

Grado en Ingeniería Electrónica y Automática
Industrial



Trabajo Fin de Grado

Diseño de controlador Z-Wave de bajo coste

Autor: Sergio Elvira Carrasco
Tutor: Fco. Javier Acevedo Rodríguez

UNIVERSIDAD DE ALCALÁ
Escuela Politécnica Superior

Grado en Ingeniería Electrónica y Automática Industrial

Trabajo Fin de Grado

Diseño de controlador Z-Wave de bajo coste

Autor: Sergio Elvira Carrasco

Tutor: Fco. Javier Acevedo Rodríguez

TRIBUNAL:

Presidente: Sergio Lafuente Arroyo

Vocal 1º: Silvia Jiménez Fernández

Vocal 2º: Fco. Javier Acevedo Rodríguez

FECHA:.....

Índice

| | |
|--|-----------|
| Índice | I |
| Índice de imágenes..... | III |
| Índice de código | V |
| 1. Resumen | 1 |
| 2. Abstract..... | 3 |
| 3. Palabras Clave (Keywords)..... | 5 |
| 4. Resumen extendido | 7 |
| 5. Memoria | 9 |
| 5.1 Introducción..... | 9 |
| 5.1.1 Planteamiento y objetivos | 11 |
| 5.1.2 Estructura de la memoria..... | 12 |
| 5.2 Marco teórico..... | 13 |
| 5.2.1 Breve revisión de la evolución de la domótica | 13 |
| 5.2.2 Estudio de los diferentes protocolos que existen..... | 15 |
| 5.3 Protocolo Z-Wave..... | 22 |
| 5.3.1 Estudio del protocolo Z-Wave..... | 22 |
| 5.3.2 Estudio de los controladores que existen actualmente en el mercado | 29 |
| 5.4 Diseño del controlador Z-Wave..... | 34 |
| 5.4.1. Instalación de Raspbian en Raspberry | 35 |
| 5.4.3 Instalación del módulo Z-Wave..... | 42 |
| 5.4.3. Instalación software Domoticz..... | 51 |
| 5.4.4. Adaptación de Z-Way con Domoticz..... | 55 |
| 5.5 Conexión a la Raspberry Pi y al control domótico a distancia..... | 61 |
| 5.5.1 Configuración de Router y puertos | 63 |
| 6. Conclusiones y líneas futuras | 66 |
| 7. Resumen económico..... | 68 |
| 8. Manuales de usuario | 70 |
| 9. Bibliografía..... | 74 |

Índice de imágenes

| | |
|--|----|
| Figura 1. Tabla con número de Partners por países | 14 |
| Figura 2. Logo del protocolo de comunicación KNX | 15 |
| Figura 3. Logo del protocolo de comunicación X10..... | 16 |
| Figura 4. Logo del protocolo de comunicación ZigBee | 18 |
| Figura 5. Logo del protocolo de comunicación EnOcean..... | 19 |
| Figura 6. Logo del protocolo de comunicación Bluetooth | 20 |
| Figura 7. Logo del protocolo de comunicación Z-Wave | 21 |
| Figura 8. Ejemplo gráfico de la NWI | 23 |
| Figura 9. Tabla de frecuencias ISM de trabajo del protocolo Z-Wave..... | 23 |
| Figura 10. Ejemplo de protocolo de comunicación..... | 26 |
| Figura 11. Tabla comparativa Z-Wave Vs resto principales protocolos | 28 |
| Figura 12. Fibaro Home Center Lite (FGHCL) | 29 |
| Figura 13. Fibaro Home Center 2 (FGHC2)..... | 30 |
| Figura 14. Eedomus Plus | 30 |
| Figura 15. Logotipo sistema JEEDOM..... | 31 |
| Figura 16. Vera Plus (izq.) y Vera Secure (der.) | 32 |
| Figura 17. Controlador Piper..... | 33 |
| Figura 18. Zipabox (izq.) y Zipatile (der.)..... | 33 |
| Figura 19. Raspberry Pi 3 Model B y módulo Z-Wave RazBerry..... | 34 |
| Figura 20. Logos de Raspberry y Raspbian..... | 35 |
| Figura 21. Pantalla principal de Raspbian | 36 |
| Figura 22. Página oficial de descargas de Raspberry | 37 |
| Figura 23. Centro de descargas de imágenes Raspbian..... | 38 |
| Figura 24. Centro de descargas de instalador NOOBS..... | 39 |
| Figura 25. Menú de instalación en NOOBS (v2.1)..... | 40 |
| Figura 26. Instalación de Raspbian | 40 |
| Figura 27. Ajuste de direcciones IP en el router..... | 43 |
| Figura 28. Ping a la dirección IP de la Raspberry para comprobar su conexión . | 44 |
| Figura 29. Estructura de funcionamiento de un sistema con Z-Way | 45 |
| Figura 30. Comparación RaZberry v1 (izq.) y v2 (der.)..... | 46 |
| Figura 31. Esquema de conexión GPIO de la Raspberry | 47 |
| Figura 32. Raspberry y RaZberry instalada..... | 47 |
| Figura 33. Añadir nuevos dispositivos desde Z-Way | 49 |
| Figura 34. Configuración del puerto al cual se conectará Domoticz | 52 |
| Figura 35. Configuración puerto HTTPS | 52 |
| Figura 36. Ruta de instalación Domoticz | 52 |
| Figura 37. Resumen de la instalación de Domoticz | 53 |
| Figura 38. Interfaz de usuario de Domoticz | 53 |
| Figura 39. Pasos para añadir Z-Way a Domoticz..... | 55 |
| Figura 40. Opciones para agregar, borrar o configurar los dispositivos Z-Wave | 56 |
| Figura 41. Ejemplo de configuración de parámetros de un dispositivo Z-Wave.. | 57 |
| Figura 42. Habilitar acceso desde otro controlador | 57 |
| Figura 43. Configuración acceso a otro controlador | 58 |
| Figura 44. Ejemplo de añadir cámaras IP..... | 58 |
| Figura 45. Configuración de notificaciones | 59 |
| Figura 46. Configuración de acciones HTTP para notificaciones | 59 |
| Figura 47. Ejemplo del LOG de un dispositivo | 60 |
| Figura 48. Ejemplo del LOG del software..... | 60 |
| Figura 49. Añadir servidor DDNS..... | 63 |
| Figura 50. Elección del domino DDNS | 63 |

| | |
|---|-----------|
| Figura 51. Configuración del servicio DDNS en el router | 64 |
| Figura 52. Configuración de puertos..... | 65 |
| Figura 53. Conexión remota a través de servidor de DNS dinámico..... | 65 |
| Figura 54. Configuración del apartado Settings del sistema Domoticz..... | 71 |
| Figura 55. Establecer los dispositivos como que van a ser usados | 72 |
| Figura 56. Selección de dispositivos favoritos..... | 72 |
| Figura 57. Escritorio con los diferentes dispositivos agregados..... | 72 |
| Figura 58. Ejemplo de parámetros configurables en un dispositivo..... | 73 |

Índice de código

| | |
|---|-----------|
| Código 1. Formatear memoria SD ya usada previamente..... | 41 |
| Código 2. Actualización del sistema | 42 |
| Código 3. Configuración IP fija en Raspberry | 44 |
| Código 4. Comandos para la instalación de Z-Way..... | 48 |
| Código 5. Deshabilitar inicio automático y Mongoose (Web server) | 50 |
| Código 6. Instalación de Domoticz..... | 51 |

1. Resumen

En este trabajo se desarrollará un controlador Z-Wave de bajo coste orientado a su instalación en viviendas, oficinas o edificios públicos, para poder controlar diferentes aspectos como puede ser la climatización, luminosidad y confort de cara al usuario final.

Actualmente existen diferentes y numerosos controladores de este tipo en el mercado, pero en su inmensa mayoría están los problemas de compatibilidad y el precio que estos suponen. La idea es que con un solo controlador, poder controlar todos los dispositivos que se quiera, sin estar limitados a solo controlar la luz o la climatización como ocurre actualmente con muchos productos en el mercado, además de poseer la característica de ser muy competitiva si se habla del precio de los diferentes controladores.

Para poder realizar el siguiente trabajo, nos basaremos en el protocolo de transmisión Z-Wave, protocolo ampliamente extendido a nivel mundial en lo que a domótica se refiere. Al tratarse de un protocolo que se podría definir como universal, hace posible que la pasarela diseñada sea compatible con un gran número de artículos disponibles en el mercado, lo que permite realizar instalaciones con dispositivos de un precio relativamente bajo y que con el tiempo seguirá bajando de precio según todas las previsiones.

En conclusión, el poder usar un controlador domótico que además se salga de los fabricados por las empresas permitirá poder ampliarlo en un futuro para añadir más opciones como es el poder controlar dispositivos de diferentes protocolos, dispositivos IP o hacer ampliaciones de funcionalidades en un futuro siguiendo trabajando sobre el controlador.

2. Abstract

In this project, we will develop a low-cost Z-Wave controller specifically orientated for use in domestic and office environments along with public buildings and public use buildings. The device will be able to automate building systems such as the heating, ventilation and air-conditioning systems, illumination (artificial and natural) and the general comfort of the end-user.

Numerous different systems exist commercially but the majority tend to suffer problems related with a lack of compatibility and high price. The intention is that a single controller could be created to activate and deactivate virtually all the devices that can be found in the aforementioned environments without being limited to switching just the lights, or air-conditioning, etc. which is exactly what happens with the majority of the products on the market. We will also try and address the pricing problem to be as competitive as possible.

To be able to complete this project we will be implementing the Z-Wave transmission protocol which is used extensively worldwide with regards to Home Automation. Being a protocol that could be defined as universal, it makes it possible for the designed gateway to be compatible with a large number of articles available in the market, allowing installations with devices of a relatively low price and that will eventually go down of price according to all forecasts.

In conclusion, the power of use of a domotic controller that compared to those manufactured by other companies, will allow to be expanded in the future to add more options such as the ability to control devices from different protocols, IP devices or make extensions of functionality in the future working on the controller.

3. Palabras Clave (Keywords)

Español:

Controlador domótico; Protocolo Z-Wave; Bajo coste; Climatización y luminosidad; Compatibilidad de distintas marcas.

English:

Home automation controller; Z-Wave Protocol; Low cost; Air conditioning and light; Different brands compatibility.

4. Resumen extendido

El trabajo aquí expuesto consiste en el diseño y programación de un entorno de control domótico de bajo coste, basándonos en dispositivos ya existentes en el mercado como puede ser una Raspberry y un adaptador Z-Wave con el cual poder comunicarse con los dispositivos a través de este protocolo. El principal objetivo que se busca con la realización de este trabajo es el de poder poner al alcance de todas las personas un controlador domótico con las ventajas que esto supone al usuario final: el poder controlar la climatización de una vivienda, una oficina o un edificio público, por poner algunos ejemplos, permite que se pueda ahorrar energía al adaptarse a las características de cada momento del lugar en el cual se han instalado los dispositivos que se quiera controlar. Estas características varían cada momento, por lo que el hecho de poder regularse por ellos mismos aporta un gran valor al ahorro energético del lugar donde se realiza la instalación.

A esto hay que añadir el poder controlar la iluminación de todas las salas que se quieran del mismo edificio, ayudando también al ahorro energético y al confort de cara al usuario final. Si se tiene en cuenta todo lo anteriormente mencionado, el confort energético puede ser muy elevado ya que, sobre todo en edificios públicos u oficinas donde la iluminación se encuentra encendida en situaciones donde es completamente innecesaria, al igual que la climatización, siendo esta última la responsable de un gran gasto energético y monetario. En las viviendas, el ahorro se puede ver influenciado sobre todo en la climatización, como por ejemplo en apagar la calefacción o el AC por la noche en caso de olvido para evitar que este gastando energía innecesaria, o al irnos de viaje evitar que se queden electrodomésticos como un radiador encendido,

Uno de los principales problemas con los que se puede encontrar durante la instalación de sistemas domóticos y de los dispositivos agregados es el montaje de todo el cableado necesario para su correcto funcionamiento, lo que según la obra o remodelación que se quiera realizar puede suponer un incremento enorme en el presupuesto final, sobre todo en edificios de vieja construcción. Con el proyecto aquí

propuesto, no solo se consigue diseñar un controlador Z-Wave de bajo coste, sino que además el protocolo en el que se basa (Z-Wave) facilita mucho la instalación y su coste, al poder transmitirse vía radio de forma inalámbrica. En la actualidad, aunque existen numerosos protocolos de comunicación inalámbrica, Z-Wave cuenta con diferentes ventajas como es la de ser un protocolo universal de facto, de bajo coste, sin sobreponerse sobre otras redes domésticas como puede ser el Wifi, y la facilidad para su uso.

También se deberá de tener en cuenta el alcance de los dispositivos vía radio, ya que al no tratarse de un sistema cableado con el cual el problema de la distancia se vería muy reducido, si se quieren realizar instalaciones largas habrá que tener en cuenta estos problemas, sin embargo, el motivo por el cual se ha escogido el protocolo Z-Wave es gracias a que cuenta con un sistema de comunicación a través de su red mallada ampliando en gran medida este alcance. Uno de los problemas de los sistemas de control domóticos realizados vía comunicaciones inalámbricas es la limitación en la cobertura de los dispositivos. Sin embargo, una de las ventajas que presenta Z-Wave para solucionar este problema es la posibilidad de extender el sistema de comunicación mediante el uso de una red mallado NWI.

Por último, se deberá tener en cuenta y se tratará el tema de la interfaz gráfica que se le ofrece al usuario (UI), la cual deberá de ser lo más simple posible, pero ofreciendo las capacidades de configuración necesarias para su completo uso. Se completará la instalación al usuario final ofreciendo un servicio de control a través de internet, permitiendo su completo control estando en una red distinta a la de nuestro controlador, permitiendo poder configurar la temperatura o la luz, por poner un ejemplo, sin necesidad de estar presente.

5. Memoria

5.1 Introducción

Actualmente, cada vez es más común ver dispositivos que están dotados de inteligencia y nos ofrecen poder controlar los aspectos generales de nuestras viviendas, como pueden ser el control de la temperatura, o el encendido y apagado de los electrodomésticos. El concepto del Internet de las Cosas (IoT) es ya un término muy común en nuestro día a día, el cual comprende a todos aquellos dispositivos con conexión a internet, lo que permite un control sobre estos a través de la red sin necesidad de estar físicamente al lado de estos dispositivos.

También se está incrementando el concepto de sostenibilidad ambiental; reduciendo el consumo energético de las viviendas se reduce la contaminación ambiental que se produce por las centrales energéticas. A lo largo de los años la idea de poder controlar la temperatura de forma más eficiente se ha ido incrementando, en gran medida controlado por los termostatos auto regulables o los radiadores de bajo consumo como pueden ser los de calor azul. A esto hay que añadirle el confort que supone y que cada vez es más buscado por el usuario final que es el poder controlar los dispositivos de nuestro hogar de forma remota.

Por otro lado, el uso de un Smartphone, una Tablet o un PC es cada vez más común en nuestra sociedad, incrementándose de forma imparable, por lo que la idea de poder controlar nuestro hogar u oficina a través de estos dispositivos supone un gran empujón a la introducción de dispositivos domóticos en nuestras vidas. Además, el hecho de poder controlar todos los aspectos desde una sola aplicación, permitiendo que

todos los dispositivos sean compatibles con el controlador domótico diseñado, aporta un gran valor a la idea que se propone en el trabajo aquí expuesto.

Aunque las instalaciones de viviendas domóticas se vieron fuertemente golpeadas debido a la gran recesión económica sufrida a nivel mundial en el año 2008, los últimos estudios indican que esta situación está viendo como las instalaciones domóticas vuelven a aumentar en número e ingresos, por lo que el diseño del controlador propuesto en este trabajo adquiere una gran importancia y valor.

El último obstáculo a enfrentar de cara al usuario final es el problema que supone la obra que puede producir una instalación, especialmente el cableado necesario. Por este motivo, nos hemos decantado por una instalación totalmente inalámbrica, permitiendo una flexibilidad total para instalar los dispositivos donde se quiera, además de ahorrar una gran cantidad de dinero al usuario final al tener que pagar una menor mano de obra. Indirectamente, al tratarse de instalaciones más baratas, se podrán amortizar antes las instalaciones con el ahorro que esto se conseguiría controlando la calefacción y la iluminación principalmente.

En resumen, la idea de la domótica es la de poder controlar los dispositivos a distancia, además de poder autorregularse por ellos mismos, a través de lo que llamaremos escenas, de tal forma que la residencia donde se instalará el sistema domótico podrá actuar en todo momento bajo diferentes situaciones y sin embargo poder adaptarse autónomamente a cada situación.

5.1.1 Planteamiento y objetivos

En el trabajo a realizar se plantea la idea del estudio y diseño de un controlador domótico de bajo coste, compatible con los productos que ya se encuentran en el mercado y fácilmente accesible para el usuario final. Lo primero que se deberá de hacer será un estudio completo del mundo domótico en la actualidad, dejando bien claro los diferentes y principales protocolos que existen actualmente, para poder elegir cuál de ellos es el más ideal para nuestro dispositivo. También será necesario conocer qué pasarelas existen y están a la venta en el mercado, de cara a conocer los productos con los cuales el controlador diseñado en el TFG competirá y ver si resultaría un producto interesante.

Para conseguirlo, se ha optado por realizar el trabajo sobre una Raspberry Pi, dispositivo de precio muy competitivo y con grandes características y opciones de configuración. Además, según el protocolo que se elija para crear el controlador domótico, será necesario adaptar un módulo que sea capaz de comunicarse con los dispositivos domóticos que se quieran instalar.

Una vez configurada la Raspberry como controladora domótica, será importante centrarse en la interfaz gráfica que será ofrecida al usuario. Esta deberá de ser lo más simple posible para facilitar el uso al usuario final, pero ofreciendo todas las opciones configurables posibles.

Por último, se configurará el poder controlar nuestro controlador domótico a través de internet para poder tener acceso a todo el control de los dispositivos a través de un Smartphone, una Tablet o un ordenador sin necesidad estar conectados en la misma red local a la que está conectado el controlador domótico.

5.1.2 Estructura de la memoria

En el apartado 5.2 se realiza la investigación y análisis de cómo ha ido avanzando la domótica hasta nuestros días. Luego se hará un estudio del estado actual de los distintos y principales protocolos de control domóticos que existen en la actualidad, para poder conocer los puntos fuertes y flacos del resto de protocolos existentes para posteriormente poder justificar que el protocolo de comunicación elegido es el que se cree más correcto y el que más se ajusta a las necesidades que puedan surgir.

El apartado 5.3 se centrará en explicar todo el protocolo Z-Wave en profundidad, protocolo escogido para la realización del proyecto aquí expuesto gracias a todas las ventajas de las que dispone, que serán explicadas más adelante. Este apartado será uno de los más importantes de cara a futuros trabajos de ampliación, debido a que será el protocolo que limitará el campo de trabajo en el cual la pasarela se podrá comunicar con los dispositivos. Por último, se realizará un repaso de los controladores que existen en el mercado ahora mismo de cara a poder conocer la situación actual con la que nos enfrentaríamos de cara a implantar el controlador domótico de bajo coste.

El apartado 5.4 será la otra parte importante del proyecto, apartado en el cual se realizará todo el diseño del controlador Z-Wave, abordando todo el tema de la configuración, resolución de posibles problemas que puedan surgir dentro de este apartado e instalación de los módulos. Dentro de este apartado también se tratará el tema de la interfaz gráfica que se mostrará al usuario final, la cual como ya se ha expuesto anteriormente deberá de ser lo más simple posible, pero siempre que sea completamente útil y configurable.

En el apartado 5.5 el tema a tratar será el de la conexión del controlador domótico a internet para poder controlarlo estando fuera de la red local en la cual se encuentra este.

En el apartado 6 se evidencian las conclusiones y las líneas a seguir en futuros proyectos de ampliación relacionados con el TFG aquí realizado.

En el apartado 7 se realizará un resumen económico de todo el material necesario para la realización del proyecto presentado, con toda la precisión que sea posible. También se hablará brevemente sobre los requisitos en cuanto a Hardware y Software que será necesario y aquellos que se han utilizado.

El apartado 8 incluye un manual de usuario del programa: como se configuran las principales características del controlador, como configurar algunos dispositivos que sirvan de ejemplo, etc. Se intentará que sea un manual lo más corto posible, pero abordando y dejado bien claro todos los temas y aspectos necesarios.

Por último y para terminal la memoria del TFG, el apartado 9 tendrá la bibliografía y las referencias que hemos usado para completar el proyecto y en las cuales se ha basado la recolección de información necesaria.

5.2 Marco teórico

5.2.1 Breve revisión de la evolución de la domótica

Los términos asociados con el concepto domótica son los de confort y seguridad. Estos dos términos son los que se han buscado a lo largo de toda la historia, desde el descubrimiento del fuego para cocinar, protegerse, calentar las estancias, etc., pasando por la edad media donde a través de molinos se podía moler el trigo recogido dejando de ser un trabajo manual, acelerado el tema confort con la llegada de la revolución industrial y la instalación de electricidad, agua, gas, teléfono y demás comodidades a las viviendas particulares (si bien con mayor acceso por parte de las clases acomodadas).

Una vez conseguido los avances previamente citados, el paso siguiente tenía que ser el de la automatización de todas las acciones cotidianas de una persona. La automatización además es símbolo de progreso, por lo que lo normal era que los primeros sitios en los que se empezase a instalar sistemas automatizados fuesen en edificios públicos y oficinas y en menor medida en las viviendas. En los años setenta, un edificio moderno debía estar dotado como mínimo de escaleras, puertas, ascensores, climatización, sistema de detección de incendios y de intrusos; todo automático.

El gran avance que permitió que la automatización se extendiese rápidamente fue el de la aparición de los microprocesadores y los ordenadores personales (PC), y su cada vez más reducido precio. Gracias a estos microprocesadores de precio asequible se pudieron empezar a automatizar las viviendas, conociendo esta acción como domótica.

Lo primero y más importante que se empezó a automatizar en las viviendas era el poder controlar la temperatura en todo momento, suponiendo un gran ahorro energético y monetario al usuario además de confort. Posteriormente y por detrás en importancia fue el control de las luces de forma automática, para después empezar a controlar todas las actividades cotidianas, como pueden ser las televisiones (gracias en gran medida a las Smart TV), el control del riego, la alimentación de las mascotas mientras no se está en la vivienda, etc.

Los primeros sistemas domóticos instalados son cableados dado que de esta forma los sistemas eran más sencillos, estables y seguros, aunque contaban y siguen contando con el problema de realizarse en viviendas en construcción dado que instalar estos sistemas en viviendas ya construidas pueden suponer un elevado coste final al usuario debido a la mano de obra necesaria para la instalación.

El hecho de ser cableadas también hizo que no creciese de forma rápida debido a la complejidad que esta representaba, estando instaladas prácticamente en viviendas de personas adineradas.

Otro factor que influyó era el de la ausencia de organismos e instituciones dedicadas a su desarrollo que asumiesen el riesgo económico que suponía apostar por esta nueva tecnología. Sin embargo, algunas se introdujeron en este mundo como pueden ser el Comité Español para la Gestión de Edificios y Viviendas (CEDOM) o el Instituto para la diversificación y Ahorro de Energía (IDEA).

El avance y creación de protocolos inalámbricos ha supuesto un gran empujón a la instalación de sistemas domóticos en un mayor número de viviendas. Esto ha sido posible gracias al incremento del alcance de estos dispositivos y de la duración de aquellos que funcionan con baterías.

En España la domótica está presente en un gran número de empresas dedicadas a la creación y/o instalación de piezas de sistemas domóticos. Esto queda patente en el ejemplo de ser el segundo país con un mayor número de partners de KNX según su web oficial, sistema domótico más extendido en el mundo, contando con un total de 4644 partners, solo por detrás de Alemania (15999), muy por encima de otros países avanzados como son UK (561), Noruega (275), EEUU (16), Francia (1748) o Dinamarca (405)

| | | | |
|--------------------------------|-------------------------|--------------------------|-----------------------------|
| Albania (8) | Estonia (22) | Lithuania (31) | Qatar (43) |
| Algeria (6) | Ethiopia (1) | Luxembourg (123) | Réunion (11) |
| Andorra (35) | Faroe Islands (3) | Macau (1) | Romania (70) |
| Angola (8) | Finland (197) | Macedonia (13) | Russian Federation (344) |
| Antarctica, Norfolk Island (1) | France (1748) | Malaysia (81) | Saudi Arabia (120) |
| Argentina (47) | French Polynesia (8) | Maldives (2) | Serbia (60) |
| Armenia (1) | Georgia (4) | Malta (6) | Singapore (179) |
| Australia (169) | Germany (15999) | Martinique (10) | Slovakia (61) |
| Austria (3529) | Gibraltar (1) | Mauritius (9) | Slovenia (60) |
| Azerbaijan (15) | Greece (778) | Mexico (44) | South Africa (44) |
| Bahrain (16) | Guadeloupe (4) | Moldova, Republic of (2) | Spain (4644) |
| Bangladesh (3) | Guatemala (3) | Monaco (5) | Sri Lanka (2) |
| Belarus (13) | Hong Kong (14) | Montenegro (4) | Suriname (1) |
| Belgium (1678) | Hungary (41) | Morocco (11) | Swaziland (3) |
| Bolivia (5) | Iceland (24) | Mozambique (1) | Sweden (827) |
| Bosnia and Herzegovina (23) | India (106) | Myanmar (1) | Switzerland (1239) |
| Brazil (82) | Indonesia (16) | Namibia (1) | Syrian Arab Republic (6) |
| Brunei (2) | Iraq (2) | Nepal (1) | Taiwan (Rep. of China) (37) |
| Bulgaria (37) | Ireland (320) | Netherlands (947) | Thailand (25) |
| Canada (14) | Israel (42) | New Caledonia (2) | Tunisia (7) |
| Cayman Islands (1) | Italy (1729) | New Zealand (21) | Turkey (219) |
| Chile (52) | Jamaica (2) | Nigeria (8) | Turkmenistan (2) |
| China (229) | Jordan (10) | Norway (275) | Ukraine (30) |
| Colombia (50) | Kazakhstan (5) | Oman (9) | United Arab Emirates (277) |
| Costa Rica (3) | Kenya (1) | Pakistan (5) | United Kingdom (561) |
| Croatia (152) | Korea, Republic of (62) | Palestine (3) | United States (16) |
| Cyprus (110) | Kosovo (2) | Panama (7) | Uruguay (14) |
| Czech Republic (403) | Kuwait (21) | Paraguay (8) | Venezuela (7) |
| Denmark (405) | Kyrgyzstan (1) | Peru (7) | Vietnam (23) |
| Dominican Republic (4) | Latvia (26) | Philippines (1) | |
| Ecuador (11) | Lebanon (53) | Poland (796) | |

Figura 1. Tabla con número de Partners por países

En la actualidad, existen numerosas organizaciones como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), el Comité Europeo de Normalización Electrotécnica (CENELEC), la KNX Association o la Z-Wave Alliance, encargadas de gestionar todos los aspectos domóticos, promocionar y mejorar sus propios protocolos.

5.2.2 Estudio de los diferentes protocolos que existen

Ante el rápido crecimiento de la tecnología en lo que respecta a la automatización de las acciones diarias o domótica, surgieron multitud de diferentes protocolos de comunicación, clasificables según el tipo de tecnología, forma de mandar la información, forma de “comunicarse” con el usuario final, etc.

Hablar y analizar todos los protocolos que actualmente existen sería un trabajo totalmente separado del actual, pues consiste en un número ampliamente cuantioso, como lo son los protocolos de comunicación: KNX, X-10, LonWorks, BACnet, ModBus, inBus, ZigBee, OSGi, INSTEON, EnOcean, Bluetooth Smart, Z-Wave, y un largo etcétera de diferentes protocolos.

A continuación, se va a realizar un estudio de los considerados principales protocolos domóticos para poder evaluarlos y elegir el que consideraremos como mejor protocolo para la realización del TFG aquí expuesto.

KNX

KNX es un estándar de protocolo de comunicaciones de red basado en OSI para su uso en edificios inteligentes (domótica e inmótica). Se trata de un protocolo de origen europeo surgido a principios de los años 90 tras la unión de tres organizaciones dedicadas a las instalaciones de edificios inteligentes en Europa: European Home Systems Protocol (EHS), European Installation Bus (EIB) y BatiBUS. En 1997 las tres organizaciones anteriormente mencionadas decidieron unirse con la idea de poder desarrollar una norma industrial en lo que respecta al tema domótico.



Figura 2. Logo del protocolo de comunicación KNX

Se trata de un protocolo de comunicación instalado en la mayoría de las instalaciones domóticas cableadas. La comunicación entre controlador y dispositivos se realiza a través de su propio sistema de cableado de par trenzado a 9600bps. Estos hilos también suministran alimentación eléctrica para los dispositivos conectados mediante este protocolo gracias a los 30 voltios en continua suministrados.

También cuenta con medios de comunicaciones a través de la red eléctrica (PL) en corrientes portadoras sobre 230Vac@50Hz a 1200/2400bps a través de la modulación SFSK permitiendo un alcance de hasta 600 metros sin necesidad de un repetidor. Esta forma de comunicación no es compatible con los sistemas eléctricos a 110Vac@60Hz por lo que no se ha visto impulsado en gran medida. Otro método de

comunicación es por radio frecuencia o por Ethernet, aunque todos estos últimos medios en menor medida que la comunicación cableada.

Debido a que se trata, en su gran mayoría, de un sistema basado en comunicación por cable, se puede apreciar que se trata de un sistema muy fiable, robusto y rápido, pero con la principal pega de tratarse de instalaciones de precio elevado, a no ser, que se realicen en instalaciones de edificios nuevos o en edificios industriales, al ser capaces de hacer frente a un elevado gasto para poder mejorar en términos de eficiencia, seguridad, etc.

La visión de futuro del protocolo KNX es la de centrarse en comunicaciones a través de ordenes TCP/IP (conocido como KNX-IP). Esto se ve apoyado a la estandarización de otros buses y protocolos de otros sistemas TCP/IP, así como el crecimiento y estandarización de estos. Esta decisión final supondría un gran avance en lo que respecta a la comunicación mediante KNX debido a la reducción de precio que supondría, así como un incremento en el número de posibles usuarios finales debido sencillo acceso que tienen los sistemas TCP/IP y el número de posibles productos compatibles.

X10

El protocolo de comunicaciones X10 cuenta con la principal característica de poder transmitir la información de control necesaria a través de la red eléctrica (ya sea a 220Vac/110Vac a 50Hz/60HZ). Se trata de un protocolo pensado para su uso en viviendas personales (hasta 250m²), no para instalaciones industriales debido en gran medida a contar con un ancho de banda limitado y un número máximo de dispositivos a controlar (hasta 256 dispositivos).



Figura 3. Logo del protocolo de comunicación X10

Desarrollado en 1978 en Escocia por la compañía Pico Electronics of Glenrothes, fue diseñado para el control remoto de los dispositivos domésticos, convirtiéndose en la primera tecnología domótica en aparecer y siendo aún hoy en la actualidad la más ampliamente disponible, favorecida por tratarse de un protocolo de comunicación que no necesita de instalación de material extra, si no que aprovecha el cableado eléctrico ya instalado en las viviendas personales.

La transmisión de la información del protocolo X10 se basa en el envío de ráfagas de pulsos de radiofrecuencia (a 120kHz) que representan información digital. Para asegurar un correcto envío de la información sin pérdidas, se transmiten dos órdenes y cada una de ellas se transmite 2 veces, por lo que toda la información enviada es transmitida con una cuádruple redundancia. Esto es gracias a que los pulsos se sincronizan con el cruce por cero de la señal de red. Si se presenta un pulso en un

semiciclo y después ausencia en el siguiente semiciclo esta señal se entenderá por un '1', y si es a la inversa se entenderá por un '0'. Primero se transmitirá una orden con el código de casa y el número del módulo, para luego transmitir la orden con la función que se quiera realizar como pueden ser, por ejemplo: 'encender', 'apagar' o 'alternar posición'.

X10 es un protocolo que actualmente está presente a nivel mundial en el mercado domótico, a pesar de contar con algunos fallos como pueden ser que los módulos de comunicación de las lámparas no pueden soportar grandes cargas o que todo el sistema es altamente sensible a los ruidos eléctricos. Para corregir estos problemas han surgido otros protocolos muy parecidos al X10 como son los protocolos Universal Powerline Bus (UPB), Lonworks o XD2, pero no han sido capaces de reemplazar al protocolo X10 debido al amplio cupo de mercado que ya dispone.

Uno de los problemas con los que se encuentra el protocolo X10 es el de las controladoras, pudiendo separarlas en dos categorías: simples y complicadas.

- Simples: Las controladoras simples suelen estar preparadas para controlar únicamente cuatro dispositivos, por lo que no permite poder automatizar una vivienda de forma útil, solo las ordenes más simples.
- Complejas/sofisticadas: Permiten el control de más dispositivos, así como realizar funciones ya programadas anteriormente según el momento del día, controlar detectores de movimiento, infrarrojos o células fotoeléctricas para realizar otras acciones. Si bien estas controladoras son muy completas, resultan de gran complejidad (como su propio nombre indica) para los usuarios finales actualmente, motivo que lo ha lastrado a la hora de instalarse en un mayor número de viviendas.

A pesar del problema de las controladoras, Un punto importante a destacar del protocolo X10 es el de la existencia de puentes capaces de 'traducir' entre diferentes protocolos, como puede ser pasar de X10 a KNX o viceversa por poner un ejemplo. X10 también es compatible con HomePlug (familia de diversas especificaciones de comunicaciones por línea eléctrica, destinadas por ejemplo a aplicaciones de banda ancha como la distribución de datos de baja velocidad, juegos y contenido de internet) siempre y cuando los circuitos domóticos queden aislados con un filtro y se deje el de fuerza para Internet, conectando el controlador a la fase aislada.

ZigBee

El protocolo de comunicación ZigBee no es un único protocolo como tal, sino la agrupación de un conjunto de protocolos del tipo denominado alto nivel de comunicación inalámbrica. El hecho de no tratarse de un único protocolo sino de un conjunto de estos ha lastrado a ZigBee debido a no poder tratarse de un posible sustituto de los otros sistemas domóticos por no ser universal entre dispositivos ZigBee de diferentes marcas.

La problemática anteriormente mencionada cada vez se ve más mermada debido a que se sigue buscando la completa compatibilidad de cualquier dispositivo ZigBee sin importar el fabricante del cual proceda estos dispositivos. Estos pasos de compatibilidad se pueden observar en las versiones que se han ido sacando a lo largo del tiempo.



Figura 4. Logo del protocolo de comunicación ZigBee

La primera versión de ZigBee se aprobó el 14 de diciembre de 2004, estando disponible únicamente a los miembros de la ZigBee Alliance. Para la comunicación con los dispositivos el protocolo se basa en el nivel físico, es decir, en el control a través de la MAC. Si bien puede operar a diferentes frecuencias según la región donde se vaya a comercializar el producto (868MHz en Europa y 915 en EEUU, por ejemplo), ZigBee usa la banda de los 2.4 GHz (la misma que la señal Wi-Fi y libre en todo el mundo) a nivel mundial, por lo que muchos fabricantes optan por diseñar sus productos para operar directamente en esa frecuencia. Para propagar la información se basa en el concepto de red mallada, por lo que no es necesario que los dispositivos estén conectados directamente con la pasarela para poder comunicarse ni será necesario la instalación de repetidores de señal, pues los propios dispositivos realizan esta función.

La tecnología usada está centrada en la sencillez y el bajo coste de esta, por lo que en algunos aspectos superan a otras redes inalámbricas como pueden ser las de la familia WPAN (por ejemplo, las redes Bluetooth). Debido a las pequeñas diferencias entre estas, una red ZigBee consume mucha menos energía que una Bluetooth, sobre todo en reposo ya que esta última no puede quedarse como tal. Otra diferencia importante es la de la velocidad, siendo en Bluetooth 12 veces superior que en ZigBee, razón por la cual una se ha usado más para aplicaciones móviles, informática casera, etc. Y la otra más orientada a la domótica.

En diciembre de 2006 se aprueba la conocida como versión 2.0 de ZigBee, con cambios importantes en la forma de comunicarse como puede ser un reemplazo en la estructura hasta ahora usada o nuevas bibliotecas. Este cambio supuso que no fuera posible una compatibilidad entre las versiones 1 y 2 a no ser que se instalase un nodo RFD que permite la compatibilidad entre estas.

En el CES de 2017, la ZigBee Alliance presentó la versión 3.0 del protocolo ZigBee, la cual apunta a que podrá garantizar por fin un elevado grado de interoperabilidad entre productos de distintos fabricantes. Gracias a este avance, ZigBee podrá ver como aumenta su número de usuarios, pues al menos en Europa, la capa de propietario con la que contaban los productos, en la práctica, supuso un gran obstáculo a su implantación. Aun así, ha conseguido establecerse como el tercer protocolo en Europa, por detrás de Z-Wave y EnOcean.

Todo apunta a que en el futuro este protocolo resultará muy próspero gracias al aumento de la compatibilidad entre dispositivos de diferentes marcas y al bajo coste que tendrán sus módulos, los cuales se esperan sean los dispositivos más baratos producidos gracias a su simpleza en comparación con otros dispositivos domóticos.

EnOcean

EnOcean es un protocolo domótico creado en Alemania por la compañía EnOcean GmbH, empresa derivada de Siemens AG fundada en el 2001. Sin embargo, el protocolo EnOcean no se formó como tal hasta que en el año 2008 la EnOcean Alliance con empresas de Europa y Norteamérica crearon una organización sin ánimo de lucro en la cual desarrollarían en conjunto las especificaciones para la interoperabilidad entre los distintos dispositivos de los fabricantes, consiguiendo un gran beneficio mutuo. Para ello decidieron operar en bandas de frecuencia sin licencia permitiendo poder solicitar la ratificación como estándar internacional, ayudando a dar a conocer la existencia de este protocolo y de los numerosos productos que disponían en el mercado.



Figura 5. Logo del protocolo de comunicación EnOcean

La principal característica de EnOcean es la de poder operar sin cables ni baterías. Esto es debido a que usa la radiofrecuencia para comunicarse con la controladora por lo que las instalaciones no resultan tan caras debido a evitar tener que realizar obras y gastar material extra como el cable, y en lo que respecta a no necesitar baterías es gracias a que aquellos dispositivos que no van alimentados a la red eléctrica como puede ser un sensor de puerta, obtiene su energía para funcionar de otras formas como pueden ser con electromagnetismo, piezogeneradores, células fotoeléctricas termopares, y un largo etcétera de otros tipos de conversores de energía. Gracias a estas características, los dispositivos con este protocolo no necesitan de un mantenimiento como puede ser el caso de otras marcas.

Como se puede apreciar, el principal objetivo de este protocolo es el de la mayor simplificación posible y un ahorro energético al generar los dispositivos mismos la energía necesaria para su funcionamiento, ganando también autonomía al no necesitar de un servicio de mantenimiento.

La forma de enviar los datos es enviar paquetes relativamente pequeños, con paquetes de solo 14 bytes de longitud y transmitidos a una velocidad de 120kbit/s, reduciendo la cantidad de energía necesaria al transmitir únicamente los '1'. La frecuencia a la cual transmiten estos dispositivos varía según la región donde se vayan a instalar, como por ejemplo 868.3 MHz en Europa, 902 MHz en América y 928 MHz en Japón.

En la actualidad, los productos que usan el protocolo EnOcean están extendidos prácticamente en su totalidad en Europa, siendo el segundo protocolo más usado, con el objetivo de establecerse también en América.

Bluetooth

La tecnología Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) con la capacidad de poder transferir voz y datos entre diferentes dispositivos compatibles con la tecnología Bluetooth. Transmite en la banda de 2.4 GHz, banda libre a nivel muy mundial y muy usada por diferentes protocolos de comunicación.



Figura 6. Logo del protocolo de comunicación Bluetooth

A lo largo de la historia se ha visto como la tecnología Bluetooth ha ido evolucionando y pasando por diferentes versiones, llegando a la nueva versión (v5.0), con fecha prevista para comienzos del año 2017. Una versión es la de Bluetooth de baja energía denominado también como Bluetooth LE, Bluetooth ULP y Bluetooth Smart, permitiendo comunicaciones de hasta 1 Mbps con un rango de alcance de 10 m sin necesidad de repetidores, y hasta 100 m con repetidores.

Actualmente existen en el mercado algunos controladores de empresas que han apostado por la tecnología Bluetooth como forma de comunicarse con sus dispositivos, sin embargo, no han conseguido un éxito notable en el mundo de la domótica. Esta situación puede cambiar ligeramente debido a la apuesta de Apple por usar esta tecnología en su aplicación HomeKit para controlar diferentes dispositivos domésticos como pueden ser las luces, la climatización, un enchufe, etc.

A pesar de tratarse de una tecnología muy estable y afianzada a nivel mundial, el uso que se le da es un uso distinto al de la domótica dado que el alcance es relativamente corto, pero puede transmitir a una velocidad muy alta. Se utiliza principalmente en teléfonos, impresoras, auriculares y módems para el envío de audio o de transferencia de archivos. Otro punto clave es el de la facilidad de conexión entre dispositivos a través de esta tecnología, ya que estos pueden indicar que tipo de servicios ofrecen.

SCP

Un protocolo en constante crecimiento aunque todavía con poca fuerza en el mercado es el Simple Control Protocol (SCP), protocolo creado por Microsoft y General Electric, los cuales están intentando establecer un protocolo para redes de control que consiga afianzarse como la solución definitiva y universal en las aplicaciones de automatización de edificios y viviendas a través de la convergencia de diferentes protocolos existentes en EEUU, tratándose de un protocolo abierto y libre de royalties. Se trata de una solución muy parecida a la que ofrece KNX en el panorama europeo.

En sus orígenes, no se ha partido de cero para el desarrollo del protocolo SCP, si no que han cogido la base de Cibus Industry Council (CIC) junto con las empresas que apostaron por el desarrollo del Universal Plug&Play (UPnP). Esta unión era previsible dado que muchas de las empresas dedicadas al CIC ya habían empezado a

trabajar en lo que pasaría a conocerse como Home PnP, y a esto hay que añadir que General Electric ya se estaba dedicando a usar el CEBus en sus productos.

La forma de transmitir la información es la misma que X-10, esto es a través de la transmisión de datos por las líneas de baja tensión (ondas portadoras). Gracias a esta forma de transmisión de información, su inmersión en el mercado podría verse favorecida pues en EEUU, a diferencia de en Europa, el sistema de control domótico a través de la red eléctrica está muy arraigado e implantado en la sociedad.

Está previsto que en un futuro se desarrolle también la comunicación a través de par trenzado y de radiofrecuencia.

Dado que no se trata de un protocolo muy extendido en el mundo domótico, no entraremos en profundidad dentro de este protocolo al tratarse de un sistema muy complejo y pensado mayoritariamente al mundo industrial.

Z-Wave

Z-Wave es un protocolo inalámbrico creado por la empresa danesa Zen-Sys, orientado para el control de dispositivos automatizables en el hogar, y no para su uso industrial.



Figura 7. Logo del protocolo de comunicación Z-Wave

El protocolo Z-Wave se está imponiendo como el protocolo de control domótico universal debido a la gran alianza de empresas con la que cuenta, así como contar con todas las ventajas de los protocolos rivales tales como la interoperabilidad entre diferentes marcas, la comunicación a través de red mallada que evita la necesidad de instalar repetidores, el alcance a medio distancia y el bajo consumo de energía.

Por estos motivos, se ha decidido que el protocolo a usar en la realización de este TFG sea el protocolo Z-Wave, del cual se hablara con mucho más detalle en el apartado “5.3 Protocolo Z-Wave”

5.3 Protocolo Z-Wave

5.3.1 Estudio del protocolo Z-Wave

El protocolo Z-Wave es un protocolo de comunicaciones inalámbricas orientado al control de dispositivos domóticos usado en su gran mayoría para la automatización de las viviendas. Z-Wave fue desarrollado por la compañía danesa Zen-Sys para más adelante, en el año 2008, ser comprada por la compañía de California Sigma Designs. En la actualidad, se constituye como estándar parcialmente abierto, siendo ratificado por la ITU (Unión Internacional de Telecomunicaciones) en 2012. Se trata del protocolo inalámbrico más usado a nivel mundial, con más de 35 millones de productos vendidos a lo largo de los años y más de 1500 productos disponibles en el mercado.

Estos datos son posibles gracias a que se trata de un protocolo altamente compatible entre todos los fabricantes de dispositivos Z-Wave. Este cúmulo de importantes marcas y fabricantes, los cuales abarcan un numeroso abanico de sectores, forman la Z-Wave Alliance, apostando por que Z-Wave se convierta en el protocolo universal a la hora de automatizar las viviendas. Los principales miembros o marcas más importantes de la Z-Wave Alliance son ADT Security Services, FAKRO, Ingersoll Rand, Jasco, LG Uplus, Nortek Security & Control, Sigma Designs y Samsung's SmartThings.

En común a todos los fabricantes, el protocolo Z-Wave cuenta con una serie de características que lo convierten en una opción muy interesante, como pueden ser:

- Dispone de un rango de comunicación de aproximadamente 30 metros (100 pies) pero con la capacidad de no necesitar repetidores pues los propios dispositivos hacen la función de repetidores hasta 4 saltos entre los nodos, lo que se conoce como Network-Wide Inclusion (NWI) o red mallada.
- Gracias a la red mallada, se puede ampliar la zona de cobertura de los dispositivos, pues estos mismos hacen de repetidores. Este salto entre nodos de la información no afecta a la hora de enviar información en lo que a pérdida de información se refiere. En la siguiente imagen se puede apreciar como los dispositivos conectados a una fuente de alimentación constante en lugar de a pilas (debido al ahorro de energía, pues los dispositivos a pilas se encuentran de forma general en modo suspensión o ahorro de energía) sirven como nodos de comunicación y de unión con aquellos dispositivos a los cuales las ordenes Z-Wave que el controlador principal (en la figura 8 un FGHC2 de la marca Fibaro) envía, pero no es capaz de llegar por distancia a esos dispositivos. Estando representadas por flechas de diferentes colores y siendo bidireccionales o unidireccionales.

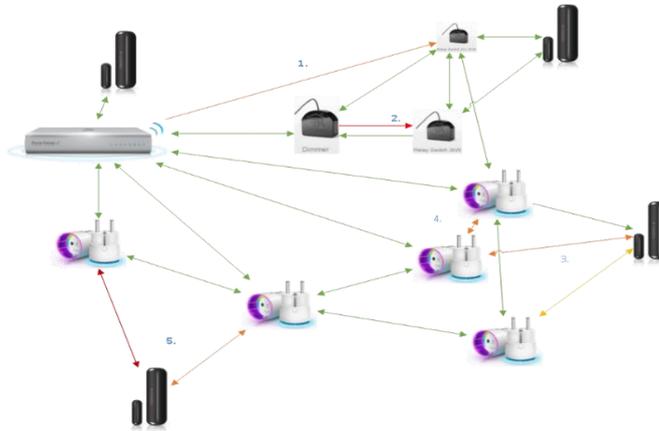


Figura 8. Ejemplo gráfico de la NWI

- Ancho de banda de 9600bps o 100Kbps, sin problema entre ambas velocidades al ser completamente interoperables.
- Capacidad de operar a distintas frecuencias según la localización de los dispositivos a lo largo del mundo. Z-wave utiliza la banda de frecuencia sin licencia industrial, científica y médica (banda ISM):

| Frecuencia en MHz | Zonas en las que se usa |
|-------------------|--|
| 865.2 | India |
| 868.1 | Malasia |
| 868.42 / 869.85 | Europa |
| 868.4 | China / Corea / EUA / Singapur / Sudáfrica |
| 869.0 | Rusia |
| 908.4/916.0 | EEUU / Canadá |
| 915.0 / 926.0 | Israel |
| 919.8 | Hong Kong |
| 921.4/919.8 | Australia / Nueva Zelanda / Brasil |
| 922.0 - 926.0 | Japón |

Figura 9. Tabla de frecuencias ISM de trabajo del protocolo Z-Wave

- Gracias a trabajar en las bandas cercanas a los 900 MHz, se evitan las interferencias con los rangos inalámbricos más usados en el día a día como pueden ser los 2.4GHz usados por las señales Wi-Fi o Bluetooth.
- Bajo consumo energético gracias a la segunda versión del protocolo Z-Wave, conocido como Z-Wave Plus, a través de la serie 500. Los dispositivos pueden llegar a estar activos solo el 0.1% del tiempo.
- Cada red Z-Wave es capaz de controlar hasta 232 dispositivos, a diferencia de otros protocolos que en este aspecto cuentan con una limitación más estricta, como por ejemplo los controladores que se comunican a través de Bluetooth solo son capaces de controlar 10 dispositivos.
- Los chips para los nodos Z-Wave son los ZW0201, basados en un microcontrolador Intel MCS-51 con un reloj interno de 16 MHz. La parte RF del chip está compuesta por un transceptor GisFSK que permite una frecuencia seleccionable a través de software. El consumo es bajo: alimentado a 2.2-3.6V consume solamente 23mA en modo de transmisión.

En lo que respecta a la arquitectura del protocolo, esta se podría dividir en tres capas:

1. Capa radio: Capa encargada de definir la manera en la que se intercambia la señal entre los dispositivos transmisores y los receptores, el medio de transmisión, la velocidad de esta, la codificación que va a seguir y la modulación. En resumen, La capa radio es la capa física, aquella que realiza la función de servir como soporte para trasladar los mensajes entre los diferentes dispositivos de este medio de comunicación.
2. Capa de red: Capa encargada de definir como los mensajes viajen desde el nodo controlador hasta su destino final sin que exista una pérdida de información ni de errores a lo largo del trayecto.
3. Capa de aplicación: Define todas las aplicaciones posibles a las cuales el dispositivo final podrá ejecutar, como pueden ser los dispositivos con fin de realizar medidas, o los que están orientados a controlar las luces.

Respecto a la capa radio, Z-Wave está diseñado para proporcionar una transmisión fiable y de baja latencia de paquetes de datos pequeños a velocidades de hasta 100kbit/s. En la actualidad, el rendimiento de la mayoría de los dispositivos más modernos es de 40 kbit/s, y de aquellos con cierta antigüedad y chips anteriores cuentan con una velocidad aproximada de 9.6kbit/s. Gracias a estas características, el protocolo Z-Wave es adecuado para aplicaciones de control de objetos y de monitorización de todo tipo de parámetros, a diferencia de la tecnología WiFi y otros sistemas LAN basados en IEEE 802.11 (estándar que define el uso de los dos niveles inferiores de la arquitectura o modelo OSI: es decir capa física y capa de enlace de datos, especificando las normas de funcionamiento de una red de área local inalámbrica), diseñados principalmente para él envió de datos a altas velocidades. Otra consideración importante en cualquier tipo de red de carácter radioeléctrico es la distancia a la cual puede comunicarse, distancia que se puede ver atenuada por los posibles obstáculos que se encuentre por el camino (como ya se describió anteriormente), problema solucionado gracias a la topología en malla donde uno o varios maestros arbitran el encaminamiento de las tramas utilizando para ello varios nodos intermediarios, aumentando la distancia de comunicación.

La modulación y transmisión de la señal es través de little endian y con codificación Manchester, el cual es un método de codificación eléctrica de una señal binaria en el que en cada tiempo de bit hay una transición entre dos niveles de señal. Es una codificación auto sincronizada, ya que en cada bit se puede obtener la señal del reloj haciendo posible una sincronización precisa del flujo de datos. Las bandas de frecuencias utilizadas, como ya se explicó anteriormente, son aquellas frecuencias ISM, las cuales compiten con las bandas de algunos teléfonos inalámbricos y otros dispositivos inalámbricos como pueden ser algunos sistemas de alarmas (la mayoría en España usan la frecuencia 868.42 MHz). Sin embargo, las frecuencias en las que opera la tecnología Z-Wave evita interferencias con otras tecnologías como WiFi, Bluetooth y otras tecnologías que operen en la concurrida banda de 2.4GHz. Aunque las bandas ISM son de uso libre, existen determinadas restricciones de tipo radioeléctrico como la potencia de emisión, canales utilizables, ciclo de trabajo o compatibilidad electromagnética.

Las capas inferiores, MAC y PHY, están descritas por ITU-T G.9959 y son totalmente compatibles con versiones anteriores. La capa MAC tiene por objetivo controlar el acceso al medio radio. La trama consta de: preámbulo, inicio de trama (SOF por sus siglas en inglés), cuerpo de trama y delimitador de fin de trama (EOF). La capa MAC tiene un mecanismo de elusión de colisiones que evita que el nodo comience a

transmitir mientras otros lo están haciendo. Esto se consigue escuchando el canal durante unos instantes antes de transmitir la trama que tiene preparada, y de estar ocupado, no enviar nada.

Respecto a lo que se conoce como capa de transporte, esta cumple la función de controlar la transferencia de información entre los dos nodos que establecen una comunicación, incluyendo las retransmisiones, sumas de integridad y asentimientos.

Existen cuatro tipos distintos de tramas:

- Trama de asentimiento. No contiene ningún dato efectivo y sirve como acuse de recibo.
- Trama dirigida. Es aquella que se envía directamente desde un nodo hacia otro. El receptor asiente el mensaje, de manera que el nodo transmisor puede saber que ha llegado correctamente. En caso de que no llegue asentimiento, la capa reenvía el mensaje de nuevo
- Trama multicast. Son aquellas que se dirigen a un conjunto de nodos. No soportan asentimiento del mensaje, lo que provoca que sean menos fiables.
- Tramas de difusión. Son dirigidas a todos los nodos de la red. Tampoco se permite su asentimiento. En la trama de este nivel viajan dos parámetros HomeID y NodeID, que identifican de manera unívoca a cada dispositivo o nodo del sistema Z-Wave: dos nodos que pertenezcan a una misma red no pueden tener el mismo identificador individual, ni ningún nodo puede tener dos HomeID.
 - HomeID: es un identificador de red Z-wave no modificable por el usuario. Posee una longitud de cuatro bytes.
 - NodeID: constituye el identificador de nodo dentro de la red. Es un campo de un byte, lo que significa que una red como máximo puede estar compuesta de 256 nodos.

Cada red Z-Wave es identificada por un ID de red o HomeID, y cada dispositivo es identificado además por un NodeID. El HomeID es la identificación común de todos los nodos pertenecientes a la red Z-Wave y se le asigna a cada dispositivo por el controlador principal cuando el dispositivo se incluye en la red. Esto hace que cada nodo solo pueda estar incluido en un controlador, sin estar permitida la comunicación entre dispositivos con diferentes HomeID, de esta forma se evitan posibles interferencias entre viviendas situadas muy próximas y dentro del alcance de la red Z-Wave.

Por último, está la capa de aplicación, capa responsable de decodificar y ejecutar comandos en la red Z-wave. Los comandos (también denominados comandos de aplicación) están englobados en un nivel jerárquico superior formando las clases de comando. Aquellas que poseen un valor dentro del rango que va desde 0x0 a 0x1F están reservadas para el funcionamiento del protocolo Z-wave, pero el resto son utilizables por los desarrolladores.

Los mensajes que estén relacionados (o conjunto de comandos) se agrupan por clases de comandos, como puede ser, por ejemplo, todos los comandos del termostato los cuales se agrupan en la clase de comando del termostato. Estas clases de comando deben de poder ser soportadas por el dispositivo al cual se envían, teniendo una versión inicial en cada dispositivo y permitiendo que la comunicación pueda seguir realizándose, aunque se produzcan futuras actualizaciones del dispositivo, es decir, las clases de comandos en las que se envían las ordenes son compatibles con versiones anteriores.

La comunicación a través de la red Z-Wave es relativamente simple gracias a una clase de comandos especial que existe en todos los dispositivos, esta es la denominada clase de comando básica. Su objetivo es asegurar que el dispositivo posee una interfaz básica sin necesidad de conocer qué otras clases de comando implementa. Existen tres tipos de mensajes, GET, SET y REPORT. El comando SET puede cambiar el estado de los dispositivos, como pueden ser pasar una luz a estado ON o a OFF. Un mensaje GET “pregunta” por un valor como puede ser si cierta luz está encendida o apagada, o qué valor tiene un dimmer en cualquier momento. Después de cada mensaje GET, se manda un mensaje REPORT con el valor que se ha solicitado al dispositivo.

Una vez mandado el comando, es la documentación Z-Wave la encargada de definir cómo se ven los mensajes. Por ejemplo, la controladora puede enviar a un enchufe doméstico un Byte con la información y la tarea que se quiere realizar, donde por ejemplo manda 255 puede significar que se encienda y 0 que se apague. Para el resto de valores, se podría considerar que son comandos más avanzados, los cuales pueden definir toda clase de parámetros configurables, que en esencia se trata de muchos Bytes mandados en cadena. El controlador con el cual se envía el comando al dispositivo y la respuesta de este es el que va a limitar la capacidad de uso de estos dispositivos, pues deben ser capaces ambos de conocer los comandos que se intercambian (al tratarse de una comunicación bidireccional)

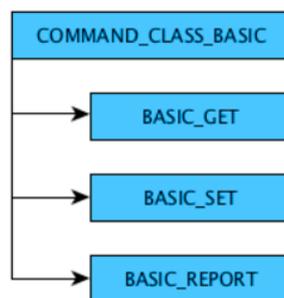


Figura 10. Ejemplo de protocolo de comunicación

Dentro del mundo de los dispositivos Z-Wave, se podrían dividir entre dispositivos maestros o controladores y dispositivos esclavos. Los maestros son aquellos que conocen la topología de toda la red siendo el primer controlador instalado el controlador primario que será el único con potestad para añadir o eliminar los nodos de la red Z-Wave. También son los encargados de enviar y recibir las ordenes de los distintos dispositivos esclavos que tenga controlados.

Los dispositivos esclavos son aquellos que reciben la trama de comandos de los controladores y los ejecutan y responden en consecuencia. Estos dispositivos conocen a los otros dispositivos esclavos que tiene dentro de su alcance y son capaces de responder ante las ordenes que reciben de estos. Dentro de esta categoría, se pueden dividir en otras dos categorías:

- Esclavos estándar los cuales no tienen acceso a la tabla de enrutamiento por lo que no se pueden comunicar directamente con otro esclavo.
- Esclavo de encaminamiento, los cuales tienen acceso parcial a las tablas de enrutamiento dotándoles de la capacidad de enviar información a un cierto número de nodos.

Respecto a la seguridad, Z-Wave se basa en un único proveedor de chip contando además con un diseño propio de este. Con las nuevas versiones del protocolo Z-Wave, se han ido implementando diferentes medidas que aumentan la seguridad de este, complicando la descryptación de los datos enviados entre dos dispositivos, o el envío de datos a un dispositivo desde fuera de su red de comunicación, siendo ya obligatorio que los nuevos dispositivos ofrezcan soporte para el modo protegido con encriptación AES-128. En diciembre de 2015, Sigma Designs anunció el lanzamiento de una nueva actualización de Z-Wave Plus a lo largo del año 2016, llamado *Security 2*, el cual se centró en mejorar los aspectos de la seguridad del núcleo Z-Wave, permitiendo que los dispositivos que usen este protocolo puedan recibir la certificación UL (Organización dedicada a la consulta y certificación relacionada con la seguridad), certificación necesaria para poder usarlos dentro de la industria de la seguridad.

En resumen, los puntos fuertes del protocolo Z-Wave son:

- Estándar internacional gracias a la gran cantidad de marcas y productos en el mercado, además de ser marcas muy conocidas como Honeywell, Samsung, D-Link, Logitech, etc.
- Compatibilidad entre todos los dispositivos Z-Wave
- Capacidad de ir agregando dispositivos a lo largo del tiempo, convirtiéndose en instalaciones modulares según el gusto del usuario final.
- Ausencia de cables de comunicación, abaratando enormemente el precio de la instalación de automatización de un hogar.
- Gran alcance. De base cuentan con un alcance de 30 metros, pero gracias a la característica de la red mallada y de hacer de repetidores, esta aumenta considerablemente.
- Inteligencia: los dispositivos son capaces de mandarse ordenes entre ellos, sin la intervención humana.

Con estos puntos fuertes, puede hacerse una comparación con otros protocolos:

| Protocolo | Puntos débiles |
|-----------|--|
| KNX RF | <p>Instalación con cable propio</p> <p>Necesidad de un instalador profesional</p> <p>Dificultad de expansión al ser cableado</p> |
| ZigBee | <p>Alto consumo energético al trabajar en 2.4 GHz</p> <p>Poca compatibilidad entre diferentes marcas</p> |
| EnOcean | <p>Coste más elevado</p> <p>Comunicación con los periféricos solo cuando se activan, al carecer de baterías</p> <p>Comunicación directa con la pasarela, no dispone de una red mallada</p> |

| | |
|-----------------|---|
| Bluetooth Smart | Pocos productos en el mercado Alto consumo energético al trabajar en 2.4 GHz Reducida distancia de transmisión |
| Wi-Fi | Inexistencia de ecosistema de control domótico Alto consumo energético al trabajar en 2.4 GHz Poca compatibilidad entre diferentes marcas |

Figura 11. Tabla comparativa Z-Wave Vs resto principales protocolos

5.3.2 Estudio de los controladores que existen actualmente en el mercado

Dado que para el TFG se ha optado por el protocolo Z-Wave, se realizará un estudio de los controladores (también son conocidos como pasarelas) más populares que trabajan con este protocolo, pues comparar la idea de una pasarela de bajo coste la cual trabaja con un determinado protocolo con otras pasarelas que no están en el mismo mercado carece completamente de sentido.

Las primeras pasarelas a estudiar serán las dos del fabricante polaco Fibaro, un referente en lo que respecta al mundo Z-Wave y uno de los pilares más importantes de la Z-wave Alliance. Estas son la Fibaro Home Center 2 (FGHC2) y la Fibaro Home Center Lite (FGHCL).

Ambas pasarelas tienen aspectos comunes como el acceso remoto a través de la web mediante su propio DDNS, lo cual facilita la conexión sin necesidad de establecer una IP exterior fija ni abrir protocolos, también permite el acceso desde una conexión local por lo que no depende completamente de la nube de Fibaro para poder controlar los dispositivos a diferencia del resto de pasarelas, o controlar los dispositivos mediante su propia aplicación para Smartphone o Tablet. También cuentan con la opción de la configuración de distintos usuarios, así como de dotarlos de algunos permisos o control de dispositivos específicos.

Ninguna de las dos pasarelas cuenta con conexión vía Wi-Fi, sino que la conexión a internet se realiza a través de cable RJ45. Otra característica común es la de la conectividad con numerosos dispositivos IP de multitud de fabricantes sin necesidad que estos se comuniquen a través del protocolo Z-Wave, gracias a los pluggins de los propios fabricantes que integran los controladores.

La pasarela FGHCL es la pasarela de bajo coste, apta para los usos más básicos al no poseer un Hardware muy potente. Cuenta con un procesador ARM Cortex A8 720 MHz, 128 MB de memoria RAM y capacidad de hacer recovery y Backup a través de la nube.



Figura 12. Fibaro Home Center Lite (FGHCL)

La pasarela FGHC2 es la pasarela de gama superior, apta para su uso en los casos más exigentes como pueden ser viviendas de gran tamaño con un número elevado de dispositivos. Las principales diferencias con la otra pasarela de Fibaro son por ejemplo la capacidad de crear escenas o dispositivos virtuales mediante programación en el lenguaje LUA, o la de controlar otras pasarelas (esclavas) desde una pasarela principal (maestra).

Cuenta con un procesador Atom Dual Core 1.6 GHz, 1 GB de memoria RAM convirtiéndolo en uno de los controladores más rápidos del mercado y además incluye un Pen Drive de 4 GB de almacenamiento únicos de cada Home Center 2 para recovery y Backup, lo que asegura una máxima respuesta ante posibles fallos eléctricos o a posibles intentos de sabotaje de la pasarela.



Figura 13. Fibaro Home Center 2 (FGHC2)

El precio de los controladores es de los más altos del mercado, pudiendo encontrarse por un precio aproximado de 279€ la pasarela FGHC1 y de 599€ para la FGHC2, siendo esta última la más potente en cuanto a hardware en el mercado.

La empresa Connected Object diseña y fabrica su propia pasarela compatible con el protocolo Z-Wave, esta es la pasarela eedomus Plus, evolución de su anterior pasarela la eedomus. Se trata de una pasarela muy extendida en Francia gracias a su simpleza y la sencillez a la hora de crear escenas de control y su compatibilidad con otros dispositivos mediante comandos IP.

Al igual que las dos pasarelas de Fibaro, cuenta con conexión a través de la nube o mediante red local, permitiendo usarla aunque los servidores de eedomus no se encuentran operativos. Esta conexión se realiza a través de cable RJ45 pues no dispone de conexión Wi-Fi. Es importante destacar la existencia de dos tipos de cuentas, una Free con la cual se puede hacer un uso normal, y unas cuentas Premium de pago con funciones avanzadas como pueden ser estadísticas a largo plazo sobre los dispositivos o notificaciones push. Permite la conexión de dispositivos de otros protocolos como EnOcean mediante la instalación de periféricos específicos. Su precio ronda los 300€, un precio que lo sitúa. en la gama alta de los controladores.

En cuanto a hardware, dispone de un procesador ARM Cortex-A8 1.0 GHz, 512 MB de memoria RAM y una memoria interna de 4 GB de almacenamiento. Es característico que lleva incorporado un micrófono y un altavoz, añadiendo un plus en cuanto a poder controlar a distancia nuestro hogar.



Figura 14. Eedomus Plus

Un proyecto muy parecido al que se plantea en este TFG es el de JEEDOM, un proyecto domótico completo compuesto por tres pasarelas: La Mini, basada en una Raspberry y un módulo Z-Wave, pero a diferencia de lo aquí propuesto, se trata de versiones más antiguas de dispositivos y se venden a un precio combinado de 136€. Ofrecen la posibilidad de instalar su sistema en una Raspberry propia, pero no ofrecen ayuda para la realización de esta. También cuenta con la pasarela JEEDOM Center, con un hardware más potente (se habla de 3 veces más potente que la versión Mini), y una pasarela PRO para los usuarios más exigentes. Esta última está compuesta por un procesador ARM A9 Quad Core, 2 GB de memoria RAM DDR3, 30GB de almacenamiento en un SSD, conexión mediante WiFi y Bluetooth v4.0, además de permitir su instalación en un carril Din gracias a su carcasa.

Se trata todavía de un sistema “en pañales”, al cual le falta mucho camino para convertirse en una solución fiable y estable de cara al usuario final. Un punto a tener en cuenta es la de poseer una interfaz de usuario demasiado simple, y algo compleja de utilizar en comparación a la interfaz que ofrece, por ejemplo, los controladores de Fibaro.

Sin lugar a dudas, se trata de un sistema de control a tener en cuenta de cara al futuro si sigue creciendo y ampliándose de la misma forma que lo está haciendo, pues al igual que el TFG aquí realizado ofrece una solución de buena calidad a un precio relativamente bajo, y más si se compara con las otras pasarelas en el mercado.



Figura 15. Logotipo sistema JEEDOM

Otra solución es la que ofrece el fabricante Vera. Cuenta con distintas pasarelas que han ido evolucionando a lo largo del tiempo, siendo la vera lite una gran revolución en el mundo de la domótica por ofrecer una pasarela de calidad decente a un precio muy competitivo. Hoy en día, ha dado un paso atrás en lo que se refiere a calidad y número de usuarios, los cuales han ido optando por otras soluciones como Fibaro, eedomus o Zipato, de la cual hablaremos más tarde. Su actual mejor controladora en el mercado es la Vera Plus, la cual cuenta con comunicación mediante protocolo Z-Wave, ZigBee, Wi-Fi y Bluetooth a un precio muy razonable (190€).

A pesar de contar con una pasarela a priori muy potente, todavía se ve afectado por los fallos de sus antecesoras como fueron una serie de fallos en los puertos USB, por ejemplo, lo cual no permitía una sensación confortable al usuario final. También se ha visto lastrada por su interfaz gráfica, al no resultar muy sencilla y atractiva al usuario final y no cambiar prácticamente nada a lo largo de todas las versiones (actualmente se encuentra por la versión UI7).

La principal diferencia de la Vera Plus con su antecesora la Vera Edge es la de poder comunicarse con más protocolos domóticos, pues a nivel de Hardware incorporan lo mismo, un procesador MIPS SoC 600 MHz, con 128 MB de memoria RAM y otros 128MB de almacenamiento en su memoria interna.

En el CES 2017, Vera presento la que será su nueva pasarela y la apuesta para el futuro, la Vera Secure, que además de las comunicaciones que ya poseía la Vera

plus, añade comunicación por radio frecuencia en la banda de los 433 Mhz, una batería de respaldo, slot para tarjeta SIM, sirena y comunicación audio bidireccional. Todas estas mejoras apuntan a que la marca empezara a centrarse en controladores orientados hacia la seguridad con un toque domótico, lo cual podría tener sentido ya que el mundo de la vigilancia no hace más que crecer a lo largo de estos años, motivo por el cual al haber apostado por esto antes que sus rivales podrían situarlos en la cabeza de los controladores m en un futuro no muy lejano.



Figura 16. Vera Plus (izq.) y Vera Secure (der.)

El penúltimo controlador que vamos a analizar se trata de un controlador domótico Z-Wave más un sistema de video vigilancia. Se trata de Piper, una pasarela que mediante conexión a internet a través de la red Wi-Fi y a través de su módulo Z-Wave nos permitirá controlar todos los dispositivos de nuestra casa, así como ofrecer imágenes de esta a alta calidad (1080p). Cuenta además con un sensor de humedad, de luminosidad y de movimiento, además de poseer una lente gran angular permitiendo grabar cerca de 180° del lugar donde se sitúa.

No se trata de una solución domótica muy potente: cuenta con un procesador TI DaVinci ARM, 128MB de memoria RAM y 256MB de memoria interna a un precio de 225€

De todas las pasarelas presentadas, se trata de la menos pensada para uso domótico a secas, sino más bien como una ayuda a un sistema de seguridad gracias a la cámara y los sensores con los que cuenta integrados, pero con el plus de poder controlar algunos dispositivos (una cantidad pequeña ya que no es muy potente en lo que se refiere a Hardware).

Un punto fuerte sobre este controlador es el de poder conectar hasta 5 pasarelas Piper en una misma vivienda, motivo por el cual para un usuario que no tenga pensado automatizar demasiado su vivienda, puede resultarle la mejor decisión posible gracias a poder incorporar en el mismo paquete un sistema de video vigilancia.



Figura 17. Controlador Piper

Para acabar el apartado 5.3.2, se analizarán los controladores del fabricante Zipato: Zipabox y Zipatile. Con un precio de mercado de aproximadamente 199€ para la Zipabox y de 379€ para el controlador de alto nivel Zipatile.

Ambas pasarelas están diseñadas para su comunicación a través de la nube, por lo que, ante un posible fallo de esta, no será posible una conexión y control de nuestros dispositivos, aunque estemos dentro de la misma red local.

La pasarela Zipabox cuenta con 64 MB de RAM, 128 MB de memoria flash y una CPU funcionando a 208MHz corriendo sobre un sistema operativo basado en Linux 2.6. Permite conexión de múltiples dispositivos de diferentes protocolos como pueden ser ZigBee, KNX o EnOcean gracias a varios acoples que se añaden a la pasarela principal, dotándola de una gran versatilidad ante la posibilidad de conectarse a diferentes dispositivos de otros fabricantes fuera de la Z-Wave Alliance. La comunicación se realiza a través de RJ45 al no disponer de módulo Wi-Fi.

La otra pasarela de la marca, la Zipatile, consiste en una Tablet con Android como SO capaz de realizar las mismas funciones que una pasarela gracias al módulo Z-Wave que lleva integrada. Presentada hace un año en el CES de 2016, cuenta con comunicación a través de Wi-Fi o de cable RJ45, 1 GB De RAM, 8 GB de memoria flash y un procesador ARM Cortex-A9 Quad-core 1.6 GHz. Dispone también de micrófono y altavoz integrado, una cámara y un sensor de movimiento, convirtiéndola en una opción ideal para un uso cotidiano pues permite controlar todos los dispositivos a través de nuestro Smartphone o a través de la pantalla que lleva incorporada. En el CES de 2017 se presentó una nueva versión de la pasarela, galardonada con el premio a la innovación gracias a las mejoras con las que cuenta como pueden ser el poder soportar de forma nativa los protocolos Z-Wave y ZigBee, soporte al dispositivo Alexa de Amazon, capaz de ejecutar TeamViewer, permite el control de gestos, asistente vocal Zipatile Talk e intercomunicador para control de accesos. Zipatile es la pasarela en la cual la marca Zipato está prestando más atención y su apuesta más seria para el futuro de cara a dominar el mercado de los controladores domóticos.



Figura 18. Zipabox (izq.) y Zipatile (der.)

5.4 Diseño del controlador Z-Wave

Una vez estudiado todo lo relacionado al mundo domótico, así como los protocolos y las diferentes pasarelas o controladoras existentes en el mercado, vamos a proceder a la instalación y creación de un controlador Z-Wave de bajo coste. Para ello, nos hemos decantado por la instalación de un módulo Z-Wave en una Raspberry Pi, concretamente se trata del módulo RaZberry de Z-Wave.Me y de la Raspberry Pi 3 Model B.

En lo que respecta a la interfaz gráfica a usar, existen diferentes gratuitas y libres en la web como puede ser Jeedom (empresa que además vende sus controladores con todos los aspectos ya configurados corriendo sobre una Raspberry Pi), Domoticz, o el propio software proporcionado por Z-Wave.me llamado Z-Way. Para este TFG, nos hemos decantado por el software Domoticz, el cual cuenta con un gran número de usuarios en la red por lo que ante posibles futuros problemas que puedan suceder, existe una gran red de usuarios dispuestos a ayudar y encontrar la solución a estos problemas.



Figura 19. Raspberry Pi 3 Model B y módulo Z-Wave RazBerry

5.4.1. Instalación de Raspbian en Raspberry

El primer paso será el de instalar un SO basado en GNU/Linux sobre el cual correrá los programas y aplicaciones que se ejecutarán en la pasarela. El sistema escogido será Raspbian, distribución del sistema operativo GNU/Linux, lanzado en junio de 2012, basado en Debian Wheezy y diseñado para la Raspberry Pi. El escritorio usado en la distribución es LXDE y como navegador predeterminado usa Midori. Entre sus puntos destacables se encuentran varias herramientas de desarrollo como pueden ser IDLE para el lenguaje de programación Python o Scratch.

Otro aspecto a destacar es la posibilidad de configurar todo el sistema operativo sin tener que modificar los archivos de configuración de forma manual gracias al menú raspi-config. Estas configuraciones permiten, por ejemplo, expandir la partición root para que ocupe todo el espacio disponible en la tarjeta de memoria, configurar el teclado o la posibilidad de hacer overclock.

Al poco de su lanzamiento, en diciembre de 2012 se lanzó una tienda de aplicaciones conocida como “Pi Store”, que en el mismo momento de su salida ya incluía aplicaciones como LibreOffice o Asterisk, o juegos como Freeciv o OpenTTD. Al igual que otras Store como la App Store o Play Store, la plataforma Pi Store cuenta con numerosas aplicaciones, imágenes, videos y próximamente documentación como revistas a disposición del usuario.

Gracias a tratarse de una distribución GNU/Linux las posibilidades de configuración son prácticamente infinitas siendo capaz de ejecutar prácticamente todo software de código abierto compilado en la propia Raspberry Pi. Algo que hace especialmente distinguible a Raspbian, es la capacidad de poseer escritorio, algo muy significativo en los ordenadores personales, convirtiéndose en una alternativa a los ordenadores más clásicos en aquellos lugares en crecimiento, permitiendo la extensión de la informática en países subdesarrollados o para gente con pocos recursos, instalándose en aquellas aplicaciones que no soliciten muchos recursos del ordenador.

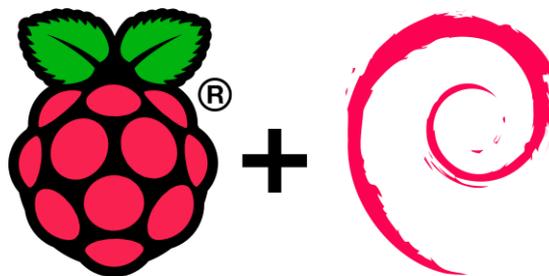


Figura 20. Logos de Raspberry y Raspbian

Para la instalación del sistema Raspbian será necesario seguir 3 pasos:

1. Obtener la imagen del SO
2. Copiarla en la memoria micro SD
3. Arrancar la Raspberry con el instalador e instalar la imagen

A continuación, se irán explicando con detalles y detenimiento los 3 pasos seguidos en la instalación de Raspbian.

Para la obtención del SO, se pueden encontrar por internet numerosos portales y sitios que tienen colgadas las imágenes de Raspbian, pero sin embargo hay dos lugares en los cuales podremos obtener la imagen de forma segura, sin posibilidad de permitir la entrada de virus en nuestros equipos, y asegurándonos que siempre obtendremos la última versión. Estos son desde la propia página de Raspbian (www.raspbian.org) y desde la página oficial de Raspberry (www.raspberrypi.org).

En la primera opción, dentro del campo Download, podremos encontrar dos subcampos que son de nuestro interés.

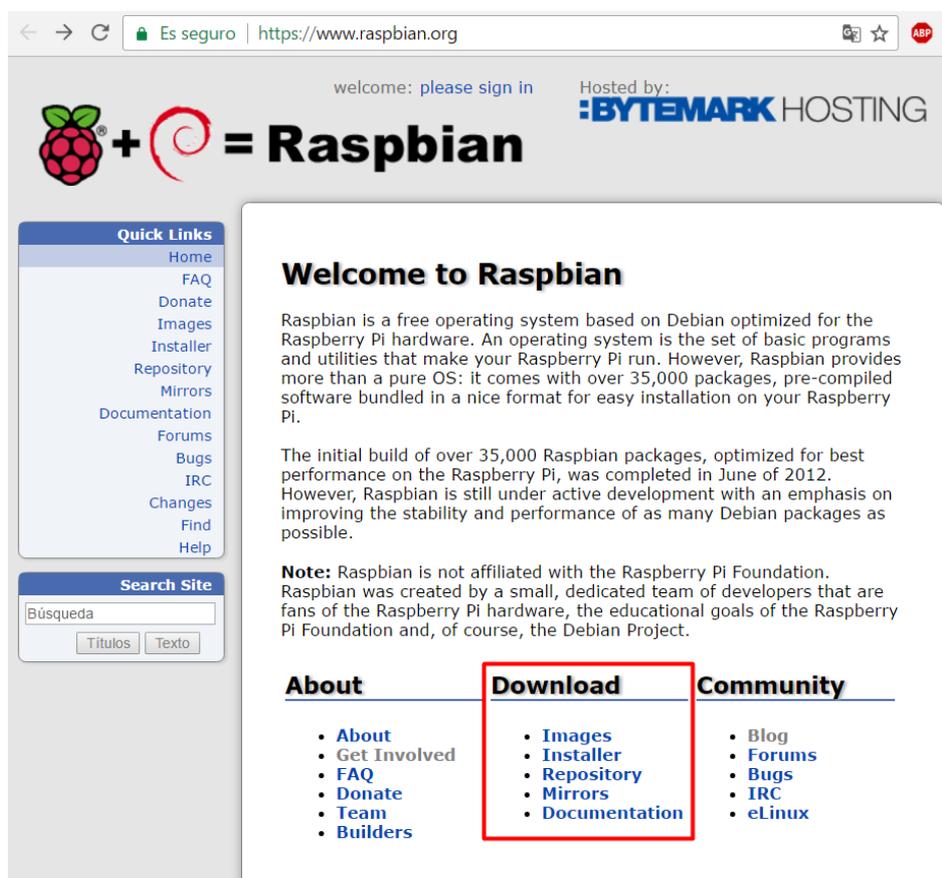


Figura 21. Pantalla principal de Raspbian

Dentro del campo Installer se encuentran los pasos que hay que seguir para la completa instalación del sistema Raspbian en nuestra Raspberry, desde el archivo a descargar como las notas y el guiado paso a paso de todo el sistema. Es importante destacar que la versión situada en ese enlace es la creada por jerry.tk y data del 19 de agosto del año 2012. El usuario jerry.tk no se encuentra activo en el foro desde enero de 2013, por lo que nos podemos encontrar con una versión antigua de este sistema.

Dentro de este campo, nos ofrece la posibilidad de realizar la instalación desde una tarjeta SD o desde un dispositivo pendrive USB, siendo esta la forma más sencilla de realizar la instalación.

En el campo Images, podremos encontrar información acerca de las imágenes de Raspbian y donde conseguirlas. Desde esta pestaña nos llevara a la página oficial de Raspberry Pi para proceder a la descarga de esta última, por lo que el proceso de instalación y descarga se explicara con más detalle más adelante cuando hablemos del proceso de instalación de Raspbian desde la página oficial de Raspberry Pi.

Resulta también muy interesante el campo de Documentation, donde se puede encontrar un gran número de archivos y documentos muy interesantes relacionados con Raspberry y el sistema Raspbian, sobre todo de cara a posibles ampliaciones de otro TFG basado en el sistema operativo o en realizar algún proyecto con la Raspberry Pi.

Para realizar la instalación de Raspbian desde la página oficial de Raspberry, deberemos irnos al campo de descargas (Downloads) dentro de la página principal. Una vez dentro de esta pestaña, podemos ver que las descargas se encuentran separadas en dos grandes campos, el de las principales descargas y el de descarga de imágenes de sistemas operativos de terceros.

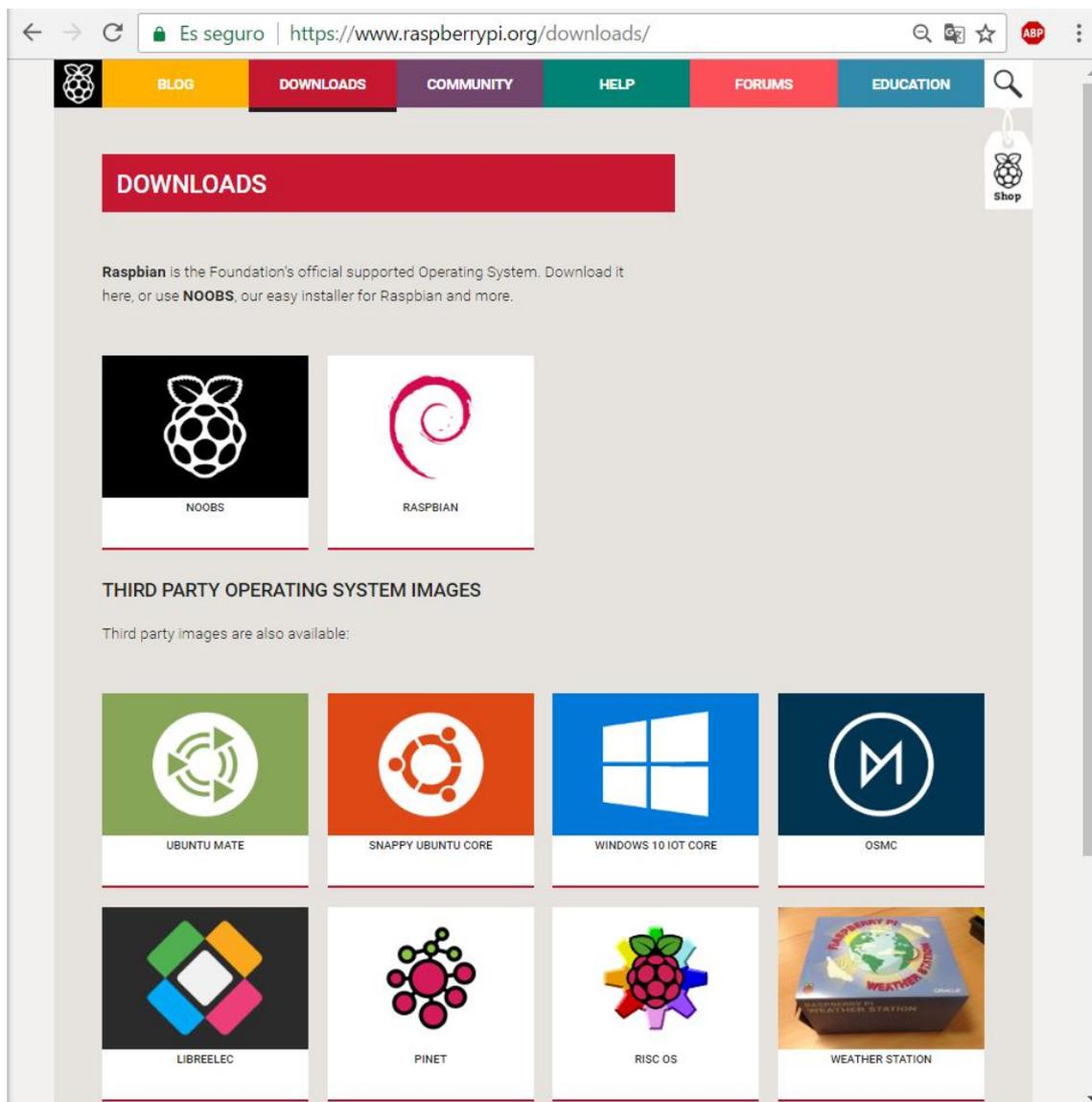


Figura 22. Página oficial de descargas de Raspberry

Como se puede apreciar, hay un número elevado de SO disponibles para Raspberry solo desde su página web, pues por la web se pueden encontrar más sistemas con la posibilidad de instalarse en la Raspberry, sistemas diferentes que pueden resultar muy interesantes según la aplicación que se le quiera dar al trabajo que se realice.

En este TFG nos resultan interesantes los dos centros de descargas principales, NOOBS y Raspbian, opciones las cuales se explicarán con más detenimiento en cada caso. Primero se evaluará la opción de Raspbian y después la de NOOBS. Dentro de Raspbian, podremos encontrar las imágenes de estas dos formas distintas: la versión LITE y la PIXEL, siendo esta última la versión más completa de Raspbian y que puede ser necesario según cada caso. Se puede apreciar que están actualizándose constantemente con las mejoras que consiguen los equipos que están detrás.

The screenshot shows the 'Downloads' section of the Raspbian website. The page title is 'RASPBIAN'. It provides information about Raspbian as the official supported operating system, including installation instructions and a list of pre-installed software like Python, Scratch, and Sonic Pi. It also includes a warning about the size of the PIXEL image (over 4GB) and suggests using specific unzip tools. At the bottom, there are two download options: 'RASPBIAN JESSIE WITH PIXEL' and 'RASPBIAN JESSIE LITE'. Each option includes a version number (January 2017), release date (2017-01-11), kernel version (4.4), and release notes link. Below each option are buttons for 'Download Torrent' and 'Download ZIP', along with the SHA-1 hash for each image.

| Image Type | Version | Release Date | Kernel Version | Release Notes |
|----------------------------|--------------|--------------|----------------|----------------------|
| Raspbian Jessie with PIXEL | January 2017 | 2017-01-11 | 4.4 | Link |
| Raspbian Jessie Lite | January 2017 | 2017-01-11 | 4.4 | Link |

Figura 23. Centro de descargas de imágenes Raspbian

Estas versiones nos valdrían para la realización del TFG, pero sin embargo se ha optado por la opción de instalación a través de NOOBS, forma en la cual es posible instalar distintas imágenes en la Raspberry, no solamente Raspbian, convirtiéndose en

una opción muy sencilla de instalar la imagen del sistema operativo que queramos en el futuro.

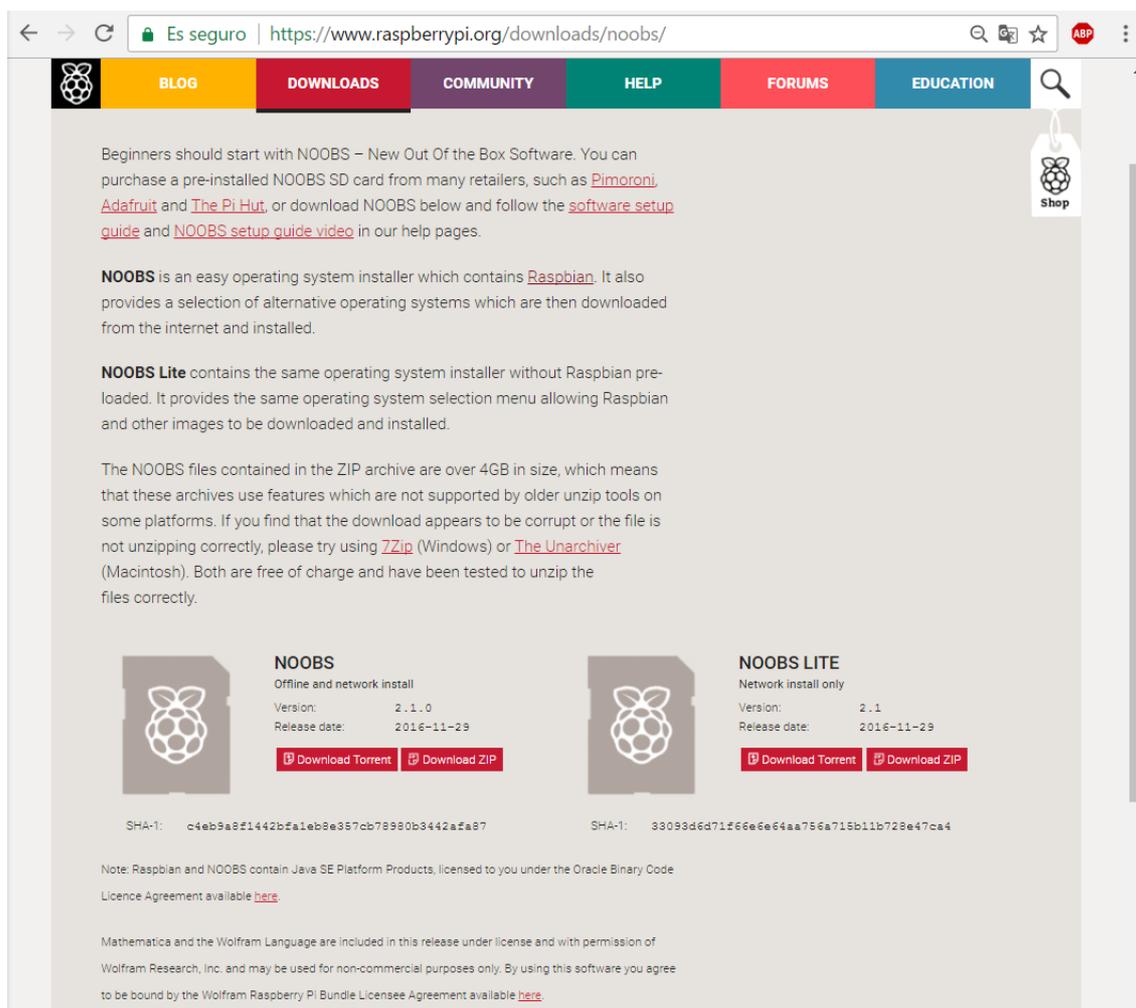


Figura 24. Centro de descargas de instalador NOOBS

Al igual que ocurre con la descarga de Raspbian, nos encontramos con una versión Lite y una versión normal. Desde este TFG hemos optado por descargarlos y usar la versión normal de NOOBS. Una vez descargado (ya sea a través de un archivo Torrent o de un archivo ZIP directamente), el siguiente paso será copiar los archivos descomprimidos en la raíz de la tarjeta micro SD que se usará en la Raspberry.

Después de realizar la copia de los archivos en la tarjeta micro SD, se introducirá esta en la ranura disponible en la Raspberry para ella y se procederá a conectar a través de cable HDMI a una pantalla y a alimentar (se recomienda un alimentador 5V-2A) la Raspberry Pi. Una vez que arranca la Raspberry, podremos encontrar una pantalla en la cual nos dará la opción de instalar el sistema operativo que queremos (esto es solo válido si la instalación se realiza a través de NOOBS)

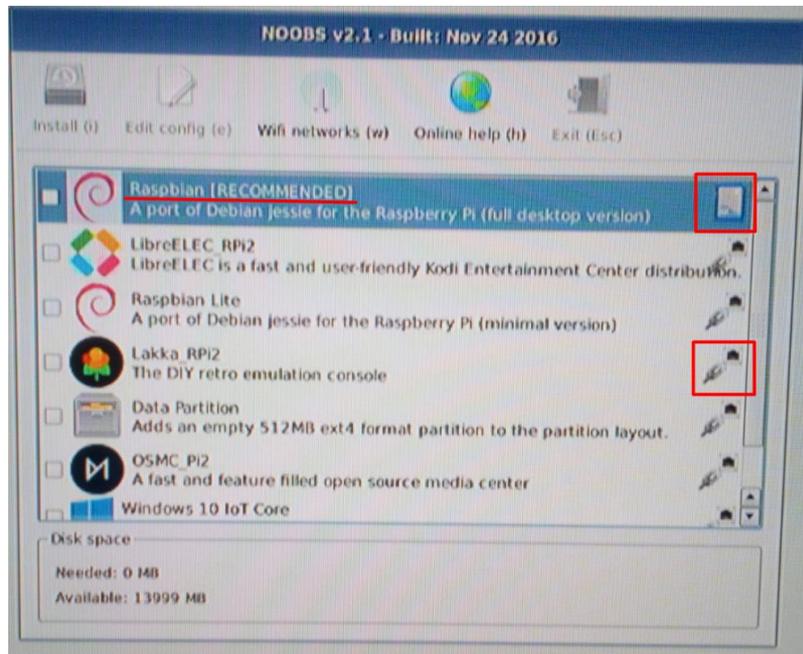


Figura 25. Menú de instalación en NOOBS (v2.1)

Como se puede apreciar en la imagen, podremos instalar Raspbian a través de la imagen localizada en la tarjeta SD (esta se encuentra de forma predeterminada al descargarnos NOOBS) o elegir entre otros sistemas operativos, los cuales se podrán descargar a través de la conexión a internet (esto se puede diferenciar gracias a los iconos situados a la derecha, diferenciables entre una tarjeta SD o una clavija RJ45 para la conexión a Internet). En este TFG, la opción elegida será la de instalar la imagen de Raspbian ubicada en la tarjeta SD. La siguiente pantalla en aparecer será la de la instalación de Raspbian en nuestra Raspberry Pi.



Figura 26. Instalación de Raspbian

Una vez acabada la instalación en la tarjeta SD, se nos mostrará el escritorio que ofrece el sistema Raspbian, un escritorio bastante común dentro de los entornos GNU/Linux. Con todo esto, ya estará perfectamente todo instalado y podremos proceder a la instalación de nuestro sistema domótico.

Es importante añadir que, si se quiere usar la tarjeta micro SD para otra aplicación en el futuro o para instalar otro SO en la Raspberry, al conectar esta a un ordenador no nos mostrará todo el contenido y espacio de la SD, sino solamente una partición de aproximadamente 1.8 GB. Para poder formatearla completamente asegurándonos recuperar todo el espacio, se puede realizar a través de varios programas o por comandos. Para Windows, primero deberemos abrir la consola de comandos, una forma de hacerlo es a través de la combinación [Tecla Win] + [R] y escribiendo *cmd*. Una vez dentro, introduciremos los siguientes comandos para formatear la SD y establecerla en formato *FAT32*:

```
C:\Users\Admin> diskpart  
  
DISKPART> list disk (vemos los dispositivos conectados, y nos quedamos con la  
posición que ocupa la tarjeta SD, por ejemplo, la posición 2)  
  
DISKPART> select disk 2 (donde pone 2 se escribe la posición que ocupe en la lista  
mostrada con el anterior comando)  
  
DISKPART> clean  
  
DISKPART> create partition primary  
  
DISKPART> format fs=fat32 quick
```

Código 1. Formatear memoria SD ya usada previamente

5.4.3 Instalación del módulo Z-Wave

El siguiente paso a realizar será la instalación del Software Domoticz. Es importante aclarar que esto se podría hacer sin estar conectados físicamente a la Raspberry Pi, a través de SSH con el programa Putty (por poner un ejemplo al tratarse de un software gratuito) desde Windows o Mac, pues las distribuciones Linux ya cuentan con comunicación a través de SSH con otros dispositivos de forma nativa, pero sin embargo hemos considerado que resulta más sencillo la configuración a través del terminal disponible en el sistema corriendo en la Raspberry Pi. Si, de todas formas, se deseara configurar por SSH, lo primero será habilitar esta opción en la configuración de la Raspberry mediante el comando `sudo raspi-config -> Interfacing options -> SSH -> Enable` y después reiniciando la Raspberry.

Una vez dentro de la terminal, lo primero será la ejecución de actualización del sistema a través de los comandos:

```
pi@raspberrypi: ~ $ sudo apt-get update
pi@raspberrypi: ~ $ sudo apt-get upgrade
```

Código 2. Actualización del sistema

De esta forma actualizaremos a la última versión nuestro sistema. Es recomendable realizar periódicamente la ejecución de ambos comandos para asegurarnos que siempre contamos con las últimas versiones en cuanto a utilidades y seguridad del sistema. Es importante destacar que primero deberemos de configurar el teclado correctamente para no tener problemas a la hora de escribir símbolos como pueden ser `–`, `|` o `/`, por poner algunos ejemplos.

Lo siguiente que haremos será establecer una IP fija a la Raspberry de cara a facilitar la conexión en un futuro. Para esta configuración, no se va a entrar en detalle dentro de la configuración de redes pues se trata de un campo muy extenso, simplemente se van a dar los pasos a seguir para ello. Lo primero será asegurarnos que vamos a situar la Raspberry en una dirección IP fuera del rango DHCP que ofrece el router que está conectado. Otra forma es la de situarla dentro de este rango, pero estableciendo en el router que la dirección IP elegida no puede darse a otro dispositivo, procedimiento más engorroso debido a la necesidad de la dirección MAC para este proceso.

Para saber el rango de direcciones que ocupa el DHCP, nos iremos a la configuración de nuestro router metiendo la dirección IP (192.168.1.1 en la gran mayoría de casos) y veremos que campos tiene asignados.

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default ▾

IP Address:
 Subnet Mask:

Enable IGMP Snooping

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:
 End IP Address:
 Leased Time (hour):
 Static IP Lease List: (A maximum 32 entries can be configured)

| MAC Address | IP Address | Remove |
|-------------|------------|--------|
| | | |

Figura 27. Ajuste de direcciones IP en el router

Como se puede ver en la figura superior, en este caso el router cuenta con una Subnet Mask 255.255.255.0 por lo que la IP deberá ser del estilo 192.168.1.XXX para poder llegar a ella. Esto es debido a que la submáscara de red se encarga de verificar que direcciones IP son a las que se puede llegar: El 255 quiere decir que todos los números deben de ser iguales, por eso las tres primeras cifras deben de ser 192.168.1, pues la submáscara empieza por tres veces 255. Lo siguiente que nos debemos de fijar es las direcciones que entran dentro del rango DHCP, en este caso son entre 128 y 199, por lo que deberemos de escoger una dirección que no entre en ese rango (tampoco es válida la dirección 1 por ser la del router ni la 255).

Las direcciones DHCP son aquellas que el router asigna de forma automática a los dispositivos que no se encuentran con una IP fija cada vez que se conectan a la red. Se puede ver como en la configuración del router usado cada 72 horas realizara una revisión de las direcciones IP que tiene asignado. Este no sucede con las IP fijas, las cuales se mantendrán constantes cada vez que se reinicie el dispositivo, razón por la cual se deben poner direcciones IP fuera del rango DHCP para evitar problemas de conflicto al haber dos dispositivos con la misma dirección IP. Es importante aclarar que cuando hablamos de dirección IP nos referimos a la dirección IP local, es decir, a la que nos ofrece el router “hacia dentro”, no a la que dirección que este posee de cara a internet.

Para este TFG, se usará la dirección IP 192.168.1.200 la cual cumple con todos los requisitos.

Una vez que se sabe que direcciones IP están disponibles, lo siguiente será establecer una dirección fija en la Raspberry. Para ello, abriremos el terminal donde a través de los siguientes comandos configuraremos varios campos:

```
pi@raspberrypi: ~ $ sudo nano /etc/dhcpd.conf
```

Esto nos abrirá una nueva pestaña con la configuración DHCP de la Raspberry. Lo # que haremos será modificar las últimas líneas añadiendo los siguientes comandos

```
interface eth0

#eth0 es para la conexión por cable, si la conexión es a través del Wifi se deberá de
# cambiar eth0 por wlan0

static ip_address=192.168.1.200

static routers=192.168.1.1 # dirección del router

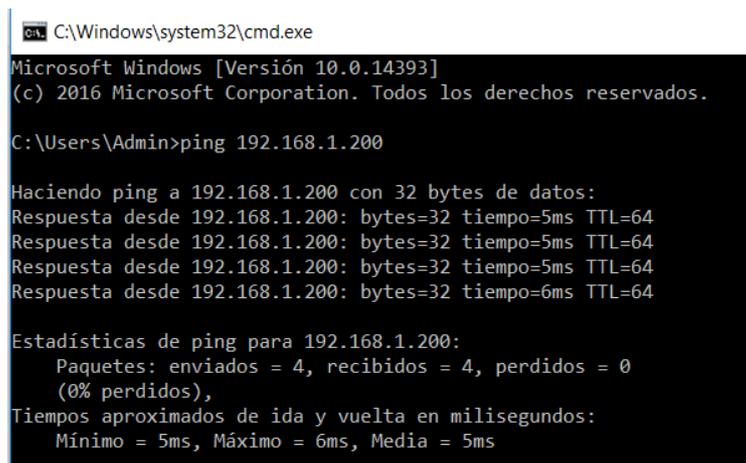
static domain_name_servers=8.8.8.8

static domain_search=8.8.4.4
```

Código 3. Configuración IP fija en Raspberry

Con las líneas nuevas escritas, se guardará los cambios hechos pulsando las teclas [Ctrl] + [o] a la vez, después se pulsará en aceptar y luego las teclas [Ctrl] + [x] para salir. Los cambios en la dirección IP no se efectuarán hasta que se reinicie la Raspberry, esto puede ser a través de los botones que incorpora el propio sistema operativo o con el comando *sudo reboot*.

Para asegurar que el proceso se ha realizado satisfactoriamente, se comprobará con el comando *ifconfig* en la consola de terminal en la Raspberry donde nos mostrará que efectivamente ya se encuentra en la dirección IP que se quería, y a haciendo ping a esa dirección desde la consola de comandos en Windows para asegurar que se establece la comunicación sin ningún problema.



```
cmd. C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Admin>ping 192.168.1.200

Haciendo ping a 192.168.1.200 con 32 bytes de datos:
Respuesta desde 192.168.1.200: bytes=32 tiempo=5ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=5ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=5ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=6ms TTL=64

Estadísticas de ping para 192.168.1.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 5ms, Máximo = 6ms, Media = 5ms
```

Figura 28. Ping a la dirección IP de la Raspberry para comprobar su conexión

El principal problema que nos encontramos al usar Domoticz es que este software no es capaz de leer ni escribir a través de los puertos GPIO integrados de la Raspberry Pi, al igual que no es posible conectarse a la placa hija instalada en ella como es el caso de la placa RaZberry que se va a usar en la realización de este TFG. Para ello será necesario que por debajo esté corriendo a la vez otro software que se encargue de esta tarea, mientras Domoticz se encargará de controlar tosa la gestión de los dispositivos, escenas programadas, etc.

El software elegido para esta función será Z-Way, un software producido por la misma compañía encargada de fabricar el módulo Z-Wave RaZberry (Z-Wave-me), el cual implementa de forma completa la torre de protocolos de Z-wave y permite al programador crear sus propias aplicaciones mediante una API basada en peticiones HTTP. Estas peticiones son atendidas en el PC donde esté instalado mediante un servidor web empotrado que responde con datos JSON. También incluye una aplicación web de ejemplo que actúa como interfaz gráfica del escenario de la red Z-wave, permitiendo a un usuario corriente utilizar sus equipos domóticos sin necesidad de escribir su propio software a partir de la API. Por un lado, se comunica con el controlador Z-Wave mediante la API oficial de Sigma Designs. De este modo, si se conecta al equipo un controlador con un transceptor Sigma, el software funcionará de manera automática.

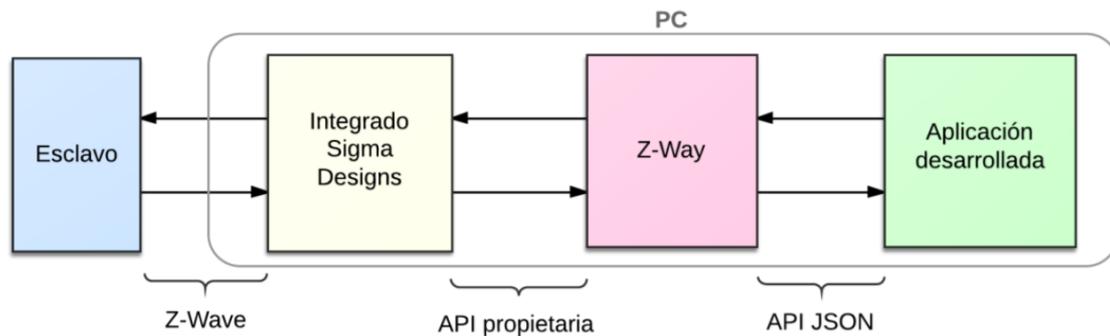


Figura 29. Estructura de funcionamiento de un sistema con Z-Way

Al otro lado, la API basada en HTTP está disponible en forma de funciones JSON, pero también se proporciona una librería en C que hace uso de ellas para permitir programar en este lenguaje. La API está dividida en cuatro partes:

- API de dispositivo Z-Wave. Implementa funciones que permiten el acceso directo a la red ZWave mediante el identificador de nodo. Las funciones de interacción con los dispositivos son las clases de comando ya mencionadas anteriormente. Adicionalmente permite el acceso mediante otras funciones a la interfaz de gestión de la red mediante las denominadas clases de función.
- API de tecnologías de terceros. Implementa la misma lógica de la API de dispositivo Z-Wave para otros sistemas inalámbricos como EnOcean.
- API JavaScript. Permite escribir funciones JavaScript que son añadidas al servidor web como módulos, de forma que pueden ser utilizadas como las que vienen por defecto.
- API de dispositivo virtual. Constituye un módulo JavaScript que asigna a cada dispositivo físico y función un dispositivo virtual. El objetivo de esto es permitir simplificar el desarrollo e implementación de la interfaz de usuario al programador.

La instalación de este software se realizará a través de comandos dentro del terminal de la Raspberry, pudiendo instalar la última versión de este o pudiendo elegir una versión previa estable o incluso elegir una versión que este en modo Beta.

En el tiempo en el que se realizó este TFG, en el mercado se podrían encontrar dos versiones de RaZberry, muy parecidas y con el mismo chipset Z-Wave 500 con comunicación a través de Z-Wave plus. La principal diferencia entre estos dos módulos es el de añadirle una antena de mayor tamaño para aumentar el alcance, aumentando también el tamaño de la placa. De esta forma, se pasa de los aproximadamente 8 metros

de alcance de la primera versión de a RaZberry hasta prácticamente el doble de alcance en la segunda versión.

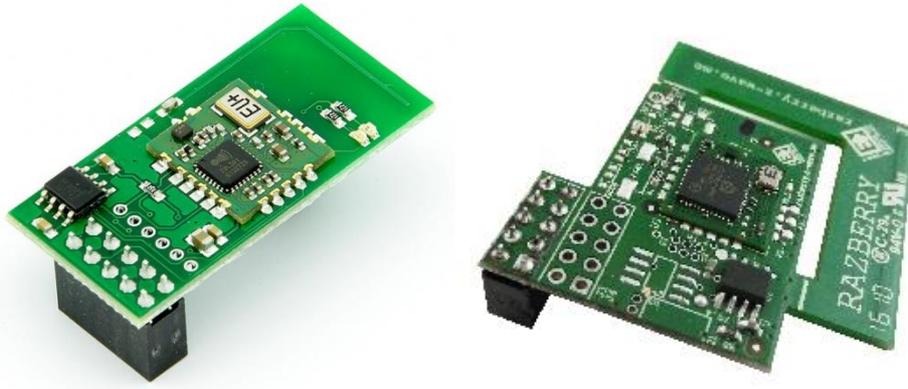


Figura 30. Comparación RaZberry v1 (izq.) y v2 (der.)

La comunicación con la Raspberry se realiza a través de los puertos GPIO que esta incluye integrados. Está compuesta principalmente por:

- GPIO Interface
- Serial EEPROM
- SOC ZM3102
- Filtro de Antena
- Antena
- LED indicador

La cantidad de pines disponibles en el GPIO ha variado de unas versiones a otras, manteniendo la compatibilidad con las versiones anteriores para evitar problemas. Las conexiones GPIO integradas en la Raspberry cuentan con el siguiente diagrama de conexiones. Cuenta con un total de 40 pines y existen dos formas de referirse a la configuración en que están colocados: por un lado, está la nomenclatura GPIO, es decir, pines pares a un lado e impares a otro lado de forma consecutiva, y por otro lado está la nomenclatura BCM, la cual se enumera no de acuerdo a la posición de los pines en la salida, sino a la posición de los pines correspondientes en el chip Broadcom, que es la CPU de la Raspberry. Es posible encontrar configuraciones que se refieran a estos pines por ambas formas, por lo que hay que tener en cuenta para no liar las terminaciones y nomenclaturas, lo que podría suponer un fallo grave en la Raspberry y conllevar a la destrucción de esta.

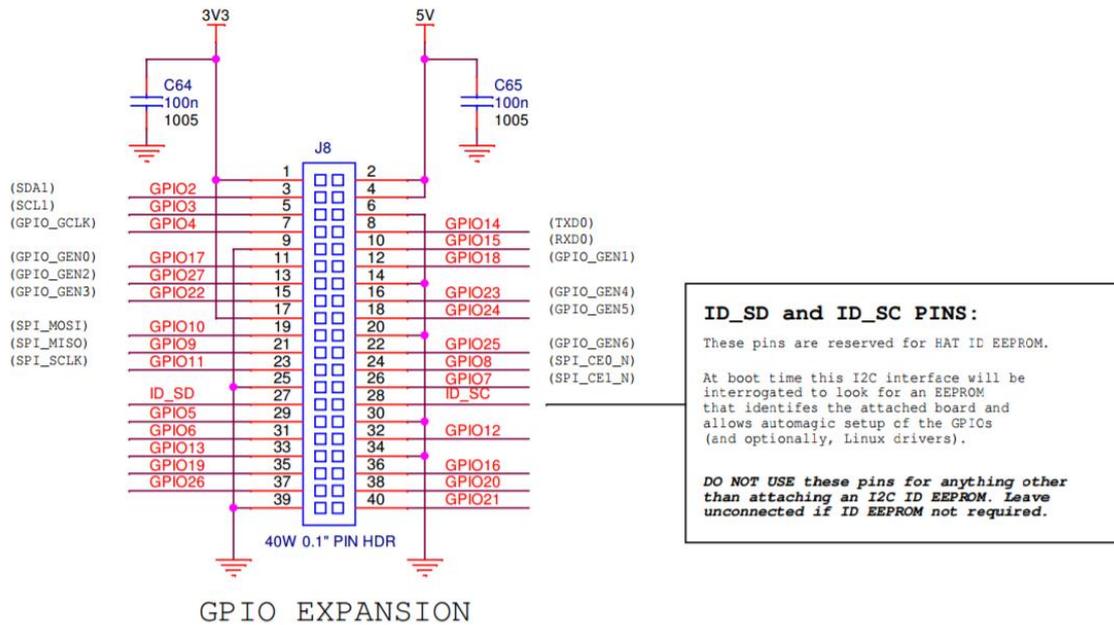


Figura 31. Esquema de conexión GPIO de la Raspberry

La conexión de la RaZberry se realizará en los primeros pines del puerto GPIO, es decir, en los puertos del 1 al 10, quedando la parte Hardware del trabajo de la siguiente manera:



Figura 32. Raspberry y RaZberry instalada

Lo siguiente será la instalación del software encargado de gestionar los puertos utilizados por la RaZberry para más adelante conectar estos con el Software Domoticz y poder controlar los dispositivos domóticos que se quieran. El software utilizado será Z-Way, software fabricado por la misma empresa que se encarga de fabricar la RaZberry.

Esto se realizará a través de comandos por la terminal de Raspberry, y existen dos formas de hacerlo. La primera consiste en descargar e instalar directamente la última versión estable que se encuentre en el servidor, comando que también se usará para una vez instalado volver a instalar la versión más reciente que se encuentre, y la segunda se podrá elegir que versión específica se instalara debido a posibles múltiples causas como pueden ser evitar un problema en la versión más reciente hasta que este sea solucionado.

En este caso, se instalará la versión v2.3.0, versión más reciente con fecha de 27 de enero de 2017. Los comandos a utilizar serán:

```
#Para la instalación de la última versión disponible o actualizar la versión ya instalada
pi@raspberrypi: ~ $ wget -q -O - razberry.z-wave.me/install | sudo bash

#Para la instalación de una versión concreta, por ejemplo, la v1.7.0-rc2
pi@raspberrypi: ~ $ wget -q -O - razberry.z-wave.me/install/v1.7.0-rc2 | sudo bash
```

Código 4. Comandos para la instalación de Z-Way

Una vez ejecutados los comandos arriba mencionados, comenzará la instalación donde nada más empezar nos pedirá si aceptamos los términos de licencia. A la mitad de la instalación se indicará un usuario y una contraseña que se deberá de conservar para posibles futuros usos o consultas, así como a la configuración en remoto a través del servidor que ofrece Z-Wave.me aunque en este trabajo la conexión en remoto se ofrecerá a través de un servidor DDNS, el cual más adelante se explicará.

Si la instalación se ha realizado de forma correcta, podremos conectarnos al módulo a través de la dirección IP de la Raspberry y del puerto 8083, puerto usado por defecto por la RaZberry, es decir, se deberá de introducir la dirección *192.168.1.200:8083* (Recordar que *192.168.1.200* es la dirección asignada a la Raspberry para este TFG, este valor deberá de cambiar según la IP de cada Raspberry). Una vez conectados, lo primero que se nos pedirá será el establecer una contraseña nueva para aumentar la seguridad de esta conexión, a la vez que se solicita agregar un correo (aunque no es obligatorio) para poder reestablecer la contraseña en un futuro, así como obtener acceso a ciertas funciones especiales. Una vez configurada la contraseña se nos mostrara la interfaz gráfica de Z-Way, la cual podría servir directamente como centro de control domótico pues cuenta con la opción de añadir o borrar dispositivos, crear escenas, instalar ciertos pluggins para comunicarse por TCP/IP con ciertos productos de otros fabricantes, etc. En el mercado existen algunas pasarelas domóticas que usan esta interface como interface principal para el usuario final como puede ser el controlador de la marca Popp

Sin embargo, la idea del TFG es la de usar la interfaz que nos proporciona Domoticz, una interfaz mucho más completa de cara al usuario final.

Lo siguiente que se hará será agregar un dispositivo Z-Wave a través de la interfaz de Z-Way para posteriormente hacer que Domoticz se conecte a esta a través del puerto 8083, puerto previamente ya establecido para que la Raspberry muestre por ahí el contenido de Z-Way. Este paso será tan sencillo como ir a la pestaña de *Ajustes* → *Devices* → *Add new* para después ir siguiendo los pasos de instalación eligiendo el fabricante del dispositivo y que dispositivo en concreto se usa. En este caso, se usarán diferentes dispositivos de la marca Fibaro, teniendo a nuestra disposición un sensor de agua (FGFS-101), un sensor de humo (FGSD-002), un enchufe inteligente (FGWPF-102), un sensor magnético (FGK-101) y un Triple sensor: movimiento, luz y temperatura (FGMS-001-ZW5). Aclara que cada función de estos dispositivos se añadirá como si fuera un dispositivo aparte, es decir, si un sensor lleva un sensor interno capaz de medir la temperatura, este lo mostrará como si se tratase de dos sensores distintos.

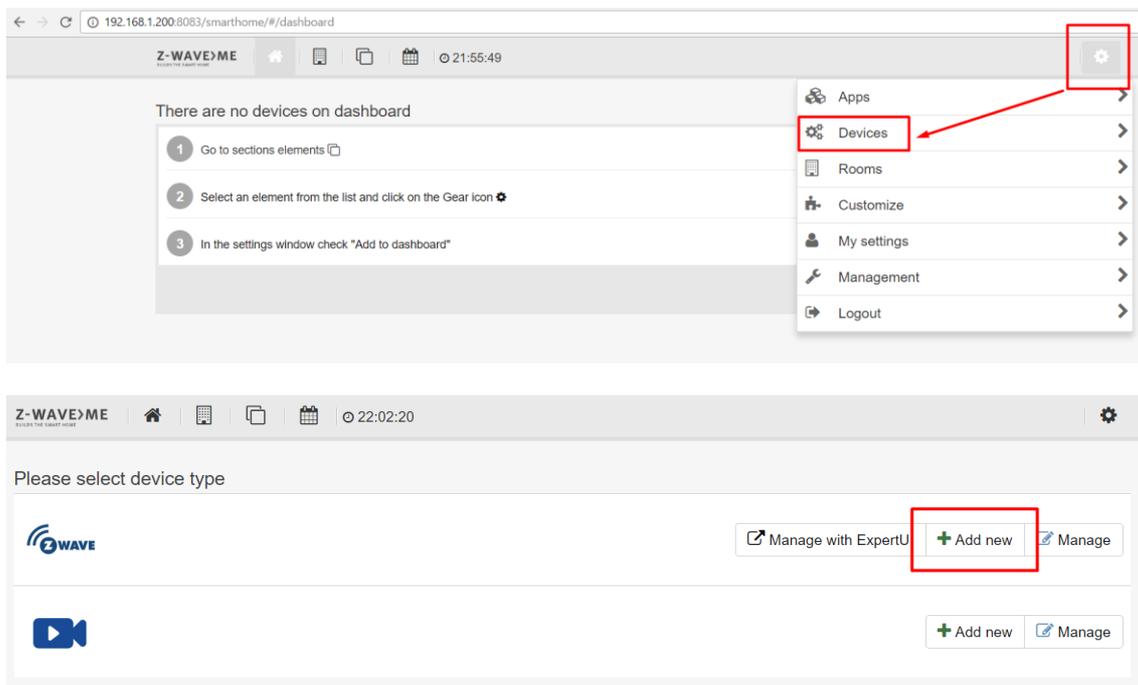


Figura 33. Añadir nuevos dispositivos desde Z-Way

Es importante añadir que es posible la conexión en remoto a través de la dirección <http://find.z-wave.me> y el usuario y contraseña que previamente se nos suministró en la instalación de Z-Way, sin embargo, en este trabajo se ha optado por usar otro tipo de conexión en remoto, configurado en el apartado 5.5 *Conexión a la Raspberry Pi y al control domótico a distancia*.

Es muy importante aclarar una serie de aspectos que se configuran de forma automática al instalar el módulo Z-Way que se deberán de modificar para una correcta conexión en el futuro:

Al añadir el módulo Z-Way a la Raspberry Pi 3 se produce el problema de incompatibilidad con el módulo Bluetooth de la Raspberry, esto es debido al nuevo mapeado de los pines pertenecientes al puerto GPIO (En las versiones este problema no existía), por lo que no pueden coexistir el módulo Bluetooth con el módulo Z-Wave. Para este proyecto, lo lógico es deshabilitar el módulo Z-Wave.

Según la versión que se instale, esto se realiza de forma automática o se deberá de inhabilitar el módulo Bluetooth o hacer un remapeado de los pines GPIO para poder realizar la instalación. Este procedimiento es muy costoso, por lo que lo recomendable es o bien instalar la última versión de Z.Way o deshabilitar manualmente el módulo Bluetooth.

Además, para poder conectarse de forma correcta con Domoticz, será necesario apagar el servidor Z-Way y deshabilitar el inicio automático para que se pueda conectar de forma correcta con el software Domoticz que se instalará más adelante. En anteriores versiones de, era necesario una vez que estos parámetros están configurados, realizar una simulación de tal forma que la Raspberry crea que la conexión se está realizando a través de un puerto USB para que se pueda conectar sin problemas con Domoticz, sin embargo, este proceso ya no es necesario y se realiza de forma automática.

Para realizar la desconexión del servidor y del inicio automático, será necesario ejecutar un único comando a través del terminal. Además, una vez realizado la anteriormente mencionado, también es aconsejable borrar el servidor web Mongoose, ya que la conexión no se va a realizar a través de del web server que ofrece, si no por otros medios como ya se ha mencionado, de tal forma que se aligerará la Raspberry y evitaremos calentamientos completamente innecesarios. Para realizar estas dos configuraciones, se deberá de introducir los siguientes comandos a través de terminal:

```
#Para la desconexión del servidor y del inicio automático

pi@raspberrypi: ~ $ sudo /etc/init.d/z-way-server stop

pi@raspberrypi: ~ $ sudo update-rc.d z-way-server remove

#Para borrar el web server Mongoose (es aconsejable realizar este paso una vez
#instalado Domoticz)

pi@raspberrypi: ~ $ sudo update-rc.d mongoose remove
```

Código 5. Deshabilitar inicio automático y Mongoose (Web server)

5.4.3. Instalación software Domoticz

Para poder controlar todo el sistema domótico de la forma más completa y simple, se instalará el Software Domoticz, el cual se encuentra disponible de forma online totalmente gratuito y con un gran apoyo por parte de la comunidad en internet, facilitando la resolución de problemas de posibles fallos que sucedan en el futuro. Para proceder a instalar el sistema Domoticz se realiza, al igual que la instalación del módulo Razberry, a través del terminal, introduciendo el comando:

```
pi@raspberrypi: ~ $ sudo curl -L install.domoticz.com | bash
```

Código 6. Instalación de Domoticz

Después de instalar los paquetes y complementos necesarios, procederemos a la configuración de Domoticz a través de una pestaña nueva que se abrirá.

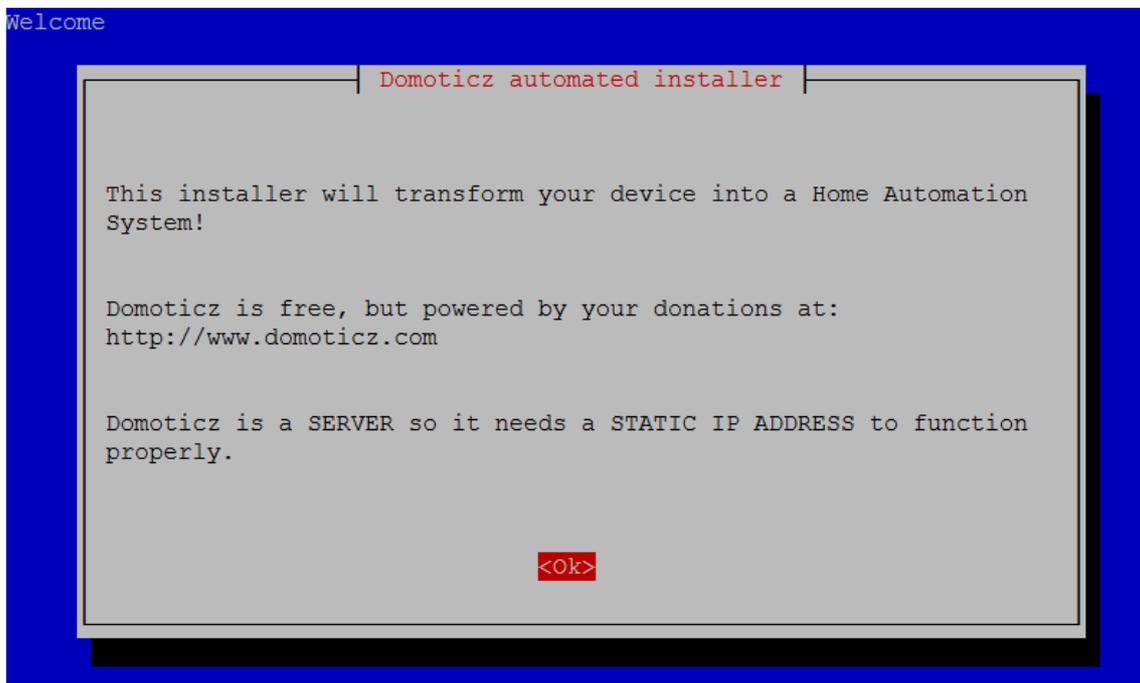


Figura 33. Menú inicial configuración Domoticz

En la siguiente pestaña se seleccionará el método de acceso: *HTTP* o *HTTPS*, en este caso seleccionaremos las dos formas de conexión para facilitar el proceso de instalación y de acceso. La siguiente será la elección del puerto al cual nos queremos conectar. Esta es una elección importante y que se deberá de tener en cuenta para poder conectarnos en el futuro. Debemos de escoger un puerto el cual no se use para ninguna otra acción de la Raspberry Pi. Por defecto viene el puerto 8080, puerto que dejaremos como elegido ya que al tratarse de una Raspberry orientada solo a ejecutar Domoticz no le hará falta usar ese puerto para nada más.

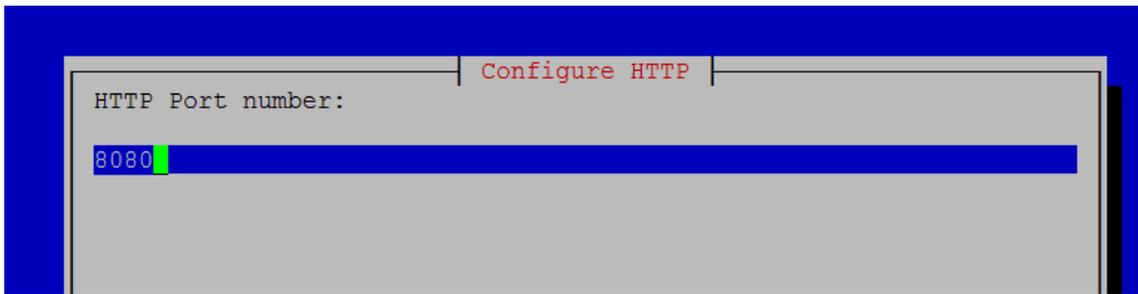


Figura 34. Configuración del puerto al cual se conectará Domoticz

El siguiente parámetro será el del puerto HTTPS que se va a usar. Por defecto viene configurado el puerto 433, puerto que en este caso no se modificará. La elección de estos puertos (tanto HTTP como HTTPS) no es arbitraria, si no que sigue unos estándares y plantillas establecidos en el mundo de redes para facilitar la conexión entre todos los usuarios y fabricantes.



Figura 35. Configuración puerto HTTPS

Lo siguiente será configurar la ruta donde se instalará Domoticz. Por defecto se instalará en la raíz de la cuenta del usuario (/home/pi) y es aconsejable no tocar este campo de cara a facilitar la solución de posibles problemas en el futuro.

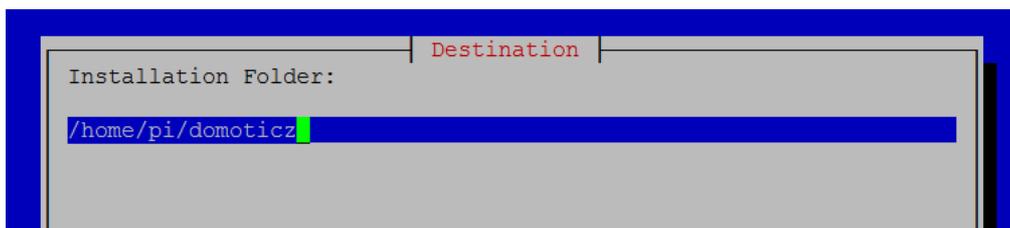


Figura 36. Ruta de instalación Domoticz

Una vez configurado todos los parámetros necesarios, Domoticz se instalará en la Raspberry de forma automática. Al finalizar se mostrará una pantalla con la información básica y un resumen para poder conectarnos a través de IP a la Raspberry, pero además a la parte dedicada de Domoticz con los puertos previamente configurados (8080 para HTTP y 433 para HTTPS)

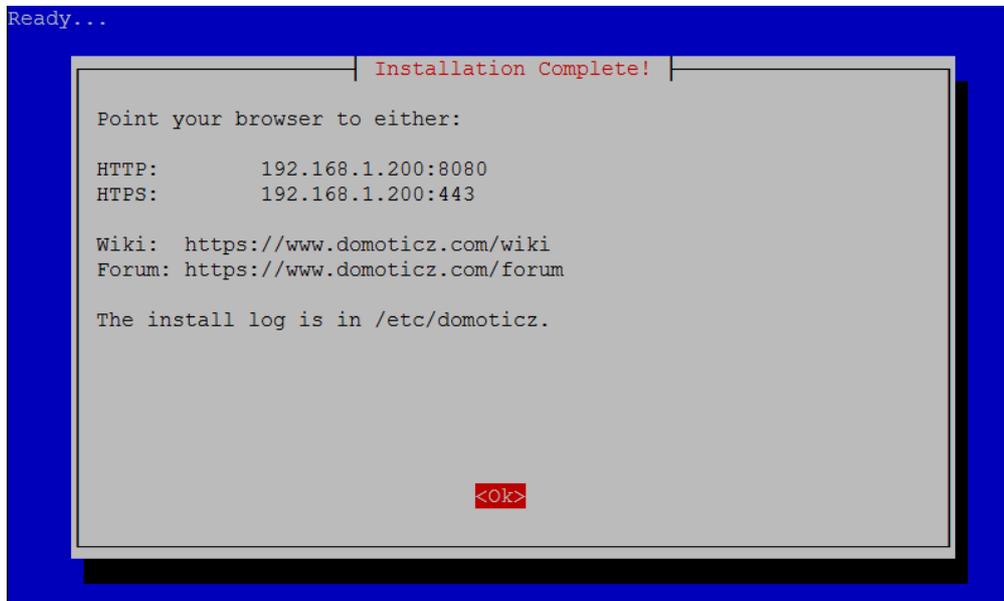


Figura 37. Resumen de la instalación de Domoticz

Por último, para comprobar que todo se ha configurado de la forma correcta, se procederá a conectar a través de IP a la dirección de la Raspberry donde se deberá de mostrar la interfaz gráfica de usuario de Domoticz. Para ello, a través de un navegador nos dirigiremos la dirección `192.168.1.200:8080`, donde podremos ver la siguiente interfaz:

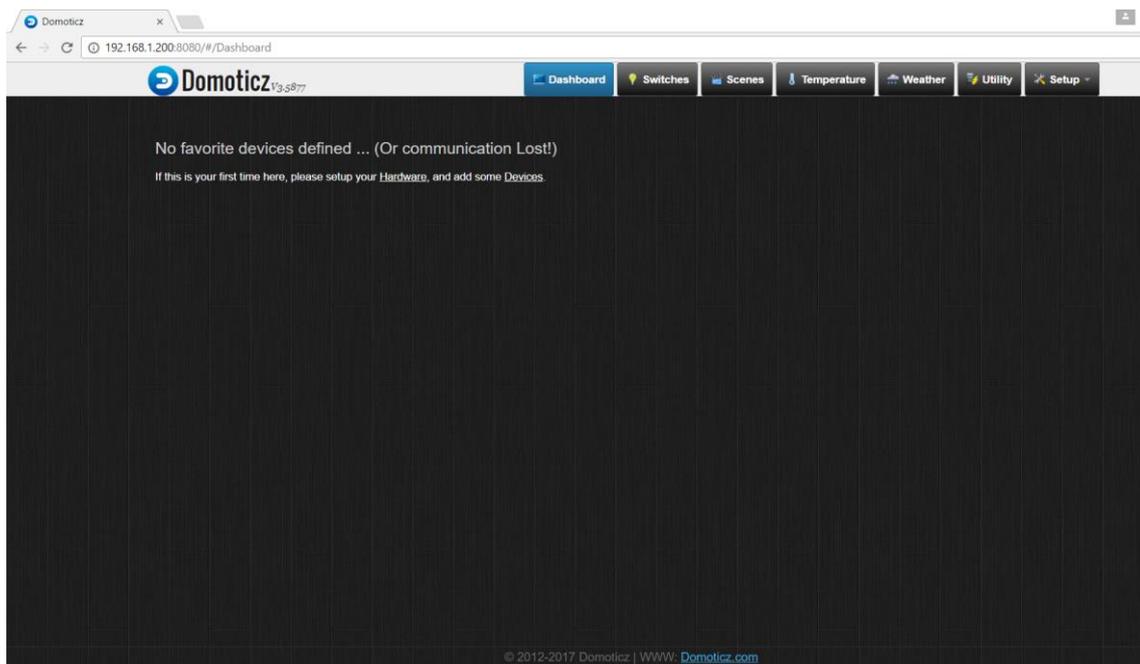


Figura 38. Interfaz de usuario de Domoticz

Como se puede apreciar en la figura superior, la interfaz nos aparecerá vacía pues aún no se ha añadido ningún dispositivo compatible con Z-Wave que se pueda controlar. Para lograr que la Raspberry se comunique a través del protocolo Z-Wave

será necesario la instalación de un módulo Z-Wave (RaZberry en este caso y previamente instalado) y lograr la comunicación entre Domoticz y RaZberry.

Es importante aclarar que al fijar la dirección IP, aunque la Raspberry se reinicie seguirá estando con la misma dirección, por lo que a través de la dirección *192.168.1.200:8080* podremos conectarnos a ella siempre que se quiera. También será posible entrar a la interfaz desde la propia Raspberry sobre la cual está corriendo metiendo la misma dirección en cualquier navegador, por lo que ofrece una solución muy fuerte al poder conectarse y configurar todo de forma visual a través de la salida HDMI que la Raspberry incorpora.

5.4.4. Adaptación de Z-Way con Domoticz

Una vez que ya se encuentra todo correctamente configurado, lo siguiente que se deberá de hacer será unir el software encargado de gestionar los pines GPIO y el módulo RaZberry para controlar los dispositivos Z-Wave con el control y la interfaz que ofrece Domoticz.

Para ello, nos conectaremos a la interfaz a través de la dirección IP de la Raspberry y del puerto 8080, puerto que ya se configuro para que sirviese a través de ese puerto su interfaz gráfica. Más adelante, se podrá configurar todos los parámetros para una correcta automatización como son el idioma, la localización etc.

Para poder ver en nuestra interfaz de Domoticz los dispositivos que ya hemos conectado a través del módulo Z-Wave al software Z-Way se deberá ir a la pestaña de configuración del Hardware. Una vez dentro, lo primero será seleccionar un nombre al Hardware externo (el módulo Z-Wave) con el cual podremos identificarlo de otros posibles hardware que se podrán añadir al futuro. Después, se seleccionará el tipo de hardware que se quiere añadir, en este caso se trata del módulo RaZberry, pero a pesar de estar conectado a los puertos GPIO y existir una opción de añadir llamada *Raspberry's GPIO port* y *Razbeery Z-Wave via LAN interface (HTTP)*, la comunicación se realizará a través de la simulación de un módulo Z-Wave a través de conexión USB, simulación que se realiza de forma automática con las últimas versiones de Z-Way y Domoticz como ya se ha explicado anteriormente. Para ello se seleccionará la opción *OpenZWave USB* en el campo Tipo. Es importante asegurarse que en el campo *Serial Port* este seleccionada la dirección */dev/ttyAMA0* como se puede apreciar en la imagen inferior.

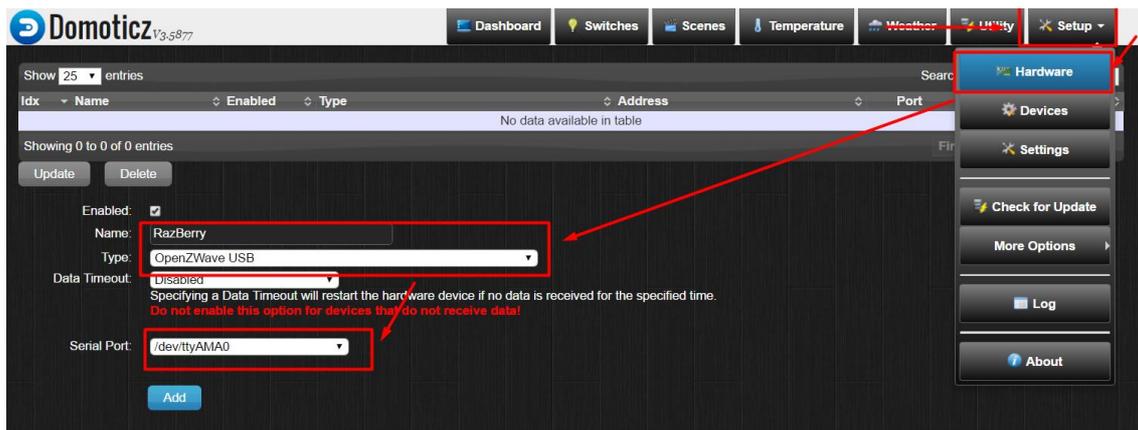


Figura 39. Pasos para añadir Z-Way a Domoticz

Una vez configurado el módulo Z-Wave con Domoticz, será posible el agregar o borrar dispositivos directamente desde la interfaz que ofrece Domoticz, sin necesidad de ir a al puerto 8083, puerto que nos ofrece la conexión Z-Way. Si ya existen dispositivos agregados previamente a través de Z-Way, estos se agregarán directamente al sistema de control Domoticz.

Para agregar, borrar o realizar más tareas relacionadas con los módulos Z-Wave, se deberá de pinchar en el botón *Setup* Localizado dentro de la pestaña

Hardware. Una vez dentro, se podrán visualizar que dispositivos están agregados, con una breve descripción si es posible. En la imagen inferior, se puede apreciar como ya se encuentra el sensor triple de la marca Fibaro FGMS001. Pinchando en *Node management* se podrán realiza las diferentes tareas mencionadas anteriormente.

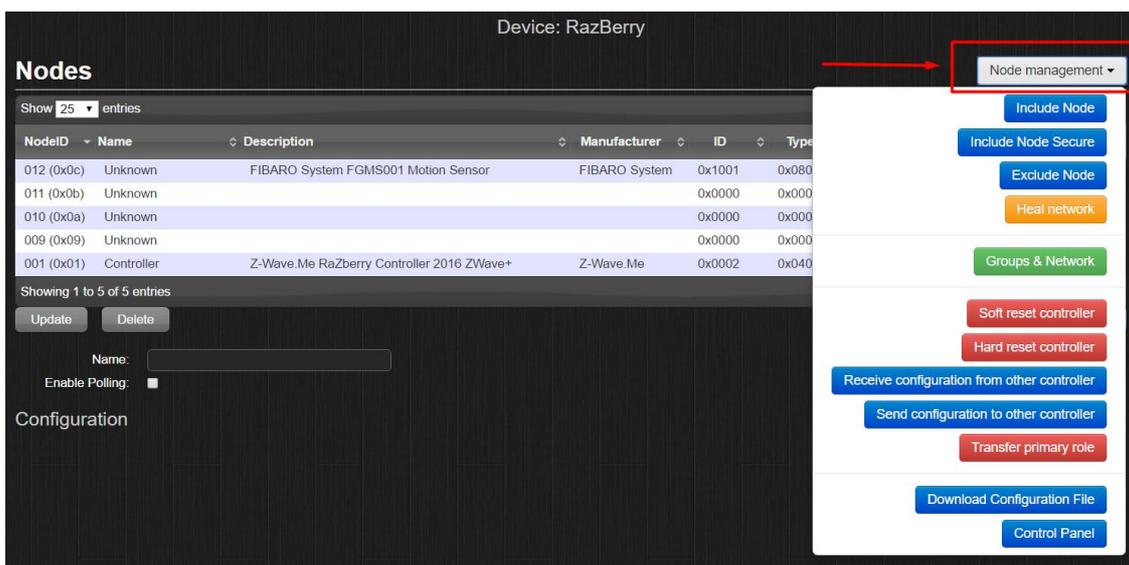


Figura 40. Opciones para agregar, borrar o configurar los dispositivos Z-Wave

Tanto si se pulsa para agregar como para borrar un dispositivo, se abrirá una nueva ventana en la cual se indicará que la pasarela se encuentra en modo aprendizaje, en ese momento se deberá de poner los dispositivos en modo aprendizaje para que se realice la configuración. En la mayoría de dispositivos Z-Wave, estos cuentan con un botón que se deberá de pulsar tres veces, aun así cada fabricante ofrece la forma que tienen sus dispositivos para ser agregados a las pasarelas domóticas.

También a través de esta pestaña, pinchando en los dispositivos que ya se encuentran agregados como es el caso del FGMS001, se podrá configurar los distintos parámetros que los dispositivos Z-Wave tiene, como pueden ser por ejemplo establecer un nombre al dispositivo, la sensibilidad del dispositivo, como debe de comportarse las notificaciones LED, etc.

Ante la existencia de numerosos dispositivos que usan el protocolo de comunicación Z-Wave, así como la gran cantidad de distintos y cada vez más fabricantes existentes, existe la posibilidad de que algunos dispositivos no permitan poder visualizar los parámetros configurables, sin embargo esto no quiere decir que sean incompatibles, si no que la configuración de los parámetros de estos dispositivos será "a ciegas" estableciendo manualmente el número del parámetro, el tipo y el valor que debe de tener.

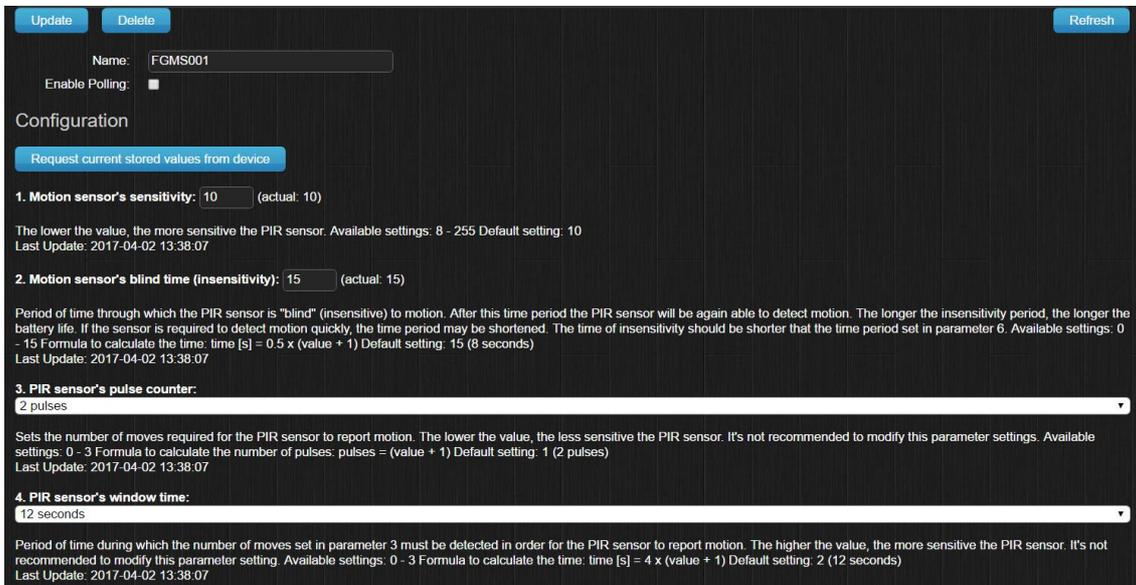


Figura 41. Ejemplo de configuración de parámetros de un dispositivo Z-Wave

De esta forma, se podrán agregar, borrar y configurar todos los dispositivos domóticos Z-wave que se quiera, para después realizar todas las escenas y automatizaciones necesarias para una completa domotización del hogar, edificio, etc.

El software Domoticz es uno de los softwares para configuración domótica más avanzado y completo que existe actualmente. En el siguiente apartado se explicarán algunos aspectos de configuración avanzada del software.

Una de las funciones más destacadas es la de compartir dispositivos de otro controlador con Domoticz instalado, ya sea compartiendo tu los dispositivos o que otro controlador los comparta contigo. Para ello, si lo que se quiere es compartir los dispositivos agregados a la controladora, se deberá de habilitar esta opción registrándose previamente en myDomoticz.

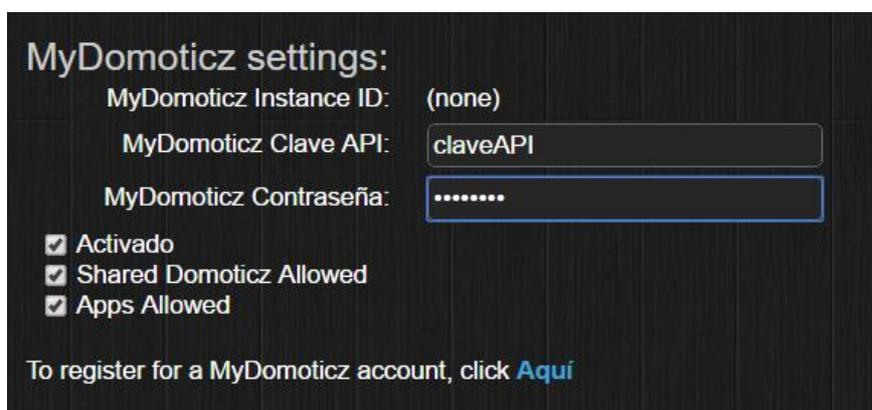


Figura 42. Habilitar acceso desde otro controlador

Para configurar el software para poder conectarse a otra pasarela remota, se deberá de hacer de la misma forma que se agrega cualquier hardware, seleccionando en el modelo de hardware "Domoticz – Remote server", donde se deberá de establecer

la dirección IP del otro controlador remoto, el puerto por el que está configurado, el nombre de usuario y contraseña para poder acceder al software (y a los dispositivos agregados a este).



The screenshot shows a configuration window for a remote server. The fields are as follows:

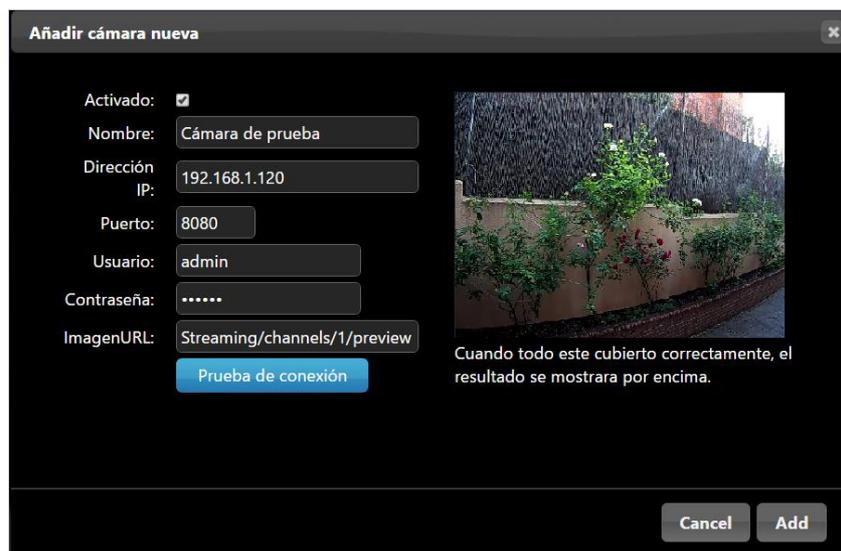
- Activado:
- Nombre: Servidor Domoticz remoto
- Tipo: Domoticz - Remote Server
- Tiempo de espera: Deshabilitado
- Dirección Remota: 192.1.1.1
- Puerto: 8080
- Usuario: admin
- Contraseña: *****

Below the 'Tiempo de espera' field, there is a warning: "Especificando un tiempo de espera, se reiniciará el dispositivo de hardware si no se reciben datos durante el tiempo especificado. ¡No habilite esta opción para dispositivos que no reciben datos!"

Figura 43. Configuración acceso a otro controlador

Otra de las cosas interesantes es la de poder visualizar la mayoría de modelos de cámaras IP de consumo del mercado. Un aspecto muy importante es el de la codificación en la que se muestran las imágenes, la gran mayoría de controladores no son capaces de conectarse a un flujo de video con codificación H.264 o similar, si no que se debe de conectar a un flujo de video configurado en codificación MJPG o MJPEG, además de realizar la petición de video a través de HHTP en lugar de RTSP (Real Time Streaming Protocol. o protocolo de transmisión en tiempo real).

La URL que permite conectarse a las cámaras lo debe de facilitar el fabricante de estas, aunque de no ser así por internet esta la gran mayoría de URL necesaria para la configuración de estas. Por ejemplo, para el fabricante de cámaras Hikvision, mayor fabricante de cámaras de CCTV del mundo, la URL para poder visualizar la cámara (después de establecer el flujo secundario de la cámara en MJPG, dado que para la gran mayoría de cámaras de este fabricante el flujo de video principal solo se puede con codificación H.264) sería *Streaming/channels/1/preview*



The screenshot shows a dialog box titled "Añadir cámara nueva" with the following fields:

- Activado:
- Nombre: Cámara de prueba
- Dirección IP: 192.168.1.120
- Puerto: 8080
- Usuario: admin
- Contraseña: *****
- ImagenURL: Streaming/channels/1/preview

Below the fields is a blue button labeled "Prueba de conexión". To the right of the fields is a preview window showing a live video feed of a garden. Below the preview window, there is a note: "Cuando todo este cubierto correctamente, el resultado se mostrara por encima." At the bottom right of the dialog are "Cancel" and "Add" buttons.

Figura 44. Ejemplo de añadir cámaras IP

Otro de los puntos importantes con los que cuenta el software Domoticz es el de poder mandar notificaciones a los usuarios (para un elevado número de sistemas, como

puede ser iOS, Android o Windows). En la siguiente imagen se puede ver como para la gran mayoría de sistemas la configuración es la misma.

Notificaciones

Prowl (iPhone/iPad):
Activado:
Clave API: **Test**
Haz click para conseguir una cuenta/clave API [Aquí](#)

PushBullet:
Activado:
Clave API: **Test**
Haz click para conseguir una cuenta/clave API [Aquí](#)

Pushover (Android/iOs):
Activado:
CLAVE DE USUARIO:
Clave API: **Test**
Haz click para conseguir una cuenta/clave API [Aquí](#)

NMA (Android):
Activado:
Clave API: **Test**
Haz click para conseguir una cuenta/clave API [Aquí](#)

Pushsafer (iOS/Android/Windows10/Chrome/Firefox):
Activado:
Clave API: **Test**
Haz click para conseguir una cuenta/clave API [Aquí](#)

Pushalot (Windows/Windows Phone):
Activado:
Clave API: **Test**
Haz click para conseguir una cuenta/clave API [Aquí](#)

Figura 45. Configuración de notificaciones

Además, está la posibilidad de realizar notificaciones más avanzadas a través de una URL. Dado que el conocimiento de este tipo de acciones se separa de la materia enseñada a lo largo del grado, no se entrará en la descripción de estos.

HTTP Personalizado/Acción:
Activado:
#FIELD1:
#FIELD2:
#FIELD3:
#FIELD4:
#TO:
URL/Acción:
(Debe comenzar con http:// o script//)
(Opcional) #SUBJECT, #MESSAGE, #PRIORITY
POST Data:
(Opcional) #SUBJECT, #MESSAGE, #PRIORITY
POST Content-Type: **Test**
POST Headers:

Figura 46. Configuración de acciones HTTP para notificaciones

Desde la opción LOG de cada dispositivo, se podrá visualizar el historial de cada sensor, a través de un gráfico a lo largo del día, del mes y del año, pudiendo descargarse de distinta forma como puede ser imagen JPG, archivo PDF, o descargar un archivo CSV para posteriormente usar estos parámetros para realizar otras tareas. Además, Domoticz incluye su propio LOG de incidencias, donde se podrá ver todo lo que ha ocurrido de cara a buscar posibles fallos que puedan ocurrir en el sistema



Figura 47. Ejemplo del LOG de un dispositivo

| Todo | Estado | Error |
|------------|--------------|---|
| 2017-04-02 | 17:17:05.660 | Domoticz V3.5877 (c)2012-2016 GizMoCuz |
| 2017-04-02 | 17:17:05.660 | Build Hash: 15b013c, Date: 2016-11-10 16:44:33 |
| 2017-04-02 | 17:17:05.660 | Startup Path: /home/pi/domoticz/ |
| 2017-04-02 | 17:17:05.918 | Sunrise: 07:56:00 SunSet:20:37:00 |
| 2017-04-02 | 17:17:05.918 | EventSystem: reset all events... |
| 2017-04-02 | 17:17:05.990 | Active notification subsystems: (0/12) |
| 2017-04-02 | 17:17:06.021 | WebServer(HTTP) started on address: :: with port 8080 |
| 2017-04-02 | 17:17:06.072 | Error: WebServer(SSL) startup failed on address 0.0.0.0 with port: 443: resolve: Host not found (authoritative) |
| 2017-04-02 | 17:17:06.073 | Error: WebServer(SSL) check privileges for opening ports below 1024 |
| 2017-04-02 | 17:17:06.073 | Proxymanager started. |
| 2017-04-02 | 17:17:06.075 | Starting shared server on: :::6144 |
| 2017-04-02 | 17:17:06.075 | TCPserver: shared server started... |
| 2017-04-02 | 17:17:06.075 | RxQueue: queue worker started... |
| 2017-04-02 | 17:17:08.076 | EventSystem: reset all events... |
| 2017-04-02 | 17:17:08.076 | EventSystem: reset all device statuses... |
| 2017-04-02 | 17:17:08.077 | EventSystem: Started |
| 2017-04-02 | 17:17:08.576 | OpenZWave: Starting... |
| 2017-04-02 | 17:17:08.585 | OpenZWave: Version: 1.4-2228-gb0e4a88-dirty |
| 2017-04-02 | 17:17:08.585 | OpenZWave: using config in: /home/pi/domoticz/Config/ |
| 2017-04-02 | 17:17:08.828 | OpenZWave: Driver Ready |
| 2017-04-02 | 17:17:08.828 | OpenZWave: Invalid NodeID received. HomeID: 4028818463, NodeID: 0 (0x00) |
| 2017-04-02 | 17:17:08.831 | OpenZWave: Value_Added: Node: 9 (0x09), CommandClass: SENSOR BINARY, Label: Sensor, Instance: 0 |
| 2017-04-02 | 17:17:08.832 | (RazBerry) Light/Switch (Sensor) |
| 2017-04-02 | 17:17:08.838 | OpenZWave: Value_Added: Node: 10 (0x0a), CommandClass: SWITCH BINARY, Label: Switch, Instance: 1 |
| 2017-04-02 | 17:17:08.839 | (RazBerry) Light/Switch (Switch) |
| 2017-04-02 | 17:17:08.844 | OpenZWave: Value_Added: Node: 11 (0x0b), CommandClass: ALARM, Label: Alarm Type, Instance: 1 |
| 2017-04-02 | 17:17:08.844 | (RazBerry) Light/Switch (Alarm Type) |
| 2017-04-02 | 17:17:08.848 | OpenZWave: Value_Added: Node: 11 (0x0b), CommandClass: ALARM, Label: Alarm Level, Instance: 1 |
| 2017-04-02 | 17:17:08.849 | (RazBerry) Light/Switch (Alarm Level) |
| 2017-04-02 | 17:17:08.853 | OpenZWave: Value_Added: Node: 11 (0x0b), CommandClass: BATTERY, Label: Battery Level, Instance: 1 |
| 2017-04-02 | 17:17:08.856 | OpenZWave: Value_Added: Node: 12 (0x0c), CommandClass: SENSOR BINARY, Label: , Instance: 0 |
| 2017-04-02 | 17:17:08.856 | OpenZWave: Value_Added: Node: 12 (0x0c), CommandClass: SENSOR MULTILEVEL, Label: , Instance: 1 |
| 2017-04-02 | 17:17:08.856 | OpenZWave: Value_Added: Unhandled Label: , Unit: |
| 2017-04-02 | 17:17:08.857 | OpenZWave: Value_Added: Node: 12 (0x0c), CommandClass: SENSOR MULTILEVEL, Label: , Instance: 3 |
| 2017-04-02 | 17:17:08.857 | OpenZWave: Value_Added: Unhandled Label: , Unit: |
| 2017-04-02 | 17:17:08.860 | OpenZWave: Value_Added: Node: 12 (0x0c), CommandClass: BATTERY, Label: , Instance: 1 |

Figura 48. Ejemplo del LOG del software

5.5 Conexión a la Raspberry Pi y al control domótico a distancia.

Un apartado muy importante en la realización de este TFG es el de poder comunicarse con el controlador domótico de forma remota, es decir, sin necesidad de estar en la misma red local que se encuentra la Raspberry Pi. Por esta razón no es posible conectarse a través de la IP local y los puertos configurados que tiene la Raspberry Pi (192.168.1.200:8080 y 192.168.1.200:8083), pues estas direcciones son simplemente direcciones locales, no son válidas para la conexión en remoto.

Para poder solucionar el problema de la conexión en remoto, se van a analizar dos formas diferentes de poder conseguirlo: la primera, será a través de una ampliación de la red local, también conocido como red privada virtual (RPV) o por sus siglas en inglés: Virtual Private Network (VPN). Se trata de una tecnología de red de computadoras la cual permite la conexión de diferentes ordenadores o dispositivos situados en distintas redes a la red local comportándose como si estuviesen conectadas a la misma red, es decir, se trata de una ampliación o extensión de la red de área local (LAN). Esto es posible gracias a establecer una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Se trata una forma de conexión en remoto muy usada a día de hoy. Algunos ejemplos de su uso son a nivel empresarial el permitir la conexión de los dispositivos como pueden ser un ordenador personal y un NAS o almacenamiento conectado en red sin necesidad de estar en la misma sucursal ambos. Para el proyecto realizado sería una opción perfectamente válida pues nos permitiría la conexión con la Raspberry Pi desde cualquier lugar del mundo como si estuviésemos en la misma red.

Es un sistema de conexión en remoto muy seguro por sus propias características, entre las que se pueden destacar respecto al tema de la conexión y la seguridad:

- Autenticación y autorización de todos los usuarios/equipos conectados. No es posible conectarse a ella sin tener los permisos necesarios.
- Cualquier mensaje que se vaya a mandar debe de estar cifrado antes de salir a internet, de tal forma que si fuese interceptado entre medias del camino no sería posible su lectura por parte de alguien que o sean los destinatarios de la misma. Es, por tanto, un sistema con confidencialidad y privacidad.
- Los datos enviados no pueden ser alterados. Esto se asegura a través de funciones de Hash.
- Los mensajes tienen que ir firmados, aquel usuario que mande un mensaje no puede negarse a firmar quien es el que lo manda, se trata por tanto de un sistema sin la posibilidad de repudio.
- Se debe realizar una auditoría y registro de actividades para asegurar el correcto funcionamiento de la red.
- Se debe de asegurar una calidad de servicio con buen rendimiento y que no exista una degradación a un nivel aceptable en la velocidad de transmisión.

El tema del conexionado y configuración, así como de los distintos tipos de VPN que hay podría darse como un tema de gran interés y complejidad, el cual podría dar para un trabajo nuevo sobre la extensión de red local.

La conexión a través de una VPN, aunque es muy segura y eficaz, posee una cierta complejidad a la hora de configurar en una Raspberry Pi, y dado que en el TFG aquí expuesto no se va a tratar el tema de la mejor conexión y más segura en formato remoto, se ha decidido buscar un formato de conexión en remoto más sencillo pero que resulte totalmente eficaz. Es por este motivo, que la conexión en remoto se realizará a través de un servidor de DNS dinámico, más conocido como DynDNS o DDNS.

Un servicio de DNS dinámico o DDNS es un servicio que permite la actualización de las bases de datos y la información en tiempo real sobre los nombres de dominio y las direcciones IP que tienen situado en un servidor de nombres. El uso que se le da a estos servicios es el de la conexión a dispositivos o servicios que no disponen de una dirección IP fija, sino una IP variable o dinámica, a través de un nombre o un dominio de internet.

Explicado de forma sencilla, consiste en una base de datos en la cual se relacionan las direcciones IP y los dominios de internet relacionados con esa dirección IP, conectándose entre ellos según se pida la dirección o el dominio, actualizándose prácticamente en tiempo real, de tal forma que, si se quisiera acceder a la web de la Escuela Politécnica Superior de la Universidad de Alcalá de Henares, se puede hacer a través de su dominio (<http://escuelapolitecnica.uah.es/>) o con la conexión a través de la dirección IP directamente. La conexión a través del dominio resulta más sencilla, pues es más fácil de recordar por el usuario final y se trata de una dirección la cual no va a cambiar, sino que es constante, a diferencia de las direcciones IP que no sean fijas, las cuales suponen una cuota temporal y consecuentemente un coste.

En la actualidad, existen diferentes servidores que se encargan de ofrecer estos servicios DDNS a los usuarios, ya sean de pago o gratuitos. Entre los más destacados y que suponen un ejemplo de estas dos formas son las plataformas DynDNS y No-IP. La primera se trata del servicio DNS dinámico más popular y más extendido, plataforma que durante mucho tiempo ofrecía un servicio completamente gratuito a los usuarios, pero desde el año 2014 cerró la parte gratuita, quedando solo la parte de pago o Premium con un precio de \$40 al año. Al tratarse de una plataforma muy fiable, el servicio que ofrecen es prácticamente a prueba de fallos o errores en la conexión, además de permitir su configuración en la gran mayoría de dispositivos que tienen la capacidad de conexión a servidores DDNS.

La otra plataforma de conexión a través de DDNS es No-IP, alternativa con gran popularidad y muy estable que cuenta con un elevado número de usuarios. Ofrece unos servicios muy similares a DynDNS pero al tratarse de una alternativa gratuita tiene algunas limitaciones como son la de registrar hasta un máximo de 3 host DDNS de forma gratuita, aunque esta capacidad es suficiente para la gran mayoría de los usuarios.

Dado que los requisitos no son muy complejos ya que únicamente se quiere el acceso a una Raspberry Pi en remoto se ha optado por la decisión de la plataforma gratuita No-IP. Aunque en el mercado existen muchas otras opciones como son FreeDNS, DNS Exit, ChangeIP o DNS-O-Matic.

5.5.1 Configuración de Router y puertos

La configuración de cada router es distinta dependiendo del fabricante y del modelo, pero se asemejan en la mayoría de los aspectos y configuraciones posibles, por lo que se podrá extrapolar a la inmensa mayoría de estos.

Lo primero será conectarnos al router a través de su dirección IP (192.168.1.1 por norma general), y una vez dentro ir a la sección de Ajustes avanzados y DNS Dinámico. En el router que se está configurando, una vez dentro habrá que pulsar en añadir para poder configurarlo.

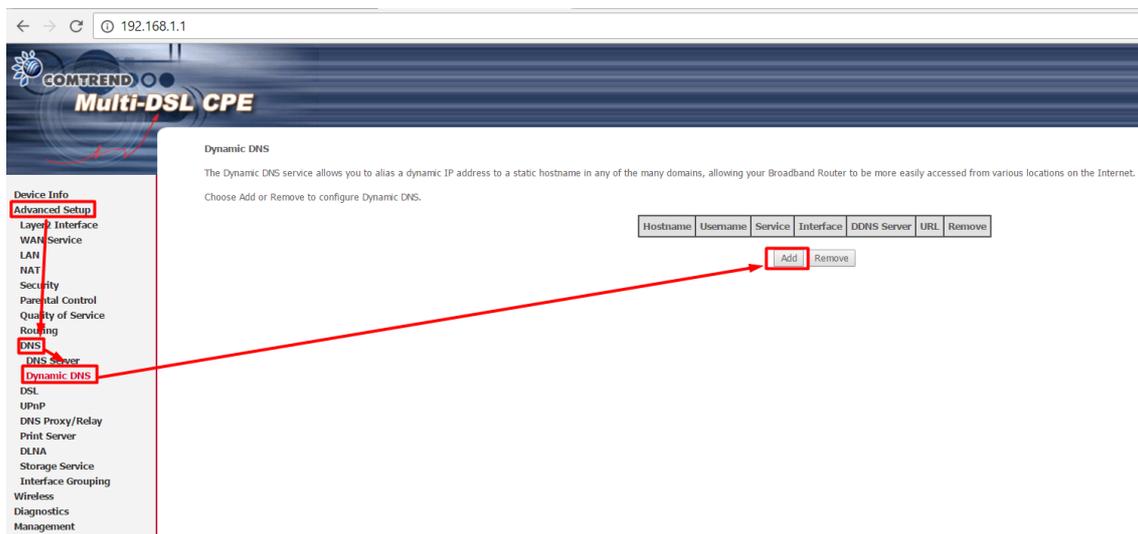


Figura 49. Añadir servidor DDNS

Por defecto, en la mayoría de router ya existen una serie de servidores de DNS dinámico pre configurados. En el que se está usando durante la realización del TFG, las plataformas de DNS disponibles son DynDNS, TZO y configurar la conexión con otro servicio DDNS (custom). Al no encontrarse el servidor No-IP, plataforma que se va a usar durante la configuración para la conexión en remoto, la opción elegida será la de personalizar la conexión rellorando los campos necesarios para su configuración.

Lo primero será crearnos una cuenta en No-IP a través de su página web (<http://www.noip.com/>) que es tan sencillo como establecer un nombre al dominio que se le quiera dar y elegir la terminación (.hopto.org, .zapro.org, .ddns.net, ...). Como ejemplo y nomenclatura que se usará durante toda la explicación se ha escogido **NOMBRE.ddns.net**

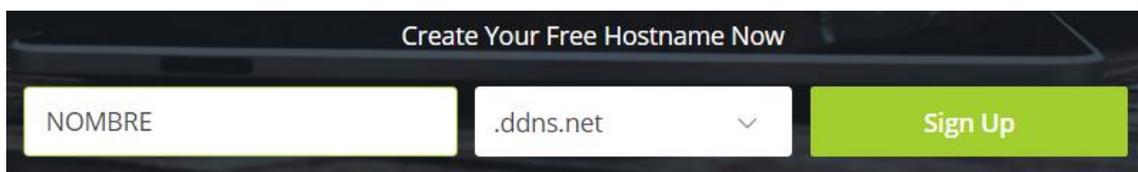


Figura 50. Elección del dominio DDNS

Una vez dentro, se deberá de seguir con la configuración a través de un email, una contraseña y un nombre de usuario. Posteriormente, será necesario activar la cuenta a través del correo de activación al email establecido previamente.

Una vez dentro, lo primero que se sugerirá será la de instalar un programa encargado de decirle a la cuenta de No-IP que se actualice con la nueva IP con la que cuenta el dispositivo en cada momento. Para evitar este programa en el cual además será necesario que el dispositivo se encuentre activo en todo momento para poder comunicar la dirección IP que tiene, la configuración y el encargado de decir a la cuenta la dirección que tiene en todo momento será el router. En los parámetros de configuración que antes nos pedían, deberán de rellenarse con el contenido que muestra la siguiente imagen.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO. Additionally, it is possible to configure a Custom Dynamic DNS service.

| | |
|---------------|-----------------------|
| DDNS provider | Custom ▼ |
| Hostname | NOMBRE.ddns.net |
| Interface | internet_atm/ppp0.1 ▼ |

Custom DDNS Settings

| | |
|---------------|---------------------|
| DynDNS Server | dynupdate.no-ip.com |
| URL | /nic/update? |
| Username | NOMBRE-USUARIO |
| Password | ***** |

Apply/Save

Figura 51. Configuración del servicio DDNS en el router

Una vez configurado este campo, el siguiente paso será el de establecer y abrir los puertos para la conexión. Lo que se va a realizar es que cada vez que desde el lado exterior del router (o tráfico WAN) se solicite la conexión a un puerto específico, el propio router lo redirección a la dirección IP local de la Raspberry Pi y al puerto por el que se está sirviendo la interfaz de usuario de Domoticz, es decir, a través de la dirección *NOMBRE.ddns.net:puerto* se conecte a la *192.168.1.200:8080*, dirección en la cual está servida la interfaz. Esta configuración también se hace desde la interfaz del router y en cada caso estará situado en un sitio distinto.

Una vez localizada la configuración de puertos, se pulsará en agregar y se procederá a su configuración. Esto es bastante sencillo, pues bastará con darle un nombre a esa conexión para poder tenerlo controlado, la dirección IP local a la cual irá destinado, la dirección del puerto Externo, la dirección del puerto interno y el tipo de protocolo. Se puede configurar una serie de puertos externos eligiendo su inicio y si final y orientar todas esas direcciones al mismo puerto interno. A la hora de elegir protocolo existen tres opciones: TCP, UDO y TCP/UDP. Las diferencias entre estos protocolos es el fin que tiene cada una: mientras TCP está pensado y orientado para la conexión, es

decir, que no se pierda información durante el trayecto, si no que todo lo que se transmite desde un punto llegue completamente sin perder nada de información al otro, pudiendo ser un protocolo de transmisión más lento, pues lleva un ACK de que le ha llegado un paquete previo y si se diese el caso de faltarle alguno se encargaría de volver a pedir que se le envíe el mismo paquete hasta asegurarse que esta toda la información al completo. El protocolo UDP es al contrario, está pensado para transmisiones más rápidas en las cuales no resulta de vital importancia que se pueda perder algún paquete durante la transmisión, siendo un protocolo de transmisión muy usado para la transmisión de tramas de video o audio, como puede ser por ejemplo en la transmisión de video de una cámara de video vigilancia IP. Lo normal sería la configuración a través del protocolo TCP, pero si existiesen dudas se puede elegir la opción TCP/UDP para asegurarnos que se abre el puerto realmente de la forma necesaria y requerida en cada caso.

Service Name:

Select a Service:

Custom Service:

Server IP Address:

| External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End |
|---------------------|-------------------|-----------|---------------------|-------------------|
| 3001 | 3001 | TCP/UDP ▼ | 8080 | 8080 |
| | | TCP ▼ | | |
| | | TCP ▼ | | |

Figura 52. Configuración de puertos

Para este TFG, se ha escogido que el puerto externo sea el 3001 al no encontrarse ocupado por ningún otro servicio y para configurarlo de tal forma que el puerto externo de conexión fuese distinto al puerto usado internamente. Una vez configurado esto, ya será posible la conexión en remoto desde cualquier lugar con la dirección *NOMBRE.ddns.net:3001*.



Figura 53. Conexión remota a través de servidor de DNS dinámico

6. Conclusiones y líneas futuras

Todo apunta a que el siguiente paso tecnológico que sufriremos será el de la cada vez mayor integración de la domótica en nuestro día a día, por este motivo el seguir el avance que esta está teniendo en nuestra sociedad se convierte en una actividad muy dinámica y entretenida.

Es importante añadir que para que pueda llegar a todo el mundo será necesario que tenga un precio relativamente bajo, y esto se está consiguiendo poco a poco gracias al número de fabricantes de productos domóticos y la universalización de un protocolo de comunicación, por lo que en los próximos años es muy posible que los actuales precios de todo lo relacionado con el mundo domótico vaya bajando de precio, pero aun así, el trabajo aquí realizado sirve como ejemplo de que se puede conseguir un controlador domótico a un precio muy razonable, además de servir como experiencia para conocer un poco más acerca del mundo GNU/Linux y del mundo de las redes y la conexión en remoto.

Esas experiencias me han servido para poder investigar por mi cuenta y conocer algunos términos acerca del mundo de las redes, como pueden ser los servidores DDNS, las diferentes formas de conexión en remoto, la conexión a través de los puertos, la importancia de la dirección IP externa y local o la comunicación con otro terminal a través de comandos por SSH, siendo un trabajo muy fructífero al abarcar tantos términos que de forma natural no se explican en el grado que he estudiado y en el cual he realizado el TFG aquí expuesto. También ha sido un trabajo que me ha aportado el conocer cómo está la situación actual en el mundo de la domótica y empezar a entender hacia donde parece que se dirige en un futuro cercano.

Los posibles trabajos futuros relacionados con el diseño de un controlador domótico de bajo precio pueden ir encaminados por distintas ramas o posibles aplicaciones nuevas que se puedan añadir:

- Mejorar la seguridad a la hora de conectarse en remoto con la Raspberry Pi. La forma de comunicación que se ha realizado es una forma simple de conexión, aunque no resulta muy segura al no necesitar ni un usuario ni contraseña para poder conectarse a ella. Se podría realizar a través de una conexión VPN como ya se explicó en el apartado 5.5 Conexión a la Raspberry Pi y al control domótico a distancia.
- Para evitar depender de otras partes o de terceros, se podría configurar para que la Raspberry hiciese de servidor DDNS, trabajo más relacionado con algún estudio sobre redes.
- Sería muy interesante ampliar la cantidad de dispositivos de diferentes protocolos con los que el controlador domótico pueda comunicarse, como puede ser con los dispositivos EnOcean mediante la instalación, por ejemplo, de un pen drive capaz de comunicarse por el protocolo EnOcean, y su integración en el sistema.
- Por último, otra posible opción de ampliación del trabajo realizado es la de la creación por completo de una interfaz gráfica más sencilla al usuario final pero capaz de gestionar todos los dispositivos

7. Resumen económico

El trabajo aquí realizado ha sido pensado para que resulte lo más económico posible, de tal forma que se puede acoplar a prácticamente todas las personas que quieran domotizar una vivienda, una comunidad, un edificio, etc. Basándonos en esta premisa, se podrá observar como al finalizar el resumen económico este queda con un precio total de un valor relativamente bajo, llegando a ser incluso más barato que otras pasarelas que actualmente se encuentran en el mercado. Para el cálculo del presupuesto total se va a calcular todos los elementos necesarios, desde los cables o alimentadores hasta los dispositivos Z-Wave utilizados.

El resumen económico se podría dividir de la siguiente forma:

- Controlador → Raspberry Pi 3 Model B. Se trata del modelo más actual de Raspberry y consecuentemente el modelo más potente y actualizado. Se puede comprar por internet a un precio de 39.9€ en Amazon.
- Módulo Z-Wave → Para poder comunicarse con los diferentes dispositivos a través del protocolo Z-Wave, será necesario añadir un dispositivo que transforme las órdenes recibidas por el puerto GPIO a ordenes Z-Wave. En la actualidad existen pen drives que pueden realizar esta función o la opción escogida para este TFG como son los módulos RaZberry (disponible en 2 versiones). Se puede comprar por 54.33€ en Amazon o por 59€ en la página zwave.es.
- Tarjeta Micro SD → Necesaria para almacenar todos los archivos y el sistema operativo en la Raspberry. Se recomienda una tarjeta micro SD de 16 GB, disponibles en Media Markt por 6.99€.
- Alimentador → Alimentado a través de 5V 2A con conexión micro USB, se podrá cargar con un gran abanico de cargadores existentes en el mercado. Se ha optado por un alimentador NorthPada con un precio de 6.22€.

- Cable HDMI → Para la visualización del escritorio ofrecido por la Raspberry. Se podría prescindir de este artículo si se conecta a través de SSH. Comprado un cable de 1.8 metros a Visiotech por un precio de 5€.
- Cable UTP → La conexión a Internet se puede realizar a través de cable UTP o por WiFi. Por si se quisiese realizar la conexión cableada, se puede comprar en Visiotech un cable UTP categoría 5E de 2 metros por 3€.
- Teclado y Ratón → Para poder controlar el escritorio y la interfaz gráfica ofrecida por la Raspberry y por los distintos Software usados. Se ha optado por un combinado de teclado y ratón de la marca Tsing que se puede obtener a través de Amazon por 13.99€.
- Pantalla → Para poder visualizar el escritorio y el soporte ofrecido por Domoticz, se puede hacer uso de una pantalla con salida HDMI dado que es el tipo de salida con el que cuenta la Raspberry. Se podría coger por ejemplo un monitor de 18.5" TFT LCD de ASUS VS197BE comprado en Media Markt por 75€

Este material podría considerarse el estrictamente necesario para la instalación del controlador domótico basado en Raspberry, ya que los dispositivos actuadores y sensores compatibles con Z-Wave pueden variar mucho según los apartados que se quieran controlar y las necesidades de cada usuario. Con esto, el presupuesto necesario para poder instalar y controlar la pasarela variara entre 107.44 y 204.43€, un precio más bajo que la gran mayoría de pasarelas Z-Wave las cuales pueden llegar a tener un valor de 599€ como la Home Center 2 de Fibaro.

Los dispositivos Z-Wave usados en la realización del TFG se pueden comprar en la web de zwave.es y los elegidos para la instalación han sido:

- FGMS-001-ZW5 → Sensor triple (movimiento, luz y temperatura) de la marca Fibaro. Completamente inalámbrico con un precio de 57.99€.
- FGK-101 → Detector magnético para la apertura de puertas y ventanas. Cuenta con la posibilidad de instalar un sensor de temperatura y cualquier sensor con salida de contacto seco. Tiene un precio de 49.99€
- FGFS-101 → Sensor de inundación con sensor de temperatura integrado. Tiene un precio de 59.29€.
- FGSD-002 → Detector de humo con sensor de temperatura integrado. Tiene un precio de 64.99€.
- FGWPF-102 → Enchufe inteligente de reducido con protección contra sobretensiones y anillo LED multicolor para poder visualizar el consumo instantáneo de aquello que se encuentre conectado a él. Tiene un precio de 64.99€.

El precio total de los cinco dispositivos compatibles con el protocolo Z-Wave los cuales se han usado durante la realización de este trabajo cuentan con un precio total 297.25€, los cuales sumados al presupuesto anteriormente mencionado para la instalación del controlador domótico, hacen un presupuesto total para la realización del trabajo de 426.68€. Como ya se explicó anteriormente, el presupuesto de los dispositivos Z-Wave puede variar mucho según, por ejemplo, las acciones que se quieran controlar, el número de estancias, etc.

8. Manuales de usuario

En este apartado se puede encontrar un pequeño manual tanto para el instalador como para el usuario final, facilitando la configuración y el uso del control domótico aquí diseñado. En la página oficial de Domoticz se puede encontrar un archivo PDF con un manual de usuario en el cual se detallan algunos pasos para la configuración del sistema domótico, pero muy genérico debido a la gran cantidad de distintos dispositivos y las distintas formas que existen de agregarse. Por este motivo, algunas de las configuraciones existentes en el manual se podrán reusar sin problema mientras que otras solo se encuentran explicadas en este TFG.

Para comenzar la configuración, lo primero que se deberá de hacer es configurar los distintos dispositivos que se vayan a controlar, para ello se deberá de ir a la pestaña de *Hardware* dentro de *Setup*, pestaña que se encarga de la configuración de la comunicación de los distintos Hardwares instalados. Una vez dentro, se configurará el dispositivo instalado como ya se explicó en el apartado 5.4.4. *Adaptación de Z-Way con Domoticz*. Para el módulo Raspberry se seleccionará la opción *OpenZWave USB*, aunque no parezca relacionado la comunicación se realiza simulando que lo que está conectado a los puertos GPIO es en realidad un pincho Z-Wave a través de la conexión USB. Según el hardware que se quiera añadir, se deberá de rellenar unos parámetros u otros, como pueden ser la dirección IP si se trata de un dispositivo online, el usuario, la contraseña, etc.

Entre sus opciones, se encuentra la de poder compartir dispositivos entre diferentes usuarios, como puede ser una estación meteorológica o diferentes interruptores inteligentes para controlar la luz.

Una vez configurados los diferentes dispositivos que se quieran controlar, se procederá a configurar el sistema domótico. Esto se realizará a través de *Setup*→*Settings* donde se configurará el nombre, contraseña, localización y demás parámetros.

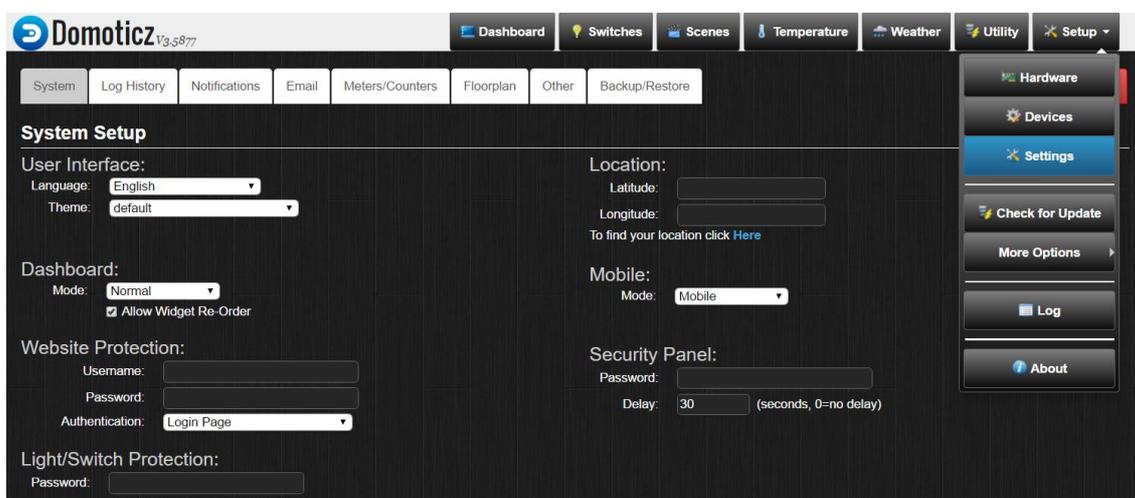


Figura 54. Configuración del apartado Settings del sistema Domoticz

Entre los diferentes parámetros configurables están el establecer el idioma, la localización de la pasarela para después usar escenas relacionadas con la climatología como pueden ser *“Si llueve, que se bajen las persianas de forma automática”* o *“A partir de X horas, enciende las luces de la entrada para que se pueda ver la puerta cuando llegue a casa”* por poner algunos ejemplos.

También se podrá configurar que pestañas queremos que se muestren, así como añadir un mapa con los planos y colocar los diferentes dispositivos en su localización.

Como resto de parámetros configurables destacables, se encuentran la de establecer un usuario y contraseña para acceder al control de la pasarela, la búsqueda de actualizaciones de forma automática, poder ver un historial de eventos, configurar las notificaciones en los teléfonos, notificaciones por email y establecer las unidades de medidas (m/s o mph por ejemplo para medir la velocidad del viento).

Para obtener una información más detallada sobre los diferentes parámetros configurables, es aconsejable visitar el manual que se encuentra en la página oficial de Domoticz como ya se avisó previamente, el cual cuenta además con diferentes capturas de la configuración. Destacar que al tratarse de un manual con algo de antigüedad (2 años en el momento que se realizó este TFG) por lo que algunas cosas han cambiado y no se muestran tal como en las fotos del manual. Sin embargo, estos posibles cambios no dificultan la configuración siendo bastante sencillo seguir los pasos.

Para poder fijar los dispositivos como Favoritos, lo primero será establecer que los vamos a usar. Para ello, habrá que ir a la pestaña de *Setup* → *Devices* y añadir los dispositivos como que van a ser usados a través de las flechas situadas a la derecha en cada dispositivo.

| Idx | Hardware | ID | Unit | Nombre | Tipo | SubTipo | Datos | Lat | Última Vista |
|-----|----------|---------|------|---------------------|--------------|--------------|---------|-----|---------------------|
| 9 | RazBerry | 0000D00 | 1 | Sensor | Light/Switch | Switch | Off | - | 2017-04-02 17:04:20 |
| 11 | RazBerry | 0000D03 | 255 | Lux FGMS001 | Lux | Lux | 770 Lux | - | 2017-04-02 17:03:53 |
| 10 | RazBerry | 0000D28 | 1 | General | Light/Switch | Switch | On | - | 2017-04-02 17:03:43 |
| 12 | RazBerry | 0D01 | 1 | Temperature FGMS001 | Temp | LaCrosse TX3 | 26.7 C | - | 2017-04-02 16:57:42 |

Figura 55. Establecer los dispositivos como que van a ser usados

Una vez asignados como que van a ser usados, dentro de la pestaña de cada dispositivo (Interruptores, temperatura, utilidades, etc.) se podrán visualizar estos dispositivos, pudiendo establecerlos como favoritos seleccionando la estrella que se encuentra en cada pestaña del dispositivo.

Lux FGMS001 **770 Lux**

 **770 Lux**
 Last Seen: 2017-04-02 17:03:53
 Type: Lux, Lux

 Log Editar Notificaciones

Figura 56. Selección de dispositivos favoritos

Una vez seleccionados los dispositivos como favoritos, estos aparecerán en la pestaña *Dashboard/Esritorio* pudiendo ver de una sola vista el estado de todos los dispositivos que tengamos agregados para posteriormente decidir qué se quiere realizar cuando estos detecten unos valores u otros. En la siguiente imagen, Se puede apreciar como en la ventana principal se podrán visualizar todos los detectores agregados, siendo en este ejemplo el sensor triple de Fibaro, donde se puede ver la temperatura donde está instalado, la luminosidad y se detecta movimiento o no (aunque este último aparezca como si se tratase de un interruptor de luz, detectará si hay movimiento o no indicándolo como apagado o encendido)

Domoticz v3.5877 Escritorio  Interruptores

2017-04-02 17:16:33 *▲07:56 ▼20:37

Dispositivos Luz/Interruptor:

Sensor Mov. **Apagado**

 Last Seen: 2017-04-02 17:13:18

Sensores de Temperatura:

Temperature FGMS001 **26.7° C**

 Last Seen: 2017-04-02 16:57:42

Sensores de Utilidades:

Lux FGMS001 **770 Lux**

 **770 Lux**
 Last Seen: 2017-04-02 17:03:53

Figura 57. Escritorio con los diferentes dispositivos agregados

Por último, para configurar todos los parámetros de los dispositivos asegurándonos que estos funcionen correctamente, se deberá de ir a la sección de configuración de nodos, agregar/excluir nodos a través del módulo Z-Wave, esto es a través de *Setup*→*Hardware*→*Setup* y seleccionar el dispositivo que se quiera configurar. Para la configuración de cada dispositivo es aconsejable visitar los manuales específicos de cada fabricante pues pueden proporcionar detalladas descripciones de todo lo que pueden hacer, como puede ser el seleccionar que tipo de pulsadores son los pulsadores en los que está instalado un módulo para controlar las persianas, si se trata de un pulsador estilo palanca, un switch on/off, etc.

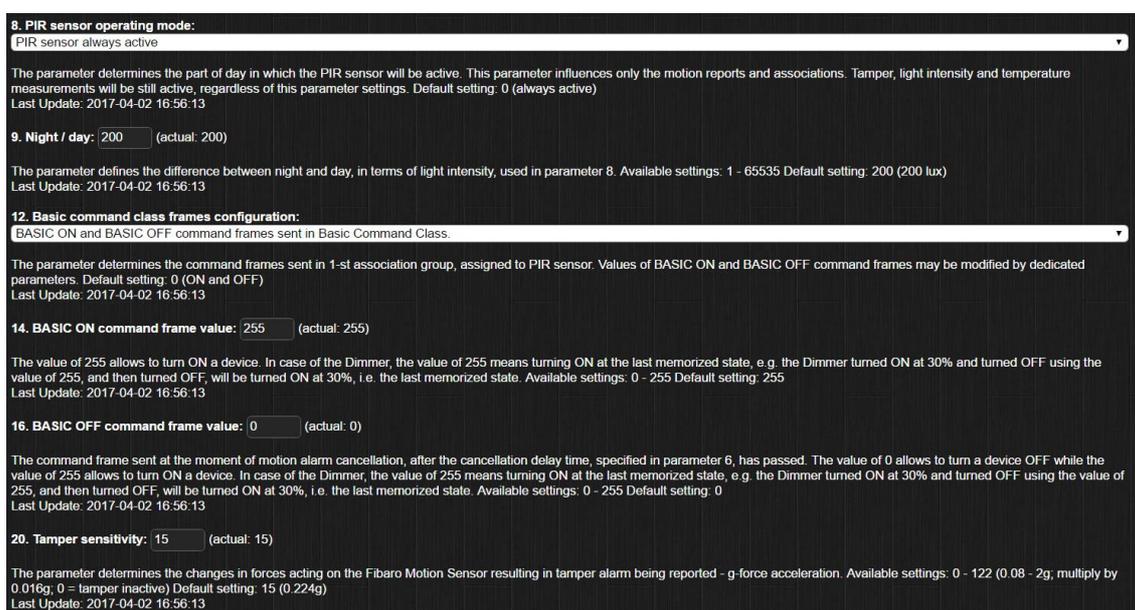


Figura 58. Ejemplo de parámetros configurables en un dispositivo

Gracias a la gran cantidad de parámetros configurables de la que disponen los dispositivos Z-Wave, estos permiten realizar una configuración ajustada a cada situación donde se quieran domotizar unas escenas, como puede ser hacer que el sensor de movimiento PIR sea más o menos sensible al movimiento para evitar falsas alarmas si se encuentran mascotas en la vivienda o es posible que pasen pájaros delante de la zona que se quiera controlar.

9. Bibliografía

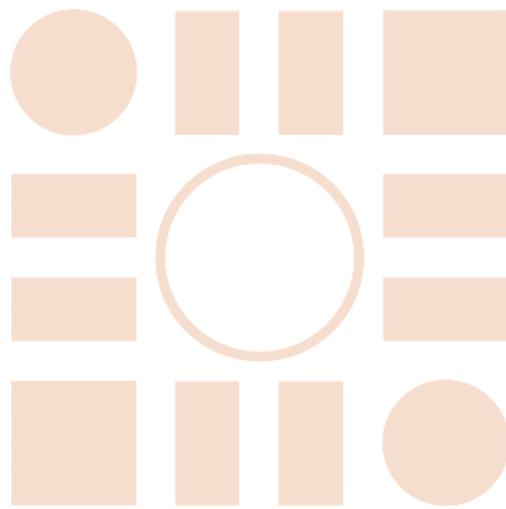
- Athom. (22 de Enero de 2017). *Información sobre comandos Z-Wave*. Obtenido de Z-Wave & Homey – A background story: https://blog.athom.com/2017/01/22/homey-z-wave-background-story/?utm_source=Athom+Newsletter&utm_campaign=a012f42077-EMAIL_CAMPAIGN_2017-01-27&utm_medium=email&utm_term=0_ac5b24c2f6-a012f42077-91383713
- Domodesk. (s.f.). *Información sobre protocolo Z-Wave*. Obtenido de A FONDO: Z-Wave, Sin Cables: <http://www.domodesk.com/a-fondo-z-wave-sin-cables>
- Domoticz. (Febrero de 2015). *Manual de usuario del programa Domoticz*. Obtenido de Domoticz Manual: <http://www.domoticz.com/DomoticzManual.pdf>
- Domoticz. (2016). *Problema con el módulo Bluetooth*. Obtenido de Domoticz, Pi3, RaZberry & Raspbian Jessie: <https://www.domoticz.com/forum/viewtopic.php?t=10964>
- KNX Partners. (Enero de 2008). Obtenido de <http://web.archive.org/web/20131231231228/http://www.knx.org/knx-partners/knxeib-partners/list/>
- Philippe. (4 de Enero de 2017). *Información sobre CES 2017*. Obtenido de Domótica doméstica: <http://www.domoticadomestica.com/ya-esta-aqui-ces-2017/>
- Raspberry. (4 de Abril de 2016). *Mapa esquemático de la Raspberry*. Obtenido de Raspberry Pi 3 Model B (Reduced Schematics): https://www.raspberrypi.org/documentation/hardware/raspberrypi/schematics/RPI-3B-V1_2-SCHEMATIC-REDUCED.pdf

- Raspberry. (s.f.). *Información general y ayuda sobre la Raspberry*. Obtenido de Raspberry: <https://www.raspberrypi.org/help/>
- Santa Barbara. (15 de Septiembre de 2015). *Información variada sobre protocolos*. Obtenido de Presentación Santa Bárbara – Home Automation: http://media.wix.com/ugd/bc1e92_54b9e22aff7f4c79b525c54c99ab612d.pdf
- Santa Barbara. (s.f.). *Información sobre Z-Wave*. Obtenido de Protocolo Z-Wave: <http://www.santabarbara.expert/protocolo-z-wave>
- Universidad de Oviedo. (s.f.). *Información sobre protocolo SCP*. Obtenido de Buses y protocolos en domótica e inmótica: <http://isa.uniovi.es/~sirgo/doctorado/UD7.pdf>
- Wikipedia. (16 de Noviembre de 2015). *Protocolo EnOcean*. Obtenido de EnOcean: <https://es.wikipedia.org/wiki/EnOcean>
- Wikipedia. (29 de Noviembre de 2016). *Información general sobre domótica*. Obtenido de Domótica: <https://es.wikipedia.org/wiki/Dom%C3%B3tica#Espa.C3.B1a>
- Wikipedia. (25 de Mayo de 2016). *Información sobre Bluetooth de baja energía*. Obtenido de Bluetooth de baja energía: https://es.wikipedia.org/wiki/Bluetooth_de_baja_energ%C3%ADa
- Wikipedia. (25 de Octubre de 2016). *Protocolo KNX*. Obtenido de KNX: <https://es.wikipedia.org/wiki/KNX>
- Wikipedia. (5 de Diciembre de 2016). *Protocolo X10*. Obtenido de X10: <https://es.wikipedia.org/wiki/X10>
- Wikipedia. (8 de Febrero de 2017). *ACK*. Obtenido de Acknowledgement (data networks): [https://en.wikipedia.org/wiki/Acknowledgement_\(data_networks\)](https://en.wikipedia.org/wiki/Acknowledgement_(data_networks))
- Wikipedia. (31 de Enero de 2017). *Distribución del sistema operativo GNU/Linux Raspbian*. Obtenido de Raspbian: <https://es.wikipedia.org/wiki/Raspbian>
- Wikipedia. (1 de Febrero de 2017). *Información sobre Bluetooth*. Obtenido de Bluetooth: <https://es.wikipedia.org/wiki/Bluetooth>
- Wikipedia. (18 de Febrero de 2017). *Información sobre DynDNS*. Obtenido de Dynamic DNS: https://en.wikipedia.org/wiki/Dynamic_DNS
- Wikipedia. (8 de Febrero de 2017). *Información sobre VPN*. Obtenido de Red privada virtual: https://es.wikipedia.org/wiki/Red_privada_virtual
- Wikipedia. (25 de Enero de 2017). *Protocolo Z-Wave*. Obtenido de Z-Wave: <https://en.wikipedia.org/wiki/Z-Wave>
- Wikipedia. (17 de Febrero de 2017). *TCP*. Obtenido de Transmission Control Protocol: https://es.wikipedia.org/wiki/Transmission_Control_Protocol
- Wikipedia. (17 de Febrero de 2017). *UDP*. Obtenido de User Datagram Protocol: https://es.wikipedia.org/wiki/User_Datagram_Protocol
- Wikipedia. (s.f.). *Protocolo ZigBee*. Obtenido de ZigBee: <https://es.wikipedia.org/wiki/ZigBee>

Z-Wave Barcelona. (s.f.). *Blog relacionado con el protocolo Z-Wave*. Obtenido de Blog Z-Wave: <http://zwavebarcelona.com/blog-zwave/>

Z-Wave.me. (s.f.). *Información sobre las actualizaciones de firmware RaZberry*. Obtenido de Download Z-Way for RaZberry: <http://razberry.z-wave.me/index.php?id=24>

Universidad de Alcalá
Escuela Politécnica Superior



ESCUELA POLITECNICA
SUPERIOR



Universidad
de Alcalá