ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO DE RADIOFRECUENCIA PARA BRINDAR GESTIÓN DE NETWORKING, SEGURIDAD Y CONFORT USANDO LOS PROTOCOLOS Z-WAVE Y ZIGBEE"

INFORME DE PROYECTO DE GRADUACIÓN

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN ELECTRICIDAD ESPECIALIZACIÓN ELECTRÓNICA Y AUTOMATIZACIÓN INDUSTRIAL

PRESENTADO POR:

GABRIEL ANDRÉS INTRIAGO VELÁSQUEZ

GUAYAQUIL – ECUADOR

2015

AGRADECIMIENTO

Al Estado Ecuatoriano por pagar mi educación en esta prestigiosa universidad.

A mi director, el Msc. Hólger Cevallos Ulloa., y a mi jefe el Ing. Tomislav Topic Granados por su ayuda y colaboración para la realización del presente trabajo.

A mis padres Raúl y Fátima y a mis hermanos Raúl y Andrés por su constante apoyo.

A Carlos Valle, quien me ayudó con el diseño de Networking.

A Eduardo Murillo, Duval Medina, Ricardo Íñiguez, Flavio Cabrera, Diógenes Villega y Guido Lindao.

DEDICATORIA

A DIOS por darme la vida y por permitirme nacer en Ecuador.

Al Club de Emprendedores de la ESPOL, mi tercer hogar.

A Rafael Vicente Correa Delgado y su Revolución Ciudadana.

A Sandro Llerena y Aníbal Vela Villao.

A Barcelona Sporting Club.

A Eckhart Tolle, Erik von Markovik y Owen Cook, mis maestros.

A Gaby Torres, mi gran amiga.

TRIBUNAL DE SUSTENTACIÓN

PhD. Sixto García

SUBDECANO DE LA FIEC

M.Sc. Hólger Cevallos Ulloa

DIRECTOR DEL PROYECTO DE GRADUACIÓN

M.Sc. Damián Larco Gómez

MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Informe, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de exámenes y títulos profesionales de la ESPOL)

GABRIEL ANDRÉS INTRIAGO VELÁSQUEZ

RESUMEN

El presente proyecto desarrolla e implementa un sistema domótico de radiofrecuencia. De manera general, se escogió la domótica de radiofrecuencia, ya que es menos costosa y más fácil de implementar que la domótica cableada, a parte, que en los últimos años ha ganado confiabilidad de operación y comunicación entre sus dispositivos.

Antes de iniciar con la parte técnica del proyecto, por cuestiones formales se inicia el documento presentando en el primer capítulo, la descripción del problema, solución, justificación, objetivos y metodología seguido del segundo capítulo donde se abarcan definiciones, conceptos y fundamentos teóricos de la domótica de manera general. Este capítulo incluye el funcionamiento y justificación de la selección de los protocolos domóticos de radiofrecuencia. Los protocolos de radiofrecuencia usados en el sistema domótico fueron Z-Wave y Zigbee, debido a su bajo consumo de potencia, funcionamiento de red en modo de malla, por la cantidad y tipo de dispositivos que usan estos protocolos en el mercado.

Luego, en el tercer capítulo se inicia la parte técnica del proyecto, con las generalidades, planos, sectorización y definición de las tres necesidades domóticas de la vivienda: networking, seguridad y confort. Posteriormente, en

el cuarto capítulo, se diseña el control del sistema domótico y se diseñan las tres necesidades domóticas las cuales son: 1) networking, 2) seguridad y 3) confort. Finalmente, en el quinto capítulo se muestra una análisis de costos dividido en tres categorías: 1) equipos, 2) instalación y 3) diseño y sumando los costos de cada categoría se realiza el costo total del proyecto.

ÍNDICE GENERAL

ABREVIATURAS

A	Amperios
AC	Corriente Alterna
AMA	Adaptación Automática del motor
AP	Access Point
Bit/s	bits por Segundo
CSMA-CA	Carrier Sense Multiple Access with collision avoidance
dBm	Decibelios por milivatio
DDR2	Double Data Rate type two
DNS	Domain Name Server
EOF	End of Frame
FSK	Frequency Shift Keying
GHz	Giga Hertz
GRC	Galvanized Rigid Conduit
HVAC	Heating, Ventilation, Air Conditioning
ID	Identificador
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
Kbit/s	Kilobits por Segundo
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol

LLC	Logical Link Control
m	Metros
MAC	Media Access Control
Mbit/s	Megabits por Segundo
MHz	Mega Hertz
MIPS	Microprocessor without Interlocked Pipeline Stages
mW	Mili Vatio
NAND	Not AND
°C	Grados Centígrados
PAN ID	Personal Area Network Identifier
QPSK	Quadrature Phase-Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
ROM	Read Only Memory
SDRAM	Synchronous Dynamic Random-Access Memory
SHF	Super High Frequency
SOF	Start of Frame
SSID	Service Set Identifier
SUC	Static Update Controller
UHF	Ultra High Frequency
UPnP	Universal Plug and Play
USB	Universal Serial Port

VAC	Voltaje de Corriente Alterna
VDC	Voltaje de Corriente Directa
VLAN	Virtual Local Area Network
W	Vatio
WAN	Wide Area Network
WLAN	Wireless Local Area Network

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente proyecto desarrolla e implementa un sistema domótico de radiofrecuencia.

En el Capítulo 1, se presenta, la descripción del problema, solución, justificación, la metodología y objetivo general y específicos del presente proyecto, objetivos y metodología empleada en el desarrollo del manual.

En el Capítulo 2, se mencionan conceptos de domótica. Se analiza la domótica de radiofrecuencia con sus ventajas y desventajas ante la domótica cableada. Se muestran las características de las redes domóticas y de networking con una pequeña descripción de los estándares de radiofrecuencia comunes en el mercado. Al final, se indica el funcionamiento y justificación de la selección de los protocolos Z-Wave y Zigbee.

En el Capítulo 3, se muestran los planos generales de la vivienda y se procede a su sectorización. Esto con la finalidad de una mejor distribución y ubicación de equipos. Luego se definen las necesidades de networking, seguridad y confort por sector de la vivienda.

En el Capítulo 4, se diseña el control del sistema domótico y también la gestión de cada una de las necesidades descritas en el capítulo 3,

incluyendo descripción de dispositivos con sus respectivas configuraciones necesarias para su correcto funcionamiento dentro del sistema domótico; se programan las escenas que permiten integrar los dispositivos y hacerlos funcionar entre ellos.

En el Capítulo 5, se realiza un análisis de costos de todo el proyecto dividido en tres categorías: equipos, instalación y diseño. Al final se suman los costos de cada categoría y se muestra el detalle de costos total del proyecto.

Finalmente, se efectúan las conclusiones y recomendaciones basadas en la realización del proyecto.

CAPÍTULO 1

ANTECEDENTES Y JUSTIFICACIÓN

1.1. Descripción del problema.

Para tener una visión más detallada y amplia de la descripción del problema, divido el problema en varios ‘subproblemas’ que se presentan a continuación:

1. Crear un sistema domótico de radiofrecuencia.
2. El sistema pueda manejar más de 100 dispositivos domóticos.
3. Crear una red privada interna de networking con dos enlaces de internet de 100 Mbps de ancho de banda.
4. A través de la red privada interna, debe estar disponible el control y monitoreo remoto y local del sistema domótico.
5. Se debe brindar la posibilidad de acceder a la red privada interna de manera alámbrica y de manera inalámbrica.

6. Monitoreo de la vivienda a través de cámaras en las siguientes secciones: frente de la vivienda, posterior de la vivienda, cocina, estudio, pasillo planta baja, biblioteca planta baja, pasillo planta alta y biblioteca planta alta.
7. Detección de apertura y cerrado de puertas que permitan iluminar sus respectivas áreas en la noche una vez abiertas.
8. Sensar el movimiento de personas durante la noche e iluminar las secciones por donde estas transitan.
9. Iluminación LED de las áreas mediante la tecnología Hue Philips.
10. Control de la climatización de la vivienda mediante termostatos.
11. Apertura de persianas dependiendo de si es día o de noche.
12. Crear una categorización para los ítems del 3 al 11 para definir las gestiones a realizar.
13. Detallar un análisis de costos de los equipos, los costos de su respectiva instalación y de diseño.

1.2. Solución.

Para definir la solución del problema planteado, voy a definir una ‘subsolución’ para cada ‘subproblema’ de la sección anterior, las mismas que se muestran a continuación:

1. Mediante el uso de los protocolos enfocados a domótica de radiofrecuencia, Z-Wave y Zigbee, se puede armar un sistema domótico de radiofrecuencia. Vale destacar que en la web se pueden encontrar una multitud de equipos que usen estos protocolos.
2. El equipo de nombre VERA3 utiliza el protocolo Z-Wave y puede manejar hasta 232 dispositivos. Se utilizarán tres de estos equipos para repartir la cantidad de equipos a utilizar en este proyecto. Dos serán esclavos de uno que será el maestro.
3. Mediante el uso de un router cisco 1941, un fortigate 80C, 4 switches catalyst cisco se crea la red privada interna. En el fortigate 80C se configura la propiedad de 'spillover' para manejar 2 enlaces de internet de 100 Mbps cada uno.
4. Se configura una VPN en la interfaz WAN1 del fortigate 80C para poder acceder de manera remota a la red privada interna. Para acceder de manera local, se lo puede hacer mediante el uso de los switches y de los puntos de acceso.
5. Con el tendido del cableado de cobre cat 6a se puede acceder a la red privada interna de manera alámbrica. No se presentarán documentos técnicos porque los realizará una empresa privada. Además que no es de relevancia hacerlo. El acceso de manera inalámbrica se lo realizará mediante el uso

de puntos de acceso inalámbricos Ruckus 7363 y 7025 y su respectivo controlador ZoneDirector 1100 conectados a la red privada interna.

6. Se instalarán 13 cámaras en la vivienda, que cubran las secciones descritas.
7. La detección de la apertura y cerrado de puertas se lo hará mediante sensores Z-Wave de la marca Aeon Labs, la iluminación mediante el sistema Hue Philips y la combinación de ambas mediante escenas dentro del VERA3 que funciona como maestro.
8. La detección de movimiento se lo hará mediante sensores Z-Wave de la marca Aeon Labs, la iluminación mediante el sistema Hue Philips y la combinación de ambas mediante escenas dentro del VERA3 que funciona como maestro.
9. Se usará el sistema Hue Philips que utiliza el protocolo Zigbee. Mediante un plugin, el VERA3 podrá controlar al sistema Hue Philips.
10. La climatización de la vivienda estará a cargo de los termostatos Z-Wave de la marca Honeywell, mediante escenas dentro del VERA3 que funciona como maestro.

11. La apertura de persianas estará a cargo de los actuadores de persiana Z-Wave de la marca Aeon Labs, mediante escenas dentro del VERA3 que funciona como maestro.
12. La categorización es la siguiente, para los ítems del 3 al 5 definiremos la gestión del networking, para los ítems del 6 al 8 definiremos la gestión de la seguridad, para los ítems del 9 al 11 definiremos la gestión del confort.
13. Investigar los costos de cada equipo y su respectiva instalación y del diseño, del 1) sistema domótico, 2) cableado y 3) networking. Con esta información se realiza el análisis de los costos totales.

1.3. Justificación.

La razón de ser de este proyecto de graduación es brindar una solución domótica alterna a la domótica cableada descrita en la descripción del problema. Además este proyecto sirve de soporte en la enseñanza de la materia "Domótica e Inmótica" de la Facultad de Ingeniería en Electricidad y Computación de la ESPOL, al abarcar temas actualizados que pueden ser agregados a la currícula de estudio. También se integran las áreas de networking, domótica de radiofrecuencia y programación, las cuales son parte fundamental y necesario de las tendencias de la domótica actual y futura.

1.4. Objetivos.

1.4.1. General.

Diseñar e implementar un sistema domótico de radiofrecuencia para brindar una gestión del networking, seguridad y confort usando los protocolos Z-Wave y Zigbee.

1.4.2. Específicos.

A continuación se listan los objetivos específicos:

- Sectorizar las áreas de la vivienda para planificar la ubicación de los equipos que serán parte del sistema domótico de radiofrecuencia.
- Implementar la red de networking que permita controlar y monitorear al sistema domótico de manera remota.
- Definir un dispositivo controlador máster que integre y controle a todos los dispositivos domóticos y las luminarias Hue Philips.
- Desarrollar un análisis de los costos del proyecto en cuanto a los equipos, a la instalación, al diseño y luego presentarlos en un resumen a manera de costos totales.

1.5. Metodología

Se presenta la metodología mediante la cual se implementa el presente proyecto:

- Definir, según los requerimientos de la vivienda, los equipos del sistema domótico.
- Configurar los equipos de networking para que funcionen entre ellos y la Internet.
- Elaborar el plan de direccionamiento IPv4 y dividir la red de la vivienda en varias subredes.
- Asignar el direccionamiento IPv4 a los diferentes equipos del sistema domótico.
- Sectorizar en áreas a la vivienda y definir cuantos y cuales equipos domóticos se colocarán en cada una de estas áreas.
- Incluir en el controlador del sistema domótico todos los equipos domóticos para su control y monitoreo.
- Programar las distintas escenas que involucren equipos domóticos y automaticen tareas del hogar.

CAPÍTULO 2

DEFINICIONES, CONCEPTOS Y FUNDAMENTOS TEÓRICOS DE DOMÓTICA PARA ESTE PROYECTO.

2.1. Introducción a la domótica.

2.1.1. Definición.

La domótica es la automatización y control centralizado y/o remoto de aparatos y sistemas eléctricos y electrotécnicos en la vivienda. Los objetivos principales de la domótica es aumentar el confort, ahorrar energía y mejorar la seguridad [1]. Cada día la domótica cambia en conjunto con la tecnología. Áreas tales como programación e internet de las cosas se van integrando poco a poco a la definición de domótica.

2.1.2. Sistemas a Gestionar.

En este proyecto vamos a gestionar 3 sistemas, los cuales se presentan a continuación:

Gestión del Networking [2], se encarga de captar, transportar, almacenar, procesar y difundir datos e información y la gestión de la información de la vivienda a distancia.

Gestión de la Seguridad [2], o también conocida como Gestión de la Vigilancia, que proporciona un sistema domótico es más amplia que las que nos pueden proporcionar cualquier otro sistema, pues integra tres campos de la seguridad que normalmente están controlados por sistemas distintos.

Gestión del Confort [2], o también conocida como Gestión de la Calidad de vida, nos proporciona una serie de comodidades, como el control automático de los servicios de calefacción, agua caliente, refrigeración, iluminación y la gestión de elementos como accesos, persianas, toldos, ventanas, riego automático, etc.

2.1.3. Fases de una instalación domótica.

Las fases de una instalación domótica son 5 y se presentan a continuación [3]:

Definición de la pre-infraestructura, sobre todo el cableado, que llegue a todos los elementos y consideraciones de futuras ampliaciones.

Trabajos en obra, consiste en la instalación propiamente dicha del sistema domótico. Instalar correctamente los dispositivos de un sistema domótico. Es importante documentar bien la instalación.

Puesta en marcha, consiste en el arranque o puesta en funcionamiento del sistema domótico. Abarca tres puntos: comprobación, formación y monitorización.

Mantenimiento, consiste en la comprobación del correcto funcionamiento y reparación del sistema domótico. Es necesario conocer el funcionamiento y necesidades de mantenimiento de sus elementos.

2.1.4. Dispositivos, arquitecturas y medios de transmisión.

Dispositivos [4], las soluciones domóticas pueden variar, dependiendo de la acción que se requiera realizar, puede ser comandado desde un dispositivo o se puede extender a amplios sistemas que controlen toda la vivienda. Los dispositivos se pueden clasificar en:

- Controlador, son dispositivos que gestionan el sistema según la programación y la información que reciba, pueden existir uno o varios controladores distribuidos en todo el sistema.
- Actuador, este dispositivo es capaz de ejecutar una acción en el sistema, después de haber recibido una orden del controlador (encender, apagar, subir, bajar, abrir cerrar, etc.)
- Sensor, este dispositivo monitorea el entorno captando información que será transmitida al sistema (sensores de movimiento, de puertas, etc.)
- Bus, es el medio de transmisión de señales, transportando información entre los dispositivos mediante un cableado propio, por las redes de otros sistemas (red eléctrica,

telefónica, etc.), la transmisión de estos datos puede también ser de forma inalámbrica.

- Interface, se refiere a la pantalla de interacción con el usuario, donde se muestra toda la información necesaria del sistema.

La Arquitectura [5] de un sistema domótico especifica el modo en que los diferentes elementos de control del sistema se van a ubicar. Existen tres arquitecturas básicas:

- Arquitectura Centralizada, aquella en la que los elementos a controlar y supervisar (sensores, luces, válvulas, etc.) han de comunicarse hasta el sistema de control de la vivienda. Todos los elementos sensores reúnen la información del sistema y se la envían al controlador para que tome las decisiones y se las comunique a los elementos actuadores. El sistema de control es el corazón de la vivienda ante cuyo fallo deja de funcionar.

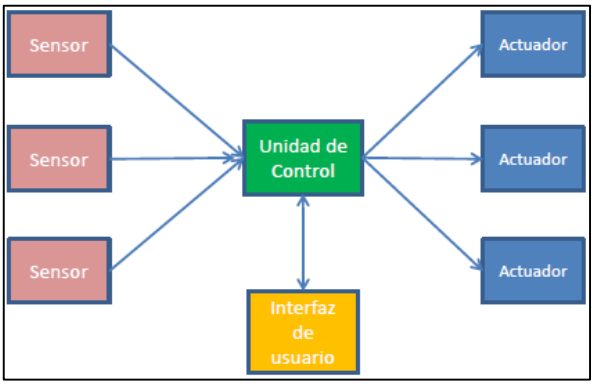


Figura 2.1: Arquitectura Centralizada.

- Arquitectura Distribuida, es aquella que es opuesta a la centralizada. Todos los elementos del sistema deben ser inteligentes, en el sentido de que son totalmente independientes. El sistema debe disponer de un bus compartido que permita la comunicación de todos los elementos.

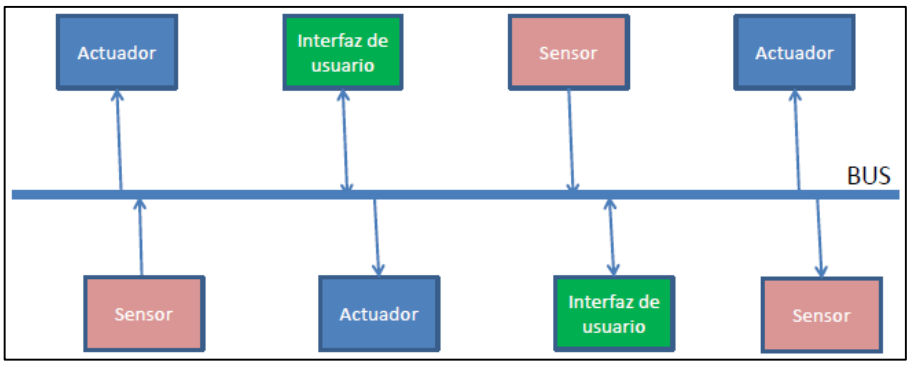


Figura 2.2: Arquitectura Distribuida.

- Arquitectura Mesh [6], o también conocida como arquitectura de malla, es en efecto un router de la red menos el cableado entre los nodos. Está construido por dispositivos que no tienen que estar cableados a un puerto como los puntos de acceso WLAN tradicionales (AP's) lo hacen. La arquitectura de malla sostiene la intensidad de la señal mediante las largas rupturas a distancias, en una serie de saltos más cortos. Los nodos intermedios no sólo aumentan la señal, también hacen cooperativamente decisiones de envío en base a su conocimiento de la red, es decir, realizan un enrutamiento. Tal arquitectura con un diseño cuidadoso puede proporcionar un gran ancho de banda, eficiencia espectral y una ventaja económica sobre el área de cobertura. La arquitectura en modo mesh se aprecia en la siguiente figura [6].

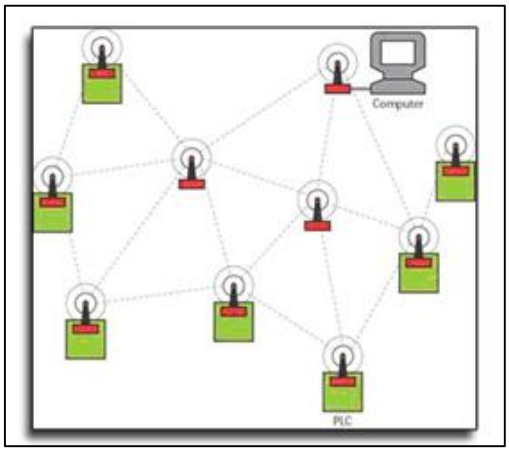


Figura 2.3: Arquitectura en modo Mesh.

Los Medios de Transmisión [7] de la información, interconexión y control, entre los distintos dispositivos de los sistemas de domótica puede ser de varios tipos. Los principales medios de transmisión son:

- Cableado Propio, la transmisión por un cableado propio es el medio más común para los sistemas de domótica, principalmente son del tipo: par apantallado, par trenzado (1 a 4 pares), coaxial o fibra óptica
- Cableado Compartido, varias soluciones utilizan cables compartidos y/o redes existentes para la transmisión de su información, por ejemplo la red eléctrica (corrientes portadoras), la red telefónica o la red de datos.

- Inalámbrica, muchos sistemas de domótica utilizan soluciones de transmisión inalámbrica entre los distintos dispositivos, principalmente tecnologías de radiofrecuencia o infrarrojo.

2.1.5. Hogar Inteligente.

Es un término muy usado en la actualidad. Se puede entender por hogar inteligente a un edificio automatizado al que se le incorpora inteligencia artificial para simplificar el mantenimiento, hacerlo tolerante a fallos, etc [8].

Un hogar inteligente [9] debe ser una vivienda domótica que además presente alguna característica que se pueda considerar como inteligente:

- Inteligencia artificial, optimizar el control y el mantenimiento de la vivienda. Se refiere a la simulación de comportamientos inteligentes mediante técnicas de inteligencia artificial: sistemas expertos, redes neuronales, etc.
- Ambiente inteligente, computación móvil o sin cables, reconocimiento de usuarios, interfaces de usuario. Está relacionado con el concepto de la sociedad de la

información donde se facilita el uso eficiente de los servicios y las interacciones naturales con el ser humano.

- Medio ambiente, desde un punto de vista ambiental se han denominado, edificios ecológicos, edificios sostenibles, etc.

2.2. Domótica de Radiofrecuencia.

La domótica de radiofrecuencia, como su nombre lo indica, busca brindar las prestaciones de la domótica cableada pero de manera inalámbrica, usando protocolos de comunicación especializados en este campo, entre los equipos del sistema domótico.

2.2.1. Funcionamiento.

Las arquitecturas de la domótica de radiofrecuencia se han vuelto famosas debido a las numerosas ventajas tales como su naturaleza plug & play, flexibilidad, interoperabilidad y la efectividad en el costo.

En general, la domótica de radiofrecuencia [10] se compone de equipos inteligentes, principalmente sensores y actuadores, los cuales se comunican entre ellos directamente o mediante un servidor centralizado para lograr funcionalidades automatizadas definidas. Sin embargo algunos estándares inalámbricos

establecidos tales como Wireless Wide Area Network (WWAN) y Wireless Local Area Network (WLAN), Code Division Multiple Access (CDMA2000), y Wideband CDMA (WCDMA), se han convertido en inviables para su uso en dispositivos inteligentes de baja potencia debido a su alto consumo de energía.

Muchas organizaciones han desarrollado tecnologías inalámbricas enfocándose en la domótica de radiofrecuencia basada en diferentes infraestructuras y principios. Más adelante se describe brevemente algunas de estas tecnologías.

2.2.2. Ventajas y desventajas de la domótica de radiofrecuencia sobre la domótica cableada.

A continuación se presenta de manera breve las características de la domótica de radiofrecuencia y de la domótica cableada así como un tabla donde se comparan ambas tecnologías.

La **Domótica de Radiofrecuencia [10]** fue diseñada para reducir el tiempo y los diferentes tipos de obstáculos creados por los cables. Por lo tanto, las redes inalámbricas son el tipo de redes de computadores en las cuales la computadora es conectada con los diferentes equipos de telecomunicaciones inalámbricamente. Es usado para diferentes propósitos tales

como la comunicación o transmisión de datos, entre otros. Estos son todos los tipos de transmisiones que están relacionados a las redes inalámbricas que son llevadas a cabo con la ayuda de diferentes tipos de ondas las cuales tienen longitudes a nivel micro en la naturaleza.

La **Domótica Cableada [10]** se basa en una tecnología la cual usa un tipo especial de cable el cual es usado para transferir datos de un lugar a otro en la forma de señales análogas o digitales, estos cables son llamados coaxiales. Ellos también transportan señales de radio de diferentes frecuencias las cuales también juegan un rol importante en la transferencia de datos entre dos sistemas operativos o computadores. La tasa de transferencia de datos máxima de esta tecnología es 10 MB por segundo. Los cables que son usados para configurar la red cableada son especiales porque ellos se comportan como analógicos y también como digitales y su velocidad es casi parecida a la del cable de par trenzado. Ethernet trabaja u opera en un pequeño rango y es un poco difícil de configurar comparado con las tecnologías de redes inalámbricas. Las redes cableadas son muy costosas para instalar porque para instalar los cables coaxiales necesitamos mucho dinero y tiempo. Entonces, en estos días la tecnología alternativa, por

ejemplo, punto a punto, es usada para reducir los excesivos costos y también disminuir la confiabilidad y la red. Entonces la gestión punto a punto es más recomendable en vez de estos costosos cables por todos lados. Ejemplos comunes son Ethernet o una LAN cableada. En la siguiente tabla [11] se muestra una comparación entre estas tecnologías.

CARACTERÍSTICAS	DOMÓTICA CABLEADA	DOMÓTICA DE RADIOFRECUENCIA
Velocidad de comunicación	Usando cables de par trenzado se alcanzan velocidades de hasta 100 Mbps, siempre y cuando la tecnología de los equipos soporten estas velocidades.	La velocidad más rápida la tiene el protocolo Wi-Fi, alcanzando una velocidad de 54 Mbps. El resto de protocolos de domótica de radiofrecuencia tienen velocidades menores a este. Algunos solo unos kbps.
Costos	Los costos son altos debido a los trabajos de obra civil necesarios para colocar el cableado en la vivienda, a parte de los costos debido a los equipos.	Sólo se necesita comprar los equipos del sistema domótico. No se requiere de trabajos de obra civil.
Ventajas	Más confiable. Comunicación muy rápida. Es más fácil hacer troubleshooting de señales, mediante el uso de instrumentos tales como voltímetros o amperímetros.	Relativamente menos costoso. No se necesitan trabajos de obra civil. No hay confusión por el uso de extensivas cantidades de cableado.
Desventajas	Difícil de identificar los cables aún cuando están etiquetados y se ve	No es tan confiable. Velocidades de

	muy desordenado cuando se instale afuera. Altos costos de instalación. El mantenimiento por lo general lo debe hacer un técnico capacitado.	comunicación bajas comparado con la domótica cableada. Difícil hacer troubleshooting de la trama de datos que envían los equipos, ya que las tramas se envían de manera inalámbrica.

Tabla 2.1: Comparación entre la domótica de radiofrecuencia y la domótica cableada.

2.2.3. Presente y futuro de la domótica de radiofrecuencia.

Se presentan los siguientes argumentos [12] sobre el presente y futuro de la domótica de radiofrecuencia.

Las ventas de los dispositivos domóticos se duplicaron desde el 2012 al 2013

Cerca de 17,23 millones de dispositivos domóticos con tecnología inalámbrica incorporada, que van desde sensores de movimiento hasta termostatos inteligentes y tomacorrientes inteligentes, se vendieron en el año 2013, cerca del doble que el año pasado.

El mercado de domótica en los Estados Unidos excederá los $5,5 billones de dólares en 2016

Las previsiones de mercado (en base a una tasa compuesta de crecimiento anual de 10.5 por ciento entre 2011 y 2016) indican un fuerte crecimiento en este segmento. Evolución de las ventas de 2010 indican que los sistemas de seguridad, entretenimiento en el hogar, y la iluminación se ponen a experimentar un mayor crecimiento de HVAC y gestión de la energía.

El número de usuarios de teléfonos inteligentes incrementarán a 207,4 millones en el 2017

La tecnología que habilita el monitoreo remoto se está popularizando y estará en la mayor parte de los habitantes de un país en los próximos años.

Más de medio billón de dispositivos domóticos inalámbricos serán instalados alrededor del mundo en el 2018

Basados en las tendencias actuales, ABI Research estima que los dispositivos domóticos inalámbricos estarán casi por todos lados en 4 años.

2.3. Red de networking y red domótica.

Las redes de networking y las redes domóticas son diferentes pero pueden interoperar. Por lo general los equipos domóticos que forman parte de una red domótica pueden formar parte de una red de networking. Lo contrario no es común pero puede suceder.

Un buen número de los dispositivos del sistema domótico utilizan direccionamiento IPv4 y la red de networking permite tener a estos dispositivos conectados entre sí; pero los sensores no necesitan conexión con el controlador o máster a través de cableado físico, utilizamos como medio de transmisión la radiofrecuencia a través de los protocolos de comunicación Z-Wave y ZigBee.

2.3.1. Características de una red de networking.

La red de networking [13] no es otra cosa que una red que normalmente usan las computadoras, teléfonos IP, impresoras, etc. como dispositivos finales para comunicarse entre ellas a través de los dispositivos intermedios tales como routers, switches, fortigates, entre otros.

La definición de red de networking, menciona que este es un conjunto de equipos informáticos y software conectados entre sí

por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

La finalidad principal para la creación de una red de networking es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

2.3.2. Características de una red domótica.

Las características de la redes domóticas, tomado del trabajo “Domótica” de la web rincón del vago, se pueden clasificar dentro los siguientes parámetros:

El **Sistema Técnico** el mismo que está compuesto de cuatro variables destacables:

La *integración* de servicios y sistemas es la convergencia de todas las estructuras en un solo equipo controlador. De esta variable depende la rapidez y eficacia del control del edificio.

La *flexibilidad* es la capacidad de añadir nuevos servicios y elementos a los sistemas existentes y en funcionamiento.

La *capacidad de re-programación* del mismo. El sistema técnico debe permitir modificar los parámetros de cada dispositivo de acuerdo con las exigencias y necesidades del usuario.

La *compatibilidad de formatos de información* es imprescindible para tener una buena interacción entre los dispositivos domóticos ya que cada uno de ellos emite un tipo de señal

propio que no tiene porque ser necesariamente el mismo al resto de dispositivos conectados.

El **Diseño Arquitectónico** para el cual hace falta tener en cuenta diversas exigencias económicas y normativas. Debido a que este proyecto basa su sistema domótica en la radiofrecuencia, es importante que la vivienda sea diseñada de tal forma que:

- Se presente la menor cantidad de interferencias que influyen en la radiofrecuencia tales como las paredes de concreto, los ductos de aire acondicionado dentro de las paredes, tuberías metálicas, etc.
- Mientras más ecológico sea la vivienda, se utilizarán menos dispositivos domóticos lo cual reduce el precio del sistema total por ejemplo al momento de iluminar una vivienda por naturaleza oscura, se necesitarán más luminarias que en una vivienda que posee una buena iluminación natural.
- Una correcta distribución de tomacorrientes alrededor de todas las áreas y ambientes de la casa, ya que hay tomacorrientes que pueden funcionar como repetidores de la señal de radiofrecuencia permitiendo llegar el sistema domótico a zonas impensables dentro de la vivienda.

2.4. Breves rasgos de estándares de radiofrecuencia comunes aplicados a la domótica.

2.4.1. Wi-Fi.

Es una tecnología inalámbrica de área local [14] que permite que un dispositivo electrónico intercambie información o se conecte al internet a través de las ondas de radio UHF de 2.4 GHz y SHF de 5 GHz.

Su nombre es una marca comercial. La Wi-Fi Alliance define al Wi-Fi como cualquier producto de red de área local inalámbrica (WLAN) que están basados en el estándar IEEE 802.11.

Algunos dispositivos pueden usar Wi-Fi por ejemplo, computadores personales, consolas de video juego, smartphones, cámaras digitales, tablets y reproductores de audio, entre otros. Estos se pueden conectar a un recurso de red tales como el Internet mediante un punto de acceso inalámbrico o Access Point (AP) por sus siglas en inglés. Tal punto de acceso tiene un rango de 20 metros o 66 pies dentro de las viviendas y un rango mucho mayor fuera de las mismas.

La cobertura puede comprender un área tan pequeña como una habitación individual con paredes que bloquean las ondas de radio, o tan grandes como muchos kilómetros cuadrados obtenidos mediante el uso de mútliples puntos de acceso superpuestos.

2.4.2. Bluetooth.

La especificación de Bluetooth [15] define un canal de comunicación a un máximo de 720 kbit/s (1 Mbit/s de capacidad bruta) con rango óptimo de 10 m (opcionalmente 100 m con repetidores).

Opera en la frecuencia de radio de 2,4 a 2,8 GHz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex con un máximo de 1600 saltos por segundo. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1 MHz; esto permite dar seguridad y robustez.

La potencia de salida para transmitir a una distancia máxima de 10 metros es de 0 dBm (1 mW), mientras que la versión de largo alcance transmite entre 20 y 30 dBm (entre 100 mW y 1 W).

2.4.3. Insteon.

Insteon es un estándar [16] ambientado al área de domótica que mezcla domótica cableada con domótica de radiofrecuencia.

Usa procesamiento de señales digitales [17] para codificar y transmitir mensajes, habilitando transmisiones rápidas de control de datos entre los dispositivos Insteon.

Permite asignar hasta 16,777,216 identificadores o ID's únicos. Hasta 65,536 tipos de dispositivos. Hasta 65,536 comandos y 256 grupos.

Esta tecnología necesita 80 bytes de memoria RAM y 3 kilobytes de memoria ROM en el dispositivo máster. Para los dispositivos esclavos se necesitan 256 bytes de memoria RAM, 256 bytes de memoria EEPROM y 7 kB de memoria FLASH.

Para la transmisión de datos inalámbricos la tecnología Insteon maneja una frecuencia de 902 a 924 MHz, con una modulación FSK, una sensitividad de -103 dBm y un rango de 150 pies a línea de vista sin obstáculos. La velocidad de comunicación es

de 38,400 bits por segundo. Los tipos de mensaje estándar son de 10 bytes y los tipos de mensaje extendidos son de 24 bytes.

2.4.4. X-10.

Es un protocolo para la comunicación [18] a través de dispositivos electrónicos usados para el área de domótica. Principalmente usa cableado de la red eléctrica de la vivienda para el control y transmisión de señales, donde las señales implican breves descargas de radiofrecuencia que representan información digital. Un protocolo de transporte basado en ondas de radio inalámbricas también es definido.

El protocolo de radio opera [19] en la frecuencia de 310 MHz en Estados Unidos y América; en Reino unido opera en la frecuencia de 418 MHz; en Europa opera en la frecuencia de 433 MHz.

Los comandos de radiofrecuencia del protocolo X10 comprenden 32 bits y se transmiten en aproximadamente 108 milisegundos lo cual implica una velocidad de comunicación de 300 bits por segundo.

En vez de los bytes de datos y dirección [20], X-10 envía dos bytes de datos con cada byte seguido inmediatamente por su bit de complemento para el chequeo de errores. Dentro de cada byte, el bit7 es receptado primero y receptado último el bit0.

2.4.5. Z-Wave.

Es un protocolo de comunicación inalámbrica [21] diseñado para domótica, específicamente para aplicaciones de control remoto en las viviendas y ambientes de iluminación comercial.

El protocolo Z-Wave está optimizado para comunicaciones confiables y de baja latencia de paquetes de datos pequeños con tasas de datos de hasta 100 kbits/s. Diseñado también para ser incorporado fácilmente en productos de consumo electrónico, incluyendo dispositivos operados por batería tales como controles remoto, alarmas de humo y sensores de seguridad.

Z-Wave funciona en la banda industrial, científica y médica, ISM por sus siglas en inglés, usando el método FSK.

Cada red Z-Wave puede incluir hasta 232 nodos, y consiste de dos conjuntos de nodos: controladores y dispositivos esclavos.

Los nodos pueden estar configurados para retransmitir los mensajes a fin de garantizar la conectividad en el ambiente de trayectorias múltiples de una vivienda.

El rango promedio de comunicación entre dos nodos es de 30.5 metros o 100 pies, y con la habilidad de saltar hasta 4 veces entre nodos, esto da una cobertura suficiente para la mayor parte de las viviendas. Este protocolo opera en la banda de los 908.42 MHz.

2.4.6. Zigbee.

Es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo [22], basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal. Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías. Posee tres características principales: 1) Su bajo consumo, 2) su topología de red en malla y 3) su fácil integración.

Zigbee utiliza la banda ISM para usos industriales, científicos y médicos; en concreto, 868 MHz en Europa, 915 MHz en

Estados Unidos y 2.4 GHz en todo el mundo. Sin embargo, a la hora de diseñar dispositivos, las empresas optarán prácticamente siempre por la banda de 2.4 GHz, por ser libre en todo el mundo. Se definen hasta 16 canales en el rango de 2.4 GHz, cada uno de ellos con un ancho de banda de 5 MHz.

Los radios utilizan un espectro de dispersión de secuencia directa. Se utiliza BPSK en los dos rangos menores de frecuencia, así como un QPSK ortogonal que transmite dos bits por símbolo en la banda de 2.4 GHz. Esta permite tasas de transmisión en el aire de hasta 250 kilobits por segundo, mientras que las bandas inferiores se han ampliado con la última revisión a esta tasa desde los 40 kilobits por segundo. Los rangos de transmisión oscilan entre los 10 y 75 metros, aunque depende bastante del entorno. La potencia de salida de las radios suele ser de 0 dBm (1 mW).

2.5. Funcionamiento y selección de los protocolos Z-Wave y Zigbee para el desarrollo de este proyecto.

2.5.1. Justificación de la selección.

Zigbee, será usado por el sistema Hue Philips y sus controladores debido a que vienen integrados de fábrica con

este protocolo de comunicación a 2.4 GHz. Ningún otro dispositivo de nuestro sistema domótico utiliza ZigBee.

Zigbee se fundamenta en el poderoso estándar de radio IEEE 802.15.4 que opera en bandas sin licencia a través del mundo [22]. Desarrolla una velocidad de comunicación de hasta 250 kilobits por segundo en los 2.4 GHz con 16 canales, 40 kilobits por segundo en los 915 MHz con 10 canales y 20 kilobits por segundo en los 868 MHz con un canal. Las distancias de transmisión son notables para una solución de baja potencia con un alcance de 10 a 1600 metros dependiendo de la potencia de salida y las condiciones del ambiente, tales como otros edificios, paredes interiores y topología geográfica.

Según la ABI Research, Zigbee compone aproximadamente el 40% de la producción de chipsets IEEE 802.15.4 en el 2010 y crecerá a casi el 55% de la producción de los mismos.

Z-Wave es un protocolo de comunicaciones inalámbrico diseñado para la automatización del hogar, específicamente para controlar de forma remota las aplicaciones en entornos residenciales y comerciales ligeras [21]. La tecnología utiliza una radio RF de baja potencia integrado y para el equipamiento

en los dispositivos y sistemas, tales como la iluminación, control de acceso residencial, sistemas de entretenimiento y electrodomésticos electrónicos para el hogar.

Debido a que hay una gran gama de productos con comunicación Z-Wave con aproximadamente 8 años en el mercado, con una comunicación estable y confiable, Z-Wave se eligió como el protocolo a usar en los sensores, además trabaja a baja frecuencia y en el orden de los 908.42 MHz para Estados Unidos de América. Esta es la frecuencia que usaremos y es de nuestro interés debido a que nos es más fácil importar equipos de Estados Unidos que de cualquier otro país. Con esto evitamos que exista interferencia con la señal de Wi-Fi que es de 2.4 GHz.

Como podemos ver, no existe interferencia entre ZigBee y Z-WAVE ya que las bandas de frecuencia en las que trabajaremos son de 2.4 GHz y 908.42 MHZ respectivamente.

2.5.2. Funcionamiento.

2.5.2.1. Z-Wave.

El protocolo Z-Wave es un protocolo half dúplex de bajo ancho de banda diseñado para comunicaciones inalámbricas confiables en una red de control de bajo costo [23]. El principal objetivo de los protocolos es comunicar mensajes cortos de control de una manera confiable desde una unidad de control a uno o más nodos en la red.

El protocolo no está diseñado para transferir largas cantidades de datos o para transferir cualquier clase de transmisión o sincronización de datos críticos.

El protocolo consiste de cuatro capas, la capa MAC que controla el medio de radiofrecuencia, la capa de transporte que controla la transmisión y recepción de las tramas de datos, la capa de enrutamiento que controla el ruteo de las tramas en la red, y finalmente la capa de aplicación que controla la carga útil (payload) en las tramas transmitidas y recibidas.

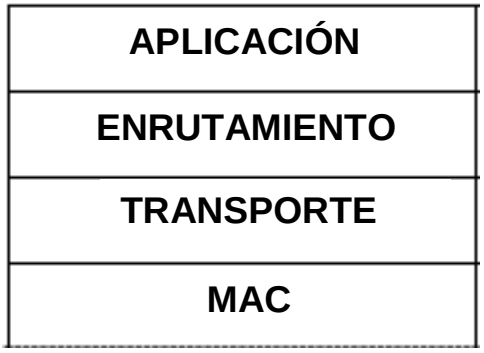


Figura 2.4: Capas del protocolo Z-Wave.

En la figura anterior se muestran las capas del protocolo Z-Wave [23]. Existen 2 tipos básicos de dispositivos; dispositivos controladores y dispositivos esclavos. Los controladores son los nodos en una red que inician comandos de control y envían comandos a otros nodos, y los nodos esclavos son los nodos responden y ejecutan comandos. Los esclavos pueden también pasar los comandos a otros nodos, lo cual hace posible para el controlador comunicarse con nodos que están fuera del alcance de ondas de radio directas.

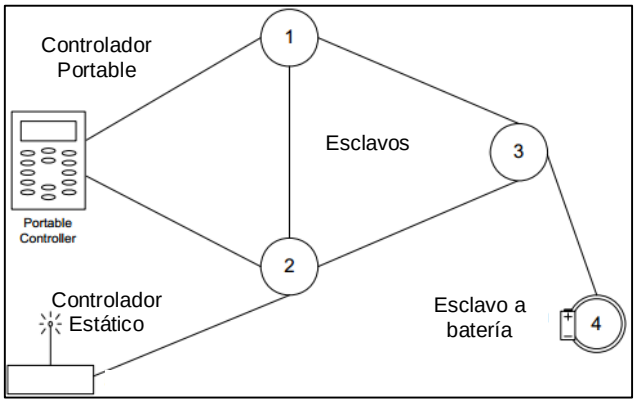


Figura 2.5: Diagrama básico de una red Z-Wave.

En la figura anterior se muestra un diagrama básico de una red Z-Wave [23]. Los controladores tienen una tabla de enrutamiento completa y por lo tanto es capaz de comunicarse con todos los nodos en una red Z-Wave. La funcionalidad disponible en un controlador depende de cuando ingresó a la red Z-Wave. Si el controlador es usado para crear una nueva red Z-Wave, él automáticamente se convierte en el controlador primario. El controlador primario es el controlador master en la red Z-Wave y puede haber sólo uno en cada red. Solo los controladores primarios tienen la capacidad de incluir/excluir nodos en la red y por lo tanto siempre tienen la última topología de la red.

Los controladores agregados a la red usando el controlador primario, son llamados controladores secundarios y no tienen la capacidad para incluir/excluir los nodos en la red.

A continuación se mencionan los diferentes tipos de controladores que existen:

Los **controladores portables** están diseñados para cambiar de posición en la red Z-Wave. El controlador portable usa un número de mecanismos para estimar la actual posición en la red y así calcular la ruta más rápida a través de la red.

Los **controladores estáticos** o static controller son controladores fijos que no deben de cambiar de posición dentro de la red y deben estar encendidos todo el tiempo. Este controlador tiene la ventaja que los esclavos de enrutamiento pueden reportar mensajes de status no solicitados a él, y también tiene la ventaja de siempre saber dónde está localizado en una red. Un controlador estático será típicamente un controlador secundario dentro de una red Z-Wave.

Los **controladores de actualización estática** o static update controller (SUC) pueden estar opcionalmente en una red. Es un tipo de controlador estático que recibe las notificaciones del controlador primario correspondiente a todos los cambios hechos en la topología de la red. Es capaz de enviar actualizaciones de la topología de la red a otros controladores y esclavos de enrutamiento bajo pedido. Es la aplicación en un controlador primario el que solicita a un controlador estático que se convierta en un SUC. Solo puede haber un SUC en cada red Z-Wave.

Los **servidores de identificación SUC** o SUC ID server (SIS) habilitan a otros controladores a incluir/excluir nodos en la red en su nombre. El SIS es el controlador primario en la red porque tiene la última actualización de la topología de la red y la capacidad de incluir/excluir nodos en la red.

Los **controladores de inclusión** son aquellos controladores adicionales que se incluyen a la red. Tienen la capacidad de incluir/excluir nodos en la red

en nombre del SIS. La topología de red de los controladores de inclusión tiene fecha desde la útlima vez que un nodo fue incluido o pidió una actualización de red al SIS. Es por esto que los controladores de inclusión no pueden ser clasificados como controladores primarios.

Los **controladores de instalación** son controladores portables, los cuales tienen funcionalidad adicional, lo cual les habilita hacer gestión de la red sofisticado y pruebas de calidad de la red comparado con otros controladores.

Los **controladores puente** o bridge controller son opcionales en una red. Son controladores estáticos extendidos, los cuales incorporan funcionalidad extra que puede ser usada para implementar controladores, dedicados a hacer la unión entre redes Z-Waves diferentes. Este controlador almacena información relacionada a los nodos en la red Z-Wave y además puede controlar hasta 128 nodos esclavos virtuales.

Un **nodo esclavo virtual** es un nodo esclavo que corresponde a un nodo, el cual reside en un tipo de red diferente.

Los **nodos esclavos** son nodos en una red Z-Wave que reciben comandos y ejecutan una acción basada en el comando. Los nodos esclavos son incapaces de enviar información directamente a los otros esclavos o controladores a menos de que ellos sean solicitados a hacerlo en un comando.

Los **esclavos de ruteo** o routing slave tienen la misma funcionalidad de cualquier esclavo. La mayor diferencia es que un esclavo de ruteo puede enviar mensajes no solicitados a otros nodos en la red. Ellos almacenan un número estático de rutas para su uso cuando se envían mensajes no solicitados a un número limitado de nodos.

Los **esclavos mejorados** o enhanced slaves tienen la misma funcionalidad que los esclavos de enrutamiento y ellos se manejan de la misma forma en la red. La diferencia entre los esclavos de ruteo y los esclavos

mejorados es que los esclavos mejorados tienen un reloj de tiempo real y una memoria EEPROM para almacenamiento de datos de aplicación.

El protocolo Z-Wave usa un único identificador de red llamado “Home ID” para separar redes Z-Wave. Este “Home ID” es un identificador único de 32 bit que es pre programado en todos los dispositivos controladores. Todos los nodos esclavos en la red tendrán inicialmente un Home ID igual a cero, y por lo tanto necesitarán tener un “Home ID” asignado a ellos por un controlador de tal forma a comunicarse con una red. Controladores en una red pueden intercambiar Home ID’s mucho más que un controlador puede controlar nodos esclavos en una red.

Los “Node ID’s” son usados para direccionar nodos individuales en una red, son únicos dentro de una red definida por un Home ID único. Un Nodo ID es un valor de 8 bit y tal como los Home ID’s son asignados a los nodos esclavos por un controlador.

CAPA MAC

La capa MAC controla el medio de radiofrecuencia. El flujo de datos posee una codificación Manchester y consiste de un preámbulo, inicio de la trama (SOF), trama de datos y un símbolo de final de la trama (EOF). La trama de datos es parte de la trama que es pasada dentro de la capa de transporte. En la siguiente figura se muestra el formato de la trama de la capa MAC [23].

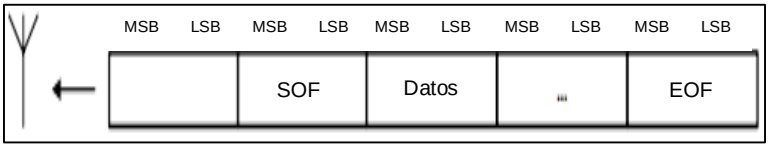


Figura 2.6: Formato de la trama de la capa MAC.

Toda la data es enviada en formato little-endian.

La capa MAC es independiente del medio de radiofrecuencia, frecuencia y método de modulación pero la capa MAC requiere ya sea acceso a la trama de datos cuando sea recibida o a toda la señal en forma binaria desde ya sea de un flujo de bits decodificado o el flujo de bits con codificación Manchester.

La data es transmitida en bloques de 8 bits, el bit más significativo va primero de izquierda a derecha y el bit menos significativo va último de izquierda a derecha. La data posee la codificación Manchester de tal forma de tener una señal libre de DC. En la siguiente figura se muestra un ejemplo de codificación Manchester del bit0 y del bit1 [23].

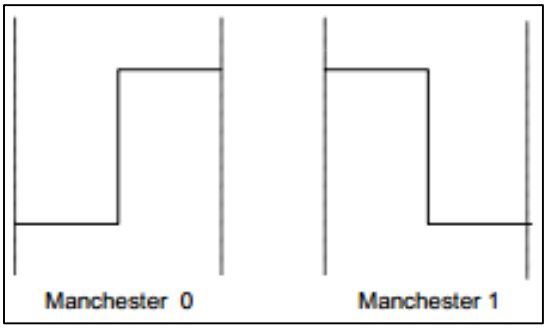


Figura 2.7: Ejemplo de Codificación Manchester del bit0 y del bit1.

La capa MAC tiene un mecanismo de evitación de colisiones que previene que los nodos empiecen a transmitir mientras otros nodos están transmitiendo. La evitación de colisiones es lograda dejando que los nodos estén en modo de recepción cuando ellos no están transmitiendo y luego retrasan una transmisión si la capa MAC está en la fase de datos del receptor. La evitación de colisiones es activa en todos los tipos

de los nodos cuando ellos tienen el radio activado. La transmisión de una trama es retrasado un número aleatorio de milisegundos.

CAPA DE TRANSPORTE

La capa de transporte controla la transferencia de los datos entre dos nodos incluyendo la retransmisión, el chequeo del checksum y las contestaciones de recepción de mensajes.

La capa de transporte contiene 4 formatos de trama básicos usados para transferir comandos en la red. Todas las 4 tramas usan el siguiente formato de trama tal como lo muestra la siguiente figura [23].

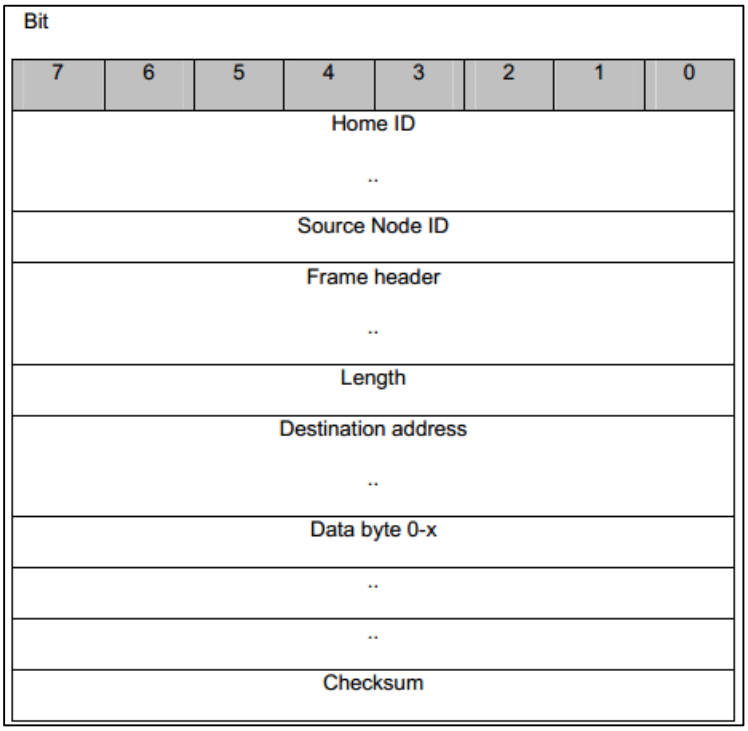


Figura 2.8: Formato de trama básica de la capa de transporte del protocolo Z-Wave.

A continuación se detallan los 4 tipos de trama:

El tipo de trama **Singlecast** son siempre transmitidas a un nodo en específico y la trama es notificada como recibida de tal forma que los transmisores saben que la trama ha sido recibida. Una transmisión singlecast tiene el siguiente flujo de trama:

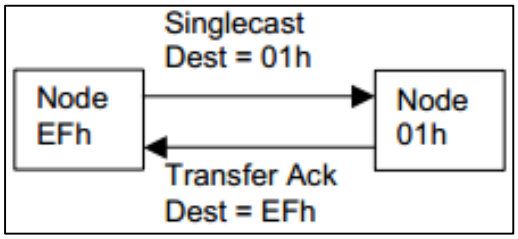


Figura 2.9: Flujo de la trama de una transmisión singlecast.

En la figura anterior se muestra el flujo de la trama de una transmisión singlecast [23]. Si la trama singlecast o la trama de notificación de transferencia está perdida o corrupta, la trama singlecast es retransmitida. A fin de evitar colisiones potenciales con sistemas paralelos las retransmisiones son retrasadas con un retraso aleatorio. El retraso aleatorio debe estar en pasos del tiempo que toma enviar una trama de tamaño máximo y recibir la transferencia de notificación de recepción.

El tipo de trama **Transferencia de Notificación de Recepción**, es una trama singlecast donde el tamaño de la sección de la data es cero. Sólo sirve para notificar la recepción de un mensaje hacia un nodo.

El tipo de trama **Multicast** se transmite a un número de nodos que van desde 1 a 232. Este tipo de trama no soporta notificación de recepción.

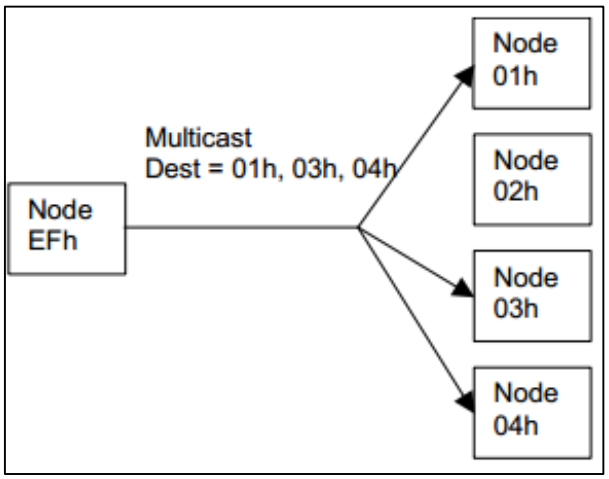


Figura 2.10: Flujo de la trama de una transmisión Multicast.

La figura anterior muestra el flujo de la trama de una transmisión Multicast [23]. La dirección de destino multicast es usada para direccionar nodos seleccionados sin tener que enviar una trama separada de cada nodo.

Nótese que una trama multicast no obtiene una notificación de recepción de tal forma que este tipo de trama no puede ser usada para comunicaciones confiables. Si las comunicaciones confiables son

necesarias una transmisión multicast debe ser seguida por una trama singlecast de cada nodo de destino.

El tipo de trama **Broadcast** es recibida por todos los nodos en una red, y la trama no es notificada de su recepción por ningún nodo.

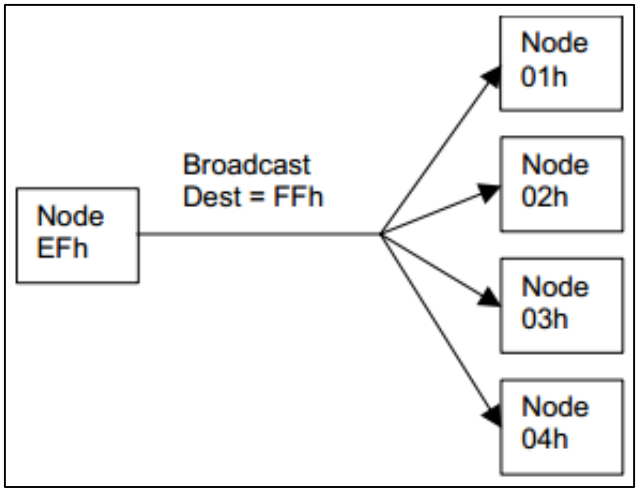


Figura 2.11: Flujo de trama de una transmisión Broadcast.

La figura anterior muestra flujo de trama de una transmisión Broadcast [23]. Note que la trama broadcast no obtiene notificación de recepción de tal forma que este tipo de trama no puede ser usado para transferencias confiables. Si es necesaria una comunicación confiable una transmisión broadcast

debe ser seguido por una trama singlecast para cada nodo de destino.

CAPA DE ENRUTAMIENTO

La capa de enrutamiento controla el ruteo de las tramas de un nodo al otro. Ambos, controladores y esclavos pueden participar en el ruteo de tramas en caso de que ellos siempre estén escuchando y tengan una posición estática. Esta capa es responsable de ambas tareas, enviar una trama con una lista repetidora correcta y también asegurar que la trama sea repetida de nodo a nodo. La capa de enrutamiento es también responsable de escanear la topología de red y mantener una tabla de ruteo en el controlador.

La capa de enrutamiento tiene dos tipos de tramas que son usadas cuando la repetición de tramas es necesaria.

El tipo de trama **Routed Singlecast** es una trama de destino de un nodo con notificación de recepción que contiene información de repetidor. La trama es

repetida de un repetidor a otro hasta que alcance su destino.

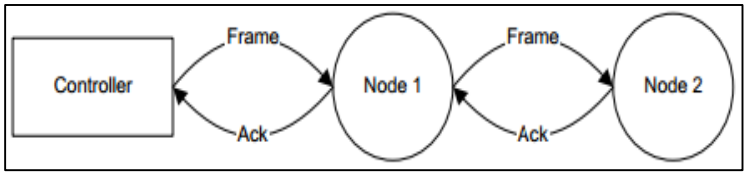


Figura 2.12: Flujo de una trama de tipo Routed Singlecast.

La figura anterior muestra el flujo de una trama de tipo Routed Singlecast [23]. La palabra 'frame' significa trama. La palabra 'Ack' es la contracción de Acknowledge. El tipo de trama Routed Acknowledge es una trama routed singlecast que es usado para decir al controlador que la trama routed singlecast ha alcanzado su destino.

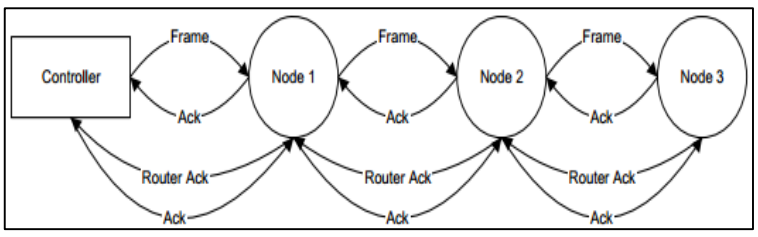
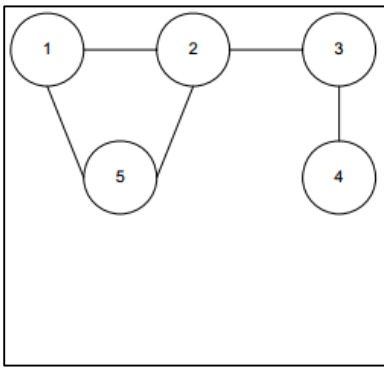


Figura 2.13: Flujo de una trama de tipo Routed Acknowledge.

La figura anterior muestra el flujo de una trama de tipo Routed Acknowledge [23]. La palabra ‘frame’ significa trama. La palabra ‘Ack’ es la contracción de Acknowledge. La Tabla de Ruteo es el lugar donde el controlador mantiene la información desde los nodos acerca de la topología de la red. La tabla es un campo donde toda la información acerca de que es lo que pueden ver los nodos los unos a los otros es mantenida.



	1	2	3	4	5	6
1	0	1	0	0	1	0
2	1	0	1	0	1	0
3	0	1	0	1	0	0
4	0	0	1	0	0	0
5	1	1	0	0	0	0
6	0	0	0	0	0	0

Figura 2.14: Topología de Red y Tabla de Ruteo.

La figura anterior muestra la topología de Red y Tabla de Ruteo [23]. La tabla de ruteo es construida por el controlador primario basado en la información que recibe de todos los nodos en la red, al momento de la instalación, acerca del alcance de cada nodo.

Encontrar la ruta a un nodo es una tarea difícil porque un controlador portable es definido como un dispositivo que será movido alrededor de varios, por ejemplo, un control remoto. Por lo tanto un controlador portable siempre tratará de alcanzar un nodo sin enrutamiento y si eso falla el controlador portable usará varias técnicas para buscar la mejor ruta al nodo.

CAPA DE APLICACIÓN

La capa de aplicación es responsable por la decodificación y ejecución de comandos en una red Z-Wave. La única parte de la capa de aplicación que es descrita en los siguientes párrafos es la asignación de los Home ID's y Node ID's y la replicación de controladores. El resto de la capa de aplicación es la implementación específica y puede ser diferente entre fabricantes.

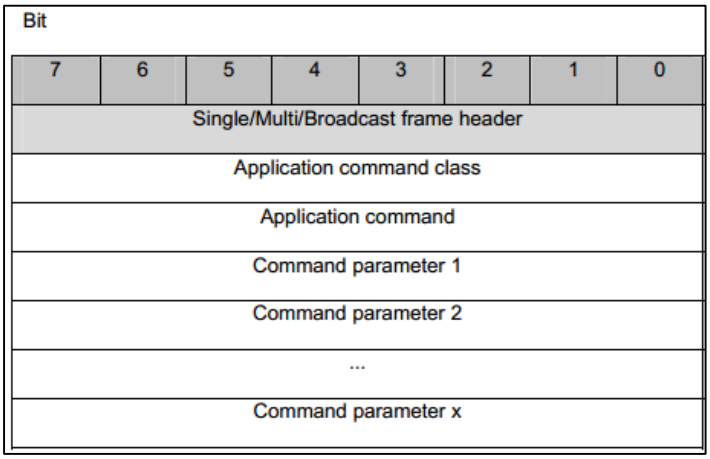


Figura 2.15: Formato de la trama de la capa de aplicación Z-Wave.

La figura anterior muestra el formato de la trama de la capa de aplicación Z-Wave [23]. Las clases de comandos de aplicación (Application command class) especifica si el comando de aplicación es para el protocolo o la aplicación Z-Wave.

El comando de aplicación (Application command) especifica el comando específico que depende la clase del comando.

Los parámetros de comandos (Command Parameter) contienen parámetros asociados con el comando específico. El número de parámetros depende del comando.

Todos los tipos de tramas a excepción de los de notificación de recepción pueden contener un comando de aplicación.

Debido a que un controlador en una red Z-Wave debería ser capaz de controlar varias y diferentes clases de nodos, es necesario tener una trama que describa las capacidades de un nodo. Algunas de las capacidades serán relacionadas al protocolo y algunas serán de aplicación específica. Todos los nodos enviarán su información del nodo cuando el botón de acción en el nodo es presionado. Un controlador puede también obtener la información de un nodo al pedírsela con una trama “get node information”.

La trama de información del nodo es enviada a cada nodo cada vez que el botón de acción es presionado. La trama es enviada de manera broadcast a cualquier controlador o esclavo que puede estar interesado en la información. Un controlador puede también solicitar la información del nodo de un nodo al enviar una trama “get node information” a él. La siguiente figura muestra el flujo de la trama “Get Node Info” [23].

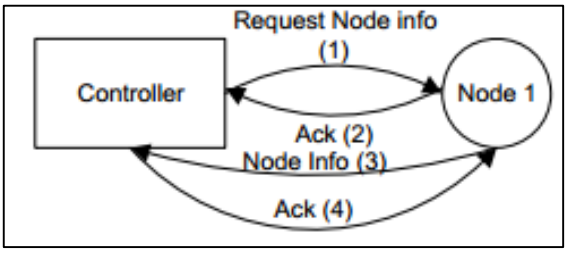


Figura 2.16: Flujo de la trama "Get Node Info".

2.5.2.2. Zigbee.

El protocolo Zigbee fue desarrollado para proveer conectividad inalámbrica para una amplia variedad de aplicaciones de red concerniente al monitoreo y control [24]. Zigbee es un estándar abierto a nivel mundial controlado por la Zigbee Alliance.

El estándar Zigbee se construye en el estándar IEEE 802.15.4. Zigbee mejora la funcionalidad de este estándar al proveer topologías extendibles y flexibles con inteligencia integrada de enrutamiento para facilitar instalaciones fáciles y de alta capacidad de resistencia al fracaso.

Las redes Zigbee también incorporan el escuchar antes de hablar y provee de medidas de seguridad rigurosas que les permiten coexistir con otras

tecnologías inalámbricas (como Bluetooth y Wi-Fi) en el mismo entorno.

La conectividad inalámbrica Zigbee significa que puede ser fácilmente instalada de manera barata, y su inteligencia y flexibilidad integrada permite a las redes adaptarse fácilmente a los cambios necesarios debido al agregar, remover o mover nodos de la red. El protocolo es diseñado de tal forma que los nodos pueden aparecer y desaparecer de la red, permitiendo que algunos dispositivos sean puestos en un modo de ahorro de energía cuando no están activos. Esto significa que muchos dispositivos en una red Zigbee pueden ser alimentados por batería, haciéndolos autónomos y de esta forma se ahorran costos de instalación.

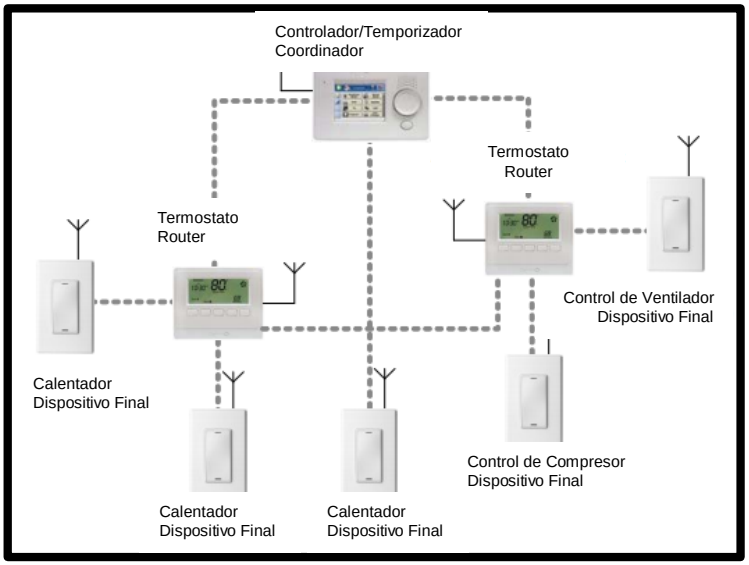


Figura 2.17: Ejemplo de una red Zigbee simple.

La figura anterior muestra un ejemplo de una red Zigbee simple [24]. Una red inalámbrica abarca un conjunto de nodos que se pueden comunicar entre ellos mismos por medio de las transmisiones de radio, de acuerdo a un conjunto de reglas de enrutamiento (al pasar mensajes entre los nodos). Una red inalámbrica Zigbee incluye tres tipos de nodos:

El Coordinador es el primer nodo a ser iniciado y es el responsable de armar la red permitiendo que otros nodos se unan a la red a través del mismo. Una vez que la red está establecida, el coordinador tiene un rol

de ruteo y también es capaz de enviar/recibir data. Cada red debe tener un y solo un coordinador.

El Router es un nodo con una capacidad de ruteo y también es capaz de enviar/recibir data. También permite que otros nodos se unan a la red a través de él, por lo que juega un rol importante en la extensión de la red. Una red puede tener varios routers.

El Dispositivo Final es un nodo el cual es capaz de enviar y recibir datos (no tiene capacidad de enrutamiento). Una red puede tener varios dispositivos finales.

Zigbee permite una variedad de topologías de red desde la más simple, topología estrella, hasta la topología más compleja, topología de árbol y también la topología flexible, la topología en forma de malla.

La topología en forma de malla tiene una estructura pequeña implícita. Es una colección de nodos que comprenden un coordinador y un número de routers y/o dispositivos finales, donde:

- Cada nodo, excepto el coordinador, está asociado con el router o el coordinador, este es el nodo a través del cual se une a la red y es conocido como su ‘parent’. Cada parent puede tener un número de ‘children’.
- Un dispositivo final puede solo comunicarse directamente con su propio parent.
- Cada router y el coordinador puede comunicarse directamente con cada uno de los routers/coordinador dentro del alcance de radio.

Una red con topología de malla es muy flexible y eficiente en términos de comunicación entre nodos.

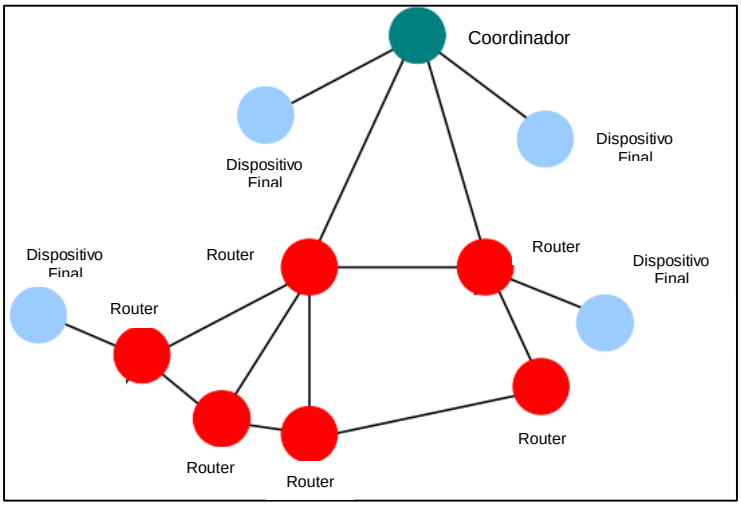


Figura 2.18: Red en modo malla.

La figura anterior muestra una red en modo malla [24]. El protocolo IEEE 802.15.4, en el que Zigbee está construido, provee una conectividad de red basada en radio que opera en una de las tres posibles bandas de radiofrecuencia: 868, 915 o 2400 MHz. Estas bandas están disponibles para su uso sin licencia, dependiendo del país.

Banda	Frecuencia MHz	kbps	# de Canales	Locación
868 MHz	868.3	20	0 (1 channel)	Europe
915 MHz	902-928	40	1-10 (10 channels)	America Australia
2400 MHz	2405-2480	250	11-26 (16 channels)	Worldwide

Tabla 2.2: Banda de las frecuencias de radio del protocolo Zigbee.

La tabla anterior muestra la banda de las frecuencias de radio del protocolo Zigbee [24]. Las bandas 868 y 915 MHz ofrecen ciertas ventajas tales como pocos usuarios, menor interferencia y menor absorción y reflexión, pero la banda de los 2400 MHz es más ampliamente usada por las siguientes razones:

- Disponibilidad mundial por su uso sin licencia
- Tasa de transferencia de datos alta y más canales

- Baja potencia de transmisión, menor consumo de energía
- Banda mucho más conocida, aceptada y estudiada por el mercado

Zigbee y el protocolo IEEE 802.15.4 emplean una variedad de técnicas para asegurar comunicaciones confiables entre los nodos de la red, esto es, para asegurar que las comunicaciones alcancen sus destinos sin corromperse. La corrupción de las comunicaciones puede resultar, por ejemplo, desde la radio interferencia o condiciones de transmisiones/recepciones pobres.

A continuación se muestran una serie de técnicas para asegurar la operación confiable:

- **Codificación de datos.** A un primer nivel, el mecanismo de codificación es aplicado a las transmisiones de radio. El método de codificación empleado en la banda de 2400 MHz usa la modulación QPSK con chips de una conversión de secuencias de símbolos de 4 bits a 32 bits. Debido

a esta codificación, hay una alta probabilidad de que un mensaje llegará a su destino intacto, aún si hay transmisiones conflictivos (más de un dispositivo transmitiendo en el mismo canal al mismo tiempo).

- **Escuchar antes de enviar.** El esquema de la transmisión también evita la transmisión de data cuando hay actividad en el canal escogido, esto es conocido como “Carrier Sense – Multiple Access with Collision Avoidance (CSMA-CA). De manera sencilla, esto significa que antes de que empiece la transmisión, un nodo escuchará en el canal para chequear si está disponible. Si la actividad es detectada en el canal, el nodo retrasa la transmisión para una cantidad aleatoria de tiempo y vuelve a escuchar; si el canal está ahora libre, la transmisión puede iniciar, de otra forma el ciclo de retraso-escucha es repetido.
- **Notificación de recepción.** Dos sistemas de notificación de recepción están disponibles para asegurar que los mensajes alcancen sus destinos. *End-to-end,* cuando un mensaje llega a su destino

final, dispositivo que lo recibe envía una notificación de recepción al dispositivo emisor del mensaje para indicar que el mensaje ha sido recibido. Este tipo de notificaciones de recepción son opcionales.

Next hop, cuando un mensaje es enrutado mediante nodos intermediarios para alcanzar su destino, el siguiente nodo de enrutamiento en la ruta envía una notificación de recepción al nodo anterior para indicar que el mismo ha recibido el mensaje. Las notificaciones de recepción Next hop son siempre implementadas.

En ambos casos, si el dispositivo emisor no recibe una notificación de recepción dentro de un cierto intervalo de tiempo, el vuelve a enviar el mensaje original (él puede reenviarlo varias veces hasta que el mensaje haya sido notificado de su recepción).

- **Frequency Agility,** cuando una red Zigbee está configurada inicialmente, el mejor canal en la banda de radio relevante es automáticamente

escogida como el canal operativo. Esto es normalmente el canal más silencioso detectado en un escaneo de energía a través de la banda, pero este no puede seguir siendo siempre el canal más silencioso si otras redes que operan en el mismo canal se introducen en las inmediaciones.

- **Route Repair**, las redes que emplean la topología de malla tienen una inteligencia incorporada para asegurar que los mensajes alcancen sus destinos. Si la ruta por default al nodo de destino está caída, debido a que un nodo intermediario se cayó, la red puede descubrir e implementar rutas alternativas para la entrega de mensajes.

La confiabilidad permite a las redes Zigbee operar aun cuando hay otras redes Zigbee cercanas operando en la misma banda de frecuencia. Es por lo tanto, que redes Zigbee adyacentes no interferirán con otras. Adicionalmente, las redes Zigbee pueden también operar en la cercanía de otras redes basadas en otros estándares, tales como Wi-Fi y Bluetooth, sin alguna interferencia.

El protocolo Zigbee se compone de cuatro capas: 1) capa de aplicación, 2) capa de red, 3) capa de enlace de datos y 4) capa física.

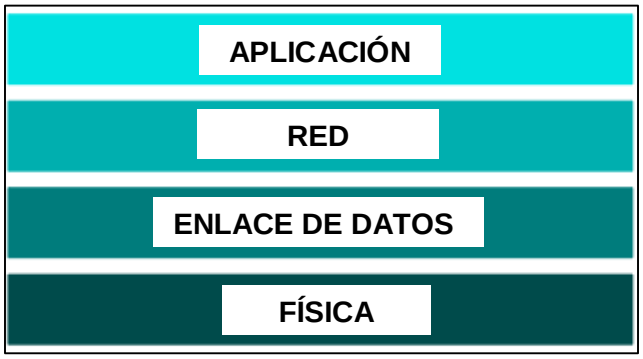


Figura 2.19: Capas del protocolo Zigbee.

La figura anterior muestra las capas del protocolo Zigbee [24]. Un nodo de enrutamiento, ya sea un router o un coordinador, contiene información acerca de sus nodos vecinos. Esta información es almacenada en una tabla de nodos vecinos de los cuales los nodos tienen comunicación directa.

En una red Zigbee, cada nodo debe tener un identificador único. Esto es logrado a través de dos direcciones:

- Dirección MAC: Es una dirección de 64 bits, la cual identifica únicamente el dispositivo; no hay dispositivos en el mundo que pueda tener las mismas direcciones MAC.
- Dirección de Red: Esta es una dirección de 16 bits que identifica al nodo en la red y es local a la red (así, dos nodos en redes separadas pueden tener las mismas direcciones de red).

Una red Zigbee debe ser identificable de manera única. Esto permite que más de una red Zigbee operen en el mismo espacio o en muy cercana entre ellas. Los nodos que operan en el mismo espacio debe ser capaz de identificar a cual red pertenecen.

Para este propósito, la red Zigbee usa dos identificadores:

- PAN ID, es un valor de 16 bits que es usado en las comunicaciones entre los nodos para identificar a las redes relevantes. Un valor para el PAN ID es seleccionado de manera aleatoria por el coordinador cuando la red inicia su

funcionamiento. Cuando otros nodos se unen a la red, ellos aprenden el PAN ID de la red y lo usan en todas las comunicaciones de la red.

- PAN ID Extendido, es un valor de 64 bits es usado en formar la red y subsecuentemente modificar la red en caso de ser necesario.

El inicio de la operación de una red conlleva los siguientes pasos: 1) se ajusta el PAN ID Extendido y la dirección de red del coordinador, 2) se selecciona el canal de radio en la banda de radiofrecuencia, 3) se selecciona el PAN ID de la red y 4) se reciben las peticiones de incorporación a la red desde otros dispositivos.

La incorporación de los routers y dispositivos finales a una red Zigbee, sigue los siguientes pasos: 1) búsqueda de la red, 2) selección del dispositivo parent más cercano al coordinador, 3) petición de incorporación a la red, 4) recepción de la respuesta sobre la incorporación y 5) aprendizaje de los ID's de la red, el PAN ID, PAN ID extendido y la dirección de que se le ha asignado.

CAPA DE APLICACIÓN

La capa de aplicación contiene las aplicaciones que corren en un nodo de la red. Estos dan al dispositivo su funcionalidad, esencialmente una aplicación convierte una entrada en data digital, y/o convierte data digital en salida. Un nodo puede correr varias aplicaciones por ejemplo, un sensor de ambiente pueda contener aplicaciones separadas para medir temperatura, humedad y presión atmosférica.

Una aplicación puede necesitar obtener información acerca de los nodos de la red en la cual corre. Para esto, usa la información guardada en los descriptores en los nodos.

Hay tres descriptores mandatorios y dos son opcionales. Los descriptores mandatorios son: Node, Node Power y Simple Descriptors, mientras los descriptores opcionales son llamados: The Complex y User Descriptors.

Un *Node Descriptor*, contiene información sobre las capacidades del nodo, incluyendo: tipo, banda de

frecuencia, código de manufactura, tamaño máximo del buffer, capacidades del IEEE 802.15.4

Un *Node Power Descriptor*, contiene información en como el nodo es alimentado: Modo de encendido, fuentes de energía disponibles, fuentes de energía actuales, nivel de la fuente de energía actual.

Un *Simple Descriptor* incluye: un endpoint en el cual la aplicación se comunica, el perfil de la aplicación que implementa, el identificador y versión del dispositivo del perfil de aplicación, si hay complex y user descriptors, lista los clusters de entrada y salida que la aplicación usa y provee respectivamente.

El **Perfil de Aplicación** o Application Profile, asegura la interoperabilidad de los dispositivos Zigbee desde diferentes fabricantes. Este perfil se relaciona a un área de aplicación particular del mercado, y contiene descripciones de los tipos de dispositivos e interfaces que son necesarias para el campo relevante a la aplicación.

Una entidad de datos (por ejemplo la medición de la temperatura) manejada por un endpoint Zigbee es referida como un atributo. La aplicación se puede comunicar mediante un juego de atributos por ejemplo, un termostato puede tener atributos para la temperatura, temperatura mínima, máxima temperatura y tolerancia.

Las aplicaciones Zigbee usan el concepto de un clúster para comunicar valores de atributos. Un clúster comprende un conjunto de atributos relacionados junto con un conjunto de comandos para interactuar con los atributos, por ejemplo, los atributos de medición de temperatura junto con los comandos para leer los valores de atributos. Un clúster tiene dos aspectos, los cuales son respectivamente interesados con la recepción y envío de comandos. Uno o ambos aspectos pueden ser usados por una aplicación Zigbee. Estos lados de un clúster se explican a continuación.

Un **Clúster de Entrada o Clúster Servidor**, es usado para almacenar atributos y recibir comandos para

manipular los atributos almacenados (para el cual el cluster podría retornar respuestas), por ejemplo, un clúster de entrada almacenaría la medición de temperatura y los atributos asociados, y respondería a los comandos los cuales hacen la petición de lecturas de estos atributos.

Un **Clúster de Salida o Cliente Clúster**, es usado para manipular atributos en el correspondiente clúster de entrada al enviarle comandos (a los cuales el clúster puede retornar respuestas). Normalmente, estos son comandos de escritura para setear valores de atributos y comandos de lectura para obtener valores de atributos (los valores de lectura son retornados en respuestas).

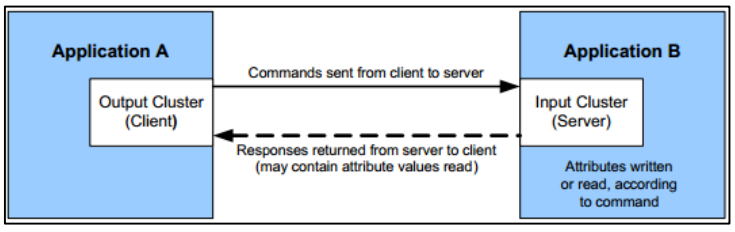


Figura 2.20: Clústers de entrada y salida.

La figura anterior muestra los clústers de entrada y salida [24]. La especificación Zigbee provee la

facilidad a los dispositivos para encontrar las características de otros nodos en la red, tales como sus direcciones, los tipos de aplicaciones que funcionan en ellos, la fuente de poder y el comportamiento en modo sleep.

El Discovery es típicamente usado cuando un nodo está siendo introducido dentro de una red configurada por usuario, tal como la seguridad doméstica o un sistema de control de iluminación. Para integrar el dispositivo dentro de una red se puede requerir al usuario iniciar el proceso de integración al presionar un botón o un similar. La primera tarea es encontrar si hay alguno de los dispositivos apropiados con lo cual el nuevo nodo se puede comunicar.

El **Device Discovery** retorna la información acerca de las direcciones de un nodo de la red. La información recuperada puede ser la dirección IEEE/MAC del nodo con una dirección de red dada, o la dirección de red de un nodo con una dirección IEEE/MAC dada. Si el nodo es un router o coordinador, puede opcionalmente proveer las direcciones de todos los dispositivos que

están asociados con él, así como también su propia dirección.

El **Service Discovery** permite a un nodo solicitar información desde un nodo remoto acerca de las características de un nodo remoto. Esta información es almacenada en un número de descriptores en el nodo remoto. Las peticiones para estos descriptores son hechos por un dispositivo durante el proceso de Discovery que es típicamente parte de la configuración e integración de los dispositivos dentro de una red Zigbee.

CAPA DE RED

La operación básica en una red es transferir data de un nodo a otro. La data es originada desde una entrada (posiblemente un switch o un sensor) en el nodo de origen, y es comunicado a otro nodo el cual puede interpretar y usar la data.

En la comunicación de datos más simple, la data es transmitida directamente desde el nodo de origen al nodo de destino. Sin embargo, si los dos nodos están

muy alejados o en un ambiente difícil, la comunicación directo no puede ser posible. En este caso, es necesario enviar la data a otro nodo dentro del alcance de la señal, el cual pasa la data a otro nodo, y así hasta que el nodo destino es alcanzado, esto es, para usar uno o más nodos intermediarios como saltos. El proceso de recibir datos destinados para otro nodo y pasarlo a otro es conocido como enrutamiento.

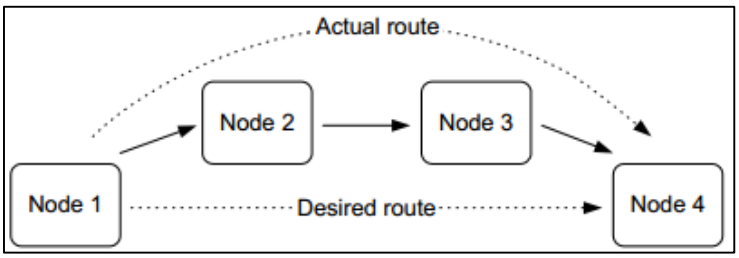


Figura 2.21: Enrutamiento de Mensajes.

En la figura anterior se muestra el enrutamiento de mensajes [24]. El enrutamiento permite que el alcance de una red pueda ser extendida más allá de las distancias soportadas por una comunicación de radio directa. Dispositivos remotos pueden unirse a una red al conectarse a un router.

Si un mensaje enviado de un nodo a otro necesita pasar a través de uno o más nodos intermediarios para alcanzar su destino final, hasta 30 saltos son permitidos), el mensaje lleva dos direcciones de destino: 1) la dirección del destino final y 2) la dirección del nodo el cual es el próximo salto.

Cuando un nuevo nodo se une a una red, debe encontrar nodos compatibles con los cuales es capaz de comunicarse, este proceso es facilitado por el mecanismo ‘Service Discovery’. El debe entonces escoger con cual de los nodos compatibles se comunicará. Un método de emparejamiento o ‘pairing’ de nodos para una fácil comunicación es provista por el mecanismo ‘binding’.

A través del **Service Discovery**, el nodo realiza una petición broadcast al resto de nodos de la red para saber los servicios que estos brindan; el mensaje se propaga por toda la red. Cualquier nodo que ha recibido la petición de los servicios, luego envía una respuesta unicast al nodo que envió la petición, por ende el nodo que envió la petición recibirá más de una

respuesta. Una respuesta incluye la dirección de red de un nodo remoto que contiene los servicios peticionados. El nodo almacena esta dirección localmente y la aplicación puede usar la dirección para todas las comunicaciones futuras al nodo remoto. Esto es lo que se llama direccionamiento directo. Alternativamente, en vez de usar direccionamiento directo en sus comunicaciones, dos nodos se pueden comunicar a través del mecanismo binding.

El mecanismo **Binding** permite a los nodos estar emparejados de tal forma que un cierto tipo de data de salida de un nodo sea automáticamente enrutada a un nodo, sin la necesidad de especificar la dirección de destino y un endpoint cada vez y cuando. Los dos nodos deben conocer que ambos existen y están dentro del alcance de sus señales de radio. Esto se realiza mediante el service discovery. Este mecanismo tiene un nodo de origen y un nodo de destino, relacionado a la dirección en la cual la data será enviada entre los nodos. Los detalles de un binding son almacenados como una entrada en una tabla

binding, normalmente mantenidos en el nodo de origen del binding o algunas veces en otro nodo.

Durante el proceso binding, la tabla binding para el nodo de origen es actualizada o si es necesaria, es creada. El binding ocurre en la capa de aplicación usando los clústers. Para que dos aplicaciones usen el mecanismo binding entre ellas, deben soportar el mismo clúster.

Estos son los posibles tipos de binding entre nodos:

- *Uno a uno,* este es un binding simple en el cual un nodo se une a otro (y únicamente con ese otro).
- *Uno a muchos,* este tipo de binding en el cual un nodo de origen se une a muchos nodos.
- *Muchos a uno,* este es un binding en el cual más de un nodo de origen es unido a un solo nodo.

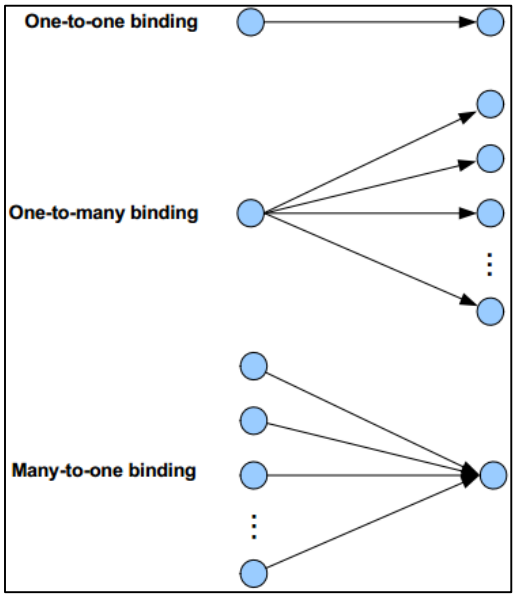


Figura 2.22: Tipos de Binding.

En la figura anterior se muestran los tipos de binding [23]. A manera de ejemplo, considaremos el caso de los interruptores y bombillos:

- En el caso de uno a uno, un interruptor controla un bombillo.
- En el caso de uno a muchos, un interruptor controla varios bombillos.
- En el caso de muchos a uno, varios interruptores controlan un solo bombillo.

CAPA DE ENLACE DE DATOS

La capa de enlace de datos es provista por el estándar IEEE 802.15.4 y es responsable por el direccionamiento – para data de salida, esta determina a donde la data es enviada y para la data de entrada determina de donde ha venido. También es responsable por armar los paquetes de datos o las tramas a ser transmitidas y por desarmar las tramas recibidas. En el estándar IEEE 802.15.4, la capa de enlace de datos es referida como la MAC y las tramas usadas son tramas MAC. Otra de las responsabilidades de esta capa es de:

- Proveer servicios para asociar/disociar dispositivos dentro de la red
- Proveer control de acceso a canales compartidos
- Generación de Beacons, los cuales son paquetes de datos que contienen toda la información de la red
- Garantiza la gestión de paquetes de datos, sólo en caso de ser necesario.

La capa de enlace de datos está compuesta por dos subcapas. La subcapa MAC y la subcapa LLC. La

subcapa LLC es común a los estándares IEEE 802 por aquello puede ser ignorada en el desarrollo de aplicaciones IEEE 802.15.4

La subcapa MAC también ofrece los siguientes servicios para la siguiente capa:

- MAC Data Service, provee un mecanismo para el traspaso de data hacia y desde la siguiente capa superior.
- MAC Management Services, provee un mecanismo para controlar los ajustes de las funcionalidades de comunicación, radio y networking, desde la siguiente capa superior.

CAPA FÍSICA

La capa física es provista por el estándar IEEE 802.15.4 y es concerniente con la interfaz al medio de transmisión físico (en este caso las ondas de radio), bits de intercambio de data con este medio, así como

el intercambio de bits de data con la capa de enlace de datos.

Más específicamente, sus responsabilidades hacia el medio incluye:

- Evaluación de canales
- Comunicación a nivel de bits, modulación de bits, demodulación de bits, sincronización de paquetes.

La capa física ofrece los siguientes servicios a la subcapa MAC:

- Data Service, provee un mecanismo para pasar la data hacia y desde la subcapa MAC.
- Management Services, provee un mecanismo para controlar los ajustes de las comunicaciones de radio y su funcionalidad desde la subcapa MAC.

CAPÍTULO 3

DESCRIPCIÓN DE LA VIVIENDA SOBRE LA CUAL SE APLICARÁN LOS ESTÁNDARES DOMÓTICOS.

3.1. Generalidades.

La vivienda sobre la cual se aplicará el diseño de este proyecto comprende una planta baja y una planta alta, con secciones claramente diferenciadas en cada planta.

El terreno donde se edifica la vivienda tiene una extensión de 1000 metros cuadrados aproximadamente. Tanto la planta alta como la planta baja tienen una extensión de construcción de aproximadamente 400 metros cuadrados. La altura de la vivienda alcanza los 10 metros.

3.2. Descripción física de la vivienda.

3.2.1. Planos Generales.

A continuación se presentan los planos de la vivienda, tanto de la planta baja como de la planta alta.

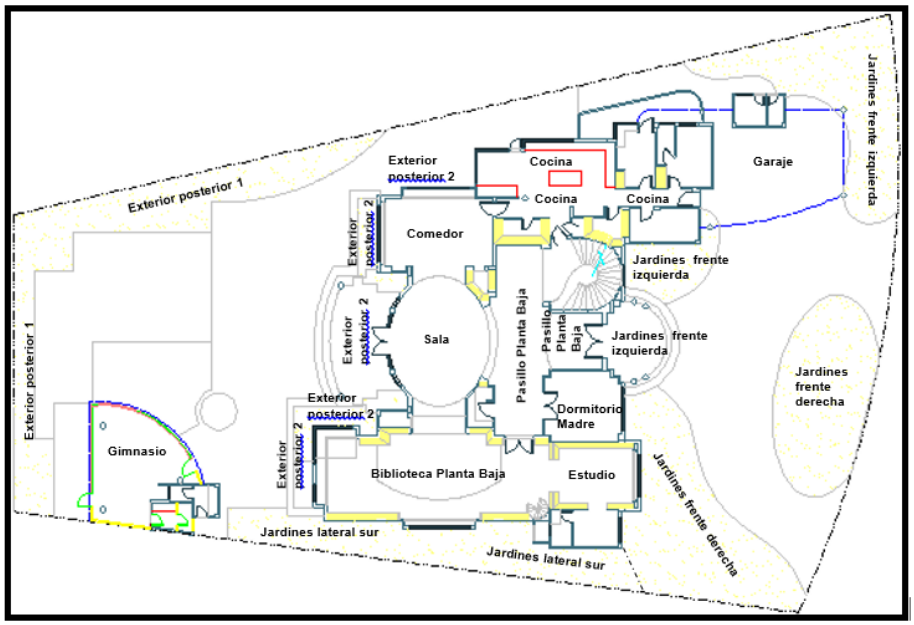


Figura 3.1: Planta baja de la vivienda.

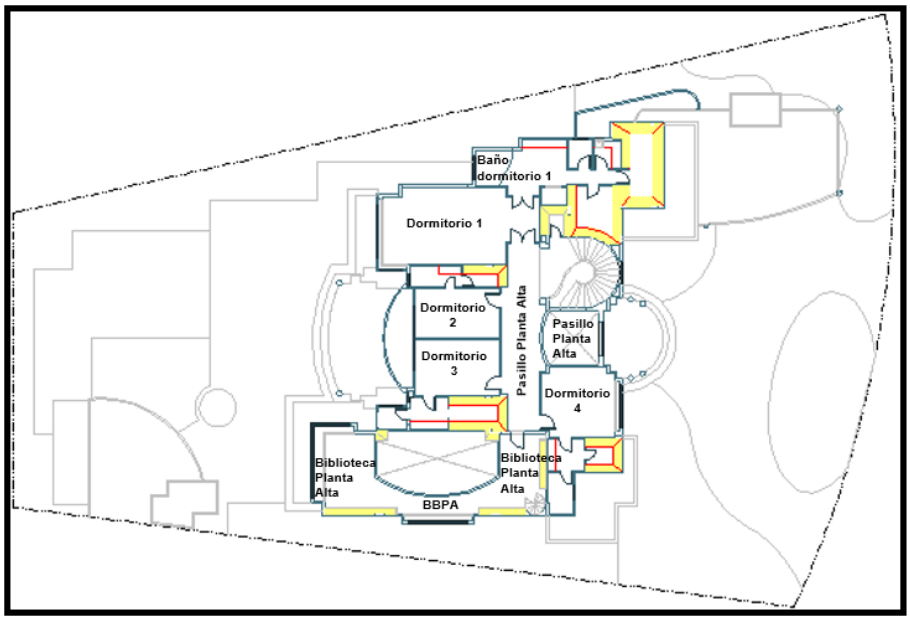


Figura 3.2: Planta alta de la vivienda.

En el siguiente subtema se muestra cual es cada sector de los planos tanto de la planta alta como de la planta baja.

3.2.2. Sectorización del Condominio.

Con la finalidad de facilitar la ubicación de cada uno de los dispositivos domóticos y para llevar un mejor control de la instalación de los mismos se procede a sectorizar la vivienda.

Los sectores a tomar en consideración en la vivienda son los siguientes:

1. Baño Dormitorio 1
2. Biblioteca Planta Alta
3. Biblioteca Planta Baja
4. Cocina
5. Comedor
6. Dormitorio 1
7. Dormitorio 2
8. Dormitorio 3
9. Dormitorio 4
10. Dormitorio Madre
11. Estudio
12. Exterior posterior 1
13. Exterior posterior 2
14. Garaje
15. Gimnasio
16. Jardines frente izquierda
17. Jardines frente derecha
18. Jardines lateral sur
19. Pasillo planta alta
20. Pasillo planta baja
21. Sala

3.3. Definición de las necesidades domóticas.

Debido a que la domótica busca proveer y brindar a los usuarios finales un entorno agradable y protegido, y con la posibilidad de monitorear y controlar lo que sucede en las viviendas, respondiendo a los avances actuales en cuanto a tecnología, se gestiona en este proyecto las áreas de networking, seguridad y confort.

3.3.1. Gestión del networking.

La vivienda debe tener una red privada interna, la misma que debe ser accesible desde la internet y también pueda salir a internet, de tal forma que desde lugares remotos a la misma se la pueda monitorear y controlar.

Se debe brindar la posibilidad de acceder a la red privada interna de dos formas, de manera alámbrica o de manera inalámbrica.

Se usarán equipos dedicados a crear una red privada interna tanto que sea cableada e inalámbrica mediante el empleo de routers, switches, firewall, controladores de puntos de acceso inalámbricos y puntos de acceso inalámbricos.

También se tendrán 2 medios físicos: 1) el cable de cobre y 2) el espacio (para la comunicación inalámbrica). La fibra óptica no será usada para ningún tipo de comunicación pero se la dejará tendida para un uso futuro.

3.3.2. Gestión de la seguridad.

La gestión de la seguridad considera los siguientes aspectos:

- Monitoreo de los sectores de la vivienda mediante cámaras
- Detección de apertura y cerrado de puertas para iluminar sus respectivas secciones durante la noche una vez abiertas mediante escenas en el VERA3 maestro.
- Sensar el movimiento de personas durante la noche para poder iluminar las áreas por donde estas transitan mediante escenas en el VERA3 maestro.

Debido a que en la vivienda está instalada una cocina eléctrica de inducción, se prescinde del uso de sensores de humo y sensores de gas.

A continuación se detalla por sector, la gestión de seguridad respectiva, mediante una tabla:

SECTOR	MONITOREO MEDIANTE CÁMARAS	APERTURA/CERRADO DE PUERTAS	SENSORES DE MOVIMIENTO
Baño dormitorio 1	0	5	0
Biblioteca planta alta	1	1	3*
Biblioteca planta baja	1	1	3*
Cocina	1	2	1*
Comedor	0	0	1*
Dormitorio 1	0	1	1*
Dormitorio 2	0	1	1*
Dormitorio 3	0	1	1*
Dormitorio 4	0	1	1*
Dormitorio madre	0	1	0
Estudio	1	1	1*
Exterior posterior 1	0	0	0
Exterior posterior 2	4	0	0
Garaje	0	0	1*
Gimnasio	0	0	0
Jardines frente izquierda	2	0	0
Jardines frente derecha	1	0	0
Jardines lateral sur	0	0	0
Pasillo planta alta	1	0	1**
Pasillo planta baja	1	1	1***

Sala	0	0	1****
TOTAL	13	16	17
*Sensor de movimiento de la marca Aeon Labs ** Sensor de movimiento de la marca Everspring *** Sensor de movimiento de la marca Schlage **** Sensor de movimiento de la marca Express Controls			

Tabla 3.1: Gestión de seguridad por sector de la vivienda.

El número de dispositivos no se basa ni en normas ni en cálculos. El número de cámaras y sus ubicaciones fueron establecidas para poder cubrir las áreas descritas en la descripción del problema. El número de sensores de apertura y cerrado de puertas y sus ubicaciones fueron establecidas a partir del número de puertas que existen en la vivienda. El número de sensores de movimiento y sus ubicaciones fueron establecidas en los sectores que consideré importantes.

3.3.3. Gestión del confort.

La gestión del confort considera los siguientes aspectos:

- Iluminación LED mediante la tecnología Hue Philips
- Control de climatización mediante termostatos mediante escenas en el VERA3 maestro.
- Apertura y cerrado de persianas dependiendo si es día o de noche mediante escenas en el VERA3 maestro.

A continuación se detalla por sector, la gestión de seguridad respectiva, mediante una tabla:

SECTOR	ILUMINACIÓN HUE PHILIPS(incluyendo el controlador Hue)	TERMOSTATOS	ACTUADORES DE PERSIANAS
Baño dormitorio 1	13	1	0
Biblioteca planta alta	19	2	4
Biblioteca planta baja	19	1	4
Cocina	14	1	0
Comedor	11	1	1
Dormitorio 1	9	1	2
Dormitorio 2	6	1	1
Dormitorio 3	6	1	1
Dormitorio 4	6	1	1
Dormitorio madre	8	1	1
Estudio	12	1	1
Exterior posterior 1	21	0	0
Exterior posterior 2	14	0	0
Garaje	7	0	0
Gimnasio	11	0	0
Jardines frente izquierda	15	0	0
Jardines frente derecha	21	0	0
Jardines lateral sur	10	0	0
Pasillo planta alta	10	0	0
Pasillo planta baja	12	1	0
Sala	16	1	2
TOTAL	260	14	18

Tabla 3.2: Gestión del Confort por sector de la vivienda.

Vale destacar que la columna ‘Iluminación Hue’ cuenta tanto a los focos Hue como a los controladores Hue.

El número de dispositivos no se basa ni en normas ni en cálculos. El número de dispositivos del sistema Hue Philips y sus ubicaciones fueron establecidas para poder cubrir la iluminación de todas las áreas de la vivienda. El número de termostatos y sus ubicaciones fueron establecidas a partir del número de sectores que existen en la vivienda donde hay uno o más aires acondicionados. El número de actuadores de persianas y sus ubicaciones fueron establecidas en los sectores donde hay persianas.

CAPÍTULO 4

DISEÑO GENERAL DEL SISTEMA DOMÓTICO.

4.1. Control del sistema domótico.

El sistema domótico del presente proyecto gestiona 3 áreas: networking, seguridad y confort. Cada área posee sus dispositivos y ciertos dispositivos de estas áreas pertenecen a otras pero no todos los dispositivos son completamente compatibles y operables entre ellos. Aun cuando usamos el dispositivo que funciona como el “control” del sistema domótico que busca compatibilizar la mayoría de dispositivos, hay algunos como los equipos de networking que no se pueden compatibilizar.

Antes de definir el control del sistema domótico como tal, voy a presentar una descripción gráfica que muestra una visión sintetizada del sistema con las áreas y dispositivos por área.

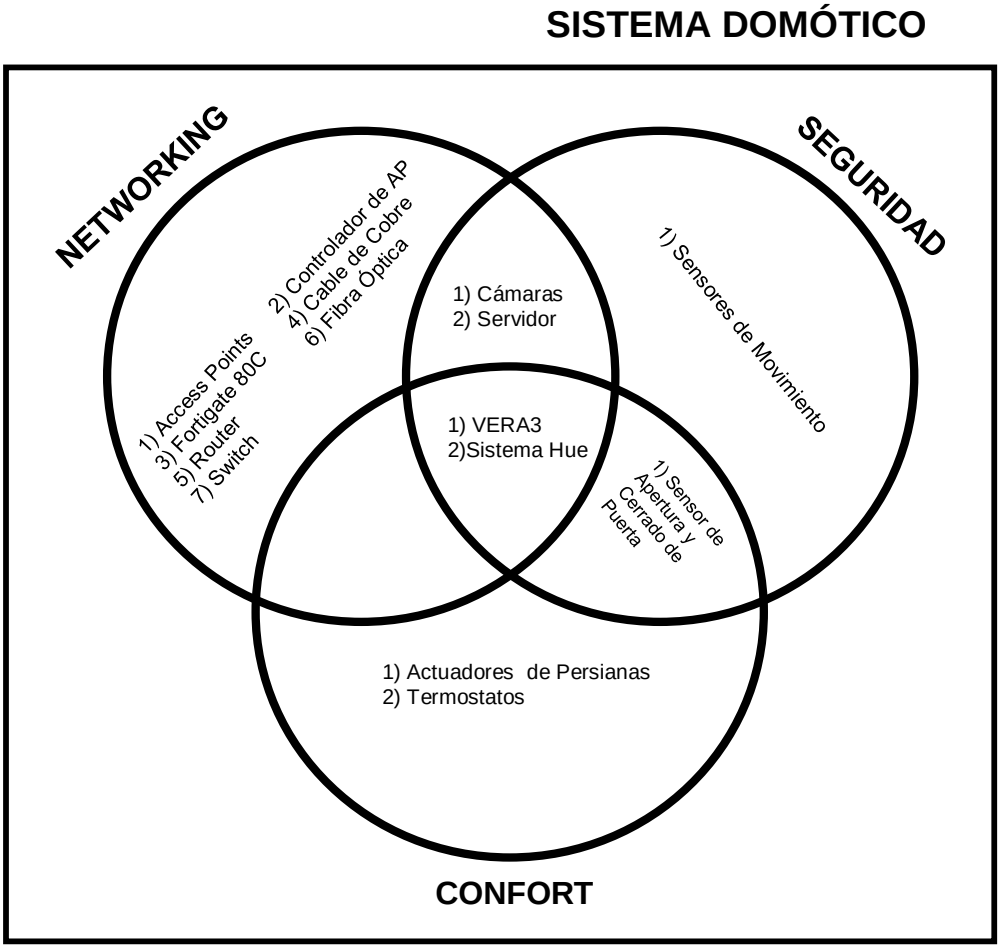


Figura 4.1: Descripción gráfica del sistema domótico.

Como apreciamos en la figura 4.1 se muestran las áreas del sistema domótico, sus propios dispositivos y dispositivos que forman parte de otras áreas. Los dos únicos dispositivos que forman parte de las tres áreas son el VERA3 y el sistema HUE. El VERA3 será el control del sistema domótico y está orientado a controlar la mayoría de dispositivos de las áreas de confort y seguridad. La ubicación de los 3 dispositivos VERA3 que usaremos será justo en la mitad de la

Biblioteca Planta Alta. Esta ubicación fue designada a base de prueba y error.

En la siguiente figura se muestra el dispositivo controlador del sistema domótico VERA3 [25].

Figura 4.2: Dispositivo controlador del sistema domótico VERA3.

Función

Este dispositivo busca controlar mayoritariamente los dispositivos de las áreas de seguridad y confort, los cuales funcionan bajo el protocolo de comunicación Z-Wave y mediante una aplicación del ‘app store’ del VERA3, incorpora a los focos de la tecnología Hue Phillips que

funcionan bajo el protocolo de comunicación Zigbee. El VERA3 nos permite realizar las configuraciones de escenas, que dan vida a la domótica, al realizar una acción dentro de la vivienda debido al estado de un sensor. El caso más sencillo, es el de la iluminación activada por un sensor de movimiento.

Especificaciones

- CPU: 500 MHz MIPS SoC
- Memoria Flash: NAND 32 MB
- Memoria SDRAM: 32 MB
- Memoria DDR2: 128 MB
- Puertos USB: 2
- Puertos WAN: 1
- Puertos LAN: 4
- Z-Wave: Incorporado con antena interna
- Wi-Fi: 802.11n
- Dimensiones: 177mm x 130mm x 34 mm (Ancho/Largo/Altura)
- Alimentación: 12V @ 2A

Características

- Manejo de hasta 200 dispositivos Z-Wave

- Envío de alertas mediante correo y mensajes de texto
- Largo alcance de señal ya sea puertas adentro o puertas afuera
- Se engancha fácilmente a la red Wi-Fi o cableada de la vivienda

Para la realización de este proyecto se usarán 3 de estos equipos con el siguiente direccionamiento IPv4:

1er VERA3 ESCLAVO

- Dirección IP → 172.16.2.1
- Máscara de Subred → 255.255.0.0
- Gateway → 172.16.0.1
- DNS → 200.93.192.148

2do VERA3 MAESTRO

- Dirección IP → 172.16.2.2
- Máscara de Subred → 255.255.0.0
- Gateway → 172.16.0.1
- DNS → 200.93.192.148

3er VERA3 ESCLAVO

- Dirección IP → 172.16.2.3
- Máscara de Subred → 255.255.0.0

- Gateway → 172.16.0.1
- DNS → 200.93.192.148

CONFIGURACIÓN

El VERA3 tiene una interfaz de usuario amigable con el usuario tal como lo muestra la siguiente figura. 'Micasaverde' es la compañía que creó este equipo.

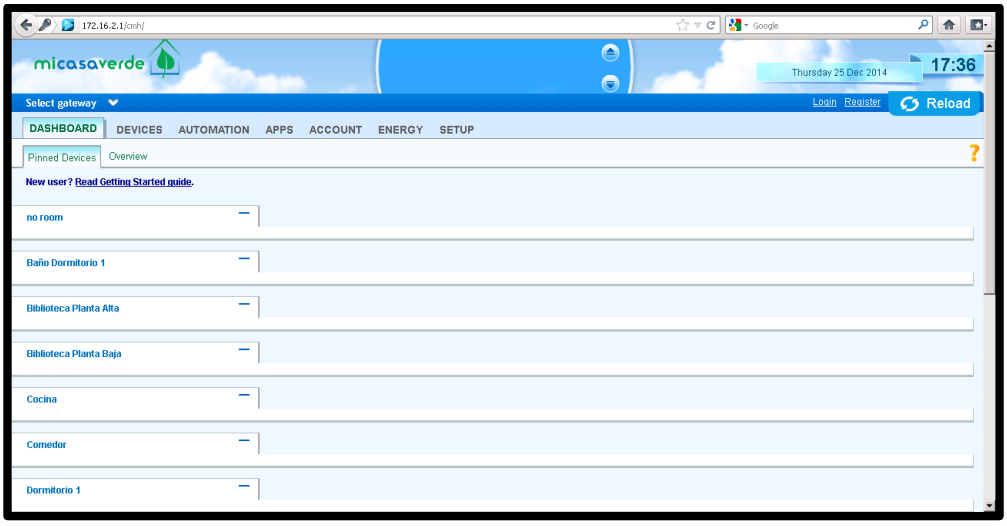


Figura 4.3: Interfaz Gráfica de Usuario del VERA3.

La mayoría de las pestañas las usaremos a excepción de las pestañas "Account" y "Energy". La configuración del VERA3 la realizamos en la pestaña 'SETUP'.

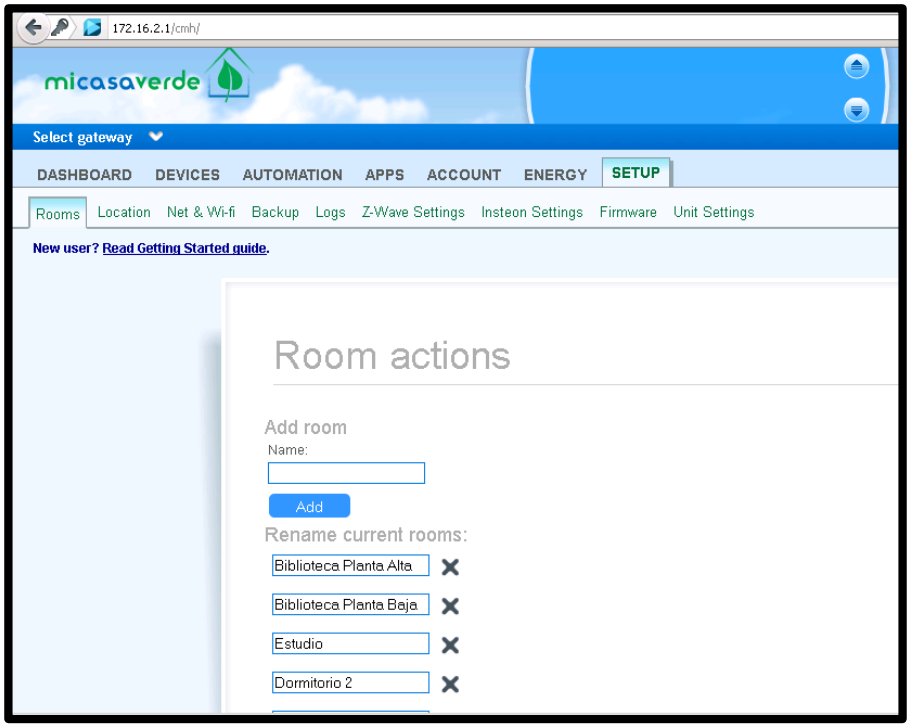


Figura 4.4: Pestaña SETUP opción Rooms.

En la figura 4.4 se muestra la pestaña ‘SETUP’ opción ‘Rooms’ que permite agregar las áreas donde se colocarán los dispositivos domóticos. Existe el ‘Room’, con nombre ‘no room’ donde se guarda todo dispositivo recién incluido en el VERA3.

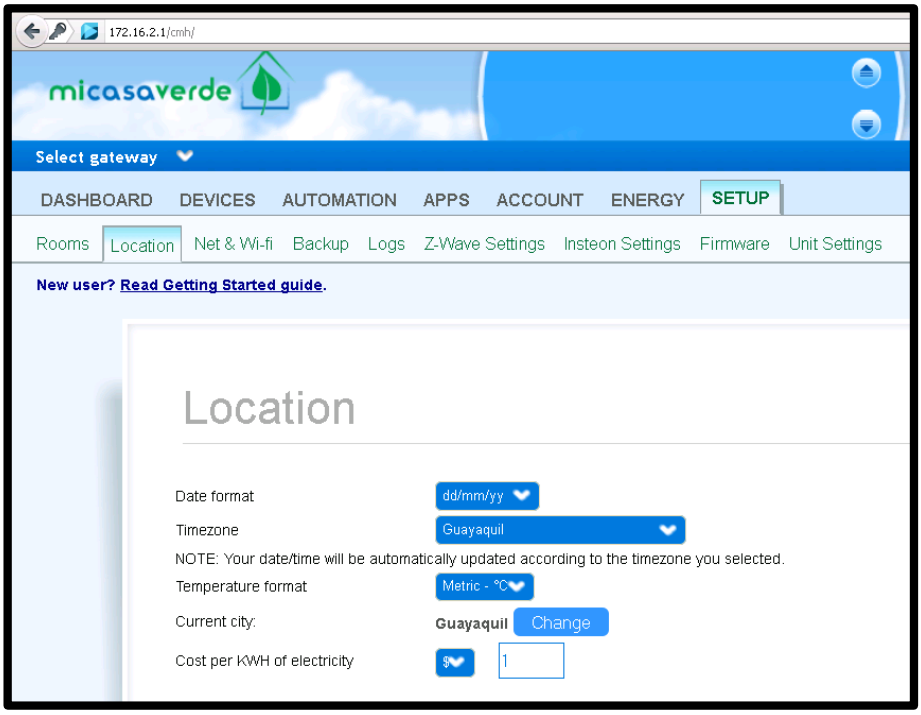


Figura 4.5: Pestaña SETUP opción LOCATION.

En la figura 4.5 se muestra la pestaña 'SETUP' opción 'Location'. En el campo "Date Format" escogemos 'dd/mmyy' que establece la fecha en días, meses y años. En el campo "Timezone" escogemos 'Guayaquil'. En el campo "Temperature Format" escogemos 'Metric-ºC' que establece la temperatura en grados centígrados. En el campo "Current City" escogemos 'Guayaquil'. El último campo no se lo usa para el desarrollo de este proyecto debido a que en este proyecto no se gestiona el consumo de energía, función para la cual fue creada este campo.

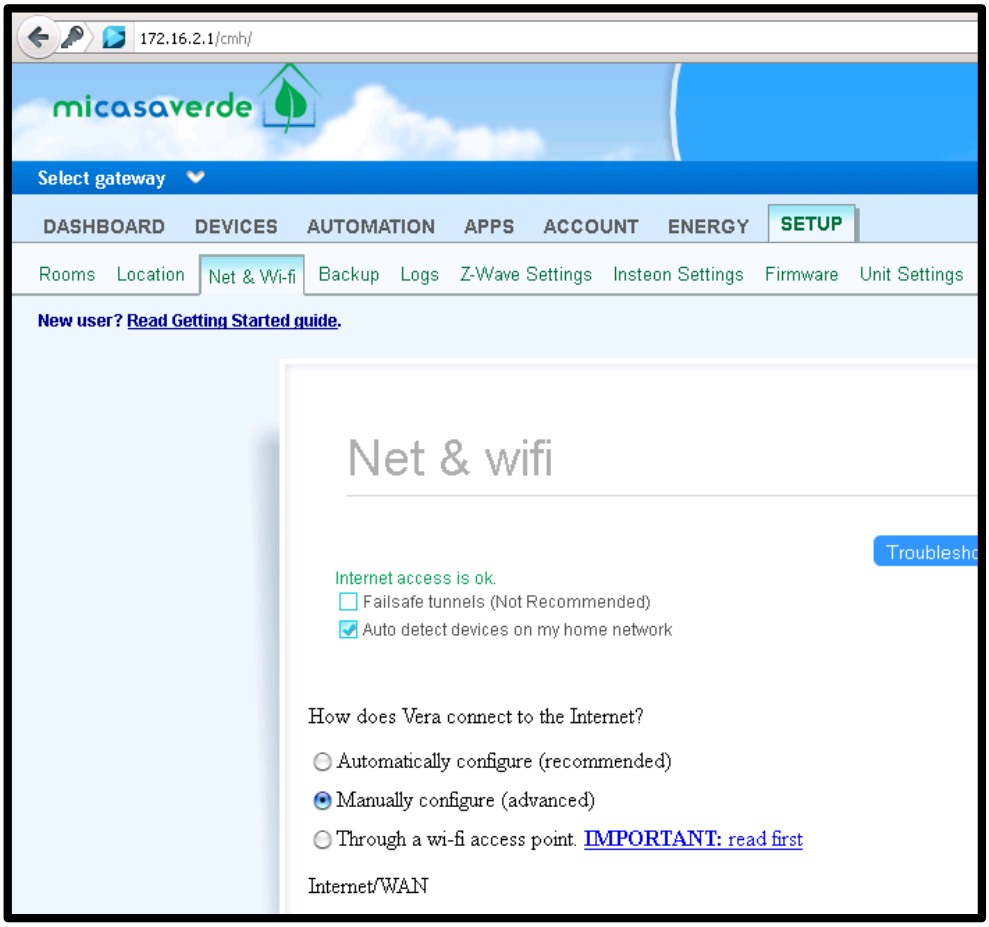


Figura 4.6: Pestaña SETUP opción Net & Wi-Fi parte 1.

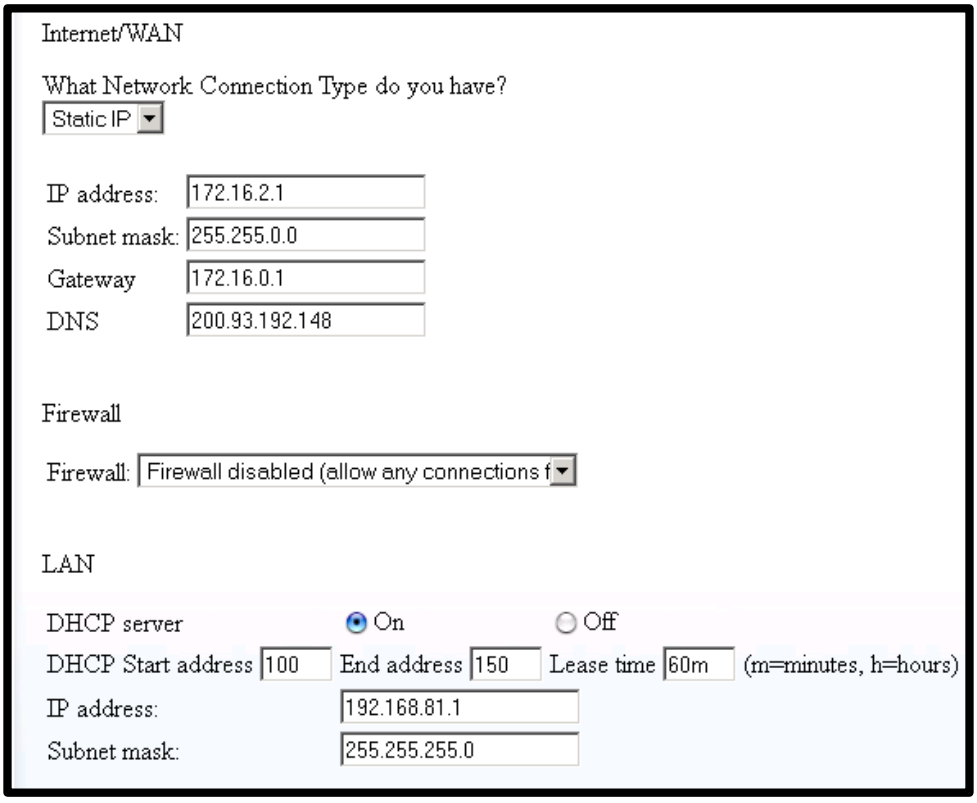


Figura 4.7: Pestaña SETUP opción Net & Wi-Fi parte 2.

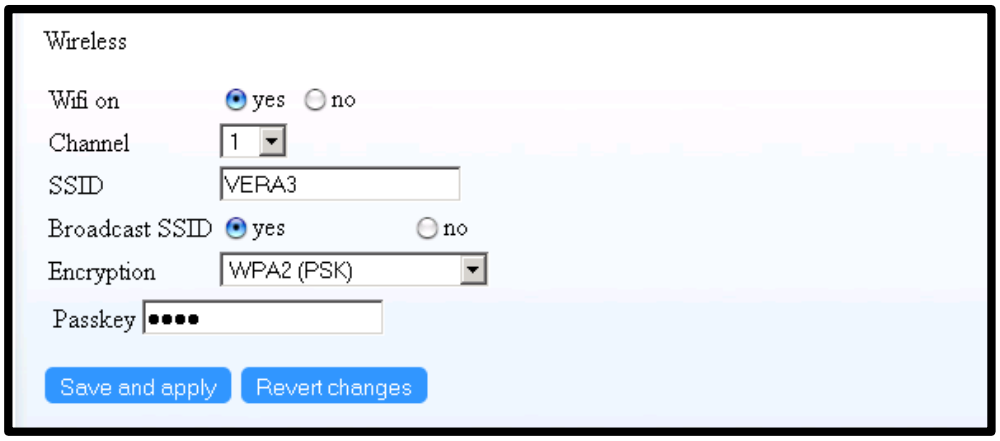


Figura 4.8: Pestaña SETUP opción Net & Wi-Fi parte 3.

En la figura 4.6 se muestra la 1era parte de la pestaña ‘SETUP’ opción ‘Net & Wi-Fi’. Marcamos la casilla ‘Auto detect devices on my home network’. En la pregunta ‘How does Vera connect to the Internet?’, escogemos manually configure (advanced).

En la figura 4.7 se muestra la 2da parte de la pestaña ‘SETUP’ opción ‘Net & Wi-Fi’ y editamos los campos a continuación y en orden. En la sección ‘Internet/WAN’ y en la pregunta ‘What network connection type do you have’, escogemos ‘Static IP’. En los campos IP address, subnet mask, Gateway y DNS se llena de acuerdo al direccionamiento respectivo. En la sección ‘Firewall’ escogemos la opción ‘Firewall disabled (allow any connections)’. En la sección ‘LAN’ y en el campo ‘DHCP server’ escogemos ‘ON’. En el campo ‘DHCP Start address, End address y Lease time, escribimos 100, 150 y 60m respectivamente. En el campo ‘IP address’ y en el campo ‘Subnet mask’ escribimos ‘192.168.81.1’ y ‘255.255.255.0’.

En la figura 4.8 se muestra la 3era parte de la pestaña ‘SETUP’ opción ‘Net & Wi-Fi’ y editamos los campos a continuación y en orden. En la sección ‘Wireless’ y en el campo ‘Wi-Fi’ seleccionamos ‘yes’. En el campo ‘Channel’ escogemos ‘1’. En el campo ‘SSID’ escogemos ‘VERA3’. En el campo ‘Broadcast SSID’ escogemos ‘yes’. En el campo ‘Encryption’ escogemos ‘WPA2 (PSK)’. Y en el campo ‘Passkey’

escogemos una clave. Damos click en la opción ‘Save and apply’ para guardar y aplicar los cambios realizados.

Las pestañas ‘Back-up’ y ‘Logs’ vienen con configuraciones por defecto y se las deja así. Estas pestañas nos sirven sólo para hacer copias de seguridad y un correcto troubleshooting en caso de fallar el VERA3.

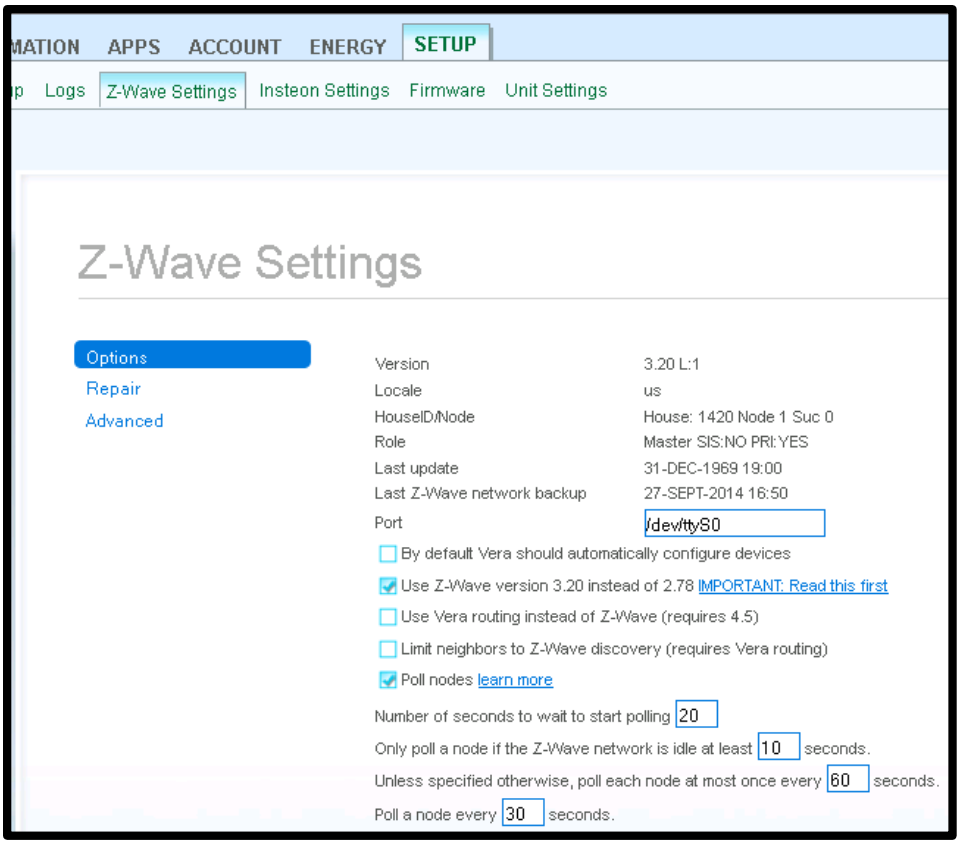


Figura 4.9: Pestaña SETUP opción Z-Wave Settings.

En la figura 4.9 se muestra la pestaña ‘SETUP’ opción ‘Z-Wave Settings’. Escogemos la subopción ‘Options’ y editamos los campos a

continuación y en orden. En el campo ‘Port’ escribimos ‘/dev/ttyS0’ que lo único que hace es decirle al VERA3 que la red Z-Wave que se va a construir se almacenará dentro de él. Marcamos la casilla ‘Use Z-Wave version 3.20 instead 2.78’ para usar la última versión del protocolo Z-Wave disponible en el VERA3 y la casilla ‘Poll Nodes’ para que el VERA3 realice el proceso de “polling” a un nodo de la red. El proceso “polling” permite saber el estatus de un nodo de la red, es decir, si está activo y alcanzable de manera directa por el controlador máster o a través de saltos, o no lo está. En el campo ‘Number of seconds to wait to start polling’ escribimos 20, es decir una cada vez que se encienda el VERA3 se esperará 20 segundos antes de hacer el proceso de polling. El campo ‘Only poll a node if the Z-Wave network is idle at least 10 seconds’ establece que el VERA3 hará un proceso de polling a los nodos si es que la red está inactiva por lo menos 10 segundos. El campo ‘Unless specified otherwise, poll each node at most once every 60 seconds’ establece que por lo menos se realiza el proceso de polling a todos los nodos por lo menos una vez cada 60 segundos. El campo “Poll a node every 30 seconds” establece que se realizará el proceso de polling a un nodo cada 30 segundos.

Las pestañas ‘Insteon Settings’, ‘Firmware’ y ‘Unit Settings’ no las usamos y se las deja con las configuraciones por defecto que vienen configuradas de fábrica.

TRABAJO DE LOS VERA3 EN CASCADA

Debido a que tenemos 3 VERA3 en nuestra vivienda, es necesario que uno ocupe el rol de maestro y los otros dos ocupen los roles de ‘esclavos’. Desde el VERA3 maestro, se podrá manejar a todos los dispositivos domóticos de los tres VERA3. En nuestro caso, hemos definido lo siguiente:

- 1er VERA3 → ESCLAVO
- 2do VERA3 → MAESTRO
- 3er VERA3 → ESCLAVO

Todos los dispositivos que no funcionen con baterías serán incluidos en el 1er VERA3. Los focos hue y sus controladores serán incluidos en el 3er VERA3. Los dispositivos que funcionen con baterías serán incluidos en el 2do VERA3 y mediante el trabajo en cascada, el 2do VERA3 podrá controlar los dispositivos de los tres VERA3.

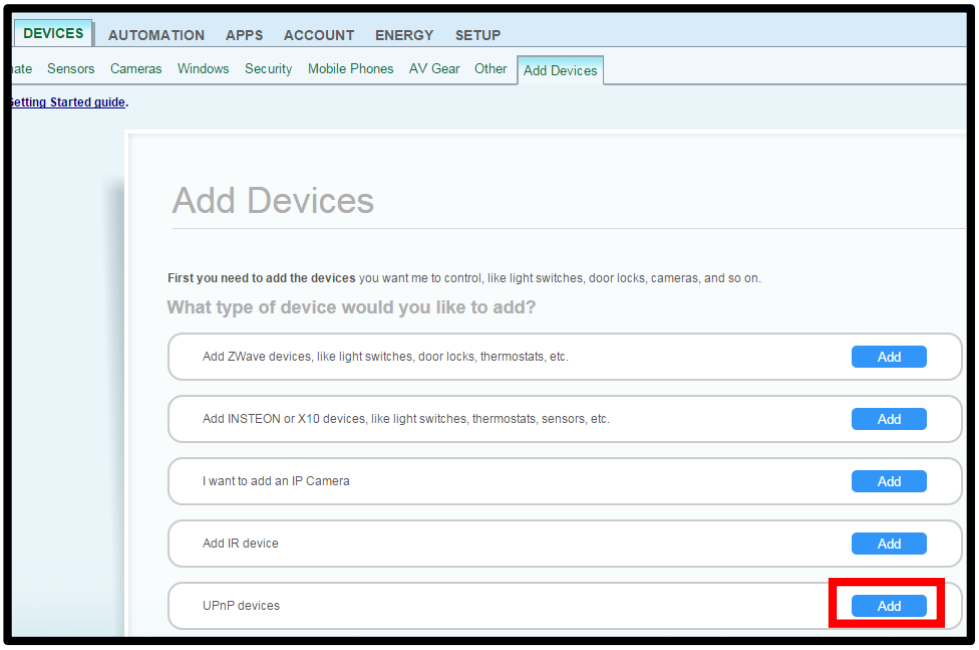


Figura 4.10: Agregar UPnP devices en la pestaña Devices con la opción Add Devices.

El VERA3 que tendrá el rol de ‘maestro’ debe agregar los dispositivos de los otros dos VERA3. Para poder realizarlo, en la pestaña ‘Devices’ y en la opción ‘Add Devices’, seleccionamos ‘Add UPnP Devices’ que significa ‘Agregar dispositivos UPnP’. Actualmente la mayoría de dispositivos electrónicos son dispositivos UPnP, el cual es un estándar que permite a los dispositivos electrónicos ser descubiertos y brindar información a otros dispositivos electrónicos a través de las redes especialmente las redes de networking.

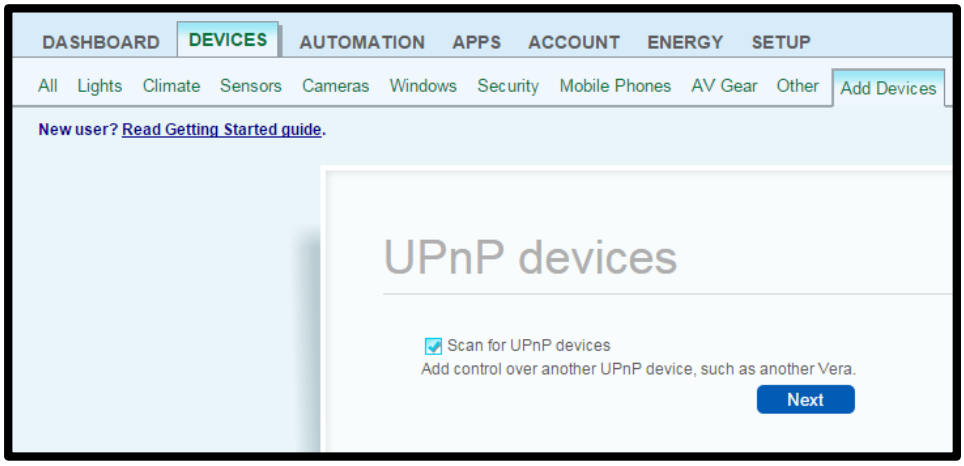


Figura 4.11: Escaneo de dispositivos UPnP.

Presionamos el botón 'Next' de la figura anterior para que el VERA3 proceda a escanear los dispositivos UPnP. En nuestro caso, el proceso de escaneo se lo realiza dentro de la red privada interna de la vivienda.

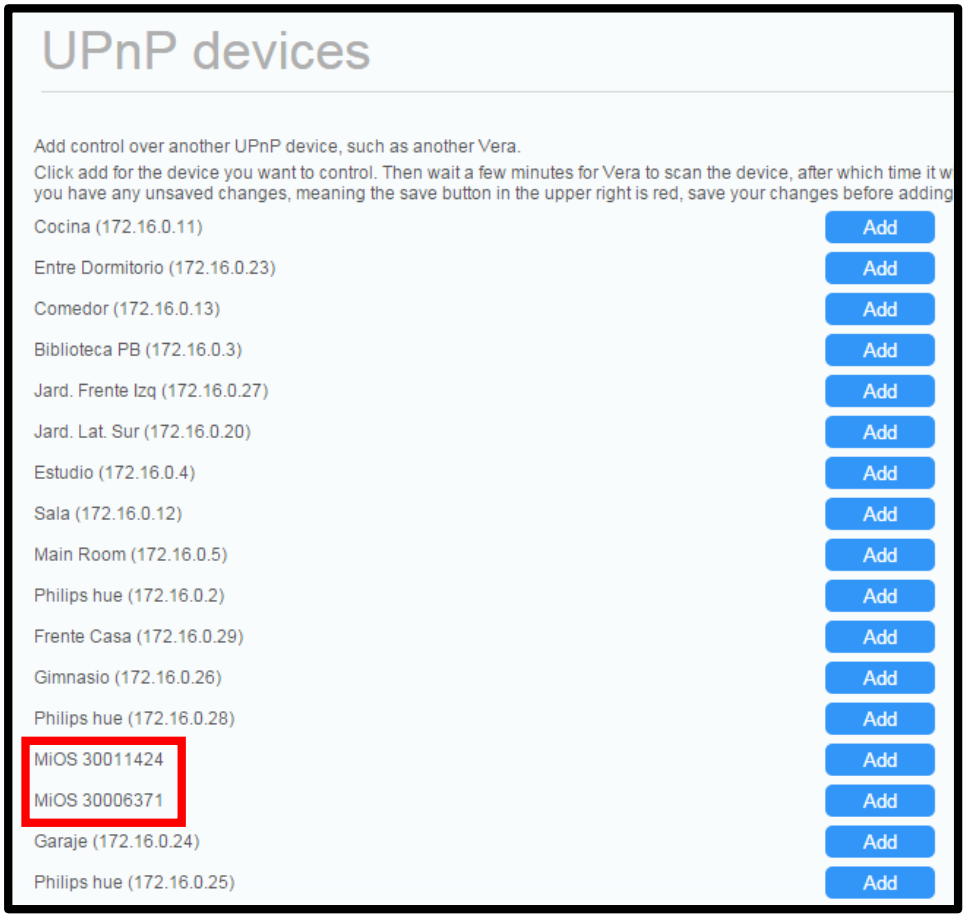


Figura 4.12: Selección de los VERA3 como dispositivos UPnP.

Se seleccionan los 2 VERA3 que aparecen en el listado de dispositivos UPnP. Los VERA3 inician con la palabra 'MiOS' que significa 'Micasaverde Operative System' y en español es, el sistema operativo de Micasaverde, la empresa que diseña y fabrica a estos dispositivos.

Figura 4.13: Inclusión de los esclavos VERA3.

Una vez seleccionados, los VERA3 aparecen dentro del 2do VERA3 en el cuarto ‘no room’ de la forma como lo muestra la figura anterior. Vale destacar, que todos los dispositivos de los dos VERA3 esclavos, también aparecen en el cuarto ‘no room’ con su nombre definido pero toca agregarlos a su ‘Room’ o área respectiva.

INCLUSIÓN DE DISPOSITIVOS A LA RED Z-WAVE

Para agregar los dispositivos de las gestiones de confort y seguridad a la red Z-Wave que gestionarán los VERA3, se debe realizar un proceso de inclusión.

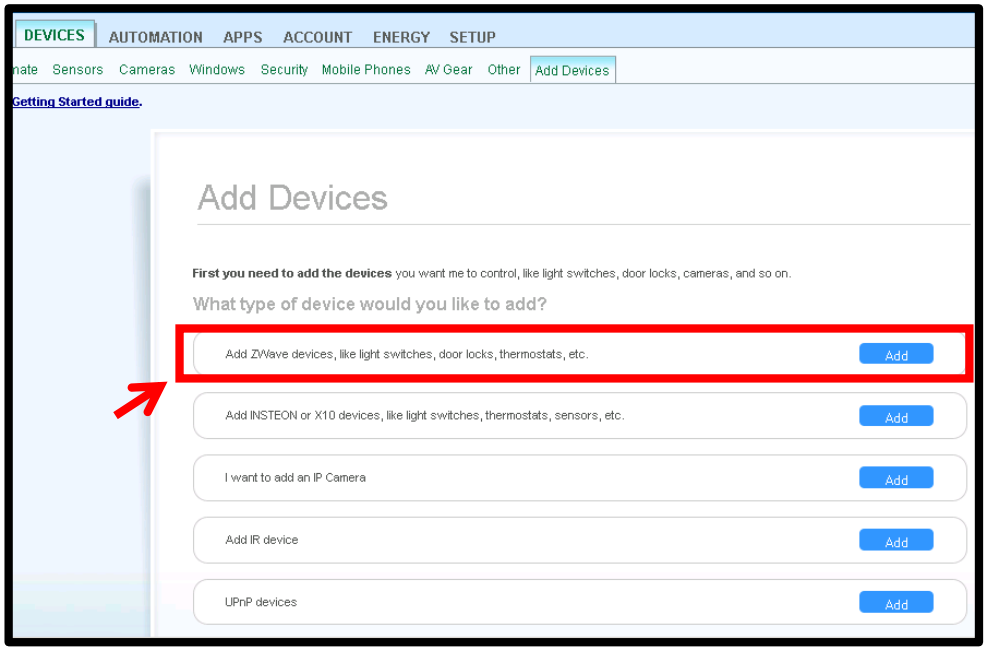


Figura 4.14: Pestaña DEVICES opción Add Devices parte 1.

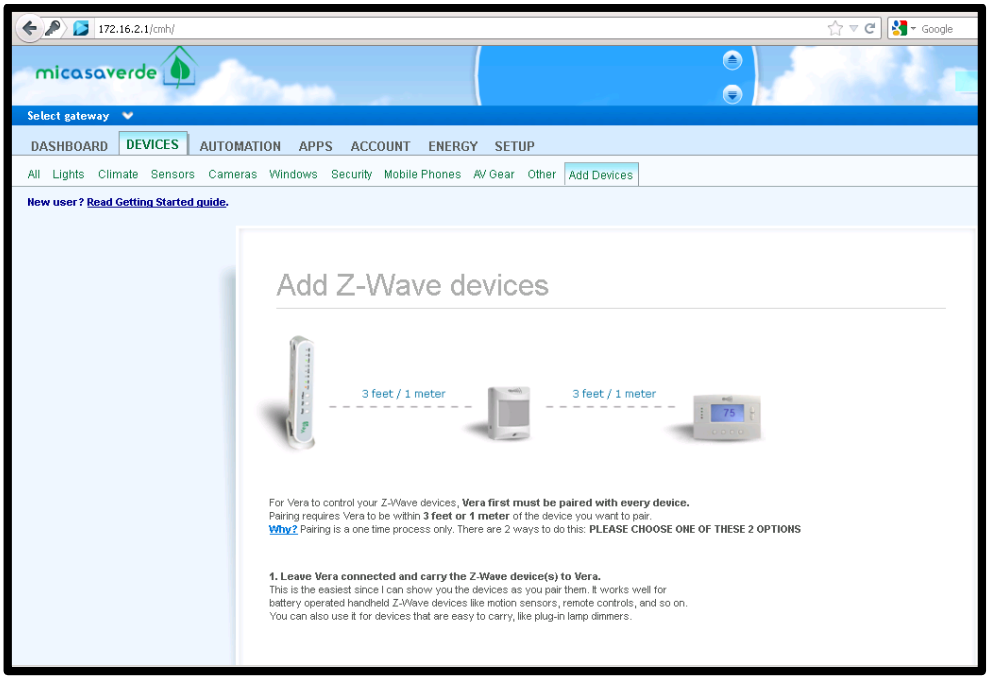


Figura 4.15: Pestaña DEVICES opción Add Devices parte 2.

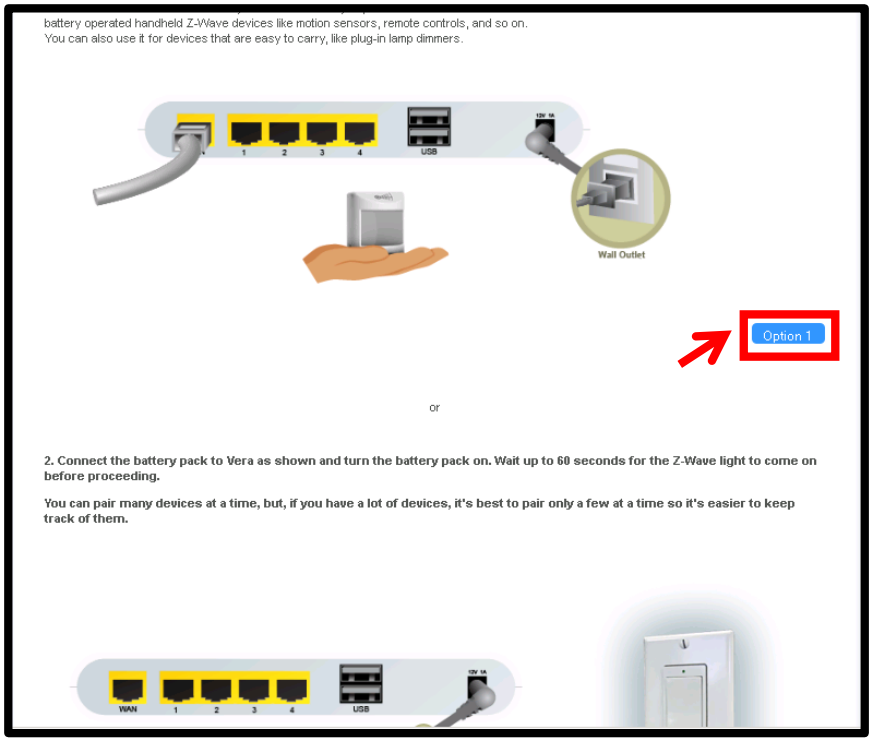


Figura 4.16: Pestaña DEVICES opción Add Devices parte 3.

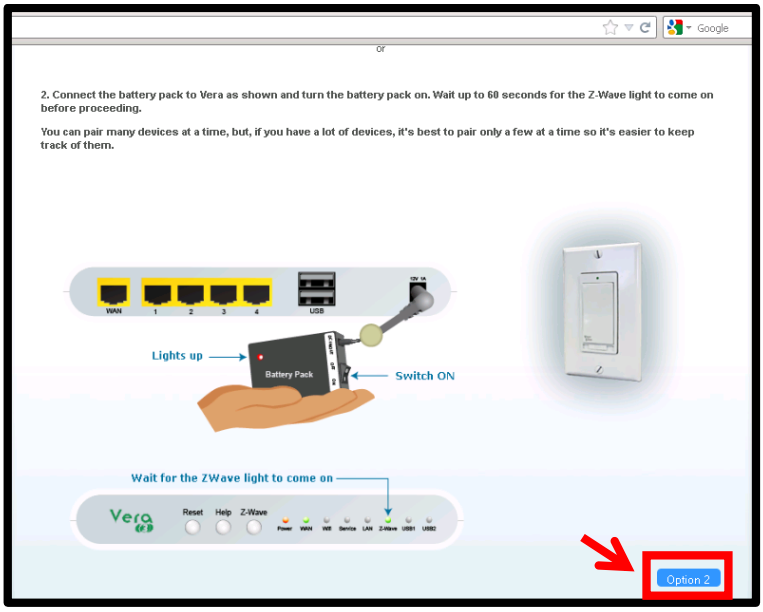


Figura 4.17: Pestaña DEVICES opción Add Devices parte 4.

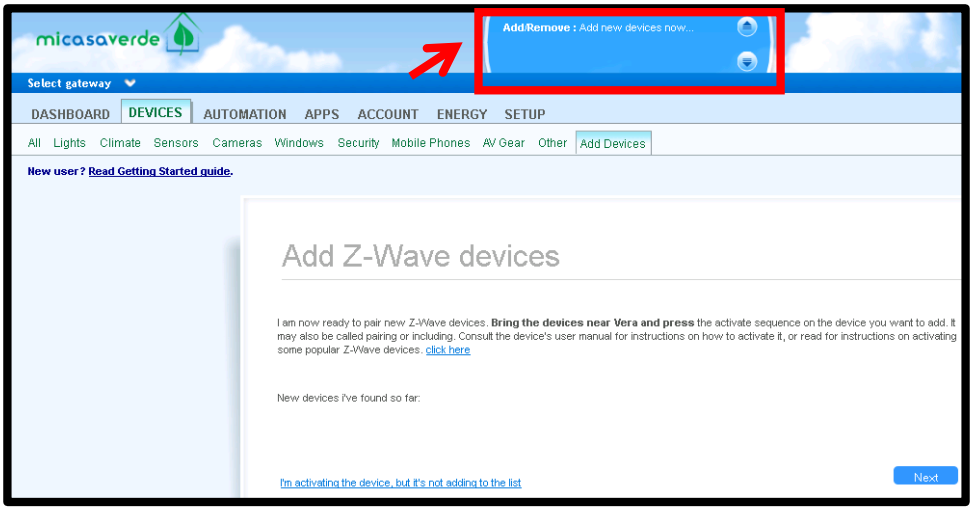


Figura 4.18: Indicador Add/Remove en cuadro de notificaciones.

Figura 4.19: Indicador Unit busy en cuadro de notificaciones.

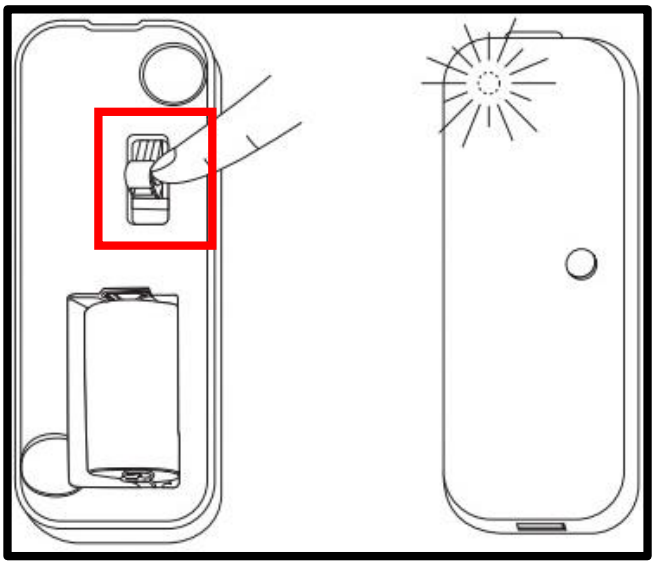


Figura 4.20: Botón de inclusión de un sensor de puerta.

En la figura 4.14, se escoge la pestaña ‘DEVICES’ y la opción ‘Add Devices’ donde se muestra la subopción ‘Add ZWave devices, like light switches, door locks, thermostats, etc.’ y escogemos ‘Add’. Luego aparece la sección ‘ADD Z-WAVE DEVICES’ y escogemos ‘Option 1’ que se aprecia mejor en la figura 4.16. En el cuadro de notificaciones aparece el mensaje ‘Add/Remove: Add new devices now…’ tal como lo muestra la figura 4.18. La ‘Option 1’ nos obliga que para incluir el dispositivo a la red Z-Wave debemos acercar el dispositivo al VERA3 con la finalidad de dejarlo en su lugar. La ‘Option 2’ que está debajo de la ‘Option 1’, tal como lo muestra la figura 4.17, nos obliga a acercar el VERA3 al dispositivo a incluir en la red Z-Wave. Una vez escogida la ‘Option 1’ se presiona el botón de inclusión del sensor tal como lo muestra la figura 4.20 [26]. Una vez presionado el botón de inclusión, en el cuadro de notificaciones aparece el mensaje ‘Unit busy’ tal como lo muestra la figura 4.19. Luego aparece el nuevo dispositivo agregado a la red Z-Wave, tal como lo muestra la figura 4.21.

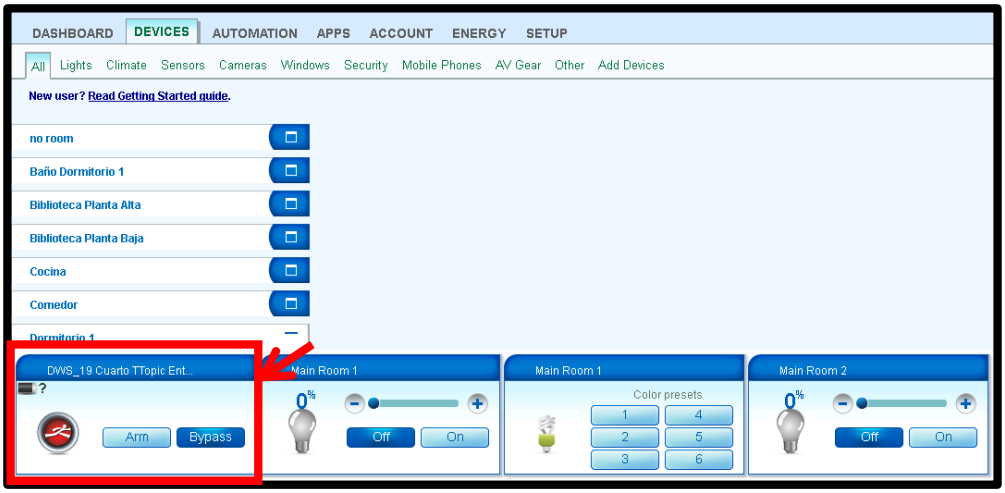


Figura 4.21: Sensor de puerta agregado a la red Z-Wave.

El nombre de todos y cada uno de los dispositivos que serán agregados a la red Z-Wave en el VERA3, estarán regidos bajo el siguiente formato, ***"<identificador de dispositivo y número de dispositivo en general> <Sector y número de dispositivo en el sector> <descripción (opcional)>"***. En secciones más adelante se detallará el identificador respectivo de cada dispositivo.

Finalmente, vale recordar que a cada dispositivo toca agregarlo a su 'Room' correspondiente tal como lo muestra la siguiente figura y donde tomamos como ejemplo a un actuador de persianas ubicado en la biblioteca planta alta.

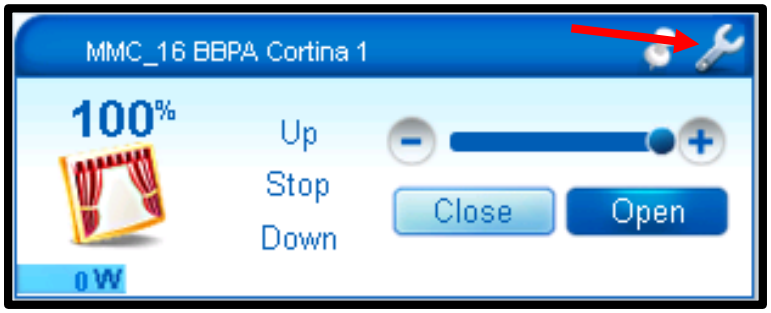


Figura 4.22: Opción que muestra el panel de configuración de cada dispositivo.

La figura anterior muestra la opción que permite visualizar el panel de configuración de cada dispositivo que tiene un símbolo parecido al de una herramienta para tuercas.

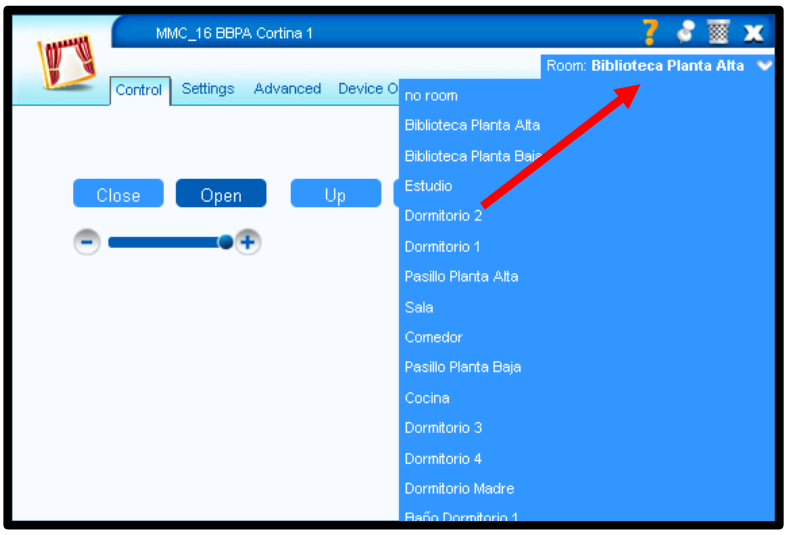


Figura 4.23: Selección del Room al cual pertenece el dispositivo.

Una vez seleccionada la herramienta de tuercas, nos aparece el panel de configuración del dispositivo y en nuestro caso seleccionamos

‘Biblioteca Planta Alta’. Para guardar esta configuración se debe presionar el botón ‘Save’ que aparece en la esquina superior derecha de la interfaz de usuario del VERA3.

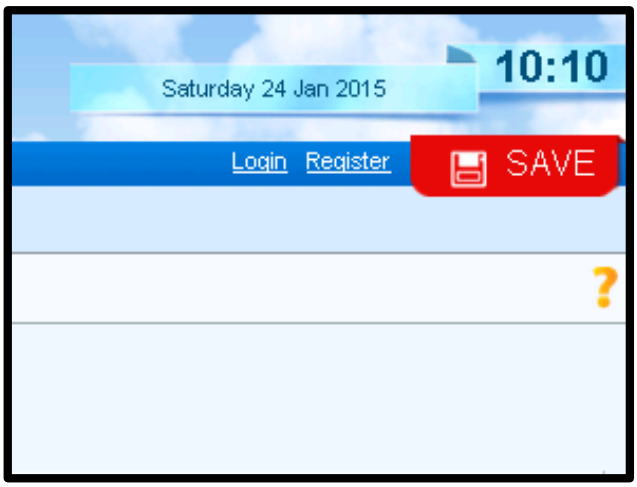


Figura 4.24: Opción ‘Save’ de la interfaz de usuario del VERA3.

Este procedimiento se lo debe realizar a cada dispositivo que se incluya en cada VERA3.

4.2. Diseño del networking.

En esta sección se detallan los equipos y los elementos de distribución y protección, así como los medios de transmisión que se necesitan para implementar el networking dentro de la vivienda. Parte de esta sección es el plan de distribución IPv4 en la cual se hace “subnetting” de redes para así asignar subredes a los distintos tipos de dispositivos de la vivienda y otros que se colocarán a futuro. Finalmente, se

describe el diseño de conexión de los equipos de red mediante un diagrama realizado en el software propietario Microsoft Visio.

4.2.1. Equipos.

4.2.1.1. Equipos de red.

Los equipos de red utilizados en este proyecto son descritos a continuación:

Router Cisco 1941 Series

Figura 4.25: Router Cisco 1941 Series.

Función

La figura anterior muestra al router cisco 1941 series [28]. Equipo que crea redes y asigna IP´s a los equipos que se conecten a las mismas si es que el servicio de DHCP es habilitado en dicho equipo, caso contrario se puede asignar de manera estática una IP a estos dispositivos para que pertenezcan a tales redes [27]. Tiene disponible conexiones LAN y WAN que pueden ser configuradas mediante tarjetas de interface intercambiable y módulos de servicios internos. Este equipo tiene el certificado WIFI y es compatible con 802.11a/b/g/n. El diseño interno de este equipo provee flexibilidad, permitiéndonos configurar nuestro router de acuerdo a nuestras necesidades. Las especificaciones se muestran a continuación [27].

Especificaciones

- Dimensiones (AlxAnxP): 4.4 cm x 34.3 cm x 29.2 cm
- Peso: 14 libras

- Voltaje de entrada: 100 a 240 VAC @ 60 Hz
- Corriente de entrada: 1.5 a 0.6 Amperios
- Potencia de consumo máximo: 80 W
- 1 puerto de consola conector RJ-45
- 1 puerto de consola mini USB tipo B versión 2.0
- 1 puerto auxiliar RJ-45
- 2 puertos USB tipo A versión 2.0
- 2 puertos Gigabit Ethernet 10/100/1000 RJ-45
- Memoria DRAM: 512 MB
- Memoria flash: 256 MB

Switch Cisco Catalyst WS-C2960S-48FPD-L

Figura 4.26: Switch Cisco Catalyst WS-C2960S-48FPD-L.

Función

La figura anterior muestra al switch cisco catalyst WS-C2960S-48FPD-L [30]. Un conmutador o switch es un

dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI [31]. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Las especificaciones se muestran a continuación [29].

Especificaciones

- Dimensiones (AlxAnxP): 4.5 cm x 44.5 cm x 38.6 cm
- Peso: 13 libras
- Voltaje de entrada: 100 a 240 VAC @ 60 Hz
- Corriente de entrada: 9 a 4 Amperios
- Hasta 870W dedicados a los puertos Power Over Ethernet
- 48 puertos Gigabit Ethernet de 10/100/1000 Mbps
- 2 interfaces Uplink para conexión a redes grandes SFP+
- 1G Small Form-Factor Pluggable o 1G/10G SFP+ slots

- Hasta 15.4W de Power Over Ethernet (PoE) cuando se lo utiliza en los 48 puertos Gigabit Ethernet
- Memoria Flash: 64 MB
- Memoria DRAM: 128 MB

Fortigate 80C

Figura 4.27: Fortigate 80C.

Función

La figura anterior muestra al fortigate 80C [33]. El Fortigate 80C, es un dispositivo ideal para pequeñas empresas, redes minoristas, hogares entre otros [32]. Este dispositivo ofrece la seguridad de la red, la conectividad y el rendimiento que se necesita en un solo dispositivo. Provee una protección avanzada contra amenazas, incluyendo firewall, control de aplicaciones, protección avanzada contra amenazas,

IPS, VPN y filtrado web. Es también una gran opción para asegurar los dispositivos móviles en entornos “Bring Your Own Device” con identificación automática de dispositivos y el acceso personalizable con políticas de seguridad. Las especificaciones se muestran a continuación [32].

Especificaciones

- Dimensiones(AlxAnxP): 4.45cm x 27.61cm x 15.57cm
- Peso: 3.3 libras
- Voltaje de entrada: 100 a 240 VAC @ 60 Hz
- Consumo de potencia(promedio/máximo): 25/30 W
- 2 10/100/1000 Interfaces WAN RJ-45
- 6 interfaces 10/100 de Conmutación Interna RJ-45
- 1 interfaz 10/100 DMZ RJ-45
- 1 interfaz de gestión de consola RJ-45
- 2 interfaces USB
- 1 slot para ExpressCard
- 1900/700/120 Mbps de rendimiento del firewall
- Hasta 1 millón de sesiones TCP
- 350 Mbps de rendimiento de IPS

- 140 Mbps de rendimiento IPSec VPN
- 70 Mbps de rendimiento SSL-VPN

ZONEDIRECTOR 1100

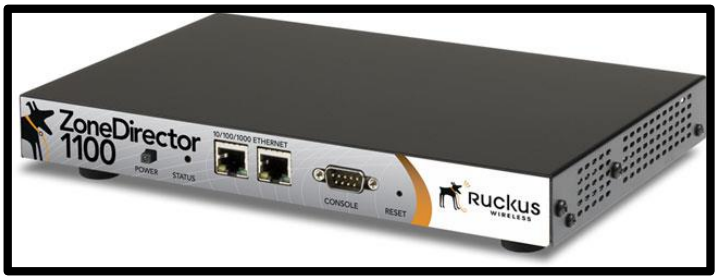


Figura 4.28: Ruckus Wireless ZoneDirector 1100.

Función

El Ruckus Wireless ZoneDirector 1100 [35] es el sistema de Ruckus de gestión centralizada de LAN inalámbrica inteligente desarrollada específicamente para las pequeñas y medianas empresas y usuarios de las zonas Wi-Fi [34]. Integra el motor de aplicación y sistema operativo inteligente de Ruckus que ofrece funciones avanzadas tales como mesh inalámbrico e inteligente, alta disponibilidad, autenticación de punto de Wi-Fi, networking de invitados y seguridad de Wi-Fi dinámico. Se integra fácilmente con la red, la

seguridad y la infraestructura de autenticación que ya están se configura fácilmente mediante un asistente basado en una aplicación Web. Los puntos de acceso Ruckus ZoneFlex son automáticamente descubiertos y son configurados por el ZoneDirector. Las especificaciones se muestran a continuación [34].

Especificaciones

- Dimensiones(AlxAnxP): 3.86cm x 15.93cm x 25cm
- Peso: 2.2 libras
- Voltaje de entrada: 12 VDC
- Corriente de entrada: 1 Amperio
- 2 puertos de 10/100/1000 Mbps con conector RJ-45
- Estándares de seguridad: WPA, WPA2, 802.11i
- Encriptación de seguridad: WEP, TKIP, AES y Ruckus Dynamic Pre-Shared Key
- Puede manejar hasta 50 puntos de acceso inalámbricos Ruckus
- Puede manejar hasta 128 SSID's.
- Maneja los protocolos de capa 3 IPv4 e IPv6
- Método de autenticación: RADIUS

ACCESS POINT RUCKUS ZONEFLEX 7363

Figura 4.29: Ruckus Wireless ZoneFlex 7363.

Función

El ZoneFlex 7363 [37] es un producto de doble banda. La capacidad máxima 802.11n hace que el ZoneFlex 7363 uno de los costos más bajos de la industria, la más alta línea de rendimiento del estándar 802.11n en puntos de acceso de medio alcance [36]. Tiene un diseño estéticamente agradable que es ideal para una variedad de entornos empresariales y puntos de acceso Wi-Fi incluyendo hoteles, escuelas, tiendas, oficinas, lugares públicos y viviendas. Su función es proveer señal de Wi-Fi en todas las áreas de la vivienda para poder acceder a la red interna privada

de la vivienda y también poder conectarse al internet. Las especificaciones se muestran a continuación [36].

Especificaciones

- Dimensiones(AlxAnxP): 3.6cm x 17.8cm x 17.8cm
- Peso: 0.875 libras
- Voltaje de entrada: 12 VDC
- Corriente de entrada: 1.5 Amperios
- Consumo de potencia: 12.95 W
- Antena de hasta 3 dBi para los 2.4 y 5 GHz
- Mitigación de interferencia: hasta 10 dB
- 1 puerto PoE 10/100/1000 Mbps con conector RJ-45
- 2 puertos 10/100 Mbps con conector RJ-45
- Hasta 256 clientes de Wi-Fi por SSID
- Hasta 32 SSID’s
- Puede ser manejado individualmente, a través del ZoneDirector o el FlexMaster
- La configuración puede ser por interface de usuario Web, SNMP mediante ZoneDirector, TR-069 mediante FlexMaster y línea de comandos de telnet y SSH HTTPS/S

- Estándares: 802.11a/b/g/n, 2.4 GHz y 5 GHz
- Canales de operación: de 1 a 11 Estados Unidos y Canadá, de 1 a 13 en Europa, de 1 a 13 en Japón.
- Seguridad de Wireless: WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i, autenticación 802.1X con el ZoneDirector.

ACCESS POINT RUCKUS ZONEFLEX 7025

Figura 4.30: Ruckus Wireless ZoneFlex 7025.

Función

El Ruckus ZoneFlex 7025 [39] es el primer switch de pared por cable e inalámbrico que integra 802.11n de

Wi-Fi de alta velocidad en un diseño elegante que puede ser instalado de forma rápida. Ideal para ofrecer servicios dentro de habitaciones y dormitorios universitarios [38]. El ZoneFlex 7025 ofrece la banda de 2.4 GHz con el estándar 802.11n de alto rendimiento y cuatro puertos RJ-45 para conexiones de LAN cableada. Se puede implementar como un dispositivo autónomo o de forma centralizada a través del Ruckus ZoneDirector. Tiene la capacidad de transmitir hasta ocho SSID y tiene las opciones de autenticación que incluyen, el estándar 802.1x basado en MAC, LDAP, RADIUS, Active Directory y por medio de una base de datos de usuario interna. Las especificaciones se muestran a continuación [38].

Especificaciones

- Dimensiones(AlxAnxP): 3.6cm x 8.5cm x 12.8cm
- Peso: 140 gramos
- Voltaje de entrada: 48 VDC o alimentación por PoE
- Consumo de potencia: 23 W con consumo de PoEy 7 W sin consumo de PoE

- 4 puertos RJ-45 de 10/100 Mbps
- El puerto RJ-45 número 4 acepta alimentación por PoE
- 1 puerto RJ-45 de 10/100 Mbps que se conecta a redes externas
- IPv4 e IPv6 como protocolos de capa 3 según el modelo OSI
- Puede ser manejado individualmente, a través del ZoneDirector o el FlexMaster
- La configuración puede ser por interface de usuario Web, SNMP mediante ZoneDirector, TR-069 mediante FlexMaster y línea de comandos de telnet y SSH HTTPS/S
- Estándares: 802.11b/g/n a 2.4 GHz
- Canales de operación: de 1 a 11 Estados Unidos y Canadá, de 1 a 13 en Europa
- Seguridad de Wireless: WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i, autenticación 802.1X con el ZoneDirector
- Hasta 100 clientes de Wi-Fi por SSID
- Hasta 8 SSID’s

4.2.1.2. Elementos de distribución y protección.

ARMARIO DE RACK

Figura 4.31: Rack.

Un rack [41] es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones [40]. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, cabinets o armarios.

Los racks se dividen en regiones de 1,75 pulgadas de altura (44,45mm). En cada región hay tres agujeros que siguen un orden simétrico. Esta región es la que se denomina altura o U. Cada columna tiene agujeros a intervalos regulares llamados unidad rack (U) agrupados de tres en tres. Verticalmente, la altura de los racks está normalizada y lo común es que existan desde 4U de altura hasta 46/47U de altura.

Es decir que un rack de 41U o 42U por ejemplo nunca puede superar los 2000 mm de altura externa. Con esto se consigue que en una sala los racks tengan dimensiones prácticamente similares aun siendo de diferentes fabricantes.

Las alturas disponibles normalmente según normativa serían 800, 1000, 1200, 1400, 1600, 1800, 2000 y 2200 mm.

La profundidad del bastidor no está normalizada, ya que así se otorga cierta flexibilidad al equipamiento [40]. No obstante, suele ser de 600, 800, 900, 1000 incluso 1200 milímetros.

En nuestra vivienda existirán 3 armarios de rack de 42U. Con este tipo de armarios se pueden colocar todos nuestros equipos de red y equipos que se colocarán en el futuro.

PATCH PANEL o PANEL DE CONEXIONES

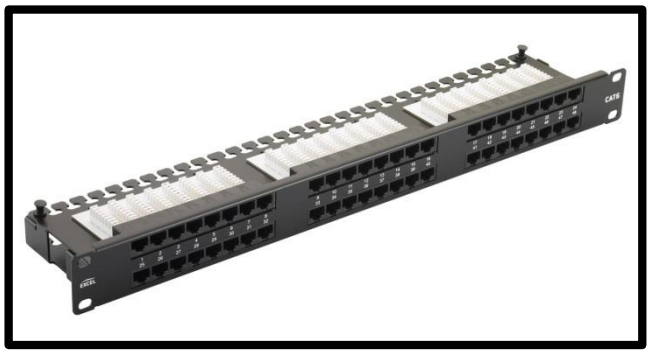


Figura 4.32: Patch Panel o Panel de conexiones.

Un panel de conexiones [43], también denominado bahía de rutas o patch panel, es el elemento encargado de recibir todos los cables del cableado estructurado [42]. Sirve como un organizador de las conexiones de la red, para que los elementos relacionados de la Red LAN y los equipos de la conectividad puedan ser fácilmente incorporados al sistema y además los puertos de conexión de los equipos activos de la red (Switch, Router, etc.) no

tengan algún daño por el constante trabajo de retirar e introducir en sus puertos. Para la realización de este proyecto usaremos 8 patch panel de categoría cat 6a que permitirán conectar a todos nuestros dispositivos y dispositivos que se conecten en el futuro.

ORGANIZADORES VERTICALES

Los organizadores verticales [44] permiten como su nombre lo indica organizar los cables de las conexiones físicas de equipos de red de manera vertical en el perímetro del rack. En nuestro proyecto usaremos dos organizadores verticales por cada armario de rack.

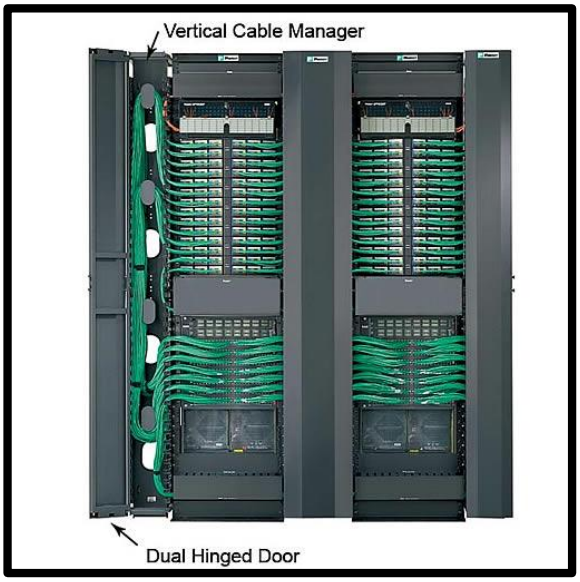


Figura 4.33: Organizador Vertical.

ORGANIZADORES HORIZONTALES

Los organizadores horizontales [45] permiten como su nombre lo indica organizar los cables de las conexiones físicas de equipos de red de manera horizontal dentro de las inmediaciones del rack. En nuestro proyecto usaremos un organizador horizontal por cada armario de rack.

Figura 4.34: Organizador Horizontal.

BANDEJA DE CABLES

Figura 4.35: Bandejas de Cables.

En la figura anterior se muestra las bandejas de cables [47]. En el cableado eléctrico de los edificios, un sistema de bandeja de cables se utiliza para alojar cables eléctricos aislados utilizados para la distribución de energía y comunicación [46]. Las bandejas de cables se utilizan como una alternativa a los sistemas abiertos de cables o conductos eléctricos, y se utilizan comúnmente para la administración de cables en la construcción comercial e industrial, aunque muy pocas veces en viviendas. Son especialmente útiles en situaciones en las que se prevén cambios en un sistema de cableado, ya que los nuevos cables se pueden instalar alojados en la bandeja, en lugar de tirar de ellos a través de una tubería.

FACEPLATES

Figura 4.36: Faceplates híbridos de Cobre y Fibra.

En la figura anterior se muestran los faceplates híbridos de cobre y fibra [49]. Son usados en edificios comerciales, industriales y viviendas para conectar cables de comunicación hacia un conmutador o switch. Están hechos para trabajar con muchos diferentes tipos de soluciones de cableado, incluidos los coaxiales, de par trenzado, HDMI, fibra óptica, etc. Los colores más comunes son de color beige y blanco [48]. Están hechos para que resulten compatibles con aberturas y cajas estándar NEMA. Los que se usan en este proyecto vienen con los 2 jacks RJ-45 tipo hembra.

TUBERÍA METÁLICA EMT

Figura 4.37: Tubería metálica de EMT.

En la figura anterior se muestra tubería metálica de EMT [51]. A veces llamado de pared delgada, se utiliza comúnmente en lugar de un conducto rígido galvanizado (GRC), ya que es menos costoso y más ligero que el GRC [50]. EMT en sí no está enroscado en sus extremos pero se puede usar con accesorios roscados que se sujeten a la misma. Los conductos están conectados entre sí y a los equipos con abrazaderas. EMT es más común en los edificios comerciales e industriales que en aplicaciones residenciales, pero no se excluye su uso. EMT se hace generalmente de acero revestido, aunque puede ser de aluminio.

TUBERÍA NO METÁLICA DE PVC

Figura 4.38: Tubería no metálica de PVC.

La tubería de PVC [53] es la más ligera en peso comparada con otros materiales de conducto, y por lo general más económicos que otros tipos de conducto. En la práctica, en América, está disponible en tres diferentes espesores de pared. La mayor parte de los diversos accesorios hechos para conducto de metal también están disponibles en forma de PVC. El material plástico resiste la humedad y muchas sustancias corrosivas, pero desde que el conducto es no conductivo, un conductor de unión adicional (conexión a tierra) debe ser jalado dentro de cada conducto. El conducto de PVC puede ser calentado y doblado en el campo, usando herramientas de calentamiento especial diseñadas para ese propósito [52].

4.2.2. Medios de transmisión.

4.2.2.1. Cable STP de cobre cat 6a.

Figura 4.39: Cable STP de cobre cat 6a.

La figura anterior muestra un cable STP de cobre cat 6a [55]. La TIA aprobó una nueva especificación estándar de rendimiento mejorados para sistemas con cables trenzados no blindado (unshielded). y cables trenzados blindados (Foiled). La especificación ANSI/TIA/EIA-568-B.2-10 indica sistemas de cables llamados Categoría 6 Aumentada o más frecuentemente "Categoría 6a", que operan a frecuencias de hasta 500 MHz (tanto para cables no blindados como cables blindados) y proveen transferencias de hasta 10 Gbit/s (10GBASE-T). La nueva especificación mitiga los efectos de

la diafonía o crosstalk. Soporta una distancia máxima de 100 metros. En el cable blindado la diafonía externa (crosstalk) es virtualmente cero [54].

En la realización de este proyecto usamos el cable cat 6a para dar conectividad a internet y a las subredes privadas internas de la vivienda. Un extremo de este cable va conectado al patch panel que se ubica en el rack y el otro extremo se lo poncha con un conector RJ-45 hembra dedicado para el cable cat 6a [54]. La siguiente figura muestra un conector hembra RJ-45 cat 6a [56].

Figura 4.40: Conector RJ-45 hembra para cable cat 6a.

4.2.2.2. Fibra Óptica.

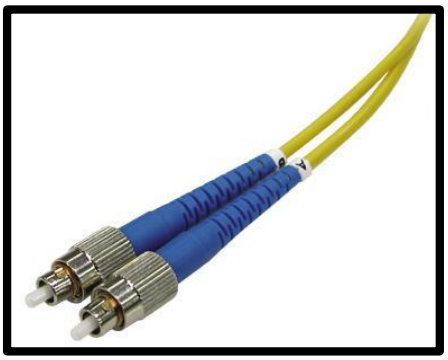


Figura 4.41: Fibra Óptica de tipo monomodo.

La fibra óptica [58] es un medio de transmisión, empleado habitualmente en redes de datos, consistente en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un led [57].

Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el

diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gbit/s). El tipo de fibra que usaremos es “SM2C g657a1”. La fibra a la que hacemos mención, es dos hilos de colores azul y anaranjado (Single Mode 2 Colors) con un radio mínimo de curvatura de hasta 30 mm [57].

Vale destacar, que la fibra óptica no se la usa en nuestro sistema domótico pero se decidió dejar el tendido de fibra en toda la vivienda para su uso futuro y cuando los dispositivos domóticos puedan comunicarse usando este medio de transmisión [57].

4.2.3. Plan de distribución IPv4.

El plan de distribución IPv4 nos permite dividir la red privada interna de la vivienda en varias subredes con la finalidad de que

cada tipo de dispositivo tenga su propia subred, dando una mejor organización y evitando posibles conflictos de direccionamiento IPv4. A continuación el plan de distribución IPv4:

HOME IP PLAN	Red IP	Mask	DHCP	VLAN	Switches	Puertos asignados a VLAN
Usuarios Wi-Fi	192.168.229.1	24	Yes	10		
Usuarios Red Ethernet Fija	192.168.230.1	24	No	11	1,2,3,4	4,5,6,7
Servidores y ZoneDirector	172.31.1.1	28	No	30	1,3	1,2,3
Switches	172.31.0.1	28	No	40	1*,2,3,4	46*, 47*, 48
Hue Controllers	172.16.0.1	24	No	50	1,2,3,4	8-12, 19 -47
Puntos de Acceso Inalámbricos	172.16.1.1	24	No	50	1	13 -18
Controladores VERA3 Z-Wave	172.16.2.1	24	No	50	1,2,3,4	8-12, 19 -47
Cámaras IP	172.16.5.1	24	No	50	1,2,3,4	8-12, 19 -47
Televisores IP	172.16.7.1	24	No	50	1,2,3,4	8-12, 19 -47
Otros dispositivos eventuales	172.16.16.1	24	No	50	1,2,3,4	8-12, 19 -47

Tabla 4.1: Plan de distribución IPv4 o Home IP Plan.

La columna “HOME IP PLAN” contiene el grupo de dispositivos a quienes se les asigna una subred.

La columna “Red IP” contiene el identificador de subred de cada grupo de dispositivos.

La columna “DHCP” indica si el servicio DHCP está habilitado para cada subred. Este servicio permite que un servidor DHCP asigne un direccionamiento IPv4 al dispositivo que busca ser parte de la red del servidor.

La columna “VLAN” indica a qué VLAN pertenece la subred.

La columna “Switches” indica en qué switches está configurada la subred.

La columna “Puertos asignados a VLAN” indica cuales puertos de los switches de la columna “Switches” están configurados con la VLAN de la subred.

* Solamente en el switch 1 se utilizan los puertos 46 y 47 para la VLAN de los switches. Esto para poder habilitar la conexión en cascada que se explicará más adelante.

4.2.4. Diseño de conexión de los equipos de red.

En esta sección se muestra el diseño de las conexiones a nivel de hardware y a nivel de software de los equipos de red. Las conexiones a nivel de hardware implican conectar los equipos con patch cords o cables de red por medio de interfaces Ethernet. Las conexiones a nivel de software implican configuraciones en el sistema operativo de los equipos de red para que puedan intercambiar información entre ellos.

CONEXIONES A NIVEL DE HARDWARE

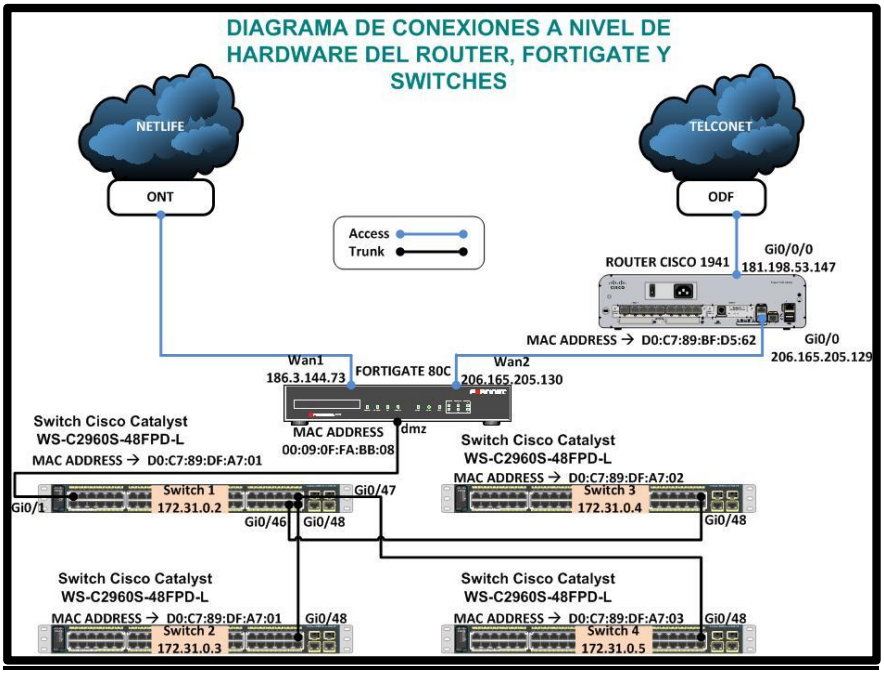


Figura 4.42: Diagrama de conexiones a nivel de hardware del router, fortigate y switches.

La figura anterior muestra que el internet se conecta a la red privada interna de la vivienda a través de dos proveedores: Netlife y Telconet. Las conexiones Access se diferencias de las Trunk, en que, por las conexiones Access solo transita una sola VLAN y por las conexiones Trunk transitan varias VLAN.

El internet proveniente de Netlife llega desde un OLT (Optical Line Termination), un dispositivo que sirve como el proveedor de servicios de punto final de una red óptica pasiva por medio

de una fibra óptica monomodo a un ONT (Optical Network Termination), el cual es un equipo que convierte la señal óptica de la luz de la fibra a señales eléctricas que se transmiten por medio de un patch cord cat 6a hasta el puerto WAN1 del fortigate 80C.

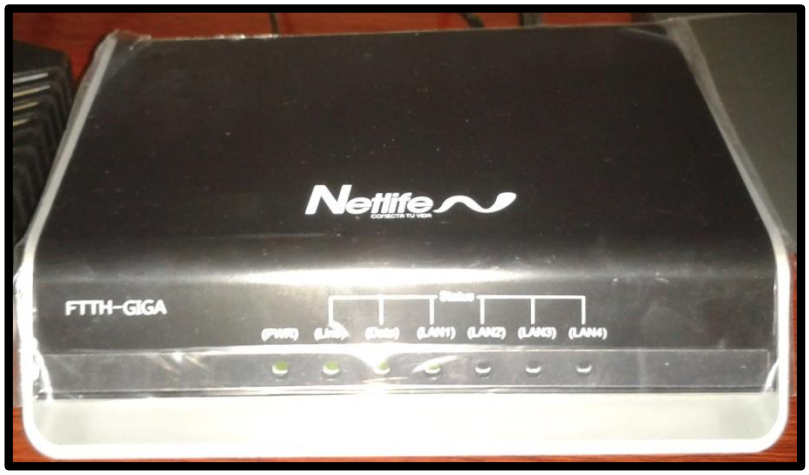


Figura 4.43: ONT de la empresa Netlife.

El internet proveniente de Telconet llega desde un switch en un nodo de la misma empresa por medio de fibra óptica monomodo hacia un ODF (Organizador de Fibra) el cual comunica la fibra con la interface Gigabit Ethernet 0/0/0 de fibra óptica del router cisco 1941. Posteriormente el router se conecta con un patch cord cat 6a al fortigate 80C a la interfaz WAN2 desde la interfaz Gigabit Ethernet 0/0. Cabe mencionar que este router hará las veces de un router “front-end”, es decir

que es el router que se comunica con otras redes públicas WAN.

El fortigate 80C es un UTM (Unified Threat Management) que tiene funcionalidades y que hará las veces de router en la red privada interna. Desde la interfaz DMZ (Demilitarized Zone) del fortigate 80C y a través de un patch cord cat 6a se conecta a la interfaz Gigabit Ethernet 0/1 del “Switch 1”. Este switch reparte la comunicación desde su interfaz Gigabit Ethernet 0/48 hacia la interfaz Gigabit Ethernet 0/48 del “Switch 2”; así también reparte la comunicación desde su interfaz Gigabit Ethernet 0/46 hacia la interfaz Gigabit Ethernet 0/48 del “Switch 3” y por último reparte la comunicación desde su interfaz Gigabit Ethernet 0/47 hacia la interfaz Gigabit Ethernet 0/48 del “Switch 4”.

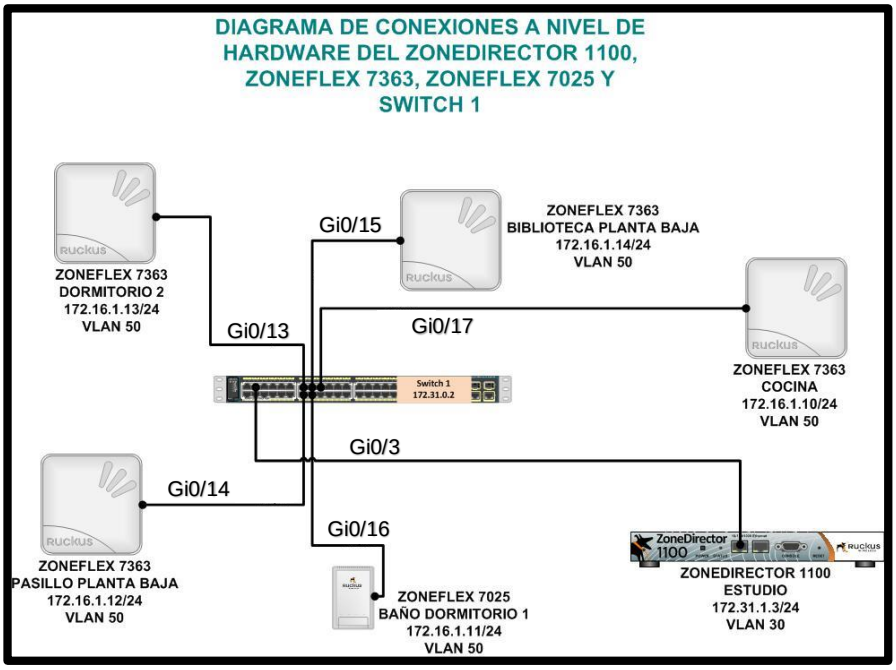


Figura 4.44: Diagrama de conexiones a nivel de hardware del zonedirector 1100, zoneflex 7363, zoneflex 7025 y switch 1.

La figura anterior muestra el diagrama de conexiones a nivel de hardware de los equipos de red inalámbricos, cada equipo con su respectiva IP, VLAN, sector de la vivienda donde se encuentra ubicado y la interfaz del “Switch 1” a la que se encuentra conectado (desde Gigabit Ethernet 13 hasta la Gigabit Ethernet 18) a través de un patch cord cat 6a.

Vale recalcar que el ZoneDirector 1100 permite configurar los puntos de acceso ZoneFlex tanto los 7363 como el 7025 a través de una interface web y muy amigable con el usuario. Con la colocación de estos equipos especialmente los puntos de

acceso ZoneFlex se busca dar cobertura de Wi-Fi a todas las áreas de la vivienda y van colocados en puntos estratégicos de la vivienda. Para colocarlos no se necesita ninguna técnica en especial, solamente ir colocando uno a uno de manera central en ciertas áreas y al final testear la intensidad de la señal en todas las áreas de la vivienda con un dispositivo cualquiera que pueda conectarse a una red Wi-Fi. Esto se debe al gran alcance que proveen los puntos de acceso ZoneFlex. El ZoneDirector es conectado en el puerto 3 del switch 1, haciendo que se encuentre en la misma VLAN que los ‘Servidores’ (VLAN 30), solo para motivos de seguridad, restringiendo la posibilidad de solo hacerle ping. Estas restricciones se ven más adelante en la tabla 4.2.

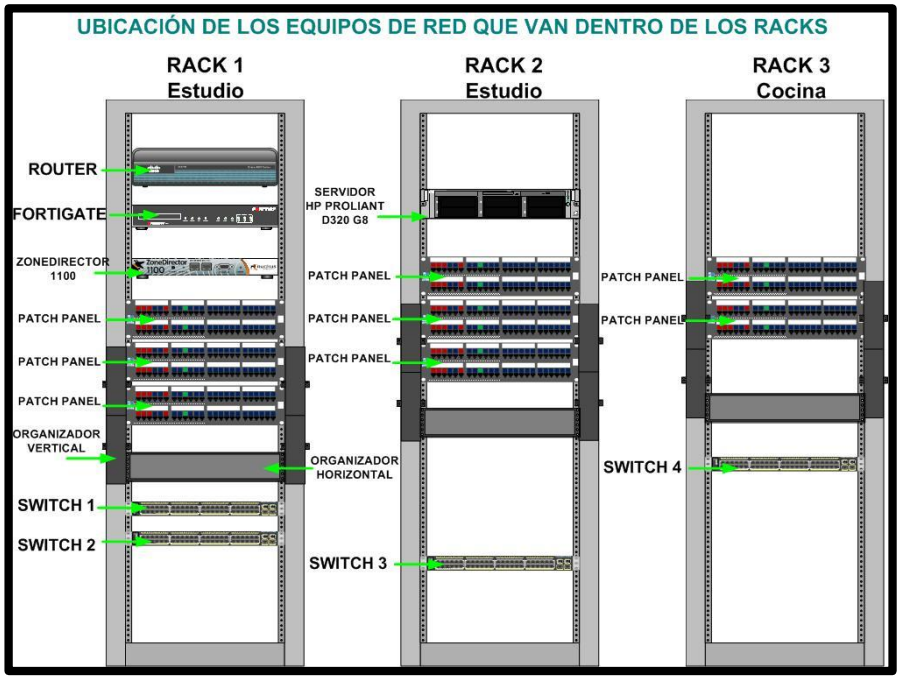


Figura 4.45: Ubicación de los equipos de red que van dentro de los Racks.

Tal como se muestra en la figura anterior se colocarán 3 racks dentro de la vivienda y cada uno con sus respectivos equipos. Los dos primeros racks se colocarán en el estudio y el tercero en la cocina. El servidor HP PROLIANT D320 G8, sirve para guardar los videos que constantemente están guardando las cámaras, se explicará su uso más adelante.

CONEXIONES A NIVEL DE SOFTWARE

Configuración del Router y del Fortigate 80C

Tenemos dos entradas de internet provenientes de las empresas Netlife y Telconet. El internet de Netlife nos provee un ancho de banda de 100 Mbps a través de la WAN1. El internet de Telconet nos provee un ancho de banda de 100 Mbps a través de la WAN2. La red interna de la vivienda tiene como internet principal el de Netlife. En caso de que el consumo de internet de la red alcance el ancho de banda total de Netlife, se realiza el proceso de “spillover”, es decir cuando se requiera más ancho de banda del provisto por Netlife se usa el ancho de banda de Telconet. Este proceso de spillover es realizado por el fortigate 80C. Así también existen subredes dentro de la red privada interna de la vivienda que son parte de VLAN’s, tal como se mostró en la tabla 4.1 y que a su vez son protegidas por el fortigate 80C.

En la interfaz Gigabit Ethernet 0/0/0 del router, se asigna el siguiente direccionamiento para poder estar dentro de la VLAN que establece el switch de la empresa Telconet que está detrás del router.

- Dirección IP → 181.198.53.147
- Máscara de Subred → 255.255.255.0
- Gateway → 181.198.53.1

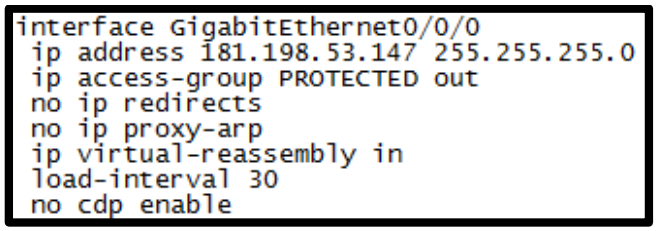


Figura 4.46: Configuración de Interface Gigabit Ethernet 0/0/0 en el Router.

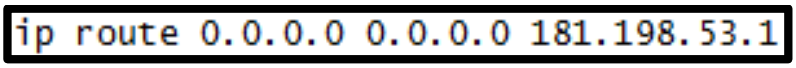


Figura 4.47: Configuración de gateway Gigabit Ethernet 0/0/0 en el Router.

A continuación la explicación de la configuración en la figura 4.46. La opción “ip address” configura la dirección ip y la máscara de la interface Gigabit Ethernet 0/0/0. La opción “ip access-group out” permite establecer listas de acceso del grupo “PROTECTED” de paquetes que pueden salir de dicha interfaz del router. Para que los paquetes entren al grupo de acceso “PROTECTED” deben seguir ciertas reglas que se establecen en el archivo de configuración del router. La opción “no ip redirects” evita que el router envíe mensajes de redirección a los clientes para evitar la saturación de la red. La opción “no ip

proxy-arp” se la suele configurar en el puerto en el que se conecta a la internet como buena práctica de configuración y así se evitar responder peticiones ARP de una máquina remota. La opción “ip virtual-reassembly in” permite reconstruir paquetes que se dirigen hacia el router y se pierden en el camino para que se vuelvan a enviar. La opción “load interval 30” permite al router saber cuanto tráfico pasa por esta interface del router en 30 segundos, esto sirve para cuestiones estadísticas. La opción “no cdp enable” deshabilita el protocolo CDP (Cisco Discovery Protocol) de capa 2 que permite descubrir otros equipos Cisco en la red y así evitar la saturación de la red.

En la figura 4.40 se muestra la opción “ip route” que permite establecer la puerta de enlace de la red en este caso 181.198.53.1, los valores 0.0.0.0 permiten establecer a la puerta de enlace anterior como una puerta de enlace de último recurso.

En la interfaz WAN1 del fortigate se asigna el siguiente direccionamiento para poder estar dentro de la red que establece el OLT:

- Dirección IP → 186.3.144.73
- Máscara de Subred → 255.255.255.224
- Gateway → 186.3.144.65

En la interfaz WAN2 del fortigate se asigna el siguiente direccionamiento para poder estar dentro de la red que establece el router:

- Dirección IP → 206.165.205.130
- Máscara de Subred → 255.255.255.248
- Gateway → 206.165.205.129

```
config system interface
    edit "wan1"
        set vdom "PROTECTED"
        set ip 186.3.144.73 255.255.255.224
        set allowaccess ping https
        set type physical
        set spillover-threshold 100000
        set alias "Wan_Netlife"
        set snmp-index 1
    next
    edit "wan2"
        set vdom "PROTECTED"
        set ip 206.165.205.130 255.255.255.248
        set allowaccess ping https
        set type physical
        set spillover-threshold 100000
        set alias "Wan_Telconet"
        set snmp-index 2
    next
```

Figura 4.48: Configuración “system interface” en el Fortigate.

La configuración “system interface” nos permite definir el direccionamiento IPv4 de las interfaces WAN de nuestro fortigate.

Existen opciones comunes tanto para la ‘wan1’ como para la ‘wan2’. La opción “set allowaccess” permite establecer los servicios disponibles para estas interfaces, en ambos casos el servicio de ‘ping’ y el servicio ‘https’. El fortigate puede virtualmente dividirse en varios fortigates es por esto que cuando usamos la opción “set vdom”, agregamos las interfaces ‘wan1’ y ‘wan2’ al fortigate virtual con nombre ‘protected’. La opción “set type physical” define que los puertos asociados a las interfaces ‘wan’ sean puertos físicos de red. La opción “set spillover-treshold” define el ancho de banda del proceso spillover que en ambos casos es de 100 Mbps. El proceso de spillover permite consumir el ancho de banda de la ‘wan1’ y cuando se sature se consume el ancho de banda de la ‘wan2’. La opción “set alias” permite asignar un nombre a las interfaces ‘wan’. Para la ‘wan1’ el nombre es ‘Wan_Netlife’ y para la ‘wan2’ el nombre es ‘Wan_Telconet’. La opción “snmp-index” establece un identificador a cada interfaz que usa el protocolo SNMP (Simple Network Management Protocol). La opción “set ip

xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx" establece el direccionamiento IPv4 en la interfaz.

```
interface GigabitEthernet0/0
 description LAN-FGT80C
 ip address 206.165.205.129 255.255.255.248 secondary
 ip address 181.198.70.153 255.255.255.248
 no ip redirects
 no ip proxy-arp
 ip virtual-reassembly in
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
```

Figura 4.49: Configuración de la interfaz Gigabit Ethernet 0/0 del router.

La figura anterior muestra la configuración de la interfaz Gigabit Ethernet 0/0 en el router. La opción "description" permite establecer un comentario sobre la LAN conectada en esa interfaz en este caso 'LAN-FGT80C'. La opción "ip address 206.165.205.129 255.255.255.248 secondary" establece el direccionamiento IPv4 en esta interfaz de manera secundaria. La opción "no ip redirects" evita que el router envíe mensajes de redirección a los clientes para evitar la saturación de la red. La opción "no ip proxy-arp" se la suele configurar en el puerto en el que se conecta a la internet como buena práctica de configuración y así se evitar responder peticiones ARP de una máquina remota. La opción "ip virtual-reassembly in" permite reconstruir paquetes que se dirigen hacia el router y se pierden

en el camino para que se vuelvan a enviar. La opción “load interval 30” permite al router saber cuánto tráfico pasa por esta interface del router en 30 segundos, esto sirve para cuestiones estadísticas. La opción “duplex auto” detecta automáticamente si la comunicación es half o full dúplex. La opción “speed auto” detecta automáticamente la velocidad de comunicación. La opción “no cdp enable” deshabilita el protocolo CDP (Cisco Discovery Protocol) de capa 2 que permite descubrir otros equipos Cisco en la red y así evitar la saturación de la red.

Una vez configuradas las conexiones a nivel de software desde el fortigate y router hacia la internet, debemos hacer las respectivas conexiones desde el fortigate hacia la red privada interna que se traduce en crear y proteger a las VLAN’s en el fortigate y configurarlas a nivel de switches.

```
config system interface
    edit "Usuarios Wi-Fi"
        set vdom "PROTECTED"
        set ip 192.168.229.1 255.255.255.0
        set allowaccess ping https ssh
        set device-identification enable
        set snmp-index 12
        set interface "dmz"
        set vlanid 10
    next
    edit "Usuarios Red Ethernet Fija"
        set vdom "PROTECTED"
        set ip 192.168.230.1 255.255.255.0
        set allowaccess ping https ssh
        set device-identification enable
        set snmp-index 15
        set interface "dmz"
        set vlanid 11
    next
    edit "Servidores"
        set vdom "PROTECTED"
        set ip 172.31.1.1 255.255.255.240
        set allowaccess ping
        set device-identification enable
        set snmp-index 6
        set interface "dmz"
        set vlanid 30
    next
    edit "Switches"
        set vdom "PROTECTED"
        set ip 172.31.0.1 255.255.255.240
        set allowaccess ping
        set device-identification enable
        set snmp-index 13
        set interface "dmz"
        set vlanid 40
    next
    edit "Dispositivos"
        set vdom "PROTECTED"
        set ip 172.16.0.1 255.255.0.0
        set allowaccess ping https
        set device-identification enable
        set snmp-index 14
        set interface "dmz"
        set vlanid 50
    next
end
```

Figura 4.50: Configuración de las VLAN's de la red privada interna en el Fortigate.

Como se muestra en la figura anterior, se configuran las VLAN's en el fortigate con sus respectivas seguridades con el fin de evitar intrusiones de personas no deseadas. A todas las VLAN's se las agrega al mismo VDOM (Virtual Domain), "PROTECTED", el cual es una unidad virtual que funciona de manera independiente de otras VDOM's, con la opción "set vdom PROTECTED". Se les asigna sus direccionamientos IPv4 respectivos, con la opción "set ip xxx.xxx.xxx.xxx

xxx.xxx.xxx.xxx” según la tabla 4.1. Con la opción “set device-identification enable” se permite la inclusión de dispositivos detectados en los análisis de vulnerabilidades de red. Se asigna un identificador SNMP con la opción “set snmp-index #”. Se les asigna el puerto del Fortigate al cual se conectan, en este caso todos van al puerto DMZ con la opción “set interface dmz”. Se les asigna a sus respectivas VLAN’s a la cual pertenecen con la opción “set vlanid #”. Para el final he dejado la opción “set allowaccess” con la cual se permite que desde una red remota se haga 1) ping, 2) se acceda mediante https o 3) se ingrese por ssh a los equipos de dichas VLAN’s.

VLAN	SERVICIOS PERMITIDOS CON ALLOWACESS	DESCRIPCIÓN
Usuarios Wi-Fi	ping, https, ssh	Se les permite que sean descubiertos mediante los 3 servicios porque son dispositivos que constantemente interactúan con la internet.
Usuarios de Red Ethernet Fija	ping, https, ssh	Se les permite que sean descubiertos mediante los 3 servicios porque son dispositivos que constantemente interactúan con la internet.
Servidores	ping	Por motivos de seguridad, sólo se les podrá hacer ping para motivos de detección de los mismos en la red.
Switches	Ping	Por motivos de seguridad, sólo se les podrá hacer ping para motivos de detección de los mismos

		en la red.
Dispositivos	ping, https	No se les permite el servicio de ssh para evitar que nadie pueda acceder a configuraciones de manera remota. Se les habilita el servicio https ya que algunos de estos dispositivos, acceden a la internet.

Tabla 4.2: Descripción de servicios permitidos a las diferentes VLAN's.

Configuración de los Switches

La configuración de las VLAN's a nivel de switches se traduce en configurar los 48 puertos de cada switch para que pertenezcan a las diferentes VLAN's según la tabla 4.1. A continuación se muestran 4 tablas que resumen las configuraciones de cada puerto de cada switch.

PUERTO	CONFIGURACIÓN
1	interface GigabitEthernet1/0/1 switchport mode trunk
2	interface GigabitEthernet1/0/2 switchport access vlan 30
3	interface GigabitEthernet1/0/3 switchport access vlan 30
4	interface GigabitEthernet1/0/4 switchport access vlan 11
5	interface GigabitEthernet1/0/5 switchport access vlan 11
6	interface GigabitEthernet1/0/6 switchport access vlan 11

7	interface GigabitEthernet1/0/7 switchport access vlan 11
8	interface GigabitEthernet1/0/8 switchport access vlan 50
9	interface GigabitEthernet1/0/9 switchport access vlan 50
10	interface GigabitEthernet1/0/10 switchport access vlan 50
11	interface GigabitEthernet1/0/11 switchport access vlan 50
12	interface GigabitEthernet1/0/12 switchport access vlan 50
13	interface GigabitEthernet1/0/13 switchport trunk native vlan 50 switchport mode trunk
14	interface GigabitEthernet1/0/14 switchport trunk native vlan 50 switchport mode trunk
15	interface GigabitEthernet1/0/15 switchport trunk native vlan 50 switchport mode trunk
16	interface GigabitEthernet1/0/16 switchport trunk native vlan 50 switchport mode trunk
17	interface GigabitEthernet1/0/17 switchport trunk native vlan 50 switchport mode trunk
18	interface GigabitEthernet1/0/18 switchport trunk native vlan 50 switchport mode trunk
19	interface GigabitEthernet1/0/19 switchport access vlan 50
20	interface GigabitEthernet1/0/20 switchport access vlan 50
21	interface GigabitEthernet1/0/21 switchport access vlan 50
22	interface GigabitEthernet1/0/22 switchport access vlan 50
23	interface GigabitEthernet1/0/23 switchport access vlan 50
24	interface GigabitEthernet1/0/24 switchport access vlan 50

25	interface GigabitEthernet1/0/25 switchport access vlan 50
26	interface GigabitEthernet1/0/26 switchport access vlan 50
27	interface GigabitEthernet1/0/27 switchport access vlan 50
28	interface GigabitEthernet1/0/28 switchport access vlan 50
29	interface GigabitEthernet1/0/29 switchport access vlan 50
30	interface GigabitEthernet1/0/30 switchport access vlan 50
31	interface GigabitEthernet1/0/31 switchport access vlan 50
32	interface GigabitEthernet1/0/32 switchport access vlan 50
33	interface GigabitEthernet1/0/33 switchport access vlan 50
34	interface GigabitEthernet1/0/34 switchport access vlan 50
35	interface GigabitEthernet1/0/35 switchport access vlan 50
36	interface GigabitEthernet1/0/36 switchport access vlan 50
37	interface GigabitEthernet1/0/37 switchport access vlan 50
38	interface GigabitEthernet1/0/38 switchport access vlan 50
39	interface GigabitEthernet1/0/39 switchport access vlan 50
40	interface GigabitEthernet1/0/40 switchport access vlan 50
41	interface GigabitEthernet1/0/41 switchport access vlan 50
42	interface GigabitEthernet1/0/42 switchport access vlan 50
43	interface GigabitEthernet1/0/43 switchport access vlan 50
44	interface GigabitEthernet1/0/44 switchport access vlan 50
45	interface GigabitEthernet1/0/45 switchport access vlan 50

46	interface GigabitEthernet1/0/46 switchport trunk native vlan 40 switchport mode trunk
47	interface GigabitEthernet1/0/47 switchport trunk native vlan 40 switchport mode trunk
48	interface GigabitEthernet1/0/48 switchport trunk native vlan 40 switchport mode trunk

Tabla 4.3: Configuraciones de los 48 puertos Gigabit Ethernet del Switch 1.

El puerto 1, es usado como puerto troncal, ya que se conecta directamente al puerto DMZ del fortigate 80C, a través del comando “switchport mode trunk”. Desde el puerto 2 al puerto 12 y desde el puerto 19 al puerto 45, se usa el comando “switchport access vlan xx” con el cual establecemos la VLAN a la cual debe pertenecer cada puerto del switch. Desde el puerto 13 al puerto 18 se usa el comando “switchport trunk native vlan 50” que asigna la VLAN respectiva al puerto y el comando “switchport mode trunk” que los convierte en puertos troncales ya que por estos puertos, a más de estar la VLAN propia de los puntos de acceso inalámbrico (VLAN 50) estará la VLAN de los Usuarios Wi-Fi (VLAN 10). Desde el puerto 46 al puerto 48, se usa el comando “switchport trunk native vlan 40” que asigna la VLAN respectiva al puerto y el comando “switchport mode trunk” que los convierte en puertos troncales ya que por estos puertos,

a más de estar la VLAN propia de los switches (VLAN 40) estarán las VLAN's de toda la red privada interna. Cada puerto se configura a su respectiva VLAN según la Tabla 4.1.

PUERTO	CONFIGURACIÓN
1	interface GigabitEthernet1/0/1 switchport access vlan 30
2	interface GigabitEthernet1/0/2 switchport access vlan 30
3	interface GigabitEthernet1/0/3 switchport access vlan 30
4	interface GigabitEthernet1/0/4 switchport access vlan 11
5	interface GigabitEthernet1/0/5 switchport access vlan 11
6	interface GigabitEthernet1/0/6 switchport access vlan 11
7	interface GigabitEthernet1/0/7 switchport access vlan 11
8	interface GigabitEthernet1/0/8 switchport access vlan 50
9	interface GigabitEthernet1/0/9 switchport access vlan 50
10	interface GigabitEthernet1/0/10 switchport access vlan 50
11	interface GigabitEthernet1/0/11 switchport access vlan 50
12	interface GigabitEthernet1/0/12 switchport access vlan 50
13	interface GigabitEthernet1/0/13 switchport access vlan 50
14	interface GigabitEthernet1/0/14 switchport access vlan 50
15	interface GigabitEthernet1/0/15 switchport access vlan 50
16	interface GigabitEthernet1/0/16 switchport access vlan 50
17	interface GigabitEthernet1/0/17 switchport access vlan 50

18	interface GigabitEthernet1/0/18 switchport access vlan 50
19	interface GigabitEthernet1/0/19 switchport access vlan 50
20	interface GigabitEthernet1/0/20 switchport access vlan 50
21	interface GigabitEthernet1/0/21 switchport access vlan 50
22	interface GigabitEthernet1/0/22 switchport access vlan 50
23	interface GigabitEthernet1/0/23 switchport access vlan 50
24	interface GigabitEthernet1/0/24 switchport access vlan 50
25	interface GigabitEthernet1/0/25 switchport access vlan 50
26	interface GigabitEthernet1/0/26 switchport access vlan 50
27	interface GigabitEthernet1/0/27 switchport access vlan 50
28	interface GigabitEthernet1/0/28 switchport access vlan 50
29	interface GigabitEthernet1/0/29 switchport access vlan 50
30	interface GigabitEthernet1/0/30 switchport access vlan 50
31	interface GigabitEthernet1/0/31 switchport access vlan 50
32	interface GigabitEthernet1/0/32 switchport access vlan 50
33	interface GigabitEthernet1/0/33 switchport access vlan 50
34	interface GigabitEthernet1/0/34 switchport access vlan 50
35	interface GigabitEthernet1/0/35 switchport access vlan 50
36	interface GigabitEthernet1/0/36 switchport access vlan 50
37	interface GigabitEthernet1/0/37 switchport access vlan 50
38	interface GigabitEthernet1/0/38 switchport access vlan 50

39	interface GigabitEthernet1/0/39 switchport access vlan 50
40	interface GigabitEthernet1/0/40 switchport access vlan 50
41	interface GigabitEthernet1/0/41 switchport access vlan 50
42	interface GigabitEthernet1/0/42 switchport access vlan 50
43	interface GigabitEthernet1/0/43 switchport access vlan 50
44	interface GigabitEthernet1/0/44 switchport access vlan 50
45	interface GigabitEthernet1/0/45 switchport access vlan 50
46	interface GigabitEthernet1/0/46 switchport access vlan 50
47	interface GigabitEthernet1/0/47 switchport access vlan 50
48	interface GigabitEthernet1/0/48 switchport trunk native vlan 40 switchport mode trunk

Tabla 4.4: Configuraciones de los 48 puertos Gigabit Ethernet del Switch 2, 3 y 4.

Desde el puerto 1 al puerto 47, se usa el comando “switchport access vlan xx” con el cual establecemos la VLAN a la cual debe pertenecer cada puerto del switch. En el puerto 48, se usa el comando “switchport trunk native vlan 40” que asigna la VLAN respectiva al puerto y el comando “switchport mode trunk” que lo convierte en puerto troncal ya que por este puerto, a más de estar la VLAN propia de los switches (VLAN 40) estarán las VLAN’s de toda la red privada interna. Cada puerto se configura a su respectiva VLAN según la Tabla 4.1.

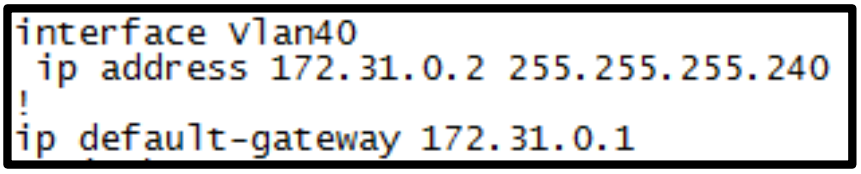


Figura 4.51: Configuración de direccionamiento IPv4 en Switch 1.

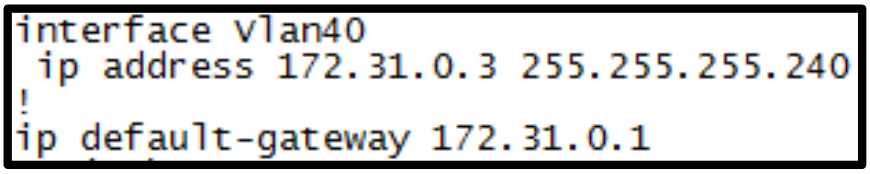


Figura 4.52: Configuración de direccionamiento IPv4 en Switch 2.

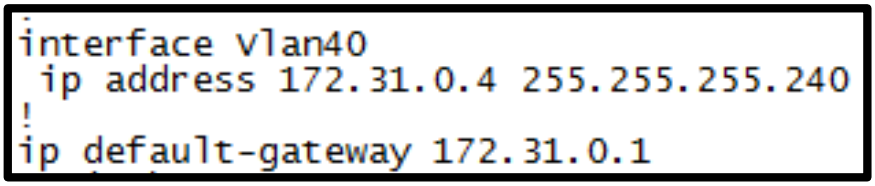


Figura 4.53: Configuración de direccionamiento IPv4 en Switch 3.

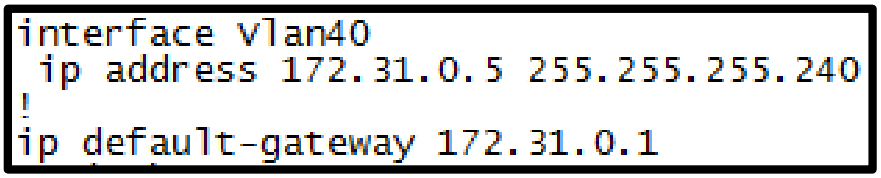


Figura 4.54: Configuración de direccionamiento IPv4 en Switch 4.

Las figuras anteriores muestran las configuraciones de las respectivas VLAN's de cada uno de los switches así también como el direccionamiento IPv4 de cada switch.

Configuración de los AP's y también del ZoneDirector

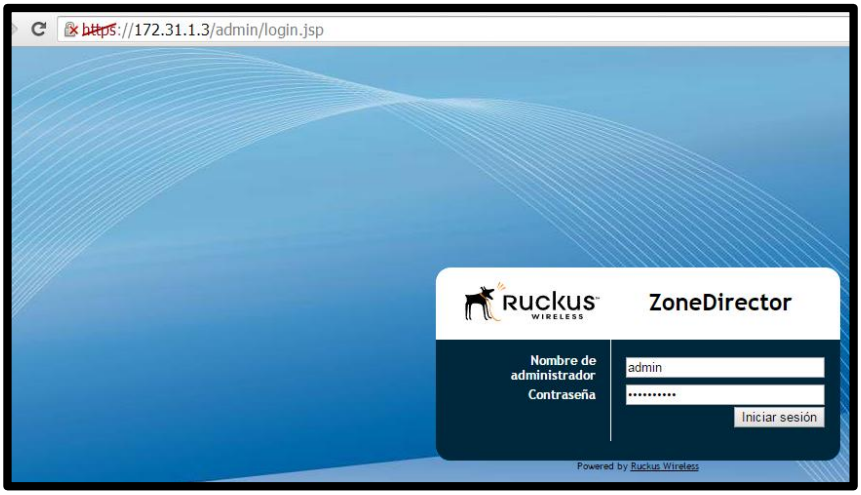


Figura 4.55: Ventana de acceso al ZoneDirector 1100.

En la figura anterior se muestra la ventana de acceso al ZoneDirector 1100 donde se debe de registrar el nombre de administrador y la contraseña. El nombre de administrador es 'admin' y la contraseña es 'acceso'.

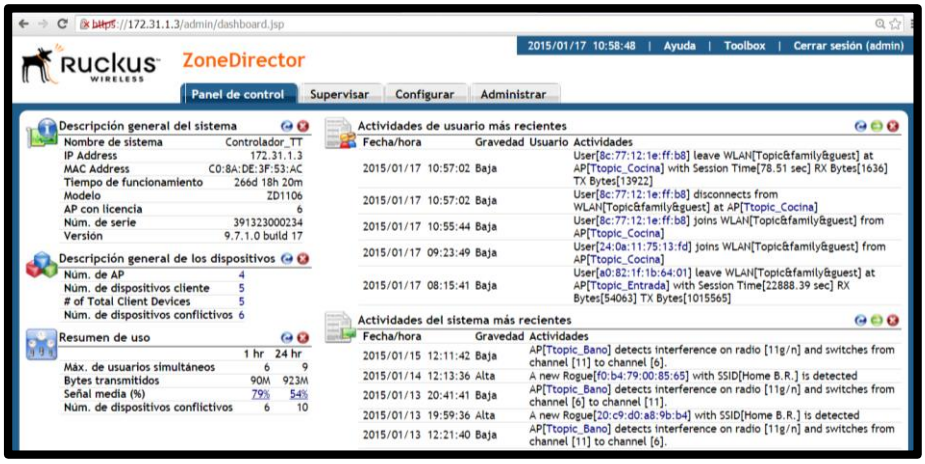


Figura 4.56: Panel de control del ZoneDirector 1100.

En la figura anterior se muestra el panel de control del ZoneDirector, donde se pueden apreciar datos importantes tales como ‘Descripción general del sistema’, ‘Descripción general de los dispositivos’, ‘Resumen de uso’ entre otros, ‘Actividades de usuario más recientes’ y ‘Actividades del sistema más recientes’.

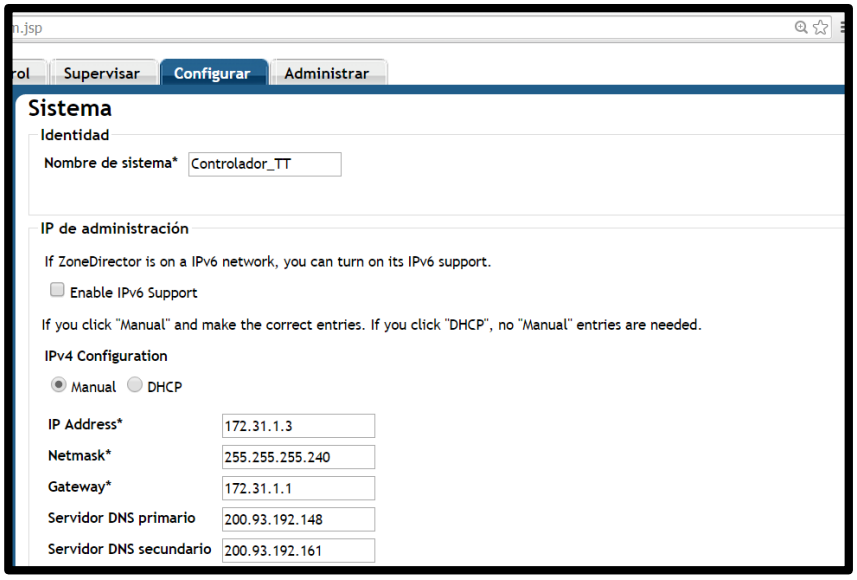


Figura 4.57: Pestaña ‘Configurar’ con la opción ‘Sistema’.

En la figura anterior se muestra la pestaña ‘Configurar’ con la opción ‘Sistema’ en la cual configuramos varios parámetros. En el campo ‘Nombre de sistema’ editamos el nombre del ZoneDirector y colocamos ‘Controlador_TT’. En la opción ‘IPv4 Configuration’ escogemos ‘Manual’. Desde el campo ‘IP

Address' hasta el campo 'Servidor DNS secundario' se editan los valores correspondientes por su direccionamiento IPv4.

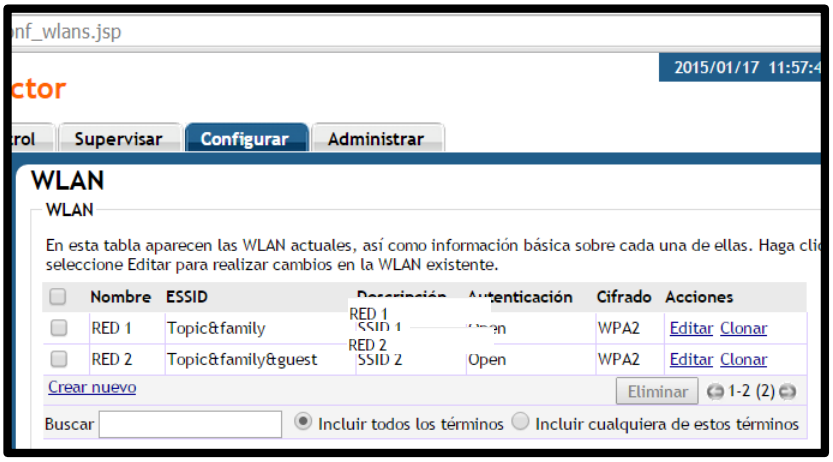


Figura 4.58: Pestaña 'Configurar' con la opción 'WLAN'.

En la figura anterior se muestra la pestaña 'Configurar' con la opción 'WLAN' donde se establecen dos SSID's (Service Set Identifier) para proveer acceso a la red privada interna de manera inalámbrica. Desde una laptop, smartphone o cualquier dispositivo electrónico nos conectamos escogiendo ya sea la SSID 'RED 1' o 'RED 2' y escribimos las contraseñas 'acceso1' y 'acceso2' respectivamente. Una vez configuradas las SSID's, cada punto de acceso automáticamente las emite. Se configuraron dos redes SSID's de iguales características para evitar que existan muchos dispositivos conectados en una sola y proveer de redundancia.

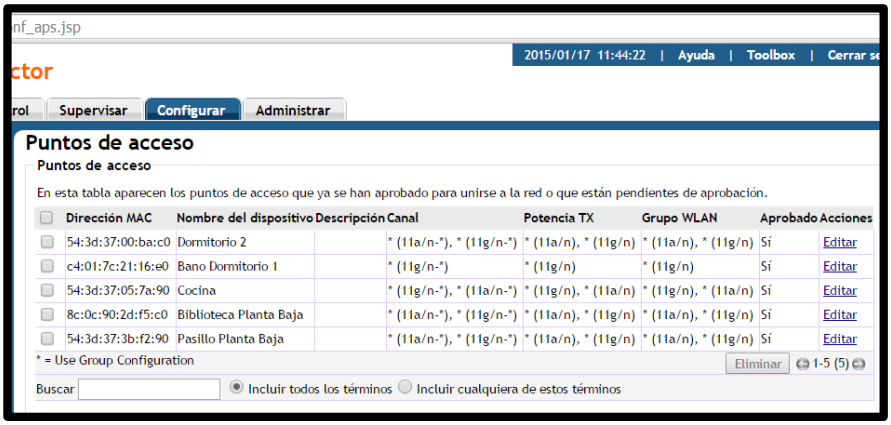


Figura 4.59: Pestaña ‘Configurar’ con la opción ‘Puntos de acceso’.

En la figura anterior se muestra la pestaña ‘Configurar’ con la opción ‘Puntos de acceso’ donde aparecen todos los puntos de acceso inalámbricos que son controlados por el ZoneDirector y que los mostramos en párrafos anteriores. A cada punto de acceso se le configura su direccionamiento IPv4 con la opción ‘Editar’ y es encontrado automáticamente en la red por el ZoneDirector.

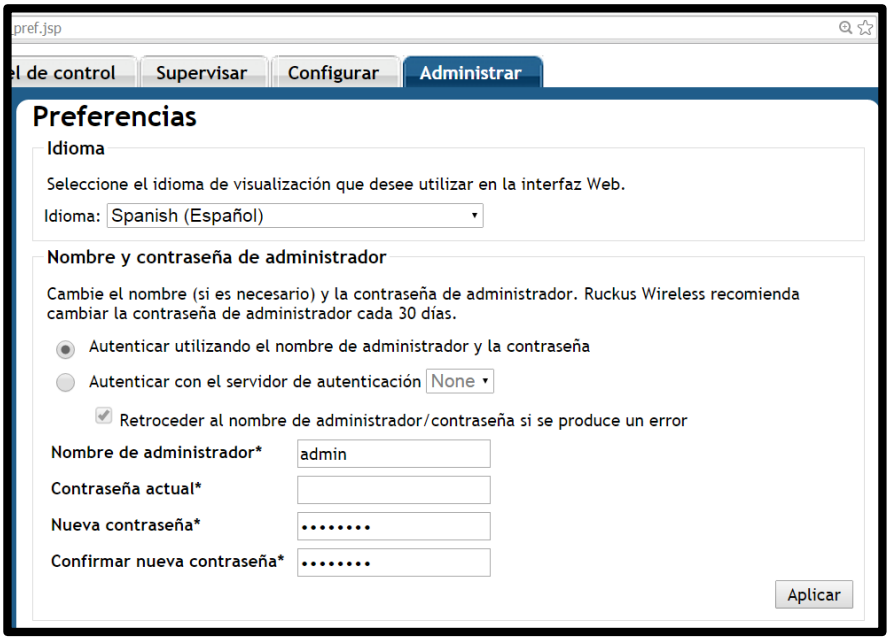


Figura 4.60: Pestaña 'Administrar' con la opción 'Preferencias'.

En la figura anterior se muestra la pestaña 'Administrar' con la opción 'Preferencias' donde se configura el idioma y el nombre de administrador y su respectiva contraseña para acceder a este servicio web de administración del ZoneDirector.

Configuración de la VPN

Finalmente para poder acceder de manera remota a la red interna de la vivienda, configuramos una VPN (Virtual Private Network) de acceso remoto en la interfaz 'Wan1' con ip 186.3.144.73 en el puerto 10443 usando https (secure hypertext

protocol). Se pudo haber configurado la VPN en la interfaz 'Wan2'.

```
config vpn ipsec phase1-interface
    edit "VPN-TN"
        set interface "wan1"
        set ike-version 2
        set local-gw 186.3.144.73:10443
        set proposal 3des-sha1 aes128-sha1
        set user acceso_admin
        set psksecret ENC e/+UAWCmdaj
+xc686u0FGHZ4kiOwK7zl0GbYQcFzoctiiYhrxjGWU5sR8bCFqBwInFeVMU0psN5AcEK2IGG
aGHgHmJ4P2W1dzG9R6BmdFYOIbreYAu3/VHvZv6Q4LLzWUIxVvA97bavtCGvcaJJfQa3m0zp
1ghI2d+/lQU82N1q/9XKMSAMkmQDz0QfYDDH+e97Exw==
    next
end
```

Figura 4.61: Configuración de la VPN en la interfaz Wan1 del fortigate 80C.

La figura anterior nos muestra el establecimiento de la VPN en la interfaz 'Wan1'. La configuración "config vpn ipsec phase1-interface" nos permite setear un túnel a través del protocolo de seguridad IP (IPSec) que permite proteger comunicaciones de VPN's. La opción "set interface wan1" nos permite definir la interfaz sobre la cual vamos a configurar la VPN, en este caso la interfaz 'Wan1'.

La opción "set ike-version 2" nos permite establecer la versión del protocolo de intercambio de la llave de internet o como se escribe en inglés Internet Key Exchange (IKE) que establece una asociación de seguridad entre dos entidades de redes distintas para dar lugar a comunicaciones seguras. La opción "set local-gw 186.3.144.73:10443" establece la dirección de la ip

pública a la cual nos conectaremos de manera remota a través del puerto 10443. Vale recalcar que no es necesario establecer a través de alguna opción el puerto 10443 ya que es un puerto que se establece por defecto en el fortigate 80C. La opción “set proposal 3des-sha1 aes128-sha1” establece dos tipos de cifrado del tráfico de la VPN recomendados por el fabricante. ‘3des’ significa ‘Triple-DES’ y permite encriptar el tráfico 3 veces con 3 llaves diferentes y verifica la autenticidad de la encriptación con ‘sha1’ que significa ‘Secure Hash Algorithm 1’. ‘aes128’ significa ‘Advanced Encryption Standard 128’ que encripta el tráfico con una llave de 128 bits y verifica la autenticidad de la encriptación con ‘sha1’ explicado anteriormente. La opción ‘set user acceso_admin’ nos permite establecer el usuario con el que se accederá a la VPN. La opción ‘set psksecret ENC xxxxx’ nos permite cifrar la contraseña para acceder a la vpn. La contraseña no cifrada es ‘conexionavpn2014’.

4.3. Diseño del sistema domótico para la gestión de la seguridad.

4.3.1. Dispositivos.

SENSORES DE MOVIMIENTO

Para la realización de este proyecto usamos 4 tipos de sensores de movimiento, descritos a continuación.

Aeon Labs Multisensor 4 in 1

Figura 4.62: Sensor de Movimiento de la marca Aeon Labs.

Descripción

Este sensor de movimiento [60] es fabricado por la empresa Aeon Labs. Puede ser ubicado ya sea en la esquina, interior o exterior de una habitación. Sensa 4 tipos de variables: 1) movimiento, 2) temperatura, 3) humedad y 4) luminosidad. En

este proyecto lo usaremos para sensar solo movimiento. El movimiento es sensado con un sensor infrarojo pasivo [59]. Las especificaciones se muestran a continuación [59].

Especificaciones

- Rango de Temperatura: -20°C to 50°C / -4°F to 122°F.
- Precisión de Temperatura: ±1°c
- Rango de humedad relativa: 20% – 90%.
- Precisión de humedad: ±5%
- Rango de Luminosidad: 0 – 1000 LUX
- Peso: 118g.
- Protección IP: IP42
- Rango de alcance de la antena Z-Wave: 300 pies en exteriores, 80 pies en interiores
- Alimentado por baterías

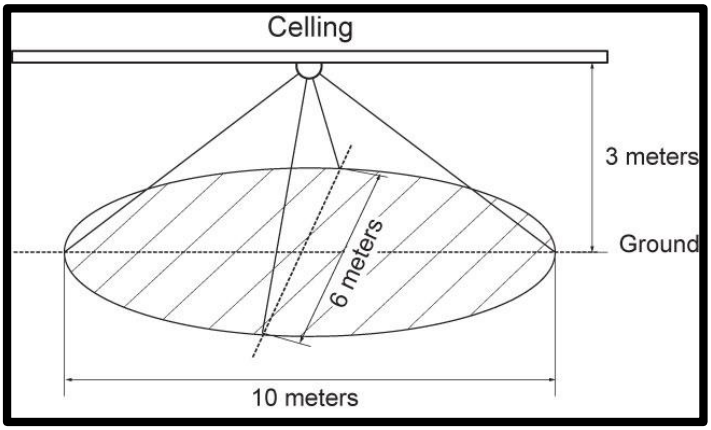


Figura 4.63: Alcance de detección de movimiento en el techo.

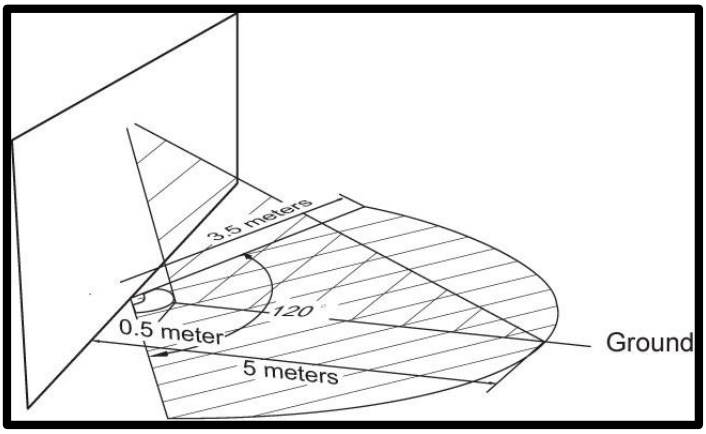


Figura 4.64: Alcance de detección de movimiento en esquina o pared.

Las figuras anteriores [61] muestran el alcance de detección de movimiento en el techo y el alcance de detección de movimiento en esquina o pared.

Everspring Motion Sensor HSP02

Figura 4.65: Sensor de movimiento de la marca Everspring.

Descripción

Este sensor de movimiento [63] es un dispositivo compatible con el protocolo de comunicación Z-Wave fabricado por la marca Everspring siendo el modelo HSP02. Usa un detector infrarrojo pasivo. Este detector de movimiento se puede controlar a través varios controladores tales como el VERA3 [62]. Las especificaciones se muestran a continuación [62].

Especificaciones

- Protocolo de comunicación: Z-Wave
- Frecuencia del protocolo Z-Wave: 908.42MHz (US)

- Ángulo de detección: 100° x 10m
- Sensibilidad de detección ajustable
- PCB ajustable para acortar o alargar el rango de detección
- Bajo consumo de potencia
- Operado por batería de 3.6V del tipo ER14250
- Rango de operación: hasta 590 pies
- Indicador de baja batería
- Dimensiones: 62.0 x 87.0 x 42.0 mm

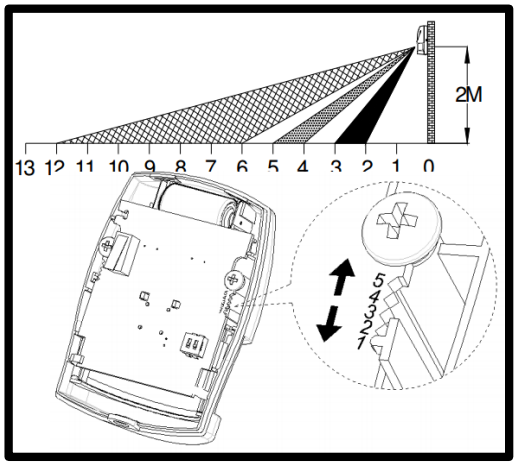


Figura 4.66: Alcance de detección de movimiento del sensor HSP02.

La figura anterior [64], muestra el alcance de detección de movimiento del sensor HSP02.

Motion Sensor Schlage RS200HC

Figura 4.67: Sensor de movimiento de la marca Schlage.

Descripción

El sensor de movimiento [66] de la marca Schlage permite detectar de forma remota la actividad dentro de la casa y a la vez permite mantenerse en contacto y en control con el controlador que maneja este sensor. Está basado en un detector infrarrojo pasivo [65]. Las especificaciones se muestran a continuación [65].

Especificaciones

- Solo para uso interior
- Amplio ángulo de detección de 120°

- Inmune a detección de animales
- Protocolo de comunicación: Z-Wave
- Frecuencia del protocolo Z-Wave: 908.42 MHz
- Rango de operación: Hasta 100 pies o 30.5 metros en línea directa
- Temperatura de operación: 0° – 49°C, 32° – 120°F
- Tipo de batería requerida: 3V Litio CR123A
- Vida aproximada de la batería: 3 años

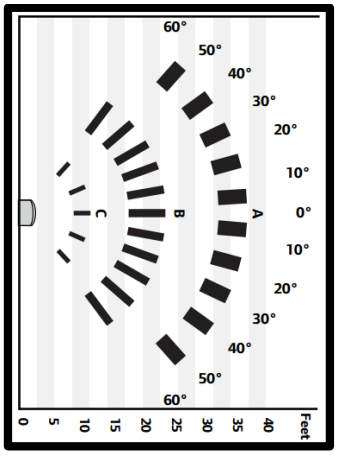


Figura 4.68: Alcance de detección de movimiento del sensor RS200HC.

La figura anterior muestra el alcance de detección de movimiento del sensor RS200HC [65].

EZ Motion Sensor Express Control B00G726FCM

Figura 4.69: Sensor de movimiento de la marca Express Control.

Descripción

Este sensor [67] fabricado por la marca Express Control está concebido principalmente como un sensor de movimiento que detecta el movimiento y envía un comando a un máximo de 4 dispositivos Z-Wave “asociados”. Estos otros dispositivos Z-Wave pueden controlar directamente las luces de una habitación. La indicación de movimiento puede ser enviado a un ordenador para control de escenas complejas de iluminación, audio, vídeo y calefacción/refrigeración. Cuando no se detecta movimiento dentro de un período preestablecido de tiempo, el sensor enviará un comando de “off” a los nodos de Z-Wave para apagar las luces. La sensibilidad del sensor de movimiento es programable para permitir que no se detecten las mascotas

pequeñas o se puede programar para ser altamente sensible incluso a un ligero movimiento [67]. Las especificaciones se muestran a continuación [67].

Especificaciones

- Protocolo de comunicación: Z-Wave
- Frecuencia del protocolo: 908.42 MHz
- Se puede asociar hasta con 4 otros dispositivos
- Rango de alcance de la señal: 150 pies en línea abierta
- Amplio ángulo de detección de movimiento de 120°
- Alcance de detección de movimiento: 30 pies
- Sensibilidad de detección ajustable
- Indicador LED de movimiento
- Rango del sensor de temperatura: 20º - 150º F
- Resolución del sensor de temperatura: 0.2º F
- Operado por 3 baterías AAA
- 1 año de vida de las baterías

SENSOR DE APERTURA Y CERRADO DE PUERTAS

Aeon Labs Door Window Sensor

Figura 4.70: Sensor de apertura y cerrado de puertas de la marca Aeon Labs.

Descripción

El sensor de apertura y cerrado de puertas [69] detecta si una puerta o ventana está abierta o cerrada. Puede asociarse con otros dispositivos de la red Z-Wave a la que pertenece e informar al controlador en este caso el VERA3 acerca de las puertas y ventanas que monitorea. Tal vez una puerta abierta significa que las luces deben encenderse y darle la bienvenida a casa. Tal vez una ventana abierta significa que una alarma debe ser disparada. Sea lo que sea que signifique, con sensores de puertas y ventanas instaladas, su red Z-Wave

tendrá tanto el poder como la inteligencia para hacerlo. Consta de dos partes, el cuerpo principal y el magneto [68]. Las especificaciones se muestran a continuación [68].

Especificaciones

- Protocolo de comunicación: Z-Wave
- Frecuencia del protocolo: 908.42 MHz
- Dimensiones: 2.0cm x 3.4cm x 7.9cm (main body)
- Operado por 2 baterías AAA
- Detección de baja batería
- Botón de inclusión Z-Wave escondido
- Rango de alcance de la antena optimizada
- Alcance de señal: 300 pies en línea directa
- Fácil uso e instalación
- Producto certificado para Estados Unidos, Europa y los mercados Australianos (FCC, CE, CTICK, ROHS)

CÁMARAS

Samsung SNV-7080R

Figura 4.71: Cámara SNV-7080R de la marca Samsung.

Descripción

La SNV-7080R [71] es una cámara domo anti-vandálica compatible con ONVIF de nuevo lanzamiento perteneciente a la gama de cámaras de 3 megapíxeles. Utiliza el chipset WiseNet2 DSP de Samsung diseñado específicamente para proporcionar a los usuarios las máximas ventajas gracias a la tecnología de cámaras megapíxel más reciente. La SNV-7080R con calificación IP66 puede funcionar de forma eficaz en entornos más exigentes expuestos a condiciones meteorológicas adversas y variables, así como a sabotaje o ataques físicos.

Además, gracias a los 15 LED de IR incorporados, la SNV-7080R posee la capacidad de capturar imágenes claras de objetos que se encuentren a una distancia de hasta 25 metros de la cámara, incluso en completa oscuridad. Capaz de mostrar varias resoluciones 1080p full HD desde formato CIF (320 x 240) a 16:9 y hasta 3 megapíxeles (2048 x 1536), estas resoluciones tienen la posibilidad de transmitirse de forma simultánea, lo que permite transmitir las secuencias más importantes a su dispositivo de visualización o de grabación [70]. Las especificaciones se muestran a continuación [70].

Especificaciones

- Alimentación mediante PoE o fuente de 12 VDC
- 1 puerto RJ-45 Ethernet de 100 Mbps
- Resolución máxima 3 M (2048 x 1536)
- Resolución admitida: 16:9 Full HD (1080p)
- Objetivo Vari-focal motorizado de 3 a 8,5 mm (2.8x)
- LED de IR incorporados
- Longitud visualizable: 25 m
- Wide Dynamic Range Full HD
- Compresión Inteligente
- Grado IP66

SERVIDOR

HP ProLiant Gen8 DL380e

Figura 4.72: Servidor HP ProLiant Gen8 DL380e.

Descripción

El servidor HP ProLiant DL380e Gen8 [73] proporciona una amplia selección de controladores, unidades, expansión de E/S y opciones de unidad posterior para que los clientes cumplan con sus diferentes requisitos de almacenamiento hoy, con escalabilidad para ampliar su solución mañana de forma rentable. Ofrece una gama de características que garantizan la seguridad de los datos y la alta disponibilidad. Incluye protección de memoria ECC, TPM, bisel protegido, así como fuente de alimentación redundante y opciones de ventilador. Con herramientas de gestión integradas, el servidor HP ProLiant DL380e Gen8 simplifica las tareas de mantenimiento y gestión del servidor, lo que permite la implementación rápida y

sencilla (HP Intelligent Provisioning), la supervisión del estado del sistema (HP Active Health System) y la facilidad de actualizaciones de firmware (HP Smart Update Manager). Para la realización de este proyecto este servidor, posee como sistema operativo el Windows Server 2008 R2 Standard [72]. Las especificaciones se muestran a continuación [72].

Especificaciones

- Sistema operativo: Windows Server 2008 R2 Standard
- Service Pack 1
- Procesador: Intel(R) Xeon(R) CPU E5-2420 0 @ 1.9 GHz
- Memoria RAM: 16 GB (15.8 GB usables) 12 núcleos
- Tipo de sistema: 64 bits
- Memoria de Disco Duro: 16 TB
- 4 Interfaces de red Ethernet HP Ethernet 1 GB 366i
- 3 interfaces USB 2.0
- Peso: 43 kg
- Dimensiones(Pro-Ancho-Largo): 44.55 x 69.85 x 8.74 cm
- Alimentación Eléctrica: 110 VAC

4.3.2. Configuración.

SENSORES DE MOVIMIENTO

Configuración en el VERA3

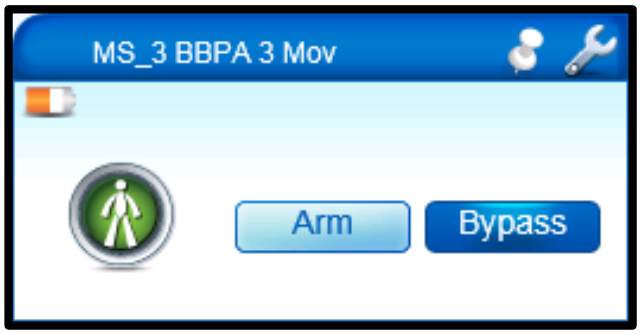


Figura 4.73: Sensor de movimiento en la interfaz gráfica del VERA3.

En la figura anterior se muestra el sensor de movimiento tal cual aparece en la interfaz gráfica del VERA3. Las opciones 'Arm' y 'Bypass' permiten habilitar y deshabilitar al sensor respectivamente. En la esquina superior derecha se encuentra un ícono de una llave de tuercas. Se da click en este ícono y se puede acceder al panel de configuración del sensor de movimiento.

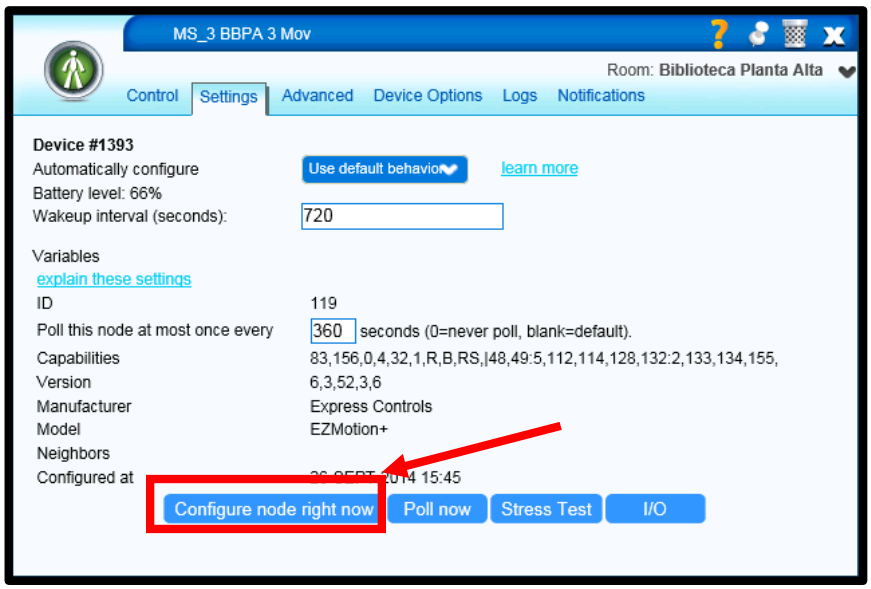


Figura 4.74: Pestaña de Settings del panel de configuración del sensor de movimiento.

En la figura anterior se muestra la pestaña de ‘Settings’ del panel de configuración del sensor de movimiento. En el campo ‘Wakeup interval(seconds)’ escribimos el intervalo en segundos en el que nuestro sensor de movimiento va a despertar ya que estos sensores funcionan con baterías y tienen que estar en un modo de ‘dormir’ durante cierto tiempo para evitar que el hardware realice procesos internos que no consuma la batería y en nuestro caso a los 720 segundos despiertan. Esto no evita que estén sensando el movimiento continuamente. En el campo ‘Poll this node at most once every ___ seconds’ escribimos 360 que corresponde a 360 segundos. Esto permite que el VERA3 revise el estado del sensor cada 360 segundos con un payload

mucho menor al que si el dispositivo estuviese despierto. Presionamos ‘Configure node right now’.

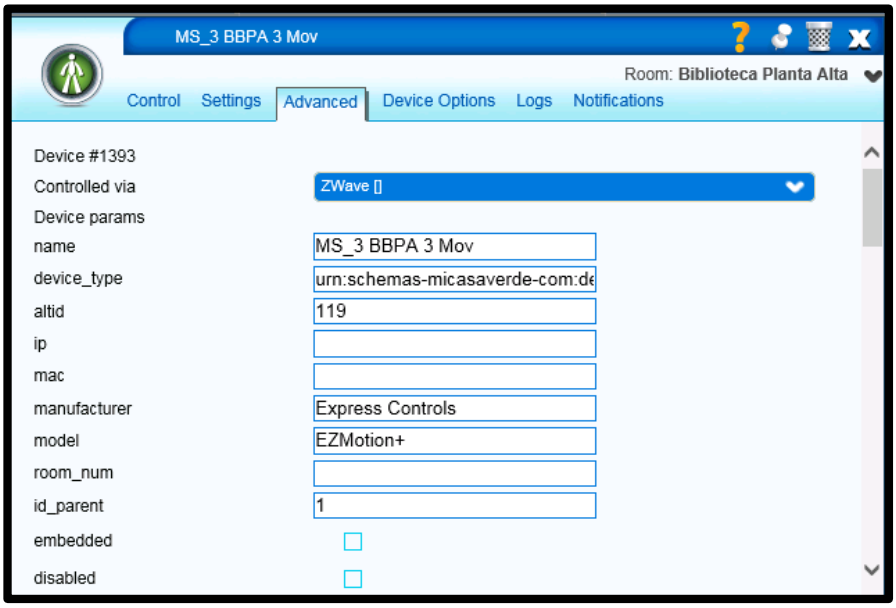


Figura 4.75: Pestaña de Advanced del panel de configuración del sensor de movimiento.

La figura anterior muestra la pestaña de ‘Advanced’ del panel de configuración del sensor de movimiento. El único campo que editamos es el campo ‘name’ donde colocamos el nombre del sensor. Para escribir el nombre del sensor nos regimos al formato establecido al final de la sección 4.1 y el identificador para los sensores de movimiento será ‘MS’ que significa ‘Movement Sensor’ o en español, ‘Sensor de Movimiento’ y nos basamos en la tabla siguiente.

NOMBRES DE LOS SENSORES DE MOVIMIENTO		
	SECTOR	**NOMBRE**
1	BIBLIOTECA PLANTA ALTA	MS_1 BBPA 1 Mov
2		MS_2 BBPA 2 Mov
3		MS_3 BBPA 3 Mov
4	BIBLIOTECA PLANTA BAJA	MS_4 BBPB 1 Mov
5		MS_5 BBPB 2 Mov
6		MS_6 BBPB 3 Mov
7	ESTUDIO	MS_7 Estudio Mov
8	SALA	MS_8 Sala Mov
9	PASILLO PLANTA BAJA	MS_9 PasilloPB Mov
10	COMEDOR	MS_10 Comedor Mov
11	COCINA	MS_11 Cocina Mov
12	GARAJE	MS_12 Garaje Mov
13	DORMITORIO 1	MS_13 Dormitorio1 Mov
14	DORMITORIO 2	MS_14 Dormitorio2 Mov
15	DORMITORIO 3	MS_15 Dormitorio3 Mov
16	DORMITORIO 4	MS_16 Dormitorio4 Mov
17	PASILLO PLANTA ALTA	MS_17 PasilloPA Mov

Tabla 4.5: Tabla de los nombres de los sensores de movimiento.

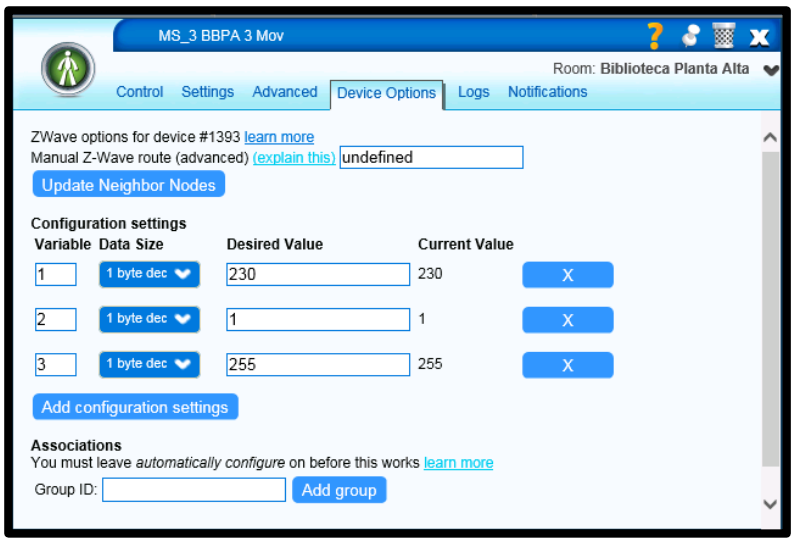


Figura 4.76: Pestaña de Device Options del panel de configuración del sensor de movimiento.

En la figura anterior se muestra la pestaña ‘Device Options’ del panel de configuración del sensor de movimiento. El único campo que editamos, el campo de ‘Variable = 2’ en la sección ‘Desired Value’ donde escribimos ‘1’. Esto permite que el sensor esté activado sólo un segundo cuando este detecte movimiento.

Para poder guardar estas configuraciones en el dispositivo, se necesita que este se encuentre despierto y esto se logra teniendo el dispositivo a la mano y presionando 3 veces el botón de inclusión, con lo cual, el dispositivo queda despierto por 10 minutos, tiempo necesario para guardar las configuraciones. Estos sensores actúan como trigger en las escenas que más adelante se mostrarán. Las escenas pueden durar un intervalo de tiempo definido por el usuario. Ese intervalo de tiempo depende ya sea del sensor o de la escena como tal y por razones logísticas es preferible que las escenas dependan de la escena y no del sensor. Esto se asegura dejando activado al sensor por un segundo.

Se debe ingresar a cada dispositivo en el ‘Room’ correspondiente, esto se muestra como hacer en la sección 4.1.

Ubicación en la vivienda

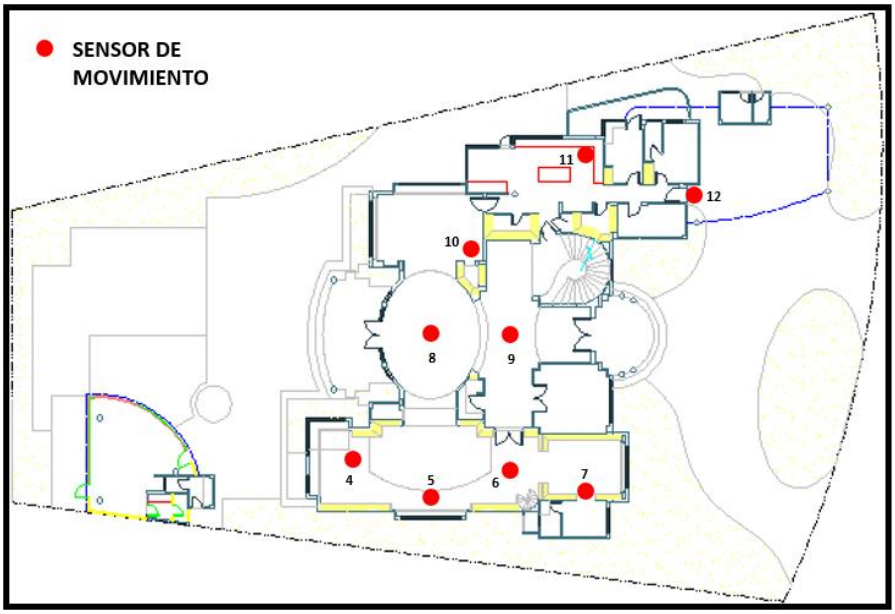


Figura 4.77: Ubicación de los sensores de movimiento en la planta baja.

En la figura anterior se muestra la ubicación de los sensores de movimiento en la planta baja de la vivienda.

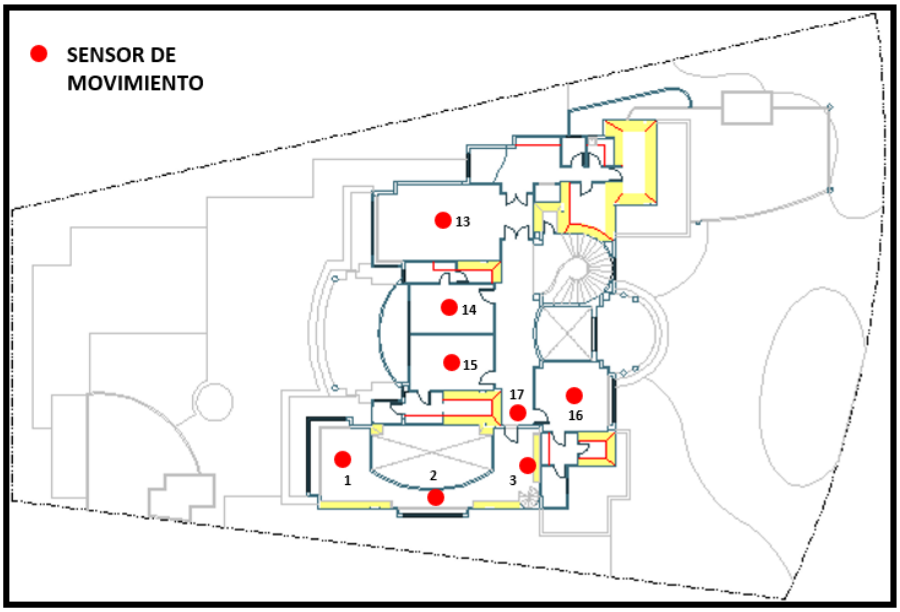


Figura 4.78: Ubicación de los sensores de movimiento en la planta alta.

En la figura anterior se muestra la ubicación de los sensores de movimiento en la planta alta de la vivienda.

SENSOR DE APERTURA Y CERRADO DE PUERTAS

Configuración en el VERA3

Figura 4.79: Sensor de apertura y cerrado de puertas en la interfaz gráfica del VERA3.

En la figura anterior se muestra el sensor de apertura y cerrado de puertas tal cual aparece en la interfaz gráfica del VERA3. Las opciones ‘Arm’ y ‘Bypass’ permiten habilitar y deshabilitar al sensor respectivamente. En la esquina superior derecha se encuentra un ícono de una llave de tuercas. Se da click en este ícono y se puede acceder al panel de configuración del sensor.

Figura 4.80: Pestaña de Settings del panel de configuración del sensor de apertura y cerrado de puertas.

En la figura anterior se muestra la pestaña de ‘Settings’ del panel de configuración del sensor de apertura y cerrado de puertas. En el campo ‘Wakeup interval (seconds)’ escribimos el intervalo en segundos en el que nuestro sensor de apertura y

cerrado de puertas va a despertar ya que estos sensores funcionan con baterías y tienen que estar en un modo de 'dormir' durante cierto tiempo para evitar que el hardware realice procesos internos que no consuma la batería y en nuestro caso a los 720 segundos despiertan. Esto no evita que estén sensando la apertura y cerrado de puertas continuamente. En el campo 'Poll this node at most once every ___ seconds' escribimos 360 que corresponde a 360 segundos. Esto permite que el VERA3 revise el estado del sensor cada 360 segundos con un payload mucho menor al que si el dispositivo estuviese despierto.

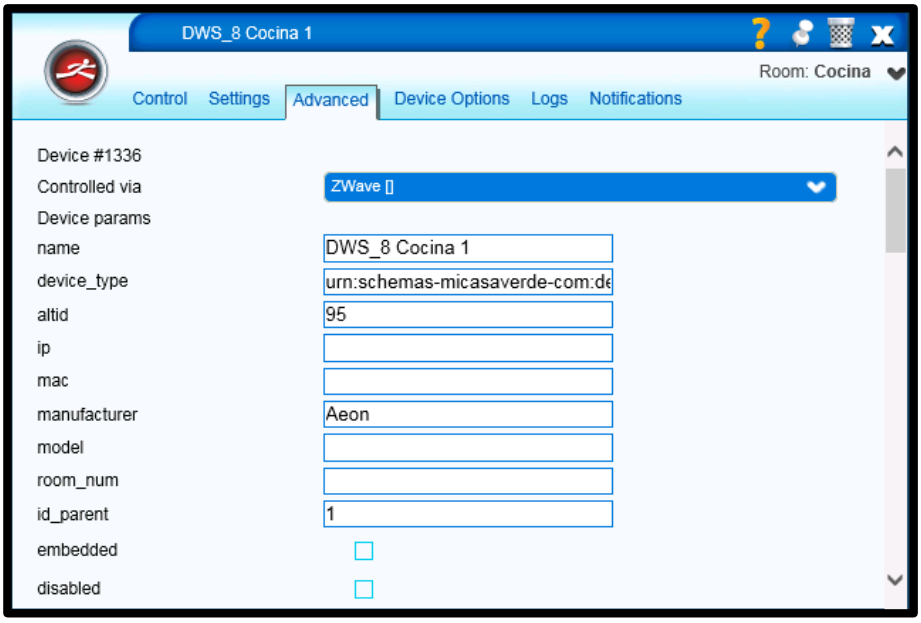


Figura 4.81: Pestaña de Advanced del panel de configuración del sensor de apertura y cerrado de puertas.

La figura anterior muestra la pestaña de ‘Advanced’ del panel de configuración del sensor de apertura y cerrado de puertas. El único campo que editamos es el campo ‘name’ donde colocamos el nombre del sensor. Para escribir el nombre del sensor nos regimos al formato establecido al final de la sección 4.1 y el identificador para los sensores de apertura y cerrado de puertas será ‘DWS’ que significa ‘Door Window Sensor’ o en español, ‘Sensor de puertas y ventanas’ y nos basamos en la tabla siguiente.

NOMBRES DE LOS SENSORES DE APERTURA Y CERRADO DE PUERTAS		
	SECTOR	**NOMBRE**
1	BAÑO DORMITORIO 1	DWS_1 BañoDormitorio1
2		DWS_2 BañoDormitorio1
3		DWS_3 BañoDormitorio1
4		DWS_4 BañoDormitorio1
5		DWS_5 BañoDormitorio1
6	BIBLIOTECA PLANTA ALTA	DWS_6 BBPA
7	BIBLIOTECA PLANTA BAJA	DWS_7 BBPB
8	COCINA	DWS_8 Cocina
9		DWS_9 Cocina
10	DORMITORIO 1	DWS_10 Dormitorio1
11	DORMITORIO 2	DWS_11 Dormitorio2
12	DORMITORIO 3	DWS_12 Dormitorio3
13	DORMITORIO 4	DWS_13 Dormitorio4
14	DORMITORIO MADRE	DWS_14 DormitorioMadre
15	ESTUDIO	DWS_15 Estudio
16	PASILLO PLANTA BAJA	DWS_16 PasilloPB

Tabla 4.6: Tabla de los nombres de los sensores de apertura y cerrado de puertas.

Vale destacar que estos sensores cambian su logo ya sea de rojo a verde dependiendo si está abierta o cerrada la puerta respectivamente. No se les necesita configurar ningún intervalo de tiempo ya que detectan estados, abierto o cerrado.

Para poder guardar estas configuraciones en el dispositivo, se necesita que este se encuentre despierto y esto se logra teniendo el dispositivo a la mano y presionando 3 veces el botón de inclusión, con lo cual, el dispositivo queda despierto por 10 minutos, tiempo necesario para guardar las configuraciones.

Se debe ingresar a cada dispositivo en el ‘Room’ correspondiente, esto se muestra como hacer en la sección 4.1.

Ubicación en la vivienda

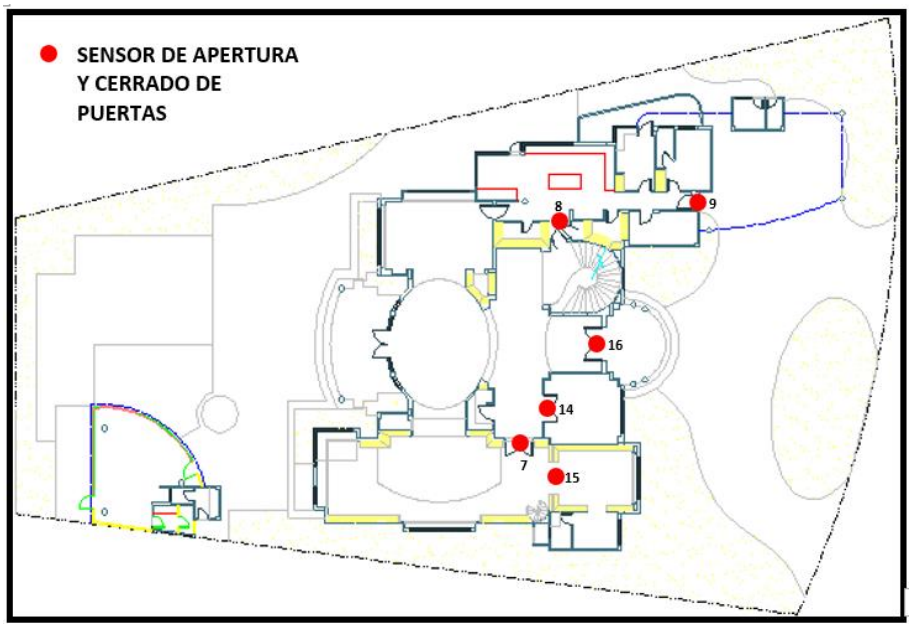


Figura 4.82: Ubicación de los sensores de apertura y cerrado de puertas en la planta baja.

En la figura anterior se muestra la ubicación de los sensores de apertura y cerrado de puertas en la planta baja de la vivienda.

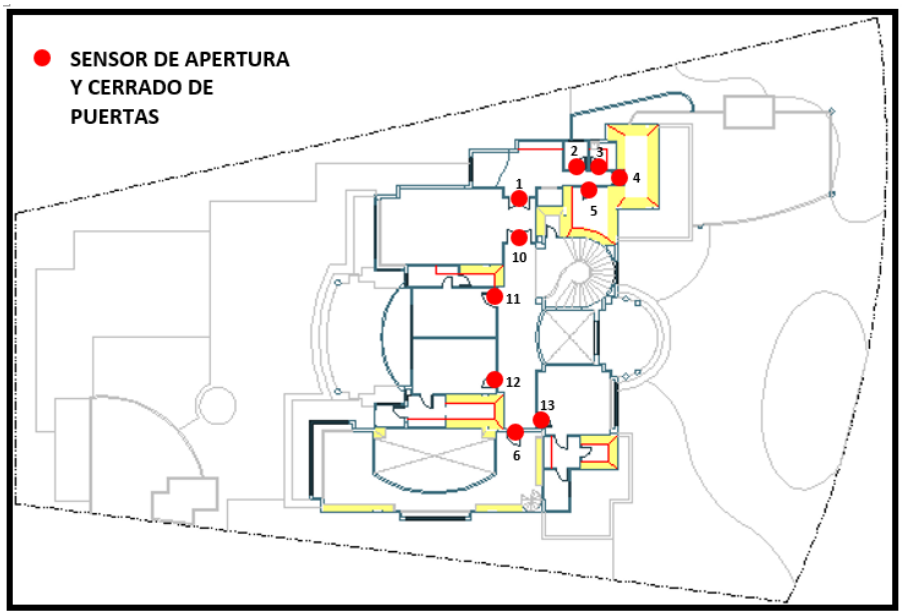


Figura 4.83: Ubicación de los sensores de apertura y cerrado de puertas en la planta alta.

En la figura anterior se muestra la ubicación de los sensores de apertura y cerrado de puertas en la planta alta de la vivienda.

CÁMARAS

PLAN IPv4 DE LAS CÁMARAS		
	SECTOR	IP
1	JARDINES FRENTE DERECHA	172.16.5.0
2	JARDINES FRENTE IZQUIERDA	172.16.5.1
3	GARAJE	172.16.5.2
4	EXTERIOR POSTERIOR 2	172.16.5.3
5	EXTERIOR POSTERIOR 2	172.16.5.4
6	EXTERIOR POSTERIOR 2	172.16.5.5
7	EXTERIOR POSTERIOR 2	172.16.5.6
8	PASILLO PLANTA ALTA	172.16.5.7
9	PASILLO PLANTA BAJA	172.16.5.8
10	BIBLIOTECA PLANTA BAJA	172.16.5.9
11	BIBLIOTECA PLANTA ALTA	172.16.5.10
12	COCINA	172.16.5.11
13	ESTUDIO	172.16.5.12

Tabla 4.7: Plan IPv4 de las cámaras.

En la tabla 4.6 se muestra el plan IPv4 de las cámaras. Se les va a configurar su direccionamiento IPv4 según esta tabla. Todas las cámaras poseen las siguientes credenciales de acceso: 1) el user es ‘admin’ y 2) el password es ‘1234’.

Configuración en las cámaras

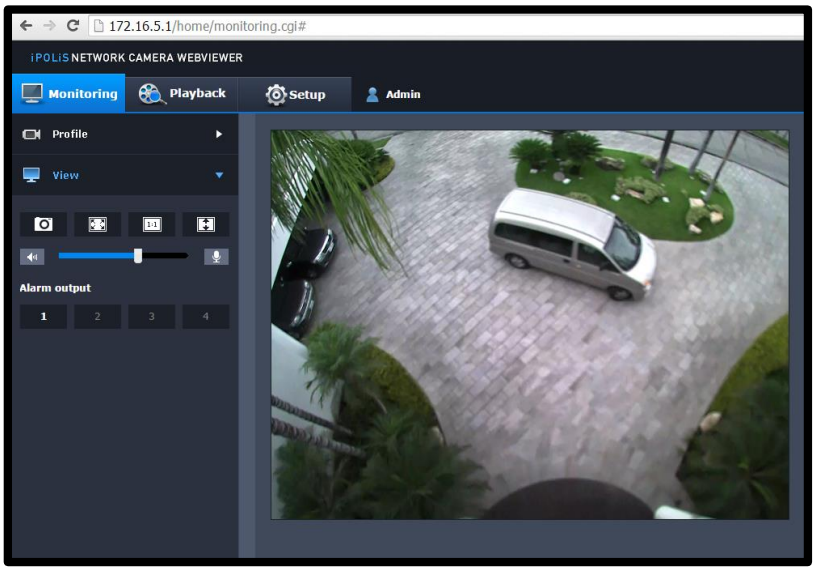


Figura 4.84: Panel de configuración de las cámaras.

La figura anterior muestra el panel de configuración de las cámaras. A este panel se accede una vez dentro de la red privada interna de la vivienda escribiendo en la sección de URL de un browser (Google Chrome, Firefox, Internet Explorer, entre otros) la IP de la cámara según la tabla 4.4.

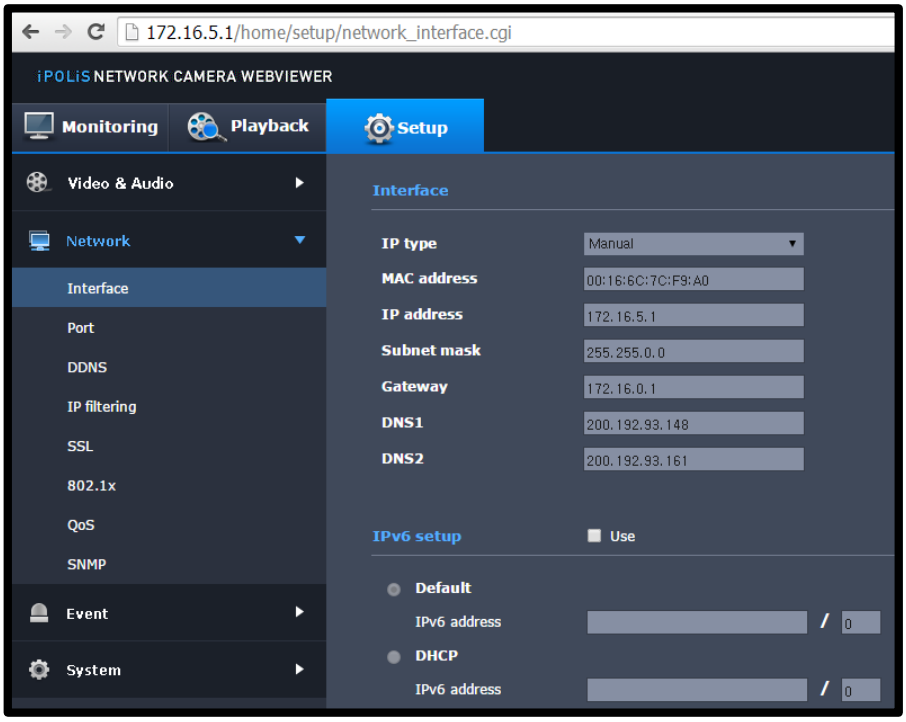


Figura 4.85: Pestaña de Setup con la opción Interface.

La opción ‘Interface’ de la pestaña de ‘Setup’ nos permite editar el direccionamiento IPv4 de las cámaras. En el campo ‘IP type’ seleccionamos ‘Manual’. El campo ‘MAC address’ no se puede editar. El campo ‘IP address’ se edita según la tabla 4.4. La ‘Subnet mask’ para todas las cámras es ‘255.255.0.0’. El ‘Gateway’ para todos los dispositivos de la VLAN 50 es ‘172.16.0.1’. El ‘DNS1’ es ‘200.192.93.148’. El ‘DNS2’ es ‘200.192.93.161’. Estos DNS son parte de la empresa Telconet.

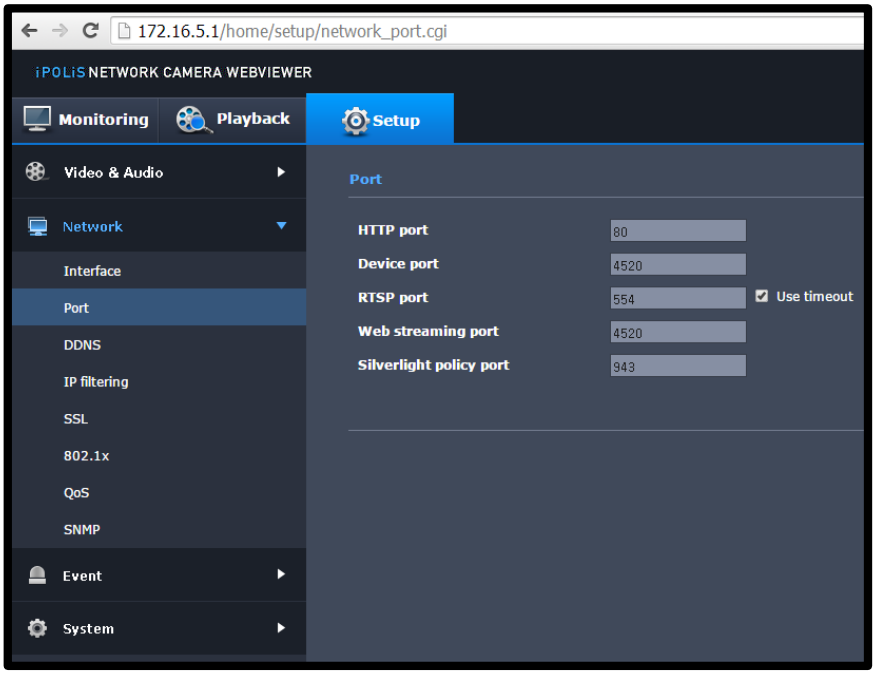


Figura 4.86: Pestaña de Setup con la opción Port.

La opción ‘Port’ de la pestaña ‘Setup’ nos permite definir los puertos que estarán habilitados para que la cámara pueda transmitir streaming de video. El campo ‘HTTP port’ (Hypertext Transfer Protocol) se fija en ‘80’. Este puerto permite, en palabras sencillas, visualizar el panel de configuración de las cámaras. El campo ‘Device port’ se fija en ‘4520’. Este puerto es el puerto de la cámara a nivel de capa de transporte según el modelo OSI. El campo ‘RTSP port’ (Real Time Streaming Protocol) se fija en ‘554’. Este puerto es el puerto de la cámara a nivel de capa de aplicación según el modelo OSI que permite establecer y controlar el streaming de video. El campo ‘Web

streaming port' se fija en '4520' y es un puerto a nivel de la capa de aplicación que permite ver vídeo o escuchar audio a través de la Web. El campo 'Silverlight policy port' se fija en '943' es un puerto propietario de la marca Windows que viene configurado por defecto.

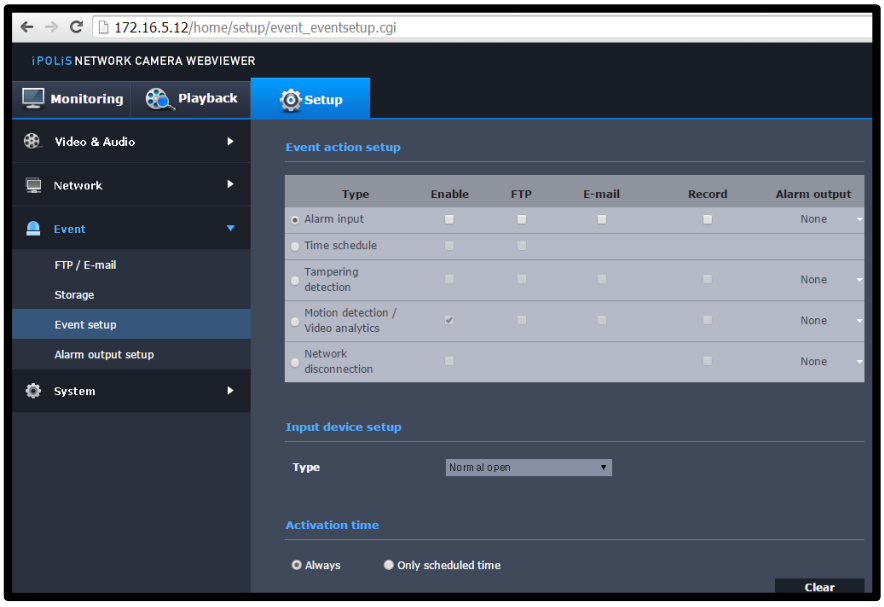


Figura 4.87: Pestaña Setup con la opción Event Setup.

Se dejará configurado que las cámaras graben solamente cuando detecten algún tipo de movimiento. En la figura anterior se muestra la pestaña 'Setup' con la opción 'Event Setup' donde en la sección 'Event action setup' en la fila de 'Motion detection / Video analytics' marcamos con un visto la casilla de la columna 'Enable'. Esto nos permite habilitar la grabación por detección

de movimiento. La sección ‘Input device setup’ no la usamos. En la sección ‘Activation time’ escogemos ‘Always’ que nos permite que la grabación por detección de movimiento sea 24/7.

Ubicación en la vivienda

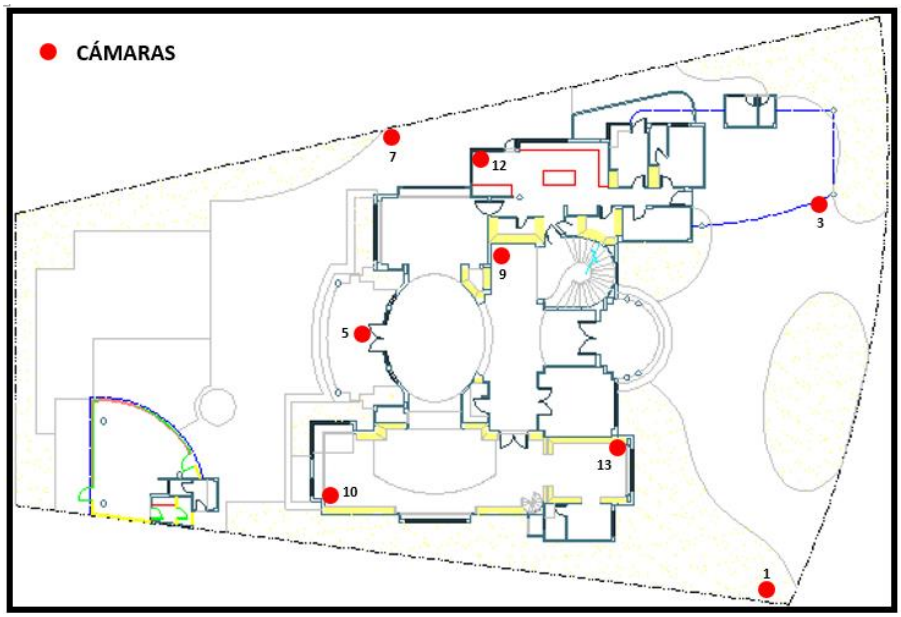


Figura 4.88: Ubicación de las cámaras en la planta baja.

En la figura anterior se muestra la ubicación de las cámaras en la planta baja de la vivienda.

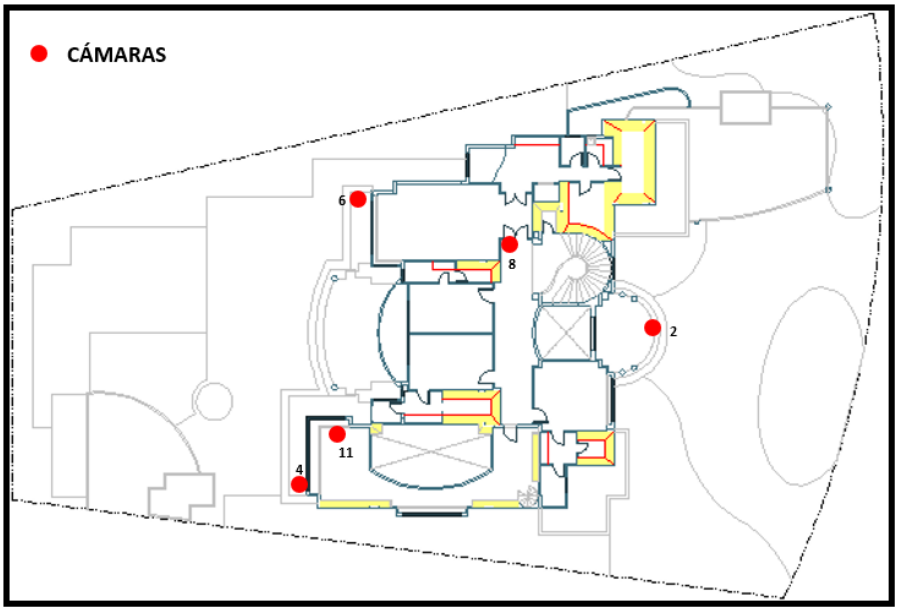


Figura 4.89: Ubicación de las cámaras en la planta alta.

En la figura anterior se muestra la ubicación de las cámaras en la planta alta de la vivienda.

SERVIDOR

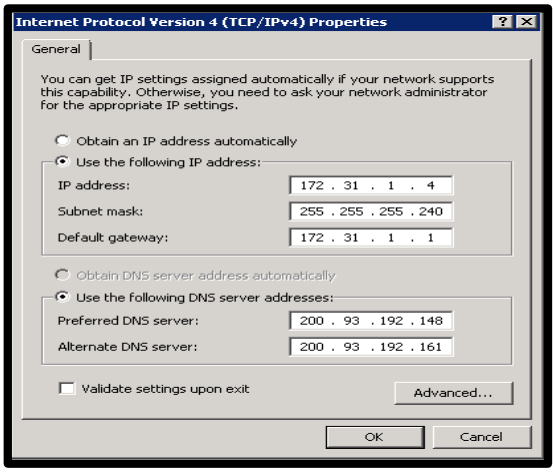


Figura 4.90: Direccionamiento IPv4 del Servidor.

La figura anterior muestra el direccionamiento IPv4 del servidor. El campo ‘IP address’ es ‘172.31.1.4’. El campo ‘Subnet mask’ es ‘255.255.255.240’. El campo ‘Default gateway’ es ‘172.31.1.1’. El campo ‘Preferred DNS server’ es ‘200.93.192.148’. El campo ‘Alternate DNS server’ es ‘200.93.192.161’. Recordamos que este servidor pertenece a la VLAN 30.

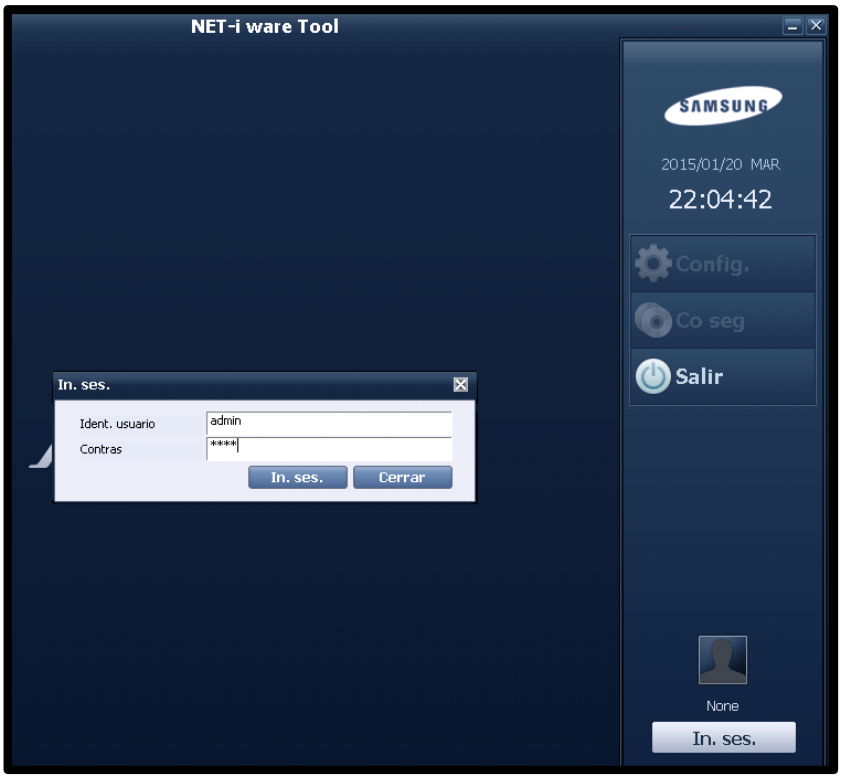


Figura 4.91: Inicio de sesión en software NET-i Ware.

La figura anterior muestra el inicio de sesión del software NET-i Ware. Este software debe ser instalado en el servidor para poder realizar las configuraciones necesarias en cuanto a la administración de las cámaras y su posterior reproducción. Esto se explica en los párrafos siguientes. Las credenciales de acceso a este software son las siguientes: 1) el usuario es 'admin' y 2) la clave es '4378'.

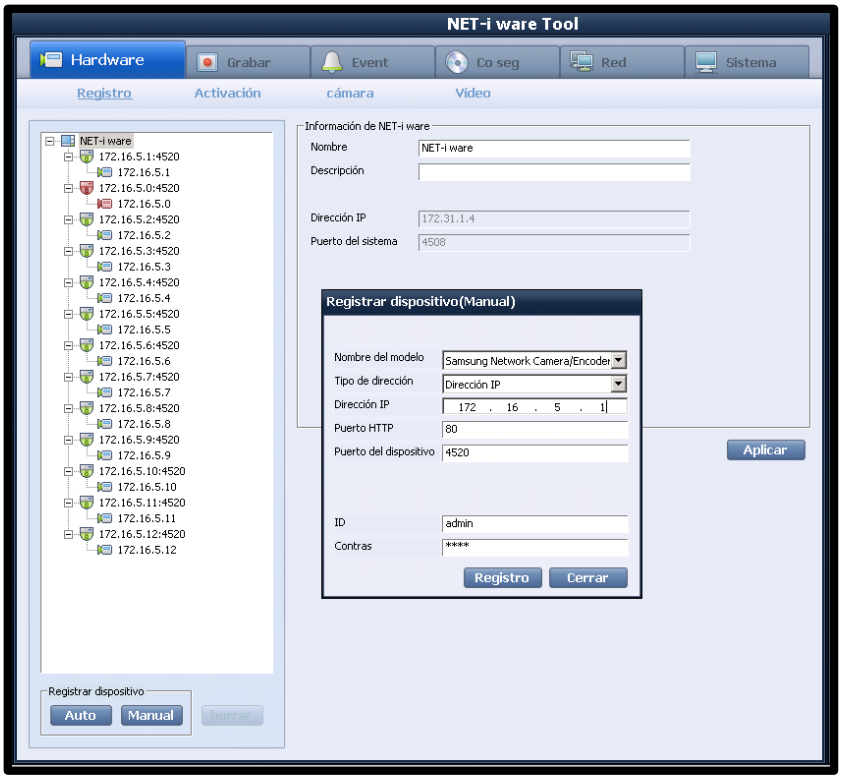


Figura 4.92: Pestaña Hardware con la opción Registro.

En la figura anterior se muestra la pestaña 'Hardware' con la opción 'Registro' que permite la inclusión de cámaras en el

NET-i Ware. En la esquina inferior izquierda tenemos dos opciones: 1) ‘Auto’ y 2) ‘Manual’. Se escogió la opción ‘Auto’ para que la inclusión de las cámaras sea rápida aunque si se desea agregar de manera manual una cámara, se da click en la opción ‘Manual’ y nos aparece una ventana con título ‘Registrar dispositivo(Manual)’ donde llenamos los campos correspondientes. Si se desea se le da un nombre y una descripción al software en los cuadros de texto que se encuentran justo por arriba de la ventana ‘Registrar dispositivo(Manual)’ de la figura anterior y posteriormente presionamos el botón ‘Aplicar’.

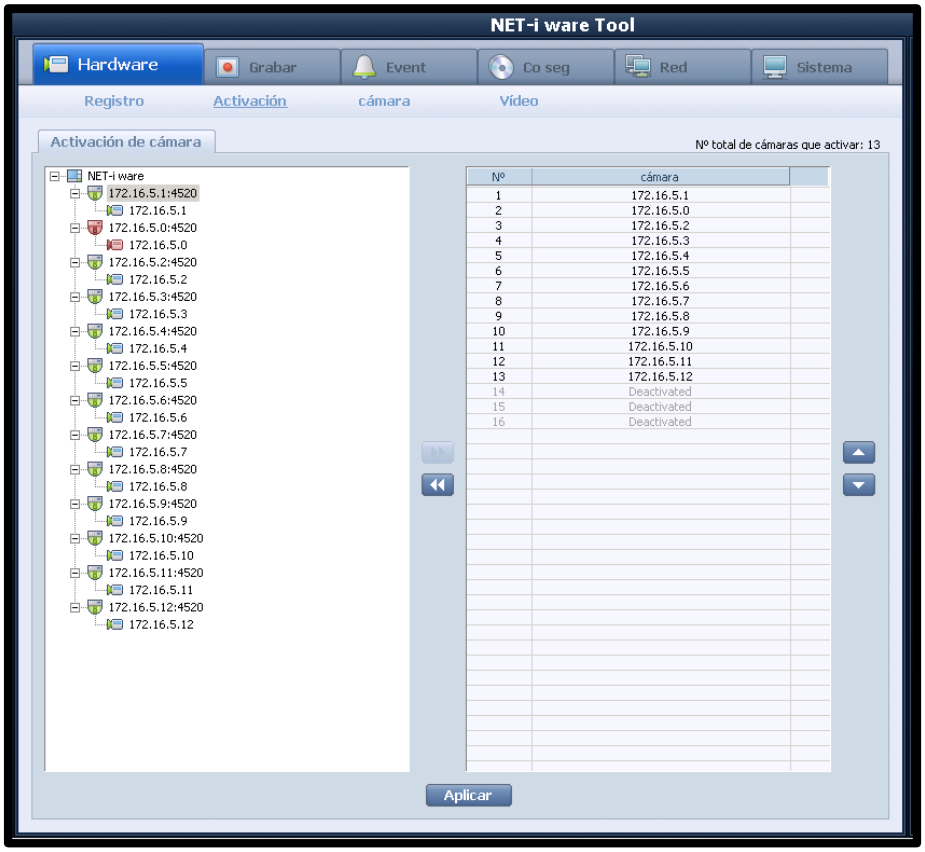


Figura 4.93: Pestaña Hardware con la opción Activación.

En la figura anterior se muestra la pestaña ‘Hardware’ con la opción ‘Activación’ que nos permite activar las cámaras dentro del software NET-i Ware. Esto quiere decir, que no es suficiente con incluir las cámaras, como lo hicimos en el párrafo anterior, también es necesario activarles. Esto se realiza seleccionando la cámara de la columna de la izquierda que se desea activar y pasarla a la columna de la derecha, presionando el botón “>>” que se encuentra en la mitad de ambas columnas. Luego presionamos el botón ‘Aplicar’.

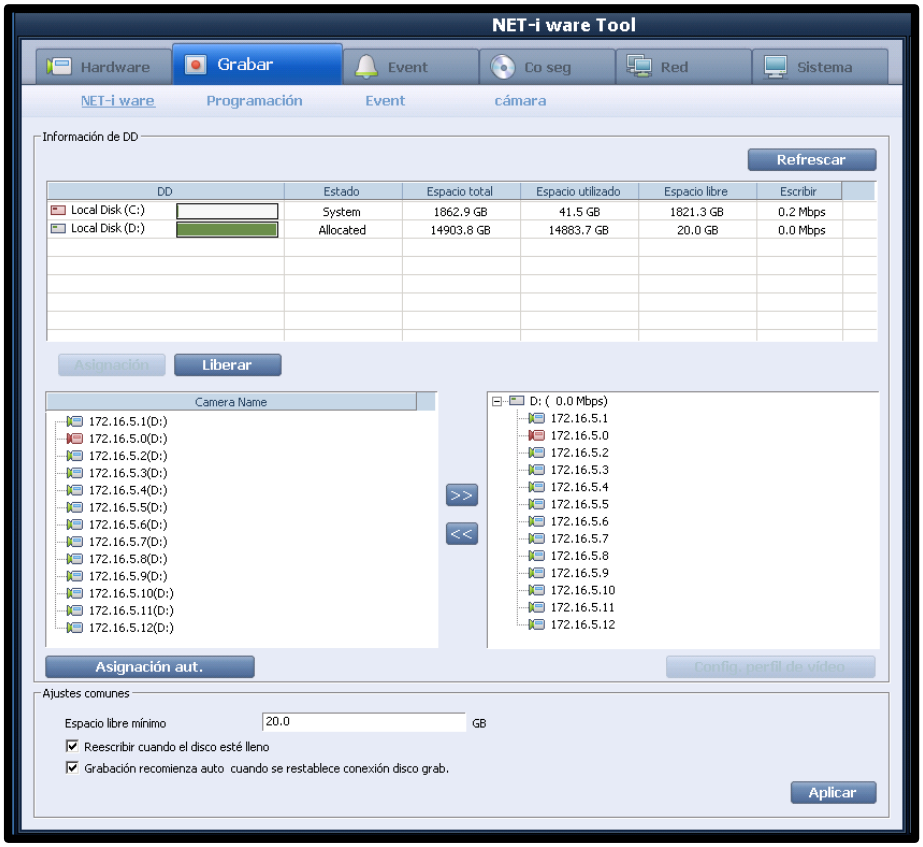


Figura 4.94: Pestaña Grabar con la opción NET-i Ware.

Ahora nos toca seleccionar el disco duro donde se grabará el video de las cámaras. En la figura anterior se muestra la pestaña ‘Grabar’ con la opción ‘NET-i Ware’. Al presionar el botón ‘Refrescar’ en la sección ‘Información de DD’ nos aparecen los dos discos duros disponibles para grabar el video de las cámaras. Cabe mencionar que antes de usar el servidor, se le pidió a un técnico que agregue un disco duro de casi 15 GB para poder ser el lugar donde se almacene el video que se encuentra en la unidad “D:”. Seleccionamos el disco “D:” y

presionamos el botón ‘Asignación’ que están un poco borrosas sus letras pero que se encuentra junto al botón ‘Liberar’. Debajo de la sección ‘Información de DD’ se encuentran dos columnas. Esto nos permite asignar cámaras al disco duro escogido, en este caso el disco “D:”. Hacemos el mismo procedimiento como lo hicimos con la pestaña ‘Hardware’ y la opción ‘Activación’. En la sección ‘Ajustes comunes’ configuramos los siguientes parámetros. En el parámetro ‘Espacio libre mínimo’ escribimos ’20 GB’, esto nos permite que nuestro disco duro siempre tenga ese espacio disponible, evitando que se encuentre completamente lleno. También marcamos las casillas ‘Reescribir cuando el disco duro esté lleno’ y ‘Grabación recomienza automáticamente cuando se reestablece conexión disco de grabación’.

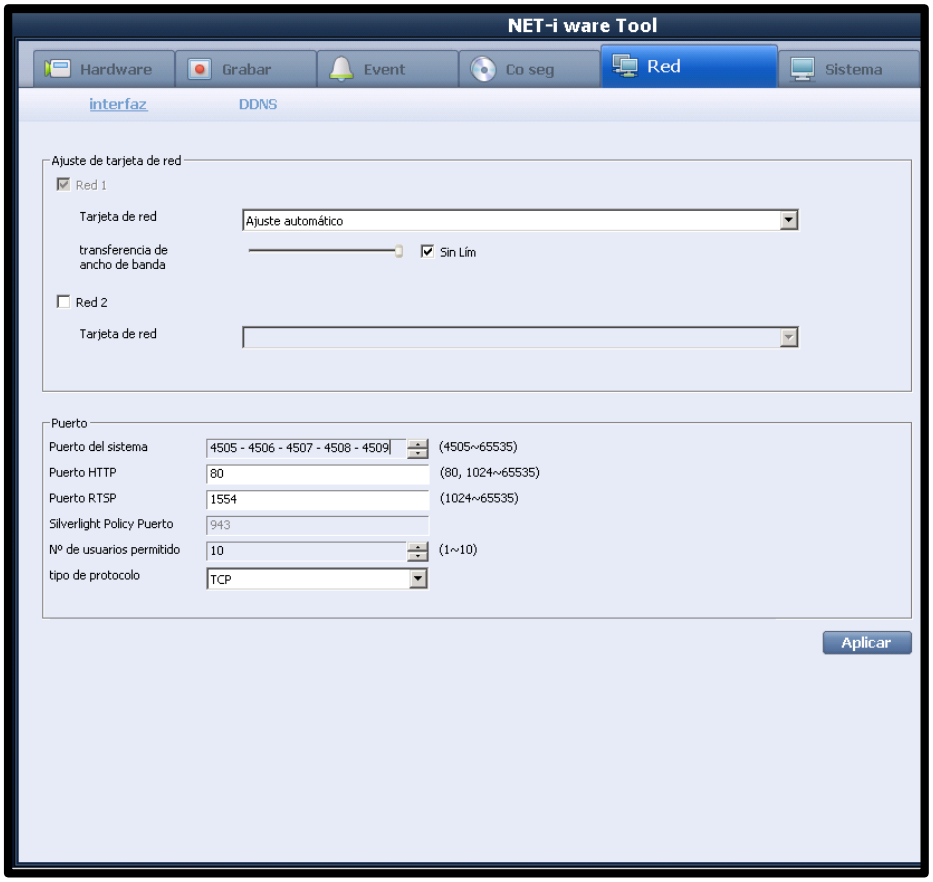


Figura 4.95: Pestaña Red con la opción Interfaz.

La pestaña ‘Red’ con la opción ‘Interfaz’ es mostrada en la figura anterior. En la sección ‘Ajuste de tarjeta de red’ escogemos ‘Ajuste automático’ en el parámetro ‘Tarjeta de red’. Esto nos permite que el software NET-i Ware identifique el direccionamiento IPv4 de la tarjeta de red de nuestro servidor. Marcamos la casilla ‘Sin Lim’ del parámetro ‘transferencia de ancho de banda’. En la sección ‘Puerto’ definimos solamente los puertos ‘80’ para el parámetro ‘Puerto HTTP’, ‘1554’ para el

parámetro ‘Puerto RTSP’ y ‘TCP’ para el parámetro ‘tipo de protocolo’. La explicación de estos puertos es la misma explicación que dimos a los puertos de las cámaras. Para guardar estos cambios presionamos el botón ‘Aplicar’.

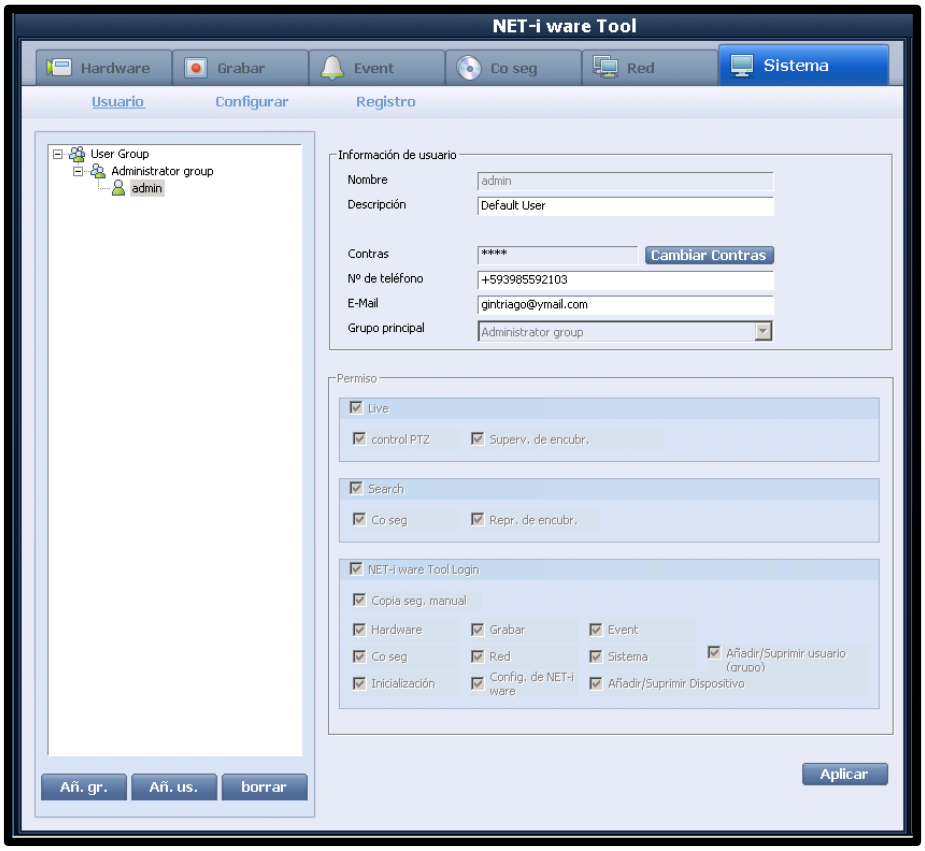


Figura 4.96: Pestaña Sistema con la opción Usuario.

Se configura el usuario ‘admin’ que viene por defecto en el software en la pestaña ‘Sistema’ con la opción ‘Usuario’ tal como lo muestra la figura anterior. Si se desea se agrega una descripción en el parámetro ‘Descripción’, en nuestro caso

hemos escrito ‘Default User’. Si presionamos el botón ‘Cambiar Contras’ podemos cambiar la contraseña de este usuario. Si se desea se agrega un número de teléfono y un correo en los parámetros ‘N° de teléfono’ y ‘E-Mail’. Para guardar estas configuraciones presionamos el botón ‘Aplicar’.

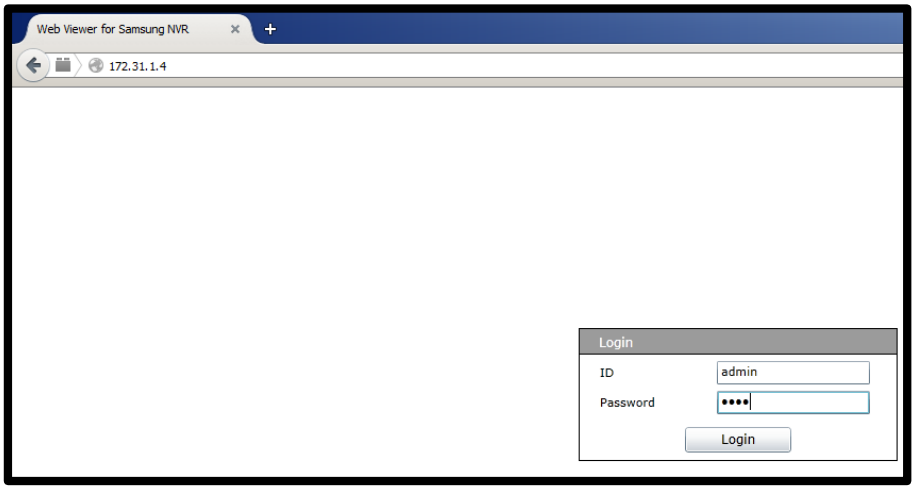


Figura 4.97: Inicio de sesión en Web Viewer.

Finalmente, para poder visualizar el video grabado por parte de las cámaras debemos escribir en la barra de URL de un browser la IP 172.31.1.4 y presionar enter. Luego de esto nos aparece el inicio de sesión, tal como lo muestra la figura anterior. El inicio de sesión se realiza mediante el ‘Web Viewer’ un visor web de la marca Samsung. Digitamos las credenciales, ID y password, que son las mismas credenciales con las que se accede al software NET-i Ware.

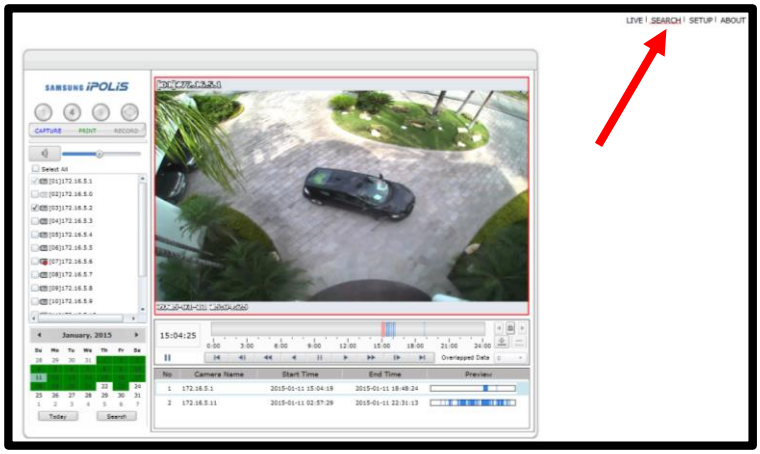


Figura 4.98: Pestaña Search del Web Viewer de Samsung.

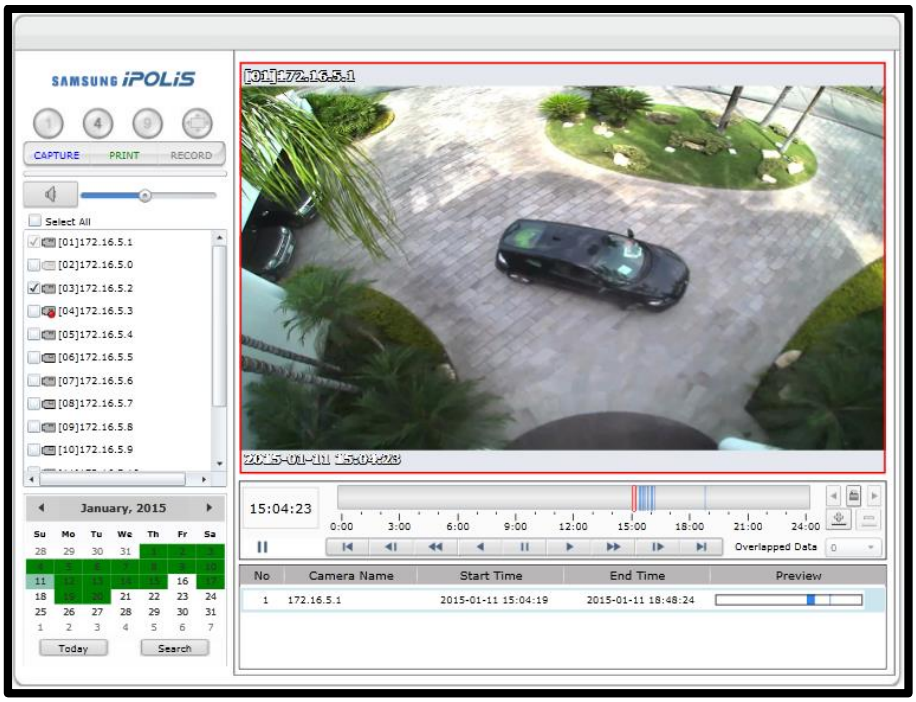


Figura 4.99: Visualización de la grabación de video.

Una vez iniciada la sesión debemos seleccionar la pestaña ‘Search’ que se encuentra en la esquina superior derecha tal como lo muestra la figura 4.98. La figura 4.99 muestra la

visualización de la grabación de video. La columna que se encuentra en la izquierda contiene a las cámaras. Se selecciona(n) la(s) casilla(s) dependiendo de la(s) cámara(s) de la(s) cual(es) se desea visualizar su(s) grabación(es). Posteriormente se presiona el botón ‘Search’ y se sombrean de verde los días donde existe grabación. Esto lo podemos apreciar en la esquina inferior izquierda de la figura 4.99. Justo debajo de la sección donde aparece el video, se encuentra una barra de tiempo que nos permite adelantar, retrasar, detener o poner play al video.

Ubicación en la vivienda

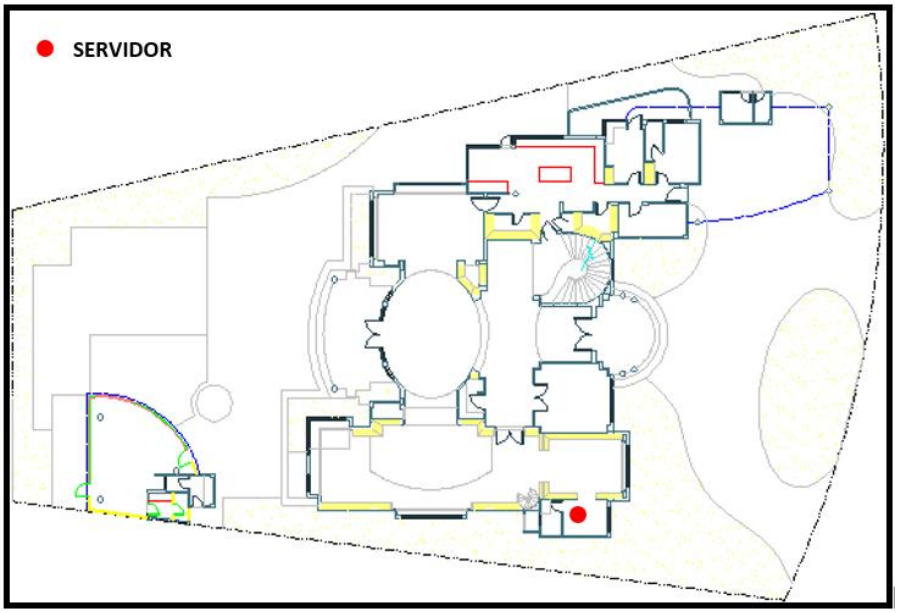


Figura 4.100: Ubicación del servidor en la planta baja.

Nuestro servidor se ubica en el estudio y debido a que posee la característica de ser rackeable, se coloca dentro del Rack 2. Esto se puede apreciar en la figura 4.45.

4.3.3. Escenas.

Las escenas son programaciones que permiten interactuar a los dispositivos domóticos entre sí y esa interacción se vuelve visible ante el usuario final proveyéndole, en nuestro caso, seguridad y confort.

Tanto las cámaras como el servidor no forman parte de la red Z-Wave por lo tanto no pueden ser configurados como parte de las escenas. A parte que esto es deseable, ya que así le proveemos de independencia a la grabación de video dentro de la vivienda. La grabación de video es muy importante porque permite tener pruebas visuales ante cualquier siniestro o eventualidad.

Es así que solamente los sensores de movimiento y los sensores de apertura y cerrado de puertas serán parte de nuestras escenas. Tal como se detalló en la sección 3.3.2, estos sensores buscan iluminar áreas durante la noche. Para que esto suceda, dentro de las escenas se los usará como

‘triggers’, es decir que darán inicio o darán por terminado una escena.

A continuación se describen las configuraciones necesarias para todas las escenas.

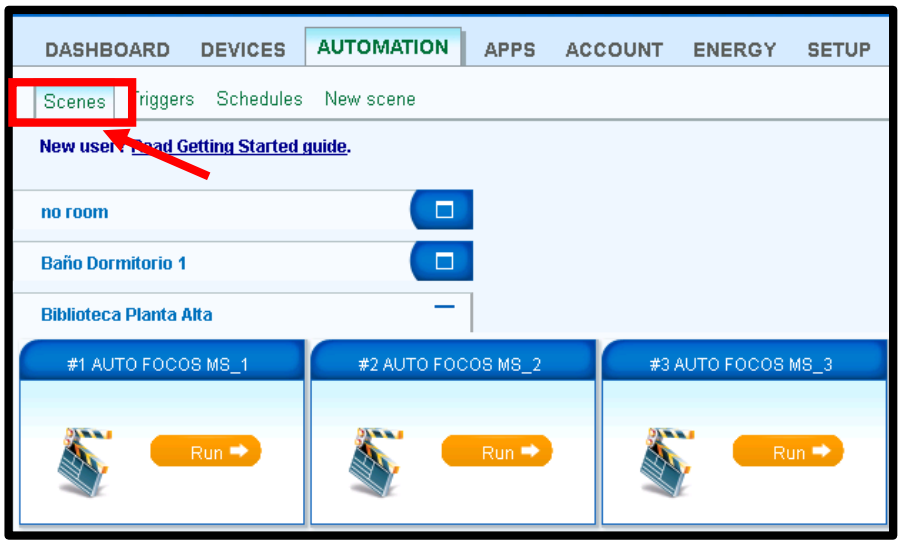


Figura 4.101: Pestaña Automation con la opción Scenes.

En la figura anterior se muestra la pestaña ‘Automation’ con la opción ‘Scenes’ de la interfaz gráfica del VERA3. Podemos apreciar tres de las escenas creadas en el sector ‘Biblioteca planta alta’.

Para crear una nueva escena seleccionamos la opción ‘New scene’ tal como lo muestra la figura anterior.

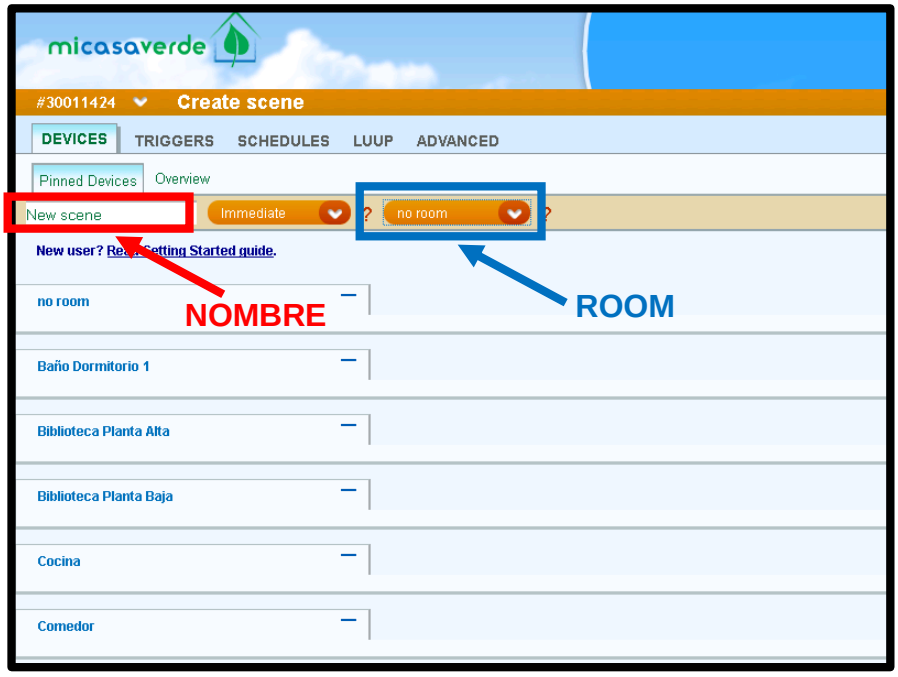


Figura 4.102: Ventana Create Scene con la pestaña Devices.

En la figura anterior se muestra la ventana 'Create scene' con la pestaña 'Devices' y opción 'Pinned Devices'. Los primeros parámetros para configurar en una escena son el 'nombre' y el 'room' tal como lo muestra la figura anterior.

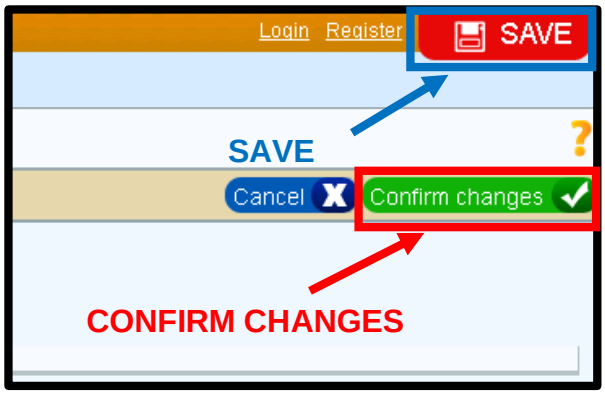


Figura 4.103: Opción de Confirm changes.

Para que cualquier cambio que se realice dentro de una escena sea guardado se debe presionar ‘Confirm changes’ como lo muestra la figura anterior. Y una vez presionado esta opción se debe presionar también la opción ‘Save’ en la esquina superior derecha como se lo mostró en párrafos anteriores.

El formato de nombres para cualquier escena es el siguiente, **“<#><número de escena en el room> <AUTO o ARM/DISARM> <ALL (opcional)> <Dispositivo principal 1> <Dispositivo principal 2 (opcional)> <trigger 1 (opcional)> <trigger 2 (opcional)> <Descripción (opcional)>”**.

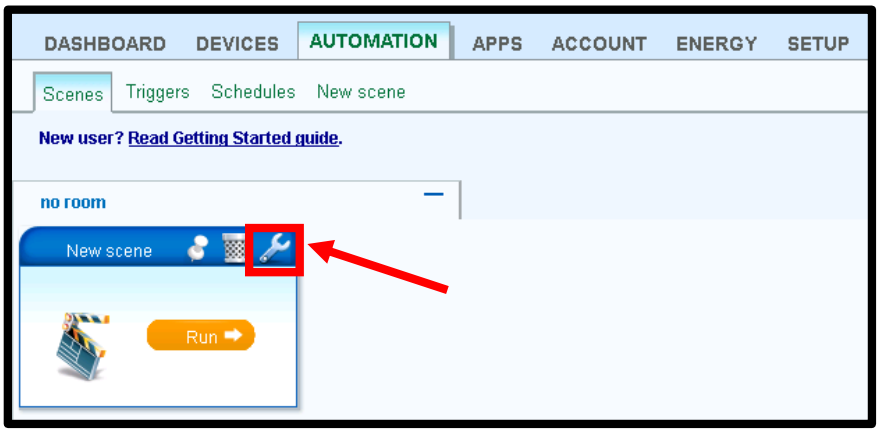


Figura 4.104: Nueva escena creada.

Una vez presionado ‘Confirm changes’ aparece la nueva escena creada en la interfaz gráfica. Para configurar la escena

presionamos la herramienta de tuercas tal como lo muestra la figura anterior.

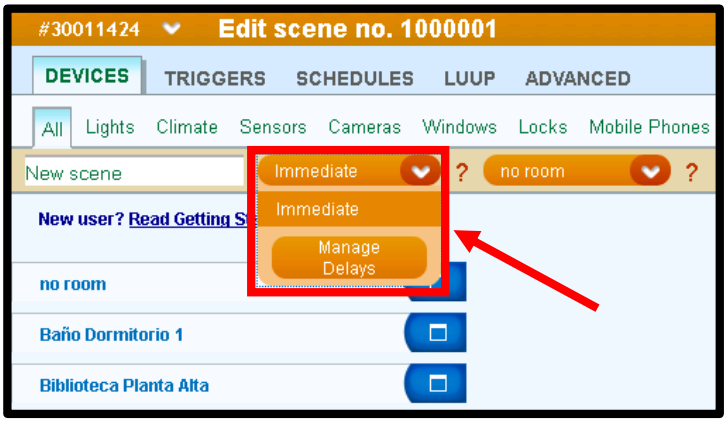


Figura 4.105: Retrasos de la escena.

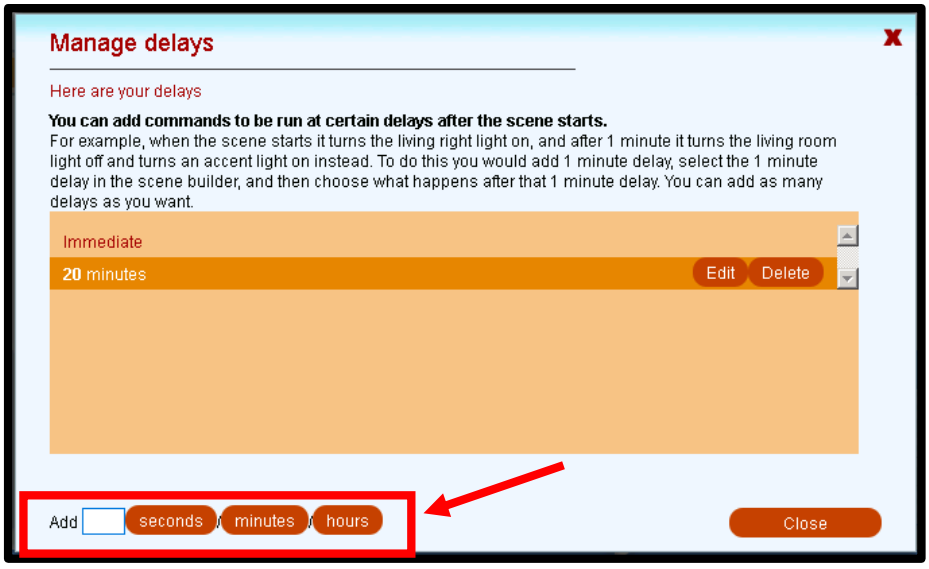


Figura 4.106: Ventana Manage delays.

En la penúltima figura se muestra la opción de retrasos de la escena, esto es, para escenas en las cuales se desea que ‘algo’

suceda a penas se active el ‘trigger’, y que luego de un tiempo se desea que ese ‘algo’ deje de pasar, sirve esta opción. Esto se entenderá mejor cuando se configura la escena de seguridad. En la última figura se muestra la edición o configuración de estos retrasos, que la interfaz gráfica del VERA3 los nombra como ‘Delays’. Se pueden agregar retrasos de segundos, minutos y horas. El único retraso que no se puede editar es ‘Inmediate’ porque este retraso permite iniciar la escena cuando se activa un ‘trigger’. Cualquier retraso agregado, sucederá obligadamente después del retraso ‘Inmediate’. El ‘cuanto después’ lo determina el tiempo asignado a dicho retraso.

Finalmente, antes de entrar en detalle con las escenas de la gestión de la seguridad, vamos a presentar las escenas que serán creadas en cada sector.

ESCENAS DE LA BIBLIOTECA PLANTA ALTA		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_1
2		#2 AUTO FOCOS MS_2
3		#3 AUTO FOCOS MS_3
4		#4 ARM/BYPASS MS_1
5		#5 ARM/BYPASS MS_2
6		#6 ARM/BYPASS MS_3
7	APERTURA Y CERRADO DE PUERTAS	#7 AUTO FOCOS DWS_6
8		#8 ARM/BYPASS DWS_6
9	TERMOSTATO	#9 AUTO TMTT_1 TMTT_1 UP
10		#10 AUTO TMTT_1 TMTT_1 DOWN
11		#11 AUTO TMTT_2 TMTT_2 UP
12		#12 AUTO TMTT_2 TMTT_2 DOWN
13	ACTUADORES DE PERSIANAS	#13 AUTO MMC_1
14		#14 AUTO MMC_2
15		#15 AUTO MMC_3
16		#16 AUTO MMC_4

Tabla 4.8: Escenas de la Biblioteca planta alta.

ESCENAS DE LA BIBLIOTECA PLANTA BAJA		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_4
2		#2 AUTO FOCOS MS_5
3		#3 AUTO FOCOS MS_6
4		#4 ARM/BYPASS MS_4
5		#5 ARM/BYPASS MS_5
6		#6 ARM/BYPASS MS_6
7	APERTURA Y CERRADO DE PUERTAS	#7 AUTO FOCOS DWS_7
8		#8 ARM/BYPASS DWS_7
9	TERMOSTATO	#9 AUTO TMTT_3 TMTT_3 UP
10		#10 AUTO TMTT_3 TMTT_3 DOWN
11	ACTUADORES DE PERSIANAS	#11 AUTO MMC_5
12		#12 AUTO MMC_6
13		#13 AUTO MMC_7
14		#14 AUTO MMC_8

Tabla 4.9: Escenas de la Biblioteca planta baja.

ESCENAS DEL BAÑO DORMITORIO 1		
	TIPO DE SENSOR	**ESCENAS**
1	APERTURA Y CERRADO DE PUERTAS	#1 AUTO FOCOS DWS_1
2		#2 AUTO FOCOS DWS_2
3		#3 AUTO FOCOS DWS_3
4		#4 AUTO FOCOS DWS_4
5		#5 AUTO FOCOS DWS_5
6		#6 ARM/BYPASS DWS_1
7		#7 ARM/BYPASS DWS_2
8		#8 ARM/BYPASS DWS_3
9		#9 ARM/BYPASS DWS_4
10		#10 ARM/BYPASS DWS_5
11	TERMOSTATO	#11 AUTO TMTT_4 TMTT_4 UP
12		#12 AUTO TMTT_4 TMTT_4 DOWN

Tabla 4.10: Escenas del Baño Dormitorio 1.

ESCENAS DEL ESTUDIO		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_7
2		#2 ARM/BYPASS MS_7
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_15
4		#4 ARM/BYPASS DWS_15
5	TERMOSTATO	#5 AUTO TMTT_12 TMTT_12 UP
6		#6 AUTO TMTT_12 TMTT_12 DOWN
7	ACTUADORES DE PERSIANAS	#7 AUTO MMC_16

Tabla 4.11: Escenas del Estudio.

ESCENAS DE LA SALA		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_8
2		#2 ARM/BYPASS MS_8
3	TERMOSTATO	#3 AUTO TMTT_14 TMTT_14 UP
4		#4 AUTO TMTT_14 TMTT_14 DOWN
5	ACTUADORES DE PERSIANAS	#5 AUTO MMC_17
6		#6 AUTO MMC_18

Tabla 4.12: Escenas de la Sala.

ESCENAS DEL PASILLO PLANTA ALTA		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_17
2		#2 ARM/BYPASS MS_17

Tabla 4.13: Escenas del Pasillo planta alta.

ESCENAS DEL PASILLO PLANTA BAJA		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_9
2		#2 ARM/BYPASS MS_9
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_16
4		#4 ARM/BYPASS DWS_16
5	TERMOSTATO	#5 AUTO TMTT_13 TMTT_13 UP
6		#6 AUTO TMTT_13 TMTT_13 DOWN

Tabla 4.14: Escenas del Pasillo planta baja.

ESCENAS DEL COMEDOR		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_10
2		#2 ARM/BYPASS MS_10
3	TERMOSTATO	#3 AUTO TMTT_6 TMTT_6 UP
4		#4 AUTO TMTT_6 TMTT_6 DOWN
5	ACTUADORES DE PERSIANAS	#5 AUTO MMC_9

Tabla 4.15: Escenas del Comedor.

ESCENAS DE LA COCINA		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_11
2		#2 ARM/BYPASS MS_11
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_8
4		#4 ARM/BYPASS DWS_8
5		#5 AUTO FOCOS DWS_9
6		#6 ARM/BYPASS DWS_9
7	TERMOSTATO	#7 AUTO TMTT_5 TMTT_5 UP
8		#8 AUTO TMTT_5 TMTT_5 DOWN

Tabla 4.16: Escenas de la Cocina.

ESCENAS DEL GARAJE		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_12
2		#2 ARM/BYPASS MS_12

Tabla 4.17: Escenas del Garaje.

ESCENAS DEL DORMITORIO 1		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_13
2		#2 ARM/BYPASS MS_13
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_10
4		#4 ARM/BYPASS DWS_10
5	TERMOSTATO	#5 AUTO TMTT_7 TMTT_7 UP
6		#6 AUTO TMTT_7 TMTT_7 DOWN
7	ACTUADORES DE PERSIANAS	#7 AUTO MMC_10
8		#8 AUTO MMC_11

Tabla 4.18: Escenas del Dormitorio 1.

ESCENAS DEL DORMITORIO 2		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_14
2		#2 ARM/BYPASS MS_14
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_11
4		#4 ARM/BYPASS DWS_11
5	TERMOSTATO	#5 AUTO TMTT_8 TMTT_8 UP
6		#6 AUTO TMTT_8 TMTT_8 DOWN
7	ACTUADORES DE PERSIANAS	#7 AUTO MMC_12

Tabla 4.19: Escenas del Dormitorio 2.

ESCENAS DEL DORMITORIO 3		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_15
2		#2 ARM/BYPASS MS_15
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_12
4		#4 ARM/BYPASS DWS_12
5	TERMOSTATO	#5 AUTO TMTT_9 TMTT_9 UP
6		#6 AUTO TMTT_9 TMTT_9 DOWN
7	ACTUADORES DE PERSIANAS	#7 AUTO MMC_13

Tabla 4.20: Escenas del Dormitorio 3.

ESCENAS DEL DORMITORIO 4		
	TIPO DE SENSOR	**ESCENAS**
1	MOVIMIENTO	#1 AUTO FOCOS MS_16
2		#2 ARM/BYPASS MS_16
3	APERTURA Y CERRADO DE PUERTAS	#3 AUTO FOCOS DWS_13
4		#4 ARM/BYPASS DWS_13
5	TERMOSTATO	#5 AUTO TMTT_10 TMTT_10 UP
6		#6 AUTO TMTT_10 TMTT_10 DOWN
7	ACTUADORES DE PERSIANAS	#7 AUTO MMC_14

Tabla 4.21: Escenas del Dormitorio 4.

ESCENAS DEL DORMITORIO MADRE		
	TIPO DE SENSOR	**ESCENAS**
1	APERTURA Y CERRADO DE PUERTAS	#1 AUTO FOCOS DWS_14
2		#2 ARM/BYPASS DWS_14
3	TERMOSTATO	#3 AUTO TMTT_11 TMTT_11 UP
4		#4 AUTO TMTT_11 TMTT_11 DOWN
5	ACTUADORES DE PERSIANAS	#5 AUTO MMC_15

Tabla 4.22: Escenas del Dormitorio Madre.

SEGURIDAD – SISTEMA HUE, SENSORES DE MOVIMIENTO, APERTURA Y CERRADO DE PUERTAS

Antes de entrar a los detalles de las escenas de la gestión de seguridad, es necesario indicar cuales serán los focos Hue

asociados a cada sensor de movimiento y a cada sensor de puerta.

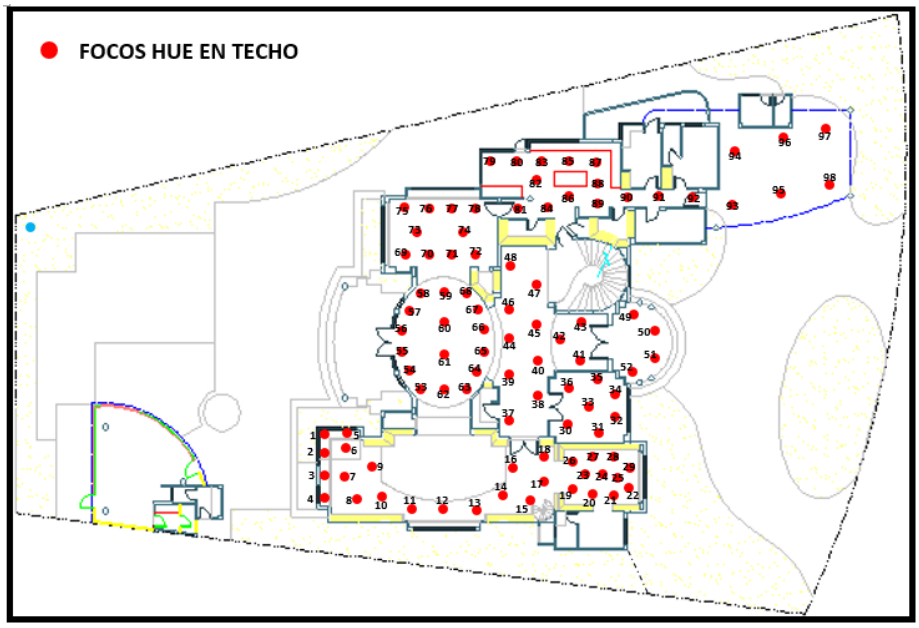


Figura 4.107: Ubicación de los focos Hue en la planta baja con identificador.

En la figura anterior se muestra la ubicación de los focos Hue en la planta baja de la vivienda con identificador del 1 al 98 que corresponde a la planta alta.

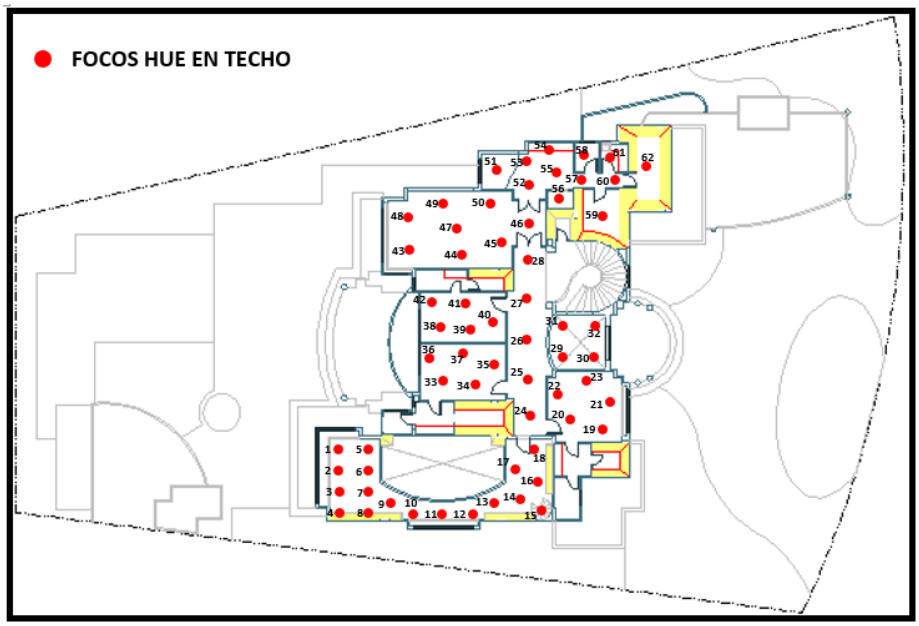


Figura 4.108: Ubicación de los focos Hue en la planta alta con identificador.

En la figura anterior se muestra la ubicación de los focos Hue en la planta alta de la vivienda con identificador del 1 al 62 que corresponde a la planta baja.

CORRESPONDENCIA FOCOS-SENSORES DE MOVIMIENTO			
	SECTOR	**NOMBRE**	**FOCOS**
1	BIBLIOTECA PLANTA ALTA	MS_1 BBPA 1 Mov	1-9 PA
2		MS_2 BBPA 2 Mov	10-12 PA
3		MS_3 BBPA 3 Mov	13-18 PA
4	BIBLIOTECA PLANTA BAJA	MS_4 BBPB 1 Mov	14-18 PB
5		MS_5 BBPB 2 Mov	11-13 PB
6		MS_6 BBPB 3 Mov	1-10 PB
7	ESTUDIO	MS_7 Estudio Mov	19-29 PB
8	SALA	MS_8 Sala Mov	53-68 PB
9	PASILLO PLANTA BAJA	MS_9 PasilloPB Mov	37-48 PB
10	COMEDOR	MS_10 Comedor Mov	69-78 PB
11	COCINA	MS_11 Cocina Mov	79-92 PB
12	GARAJE	MS_12 Garaje Mov	93-98 PB
13	DORMITORIO 1	MS_13 Dormitorio1 Mov	43-50 PA
14	DORMITORIO 2	MS_14 Dormitorio2 Mov	38-42 PA
15	DORMITORIO 3	MS_15 Dormitorio3 Mov	33-36 PA
16	DORMITORIO 4	MS_16 Dormitorio4 Mov	19-23 PA
17	PASILLO PLANTA ALTA	MS_17 PasilloPA Mov	24-28 PA

Tabla 4.23: Correspondencia Focos-Sensores de Movimiento.

CORRESPONDENCIA FOCOS-SENSORES DE APERTURA Y CERRADO DE PUERTAS			
	SECTOR	**NOMBRE**	**FOCOS**
1	BAÑO DORMITORIO 1	DWS_1 BañoDormitorio1	51-57,60 PA
2		DWS_2 BañoDormitorio1	58 PA
3		DWS_3 BañoDormitorio1	61 PA
4		DWS_4 BañoDormitorio1	62 PA
5		DWS_5 BañoDormitorio1	59 PA
6	BIBLIOTECA PLANTA ALTA	DWS_6 BBPA	13-18 PA
7	BIBLIOTECA PLANTA BAJA	DWS_7 BBPB	14-18 PB
8	COCINA	DWS_8 Cocina	79-89 PB
9		DWS_9 Cocina	90-92 PB
10	DORMITORIO 1	DWS_10 Dormitorio1	43-50 PA
11	DORMITORIO 2	DWS_11 Dormitorio2	38-42 PA
12	DORMITORIO 3	DWS_12 Dormitorio3	33-37 PA
13	DORMITORIO 4	DWS_13 Dormitorio4	19-23 PA
14	DORMITORIO MADRE	DWS_14 DormitorioMadre	30-36 PB
15	ESTUDIO	DWS_15 Estudio	19-29 PB
16	PASILLO PLANTA BAJA	DWS_16 PasilloPB	41-43 PB

Tabla 4.24: Correspondencia Focos-Sensores de apertura y cerrado de puertas.

Las premisas bajo las cuales creamos las escenas en esta parte son las siguientes: 1) ‘noche’ corresponde al intervalo de tiempo, después de las 6 de la tarde y antes de las 6 de la mañana, 2) ‘día’ corresponde al intervalo de tiempo, después de las 6 de la mañana y antes de las 6 de la tarde, 3) no encender luces a través de los sensores en la mañana, 4) en la noche, cuando se active un sensor de movimiento, dejará encendidas sus respectivas luces por 20 minutos y cuando se active un sensor de apertura y cerrado de puertas, dejará encendidas sus respectivas luces por 5 minutos, 5) en la noche, cuando se active un sensor de puertas, dejará encendidas sus respectivas luces por 5 minutos, 6) tanto los sensores de movimiento y los sensores de apertura y cerrado de puertas funcionarán como triggers y 7) los focos actuarán como dispositivos principales.

Escena para los sensores de movimiento

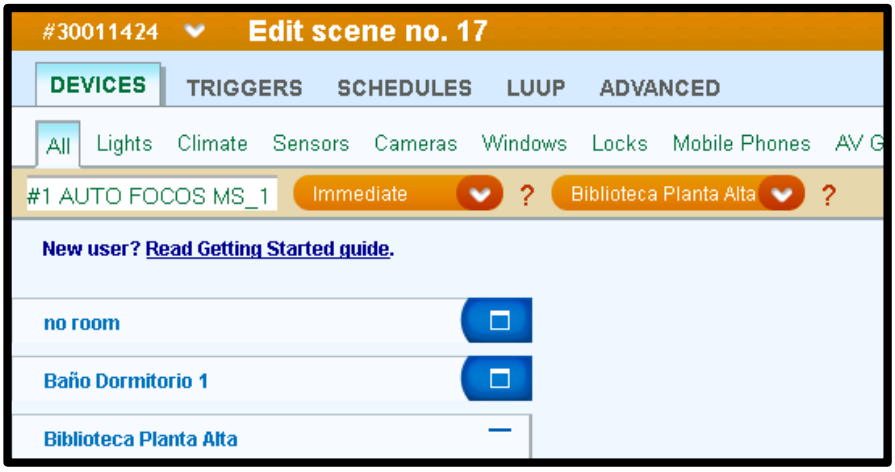


Figura 4.109: Escena para los sensores de movimiento con retraso Inmediate.

Vamos a mostrar la edición de una escena de manera general para los sensores de movimiento ya que esta se repite en todos los sectores donde existan este tipo de sensores. En la figura anterior, tomamos como ejemplo a los focos del trigger ‘MS_1’ que se encuentra en la Biblioteca Planta Alta. Seleccionamos como retraso a ‘Inmediate’. Recordamos que inmediate funcionará a penas los sensores de movimiento detecten movimiento.

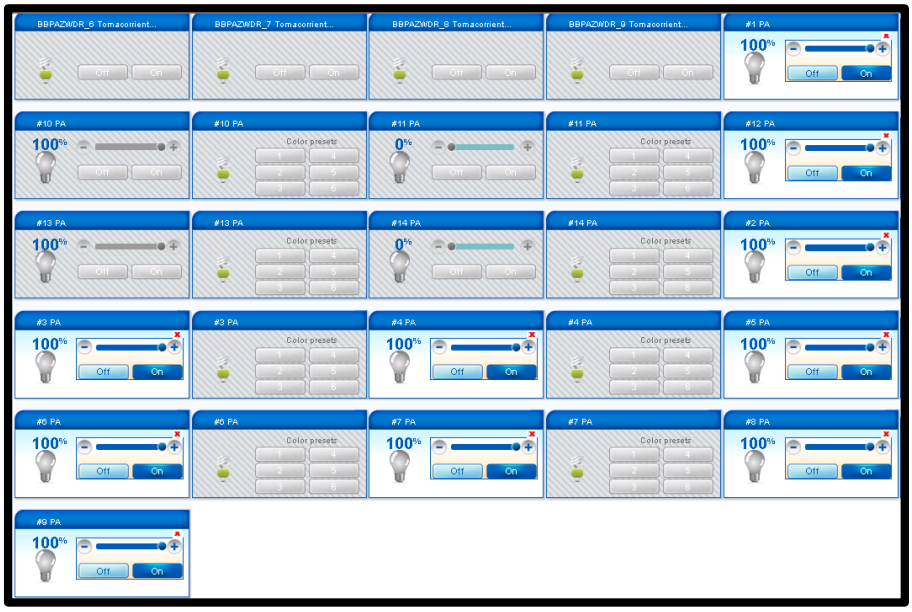


Figura 4.110: Prender focos del 1 al 9 PA en el retraso Inmediate.

En la figura anterior se muestran los focos del 1 al 9 PA en el retraso Inmediate. Se nota que se escoge en todos los focos, la opción ‘ON’ que permite encender los focos a penas (inmediate) detecte movimiento el sensor.

Figura 4.111: Escena para los sensores de movimiento con retraso de 20 minutos.

Debido a que las escenas de los sensores movimientos duran 20 minutos, debemos crear un retraso de 20 minutos tal como lo muestra la figura anterior.

Figura 4.112: Apagar focos del 1 al 9 PA en el retraso de 20 min.

En la figura anterior se muestran los focos del 1 al 9 PA en el retraso de 20 minutos. Se nota que se escoge en todos los focos, la opción ‘OFF’ que permite apagar los focos luego de 20 minutos que se detectó el movimiento a través del sensor.

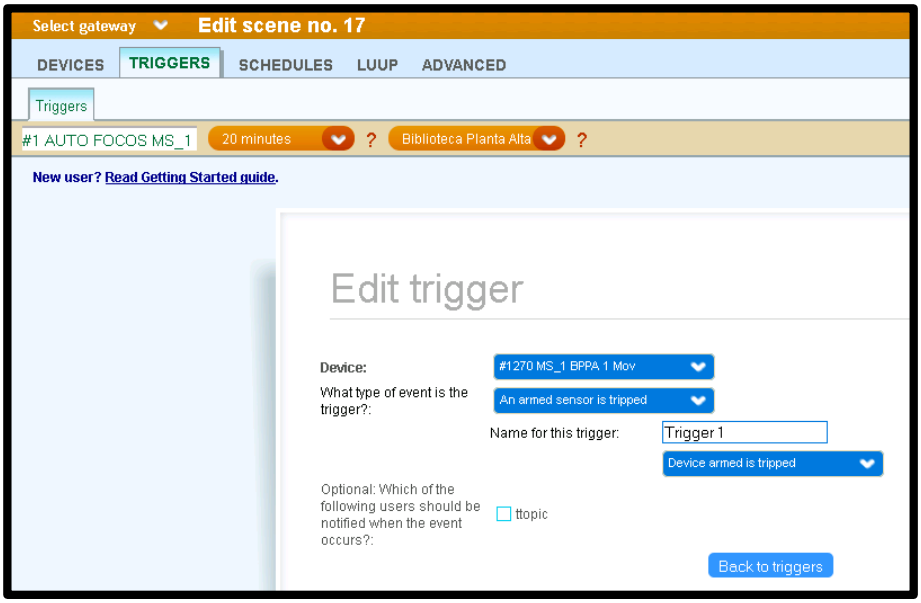


Figura 4.113: Pestaña TRIGGERS con la opción Triggers.

Luego, configuramos como trigger al sensor de movimiento tal como lo muestra la figura anterior. En el campo 'Device' escogemos el sensor de movimiento. En el parámetro 'What type of event is the trigger?', escogemos 'An armed sensor is tripped', esto indica que solo se detectará movimiento cuando la opción 'ARM' del sensor esté activada. Esto nos permitirá que sólo se prendan los focos en el horario establecio y se explicará más adelante. En el parámetro 'Name for this trigger' escribimos un nombre para este trigger, en nuestro caso, 'Trigger 1'. Debajo, escogemos la opción 'Device armed is tripped'; esto nos permite indicar que la escena empiece cuando se detecte movimiento. Presionamos 'Confirm Changes'.

Hasta el momento, pareciera que ya tenemos la escena configurada pero no es así. Necesitamos que la detección de movimiento y el encendido de las luces sea solamente en la noche. Para esto va a ser necesaria otra escena que nos permite activar o colocar en ‘ARM’ a los sensores en la noche y desactivar o colocar en ‘BYPASS’ a los sensores en el día.

Figura 4.114: Escena para activar/desactivar los sensores de movimiento.

La figura anterior muestra la escena para activar/desactivar los sensores de movimiento.

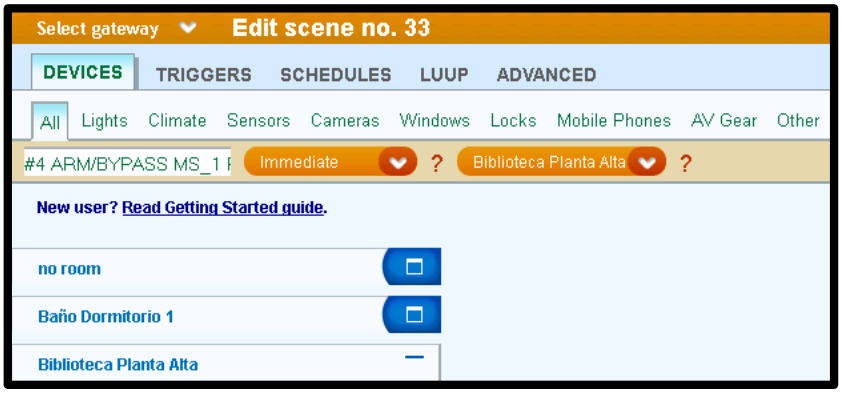


Figura 4.115: Escena para activar/desactivar los sensores de movimiento con retraso Inmediate.

Figura 4.116: Opción Arm del sensor de movimiento escogida en el retraso Inmediate.

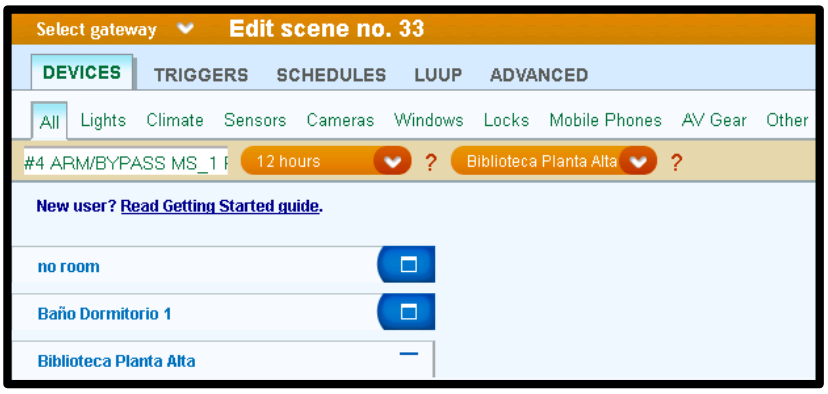


Figura 4.117: Escena para activar/desactivar los sensores de movimiento con retraso de 12 horas.

Figura 4.118: Opción Bypass del sensor de movimiento escogida en el retraso de 12 horas.

Con las cuatro figuras anteriores es fácil entender lo que se ha buscado realizar. Cuando estamos en el retraso ‘Inmediate’, activamos al sensor al seleccionar la opción ‘ARM’. Cuando estamos en el retraso ‘12 horas’, desactivamos al sensor al seleccionar la opción ‘BYPASS’. Pero nos falta darle un inicio a todo esto porque hasta hora, la escena sabe que a lo que inicia debe activar el sensor y luego de 12 horas debe desactivarlo; lo que no sabe es a qué hora específica del día debe iniciar. No sabe cual es el punto de partida. Es ahí donde debemos configurar un ‘Horario’ o ‘Schedule’ en inglés.

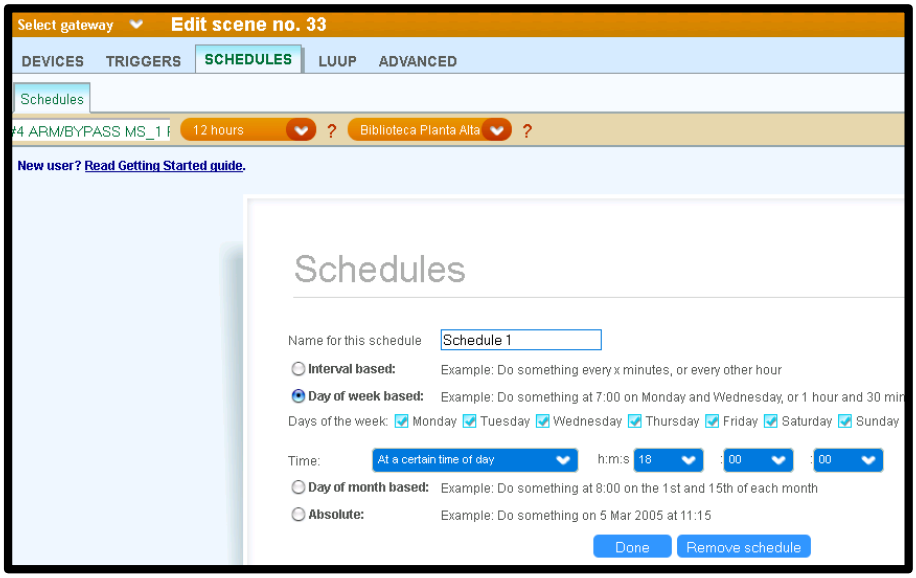


Figura 4.119: Configuración de Schedule para la escena que activa/desactiva los sensores de movimiento.

En la figura anterior, se muestra la pestaña ‘SCHEDULES’ con la opción ‘Schedules’. En el parámetro, ‘Name for this schedule’ escribimos un nombre para este Schedule, en nuestro caso, ‘Schedule 1’. Escogemos la opción ‘Day of week based’ y marcamos la casilla de todos los días. En el parámetro ‘Time’, escogemos, ‘At a certain time of day’ con la hora ’18:00:00’. Seleccionamos ‘Done’ y luego ‘Confirm changes’. Una vez configurado nuestro Schedule, aseguramos que todos los días a las seis de la tarde, activemos nuestro sensor de movimiento y a las seis de la mañana lo desactivemos. Desactivado nuestro sensor, este no podrá iniciar ninguna escena.

Escena para los sensores de apertura y cerrado de puertas

Gracias a que en los párrafos anteriores, explicamos a detalle el funcionamiento de las escenas para los sensores de movimiento, se nos hará más fácil poder explicar el funcionamiento de las escenas de aquí en adelante.

Figura 4.120: Escena para los sensores de apertura y cerrado de puertas.

La figura anterior muestra la escena para los sensores de apertura y cerrado de puertas. En este caso, haremos la escena con el sensor ‘DWS_6’ que pertenece a la Biblioteca planta alta.

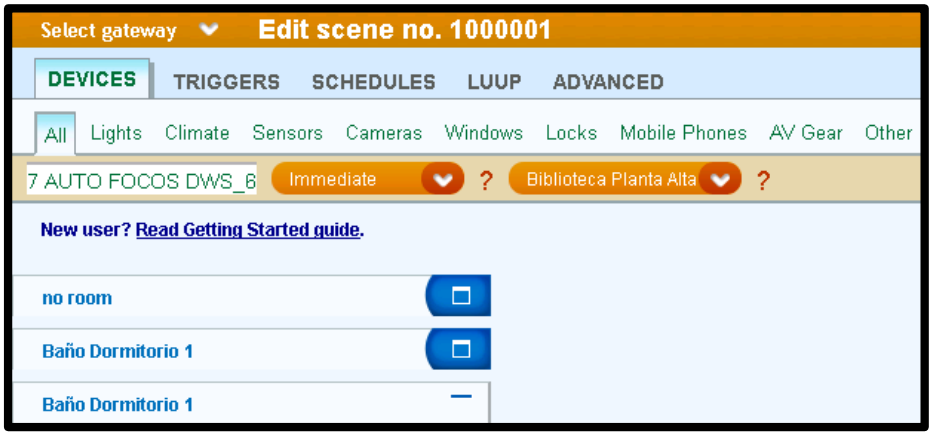


Figura 4.121: Escena para los sensores de apertura y cerrado de puertas con retraso Inmediate.

Se muestra la escena para los sensores de apertura y cerrado de puertas con retraso Inmediate en la figura anterior.

Figura 4.122: Encender focos del 13 al 18 PA en el retraso Inmediate.

En la figura anterior se muestran los focos del 13 al 18 PA en el retraso Inmediate. Se nota que se escoge en todos los focos, la opción ‘ON’ que permite encender los focos a penas (inmediate) detecte la apertura de la puerta el sensor.

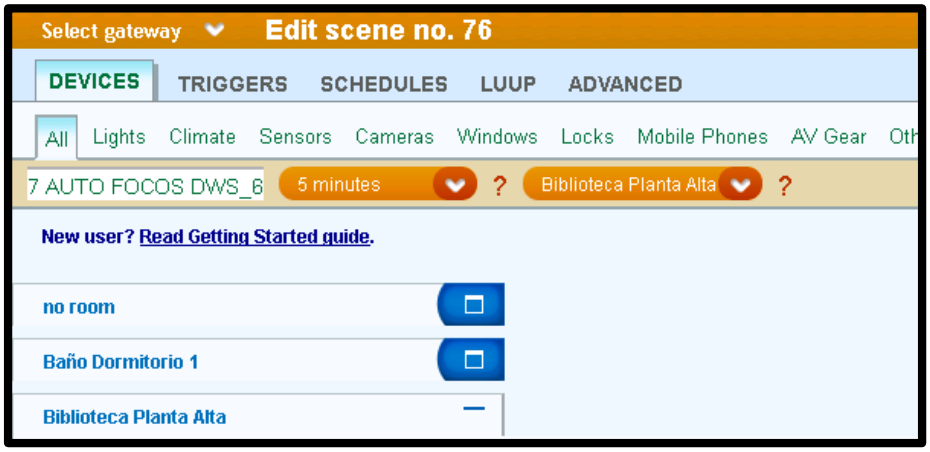


Figura 4.123: Escena para los sensores de apertura y cerrado de puertas con retraso de 5 min.

Debido a que las escenas de los sensores de apertura y cerrado de puertas duran 5 minutos, debemos crear un retraso de 5 minutos tal como lo muestra la figura anterior.

Figura 4.124: Apagar focos del 13 al 18 PA en el retraso 5 min.

En la figura anterior se muestran los focos del 13 al 18 PA en el retraso de 5 minutos. Se nota que se escoge en todos los focos,

la opción ‘OFF’ que permite apagar los focos luego de 20 minutos que se detectó el movimiento a través del sensor.

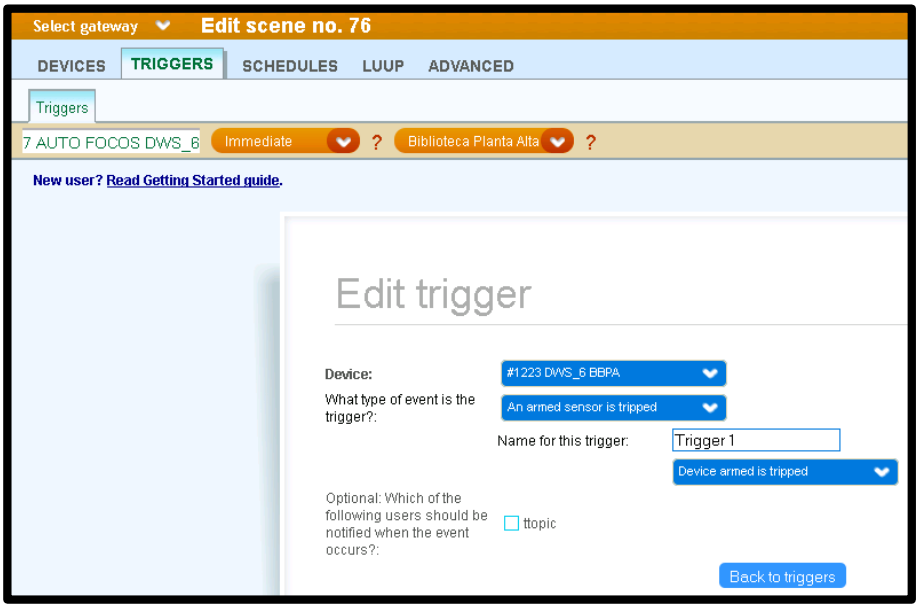


Figura 4.125: Pestaña TRIGGERS con la opción Triggers.

Luego, configuramos como trigger al sensor de apertura y cerrado de puertas tal como lo muestra la figura anterior. En el campo ‘Device’ escogemos el sensor de apertura y cerrado de puertas. En el parámetro ‘What type of event is the trigger?’, escogemos ‘An armed sensor is tripped’, esto indica que solo se detectará movimiento cuando la opción ‘ARM’ del sensor esté activada. Esto nos permitirá que sólo se prendan los focos en el horario establecido y se explicará más adelante. En el parámetro ‘Name for this trigger’ escribimos un nombre para

este trigger, en nuestro caso, ‘Trigger 1’. Debajo, escogemos la opción ‘Device armed is tripped’; esto nos permite indicar que la escena empiece cuando se detecte movimiento. Presionamos ‘Confirm Changes’.

Hasta el momento, pareciera que ya tenemos la escena configurada pero no es así. Necesitamos que la detección de movimiento y el encendido de las luces sea solamente en la noche. Para esto va a ser necesaria otra escena que nos permite activar o colocar en ‘ARM’ a los sensores en la noche y desactivar o colocar en ‘BYPASS’ a los sensores en el día.

Figura 4.126: Escena para activar/desactivar los sensores de apertura y cerrado de puertas.

La figura anterior muestra la escena para activar/desactivar los sensores de apertura y cerrado de puertas.

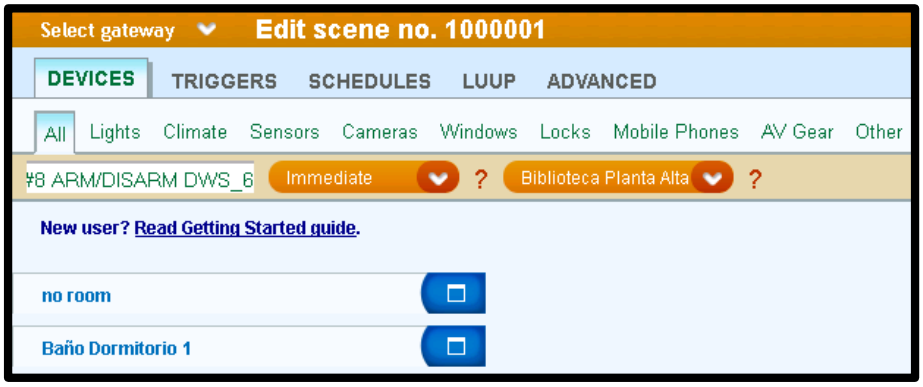


Figura 4.127: Escena para activar/desactivar los sensores de apertura y cerrado de puertas con retraso Inmediate.

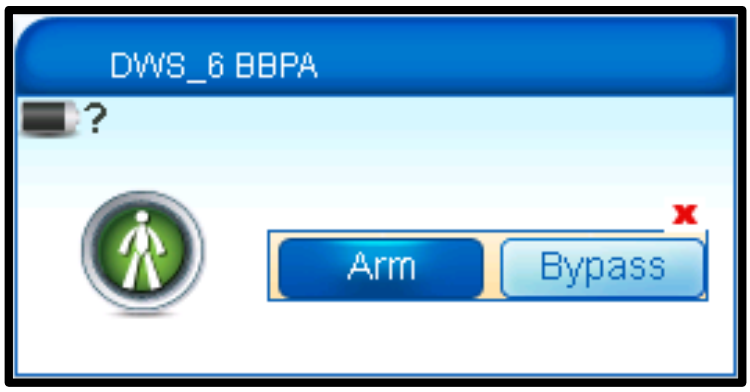


Figura 4.128: Opción Arm del sensor de apertura y cerrado de puertas escogida en el retraso Inmediate.

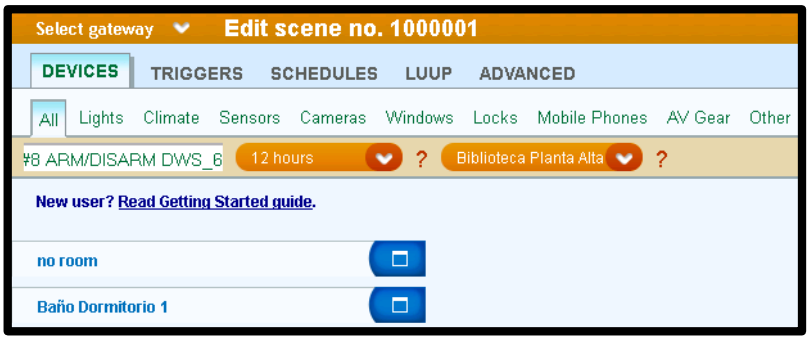


Figura 4.129: Escena para activar/desactivar los sensores de apertura y cerrado de puertas con retraso de 12 horas.

Figura 4.130: Opción Bypass del sensor de apertura y cerrado de puertas escogida en el retraso de 12 horas.

Con las cuatro figuras anteriores es fácil entender lo que se ha buscado realizar. Cuando estamos en el retraso ‘Inmediate’, activamos al sensor al seleccionar la opción ‘ARM’. Cuando estamos en el retraso ‘12 horas’, desactivamos al sensor al seleccionar la opción ‘BYPASS’. Pero nos falta darle un inicio a todo esto porque hasta hora, la escena sabe que a lo que inicia debe activar el sensor y luego de 12 horas debe desactivarlo; lo que no sabe es a qué hora específica del día debe iniciar. No sabe cual es el punto de partida. Es ahí donde debemos configurar un ‘Horario’ o ‘Schedule’ en inglés.

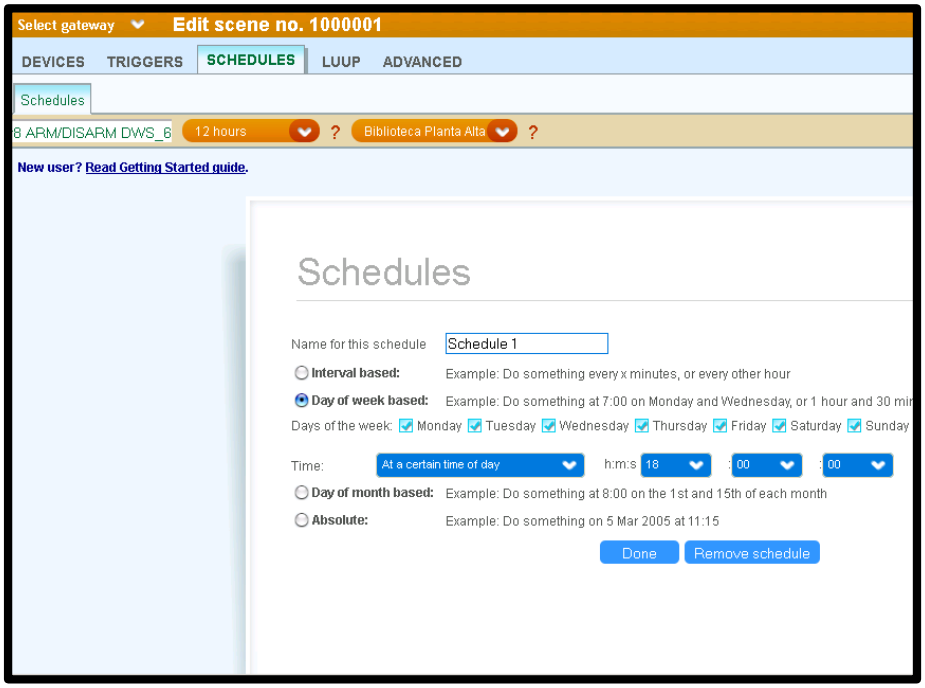


Figura 4.131: Configuración de Schedule para la escena que activa/desactiva los sensores de apertura y cerrado de puertas.

En la figura anterior, se muestra la pestaña ‘SCHEDULES’ con la opción ‘Schedules’. En el parámetro, ‘Name for this schedule’ escribimos un nombre para este Schedule, en nuestro caso, ‘Schedule 1’. Escogemos la opción ‘Day of week based’ y marcamos la casilla de todos los días. En el parámetro ‘Time’, escogemos, ‘At a certain time of day’ con la hora ’18:00:00’. Seleccionamos ‘Done’ y luego ‘Confirm changes’. Una vez configurado nuestro Schedule, aseguramos que todos los días a las seis de la tarde, activemos nuestro sensor de apertura y cerrado de puertas y a las seis de la mañana lo desactivemos.

Desactivado nuestro sensor, este no podrá iniciar ninguna escena.

4.4. Diseño del sistema domótico para la gestión del confort.

4.4.1. Dispositivos.

HUE PHILIPS

HUE Philips Bulbs and Controller

Figura 4.132: Controlador y focos HUE Philips.

Descripción

El sistema HUE PHILIPS [76] consta de 3 partes principales: 1) focos, 2) controlador y 3) aplicación. Hue cobra vida en las bombillas LED inalámbricas. Ofrecen una gran luminosidad. Todos los tonos de blanco. Y todos los colores del espectro. No

solo se ven fantásticas. También son prácticas. Se atenúan. Parpadean. Envían impulso. Hacen prácticamente cualquier cosa que tú desees. Y se pueden enroscar en los portalámparas actuales. El controlador es el núcleo del sistema HUE. El puente es literalmente un puente entre la aplicación y las bombillas. Vinculado a Wi-Fi a través de tu punto de acceso inalámbrico, puede conectar hasta 50 focos a la vez. Otra de sus funciones es conectar tu sistema con el mundo exterior. Te permite controlar tus luces a distancia o vincularlas con el resto de la web, fuentes de noticias o incluso tu bandeja de entrada. Es realmente muy inteligente [74]. La aplicación depende más bien del usuario, se puede utilizar la aplicación propia del sistema HUE Philips o desarrollar una que los permita utilizarlos. En nuestro caso, los HUE Philips y los controladores se configurarán a través de la aplicación de la compañía Philips y serán luego usados por el VERA3 [75]. Las especificaciones se muestran a continuación [75].

Especificaciones Focos

- Protocolo de comunicación: Zigbee
- Frecuencia del protocolo: 2.4 GHz
- 9 W de consumo de potencia

- 15000 horas de vida útil
- Voltaje de entrada: 120 VAC @ 50-60 Hz
- Hasta 600 lúmenes
- Hasta 16 millones de colores

Especificaciones Controlador

- Protocolo de comunicación: Zigbee
- Frecuencia del protocolo: 2.4-2.4835 GHz
- Puede manejar hasta 50 focos
- Consumo de corriente: Hasta 600mA
- Dimensiones: 100mm de diámetro y 25 mm de altura
- Voltaje de entrada: 5 VDC @ 50-60 Hz

ACTUADORES DE PERSIANAS

Aeon Labs DSC14104-ZWUS - Z-Wave Micro Motor Controller

Figura 4.133: Actuador de persiana de la marca Aeon Labs.

Descripción

El actuador de persianas [78] de Aeon Labs es un controlador de motor Z-Wave de bajo costo utilizado específicamente para permitir comandar mediante este protocolo el control del motor de la persiana a través de 3 cables: 2 de línea y 1 neutro. También puede reportar el consumo de potencia inmediato o el uso de energía kWh durante un período de tiempo [77]. Las especificaciones se muestran a continuación [77].

Especificaciones

- Protocolo de comunicación: Z-Wave
- Frecuencia del protocolo: 908.42 MHz
- Voltaje de entrada: 90-260 VAC @ 50-60 Hz
- Corriente de salida: 2.5 Amperios de corriente alterna
- Alcance de señal desde el controlador: 15 metros
- Temperatura de operación: De 0 a 40 ºC
- Humedad de operación: 95%
- Dimensiones AnxProfxAl: 52mm x 49mm x 18.5mm

TERMOSTATOS

Honeywell YTH8320ZW1007/U Z-Wave

Figura 4.134: Termostato de la marca Honeywell.

Descripción

Este termostato [79] de la marca Honeywell se puede integrar con otros dispositivos de automatización del hogar. Puede ser configurado para satisfacer prácticamente cualquier requisito de programación. El dueño de casa puede poner el termostato en un modo de ahorro de energía. Gran pantalla retroiluminada, con un área de visualización de 10 pulgadas-cuadrada. Permite al consumidor personalizar fácilmente el termostato. Menú de programación guía al usuario a través del proceso de programación ya que sólo muestra la información y opciones necesarias en cada pantalla. Posee un reloj de tiempo real. Mantiene el tiempo durante un corte de energía y actualizará automáticamente la hora al horario de verano. La línea de soporte técnico está en el paquete y en el manual de instalación [79]. Las especificaciones se muestran a continuación [79].

Especificaciones

- Protocolo de comunicación: Z-Wave
- Frecuencia del protocolo: 908.42 MHz
- Peso: 1.43 libras
- Dimensiones AnxProfxAl: 166mm x 36mm x 125mm

- Voltaje de entrada: 18 a 30 VAC
- Frecuencia de operación: 50 a 60 Hz
- Elemento de medición: Termistor
- Terminales disponibles: R, RC, Y, Y2, G, C, W-O/B, E, AUX, K
- Rango de temperatura: 4.5 a 32 °C para calentamiento; 10 a 37 °C para enfriamiento
- Tipos de sistema: 1H/1C, 2H/1C, 2H/2C, 1H/2C, 2H/2C, 3H/2C.
- Error de +/- 1 °C para la temperatura seteada

4.4.2. Configuración.

HUE PHILIPS

PLAN IPv4 DE LOS CONTROLADORES HUE		
	SECTOR	IP
1	Biblioteca Planta Alta	172.16.0.2
2	Biblioteca Planta Baja	172.16.0.3
3	Estudio	172.16.0.4
4	Dormitorio 1	172.16.0.5
5	Dormitorio 2	172.16.0.6
6	Dormitorio 3	172.16.0.7
7	Dormitorio 4	172.16.0.8
8	Dormitorio Madre	172.16.0.9
9	Baño Dormitorio 1	172.16.0.10
10	Cocina	172.16.0.11
11	Sala	172.16.0.12
12	Comedor	172.16.0.13
13	Pasillo planta baja	172.16.0.14
14	Jardines frente derecha	172.16.0.29
15	Jardines lateral sur	172.16.0.20
16	Pasillo planta alta	172.16.0.23
17	Garaje	172.16.0.24
18	Exterior posterior 1	172.16.0.25
19	Gimnasio	172.16.0.26
20	Jardines frente izquierda	172.16.0.27
21	Exterior posterior 2	172.16.0.28

Tabla 4.25: Plan IPv4 de los controladores Hue.

Recordemos que los controladores Hue, recopilan los focos de cada sección donde son colocados y son estos mismos controladores Hue que se conectan a la red privada interna es por esto que en la tabla anterior se muestra el plan IPv4 de estos equipos.

Configuración en la aplicación Hue Philips para iOS

Debemos descargar una aplicación en un dispositivo con sistema operativo iOS de la marca Apple Inc.

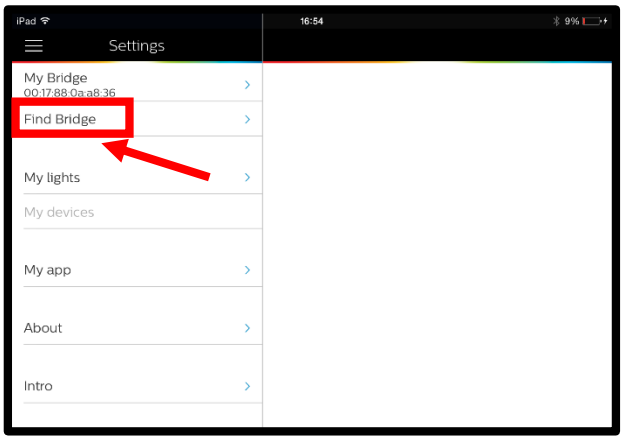


Figura 4.135: Panel de configuración del sistema Hue Philips.

En la figura anterior se muestra la primera ventana de configuración del sistema Hue Philips. Seleccionamos la opción 'Find Bridge' que nos permite detectar en la red privada interna todos los controladores Hue.

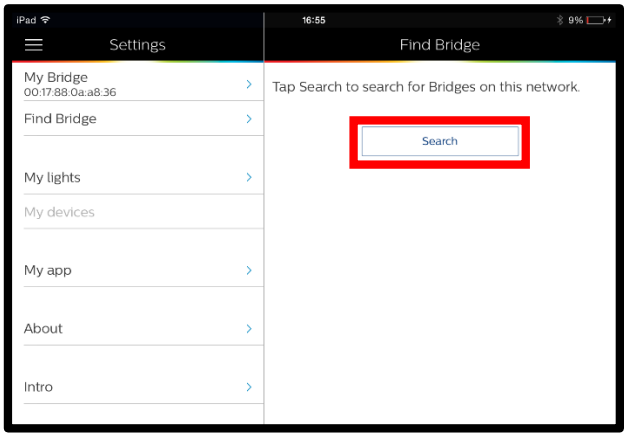


Figura 4.136: Opción Find Bridge.

Se selecciona el botón ‘Search’, que permite buscar los controladores Hue conectados a la red privada interna.

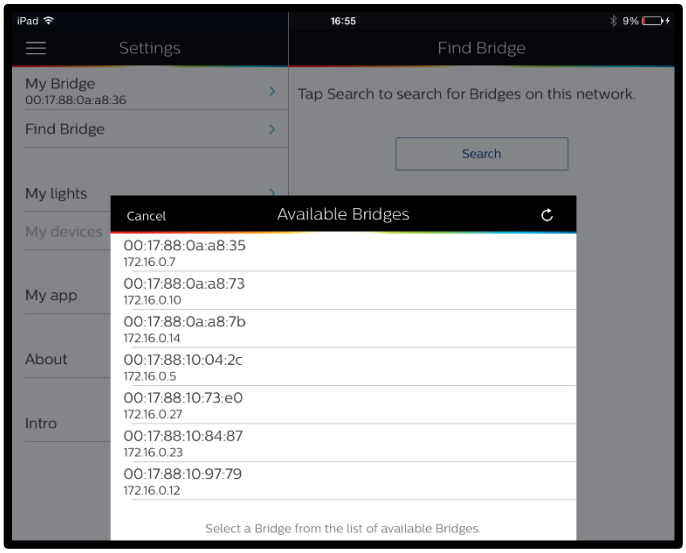


Figura 4.137: Controladores Hue disponibles en la red privada interna.

En la figura anterior se muestran los controladores Hue disponibles en la red privada interna. Se escoge el que se desea configurar. Al inicio, se los debe identificar por su dirección MAC la cual viene estampada en el controlador Hue.

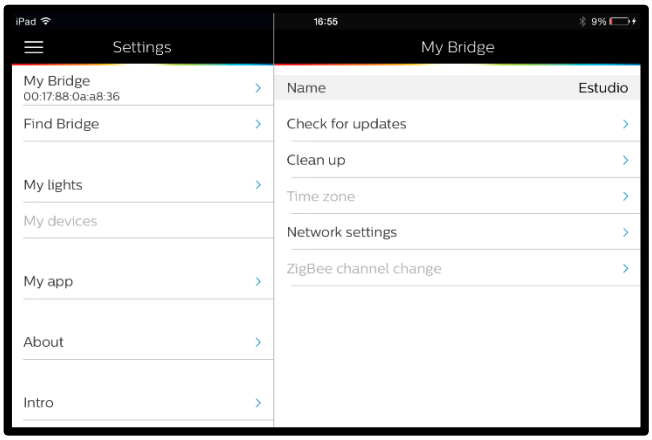


Figura 4.138: Controlador Hue detectado.

En la figura anterior se muestra un controlador Hue detectado. En el parámetro ‘Name’ se configura el nombre del controlador, en este caso, el del Estudio. En el parámetro ‘Network settings’ se configura el direccionamiento IPv4 del controlador Hue, tal como lo muestra la siguiente figura.

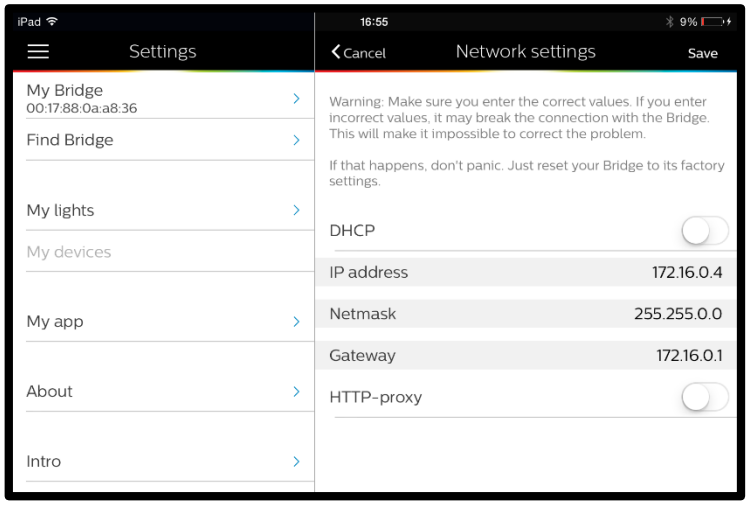


Figura 4.139: Configuración del direccionamiento IPv4 del controlador Hue.

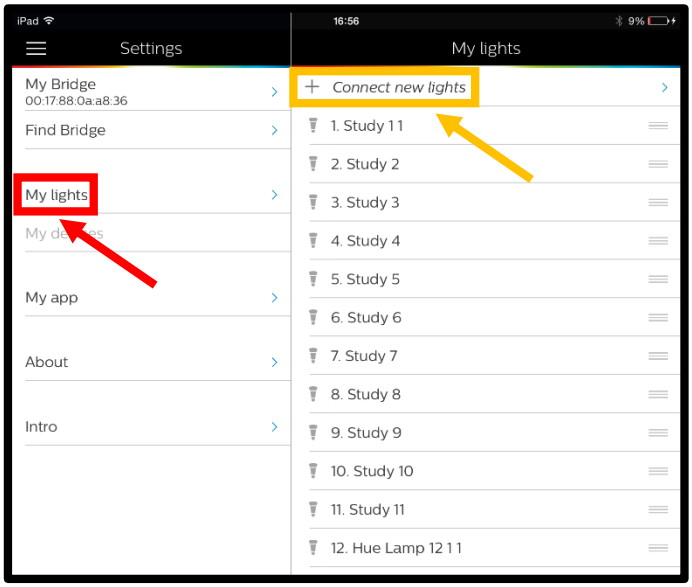


Figura 4.140: Inclusión de focos Hue a sus controladores.

Una vez configurado el direccionamiento IPv4 del controlador Hue, incluimos los focos Hue a sus respectivos controladores. Para esto necesitamos tener los focos Hue encendidos.

Seleccionamos la opción ‘My lights’ y luego la subopción ‘Connect new lights’. Automáticamente se detectan los focos y se les edita el nombre según la conveniencia.

Existe la posibilidad de manejar los focos Hue a través de la aplicación propia de Philips en un dispositivo electrónico, puede ser un smartphone, tablet, entre otros. Es decir que se pueden apagar, prender y cambiar su tonalidad. Es por esto que se considera al sistema Hue en general como parte de la gestión del confort y es complemento de otros dispositivos en las escenas.

Figura 4.141: Control del sistema Hue a través de la aplicación para equipos con iOS como sistema operativo.

Configuración en el VERA3

También debemos configurar a los controladores Hue en el VERA3 para poder incluirlos en las escenas. Para aquello necesitamos instalar una aplicación en el VERA3.

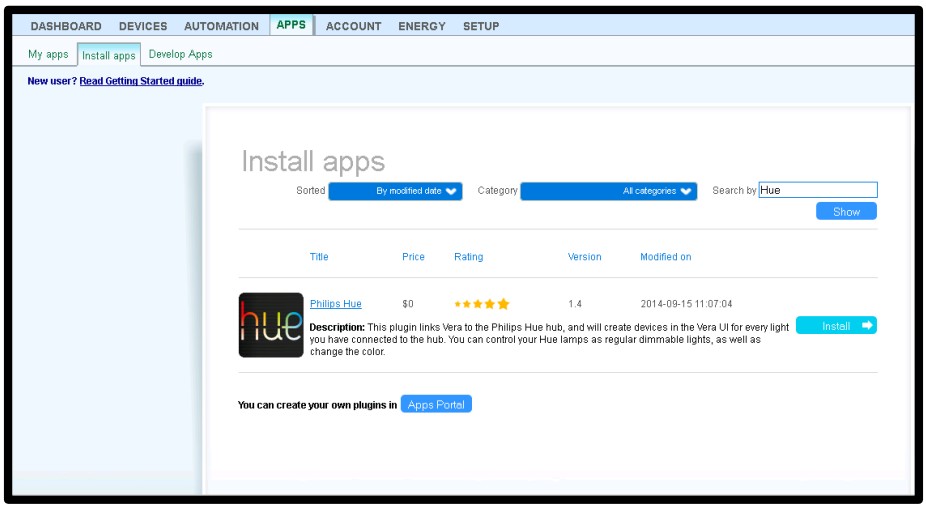


Figura 4.142: Pestaña APPS con la opción Install apps.

La figura anterior nos muestra un portal donde podemos buscar aplicaciones que pueden servirnos el VERA3. Este es el caso del sistema Hue. El sistema Hue funciona con el protocolo Zigbee y el VERA3 con el protocolo Z-Wave es por esto que no podemos configurar en el VERA3 a los controladores Hue como lo hacemos con los otros sensores. La aplicación permite que el VERA3 a través de la red privada interna, controle y maneje a los controladores Hue y así manejar a los focos Hue.

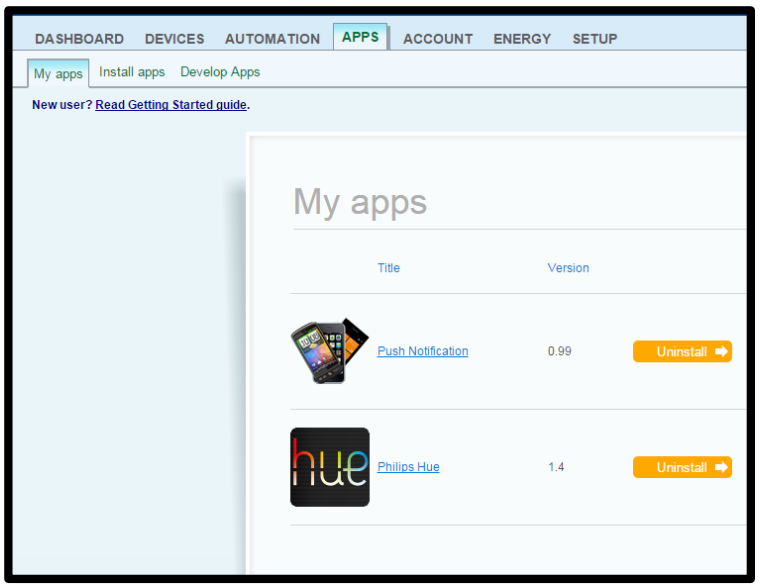


Figura 4.143: Instalación de la aplicación Philips Hue.

Una vez instalada la aplicación Philips Hue en el VERA3, esta aparece en la pestaña ‘APPS’ en la opción ‘My apps’.

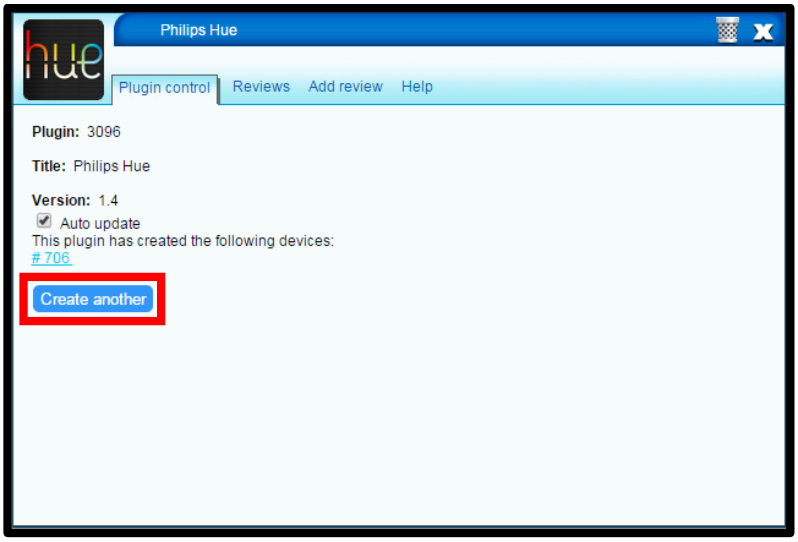


Figura 4.144: Panel de configuración de la aplicación Philips Hue.

Al seleccionar la aplicación Philips Hue, se nos muestra el panel de configuración. Seleccionamos la opción ‘Create another’ con lo cual creamos un dispositivo en el VERA3 que represente a un controlador Hue en específico.

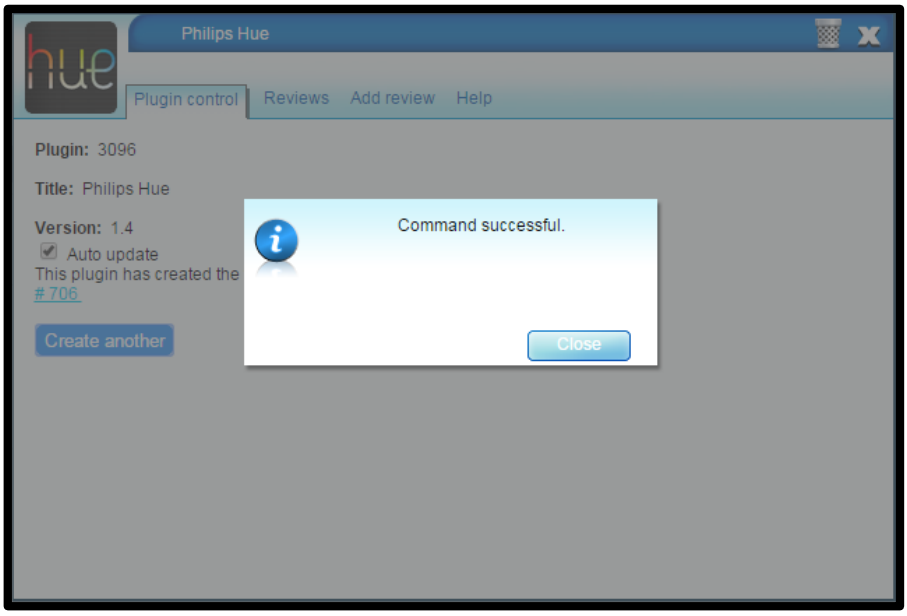


Figura 4.145: Creación exitosa de un controlador Hue en el VERA3.

Una vez creado el controlador Hue, nos aparece una ventana que indica ‘Command successful’ o en español, ‘Comando exitoso’.

Figura 4.146: Controlador Hue de la Biblioteca Planta Baja.

El controlador Hue aparece en la interfaz gráfica de usuario del VERA3 tal como lo muestra la figura 4.114 y dicho sea de paso en el 'Room' 'no room'. Se lo debe agregar al 'Room' correspondiente de la forma como se indica en la sección 4.1.

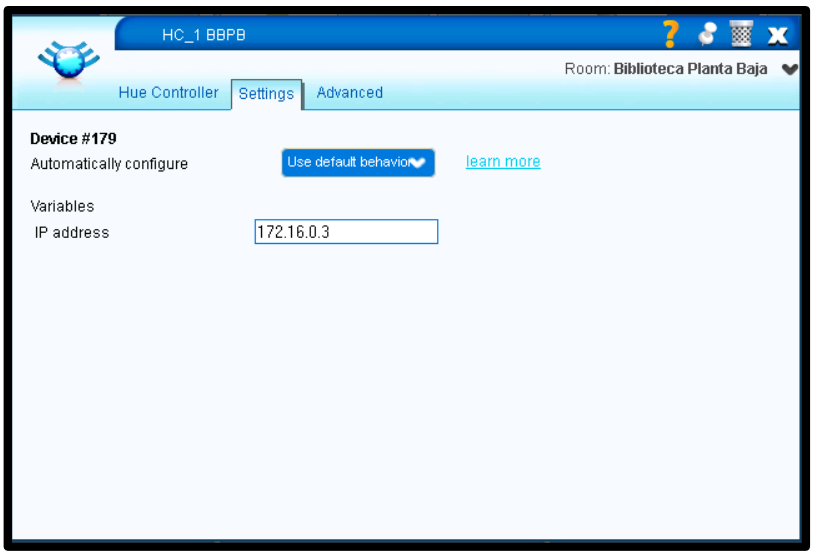


Figura 4.147: Pestaña Settings del panel de configuración del controlador Hue.

En la pestaña ‘Settings’ del panel de configuración del controlador Hue en el VERA3 y en el parámetro ‘IP Address’ se escribe la IP del controlador Hue correspondiente según la tabla 4.5.

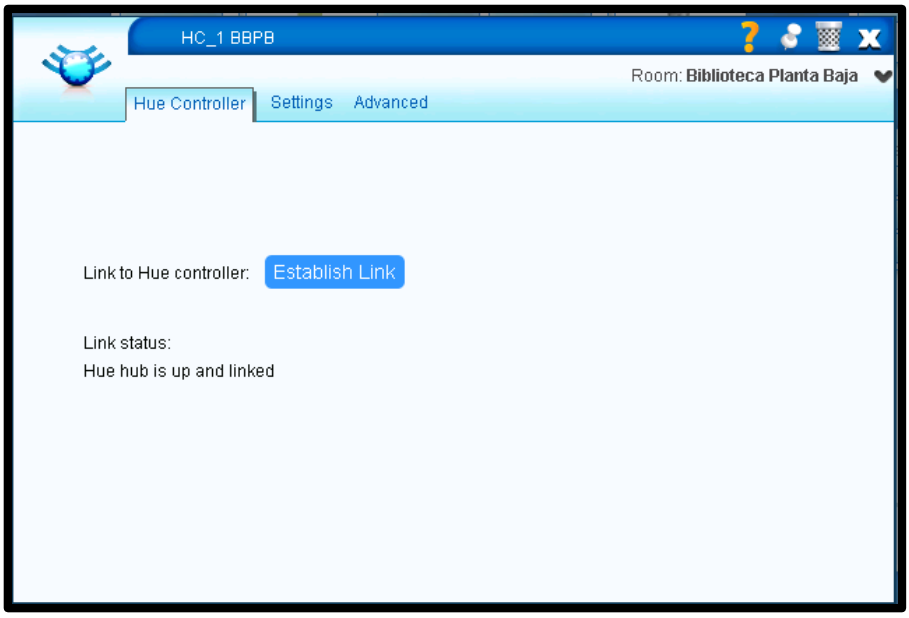


Figura 4.148: Pestaña Hue Controller del panel de configuración del controlador Hue.

Una vez editada la ‘IP Address’ en la pestaña ‘Settings’, vamos a la pestaña ‘Hue Controller’ y presionamos el botón ‘Establish Link’ para que el VERA3 pueda controlar a los controladores Hue. Mientras presionamos el botón ‘Establish Link’ al mismo tiempo debemos presionar el botón que tienen todos los controladores Hue en el medio de ellos.

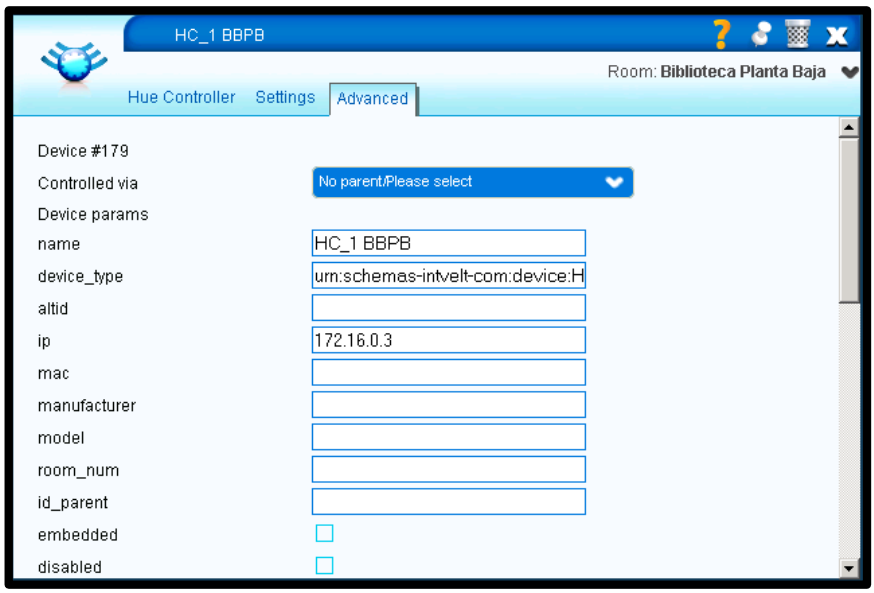


Figura 4.149: Pestaña Advanced del panel de configuración del controlador Hue.

En la figura anterior se muestra la pestaña ‘Advanced’ donde se edita el parámetro ‘Device params name’ y se escribe, en nuestro caso, “HC_2 BBPB”, según el formato establecido al final de la sección 4.1 y el identificador para los controladores Hue será ‘HC’ que significa ‘Hue Controller’ o en español, ‘Controlador Hue’.

Se debe ingresar a cada dispositivo en el ‘Room’ correspondiente, esto se muestra como hacer en la sección 4.1.

Ubicación en la vivienda

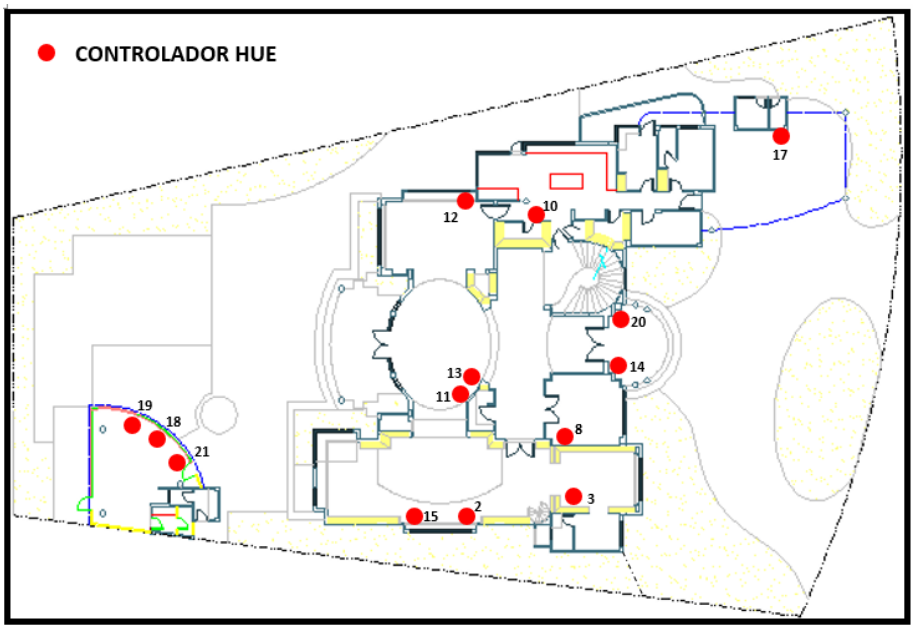


Figura 4.150: Ubicación de los controladores Hue en la planta baja.

En la figura anterior se muestra la ubicación de los controladores Hue en la planta baja.

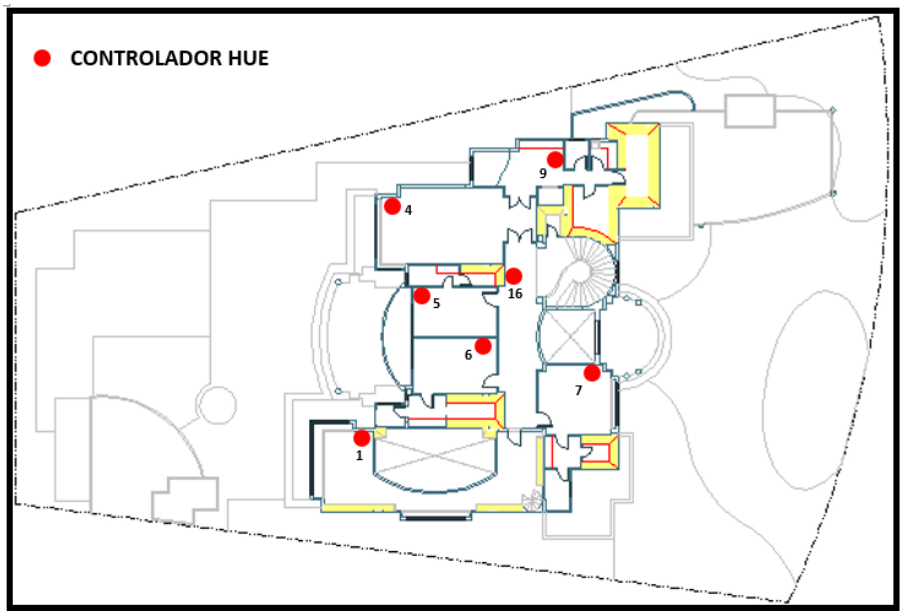


Figura 4.151: Ubicación de los controladores Hue en la planta alta.

En la figura anterior se muestra la ubicación de los controladores Hue en la planta alta de la vivienda.

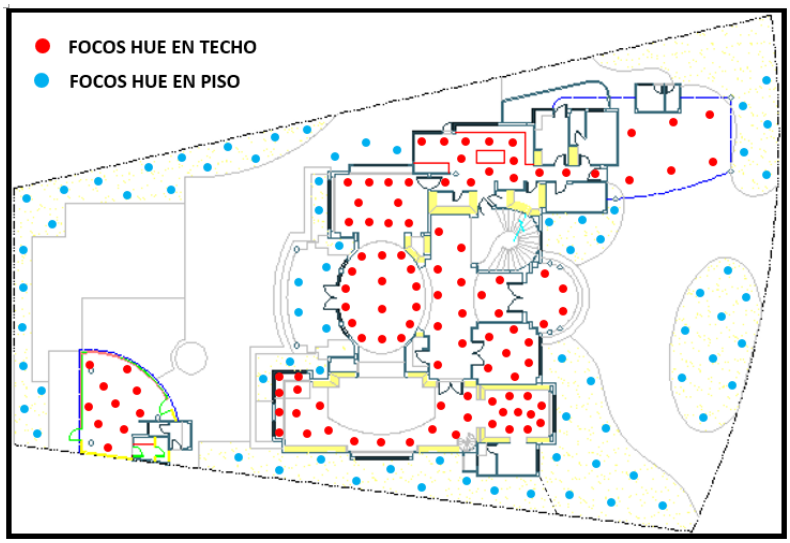


Figura 4.152: Ubicación de los focos Hue en la planta baja.

En la figura anterior se muestra la ubicación de los focos Hue en la planta baja.

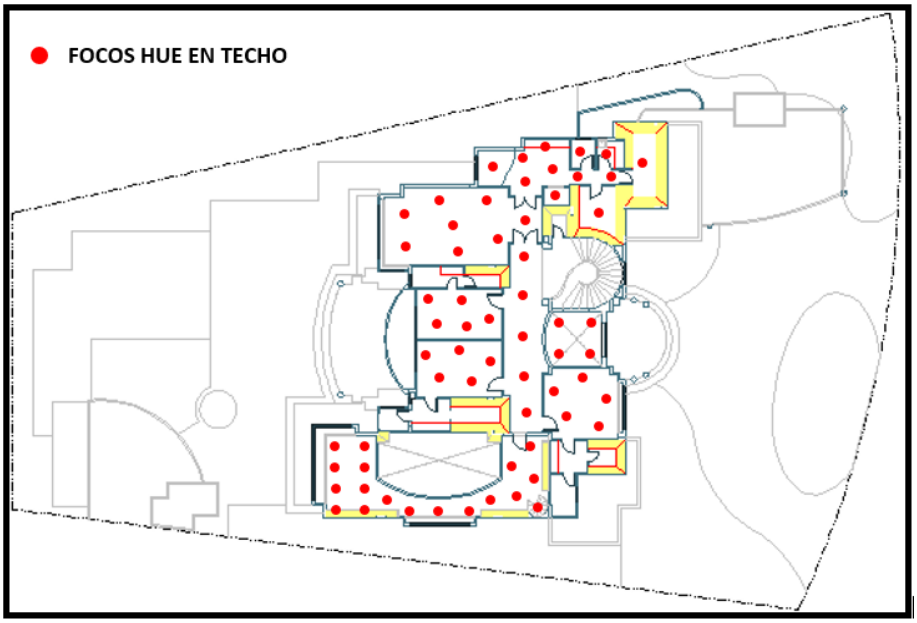


Figura 4.153: Ubicación de los focos Hue en la planta alta.

En la figura anterior se muestra la ubicación de los focos Hue en la planta alta de la vivienda.

ACTUADORES DE PERSIANAS

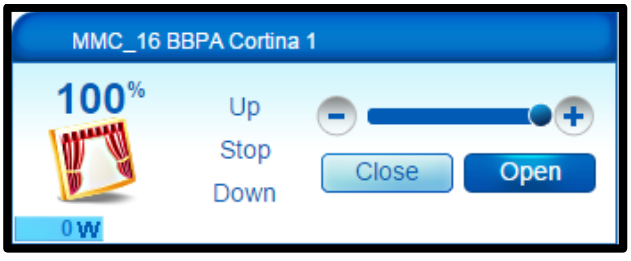


Figura 4.154: Actuador de persianas en la interfaz gráfica del VERA3.

En la figura anterior se muestra el actuador de persianas tal cual aparece en la interfaz gráfica del VERA3. Las opciones 'Close' y 'Open' permiten cerrar y abrir las persianas respectivamente. Las opciones 'Up', 'Stop' y 'Down' permiten subir, parar y bajar las persianas. En la esquina superior derecha se encuentra un ícono de una llave de tuercas. Se da click en este ícono y se puede acceder al panel de configuración del actuador de persiana.

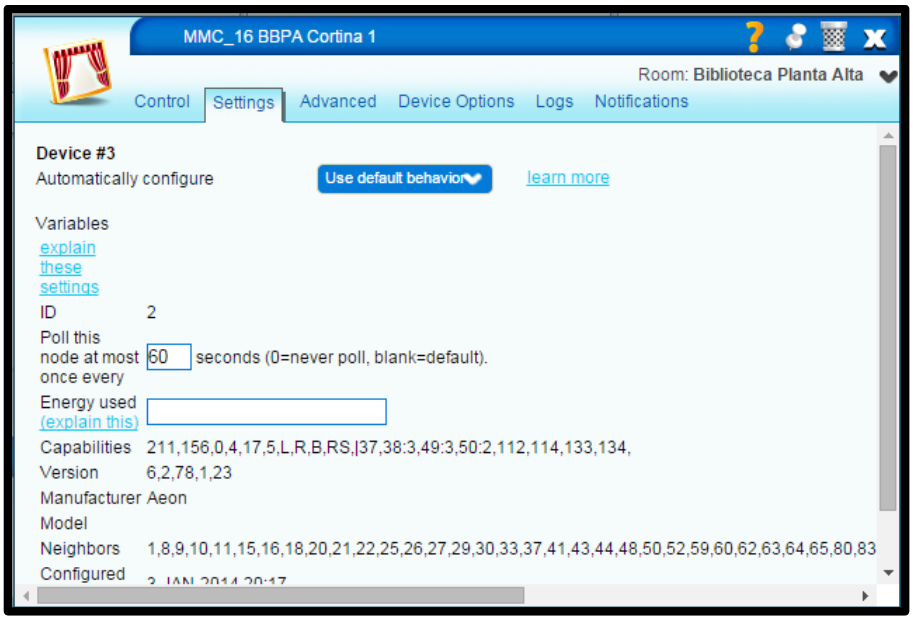


Figura 4.155: Pestaña Settings del panel de configuración del actuador de persianas.

En la figura anterior se muestra la pestaña ‘Settings’ donde se configura el parámetro ‘Poll this node at most ___ seconds’ y se escriba 60 que corresponde a 60 segundos.

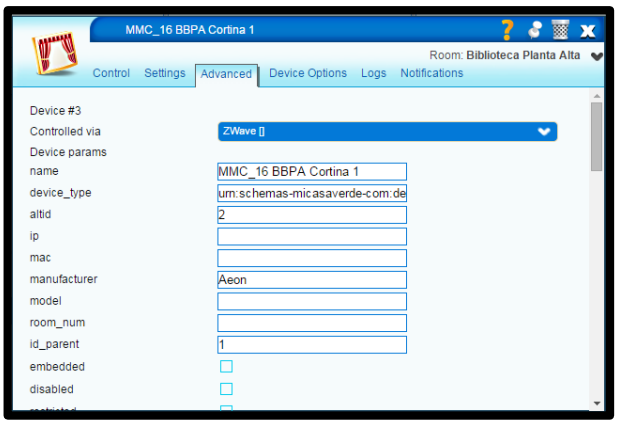


Figura 4.156: Pestaña Advanced del panel de configuración del actuador de persianas.

En la figura anterior se muestra la pestaña ‘Advanced’ donde editamos el parámetro ‘Device params name’ y escribimos en nuestro caso, ‘MMC_16 BBPA Cortina 1’ según el formato establecido al final de la sección 4.1 y el identificador para los actuadores de persiana será ‘MMC’ que significa ‘Micro motor controller’ o en español, ‘Micro controlador de motor’ y basados en la siguiente tabla.

NOMBRES DE LOS ACTUADORES DE PERSIANAS		
	SECTOR	**NOMBRE**
1	BIBLIOTECA PLANTA ALTA	MMC_1 BBPA
2		MMC_2 BBPA
3		MMC_3 BBPA
4		MMC_4 BBPA
5	BIBLIOTECA PLANTA BAJA	MMC_5 BBPB
6		MMC_6 BBPB
7		MMC_7 BBPB
8		MMC_8 BBPB
9	COMEDOR	MMC_9 Comedor
10	DORMITORIO 1	MMC_10 Dormitorio1
11		MMC_11 Dormitorio1
12	DORMITORIO 2	MMC_12 Dormitorio2
13	DORMITORIO 3	MMC_13 Dormitorio3
14	DORMITORIO 4	MMC_14 Dormitorio4
15	DORMITORIO MADRE	MMC_15 DormitorioMadre
16	ESTUDIO	MMC_16 Estudio
17	SALA	MMC_17 Sala
18		MMC_18 Sala

Tabla 4.26: Tabla de los nombres de los actuadores de persianas.

Se debe ingresar a cada dispositivo en el 'Room' correspondiente, esto se muestra como hacer en la sección 4.1.

Ubicación en la vivienda

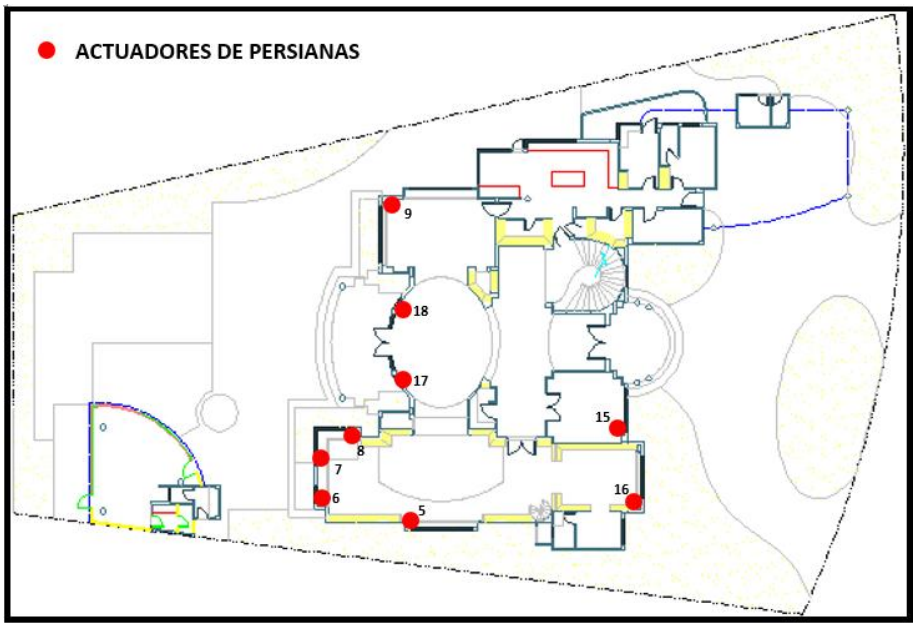


Figura 4.157: Ubicación de los actuadores de persianas en la planta baja.

En la figura anterior se muestra la ubicación de los actuadores de persianas en la planta baja de la vivienda.

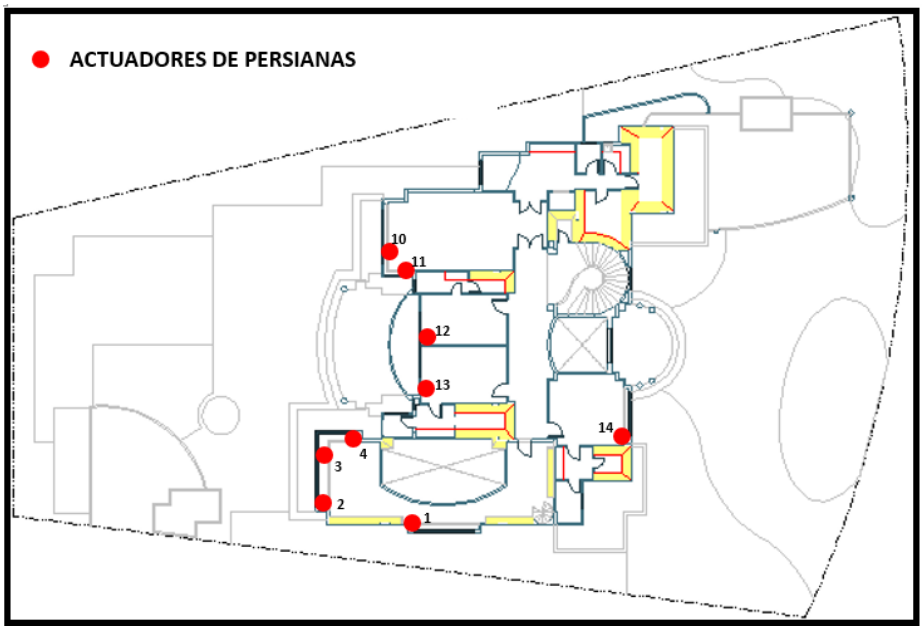


Figura 4.158: Ubicación de los actuadores de persianas en la planta alta.

En la figura anterior se muestra la ubicación de los actuadores de persianas en la planta alta de la vivienda.

Conexión física con las persianas

En la siguiente figura se muestra una gráfico que indica las conexiones físicas entre el actuador de persianas y las persianas.

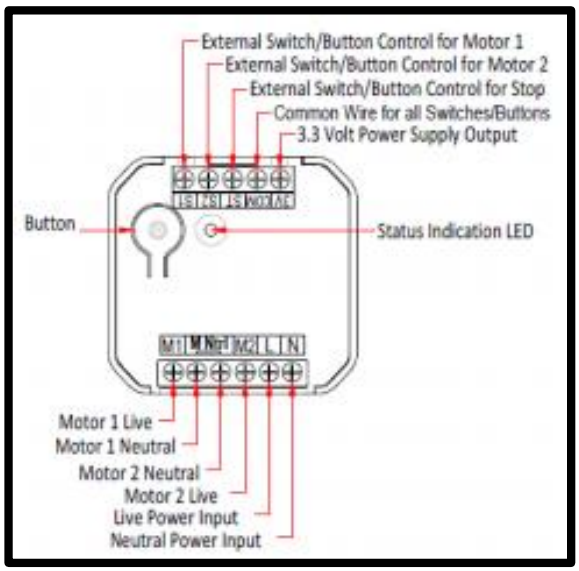


Figura 4.159: Conexiones físicas entre el actuador de persianas y las persianas.

Sólo se usan las terminales físicas de la parte inferior de la figura. Recordamos que tenemos 3 cables que vienen del motor. 2 líneas y 1 neutro. La primera línea se conecta en el terminal que dice ‘Motor 1 Live’. La segunda línea se conecta en el terminal que dice ‘Motor 2 Live’. El neutro de la persiana se conecta ya sea en el terminal ‘Motor 1 Neutral’ o ‘Motor 2 Neutral’. Finalmente se conecta el actuador de persiana al tomacorriente en los terminales que dicen ‘Live Power Input’ y ‘Neutral Power Input’, donde se conecta la línea y neutro del tomacorriente respectivamente.

TERMOSTATOS

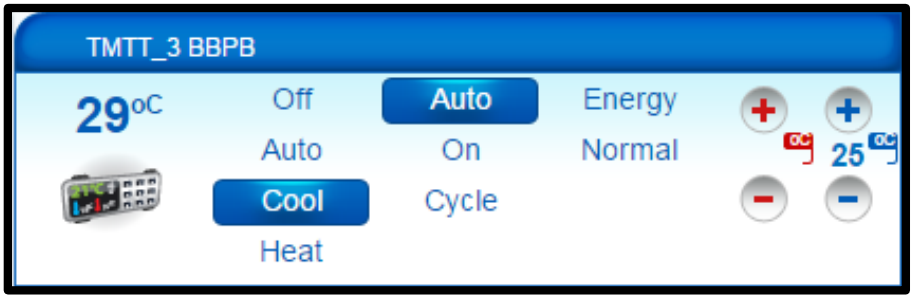


Figura 4.160: Termostato en la interfaz gráfica del VERA3.

En la figura anterior se muestra el termostato tal cual aparece en la interfaz gráfica del VERA3. Las opciones 'Off', 'Auto', 'Cool' y 'Heat' permiten apagar, automáticamente prender o apagar el aire acondicionado, encender el aire acondicionado o encender el calentamiento respectivamente. Las opciones 'Auto', 'ON' y 'Cycle' permiten apagar o prender automáticamente el ventilador si se enciende el aire acondicionado, enceder el ventilador y encender el ventilado según un ciclo. Esta última opción no se usa. En la esquina superior derecha se encuentra un ícono de una llave de tuercas. Se da click en este ícono y se puede acceder al termostato.

Figura 4.161: Pestaña Settings del panel de configuración del termostato.

En la figura anterior se muestra la pestaña ‘Settings’ donde se configura el parámetro ‘Poll this node at most ___ seconds’ y se escriba 60 que corresponde a 60 segundos.

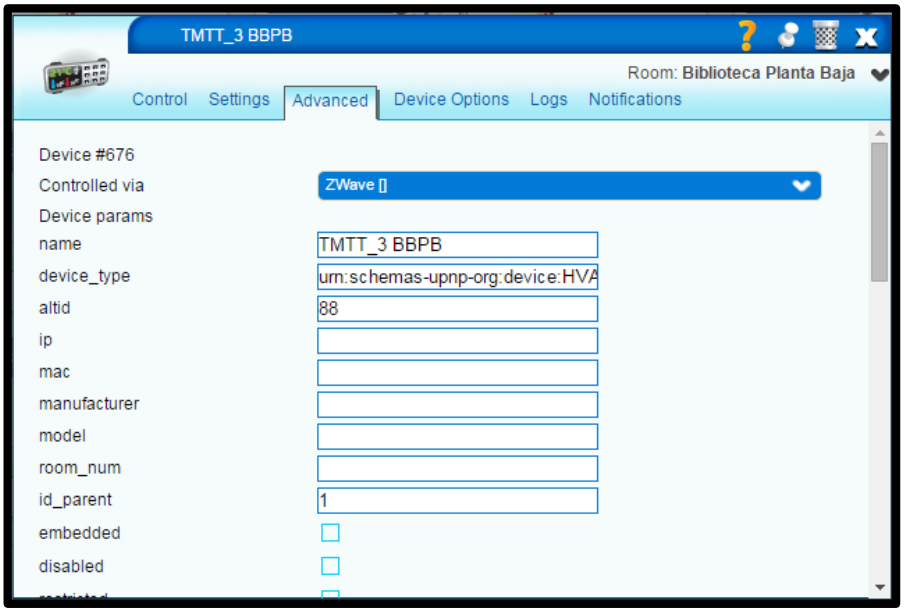


Figura 4.162: Pestaña Advanced del panel de configuración del termostato.

En la figura anterior se muestra la pestaña ‘Advanced’ donde editamos el parámetro ‘Device params name’ y escribimos en nuestro caso, ‘TMTT_3 BBPB’ según el formato establecido al final de la sección 4.1 y el identificador para los termostatos será ‘TMTT’ que significa ‘Thermostat’ o en español, ‘Termostato’ y nos basamos en la siguiente tabla.

NOMBRES DE LOS TERMOSTATOS		
	SECTOR	**NOMBRE**
1	BIBLIOTECA PLANTA ALTA	TMTT_ 1 BBPA
2		TMTT_2 BBPA
3	BIBLIOTECA PLANTA BAJA	TMTT_3 BBPB
4	BAÑO DORMITORIO 1	TMTT_4 BañoDormitorio1
5	COCINA	TMTT_5 Cocina
6	COMEDOR	TMTT_6 Comedor
7	DORMITORIO 1	TMTT_7 Dormitorio1
8	DORMITORIO 2	TMTT_8 Dormitorio2
9	DORMITORIO 3	TMTT_9 Dormitorio3
10	DORMITORIO 4	TMTT_10 Dormitorio4
11	DORMITORIO MADRE	TMTT_11 DormitorioMadre
12	ESTUDIO	TMTT_12 Estudio
13	PASILLO PLANTA BAJA	TMTT_13 PasilloPB
14	SALA	TMTT_14 Sala

Tabla 4.27: Tabla de nombres de los termostatos.

Se debe ingresar a cada dispositivo en el 'Room' correspondiente, esto se muestra como hacer en la sección 4.1.

Ubicación en la vivienda

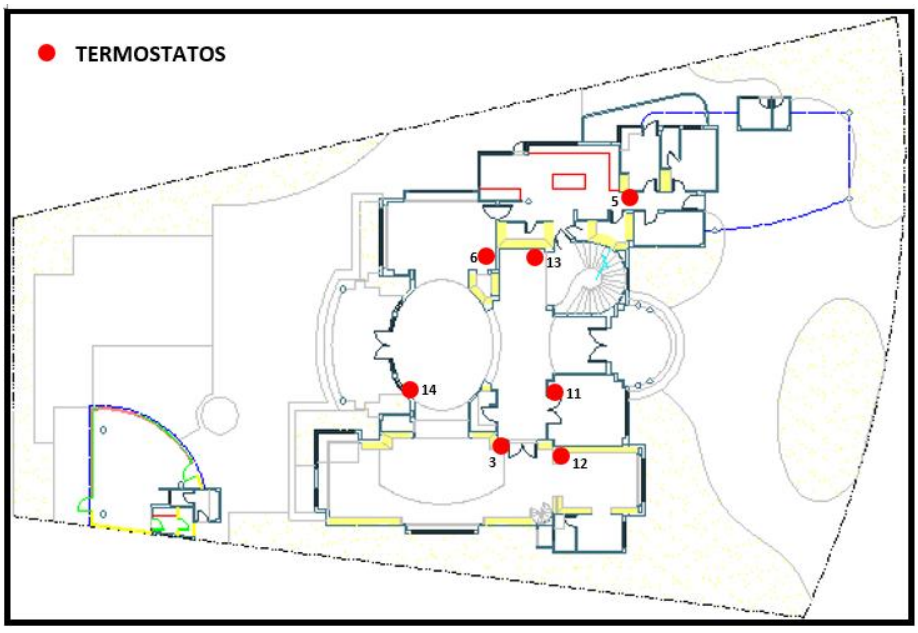


Figura 4.163: Ubicación de los termostatos en la planta baja.

En la figura anterior se muestra la ubicación de los termostatos en la planta baja de la vivienda.

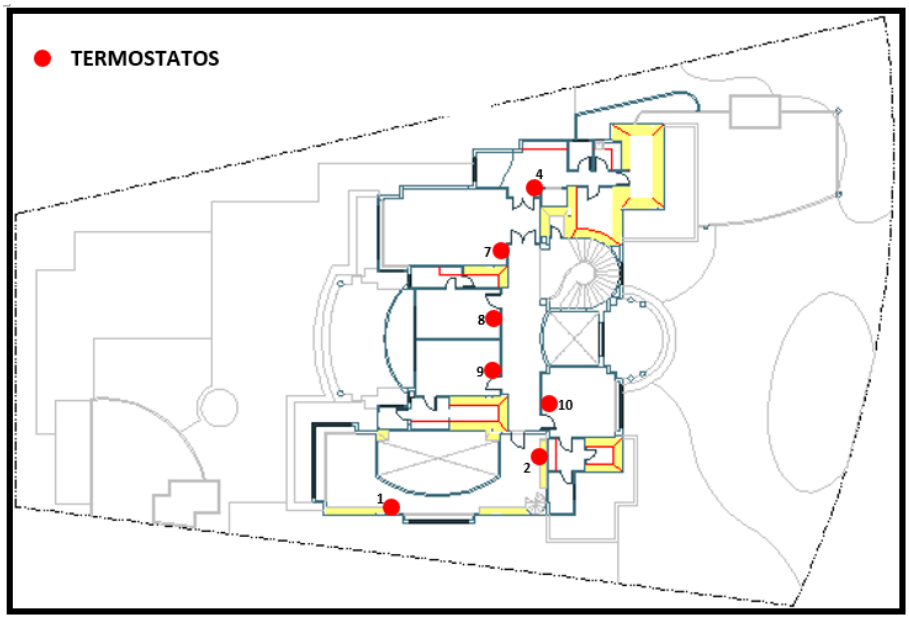


Figura 4.164: Ubicación de los termostatos en la planta alta.

En la figura anterior se muestra la ubicación de los termostatos en la planta alta de la vivienda.

Conexión física con las persianas

La siguiente figura muestra las conexiones físicas entre los aires acondicionados y los termostatos.

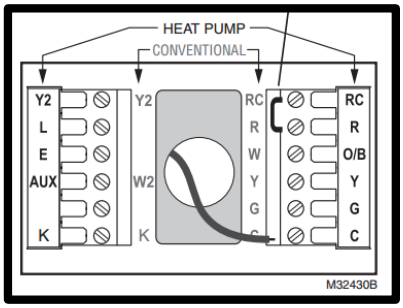


Figura 4.165: Conexiones físicas entre los aires acondicionados y los termostatos.

Todos los aires acondicionados manejan dos etapas en la refrigeración es por esto que se usan los terminales: RC, R, Y, G, C y Y2. Si se usara una sola etapa en la refrigeración, se obviaría el terminal Y2.

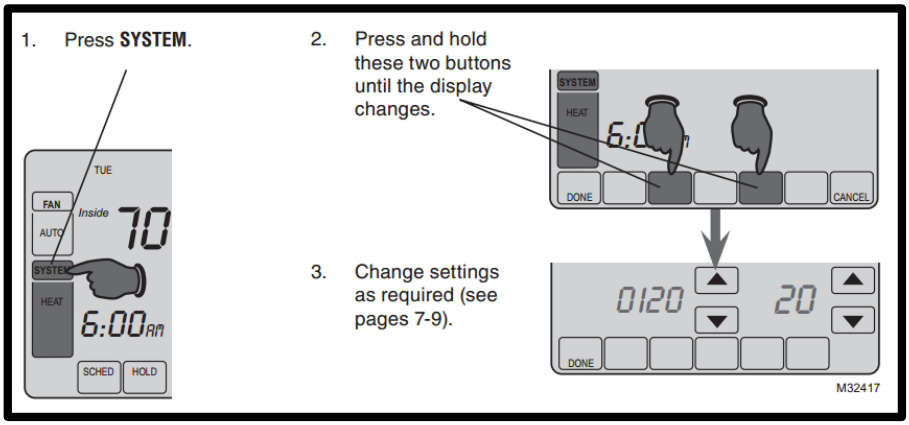


Figura 4.166: Pasos para entrar al modo de configuración.

En la figura anterior se muestran los pasos para entrar al modo de configuración. 1) Se debe presionar la opción ‘System’. 2) Mantener presionado los botones que se indican en la pantalla

del termostato hasta que dicha pantalla cambie. 3) Cambiar de configuración con las pestañas de subir o bajar.

0170	**System type**	**1**	**1 heat/1 cool conventional**
		2	1 heat/1 cool heat pump (no aux. heat)
		3	Heat only (2-wire systems)
		4	Heat only with fan
		5	Hot water Series 20 system (power to open & close zone valves/normally open zone valves)
		6	Cool only
		7	2 heat/1 cool heat pump (with aux. heat)
		8	2 heat/2 cool multistage conventional
		9	2 heat/1 cool multistage conventional
		10	1 heat/2 cool multistage conventional
		11	2 heat/2 cool heat pump (no aux. heat)
		12	3 heat/2 cool heat pump (with aux. heat)

Figura 4.167: Configuración 0170 del termostato Honeywell.

La figura anterior muestra la configuración 0170 del termostato Honeywell. En esta configuración escogemos la opción 8 que indica un sistema 2H/2C, esto es, 2 etapas en calentamiento y 2 etapas en refrigeración. No se usan las etapas de calentamiento.

4.4.3. Escenas.

CONFORT – ACTUADORES DE PERSIANAS, TERMOSTATOS

Las premisas bajo las cuales creamos las escenas en esta parte son las siguientes: 1) ‘noche’ corresponde al intervalo de tiempo, después de las 6 de la tarde y antes de las 6 de la

mañana, 2) ‘día’ corresponde al intervalo de tiempo, después de las 6 de la mañana y antes de las 6 de la tarde, 3) el set point de la temperatura en la vivienda debe ser de 26 °C 4) cuando la temperatura de la vivienda pase los 28 °C, se debe encender el aire acondicionado, 5) cuando la temperatura de la vivienda baje de los 24 °C se debe apagar el aire acondicionado, 6) las persianas de la vivienda deben subir en la noche y 7) las persianas de la vivienda deben bajar en el día.

Cabe mencionar, que las configuraciones que vamos a realizar se replican a todos los sectores donde existan termostatos y actuadores de persianas.

Escenas para Termostatos

Figura 4.168: Escena para encender los aires acondicionados.

En la figura anterior se muestra la escena para encender el aire acondicionado cuando la temperatura pase los 28 °C.

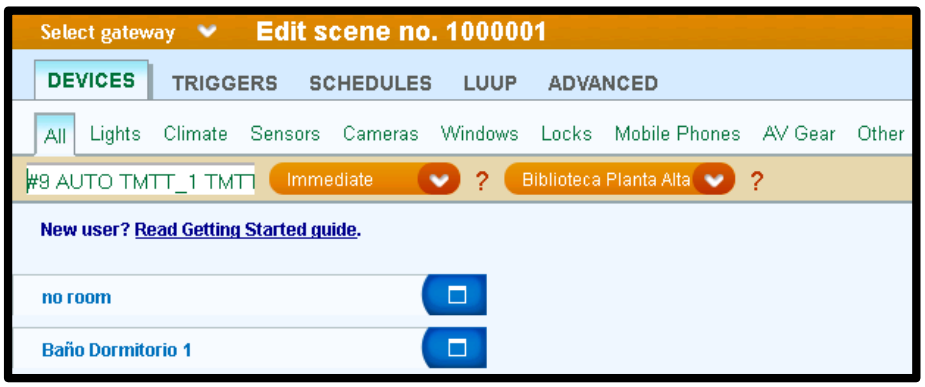


Figura 4.169: Escena para encender el aire acondicionado con retraso Inmediate.

La figura anterior muestra la escena para encender el aire acondicionado con el retraso Inmediate. Cabe mencionar que no se creará otro retraso ya que para esta escena no lo necesitaremos. Esta escena se activará cuando, el trigger, que en este caso es el termostato TMTT_1 en la Biblioteca planta alta, detecte que la temperatura subió por sobre los 28 °C. Cuando esto suceda, el dispositivo principal, que dicho sea de paso es el mismo termostato TMTT_1, encenderá el aire acondicionado.

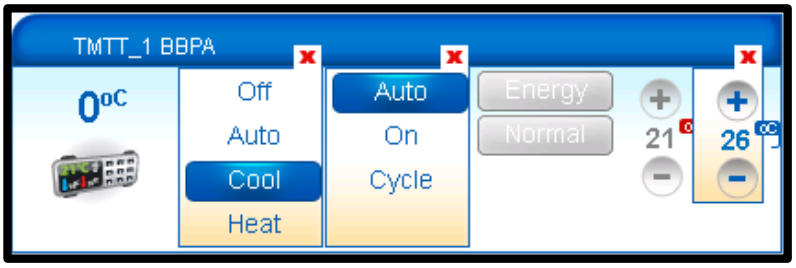


Figura 4.170: Opción Cool, Auto y set point de 26 °C para el termostato.

La figura anterior nos muestra, que escogemos la opción Cool, Auto y un set point de 26 °C que nos permite, encender el aire acondicionado, el ventilador y fijar que el aire acondicionado llegue a una temperatura de 26 °C respectivamente.

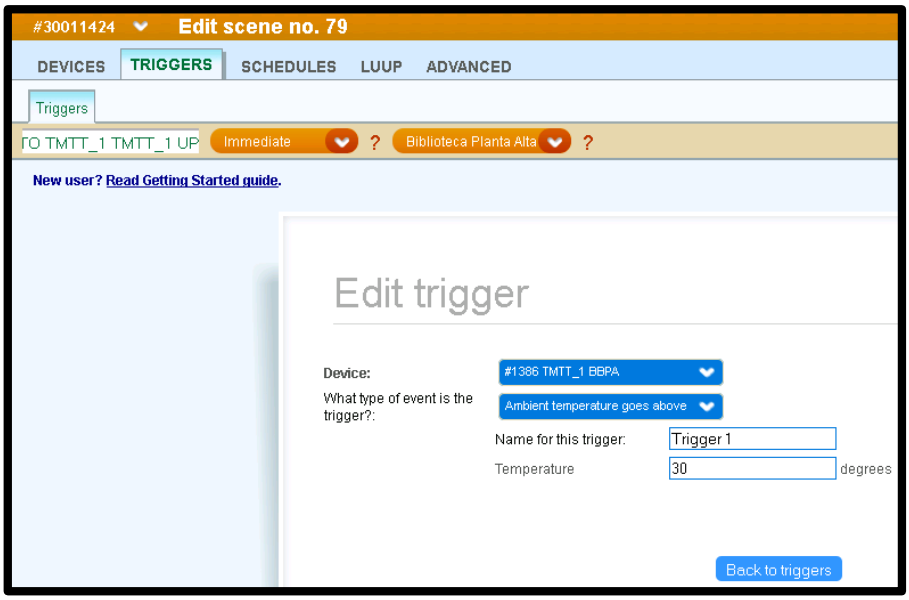


Figura 4.171: Pestaña TRIGGERS con la opción Triggers.

La figura anterior muestra la pestaña ‘TRIGGERS’ con la opción Triggers. En el parámetro ‘Device’ escogemos ‘TMTT_1 BBPA’. En el parámetro ‘What type of event is the trigger?’ escogemos ‘Ambient temperature goes above’ que en español significa, ‘Temperatura ambiente sube por sobre’. En el parámetro ‘Name for this trigger’ escogemos ‘Trigger 1’. En el parámetro ‘Temperature _____ degrees’ escribimos 28. Finalmente presionamos, ‘Confirm changes’.

Hasta ahora, esta escena nos permite encender el aire acondicionado cuando la temperatura sobrepase los 28 °C. Nos falta crear una escena que apague el aire acondicionado cuando la temperatura este por debajo de los 24 °C. Con esto damos una ventana de 4 °C entre el límite superior y el inferior de temperatura.

Figura 4.172: Escena para apagar el aire acondicionado.

La figura anterior nos muestra la escena para apagar el aire acondicionado cuando la temperatura este por debajo de los 24 °C.

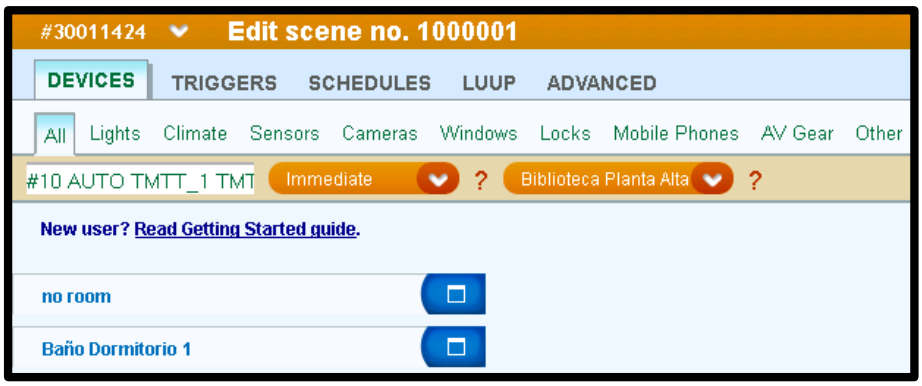


Figura 4.173: Escena para apagar el aire acondicionado con retraso Inmediate.

La figura anterior muestra la escena para apagar el aire acondicionado con el retraso Inmediate. Cabe mencionar que no se creará otro retraso ya que para esta escena no lo necesitaremos. Esta escena se activará cuando, el trigger, que en este caso es el termostato TMTT_1 detecte que la temperatura este por debajo de los 24 °C. Cuando esto suceda, el dispositivo principal, que dicho sea de paso es el mismo termostato TMTT_1, apagará el aire acondicionado.

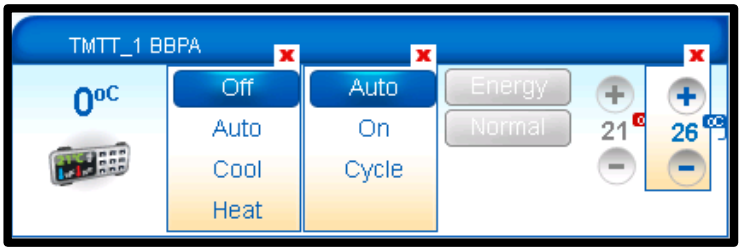


Figura 4.174: Opción Off, Auto y set point de 26 °C para el termostato.

La figura anterior nos muestra, que escogemos la opción Off, Auto y un set point de 26 °C que nos permite, apagar el aire acondicionado, el ventilador y fijar que el aire acondicionado llegue a una temperatura de 26 °C respectivamente.

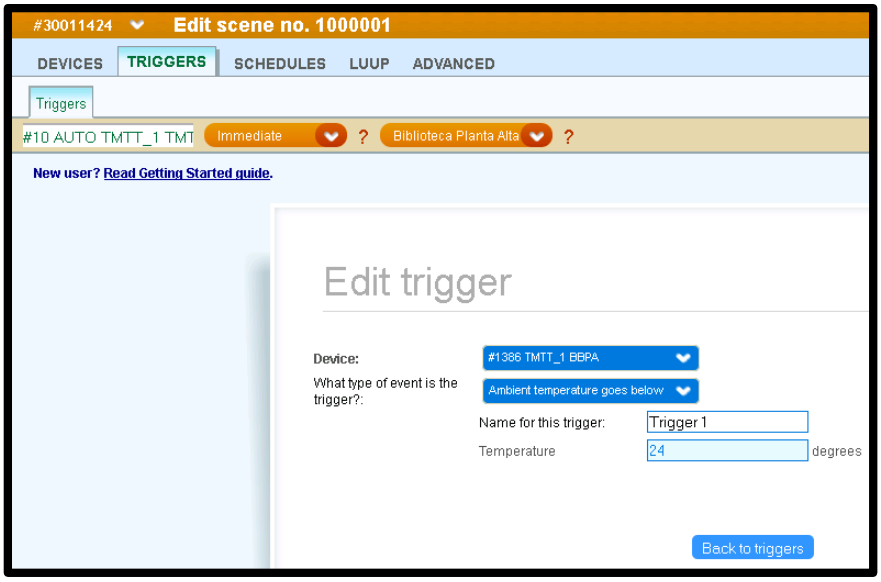


Figura 4.175: Pestaña TRIGGERS con la opción Triggers.

La figura anterior muestra la pestaña ‘TRIGGERS’ con la opción Triggers. En el parámetro ‘Device’ escogemos ‘TMTT_1 BBPA’.

En el parámetro ‘What type of event is the trigger?’ escogemos ‘Ambient temperature goes below’ que en español significa, ‘Temperatura ambiente por debajo’. En el parámetro ‘Name for this trigger’ escogemos ‘Trigger 1’. En el parámetro ‘Temperature _____ degrees’ escribimos 24. Finalmente presionamos, ‘Confirm changes’.

Escenas para Actuadores de Persianas

Figura 4.176: Escena para subir/bajar persianas.

En la figura anterior se muestra la escena para subir/bajar persianas. Las persianas subirán siempre y cuando sea de noche y bajarán siempre y cuando sea de día.

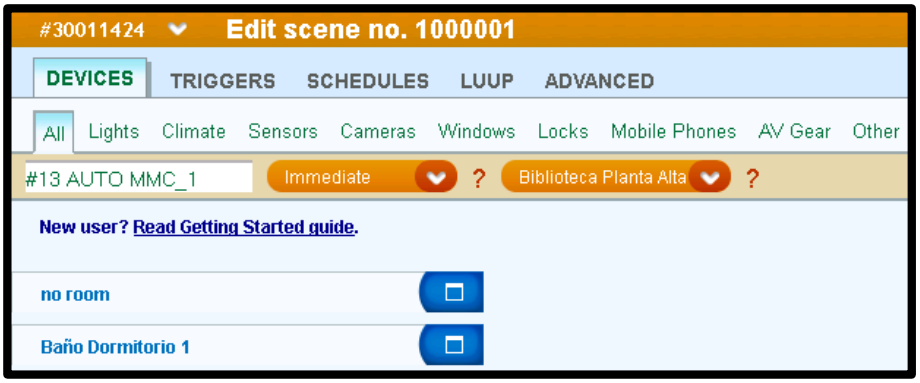


Figura 4.177: Escena para subir/bajar la persiana con retraso Inmediate.

La figura anterior muestra la escena para subir/bajar persianas con retraso 'Inmediate'. En este ejemplo usaremos el actuador de persianas 'MMC_1' que se encuentra en la Biblioteca planta alta.

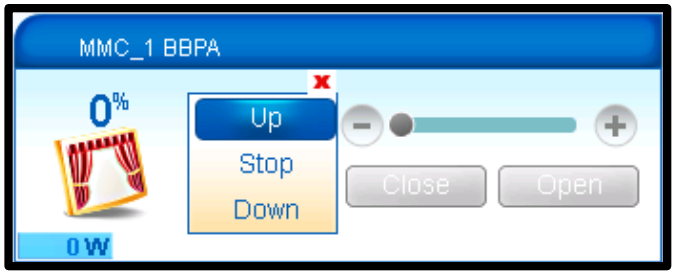


Figura 4.178: Opción Up para el actuador de persianas.

En la figura anterior se muestra la opción 'Up' para el actuador de persianas. Esto nos permite subir la persiana a penas (inmediate) se active la escena. La escena se activará cuando sean las 18h00 de cada día.

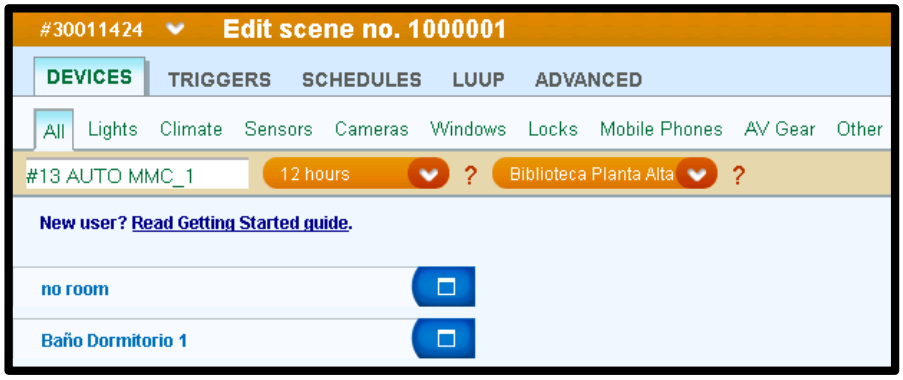


Figura 4.179: Escena para subir/bajar la persiana con retraso 12 horas.

La figura anterior muestra la escena para subir/bajar la persiana con retraso de 12 horas.

Figura 4.180: Opción Down para el actuador de persiana.

En la figura anterior se muestra la opción 'Down' para el actuador de persianas. Esto nos permite bajar la persiana después de que se active la escena. El 'después' tiene una duración de 12 horas que la configuramos con el retraso de 12 horas. Las persianas suben cuando la escena se activa, es decir, cuando sean las 18h00 de cada día, las persianas subirán

pero luego de 12 horas, es decir a las seis de la mañana del otro día, estas persianas bajarán.

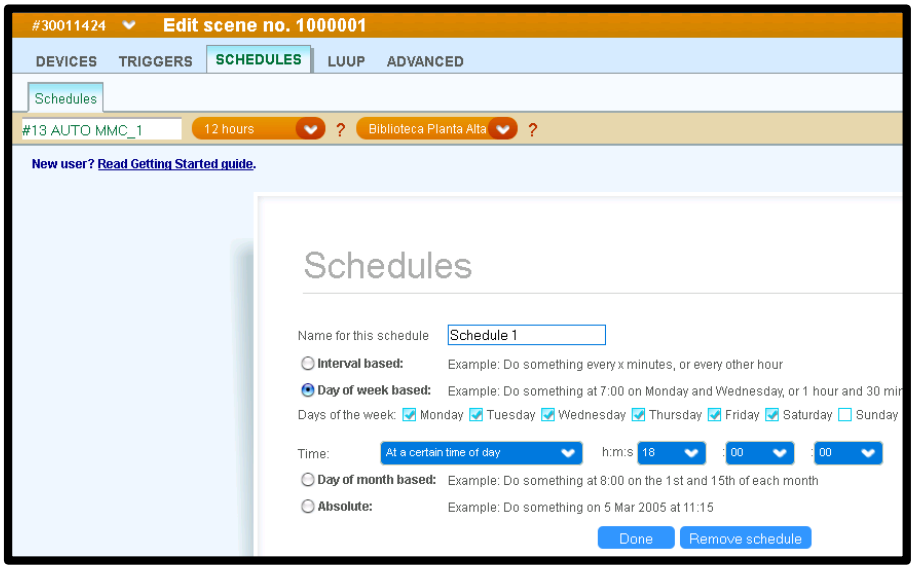


Figura 4.181: Configuración de Schedule para la escena que sube/baja la persiana.

La figura anterior nos muestra la configuración de ‘Schedule’ para la escena que sube/baja la persiana. En el parámetro, ‘Name for this schedule’ escribimos un nombre para este Schedule, en nuestro caso, ‘Schedule 1’. Escogemos la opción ‘Day of week based’ y marcamos la casilla de todos los días. En el parámetro ‘Time’, escogemos, ‘At a certain time of day’ con la hora ’18:00:00’. Seleccionamos ‘Done’ y luego ‘Confirm changes’. Una vez configurado nuestro Schedule, aseguramos

que todos los días a las seis de la tarde, subamos la persiana y a las seis de la mañana la bajemos.

CAPÍTULO 5

ANÁLISIS DE COSTOS DEL PROYECTO.

5.1. Detalle de costos de los equipos.

5.1.1. Sistema Domótico.

DETALLE DE COSTOS DE EQUIPOS							
	DISPOSITIVO	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	PESO UNITARIO EN LIBRAS	PESO TOTAL EN LIBRAS
1	VERA3	3	$ 299.00	$ 897.00	0.86	2.58
2	FOCOS HUE	239	$ 59.97	$ 14,332.83	0.35	83.65
3	CONTROLADORES HUE	21	$ 40.00	$ 840.00	0.25	5.25
4	SENSOR DE MOVIMIENTO AEON LABS	14	$ 47.80	$ 669.20	0.55	7.7
5	SENSOR DE MOVIMIENTO EVERSPRING	1	$ 32.00	$ 32.00	0.2	0.2
6	SENSOR DE MOVIMIENTO SCHLAGE	1	$ 54.52	$ 54.52	0.21875	0.21875
7	SENSOR DE MOVIMIENTO EXPRESS CONTROLS	1	$ 45.00	$ 45.00	0.2	0.2
8	SENSORES DE APERTURA Y CERRADO DE PUERTAS	16	$ 37.50	$ 600.00	0.15	2.4
9	ACTUADORES DE PERSIANAS	18	$ 49.95	$ 899.10	0.1	1.8
10	TERMOSTATOS	14	$ 149.99	$ 2,099.86	1.43	20.02
			SUBTOTAL	$ 20,469.51	TOTAL DE PESO DE CARGA EN LIBRAS	124.01875
		FLETE	COSTO TOTAL POR PESO DE CARGA EN LIBRAS	$ 622.68	COSTO POR LIBRA	$ 4.90
		ARANCELES	IMPUESTO A LA SALIDA DE CAPITALES 5%	$ 1,023.48	COSTO POR NACIONALIZACIÓN	$ 10.00
			FODINFA 0.5%	$ 102.35	SEGURO	$ 4.99
			IVA 12%	$ 2,456.34	COSTO TOTAL POR PESO DE CARGA EN LIBRAS	$ 622.68
			TOTAL	$ 24,674.36		

Tabla 5.1: Costos de equipos domóticos.

En la tabla anterior se muestran los costos de los dispositivos domóticos. El precio unitario de cada dispositivo se lo ha tomado como referencia de las tiendas online donde fueron comprados, estas son, ‘amazon’ y ‘ebay’. Adicional a estos precios, debemos considerar los costos por flete y por aranceles de importaciones según la legislación ecuatoriana. Las dos últimas columnas muestran el detalle del costo del flete, en el cual existen tres cargos: 1) costo por libra, 2) costo por naturalización y 3) costo por seguro. Estos costos fueron tomados como referencia de la empresa ‘produbox’. Los aranceles de importaciones son: 1) impuesto de la salida de capitales, 2) FODINFA (Fondo de desarrollo de la infancia) y 3) IVA (Impuesto al valor agregado). Estos últimos aranceles son gravados sobre el subtotal.

5.1.2. Cableado de fibra óptica y STP de cobre cat 6a.

DETALLE DE COSTOS DE EQUIPOS				
	DISPOSITIVO	CANTIDAD	PRECIO UNITARIO INCLUIDO IVA	PRECIO TOTAL
1	CABLE DE FIBRA ÓPTICA SM2C G657A1 (metros)	1700	$ 0.68	$ 1,156.00
2	CABLE DE COBRE STP CAT6a (metros)	1700	$ 1.46	$ 2,482.00
3	FACEPLATE JACK RJ-45 CAT6a	160	$ 6.68	$ 1,068.80
4	ARMARIO RACK 42U LANPRO	3	$ 768.50	$ 2,305.50
5	PATCH PANEL 48 PUERTOS CAT6a	8	$ 150.00	$ 1,200.00
6	BANDEJAS DE SOPORTE DE CABLE 6'' x 12'	35	$ 22.43	$ 785.05
7	TUBERÍA METÁLICA EMT 1/2''	50	$ 1.47	$ 73.50
8	TUBERÍA DE PVC 1/2''	1700	$ 0.83	$ 1,411.00
			TOTAL	$ 10,481.85

Tabla 5.2: Costos de equipos de fibra y cobre.

En la tabla anterior se muestran los costos de equipos de fibra y cobre. Los precios unitarios de los ítems 1 al 5, fueron consultados con personal de la empresa Telconet. Los precios unitarios de los ítems 6 al 8, fueron consultados con varios proveedores locales.

El valor 1700 en la cantidad de los ítems 1 y 2 significa 1700 metros, esto es, que se compraron 1700 metros de cable de cobre y fibra óptica. La cantidad del ítem 3 es 160 debido a que existen 160 puntos de conexión a cobre y a fibra alrededor de toda la vivienda.

Cada punto de conexión contiene dos puntos de cobre y dos puntos de fibra. El resto de ítems fueron comprados por las exigencias del proyecto.

Todos los precios unitarios incluyen el IVA.

5.1.3. Networking.

DETALLE DE COSTOS DE EQUIPOS				
	DISPOSITIVO	CANTIDAD	PRECIO UNITARIO INCLUIDO IVA	PRECIO TOTAL
1	Ruckus Access Point Zoneflex 7363	4	$ 445.00	$ 1,780.00
2	Ruckus Access Point Zoneflex 7025	1	$ 211.25	$ 211.25
3	Ruckus ZoneDirector 1100	1	$ 1,325.00	$ 1,325.00
4	Fortigate 80C	1	$ 715.00	$ 715.00
5	Router Cisco 1941 Series	1	$ 651.00	$ 651.00
6	Switch Catalyst WS-C2960S-48FPD-L	4	$ 2,433.10	$ 9,732.40
7	Cámara SNV-7080R	13	$ 680.00	$ 8,840.00
8	Servidor	1	$ 3,186.10	$ 3,186.10
			TOTAL	**$ 26,440.75**

Tabla 5.3: Costos de equipos de networking.

En la tabla anterior, se muestra el detalle de costos de equipos de networking. Los precios unitarios de estos equipos fueron consultados con personal de la empresa Telconet.

Todos los precios unitarios incluyen IVA.

5.2. Detalle de costos de la instalación.

5.2.1. Sistema Domótico.

DETALLE DE COSTOS DE INSTALACIÓN							
	ACTIVIDAD	HORAS POR DISPOSITIVO	# DE DISPOSITIVOS	TOTAL DE HORAS	COSTO HORA JEFE	COSTO HORA AYUDANTE	COSTO POR ACTIVIDAD
1	INSTALACIÓN DE VERA3	0.16	3	0.48	$ 3.75	$ 2.50	$ 3.00
2	INSTALACIÓN DE CÁMARAS	2	13	26	$ 3.75	$ 2.50	$ 162.50
3	INSTALACIÓN DE SENSORES DE MOVIMIENTO	0.5	17	8.5	$ 3.75	$ 2.50	$ 53.13
4	INSTALACIÓN DE CONTROLADORES HUE	0.5	21	10.5	$ 3.75	$ 2.50	$ 65.63
5	INSTALACIÓN DE FOCOS HUE	0.25	239	59.75	$ 3.75	$ 2.50	$ 373.44
6	INSTALACIÓN DE SENSORES DE APERTURA Y CERRADO DE PUERTAS	0.25	16	4	$ 3.75	$ 2.50	$ 25.00
7	INSTALACIÓN DE ACTUADORES DE PERSIANAS	0.75	18	13.5	$ 3.75	$ 2.50	$ 84.38
8	INSTALACIÓN DE TERMOSTATOS	0.75	14	10.5	$ 3.75	$ 2.50	$ 65.63
						SUBTOTAL	$ 832.69
						IVA 12%	$ 99.92
						TOTAL	**$ 932.61**

Tabla 5.4: Costos de instalación domótica.

En la tabla anterior se muestran los costos de instalación de los dispositivos domóticos. Se ha considerado una cantidad de horas por la instalación de cada dispositivo, en base a la experiencia personal de mi parte en este proyecto.

Es importante indicar que para la instalación se requieren dos personas: 1) un jefe y 2) un ayudante. El costo de la hora del jefe y ayudante resultan de la división de un sueldo de $600 y $400 respectivamente para 160, que representan las 160 horas laborables en el mes. El costo de cada actividad, se obtiene de la multiplicación entre el total de horas de cada dispositivo y la

suma de los dos costos por hora. Finalmente se cobra el IVA al subtotal obtenido por servicios prestados.

5.2.2. Cableado de fibra óptica y STP de cobre cat 6a.

DETALLE DE COSTOS DE INSTALACIÓN				
	ACTIVIDAD	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
1	TENDIDO DE CABLEADO DE COBRE	320	$ 40.00	$ 12,800.00
2	TENDIDO DE CABLEADO DE FIBRA ÓPTICA	320	$ 32.00	$ 10,240.00
3	CERTIFICACIÓN DE CABLEADO DE COBRE	320	$ 10.00	$ 3,200.00
4	CERTIFICACIÓN DE CABLEADO DE FIBRA ÓPTICA	320	$ 2.00	$ 640.00
5	INSTALACIÓN DE ARMARIOS DE RACKS	3	$ 80.00	$ 240.00
			SUBTOTAL	$ 27,120.00
			IVA 12%	$ 3,254.40
			TOTAL	**$ 30,374.40**

Tabla 5.5: Costos de instalación de la fibra y cobre.

En la tabla anterior se muestran los costos de instalación de la fibra y cobre. En la vivienda, existen 320 puntos de fibra y cobre. Una vez realizado el tendido del cableado, es necesario certificarlo, es decir, verificar que no hay cortes o daños del cableado en puntos intermedios. En el caso de la fibra solo se verifican cortes y en el caso del cobre se verifica y se ponchan los cables en ambos extremos. Los costos unitarios fueron provistos por personal de la empresa Ancascorp.

5.2.3. Networking.

DETALLE DE COSTOS DE INSTALACIÓN							
	ACTIVIDAD	HORAS POR DISPOSITIVO	# DE DISPOSITIVOS	TOTAL DE HORAS	COSTO HORA JEFE	COSTO HORA AYUDANTE	COSTO POR ACTIVIDAD
1	INSTALACIÓN DEL ROUTER	0.25	1	0.25	$ 3.75	$ 2.50	$ 1.56
2	INSTALACIÓN DEL ZONEDIRECTOR 1100	0.25	1	0.25	$ 3.75	$ 2.50	$ 1.56
3	INSTALACIÓN DEL ZONEFLEX 7363	0.75	4	3	$ 3.75	$ 2.50	$ 18.75
4	INSTALACIÓN DEL ZONEFLEX 7025	1	1	1	$ 3.75	$ 2.50	$ 6.25
5	INSTALACIÓN DEL FORTIGATE 80C	0.15	1	0.15	$ 3.75	$ 2.50	$ 0.94
6	INSTALACIÓN DE LOS SWITCHES	0.5	4	2	$ 3.75	$ 2.50	$ 12.50
7	INSTALACIÓN DEL SERVIDOR	0.5	1	0.5	$ 3.75	$ 2.50	$ 3.13
						SUBTOTAL	$ 44.69
						IVA 12%	$ 5.36
						TOTAL	$ 50.05

Tabla 5.6: Costos de la instalación del networking.

En la tabla anterior se muestran los costos de la instalación del networking en la vivienda.

Se ha considerado una cantidad de horas por la instalación de cada dispositivo, en base a la experiencia personal de mi parte en este proyecto.

Es importante indicar que para la instalación se requieren dos personas: 1) un jefe y 2) un ayudante. El costo de la hora del jefe y ayudante resultan de la división de un sueldo de $600 y $400 respectivamente para 160, que representan las 160 horas laborables en el mes. El costo de cada actividad, se obtiene de la multiplicación entre el total de horas de cada dispositivo y la

suma de los dos costos por hora. Finalmente se cobra el IVA al subtotal obtenido por servicios prestados.

5.3. Detalle de costos del diseño.

5.3.1. Sistema Domótico.

DETALLE DE COSTOS DE DISEÑO						
	ACTIVIDAD	HORAS POR DISPOSITIVO	# DE DISPOSITIVOS	TOTAL DE HORAS	COSTO HORA TÉCNICO	COSTO POR ACTIVIDAD
1	CONFIGURACIÓN DE LOS VERA3	0.5	3	1.5	$ 4.68	$ 7.02
2	INCLUSIÓN Y CONFIGURACIÓN DE LOS SENSORES DE MOVIMIENTO	0.5	17	8.5	$ 4.68	$ 39.78
3	INCLUSIÓN Y CONFIGURACIÓN DE LOS SENSORES DE APERTURA Y CERRADO DE PUERTAS	0.5	16	8	$ 4.68	$ 37.44
4	CONFIGURACIÓN DE LAS CÁMARAS	0.25	13	3.25	$ 4.68	$ 15.21
5	CONFIGURACIÓN DEL SERVIDOR	1	1	1	$ 4.68	$ 4.68
6	CONFIGURACIÓN DE LOS CONTROLADORES HUE Y SUS RESPECTIVOS FOCOS HUE	0.33	21	6.93	$ 4.68	$ 32.43
7	CONFIGURACIÓN DEL SISTEMA HUE EN EL VERA3	0.75	21	15.75	$ 4.60	$ 72.45
8	INCLUSIÓN Y CONFIGURACIÓN DE LOS ACTUADORES DE PERSIANAS	0.5	18	9	$ 4.68	$ 42.12
9	INCLUSIÓN Y CONFIGURACIÓN DE LOS TERMOSTATOS	0.5	14	7	$ 4.68	$ 32.76
					SUBTOTAL	$ 283.89
					IVA 12%	$ 34.07
					TOTAL	$ 317.96

Tabla 5.7: Costos del diseño domótico.

En la tabla anterior se muestran los costos del diseño de la domótica.

Se ha considerado una cantidad de horas por la instalación de cada dispositivo, en base a la experiencia personal de mi parte en este proyecto.

Es importante indicar que para la instalación se requiere solamente de un técnico. El costo de la hora del técnico resulta de la división de un sueldo de $750 para 160, que representan las 160 horas laborables en el mes. El costo de cada actividad, se obtiene de la multiplicación entre el total de horas de cada dispositivo y el costo por hora del técnico. Finalmente se cobra el IVA al subtotal obtenido por servicios prestados.

5.3.2. Cableado de fibra óptica y STP de cobre cat 6a.

DETALLE DE COSTOS DE INSTALACIÓN				
	ACTIVIDAD	HORAS	COSTO UNITARIO	COSTO TOTAL
1	DISEÑO DEL TENDIDO DE CABLEADO DE COBRE	4	$ 40.00	$ 160.00
2	DISEÑO DEL TENDIDO DE CABLEADO DE FIBRA ÓPTICA	4	$ 40.00	$ 160.00
			SUBTOTAL	$ 320.00
			IVA 12%	$ 38.40
			TOTAL	$ 358.40

Tabla 5.8: Costos del diseño del cableado de fibra y cobre.

En la tabla anterior se muestran los costos del diseño del cableado de fibra y cobre. Los costos unitarios y horas fueron consultados con personal de la empresa Ancascorp. Se cobra el IVA al subtotal obtenido por servicios prestados.

5.3.3. Networking.

DETALLE DE COSTOS DE DISEÑO						
	ACTIVIDAD	HORAS POR DISPOSITIVO	# DE DISPOSITIVOS	TOTAL DE HORAS	COSTO HORA TÉCNICO	COSTO POR ACTIVIDAD
1	DISEÑO DEL PLAN IPv4	3	1	3	$ 7.50	$ 22.50
2	CONFIGURACIÓN DEL ROUTER CISCO 1941	2.5	1	2.5	$ 7.50	$ 18.75
3	CONFIGURACIÓN DEL FORTIGATE 80C	3	1	3	$ 7.50	$ 22.50
4	CONFIGURACIÓN DEL SWITCH 1	2	1	2	$ 7.50	$ 15.00
5	CONFIGURACIÓN DEL SWITCH 2	2	1	2	$ 7.50	$ 15.00
6	CONFIGURACIÓN DEL SWITCH 3	2	1	2	$ 7.50	$ 15.00
7	CONFIGURACIÓN DEL SWITCH 4	2	1	2	$ 7.50	$ 15.00
8	CONFIGURACIÓN DEL ZONEDIRECTOR 1100	3	1	3	$ 7.50	$ 22.50
9	DIAGRAMAS DE VISIO	2	3	6	$ 7.50	$ 45.00
					SUBTOTAL	$ 191.25
					IVA 12%	$ 22.95
					TOTAL	$ 214.20

Tabla 5.9: Costos del diseño del networking.

En la tabla anterior se muestran los costos del diseño del networking.

Se ha considerado una cantidad de horas por la instalación de cada dispositivo, en base a la experiencia personal de mi parte en este proyecto.

Es importante indicar que para la instalación se requiere solamente de un técnico. El costo de la hora del técnico resulta de la división de un sueldo de $1200 para 160, que representan las 160 horas laborables en el mes. El costo de cada actividad, se obtiene de la multiplicación entre el total de horas de cada dispositivo y el costo por hora del técnico. Finalmente se cobra el IVA al subtotal obtenido por servicios prestados.

5.4. Detalle de costos totales.

DETALLE DEL COSTO TOTAL			
	ACTIVIDAD	**COSTO**	
1	EQUIPOS DEL SISTEMA DOMÓTICO	$	24,674.36
2	EQUIPOS DE FIBRA Y COBRE	$	10,481.85
3	EQUIPOS DE NETWORKING	$	26,440.75
4	INSTALACIÓN DEL SISTEMA DOMÓTICO	$	932.61
5	INSTALACIÓN DE FIBRA Y COBRE	$	30,374.40
6	INSTALACIÓN DE NETWORKING	$	50.05
7	DISEÑO DEL SISTEMA DOMÓTICO	$	317.96
8	DISEÑO DE FIBRA Y COBRE	$	358.40
9	DISEÑO DEL NETWORKING	$	214.20
	TOTAL	**$**	**93,844.58**

Tabla 5.10: Detalle del costo total del proyecto.

En la tabla anterior se muestra el detalle del costo total del proyecto. La suma de todos estos costos alcanza los $93844.58.

CONCLUSIONES

Las conclusiones de mayor relevancia que se pueden realizar a partir de todo lo expuesto anteriormente del presente proyecto de graduación son:

1. Mediante el presente proyecto, se ha logrado diseñar e implementar un sistema domótico de radiofrecuencia que brinda las gestiones de networking, seguridad y confort usando los protocolos Z-Wave y Zigbee y usando como controlador domótico principal al VERA3.

2. La gestión de networking brinda una red privada interna que puede ser accedida ya sea local y remotamente desde cualquier dispositivo en la internet usando un cliente VPN con un ancho de banda inicial de 100 Mbps, y en caso de requerir más ancho de banda, se tiene a disposición 100 Mbps extras. A su vez este acceso está protegido contra amenazas e intrusiones a través de un equipo que hace las veces de firewall y router dentro de la vivienda, que es el fortigate 80C. Una vez dentro de la red privada interna, es posible acceder a subredes agrupadas en VLAN's para los distintos dispositivos, ya sea de manera alámbrica o inalámbrica.

Los servicios inalámbricos son prestados por accesos de punto inalámbricos y supervisados por un controlador inalámbrico. La conexión alámbrica se realiza a través de los switches configurados en cascada.

3. La gestión de la seguridad brinda monitoreo de la vivienda a través de cámaras infrarrojas capaces de grabar en el día y en la noche y que almacenan todo este video en un servidor pero solo cuando detectan movimiento. Es en este mismo servidor donde se instala el software Net-i Ware, propio de las cámaras, que nos permite visualizar grabaciones de aproximadamete 30 días posteriores a la fecha actual de la búsqueda. Es posible detectar movimiento y la apertura o cerrado de puertas dentro de la vivienda. Mediante la creación y uso de las escenas, esta detección nos permite encender las luces en los sectores donde se detectó movimiento o la apertura/cierre de una puerta, cuando sea de noche.

4. La gestión del confort brinda iluminación a través del sistema Hue Philips que se comunica a través del protocolo Zigbee entre el controlador Hue y los focos Hue. Este sistema puede ser controlado a través del VERA3, el controlador principal de los dispositivos domóticos, que aunque se comunique mediante el protocolo Z-Wave, puede controlar al sistema Hue Philips, usando una aplicación instalada en nuestro controlador de manera gratuita. Vale destacar, que la gestión del confort también brinda climatización de la vivienda a través de termostatos, los cuales son

usados en escenas, para encender los aires acondicionados de la vivienda cuando la temperatura del sector en el que se encuentran pase los 28 °C y cuando la temperatura se encuentre por debajo de los 24 °C, los apague. Actuadores de persianas, mediante escenas, bajarán las persianas de los sectores donde se encuentren cuando sea de día y las subirán cuando sea de noche.

RECOMENDACIONES

1. Es mandatorio realizar un correcto etiquetado del nombre de cada dispositivo antes de ser instalados en una vivienda ya que de no realizarlo existe la posibilidad de incluir dispositivos a la red en sectores que no les corresponde y en proyectos como este, en el que existe una gran cantidad de dispositivos, toma mucho tiempo la corrección de errores.

2. Incluir e instalar uno a uno los dispositivos Z-Wave para poder verificar que el VERA3 tiene alcance de señal hacia ellos. Caso contrario tocará sacar el dispositivo y colocarlo en una mejor posición.

3. De manera frecuente, se recomienda que se realice un proceso de 'Healing' a la red Z-Wave porque la red tiende a desmoronarse ya que al ser una red de modo malla, si un nodo falla, pueden fallar varias rutas de acceso desde el VERA3 hasta algún dispositivo. Este proceso de

‘Healing’ se lo puede realizar mediante la interfaz web del VERA3 y en google se encuentra información al respecto.

4. En caso de querer agregar más funcionalidades a una escena, se recomienda leer sobre ‘LUUP’, el lenguaje de programación del VERA3 que mezcla, al lenguaje de programación Lua y a la tecnología Universal Plug&Play.

BIBLIOGRAFÍA

[1] Ingeniatic, Domótica, http://bit.ly/1CP2c0S, fecha de consulta 3 de noviembre del 2014.

[2] Domoservice, Dossier Divulgativo, http://bit.ly/1wRJSNT, fecha de consulta 5 de noviembre del 2014

[3] Tecsup Virtu@al, texto 4, http://bit.ly/1z23vZk, fecha de consulta 5 de noviembre del 2014

[4] Carlos, Domótica en el hogar, http://bit.ly/1Eytk6r, fecha de consulta 5 de noviembre del 2014

[5] jmhuidobro, Edificios Inteligentes y Domótica, http://bit.ly/1Cnstox, fecha de consulta 5 de noviembre del 2014

[6] Wikipedia, Red inalámbrica mallada, http://bit.ly/16goL2D, fecha de consulta 5 de noviembre del 2014

[7] Madero, Pedro, Domótica y Aplicaciones para el Hogar, http://bit.ly/160Gs5H, fecha de consulta 6 de noviembre del 2014

[8] Ortiz, Mario, Optimización del Sistema Inmótica en el Hotel Renaissance de Barcelona, http://bit.ly/1Dl5TcV, fecha de consulta 7 de noviembre del 2014

[9], Junta de Castilla y León, Vivienda Conectada - Las TIC en el Hogar, http://bit.ly/18FmbUJ, fecha de consulta 7 de noviembre del 2014

[10], Rathnayaka Dinusha, Potdar Vidyasagar, Kuruppu Samitha, Evaluation of Wireless Home Automation Technologies, http://bit.ly/168wXkD, fecha de consulta 7 de noviembre del 2014

[11] WiFiNotes, Wired vs Wireless home networks, http://bit.ly/1EXVLbv, fecha de consulta del 8 de noviembre del 2014

[12] iWatchLife, Five Stats that Prove the Home Automation Tsunami is Headed Your Way, http://bit.ly/1vdHr9B, fecha de consulta 8 de noviembre del 2014

[13] Wikipedia, Red de Computadoras, http://bit.ly/1aEiPkL, fecha de consulta 8 de noviembre del 2014

[14] Wikipedia, Wi-Fi, http://en.wikipedia.org/wiki/Wi-Fi, fecha de consulta 8 de noviembre del 2014

[15] Wikipedia, Bluetooth, http://bit.ly/1LzUaNz, fecha de consulta 8 de noviembre del 2014

[16] Wikipedia, Insteon, http://bit.ly/1z29ptb, fecha de consulta 9 de noviembre del 2014

[17] Insteon, Insteon Details, http://bit.ly/1tQzIlR, fecha de consulta 9 de noviembre del 2014

[18] Wikipedia, X-10, http://bit.ly/1DtZlJf, fecha de consulta 9 de noviembre del 2014

[19] Houston, Dave, X-10 RF PROTOCOL, http://bit.ly/1zqCWNV, fecha de consulta 9 de noviembre del 2014

[20] cm19a, The X10 RF and CM19a Guide, http://bit.ly/1BLpxwF, fecha de consulta 9 de noviembre del 2014

[21] Wikipedia, Z-Wave, http://bit.ly/1DtZEns, fecha de consulta 9 noviembre del 2014

[22] Wikipedia, ZigBee, http://bit.ly/1Kifq75, fecha de consulta 9 de noviembre del 2014

[23] Zensys, Z-Wave Protocol Overview, http://bit.ly/1Cnv5CS, fecha de consulta 10 de noviembre del 2014

[24] ZigBee, Standards, http://bit.ly/168zATx, fecha de consulta 10 de noviembre del 2014

[25] Vumnahata, Vera3 Picture, http://bit.ly/1zszK2J, fecha de consulta 2 de diciembre del 2014

[26] Getvera, Vera3, http://bit.ly/1z2aUrv, fecha de consulta 2 de diciembre del 2014

[27] Cisco, Cisco 1900 Series Integrated Services Router Hardware Installation, fecha de consulta 2 de diciembre del 2014

[28] Mercado Libre, Router Cisco 1941 Picture, http://bit.ly/1z2baqn, fecha de consulta 2 de diciembre del 2014

[29] Cisco, Cisco Catalyst 2960-S Series Switches, http://bit.ly/1vo3mA1, fecha de consulta 2 de diciembre del 2014

[30] Router-Switch, Switch Catalyst C2960S-48FPD Picture, http://bit.ly/1ogIFQE, fecha de consulta 2 de diciembre del 2014

[31] Wikipedia, Conmutador (dispositivo de red), http://bit.ly/1DlaI5T, fecha de consulta 2 de diciembre del 2014

[32] Fortinet, Fortigate/FortiWiFi - 80 Series, http://bit.ly/18FpfjY, fecha de consulta 2 de diciembre del 2014

[33] PacketWorks, Fortigate 80C, http://bit.ly/1uQaSh0, fecha de consulta 2 de diciembre del 2014

[34] Ruckus Wireless, ZoneDirector 1100 datasheet, http://bit.ly/168AcbK, fecha de consulta 2 de diciembre del 2014

[35] Barco Desinc, ZoneDirector 1100 Picture, http://bit.ly/1LzWEeN, fecha de consulta 2 de diciembre del 2014

[36] Ruckus Wireless, ZoneFlex 7363, http://bit.ly/1zsAtB0, fecha de consulta 6 de diciembre del 2014

[37] By far the cheapest, Zoneflex 7363 Picture, http://bit.ly/1Afsudp, fecha de consulta 6 de diciembre del 2014

[38] Ruckus Wireless, ZoneFlex 7025 Datasheet, http://bit.ly/1CnvQvC, fecha de consulta 6 de diciembre del 2014

[39] Ruckus Security, Zoneflex 7025 Picture, http://bit.ly/168BKCx, fecha de consulta 6 de diciembre del 2014

[40] Wikipedia, Rack, http://es.wikipedia.org/wiki/Rack, fecha de consulta 6 de diciembre del 2014

[41] Inselec, Rack Picture, http://bit.ly/1z2gPwP, fecha de consulta 6 de diciembre del 2014

[42] Wikipedia, Panel de conexiones, http://bit.ly/1dom815, fecha de consulta 6 de diciembre del 2014

[43] Excel Networking, Patch Panel Picture, http://bit.ly/1EXY9Pt, fecha de consulta 6 de diciembre del 2014

[44] Cable Organizer, Vertical Cable Organizer Picture, http://bit.ly/168BUd4, fecha de consulta 11 de diciembre del 2014

[45] ChatsWorth, Horizontal Cable Organizer Picture, http://bit.ly/1EyyJdH, fecha de consulta 11 de diciembre del 2014

[46] Wikipedia, Cable Tray, http://en.wikipedia.org/wiki/Cable_tray, fecha de consulta 6 de diciembre del 2014

[47] Tradeget, Cable Tray, http://bit.ly/1Dleo7J, fecha de consulta 6 de diciembre del 2014

[48] Wikipedia, Keystone Wall Plate, http://bit.ly/1z2hj5V, fecha de consulta 6 de diciembre del 2014

[49] ML Static, Faceplate picture, http://bit.ly/1tQI9O6, fecha de consulta 6 de diciembre del 2014

[50] Wikipedia, Metal Conduits, http://bit.ly/1BLz0nE, fecha de consulta 6 de diciembre del 2014

[51] Sapa Group, EMT picture, http://bit.ly/1K0p6Vq, fecha de consulta 6 de diciembre del 2014

[52] Wikipedia, Electrical Conduit, http://bit.ly/1BLz0nE, fecha de consulta 6 de diciembre del 2014

[53] Wikipedia, Electrical Conduit, http://bit.ly/160YjcC, fecha de consulta 6 de diciembre del 2014

[54] Wikipedia, Cable de categoría 6, http://bit.ly/1LA2yMW, fecha de consulta 6 de diciembre del 2014

[55], Preciolandia, Cable Cat 6a Picture, http://bit.ly/1Afx5MM, fecha de consulta 6 de diciembre del 2014

[56] LANPRO, Jacks CAT 6a, http://bit.ly/1zqNPPJ, fecha de consulta 6 de diciembre del 2014

[57] Wikipedia, Fibra Óptica, http://bit.ly/1610Fbs, fecha de consulta 6 de diciembre del 2014

[58] Compu Canjes, Fibra Óptica Picture, http://bit.ly/1Du5bdD, fecha de consulta 6 de diciembre del 2014

[59] Aeon Labs, Multisensor, http://bit.ly/1zsDNfx, fecha de consulta 6 de diciembre del 2014

[60] Asihome, Multisensor Picture, http://bit.ly/1K0quYl, fecha de consulta 26 de diciembre del 2014

[61] Aeon Labs, Multisensor Manual, http://bit.ly/1Kikt7z, fecha de consulta 6 de diciembre del 2014

[62] Everspring, HSP02 Wireless Z-wave PIR Detector, http://bit.ly/1zKBSGl, fecha de consulta 27 de diciembre del 2014

[63] Smarthome, Motion Sensor HSP02 Picture, http://bit.ly/1z2jR3S, fecha de consulta 6 de diciembre del 2014

[64] UK Automation, HSP02 Picture, http://bit.ly/1KikwjB, fecha de consulta 27 de diciembre del 2014

[65] Schlage, Motion Sensor Installation Instructions, http://bit.ly/1ypO09I, fecha de consulta 27 de diciembre del 2014

[66] Smarthome, Schlage RS200HC Picture, http://bit.ly/1zKC0Wm, fecha de consulta 27 de diciembre del 2014

[67] Express Controls, EZMotion+, http://bit.ly/1LA3BMV, fecha de consulta 27 de diciembre del 2014

[68] Smarthome USA, Aeon Labs Door/Window Sensor, http://bit.ly/18FsYxK, fecha de consulta 27 de diciembre del 2014

[69] Cloudfront, Door Window Sensor Picture, http://bit.ly/1AfykLM, fecha de consulta 27 de diciembre del 2014

[70] Samsung, SNV-7080R, http://bit.ly/1zqPpky, fecha de consulta 27 de diciembre del 2014

[71] Samsung, SNV-7080R Picture, http://bit.ly/1HFgFBa, fecha de consulta 27 de diciembre del 2014

[72] HP, HP ProLiant Gen8 DL380e, http://bit.ly/1z2kJpl, fecha de consulta 27 de diciembre del 2014

[73] Channel Central, HP ProLiant Gen8 DL380e Picture, http://bit.ly/168DDiK, fecha de consulta 27 de diciembre del 2014

[74] MeetHue, El sistema, http://bit.ly/1LA4mWd, fecha de consulta 7 de enero del 2015

[75] MeetHue, Tech Specs, http://bit.ly/1zqQ4m0, fecha de consulta 7 de enero del 2015

[76] Arstechnica, Hue Philips Picture, http://bit.ly/1z0Ddlg, fecha de consulta 7 de enero del 2015

[77] Zwaveproducts, Aeon Labs DSC14104-ZWUS - Z-Wave Micro Motor Controller, http://bit.ly/1zVuulB, fecha de consulta 7 de enero del 2015

[78] Vesternet, Micro Motor Controller Picture, http://bit.ly/1Dzxfge, fecha de consulta 7 de enero del 2015

[79] Amazon, Honeywell, Inc. TH8320ZW1000 ZwaveStat 7dayMultistage Vpro, http://amzn.to/1L4vMDm, fecha de consulta 22 de enero del 2015

ANEXOS

ANEXO 1. ARCHIVO DE CONFIGURACIÓN DEL FORTIGATE 80C

```
#config-version=FGT80C-5.00-FW-
build228-
130809:opmode=0:vdom=1:user=admin
#conf_file_ver=16962374523673432055
#buildno=0228
#global_vdom=1

config vdom
edit root
end

config vdom
edit PROTECTED
end

config global
config system global
    set fgd-alert-subscription advisory
latest-threat
    set gui-dlp disable
    set gui-dynamic-routing enable
    set gui-endpoint-control disable
    set gui-explicit-proxy disable
    set gui-spamfilter disable
    set gui-sslvpn-personal-bookmarks
enable
    set gui-sslvpn-realms enable
    set gui-vulnerability-scan disable
    set gui-wireless-controller disable
    set hostname "FGT80C-GYE-TTOPIC"
    set management-vdom "PROTECTED"
    set timezone 11
    set vdom-admin enable
end
config system accprofile
    edit "prof_admin"
        set admingrp read-write
        set authgrp read-write
        set endpoint-control-grp read-write
        set fwgrp read-write
        set loggrp read-write
        set mntgrp read-write
        set netgrp read-write
        set routegrp read-write
        set sysgrp read-write
        set updategrp read-write
        set utmgrp read-write
        set vpngrp read-write
        set wanoptgrp read-write
        set wifi read-write
    next
end
config wireless-controller vap
    edit "mesh.root"
        set vdom "root"
        set mesh-backhaul enable
        set ssid "fortinet.mesh.root"
        set passphrase ENC PNNJKDFf/
+AXV0dKLolTDxI2uf12RTSIWF46LKPw0
MUQKWdQdg==
    next
    edit "mesh.PROTECTED"
        set vdom "PROTECTED"
        set mesh-backhaul enable
        set ssid "fortinet.mesh.PROTECTED"
        set passphrase ENC
8P2MTDSgoFFTq9jBjodYM9yJF0IhAsPtA
p/7l5CVTOSc6nvhI2HI/5yrwARlsmUPyVg
nzJkzAE64PFtiuLZ+/0D+hM/YVE9ZlggV/
Wez6/R7xlwkSYgJ2VIQ==
    next
end
config system interface
    edit "wan1"
        set vdom "PROTECTED"
        set ip 186.3.144.73 255.255.255.224
        set allowaccess ping https
        set type physical
        set spillover-threshold 100000
        set alias "Wan_Netlife"
        set snmp-index 1
    next
    edit "wan2"
        set vdom "PROTECTED"
        set ip 206.165.205.130
255.255.255.248
        set allowaccess ping https
        set type physical
        set spillover-threshold 100000
        set alias "Wan_Telconet"
        set snmp-index 2
    next
    edit "Usuarios Wi-Fi"
        set vdom "PROTECTED"
        set ip 192.168.229.1 255.255.255.0
        set allowaccess ping https ssh
        set device-identification enable
        set snmp-index 12
        set interface "dmz"
        set vlanid 10
    next
    edit "Usuarios Red Ethernet Fija"
        set vdom "PROTECTED"
        set ip 192.168.230.1 255.255.255.0
        set allowaccess ping https ssh
        set device-identification enable
        set snmp-index 15
        set interface "dmz"
        set vlanid 11
    next
    edit "Servidores"
        set vdom "PROTECTED"
        set ip 172.31.1.1 255.255.255.240
        set allowaccess ping
        set device-identification enable
        set snmp-index 6
        set interface "dmz"
        set vlanid 30
    next
    edit "Switches"
        set vdom "PROTECTED"
        set ip 172.31.0.1 255.255.255.240
        set allowaccess ping
        set device-identification enable
        set snmp-index 13
        set interface "dmz"
        set vlanid 40
    next
    edit "Dispositivos"
        set vdom "PROTECTED"
        set ip 172.16.0.1 255.255.0.0
        set allowaccess ping https
        set device-identification enable
        set snmp-index 14
        set interface "dmz"
        set vlanid 50
    next
end
config system stp
    set status disable
end
config system admin
    edit "admin"
        set accprofile "super_admin"
        set vdom "root"
            config dashboard-tabs
                edit 1
                    set name "Status"
                next
                edit 2
                    set columns 1
                    set name "Top Sources"
                next
                edit 3
                    set columns 1
                    set name "Top Destinations"
                next
                edit 4
                    set columns 1
                    set name "Top Applications"
                next
            end
            config dashboard
                edit 43
                    set widget-type tr-history
                    set name "Netlife"
                    set tab-id 1
                    set column 1
                    set interface "wan1"
                    set refresh enable
                next
                edit 45
                    set widget-type sysop
                    set tab-id 1
                    set column 1
                next
                edit 1
                    set tab-id 1
                    set column 1
                next
                edit 2
                    set widget-type licinfo
                    set tab-id 1
                    set column 1
                next
                edit 44
                    set widget-type tr-history
                    set name "Telconet"
                    set tab-id 1
                    set column 2
                    set interface "wan2"
                    set refresh enable
                next
                edit 3
                    set widget-type sysres
                    set tab-id 1
                    set column 2
                next
                edit 42
                    set widget-type gui-features
                    set tab-id 1
                    set column 2
                next
                edit 4
                    set widget-type jsconsole
                    set tab-id 1
                    set column 2
                next
                edit 5
                    set widget-type alert
                    set tab-id 1
                    set column 2
                    set top-n 10
                next
                edit 21
                    set widget-type sessions
                    set tab-id 2
                    set column 1
                    set top-n 25
                    set sort-by msg-counts
                next
                edit 31
                    set widget-type sessions
                    set tab-id 3
                    set column 1
                    set top-n 25
                    set sort-by msg-counts
                    set report-by destination
                next
                edit 41
                    set widget-type sessions
                    set tab-id 4
                    set column 1
                    set top-n 25
                    set sort-by msg-counts
                    set report-by application
                next
            end
            config login-time
                edit "admin"
                    set last-failed-login 2013-11-
01 06:55:43
                    set last-login 2013-11-01
09:47:01
                next
            end
        set password ENC
+dp+dqPlvzKHbWb1Y2GRpr5vLfkw=
    next
    edit "ttopic"
        set trusthost1 192.168.229.0
255.255.255.0
        set accprofile "supin"
        set vdom "root"
        set password ENC
AK1paHu/4wJQXzwwotDJStmYg3DNjbpQ
IcAI=
    next
end
config system ha
    set override disable
end
config system dns
    set primary 200.93.192.148
    set secondary 200.93.192.161
end
config system replacemsg-image
```

```
    edit "logo_fnet"
        set image-base64 ''
        set image-type gif
    next
    edit "logo_fguard_wf"
        set image-base64 ''
        set image-type gif
    next
    edit "logo_fw_auth"
        set image-base64 ''
        set image-type png
    next
    edit "logo_v2_fnet"
        set image-base64 ''
        set image-type png
    next
    edit "logo_v2_fguard_wf"
        set image-base64 ''
        set image-type png
    next
end
config system replacemsg mail "email-block"
end
config system replacemsg mail "email-dlp-subject"
end
config system replacemsg mail "email-dlp-ban"
end
config system replacemsg mail "email-filesize"
end
config system replacemsg mail "partial"
end
config system replacemsg mail "smtp-block"
end
config system replacemsg mail "smtp-filesize"
end
config system replacemsg http "bannedword"
end
config system replacemsg http "url-block"
end
config system replacemsg http "urlfilter-err"
end
config system replacemsg http "infcache-block"
end
config system replacemsg http "http-block"
end
config system replacemsg http "http-filesize"
end
config system replacemsg http "http-dlp-ban"
end
config system replacemsg http "http-archive-block"
end
config system replacemsg http "http-contenttypeblock"
end
config system replacemsg http "https-invalid-cert-block"
end
config system replacemsg http "http-client-block"
end
config system replacemsg http "http-client-filesize"
end
config system replacemsg http "http-client-bannedword"
end
config system replacemsg http "http-post-block"
end
config system replacemsg http "http-client-archive-block"
end
config system replacemsg http "switching-protocols-block"
end
config system replacemsg webproxy "deny"
end
config system replacemsg webproxy "user-limit"
end
config system replacemsg webproxy "auth-challenge"
end
config system replacemsg webproxy "auth-login-fail"
end
config system replacemsg webproxy "auth-authorization-fail"
end
config system replacemsg webproxy "http-err"
end
config system replacemsg ftp "ftp-dl-blocked"
end
config system replacemsg ftp "ftp-dl-filesize"
end
config system replacemsg ftp "ftp-dl-dlp-ban"
end
config system replacemsg ftp "ftp-explicit-banner"
end
config system replacemsg ftp "ftp-dl-archive-block"
end
config system replacemsg nntp "nntp-dl-blocked"
end
config system replacemsg nntp "nntp-dl-filesize"
end
config system replacemsg nntp "nntp-dlp-subject"
end
config system replacemsg nntp "nntp-dlp-ban"
end
config system replacemsg fortiguard-wf "ftgd-block"
end
config system replacemsg fortiguard-wf "http-err"
end
config system replacemsg fortiguard-wf "ftgd-ovrd"
end
config system replacemsg fortiguard-wf "ftgd-quota"
end
config system replacemsg fortiguard-wf "ftgd-warning"
end
config system replacemsg spam "ipblocklist"
end
config system replacemsg spam "smtp-spam-dnsbl"
end
config system replacemsg spam "smtp-spam-feip"
end
config system replacemsg spam "smtp-spam-helo"
end
config system replacemsg spam "smtp-spam-emailblack"
end
config system replacemsg spam "smtp-spam-mimeheader"
end
config system replacemsg spam "reversedns"
end
config system replacemsg spam "smtp-spam-bannedword"
end
config system replacemsg spam "smtp-spam-ase"
end
config system replacemsg spam "submit"
end
config system replacemsg im "im-file-xfer-block"
end
config system replacemsg im "im-file-xfer-name"
end
config system replacemsg im "im-file-xfer-infected"
end
config system replacemsg im "im-file-xfer-size"
end
config system replacemsg im "im-dlp"
end
config system replacemsg im "im-dlp-ban"
end
config system replacemsg im "im-voice-chat-block"
end
config system replacemsg im "im-video-chat-block"
end
config system replacemsg im "im-photo-share-block"
end
config system replacemsg im "im-long-chat-block"
end
config system replacemsg alertmail "alertmail-virus"
end
config system replacemsg alertmail "alertmail-block"
end
config system replacemsg alertmail "alertmail-nids-event"
end
config system replacemsg alertmail "alertmail-crit-event"
end
config system replacemsg alertmail "alertmail-disk-full"
end
config system replacemsg admin "pre_admin-disclaimer-text"
end
config system replacemsg admin "post_admin-disclaimer-text"
end
config system replacemsg auth "auth-disclaimer-page-1"
end
config system replacemsg auth "auth-disclaimer-page-2"
end
config system replacemsg auth "auth-disclaimer-page-3"
end
config system replacemsg auth "auth-reject-page"
end
config system replacemsg auth "auth-login-page"
end
config system replacemsg auth "auth-login-failed-page"
end
config system replacemsg auth "auth-token-login-page"
end
config system replacemsg auth "auth-token-login-failed-page"
end
config system replacemsg auth "auth-success-msg"
end
config system replacemsg auth "auth-challenge-page"
end
config system replacemsg auth "auth-keepalive-page"
end
config system replacemsg auth "auth-portal-page"
end
config system replacemsg auth "auth-password-page"
end
config system replacemsg auth "auth-fortitoken-page"
end
```

```
config system replacemsg auth "auth-next-fortitoken-page"
end
config system replacemsg auth "auth-email-token-page"
end
config system replacemsg auth "auth-sms-token-page"
end
config system replacemsg auth "auth-email-harvesting-page"
end
config system replacemsg auth "auth-email-failed-page"
end
config system replacemsg auth "auth-cert-passwd-page"
end
config system replacemsg auth "auth-guest-print-page"
end
config system replacemsg auth "auth-guest-email-page"
end
config system replacemsg captive-portal-dflt "cpa-disclaimer-page-1"
end
config system replacemsg captive-portal-dflt "cpa-disclaimer-page-2"
end
config system replacemsg captive-portal-dflt "cpa-disclaimer-page-3"
end
config system replacemsg captive-portal-dflt "cpa-reject-page"
end
config system replacemsg captive-portal-dflt "cpa-login-page"
end
config system replacemsg captive-portal-dflt "cpa-login-failed-page"
end
config system replacemsg sslvpn "sslvpn-login"
end
config system replacemsg sslvpn "sslvpn-limit"
end
config system replacemsg ec "endpt-download-portal"
end
config system replacemsg ec "endpt-download-portal-mac"
end
config system replacemsg ec "endpt-download-portal-ios"
end
config system replacemsg ec "endpt-download-portal-aos"
end
config system replacemsg ec "endpt-download-portal-other"
end
config system replacemsg device-detection-portal "device-detection-failure"
end
config system replacemsg nac-quar "nac-quar-virus"
end
config system replacemsg nac-quar "nac-quar-dos"
end
config system replacemsg nac-quar "nac-quar-ips"
end
config system replacemsg nac-quar "nac-quar-dlp"
end
config system replacemsg traffic-quota "per-ip-shaper-block"
end
config system replacemsg utm "virus-html"
end
config system replacemsg utm "virus-text"
end
config system replacemsg utm "dlp-html"
end
config system replacemsg utm "dlp-text"
end
config vpn certificate ca
end
config vpn certificate local
end
config user device-category
    edit "ipad"
    next
    edit "iphone"
    next
    edit "gaming-console"
    next
    edit "blackberry-phone"
    next
    edit "blackberry-playbook"
    next
    edit "linux-pc"
    next
    edit "mac"
    next
    edit "windows-pc"
    next
    edit "android-phone"
    next
    edit "android-tablet"
    next
    edit "media-streaming"
    next
    edit "windows-phone"
    next
    edit "windows-tablet"
    next
    edit "fortinet-device"
    next
    edit "ip-phone"
    next
    edit "router-nat-device"
    next
    edit "other-network-device"
    next
    edit "collected-emails"
    next
    edit "all"
    next
end
config antivirus service "http"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "https"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "ftp"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "ftps"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "pop3"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "pop3s"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "imap"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "imaps"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "smtp"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "smtps"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "nntp"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "im"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config system resource-limits
end
config system vdom-property
    edit "root"
        set description "property limits for vdom root"
    next
    edit "PROTECTED"
        set description "property limits for vdom PROTECTED"
    next
end
config system session-sync
end
config system fortiguard
    set webfilter-sdns-server-ip "207.1.12.120"
end
config ips global
    set default-app-cat-mask 1844674400591
end
config ips dbinfo
    set version 1
end
config log fortianalyzer setting
    set status enable
    set server 141.188.140.198
    set reliable enable
end
config gui console
    unset preferences
end
config system session-helper
    edit 1
        set name pptp
        set port 1723
        set protocol 6
    next
    edit 2
        set name h323
        set port 1720
        set protocol 6
    next
    edit 3
        set name ras
        set port 1719
        set protocol 17
    next
    edit 4
        set name tns
        set port 1521
        set protocol 6
    next
    edit 5
        set name tftp
        set port 69
        set protocol 17
    next
    edit 6
        set name rtsp
        set port 554
        set protocol 6
    next
    edit 7
        set name rtsp
        set port 7070
        set protocol 6
    next
    edit 8
        set name rtsp
        set port 8554
        set protocol 6
    next
```

```
    edit 9
        set name ftp
        set port 21
        set protocol 6
    next
    edit 10
        set name mms
        set port 1863
        set protocol 6
    next
    edit 11
        set name pmap
        set port 111
        set protocol 6
    next
    edit 12
        set name pmap
        set port 111
        set protocol 17
    next
    edit 13
        set name sip
        set port 5060
        set protocol 17
    next
    edit 14
        set name dns-udp
        set port 53
        set protocol 17
    next
    edit 15
        set name rsh
        set port 514
        set protocol 6
    next
    edit 16
        set name rsh
        set port 512
        set protocol 6
    next
    edit 17
        set name dcerpc
        set port 135
        set protocol 6
    next
    edit 18
        set name dcerpc
        set port 135
        set protocol 17
    next
    edit 19
        set name mgcp
        set port 2427
        set protocol 17
    next
    edit 20
        set name mgcp
        set port 2727
        set protocol 17
    next
end
config system auto-install
    set auto-install-config enable
    set auto-install-image enable
end
config system ntp
    set ntpsync enable
    set syncinterval 60
end

end

config vdom
edit root
config system settings
    set sip-tcp-port 5060
    set sip-udp-port 5060
end
config system replacemsg-group
    edit "default"
        set comment "default"
    next
end
config firewall address
    edit "all"
    next
    edit "SSLVPN_TUNNEL_ADDR1"
        set type iprange
        set end-ip 10.212.134.210
        set start-ip 10.21.14.210
    next
end
config firewall multicast-address
    edit "all"
        set end-ip 219.255.255.255
        set start-ip 224.0.0.0
    next
    edit "all_hosts"
        set end-ip 224.0.0.1
        set start-ip 224.0.0.1
    next
    edit "all_routers"
        set end-ip 224.0.0.2
        set start-ip 224.0.0.2
    next
    edit "Bonjour"
        set end-ip 224.0.0.251
        set start-ip 224.0.0.251
    next
    edit "EIGRP"
        set end-ip 224.0.0.10
        set start-ip 224.0.0.10
    next
    edit "OSPF"
        set end-ip 224.0.0.6
        set start-ip 224.0.0.5
    next
end
config firewall address6
    edit "all"
    next
    edit "SSLVPN_TUNNEL_IPv6_ADDR1"
        set ip6 fdff:ffff::1/120
    next
end
config firewall service category
    edit "General"
        set comment "general services"
    next
    edit "Web Access"
        set comment "web access"
    next
    edit "File Access"
        set comment "file access"
    next
    edit "Email"
        set comment "email services"
    next
    edit "Network Services"
        set comment "network services"
    next
    edit "Authentication"
        set comment "authentication service"
    next
    edit "Remote Access"
        set comment "remote access"
    next
    edit "Tunneling"
        set comment "tunneling service"
    next
    edit "VoIP, Messaging & Other
Applications"
        set comment "VoIP, messaging, and
other applications"
    next
    edit "Web Proxy"
        set comment "Explicit web proxy"
    next
end
config firewall service custom
    edit "ALL"
        set category "General"
        set protocol IP
    next
    edit "ALL_TCP"
        set category "General"
        set tcp-portrange 1-65535
    next
    edit "ALL_UDP"
        set category "General"
        set udp-portrange 1-65535
    next
    edit "ALL_ICMP"
        set category "General"
        set protocol ICMP
        unset icmptype
    next
    edit "ALL_ICMP6"
        set category "General"
        set protocol ICMP6
        unset icmptype
    next
    edit "GRE"
        set category "Tunneling"
        set protocol IP
        set protocol-number 47
    next
    edit "AH"
        set category "Tunneling"
        set protocol IP
        set protocol-number 51
    next
    edit "ESP"
        set category "Tunneling"
        set protocol IP
        set protocol-number 50
    next
    edit "AOL"
        set visibility disable
        set tcp-portrange 5190-5194
    next
    edit "BGP"
        set category "Network Services"
        set tcp-portrange 179
    next
    edit "DHCP"
        set category "Network Services"
        set udp-portrange 67-68
    next
    edit "DNS"
        set category "Network Services"
        set tcp-portrange 53
        set udp-portrange 53
    next
    edit "FINGER"
        set visibility disable
        set tcp-portrange 79
    next
    edit "FTP"
        set category "File Access"
        set tcp-portrange 21
    next
    edit "FTP_GET"
        set category "File Access"
        set tcp-portrange 21
    next
    edit "FTP_PUT"
        set category "File Access"
        set tcp-portrange 21
    next
    edit "GOPHER"
        set visibility disable
        set tcp-portrange 70
    next
    edit "H323"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 1720 1503
        set udp-portrange 1719
    next
    edit "HTTP"
        set category "Web Access"
        set tcp-portrange 80
    next
    edit "HTTPS"
        set category "Web Access"
        set tcp-portrange 443
    next
    edit "IKE"
        set category "Tunneling"
        set udp-portrange 500 4500
    next
    edit "IMAP"
        set category "Email"
        set tcp-portrange 143
    next
    edit "IMAPS"
        set category "Email"
        set tcp-portrange 993
    next
    edit "Internet-Locator-Service"
        set visibility disable
        set tcp-portrange 389
    next
    edit "IRC"
        set category "VoIP, Messaging &
Other Applications"
```

```
        set tcp-portrange 6660-6669
    next
    edit "L2TP"
        set category "Tunneling"
        set tcp-portrange 1701
        set udp-portrange 1701
    next
    edit "LDAP"
        set category "Authentication"
        set tcp-portrange 389
    next
    edit "NetMeeting"
        set visibility disable
        set tcp-portrange 1720
    next
    edit "NFS"
        set category "File Access"
        set tcp-portrange 111 2049
        set udp-portrange 111 2049
    next
    edit "NNTP"
        set visibility disable
        set tcp-portrange 119
    next
    edit "NTP"
        set category "Network Services"
        set tcp-portrange 123
        set udp-portrange 123
    next
    edit "OSPF"
        set category "Network Services"
        set protocol IP
        set protocol-number 89
    next
    edit "PC-Anywhere"
        set category "Remote Access"
        set tcp-portrange 5631
        set udp-portrange 5632
    next
    edit "PING"
        set category "Network Services"
        set protocol ICMP
        set icmptype 8
        unset icmpcode
    next
    edit "TIMESTAMP"
        set protocol ICMP
        set visibility disable
        set icmptype 13
        unset icmpcode
    next
    edit "INFO_REQUEST"
        set protocol ICMP
        set visibility disable
        set icmptype 15
        unset icmpcode
    next
    edit "INFO_ADDRESS"
        set protocol ICMP
        set visibility disable
        set icmptype 17
        unset icmpcode
    next
    edit "ONC-RPC"
        set category "Remote Access"
        set tcp-portrange 111
        set udp-portrange 111
    next
    edit "DCE-RPC"
        set category "Remote Access"
        set tcp-portrange 135
        set udp-portrange 135
    next
    edit "POP3"
        set category "Email"
        set tcp-portrange 110
    next
    edit "POP3S"
        set category "Email"
        set tcp-portrange 995
    next
    edit "PPTP"
        set category "Tunneling"
        set tcp-portrange 1723
    next
    edit "QUAKE"
        set visibility disable
        set udp-portrange 26000 27000
27910 27960
    next
    edit "RAUDIO"
        set visibility disable
        set udp-portrange 7070
    next
    edit "REXEC"
        set visibility disable
        set tcp-portrange 512
    next
    edit "RIP"
        set category "Network Services"
        set udp-portrange 520
    next
    edit "RLOGIN"
        set visibility disable
        set tcp-portrange 513:512-1023
    next
    edit "RSH"
        set visibility disable
        set tcp-portrange 514:512-1023
    next
    edit "SCCP"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 2000
    next
    edit "SIP"
        set category "VoIP, Messaging &
Other Applications"
        set udp-portrange 5060
    next
    edit "SIP-MSNmessenger"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 1863
    next
    edit "SAMBA"
        set category "File Access"
        set tcp-portrange 139
    next
    edit "SMTP"
        set category "Email"
        set tcp-portrange 25
    next
    edit "SMTPS"
        set category "Email"
        set tcp-portrange 465
    next
    edit "SNMP"
        set category "Network Services"
        set tcp-portrange 161-162
        set udp-portrange 161-162
    next
    edit "SSH"
        set category "Remote Access"
        set tcp-portrange 22
    next
    edit "SYSLOG"
        set category "Network Services"
        set udp-portrange 514
    next
    edit "TALK"
        set visibility disable
        set udp-portrange 517-518
    next
    edit "TELNET"
        set category "Remote Access"
        set tcp-portrange 23
    next
    edit "TFTP"
        set category "File Access"
        set udp-portrange 69
    next
    edit "MGCP"
        set visibility disable
        set udp-portrange 2427 2727
    next
    edit "UUCP"
        set visibility disable
        set tcp-portrange 540
    next
    edit "VDOLIVE"
        set visibility disable
        set tcp-portrange 7000-7010
    next
    edit "WAIS"
        set visibility disable
        set tcp-portrange 210
    next
    edit "WINFRAME"
        set visibility disable
        set tcp-portrange 1494 2598
    next
    edit "X-WINDOWS"
        set category "Remote Access"
        set tcp-portrange 6000-6063
    next
    edit "PING6"
        set protocol ICMP6
        set visibility disable
        set icmptype 128
        unset icmpcode
    next
    edit "MS-SQL"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 1433 1434
    next
    edit "MYSQL"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 3306
    next
    edit "RDP"
        set category "Remote Access"
        set tcp-portrange 3389
    next
    edit "VNC"
        set category "Remote Access"
        set tcp-portrange 5900
    next
    edit "DHCP6"
        set category "Network Services"
        set udp-portrange 546 547
    next
    edit "SQUID"
        set category "Tunneling"
        set tcp-portrange 3128
    next
    edit "SOCKS"
        set category "Tunneling"
        set tcp-portrange 1080
        set udp-portrange 1080
    next
    edit "WINS"
        set category "Remote Access"
        set tcp-portrange 1512
        set udp-portrange 1512
    next
    edit "RADIUS"
        set category "Authentication"
        set udp-portrange 1812 1813
    next
    edit "RADIUS-OLD"
        set visibility disable
        set udp-portrange 1645 1646
    next
    edit "CVSPSERVER"
        set visibility disable
        set tcp-portrange 2401
        set udp-portrange 2401
    next
    edit "AFS3"
        set category "File Access"
        set tcp-portrange 7000-7009
        set udp-portrange 7000-7009
    next
    edit "TRACEROUTE"
        set category "Network Services"
        set udp-portrange 33434-33535
    next
    edit "RTSP"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 554 7070 8554
        set udp-portrange 554
    next
    edit "MMS"
        set visibility disable
        set tcp-portrange 1755
        set udp-portrange 1024-5000
    next
    edit "KERBEROS"
        set category "Authentication"
        set tcp-portrange 88
        set udp-portrange 88
    next
    edit "LDAP_UDP"
```

```
        set category "Authentication"
        set udp-portrange 389
    next
    edit "SMB"
        set category "File Access"
        set tcp-portrange 445
    next
    edit "webproxy"
        set explicit-proxy enable
        set category "Web Proxy"
        set protocol ALL
        set tcp-portrange 0-65535:0-65535
    next
end
config firewall service group
    edit "Email Access"
        set member "DNS" "IMAP" "IMAPS"
"POP3" "POP3S" "SMTP" "SMTPS"
    next
    edit "Web Access"
        set member "DNS" "HTTP" "HTTPS"
    next
    edit "Windows AD"
        set member "DCE-RPC" "DNS"
"KERBEROS" "LDAP" "LDAP_UDP"
"SAMBA" "SMB"
    next
    edit "Exchange Server"
        set member "DCE-RPC" "DNS"
"HTTPS"
    next
end
config webfilter ftgd-local-cat
    edit "custom1"
        set id 140
    next
    edit "custom2"
        set id 141
    next
end
config ips sensor
    edit "default"
        set comment "prevent critical attacks"
            config entries
                edit 1
                    set severity medium high
critical
                next
            end
    next
    edit "all_default"
        set comment "all predefined
signatures with default setting"
            config entries
                edit 1
                next
            end
    next
    edit "all_default_pass"
        set comment "all predefined
signatures with PASS action"
            config entries
                edit 1
                    set action pass
                next
            end
    next
    edit "protect_http_server"
        set comment "protect against HTTP
server-side vulnerabilities"
            config entries
                edit 1
                    set location server
                    set protocol HTTP
                next
            end
    next
    edit "protect_email_server"
        set comment "protect against EMail
server-side vulnerabilities"
            config entries
                edit 1
                    set location server
                    set protocol SMTP POP3
IMAP
                next
            end
    next
    edit "protect_client"
        set comment "protect against client-
side vulnerabilities"
            config entries
                edit 1
                    set location client
                next
            end
    next
end
config firewall shaper traffic-shaper
    edit "high-priority"
        set maximum-bandwidth 1048576
        set per-policy enable
    next
    edit "medium-priority"
        set maximum-bandwidth 1048576
        set per-policy enable
        set priority medium
    next
    edit "low-priority"
        set maximum-bandwidth 1048576
        set per-policy enable
        set priority low
    next
    edit "guarantee-100kbps"
        set guaranteed-bandwidth 100
        set maximum-bandwidth 1048576
        set per-policy enable
    next
    edit "shared-1M-pipe"
        set maximum-bandwidth 1024
    next
end
config application list
    edit "default"
        set comment "monitor all
applications"
            config entries
                edit 1
                    set action pass
                next
            end
    next
    edit "block-p2p"
            config entries
                edit 1
                    set category 2
                next
            end
    next
    edit "monitor-p2p-and-media"
            config entries
                edit 1
                    set action pass
                    set category 2
                next
                edit 2
                    set action pass
                    set category 5
                next
            end
    next
end
config dlp filepattern
    edit 1
            config entries
                edit "*.bat"
                next
                edit "*.com"
                next
                edit "*.dll"
                next
                edit "*.doc"
                next
                edit "*.exe"
                next
                edit "*.gz"
                next
                edit "*.hta"
                next
                edit "*.ppt"
                next
                edit "*.rar"
                next
                edit "*.scr"
                next
                edit "*.tar"
                next
                edit "*.tgz"
                next
                edit "*.vb?"
                next
                edit "*.wps"
                next
                edit "*.xl?"
                next
                edit "*.zip"
                next
                edit "*.pif"
                next
                edit "*.cpl"
                next
            end
        set name "builtin-patterns"
    next
    edit 2
            config entries
                edit "bat"
                    set filter-type type
                    set file-type bat
                next
                edit "exe"
                    set filter-type type
                    set file-type exe
                next
                edit "elf"
                    set filter-type type
                    set file-type elf
                next
                edit "hta"
                    set filter-type type
                    set file-type hta
                next
            end
        set name "all_executables"
    next
end
config dlp fp-sensitivity
    edit "Private"
    next
    edit "Critical"
    next
    edit "Warning"
    next
end
config dlp sensor
    edit "default"
        set comment "summary archive email
and web traffic"
        set summary-proto smtp pop3 imap
http-get http-post
    next
end
config webfilter content
end
config webfilter urlfilter
end
config spamfilter bword
end
config spamfilter bwl
end
config spamfilter mheader
end
config spamfilter dnsbl
end
config spamfilter iptrust
end
config client-reputation profile
        config web
            edit 1
                set group 1
                set level medium
            next
            edit 2
                set group 5
                set level critical
            next
        end
        config application
            edit 1
                set category 2
            next
            edit 2
                set category 6
                set level medium
            next
            edit 3
                set category 19
```

```
            set level high
        next
    end
end
config icap profile
    edit "default"
    next
end
config vpn ssl settings
    set port 443
end
config vpn ssl web portal
    edit "full-access"
        set allow-access web ftp smb telnet
ssh vnc rdp ping citrix rdpnative
portforward
        set page-layout double-column
            config widget
                edit 1
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set split-tunneling enable
                    set ip-pools
"SSLVPN_TUNNEL_ADDR1"
                    set ipv6-pools
"SSLVPN_TUNNEL_IPv6_ADDR1"
                next
                edit 2
                    set name "Session
Information"
                    set type info
                next
                edit 3
                    set name "Bookmarks"
                    set allow-apps web ftp smb
telnet ssh vnc rdp citrix rdpnative
portforward
                next
                edit 4
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb
telnet ssh vnc rdp ping citrix rdpnative
portforward
                next
                edit 5
                    set name "Login History"
                    set type history
                next
                edit 6
                    set name "FortiClient
Download"
                    set type forticlient-download
                    set column two
                next
            end
    next
    edit "web-access"
        set allow-access web ftp smb telnet
ssh vnc rdp ping citrix rdpnative
portforward
            config widget
                edit 1
                    set name "Session
Information"
                    set type info
                next
                edit 2
                    set name "Bookmarks"
                    set allow-apps web ftp smb
telnet ssh vnc rdp citrix rdpnative
portforward
                next
            end
    next
    edit "tunnel-access"
            config widget
                edit 1
                    set name "Tunnel Mode"
                    set type tunnel
                    set split-tunneling enable
                    set ip-pools
"SSLVPN_TUNNEL_ADDR1"
                    set ipv6-pools
"SSLVPN_TUNNEL_IPv6_ADDR1"
                next
                edit 2
                    set name "Session
Information"
                    set type info
                next
            end
    next
end
config user fortitoken
    edit "FTKMOB35056EA463"
        set license "FTMTRIAL00031658"
    next
    edit "FTKMOB35CE4517F8"
        set license "FTMTRIAL00031658"
    next
end
config user local
    edit "guest"
        set type password
        set passwd ENC
Vwa2Hsw/IRgWStf31SQ8xU9Jon2jdOQ/T
VeRLL5VC2/
/l0uZw7LO10A9YdzXPKxvmgQdCrL8M+Z
vZYTc3A==
    next
end
config user group
    edit "FSSO_Guest_Users"
        set group-type fsso-service
    next
    edit "Guest-group"
        set member "guest"
    next
end
config voip profile
    edit "default"
        set comment "default VoIP profile"
    next
    edit "strict"
            config sip
                set malformed-request-line
discard
                set malformed-header-via
discard
                set malformed-header-from
discard
                set malformed-header-to discard
                set malformed-header-call-id
discard
                set malformed-header-cseq
discard
                set malformed-header-rack
discard
                set malformed-header-rseq
discard
                set malformed-header-contact
discard
                set malformed-header-record-
route discard
                set malformed-header-route
discard
                set malformed-header-expires
discard
                set malformed-header-content-
type discard
                set malformed-header-content-
length discard
                set malformed-header-max-
forwards discard
                set malformed-header-allow
discard
                set malformed-header-p-
asserted-identity discard
                set malformed-header-sdp-v
discard
                set malformed-header-sdp-o
discard
                set malformed-header-sdp-s
discard
                set malformed-header-sdp-i
discard
                set malformed-header-sdp-c
discard
                set malformed-header-sdp-b
discard
                set malformed-header-sdp-z
discard
                set malformed-header-sdp-k
discard
                set malformed-header-sdp-a
discard
                set malformed-header-sdp-t
discard
                set malformed-header-sdp-r
discard
                set malformed-header-sdp-m
discard
            end
    next
end
config webfilter profile
    edit "default"
        set comment "default web filtering"
        set post-action comfort
            config ftgd-wf
                config filters
                    edit 1
                        set action warning
                        set category 2
                    next
                    edit 2
                        set action warning
                        set category 7
                    next
                    edit 3
                        set action warning
                        set category 8
                    next
                    edit 4
                        set action warning
                        set category 9
                    next
                    edit 5
                        set action warning
                        set category 11
                    next
                    edit 6
                        set action warning
                        set category 12
                    next
                    edit 7
                        set action warning
                        set category 13
                    next
                    edit 8
                        set action warning
                        set category 14
                    next
                    edit 9
                        set action warning
                        set category 15
                    next
                    edit 10
                        set action warning
                        set category 16
                    next
                    edit 11
                        set action warning
                    next
                    edit 12
                        set action warning
                        set category 57
                    next
                    edit 13
                        set action warning
                        set category 63
                    next
                    edit 14
                        set action warning
                        set category 64
                    next
                    edit 15
                        set action warning
                        set category 65
                    next
                    edit 16
                        set action warning
                        set category 66
                    next
                    edit 17
                        set action warning
                        set category 67
                    next
                    edit 18
                        set action block
                        set category 26
                    next
                end
```

```
        end
      set extended-utm-log disable
    next
    edit "web-filter-flow"
      set comment "flow-based web filter
profile"
      set inspection-mode flow-based
      set post-action comfort
        config ftgd-wf
          config filters
            edit 1
              set action warning
              set category 2
            next
            edit 2
              set action warning
              set category 7
            next
            edit 3
              set action warning
              set category 8
            next
            edit 4
              set action warning
              set category 9
            next
            edit 5
              set action warning
              set category 11
            next
            edit 6
              set action warning
              set category 12
            next
            edit 7
              set action warning
              set category 13
            next
            edit 8
              set action warning
              set category 14
            next
            edit 9
              set action warning
              set category 15
            next
            edit 10
              set action warning
              set category 16
            next
            edit 11
              set action warning
            next
            edit 12
              set action warning
              set category 57
            next
            edit 13
              set action warning
              set category 63
            next
            edit 14
              set action warning
              set category 64
            next
            edit 15
              set action warning
              set category 65
            next
            edit 16
              set action warning
              set category 66
            next
            edit 17
              set action warning
              set category 67
            next
            edit 18
              set action block
              set category 26
            next
          end
        end
      set extended-utm-log disable
    next
end
config webfilter override
end
config webfilter override-user
end
config webfilter ftgd-warning
end
config webfilter ftgd-local-rating
end
config webfilter search-engine
    edit "google"
      set hostname ".*\\.google\\..*"
      set url
"^\\/((custom|search|images|videosearch|w
ebhp)\\?)"
      set query "q="
      set safesearch url
      set safesearch-str "&safe=active"
    next
    edit "yahoo"
      set hostname ".*\\.yahoo\\..*"
      set url
"^\\/search(\\/video|\\/images){0,1}(\\?|;)"
      set query "p="
      set safesearch url
      set safesearch-str "&vm=r"
    next
    edit "bing"
      set hostname "www\\.bing\\.com"
      set url
"^(\\/images|\\/videos)?(\\/search|\\/async)\\
?"
      set query "q="
      set safesearch url
      set safesearch-str "&adlt=strict"
    next
    edit "yandex"
      set hostname "yandex\\..*"
      set url
"^\\/(yand){0,1}(search)[\\/]{0,}.{0,}\\?"
      set query "text="
      set safesearch url
      set safesearch-str "&fyandex=1"
    next
    edit "youtube"
      set hostname ".*\\.youtube\\..*"
      set safesearch header
    next
    edit "baidu"
      set hostname ".*\\.baidu\\.com"
      set url "^\\/s?\\?"
      set query "wd="
    next
    edit "baidu2"
      set hostname ".*\\.baidu\\.com"
      set url "^\\/(ns|q|m|i|v)\\?"
      set query "word="
    next
    edit "baidu3"
      set hostname "tieba\\.baidu\\.com"
      set url "^\\/f\\?"
      set query "kw="
    next
end
config antivirus profile
    edit "default"
      set comment "scan and delete virus"
        config http
          set options scan
        end
        config ftp
          set options scan
        end
        config imap
          set options scan
        end
        config pop3
          set options scan
        end
        config smtp
          set options scan
        end
        config nntp
          set options scan
        end
        config im
          set options scan
        end
    next
    edit "AV-flow"
      set comment "flow-based scan and
delete virus"
      set inspection-mode flow-based
        config http
          set options scan
        end
        config ftp
          set options scan
        end
        config imap
          set options scan
        end
        config pop3
          set options scan
        end
        config smtp
          set options scan
        end
        config nntp
          set options scan
        end
        config im
          set options scan
        end
    next
end
config spamfilter profile
    edit "default"
      set comment "malware and phishing
URL filtering"
    next
end
config web-proxy global
    set proxy-fqdn "default.fqdn"
end
config firewall schedule recurring
    edit "always"
      set day sunday monday tuesday
wednesday thursday friday saturday
    next
end
config firewall profile-protocol-options
    edit "default"
      set comment "all default services"
        config http
          set ports 80
          set options no-content-summary
          unset post-lang
        end
        config ftp
          set ports 21
          set options no-content-summary
splice
        end
        config imap
          set ports 143
          set options fragmail no-content-
summary
        end
        config mapi
          set ports 135
          set options fragmail no-content-
summary
        end
        config pop3
          set ports 110
          set options fragmail no-content-
summary
        end
        config smtp
          set ports 25
          set options fragmail no-content-
summary splice
        end
        config nntp
          set ports 119
          set options no-content-summary
splice
        end
        config im
          unset options
        end
        config dns
          set ports 53
        end
    next
end
config firewall deep-inspection-options
    edit "default"
      set comment "all default services"
        config https
          set ports 443
```

```
            end
            config ftps
                set ports 990
            end
            config imaps
                set ports 993
            end
            config pop3s
                set ports 995
            end
            config smtps
                set ports 465
            end
        next
    end
    config firewall identity-based-route
    end
    config firewall policy
    end
    config firewall local-in-policy
    end
    config firewall policy6
    end
    config firewall local-in-policy6
    end
    config firewall ttl-policy
    end
    config firewall policy64
    end
    config firewall policy46
    end
    config firewall interface-policy
    end
    config firewall interface-policy6
    end
    config firewall sniff-interface-policy
    end
    config firewall sniff-interface-policy6
    end
    config firewall DoS-policy
    end
    config firewall DoS-policy6
    end
    config firewall sniffer
    end
    config endpoint-control profile
        edit "default"
            config forticlient-winmac-settings
                set forticlient-av enable
                set forticlient-wf enable
                set forticlient-wf-profile "default"
                set forticlient-ui-options av wf af
    vpn vs
            end
            config forticlient-android-settings
                set forticlient-wf enable
                set forticlient-wf-profile "default"
            end
            config forticlient-ios-settings
                set forticlient-wf enable
                set forticlient-wf-profile "default"
            end
        next
    end
    config wireless-controller wids-profile
        edit "default"
            set comment "default wids profile"
            set wireless-bridge enable
            set deauth-broadcast enable
            set null-ssid-probe-resp enable
            set long-duration-attack enable
            set invalid-mac-oui enable
            set weak-wep-iv enable
            set auth-frame-flood enable
            set assoc-frame-flood enable
            set spoofed-deauth enable
            set asleap-attack enable
            set eapol-start-flood enable
            set eapol-logoff-flood enable
            set eapol-succ-flood enable
            set eapol-fail-flood enable
            set eapol-pre-succ-flood enable
            set eapol-pre-fail-flood enable
        next
    end
    config wireless-controller wtp-profile
        edit "11n-only"
            config platform
                set type 60C
            end
            set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
        next
        edit "FAP112B-default"
            config platform
                set type 112B
            end
            set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
        next
        edit "FAP220B-default"
            set ap-country US
            config radio-1
                set band 802.11n-5G
            end
            config radio-2
                set band 802.11n
            end
        next
        edit "FAP210B-default"
            config platform
                set type 210B
            end
            set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
        next
        edit "FAP222B-default"
            config platform
                set type 222B
            end
            set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set band 802.11n-5G
            end
        next
        edit "FAP320B-default"
            config platform
                set type 320B
            end
            set ap-country US
            config radio-1
                set band 802.11n-5G
            end
            config radio-2
                set band 802.11n
            end
        next
        edit "FAP11C-default"
            config platform
                set type 11C
            end
            set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
        next
    end
    config router rip
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "ospf"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    end
    config router ripng
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "ospf"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    end
    config router ospf
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    end
    config router ospf6
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    end
    config router bgp
        config redistribute "connected"
        end
        config redistribute "rip"
        end
        config redistribute "ospf"
        end
        config redistribute "static"
        end
        config redistribute "isis"
        end
        config redistribute6 "connected"
        end
        config redistribute6 "rip"
        end
        config redistribute6 "ospf"
        end
        config redistribute6 "static"
        end
        config redistribute6 "isis"
        end
    end
    config router isis
        config redistribute "connected"
        end
        config redistribute "rip"
        end
        config redistribute "ospf"
        end
        config redistribute "bgp"
        end
        config redistribute "static"
        end
    end
    config router multicast
    end
    end

    config vdom
    edit PROTECTED
    config system settings
        set v4-ecmp-mode usage-based
        set sip-tcp-port 5060
        set sip-udp-port 5060
    end
    config system replacemsg-group
        edit "default"
            set comment "default"
        next
    end
    config system dhcp server
```

```
    edit 4
        set default-gateway 10.55.226.1
        set dns-service default
        set interface "Voz"
            config ip-range
                edit 1
                    set end-ip 10.55.226.254
                    set start-ip 10.55.226.2
                next
            end
        set netmask 255.255.255.0
    next
    edit 3
        set default-gateway 192.168.229.1
        set dns-service default
        set interface "Usuarios"
            config ip-range
                edit 1
                    set end-ip 192.168.229.254
                    set start-ip 192.168.229.2
                next
            end
        set netmask 255.255.255.0
    next
    edit 5
        set default-gateway 172.16.0.1
        set dns-service default
        set interface "Dispositivos"
            config ip-range
                edit 1
                    set end-ip 172.16.0.254
                    set start-ip 172.16.0.2
                next
            end
        set netmask 255.255.0.0
        set option1 43
'3138312e3139382e31302e313436'
    next
end
config firewall address
    edit "all"
    next
    edit "SSLVPN_TUNNEL_ADDR1"
        set type iprange
        set end-ip 10.212.134.210
        set start-ip 10.212.134.200
    next
    edit "Local-Subnet"
        set subnet 172.16.0.0 255.255.0.0
    next
    edit "Servidores"
        set subnet 172.31.1.0
255.255.255.240
    next
end
config firewall multicast-address
    edit "all_hosts"
        set end-ip 224.0.0.1
        set start-ip 224.0.0.1
    next
    edit "all_routers"
        set end-ip 224.0.0.2
        set start-ip 224.0.0.2
    next
    edit "Bonjour"
        set end-ip 224.0.0.251
        set start-ip 224.0.0.251
    next
    edit "EIGRP"
        set end-ip 224.0.0.10
        set start-ip 224.0.0.10
    next
    edit "OSPF"
        set end-ip 224.0.0.6
        set start-ip 224.0.0.5
    next
    edit "all"
        set end-ip 239.255.255.255
        set start-ip 224.0.0.0
    next
end
config firewall address6
    edit "all"
    next
    edit "SSLVPN_TUNNEL_IPv6_ADDR1"
        set ip6 fdff:ffff::1/120
    next
end
config firewall service category
    edit "General"
        set comment "general services"
    next
    edit "Web Access"
        set comment "web access"
    next
    edit "File Access"
        set comment "file access"
    next
    edit "Email"
        set comment "email services"
    next
    edit "Network Services"
        set comment "network services"
    next
    edit "Authentication"
        set comment "authentication service"
    next
    edit "Remote Access"
        set comment "remote access"
    next
    edit "Tunneling"
        set comment "tunneling service"
    next
    edit "VoIP, Messaging & Other
Applications"
        set comment "VoIP, messaging, and
other applications"
    next
    edit "Web Proxy"
        set comment "Explicit web proxy"
    next
end
config firewall service custom
    edit "ALL"
        set category "General"
        set protocol IP
    next
    edit "ALL_TCP"
        set category "General"
        set tcp-portrange 1-65535
    next
    edit "ALL_UDP"
        set category "General"
        set udp-portrange 1-65535
    next
    edit "ALL_ICMP"
        set category "General"
        set protocol ICMP
        unset icmptype
    next
    edit "ALL_ICMP6"
        set category "General"
        set protocol ICMP6
        unset icmptype
    next
    edit "GRE"
        set category "Tunneling"
        set protocol IP
        set protocol-number 47
    next
    edit "AH"
        set category "Tunneling"
        set protocol IP
        set protocol-number 51
    next
    edit "ESP"
        set category "Tunneling"
        set protocol IP
        set protocol-number 50
    next
    edit "AOL"
        set visibility disable
        set tcp-portrange 5190-5194
    next
    edit "BGP"
        set category "Network Services"
        set tcp-portrange 179
    next
    edit "DHCP"
        set category "Network Services"
        set udp-portrange 67-68
    next
    edit "DNS"
        set category "Network Services"
        set tcp-portrange 53
        set udp-portrange 53
    next
    edit "FINGER"
        set visibility disable
        set tcp-portrange 79
    next
    edit "FTP"
        set category "File Access"
        set tcp-portrange 21
    next
    edit "FTP_GET"
        set category "File Access"
        set tcp-portrange 21
    next
    edit "FTP_PUT"
        set category "File Access"
        set tcp-portrange 21
    next
    edit "GOPHER"
        set visibility disable
        set tcp-portrange 70
    next
    edit "H323"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 1720 1503
        set udp-portrange 1719
    next
    edit "HTTP"
        set category "Web Access"
        set tcp-portrange 80
    next
    edit "HTTPS"
        set category "Web Access"
        set tcp-portrange 443
    next
    edit "IKE"
        set category "Tunneling"
        set udp-portrange 500 4500
    next
    edit "IMAP"
        set category "Email"
        set tcp-portrange 143
    next
    edit "IMAPS"
        set category "Email"
        set tcp-portrange 993
    next
    edit "Internet-Locator-Service"
        set visibility disable
        set tcp-portrange 389
    next
    edit "IRC"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 6660-6669
    next
    edit "L2TP"
        set category "Tunneling"
        set tcp-portrange 1701
        set udp-portrange 1701
    next
    edit "LDAP"
        set category "Authentication"
        set tcp-portrange 389
    next
    edit "NetMeeting"
        set visibility disable
        set tcp-portrange 1720
    next
    edit "NFS"
        set category "File Access"
        set tcp-portrange 111 2049
        set udp-portrange 111 2049
    next
    edit "NNTP"
        set visibility disable
        set tcp-portrange 119
    next
    edit "NTP"
        set category "Network Services"
        set tcp-portrange 123
        set udp-portrange 123
    next
    edit "OSPF"
        set category "Network Services"
        set protocol IP
        set protocol-number 89
    next
    edit "PC-Anywhere"
        set category "Remote Access"
        set tcp-portrange 5631
```

```
        set udp-portrange 5632
    next
    edit "PING"
        set category "Network Services"
        set protocol ICMP
        set icmptype 8
        unset icmpcode
    next
    edit "TIMESTAMP"
        set protocol ICMP
        set visibility disable
        set icmptype 13
        unset icmpcode
    next
    edit "INFO_REQUEST"
        set protocol ICMP
        set visibility disable
        set icmptype 15
        unset icmpcode
    next
    edit "INFO_ADDRESS"
        set protocol ICMP
        set visibility disable
        set icmptype 17
        unset icmpcode
    next
    edit "ONC-RPC"
        set category "Remote Access"
        set tcp-portrange 111
        set udp-portrange 111
    next
    edit "DCE-RPC"
        set category "Remote Access"
        set tcp-portrange 135
        set udp-portrange 135
    next
    edit "POP3"
        set category "Email"
        set tcp-portrange 110
    next
    edit "POP3S"
        set category "Email"
        set tcp-portrange 995
    next
    edit "PPTP"
        set category "Tunneling"
        set tcp-portrange 1723
    next
    edit "QUAKE"
        set visibility disable
        set udp-portrange 26000 27000
27910 27960
    next
    edit "RAUDIO"
        set visibility disable
        set udp-portrange 7070
    next
    edit "REXEC"
        set visibility disable
        set tcp-portrange 512
    next
    edit "RIP"
        set category "Network Services"
        set udp-portrange 520
    next
    edit "RLOGIN"
        set visibility disable
        set tcp-portrange 513:512-1023
    next
    edit "RSH"
        set visibility disable
        set tcp-portrange 514:512-1023
    next
    edit "SCCP"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 2000
    next
    edit "SIP"
        set category "VoIP, Messaging &
Other Applications"
        set udp-portrange 5060
    next
    edit "SIP-MSNmessenger"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 1863
    next
    edit "SAMBA"
        set category "File Access"
        set tcp-portrange 139
    next
    edit "SMTP"
        set category "Email"
        set tcp-portrange 25
    next
    edit "SMTPS"
        set category "Email"
        set tcp-portrange 465
    next
    edit "SNMP"
        set category "Network Services"
        set tcp-portrange 161-162
        set udp-portrange 161-162
    next
    edit "SSH"
        set category "Remote Access"
        set tcp-portrange 22
    next
    edit "SYSLOG"
        set category "Network Services"
        set udp-portrange 514
    next
    edit "TALK"
        set visibility disable
        set udp-portrange 517-518
    next
    edit "TELNET"
        set category "Remote Access"
        set tcp-portrange 23
    next
    edit "TFTP"
        set category "File Access"
        set udp-portrange 69
    next
    edit "MGCP"
        set visibility disable
        set udp-portrange 2427 2727
    next
    edit "UUCP"
        set visibility disable
        set tcp-portrange 540
    next
    edit "VDOLIVE"
        set visibility disable
        set tcp-portrange 7000-7010
    next
    edit "WAIS"
        set visibility disable
        set tcp-portrange 210
    next
    edit "WINFRAME"
        set visibility disable
        set tcp-portrange 1494 2598
    next
    edit "X-WINDOWS"
        set category "Remote Access"
        set tcp-portrange 6000-6063
    next
    edit "PING6"
        set protocol ICMP6
        set visibility disable
        set icmptype 128
        unset icmpcode
    next
    edit "MS-SQL"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 1433 1434
    next
    edit "MYSQL"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 3306
    next
    edit "RDP"
        set category "Remote Access"
        set tcp-portrange 3389
    next
    edit "VNC"
        set category "Remote Access"
        set tcp-portrange 5900
    next
    edit "DHCP6"
        set category "Network Services"
        set udp-portrange 546 547
    next
    edit "SQUID"
        set category "Tunneling"
        set tcp-portrange 3128
    next
    edit "SOCKS"
        set category "Tunneling"
        set tcp-portrange 1080
        set udp-portrange 1080
    next
    edit "WINS"
        set category "Remote Access"
        set tcp-portrange 1512
        set udp-portrange 1512
    next
    edit "RADIUS"
        set category "Authentication"
        set udp-portrange 1812 1813
    next
    edit "RADIUS-OLD"
        set visibility disable
        set udp-portrange 1645 1646
    next
    edit "CVSPSERVER"
        set visibility disable
        set tcp-portrange 2401
        set udp-portrange 2401
    next
    edit "AFS3"
        set category "File Access"
        set tcp-portrange 7000-7009
        set udp-portrange 7000-7009
    next
    edit "TRACEROUTE"
        set category "Network Services"
        set udp-portrange 33434-33535
    next
    edit "RTSP"
        set category "VoIP, Messaging &
Other Applications"
        set tcp-portrange 554 7070 8554
        set udp-portrange 554
    next
    edit "MMS"
        set visibility disable
        set tcp-portrange 1755
        set udp-portrange 1024-5000
    next
    edit "KERBEROS"
        set category "Authentication"
        set tcp-portrange 88
        set udp-portrange 88
    next
    edit "LDAP_UDP"
        set category "Authentication"
        set udp-portrange 389
    next
    edit "SMB"
        set category "File Access"
        set tcp-portrange 445
    next
    edit "webproxy"
        set explicit-proxy enable
        set category "Web Proxy"
        set protocol ALL
        set tcp-portrange 0-65535:0-65535
    next
end
config firewall service group
    edit "Email Access"
        set member "DNS" "IMAP" "IMAPS"
"POP3" "POP3S" "SMTP" "SMTPS"
    next
    edit "Web Access"
        set member "DNS" "HTTP" "HTTPS"
    next
    edit "Windows AD"
        set member "DCE-RPC" "DNS"
"KERBEROS" "LDAP" "LDAP_UDP"
"SAMBA" "SMB"
    next
    edit "Exchange Server"
        set member "DCE-RPC" "DNS"
"HTTPS"
    next
end
config webfilter ftgd-local-cat
    edit "custom1"
        set id 140
    next
    edit "custom2"
```

```
        set id 141
    next
end
config ips sensor
    edit "default"
        set comment "prevent critical attacks"
            config entries
                edit 1
                    set severity medium high
critical
                next
            end
    next
    edit "all_default"
        set comment "all predefined
signatures with default setting"
            config entries
                edit 1
                next
            end
    next
    edit "all_default_pass"
        set comment "all predefined
signatures with PASS action"
            config entries
                edit 1
                    set action pass
                next
            end
    next
    edit "protect_http_server"
        set comment "protect against HTTP
server-side vulnerabilities"
            config entries
                edit 1
                    set location server
                    set protocol HTTP
                next
            end
    next
end
config firewall shaper traffic-shaper
    edit "high-priority"
        set maximum-bandwidth 1048576
        set per-policy enable
    next
    edit "medium-priority"
        set maximum-bandwidth 1048576
        set per-policy enable
        set priority medium
    next
    edit "low-priority"
        set maximum-bandwidth 1048576
        set per-policy enable
        set priority low
    next
    edit "guarantee-100kbps"
        set guaranteed-bandwidth 100
        set maximum-bandwidth 1048576
        set per-policy enable
    next
    edit "shared-1M-pipe"
        set maximum-bandwidth 1024
    next
end
config application list
    edit "default"
        set comment "monitor all
applications"
            config entries
                edit 1
                    set action pass
                next
            end
    next
    edit "block-p2p"
            config entries
                edit 1
                    set category 2
                next
            end
    next
    edit "monitor-p2p-and-media"
            config entries
                edit 1
                    set action pass
                    set category 2
                next
                edit 2
                    set action pass
                    set category 5
                next
            end
    next
end
config dlp filepattern
    edit 1
            config entries
                edit "*.bat"
                next
                edit "*.com"
                next
                edit "*.dll"
                next
                edit "*.doc"
                next
                edit "*.exe"
                next
                edit "*.gz"
                next
                edit "*.hta"
                next
                edit "*.ppt"
                next
                edit "*.rar"
                next
                edit "*.scr"
                next
                edit "*.tar"
                next
                edit "*.tgz"
                next
                edit "*.vb?"
                next
                edit "*.wps"
                next
                edit "*.xl?"
                next
                edit "*.zip"
                next
                edit "*.pif"
                next
                edit "*.cpl"
                next
            end
        set name "builtin-patterns"
    next
    edit 2
            config entries
                edit "bat"
                    set filter-type type
                    set file-type bat
                next
                edit "exe"
                    set filter-type type
                    set file-type exe
                next
                edit "elf"
                    set filter-type type
                    set file-type elf
                next
                edit "hta"
                    set filter-type type
                    set file-type hta
                next
            end
        set name "all_executables"
    next
end
config dlp fp-sensitivity
    edit "Private"
    next
    edit "Critical"
    next
    edit "Warning"
    next
end
config dlp sensor
    edit "default"
        set comment "summary archive email
and web traffic"
            set summary-proto smtp pop3 imap
http-get http-post
    next
end
config webfilter content
end
config webfilter urlfilter
end
config spamfilter bword
end
config spamfilter bwl
end
config spamfilter mheader
end
config spamfilter dnsbl
end
config spamfilter iptrust
end
config client-reputation profile
        config web
            edit 1
                set group 1
                set level medium
            next
            edit 2
                set group 5
                set level critical
            next
        end
        config application
            edit 1
                set category 2
            next
            edit 2
                set category 6
                set level medium
            next
            edit 3
                set category 19
                set level high
            next
        end
end
config icap profile
    edit "default"
    next
end
config vpn ssl settings
    set tunnel-ip-pools
"SSLVPN_TUNNEL_ADDR1"
end
ssh vnc rdp ping citrix rdpnative
portforward
        set page-layout double-column
            config widget
                edit 1
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set split-tunneling enable
                    set ip-pools
"SSLVPN_TUNNEL_ADDR1"
                    set ipv6-pools
"SSLVPN_TUNNEL_IPv6_ADDR1"
                next
                edit 2
                    set name "Session
Information"
                    set type info
                next
                edit 3
                    set name "Bookmarks"
                    set allow-apps web ftp smb
telnet ssh vnc rdp citrix rdpnative
portforward
                next
                edit 4
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb
telnet ssh vnc rdp ping citrix rdpnative
portforward
                next
                edit 5
                    set name "Login History"
                    set type history
                next
                edit 6
                    set name "FortiClient
Download"
                    set type forticlient-download
                    set column two
                next
            end
    next
```

```
    edit "web-access"
        set allow-access web ftp smb telnet
ssh vnc rdp ping citrix rdpnative
portforward
            config widget
                edit 1
                    set name "Session
Information"
                    set type info
                next
                edit 2
                    set name "Bookmarks"
                    set allow-apps web ftp smb
telnet ssh vnc rdp citrix rdpnative
portforward
                next
            end
    next
    edit "tunnel-access"
            config widget
                edit 1
                    set name "Tunnel Mode"
                    set type tunnel
                    set split-tunneling enable
                    set ip-pools
"SSLVPN_TUNNEL_ADDR1"
                    set ipv6-pools
"SSLVPN_TUNNEL_IPv6_ADDR1"
                next
                edit 2
                    set name "Session
Information"
                    set type info
                next
            end
    next
end
config user fortitoken
    edit "FTK200317CZKRW69"
    next
end
config user local
    edit ""
        set type password
        set email-to ""
        set passwd-time 2013-09-16
16:06:09
        set passwd ENC
a6vpew3nTrEG9iGbPgMMCCGKOdqCxC
FKbxbvL5Xdtxejx2Dn/C6VGxRUVah4Gz7
4Gr0Y11NR6Q6Ujcm0/mzDG0vNqIGwzZ
LSOfg2ZqqFNP3YKWuT2CCdgnijet4/g==
    next
    edit "acceso_admin"
        set type password
        set passwd-time 2013-10-23
16:21:00
        set passwd ENC
RmgiUuiATh2vlTcCOf6b8wtvVrekUHlqtJo
SbU1M/mVOg0Z8NGB3xzw2cyVxoRuvq
WGdvuVayG4UyjDJo6CS7sYcmrn08x2wf
KHj1LuGXzsytHeUAZw==
    next
end
config user group
    edit "FSSO_Guest_Users"
        set group-type fsso-service
    next
    edit "VPN"
        set member "ttopic" "acceso_admin"
    next
end
config user device
    edit "Ruckus_Entrada"
        set mac 8c:0c:90:34:a6:e0
    next
    edit "Ruckus_Piscina"
        set mac 54:3d:37:00:ba:00
    next
end
config voip profile
    edit "default"
        set comment "default VoIP profile"
    next
    edit "strict"
            config sip
                set malformed-request-line
discard
                set malformed-header-via
discard
                set malformed-header-from
discard
                set malformed-header-to discard
                set malformed-header-call-id
discard
                set malformed-header-cseq
discard
                set malformed-header-rack
discard
                set malformed-header-rseq
discard
                set malformed-header-contact
discard
                set malformed-header-record-
route discard
                set malformed-header-route
discard
                set malformed-header-expires
discard
                set malformed-header-content-
type discard
                set malformed-header-content-
length discard
                set malformed-header-max-
forwards discard
                set malformed-header-allow
discard
                set malformed-header-p-
asserted-identity discard
                set malformed-header-sdp-v
discard
                set malformed-header-sdp-o
discard
                set malformed-header-sdp-s
discard
                set malformed-header-sdp-i
discard
                set malformed-header-sdp-c
discard
                set malformed-header-sdp-b
discard
                set malformed-header-sdp-z
discard
                set malformed-header-sdp-k
discard
                set malformed-header-sdp-a
discard
                set malformed-header-sdp-t
discard
                set malformed-header-sdp-r
discard
                set malformed-header-sdp-m
discard
            end
    next
end
config webfilter profile
    edit "default"
        set comment "default web filtering"
        set post-action comfort
            config ftgd-wf
                config filters
                    edit 1
                        set action warning
                        set category 2
                    next
                    edit 2
                        set action warning
                        set category 7
                    next
                    edit 3
                        set action warning
                        set category 8
                    next
                    edit 4
                        set action warning
                        set category 9
                    next
                    edit 5
                        set action warning
                        set category 11
                    next
                    edit 6
                        set action warning
                        set category 12
                    next
                    edit 7
                        set action warning
                        set category 13
                    next
                    edit 8
                        set action warning
                        set category 14
                    next
                    edit 9
                        set action warning
                        set category 15
                    next
                    edit 10
                        set action warning
                        set category 16
                    next
                    edit 11
                        set action warning
                    next
                    edit 12
                        set action warning
                        set category 57
                    next
                    edit 13
                        set action warning
                        set category 63
                    next
                    edit 14
                        set action warning
                        set category 64
                    next
                    edit 15
                        set action warning
                        set category 65
                    next
                    edit 16
                        set action warning
                        set category 66
                    next
                    edit 17
                        set action warning
                        set category 67
                    next
                    edit 18
                        set action block
                        set category 26
                    next
                end
            end
    next
end
config webfilter override
end
config webfilter override-user
end
config webfilter ftgd-warning
end
config webfilter ftgd-local-rating
end
config webfilter search-engine
    edit "google"
        set hostname ".*\\.google\\..*"
        set url
"^\\/((custom|search|images|videosearch|w
ebhp)\\?)"
        set query "q="
        set safesearch url
        set safesearch-str "&safe=active"
    next
    edit "yahoo"
        set hostname ".*\\.yahoo\\..*"
        set url
"^\\/search(\\/video|\\/images){0,1}(\\?|;)"
        set query "p="
        set safesearch url
        set safesearch-str "&vm=r"
    next
    edit "bing"
        set hostname "www\\.bing\\.com"
        set url
"^(\\/images|\\/videos)?(\\/search|\\/async)\\
?"
        set query "q="
        set safesearch url
        set safesearch-str "&adlt=strict"
    next
    edit "yandex"
        set hostname "yandex\\..*"
        set url
"^\\/(yand){0,1}(search)[\\/]{0,}.{0,}\\?"
```

```
        set query "text="
        set safesearch url
        set safesearch-str "&fyandex=1"
    next
    edit "youtube"
        set hostname ".*\\.youtube\\..*"
        set safesearch header
    next
    edit "baidu"
        set hostname ".*\\.baidu\\.com"
        set url "^\\/s?\\?"
        set query "wd="
    next
    edit "baidu2"
        set hostname ".*\\.baidu\\.com"
        set url "^\\/(ns|q|m|i|v)\\?"
        set query "word="
    next
    edit "baidu3"
        set hostname "tieba\\.baidu\\.com"
        set url "^\\/f\\?"
        set query "kw="
    next
end
config vpn ipsec phase1-interface
    edit "VPN-TN"
        set interface "wan1"
        set ike-version 2
        set local-gw 186.3.144.73
        set proposal 3des-sha1 aes128-sha1
                    set user acceso_admin
        set psksecret ENC
e/+UAWCmdaj+xc686u0FGHZ4kiOwK7zl
0GbYQcFzoctiiYhrxjGWU5sR8bCFqBwIn
FeVMU0psN5AcEK2IGGaGHgHmJ4P2W
1dzG9R6BmdFYOlbreYAu3/VHvZv6Q4LL
zWUIxVvA97bavtCGvcaJJfQa3m0zp1ghl2
d+/lQU82N1q/9XKMSAMkmQDz0QfYDD
H+e97Exw==
    next
end
config vpn ipsec phase2-interface
    edit "VPN-Telconet"
        set phase1name "VPN-TN"
        set proposal 3des-sha1 aes128-sha1
    next
end
config antivirus profile
    edit "default"
        set comment "scan and delete virus"
            config http
                set options scan
            end
            config ftp
                set options scan
            end
            config imap
                set options scan
            end
            config pop3
                set options scan
            end
            config smtp
                set options scan
            end
            config nntp
                set options scan
            end
            config im
                set options scan
            end
    next
end
config spamfilter profile
    edit "default"
        set comment "malware and phishing
URL filtering"
    next
end
config web-proxy global
    set proxy-fqdn "default.fqdn"
end
config firewall schedule recurring
    edit "always"
        set day sunday monday tuesday
wednesday thursday friday saturday
    next
end
config firewall profile-protocol-options
    edit "default"
        set comment "all default services"
            config http
                set ports 80
                set options no-content-summary
                unset post-lang
            end
            config ftp
                set ports 21
                set options no-content-summary
splice
            end
            config imap
                set ports 143
                set options fragmail no-content-
summary
            end
            config mapi
                set ports 135
                set options fragmail no-content-
summary
            end
            config pop3
                set ports 110
                set options fragmail no-content-
summary
            end
            config smtp
                set ports 25
                set options fragmail no-content-
summary splice
            end
            config nntp
                set ports 119
                set options no-content-summary
splice
            end
            config im
                unset options
            end
            config dns
                set ports 53
            end
    next
end
config firewall deep-inspection-options
    edit "default"
        set comment "all default services"
            config https
                set ports 443
            end
            config ftps
                set ports 990
            end
            config imaps
                set ports 993
            end
            config pop3s
                set ports 995
            end
            config smtps
                set ports 465
            end
    next
end
config firewall identity-based-route
end
config firewall policy
    edit 1
        set srcintf "Voz"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 2
        set srcintf "Usuarios"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 3
        set srcintf "Switches"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 4
        set srcintf "Servidores"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 5
        set srcintf "Dispositivos"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 6
        set srcintf "Usuarios"
        set dstintf "Dispositivos"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 7
        set srcintf "Voz"
        set dstintf "wan2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 8
        set srcintf "Usuarios"
        set dstintf "wan2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 9
        set srcintf "Switches"
        set dstintf "wan2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 10
        set srcintf "Servidores"
        set dstintf "wan2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 11
```

```
        set srcintf "Dispositivos"
        set dstintf "wan2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 12
        set srcintf "wan1"
        set dstintf "ssl.PROTECTED"
        set srcaddr "all"
        set dstaddr "Servidores"
        set action ssl-vpn
        set identity-based enable
            config identity-based-policy
                edit 1
                    set schedule "always"
                    set groups "VPN"
                    set service "ALL"
                    set sslvpn-portal "tunnel-
access"
                next
            end
    next
    edit 13
        set srcintf "ssl.PROTECTED"
        set dstintf "Servidores"
        set srcaddr
"SSLVPN_TUNNEL_ADDR1"
        set dstaddr "Servidores"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 14
        set srcintf "Voz"
        set dstintf "VPN-TN"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 15
        set srcintf "VPN-TN"
        set dstintf "Voz"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
config firewall local-in-policy
end
config firewall policy6
end
config firewall local-in-policy6
end
config firewall ttl-policy
end
config firewall policy64
end
config firewall policy46
end
config firewall interface-policy
end
config firewall interface-policy6
end
config firewall sniff-interface-policy
end
config firewall sniff-interface-policy6
end
config firewall DoS-policy
end
config firewall DoS-policy6
end
config firewall sniffer
end
config endpoint-control profile
    edit "default"
        config forticlient-winmac-settings
            set forticlient-av enable
            set forticlient-wf enable
            set forticlient-wf-profile "default"
            set forticlient-ui-options av wf af
vpn vs
        end
        config forticlient-android-settings
            set forticlient-wf enable
            set forticlient-wf-profile "default"
        end
        config forticlient-ios-settings
            set forticlient-wf enable
            set forticlient-wf-profile "default"
        end
    next
end
config wireless-controller wids-profile
    edit "default"
        set comment "default wids profile"
        set wireless-bridge enable
        set deauth-broadcast enable
        set null-ssid-probe-resp enable
        set long-duration-attack enable
        set invalid-mac-oui enable
        set weak-wep-iv enable
        set auth-frame-flood enable
        set assoc-frame-flood enable
        set spoofed-deauth enable
        set asleap-attack enable
        set eapol-start-flood enable
        set eapol-logoff-flood enable
        set eapol-succ-flood enable
        set eapol-fail-flood enable
        set eapol-pre-succ-flood enable
        set eapol-pre-fail-flood enable
    next
end
config wireless-controller wtp-profile
    edit "FAP112B-default"
            config platform
                set type 112B
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
    next
    edit "FAP220B-default"
        set ap-country US
            config radio-1
                set band 802.11n-5G
            end
            config radio-2
                set band 802.11n
            end
    next
    edit "FAP223B-default"
            config platform
                set type 223B
            end
        set ap-country US
            config radio-1
                set band 802.11n-5G
            end
            config radio-2
                set band 802.11n
            end
    next
    edit "FAP210B-default"
            config platform
                set type 210B
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
    next
    edit "FAP222B-default"
            config platform
                set type 222B
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set band 802.11n-5G
            end
    next
    edit "FAP320B-default"
            config platform
                set type 320B
            end
        set ap-country US
            config radio-1
                set band 802.11n-5G
            end
            config radio-2
                set band 802.11n
            end
    next
    edit "FAP11C-default"
            config platform
                set type 11C
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
    next
    edit "FAP14C-default"
            config platform
                set type 14C
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
    next
    edit "FAP28C-default"
            config platform
                set type 28C
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
    next
    edit "11n-only"
            config platform
                set type 60C
            end
        set ap-country US
            config radio-1
                set band 802.11n
            end
            config radio-2
                set mode disabled
            end
    next
end
config router rip
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "ospf"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
end
config router ripng
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "ospf"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
end
config router static
```

```
    edit 2
        set device "wan2"
        set gateway 206.165.205.129
    next
    edit 3
        set device "ssl.PROTECTED"
        set dst 10.212.134.0 255.255.255.0
    next
    edit 4
        set device "wan1"
        set gateway 186.3.144.65
    next
    edit 5
        set device "VPN-TN"
        set dst 172.24.4.8 255.255.255.255
    next
    edit 6
        set device "VPN-TN"
        set dst 10.55.192.0 255.255.248.0
    next
end
config router ospf
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
end
config router ospf6
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
end
config router bgp
        config redistribute "connected"
        end
        config redistribute "rip"
        end
        config redistribute "ospf"
        end
        config redistribute "static"
        end
        config redistribute "isis"
        end
        config redistribute6 "connected"
        end
        config redistribute6 "rip"
        end
        config redistribute6 "ospf"
        end
        config redistribute6 "static"
        end
        config redistribute6 "isis"
        end
end
config router isis
        config redistribute "connected"
        end
        config redistribute "rip"
        end
        config redistribute "ospf"
        end
        config redistribute "bgp"
        end
        config redistribute "static"
        end
end
config router multicast
end
config router gwdetect
    edit 1
        set failtime 2
        set interface "wan1"
        set interval 2
        set server "200.93.195.1"
    next
    edit 2
        set failtime 2
        set interface "wan2"
        set interval 2
        set server "200.93.195.1"
    next
end
end
```

ANEXO 2. STARTUP CONFIG DEL ROUTER CISCO

1941 SERIES

```
Current configuration : 7531 bytes
!
! Last configuration change at 09:45:56
ECT Fri Nov 1 2013 by iac
! NVRAM config last updated at 09:45:57
ECT Fri Nov 1 2013 by iac
! NVRAM config last updated at 09:45:57
ECT Fri Nov 1 2013 by iac
version 15.1
service timestamps debug datetime
localtime
service timestamps log datetime localtime
service password-encryption
no service dhcp
!
hostname ttopic-lagunadorada
!
boot-start-marker
boot-end-marker
!
!
logging buffered 4096
no logging console
enable secret 4
rt3HX0VBJOemy86n2AWnj3WihhGQvgVq
eGyTG7rFrlU
!
no aaa new-model
clock timezone ECT -5 0
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
ip dhcp pool ccp-pool
 import all
 network 10.10.10.0 255.255.255.248
 default-router 10.10.10.1
 lease 0 2
!
!
ip domain name telconet.net
ip name-server 200.93.192.148
ip name-server 200.1.110.1
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-
497965151
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-
Certificate-497965151
 revocation-check none
 rsakeypair TP-self-signed-497965151
!
!
crypto pki certificate chain TP-self-signed-
497965151
 certificate self-signed 01
69666963 6174652D 34393739 36353135
31301E17 0D313330 32313132 32353333
  335A170D 32303031 30313030
30303030 5A303031 2E302C06
03550403 1325494F
  532D5365 6C662D53 69676E65
04D9B889 24CB37AD
  46A0DE70 903A5BE7 40D0703E
B93F110C 81FAC275 FA231018
90BAC21F 30D78074
  F839B71E 9EB833FC 47FFEDD4
  02030100 01A35330 51300F06
D36C4B30 1D060355
  1D0E0416 0414744E 65E75448
7A5473F5 9E87D9F7 6397D5D3
C8752211 3B9855FC
  746CF697 AD455047 FB8F165A
C6822C89 7ECA4C28 C6220F8C
1CD58664 F6C1CCE8
  767437F8 A77F3DC9 77EB4782
E538CDC2 950BC0DE 0D69081D
864BB40B F58A5C89
  9B3C07BB 3005F51D DB6C9A79
613BDBC1 BD457BA8 5D9EF7D1
11A83347 FFB2EAA4
  2B0AB1FF D1004116 DB109C07 6A
      quit
license udi pid CISCO1941/K9 sn
FTX170780KA
!
!
username telcuio privilege 10 secret 1
9aWRoELyLs22dPAAw29knXOcyE
username tlc privilege 10 secret 1
.lxTOy.lg2udJeAgw61c96vMmMHU
username standbyc privilege 10 secret 1
ojfMcP2L8YeleOVpHNObJeBVLM
username iac privilege 10 secret 1
rt3HX0Wnj3WihhGQvgVqeGyTG7rFrlU
username ttopic privilege 10 secret 1
lpufq745ar4cDBC.As/wKo0zfMOr7UZ6
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description LAN-FGT80C
 ip address 206.165.205.129
255.255.255.248 secondary
 ip address 181.198.70.153
255.255.255.248
 no ip redirects
 no ip proxy-arp
 ip virtual-reassembly in
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0
 ip address 181.198.53.147 255.255.255.0
 ip access-group PROTECTED out
 no ip redirects
 no ip proxy-arp
 ip virtual-reassembly in
 load-interval 30
 no cdp enable
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 181.198.53.1
!
ip access-list extended PROTECTED
 deny   tcp any any eq 135
 deny   tcp any any eq 139
 deny   tcp any any eq 445
 deny   udp any any eq netbios-ns
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 permit ip any any
!
access-list 1 permit 200.110.89.254
access-list 1 permit 200.93.195.82
access-list 1 permit 200.93.195.81
access-list 1 permit 10.10.10.5
access-list 1 permit 200.93.221.82
access-list 1 permit 206.165.205.130
access-list 1 permit 201.218.18.40
access-list 1 permit 200.93.221.125
access-list 1 permit 200.93.221.126
access-list 1 permit 200.93.195.109
access-list 1 permit 200.93.195.22
access-list 1 permit 200.93.222.11
access-list 1 permit 200.93.195.21
access-list 1 permit 200.93.221.15
access-list 1 permit 200.93.194.30
access-list 1 permit 200.93.216.29
access-list 1 permit 200.93.219.27
access-list 1 permit 200.93.219.24
access-list 1 permit 200.93.195.131
access-list 1 permit 200.93.195.184
access-list 1 permit 200.110.72.30
access-list 1 permit 200.93.192.166
access-list 1 permit 200.110.72.29
access-list 1 permit 200.110.72.25
access-list 1 permit 200.93.192.171
access-list 1 permit 200.93.195.169
access-list 1 remark
ACCESOS_NACIONAL
access-list 1 permit 190.95.165.0
0.0.0.255
access-list 1 permit 201.218.38.0
0.0.0.255
access-list 98 permit 200.93.216.92
access-list 98 permit 200.93.221.82
access-list 98 permit 201.218.2.13
access-list 98 permit 200.93.221.125
access-list 98 permit 200.93.221.126
access-list 98 permit 200.93.195.21
access-list 98 permit 200.93.221.15
access-list 98 permit 200.93.220.23
access-list 98 permit 200.93.216.38
access-list 98 permit 200.110.95.150
access-list 98 permit 201.218.15.156
access-list 98 permit 200.93.18.40
access-list 98 permit 200.93.192.236
access-list 98 permit 200.93.192.235
access-list 98 permit 200.93.192.234
access-list 98 permit 200.93.192.150
access-list 98 permit 200.93.192.162
access-list 98 permit 200.110.72.25
access-list 98 permit 200.93.192.171
access-list 98 remark SNMP_NACIONAL
access-list 98 permit 190.95.165.0
0.0.0.255
access-list 98 permit 201.218.38.0
0.0.0.255
!
!
snmp-server community $3.v/q/$ RO 98
!
control-plane
!
!
banner login ^C
**************************************************
***************
Acceso Restringido a Personal autorizado
**************************************************
***************
Violaciones a este sistema estan
penalizadas en
la Ley de Comercio Electronico
Ecuatoriana y demas
Leyes Internacionales
**************************************************
***************^C
!
line con 0
 login local
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta
mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class 1 in
 privilege level 15
 login local
 transport input ssh
line vty 5 5
 access-class 1 in
 privilege level 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
ntp server 200.93.192.169
end
```

ANEXO 3. STARTUP CONFIG DEL SWITCH

CATALYST #1

```
Using 5911 out of 524288 bytes
!
! NVRAM config last updated at 13:08:17
EC Thu Jul 17 2014 by cert
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sw1casattopic
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$RJ04$0bFsBXIUDb
!
username cert privilege 15 secret 5
$1$JJ4S$DHVpLINle/Cd0
username ttopic privilege 15 secret 5
$1$TDMu$OSu3vRfh.a0
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
aaa session-id common
clock timezone EC -5
switch 1 provision ws-c2960s-48fpd-l
!
!
!
!
crypto pki trustpoint TP-self-signed-
2313135872
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-
Certificate-2313135872
 revocation-check none
 rsakeypair TP-self-signed-2313135872
!
!
crypto pki certificate chain TP-self-signed-
2313135872
 certificate self-signed 01 nvram:IOS-Self-
Sig#3232.cer
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport access vlan 30
!
interface GigabitEthernet1/0/3
 switchport access vlan 30
!
interface GigabitEthernet1/0/4
 switchport access vlan 11
!
interface GigabitEthernet1/0/5
 switchport access vlan 11
!
interface GigabitEthernet1/0/6
 switchport access vlan 11
!
interface GigabitEthernet1/0/7
 switchport access vlan 11
!
interface GigabitEthernet1/0/8
 switchport access vlan 50
!
interface GigabitEthernet1/0/9
 switchport access vlan 50
!
interface GigabitEthernet1/0/10
 switchport access vlan 50
!
interface GigabitEthernet1/0/11
 switchport access vlan 50
!
interface GigabitEthernet1/0/12
 switchport access vlan 50
!
interface GigabitEthernet1/0/13
 switchport trunk native vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/14
 switchport trunk native vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport trunk native vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/16
 switchport trunk native vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 switchport trunk native vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/18
 switchport trunk native vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/19
 switchport access vlan 50
!
interface GigabitEthernet1/0/20
 switchport access vlan 50
!
interface GigabitEthernet1/0/21
 switchport access vlan 50
!
interface GigabitEthernet1/0/22
 switchport access vlan 50
!
interface GigabitEthernet1/0/23
 switchport access vlan 50
!
interface GigabitEthernet1/0/24
 switchport access vlan 50
!
interface GigabitEthernet1/0/25
 switchport access vlan 50
!
interface GigabitEthernet1/0/26
 switchport access vlan 50
!
interface GigabitEthernet1/0/27
 switchport access vlan 50
!
interface GigabitEthernet1/0/28
 switchport access vlan 50
!
interface GigabitEthernet1/0/29
 switchport access vlan 50
!
interface GigabitEthernet1/0/30
 switchport access vlan 50
!
interface GigabitEthernet1/0/31
 switchport access vlan 50
!
interface GigabitEthernet1/0/32
 switchport access vlan 50
!
interface GigabitEthernet1/0/33
 switchport access vlan 50
!
interface GigabitEthernet1/0/34
 switchport access vlan 50
!
interface GigabitEthernet1/0/35
 switchport access vlan 50
!
interface GigabitEthernet1/0/36
 switchport access vlan 50
!
interface GigabitEthernet1/0/37
 switchport access vlan 50
!
interface GigabitEthernet1/0/38
 switchport access vlan 50
!
interface GigabitEthernet1/0/39
 switchport access vlan 50
!
interface GigabitEthernet1/0/40
 switchport access vlan 50
!
interface GigabitEthernet1/0/41
 switchport access vlan 50
!
interface GigabitEthernet1/0/42
 switchport access vlan 50
!
interface GigabitEthernet1/0/43
 switchport access vlan 50
!
interface GigabitEthernet1/0/44
 switchport access vlan 50
!
interface GigabitEthernet1/0/45
 switchport access vlan 50
!
interface GigabitEthernet1/0/46
 switchport trunk native vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/47
 switchport trunk native vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/48
 switchport trunk native vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
!
interface Vlan40
 ip address 172.31.0.2 255.255.255.240
!
ip default-gateway 172.31.0.1
no ip http server
no ip http secure-server
!
line con 0
line vty 5 15
!
ntp server 200.93.192.169
end
```

ANEXO 4. STARTUP CONFIG DEL SWITCH

CATALYST #2, #3 Y #4

```
Using 4306 out of 524288 bytes
!
! Last configuration change at 13:08:51 EC Thu Jul 17 2014 by cert
! NVRAM config last updated at 13:08:56 EC Thu Jul 17 2014 by cert
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sw2casattopic
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$RJ04$0bFsBWkdA3yYh1
!
username cert privilege 15 secret 5 $1$JJ4S$O9BINle/Cd0
username ttopic privilege 15 secret 5 $1$TDMu$OQZA3vRfh.a0
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
aaa session-id common
clock timezone EC -5
switch 1 provision ws-c2960s-48fpd-l
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 30
!
interface GigabitEthernet1/0/2
 switchport access vlan 30
!
interface GigabitEthernet1/0/3
 switchport access vlan 30
!
interface GigabitEthernet1/0/4
 switchport access vlan 11
!
interface GigabitEthernet1/0/5
 switchport access vlan 11
!
interface GigabitEthernet1/0/6
 switchport access vlan 11
!
interface GigabitEthernet1/0/7
 switchport access vlan 11
!
interface GigabitEthernet1/0/8
 switchport access vlan 50
!
interface GigabitEthernet1/0/9
 switchport access vlan 50
!
interface GigabitEthernet1/0/10
 switchport access vlan 50
!
interface GigabitEthernet1/0/11
 switchport access vlan 50
!
interface GigabitEthernet1/0/12
 switchport access vlan 50
!
interface GigabitEthernet1/0/13
 switchport access vlan 50
!
interface GigabitEthernet1/0/14
 switchport access vlan 50
!
interface GigabitEthernet1/0/15
 switchport access vlan 50
!
interface GigabitEthernet1/0/16
 switchport access vlan 50
!
interface GigabitEthernet1/0/17
 switchport access vlan 50
!
interface GigabitEthernet1/0/18
 switchport access vlan 50
!
interface GigabitEthernet1/0/19
 switchport access vlan 50
!
interface GigabitEthernet1/0/20
 switchport access vlan 50
!
interface GigabitEthernet1/0/21
 switchport access vlan 50
!
interface GigabitEthernet1/0/22
 switchport access vlan 50
!
interface GigabitEthernet1/0/23
 switchport access vlan 50
!
interface GigabitEthernet1/0/24
 switchport access vlan 50
!
interface GigabitEthernet1/0/25
 switchport access vlan 50
!
interface GigabitEthernet1/0/26
 switchport access vlan 50
!
interface GigabitEthernet1/0/27
 switchport access vlan 50
!
interface GigabitEthernet1/0/28
 switchport access vlan 50
!
interface GigabitEthernet1/0/29
 switchport access vlan 50
!
interface GigabitEthernet1/0/30
 switchport access vlan 50
!
interface GigabitEthernet1/0/31
 switchport access vlan 50
!
interface GigabitEthernet1/0/32
 switchport access vlan 50
!
interface GigabitEthernet1/0/33
 switchport access vlan 50
!
interface GigabitEthernet1/0/34
 switchport access vlan 50
!
interface GigabitEthernet1/0/35
 switchport access vlan 50
!
interface GigabitEthernet1/0/36
 switchport access vlan 50
!
interface GigabitEthernet1/0/37
 switchport access vlan 50
!
interface GigabitEthernet1/0/38
 switchport access vlan 50
!
interface GigabitEthernet1/0/39
 switchport access vlan 50
!
interface GigabitEthernet1/0/40
 switchport access vlan 50
!
interface GigabitEthernet1/0/41
 switchport access vlan 50
!
interface GigabitEthernet1/0/42
 switchport access vlan 50
!
interface GigabitEthernet1/0/43
 switchport access vlan 50
!
interface GigabitEthernet1/0/44
 switchport access vlan 50
!
interface GigabitEthernet1/0/45
 switchport access vlan 50
!
interface GigabitEthernet1/0/46
 switchport access vlan 50
!
interface GigabitEthernet1/0/47
 switchport access vlan 50
!
interface GigabitEthernet1/0/48
 switchport trunk native vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan40
 ip address 172.31.0.3 255.255.255.240
!
ip default-gateway 172.31.0.1
no ip http server
no ip http secure-server
!
line con 0
line vty 5 15
!
ntp server 200.93.192.169
end
```