/images/c/c8/Matsumoto1.pdf. [Último acceso: 2018].

[9] Malik, «Evolution of Power Systems into Smarter Networks,» Journal of Control, Automation and Electrical Systems, 2013.

[10] M. P. S. Commission, «Electronic Filling and Information Systems,» Missouri Smart GRid Report, Missouri, 2010.

[11] A. S. (L+G), «Prime Spececification,» Prime Alliance, 2015.

[12] G.-P. Alliance, «G3-PLC Alliance Org,» G3-PLC Alliance, 2016. [En línea]. Available: http://www.g3-plc.com/home/. [Último acceso: 2018].

[13] M. a. More, Meters and More, 2016. [En línea]. Available: http://www.metersandmore.com/. [Último acceso: 2018].

[14] M. Hoch, «Comparison of PLC G3 and PRIME.,» IEEE Power Line Communications and Its Applications International Symposium, 2011, April.

[15] Sendin, Berganza, Arzuaga, Pulkkinen y Kim, «Performance results from 100,000+ PRIME smart meters deployment in Spain,» IEEE Third International Conference, 2012, November.

[16] Z. Sadowski, «Compartison of PLC G3 and PRIME,» IEEE Power Line Communications and Its Applications International Symposium, 2015, June.

[17] Sendin, Kim, Bois, Munoz y A. Llano, «Prime v1.4 evolution. A future proof of reality beryond metering,» IEEE Smart Grid Communications International Conference, 2014, November.

[18] M. a. M. O. Technologies, «Meters and More Technical Specification,» Meters and More, Bélgica, 2015.

[19] G.-P. Alliance, «Narrowband orthogonal frequency division,» ITU-T, 2014.

[20] A. Lasciandare, «Meters and Mores implementation state,» Meters and More Open Technologies, Italy, 2016.

[21] P. Alliance, «Prime Alliance,» Prime Alliance, 2014. [En línea]. Available: http://www.prime-alliance.org/. [Último acceso: 2018].

[22] M. Korki, V. L. Hai, C. H. Foh, L. Xiao y N. Hosseinzadeh, «MAC Performance Evaluation in Low Voltage PLC Networks,» ENERGY 2011 : The First International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, 2011.

[23] J. M. Domingo, "Improvements in the plc systems for smart grid," Doctoral dissertation, Universidad Pontificia Comillas, 2013.

[24] F. Red, «Inventario - Proyectos de Smart Grids,» Futura Red, Enero 2018. [En línea]. Available: http://www.futured.es/smart-grids/. [Último acceso: Abril 2018].

[25] H. A., «Smart Metering Technology Promotes Energy Efficiency for a Greener World,» Analog Dialogue, 2009.

[26] M. D., «Electronico Energy Meter,» 2015. [En línea]. Available: https://dmohankumar.wordpress.com/2010/04/18/electronic-energy-meter-2/. [Último acceso: 2018].

[27] O. K. F. H. a. R. S. Longe O.M, «Wireless Sensor Networks and Advanced Metering Infrastructure Deployment in Smart Grid. Chapter of e-Infrastructure and e-Services for Developing Countries,» Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2014.

[28] Effah y Owusu, «Evolution and Efficiencies of Energy Metering Technologies in Ghana,» Global Journal of Researches in Engineering: Electrical and Electronics Engineering, 2014.

[29] Soares, «Tecnologías de Futuro para Smart Grid.,» Alcatel-Lucent, 2012.

[30] Singh y Sandula, «Minimizin Electricity Theft: A review.,» International Journal of Advance Foundation and Research in Science & Engineering, 2015.

[31] Mohassel, Fung, Mohammadi y Raahemifar, «A survey on Advanced Metering Infrastructure.,» Electrical power and Energy Systems, 2014.