Informe Técnico: Protocolo ZigBee (IEEE 802.15.4)

Javier Martín Moreno – jmartin@dtic.ua.es
Daniel Ruiz Fernández – druiz@dtic.ua.es

Junio de 2007

Índice

1 Introducción....4
1.1 Objetivo....4
1.2 Bandas de operación....4
1.3 Nodos y topología de red....5
1.4 Seguridad....8
2 Capa de Aplicación....8
2.1 Subcapa de Soporte....9
2.2 Estructura de Aplicación....9
2.2.1 Servicio de Parejas Clave-Valor....9
2.2.2 Servicio de Mensajes....9
2.3 Direccionamiento de Terminales....10
2.4 Fundamentos de comunicación de la capa de Aplicación....10
2.4.1 Perfiles....10
2.4.2 Clusters....10
2.5 Descubrimiento....10
2.5.1 Dispositivo de Descubrimiento....10
2.5.2 Servicio de Descubrimiento....11
2.6 Enlace....11
2.7 mensajes....12
2.7.1 Direccionamiento Directo....12
2.7.2 Direccionamiento Indirecto....12
2.7.3 Direccionamiento Broadcast....12
2.8 Objetos de dispositivos ZigBee....12
2.8.1 Gestión de Descubrimiento....13
2.8.2 Gestión de Enlace....13
2.8.3 Gestión de Seguridad....13
2.9 Dispositivos ZigBee....13
2.9.1 Coordinador....13
2.9.2 Router....15
2.9.3 Dispositivo Final....16
2.10 Dispositivos y Servicio de Descubrimiento....16
2.11 Dispositivos de Gestión....16
2.11.1 Gestor de Seguridad....16
2.11.2 Gestor de Enlace....17
2.11.3 Gestor de Red....17
2.11.4 Gestor de Nodos....17
3 Capa de Red....17
3.1 Descripción General....18
3.1.1 Servicio de Datos....18
3.1.2 Servicio de Control....19
3.2 Especificación del Servicio....19
3.3 Funcionalidades....20
3.3.1 Creación de una Nueva Red....20
3.3.2 Incorporación de Nuevos Dispositivos a la Red....21
3.3.3 Incorporación a una Red....22
4 Especificación de los Servicios de Seguridad....24

4.1 Arquitectura de Seguridad 24
4.1.1 Claves de Seguridad 24
4.1.2 Arquitectura de Seguridad 25
4.2 Seguridad MAC 25
4.3 Seguridad NWK (Red) 25
4.4 Seguridad en APL 26
4.4.1 Establecimiento de Clave 26
4.4.2 Transporte de Clave 27
4.4.3 Actualización de Dispositivos 27
4.4.4 Eliminación de dispositivos 27
4.4.5 Petición de Clave 27
4.5 Rol del Centro de Validación 27
5 Dispositivos ZigBee 28
5.1 Dispositivos de Bajo Nivel 28
5.2 Dispositivos de Alto Nivel 33
6 Sistema Operativo 34
7 Comparativa Bluetooth vs ZigBee 35
7.1 Sensores de control ZigBee 35
7.2 Eliminación de cables con Bluetooth 35
8 Bibliografía 36

1 Introducción

ZigBee es una nueva tecnología de inalámbrica de corto alcance y bajo consumo originaria de la antigua alianza HomeRF y que se definió como una solución inalámbrica de baja capacidad para aplicaciones en el hogar como la seguridad y la automatización.

Entre las aplicaciones que puede tener están:

- Domótica.
- Automatización industrial.
- Reconocimiento remoto.
- Juguetes interactivos.
- Medicina.
- Etc.

1.1 Objetivo

El objetivo de esta tecnología no es obtener velocidades muy altas, ya que solo puede alcanzar una tasa de 20 a 250Kbps en un rango de 10 a 75 metros, si no que es obtener sensores cuyos transceptores tengan un muy bajo consumo energético. De hecho, algunos dispositivos alimentados con dos pilas AA puedan aguantar 2 años sin el cambio de baterías. Por tanto, dichos dispositivos pasan la mayor parte del tiempo en un estado latente, es decir, durmiendo para consumir mucho menos.

1.2 Bandas de operación

ZigBee opera en las bandas libres de 2.4Ghz, 858Mhz para Europa y 915Mhz para Estados Unidos. En la siguiente figura se puede ver el espectro de ocupación en las bandas del protocolo 802 (incluyendo ZigBee).

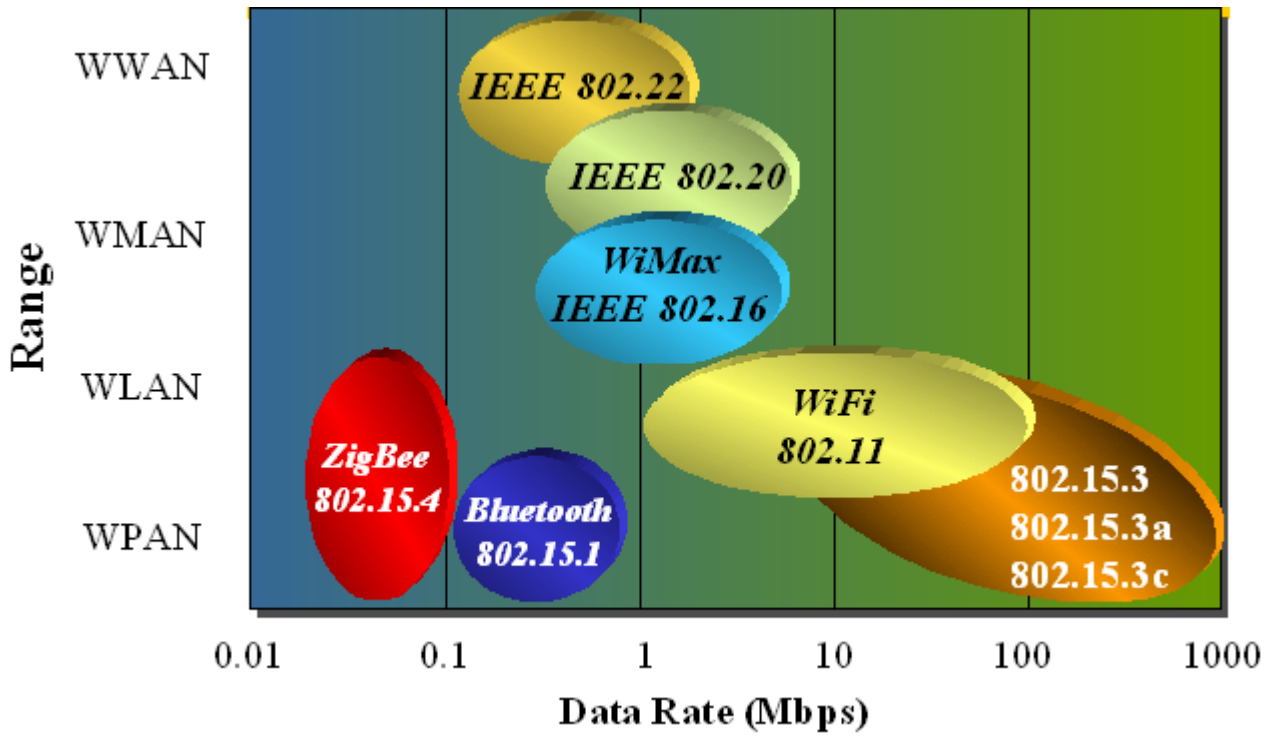

Ilustración 1. Tecnologías en 2.4GHz

En la banda de 2.4Ghz usa la modulación de espectro expandido DSSS (Direct Sequence Spread Spectrum). A una velocidad de transmisión de 250Kbps y a una potencia de 1mW cubre aproximadamente unos 13 metros de radio.

En la siguiente figura se muestran las características de radio de las señales.

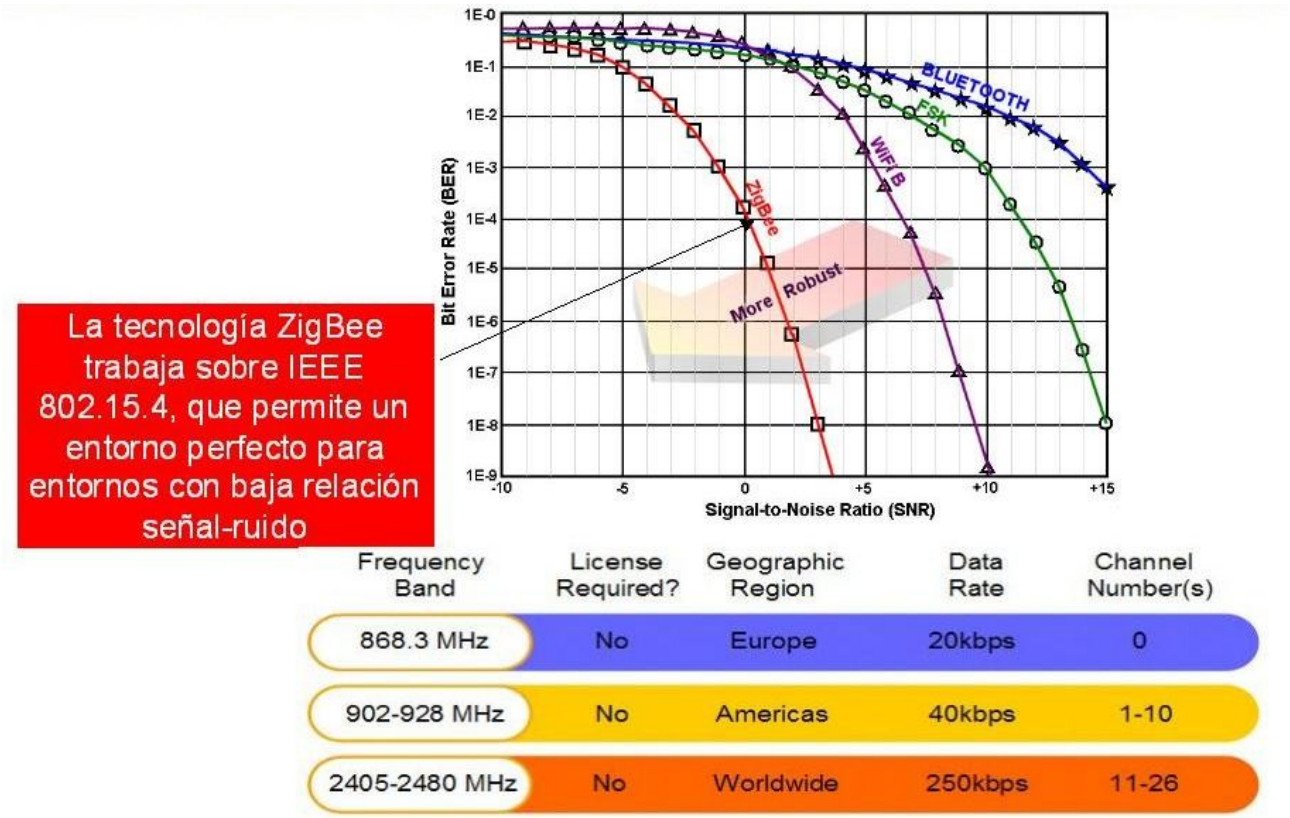

Ilustración 2. Características de radio

En la siguiente tabla se puede observar la distancia en función de la potencia transmitida y la velocidad de transmisión:

Potencia(mW) / Velocidad(Kbps)	1mW	10mW	100mW
28 Kbps	23m	54m	154m
250 Kbps	13m	29m	66m

Tabla 1. Distancia de transmisión

En cuanto a la gestión del control de acceso al medio hace uso de CSMA/CA (Carrier Sense Multiple Acces with Collision Avoidance) y es posible usar ranuras temporales TDMA (Time Division Multiple Access) para aplicaciones de baja latencia.

1.3 Nodos y topología de red

En una red ZigBee pueden haber hasta 254 nodos, no obstante, según la agrupación que se haga, se pueden crear hasta 255 conjuntos/clusters de nodos con lo cual se puede llegar ha tener 64770 nodos para lo que existe la posibilidad de utilizar varias topologías de red: en estrella, en malla o en grupos de árboles, como puede verse a continuación:

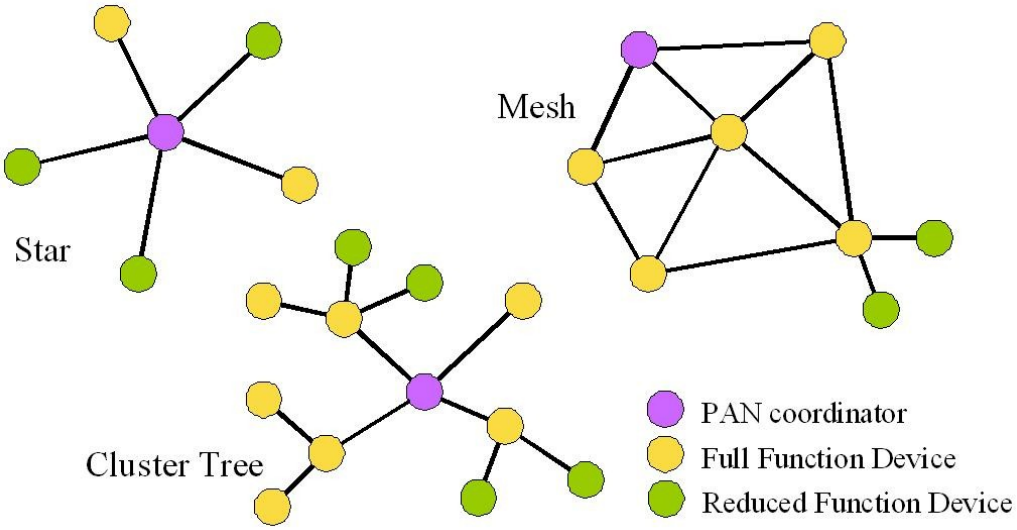

Ilustración 3. Topologías de Red

Se permite un encaminamiento o enrutamiento de saltos múltiples, también conocido como multi-hop, que permite que estas redes abarquen una gran superficie.

En ZigBee hay tres tipos de dispositivos:

- Coordinador
  - Sólo puede existir uno por red.
  - Inicia la formación de la red.
  - Es el coordinador de PAN.
- Router
  - Se asocia con el coordinador de la red o con otro router ZigBee.
  - Puede actuar como coordinador.
  - Es el encargado del enrutamiento de saltos múltiples de los mensajes.
- Dispositivo final
  - Elemento básico de la red.
  - No realiza tareas de enrutamiento.

Una posible configuración de una red sería la siguiente:

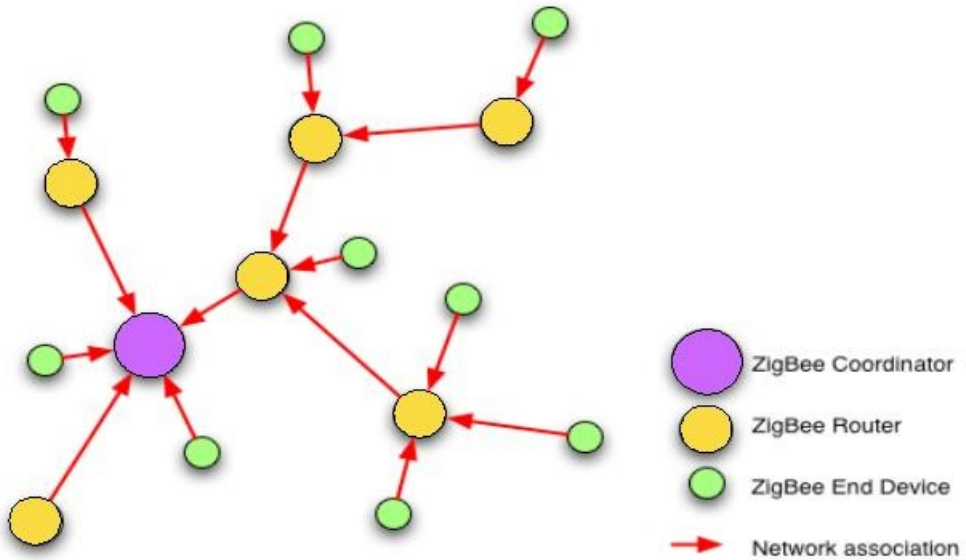

Ilustración 4. Ejemplo de red ZigBee

Otro punto importante es el soporte y la disponibilidad total de la malla, es decir, que ante caídas de nodos, la red busca caminos alternativos para el intercambio de mensajes, un ejemplo se puede ver a continuación.

Supongamos que disponemos de una red en la cual los nodos están conectados en malla y se intercambian datos entre un interruptor y una lámpara.

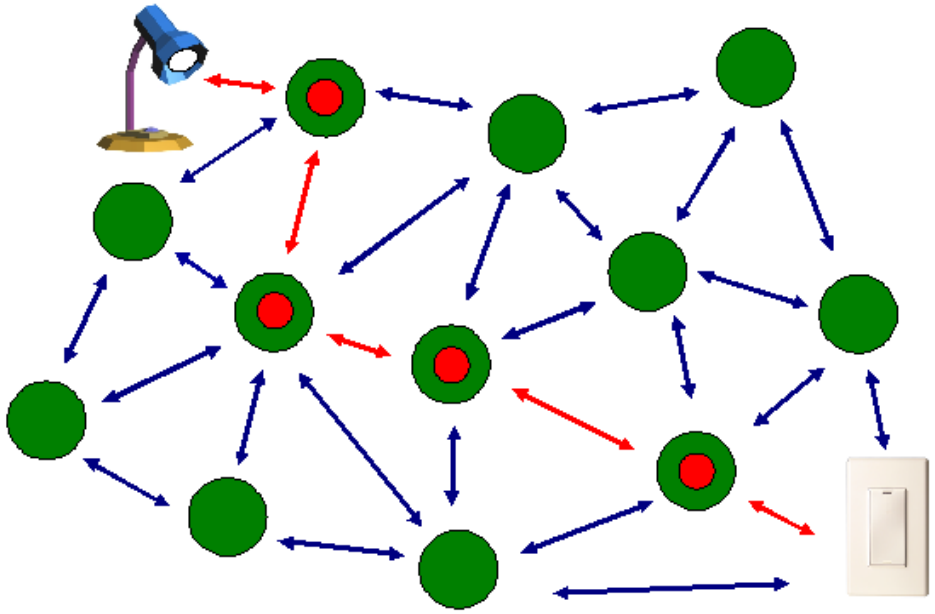

Ilustración 5. Camino de comunicación (interconexión)

Si algunos de los nodos que contiene falla y dichos nodos formaban parte del camino que seguían los mensajes en la comunicación, la red podría sufrir una caída:

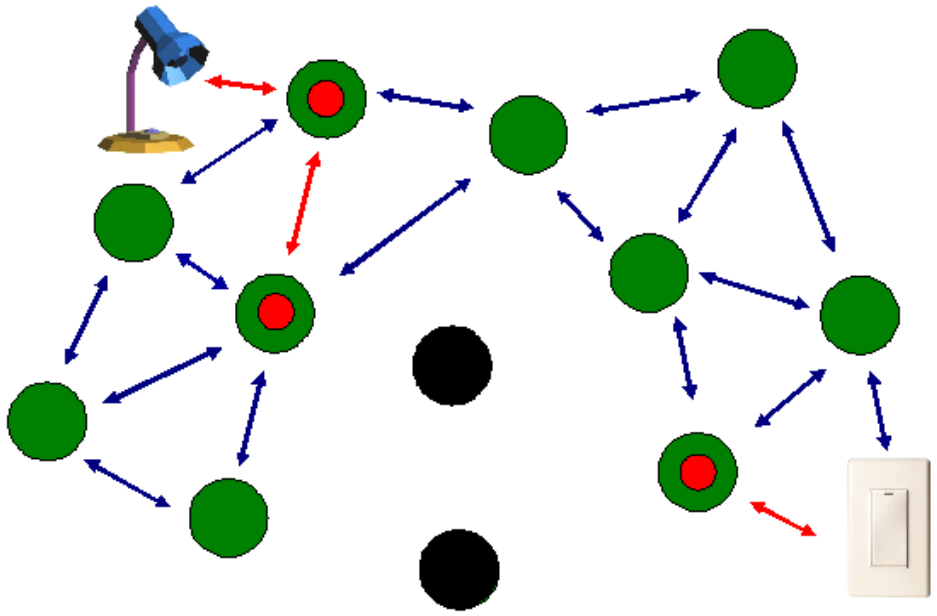

Ilustración 6. Caída de dos nodos de red

ZigBee permite que se puedan establecer rutas alternativas para seguir comunicando los dispositivos:

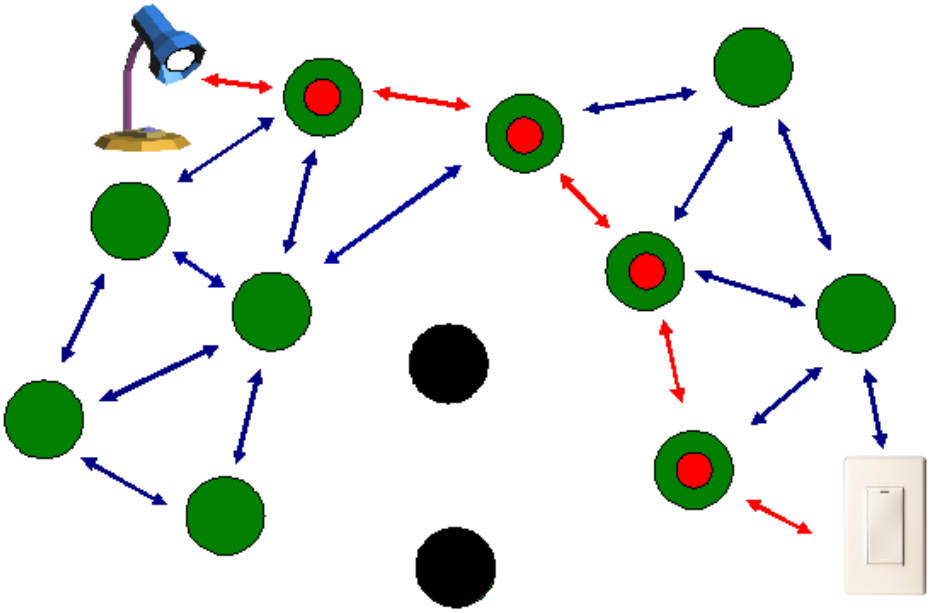

Ilustración 7. Creación de un camino alternativo

1.4 Seguridad

En cuanto a seguridad, ZigBee puede utilizar la encriptación AES de 128bits, que permite la autentificación y encriptación en las comunicaciones. Además, existe un elemento en la red llamado Trust Center (Centro de validación) que proporciona un mecanismo de seguridad en el que se utilizan dos tipos de claves de seguridad, la clave de enlace y la clave de red.

2 Capa de Aplicación

La pila de arquitectura ZigBee consta de varios componentes en capas como IEEE 802.15.4 2003 en la capa de Control de Acceso al Medio (MAC), la capa física (PHY) y la capa de red Zigbee (NWK).

La capa de aplicación de ZigBee se subdivide en la subcapa APS, la capa ZDO (Zigbee Device Objects) y los objetos de aplicación definidos por cada uno de los fabricantes.

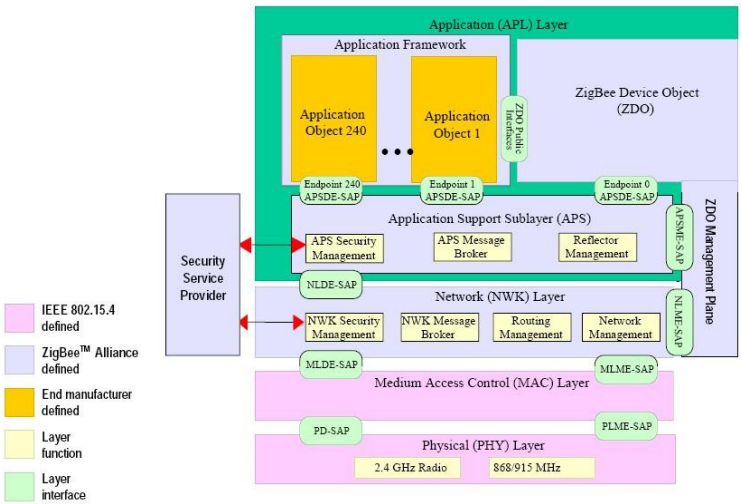

Ilustración 8. Pila de protocolo ZigBee

2.1 Subcapa de Soporte

La subcapa de soporte de aplicación (APS) proporciona un interfaz entre la capa de red (NWK) y la capa de aplicación (APL) a través de un conjunto de servicios que se utilizan junto a los ZDO y otros objetos que hayan sido definidos por los fabricantes. Los servicios los ofrecen dos entidades: la entidad de datos APS (APSD) a través del servicio de punto de acceso APSDE (APSDE-SAP) y la entidad gestora del APS (APSME-SAP) a través de un servicio que ofrece el punto de acceso APSE-SAP. APSDE proporciona el servicio necesario para la transmisión de datos y el transporte de de datos de aplicación entre dos o más dispositivos en la misma red. APSME proporciona el servicio de descubrimiento y enlace de dispositivos y mantiene una base de datos de los objetos llamado “APS Information Base (AIB)”.

2.2 Estructura de Aplicación

Dentro de la estructura de aplicación, los objetos de envían y reciben datos a través del APSDE-SAP. El control y la gestión de los objetos de aplicación es llevada a cabo por los interfaces de los ZDO.

El servicio de datos ofrecido por el APSDE-SAP, incluye primitivas de petición, confirmación, respuesta e indicación (request, confirm, response, indication) para la transferencia de datos. La primitiva *request* soporta la transferencia de datos entre pares de entidades objeto de aplicación. La primitiva *confirm* da los resultados de una llamada de la primitiva *request*. La primitiva *indication* se usa para indicar la transferencia de datos desde un APS a la entidad objeto de aplicación.

Se pueden definir mas de 240 objetos de aplicación llamados terminales, con interfaces que para cada uno de los terminales se enumeran del 1 al 240. Hay dos terminales adicionales que utiliza el APSDE-SAP; el 0 está reservado para el interfaz de datos de los ZDO y el 255 se reserva para que el interfaz de datos realice las peticiones de broadcast de datos para todos los objetos de aplicación. Los terminales que van del 241 al 254 se reservan para usos futuros.

2.2.1 Servicio de Parejas Clave-Valor

El servicio de pares key-valor (KVP) permite a los atributos definidos, que en los objetos de aplicación se puedan utilizar primitivas como *get*, *get response*, *set* y *set response*.

Además, KVP utiliza estructuras de datos de marcado XML en una versión más reducida. Esta solución proporciona un mecanismo de instrucciones y control para la gestión de pequeños dispositivos que permiten a las puertas de acceso la difusión de los datos XML.

2.2.2 Servicio de Mensajes

Existen varias áreas de aplicación en ZigBee que tiene protocolos de direccionamiento propietarios y que no funcionan bien con KVP. Por tanto, existen cabeceras que KVP asume y que sirven para controlar el estado de las variables, que permitan seleccionar, obtener o realizar las acciones necesarias que se puedan producir ante ciertos eventos que requieran los dispositivos para mantener las variables de estado de comunicación.

2.3 Direccionamiento de Terminales

ZigBee proporciona un subnivel de direccionamiento, que se usa de manera conjunta con otros mecanismos como es el protocolo IEEE802.15.4. Por ejemplo; hay un número de terminales (endpoints) que se pueden utilizar para identificar interruptores y bombillas. El terminal 0 está reservado para la gestión de dispositivos y es utiliza para direccionar los descriptores del nodo. Cada subunidad que se identifica en un nodo (como pueden ser los interruptores y las bombillas) se asigna a un terminal específico dentro del rango 1-240.

Para permitir una diferenciación de productos en el mercado, los fabricantes pueden añadir clusters que contengan atributos extra para sus propios perfiles. Estos clusters específicos no forman parte de la especificación de ZigBee y su interoperabilidad no está garantizada. Dichos servicios deben ser indicados en cada uno de los terminales descritos por parte del fabricante, acompañando a poder ser la nueva hoja de especificaciones.

2.4 Fundamentos de comunicación de la capa de Aplicación

2.4.1 Perfiles

Los perfiles son acuerdos a los que se llega por mensajes. El formato de estos mensajes y las acciones producidas, permiten a las aplicaciones residir en cada uno de los dispositivos individuales para enviar instrucciones, realizar peticiones de datos o procesar instrucciones/datos para crear así una aplicación **distribuible** e **interoperable**. Los perfiles son desarrollados por cada uno de los fabricantes ZigBee, que en base a las necesidades que existen en el mercado, proporcionan soluciones tecnológicas específicas.

Los perfiles por tanto tratan de unificar la tecnología con las necesidades del mercado.

2.4.2 Clusters

Los clusters son identificados por un identificador de cluster (Cluster ID), éste cluster se asocia al dispositivo que produce los flujos de datos. Los identificadores de clusters son únicos dentro de un mismo perfil. Los enlaces se producen por la relación existente entre identificadores de clusters de salida y de entrada, asumiendo que ambos clusters están dentro de un mismo perfil.

2.5 Descubrimiento

2.5.1 Dispositivo de Descubrimiento

El servicio de descubrimiento (Device Discovery), es el proceso por el cual un dispositivo ZigBee descubre otros dispositivos. Para ello, realiza preguntas/solicitudes que se envían por broadcast o unicast. Hay dos formas de realizar las peticiones de descubrimiento de servicios y dispositivos: la petición de dirección IEEE y la petición de dirección de NWK. La petición de IEEE es unicast y asume que la dirección NWK es conocida. La petición de dirección NWK es por broadcast y lleva la dirección de IEEE como datos de negociación de parámetros.

Las respuestas al elemento que ha realizado las peticiones broadcast o unicast de

mensajes de descubrimiento pueden variar según provengan de un tipo de dispositivos lógicos u otros, como se indica a continuación:

- **Terminal:** responde a las peticiones de descubrimiento de dispositivos enviando su propia dirección IEEE o la dirección NWK (dependiendo de la petición).
- **Coordinador:** responde a la petición enviando su dirección IEEE o NWK y las direcciones IEEE o NWK que tiene asociadas como coordinador ZigBee (dependiendo del tipo de petición).
- **Router:** responde a peticiones enviando su dirección IEEE o NWK y las direcciones IEEE o NWK de todos los dispositivos que tiene asociados como router ZigBee (dependiendo de la petición).

2.5.2 Servicio de Descubrimiento

El servicio de descubrimiento es el proceso por el cual los servicios que en un instante de tiempo están disponibles en los terminales o en los dispositivos receptores y que son descubiertos por dispositivos externos. El servicio de descubrimiento realiza las peticiones de sondeo para cada terminal de cada dispositivo o por el uso de servicios de sondeo tipo broadcast o unicast.

El proceso del servicio de descubrimiento en ZigBee es la clave para interconectar dispositivos dentro de una red. A través de dichas peticiones de los descriptores de cada nodo especificado, las peticiones por broadcast para preguntar a los dispositivos cuales son los objetos de aplicación que tienen sus dispositivos.

2.6 Enlace

En ZigBee, hay un concepto de nivel de aplicación que utiliza los identificadores de clusters en los terminales de manera individual en cada uno de los nodos. Se llama enlace a la creación de un vínculo entre los dispositivos de aplicación de la red y los terminales.

La información de cómo los clusters se emparejan con los nodos se indica en una tabla de enlace (binding table).

El enlace se lleva a cabo después de que el en enlace de comunicaciones se haya establecido. Una vez el enlace se establece es ya en la implementación en la que se decide de qué manera un nodo puede llegar a formar parte de la red o no. Además, también depende de la seguridad definida para realizar la operación y de cómo se haya implementado. El enlace sólo se permite si la implementación de la seguridad de la red de todos y cada uno de los dispositivos lo permite.

La tabla de enlace se implementa en el coordinador ZigBee. Esto es porque se necesita que la red esté continuamente operativa y disponible, con lo que es más probable que el coordinador sea el que pueda ofrecer este servicio. Por otro lado, algunas aplicaciones pueden necesitar tener esta tabla de enlace duplicada, para que esté disponible por si ocurre un fallo de almacenamiento de la tabla original. Las copias de seguridad de la tabla de enlace y/o de otros elementos de datos sobre el coordinador ZigBee ya no pertenecen a la especificación de ZigBee 1.0, por lo que es responsabilidad del software de aplicación.

2.7 mensajes

2.7.1 Direccionamiento Directo

Una vez los dispositivos se han asociado, las instrucciones entre los elementos se pueden enviar y recibir, de forma que ya pueden ser enviadas de un dispositivo a otro.

El direccionamiento directo asume que el descubrimiento del dispositivo y el servicio de descubrimiento tienen identificados un dispositivo con un terminal, el cual quiere realizar peticiones de servicios. El direccionamiento directo define una manera de realizar el direccionamiento en el que se envíen mensajes a los dispositivos incluyendo su dirección y la información de los terminales que contiene.

2.7.2 Direccionamiento Indirecto

El uso del direccionamiento directo requiere de un dispositivo controlador que tenga el conocimiento de todas las direcciones, de los terminales, de los clusters identificadores y de los atributos identificadores de un dispositivo que quiere comunicarse y que tiene su información almacenada en una tabla de enlace (binding table) en un coordinador ZigBee. Este coste de almacenamiento es mayor que el que se produce en la creación de un mensaje de direccionamiento indirecto entre pares de dispositivos. La dirección IEEE compuesta de 10bytes además de un byte adicional que se necesita son suficientes para que dispositivos sencillos como pudieran ser interruptores (switches) alimentados por baterías, se sobrecargarían al almacenar toda la información que hay en la tabla. Para estos dispositivos, el direccionamiento indirecto resulta más adecuado.

Cuando un dispositivo fuente/emisor contiene varios atributos, el identificador de cluster se utiliza para realizar el direccionamiento y los atributos identificadores se usan para identificar un atributo en particular incluido en el cluster.

2.7.3 Direccionamiento Broadcast

Una aplicación puede enviar mensajes broadcast a todos los terminales de un dispositivo dado. Este direccionamiento forma parte del direccionamiento broadcast llamado broadcast de aplicación. La dirección de destino está formada por 16 bits de la dirección broadcast de la red y hay que indicar el flag de broadcast en la trama APS dentro del campo de control. El origen debe incluir el identificador de cluster, el perfil identificador y el campo del terminal origen en la trama APS.

2.8 Objetos de dispositivos ZigBee

Los objetos de dispositivos ZigBee (ZigBee Device Objects, ZDO) representan la clase base de la funcionalidad que proporciona un interfaz entre los objetos de aplicación, el perfil del dispositivo y el APS. Los ZDO se encuentran entre el framework de aplicación y la subcapa de soporte de aplicación. Permite así que se cumplan todos los requisitos de las aplicaciones que operan con la pila de protocolo ZigBee. Los ZDO son responsables de:

- Inicializar la subcapa de soporte de aplicación (APS), la capa de aplicación (NWK), y los servicios de especificación (SSS).
- La información de configuración desde la aplicación para determinar e implementar el descubrimiento y la gestión de la seguridad, red y enlace.

Los ZDO proporcionan interfaces públicos para los objetos de aplicación en la capa del framework de aplicación para tener el control de dispositivo y realizar las funciones necesarias definidas por los objetos de aplicación. Los interfaces de los ZDO tienen poca presencia en la pila de protocolo ZigBee. En el terminal 0, a través del ADSDE-SAP para datos y a través del APSME-SAP para los mensajes de control. Los interfaces públicos proporcionan la gestión de las direcciones de dispositivos, el descubrimiento, el enlace (binding) y las funciones de seguridad incluidos en la capa del framework de aplicación de la pila de protocolo de ZigBee.

2.8.1 Gestión de Descubrimiento

El descubrimiento se gestiona dependiendo de los objetos de aplicación. Cuando se solicita, la dirección IEEE de la petición del dispositivo tiene que ser devuelta (si el dispositivo es un dispositivo final) o bien con las direcciones de los dispositivos de todas las asociaciones (si el dispositivo es un dispositivo coordinador o router). Todo esto se produce por un dispositivo que se encarga del descubrimiento de los dispositivos ZigBee.

También sirve para proporcionar otros servicios que se pueden ofrecer a los dispositivos finales (end devices) definidos en el dispositivo por los objetos de aplicación que contiene. Un dispositivo puede descubrir terminales activos, además puede descubrir servicios específicos que coincidan con un criterio dado (como pueden ser los identificadores de perfiles y de clusters).

2.8.2 Gestión de Enlace

La gestión del enlace la proporcionan los objetos de aplicación, de manera que estos objetos en cada uno de los dispositivos ZigBee puedan conectar todas las capas de la pila de protocolo a través de varias conexiones, que puedan proporcionar varios nodos en la red ZigBee. Las tablas de enlace se construyen y se publican en las peticiones de enlace y sus respuestas resultantes. Los dispositivos finales y las instrucciones tanto de enlace como de desenlace (abandono de la red) entre los dispositivos se soporta a través de los perfiles ZigBee mencionados anteriormente.

2.8.3 Gestión de Seguridad

La gestión de seguridad la proporcionan también los objetos de aplicación para habilitar o deshabilitar la parte de seguridad en el sistema. Si está habilitada, la gestión de claves se lleva a cabo haciendo el uso de lo que se conoce como claves maestras (master keys), claves de red (network keys) que permiten establecer una clave de enlace (link key).

2.9 Dispositivos ZigBee

2.9.1 Coordinador

2.9.1.1 Inicialización

Normalmente se crea una única copia de los parámetros de configuración de la red para los objetos pertenecientes a los ZDO. Además, se pueden definir parámetros para describir el Node Descriptor, Power Descriptor, Simple Descriptor, e incluso los terminales activos.

La aplicación del dispositivo realiza una petición en la lista de canales para realizar una búsqueda o escaneo de los canales indicados. La confirmación resultante obtiene una lista detallada de los PANs activos. La aplicación del dispositivo compara la lista de canales con la lista de red y selecciona uno de los canales que se encuentre libre. Una vez se identifica el canal, la aplicación del dispositivo selecciona los atributos de seguridad de la capa y trama correspondientes a los parámetros de configuración. Después la aplicación chequea si se ha podido establecer el PAN en el canal.

2.9.1.2 Operación Normal

En este estado, el coordinador ZigBee debe permitir que otros dispositivos se unan a la red basándose en sus parámetros de configuración; como pudieran ser la duración de la incorporación del dispositivo a la red o el número máximo de elementos que se pueden unir.

El coordinador ZigBee debe responder a cualquier dispositivo u operaciones del servicio de descubrimiento de su propio dispositivo o de cualquier dispositivo que tenga asociado y que esté dormido. La aplicación del dispositivo debe asegurarse de que el número de entradas de enlace no excede de los indicados en los parámetros de configuración. Por tanto, el coordinador ZigBee tiene que soportar el control del proceso de incorporación a la red de cualquier dispositivo.

El coordinador tiene que mantener una lista de los dispositivos asociados y facilitar el soporte para elementos huérfanos, permitiendo que se vuelvan a unir a la red, permitiendo que los dispositivos se incorporen directamente en la red.

Por otro lado, el coordinador ZigBee debe soportar primitivas que permitan eliminar o desasociar los dispositivos que estén bajo su control. El coordinador procesa las peticiones de solicitud del router o de los dispositivos finales. Una vez recibida la solicitud de desconexión el coordinador espera un tiempo para recibir una segunda petición de desconexión. Si le llega en un tiempo determinado, el coordinador ZigBee pasará a examinar el identificador del perfil (Profile ID) para ver si coincide. Si coincide, lo incluye en una lista llamada AppOutClusterList para que deje de pertenecer a la red. Si no coincide se enviará un error al dispositivo que solicita la desconexión, es decir, el dispositivo seguirá perteneciendo a la red.

2.9.1.3 Operación del Centro de Validación

El coordinador ZigBee tiene la función de ser el Centro de Validación (Trust Center) cuando la seguridad está habilitada en la red. Al centro de validación se le notifica si existen nuevos dispositivos en la red por medio del APSME. El centro de validación puede permitir que el dispositivo permanezca en la red o bien se le fuerce a salir de ella.

Si el centro de validación decide permitir que el dispositivo permanezca en la red, debe establecer una clave maestra con el dispositivo a no ser que ya exista una clave maestra previa entre ellos. Una vez intercambiada dicha clave, el centro de validación y el dispositivo ahora negociarán una clave para establecer la conexión.

El centro de validacíon entonces proporciona al dispositivo la clave de red (NWK) para que el dispositivo pueda establecer peticiones al coordinador.

2.9.2 Router

2.9.2.1 Inicialización

Por regla general se crea una única copia de los parámetros de configuración de la red para los objetos pertenecientes a ZDO.

Si se puede, se crean los elementos de configuración para el Complex Descriptor, el User Descriptor, el número máximo de entradas de enlace y la clave maestra.

La aplicación del dispositivo utiliza el ChannelList y sus parámetros de configuración para buscar o escanear los canales que se le indiquen. El resultado permite obtener la lista de red con los PAN activos en la red. Entonces se realizan varias peticiones de descubrimiento para obtener cuales son realmente los elementos que existen en la red y asociar los enlace en la capa de red. La aplicación del dispositivo compara el ChannelList con la NetworkList para seleccionar los PAN existentes que se deben unir. Una vez que el PAN al que unirse se ha identificado, la aplicación del dispositivo debe realizar una petición para asociar el PAN en el canal. Después debe chequear el estado de verificación de la asociación en el coordinador u otros routers seleccionados en ese PAN.

Si la red tiene la seguridad activada, el dispositivo tiene que esperar a que el centro de validación le proporcione la clave maestra y establecer con éste la clave de enlace. Una vez establecido espera a que el centro de validación de pase la clave de red. Ahora ya que está autenticado puede funcionar como un router de la red.

2.9.2.2 Operación Normal

En este estado, el router debe permitir que otros dispositivos se unan a la red basándose en los parámetros de configuración que tiene, como el número de elementos máximos o el tiempo en el que puede estar un elemento en la red. Cuando un dispositivo nuevo se une a la red, la aplicación del dispositivo debe ser informada. Cuando se haya admitido en el PAN, el router debe indicarle la confirmación de la conexión. Si la seguridad está habilitada, el dispositivo debe informar al centro de validación.

El router ZigBee debe responder a cualquier dispositivo descubierto o a operaciones del servicio de descubrimiento, tanto de su propio dispositivo como de cualquier otro asociado que pudiera estar dormido.

Si la seguridad está activada, el router debe utilizar la clave maestra para establecer los procedimientos para la gestión de la clave de enlace (Link Keys). El router debe soportar el establecimiento de una clave maestra con el dispositivo remoto y establecer entonces la clave de enlace. El router tiene que poder almacenar y eliminar las claves de enlace para destinos conocidos que requieran que la comunicación sea segura con lo que debe poder recibir las claves del centro de validación.

El router debe permitir también la eliminación de la red de dispositivos asociados bajo su control de aplicación.

El router mantiene una lista con los dispositivos asociados y tiene que facilitar el soporte para que los procesos de de búsqueda e incorporación de elementos huérfanos de los dispositivos que previamente han estado asociados, puedan volver a unirse a la red.

2.9.3 Dispositivo Final

2.9.3.1 Inicialización

La aplicación del dispositivo debe obtener de la lista de canales la configuración para escanear los canales especificados. El resultado debe contener una lista de red (Network List) detallando los PAN activos en la red. Al igual que el router, se realizan varias peticiones de descubrimiento para saber cuantos elementos son los que hay en la red. La aplicación del dispositivo debe comparar la lista de canales con la lista de red para deducir a qué red debe unirse. En el algoritmo debe indicarse entre otras cosas: el modo de operación de la red, identificación del router o coordinador de la red, capacidad del router o coordinador, coste de enrutamiento, etc. Una vez hecho, debe chequear la asociación con el router o el coordinador ZigBee en el PAN.

Si la red tiene la seguridad habilitada, el dispositivo tiene que esperar a que el centro de validación negocie primero la clave maestra, seguido de la clave de enlace y finalmente la clave de red (NWK), tras lo que se considerará que estará autenticado y listo para unirse a la red.

2.9.3.2 Operación Normal

El dispositivo final ZigBee debe responder a cualquier dispositivo descubierto o a las peticiones de operación del servicio de descubrimiento de su propio dispositivo.

Si la seguridad está habilitada, igual que en el apartado anterior, debe negociar primero la clave maestra y seguidamente la clave de enlace, con lo que tiene que poder almacenar también las claves de enlace de los destinos que requieran una comunicación segura. Debe poder gestionar estas claves, tanto para almacenar como para eliminar. Por tanto tiene que poder mantener una comunicación con el centro de validación para actualizar las claves de red (NWK key).

2.10 Dispositivos y Servicio de Descubrimiento

El dispositivo y las funciones del servicio de descubrimiento soportan:

- El dispositivo de descubrimiento.
- El servicio de descubrimiento.

2.11 Dispositivos de Gestión

2.11.1 Gestor de Seguridad

El gestor de seguridad determina que seguridad está habilitada o deshabilitada. Si está habilitada debe permitir:

- Establecer una clave.
- Transportar la clave.
- Autenticación.

2.11.2 Gestor de Enlace

La función de gestión del enlace soporta:

- El enlace de los dispositivos finales.
- El enlace y desenlace.

2.11.3 Gestor de Red

La función del gestor de la red debe soportar:

- El descubrimiento de la red.
- La formación de la red.
- Permitir y denegar asociaciones.
- Asociaciones y desasociaciones.
- Descubrimiento de rutas.
- Reseteo de la red.
- Habilitación e Inhabilitación del estado del receptor de radio.

2.11.4 Gestor de Nodos

El gestor de nodos soporta la petición y respuesta de la funciones de gestión. Esta funciones de gestión solo proporcionan visibilidad a dispositivo externos en cuanto al estado del dispositivo receptor de la petición.

3 Capa de Red

Las primitivas de confirmación de la capa de red, suelen incluir parámetros encargados de informar acerca del estado de las solicitudes que genera la capa inmediatamente superior, la capa de aplicación. Estos parámetros son los que aparecen en la siguiente tabla.

Nombre	Valor	Descripción
SUCCESS	0x00	La solicitud ha finalizado correctamente.
INVALID_PARAMETER	0xc1	Parámetro inválido.
INVALID_REQUEST	0xc2	La solicitud se deniega en función del estado actual de la capa de red.
NOT_PERMITED	0xc3	Solicitud no permitida.
STARTUP_FAILURE	0xc4	Fallo en la inicialización de la red.
ALREADY_PRESENT	0xc5	Indica que un dispositivo que ya existe en la red, dispone de la dirección que se pretende obtener.
SYNC_FAILURE	0xc6	Fallo de sincronización (problema con la MAC).
TABLE_FULL	0xc7	Indica que no dispone de más espacio para almacenar direcciones de dispositivos en la tabla de encaminamiento.
UNKNOWN_DEVICE	0xc8	Error porque el dispositivo indicado no aparece en la tabla de encaminamiento del dispositivo.
UNSUPPORTED_ATTRIBUTE	0xc9	Identificador de atributo no soportado o reconocido.

Nombre	Valor	Descripción
NO_NETWORKS	0xca	Fallo provocado por la inexistencia de redes disponibles.
LEAVE_UNCONFIRMED	0xcb	Fallo en el descubrimiento del propio dispositivo al resto de la red.
MAX_FRM_CNTR	0xcc	Proceso de Seguridad. Trama fuera de rango
NO_KEY	0xcd	Proceso de Seguridad. La solicitud carece de llave de paso.
BAD_CCM_OUTPUT	0xce	Proceso de Seguridad. El sistema de seguridad ha producido errores en su salida.

Tabla 2. Primitivas de Confirmación

3.1 Descripción General

La capa de red es necesaria para ofrecer servicios a la capa inmediatemente superior, la capa de Aplicación, que permitan realizar operaciones sobre la capa inmediatamente inferior a la misma, la sub-capa de MAC, definida en el IEEE 802.15.4-2003. Es decir, la capa de red hace de interfaz entre la capa de Aplicación y la de MAC. Para esto, la capa de red dispone en esta interfaz de dos servicios, con los que cubre las necesidades de la capa de Aplicación. Estos dos servicios se conocen como Servicio de Datos y Servicio de Control.

La comunicación entre la capa de Aplicación y la sub-capa MAC, se lleva a cabo en el SAP de la capa de Red. Unilizando las interfaces descritas anteriormente. Esto se traduce de forma que, entre la capa de Aplicación y la de Red existen dos SAP ,uno por cada servicio que la capa de Red oferta a la de Aplicación. De la misma forma que aparecen otros dos SAP más entre la capa de Red y la sub-capa de MAC.

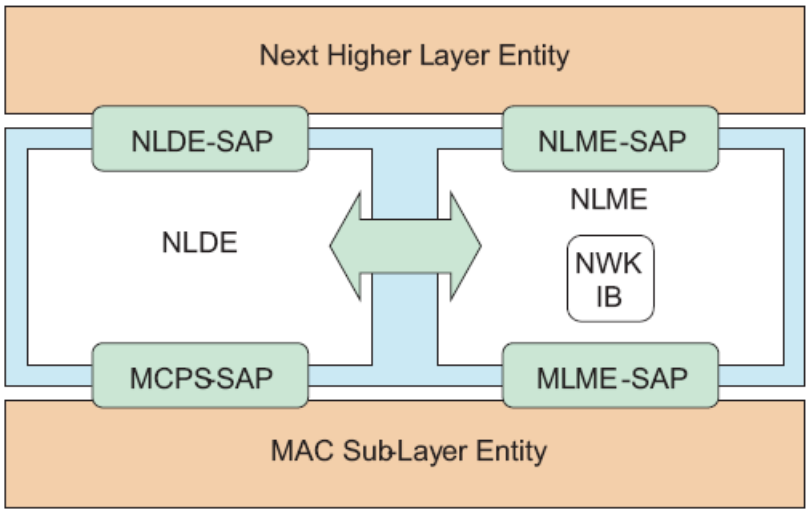

Ilustración 9. Capa de Red

3.1.1 Servicio de Datos

Este servicio de interfaz, es también conocido con NLDE (Network Layer Data Entity). Provee de un servicio de datos, que permite a cualquier aplicación comunicarse con las mismas unidades de datos, con dos o más dispositivos. Obviamente todos los dispositivos

que intervengan en esta comunicación deberán estar en la misma red de interconexión.

Esta interfaz dispone de los siguientes servicios:
- Generación de la PDU de la capa de Red (NPDU).
- Especificación de la topología de encaminamiento.

3.1.2 Servicio de Control

El también conocido como NLME (Network Layer Management Entity), es un servicio ofertado desde la capa de Red a la superior, que permite a la capa de Aplicación interactuar o comunicarse con la pila directamente.

Esta interfaz dispone de los siguientes servicios:
- Configuración de un nuevo dispositivo. Esto permitirá la incialización de un dispositivo Coordinador, así como el descubrimiento de nuevos dispositivos dentro de la red de interconexión.
- Inicialización de una nueva red.
- Integración y salida de una red.
- Direccionamiento.
- Descubrimiento de vecinos.
- Descubrimiento de ruta.
- Recepción de control.

3.2 Especificación del Servicio

Además de la posibilidad de comunicación entre la capa de Aplicación y la de Red, la capa de Red de ZigBee dispone de un canal de comunicación directa entre los servicios de la misma capa. Es decir, dispone de una interfaz para comunicar los servicios intermedios de Datos y de Control. Mediante esta nueva interfaz, el servicio de Control podrá utilizar los servicios de su capa contigua, la de Datos.

Dentro de cada uno de los servicios de la capa de Red, en las interfaces de comunicación, se definen las primitivas de comunicación entre las capas de Aplicación y de MAC. De la misma forma que sucede en la comunicación entre los servicios de la propia capa. Estas primitivas son las siguientes:
- **Formación de Red.** Las primitivas que aquí se engloban, definen como la capa superior de un dispositivo ZigBee puede inicializarse a si mismo como dispositivo coordinador de una nueva red.
- **Admisión de Dispositivos.** Grupo de primitivas que permiten tanto a un dispositivo coordinador como a un router la posibilidad de incorporar dispositivos a su red, mediante descubrimiento de los mismos.
- **Conversión a Router.** Estas primitivas son las que utiliza un dispositivo ZigBee tipo router, tras haber sido admitido en una nueva red, para ejercer como router en la misma, reconfigurando su trama para esto.
- **Incorporación a una Red.** Se trata de una serie de primitivas utilizadas para la incorporación de dispositivos a una red ZigBee. Dentro se clasifican en tres grupos.
  - **Incorporación a una red por asociación.** Cuando un dispositivo pretende entrar a formar parte de la red del vecino más cercano que ha encontrado.
  - **Incorporación a una red directamente.**
  - **Reincorporación a una red.** Esto sucede en el caso de que un dispositivo se despierte y no sea capaz de encontrar su red.

- **Incorporación directa de Dispositivos.** Se trata de una serie de primitivas que permiten tanto a los routers como coordinadores de una red ZigBee la incorporación directa de un dispositivo a su red, sin necesidad de que este dispositivo lo solicite.
- **Abandonar una Red.** Grupo de primitivas utilizadas por los dispositivos para abandonar la red a la que pertenecen. También pueden ser utilizadas por otros dispositivos vecinos para informar al coordinador o router de que algún dispositivo pretende abandonar la red. Así mismo estas primitivas las utilizan los coordinadores para notivicar al dispositivo en cuestión, que ha abandonado correctamente la red.
- **Reseteo de Dispositivos.** Primitivas utilizadas para que los dispositivos puedan resetear su capa de red.
- **Sincronización.** Juego de primitivas que los dispositivos utilizan para sincronizar su comunicación con los dispositivos coordinadores o routers.
- **Mantenimiento de la capa de Red.** Este último grupo de primitivas es utilizada por la capa superior de los dispositivos para leer y escribir en la base de información de la capa de red.

3.3 Funcionalidades

Todos los dispositivos ZigBee disponen de dos funcionalidades:

- Incorporación a una Red.
- Abandonar una red.

Además de estas funcionalidades, los dispositivos Coordinadores y Routers disponen de una serie de funcionalidades adicionales:

- Permitir a otros dispositivos incorporarse a la red. De dos formas distintas:
  - Por indcaciones de la sub-capa de MAC.
  - Por solicitud de incorporación desde la capa de Aplicación.
- Permitir a los dispositivos miembros de la red abandonarla. De la misma forma que sucedía en el caso anterior, dispone de dos posibilidades:
  - Por indcaciones de la sub-capa de MAC.
  - Por solicitud de incorporación desde la capa de Aplicación.
- Asignación de direcciones de red lógicas.
- Mantenimiento de una tabla o lista de dispositivos cercanos o vecinos.

Por último, los dispositivos Coordinadores, disponen de una funcionalidad particular. Esta es la que les permite crear o establecer nuevas redes de datos entre dispositivos.

3.3.1 Creación de una Nueva Red

Este procedimiento sólo puede ser iniciado por dispositivos Coordinadores, que no se encuentren ya dentro de una red ZigBee. Es decir, un coordinador, sólo puede aparecer en una red. Pero en el caso de que cualquier otro tipo de dispositivo o de que un Coordinador asociado ya a una red, iniciase este procedimiento sería denegado por la capa de Red.

Una vez iniciado el procedimiento, desde el interfaz de control de Red, se comunica con la subcapa de MAC para comprobar si existen posibles interferencias (otros coordinadores haciendo la misma operación por ejemplo). Esta comprobación se hace utilizando varios canales, hasta que se encuentra uno disponible, el cuál es reservado para la nueva red.

En caso de que no se encuentre ningún canal disponible, se notificará a la capa superior y se abandonará el proceso de establecimiento de la red.

Una vez encontrado un canal disponible, este es ocupado y se le asigna un nombre a la subred a partir del ID del PAN. El cuál obviamente no puede ser el de broadcast. Este parámetro es elegido aleatoriamente y siempre dejando 16bits disponibles, reservados para futuras ampliaciones de la red. Al finalizar esta secuencia, el nuevo ID es comunicado a la subcapa inferior (MAC).

Entonces, y sino aparecen conflictos con el ID del PAN, se escoge y establece la nueva dirección de red. Hecho esto, se notifica que el proceso ha finalizado correctamente y se inicializan los parámetros del coordinador en base a los parámetros de identificación obtenidos.

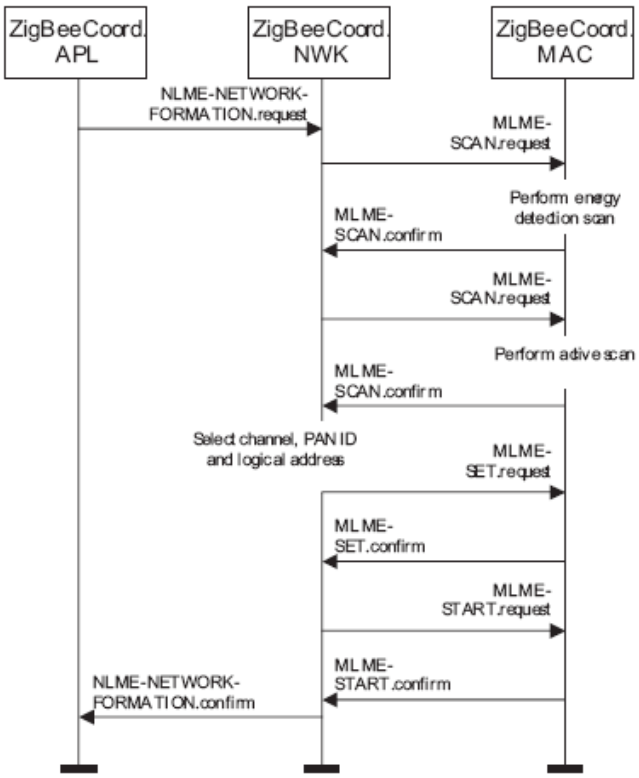

Ilustración 10. Creación de una Nueva Red

A continuación se muestra todo este proceso, en un diagrama de comunicación, en el que se puede apreciar además las primitivas utilizadas en todo el proceso.

3.3.2 Incorporación de Nuevos Dispositivos a la Red

Este procedimiento sólo puede ser iniciado por dispositivos ZigBee que sean Coordinador o Router. En caso de que otro dispositivo iniciase este proceso, sería cancelado por el Servicio de Control de la capa de Red.

Entonces se habilita el parámetro *PermitDuration* y la sub-capa de MAC se configura para permitir la asociación con nuevas direcciones MAC.

Desde este momento, el dispositivo está esperando que nuevos dispositivos acepten su oferta para formar parte de la red. Este proceso no tiene una duración determinada, sólo

finalizará en el caso de que aparezca otra orden o primitiva que la anule.

A continuación se muestra todo este proceso, en un diagrama de comunicación, en el que se puede apreciar además las primitivas utilizadas en todo el proceso.

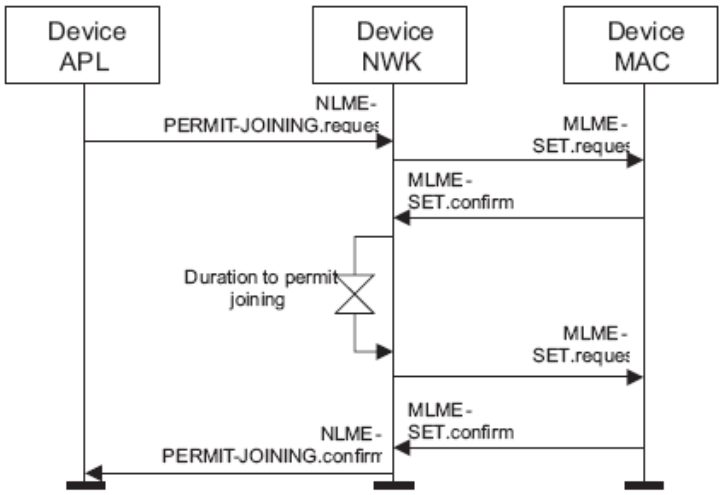

Ilustración 11. Incorporación de Nuevos Dispositivos a la Red

3.3.3 Incorporación a una Red

En este momento aparece la diferenciación entre *padre* e *hijo*. Llamaremos padre al dispositivo que permite que otros dispositivos se conecten a su red, es decir, se tratará de un dispositivo Coordinador o en su defecto un Router. Mientras que el hijo pasará a ser el nuevo dispositivo que pretende formar parte de la red.

La incorporación a una nueva red, puede hacerse de dos formas distintas.

- Por asociación.
- Directamente.

También hay que tener en cuenta que un dispositivo puede reincorporarse a una red. Bien por haber estado dormido durante un largo periodo de tiempo o bien porque ha perdido su red y busca una nueva.

3.3.3.1 Incorporación a una Red por Asociación

Para la incorporación de un dispositivo a una red por asociación, aparecen dos procesos distintos, pero paralelos. Estos son los procesos correspondientes al padre y al hijo.

3.3.3.1.1 Procedimiento del Hijo

El procedimiento empieza cuando el dispositivo escanea desde la sub-capa de MAC los canales disponibles. Es decir, en este caso el dispositivo estará buscando canales en los que haya algún tipo de tráfico. Este proceso de escaneo por canales tendrá una duración determinada por canal, al contrario que sucedía en el caso anterior.

Una vez escogido el canal, se procesan las tramas encontradas en el mismo, en busca de alguna cuya longitud sea distinta de cero. Entonces el dispositivo comprueba si la comunicación efectivamente es entre dispositivos de tecnloogía ZigBee. De ser así localiza el identificador de la red.

A continuación, toda esta información es procesada por el dispositivo, el número de redes que ha encontrado, dispositivos cercanos, etc. Buscando, en cuál de todas las redes localizadas se le permite la incorporación. Pasando a trabajar con el identificador de dicha red.

En este momento, el dispositivo, también puede decidir desechar las redes encontradas y volver a analizar los canales de comunicación en busca de otras que cumplan sus necesidades.

Si el dispositivo es un Router, deberá indicarlo en su siguiente comunicación, en la que intentará finalmente incorporarse a la red.

Acto seguido, el dispositivo hace una lista individual de los dispositivos cercanos a él (vecinos). Para comprobar la distancia a la que se encuentra del padre. Si este es muy distante, podría acceder a través de la asociación con otros dispositivos, sólo si el coste de esta asociación no supera una distancia de tres dispositivos asociados. En caso de que esta condición no se cumpla, el proceso se anulará nuevamente.

En caso de encontrar un vecino, que cumpla las condiciones, la capa de MAC se habilita de forma que solicite una dirección de red. Este proceso puede fallar, por diversas causas, como que el dispositivo elegido desaparezca de la red. Si esto ocurriese el proceso sería anulado y se volvería a empezar.

Si el proceso se completa satisfactoriamente, es decir, el dispositivo es aceptado en la red. Le es asignada una dirección de red de 16bits única en toda la red. Además se actualiza la tabla de dispositivos de su vecino, para que sepa que ese dispositivo ya forma parte de la red y que accederá a la misma a través de él.

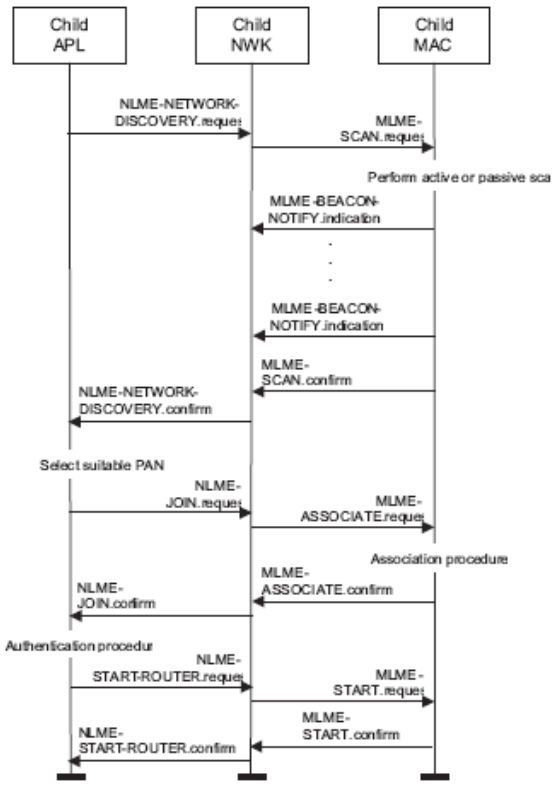

Ilustración 12. Incorporación a una red por Asociación (Hijo)

3.3.3.1.2 Procedimiento del Padre

Este procedimiento es iniciado por la llegada de una solicitud de incorporación a la subcapa de MAC del dispositivo. Los dispositivos que pueden aceptar estos mensajes y permitir la incorporación a la red son sólo los Coordinadores y Routers. En caso de que otro dispositivo intente aceptar estos mensajes al capa de red los eliminará.

A continuación, el dispositivo comprueba por qué un dispositivo que ya es de su red, solicita su incorporación. Tras esto comprueba que lo que pretende el dispositivo es informar del descubrimiento de un nuevo dispositivo en la red cercano a si mismo. Entonces se asigna a este nuevo dispositivo su dirección lógica y única de red.

Aunque también puede darse el caso de que el dispositivo padre no disponga de espacio de memoria física para recordar a este nuevo dispositivo. Caso en el que la incorporación no podrá ser llevada a cabo y por lo tanto el proceso será anulado.

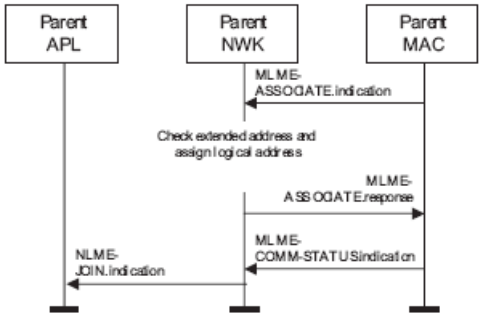

Ilustración 13. Incorporación a una red por Asociación (Padre)

3.3.3.2 Incorporación a una red Directamente

En este caso el proceso de incorporación a una red es mucho más sencillo. Ya que la comunicación es directa entre padre e hijo, sin utilizar intermediarios.

El hijo, una vez encontrada una red en la que un dispositivo Controlador o Router se encuentra próximo. Se le envía la petición de unión a la red. Si el dispositivo padre dispone de memoria física suficiente para almacenar la nueva dirección de este dispositivo. Genera una nueva dirección lógica de red, se la envía al nuevo dispositivo hijo y la almacena en su tabla en encaminamiento.

4 Especificación de los Servicios de Seguridad

4.1 Arquitectura de Seguridad

4.1.1 Claves de Seguridad

La seguridad en una red de dispositivos ZigBee se basa en claves de enlace y de red. En una comunicación por unicast entre pares de entidades APL la seguridad se basa en claves de 128bits entre los dos dispositivos. Por otro lado, la comunicación existente cuando es por broadcast, también las claves para la seguridad se establecen de 128bits entre todos los dispositivos de la red.

Un dispositivo adquiere la clave de enlace mediante el transporte de clave, establecimiento de clave o dada en la preinstalación desde el fabricante. Por otro lado,

para el establecimiento de la clave de red hay dos maneras: el transporte de clave y la preinstalación. Como se ha mostrado en apartados anteriores el establecimiento de clave se obteniendo previamente una clave de enlace basándose en una clave maestra. Esta clave maestra puede ser obtenida por el transporte de dicha clave o en fábrica.

La clave de red tiene que ser usada por las capas MAC, NWK y APL de ZigBee. Las claves maestras y las de enlace solo pueden ser usadas en la subcapa APS, de hecho, las claves maestras y de enlace deben estar disponibles solo en la capa APL.

4.1.2 Arquitectura de Seguridad

Las aplicaciones ZigBee se comunican usando el estandar de wireless IEEE 802.15.4 que especifica que hay dos capas, la capa física (PHY) y la capa de control de acceso al medio (MAC). ZigBee construye en estas capas una capa de red (NWK) y otra de aplicación (APL). La capa de MAC proporciona servicios de que permiten la fiabilidad y la comunicación directa entre dispositivos. La capa de red (NWK) proporciona enrutado y funciones de multi-hop que se puedan necesitar para crear cada una de las topologías que se necesiten como la de estrella, malla, árbol, etc. La capa APL incluye la subcapa de soporte de aplicación (APS), los ZDO y las aplicaciones. El ZDO es responsable de toda la gestión de dispositivos mientras que la capa APS proporciona el servicio necesario para los ZDO y las aplicaciones ZigBee.

4.2 Seguridad MAC

Cuando una trama en la capa MAC tiene que ser asegurada, ZigBee tiene que usar la capa de seguridad que se indica en la especificación 802.15.4.

La capa MAC se encarga de su propio proceso de seguridad aunque sean las capas superiores las encargadas de determinar el nivel de seguridad a usar. La siguiente figura muestra un ejemplo de los campos de seguridad que tienen que ser incluidos en las tramas en las que se indica que tiene que existir seguridad a nivel de MAC.

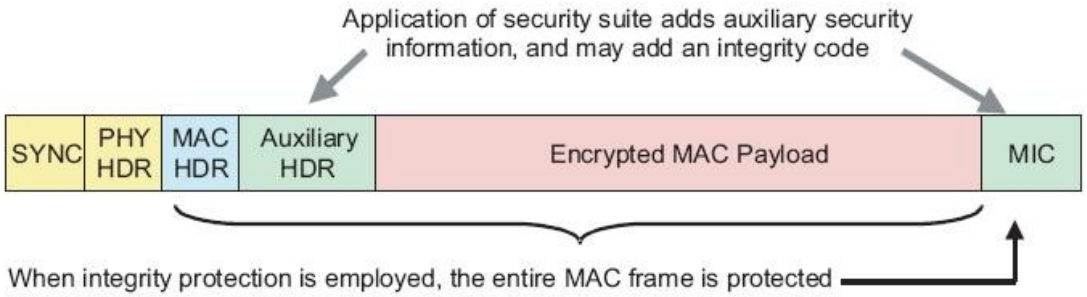

Ilustración 14. Seguridad en MAC

4.3 Seguridad NWK (Red)

Cuando una trama en la capa de red necesita ser asegurada, ZigBee debe usar ciertos mecanismos de protección de los datos. Al igual que la capa MAC, el mecanismo de protección de trama en la capa de red NWK usa de la encriptación *Advanced Encription Standard*, es decir, AES. Sin embargo son las capas superiores las que deben indicar el nivel de seguridad que se tiene que aplicar.

Una responsabilidad de la capa de red (NWK) es enrutar los mensajes sobre enlace multi-hop. La capa de red tiene que enviar como broadcast sus peticiones de enrutado y recibir las respuestas. Se realiza de manera simultánea el enrutamiento de los mensajes de peticiones que se envían a los dispositivos cercanos y los que se reciben de ellos. Si la clave de enlace apropiada se indica, la capa de red usa esta clave de enlace para asegurar sus tramas de red. Si por el contrario no se indica, para poder asegurar los mensajes de la capa de red usa su propia clave de red para asegurar las tramas de red. Por tanto en el formato de la trama se indica de manera explícita la clave que se ha usado para protegerla.

La siguiente figura muestra los campos que se deben incluir en una trama de red.

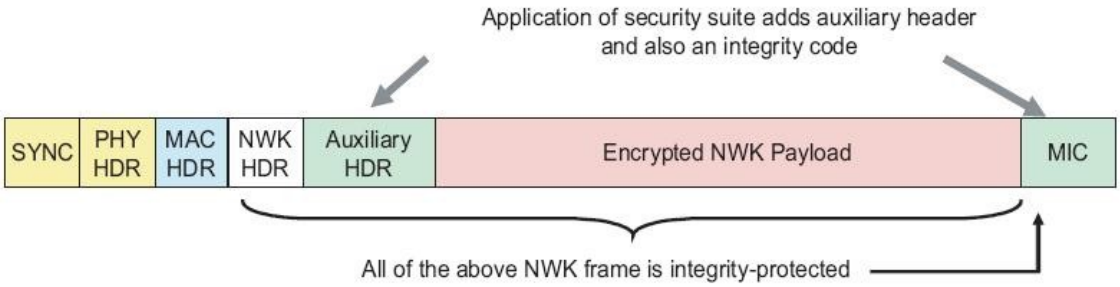

Ilustración 15. Seguridad en NWK

4.4 Seguridad en APL

Cuando una trama en la capa APL necesita ser asegurada, la subcapa APS es la encargada de gestionar dicha seguridad. La capa APS permite que la seguridad de trama se base en las claves de enlace y de red (Link y Network Keys) como se ha visto en apartados anteriores. La siguiente figura muestra los campos para proporcionar seguridad en una trama del nivel APL.

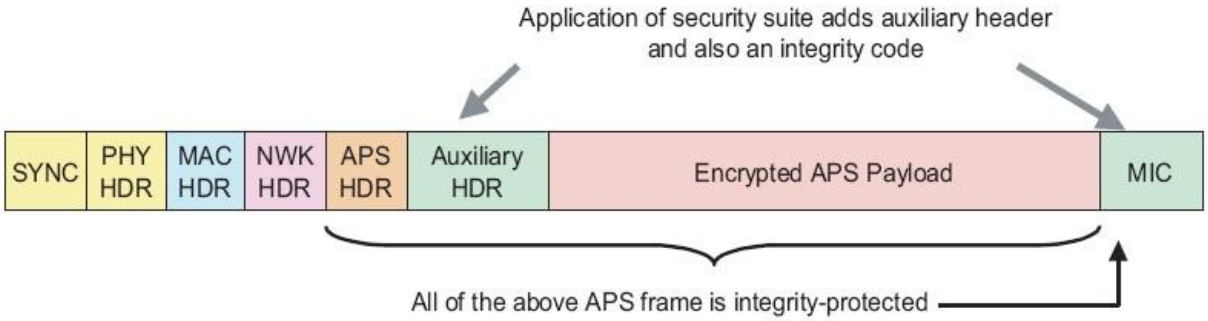

Ilustración 16. Seguridad en APL

4.4.1 Establecimiento de Clave

Los servicios de establecimiento de clave en la subcapa APS proporcionan el mecanismo por el cual un dispositivo ZigBee puede obtener una clave secreta compartida (la clave de enlace) con otro dispositivo ZigBee. En establecimiento de clave existen dos elementos: el que inicia la comunicación y el que responde, que normalmente es el que le dará la validación. La información de validación, es decir, la clave maestra da paso a que el elemento iniciador pueda establecer una clave de enlace.

En el establecimiento del protocolo de clave simétrica *Symmetric-Key Key Establishment* (SKKE), el dispositivo iniciador establece una clave de enlace con el receptor usando la clave maestra. Esta clave maestra, puede venir dada de fábrica o que se implemente desde el centro de validación, que puede ser un tercer elemento o bien puede venir dada como datos introducidos por usuario.

4.4.2 Transporte de Clave

El servicio de transporte de clave proporciona tanto la posibilidad de transportar la clave de manera segura y no segura de un dispositivo a otros. La instrucción o comando de transportar clave segura significa transportar las claves maestras, de enlace, de red desde el centro de validación a los dispositivos. Este comando no protege con criptografía la clave que tiene que ser cargada.

4.4.3 Actualización de Dispositivos

El servicio de actualización de dispositivos proporciona una forma segura para que un dispositivo, como un router, informe a otro dispositivo, como el centro de validación, que existe un tercer dispositivo que ha cambiado su estado y que por tanto hay que actualizarlo, como pudiera ser la inclusión o eliminación de un dispositivo en la red. De esta manera el centro de validación mantiene una lista precisa de los dispositivos activos en la red.

4.4.4 Eliminación de dispositivos

El servicio de eliminación de dispositivos proporciona una forma segura por la cual un dispositivo como el centro de validación puede informar a otros, como son los routers de que uno de sus hijos tiene que ser eliminado de la red. De esta manera se puede eliminar un dispositivo de la red que no ha cumplido los requisitos de seguridad dados por el centro de validación que haya en la red.

4.4.5 Petición de Clave

El servicio de petición de clave proporciona una manera segura para los dispositivos pedir la clave de red o bien la clave maestra a otro dispositivo como es el centro de validación.

4.5 Rol del Centro de Validación

Por temas de seguridad, ZigBee define el rol de Centro de Validación. Este elemento es un dispositivo validado por los dispositivos de la red para distribuir las claves para que gestione la configuración de aplicación de los dispositivos. Todos los miembros de la red deben reconocer solo a un centro de validación (Trust Center) y debe existir solo y solo un centro de validación por cada red segura.

Las funciones dadas por el Centro de Validación pueden ser subdivididas en tres roles: el gestor de la validación, el gestor de la red y el gestor de la configuración. Un dispositivo se encarga de validar el gestor de validación para identificar los dispositivos que toman el rol en dicha red y el gestor de configuración. El gestor de red se encarga de gestionar la clave de red, tanto para tenerla como para distribuirla. El gestor de configuración se encarga del enlace (binding) de dos aplicaciones y facilitar la seguridad entre estos dos

dispositivos que gestiona, como por ejemplo distribuyendo las claves maestras o de enlace. Para simplificar el manejo de estros tres roles, se incluyen dentro de un único dispositivo, el centro de validación.

5 Dispositivos ZigBee

Desde que en 2005 apareciese la primera especificación beta del protocolo ZigBee. No han dejado de surgir distintos tipos de dispositivos capaces de utilizar dicha tecnología.

En principio, para este tipo de dispositivos se consideró, que debido a su bajo coste de fabricación, el precio no sería muy superior a los tres euros por componente. Así como, que se fabricaron cuarenta mil dispositivos durante su primer año de vida y se espera que sean cuatrocientos mil los que vean la luz este mismo año. Lo segundo al parecer se cumplió sin mayores complicaciones. El problema fue que el primer objetivo (por llamarlo de alguna forma) no se cumplió del todo. Finalmente un dispositivo ZigBee tiene un coste alrededor de los cuarenta euros, como mínimo.

De todas formas, se trata de una tecnología en la que muchas empresas han puesto sus expectativas de futuro y por lo tanto, han aparecido multitud de dispositivos. Fabricando componentes de bajo nivel, que llevan embebido procesadores y sistemas capaces de trabajar con este protocolo, como dispositivos comerciales, listos para utilizar el protocolo directamente desde cualquier ordenador, PDA o teléfono móvil.

Como nota interesante, consideramos de gran relevancia un estudio acerca de dispositivos ZigBee, llevado a cabo por la empresa de análisis West Technology Research Solutions, en el que prevén que para el año 2008 habrían más de trescientos millones de dispositivos que integren la tecnología ZigBee, sólo en el campo de la Domótica.

5.1 Dispositivos de Bajo Nivel

Actualmente hay varias empresas que entre sus componentes electrónicos ofrecen componentes Zigbee. De entre todas hemos escogido dos, las cuáles tienen ya varios dispositivos comercializados. También hay empresas que venden paquetes o conjuntos de desarrollo más especializados, pero estos son suministrados con su propio sistema de desarrollo, lo que provoca que no sean del todo compatibles con el resto de dispositivos ZibBee.

La primera empresa desarrolladora de dispositivos ZigBee que hemos elegido, es una alianza entre dos, que son rfSolutions y FlexiPanel. Esta alianza a dado a la luz diversos dispositivos ZigBee, tanto de bajo como de alto nivel.

El dispositivo más bajo de que dispone la compañía recibe el nombre de EasyBee. Se trata de un transceptor RF que cumple la normativa IEEE 802.15.4. Preparado para trabajar dentro de una red ZigBee como un dispositivo final.

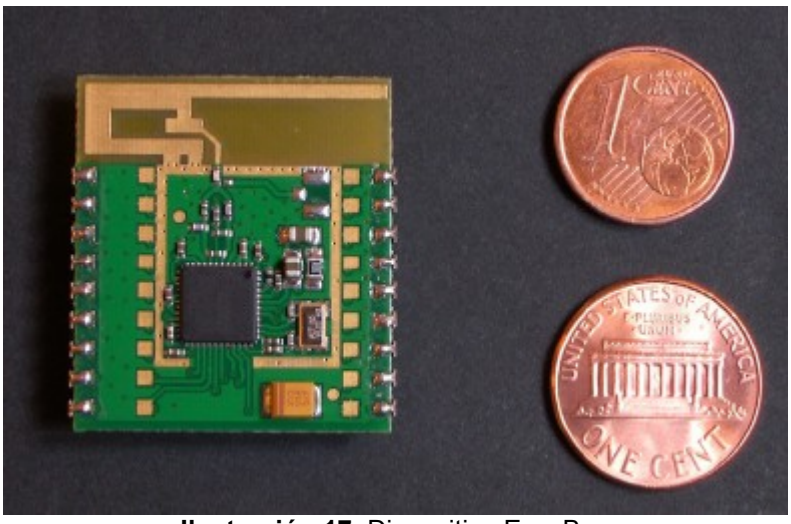

Ilustración 17. Dispositivo EasyBee

Se trata de un dispositivo de reducidas dimensiones, tan sólo 26mmx20mm, con un consumo de energía de 2.1V a 3.6V y con capacidad para estar operativo en condiciones climáticas adversas, pues puede trabajar con temperaturas entre -40ºC y 85ºC. Además puede comunicarse con otros dispositivos ZigBee que se encuentren hasta a doscientos metros de distancia, con una tasa de transferencia de datos de hasta 25kbps.

Las aplicaciones para la que se ha orientado este dispositivo son:

- Reemplazar el cableado de cualquier red.
- Automatismos en viviendas.
- Redes y control industrial.
- Sensores para redes inalámbricas.

A continuación, este conjunto de empresas ha desarrollado otro dispositivo más potente, denominado Pixie. Este dispositivo no es uno sólo, sino que se trata de una serie, hasta ahora compuesta por dos dispositivos. Orientados para ejercer el rol de Coordinador y Router, dentro de una red ZigBee. Dentro de la serie Pixie, han recibido el nombre de Pixie y Pixie Lite respectivamente.

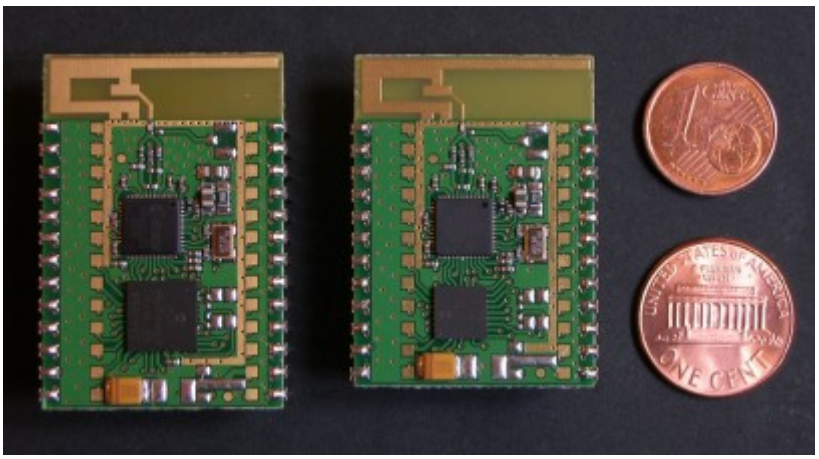

Ilustración 18. Dispositivos Pixie y Pixie Lite

Se trata de dispositivos con las mismas características técnicas que el dispositivo final EasyBee, pero con mayor capacidad de procesamiento, lo que les permite ejercer como dispositivos más potentes que estos, dentro de una red ZigBee.

Además, como característica técnica muy interesante, todos estos dispositivos disponen de la posibilidad de ser conectados a una antena externa, lo que les otorgaría un alcance mucho mayor para formar una red ZigBee.

Otro elemento interesante desarrollado por este compendio de empresas es un cable de conexión USB. Dicho así puede no parecer interesante, pero al contrario, puesto que se trata de un cable con el que se puede conectar un ordenador a los dispositivos ZigBee desarrollados por estas empresas. Una vez conectado, el cable se convierte en una conexión serie a través de USB, desde donde podremos configurar y manejar nuestros dispositivos ZigBee e incluso entrar en la red, en la que se encuentre el dispositivo al que nos encontremos conectados. Este elemento ha sido bautizado con el nombre de Pixie Configuration Tool.

Ilustración 19. Pixie Configuration Tool

Y por último, estas dos empresas han desarrollado su producto más interesante orientado a desarrolladores, que ha sido denominado Pixie Evaluation Kit. Con este producto cualquier desarrollador interesado en esta tecnología (protocolo) podrá probar físicamente sus diseños de dispositivos ZigBee. Así como trabajar directamente sobre los dispositivos ofertados por estas empresas, con los que es totalmente compatible. Esto permitirá el control total de los dispositivos, así como su programación directa y análisis de su funcionamiento.

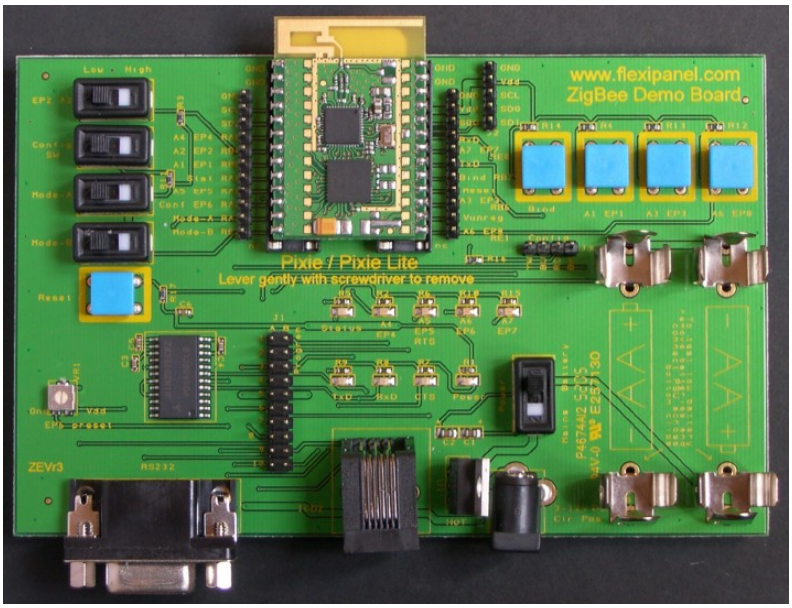

Ilustración 20. Pixie Evaluation Kit

Otra empresa que tiene ya desarrollos de dispositivos de bajo nivel ZigBee operativos es Telegesis. Esta empresa, al contrario que sucedía anteriormente, dispone de dispositivos que implementan el protocolo ZigBee, pero que pueden ejercer de dispositivos finales para una red ZigBee, así como de Routers y Coordinadores, lo que se llama un todo en uno. Así como un kit de desarrollo bajado en sus dispositivos.

En primer lugar aparece el denominado ETRX1. Se trata de un dispositivo de bajo coste y preparado para ser integrado en una red ZigBee. Algo mayor que los dispositivos anteriores 27.75x20.45mm, un consumo ligeramente superior 2.7V a 3.6V y mismas características físicas para trabajar a temperaturas de entre -40ºC y 85ºC. Pero aun siendo más grandes y consumir más, hay que tener en cuenta que se trata de un dispositivo que puede ejercer, tanto de dispositivo final, como de Coordinador.

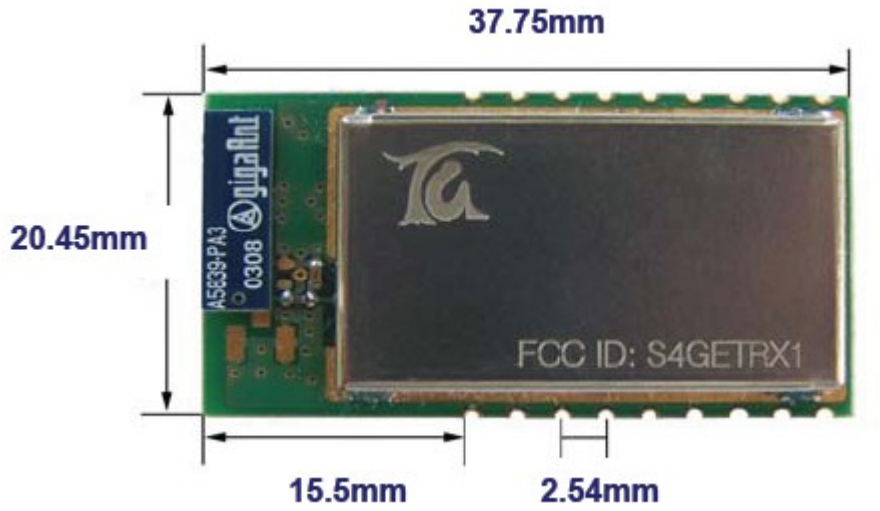

Ilustración 21. ETRX1

Las aplicaciones para las que ha sido orientado este dispositivo son:

- Lectura automática de métricas (ARM Automatic Meter Reading).
- Alarmas Wireless y Seguridad.
- Automatismos de viviendas.
- Sensores de presencia inalámbricos.
- Control industrial.
- Periféricos de PC.

A continuación de este dispositivo apareció el denominado ETRX2. Un modelo algo menos económico, pero más atractivo todavía. Pues a las características de los módulos anteriores, podemos añadirle el hecho de que disponga de 128k de memoria flash y otros 5kbytes de SRAM. Lo que le permite poder actuar como cualquier tipo de dispositivo dentro de una red ZigBee. Añadiendo además la posibilidad de tres tipos de antenas simultáneas conectadas al dispositivo, lo que haría que la conexión se pudiese dar a distancias muy superiores que las indicadas en el estándar del protocolo.

Las aplicaciones para las que ha sido orientado este dispositivo son todos los del dispositivo anterior, más algunas otras más potentes:

- Controles industriales M2M.
- Sistemas ZigBee futuros.

Ilustración 22. ETRX2

Para programar ambos dispositivos se dispone de un interfaz en línea de comandos, que según define el fabricante es muy intuitivo y sencillo. Lo que hace que no sea necesaria mucha experiencia en módulos RF para su programación.

Para finalizar, esta empresa también dispone, tal y como se indicó anteriormente, de un kit para desarrolladores que pretendan adentrarse en este nuevo protocolo. Este kit se bautizó con el nombre de ETRX1DVK Devkit, habiendo evolucionado a ETRX2DVK Devkit. Al igual que ocurría en el caso anterior, está orientado para trabajar sobre dispositivos de este fabricante, con la posibilidad de hacer modificaciones, ampliaciones y nuevos desarrollos. La mayor diferencia con el kit anterior, radica en que la interconexión para poder programar los dispositivos es a través de cable serie directamente, sin tener que utilizar un USB que finalmente trabajaba como serie.

Lo que sí contiene este kit, son algunos dispositivos del modelo ETRX1 o ETRX2 para poder empezar a trabajar y testear desde el primer momento.

Ilustración 23. ETRX2DVR Devkit

5.2 Dispositivos de Alto Nivel

Como dispositivos de alto nivel, comprenderemos los dispositivos ZigBee desarrollados, que son totalmente independientes y que no están compuestos sólo por los componentes electrónicos que soportan el estándar, sino que además ya disponen de interfaz que nos permite trabajar con ellos directamente sobre redes ZigBee.

Este apartado se encuentra aun algo verde, dado que no hay muchos dispositivos finales para el consumidor disponibles que implementen este protocolo. Aunque algunos hay y bastante interesantes.

En primer lugar veremos dos dispositivos de la empresa Telegesis, que por ahora parece ser una de las que más está apostando por el protocolo de cara al usuario final.

Esta empresa ha desarrollado un dispositivo ZigBee que es totalmente operativo, dentro de un PenDrive o pastilla USB. Basado en la tecnología de su dispositivo de bajo nivel ETRX1 y posteriormente ETRX2, recibe el nombre de ETRX1USB y ETRX2USB respoectivamente. Y se trata de un dispositivo que trabaja en la banda de frecuencia de los 2.4GHz, con alcance de hasta 100m de distancia para encontrar otros dispositivos ZigBee, antena omnidireccional y capacidad de utilizar hasta 16 canales para las búsquedas de dispositivos.

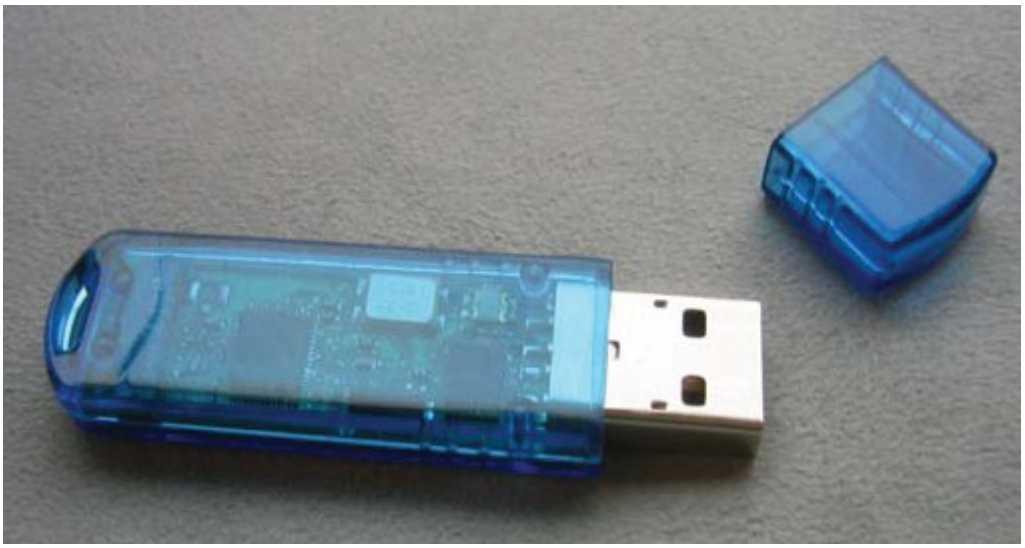

Ilustración 24. ETRX1USB

Tras este dispositivo, la empresa fabricó otro dispositivo ZigBee más interesante todavía que el que acabamos de ver. Se trata de un dispositivo con el nombre de ETRX1CF, evolucionado con el sistema ETRX2 a ETRX2CF y que como de su nombre se puede extraer, se trata de un dispositivo en formato de tarjeta Compact Flash. Lo que le permite ser utilizado desde un ordenador, utilizando el mismo sistema que las tarjetas PCMCIA. De la misma forma que lo podríamos utilizar desde una agenda electrónica o PDA. Por lo demás tiene las mismas características y especificaciones que su hermano USB.

Ilustración 25. ETRX1CF en PDA

Ilustración 26. ETRX2 en PC y PDA

Además de estas dos empresas desarrolladoras de dispositivos ZigBee, hay muchísimas otras, dentro de las cuales nos gustaría también destacar a la Coreana Pantech&Curitel. Quien ha desarrollado ya el primer teléfono móvil que integra la tecnología ZigBee en sus entrañas. Este modelo no es más que un prototipo por el momento y se desconoce su fecha de comercialización, pero por el momento ha demostrado que puede ser integrado en cualquier tipo de dispositivo.

6 Sistema Operativo

Una vez ensamblados los dispositivos que integran ZigBee, el fabricante añade el sistema operativo embebido que utilizarán para operar y que permitirán la comunicación de desarrolladores con estos, para su programación o adaptación al entorno de operación. Existen actualmente dos posibilidades de sistema operativo; uno basado en Hyperterminal y otro conocido como TinyOS.

El sistema operativo de Hyperterminal es un entorno sencillo que permite la comunicación con los dispositivos a través de comandos AT. Utiliza el mismo sistema de comunicación que los antiguos módems, mediante un puerto serie RS232. Los comandos AT que utiliza son los estándares para realizar las operaciones más básicas (AT para comprobar si el dispositivo está operativo, ATZ para resetearlo, etc.), además se han implementado una serie de comandos AT especiales preparados para este tipo de dispositivos que nos permiten crear una red, expulsar dispositivos, buscar una red, enviar información de un dispositivo a otro o a todos los dispositivos, etc. También y dependiendo del fabricante, se

han incluido comandos AT propietarios, como es el caso de los dispositivos desarrollados por Telegesis, que además proporciona un entorno de acceso propio, que contiene las opciones más comunes en botones que permiten que la comunicación y las operaciones se realicen en pocos clics de ratón.

La segunda opción ha sido bautizada como TinyOS, es un sistema operativo basado en Unix y de código libre bajo licencia open source, orientado a componentes para redes de sensores inalámbricas. Desarrollado por un consorcio o asociación encabezado por la Universidad de California, en cooperación con Itel Research. Suele ser utilizado en los dispositivos ZigBee OEM. De la misma forma que sucedía en el caso de Hyperteminal, para comunicarnos con los dispositivos ZigBee será necesario hacerlo a través de un puerto serie. En cuanto al desarrollo de aplicaciones, puede trabajarse con distintos leguajes de programación, aunque las aplicaciones suelen ser implementadas principalmente en una variante de C conocido como nesC (release 1.2.8 actualmente), orientado y optimizado para las limitaciones de memoria y comunicación de este tipo de redes; otros dos lenguajes también muy extendidos en este tipo de dispositivos son Java (Eclipse dispone de una librería de programación) y el código interpretado Bash. Desde TinyOS se proporciona interfaces, módulos y configuraciones específicas e interfaces estándar para entradas y salidas de hardware. Actualmente la versión estable del sistema es la TinyOS 2.0 y dispone de entorno de programación para Linux, Windows NT, Windows 2000 y Windows XP y la versión inestable que se encuentra en desarrollo actualmente es la 2.04 conocida como Boomerang.

7 Comparativa Bluetooth vs ZigBee

Bluetooth y ZigBee tienen mucho en común. Los dos son dos tipos de *redes de área personal wireless* o WPANs. Los dos funcionan en la banda sin licencia de 2.4Ghz y los dos consumen poca energía.

7.1 Sensores de control ZigBee

El protocolo ZigBee define un tipo de sensor para aplicaciones comerciales y de hogar como control de calefacción, aire acondicionado o control de alumbrado. Para ello se combina con IEEE 802.15.4 que define que la capa física y MAC, con las de red, seguridad y de software de aplicación se especifican por ZigBee Alliance, un consorcio de empresas tecnológicas.

7.2 Eliminación de cables con Bluetooth

Bluetooth, tal y como se conoce, elimina el cableado entre los productos electrónicos y los accesorios, como por ejemplo entre los ordenadores e impresoras o entre los teléfonos y los auriculares. Bluetooth está más orientado hacia la movilidad del usuario y eliminar el cableado a corta distancia. La meta de ZigBee es más para la automatización a gran escala y el control remoto.

Existen algunas diferencias técnicas entre los dos protocolos:

	Bluetooth	**ZigBee**
Técnica de Modulación	FHHS	DSSS
Tamaño de la pila de Protocolo	250kbyte	28kbyte

Batería	Frecuentes Recargas	Hasta 2 años
Velocidad Máxima	1Mbits/s	250kbits/s
Área de Red	Hasta 100m	Más de 70m
Tiempo de Incorporación	3 segundo	30 milisegundos

8 Bibliografía

ZigBee Alliance Web Site – http://www.zigbee.org
IEEE 802.15 Web Site – http://www.ieee802.org/15
FlexiPanel Web Site – http://www.flexipanel.com
Domodesk Web Site – http://www.domodesk.com
Silicon Laboratories Web Site – http://www.silabs.com
Palo Wireless Web Site – http://www.palowireless.com
TinyOS Web Site – http://www.tinyos.net

Agradecimientos:
- Joanie Wexler de Network World
- Este trabajo ha sido financiado por la Generalitat Valenciana dentro de la acción especial AE/2007/078.