# AGRADECIMIENTOS

En mi primer lugar, me gustaría agradecer a mis tutores de proyecto Jorge Portilla y Gabriel Mujica. Agradecer su colaboración y su experiencia en redes de sensores inalámbricas.

Dar las gracias también a mi familia por su constante apoyo y ánimo en épocas difíciles.

# RESUMEN

El mundo tiende a compartir cada vez más información, a estar cada vez más interconectado. Cada vez existe un mayor número de dispositivos conectados entre ellos y con Internet de múltiples maneras. De todo esto surge lo que se conoce, en inglés, como **Internet of Things** o **IoT**, o en español, Internet de las cosas.

Este concepto consiste en redes de sensores capaces de monitorizar su entorno, reaccionando ante posibles cambios.

# INDICE

[AGRADECIMIENTOS 3](#_Toc66034721)

[RESUMEN 4](#_Toc66034722)

[INDICE 5](#_Toc66034723)

[ABREVIATURAS Y ACRÓNIMOS 7](#_Toc66034724)

[ILUSTRACIONES 8](#_Toc66034725)

[ECUACIONES 9](#_Toc66034726)

[TABLAS 10](#_Toc66034727)

[CÓDIGOS 11](#_Toc66034728)

[1. INTRODUCCIÓN 12](#_Toc66034729)

[2. ESTADO DEL ARTE 13](#_Toc66034730)

[2.1. Internet of Things (IoT) 13](#_Toc66034731)

[2.1.1. Introducción [2] 13](#_Toc66034732)

[2.1.2. Componentes [2] 14](#_Toc66034733)

[2.1.2.1. Dispositivo 14](#_Toc66034734)

[2.1.2.2. Red Local 15](#_Toc66034735)

[2.1.2.3. Internet 15](#_Toc66034736)

[2.1.2.4. Servicios Backend 15](#_Toc66034737)

[2.1.2.5. Aplicaciones 16](#_Toc66034738)

[2.1.3. Sensores 16](#_Toc66034739)

[2.1.4. Arquitectura [3] 17](#_Toc66034740)

[2.1.4.1. Capa de Sensorizado 17](#_Toc66034741)

[2.1.4.2. Capa de Red 17](#_Toc66034742)

[2.1.4.3. Capa de Servicio 18](#_Toc66034743)

[2.1.4.4. Capa de Interfaz 18](#_Toc66034744)

[2.2. 6LoWPAN [4] 19](#_Toc66034745)

[2.2.1. Significado 6LoWPAN [4] 19](#_Toc66034746)

[2.2.2. Pila de Protocolos de 6LoWPAN [4]–[6] 20](#_Toc66034747)

[2.2.3. Principales características de 6LoWPAN [7] 20](#_Toc66034748)

[2.2.3.1. Compresión de cabecera 21](#_Toc66034749)

[2.2.3.2. Enrutamiento 21](#_Toc66034750)

[2.2.3.3. Seguridad 21](#_Toc66034751)

[2.2.3.4. Protocolos de aplicación 21](#_Toc66034752)

[2.2.4. Retos de 6LoWPAN 22](#_Toc66034753)

[2.2.5. Implementaciones y aplicaciones para 6LoWPAN [5], [7] 22](#_Toc66034754)

[2.2.5.1. Contiki 22](#_Toc66034755)

[2.2.5.2. TinyOS 23](#_Toc66034756)

[2.2.5.3. Thread 23](#_Toc66034757)

[2.3. THREAD 24](#_Toc66034758)

[2.3.1. Introducción a Redes THREAD [8], [10]–[12] 24](#_Toc66034759)

[2.3.2. Tipos de dispositivos 25](#_Toc66034760)

[2.3.3. Protocolo Thread 26](#_Toc66034761)

[2.3.3.1. Redes de área Privada - Private Area Network (PAN) [12] 27](#_Toc66034762)

[2.3.3.2. Capa Física [12], [14] 29](#_Toc66034763)

[2.3.3.3. Capa MAC (o enlace de Datos). [12], [14] 30](#_Toc66034764)

[2.3.3.4. Capa de adaptación 6LoWPAN [12] 30](#_Toc66034765)

[2.3.3.5. Capa de Red [12] 31](#_Toc66034766)

[Protocolo de Enrutamiento 31](#_Toc66034767)

[2.3.3.6. Capa de Transporte [12] 32](#_Toc66034768)

[2.3.3.7. Seguridad y Comisión de dispositivos [10], [12] 32](#_Toc66034769)

[3. OBJETIVOS 35](#_Toc66034770)

[4. MÉTODOS Y EQUIPO 36](#_Toc66034771)

[5. EXPERIMENTOS 37](#_Toc66034772)

[6. RESULTADOS Y ANÁLISIS 38](#_Toc66034773)

[7. CONCLUSIONES 39](#_Toc66034774)

[8. LINEAS FUTURAS 40](#_Toc66034775)

[9. PLANIFICACIÓN TEMPORAL Y PRESUPUESTO 41](#_Toc66034776)

[10. BIBLIOGRAFÍA 42](#_Toc66034777)

# ABREVIATURAS Y ACRÓNIMOS

|  |  |
| --- | --- |
| IoT | Internet of Things |
| WAN | Wide Area Network |
| LAN | Local Area Network |
| MAN | Metropolitan Area Network |
| PAN | Personal Area Network |
| LPWAN | Low Power Wide Area Network |
| WSN | Wireless Sensor Networks |
| M2M | Machine to Machine |
| LTE | Long Term Evolution |
| IPv6 | Internet Protocol version 6 |
| IPv4 | Internet Protocol version 4 |
| SOA | Service Oriented Architecture |
| QoS | Quality of Service |
| IFP | InterFace Profile |
| SPP | Service Provisioning Process |
| WSDL | Web Services Description Language |
| 6LoWPAN | IPv6 over Low power Wide Personal Area Network |
| WPAN | Wide Personal Area Network |
| RPL | IPv6 Routing Protocol for Low Power and Lossy Networks |
| DAG | Direct Acyclical Graphic |
| DODAG | Destination Oriented DAG |
| AES | Advanced Encryption Standar |
| DTLS | Datagram Transport Layer Security |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| CoAP | Constrained Application Protocol |
| MQTT-SN | Message Queue Telemetry Transpor for Sensor Networks |
| BLIP | Berkeley Low-power IP stack |
| REED | Router Eligible End Device |
| FTD | Full Thread Device |
| MTD | Minimal Thread Device |
| ED | End Device |
| FED | Full End Device |
| MED | Minimal End Device |
| SED | Sleepy End Device |
| MeshCoP | Mesh Commissioning Protocol |
| BR | Border Router |
| JD | Joiner Device |
| JR | Joiner Router |
| JS | Joiner Session |
| ULA | Unique Local Address |
| GUA | Global Unique Address |
| EID | Endpoint Identifier |
| REST | Representational State Transfer |
| KEK | Key Encryption Key |
| IID | Interface Identifier (from the JD) |

# ILUSTRACIONES

[Ilustración 1 Estructura Básica 6LoWPAN [6] 20](#_Toc66034709)

[Ilustración 2 Arquitectura en Contiki [7] 23](#_Toc66034710)

[Ilustración 3 Ejemplo de una topología de Red Thread en malla [9] 26](#_Toc66034711)

[Ilustración 4 Pila de Protocolo Thread en un sistema IoT [12], [13] 27](#_Toc66034712)

[Ilustración 5 Ejemplo PAN Thread [12], [13] 28](#_Toc66034713)

# ECUACIONES

# TABLAS

[Tabla 1 Diferencias M2M – IoT [2] 15](#_Toc61101566)

# CÓDIGOS

# INTRODUCCIÓN

# ESTADO DEL ARTE

En los últimos años, se han ido desarrollando cada vez más las tecnologías para Internet of Things, IoT. Entre estas tecnologías están las tecnologías de comunicaciones inalámbricas tanto a redes de áreas pequeñas como de áreas extensas. Estas últimas, conocidas como WAN (wide área network), son usadas como base para la gran mayoría de arquitecturas en proyectos IoT.

En este estudio nos centraremos en las características de una de ellas: Thread. Para esto conviene conocer mínimamente las tecnologías IoT, y en concreto, el modelo de la tipología red WAN sobre la que mejor se aplica IoT en casos de conexiones inalámbricas: LPWAN.

## Internet of Things (IoT)

En el IoT, un gran número de tecnologías inalámbricas, como el WiFi, el Bluetooth, LoRa, NB-IoT, 2G/3G/4G, etc., han sido usadas en diversas aplicaciones, conectando entre si a millones de dispositivos de manera inalámbrica. 3G y 4G son muy usados en IoT, pero no están totalmente optimizados para aplicaciones de este tipo. A pesar de esto, el 4G ha mejorado bastante algunas de las capacidades de las redes móviles, dando a los dispositivos IoT acceso a Internet. Dentro de la conectividad 4G hay varios tipos de tecnologías como BLE, WiMaxb, LTE, Zigbee, LoRa, NB-IoT, etc. [1]

### Introducción [2]

Mientras que IoT ofrece muy buenas oportunidades, sigue siendo un reto pendiente el manejo de todo lo que lleva integración continua del mundo físico. Actualmente hay dos APIs para las comunicaciones IoT:

* REST basado en API.
* WebSocket basado en API.

IoT es un término paraguas, que acoge a muchas tecnologías dentro de sí. Las siguientes tecnologías son ejemplos de las que dan paso al desarrollo de IoT:

* WSN.
* Cloud Computing.
* Big Data Analytics.
* Sistemas Embebidos
* Arquitectura y Protocolos de Seguridad
* Protocolos de Comunicación
* Servicios Web.
* Internet Móvil
* Motor de búsqueda semántico.

Dentro de todas estas tecnologías, las WSN son el corazón de IoT. Dentro de la tecnología IoT hay tres principales objetivos:

* Dar un puente entre la parte rica y la parte pobre.
* Distribuir los recursos del mundo a los necesitados.
* Ser más proactivo y menos reactivo.

También existe otra tecnología M2M, cuya comunicación se basa en redes de dispositivos intercambiando o enviando datos sin interacción humana. Las diferencias entre M2M e IoT las indicamos en esta tabla.

|  |  |
| --- | --- |
| **M2M** | **IoT** |
| Centrada en la capa por debajo de la capa de red. | Centrado en la capa por encima de la capa de red. |
| Sensado y actuación pueden no estar involucrados. | Sensado y actuación pueden estar involucrados. |
| Énfasis en hardware. | Énfasis en software. |
| La nube no está involucrada. | La nube esta involucrada. |

Tabla Diferencias M2M – IoT [2]

A nivel de hardware hay ciertos requisitos hardware que llevan tanto al desarrollo de una infraestructura IoT como en el de redes de comunicación:

1. Fuente de alimentación y Manejo de la alimentación.
2. Sensores o Actuadores.
3. Procesador y Espacio de memoria.
4. Comunicaciones Inalámbricas.
5. UI/UX.

### Componentes [2]

Los principales componentes funcionales de las tecnologías IoT son:

* Componente para la interacción y comunicación con otros IoT.
* Componente para operaciones de procesado y análisis de los datos.
* Componente para la interacción con internet.
* Componente para el manejo de servicios Web de la aplicación.
* Componentes para la integración de los servicios de la aplicación.
* Interfaz de usuario para acceder al IoT.

#### Dispositivo

Los dispositivos IoT tienen identidades únicas. Es un dispositivo físico que está embebido con sensores, actuadores, electrónica, software, una red de conectividad con otros objetos con los que intercambiar datos. Se realizan tareas como sensorizado, actuación y monitorización de manera remota. Hay mucha variedad de dispositivos, pero todos se pueden reducir a dos tipos: dispositivos estándar o dispositivos restringido. Los datos son intercambiados con otros dispositivos y aplicaciones, incluso enviando esos datos a servidores centralizados o aplicaciones basadas en procesamiento de datos en la nube.

Los dispositivos restringidos son pequeños, al igual que sus capacidades de cómputo, memoria y otras características. Estos pequeños dispositivos restringidos necesitan de un dispositivo que haga de Gateaway para poder conectarse a la plataforma de la nube.

Los dispositivos estándar son similares a pequeños ordenadores y dirigen los datos directamente a la nube de la red sin necesidad de un Gateaway.

#### Red Local

Como se ha comentado anteriormente, IoT es una red de dispositivos interconectados y se generarán una gran cantidad de datos. Estas redes son usadas para transmitir las señales que se recogerán posteriormente en los sensores con el resto de diferentes componentes, como los routers, puentes, LAN, WAN y MAN. Esta conectividad de las redes para los sensores se puede utilizar cualquiera de las tecnologías disponibles como el Wi-Fi, LTE, etc. Para la generación de esta red se deben seguir las siguientes bases:

* Alta tasa de datos.
* Bajos precios en uso de datos.
* Despliegue IPV6

#### Internet

El Internet es el sistema de redes de ordenadores interconectados globalmente usando el protocolo de internet para unir los diferentes dispositivos. Internet da la posibilidad de nuevos servicios, acelerando y permitiendo nuevas zonas de interacción con mensajes instantáneos y social networking, entre otros.

#### Servicios Backend

Los servicios principales que se ofrecen son:

* Monitorización de dispositivos.
* Servicios de control de dispositivos.
* Servicios de publicación de datos.
* Servicios de búsqueda de datos.

Estos Servicios Backend se definen como un conjunto de servicios basados en la nube que ayudan a construir la aplicación IoT o aplicación Backend. Tienen un rápido almacenamiento de datos y una fácil gestión de usuarios. Para toda estrategia de una empresa IoT es una solución bonita. La parte delantera de una solución IoT asegura al usuario final un aumento de seguridad o añadirá valor en sus vidas.

Una vez se recolectan los datos con el producto, se envían a la nube, donde se guardarán en servidores que permitirán al usuario computarlos.

#### Aplicaciones

Las principales aplicaciones para IoT son:

* Smart Home
* Accesorios
* Coches conectados
* Smart Cities
* IoT en la Agricultura

### Sensores

Los sensores son el componente más importante en IoT. Es el dispositivo que se opera con baja potencia, menos energía y recursos limitados de almacenamiento. Hay dos tipos de clases de sensores, según nos fijemos en **el tipo de** **salida** o el **tipo de dato.**

Según el **tipo de salida** tenemos las siguientes clases de sensores:

1. **Sensores Analógicos:** Estos sensores generan una señal continua de salida. Sensores de este tipo son como los acelerómetros, sensor de presión, de sonido, de temperatura, etc. Sensores que captan cantidades analógicas y que son continuas en la naturaleza.
2. **Sensores Digitales:** Son usados para medidas analíticas generalmente. Producen una salida binaria, un “1” lógico o un “0” lógico, son valores discretos que pueden ser un solo “bit” (transmisión serie) o un conjunto de bits formando un único “byte” de salida (transmisión paralela).

Por otro lado, según el **tipo de dato** tenemos las siguientes clases de sensores:

1. **Sensores escalares:** La señal de salida generada por el sensor, o el voltaje, es proporcional a la magnitud que se está midiendo. Mediciones físicas como temperatura, presión, etc., son magnitudes escalares cuyo valor es suficiente información. Dichas mediciones también variarán respondiendo proporcionalmente a los cambios en la medida realizada.
2. **Sensores vectoriales:** Se produce una señal de salida, o voltaje, proporcionales tanto a la magnitud medida como la orientación de lo que se mide. Ejemplos de esto pueden ser imágenes, sonido, velocidad, aceleración, orientación, etc., medidas de las cuales solo el valor o magnitud no da una información completa. Por ejemplo, un cuerpo con una aceleración, puede tener una aceleración en sus tres ejes, por lo que una información completa sería la aceleración de los 3 ejes, no solo la magnitud del vector resultante de los 3 ejes.

### Arquitectura [3]

La arquitectura de las tecnologías IoT es una arquitectura orientada al servicio (SOA por sus siglas en inglés). A continuación, se explicará una arquitectura SOA de cuatro capas, la cuál se ha pensado desde el punto de vista de las funcionalidades.

Este diseño se compone de las capas de Sensorizado, Red, Servicio e Interfaz.

#### Capa de Sensorizado

IoT puede considerarse una red física globalmente interconectada, en la cual, las cosas pueden ser conectadas o ser controladas remotamente. Cada vez más dispositivos cuentan con equipamiento de RFID o sensores inteligentes, por lo que la conectividad cada vez es más sencilla. En esta capa, los sistemas inalámbricos inteligentes con sensores, toman las medidas e intercambian la información con diferentes dispositivos. Esto ayuda a identificar cambios en el ambiente.

#### Capa de Red

La función de esta capa es la de conectar todo entre sí y permitir el envío de información entre dispositivos. Además, es capaz de añadir información sobre las infraestructuras IT existentes. En la arquitectura SOA de IoT, los servicios, aportados por los dispositivos, son desplegados en redes heterogéneas y los dispositivos relacionados se introducen en el servicio de Internet.

Este proceso puede involucrar el manejo y control de QoS (Quality of Service) para así cumplir con los requerimientos de los usuarios y/o aplicaciones. Por otro lado, es importante que se automatice el encontrar y mapear los dispositivos o “cosas” para una dinámica red cambiante. Estos dispositivos necesitan que se les asigne un rol automáticamente, para desplegar, manejar y organizar (scheduling) comportamientos de los dispositivos y ser capaces de cambiar de rol en cualquier momento según necesite. Esto habilita a los dispositivos para colaborar en la realización de las distintas tareas. Para diseñar esta capa, los diseñadores necesitan:

* Tecnologías de gestión de redes para redes heterogéneas.
* Eficiencia energética.
* Requerimientos QoS.
* Procesamiento de datos y señales.
* Seguridad.
* Privacidad.

#### Capa de Servicio

Esta capa se apoya en la tecnología del Middleware que aporta funcionalidades para integrar de manera correcta servicios y aplicaciones en IoT. La tecnología Middleware provee a IoT con una plataforma coste-eficiencia, donde pueden ser reusadas las plataformas Hardware and Software. La principal actividad de esta capa implica las especificaciones de servicio para middleware. Una capa de servicio bien diseñada será capaz de identificar los requerimientos comunes de aplicación y dar APIs y protocolos para soportar los servicios, aplicaciones y necesidades de usuario requeridas. Además, se procesan todos los problemas orientados al servicio, incluyendo el intercambio y almacenamiento de información, gestión de datos, comunicación y motor de búsqueda. Los componentes de esta capa son:

* Descubrimiento de Servicio: Encontrar objetos que puedan aportar los servicios requeridos y la información deseada de manera eficiente.
* Composición de Servicio: Habilita la interacción entre los dispositivos conectados. Esta fase es para hacer el scheduling, u organización, o recrear servicios más ajustados de cara a conseguir la manera más fiable de lograr los requerimientos.
* Gestión de la confianza: Buscando un mecanismo de confianza que pueda evaluar y usar la información aportada por los otros servicios para crear un sistema de confianza.
* Servicio APIs: Apoyando la interacción entre los servicios requeridos en IoT.

#### Capa de Interfaz

En IoT hay muchos dispositivos involucrados, los cuáles son de diferentes proveedores y no siempre usan los mismos estándares o protocolos, por lo que suele haber problemas en las comunicaciones e intercambios de información entre los dispositivos. Cómo el número de dispositivos sigue creciendo, este problema se incrementa y se hace más dificultoso. Va apareciendo la necesidad de una capa de Interfaz que simplifique la gestión y la interconexión de los distintos dispositivos. Un perfil de interfaz (InterFace Profile, IFP) puede ser visto con un subconjunto de los estándares de servicios que ayudan a la interacción con aplicaciones dentro de la red. Los perfiles de interfaz son usados para describir las especificaciones entre las aplicaciones y los servicios. Los servicios, en su respectiva capa, corren en una limitada red de infraestructuras para encontrar eficientemente nuevos servicios para una aplicación y conectarlos a la red.

Tradicionalmente, la capa de servicio daba una API universal a las aplicaciones. Sin embargo, con los nuevos resultados de investigaciones sobre SOA-IoT, se ha visto que el Proceso de provisionamiento de servicios (SPP de sus siglas en inglés) puede también dar una interacción efectiva entre aplicaciones y servicios. El SPP empieza haciendo una “consulta de tipos” que envía una petición a los servicios con un formato WSDL genérico y usan un mecanismo de búsqueda para encontrar servicios potenciales. Basados en el contexto de aplicación y la información QoS, todas las instancias de servicios se clasifican y un mecanismo de provisionamiento según demanda se usará para identificar los servicios que encajen con los requerimientos de la aplicación. Finalmente se evalúa el proceso.

## 6LoWPAN [4]

Muchas de las soluciones patentadas, como ZigBee, están vinculadas verticalmente o perpendicularmente a una capa de enlace y los perfiles de aplicación solamente resuelven una pequeña parte de las múltiples aplicaciones para redes inalámbricas integradas. Estas también se encuentran con problemas a la hora de evolucionarlas, integración a Internet y de escalabilidad.

**6LoWPAN** consigue vencer estos problemas gracias al uso de IPV6, en dispositivos integrados de bajo consumo y procesamiento limitado, sobre redes inalámbricas de bajo ancho de banda.

### Significado 6LoWPAN [4]

6LoWPAN es la abreviación de **IPv6 over Low power Wireless Personal Area Networks**

Vayamos ahora a desglosar por partes:

1. **6 en 6LoWPAN**

El **6** se debe a que este sistema está basado en IPv6. IPv6 es el nuevo Protocolo de Internet, y será el que termine reemplazando a IPv4, debido a que este se está llegando al límite de su rango de direcciones IP posibles.

Mientras que **IPv4** ofrece **232** direcciones (4,294,967,296 direcciones posibles IP en Internet), **IPv6** ofrece **2128** direcciones posibles (3.4x1038 direcciones).

1. **Lo en 6LoWPAN**

**Lo** se debe a Low Power o baja potencia. Usualmente las comunicaciones IP van contrarias a un bajo consumo de potencia. Pero se ha logrado gracias a los sensores inalámbricos y un gran desarrollo, llegar a reducir bastante el consumo.

1. **WPAN en 6LoWPAN**

**WPAN** corresponde a Wireless Personal Area Networks. Una WPAN es la red personal en área que conecta los dispositivos de una persona. Un ejemplo de este tipo de redes son las redes Bluetooth, usadas para conectar, por ejemplo, los smartphones con cascos o auriculares Bluetooth, o incluso con un sistema de manos libres.

En 6LoWPAN se pueden crear redes en mallas, incluyendo una mayor distancia. Debido al uso de 868/915 MHz en vez de 2400 MHz, la cobertura dentro de edificios es mucho mayor.

### Pila de Protocolos de 6LoWPAN [4]–[6]

El concepto básico de la pila del 6LoWPAN, lo ilustramos en la siguiente imagen:

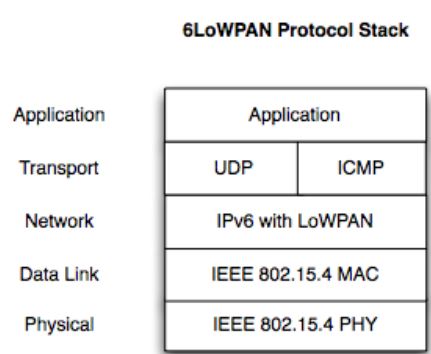


Ilustración Estructura Básica 6LoWPAN [6]

LoWPAN es una capa de adaptación. Aquí el sistema operativo es una parte clave del desarrollo en 6LoWPAN, en términos de la huella en memoria y en funcionalidad.

Gracias a los esfuerzos de los diferentes equipos de trabajo en la investigación de la suite con el protocolo IPv6 basada en el estándar IEEE 802.15.4, se consigue crear una red 6LoWPAN autoorganizada con protocolo de enrutamiento.

La tecnología de las capas bajas de 6LoWPAN apoyan el estándar IEEE 802.15.4 de las capas física (PHY) y MAC. Uno de los problemas se encuentra en el tamaño de la Payload de la capa MAC en IPv6, ya que esta es mayor de lo que la capa baja de 6LoWPAN puede soportar. Para una buena conectividad entre las capas MAC y de red se recomienda añadir una capa de adaptación (LoWPAN) entre medias de las dos capas. Esta capa de adaptación se encargaría de la compresión de la cabecera, la fragmentación, el reensamblaje y el reenvío de la ruta de la red enmallada.

### Principales características de 6LoWPAN [7]

Como se ha indicado tanto en el apartado anterior como en *Ilustración 1,* 6LoWPAN es una capa de adaptación IoT IPv6, la cuál está sobre el estándar IEEE 802.15.4.

Este estándar es un estándar de WPAN de baja potencia y baja velocidad que usa CSMA/CA y con una configuración típica con un rango de 10 a 100 m y una tasa de rango de datos sin procesar de 2 a 250 KBits/s, estando en la banda de 2.4 GHz ISM. Este estándar también permite trabajar en la banda de 900MhHz (banda sub-G), aportando hasta unos pocos kilómetros de rango, pero bajando la tasa de datos.

#### Compresión de cabecera

Para una transmisión eficiente de paquetes IPv6 a través de los enlaces IEEE 802.15.4, se necesitará una capa de adaptación, la cual comprimirá la cabecera de 40 a 7 bytes. Cabeceras de extensión IPv6 se comprimirán de igual manera, como las cabeceras UDP.

#### Enrutamiento

Debido a las limitaciones de las redes 6LoWPAN, la mayoría de los protocolos de enrutamiento en IPv6 no son compatibles, por lo que se ha desarrollado un nuevo protocolo de enrutamiento para 6LoWPAN: **IPv6 Routing Protocol for Low Power and Lossy Networks (RPL).**

Debido a que las redes con perdidas (Lossy Networks) no tienen topologías predefinidas, RPL organiza una topología como un Gráfico Acíclico Directo (DAG) particionado en uno o más DAGs Orientados a Destino (DODAGs).

También, RPL está pensado para ser usado en redes con bastantes nodos, los cuales tendrán recursos limitados y las redes estarán “manejadas” por uno o pocos “supernodos” o border routers en el caso de 6LoWPAN.

#### Seguridad

Al ser IEEE 802.15.4 un protocolo de capas de enlace y física inalámbricas, será conveniente disponer de un protocolo de seguridad en la capa de enlace. IEEE 802.15.4 usa el Estándar de Encriptación Avanzado (AES por sus siglas en inglés) en el Contador con modo CBC-MAC. El problema está en que esto solo cubre el segmento del enlace que lo usa, pero no tiene seguridad end-to-end. Para asegurar dicha seguridad end-to-end, como en Internet, se necesita añadir medidas en las capas altas como en las capas de red y de aplicación.

Para la capa de red, se ha propuesto el protocolo IPSec adaptado para soportar 6LoWPAN y prometiendo seguridad end-to-end.

En la capa de aplicación, el protocolo principal como candidato es el DTLS o *Datagram Transport Layer Security*. Al contrario de TLS, que trabaja en TCP, DTLS trabaja en UDP, el cuál es adecuado para redes limitadas como es el caso de 6LoWPAN.

#### Protocolos de aplicación

Actualmente hay muchos protocolos de aplicación disponibles para 6LoWPAN, pero los dos más populares son Constrained Applicacion Protocol (CoAP) y Message Queuing Telemetry Transport-Sensor Network MQTT-SN.

Debido a la popularidad de los servicios web, se desarrolló CoAP como un HTTP ligero para 6LoWPAN. Al ser dispositivos con limitaciones, se usa UDP con un sistema propio de retransmisión basado en mensajes. Se usa UDP en vez de TCP debido al menos uso de recursos. CoAP tiene arquitectura REST, debido a que requiere muchos menos recursos y permite a los desarrolladores Web programar para IoT. Entre CoAP y HTTP es fácil traducir mediante dispositivos proxy. CoAP también permite trabajar con medidas de seguridad como DTLS.

MQTT-SN, usa igualmente UDP, pero al contrario que CoAP, MQTT es un protocolo ligero de publicador-suscriptor. Este sistema desengancha productores y consumidores, por lo que es necesario un intermediario.

### Retos de 6LoWPAN

Debido a las limitaciones de recursos que tienen los nodos, como de energía, memoria y potencia de procesamiento, hay varios retos a la hora del diseño e implementación de 6LoWPAN, puesto que este implementa IPv6. Algunos de los principales retos son:

* **Sobrecarga de cabecera:** La capa de enlace en 6LoWPAN tiene una Unidad Máxima de Transferencia (MTU) de 127 bytes, mientras que la MTU de IPv6 es de al menos 1280 bytes con una cabecera de 40 bytes. Esto implica que transmitir directamente los paquetes IPv6 es ineficiente debido al alto ratio cabecera/payload y se generan frecuentes fragmentaciones y desfragmentaciones.
* **Neighbor Discovery Protocol:** IPv6 usa este protocolo NDP, el cual se encarga de reconocer a los diferentes equipos cercanos en la red, para configurarse solo combinando la información del prefijo de la red con el mensaje de anuncio del router y el ID del host de la dirección de su capa de enlace. Esto formará una dirección de 128 bytes. NDP ayuda bastante en 6LoWPAN debido a que simplifica enormemente la asignación de direcciones IP a muchos dispositivos. A pesar de esto, el protocolo está aún en proceso de adaptarse para redes limitadas.
* **Redes con pérdidas:** Debido a la movilidad, las interferencias, etc, estas limitadas redes, con enlaces inalámbricos, no son muy fiables. Esto implica un reto en el enrutamiento debido a que se requiere una relativamente estable y lentamente variable topología de red.
* **Seguridad:** En todo tipo de redes, la seguridad siempre es un asunto importante. En redes estándar TCP/IP, se usa seguridad end-to-end, como es el caso de IPSec en la capa de red o en Transport Layer Security (TLS) en la capa de aplicación.

### Implementaciones y aplicaciones para 6LoWPAN [5], [7]

Actualmente, hay numerosas implementaciones de código abierto para 6LoWPAN. Las más populares son: Contiki, TinyOs, Linux y Thread (en especial el software OpenThread desarrollado por Google).

#### Contiki

Contiki es un sistema operativo hibrido basado en Unix. Contiki es de código abierto, muy portable y con capacidad de multitarea y control de eventos, el cuál fue pensado para una eficiencia en memoria en sistemas de redes embebidos y redes de sensores inalámbricos. Puede estar en nodos con capacidades de memoria tan baja como 20 KB en RAM y 100 KB en ROM. Contiki permite comunicaciones IP, pudiendo tanto IPv4 e IPv6.

Gracias a la multitarea y manejo de eventos, se soporta una carga dinámica y reemplazamiento de servicios o programas individualmente. La arquitectura utilizada es la mostrada en la siguiente imagen:

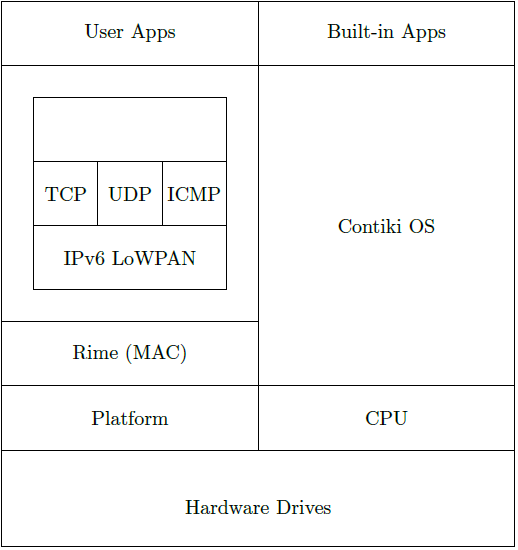


Ilustración Arquitectura en Contiki [7]

#### TinyOS

Otro sistema basado en Unix, pensado para dispositivos limitados y de baja potencia. TinyOs 2.X soporta 6LoWPAN gracias a BLIP (*Berkeley Low-power IP stack).* BLIP es la pila de 6LoWPAN más avanzada en cuanto a funcionalidades. Implementa las características básicas definidas en RFC4844, como compresión de la cabecera, fragmentación y direccionamiento, incluyendo también ICMPv6 y paquetes UDP. BLIP implementa también *Descubrimiento de vecinos o Neighbor Discovery*, en una versión reducida, configurar una dirección local de enlace en el arranque de los nodos y una dirección global si se recibe el anuncio del enrutador.

En comparación con versiones anteriores, BLIP soporta redes de malla.

#### Thread

Ver [apartado 2.3.](#_THREAD)

## THREAD

Thread es una especificación IoT gratuita, con redes en malla, basada en 6LoWPAN y en IPv6 [8]. Esta ha sido desarrollada por empresas como Samsung, Google y muchas otras grandes compañías. Como se indica en la especificación THREAD [9], este protocolo es un estándar abierto para comunicaciones inalámbricas dispositivo a dispositivo, económico, de baja potencia y fiable. [7]

### Introducción a Redes THREAD [8], [10]–[12]

Thread está específicamente diseñado para ambientes donde es necesario o deseado una red basada en comunicaciones IP y, además, se permite una variedad de capas de aplicación a ser usadas.

Las características generales del protocolo y las redes Thread son [10]:

* **Simplicidad.** La instalación de la red, la puesta en marcha y la operativa son muy simples. Esto se debe a que los protocolos fluidos para formar, unir y mantener una red Thread permiten una autoconfiguración y arreglar problemas de enrutado a la vez que ocurren.
* **Seguridad.** No se permite unirse a dispositivos a una red Thread si no están autorizados. Todas las comunicaciones están encriptadas y seguras.
* **Redes pequeñas y grandes.** La cantidad de nodos conectados puede variar entre unos pocos y cientos de dispositivos comunicándose sin problemas. Esto se debe a que la capa de red está diseñada para optimizar el uso de la red en función del uso esperado.
* **Rango.** Los típicos dispositivos junto con una red en malla pueden dar rango suficiente para cubrir una casa. La tecnología de propagación del espectro, se usa en la capa física para tener una buena inmunidad a interferencias.
* **Sin fallos.** La pila del protocolo está diseñada para dar operar segura y fiablemente incluso con fallos o perdidas en dispositivos individualmente.
* **Baja potencia.** Los dispositivos suelen operar durante años con baterías tipo AA gracias al uso de un ciclo duty ajustado.

### Tipos de dispositivos

En estas redes, hay 2 clasificaciones para los posibles tipos de nodos que puede haber en la propia red.

Para una topología básica tendríamos los siguientes tipos de dispositivos: [8], [10]

* **Border Routers.** Es un router específico que da conectividad desde redes 802.15.4 a redes adyacentes en otras capas físicas, como Wi-Fi o Ethernet. Da servicio a los dispositivos dentro de la red, incluyendo servicio de enrutamiento para operaciones fuera de red.
* **Routers.** Estos se encargan de dar servicios de enrutamiento a los distintos dispositivos de red. También se encargan de servicios de seguridad y de unión a los diferentes dispositivos que quieran unirse a la red. Estos routers, no están pensados para un modo “dormido”. Pueden degradar su funcionalidad y convertirse en REEDs (Router-Eligible End Devices).
* **Router-Eligible End Devices.** Estos REEDs pueden convertirse en Routers, pero acorde a la topología o condiciones de la red, no actúan como Routers. Estos dispositivos, por lo general, no reenvían mensajes ni dan servicios de unión y seguridad para otros dispositivos dentro de la red Thread. Su cambió a Routers es manejado por la propia red automáticamente sin necesidad de un usuario.
* **Sleepy End Devices.** Son dispositivos anfitriones o Host de la red. Solo se pueden comunicar a través de su Router Padre, y no pueden reenviar mensajes para otros dispositivos. Pueden operar con muy bajo consumo ya que receptor está desactivado y solo se despierta periódicamente para comunicarse con su padre.

Desde el punto de vista de funcionalidad, se podrían agrupar los dispositivos Thread en dos diferentes tipos, y dentro de cada tipo, cada dispositivo puede adoptar ciertos roles. Estos dos principales tipos son:

* **Full Thread Device (FTD).** Puede comunicarse con otros dispositivos bidireccionalmente y con los nodos hijos (MTD) unidos a él. Estos dispositivos pueden adquirir los siguientes roles:
  + **Leader:** Es el dispositivo Thread responsable del manejo de la asignación de ID de router. Es el único dispositivo en una partición de red Thread que actúa como árbitro central y distribuidor del estado de configuración de la red.
  + **Border Router. (**Misma funcionalidad comentada en la primera clasificación.)
  + **Active Router.** (Misma funcionalidad comentada en la primera clasificación.)
  + **REEDs.** (Misma funcionalidad comentada en la primera clasificación.) Pueden tener varios nodos hijos y mantener enlaces con los Routers vecinos.
  + **Full End Device (FED).** Es un FTD normal, que siempre actuará como un Dispositivo Final (End Device – ED). Un dispositivo FED nunca pedirá convertirse en Router, como haría un REED.
* **Minimal Thread Device (MTD).** Estos dispositivos solo pueden comunicar con el padre FTD al que están unidos. Los roles que pueden adquirir son:
  + **Minimal End Device (MED).** Es un dispositivo MTD cuyo receptor está habilitado todo el tiempo y puede comunicarse con su nodo padre en cualquier momento.
  + **Sleepy End Device.** **(**Misma funcionalidad comentada en la primera clasificación.)

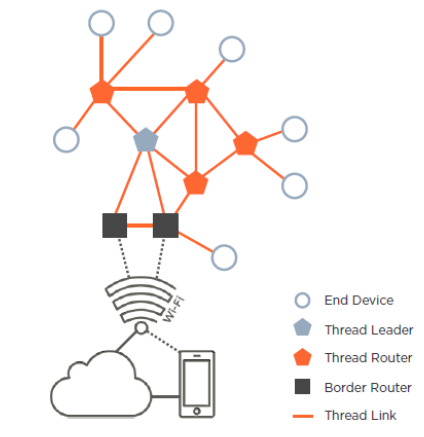


Ilustración Ejemplo de una topología de Red Thread en malla [9]

Un Router o un Border Router puede asumir el rol de líder para ciertas funciones dentro de la red Thread. Este líder tendrá que tomar decisiones dentro de la red, como asignar las direcciones de los Routers y permitir nuevas solicitudes de Routers. Si el nodo Líder se falla, un nodo Router o Border Router asumirá ese rol de manera automática, asegurando así ningún punto singular de fallo.

### Protocolo Thread

En este apartado describiremos la pila del protocolo Thread con las diferentes capas que la integran, las cuales podemos ver en *Ilustración 4*:

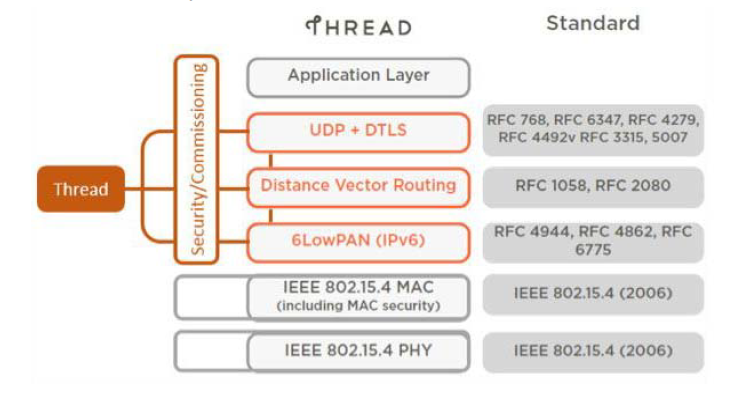


Ilustración Pila de Protocolo Thread en un sistema IoT [12], [13]

#### Redes de área Privada - Private Area Network (PAN) [12]

Las redes de área privada (PAN) son redes de área local, las cuáles incluyen hardware de comunicaciones y de computación, junto con sensores y actuadores. Estas redes se conectan al resto de Internet gracias a los Gateways o puertas.

Antes de que un dispositivo pueda unirse a una PAN, este debe ser puesto dentro del servicio o ser “oficial” dentro de la red. En caso del protocolo Thread, para este proceso de puesta en servicio o *commissioning,* se usa *MeshCoP* (Mesh Commissioning Protocol). Este protocolo MeshCoP permite a una red de malla una segura autenticación, puesta en servicio y la unión de nuevos dispositivos desconocidos. Más adelante se entrará más en detalle de este protocolo.

Un ejemplo de una PAN Thread se muestra en la Ilustración 5:

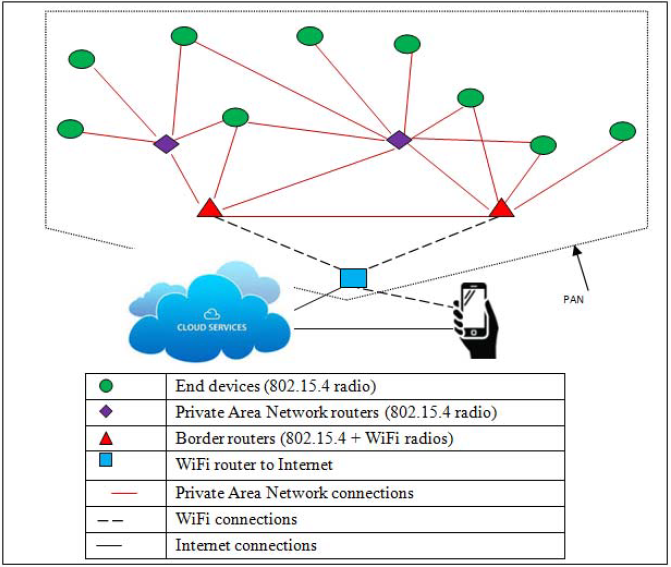


Ilustración Ejemplo PAN Thread [12], [13]

Las redes PAN que usen el protocolo Thread tendrán las siguientes características:

* **Nodos.** Las redes Thread se componen de nodos. Cada dispositivo o nodo tendrá unas determinadas características, unos darán conectividad a Internet a la PAN, otros solo podrán trasmitir a su vecino más cercano, otros podrán mandar datos de un nodo a otro. Los distintos tipos de dispositivos o nodos posibles son los vistos la sección [2.3.2. Tipos de dispositivos](#_Tipos_de_dispositivos).
* **Topología.** Uno de los requerimientos para las PAN Thread es no tener un punto singular de fallo. Para esto, Thread ha escogido una topología de red enmallada o de malla para sus redes PAN. El motivo de esta topología es su alta resiliencia, escalabilidad, robustez y una habilidad de auto reparación en caso de fallo de algún componente.
* **Enlaces de comunicación.** Para estos enlaces de la red, las redes PAN Thread usan radios inalámbricas. Estas radios inalámbricas trabajan en la frecuencia de 2450 MHZ y se basan en el estándar IEEE 802.15.4. Se detallará más en profundidad posteriormente.
* **Enrutamiento.** Cada nodo puede transmitir al nodo vecino más cercano, por lo que, si el destinatario no es ese nodo cercano, se enviarán los datos a través de múltiples nodos. Estos enlaces se configuran automáticamente por el software Thread. Se detallará más en profundidad posteriormente.
* **Identificación de dispositivos.** Cada nodo en una red PAN Thread tiene una dirección IPv6, la cual es comprimida con 6LoWPAN. Se detallará más en profundidad posteriormente.
* **Transmisión de datos.** Todos los enlaces de datos son encriptados en la capa de Enlace y/o en la capa de Transporte.
* **Recursos informáticos.** Todos los nodos necesitan alguna forma de computación, para formar los paquetes de datos, encriptación/desencriptación de datos, realizar la transmisión, etc.
* **Servicio ubicuo.** Se ofrece a sus usuarios un servicios siempre disponible.
* **Semántica.** Se analiza vía software, en la nube, los sensores y los datos de entrada, junto con el resto de información y se da una respuesta basada en contexto para el sistema IoT.
* **Gateways.** Las redes PAN Thread, pueden disponer de múltiples gateways, como los border routers, para conectarse a Internet. Añaden redundancia y eliminan puntos de fallo. Estos Border Routers pueden conectarse tanto vía radio al resto de nodos como vía cable o inalámbrica a Internet o al servidor en la nube.

Todas estas características están diseñadas bajo estas cinco restricciones:

* **Bajo consumo.** Debido a que mucho de los dispositivos están conectados a baterías, y el alargar la vida de dicha batería es un deber. Incluso si estuvieran conectados a la red eléctrica, si no son de bajo consumo, puede generarse un considerable gasto debido a la gran cantidad de componentes.
* **Bajo coste.** Es importante que el sistema tenga dispositivos bajo coste y de bajo coste de mantenimiento, si lo que se quiere es un sistema ubicuo.
* **Seguridad.** Es importante mantener la seguridad de la PAN y de la nube.
* **Interfaz de usuario.** Los dispositivos IoT suelen carecer de interfaz de usuario, por lo que será de gran utilidad que estos dispositivos tengan la facilidad de conectarse a dispositivos con una buena GUI, como un ordenador.
* **Retos de comunicación.** Estas redes PAN, trabajan en interiores, donde suele haber bastantes obstáculos para la comunicación. Aparte, esos obstáculos, pueden variar su posición, al igual que pueden hacerlo los dispositivos, aparecen nuevos dispositivos y los viejos desaparecen. Varios dispositivos móviles pueden salir y reunirse a la red sin ser notificados. Thread usa DTLS para poder solventa este tipo de comunicaciones poco fiables. DTLS asume una capa de Transporte poco fiable. Debido al bajo consumo, la señal de comunicaciones es débil, por lo que lo complica más, por lo que una de las medidas tomadas es el envío de paquetes pequeños y con redundancia para tener cierta tolerancia a errores.

#### Capa Física [12], [14]

Los dispositivos Thread soportan una interfaz cumpliendo las especificaciones definidas en IEEE 802.15.4 relativos a los 2450 MHz. Thread también usa modulación O-QPSK y tiene una tasa de datos de 250 kbps. Las señales de radio de Thread pueden alcanzar un salto máximo de 30 metros entre nodo y nodo, pudiendo dar hasta un máximo de 36 y conectando hasta más de 250 dispositivos en una PAN.

#### Capa MAC (o enlace de Datos). [12], [14]

Otra parte por implementar de la especificación IEEE 802.15.4 en los dispositivos Thread es un conjunto de Control de Acceso a los Medios (Media Access Control – MAC). Dependiendo de si el dispositivo tiene o no capacidad de enrutamiento, los dispositivos tendrán que funcionar como un dispositivo MAC conmpleto (MAC Full Function Device – FFD) o como un dispositivo MAC reducido (MAC Reduced Function Device – RFD).

Las capacidades MAC que debe de tener un dispositivo Thread son:

* Uso de Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA).
* Tener tipos de escaneo activo y de detección de Detección de Energía (ED).
* Ser capaz de generar y recibir los siguientes paquetes / Frames MAC.
  + Paquetes de datos MAC y de Acknowledgement.
  + Paquetes de solicitud de datos y de solicitud del Beacon.
  + Paquete Beacon cuando se recibe solicitud de FFD.
* Dar un enlace fiable entre dos entidades MAC.
* Implementar paquete de seguridad MAC basado en la configuración de la PAN.

Por otro lado, los dispositivos Thread MAC no se les permite:

* Operar con un modo periódico de Beacon activado.
* Garantizar mecanismos de espacios de tiempo.
* Generar o implementar los siguientes paquetes de comandos:
  + Solicitud de Asociación.
  + Respuesta a Asociación.
  + Solicitud de Desasociación, conflicto con PAD ID.
  + Notificación de huérfanos.
  + Realineación de Coordinadores.
  + Modo Coordinador de PAN FDD.
* Direccionamiento 00 para paquetes de Datos o comandos MAC.
* Cualquier otro paquete de opciones de seguridad, excepto las mencionadas en la configuración de la PAN.

El datagrama que hace el Establecimiento del Enlace MAC (MLE) puede ser o no seguro. Para un MLE seguro, se indica con un byte inicial de valor 0, seguido de un byte de cabecera auxiliar, mientras que cuando no es seguro, el valor del byte inicial es 255 y no tiene ningún byte de cabecera auxiliar.

En Thread hay 18 MLE datagramas de comandos genéricos disponibles, los cuales tratan varios aspectos de establecer enlaces, solicitudes de datos, enrutamiento y descubrimiento de nodos vecinos. Estos comandos MLE pueden ser secuenciados para tareas de alto nivel.

La estructura del paquete MAC de IEEE 802.15.4-2006 (sección 7.2.1) [15] es la siguiente:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FC | SQ | DstPID | Dst | SrcPID | Src | AuxSec | UD | FCS |

Tabla MAC Layer Frame

* **FC** 🡪 Frame Control (2 bytes).
* **SQ** 🡪 Sequence number (1 byte).
* **DstPID 🡪** Destination PID (0/2 bytes).
* **Dst 🡪** Destination Address (0/2/8 bytes).
* **SrcPID 🡪**  Source PAN ID (0/2 bytes).
* **Src 🡪** Source Address (0/2/8 bytes).
* **AuxSec 🡪** Auxiliary Security Header (0/5/6/10/14 bytes). Contiene también los campos de Control de Seguridad (Security Control), un contador de paquete (Frame Counter) y un Identificador de Clave (Key Identifier).
* **UD 🡪** User data (variable bytes).
* **FCS 🡪** ITU-T-CRC-16 (2 bytes).

#### Capa de adaptación 6LoWPAN [12]

Thread usa IPv6 over Low-power Wireless Personal Area Network o 6LoWPAN, según se especifica en RFC 4944 [16] y RFC 6282 [17]. 6LoWPAN permite el uso de IPv6 dentro de las PAN, a pesar de que Thread las implementa con unas restricciones menores. Esta capa permite la fragmentación y el reensamblaje de los paquetes IPv6 procedentes y destinados a la capa MAC.

Esta capa está diseñada para llevar el datagrama con enlaces restringidos, como el estándar IEEE 802.15.4, con anchos de banda limitados, pequeñas memorias, bajas potencias de consumo y transmisiones de un máximo de 250 kbps.

IEEE 802.15.4 especifica una MTU, unidad máxima de transmisión, de 127 bytes, de los cuales 80 octetos de los habilitados en la payload de la MAC están disponibles. 6LoWPAN también permite un encabezado de dirección de la malla admitiendo el reenvío sub-IP.

Debido a la compresión de cabecera en datagramas IPv6, 6LoWPAN reduce bastante las cabeceras IPv6 y UDP a tan solo unos bytes [17].

#### Capa de Red [12]

Los dispositivos Thread deben implementar la especificación IPv6, RFC 2460 [18], al igual que la arquitectura de direccionamiento IPv6, RFC 4291 [19]. Thread usa dos campos para el direccionamiento.

* Enlace Local, el cuál es accesible en una transmisión de radio.
* Ámbito Local, el cuál es accesible dentro de la PAN mediante saltos.

Los dispositivos Thread deben admitir una dirección de enlace local y al menos dos direcciones de Ámbito Local para uso de comunicaciones internas a la PAN. Si hay disponibilidad de recursos, los dispositivos Thread podrían admitir direcciones IPv6 adicionales como la Unique Local Address (ULA) y la Global Unique Address (GUA). También deberán soportarse también direcciones Multicast de Enlace Local y de internas de la malla.

Las direcciones Unicast IPv6 son usadas para el uso interno de la malla. Las Unicast pueden ser localizadores de enrutamientos, localizador de cualquier tipo (Líder, DHCPv6, Servicio, Commision, Descubrimiento de Vecinos) o incluso Identifcador de Punto Final (EID – Endpoint Identifier).

Las redes Thread no depende del Protocolo de Configuración de Host Dinámico v6 (DHCPv6), por lo que los dispositivos no tendrán que implementarlo. Lo que si que deberán implementar es el Protocolo para Control de Mensajes Internet (ICMPv6), RFC 4443 [20].

##### Protocolo de Enrutamiento

Para el enrutamiento, Thread usa un simple protocolo de enrutamiento por vector de distancia. El enrutamiento dentro de la PAN está basado en RIPng (estándares RFC 2080 y RFC 1058). Los rúters de la PAN envían periódicamente sus “costes” de enrutamiento a todos los demás rúters junto con la calidad de enlace de un salto. Los costes de enrutamiento para un mensaje se sacarán de este último dato.

Cada rúter crea y mantiene una base de datos con los enrutamientos por cada interfaz que usa enrutamientos por distancias. Estas bases contienen:

* Id del rúter.
* Enlace
* Ruta

Los rúters de la PAN mantienen un seguimiento de la versión Thread de los enlaces de sus hijos y, de manera proactiva, manda actualizaciones de versiones más nuevas. Además, si el rúter es un nodo Leader, este tiene una base de datos con las asignaciones de id. Los rúters Lideres recogen, comparan y distribuyen la información sobre los Border Routers y otros servidores disponibles para la red Thread vía MLE.

Thread tiene el concepto de set completo y de set estable de nodos de red. Las redes Thread se pueden dividir en diferentes sets para romper las comunicaciones. Por lo tanto, se incluye una provisión para que cada set actúe como una red diferente, pudiendo unirse luego como una sola red. Si no hay un nodo Líder alcanzable o disponible, un REED o un Border Router pueden generar una nueva partición en la red.

#### Capa de Transporte [12]

Esta capa de transporte en Thread está basada en User Datagram Protocol (UDP), descrito en RFC 768 [21], y en Requerimientos para Host De Internet, RFC 1122 [22].

Para el protocolo de mensajería, Thread usa Constrained Application Protocol (CoAP) [23], [24] debido a las limitaciones de baja memoria y de baja capacidad de procesamiento. El protocolo usado por CoAP es un UDP, que obliga a usar DTLS (Datagram Transport Layer Security)., RFC 6347 [25].

CoAP tiene un conjunto de modos de seguridad y de implementación obligatoria cifrados. CoAP toma prestado algunos conceptos del protocolo Representational State Transfer (REST). Los modos en los que opera CoAP son:

* Modo sin seguridad (“no security”).
* Modo Clave Pre-Compartida (“Pre-shared key”).
* Modo Certificado (“certificate”).

CoAPs (CoAP seguro) puede también configurarse en el modo “raw public key”, definido en RFC 7250 [26]. En el modo de Clave Pre-Compartida, CoAP junta claves Pre-Compartidas con una lista de los correspondientes nodos de comunicación. En cuanto al modo Certificado, esta muy bien establecido, pero se desaconseja su uso debido a las limitaciones de recursos.

El modo sin seguridad es solo recomendable cuando en la capa de Enlace de Datos hay encriptación disponible y en uso.

Thread usa encriptación DTLS en la capa de Transporte en caso de que el hardware no soporte la encriptación de los datos. Otra posibilidad es una doble encriptación, tanto en la capa de transporte como en la de enlace de datos, lo cual reduce el ratio de compresión, dejando paso a su vez a más transmisiones de paquetes y potencias consumidas mayores-

#### Seguridad y Comisión de dispositivos [10], [12]

Para dicha comisión Thread usa MeshCoP (Mesh Commissioning Protocol), el cual permite una autenticación, una comisión y una unión a la red de nuevos dispositivos desconocidos a la red de manera segura.

Una PAN Thread es una malla de dispositivos autónoma que se autoconfigura con la interfaz y la capa de enlace a nivel de seguridad de IEEE 802.15.4. Cada dispositivo de la PAN debe poseer una clave maestra secreta compartida y actualizada.

Para añadir a la PAN un dispositivo, primero habrá que autenticarlo manualmente como un dispositivo elegible para unirse a la red, prosiguiendo con la comisión del dispositivo y compartiéndole la clave maestra de la PAN a través de un canal seguro.

Los dos principales métodos para la comisión que tiene Thread son:

* Usando el método Out-of-band, configurar directamente sobre el dispositivo toda la información necesaria para la comisión. Esta información permitirá a los dispositivos que quieran unirse, que se unan a la red Thread correcta.
* Establece una sesión de comisión entre un aplicación de comisión, ya sea en web, teléfono móvil, etc y el dispositivo que se quiere unir. Esta aplicación de comisión le da la información necesaria al dispositivo para que se conecte a la red adecuada.

Antes de que un dispositivo sea autenticado, el propio Comisario deberá autenticarse también. Para ello se establece una conexión socket cliente/servidor, la cuál se le llamará Sesión de Comisión y sucede entre el Comisario y el propio Border Router (BR) usando DTLS (RFC 6347 [25]) o TLS (RFC 5246 [27]). Esta sesión abierta usa un determinado puerto UDP y se usa una credencial conocida como Pre-Shared Key for Commissioner. Tras terminar esta autenticación, el Comisario se registra con el BR, y este último comparte la información del Comisario al Nodo Leader, el cuál procederá a aceptar o rechazar al Comisario. En caso de ser aceptado el Comisario, el Líder manda su información a los Joiner Routers (JR) de la PAN.

Cuando un dispositivo desea unirse a la PAN, se le llama Joiner Device (JD). Para unirse a la PAN, el JD debe enviar mensajes de Descubrimiento Solicitud/Respuesta usando MLE en modo inseguro a un JR. Antes de que el tiempo de unión expire y si la unión de dispositivos a la red está activada, el JR deberá enviar una Respuesta de Descubrimiento con un puerto UDP de unión. Si no está activada la unión de dispositivos a la red, no se enviará ninguna respuesta. Tras recibir este mensaje de Respuesta, la unión del JD se dará por validada.

Una vez en la red, el JD mandará un saludo vía DTLS al JR, estableciendo con él una Joiner Session (JS). El JR mandará mensajes UDP al BR, el cuál los transmitirá al Comisario. A pesar de manejar estos mensajes, ni el BR ni el JR tienen acceso al contenido de los mensajes, solo los transmiten al puerto UDP indicado. Para afianzar una confianza entre dispositivos, hay un intercambio de mensajes entre el JD y el Comisario.

El Comisario chequea el Identificador de Interfaz del JD (IID) y sus credenciales y si todo está correcto, el JD recibirá con los datos y los servicios apropiados, a la vez que comparte su Key Encryption Key (KEK) y finalmente se cierra la JS.

Finalmente, el Comisario enviará una señal al JR que al JD se le compartirán las credenciales de la red. Finalmente, el Comisario le proporciona un secreto compartido entre JD y JR, completando así la unión del JD.

# OBJETIVOS

# MÉTODOS Y EQUIPO

# EXPERIMENTOS

# RESULTADOS Y ANÁLISIS

# CONCLUSIONES

# LINEAS FUTURAS

# PLANIFICACIÓN TEMPORAL Y PRESUPUESTO

# BIBLIOGRAFÍA

[1] S. Li, L. Da Xu, and S. Zhao, “5G Internet of Things: A survey,” *J. Ind. Inf. Integr.*, vol. 10, no. February, pp. 1–9, 2018.

[2] R. M. Gomathi, G. H. S. Krishna, E. Brumancia, and Y. M. Dhas, “A Survey on IoT Technologies, Evolution and Architecture,” *2nd Int. Conf. Comput. Commun. Signal Process. Spec. Focus Technol. Innov. Smart Environ. ICCCSP 2018*, no. Icccsp, pp. 1–5, 2018.

[3] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[4] A. J. Albarakati, J. Qayyum, and K. a. Fakeeh, “A Survey on 6LowPAN & its Future Research Challenges,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 10, pp. 558–570, 2014.

[5] Y. Chen *et al.*, “6LoWPAN stacks: A survey,” *7th Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2011*, pp. 6–9, 2011.

[6] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, no. c. 2009.

[7] Z. Yang and C. H. Chang, “6LoWPAN overview and implementations,” *Proc. 2019 Int. Conf. Embed. Wirel. Syst. Networks*, pp. 357–361, 2019.

[8] W. Rzepecki, L. Iwanecki, and P. Ryba, “IEEE 802.15.4 thread mesh network - Data transmission in harsh environment,” *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2018*, pp. 42–47, 2018.

[9] Thread Group, “Thread 1.1. 1 Specification.” Thread Group, 2017.

[10] Kirale, “KTWM102 Thread NCP module.” pp. 1–17.

[11] Kirale, “Kirale Command-Line Shell,” 2019.

[12] I. Unwala, Z. Taqvi, and J. Lu, “Thread: An IoT protocol,” *IEEE Green Technol. Conf.*, vol. 2018-April, pp. 161–167, 2018.

[13] J. Gopaluni, I. Unwala, J. Lu, and X. Yang, “Implementation of GUI for open thread,” *Proc. - 2018 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2018*, pp. 1015–1018, 2018.

[14] I. Unwala, Z. Taqvi, and J. Lu, “IoT security: ZWave and thread,” *IEEE Green Technol. Conf.*, vol. 2018-April, pp. 176–182, 2018.

[15] “IEEE Standards, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low- Rate Wireless Personal Area Networks (WPANs), IEEE Std 802.15.4,” 2006.

[16] “RFC 4944, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks",” 2007. [Online]. Available: https://tools.ietf.org/html/rfc4944.

[17] “RFC 6282 ‘Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,’” 2019. [Online]. Available: https://tools.ietf.org/html/rfc6282.

[18] “RFC 2460 ‘Internet Protocol, Version 6 (IPv6) Specification,’” 1998. .

[19] “RFC 4291 ‘IP Version 6 Addressing Architecture,’” 2006. [Online]. Available: https://www.ietf.org/rfc/rfc4291.

[20] “RFC 4443 ‘Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,’” 2006. [Online]. Available: https://tools.ietf.org/html/rfc4443.

[21] “RFC 768 ‘ User Datagram Protocol,’” 1980. [Online]. Available: https://tools.ietf.org/html/rfc768.

[22] “RFC 1122 ‘Requirements for Internet Hosts -- Communication Layers,’” 1989. [Online]. Available: https://tools.ietf.org/html/rfc1122.

[23] M. B. Tamboli and D. D. Ambawade, “Secure and efficient CoAP based authentication and access control for internet of things (IoT),” *2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc.*, pp. 1245–1250, 2017.

[24] C. Bormann, A. P. Castellani, and Z. Shelby, “CoAP: An application protocol for billions of tiny internet nodes,” *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, 2012.

[25] “RFC 6347 ‘Datagram Transport Layer Security Version 1.2,’” 2012. [Online]. Available: https://tools.ietf.org/html/rfc6347.

[26] “RFC 7250 ‘Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS),’” 2014. [Online]. Available: https://tools.ietf.org/html/rfc7250.

[27] “RFC 5246 ‘The Transport Layer Security (TLS) Protocol Version 1.2,’” 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246.